iPECS SBG-1000 User Manual
(IP-PBX Features)

Revision History

ISSUE	DATE	DESCRIPTION OF CHANGES
1.0	2011, August	Initial Release

Table Of Contents

1. INTRODUCTION

1.1 OVERVIEW

Smart Business gateway (iPECS SBG-1000) is LG-Ericsson's internet Protocol (iP) Enterprise Communications Solution designed to meet the telecommunication needs of small-sized business. Smart Business gateway uses advanced packet voice and IP switching technology, which is combined with a rich feature content, to set a new standard in Voice over IP (VoIP) systems.

The system consists of basic one FXS port, eight 10/100 Base-T LAN Ethernet ports (including four POE ports) and one Wan Ethernet port, one USB port. iPECS SBG-1000 is installed on the desk and powered from an AC/DC adapter, which converts 100~240VAC to 48VDC. With optional board, the system can have one/two FXO ports or one BRI port additionally and FXS can be increased two ports.

iPECS SBG-1000 supports a variety of Phones; LIP Phones using iPECS Protocol, SIP Terminals (WIT-400H, 88xx), and analog single-line devices. With the LIP Phones, commonly-used features are activated with the touch of a single button. Additionally, most functions can be accessed from any telephone by dialing specific codes.

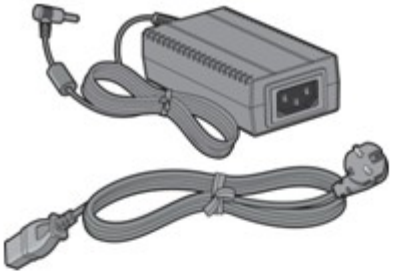
Providing an environment rich in features, in addition to a fully featured voice intercom, the iPECS SBG-1000 incorporates built-In Auto-Attendant (AA) and Voice Mail (VM), Remote Management such as Web Based Admin.

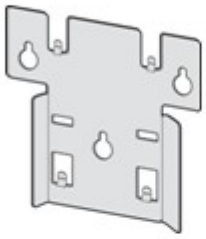
By employing packet voice and IP switching, the iPECS SBG-1000 infrastructure can be employed for, or can share the enterprise data network. Further, since all terminals have a unique IP address, they can be moved anywhere with access to a network that can connect to iPECS SBG-1000 and function without the need for "re-programming". The use of the single common infrastructure and ability to easily install or relocate telephones results in significant savings from the time of installation and throughout the life of the system.

1.2 HARDWARE COMPONENTS

iPECS SBG-1000 is shipped with the iPECS SBG-1000 module, a power adaptor and a power cord as shown in Figure 1.2-1.


iPECS SBG-1000

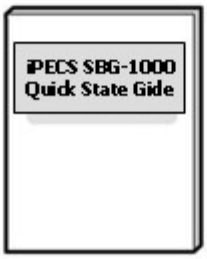

Adapter & Power Cord


Wall Mount Bracket


Insert & Screw

CD manual


Cable Ties



Quick Start Guide

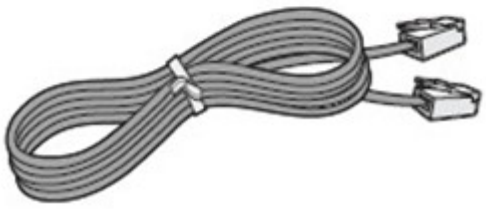

LAN Cable

Figure 1.2-1 Components in iPECS SBG-1000 package

To obtain terminal options with iPECS SBG-1000, contact an authorized agent of LG-Ericsson Co., Ltd.

Table 1.2-1 iPECS SBG-1000 products

No.	Product	Description	Remark
1	Smart Business gateway	Smart Business gateway Gateway Module	Basic
2	AC/DC Adaptor	AC/DC Adaptor for module, (48VDC, 0.8A)	Basic
3	AC Power Cord	AC power cord for an Adaptor	Basic
4	LIP Phones	LG-Ericsson LIP Phones using iPECS protocol	Option
5	SIP Terminals	LIP-8002, IP-DECT, Dual Mode Wireless Phones	Option
6	POTS Terminals	analogue single line devices	Option
7	DECT Phones	LG-Ericsson System DECT Phones	Option

1.3 MANUAL APPLICATION

This document provides detailed information covering description and operation of the numerous features available in the iPECS SBG-1000 system software. The document is written assuming the system employs the default numbering plan.

1.3.1 Organization

Features are arranged in two different major groupings as follows:

- Section 2 Call Features
- Section 3 Web Administration

1.3.2 Feature Information

Each section is an alphabetical listing of features with the description and operation of each. The structure is divided into 6 parts as below:

- **Description:** explains the nature of the feature.
- **Operation:** gives detailed step-by-step operation of the feature for Keysets and SLTs.
- **Conditions:** explains known feature interactions and constraints related to the feature.
- **Programming:** lists database entries that may be required for proper feature operation.
- **Reference:** lists related topical information to aid in understanding the feature.
- **Hardware:** lists hardware required for proper feature operation.

1.4 SYSTEM CAPACITIES

The iPECS SBG-1000 is presently available in one configuration as shown in the Table 1.4-1.

Table 1-4-1 Smart Business gateway Capacity Chart

DESCRIPTION		CAPACITY
		Smart Business gateway – iPECS SBG-1000
Stations	IP Extension	11 / 23[1)]
	FXS (FAX, SLT)	1 / 2[2)]
	SIP Extension	6
	DECT	6[3)]
	Total	12 / 24[1)]

DESCRIPTION		CAPACITY
		Smart Business gateway – iPECS SBG-1000
VoIP channel		3 / 4 / 6[1)]
FXO port (Analog trunk)		0 / 1 / 2[2)]
BRI port		0 / 1[2)]
Auto Attendant channels		4
Attendants		1
PFT		1[4)]
USB Host Port		1
Paging Zones		10
Common Speed Dial		800 (23 digits)
Individual Speed Dial		20 (23 digits)
Last Number Redial		15 (23 digits)
Save Number Redial		1 (23 digits)
SMDR Buffer		5000
Station Groups		10
Station Group Members		12 / 24[1)]
Authorization Codes	Station	12 / 24[1)]
	System	100
Voice Mail Box		240 / 480 minutes[5)]

1) Capacity S/W license decides the number of total stations and the maximum available number of VoIP channel.

Capacity S/W License	DECT Usage	Total Stations	VoIP Channel
Normal	OFF	12	3
	OFF	24	6
Extended	ON	12	3
	ON	24	4

2) Basic iPECS SBG-1000 has only 1 FXS port and FXS, FXO and BRI port capacity depends on the optional board as follows.

Optional Board	FXS	FXO	BRI
CSIU	Basic 1 + 1 = 2	1	0
CIU1	Basic 1	1	0
CIU2	Basic 1	2	0
BRIU	Basic 1	0	1

3) Up to six (6) DECT stations can be registered but only four (4) DECT stations can place a call or get a ring simultaneously.
4) PFT is connected to FXO LINE1 and it works only with CSIU, CIU1 and CIU2.
5) The capacity for Voice Mail Box depends on the lock key for the VSF Memory Extend.

1.5 HARDWARE DESCRIPTION

iPECS SBG-1000 can be mounted on any flat surface itself. The external AC/DC adaptor (48Vdc /0.8A) feeds power to the System. iPECS SBG-1000 includes battery back-up circuitry using a long-life Lithium battery to maintain the real-time clock and prevent loss of system database during power fail.

Connection ports

- In the right side
  - One WAN port (RJ-45: 10/100/1000 Base-T Ethernet port)
  - 8 LAN ports (RJ-45: 10/100 Base-T Ethernet port)
  - One basic FXS port (RJ-45)
  - One MISC port for Relay Contact and Alarm Detection
  - 48 VDC Power Input Jack
- In the left side
  - One USB Port in the left side

Buttons

- In the right side
  - Reset to Default button
- In the left side
  - WPS (WiFi Protect Setup) button
  - Reset button

Indicators

The following LAN LEDs provide visual representation of iPECS SBG-1000 LAN ports activities and status in normal state.

Table 1.5-1 iPECS SBG-1000 LAN Activities and Status

Name	LED Color	Status	Description
LINK/ACT	Green	ON	Valid LAN Link
		OFF	Link Fail
		FLASH	TX/RX Activity
10/100	Orange	ON	100 Mbps
		OFF	10 Mbps

The following WAN LEDs provide visual representation of iPECS SBG-1000 WAN port activities and status in normal state.

Table 1.5-2 iPECS SBG-1000 WAN Activities and Status

Name	LED Color	Status	Description
LINK	Green	ON	Valid LAN Link
		OFF	Link Fail
ACT	Orange	ON	100 Mbps
		OFF	10 Mbps

Status LEDs on the top panel indicate operation states of the iPECS SBG-1000 as shown in below Table 1.5-3.

Table 1.5-3 iPECS SBG-1000 Operation States

Icon	Name	LED Color	Status	Description
	POWER	Blue	ON	Power On
			OFF	No Power
	WAN	Pure Green	ON	Valid WAN Link
			OFF	WAN Link Fail
	WLAN	Pure Green	ON	WLAN is Running
			OFF	WLAN is Not Initialized
			BLINK	WPS is in progress
	PBX	Pure Green	BLINK	Call Task is Running
			ON/OFF	Call Task Not Initialized

1.6 SPECIFICATIONS

Environmental Specification		
	Degrees (℃)	**Degrees (°F)**
Operation Temperature	0 ~ 40	32 ~ 104
Optimum Operation Temperature	20 ~ 26	68 ~ 78
Storage Temperature	0 ~ 70	32 ~ 158
Relative Humidity	0~80% RH non-condensing	

Power Adaptor Specification*	
AC Input	AC100-240V, 50/60Hz, 1A max.
DC Output	DC48V, 0.8A max

** A Power adaptor is delivered with Smart Business gateway.*

FXS Specification (Basic SLT or CSIU)		
Connector	RJ-45	
Loop Distance	1.5 Km	AWG #24 (0.5mm)
Ring Capacity	60Vrms (up to 3 REN)	
Ring Frequency	25Hz	

FXO Specification (CIU1, CIU2 or CSIU)	
Connector	RJ-45
REN (Ringer Equivalent Number)	0.7B

Ethernet Specification (LAN port 1 ~ LAN port 8)	
Connector	RJ-45 shielded
LAN Interface	10/100 BASE-T (Auto-Negotiation), 10 Mbps or 100 Mbps, IEEE 802.3
Maximum Wiring Distance Cable	100 m/ 0.328kft, Category 5 UTP cable

Ethernet Specification (WAN port)	
Connector	RJ-45 shielded
WAN Interface	10/100/1000 BASE-T (Auto-Negotiation), 10 Mbps or 100 Mbps or 1000 Mbps, IEEE 802.3/ IEEE 802.3ab/ IEEE 802.3az
Maximum Wiring Distance Cable	100 m/ 0.328kft, Category 5e UTP cable for 1000 Mbps

PoE Specification (LAN port 1 ~ LAN port 4 only, LAN port 5 ~ LAN port 8 are not supported)	
Interface specification	IEEE 802.3af (Total budgets : 20 W)

WiFi Specification	
Interface specification/ Frequency	IEEE 802.11 b/g/n (Draft 2.0), 2x2 MIMO, 2.412GHz ~ 2.472GHz

DECT Specification (WiFi Version – not supported)	
Interface specification	CAT-iq 2.0, DECT 6.0
Frequency	1,880MHz ~ 1,900MHz for Europe, 1,920MHz ~ 1,930MHz for US

USB Specification	
Connector	USB Female Plug type A
Mode	Host V 1.1 / 2.0

Physical Specification		
W x D x H	278 x 233 x 34 mm	10.94 x 9.17 x 1.34 in
Weight (with CIU1 back-up)	860.5g	1.90 lbs

2. CALL FEATURES

2.1 SYSTEM TIME

2.1.1 LCD Date/Time Format Control

Description

The Attendant can select the format of the time and date provided to the LCD of all LIP Phones in the system.

The Attendant can select (toggle between) two formats for both time and date. The formats are:

- Date: Month/day/year or Year/month/date
- Time: 12 hour or 24 hour (military)

Operation

Attendant

To Change LCD Date Format (toggle):

1. Press the **[PGM]** button.
2. Dial '021' (Date Display Format program code).

To Change LCD Time Format (toggle):

1. Press the **[PGM]** button.
2. Dial '022' (Time Display Format program code).

Conditions

Programming

Related Features

Attendant Position

Hardware

2.1.2 Auto Service Mode Control

Description

The service mode defines different ring assignments and answering privileges for the system. The service mode can be controlled automatically through definitions in the Day/Night/Timed Mode

Table, which defines the time of day for the Day, Night and Timed shift modes. The Attendant may change the system mode selection from automatic to manual.

Operation

System
Operation of this feature is automatic.

Conditions

Programming

VOICE CONFIG System Data – Day/Night/Timed Schedule

Related Features

Off-Hook Signaling
Day/Night/Timed Ring Mode
CO Ring Assignment

Hardware

2.1.3 Day/Night/Timed Ring Mode

Description

The Ring Mode is controlled automatically by the system clock. Ring assignments are applied based on the time of day and day of week. Three modes of ring (Ring Assignments) are provided, Day, Night and Timed.

The Attendant controls the system Ring Service mode changing from Auto Service Mode to Day, Night or Timed service mode. Based on the service mode selected, different ring assignments, answering privileges are invoked for system users.

Operation

Attendant
To change Day/Timed/Night Ring Mode manually;

1. Press the **[DND]** button.
2. Dial 1~4. (1: Day mode, 2: Night mode, 3: Timed mode, 4: Auto Service mode)
3. Press **[HOLD/SAVE]** button.

Conditions

1. Only Attendants can change Day/Timed/Night Ring Mode for the system manually and program the Auto Ring Mode Selection Table.

2. Stations receive incoming ring for CO lines based on database assignment and the system mode (Day/Night/Timed) when the call arrives.
3. When the Day/Night/Timed Mode Table is programmed, the ring is changed automatically based on the times assigned in the table.
4. The Attendant always has manual control of System mode by enabling/disabling the Auto Service Mode Control.

Programming

VOICE CONFIG CO Line Data – Call Routing by Line
CO Line Data – Ring Assignment Table
System Data – Day/Night/Timed Schedule

Related Features

CO Ring Assignment

Hardware

2.2 CALL FORWARD

Description

Users may have selected incoming calls re-routed to other stations, station groups, the VSF, or over a system CO line (Off-Net).

The user selects the type and condition under which calls are to be forwarded by entering a Call Forward code as follows:

- Code 0: Remote Call Forward; forwards all calls to the station, except recalls, activated from a remote station, Call Forward, Follow-me.
- Code 1: Unconditional; all calls to the station, except recalls, are forwarded internally or externally immediately upon receipt.
- Code 2: Busy; if the station is busy, forwards all calls, except recalls, to the selected station.
- Code 3: No Answer; forwards all calls, except recalls, to the selected station when the station does not answer within the No Answer timer.
- Code 4: Busy/No Answer; forwards calls if the selected station is busy or does not answer within the No Answer timer.
- Code 6: Off-Net Unconditional; all calls to the station, except recalls, are forwarded internally or externally (SLT only).
- Code 7: Off Net Busy; forwards all calls, except recalls, to the selected station when station is busy (SLT only).

- Code 8: Off Net No Answer; forwards all calls, except recalls, to the selected station when the station does not answer within the No Answer timer (SLT only).
- Code 9: Off Net Busy/No Answer; forwards calls if the selected station is busy or does not answer within the No Answer timer (SLT only).

Operation

LIP Phone

To activate Call Forward, Unconditional or Busy/No Answer:

1. Lift the handset or press the **[SPEAKER]** button to receive dial tone.
2. Press the **[FWD]** button.
3. Dial desired Call Forward code (1-4).
4. Dial the station or station group to receive calls.
5. Replace the handset, return to idle.

To activate Call Forward, Off Premise (to an external number):

1. Lift the handset or press the **[SPEAKER]** button to receive dial tone.
2. Press the **[FWD]** button.
3. Dial Forward condition (1-4)
4. Press **[SPEED]** button and desired bin number.
5. Replace the handset, return to idle.

To activate Call Forward, Remote (Follow-me):

1. Lift the handset or press **[SPEAKER]** button to receive dial-tone
2. Press the **[FWD]** button,
3. Dial Call Forward code '0',
4. Dial the station's Authorization Code (Station number + password),
5. Dial Forward condition (1-4),
6. Dial the destination station or station group,
7. Replace the handset, return to idle.

To deactivate Call forward:

1. Press flashing **[FWD]** button, Call Forward will deactivate and the **[FWD]** button LED is off.

SLT

To activate Call Forward, Unconditional, Busy/No Answer to an internal number:

1. Lift the handset to receive dial tone.
2. Dial 54 (Call Forward code).
3. Dial desired Call Forward code (1-4).
4. Dial station or station group to receive the calls.
5. Replace the handset, return to idle.

To activate Call Forward, to an external number:

1. Lift the handset to receive dial tone.
2. Dial 54 (Call Forward code).
3. Dial Call Forward code (6-9),

4. Dial Speed Dial bin number.
5. Replace handset to return to idle.

To activate Call Forward, Remote (Follow-me):

1. Lift the handset.
2. Dial 54 (Call Forward code).
3. Dial Remote Forward code '0'
4. Dial the station's Authorization Code (Station + Password),
5. Dial Forward condition (1-4)
6. Dial the destination station or station group.
7. Replace handset return to idle.

To deactivate the Call forward:

1. Lift the handset, receive stutter dial-tone,
2. Dial 54 (Call Forward code).
3. Dial '#' to cancel Call Forward.

Conditions

1. A station receiving a forwarded call can transfer the call to the forwarding station.
2. A forwarded intercom call will signal the receiving station in the Tone Signaling mode, regardless of the Intercom Signaling Mode at the station.
3. Calls cannot be forwarded to a station in DND; if attempted, an error tone is returned.
4. Active Call Back or Queue requests are not canceled when attempting to activate Call Forward.
5. When Call Forward is active, a station can make outgoing calls (internal or external) but cannot activate a Call back or Queue request.
6. For CO calls, manually activated Call Forward will override any Preset Call Forward assigned for the station or CO line.
7. Call Forward status is maintained in the system's non-volatile memory for protection from power outage.
8. A station in a Station Hunt Group (Circular or Terminal) can be assigned to receive incoming hunt calls, overriding any Call Forward (the system either recognizes the Forward condition and bypasses hunt calls around the station, or routes hunt calls to the station based on the system database; Member Forward).
9. Off-Net Call Forward of incoming CO calls is essentially an automated DISA call that will establish an Unsupervised Conference; these calls are subject to the conditions of a DISA call and Unsupervised Conference and may require entry of an Authorization Code.
10. Off-Net forward calls are not answered until the system completes dialing of the external call; the call, regardless of internal or external, is then connected to the Off-Premise call.
11. An unlimited number of stations may be set-up in a Call Forward chain, forwarding calls from one station to the next; a station cannot forward calls to a station already a part of the chain.
12. Calls to a Call Forward chain will progress as appropriate through the chain to the last station; if the last station enters DND, CO calls revert to the previous station while intercom calls receive a DND tone.

13. No Answer forward will employ the Station No Answer Forward Timer unless it is set to zero in which case the System No Answer Timer is used.
14. If the Attendant activates Unconditional Call Forward, the receiving station will receive Attendant calls and recall ring; if the receiving station is an LIP Phone, the user will be able to activate features normally reserved for a Main Attendant.

Programming

VOICE CONFIG System Data – Call Feature Timer – Call Forward No Answer Timer

Related Features

DND (Do Not Disturb)
Station Groups
Individual Speed Dial
Common Speed Dial
Intercom Answer Mode
Call Forward, Preset

Hardware

2.3 CALL FORWARD, PRESET

Description

With Preset Call Forward, calls to a station forward to a pre-determined destination assigned in the system database. Preset Station Call Forward can define separate treatments for CO calls and intercom calls. In addition, separate busy and no-answer treatments are defined, and calls can be directly forward to the users Voice Mail box. Call treatments available include:

- Unconditional; all calls are immediately forwarded
- Internal Busy; Intercom calls encountering a busy signal are forwarded immediately
- ICM No-Answer; Intercom calls not answered in the No-Answer time are forwarded (Note: calls to a busy station are also forward after the No-Answer time)
- External Busy; external calls that encounter busy are forwarded immediately
- External No-Answer; external calls, not answered in the No-Answer time are forward (Note: calls to a busy station also are forward after the No-Answer time)

Operation

System

Operation of Preset Call Forward is automatic.

Conditions

1. A station receiving a forwarded call can transfer the call to the forwarding station.
2. Calls cannot be forwarded to a station in DND; if attempted, an error tone is returned.

3. Manual Forward has higher priority than Preset Forward and overrides any Preset Forward setting.
4. Calls to a Preset Call Forward chain will progress as appropriate through the chain to the last station. If a station in manual Call Forward or DND is encountered, it is bypassed and the next station in the chain is signaled. If the last station has entered DND, CO calls revert to the previous station, signaling until answered or abandoned.
5. Internal Busy or No Answer will only operate when the internal call encounters a busy state or no answer, respectively. External Busy or External No Answer will only operate when the external call encounters a busy state or no answer, respectively.
6. Preset call forward status is not shown in the station's LCD display.
7. A station in a Station Hunt Group (Circular or Terminal) can be assigned to receive incoming hunt calls, overriding any Call Forward. That is, either the system recognizes the Forward condition and bypasses hunt calls around the station or routes hunt calls to the station based on the system database.
8. No Answer forward will employ the Station No Answer Forward Timer unless it is set to zero in which case the System No Answer Timer is used.

Programming

VOICE CONFIG	Station Data – Preset Call Forward
	System Data – Call Feature Timer – Call Forward No Answer Timer

Related Features

Call Forward
Off-Hook Signaling
VSF Integrated Auto Attd/Voice Mail
DND (Do Not Disturb)

Hardware

2.4 CALL PARK

Description

A user may place an active CO call in a special holding location (Call Park/Park Orbit) for easy access from any station in the system (default=601-610).

Operation

LIP Phone

To park an active external call:

1. Press the **[TRANS]** button.
2. Dial the Call Park/Park Orbit code (601-610).
3. Return to idle.

To retrieve a parked call:

1. Lift the handset or press the **[SPEAKER]** button,
2. Dial the Call Park/Park Orbit code (601-610).

SLT

To park an active external call:

1. Momentarily press the hook-switch.
2. Dial the Call Park/Park Orbit code (601-610).
3. Return to idle.

To retrieve a parked call:

1. Lift the handset.
2. Dial the Call Park/Park Orbit code (601-610).

Conditions

1. If the selected Call Park/Park Orbit returns a busy signal, the user may dial another Call Park/Park Orbit without the need to disconnect.
2. Intercom calls cannot be placed in a Call Park/Park Orbit location.
3. A Parked call will recall to the station that parked the call should the Call Park Timer expire; the normal Hold Recall process is then initiated.
4. A Parked call will indicate busy at all appearances.

Programming

VOICE CONFIG System Data – Call Feature Timer – Call Park Recall Timer

Related Features

Hold Recall
Attendant Recall

Hardware

2.5 CALL PICK-UP

2.5.1 Directed Call Pick-Up

Description

A station may answer incoming and transferred intercom, CO and IP calls ringing at another station (Call Pick-Up). All ringing calls are subject to Directed Call Pick-up except Queue Callbacks.

LIP phone users may assign a Flex button as a **{DIRECTED CALL PICK-UP}** button.

Operation

LIP Phone

To assign a **{DIRECTED CALL PICK-UP}** button:

1. Lift the handset or press **[SPEAKER]**.
2. Dial **[PGM]** + **{FLEX}** + '7' + **[SAVE].**

To Pick-up a call ringing at another station:

1. Lift the handset or press **[SPEAKER]**.
2. Dial 7 (Directed Call Pick-up code).
3. Dial the ringing station's intercom number.

OR

1. Lift the handset or press **[SPEAKER]**.
2. Press the **{DIRECTED CALL PICK-UP}** button.
3. Dial the ringing station's intercom number.

SLT

To Pick-up a call ringing at another station:

1. Lift the handset
2. Dial 7 (Directed Call Pick-up code).
3. Dial the ringing station's number.

Conditions

1. To pick-up a CO call, the station must have an idle appearance button available.
2. When several calls are ringing at a station simultaneously, Call Pick-up will connect the first-in, highest priority call. Call priority order is: CO transferred call > CO hold-recalled call > CO incoming call > queued call.
3. Queue callback and Private Line calls are not subject to Call Pick-up; any attempts receive an error tone.
4. Only ringing intercom calls are subject to Call Pick-up; handsfree announced calls cannot be picked up by another station.

Programming

Related Features

Intercom Answer Mode
Ringing Line Preference
Group Call Pick-Up

Hardware

2.5.2 Group Call Pick-Up

Description

A station can answer (Call Pick-Up) incoming and transferred intercom, CO and IP calls ringing at another station. All ringing calls, except Private Line and Queue Callbacks, are subject to Pick-up by other stations in the same group.
LIP phone users may assign a Flex button as a **{GROUP CALL PICK-UP}** button.

Operation

LIP Phone

To assign a **{GROUP CALL PICK-UP}** button:

1. Lift the handset, press **[PGM]** + **{FLEX}** + '**' + **[SAVE].**

To Pick-up a call ringing at another station:

1. Lift the handset or press **[SPEAKER]**.
2. Dial '** (Group Call Pick-up code).

OR, 2. Press the **{GROUP CALL PICK-UP}** button.

SLT

To Pick-up a call ringing at another station:

1. Lift the handset.
2. Dial '** (Group Call Pick-up code).

Conditions

1. To pick-up a CO call, the station must have an idle appearance button available.
2. When several calls are ringing simultaneously, Call Pick-up will connect the first-in, highest priority call. Call priority order is: CO transferred call > CO hold-recalled call > CO incoming call > queued call.
3. Queue callback calls are not subject to Call Pick-up; any attempt will receive an error tone.
4. Only ringing intercom calls are subject to Call Pick-up; handsfree announced calls can not be picked up by another station
5. When a station belongs to multiple groups, calls to the station group with lowest sequential group number are answered first. For example, if an incoming call is ringing at both Station Groups 620 and 621; when Station 100 (member to both Station Groups) responds to the ringing and picks up, the call to Station Group 620 will be answered first (by default).

Programming

VOICE CONFIG Station Group Data

Related Features

Intercom Answer Mode
Directed Call Pick-Up
Station Groups

Hardware

2.6 CALL TRANSFER

2.6.1 Call Transfer, Station

*D*escription

CO calls can be transferred to other stations in the Smart Business gateway (iPECS SBG-1000) system. Calls can be transferred announcing the call (screened) or without an announcement (unscreened).

When a CO call is transferred, the Transfer Recall Timer is initiated. If the timer expires before the call is answered, the Hold Recall process is initiated.

Users can transfer an active Intercom call to other stations in the iPECS SBG-1000 system, using either screened or unscreened transfer. When used, the Intercom station is placed on Exclusive Hold, and the Transfer Recall timer is initiated. if the timer expires before the Intercom call is answered, the call will bounce back (recall) to the transferring station until answered or abandoned.

Operation

LIP Phone

While on a CO call, to perform a Screened Call Transfer:

1. Press **[TRANS]**.
2. Dial the station to receive the transfer.
3. At answer or splash tone announce the call.
4. Hang-up to complete the transfer.

OR

1. Press the **{DSS/BLF}** button for the desired station.
2. At answer or splash tone, announce the call.
3. Hang-up to complete the transfer.

While on a CO call, to perform an Unscreened Call Transfer:

1. Press **[TRANS]**.
2. Dial the station to receive the transfer.
3. Hang-up to complete the transfer.

OR

1. Press the **{DSS/BLF}** button for the desired station.
2. Hang-up to complete the transfer.

To perform an Screened Transfer while on an ICM call:

1. Press **[TRANS]** button.
2. Dial Station to receive call.
3. At answer or Splash tone, announce call.
4. Hang-up to return to idle.

OR

1. Press **{DSS/BLF}** button for the desired station.
2. At answer or Splash tone, announce call.

3. Hang-up to return to idle.

To perform an Unscreened Transfer while on an ICM call:
1. Press **[TRANS]** button.
2. Dial Station to receive call.
3. Hang-up to return to idle.

OR
1. Press **{DSS/BLF}** button for the desired station.
2. Hang-up to return to idle.

SLT

While on a CO call, to perform a Screened Call Transfer:
1. Momentarily depress the hook-switch.
2. Dial the station to receive the transfer.
3. At answer or splash tone announce the call.
4. Hang-up to complete the transfer.

While on a CO call, to perform an Unscreened Call Transfer:
1. Momentarily depress the hook-switch.
2. Dial the station to receive the transfer.
3. Hang-up to complete the transfer.

To perform a Screened transfer of an active Intercom call:
1. Momentarily depress the Hook-switch.
2. Dial Station to receive call.
3. At answer or Splash tone, announce call.
4. Hang-up to return to idle.

While on an Intercom call, Unscreened call transfer:
1. Momentarily depress the Hook-switch.
2. Dial Station to receive call.
3. Hang-up to return to idle.

Conditions

1. The transferring station may camp a call at a busy station (refer to Camp-On).
2. The LED of a **{LOOP}** button will display the status of a call until the station no longer has call supervision (ex., the call is successfully transferred).
3. To prevent Toll abuse, CO lines without an active call (either incoming or dialed digits on outgoing) cannot be transferred.
4. For outgoing CO Line calls, the system will monitor the CO Line for dial-tone to prevent Toll abuse; when an IP Line is seized, the system does not monitor for dial-tone.
5. While on intercom call transfer, the **[ICM]** button provides an appearance for the transferred station; LED indicates status and pressing the button connects to the station.
6. A station in DND or out-of-service can not receive a transfer; any attempt will result in an error tone.

Programming

VOICE CONFIG System Data – Call Feature Timer – Transfer Recall Timer

Related Features

Hold Recall
Call Transfer,
Call Waiting/Camp-On
Station Flexible Buttons
DND (Do Not Disturb)

Hardware

2.6.2 Call Transfer, CO

Description

A station may be permitted to transfer a CO call to another CO line, establishing an Unsupervised Conference between the two external parties.

If the receiving party is called through an ISDN path, the Transfer Hold Recall Timer is initiated and if it expires, Hold Recall is initiated.

Operation

LIP Phone

While on a CO call, to perform a Screened Call Transfer:

1. Press **[TRANS]**.
2. Place CO call to forward party.
3. At answer, announce the call.
4. Hang-up to complete the transfer.

While on a CO call, to perform an Unscreened Call Transfer:

1. Press **[TRANS]**.
2. Place CO call to forward party.
3. Hang-up to complete the transfer.

SLT

While on a CO call, to perform a Screened Call Transfer:

1. Momentarily depress the hook-switch.
2. Place CO call to forward party.
3. At answer, announce the call.
4. Hang-up to complete the transfer.

While on a CO call, to perform an Unscreened Call Transfer:

1. Momentarily depress the hook-switch.
2. Place CO call to forward party.
3. Hang-up to complete the transfer.

Conditions

1. For this feature, at least one of the two CO lines (transferred or receiving) must provide detection of disconnect supervision and lost loop condition.
2. If during transfer to an external party, the user presses the CO line of the original call, the outgoing call is disconnected and the original call is connected to the user.

Programming

VOICE CONFIG	Station Data – Authorization Code & COS – Offnet FWD
	System Data – Call Feature Timer – Transfer Recall Timer

Related Features

Hold Recall
Call Transfer, Station

Hardware

2.6.3 Call Transfer, Voice Mail

Description

CO calls can be directly transferred to a station's VSF voice mail-box.

Operation

LIP Phone

While on a CO call, to perform a Call Transfer:

1. Press **[TRANS]**.
2. Press **[MSG/CALLBK]** button.
3. Dial the number or press the **{DSS/BLF}** button for the desired station.
4. Hang-up to complete the transfer.

Conditions

1. The LED of a **{LOOP}** button will display the status of a call until the station no longer has call supervision (ex., the call is successfully transferred).

Programming

VOICE CONFIG	Station Data – Preset Call Forward
	System Data – Call Feature Timer – Transfer Recall Timer

Related Features

Hold Recall
Call Waiting/Camp-On
VSF Voice Mail

Hardware

LIP Phone

2.7 CALL WAITING/CAMP-ON

Description

Call Waiting is used to notify a busy station that a call is waiting. The busy station is notified of the waiting call with a Camp-On tone. For users of an LIP Phone, the LED of the **[HOLD]** button will flash.

After receiving a busy signal, the calling station camps on to the called station. The called station can respond by:

- answering the waiting call, which places the active call on hold,
- activating One-Time DND, or
- ignoring the Camp-On tone.

Operation

To activate a Camp-On while receiving the Intercom busy tone:

1. Press the '*' button, called and calling stations receive Camp-On tone.

Conditions

1. The user may only Camp-On to a station in busy mode; a user may not Camp-On to a station in DND, a conference, receiving a Page, etc.
2. The Camp-On procedure can be employed by an Attendant to activate DND Override.
3. If the calling station disconnects from the call after activating Camp-On, Camp-On is cancelled.
4. A Camp-On tone is sent each time the calling user presses the '*' button.

Programming

Related Features

DND (Do Not Disturb)
Intercom Call (ICM Call)
Voice Over

Hardware

2.8 CO ACCESS

Description

Stations can access outgoing CO lines based on CO Group Access programming. LIP Phones may use flexible buttons assigned to access a specific **{CO}** line button for outgoing calls or a **{LOOP}** button.

Individual users may be allowed to assign CO access flexible buttons.

Operation

LIP Phone

To place an outgoing CO call:

1. Lift the handset or press the **[SPEAKER]** button.
2. Press desired **{CO}** line, **{LOOP}** button or dial the CO line or Group access code.

To answer an incoming CO call:

1. Lift the handset or press the **[SPEAKER]** button.

OR

1. Press flashing **{CO}** line, **{LOOP}** button and lift the handset to speak privately

SLT

To place an outgoing CO call:

1. Lift handset.
2. Dial the CO line or Group access code.

To answer an incoming CO call:

1. Lift handset.

Conditions

1. When a user dials Access Random CO Line code, the system will search for an idle CO line; the system may continue to search through all CO lines for an available line.
2. A telephone user not allowed access to a CO line will receive an error tone when access is attempted. The station may receive transferred calls on such denied access lines but will not be able to flash or use the CO line for an outgoing call.
3. A station denied access to a CO line but assigned to ring for the CO line will receive ring; the user may transfer the call using a flashing LED **{CO}** line button but cannot make an outgoing call on the CO line.
4. CO lines placed on hold may be retrieved by dialing the 8# (retrieve held CO code) and the CO line number.
5. The Tx path to a station will be muted until the system has verified the Toll Restriction for the CO line.

Programming

VOICE CONFIG	Station Data – Common Attributes – CO Group Access

CO Line Data – Call Routing by Line
CO Line Data – Call Routing by Caller Number
CO Line Data – Ring Assignment Table

Related Features

CO Ring Assignment

Hardware

2.9 CO QUEUING

Description

When CO lines are busy, permitted users can request to be placed in queue awaiting the CO line, or a CO line in the same group to become available. When an appropriate CO line becomes available, the system calls the waiting station on a first-in, first-out basis.

Operation

LIP Phone

To request to be placed in queue for a busy CO line:

1. Press busy **{CO}** or **{CO GRP}** button.
2. Press the **[MSG/CALLBK]** button; confirmation tone is received.
3. Hang-up, the **[MSG/CALLBK]** LED flashes.

To cancel the queue from the queued station:

1. Press the **[MSG/CALLBK]** button, the **[MSG/CALLBK]** LED extinguishes.

SLT

To request to be placed in queue while receiving an All Lines Busy signal:

1. Momentarily press the hook-switch.
2. Dial 56 (Callback feature code).

To cancel the queue from the queued station:

1. Lift the handset.
2. Dial 56 (Callback feature code).

System

When a CO line becomes available:

1. The System will send a distinctive Queue recall to the station that was first-in queue, the appropriate **{CO}** LED button will flash
2. The CO line and station will appear busy to all other users.

Conditions

1. A CO line can have any number of simultaneous queue requests.
2. A station may only have a single active CO queue request; activating a new queue request will replace, and cancel an existing queue.
3. A Queue recall will always signal the station with a tone ring, ignoring the station's assigned Intercom Signaling mode.
4. Queue recall will bypass a busy station, and place the station at the bottom of the queue list.
5. Queue recall will signal a station for 15 seconds, after which, the station is removed from the queue (the queue is cancelled).

Programming

Related Features

CO Access

Hardware

2.10 THREE-PARTY VOICE CONFERENCE

Description

The system will allow three internal and external parties to be connected on a call, conference. An unlimited number of 3-party conferences may be established.

Operation

LIP Phone

To establish an ad-hoc conference:

1. Establish first call.
2. Press the **[CONF]** button; the LED will light, and the connected party is placed on exclusive hold (the user receives dial-tone).
3. Place second call.
4. When connected, press **[CONF]**; the new call is placed on exclusive hold.
5. Press **[CONF]** button to establish 3-party conference.

To place a conference on hold:

1. Press the **[HOLD]** button; the **[CONF]** button LED will flash.

To retrieve held conference:

1. Lift the handset
2. Press **[CONF]** button; all parties will be reconnected.

Conditions

1. The **[CONF]** button remains illuminated at the initiators phone for the duration of the conference.
2. There is no limit on the number of 3-way conferences the system will support.
3. If the system receives a disconnect signal and no internal parties remain in the conference, the conference is terminated and all parties are disconnected. If an internal party is still connected when a disconnect signal is received, the connection to remaining parties is maintained.
4. The normal Hold Recall process is applied to a conference on hold using the Unsupervised Conference recall Timer for recall timing.
5. If while setting up a conference, system error tone is received, the initiator must press the **[CONF]** button to obtain the Intercom dial-tone.
6. A station that is busy, in DND or other non-idle state, cannot be added to a conference.
7. SLT can join a conference call, but can not make a conference call

Programming

Related Features

Automatic Speaker Select
Hold Recall

Hardware

2.11 CUSTOMER SITE NAME

Description

A Customer Name, up to 24 characters, may be entered into the system database. The name is displayed on the SMDR and database outputs as well as during an Admin session.

Operation

System
Operation of this feature is automatic when a name is assigned.

Conditions

Programming

VOICE INSTALL	System – Identification – Site Name
SYSTEM ID	Customer Site Name (PGM 100-Btn 2)

Related Features

Hardware

2.12 FAX

Description

Data transmitted over CO lines is subject to distortion and errors if system tones (ex., Camp-On, Override) are applied during transmission. To eliminate such errors, stations that use analog data (modems or Fax) can be assigned to block incoming system tones.

Operation

System

System tones are automatically blocked when FAX utilization is set to “ON”.

Conditions

1. Stations or an Attendant attempting to Camp-On or Override a station with FAX utilization will receive an error tone.
2. When FAX utilization is enabled, the system will not apply audio gain to the call.

Programming

VOICE INSTALL FAX – FAX Configuration – FAX Utilization

Related Features

Call Waiting/Camp-On

Hardware

2.13 DELAYED CO RING

Description

Ring signals for an incoming CO call can be sent to stations immediately upon detection or after an assigned ring cycle delay. The delay can be up to 9 system ring cycles, thus allowing other stations to answer the call.

Operation

System

Delay Ring operation is automatic when assigned:

Conditions

1. Delay Ring can be assigned for a station.
2. If no delay is entered when programming Ring assignments, the station will immediately ring when a call is received.
3. Private Lines may be assigned with delayed ring.

Programming

VOICE CONFIG	CO Line Data – Call Routing by Line
	CO Line Data – Ring Assignment Table

Related Features

CO Ring Assignment

Hardware

2.14 DELAYED AUTO ATTENDANT

Description

An incoming CO call can be routed to the VSF Auto Attendant either immediately upon detection or after a delay of up to 30 seconds. This allows other stations assigned immediate ring the opportunity to answer before the call is routed to the Auto Attendant.

Operation

System

Operation of this feature is automatic when assigned.

Conditions

1. When Delayed Auto Attendant Ring is assigned, after the delay, the call will no longer ring assigned stations and will only ring to the VSF Auto Attendant.
2. If no delay is entered, the call immediately will ring to the VSF Auto Attendant.
3. To assign Delayed Attendant ring, at least one station or Station Group must be assigned for immediate ring.
4. Ring is assigned to a VSF Auto Attendant announcement (01-70) as a “station type” with a delay from 00 to 30 seconds.

Programming

VOICE CONFIG	CO Line Data – Call Routing by Line
	CO Line Data – Ring Assignment Table

Related Features

CO Ring Assignment

Hardware

2.15 DIAGNOSTIC/MAINTENANCE

Description

The system software incorporates various diagnostic and maintenance routines that may be "called" remotely or locally through the systems RS-232 serial ports, a TCP/IP connection using a Web browser or telnet terminal established over IP networks. Routines that can be accessed include trace functions at the device level, commands for diagnostics and maintenance, and tools for manipulation at the OS level.

Operation

Conditions

Programming

Related Features

Hardware

2.16 DIAL-BY-NAME

Description

A name, up to 16 characters, may be assigned to each Individual and Common Speed Dial. In addition, each station may be assigned a 12-character name. When assigned, a user may place an intercom call to another station or select a Station or Common Speed Dial using the name.

The user selects from one of three Dial-by-Name directories and enters characters employing 2 dial pad buttons for each character (refer to Character Entry Chart Table). The system finds and displays the nearest match to the user entries. The user may continue entering characters or scroll the directory at any point using the **[VOL▲]/[VOL▼]** button and select a name to call. The number associated with a selected name may be displayed by using the **[TRANS]** button.

Operation

LIP Phone

To use Dial by Name:

1. Press soft key **[DIR]**.
2. Dial the desired directory.
3. Search the directory using the **[VOL▲]/[VOL▼]** button or by entering the number .

Table 2.16.1 Character Entry Chart

Q – 11 Z – 12 . – 13 1 – 10	A - 21 B - 22 C - 23 2 - 20	D - 31 E - 32 F - 33 3 - 30
G – 41 H - 42 I - 43 4 - 40	J - 51 K - 52 L - 53 5 - 50	M - 61 N - 62 O - 63 6 - 60
P - 71 R - 72 S - 73 Q - 7* 7 - 70	T - 81 U - 82 V - 83 8 - 80	W - 91 X - 92 Y - 93 Z - 9# 9 - 90
Blank - *1 : - *2 , - *3	0-00	#

4. Press the **[SAVE]** button to place the call.

To toggle between the name and number display:
1. Press the **[NAME/TEL]** soft button or **[TRANS/PGM]** button.

To program the station user name:
1. Press the **[PGM]** button.
2. Dial 34 (User Name Program code).
3. Dial the name, up to 12 characters.
4. Press **[SAVE]**.

Attendant
To program a name for another station:
1. Press the **[PGM]** button.
2. Dial 031 (Attendant User Name Program code).
3. Dial the station number.
4. Dial the name, up to 12 characters.
5. Press **[SAVE]**.

Conditions

1. Available characters are A to Z, space and period.
2. The LCD will display multiple names (one per LCD line, up to 16 characters).
3. If a user selects a directory with no entries or there is no match to the user entry, error tone is provided.
4. Dial-by-Name is only available to LIP Phones with a display; other users will receive error tone if an attempt is made to access Dial-by-Name.

5. A user may both scroll and enter characters to search a directory using the **[VOL▲]/[VOL▼]** buttons.

Programming

Related Features

Individual Speed Dial
Common Speed Dial

Hardware

LIP Phone w/Display

2.17 DND (DO NOT DISTURB)

Description

A station can be placed in DND to block incoming CO and Intercom calls, transfers and paging announcements.

Operation

LIP Phone

To activate DND:
1. Press the **[DND]** button; the **[DND]** button LED illuminates.

To remove DND:
1. Press the **[DND]** button; the **[DND]** button LED extinguishes.

SLT

To activate DND:
1. Dial 53 (DND feature code); confirmation tone is received.

To remove DND:
1. Dial 53 (DND feature code), confirmation tone is received.

Conditions

1. Pressing the **[DND]** button while ringing will activate One-Time DND.
2. An Attendant may cancel DND for other stations.
3. DND service is not available to Attendants.
4. Recalls for CO calls will override the DND feature.
5. A station in DND is out-of-service for all incoming calls including Station Group calls.
6. A station in DND is bypassed by calls forwarded to the station; if the last station in a Call Forward chain is in DND, the call will ring to the previous station in the chain.
7. When calling a station in DND, the LIP Phone display will indicate the DND status.

Programming

Related Features

Feature Cancel
Call Forward
Station Groups

Hardware

2.18 EMERGENCY CALL

Description

Regardless of a station's CO accessibility, the user may dial assigned Emergency numbers.

Operation

System

The system will automatically override any toll restrictions and process an assigned Emergency number.

Conditions

Programming

VOICE CONFIG System Data – Emergency Dialing

Related Features

Hardware

2.19 FLEXIBLE NUMBERING PLAN

Description

User access to the iPECS SBG-1000 system resources and features is accomplished through feature codes or LIP Phone buttons. The Administrator, if desired, assigns codes for individual functions in the Flexible Numbering Plan. The feature codes are defined in the system's Flexible Numbering Plan.

Operation

System

System implements feature activation based on the Flexible Numbering Plan.

Conditions

1. Feature codes can be 1-3 digits in length.
2. During programming, conflicts in the Numbering Plan are not allowed; the existing non-conflicting Numbering Plan is used until correctly updated.

Programming

VOICE INSTALL Numbering Plan

Related Features

Hardware

2.20 HEADSET COMPATIBILITY

Description

An industry standard headset can be connected to an LIP Phone in place of or in addition to the handset. The station is then programmed for Headset operation.

In the Headset mode, pressing the **[SPEAKER]** button will send audio to the Headset instead of the speakerphone. In addition, when in the Headset mode, ring signals can be delivered to the speaker or the headset as defined in the system database.

Operation

LIP Phone

To change operation from Speakerphone to Headset:

1. Press the **[PGM]** button.
2. Dial 12 (Headset select code).
3. Dial ‘0’ to select Headset, ‘1’ to select Speakerphone.

OR,

1. Press **[HEADSET]** button.
2. Dial ‘0’ to select Headset, ‘1’ to select Speakerphone.

To change the device to receive ring signals:

1. Press the **[PGM]** button.
2. Dial 13 (Ring select code).
3. Dial ‘1’ for Speaker, ‘2’ for Headset or ‘3’ for both.

To place/answer calls using the headset:

1. Press the **[SPEAKER]** with the phone in Headset mode.

Conditions

1. The Intercom Signaling Mode can be set in the Headset mode as with the Speakerphone mode.
2. The station always receives Page announcements over the speaker of the LIP Phone.
3. Although the phone is in the headset mode, the system will monitor the hook-switch status. If a user lifts the handset to go off-hook, audio is delivered to the handset.

Programming

VOICE CONFIG	Station Data – Common Attributes – Headset Ring
	Station Data – Common Attributes – Headset or Speaker Mode

Related Features

Speakerphone
Paging

Hardware

2.21 HOLD

2.21.1 Hold

Description

CO lines may be placed in a waiting state such that other stations in the system are able to access the CO line. Stations must have System database access to the CO line to access the held call.

If the call remains on hold at expiration of the System Hold Recall Timer, normal Hold Recall will be activated.

Operation

LIP Phone

To place a call on System Hold:

1. Press the **[HOLD]** button.

To access a call from System Hold:

1. Lift the handset or press the **[SPEAKER]** button.
2. Press the **{CO}** line button.

OR

1. Lift the handset or press the **[SPEAKER]** button.
2. Dial 8# (Held CO Call Access code).
3. Dial the CO line number

SLT

To place a call on System Hold:

1. Momentarily press the hook-switch.
2. Dial 67 (System Hold feature code).

To access a call from System Hold:

1. Lift the handset.
2. Dial 8# (Held CO Call Access code).
3. Dial the CO line number.

Conditions

1. When a CO line is placed on System Hold, the button LED will flash at 30 ipm (it will wink at the holding station and will flash at all other stations).
2. A call on System Hold can be retrieved from any station allowed access to the CO line in the system database using the CO line button or the Held CO call access code.
3. The LED of **{LOOP}** buttons will display the CO line status.

Programming

VOICE CONFIG	System Data – Call Feature Timer – Attendant Recall Timer
	System Data – Call Feature Timer – System Hold Recall Timer

Related Features

Call Transfer,
Hold Recall

Hardware

2.21.2 Hold Recall

Description

When a user places a CO call on hold, a hold timer is activated. If the timer expires, the held call will recall at the station for the I-Hold Recall time. If the call remains unanswered, the call is placed on System Hold and the Attendant also receives a recall for the Attendant Recall time. If still unanswered after the Attendant Recall time, the CO call is disconnected and the appropriate circuits are returned to idle.

Operation

Hold Recall operation is automatic.

Conditions

1. Separate timers are assigned for the various types of hold: System, Transfer, etc.
2. If the I-Hold timer is set to zero, the station will not receive a recall; if the Attendant Recall timer is set to zero, the also Attendant will not receive a recall.
3. If the specific Hold timer is set to zero, recall is disabled.

Programming

VOICE CONFIG	System Data – Call Feature Timer – Attendant Recall Timer System Data – Call Feature Timer – System Hold Recall Timer System Data – Call Feature Timer – Transfer Recall Timer

Related Features

Call Transfer,
Hold

Hardware

2.21.3 Automatic Hold

Description

While on an active CO call, the system will place the call on hold automatically if the user presses the **[FLASH]**, **[CONF]**, **{DSS/BLF}** or other feature buttons. In addition, the station can be programmed to support CO to CO Automatic Hold. In this case, pressing a CO button while on a CO call will place the active call on hold and access the selected CO line.

Operation

LIP Phone

To use Automatic Hold while on an active CO call:

1. Press the desired feature button or **{CO}**; the active call is placed on Hold.

Conditions

1. There is no limit on the number of calls that can be placed on Hold using Automatic Hold.

Programming

Related Features

Hold Recall

Hardware

LIP Phone

2.22 CALL ROUTING BY CALLER NUMBER

Description

The system can employ caller number to determine the routing of incoming external calls. Each CO Line may be assigned to employ call routing by caller number. The system will compare the

received caller number to entries in the Call Routing by Caller Number Table, and if a match is found, will route the call to the destination defined in the Ring Assignment Table. Destinations can be the VSF, a station or a station group.

Operation

System

System implements routing automatically based on database entries and the received caller number.

Conditions

1. For analog CO Lines, the system will await receipt of valid ICLID for the ICLID Ring Timer. At expiration of the timer, if ICLID is not received, the call is routed based on the type and other programming (Ring assignments, etc.).
2. If the received caller number does not match an entry in the Call Routing by Caller Number Table, the call is routed based on the type and other programming (Ring assignments, etc.) for CO Line.
3. The caller number received from the CO Line may be a telephone number or name that must match an Call Routing by Caller Number Table entry.

Programming

VOICE CONFIG	CO Line Data – Call Routing by Line
	CO Line Data – Call Routing by Caller Number
	CO Line Data – Ring Assignment Table

Related Features

CO Ring Assignment

Hardware

2.23 IP FAX RELAY, T.38 SUPPORT

Because of their nature, Fax tones do not transmit well through IP networks, particularly when compression is employed. To address this, iPECS SBG-1000 supports the T.38 protocol that defines the translation of fax tones to digital signals. When Fax tone is detected on a port of an iPECS SBG-1000, the system will activate a T.38 Fax relay channel to the appropriate Line or SLT module.

Operation

Operation of this feature is automatic.

Conditions

Programming

VOICE INSTALL FAX – FAX – T.38

Related Features

Hardware

2.24 LNR (LAST NUMBER REDIAL)

Description

The last number dialed is stored (up to 23 digits) in the station's Last Number Redial buffer. The user may request the system redial the last dialed number without the need to dial the number.

For LIP Phones with displays, the last 15 numbers are stored in the LNR buffer. The user may view the numbers using the **[VOL▲]/[VOL▼]** button and select the number to dial from the list.

Operation

LIP Phone

To assign a Flex button as an {redial} button:

1. Press **[PGM]** + **{FLEX}** + **[PGM]** + '54' + **[SAVE]**

To use Last Number Redial:

1. Lift the handset or press the **[SPEAKER]** button.
2. Press the **{REDIAL}** button.
3. Press the **[VOL▲]/[VOL▼]** button to highlight the desired number.
4. Press **[SAVE]** or **{REDIAL}** to dial the number highlighted.

SLT

To use Last Number Redial:

1. Lift the handset.
2. Dial '52', the Last Number Redial code.

Conditions

1. For LIP Phones with display, the redial buffer will store duplicate numbers unless dialed consecutively.
2. When the CO line used for the original call is busy, the system will select an idle line from the same CO line Group to place the call.
3. Using Last Number Redial will cancel Automatic Called Number Redial if active.
4. The LNR buffer is not stored in non-volatile memory and will be erased if power to the system is lost.
5. Manually dialing a Flash during an outgoing call will cause only those digits dialed after the Flash to be stored in the LNR buffer.

Programming

Related Features

Save Number Redial (SNR)
Individual Speed Dial
Common Speed Dial

Hardware

2.25 MOH (MUSIC-ON-HOLD)

Description

When a call is placed on hold, the system will deliver audio from the defined MOH source. In this way, the connected user can determine that the connection is still active.

A message or music recorded in the VSF can be employed as MOH. The Attendant records the VSF announcement for MOH and VSF MOH is assigned as the MOH source.

Operation

System
Operation of MOH is automatic.

Attendant
To record a VSF announcement for MOH:

1. Press the **[PGM]** button.
2. Dial 05 (VSF Record code).
3. Dial 071 (VSF MOH Announcement number).
4. The current announcement is played followed by the “Press # to record” prompt.
5. Dial ‘#’.
6. After the record prompt and beep-tone, record message.
7. Press the **[SAVE]** button to stop recording and save the message.

Conditions

1. Only VSF announcement number 71 may be used for the MOH message.

Programming

VOICE CONFIG	Station Data – Station Hold Music
	CO Line Data – CO Hold Music

Related Features

Hold

Hardware

2.26 REGISTRATION & REGISTRATION TABLE

Description

To eliminate the potential for unintended device registration, the system can be programmed to allow local device registration employing MAC addresses. Using the defined MAC address registration, the system allows devices with matching MAC addresses to register.

The Registration Table permits entry of up to 12 MAC addresses to be registered for the device; entering the MAC address permits the device to register with the system. If the device which has the matching MAC address is successfully registered, the MAC address is removed from the Registration Table.

Operation

Operation of registration is automatic based on the system database.

Conditions

Programming

VOICE INSTALL Station Registration – Registration Table

Related Features

Hardware

2.27 RINGING LINE PREFERENCE

Description

A station is automatically connected to incoming calls by lifting the handset or pressing the **[SPEAKER]** button when assigned Ringing Line Preference (RLP).

Operation

LIP Phone

To answer a call while the station is ringing:

1. Lift the handset or press the **[SPEAKER]** button.

Conditions

1. When multiple calls are ringing at the station, a priority defines the order in which calls are answered. The priority is:
   Transfer > recalls > incoming calls > queued calls
2. Intercom calls are always given the lowest answering priority.

3. SLTs operate only in the RLP mode; when ringing, lifting the handset connects the SLT to the ringing call.

Programming

Related Features

Automatic Speaker Select

Hardware

2.28 SPEED DIAL

2.28.1 Display Security

Description

Individual and Common Speed Dial numbers may be programmed so that the digits are not displayed on the LCD of LIP phones.

Operation

To assign Display Security to a Speed Dial number:

1. Dial "*" as the first digit of the Speed Dial number.

Conditions

1. The number is displayed when programming a Speed Dial number.
2. Display Security does not affect the SMDR output.
3. Display Security is provided on all CO calls including calls that are transferred or recall.

Programming

VOICE CONFIG	Station Data – Individual Speed Dial
	CO Line Data – Common Speed Dial

Related Features

Speed Dial

Hardware

2.28.2 Individual Speed Dial

Description

Each user can store commonly dialed numbers for easy access using Individual Speed Dial bins. Each station has access to 20 Speed Dial numbers. Each Speed Dial number can be up to 23 characters in length and may include special instruction codes.

Special instruction codes available are:

'*' as 1st digit Activate Display Security, do not display number.

LIP Phone users may assign a Flex button for One-Touch access to a specific Speed Dial bin. In addition, the LIP Phone user may assign a Telephone number directly to a Flex button. In this case, the telephone number is allocated to the highest numbered available Individual Speed Dial bin.

Operation

LIP Phone

To assign a Flex button as an {individual speed dial} button:

1. Press **[PGM]** + **{FLEX}** + **[SPD/DEL]** + Individual Speed Dial bin number + **[SAVE]**

To dial using an Individual Speed Dial:

1. Lift handset or press the **[SPEAKER]** button.
2. Press the **[DIR]** soft button.
3. Press the **[SPEED]** soft button.
4. Dial the desired bin number (00–19).

To program an Individual Speed Dial number:

1. Press the **[DIR]** soft button.
2. Press the **[SPEED]** soft button.
3. Press the **[ADD]** soft button.
4. Dial the Speed Dial bin number (00-19).
5. Dial the number to be stored.
6. Press the **[SAVE]** button.
7. If desired, enter a name.
8. Press the **[SAVE]** button.

SLT

To dial using an Individual Speed Dial:

1. Lift handset.
2. Dial 58 (SLT Speed Dial access code).
3. Dial the desired bin number ('00' – '19').

To program an Individual Speed Dial number:

1. Dial 55 (SLT Speed Programming code).
2. Dial the Speed Dial bin number (00-19).
3. Dial the number to be stored.

4. Momentarily press the hook-switch.
5. If desired, enter a name (refer to Character Entry Chart Table).
6. Momentarily press the hook-switch.

Alpha-numeric characters may be entered to name the Speed Dial number using the chart below.

Table 2.72-1 Character Entry Chart

Q – 11 Z – 12 . – 13 1 – 10	A - 21 B - 22 C - 23 2 - 20	D - 31 E - 32 F - 33 3 - 30
G – 41 H - 42 I - 43 4 - 40	J - 51 K - 52 L - 53 5 - 50	M - 61 N - 62 O - 63 6 - 60
P - 71 R - 72 S - 73 Q - 7* 7 - 70	T - 81 U - 82 V - 83 8 - 80	W - 91 X - 92 Y - 93 Z - 9# 9 - 90
Blank - *1 : - *2 , - *3	0-00	#

Conditions

1. Accessing an empty Speed Dial bin will return an error tone.
2. All Speed Dial numbers stored in memory are protected from power loss.
3. A name can be entered for a Speed Dial number to permit access from the Dial-by-Name directory.
4. Stored speed dial number should not include CO access code.

Programming

VOICE CONFIG Station Data – Individual Speed Dial

Related Features

Dial-by-Name
Display Security
LNR (Last Number Redial)
Save Number Redial (SNR)
Common Speed Dial
Flex Button Direct Speed Dial Assignment

Hardware

2.28.3 Common Speed Dial

Description

Commonly dialed numbers can be stored by the Attendant or by the Administrator in Web Admin for easy access by stations. Up to 800 Common Speed Dial numbers are available. Each Speed Dial number can be up to 23 characters in length and may include special instruction codes.

Special instruction codes available are:

'*' as 1st digit Activate Display Security.

LIP Phone users may assign a Flex button for One-Touch access to a specific Common Speed Dial bin.

Operation

LIP Phone

To assign a Flex button as a {common speed dial} button:

[PGM] + **{FLEX}** + **[SPD/DEL]** + Common Speed Dial bin number + **[SAVE]**

To dial using a Common Speed Dial:

1. Lift handset or press the **[SPEAKER]** button.
2. Press the **[DIR]** soft button.
3. Press the **[SPEED]** soft button.
4. Dial the desired bin number ('200'-'999').

SLT

To dial using a Common Speed Dial:

1. Lift handset.
2. Dial '58', the SLT Speed Dial access code.
3. Dial the desired bin number ('200'-'999').

Attendant

To program a Common Speed Dial number:

1. Press the **[DIR]** soft button.
2. Press the **[SPEED]** soft button.
3. Press the **[ADD]** soft button.
4. Dial the Speed Dial bin number ('200'-'999').
5. Dial the number to be stored.
6. Press the **[SAVE]** button.
7. If desired, enter a name, see Alpha-numeric entry chart under Individual Speed Dial.
8. Press the **[SAVE]** button.

Conditions

1. Accessing an empty Speed Dial bin will return error tone.
2. All Speed Dial numbers are stored in memory protected from power loss.

3. A name can be entered for a Speed Dial number to permit access from the Dial-by-Name directory.
4. Stored speed dial number should not include CO access code.

Programming

VOICE CONFIG CO Line Data – Common Speed Dial

Related Features

Dial-by-Name
Display Security
LNR (Last Number Redial)
Save Number Redial (SNR)
Individual Speed Dial

Hardware

2.29 STATION GROUPS

Description

Stations can be grouped for incoming call routing and Call Pick-up purposes. Up to 12 Station Groups can be defined with up to 24 stations in a group. Seven types of groups can be defined:

- Circular
- Terminal
- Ring
- Pick-Up
- VSF-Voice Mail
- IPCR
- Net VM (Centralized External VM)

Circular Station Group

In Circular Hunt, calls to a station in the group will go to the station, if unavailable or unanswered in the hunt no answer time; the call will be directed to the next station defined in the group. The call will continue to hunt until each station in the group has been tried. The call remains at the last station or passes to a designated overflow station or group.

A Circular Station Group can be assigned with a pilot number (the Station Group Number) so that calls to the pilot number will hunt. In this case, the call will be directed to the first station in the group, and if needed, hunt through each station in the group until reaching the last station. The call may remain at the last station, passed to an overflow destination or sent to a voice mail-box.

Terminal Station Group

Calls to a station in a Terminal Station Group that encounter an unavailable or unanswered status will be routed through the hunt process. The call will proceed to the next listed station in the group

until reaching the last listed station in the group. The call may remain at the last station or be routed to an Overflow destination.

A Terminal Hunt Group can be assigned with a pilot number (the Station Group number) so that calls to the pilot number will hunt. In this case, the call will route as described for Circular Pilot Number hunting.

Station Ring Group
A call to any station in the Group will cause all stations in the group to ring and any station in the group may answer the call. If the call remains unanswered beyond the Overflow timer, the call is sent to the Overflow destination, which can be a Station, Station Group or Voice Mail-box.

Multiple calls can be received by a Station Ring Group and can be serviced in any order.

Pick-Up Station Group
A station can be assigned to a Call Pick-Up group and may then pick-up (answer) calls to other stations in the group employing the system's Group Call Pick-Up feature.

VSF AA/VM Group
The VSF memory is employed by the integrated Smart Business gateway AA/VM application. Incoming calls can be directed to one of 70 user-recorded announcements, which may request further routing instructions from the user in the form of caller dialed digits. These digits are employed to route the caller as defined in the system CCR (Customer Controlled Routing) Tables.

The VSF AA/VM Group Voice Mail application receives calls forwarded or recalling from a station. Such calls will receive the user's pre-recorded greeting and may leave voice messages. The user may call the VSF AA/VM Group to review and manage the integrated Voice Mail application.

IPCR
This group is defined to support IP Call Recording service.

Net VM
This group is defined to support a Centralized Voice Mail system for a networked environment. At supported systems, the group is used to handle the AA/VM requirements from the central iPECS. The Net VM group may be an external VM system or the iPECS Feature Server.

Group Announcements
Station Group routing can be augmented with announcements recorded in the VSF AA/VM. Callers can be routed to one of several user-recorded announcements. The system answers the call and plays the defined 1st announcement to the caller. The announcement may provide the caller with routing options for Caller Controlled Routing. The 1st announcement may be "Guaranteed" meaning it will play in full before routing the call. A 2nd announcement can be provided to the caller when queue timers expire.

Operation

Conditions

1. Station Group calls are not routed to member stations that are in DND.
2. When a member of a Circular, Terminal, or Ring Group activates Call Forward, calls to the group may still route to the member based on the Member Forward option.
3. A call transferred to a Station Group will follow the routing for the group and will not initiate the Transfer Recall process.
4. Calls to a Station Group receive either a ring-back tone or MOH while queued to the group.
5. Calls which are not answered in the Overflow time, are routed to the defined Overflow destination, station, group, etc. If no Overflow destination is defined, the call is dropped after expiration of the Overflow timer.
6. One of the 70 VSF announcements may be assigned as the Overflow destination. These announcements allow for Caller Controlled Routing.
7. iPECS SBG-1000 has two default station groups. Group 631 is default Ring group which includes all stations in member list. Group 630 is default VSF-Voice Mail group.

Programming

VOICE CONFIG	Station Group Data – Station Group Assignment
	Station Group Data – Station Group Attributes

Related Features

Group Call Pick-Up
MOH (Music-On-Hold)
VSF Integrated Auto Attd/Voice Mail

Hardware

2.30 SMDR (STATION MESSAGE DETAIL RECORDING)

2.30.1 Call Cost Display

Description

Each SMDR call record includes a “Cost” field, which is a calculated estimate of the cost of the call. The call cost updates in real-time and displays on the LIP Phone LCD in place of the call duration.

The cost is determined by:

- Fixed charge per “Call Meter Pulse”,
- ISDN Advice of Charge, or
- Estimated cost updated based on Elapsed Call Timer and assigned costing.

The technique selected to determine cost is based on the type of facility (analog CO, ISDN, or VoIP), services provided by the carrier and the system database.

Analog CO
Where “Call Metering Pulse” service is available from the carrier, the system will apply the “SMDR Cost per Unit Pulse” and the “SMDR Decimal” to the Call Metering received to estimate the call cost.

When no “Metering Type” is selected, the system call duration is used with the cost/pulse and decimal values to estimate the cost of the call. The cost is updated periodically using the “Elapsed Call Timer” duration.

ISDN
ISDN providers may support “Advice of Charge” information in the ISDN Facility Message. If assigned, the system will use this information to display and output call cost.

VoIP
For VoIP calls, the system uses the call duration, cost/pulse and decimal values to establish the call cost estimate. The cost is updated periodically according to the “Elapsed Call Timer”.

Operation

System
Call cost is estimated automatically and output to LIP Phone displays and the SMDR TCP port

Conditions

1. The call cost display begins after the “SMDR Start Timer” expires, if enabled, or at receipt of the first Call Meter Pulse.
2. Once connected to the system, the call duration includes the total time the call is connected including periods when the call is on hold, in queue, etc.
3. To enable Call Cost Display, the “SMDR Cost per Unit Pulse” and “SMDR Decimal” must be assigned; when not assigned, the call duration is provided by the system.

Programming

VOICE CONFIG	System Data – SMDR Attributes – Call Metering
	System Data – SMDR Attributes – SMDR Cost Per Metering Pulse
	System Data – SMDR Attributes – SMDR Decimal Position
	System Data – SMDR Attributes – Record Start Guaranteed Time

Related Features

SMDR (Station Message Detail Recording)
Lost Call Recording
Traffic Analysis

Hardware

2.30.2 SMDR Call Records

Description

SMDR (Station Message Detail Recording) provides detailed information on incoming and outgoing calls. Assignable options in the system database permit recording of all calls, all outgoing calls or toll calls and calls that exceed a fixed duration. Call records are output either upon completion of the call (real-time) or in response to a request from the Attendant.

The SMDR record output is as shown in the figure below. There are two flexible fields, Field I and Field II. Each Field is defined to show Ring duration, CLI (Caller Id) or CPN (Called Party Number).

```
STA  CO  TIME     START         DIAL/CLI/CPN NUM-1      COST    ACCOUNT CODE DIAL/CLI/CPN NUM II
SSSS BBB DD:DD:DD EE:EE FF/FF/FF HCCCCCCCCCCCCCCCCCCCCC sssssssss aaaaaaaaaaa hccccccccccccccccccc
```

The various fields or items for a Call Record are:

- STA: 2~4 digit station number.
- CO: 3 digit CO Line number
- Time: Call duration in hours, minutes and seconds
- Start: Date and time call was placed/received
- NUM I: Flex Field I outgoing call dialed number & incoming call Ring duration, CLI or CPN
- Cost: Cost of Call
- Account Code:Account code entered for call (Not used in iPECS SBG-1000), MSN CLI
- NUM II: Flex Field II incoming call Ring duration, CLI or CPN

Operation

System

For real-time SMDR, records are output after completion of the call as shown in the figure above:

Attendant

To print SMDR records:

1. Press the **[PGM]** button.
2. Dial 0111 (SMDR print code).
3. Enter the desired station range.
4. Press the **[SAVE]** button.

To delete stored records:

1. Press the **[PGM]** button.
2. Dial 0112 (SMDR delete code).
3. Enter the desired station range.
4. Press the **[SAVE]** button.

To abort SMDR printing:

1. Press the **[PGM]** button.
2. Dial 0114 (SMDR abort code).

3. Press the **[SAVE]** button.

Conditions

1. For SMDR, if the first dialed digit(s) match the programmed LD code or the number of dialed digits exceeds the LD digit count, the call is considered an LD call. When behind a PBX, LD determination is made only if a PBX Trunk Access code is dialed as the first digit(s).
2. Except for DISA calls, the duration of ring for an incoming call is provided in the Dialed number field.
3. A header, including the assigned "Customer Site Id" is output after two blank lines and is repeated every 66th line.
4. The SMDR output is a simple ASCII stream of up to 80 characters per line.
5. When enabled, SMDR call record timing begins after the "SMDR Start Timer" expires and ends at call completion.
6. For incoming calls, the "NUM I" and "NUM II" fields will display the assigned data item – Ring Service time, CLI, or CPN. For outgoing calls, the NUM I field will always display the dialed number, user or system.
7. For outgoing calls which are starting with MSN CLI button, "Account Code" fields will display MSN CLI, if print MSN is configured to "ON".

Programming

VOICE CONFIG	System Data – SMDR Attributes
	System Data – SMDR Attributes – SMDR Ring/CLI/CPN Service-I
	System Data – SMDR Attributes – SMDR Ring/CLI/CPN Service-II
	System Data – SMDR Attributes – Print MSN

Related Features

Call Cost Display
Lost Call Recording
Traffic Analysis

Hardware

2.30.3 Lost Call Recording

Description

Incoming calls where the caller hangs up before answer or while in a hold state are considered Abandoned or Lost calls. Special SMDR call records are provided for lost calls in real-time, as they occur, and a summary Lost Call count report is available on demand.

The real-time Lost Call records provide details on the called party, when and how long the call rang or was on hold before being abandoned, etc. Description of the record details is provided in the following charts. As noted in the charts, the dialed number field indicates the type of call and the ring or hold duration before the call was abandoned. The first character in the NUM I field is the status of the call when abandoned:

- R: normal ring to a station,
- G: ring to a station group and
- H: call placed in a hold state, including Transfer hold.

```
STA  CO  TIME     START        DIAL/CLI/CPN NUM-1  COST  ACCOUNT CODE DIAL/CLI/CPN NUM II
EXT  001 00:00:00 14/05/02 15:45 R RING 01:35
```

- Incoming call on CO Line 1 received on May 14, 2002 at 3:45 pm, rang the assigned stations for 1 minute and 35 seconds.

```
STA  CO  TIME     START        DIAL/CLI/CPN NUM-1  COST  ACCOUNT CODE DIAL/CLI/CPN NUM II
101  002 00:00:00 14/05/02 16:45 R RING 02:03
```

- Station 101 rang for an incoming call on CO Line 2 on May 14, 2002 at 4:45 pm, rang for 2 minutes and 3 seconds.

```
STA  CO  TIME     START        DIAL/CLI/CPN NUM-1  COST  ACCOUNT CODE DIAL/CLI/CPN NUM II
101  001 00:00:00 15/05/02 09:35 R 100 RING 00:49
```

- Incoming call on CO Line 1 on May 15, 2002 at 9:35 am forward from station 101 to station 100 and rang for 49 seconds.

```
STA  CO  TIME     START        DIAL/CLI/CPN NUM-1  COST  ACCOUNT CODE DIAL/CLI/CPN NUM II
104  002 00:00:00 16/05/02 11:06 G621 RING 01:32
```

- Incoming call on CO Line 2 on May 16, 2002 at 11:06 am routed to station 104 of Station Group 620 and rang for 1 minute and 49 seconds.

```
STA  CO   TIME     START        DIAL/CLI/CPN NUM-1  COST  ACCOUNT CODE DIAL/CLI/CPN NUM II
621  001  00:00:00 16/05/02 14:03 G621 RING 00:39
```

- Incoming call on CO Line 1 on May 16, 2002 at 2:03 pm routed to Station Group 621 and rang for 39 seconds.

```
STA  CO   TIME     START        DIAL/CLI/CPN NUM-1  COST  ACCOUNT CODE DIAL/CLI/CPN NUM II
100  002  00:03:32 16/05/02 15:30 H100 03:02
```

- Call on CO Line 2 on May 16, 2002 at 3:30 pm placed on hold by station 100 for 3 minutes and 2 seconds had total duration of 3 minutes and 32 seconds.

```
STA  CO   TIME     START         DIAL/CLI/CPN NUM-1  COST  ACCOUNT CODE DIAL/CLI/CPN NUM II
129  001  00:00:45 18/05/02 08:40 H100 RING 00:33
```

- Call on CO Line 1 on May, 18, 2002 at 8:40 am was transferred by station 100 to station 129 was on hold for 33 seconds.

The output for the Lost Call summary count report is shown in the figure below:

```
Lost call count start time: 05/01/02 09:31
Current time 26/04/02 16:32
Total Lost call count until now: 121
```

Operation

Attendant

To print the summary Lost Call Count report:

1. Press the **[PGM]** button.
2. Dial 0115 (Lost Call Count report code).
3. Press the **[SAVE]** button.

To reset the Lost Call summary Count:

1. Press the **[PGM]** button.
2. Dial '0116', the Lost call Count reset code.
3. Press the **[SAVE]** button.

Conditions

1. When the Lost Call Count is reset, the SMDR port will provide a "count reset" message.
2. Individual Lost Call records are only available real-time and not on-demand.
3. "Print Incoming Calls" and "Print Lost Calls" must be enabled in the SMDR Attributes for the system to output real-time Lost Call records and for the Lost Call Count summary report.
4. The fields of a Lost Call Record are the same as a normal SMDR Call Record.

Programming

VOICE CONFIG System Data – SMDR Attributes

Related Features

Call Cost Display
SMDR Call Records
Traffic Analysis

Hardware

RS-323 device to capture SMDR

2.31 SYSTEM ADMIN PROGRAMMING

2.31.1 Keyset Administration

Description

The system database can be accessed and modified using the keypad and Flex buttons of an LIP Phone. The display of the LIP Phone can be used to view items in the iPECS SBG-1000 database. The user may be required to enter a password for access to Keyset Admin. operation.

Operation

Attendant

To program in Keyset Administration:

1. Press the **[PGM]** button.
2. Dial '***#**', Enter Admin code
3. Enter Password; confirmation tone will be heard.
4. Enter PGM code (100 or 102)
5. Press the desired **{FLEX}** button.
6. Enter new value
7. Press the **[SAVE]** button; a confirmation tone is heard

Conditions

1. Only an Attendant can enter and change system database items.
2. System ID (PGM100), and System IP Address Plan (PGM102) can be programmed using Keyset Admin. operation.
3. If new value is invalid, an error tone is heard and the old value is displayed again.

Programming

Related Features

Web Administration

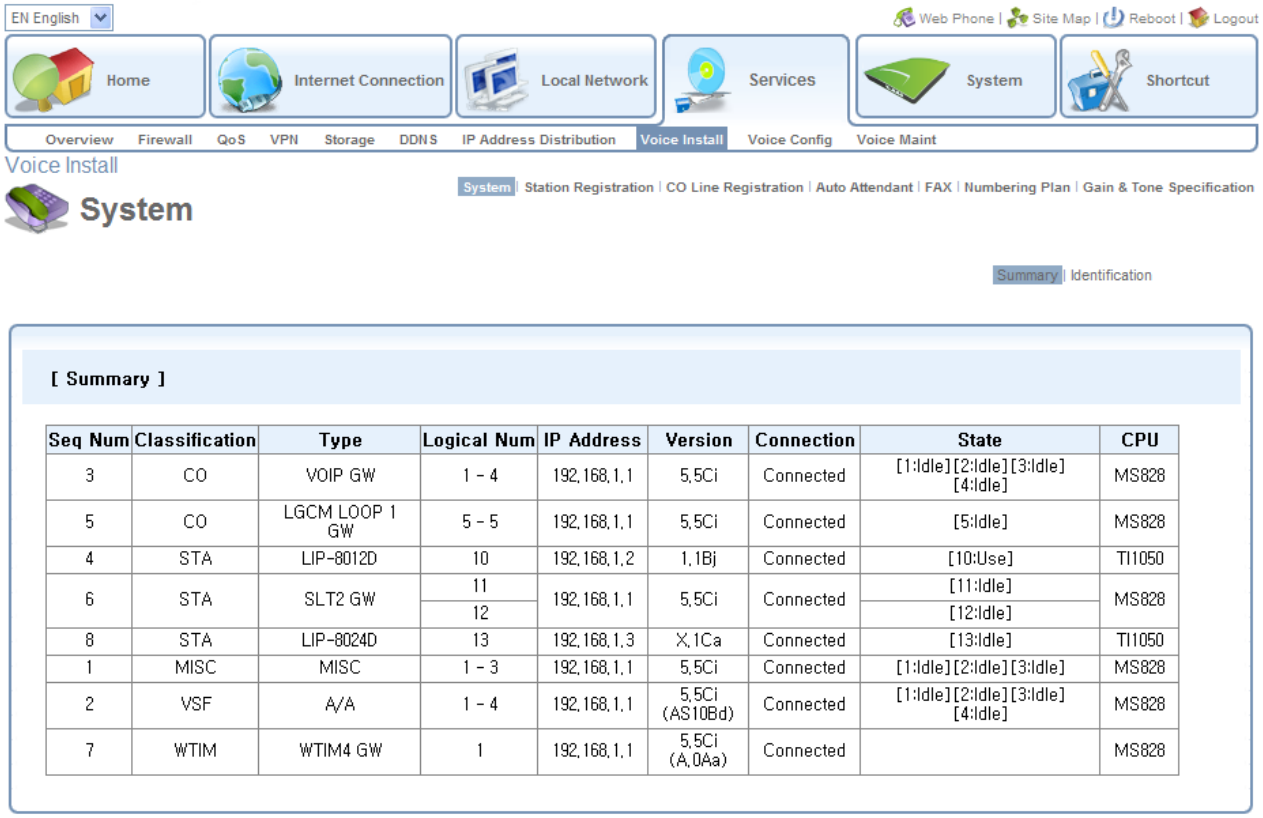
Hardware

2.31.2 Web Administration

Description

The system database is accessed and modified via a LIP Phone or the Network interface. The Network accesses the system's Web server, using the user's Web browser. When properly configured, the user can remotely access the System database.

Web administration consists of 3 Tabs across the top of the screen; each tab has multiple menu items.



Seq Num	Classification	Type	Logical Num	IP Address	Version	Connection	State	CPU
3	CO	VOIP GW	1 - 4	192.168.1.1	5.5Ci	Connected	[1:Idle] [2:Idle] [3:Idle] [4:Idle]	MS828
5	CO	LGCM LOOP 1 GW	5 - 5	192.168.1.1	5.5Ci	Connected	[5:Idle]	MS828
4	STA	LIP-8012D	10	192.168.1.2	1.1Bj	Connected	[10:Use]	TI1050
6	STA	SLT2 GW	11	192.168.1.1	5.5Ci	Connected	[11:Idle]	MS828
			12				[12:Idle]	
8	STA	LIP-8024D	13	192.168.1.3	X.1Ca	Connected	[13:Idle]	TI1050
1	MISC	MISC	1 - 3	192.168.1.1	5.5Ci	Connected	[1:Idle] [2:Idle] [3:Idle]	MS828
2	VSF	A/A	1 - 4	192.168.1.1	5.5Ci (AS10Bd)	Connected	[1:Idle] [2:Idle] [3:Idle] [4:Idle]	MS828
7	WTIM	WTIM4 GW	1	192.168.1.1	5.5Ci (A.0Aa)	Connected		MS828

Figure 2.72-1 iPECS SBG-1000 Web Admin. Voice Install View

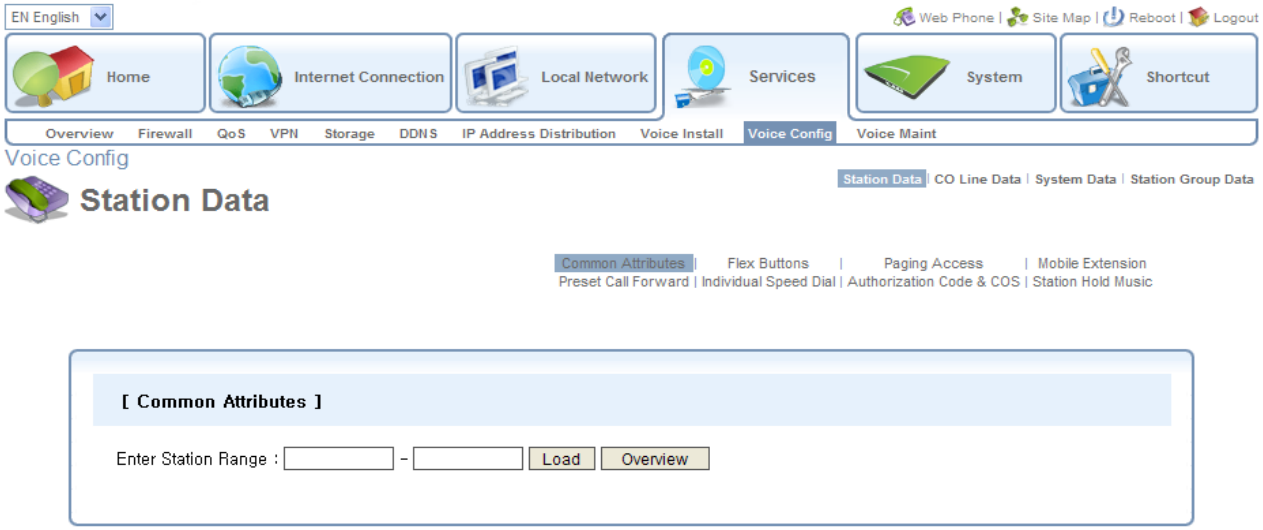


Figure 2.72-2 iPECS SBG-1000 Web Admin. Voice Config View

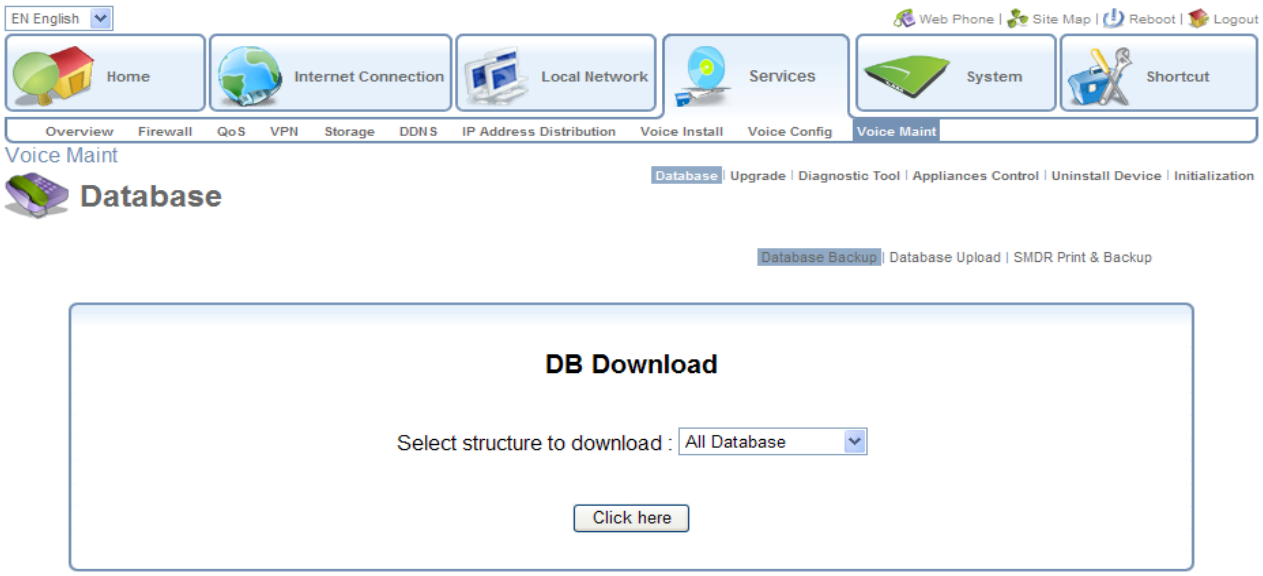


Figure 2.72-3 iPECS SBG-1000 Web Admin. Voice Maint View

For more information on database administration and maintenance, refer to the detailed feature description and operation.

Operation

Operation is detailed in the each feature description and operation.

Conditions

Programming

Related Features

Keyset Administration

Hardware

2.32 TRAFFIC ANALYSIS

Description

The iPECS SBG-1000 monitors, stores and periodically or upon request outputs various traffic statistics covering system resources. The output from the system can be used to:

- Monitor and evaluate system performance
- Observe usage trends and recommend possible corrective actions,
- Determine possible trunk problems (i.e. blocking level too high), and/or
- Recommend system upgrades.

Attendants enable Periodic Reporting. Once enabled, the system continues to monitor and output the requested report until the Periodic Report is disabled. On demand reports selected by the Attendant. The Traffic Report is sent to the defined TCP port.

System resources covered by Traffic Reports are:

- Attendant Traffic Report
- Call Summary Report
- Hourly Call Report
- H/W Unit Usage Summary Report
- CO Summary Report
- Hourly CO Report

Summary Traffic Reports cover one of five Analysis periods selected at time of print:

- Today's peak activity hour (within 24 hours)
- Yesterday's peak activity hour (24 hours prior to Today's activity)
- Last hour activity
- Today's total activity
- Yesterday's total activity.

Operation

Attendant

To print the All Summary Traffic Report periodically:

1. Press the **[PGM]** button.
2. Dial 0122 (All Summary report code).
3. Select hour for print (00-23).
4. Select minute for print (00-59).
5. Select Analysis Period (1-5).
6. Press the **[SAVE]** button.

To cancel the periodic All Summary Report:

1. Press the **[PGM]** button.
2. Dial 0123 (Cancel All Summary report code).

To print a traffic report:

1. Press the **[PGM]** button.
2. Dial 0121, or 0124-0129 (report code),
   - 0121 All Summary Traffic Reports
   - 0124 Attendant Traffic Report
   - 0125 Call Summary Report
   - 0126 Hourly Call Report
   - 0127 Hardware Usage Summary Report
   - 0128 CO Summary Report
   - 0129 Hourly CO Report
3. Press the **[SAVE]** button.

Conditions

1. The Print All Summary Traffic Reports generates the Attendant, Call Summary and CO Summary Traffic Reports.

Programming

Related Features

SMDR Call Records

Hardware

device to capture reports

2.32.1 Traffic Analysis, Attendant

Description

The Attendant Traffic Report covers operational statistics for the Attendants. The report outputs periodically or the Attendant requests output of the report for a defined Analysis period. The following is a sample report and description of the report fields.

```
================================================================================
Site Name   : abc co
Report Type : Attendant Traffic Report - Today Peak
Date        : 19/01/11 15:03
================================================================================

 Atd  Meas --------- Calls ---------  ------ Time ------   Time   Speed  Atd
 No   Hour  Total  Ans Abnd H-Abd Held  Avail   Talk   Held  NoAns  Ans    Type
  10  13:00   104   82   22     3   18  10:12  14:21  01:23  00:52  00:23  Sys

================================ print completed ================================
```

Field	Description
ATD No	Attendant Station Number
Meas Hour	(Measurement Hour) Hour data accumulation began
Calls Total	Total number of calls, except group & recalls, routed to the Attendant
Calls Ans	(Calls Answered) Calls answered during the Analysis period
Calls Abdn	(Calls Abandoned) Calls abandoned before answer by the Attendant, does not include calls abandoned while on hold.
Call H-Abdn	(Calls Abandoned from Hold) Calls abandoned while on hold
Calls Held	Number of calls placed on hold by the Attendant
Time Avail	(Time Available) Time attendant was available to handle new calls
Time Talk	Total time the Attendant was active on calls
Time Held	Time Attendant had calls on hold
Time NoAns	(Time No Answer) Average time calls were ringing or in queue for attendant before abandoned
Speed Ans	(Speed of Answer) Average time calls rang before answer by Attendant
ATD type	(Attendant Type) System or Main

Operation

Attendant

To print the Attendant Traffic Report:

1. Press the **[PGM]** button.
2. Dial 0124 (Attendant Traffic report code).
3. Select Analysis Period (1-5).
4. Press the **[SAVE]** button.

Conditions

1. The Peak Hour is the hour when the system has the highest total call volume.

Programming

Related Features

SMDR (Station Message Detail Recording)

Hardware

Device to capture reports

2.32.2 Traffic Analysis, Call Reports

Description

Call activity statistics are provided in the Hourly Call Reports.

Hourly Call Report

The Hourly Call Report covers hourly completed call activity for the selected Analysis period. The report indicates the number of completed calls for each hour during the Analysis period as shown:

```
================================================================================
Site Name   :
Report Type : Call Hourly Report
Date        : 19/01/11 15:38
================================================================================

  Anal Hour           # Calls Completed
   15:00                    0
   14:00                    0
.....
.....
   17:00                  211
   16:00                  543
   Total Calls    :        754

================================ print completed ================================
```

Operation

Attendant

To print the Hourly Call Report

1. Press the **[PGM]** button.
2. Dial 0126 (Hourly Call report code).

Conditions

Programming

Related Features

SMDR (Station Message Detail Recording)

Hardware

Device to capture reports

2.32.3 Traffic Analysis, H/W Usage

Description

The Hardware Usage report provides statistics for the system's special Hardware resources such as the VSF as shown in the following sample report.

```
================================================================================
Site Name   : abc co
Report Type : H/W Unit Usage Summary Report - Today Peak
Date        : 19/01/11 14:52
================================================================================

  Unit  Num     Anal    Total  Total
  Type  Unit    Hour    Req    Denied
   VSF    4    00:00      0       0

================================ print completed ================================
```

Operation

Attendant

To print the Hardware Usage Summary Report:

1. Press the **[PGM]** button.
2. Dial 0127 (H/W Usage Summary report code).
3. Select Analysis Period (1-5).
4. Press the **[SAVE]** button.

Conditions

Programming

Related Features

SMDR (Station Message Detail Recording)

Hardware

Device to capture reports

2.32.4 Traffic Analysis, CO Reports

Description

The CO Traffic Summary and Hourly reports provide statistics on a summary or hourly basis for CO Group activity. The following provides a sample report and description of the major fields in the report.

```
================================================================================
Site Name   : abc co
Report Type : CO Group Summary Report - Today Peak
Date        : 19/01/11 19:43
================================================================================

 Peak Hour For All CO: 10:00
 Grp Num  Anal   Total Total Inc.  Out.   Grp    %    %
 No  COs  Hour   Usage Seize Seize Seize  Ovfl  ACB  FAO
  1   6 10:00      1    3    0    3    0   0 ---
  2   2 00:00      0    0    0    0    0   0 ---

================================ print completed ================================
```

Field	Description
Grp No.	CO Group number
Num COs	The number of CO lines in the group
Anal Hour	(Analysis hour) hour during the analysis period with peak usage.
Total Usage	Total number of call attempts on CO lines in the Group
Total Seize	Total number of times CO lines in the group were used for any call
Inc Seize	(Incoming Seizures) Total number of incoming calls answered for CO lines in the group.
Out Seize	(Outgoing Seizures) Total number of outgoing calls attempted on CO lines in the group.
ACB	(All COs Busy) Percentage of the time that all CO lines in the group were simultaneously busy.
FAO	(Failed Attempts Outgoing) Percentage of outgoing calls offered to the CO lines in the group that were denied due to All Trunks Busy condition.

Operation

Attendant

To print the CO Traffic Summary Report:

1. Press the **[PGM]** button.
2. Dial 0128 (CO Traffic Summary report code).
3. Select Analysis Period (1-5).
4. Press the **[SAVE]** button.

To print the CO Hourly Traffic Report:

1. Press the **[PGM]** button.
2. Dial 0129 (CO Hourly Traffic report code).
3. Select CO Group (00-05).

Conditions

Programming

Related Features

SMDR (Station Message Detail Recording)

Hardware

Device to capture reports

2.33 VSF INTEGRATED AUTO ATTD/VOICE MAIL

2.33.1 VSF

Description

The Voice Store & Forward (VSF) unit, which is equipped in iPECS SBG-1000, provides the system memory to support the integrated Auto Attendant, Voice Mail and system announcement applications available in the System. The memory is employed to store Auto Attendant announcements, voice mail, greetings and messages, and various system prompts. The system prompts (time, date, etc.) are used by the Auto Attendant and Voice Mail applications as well as other system features. The VSF has a storage capacity of up to 240/480 minutes of announcement and message storage; approximately 10 minutes of storage is generally used for fixed system prompts. The capacity of VSF storage depends on the lock key for the VSF Memory Extend.

2.33.2 VSF-Auto Attendant

Description

When a call comes into the system through a CO line, the call may be routed to one of 70 user recorded VSF Announcements. An announcement is assigned as a Station Group announcement or as Auto Attd announcement with an CCR Table that permits Caller Controlled Routing (CCR).

Station Group announcements are played when a call is routed to the group based on definitions in the Station Group Attributes.

For an Auto Attd Announcement the system will play the announcement and monitor for digits from the connected external party. A CCR Table defines a dialed digit (0 – 9) to a route. Each single digit is defined a corresponding route:

- Station
- Station group
- Speed Dial number
- Page Zone
- Voice Mail
- VSF Announcement

In addition, the system will monitor digits for a station number. If the user dials a station number, the Auto Attd will complete an unsupervised call transfer to the station.

Operation

Attendant

To record an Auto Attd Announcement:

1. Press the **[PGM]** button.
2. Dial 05 (Message Record code).
3. Dial the appropriate number from 001-072 (Announcement number).
4. The current announcement is played followed by the Press # to record prompt.
5. Dial '#'.
6. After the record prompt and beep-tone, record message.
7. Press the **[SAVE]** button to stop recording and save the message.

To delete a recording:

1. Press the **[PGM]** button.
2. Dial 05 (Message Record code).
3. Dial the appropriate number from 001-072 (Announcement number).
4. The current announcement is played followed by the "Press # to record" prompt.
5. Dial '#'.
6. Press the **[SPEED]** button during playback to erase message

System

Operation of the CCR Tables and Auto Attendant are automatic.

Conditions

1. There are no individual time limits on an Auto Attendant announcement.
2. The external caller may receive a ring-back tone before playback of a VSF announcement.
3. The Attendant must "Save" a recording before returning to the on-hook state, otherwise, the existing recording is used.
4. To record or delete an Auto Attendant message, all of the VSF channels must be idle.

5. The external caller may dial at any time during an Auto Attendant announcement and must dial prior to the expiration of the CCR Analysis timer.
6. If the external caller dials an invalid selection or station, the system will play the 'Invalid Entry' prompt and allow re-entry using the DISA Retry Counter.
7. If the external caller dials more than a single digit, the call is routed based on the System Numbering Plan.
8. Calls routing by an Auto Attendant (CCR) Announcement are interactive DISA calls and are subject to conditions of a DISA call.
9. The '*' digit is reserved in the CCR Tables to repeat the current or previous Auto Attd announcement.
10. The '#' digit is reserved for callers to access their Voice Mail-box remotely.
11. A CCR Announcement may be programmed to disconnect after playing.
12. The Auto Attd Announcement feature is supported for DISA and DID calls.
13. System announce number 71 is for the MOH.

Programming

VOICE CONFIG	Station Group Data
	CO Line Data – Call Routing by Line
	CO Line Data – Ring Assignment Table
	CO Line Data – Call Routing by Auto Attendant
	System Data – Call Feature Timer – VSF User Maximum Record Timer
	System Data – Call Feature Timer – VSF Valid User Message Timer

Related Features

Station Groups
Remote Message Retrieval

Hardware

VSF

2.33.3 VSF Voice Mail

2.33.3.1 Message Storage

Description

When a station activates Call Forward to the VSF Group, a call is transferred to a VSF mail box or a transferred call recalls to the VSF, the call is handled by the iPECS SBG-1000 Mail application. The caller connects to the called station's User Greeting followed by a beep tone.

The remote caller can record a message and hang-up or dial '*' for further options. When disconnect occurs, the VM application stores the message in the called user's voice mail-box and activates the Message Waiting indication at the user's station.

Operation

Remote Caller

To leave a voice message after hearing announcement:

1. Wait for the beep, then leave a message.
2. Hang up to quit recording,

Or,

2. Dial '*' for more options.

Conditions

1. Two timers are provided to control voice message length. The Valid User Message Timer establishes the minimum voice message length; voice messages shorter than this timer are not stored. The VSF User Maximum Record Timer establishes the maximum voice message length; when the VSF User Maximum Record Timer expires while recording a voice message, confirmation tone is heard and the message is saved for the destination station.
2. If all the VSF channels are in use, the Ring Back tone is provided until a VSF channel is available.
3. All stations including, SLTs can leave and receive voice messages.
4. Individual User Greetings and Voice Mails are protected from AC power loss.

Programming

VOICE CONFIG	Station Data – Preset Call Forward – Transfer Mail Box
	System Data – Call Feature Timer – Call Forward No Answer Timer
	System Data – Call Feature Timer – VSF User Maximum Record Timer
	System Data – Call Feature Timer – VSF Valid User Message Timer

Related Features

Call Forward
Station Message Wait/Call Back
VSF Voice Mail
Call Transfer, Voice Mail

Hardware

VSF

2.33.3.2 Message Retrieval

Description

A user can access their Mail Box locally by placing a call to the VSF Voice Mail group, or from an LIP Phone, by pressing the **[MSG]** button, or by pressing a **{VMAIL-BOX}** button while off-hook receiving Intercom dial tone.

Prompts are then received to guide the user in the Voice Mail Box operation. The user must enter a Mail Box number, generally the station number, and a corresponding password in response to the "Request for Password" *("Please enter your password code."*) prompts.

If the user enters a valid and matching Mail box and password, the "Number of Messages" prompt *("You have xx new messages, You have yy saved messages."*) is received. At this point, the user also receives the "VM long option prompt" *("To play new messages, press one, to play saved messages, press two, to set greeting or password, press eight, to disconnect, press pound, Press 0 for the operator, Press nine to hear this message again.")*.

When the user responds by dialing 1, the first new message is played. At the end of message playback, the "New Message option" prompt is played *("To replay message, press one, to listen to the next message, press two, to delete message, press three, to forward message, press four, to call the sender, press five, to skip message, press six, to return to main menu, press nine.")*. This process is repeated until the last new message is played and the "No Message" prompt *("No Messages")* is played.

When the user dials 2 in response to the "Number of Messages" prompt, the first-saved message is played. At the end of the message, the "Saved Message option" prompt is played *("To replay message, press one, to listen to the next message, press two, to delete message, press three, to forward message, press four, to call the sender, press five, to return to main menu, press nine.")*. This process is repeated until the last new message is played and the "No Message" prompt *("No Messages")* is played.

In addition to the options indicated in the prompt, a user can record a memo, which is attached to the current voice mail by dialing the digit 7. The current voice mail and memo can then be forwarded to other Smart Business gateway users.

When the user dials 9 in response to the "Number of Messages" prompt or during or at the end of a message the "VM long Options" prompt is played.

Operation

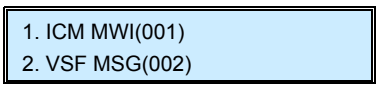
***LIP P*hone**

To assign a {vmail-box} Flex button:

1. **[PGM]** + **{FLEX}** + VM group + Mail-box (station) number + **[SAVE]**

To retrieve Voice Mail locally:

1. Lift the handset or press the **[SPEAKER]** button.
2. Press **[MSG]** button; the message contents summary is shown.



3. Dial digit '2' to select VSF Messages
4. Dial the Mail Box and corresponding password to receive the "Number of Messages" prompt.
5. Dial desired option code.
6. At completion of session, hang-up to return to idle.

Or,

1. Lift the handset or press the **[SPEAKER]** button
2. Press **{VMAIL-BOX}** button.
3. Dial the Mail Box and corresponding password to receive the "Number of Messages" prompt.

4. Dial desired option code.
5. At completion of session, hang-up to return to idle.

To attach a memo to the current voice message:

1. During or after the New or Old Message option prompt, dial ‘7’.
2. At the beep, record the memo.
3. Dial ‘*’ to stop recording and store the memo.
4. During or after the New/Old option prompt, dial 4 to forward the message and memo.

SLT

To retrieve Voice Mail locally:

1. Lift the handset.
2. Dial the Voice Mail Group to receive the “Mail Box & Password” prompts sequentially.
3. Dial the Mail Box and corresponding password to receive the “Number of Messages” prompt.
4. Dial desired option code.
5. At completion of session, hang-up to return to idle.

To attach a memo to the current voice message:

1. During or after the New or Old Message option prompt, dial ‘7’.
2. At the beep, record the memo.
3. Dial * to stop and store the memo.
4. During or after the New Old option prompt, dial ‘4’ to forward the message and memo.

Conditions

1. If no new/old messages are available, pressing ‘1’ or ‘2’, is an invalid operation and the user receives the “Invalid Entry” prompt or “No Message” prompt.
2. If the dialed number is not recognized, the "Invalid Entry" prompt is played. After the second invalid entry, the user is disconnected.
3. The user may dial digits at any time during a voice mail playback, system prompt or silence; the user must dial a digit in response to a system prompt within the CCR Analysis timer or the system will disconnect and return error tone.
4. Messages are retrieved in LIFO (Last in First out) order.

Programming

Related Features

Message Retrieval Options
Remote Message Retrieval

Hardware

VSF

2.33.3.3 Remote Message Retrieval

Description

The system permits remote users access to their mailbox. After accessing the VSF Voice Mail, operation follows the local procedures.

Operation

Remote Caller

To access Voice Mailbox from a remote location

1. Lift the handset.
2. Dial the telephone number of a DISA assigned CO line assigned for answer by a VSF Auto Attd.
3. Upon answer, dial '#' to receive the "Request for Mail Box number" prompt.
4. Follow local access procedures.

Conditions

1. The conditions associated with Message Retrieval and Message Retrieval Options apply.
2. The conditions associated with DISA apply.

Programming

Related Features

Message Retrieval Options
VSF-Auto Attendant
Message Retrieval

Hardware

VSF

2.33.3.4 Message Retrieval Options

Description

The user may dial the digit 9 to receive the "VM Long Options" prompt while in the Voice Mail Box, including during or after a voice message or system prompt, except when an option has been selected that requires user dialing. Some options involving user dialing include the Message Retrieval Option 1/2 (Play New/Saved Message), 7 (Cancel or Forward message, Remote Access Only) or 8 (Mail Box settings), refer to Table. The "VM long Options" prompt is:

"To play new messages, press one, to play saved messages, press two, to set station forwarding, press seven (This option is available only for remote access), to set greeting or password, press eight, to disconnect, press pound, Press 0 for the operator, Press nine to hear this message again."

The VSF Voice Mail will respond to incoming digits as shown in the following table.

Digit	Function
1	Play New Msg
2	Play Saved Msg
7	Set Cancel/Fwd, available only for remote access
8	Mail Box Setting, "Mailbox Settings" prompt
9	VM Long options
#	Drop, "Goodbye"
0	Attd Call, Call to Attendant.

Operation

LIP Phone

To access a Message Retrieval option

1. At any time after the “Number of Messages” prompt, dial a Message Retrieval Option digit. The system initiates the selection providing any needed prompts.

SLT

To access a Message Retrieval option

1. At any time after the “Number of Messages” prompt, dial a Message Retrieval Option digit. The system initiates the selection providing any needed prompts.

Conditions

1. The user must begin dialing within the CCR Analysis timer in response to a system prompt. If the timer expires, the system will disconnect the call and the user will receive an error tone.
2. If the user remains off-hook after a call placed through the voice mail is complete, the user will be returned to the previous place in the Voice Mail Box. If the user hangs up, the VSF will recall at the user Station, and upon answer will play “Request Mail Box Number” prompt.

Programming

Related Features

Message Retrieval
Remote Message Retrieval
Voice Mailbox Settings

Hardware

VSF

2.33.3.5 Voice Mailbox Settings

Description

The user can program the Mail Box settings for their mailbox including a security password and a greeting. When a user presses "8" while retrieving messages, the "Mailbox Setting" prompt, *(“To*

edit your greeting, press one, to edit you password, press two. To return to main menu, press nine").

Operation

To program Mail Box settings while “in” the Voice Mail Box:

1. Press ‘8’, for Mail Box settings; the “Mail Box Setting” prompt is received.

To enter a new password:

1. Dial ‘2’ to receive the “Password Entry” prompt (“Please enter your new password and press pound when finished.").
2. Dial new password.
3. Press ‘#’; the “Reenter Password” prompt will be heard ("Please re-enter your password to confirm and press pound when finished.").
4. Dial new password again.
5. Press ‘#’ and the “Password Confirmation” prompt will be heard *("Your password is saved.")*.

To create a new greeting:

1. Dial ‘1’ to hear the “Greeting Option” prompt ("To listen to your current greeting, press five to record a new greeting, press seven, to return to the main menu, press nine.”).
2. Dial ‘5’, to hear your greeting.

OR

3. Dial ‘7’ to hear the “Record Greeting” prompt ("At the tone, record your new greeting, press # when done.").
4. After the beep, record your desired greeting speaking in a normal voice.
5. Press ‘#’ and receive the “Greeting Confirmation” prompt ("Your greeting is saved.").

Conditions

1. If the user is external, the user must begin dialing within the CCR Analysis time, if not the call is released.
2. If the dialed number is not recognized, the "Invalid Entry" prompt is played.
3. The user must assign a password (Authentication code, up to 12 digits) before access to the mailbox will be allowed.

   📖 ***NOTE:*** *A greeting does not have to be recorded.*

Programming

Related Features

Message Storage
Message Retrieval
Remote Message Retrieval
Message Retrieval Options

Hardware

VSF

2.33.3.6 Call Forward from VM

Description

External users can activate or deactivate Call Forward for their station. Pressing ‘7’ while retrieving messages will return the "Mailbox Set Forward" prompt, (“To forward calls to another extension, press one. to cancel forwarding, press 2 to return to the main menu, press nine.”).

Operation

To activate Call Forward while in the VM:

1. Press ‘7’, for Mail Box set forward, the “Mail Box Set Forward” prompt is received.

To activate Call Forward:

1. Dial ‘1’ and receive the “Password Entry” prompt (“Please enter the number to forward to ...").
2. Dial the Station Number as follows:
   - To forward to another station, dial the station number.
   - To forward calls Off-net, dial ‘*’ and enter Individual Speed number. If the Individual Speed bin is valid, the confirmation announcement “forwarded to station ('xxx')” or “forwarded to speed bin number (yyyy)” is played.

To deactivate Call Forward:

1. Dial ‘2’ and receive the “Station forwarding is canceled” prompt.

To return to the Main menu:

1. Dial ‘9’ and receive the “Mail Box Settings” prompt.

Conditions

1. If the user is external, the user must begin dialing within and dial subsequent digits within the VSF Inter-Digit Timer; if not, the call is released.
2. This Mail Box Set Forward is only available for external users.

Programming

Related Features

Message Storage
Message Retrieval
Remote Message Retrieval
Message Retrieval Options

Hardware

VSF

2.33.3.7 Outbound Message Notification

Description

The VSF is able to dial an external number to notify a user of a new voice message. The system employs the mobile extension number registered for the station receiving the message. When a caller leaves a message with notification configured, the system places a call to the registered mobile extension. When the user answers, the extension prompt is played followed by the new message prompt, ("You have xx new messages."). The new message prompt indicates the number of unheard messages.

The user must listen to the new message to confirm the notification. If the user takes no action within the CCR Inter-digit timer or hangs-up, the call is disconnected and the system will retry the call after the retry timer expires, until the user listens to the message or the number of attempts reaches the retry counter. If the user does not answer, the ISDN or VoIP connection times out or disconnects before answer, or is busy, the system disconnects the notification and will retry the call after the retry timer. The system will retry the notification until the notification is successful or the number of call attempts reaches the Retry count.

Operation

Operation of message notification is automatic when configured.

Condition

1. Outbound notification over a PSTN line is not available.
2. Caller Id will be the external caller who left the message or, for messages from another station, Caller Id will be the station receiving the message.
3. If VSF Notify is changed to 'Not Use', any existing notification will be terminated after the initial notification call.
4. For proper operation, the Station COS and CO Group access for the station must be such as to allow the notification call.
5. The destination of the notification is the Mobile telephone number assigned in Mobile Extension table.
6. If all lines in the assigned CO group are busy when the system attempts to place the notification call, the System will continuously try to seize CO line until a line is successfully seized.
7. The Retry counter is incremented after the system access the CO line for notification.
8. The Retry count is from 1 to 9; the retry interval is from 1 to 3 minutes.
9. If a new message is logged before answer of the notification call, the message will be available to the user and a new notification is not invoked. If a new message is received after answering the notification call, the System will invoke another notification call. The user will receive the notification after returning to idle.

Programming

VOICE CONFIG Station Data – Mobile Extension

Related Features

Mobile Extension

Message Retrieval
Remote Message Retrieval
Message Retrieval Options

Hardware

VSF

2.34 WAKE-UP ALARM

Description

This feature allows a user or Attendant to set a wake-up time or desired time to be alerted. When the time is reached, the system will signal with an audible and visual signal.

Operation

Attendant

To register Wake-Up:

1. Press the **[PGM]** button.
2. Dial 023 (Attendant Station Program code).
3. Dial the desired station range, for a single station, enter an '*' in place of the second station number.
4. Dial 2-digit hour and 2-digit minute for alerting.
5. For a daily (repeating alarm), dial '#'.
6. Press **[SAVE]** button.

To erase Wake-Up:

1. Press the **[PGM]** button.
2. Dial 024 (Attendant Station Program code).
3. Dial the desired station range, for a single station, enter an '*' in place of the second station number.
4. Press **[SAVE]** button.

LIP Phone:

To register Wake-Up:

1. Press the **[PGM]** button.
2. Dial 21 (Set Wake-up code).
3. Dial 2-digit hour and 2-digit minute for alerting (hh:mm).
4. For a daily (repeating alarm), press '#'.
5. Press **[SAVE]** button.

To stop the alarm notification:

1. Lift the handset or press **[SPEAKER]**.

To erase Wake-Up:

1. Press the **[PGM]** button.
2. Dial 22 (Erase Wake-up code).
3. Press **[SAVE]** button.

SLT

To stop the alarm notification:

1. Lift the handset.

Conditions

1. When receiving a wake up signal, lifting the handset will be heard Wake-up alarm prompt.
2. The Wake-up alarm Ring signal is 30 seconds, On/90 seconds, Off (3 times). If no action is taken by the user, the ring signal is given to the Attendant with a display designating the station number that did not respond.
3. Time (hh:mm) must be entered in the Military 24-hour format.
4. The daily alarm will reset and repeat each day until erased (cancelled)' the One-time alarm will reset and cancel automatically.

Programming

Related Features

Hardware

2.35 DIRECT STATION SELECT/BUSY LAMP FIELD (DSS/BLF)

Description

When a Flex button on an LIP Phone is assigned as a **{DSS}** button it also serves as a Busy Lamp Field; the LED indicates the status of the associated station or system facility.

Operation

LIP Phone

Operation of this feature is automatic for assigned Flex buttons.

Conditions

1. A station receiving ICM ringing that is busy will show the DSS button LED on all other stations flashing at 30 ipm.
2. A station receiving ICM ringing will receive visual indication with a flashing LED of the Flex button associated with the calling station.
3. When a station receives a Camp-On, the LED of the DSS button associated with the calling station will flash.

4. The station is considered busy when:
   - in use,
   - receiving ICM Ring at an LIP Phone,
   - receiving any ring at an SLT.

Programming

Related Features

Intercom Call (ICM Call)
Station User Programming & Codes

Hardware

2.36 INTERCOM CALL (ICM CALL)

Description

A non-blocking ICM is available to all stations in the system. Users may place an intercom call to other stations in the system by dialing applicable digits as defined in the system Numbering Plan.

Operation

LIP Phone

To place an intercom call:

1. Lift the handset or press the **[SPEAKER]** button to receive ICM dial tone.
2. Dial station number or press the **{DSS/BLF}** button.
3. For ring-back tone, await answer or
   For Intercom splash-tone, speak and await answer.

SLT

To place an intercom call:

1. Lift the handset to receive ICM dial tone.
2. Dial station number.
3. For ring-back tone, await answer or,
   For Intercom splash-tone, speak and await answer.

Conditions

1. Intercom Dial tone will time-out if action is not taken within Dial-Tone Time or, if the time between digits exceeds the Inter-digit Timer; error tone is received on dial tone time-out.
2. ICM Dial tone is halted after dialing the first digit.
3. If the called station is busy, Intercom Busy tone is provided for the Busy Tone time (7 sec.) then, Error tone is sent by the system; the caller may disconnect or activate a feature such as Message Wait/Callback.

4. For LIP Phone users, consecutive Intercom calls can be placed without the need to regain ICM dial tone (no need to hang-up) between calls; the user simply presses another **{DSS/BLF}** button.
5. An Intercom call to a station in the HF answerback or Voice Announce mode (H or P Intercom Signaling Mode) is not considered answered unless the called user lifts the handset or presses the **[SPEAKER]** button (goes off-hook).

Programming

VOICE CONFIG	System Data – Call Feature Timer - ICM Dial Tone Timer
	System Data – Call Feature Timer – Inter Digit Timer

Related Features

Intercom Answer Mode
Speakerphone

Hardware

2.37 INTERCOM CALL HOLD

Description

While on an active ICM Call, LIP Phone users can place the ICM Call on hold; the held station will receive the assigned Music-on-Hold. The call is placed on Exclusive Hold and recalls at the holding station when the Exclusive Hold Recall timer expires.

Operation

LIP Phone

To assign a **{ICM}** Flex button:

1. **[PGM]** + **{FLEX}** + **[PGM]** + '53' + **[SAVE]**

To place an active ICM call on hold:

1. Press the **[HOLD]** button; the ICM dial tone is received and the **{ICM}** button LED will flash at the exclusive hold rate and the ICM dial tone is received.

To retrieve the held ICM call:

1. Press the **{ICM}** button or the **{DSS/BLF}** button associated with the held station; the **{ICM}** button LED will be On and the ICM call connected.

Conditions

1. Only one ICM call may be placed on hold at a time.

Programming

Related Features

MOH (Music-On-Hold)
Intercom Call (ICM Call)
Hold Recall

Hardware

LIP Phone

2.38 INTERCOM CALLER CONTROLLED ICM SIGNALING

Description

A user can change the signaling mode of an Intercom call from Tone ring to Voice announce, or Voice announce to Tone ring.

Operation

LIP Phone

To change the ICM Signaling mode:

1. Place intercom call.
2. Dial '#', ICM Signaling mode will change from Voice announce to Tone ring or Tone ring to Voice announce.

SLT

To change the ICM Signaling mode:

1. Place intercom call as normal.
2. Dial '#', ICM Signaling mode will change from Voice announce to Tone ring, or Tone ring to Voice announce.

Conditions

1. If the signaling mode is changed, the call is not subject to Call Forward, No Answer.
2. The signaling mode for a specific Intercom call can only be changed once and can not be changed back to the original signaling mode.
3. Changing the signaling mode does not affect privacy at the called station.

Programming

Related Features

Intercom Answer Mode

Hardware

2.39 INTERCOM LOCK-OUT

Description

If the user takes no action after going off-hook for the Dial Tone timer or fails to dial an additional digit within the Inter-digit timer, the station will receive an error tone for 30 seconds and be placed out-of-service (locked-out). The LED of associated **{DSS/BLF}** buttons will flutter (flash) rapidly to indicate the out-of-service status.

For LIP Phone users, if the **[SPEAKER]** is used, the station will receive an error tone for 30 sec. and then automatically return to idle.

Operation

System

Operation of Intercom Lock-out is automatic based on the Dial Tone & Inter-digit timers.

Conditions

1. Error tone is presented for 30 sec. followed by 30 sec. of Howler tone followed by lock-out and silence.

Programming

VOICE CONFIG	System Data – Call Feature Timer - ICM Dial Tone Timer
	System Data – Call Feature Timer – Inter Digit Timer

Related Features

Intercom Call (ICM Call)

Hardware

2.40 INTERCOM STEP CALL

Description

When the busy tone is received on a dialed Intercom call, the user may place a call to another station by dialing the last digit of the station number. The system replaces the last digit of the previously dialed busy station with the dialed digit and places an Intercom call to the new station number.

Operation

LIP Phone

To activate step call, while receiving busy on a dialed Intercom call:P

1. Dial a digit other than the last digit of the busy station’s intercom number.

Conditions

1. If the user dials the last digit of the busy station, Camp-On will be activated.
2. After receiving busy tone, if the user takes no action for the Busy Tone timer, the system will start the Intercom Lock-out procedure.
3. For Step Call to work, the ICM Station called must have the same digits except for the last digit.

Programming

Related Features

Intercom Lock-Out
Intercom Call (ICM Call)

Hardware

2.41 MESSAGE WAIT/CALL BACK

2.41.1 Station Message Wait/Call Back

Description

A station can activate a Message Wait indication requesting a Call Back when the called station does not answer or is in DND. A station may receive a Message Wait from any number of other stations in the system. The station receiving the Message Wait can return the calls to the station using the **[MSG/CALLBK]** button.

When a busy station is called, the calling user may request to be placed in a queue to receive a Call Back. When the called station returns to idle, the system signals the initiating station with Callback ring. When the user answers, the now idle station is called.

Operation

LIP Phone

To leave a Message Wait, while receiving ring back tone or no response on a call announce (H or P mode):

1. Press the **[MSG/CALLBK]** button; confirmation tone received.
2. Hang up, Message Wait is activated.

To leave a Message Wait, while receiving DND tone:

1. Press the **[MSG/CALLBK]** button; confirmation tone received.
2. Hang-up, Message Wait is activated.

To leave a Call Back (queue for a station), while receiving busy notification:
1. Press the **[MSG/CALLBK]** button; the user receives confirmation tone.
2. Hang up, to return to idle.

To respond to a Call back recall received when the busy station becomes available:
1. Lift the handset, or press the **[SPEAKER]** button.
2. Previously busy station is called.

To retrieve Station Messages Waiting:
1. Press **[MSG/CALLBK]** button; either the message contents summary will be shown as below.

1. ICM MWI(001)
2. VSF MSG(002)

2. Dial '1' to select ICM MWI (Station Message Wait)
    - '1' – ICM MWI, Station Message Wait,
    - '2' – VSF MSG, VSF Message Wait

To return a call from the current Station Message:
1. Press the **[SAVE]** button.

To delete the first Message Wait from the list:
1. Press '*' button
2. Press '1' button to confirm the deletion, the list is updated removing the first station number in the list.

To delete all Message Waits:
1. Press '*' button.
2. Press '3' button.

SLT

To leave a Message Wait, while receiving ring back tone or no response on a call announce (H or P mode):
1. Momentarily press the hook switch.
2. Dial 56 (Message Wait/Call Back code).
3. Hang up, Message Wait is activated.

To leave a Message Wait, while receiving DND tone:
1. Momentarily press the hook switch.
2. Dial 56 (Message Wait/Call Back code).
3. Hang up, Message Wait activated.

To retrieve a Station Message Wait:
1. Dial 57 (Message Wait/Call Back Answer code).

To leave a Call Back (queue for a station), while receiving busy:
1. Momentarily press the hook switch.
2. Dial 56 (Message Wait/Call Back code).
3. Hang up, return to idle.

To respond to a Call back recall, received when the busy station becomes available:

1. Lift the handset.
2. Previously busy station is called.

Conditions

1. A Message Wait/Call Back return call will always ring at the receiving station overriding the Intercom signaling mode selected.
2. A station can leave only one callback request at a time.
3. If a station is attempting to leave a message and the system Message Wait queue is full, the station will receive ICM busy tone.
4. A Message Wait reminder tone can be enabled to remind the user of messages waiting.
5. A station in Call Forward can leave a message wait.
6. A Message Wait indication is left at the originally-called station even if the call is forwarded.
7. An LIP Phone with LCD may call back to the station(s) that left messages in any desired order, or the normal (“oldest first”) order.
8. Placing an Intercom call to a station will cancel any existing Message Wait from that station.

Programming

VOICE CONFIG System Data – Call Feature Timer – MSG Wait Reminder Tone Timer

Related Features

Message Wait Reminder Tone

Hardware

2.41.2 Message Wait Reminder Tone

Description

LIP Phones can be sent a tone as a periodic reminder to the user of message waits in queue. This tone is sent to the station only while idle and is heard over the speaker.

Operation

System

Reminder tone is sent to stations automatically when assigned.

Conditions

1. Interval set between tones can be 00 to 60 minutes; the 00 setting disables the reminder tone.
2. The reminder tone will continue until all messages have been retrieved.
3. A station that is busy or in DND will not receive the Message Wait Reminder tone until it returns to idle.

Programming

VOICE CONFIG System Data – Call Feature Timer – MSG Wait Reminder Tone Timer

Related Features

Message Wait/Call Back

Hardware

LIP Phone

2.42 PAGING

2.42.1 Paging & All Call Paging

Description

A station can connect and transmit voice announcements to any or all of the system Paging zones. Stations are grouped into “zones” to receive pages to the zone. Stations not assigned to any zone will not receive a page including All Call pages.

A page warning tone will be provided to the Paging Zone(s) prior to the audio connection. The user is allowed to continue the page for the specified Page Time-out timer after which the user is disconnected and the Paging Zone(s) is returned to idle.

The default Paging Zone dial access codes are as follows:

Paging Zones	501~510
All Call Page	500

Flexible buttons of an LIP Phone may be assigned to access a Paging Zone as a **{PAGING ZONE}** button.

Operation

LIP Phone

To assign a Flex button as a {paging zone} button:

1. Lift the handset, and press **[PGM]** + **{FLEX}** + Paging Zone number + **[SAVE]**

To make a page:

1. Lift the handset.
2. Dial the desired paging code or press a **{PAGING ZONE}** button.
4. After the Page Warning Tone, make announcement.
5. Replace the handset to return to idle.

To queue for a page when busy is received:

1. Press the **[MSG/CALLBK]** button.
2. Replace the handset to return to idle.

SLT

To make a page:

1. Lift the handset.
2. Dial the desired paging code.
3. After the Page Warning Tone, make announcement.
4. Replace the handset, to return to idle.

To queue for a page when busy is received:

1. Dial 56 (Call Back code).
2. Replace the handset returning to idle.

Conditions

1. Stations dialing a Page Code will be queued when any of the other Paging zones are busy.
2. If an LIP Phone user attempts to page using the speakerphone, pre-selection will be activated and display will show "LIFT THE HANDSET TO PAGE".
3. Stations receiving a page are considered idle for other incoming calls and ring will override Page announcements over an LIP Phone speaker.
4. Stations in DND or busy will not receive Page announcements.
5. A station accessing a Paging Zone is considered busy.
6. Stations which are not included in a Paging Zone will not receive any page, including All Call.
7. A station is permitted only one Paging Zone queue request at a time; if a station attempts another Paging Zone queue, only the last-received queue request is honored.
8. When a busy Paging Zone becomes idle, the system will select the oldest paging queue, and signal the appropriate station; the signaled station will have an audible ring (distinctive ring) indicating the queue callback.
9. The All Call Paging, while signaling the queued station, is considered busy; additionally, All Call Paging is considered busy when any paging zone is active.
10. The queue recall is always in tone ring mode regardless of the station's ICM signaling mode.
11. If the waiting station is idle, the Call Back ring signals the station for 15 sec., after which the queue is canceled and the next station in the queue is signaled.
12. If the waiting station is busy, and the Paging zone becomes available, the next idle station in the Paging Queue list is signaled and the busy waiting station is placed at the bottom of the Paging Queue list. If there is no idle next station in the Paging Queue, the Paging Queue is canceled.
13. When the waiting station goes to idle, and both a "Paging Queue" and "CO Call back Queue" exist, the Paging Queue is given priority.

Programming

VOICE CONFIG	Station Data – Paging Access
	System Data – Call Feature Timer – Paging Timeout Timer

Related Features

Meet Me Page Answer

Hardware

2.42.2 Meet Me Page Answer

Description

Any station may respond to a “Meet Me” Page request over a Paging Zone; the user can answer the page from any station and be connected to the paging party.

Flexible buttons of an LIP Phone may be assigned as a **{MEET ME}** button.

Operation

LIP Phone

To assign a Flex button as a {meet me} button:

1. Lift the handset, press **[PGM]** + **{FLEX}** + ‘511’ + **[SAVE].**

To answer a page with Meet Me Page:

1. Lift the handset, or press the **[SPEAKER]** button.
2. Dial 511 (Meet Me Page code) or press the **{MEET-ME}** button.
   Or
3. Press the [HOLD] button.

SLT

To answer a page with Meet Me Page:

1. Lift the handset to receive intercom dial tone.
2. Dial 511 (Meet Me Page code).

Conditions

1. A Meet Me Page must be answered within the Page Time-out timer.
2. A station may answer a Meet Me Page from any station regardless of pickup/paging group assignments and page access permission.
3. The paging party must remain off-hook until the paged party answers the Meet Me request; the initiator may press the Mute button to eliminate transmitting over the page circuit while waiting for the party to answer.

Programming

VOICE CONFIG	System Data – Call Feature Timer – Paging Timeout Timer

Related Features

Paging & All Call Pag

Hardware

2.43 CO RING ASSIGNMENT

Description

Each station in the system can be programmed to provide an audible signal when the system detects an incoming call on specified CO lines. Separate ring assignments are made for Day, Night and Timed Ring operation mode. In addition, the audible signal at the station can be delayed by 1 to 9 ring cycles allowing other stations to answer the call first.

Operation

System

Operation of this feature is automatic.

Conditions

1. Separate assignments are made for stations to ring in the Day, Night, and/or Timed Ring mode.
2. A busy station receives the Muted ring or Call Waiting tones (as appropriate) for the station's off-hook ring assignment.
3. The system Ring mode can be selected manually or automatically. In Automatic mode, Day/Night selection is determined based on the Automatic Ring Mode Selection table; the Attendant has manual control over the Ring mode selection.
4. The Attendant's LCD displays Night and Timed Ring Mode and the **[DND]** button LED will flash.
5. If a CO line is not assigned to ring at any station, incoming calls on the CO line will ring the first available Attendant.

Programming

VOICE CONFIG	CO Line Data – Call Routing by Line
	CO Line Data – Ring Assignment Table
	System Data – Day/Night/Timed Schedule

Related Features

Day/Night/Timed Ring Mode
Off-Hook Signaling

Hardware

2.44 CO LINE RELEASE GUARD TIME

Description

To assure that the PSTN switching equipment has sufficient time to restore the idle status, the system will hold CO lines in a busy state to users after release of a CO line by a station. The time

between station disconnect and when the system changes the CO line status from busy to idle is the CO Line Release Guard time.

Operation

System

Operation of this feature is automatic.

Conditions

Programming

VOICE CONFIG	System Data – Call Feature Timer – CO Release Guard Timer

Related Features

Hardware

2.45 IP TRUNKING

2.45.1 SIP Service

Description

When assigned to support Session Initiation Protocol (SIP), VoIP channels provide protocol conversion between SIP and the iPECS protocol. This permits the VoIP channel to connect to external SIP networks for call services. In addition, to the IETF RFC-3261 SIP draft standard, iPECS SBG-1000 VoIP channels support other SIP-related RFCs including:

RFC-2617	HTTP Authentication, Basic & Digest
RFC-3515	Refer Method
RFC-3264	Offer/Answer Model
RFC-3265	SIP Basic Call Flow Examples
RFC-3891	SIP “Replaces” Header

Using the SIP database assignments, the system will register and authenticate with the SIP proxy server permitting the system to interoperate employing SIP to establish, manage and terminate real-time voice sessions with external parties.

Operation

System

Operation of SIP Service is automatic.

Conditions

Programming

VOICE INSTALL	CO Line Registration – Server Information
	CO Line Registration – SIP ID Configuration

Related Features

Hardware

2.46 CALLING/CALLED PARTY IDENTIFICATION

Description

The iPECS SBG-1000 system receives calling party identification in SIP INVITE message or the ISDN call Set-up message, Calling Line Identification Presentation (CLIP). The answering party identification, which may be different from the called party, is received in SIP 200 OK message or the ISDN connect message, Connected Line Identification Presentation (COLP). When provided, the LCD of LIP Phones displays the identification, which is included in call records.

LIP Phone Display is shown:

```
LINE RINGING
CLI 03438502821
```

The system will also compare the identification to programmed Speed Dial bins; when a match exists, the Name of the Speed Dial bin displays in place of the number, CO Name display.

The system will send calling and answering party identification in the appropriate messages to SIP or the ISDN based on the database. Identification messages may be restricted, not reported, to the far-end user. Calling Line Identification Restriction and Connected Line Identification Restriction may be enabled in the system database or by **{CLIR}** and **{COLR}** Flex buttons.

Operation

System

Operation of this feature is automatic.

LIP Phone

To program **{CLIR}** button:

[PGM] + **{FLEX}** + **[PGM]** + '43' + **[SAVE]**

To program **{COLR}** button:

[PGM] + **{FLEX}** + **[PGM]** + '44' + **[SAVE]**

To activate CLIR or COLR, before placing or answering a SIP call or an ISDN call

1. Press the **{CLIR}** or **{COLR}** Flex button.

Conditions

1. This feature may not be available in the specific SIP/ISDN service area or may be a subscription service.

Programming

Related Features

Hardware

2.47 ANSWERING MACHINE EMULATION

Description

When a call is sent to a voice mail-box, the associated station can be assigned to notify the user and allow the user to screen the call. Two methods of notification and call screening are:

- Ring mode – the user is notified by the Answering Machine Emulation (AME) Flex button (if programmed), which will flash; the user may press the Flex button to screen the caller as the voice message is stored.
- Speaker mode - when the call is sent to the Voice Mail-box, the caller's voice is automatically broadcast over the speaker of the user's LIP Phone.

The user may terminate screening, and either leave the caller in voice mail to record a message, talk with the caller and record the conversation in the mail-box, or answer the call and disconnect the Voice Mail.

The user's LIP Phone must be assigned with an AME Flex button for proper operation.

Operation

LIP Phone

To assign an {AME} button:

Ring Mode

1. Lift the handset, and press **[PGM]** + **{FLEX}** + '64' + '0' + **[SAVE]**

Speaker Mode

1. Lift the handset, and press **[PGM]** + **{FLEX}** + '64' + '1' + **[SAVE]**

To screen a call in the Ring mode:

1. Press the flashing **{AME}** button, the caller's voice is broadcast over the station speaker and simultaneously stored in the Voice Mail-box.

To stop the voice broadcast/screening and leave the caller in Voice Mail:
1. Press the illuminated **[SPEAKER]** button.

To talk with the caller and record the conversation in Voice Mail:
1. Press the illuminated **[MUTE]** button.

To answer the call and cancel the voice message:
1. Press the illuminated **{AME}** button, the caller is connected and Voice Mail is disconnected.

Conditions

1. AME is supported only on an LIP Phone (an **{AME}** Flex button must be assigned on the phone).
2. If the user answers the call using the **{AME}** button, the caller is connected in the normal manner, the Voice Mail is disconnected, and any message recorded by the caller is not stored (when VSF is in use).

Programming

Related Features

VSF Integrated Auto Attd/Voice Mail

Hardware

LIP Phone

2.48 AUTO CALLED NUMBER REDIAL (ACNR)

Description

This feature allows a station user to request and have the system retry a busy or no answer external call until the call is connected or the feature is cancelled.

Operation

LIP Phone

To assign a Flex button as an {redial} button:
1. Press **[PGM]** + **{FLEX}** + **[PGM]** + '54' + **[SAVE]**

To activate ACNR while receiving busy, no answer:
1. Press the **{REDIAL}** button or **[ACNR]** soft button.
2. Hang-up handset, or press **[SPEAKER]**.

To cancel ACNR while idle:
1. Press flashing **{REDIAL}** button or **[STOP]** soft button.

To cancel ACNR during an ACNR attempt:
1. Lift the handset or press the **[MUTE]** or flashing **{REDIAL}** button.

System

1. The system initiates the ACNR process, starting the ACNR Pause Timer.
2. At expiration of the timer, the system attempts the previous call.
3. When the called party answers, the calling user may answer by lifting the handset or using speakerphone to communicate with called party.

Conditions

1. Four timers and a retry counter can be programmed.
   - ACNR Pause Timer – Time allowed between ACNR attempts.
   - ACNR Delay Timer – At expiration of Pause Timer, if no line is available, the system will wait for delay timer before retry attempt.
   - ACNR Tone Detect – After dialing, the system will abandon retry if no tone or answer is detected within the Tone Detect time.
   - ACNR Retry Count – Count determines the number of times system will retry before ACNR is automatically cancelled.
2. The call will be placed on the same path as originally used; if the path is busy, an available CO line in the same group will be seized.
3. The ACNR Retry Counter decreases by one when the system completes the dialed number.
4. When the ACNR Pause Timer expires, if the station is in a busy state, the ACNR Delay Timer is invoked.
5. Upon completion of dialing, the system will monitor the call for progress signals.

Programming

VOICE CONFIG	System Data – Call Feature Timer – ACNR Delay Timer
	System Data – Call Feature Timer – ACNR Pause Timer
	System Data – Call Feature Timer – ACNR Retry Counter
	System Data – Call Feature Timer – ACNR Tone Detect Timer

Related Features

LNR (Last Number Redial)
Speakerphone
Mute

Hardware

LIP Phone

2.49 AUTO RELEASE OF [SPEAKER]

Description

After completion of certain features, the **[SPEAKER]** turns off automatically, returning the LIP Phone to idle.

Operation

System

Auto Release of [speaker] operation is automatic for supported features.

Conditions

1. This feature applies to all User and Attendant Programming except CO line Disable and Version Display.
2. Auto Release of **[SPEAKER]** also applies to features including Call Park, Call Back, Call Forward and CO Queuing.
3. If, during Station User Programming, erroneous data is entered, error tone is received and the user must correct the error before the station will return to idle automatically.

Programming

Related Features

Hardware

LIP Phone

2.50 AUTOMATIC SPEAKER SELECT

Description

LIP Phones can access a CO line or an internal circuit by pressing the appropriate button without the need to lift the handset or press the **[SPEAKER]** button. Audio from the CO line or called station is sent to the speaker as if the user pressed the **[SPEAKER]** button and the speakerphone's MIC is activated.

Operation

LIP Phone

To access an internal or external system resource:

1. Press an assigned **{FLEX}** button.

Conditions

1. For LIP Phones not equipped/assigned with speakerphone, the user must lift the handset to be heard.
2. Paging while on the speakerphone may cause feedback from the paging equipment; if Auto Speaker is enabled and a **{PAGING ZONE}** button is pressed, the display will show "LIFT THE HANDSET". To complete the page, the user must lift the handset within the predefined 5-second period or the Station will return to idle.

Programming

Related Features

Hardware

LIP Phone

2.51 CALL LOG DISPLAY

Description

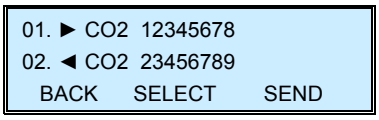
Users with LIP Phones that have Soft keys (8012D and 8024D) can view a log of incoming, outgoing and missed calls on the display.

Operation

LIP Phone

To access the Call Log menu:

1. Press the **{LOG}** soft button; the following will display,



2. Use the Up/Down Navigation keys to view the other log contents.

Conditions

Related Features

Hardware

LIP 8012D, 8024D Phone

2.52 CALL WAIT

Description

When a busy LIP Phone receives a incoming CO call, the muted ring is heard, giving a audible indication of the call; DID Call Wait must be enabled in Station User Programming.

Operation

When programmed, operation of this feature is automatic.

Conditions

1. The incoming CO call will follow the call routing defined in Exceptional Call Routing after the expiration of the DID/DISA no answer timer expires.
2. The LIP Phone must have an appearance button programmed for the CO line.
3. Assigning the CO line with ICLID routing automatically disables DID Call Wait.

Programming

VOICE CONFIG	Station Data – Common Attributes – DID Call Wait System Data – Call Utility Timer – DID/DISA No Answer Timer

Related Features

Call Routing

Hardware

LIP Phone

2.53 DND - ONE TIME DND

Description

A station can reject and terminate a ringing or off-hook muted ringing call by pressing the **[DND]** button. When the station returns to the idle status, DND is cancelled and the **[DND]** LED extinguishes.

Operation

LIP Phone

To activate One Time DND while on a call:

1. When receiving a call, press the **[DND]** button; the **[DND]** LED illuminates, and station enters DND status.

System

To deactivate DND:

1. When the station returns to idle, DND is disabled and the **[DND]** LED extinguishes.

Conditions

1. CO recalls override One Time DND.
2. The Attendant can override stations in One Time DND using Camp-On or Intrusion; the Attendant Station does not have One Time DND service.
3. One Time DND cancels existing Callback requests.
4. When DND is activated, the DND message “DO NOT DISTURB STA [XXX]” will display to a Station attempting Camp-on at the called Station.
5. DND LED illumination is only applied while muted ringing.

Programming

Related Features

Call Waiting/Camp-On
DND (Do Not Disturb)

Hardware

LIP Phone

2.54 FLEX BUTTON DIRECT SPEED DIAL ASSIGNMENT

Description

A user may program a telephone number directly to a Flex button without the need to assign the number to a Speed Dial bin. In this case, the telephone number is allocated to the highest numbered Individual Speed Dial bin available.

Operation

LIP Phone

To assign a telephone number to a Flex button:

1. Press the **[PGM]** button.
2. Press the desired Flex button.
3. Press the soft button below the “TEL NUM” display selection.
4. Dial the telephone number.
5. Press the **[HOLD/SAVE]** button
6. Dial the name to be associated with the number (optional).
7. Press the **[HOLD/SAVE]** button.

To place a call using the Flex button:

1. Lift the handset or press the **[SPEAKER]** button.
2. Press the assigned Flex button.

Conditions

1. This feature is available to LIP phone users only.
2. When a Flex button is assigned with a telephone number, the system will allocate the number to the highest available Individual Speed Dial bin number; if no bin is available, the user will receive an error tone when attempting to assign the telephone number.
3. The telephone number may include any of the special Speed Dial instructions **(**display security, etc.).

Programming

Related Features

Individual Speed Dial

Hardware

LIP 8012D, 8024D phone

2.55 INTERCOM ANSWER MODE

Description

Each LIP Phone can select the answer mode used for incoming ICM calls while the station is idle. There are three answer modes available:

- Handsfree (H) – When an ICM call is received, the user receives splash tone followed by the ICM caller's voice; the user may respond to the caller without lifting the handset or pressing the **[SPEAKER]** button.
- Privacy (P) – When an ICM call is received, the user receives splash tone followed by the ICM caller's voice; to respond, the user must lift the handset or press the **[SPEAKER]** button.
- Tone (T) – An ICM call will cause the LIP Phone to provide an audible ICM ring tone; the user must lift the handset or press **[SPEAKER]** to answer.

📖 ***NOTE:*** *A SLT always functions in Tone ring mode.*

Operation

LIP Phone

To change ICM Answer Mode:

1. Press **[PGM]** button; the **[SPEAKER]** button LED lights steady.
2. Dial 11 (Station User Program code); confirmation tone is received.
3. Dial the desired ICM Answer Mode code (1=H, 2=T, 3=P).
4. Press the **[SAVE]** button.

Conditions

1. Regardless of ICM Answer Mode selected by the user, Message Wait, Callback, Call Forward and Attendant Override will ring in Tone mode.
2. Page announcements are not affected by ICM Answer Mode Selection.
3. The default ICM Answer Mode is Tone ring; the active mode is stored in battery-protected memory.

Programming

Related Features

Intercom Call (ICM Call)
Paging
Message Wait/Call Back
Call Forward

Hardware

LIP Phone

2.56 MUTE

Description

An LIP Phone can turn off audio transmission from the handset, speakerphone or headset microphone (Mic Mute).

Operation

LIP Phone

To Mute the Microphone:

1. Press the **[MUTE]** button; the **[MUTE]** button LED illuminates, the microphone (Handset, Speakerphone, Headset) is muted, and the connected party receives silence.

To activate the microphone:

1. Press the illuminated **[MUTE]** button; the **[MUTE]** button LED extinguishes, and the microphone is activated, transmitting audio to the connected party.

Conditions

1. Changing from speakerphone to handset or vice versa during a mute condition will eliminate mute status.
2. Returning to idle or placing another CO or intercom call will deactivate mute status and return to the normal (active microphone) status.

Programming

VOICE CONFIG Station Data – Common Attributes – Headset Ring

Related Features

Speakerphone
Headset Compatibility

Hardware

LIP Phone

2.57 OFF-HOOK SIGNALING

Description

Off-hook Signal is a muted ring signal delivered to the LIP Phone speaker. When an off-hook station receives a call, or a CO call rings into the system for the off-hook station, the station will receive the assigned Off-hook Signal (ring), or a Camp-On in the case of ICM calls (Voice-Over Announcement or Off-hook ring signal may be received).

Operation

System

Operation of Off-hook ring signals is automatic.

Conditions

1. While using the speakerphone, a Camp-On tone is provided over the speaker in place of the assigned Off-hook ring Signal.
2. DND overrides and terminates any Off-hook signaling.
3. Off-hook ring signals terminate when the call is answered, forwarded, or abandoned.
4. A Station that receives an off-hook signal will receive normal ring signaling once the Station returns to idle.

Programming

Related Features

Call Waiting/Camp-On
CO Ring Assignment
DND (Do Not Disturb)
DND - One Time DND

Hardware

LIP Phone

2.58 ON-HOOK DIALING

Description

LIP Phones equipped with a Speakerphone allow users to place as well as receive calls while the handset is on-hook. Once the user activates the speakerphone by pressing the **[SPEAKER]** button or Automatic Speaker Select, a dial tone is received and the user may dial the desired number.

Operation

LIP Phone

To activate On-Hook Dialing:

1. Press the **[SPEAKER]** button; dial tone is received and the **[SPEAKER]** button LED lights.
2. Place desired call (dial station ICM number, or select CO path and dial).

Conditions

1. If the outgoing call is not answered, the user must press the illuminated **[SPEAKER]** button to return to idle.
2. When the speakerphone is used, the microphone is active unless the **[MUTE]** button is pressed (**[MUTE]** button LED is illuminated).

Programming

Related Features

Mute
Speakerphone
Automatic Speaker Select
Headset Compatibility

Hardware

LIP Phone

2.59 SAVE NUMBER REDIAL (SNR)

Description

The last dialed number on a CO call may be stored (up to 23 digits) in a buffer for future use. This number is saved in memory until the user requests a new number be stored. Numbers dialed for subsequent calls do not affect the Save Number buffer.

Operation

LIP Phone

To save a dialed number, while on a CO call:

1. After dialing (before hanging up), press the right navigation button.
2. Press the soft **[SAVE]** button.

To dial a saved number:

1. Lift the handset or press the **[SPEAKER]** button.
2. Press the soft **[DIR]** button.
3. Press the soft **[SPEED]** button.
4. Press '#'.

Conditions

1. The saved number can be a maximum of 23 digits.
2. Dialing the saved number will automatically seize the CO line that was used for the original call. If the CO line is busy, a CO line from the same group will be selected and the saved number dialed. If all CO lines from the group are busy, the user will receive All Lines busy tone and may queue.
3. If there is no **{CO}** button, the call will be presented on a **{LOOP}** button.
4. Save Number Redial is protected from power failure.

Programming

Related Features

Individual Speed Dial
Common Speed Dial
LNR (Last Number Redial)

Hardware

LIP Phone

2.60 SPEAKERPHONE

Description

LIP Phones equipped with speakerphone circuitry enable the telephone to be used hands-free in two-way conversations.

Operation

LIP Phone

To activate the Speakerphone:

1. Press the **[SPEAKER]** button; **[SPEAKER]** LED lights steady.

To switch from Handset to Speakerphone:

1. When Handset is in use, press the **[SPEAKER]** button; **[SPEAKER]** LED lights steady.
2. Replace Handset, and Speakerphone is activated.

To terminate a Speakerphone call:

1. When Speakerphone is in use, press the **[SPEAKER]** button; **[SPEAKER]** LED extinguishes.

Conditions

1. If Automatic Speaker Select is enabled for the station, pressing a DSS, CO/LOOP or Speed Dial button will automatically activate the speakerphone.
2. The **[MUTE]** button LED indicates the status of the Microphone; when lit, the Microphone is inactive.
3. When Headset operation is assigned for the station, the Speakerphone is disabled and the **[SPEAKER]** button activates the Headset audio path instead of the speaker.

Programming

VOICE CONFIG Station Data – Common Attributes – Headset Ring

Related Features

Mute
Automatic Speaker Select
Headset Compatibility

Hardware

LIP Phone

2.61 STATION FLEXIBLE BUTTONS

Description

The LIP Phone incorporates a field of “Flex” buttons as well as the fixed feature buttons. The Flex buttons are assigned in the system database to access features, functions or resources of the system. Specifically, Flex buttons can be assigned as:

- Empty button – has no system database assignment.
- **{DSS/BLF}** button – used to place One-touch ICM calls to a designated station and display Station status.
- Flex Numbering Plan button – activates the feature associated with the assigned digits from the Flexible Numbering Plan.
- Speed Dial bin button – accesses and dials the number from the assigned Speed Dial bin.
- Loop button – provides an appearance for incoming CO calls when a direct CO appearance is not available; the Loop button LED provides the status for the duration of the call (must be programmed using Web. Admin.).
- Station User Program Code button – accesses or activates the special features available with Station User Program Codes (refer to Section 3.67).
- CO Line Appearance button – provides access to the individual CO Line assigned to the Flex button. The CO Line button LED provides the status of the CO Line. This button is only available in an attendant station.

With the exception of CO Line buttons and Loop button, Flex buttons can be assigned at the station by the end-user.

Operation

LIP Phone

To assign a Flex button at the station:

1. Press the **[PGM]** button.
2. Press the desired Flex button.
3. Dial the digits from the Flexible Numbering Plan.
4. Press the **[SAVE]** button.

OR

1. Press the **[PGM]** button.
2. Press the desired Flex button.
3. Press the **[PGM]** button.
4. Dial the digits from the Station User Program Code (refer to Section 3.67) or Fixed Number Plan.
5. Press the **[SAVE]** button.

Conditions

1. The **{LOOP}** buttons provide a status indication for the call as long as the station has supervisory control.

2. A station may have multiple **{LOOP}** buttons.
3. The priority for the appearance of a CO call transfer is first a direct CO Line appearance (**{CO}** button), if not available, a **{LOOP}** appearance is used. If there is no appearance available, the transferring station recalls immediately.

Programming

VOICE INSTALL	Numbering Plan
VOICE CONFIG	Station Data – Flex Buttons

Related Features

Flexible Numbering Plan
Station User Programming & Codes

Hardware

LIP Phone

2.62 STATION USER PROGRAMMING & CODES

*Descrip*tion

LIP Phone users can program an array of functions and features, access status information and assign special features codes to Flex buttons. The Station User Program Codes used for these purposes are fixed as listed, and shown below.

Table 2.72-2 Station User Programming

Code	Description	Entries
11	ICM Answer Mode	1: H, 2: T, 3: P
12	Headset/Speakerphone mode	0:H, 1:S
13	Select Headset Ring type	1:S, 2:H, 3:Both
21	Set Wake-Up Time	Once/Permanent & Hour/Min
22	Erase Wake-Up Time	
31	LCD Display Language	Domestic/English
32	Sys version display	
33	Select BGM source	(0~1)
34	User Name registration	‘name’
35	Display Phone IP Address	
36	Display Phone MAC Address	
37	Display Phone Version	
38	Network Configuration	
41	Forced Forward to Destination	Station Group Number
42	**{Call Log Display}** button	

Code	Description	Entries
43	CLIR Service	
44	COLR Service	
4*	LOOP button	
50	CALLBACK button	Button PGM only
51	CONF button	Button PGM only
52	MUTE button	Button PGM only
53	ICM button	Button PGM only
54	REDIAL button	Button PGM only

In addition, a Station User Program Menu display is provided by the LIP Phone display to assist the user in programming Station User Program Code features and functions.

- **[VOL▲]/[VOL▼]** buttons – used to scroll through menu items and the dial pad is used to enter a selection.
- Program Codes – also used to assign a function/feature to a Flex button.

USER PROGRAM MENU Displays:

First top-level Menu selection

```
[1] KEYSET
[2] WAKE UP TIME
```

Under selection [1] Keyset, select 1~3 as below

```
[1] ANSWER MODE
[2] HEADSET OR SPK MODE
```

```
[3] HEADSET RING MODE
[1] ANSWER MODE
```

Under selection [2] Wake Up Time, select 1~2 as below

```
[1] SET WAKE UP TIME
[2] WAKE UP DISABLE
```

Next top-level Menu selection

```
[3] SUPPLEMENTARY
[4] SERVICES
```

Under selection [3] Supplementary, select 1~7 as below

```
[1] LCD DISPLAY LANGUAGE
[2] iPECS SBG-1000 INFO
```

```
[3] BGM
[4] REGISTER STA NAME
```

```
[5] DISP PHONE IP ADDR
[6] DISPLAY MAC ADDR
```

[7] DISP PHONE VERSION
[8] NETWORK CONFIG

Under selection [4] Services select 1~4 as below

[1] FORCED FWD TO DEST
[2] CALL LOG DISPLAY

[3] CLIR SERVICE
[4] COLR SERVICE

Operation

LIP Phone

To assign a Station User Program Code to a Flex button:

1. Press the **[PGM]** button; the Station User Program Menu is displayed.
2. Press the desired Flex button.
3. Dial the desired Station User Program Code and additional inputs that may be required.
4. Press the **[SAVE]** button.

To activate a Station User Program Code feature or function:

1. Press the **[PGM]** button; the Station User Program Menu is displayed.
2. Use the **[VOL▲]/[VOL▼]** buttons (as needed) to display the desired menu item, or dial the desired Station User Program Code and additional inputs as required.

Programming

Conditions

Related Features

Station Flexible Buttons
Station Message Wait/Call Back
Wake-Up Alarm
Headset Compatibility
Attendant Station Program Codes

Hardware

LIP Phone w/Display

2.63 VOICE OVER

Description

Voice Over allows LIP Phones to receive a voice announcement through the handset receiver while off-hook on a call (CO or Intercom). The Voice Over is muted so as not to interfere with the existing conversation. The called station user may then respond to the calling party using Camp-On response or DND.

Operation

LIP Phone

Placing a Voice Over (OHVO) while receiving busy:

1. Dial '#'.
2. After splash tone, begin announcement.

Responding to a Voice Over announcement:

1. Use Camp-On response procedure or One-Time DND.

SLT

Placing a Voice Over (OHVO) while receiving busy:

1. Dial '#'.
2. After splash tone, begin announcement.

Conditions

1. When the called station responds via Camp-On, all conditions and options available to Camp-On apply.
2. OHVO may be used to notify the called party of a transferred call (CO Line or Intercom) by announcing the call then releasing to complete the transfer.
3. When a call is transferred via OHVO the receiving station will receive a ringing after the transfer is complete.
4. If the receiving station is in conference or using the Speakerphone, Voice Over is not available; Camp-On will be activated and a Camp-On tone sent to the receiving station.
5. If the receiving station is SLT or SIP extension, Voice Over is not available.

Programming

VOICE CONFIG Station Data – Common Attributes – Voice Over

Related Features

Call Waiting/Camp-On

Hardware

LIP Phone to receive Voice Over

2.64 ATTENDANT POSITION

Description

By default, Station 10 is the Attendant on the iPECS SBG-1000 system. The Attendant position must be equipped with an LIP multi-button Phone.

Operation

Condition

1. Attendant is assigned as Station 10 (default, logical number).
2. Attendant calls and recalls are always routed to the attendant.

Programming

Related Features

Hardware

LIP Phone

2.65 ATTENDANT RECALL

Description

Unanswered or abandoned CO calls that remain unanswered for the Hold or Transfer Hold timer (when appropriate), will recall the station placing the call on hold. If the call remains unanswered for the assigned Recall time, the Attendant will receive a recall. Both the Attendant and station will receive the recall signal for the Attendant Recall Timer period after which the system will disconnect and return the CO line to idle.

Operation

System

Attendant recall operation is automatic.

Conditions

Programming

VOICE CONFIG	System Data – Call Feature Timer – Attendant Recall Timer
	System Data – Call Feature Timer – I-Hold Recall Timer

Related Features

Hold
Call Transfer

Hardware

2.66 ATTENDANT STATION PROGRAM CODES

Description

Using the Attendant Station Program Codes, the Attendant can print SMDR and Traffic reports on-demand, control certain user features, record VSF announcements, and enable/disable Auto Service Mode Control, etc. Items are available using the Program Code directly or scrolling through the multi-level display menu. The following indicates the menu displays, including the digit for selecting the item, the item description and further required entries. The various levels of the display menu are indicated by indentation.

Operation

Attendant

To activate an Attendant Station Program Code feature or function:

1. Press the **[PGM]** button, the Attendant Station Program Menu is displayed.
2. Dial '0' to access Attendant Station Program codes (refer to Attendant Station Program Codes below).
3. Enter desired code, or use the **[VOL▲]/[VOL▼]** buttons to display the desired menu item and enter the desired code.
4. Dial additional inputs, as necessary.

Table 2.72-3 Attendant Station Programming

[1] PRINT
  [1] SMDR
    [1] PRINT SMDR STA BASE
      station range input
    [2] DELETE STATION BASE
      station range input
    [3] DISPLY CALL CHARGE
    [4] ABORT PRINTING
    [5] PRINT LOST CALL
    [6] DELETE LOST CALL
  [2] TRAFFIC
    [1] PRINT ALL SUMMARY
      enter Analysis time & type
    [2] PRINT ALL PERIDICLLY

enter Analysis time, type & Print time
[3] ABORT PERIDIC PRINTING
[4] PRINT ATD TRAFFIC
enter Analysis time & type
[5] PRINT CALL SUMMARY
[6] PRINT CALL HOURLY
enter Analysis time & type
[7] PRINT H/W USAGE
enter Analysis time & type
[8] PRINT CO SUMMARY
enter Analysis time & type
[9] PRINT CO HOURLY
enter CO Group

[2] CLOCK/WAKEUP
[1] LCD DATE MODE CHAGE
[2] LCD TIME MODE CHAGE
[3] ATD SET WAKE UP TIME
enter station range
[4] ATD WAKE UP DISABLE
enter station range

[3] STATION SET
[1] REG STATION NAME
enter station number
[2] DND/FWD CANCEL
enter station range
[3] LCD Display Language
select language
[4] SET ICM ONLY MODE
enter station range
[5] RESTORE COS
enter station range

[4] ISOLATE CO FAULT

[5] REC VSF ANNCEMENT
enter VSF Announcement (001~072)

[9] USB UPGRADE

[#] WHTU SUBSCRIBE

Condition

Programming

Related Features

SMDR (Station Message Detail Recording)
Traffic Analysis
VSF Integrated Auto Attd/Voice Mail
Dial-by-Name
Station User Programming & Codes

Hardware

LIP Phone

2.67 ATTENDANT CALL/QUEUING

Description

Any station can call the Attendant by dialing the Attendant Call code '0'. When an Attendant call encounters a busy signal, the call is queued to the Attendant; the call will be delivered to the Attendant.

Operation

To call the Attendant:
1. Dial Attendant Call Code.

Condition

1. The ICM calling party will receive ring-back tone or MOH (as specified) while queuing.
2. Calls to the Attendant's station intercom number are sent to the Attendant station dialed as with any intercom call.

Programming

VOICE CONFIG Station Data – Station Hold Music

Related Features

Attendant Position
Intercom Call (ICM Call)

Hardware

2.68 DISABLE OUTGOING CO ACCESS

Description

The Attendant can place CO lines out-of service, disabling outgoing calls on the CO path. This is normally done in the event of an undetected fault interrupt service on a CO path. Incoming calls continue to be processed normally.

Operation

Attendant

To disable/enable Outgoing CO access (toggle):

1. Press the **[PGM]** button.
2. Dial 04 (Attendant Station Program code).
3. Press the **{CO}** button of the line(s) to be disabled; confirmation tone is heard and the selected line(s) changed to inactive status.

Conditions

1. If the desired CO line is in use, the Attendant may still disable the CO line; the feature will take effect after the desired CO line returns to idle.
2. Once the line is disabled, the Attendant appearances for the disabled CO line will flutter at 240 ipm (inactive status), while other stations will show the CO line as busy (LED solid On).
3. The CO line outgoing access status is stored in battery-protected memory in case of a power failure.
4. Multiple CO lines may be enabled/disabled without redialing the Attendant Station Program code; confirmation tone is heard after each CO line is enabled/disabled.
5. Incoming calls on a disabled CO line will continue to operate normally.

Programming

Related Features

Attendant Position

Hardware

2.69 FEATURE CANCEL

Description

The Attendant can cancel features such as DND and Call Forwarding that are active at other stations.

Operation

Attendant

To deactivate DND/Call Forward at other stations:

1. Press the **[PGM]** button.
2. Dial 032 (Attendant Station Program code).
3. Dial the desired station range, or the same station number twice for a single station.
4. Press the **[SAVE]** button; a confirmation tone is heard, and the Attendant station returns to idle status.

Conditions

Programming

Related Features

Call Forward
DND (Do Not Disturb)
Attendant Position

Hardware

2.70 SLT BROKER CALL

Description

Broker Call allows the SLT user to engage in 2 calls at once, alternating between the two parties, so that the conversation with each party is private.

There are two types of Broker Call, Transfer and Camped On:

- Transfer Broker Call – 2nd Call is originated by SLT user.
- Camped On Broker Call – 2nd Call is delivered to the SLT through a Camp-On.

Operation

SLT

To activate a Transfer Broker Call:

1. While on an active call (external or intercom), momentarily press the hook-switch, intercom dial tone received and call is placed in Exclusive Hold state.
2. Place second call.
3. To alternate between calls momentarily press the hook-switch.

To activate a Camp-On Broker Call:

1. While on an active call (external or intercom).

2. Receive a Call Waiting/Camp-On tone.
3. Momentarily press the hook-switch, intercom dial tone received and call is placed in Exclusive Hold state.
4. Dial 66 (Camp-On Answer feature code); camped-on call is connected.

To alternate between the calls:
1. Momentarily press the hook-switch.
2. Dial 66 (Camp-On Answer feature code).

Conditions

1. After performing the hook-switch flash, if the call results in an error, busy, no answer or an abnormal state, the SLT user may momentarily press hook-switch to retrieve the held call.
2. During a Transfer Broker Call, if the SLT user goes on-hook, the Broker Call parties are connected completing a Call Transfer.
3. During a Transfer Broker Call, if the active caller disconnects from the SLT user, the held party (if another station), is connected to the SLT.
4. If the held party is a CO call, the SLT user receives error tone and may go on-hook to receive recall and retrieve the held call
5. During a Camp-On Broker Call, if the SLT user goes on-hook, the active call is disconnected and the held call recalls to the SLT.
6. During a Camp-On Broker Call, if the active party disconnects from the SLT, the SLT user receives error tone; the SLT user may momentarily press the hook-switch to retrieve the held party or go on-hook and receive recall.
7. If after the hook-switch flash, the user takes no action for the dial tone timer, the SLT will receive an error tone; if the SLT returns to an on-hook state, the SLT automatically will receive a recall ring.

Programming

Related Features

Message Wait/Call Back
Call Waiting/Camp-On
Call Transfer

Hardware

2.71 SLT HOWLER TONE

Description

When a SLT station goes off-hook and does not initiate dialing in the Dial tone timer duration, delays dialing between digits in excess of the inter-digit time, or stays off-hook at the completion of activating a feature or program, the station will receive the howler tone as an error indication and the call attempt will be abandoned. In order to complete the call, the user must return to on-hook and restart the call.

Operation

System

The system will deliver howler tone automatically, as required

Conditions

1. Howler Tone is sent after a period, of about 30 sec. of error tone.
2. Lock-out occurs when howler tone starts.

Programming

Related Features

Intercom Lock-Out

Hardware

2.72 DIALING RESTRICTIONS

2.72.1 Class of Service

Description

Dialing privileges can be assigned for each station; the dialing privileges are designated according to the Station Class of Service (COS) assignments as shown in the following tables. Users placing an outgoing call or dialing after answering a call will be allowed one of the four Station COS privileges assigned.

Table 2.72-1 Station Class of Service

Station COS	Dialing Restriction
1	No restrictions are placed on dialing.
2	Assignments in Exception Table A are monitored for allow and deny numbers.
3	Assignments in Exception Table B are monitored for allow and deny numbers.
4	Assignments in Exception Tables A & B are monitored for allow and deny numbers.

- Toll Exception Tables – Each Toll Exception Table permits entry of 50 Allow codes and 50 Deny codes. Each code can contain up to 20 digits including digits 0-9, "#" as a wild card (any digit) and "*" as the end of entry mark (refer to Station Class of Service table to determine application of Toll Exception).
- Exception Table process – As digits are dialed, they are compared to entries in the appropriate Exception Table. Based on the Allow and Deny entries, the system applies the following rules to allow or deny calls.
  - Rule 1 – If a table has no entries, no restrictions are applied.
  - Rule 2 – If there are only Deny entries, restrictions are provided as Deny only.
  - Rule 3 – If there are only Allow entries, restrictions are provided as Allow only.
  - Rule 4 – If there are both Allow and Deny entries, the Deny entries are searched. If the dialed number matches a Deny entry, the call is restricted; if no match is found the call is allowed.

Operation

System

The system automatically applies the assigned COS.

Conditions

1. Dialing privileges are based on Station COS.

Programming

VOICE CONFIG	Station Registration – Authorization Code & COS
	System Data – Toll Exception Table

Related Features

Day, Night & Timed Station COS
Temporary Station COS/Lock

Hardware

2.72.2 Day, Night & Timed Station COS

Description

Each station is assigned a COS for three modes: Day, Night and Timed service modes. The service mode is generally controlled by the System Attendant. Based on the mode, appropriate dialing privileges are established.

Operation

System

Dialing restrictions are automatically applied based on COS assignments:

Conditions

Programming

VOICE CONFIG	Station Registration – Authorization Code & COS
	System Data – Toll Exception Table

Related Features

Class of Service
Temporary Station COS/Lock
Day/Night/Timed Ring Mode

Hardware

2.72.3 Temporary Station COS/Lock

Description

The Attendant can change the Station's Class of Service to temporarily preventing unauthorized toll dialing from the station (ex., lock the station). The station is still allowed to place internal calls and Emergency number calls.

Operation

System Attendant

To activate Temporary COS:

1. Press the **[PGM]** button.
2. Dial 034 (Temp COS code).
3. Dial the Station range.
4. Press the **[SAVE]** button.

To restore the assigned COS:

1. Press the **[PGM]** button.
2. Dial 035 (Restore COS code).
3. Dial station range
4. Press the **[SAVE]** button.

Conditions

1. The station is restored to the Station COS as appropriate for the active service mode, Day, Night, or Timed.

Programming

VOICE CONFIG	Station Data – Authorization Code & COS
	System Data – Toll Exception Table

Related Features

Class of Service
Day/Night/Timed Ring Mode

Hardware

2.73 SIP EXTENSION SERVICE

Description

The iPECS SBG-1000 system supports standard SIP phones; compatible SIP phones support the IETF standard RFC3261 for real-time communications over the internet. Once registered, iPECS SBG-1000 will deliver services to the SIP Phone.

Three steps should be followed for SIP phones to be registered to iPECS SBG-1000 and receive services from the system: SIP phone Lock key installation, Station User Login configuration for SIP phone, and SIP phone configuration.

Operation

Web Admin

To install the Lock key:

1. Enter Web Admin.
2. Select Voice Maintenance>Appliances Control>Lock Key Install.
3. Enter the proper Lock key in SIP Phone field.
4. Click **[Save]** button

To configure Station User Login for SIP phone:

1. Enter the Web Admin.
2. Select Voice Install>Station Registration>Station User Login.
3. Enter ID, Password and Desired Number.
4. Click **[Save]** button

WIT-400H

1. Press Menu + 8.Settings + 1.Profile Settings.
2. Edit System Default profile or add new profile about WLAN and network configuration.
3. Press Menu + 8.Settings + 2.SIP Setting.
4. Edit Phone Number, Display Name, Password, SIP Domain, Proxy IP and Proxy Port. The Phone Number must be the desired station number and also the SIP Domain and the Proxy IP should be the iPECS SBG-1000 LAN IP address.
5. Press Menu + 8.Settings + 3.Provisioning Setting.
6. Edit Address. The address should be the iPECS SBG-1000 LAN IP address.
7. Press Menu + 8.Settings + 1.Profile Settings.
8. Select the profile which you want to connect.

Please refer to the WIT-400H User Guide for the details.

SIP Phone

To set-up the SIP Phone:

1. Configure SIP Phone settings (ex. IP address, Subnet mask, Gateway, Telephone number, Proxy address, Expiration timer, Domain address etc.). The Telephone number must be the desired unused station number and also the proxy address and the domain address should be the iPECS SBG-1000 IP address (refer to the SIP phone User Guide for further information).
2. Boot the SIP Phone, which will register it with iPECS SBG-1000.

Conditions

1. Up to 6 SIP phones will be supported with Lock key. LG-Ericsson SIP extensions such as WIT-400H and LIP-8002 can be used without Lock key.
2. Desired Number for SIP phone should exist in station number list and also should be not assigned for other extension.
3. The Station User name will be overwritten by the SIP Phone Display Name setting.
4. If the Station number is changed in the iPECS SBG-1000 database, the SIP Phone should be reconfigured and re-registered with the changed telephone number.
5. When SIP Phones are used with iPECS SBG-1000, service tones from the system will not be heard (Confirmation tone, etc.).
6. iPECS SBG-1000 can not support full system feature with SIP extension such as WIT-400H, LIP-8002 and etc. For example, tones and LCD display messages for SIP extension can not be fully controlled by iPECS SBG-1000.

Programming

VOICE MAINT	Appliances Control – Lock Key Install
VOICE INSTALL	Station Registration – Registration Table

Related features

Hardware

2.74 PRIME LINE IMMEDIATELY/DELAYED

Description

When a user goes to an off-hook state, the system normally provides ICM dial tone. If desired, a station can be assigned to access a pre-assigned system resource (Prime Line). The Prime Line can be any of the Idle Line Settings:

- Seize a CO Line,
- Call another station,
- Activate a Flex button feature.

Prime Line access can be defined as immediate or delayed. When assigned immediate, upon an off-hook event, the system provides access to the Prime Line. With Delayed Prime Line, the station

user receives normal Intercom dial tone for the Prime Line Delay timer and after the delay, the Prime Line is accessed.

Operation

LIP Phone

To access the station's Prime Line

1. Lift the handset or press **[SPEAKER]** button and take no action, Prime Line as assigned will be accessed.

Conditions

1. Any of the station's Flex buttons may be assigned as the Prime Line. When the user lifts the handset or presses the **[SPEAKER]** button, the system will act as if the user had pre-selected the button prior to going off-hook.
2. Selection of another Flex button or Feature button just prior to an off-hook event will override the Prime Line assignment.
3. When Delayed Prime Line is set, the user must wait, taking no action until the Prime Line is accessed. The user receives ICM dial tone during this period and may dial any valid numbering plan digit(s) or select a Flex button or feature button.
4. If the Prime Line Delay Timer is greater than Dial tone timer, the Delayed Prime Line will not activate. It will be necessary to reduce the delay timer or extend the Dial tone timer.

Programming

VOICE CONFIG	Station Data – Common Attributes – Prime Line
	Station Data – Common Attributes – Idle Line Selection
	System Data – Call Feature Timer – Prime Line Delay Timer

Related Features

Speakerphone
Intercom Call (ICM Call)
Station Flexible Buttons

Hardware

LIP Phone

2.75 INTERNATIONAL CALL RESTRICTION

Description

Outgoing international call is normally very expensive. International call can be restricted by program.

When international call restriction is programmed, iPECS SBG-1000 tries to compare dialed digits to CO with programmed international prefix. If digits are matched, call should be released and access deny message will be displayed on LCD with error tone.
When CO-CO international call is programmed to be restricted, following 3 cases should be restricted.

1) CO call transfer to international call
2) international outgoing call transfer to CO call
3) CO call forward to international call

Operation

When programmed, operation of this feature is automatic.

Conditions

1. When all international call is programmed to be restricted, all outgoing international call is restricted. Incoming CO call can not restricted by this rule.
2. If call transfer is restricted, transferee call should be recalled after transferor hang up.

Programming

VOICE CONFIG System Data – International Call

Related Features

Call Transfer,
Call Forward
Call Forward, Preset

Hardware

2.76 IP SYSTEM DECT

Description

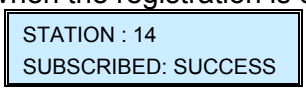
iPECS SBG-1000 supports office building mobility employing Digital European Cordless Technology (DECT). iPECS SBG-1000 has the internal Wireless Telephone Interface Module (WTIM). The internal WTIM manages up to six (6) DECT phones (GDC-450H or LWS-WK) and maintain an uninterrupted communications link to iPECS features and resources.

For further information on installation and operation of the IP System DECT solution, refer to the IP System DECT Manual.

Operation

System Attendant
To register DECT phone to iPECS SBG-1000:

1. Press the **[PGM]** button.
2. Dial 0# (WHTU SUBSCRIBE code).
3. Press the **[FLEX 1]** button.
4. Dial the Station number to be used for DECT phone.
5. Dial the phone type. 3 is for GDC-34x/4xx and 4 is for LWS-WK.
6. Press the **[SAVE]** button.
7. Proceed to instruction below for GDC-450H or LWS-WK.
8. When the registration is completed below message is shown on LCD of attendant.



GDC-450H

To register GDC-450H to iPECS SBG-1000

1. Press the **Menu** button to display the menu.
2. From the menu use the **Navigation** button to highlight Phone Register.
3. Press the **OK** button; this displays the Phone Register menu.
4. Select “LWS Subscription” using the up and down arrows of the **Navigation** button and press the **OK** button.
5. The GDC-450H searches for the iPECS/iPECS SBG-1000, displaying and “Searching..1”. When a iPECS/iPECS SBG-1000 is found, its RFPI, is displayed. The RFPI of your iPECS/iPECS SBG-1000 is available from your System Administrator, or perhaps the attendant.
6. Press **OK** button while highlighting the RFPI to continue the registration to the system, or Press **No** button to continue the search.
7. Press **OK** button; on successful registration, a confirmation tone is received at the GDC-450H and the iPECS/iPECS SBG-1000.
8. If the registration fails, repeat procedure from Step 1 to 7 at the System Attendant and Step 1 to 8 from the GDC-450H.

LWS-WK

To register LWS-WK to iPECS SBG-1000

1. Press **[MENU]** button to display the menu.
2. Highlight “Phone Register” using the Navigation up/down key, and then press **[OK]** soft button or Navigation ‘OK’ key.
3. Select “Subscription” using the Navigation up/down key, and then press **[OK]** soft button or Navigation ‘OK’ key.
4. Display [Searching..1].
5. The system [RFPI : eg. 01234567890123] will be displayed when a system is found.
6. Press **[OK]** soft button or Navigation ‘OK’ key. In a few second, a confirmation tone is received at the LWS-WK.
7. If the registration fails, repeat procedure from Step 1 to 7 at the System Attendant and Step 1 to 6 from the LWS-WK.

Conditions

1. Up to six (6) DECT phones can be registered and maximum 4 DECT calls can be placed simultaneously.

2. During the registration of DECT phone, Monitor or Speaker button at the iPECS/iPECS SBG-1000 attendant phone should not be pressed until the DECT phone completes the registration and registration confirmation tone is heard.

Programming

VOICE INSTALL Station Registration – DECT Registration

Related Features

Hardware

GDC-450H handsets

2.77 ALARM SIGNAL/DOOR BELL

Description

The system can be configured to recognize the status of an external contact (normally open or closed). The system will signal to the Attendant Station when the contact activates. This capability is commonly employed to provide remote Alarm or Door Bell signals to the user.

The Attendant Station receives the Alarm Signal, either a single tone burst repeated at 1-minute intervals or a continuous tone. The Alarm Signal may be terminated at the user's phone by dialing the Alarm Stop code or, if assigned, pressing the **{ALARM STOP}** button. To rearm the Alarm function, the alarm condition must be cleared and the Alarm signal terminated.

When used as a Door Bell, the Attendant Station receives a single tone burst each time the external contact is activated and no reset is required.

Operation

System

At detection of contact operation, the Alarm/Door Bell signal is sent to assigned stations.

LIP Phone

To assign a Flex button as an **{ALARM STOP}** button to terminate the Alarm Signal:

[PGM] + **{FLEX}** + '65' + **[SAVE]**

To terminate an Alarm Signal while idle:

1. Dial the Flex Numbering Plan code 65, confirmation tone is received and the Alarm Signal is terminated. If the alarm condition is cleared, the system will automatically rearm the alarm monitoring.

Or,

2. Press the **{ALARM STOP}** button.

Conditions

1. The Alarm contacts must be “dry”, no voltage or current source connected.
2. The Attendant Station will show “ALARM” or “DOOR BELL” as appropriate.

Programming

VOICE CONFIG System Data – Alarm Attributes

Related Features

Door Open

Hardware

LIP Phone
External contact connected to Alarm input of iPECS SBG-1000, refer to iPECS SBG-1000 **Quick Start Guide.**

2.78 DOOR OPEN

Description

The iPECS SBG-1000 hardware is equipped with relays that activate External Control Contacts. The contacts can be assigned to one of several functions including a Door Open Contact. When used as a Door Open Contact, the contact is connected to a door-lock release mechanism. When the Attendant Station receives the Door Bell signal, the user may dial the Door Open code to activate the contact.

LIP Phone users may assign a Flex button as a **{DOOR OPEN}** button.

Operation

LIP Phone

To assign a Flex button as an **{DOOR OPEN}** button to terminate the Alarm Signal:

[PGM] + **{FLEX}** + Door Open code (‘#*’) + **[SAVE]**

To activate the relay contact

1. Lift handset or press **[SPEAKER]** button.
5. Dial Door Open code, ‘#*’.
6. Hang-up to return to idle.

Or,

1. Lift handset or press **[SPEAKER]**.
7. Press the **{DOOR OPEN}** button
8. Hang-up to return to idle.

Conditions

1. The contacts are rated at 1 amp, 24 VDC.

Programming

VOICE CONFIG System Data – Alarm Attributes

Related Features

Alarm Signal/Door Bell

Hardware

External Control Contact connected to a door-lock release mechanism.

2.79 MOBILE EXTENSION

Description

A mobile phone may be registered to a station allowing the mobile phone to place and receive calls through the system. SIP or ISDN DID calls are sent to the user's LIP Phone and the active registered mobile phone simultaneously. If the mobile phone is paired with a Hunt group station, Hunt group calls routed to the station also ring to the active mobile phone when enabled.

The mobile phone users can access the facilities of the iPECS SBG-1000 to place internal and external calls as well as activate/access features. To access system facilities and resources, the mobile user calls the SIP number or the ISDN DID number of the corresponding LIP Phone. When the call is received, the system matches the CLI to the mobile phone and provides the mobile user with system dial tone.

Operation

System

Incoming SIP or ISDN DID calls are sent to active mobile phones automatically.

Mobile Phone

To place a call from the mobile extension using the iPECS SBG-1000:

1. Dial the SIP number or the ISDN DID number of the station, the system will check the CLID, answer the call and the user will receive intercom dial tone.
2. Place internal or external iPECS SBG-1000 call as normal.

To Transfer a call from the mobile extension using the iPECS SBG-1000:

1. Dial '*' while on an iPECS SBG-1000 call.
2. Dial the desired extension, the call is transferred and the mobile phone returns to idle.
   Note: the mobile may reconnect by dialing '#'.

Conditions

1. When the mobile phone places an external call through iPECS, the CLI of the corresponding station is used.
2. The Mobile Extension features are supported via system digital (SIP and ISDN) lines only.
3. Message Wait and Callback cannot be activated to a mobile phone.
4. The Mobile Extension feature is not supported over a distributed networked environment.
5. When an incoming SIP or ISDN call is received, the system will access an SIP or ISDN line and place a call to the mobile phone. Thus, an SIP or ISDN line must be available for the system to notify the mobile user of the incoming call.
6. Hold and Transfer Recalls to the mobile phone are sent to mobile phone and the associated station.
7. Circular and Terminal Hunt Group calls can be routed to the active Mobile Extension.

Programming

VOICE CONFIG Station Data – Mobile Extension

Related Features

DND (Do Not Disturb)
Station Message Wait/Call Back
Attendant Recall
Distributed Control Network

Hardware

LIP Phone

2.80 SYSTEM NETWORKING

2.80.1 Distributed Control Network

Description

In the Distributed Control Network, each iPECS SBG-1000 system maintains control over the devices registered to it. The networked systems communicate allowing other networked systems access to resources over the network. In addition, other features and functions as detailed in the following sections of this manual are available to users in a distributed network environment. The iPECS SBG-1000 permits remote access to various resources through registered gateway Modules and terminals.

In addition, iPECS SBG-1000 will request access to resources of remote systems. The user-dialed number is analyzed and the call routed according to the Net numbering table. Should the main path fail to respond, the iPECS SBG-1000 routes the call employing the alternative Speed Dial route assigned.

iPECS SBG-1000 supports H.450 over IP, for the basic networking functions and the proprietary iPECS protocol for the advanced networking features.

Operation

Operation of Distributed Networking is automatic when configured & defined

Conditions

1. To use the networking features, the software lock-key installation is required. Each iPECS SBG-1000 system has a unique software lock-key. To get the software lock-key, contact the distributor of iPECS SBG-1000 system.
2. Unified Dialing Plan (UDP): Each station can have a unique number up to 7 digits in the networked systems, but it depends on their own numbering plan.
3. The alternative route employs a Speed Dial number to place a call and is not a Networked call. Thus, the Distributed Control Network features are not available.

Programming

Related Features

Hardware

2.80.1.1 Net Call

Description

A station user can make a call to a station in other systems by dialing only a station number just as an intercom call within the same system.

Operation

1. Lift Handset or press the **[SPEAKER]** button. The system provides a user with a dial tone.
2. Dial the station number of other systems, or press the {NET DSS} button of other systems.
3. The station seizes the network CO line according to the net routing table, and the system sends a digit stream that is modified by the net routing table.
4. The called party receives a digit stream that is sent by calling party, and analyzes it using the net routing table to determine
5. The right destination. The called station receives a ringing signal.
6. The LED of [Network CO] button will be extinguished when the Net Call is cleared.

Conditions

1. Net call must be used without seizing a CO line.
2. User hears an error tone if there is no idle networking path.
3. In spite of ICM mode, the called party receives a ringing signal for the networking call.
4. When system detects the fatal error from the network, system sends the digit stream to the network using the alternate speed dial bin. In this case, the call is not a networking call.

Programming

VOICE INSTALL CO Line Registration – Net Basic Attributes

CO Line Registration – Net CO Line Attribute
CO Line Registration – Net Numbering Plan

Related Features

Hardware

2.80.1.2 Net Transfer

Description

A station user can transfer any kind of CO line to a station in other systems by pressing **[TRANS]** button and dialing a transferred station such as a call transfer within the same system. There are two kinds of transfer, screened and unscreened transfer.

There are two kinds of standard transfer method in H.450; Transfer by join and Transfer by rerouting. The main difference is how control the connecting path between transferring and transferred station. In case of Transfer by join, additional connecting path will be needed to transfer the call to another station. In case of Transfer by rerouting, new connecting path is used to transfer the call and old connecting path of transferring station will be cleared.

Operation

Screened transfer

1. Press the **[TRANS]** button at a station during conversation with a CO line. The CO line is placed on Exclusive Hold.
2. Dial the station number of another system to transfer the call. The transferred station of another system receives a ring signal.
3. Announce when the transferred station answers. Both stations can make a conversation each other, but the held CO is still in waiting on Transfer hold.
4. Hang-up to complete the transfer.

Unscreened transfer

1. Press the **[TRANS]** button at a station during conversation with a CO line. The CO line is placed on Exclusive Hold.
2. Dial the station number of another system to transfer the call.
3. Hang-up to complete the transfer.

Conditions

1. If both of transferred and transferred-to stations are located in the same system, the networking path will be cleared. That is, the transfer call will be setup as intercom call.
2. The transfer will be canceled when user presses the flashing [CO] or **[TRANS]** button.
3. Net Transfer call does not recall to the origination.
4. User hears an error tone if there is no idle networking path.
5. Net transfer is not activated to a busy station.

Programming

VOICE INSTALL	CO Line Registration – Net Basic Attributes
	CO Line Registration – Net Supplementary Attr.
	CO Line Registration – Net CO Line Attribute
	CO Line Registration – Net Numbering Plan

Related Features

Hardware

2.80.1.3 Identification Service

Description

Calling Name Identification Presentation (CNIP): When a user makes a net call and a name of station is programmed in the Station Name field, the system includes the name of calling party to the called party between systems.

Operation

1. A Net Call is arrived a station with LCD display.
   While ringing, the CNI will be displayed if they are included in the Setup message.

Conditions

VOICE INSTALL	CO Line Registration – Net Basic Attributes

Programming

VOICE INSTALL	CO Line Registration – Net Basic Attributes

Related Features

Hardware

2.80.1.4 Call Completion

Description

There are two kinds of call completion as follows;

Completion of Calls to Busy Subscribers (CCBS):

After calling a user in another system using basic call and encountering a busy tone. A station user can be notified when the busy destination of another system becomes idle. If the user wants to make a call to the destination on that notification, the call can be reinitiated to the destination of another system again.

Completion of Calls on No Reply (CCNR):
After calling a user in another system using basic call and encountering no reply. The caller can be notified when the destination becomes an idle status after some actions. If the caller wants to make a call to the destination, the call can be reinitiated to the destination again.

Operation

To make CCBS (Call Back)

1. Dial the station of another system that is a busy.
2. Press the [CALLBK] button while a busy tone is provided.
3. The call is cleared after a confirmation tone.
4. The busy station goes to Idle; the originator receives a call-back ring.
5. When the originator answers to the call-back ring, a new call will be activated to the calling station.

Conditions

1. Stand-alone IP Phone that supports H.450 can activate the Call Completion feature.
2. A station can leave or have only one callback message, and a new request will be left message wait indication message on busy station.
3. A voice message cannot be left even though the VSF is installed in a local system.
4. When the originator does not answer the call back ring within net timer, the call will be cleared.
5. There are two modes: One is connection mode and the other is connectionless mode. This can be selectable at Net Basic Attributes.

Programming

VOICE INSTALL	CO Line Registration – Net Basic Attributes
	CO Line Registration – Net CO Line Attribute
	CO Line Registration – Net Numbering Plan

Related Features

Hardware

2.80.1.5 Call Offer

Description

A busy user on one node is given notification that another call is waiting from another node. It is similar to a Camp-On function.

Operation

To activate Call Offer

1. Dial a busy station number of another system. The caller hears a busy tone.
2. Press the [CAMP ON] button or '*' during hearing a busy tone.
   The busy station receives an off-hook muted ring.

The calling station hears a ring-back tone instead of a busy-tone.

To answer the Call Offer

1. Press the flashing CO line button while receiving a muted ring.

Or,

2. The muted ring is changed to normal CO ring when you go on-hook state. Then you can answer the offered call.

Conditions

1. Call Offer is only applied to a station that is in talk status.
2. During a conference or paging, call offer is not activated.

Programming

VOICE INSTALL CO Line Registration – Net Basic Attributes

Related Features

Hardware

2.81 STATION CALL COVERAGE

Description

The Call Coverage feature permits a LIP Phone user to receive ring and answer calls directed to a covered station. This feature is generally employed to allow a Secretarial answering position to cover calls to other stations. When a covered station rings, the **{CALL COVERAGE}** button LED will flash and the covering station may receive ring (immediate or delayed) for the call. The covering station can answer the call using the **{CALL COVERAGE}** button, terminating ring at other stations. Once answered, the LED of **{CALL COVERAGE}** buttons for the station at other covering stations will extinguish.

Operation of this feature requires a **{CALL COVERAGE}** button at the covering LIP Phone and the covered station must activate call coverage. A station can have multiple Call Coverage buttons each covering a different station and multiple stations can have a Call Coverage button for a given station.

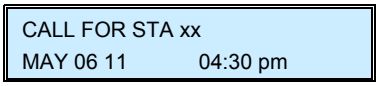
Operation

LIP Phone

To assign a **{CALL COVERAGE}** button at the covering station

[PGM] + **{FLEX}** + '*#' + covered Station number + **[SAVE]**

When a covered station receives a call, the covering station will receive the following display:



Conditions

1. A LIP Phone user may cover for an SLT or other stations. However, since a Flex button is required, an SLT cannot provide coverage for other stations.
2. When off-hook or in DND, the covering station will only receive a visual indication of the call from the LED of the **{CALL COVERAGE}** button and display, no off-hook ring is provided.
3. The **{CALL COVERAGE}** button will provide an appearance for CO lines that do not appear on the covering station except for Private Lines. To cover for Private Lines, the covering station must have an appearance and be allowed access to the Private Line.

Programming

Related Features

Hardware

2.82 IP CALL RECORDING

Description

System can record automatically or manually using IPCR server. IPCR(IP call recording) Server can be registered to iPECS SBG-1000 system. The station with agent ID is automatically recorded about call, external call.

Operation

Registration

Before registration, you should install the IPCR server in PC based on linux(os:fedora 12) using install CD or downloading from our BCS web site.

1. IPCR setting before registration to system.
   1.1) PBX registration(system IP, SIP ID, SIP Password)
   1.2) IPCR Server registration
   1.3) User registration
   1.4) Channel registration
2. System should set register MAC table for IPCR's MAC or set to "All Stations" in Registratio n Table page.
3. If SIP ID is not allowed, SIP ID and password should be set in PGM 443.

Programming Agent ID

1. Enter the number of IPCR's order in IPCR Agent page.
2. Match Agent ID to favorite station.
3. You can see the ACR(Auto-call recording) or ODR(On Demand Recording).
4. You should choice STN Type for station. But DID Type is for the future.

Two way recording

1. You should set IPCR group(ex: 620) and the SIP number of the IPCR as the member of IP CR Group.
2. Automatic Recording Destination should be set the IPCR Group(ex: 620).

Operation

1. IP-Phone(S100) without agent ID answered from IP-phone(S101) with agent ID(A500).
2. If S101 can conference 3 way, S101 connects IPCR with the agent ID(A500).
3. If you have flex button with two-way record of IPCR Group (620) and agent ID is ACR, it's flashed during two way recording. But it's ODR, first time, it's not flashed. After pressing the flex button (two way record), it's flashed. ACR is unconditionally recorded after connection and ODR is conditionally by user's choice.
4. Even though it's ODR, it can be recorded during talking. If users don't press the two-way recording button within talking, it's erased.

Conditions

1. You can search the recorded using Web Admin of IPCR.
2. IPCR server can be registered up to 10 servers in a system.

Programming

VOICE CONFIG	Station Group Data – IPCR Agent
	Station Group Data – Station Group Assignment
	Station Data – Common Attributes - Automatic Talk Recording Dest

Related features

Hardware

2.83 AUTHORIZATION CODES (PASSWORD)

Description

Authorization Codes provide a means to control access to Off Premise Call Forward or DISA and may be required for outgoing CO Line access based on configuration of the iPECS SBG-1000 database. When users dial an Authorization Code that matches an Authorization Code stored in the database, the system invokes the Station COS or the COS assigned to Authorization code. Each Authorization code has separate Day/Night mode COS assignments.

There are two types of Authorization Codes, Station and System. A Station Authorization Code is specifically related to a given station and intended for a single user. The System Authorization Codes are intended for use by any station in the system.

The Station Authorization Codes includes the associated station number and the assigned code. The structure of the System Authorization code can be set as either "*", or "*" the Authorization

table index and the code digits. The later allows duplicate codes to be employed using entry of table index to provide a unique identification of the entry.

Operation

LIP Phone

To enter an Authorization Code when second dial tone is received

1. Dial the station number for the Station Authorization code or, for a System Authorization Code, dial '*' or '*' and the Authorization table index.
2. Dial the corresponding Authorization Code.
3. Place call as normal.

SLT

To enter an Authorization Code when second dial tone is received

1. Dial the station number for the Station Authorization code or, for a System Authorization Code, dial '*' or '*' and the Authorization table index.
2. Dial the corresponding Authorization Code.
3. Place call as normal.

DISA

To enter an Authorization Code when second dial tone is received

1. Dial the station number for a Station Authorization code or, for a System code, '*' or '*' and the Authorization table index,
2. Dial the corresponding Authorization Code.
3. Place call as normal.

Conditions

1. When a DISA Line is marked for Authorization Code entry, the caller will hear DND Warning tone and must input a valid Authorization Code to continue. In case of an entry error, the user may retry entry of the code. In case of multiple entry errors, the user may retry entry based on the DISA Retry counter.
2. A user must enter a valid code within the number of attempts assigned as the Auth Retry Count.
3. The default Station Authorization code is the station number and "*".
4. The total number of Authorization codes is provided in Table 1.4-1.
5. An Authorization code may include any dial pad digit except '#'.
6. Duplicate or conflicting System Authorization codes are not allowed when using the older "*" and code operation. For example, code '1234' conflicts with code '123' and cannot be recognized as a unique code. Since the index operation employs the table index and the station number forms part of the Station code, conflicts will not occur and duplicate codes are allowed for these types of Authorization code.
7. Use of Authorization codes varies based on the system nation code. In some regions, particularly the US and UK, a System Authorization code may be required for DISA access. Entering a Station code on a DISA line will fail in these areas.

Programming

VOICE CONFIG	Station Data – Authorization Code & COS
	System Data – System Attributes – DISA Retry Count
	System Data – System Attributes – Auth Retry Count
	System Data – System Attributes – Old Auth Code Usage

Related features

Auto Service Mode Control
CO/IP AccessCO Access
Temporary Station COS/Lock
Call Forward
Station User Programming & Codes

Hardware

2.84 USB UPGRADE

Description

The Attendant can upgrade iPECS SBG-1000 via USB memory. Before upgrading, a user must save the iPECS SBG-1000 Rom file (GS87MXXXX.rom) in the top directory of USB memory.

Operation

Attendant

To upgrade iPECS SBG-1000 in Attendant phone

1. Save the iPECS SBG-1000 Rom file (GS87MXXXX.rom) in the top directory of USB memory.
2. Insert the USB memory into the USB port on iPECS SBG-1000.
3. Press the **[PGM]** button.
4. Dial 09 (Attendant Station Program code).
5. Number of iPECS SBG-1000Rom file in USB memory is displayed.

```
ROM FILE NUM : TOTAL 2
PRESS 0-1 TO VIEW FILE
```

6. Dial Number of iPECS SBG-1000 Rom file to display iPECS SBG-1000 Rom file name.

```
0 : GS87M10Ar.rom
PRESS [SAVE] TO UPGRADE
```

7. Press the **[SAVE]** button to upgrade iPECS SBG-1000.

```
0 : GS87M10Ar.rom
COPY IN PROGRESS
```

```
0 : GS87M10Ar.rom
BURNING IN PROGRESS
```

8. Following upgrade, result confirmation is displayed.

```
0 : GS91MA0Af.rom
PRESS [SAVE] TO RESTART
```

9. Press the **[SAVE]** button to restart iPECS SBG-1000.

Conditions

1. USB upgrade using the Attendant Station programming will support up to 10 ROM image files.

Programming

Related Features

Hardware

3. WEB ADMINISTRATION

Smart Business gateway (iPECS SBG-1000) incorporates a Web Server. Using a Web browser the system's Web Server can be accessed and the database managed in a user-friendly environment. In addition to modifying the system database, Web Admin provides for system file upload, remote upgrade, and database download.

http://192.168.1.1

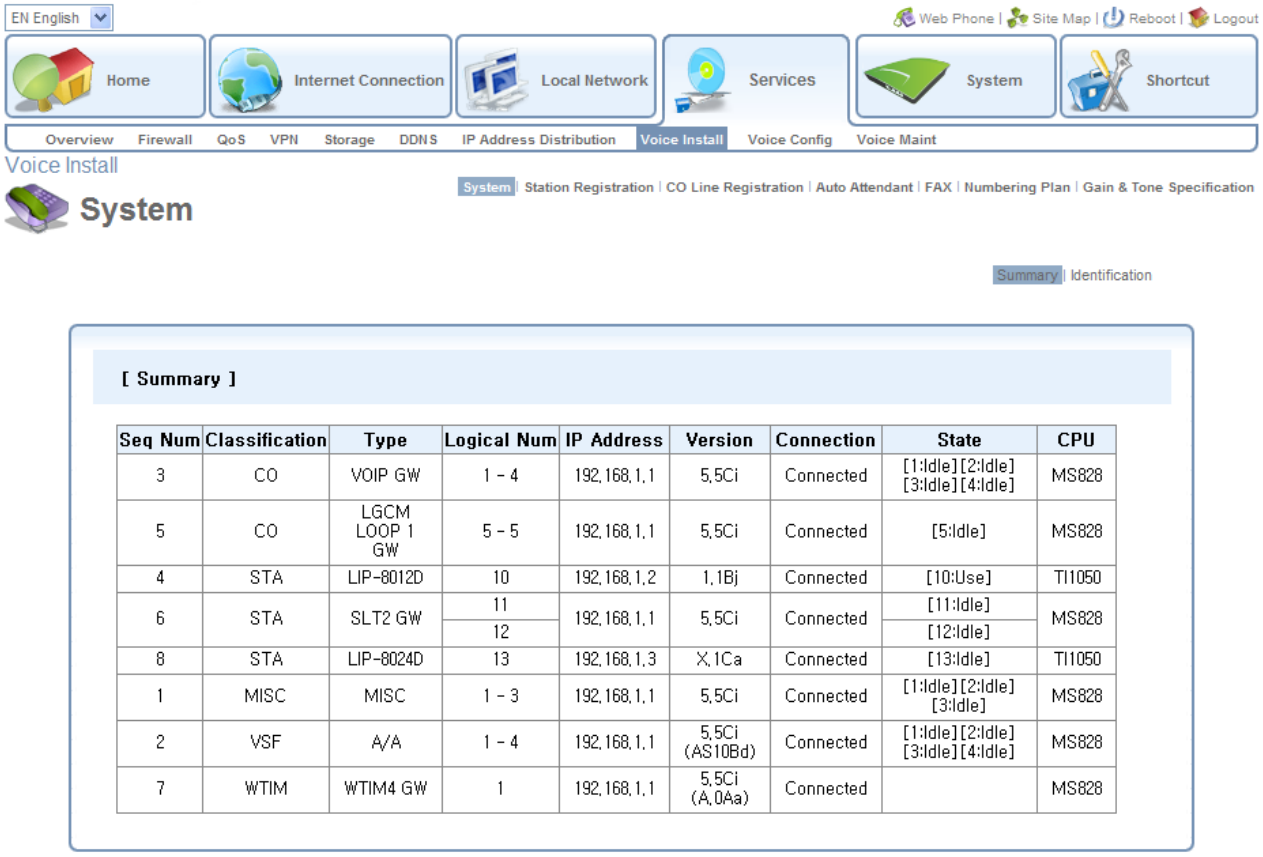
When accessed, the system will display the iPECS SBG-1000 Web Admin. Log In screen where the user must enter an assigned ID and password.

Items in the Menu bar can be clicked to display the items listed which are described further in the following sections:

- Voice Installation – access to database for system installation
- Voice Configuration – access to database for system configuration including Station, SIP Line data
- Voice Maintenance – permits database download and system or device upgrade

3.1 VOICE INSTALLATION

In this section, the user can see or change the database for system installation including the nation code, Station Registration, Station/CO Line Registration, Auto Attendant, FAX, numbering plan, Admin Authorization. Gain & Tone specification, and System Tone Frequency can be modified.



Seq Num	Classification	Type	Logical Num	IP Address	Version	Connection	State	CPU
3	CO	VOIP GW	1 - 4	192.168.1.1	5.5Ci	Connected	[1:Idle] [2:Idle] [3:Idle] [4:Idle]	MS828
5	CO	LGCM LOOP 1 GW	5 - 5	192.168.1.1	5.5Ci	Connected	[5:Idle]	MS828
4	STA	LIP-8012D	10	192.168.1.2	1.1Bj	Connected	[10:Use]	TI1050
6	STA	SLT2 GW	11	192.168.1.1	5.5Ci	Connected	[11:Idle]	MS828
			12				[12:Idle]	
8	STA	LIP-8024D	13	192.168.1.3	X.1Ca	Connected	[13:Idle]	TI1050
1	MISC	MISC	1 - 3	192.168.1.1	5.5Ci	Connected	[1:Idle] [2:Idle] [3:Idle]	MS828
2	VSF	A/A	1 - 4	192.168.1.1	5.5Ci (AS10Bd)	Connected	[1:Idle] [2:Idle] [3:Idle] [4:Idle]	MS828
7	WTIM	WTIM4 GW	1	192.168.1.1	5.5Ci (A.0Aa)	Connected		MS828

3.1.1 System

3.1.1.1 Summary

This page displays information of registered devices including the device type, logical number, IP address, version of device, connection status and current state of each devices, and also known CPU type.

3.1.1.2 Identification

Under Identification, the country is identified using International Dial codes (Nation Code). A Site Name (up to 24 characters) and My Area Code (local area code) maybe defined. The Site Name is primarily useful for the installer/programmer as a reference to customer. This information is used to set gain, frequencies and other system characteristics specific to the country and regional regulatory requirements.

In addition, the system can be programmed to select the base Flexible Number Plans, which are the numbering plans for the normal case and for the networking case. Individual items from the selected base Numbering Plan can be changed under Flexible Numbering Plan in section 3.1.6.

3.1.2 Station Registration

3.1.2.1 Station List & Replacement

Registered station list is displayed on this page; a user can see IP address, device type, version of device, connect status of registered devices. In addition, a user can change the logical number of station, station name, remark and so on.

3.1.2.2 Registration Table

By entering device MAC addresses, the system will allow the device to register.

While initial installation, you may want to register all connected stations without MAC address programming. Then you should select “All Stations” in front of Save button on the “Registration Table” web page and click Save button. After all connected stations are registered, you should select back to “MAC matched Station Only” to prevent unintended device registration. While “All Stations” can be registered, 4th LED – IP-PBX LED will be flashing more rapidly as warning sign.

3.1.2.3 Station User Login

Station User Login is primarily intended for Phontage and SIP extension registration. A station must register with the system each time it is connected to the system. A user may register the Phone employing a Login code (User ID) and password. Once registered, the station number is assigned. Once registered, this User ID must match the password for future registrations. The ID and password can be pre-assigned along with desired station number and a remark. A link-paired station can be assigned or pre-assigned by assign the same Desired-Number as a Master station.

Table 3.1.2.3 Station User Login

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Registered Number	Station number registered to the station, displayed only after registration	Station number	
Linked	Indicates Linked pair status and station number, displayed only	M or S	
ID	User Login ID.	12 Characters	
Password	User Login password	12 digits	
Desired Number	Station number desired for the device.	Station number	

3.1.2.4 DECT Registration

On this page, the DECT id and authorization codes are defined. In addition, a pull down menu selects one of four subscription events, subscribe, (de)subscription, mobility or display registered stations. A separate password box permits password entry to terminate (erase) all DECT subscriptions.

Table 3.1.2.4 DECT Registration

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Park Code	PARK (Portable Access Rights Key) Code : Unique System Id entered at DECT handset subscription to identify the system. To assign a PARK code, enter code and click [SAVE].	14 digits	
AC Code	Authentication Code entered at DECT handset to verify subscription. To assign AC Code, enter AC value and click [SAVE].	Up to 8 digits	
DECT Subscribe Enable	Enables the system to accept subscription from a DECT handset.		
Desired Station	Desired station number for the wireless DECT handset		
Type of Phone	Two types of phones may be selected including type for GDC-450H and type for LWS-WK.	GDC-34x/4xx LWS-WK	GDC-34x/4xx
	Press [SEND] after entering the number and type.		
DECT Unsubscribe	Terminates the subscription for a DECT handset.		
Station Number	Enter the registered station number and click [SEND], the subscription is terminated and the wireless DECT handset will no longer be serviced.	Station number	
DECT Mobility	When a DECT handset is registered at multiple systems that are networked, calls can be routed over the network to the DECT handset location.		
Station Number	Enter the registered station number, select Mobility ON or OFF and click [SEND].	Station number	
Registered Stations	Displays all registered DECT handsets.		

3.1.3 CO Line Registration

3.1.3.1 CO Channel List

CO channel list is displayed on this page; a user can view CO line numbers, and connect status of each CO channel. In addition, a user can change the usage of each CO channel and jump to routing program for each CO line types.

3.1.3.2 MSN Configuration

This page is enabled only when iPECS SBG-1000 has BRI port (BRIU option board is installed).

MSNs can be assigned in iPECS SBG-1000 up to 5 Calling/Called IDs. Those values are used for CLI of outgoing call and for incoming call routing. Last 3 digits of IDs are treated as flexible DID table bin while incoming call routing.

3.1.3.3 SIP ID Configuration

Various parameters must be entered for proper operation of SIP Trunking including SIP registration related information and the program for incoming call routing.

Table 3.1 SIP ID Configuration Attributes

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Table Utility	If registration is enabled (refer to Registration Option) the iPECS SBG-1000 can send the User ID to the SIP Proxy for registering the ID. Otherwise, the Authentication user ID and password are used.	USE/NOT USE	NOT USE
Registration Option	In some situations (during provisioning of the SIP Server or Proxy), it may be desirable not to attempt registration. This field may be used to determine if registration should occur.	Register Provision	Provision
Register User Name	User ID@Domain.	64 characters	
Authentication User ID	Authentication name assigned in SIP Proxy when required for registration.	64 characters	
Authentication User Password	User password as assigned in SIP Proxy when required for registration.	128 characters	
Contact Number	User ID.		
Name of Called Number	Name of Called Number		
Route To (Day-Mode Period)	Call routing destination in Day-Mode		Station Group 631
Route To (Night-Mode Period)	Call routing destination in Night-Mode		Station Group 631
Route To (Timed-Mode Period)	Call routing destination in Timed-Mode		Station Group 631
See Caller Number First	Call is routing according to the 'Call Routing by Caller Number' if caller number is matched	ON/OFF	OFF

3.1.3.4 Server Information

Various parameters must be entered for proper operation of SIP Trunking including SIP proxy and Registration.

Table 3.1 Server Information Attributes

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Proxy Server Address	SIP Proxy server IP address.	IP address	
Proxy Server Port	Default port for SIP messages to proxy.	Port	5060
Proxy Registration Timer	Time-out for registration.		3600
Domain	Domain name associated with VOIP channels. Is used in SIP "TO: header message" to SIP Server. Required when the Proxy uses a port other than 5060.	Max 32 Characters	
SIP Pound Use	ON: Send digit '#' when user press '#' OFF: The '#' is used for sending complete.	OFF ON	ON
CODEC Priority Configuration	1st . priority 2nd. priority 3rd. priority 4th. priority 5th. Priority 1) If speficy priority to a specific CODEC then it will work for negotiation RTP data. 2) If only 1st. priority is specified and the others are none, then it will work as single CODEC only does.	none g.711-u g.711-a g.723.1 g.729 g.729-a	none

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Fail Over Usage	SIP Module Service Down ON or OFF when in Registration Fail or Link Down	0: OFF 1: ON	ON
No Response Time to Fail Over	Call Setup No Response : no response timer after send outgoing setup message to SIP proxy server - 0 or [Empty] : do not use 'no response timer' 3~10 : wait for 3 to 10 second	0, 3 ~ 10 sec	5 sec
Fail Over CO Group Number	FailOver CO Group Number : Case #1 - when SIP CO line is in connected/alive state : after no response time, setup message will be re-sent using this failover CO line group Case #2 – when SIP CO line is in disconnected/OOS state : setup message will be sent using this failover CO line group	1 ~ Max Number of CO Group	none

3.1.3.5 Network Basic Attributes

Selecting Network Basic Attributes will display the Network Basic Attributes entry page.

Table 3.1.3.5 Network Basic Attributes

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Net Enable	Enable Networking function	1:ON 0:OFF	OFF
Net Retry Count	Reserved for future usage	00-99	00
Net CNIP Enable	The name of calling station is sent to the called system between iPECS systems. CNIP is displayed at called party stations display based on the programming	1:ON 0:OFF	ON
Net CONP Enable	Reserved for future usage	1:ON 0:OFF	OFF
Net Signal Method	Select the information element type for QSIG supplementary service message.	1:FAC 0:UUS	FAC
Net Cas Enable	It is not used.	1:ON 0:OFF	OFF
Net VPN Enable	Reserved for future usage	1:ON 0:OFF	OFF
Net CC Retain Mode	It is not used.	1:ON 0:OFF	OFF

3.1.3.6 Network Supplementary Attributes

Selecting Network Supplementary Attributes will display the Network Supplementary Attributes entry page.

Table 3.1.3.6 Network Supplementary Attributes

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Net Transfer Mode	Select type for Transfer and Call forward – Rerouting or Join	1:RERT 0:JOIN	RERT
TCP Port for Blf	TCP port for sending BLF message to BLF Manager	0000-9999	9500

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
UDP Port for Blf	UDP port for sending BLF message to BLF Manager	0000-9999	9501
Blf Manager IP	IP Address of BLF Server used only when iPECS is configured with LDK systems for Voice Networking.		0.0.0.0
Duration of BLF Status	Duration of BLF status message sending to BLF Server	01-99 (100 msec)	10
Multicast IP	IP address of Multicast for BLF service		0.0.0.0
Net Trans Rcl timer	Network transfer fault recall timer to be used when no responses from other systems.	001-300 (msec)	10
NET Reroute CO Group	The start times for Day, Night and start and end times for Timed modes are entered for each day of week. After Timed end time the mode goes to day if time is less than Night mode.	MFIM & MFIM100:& IPECS-Micro& IPECS-50 00-20 Other MFIM: 00-72	0

3.1.3.7 Network CO Line Attributes

Selecting Network CO Line Attributes will display the Network CO Line Group entry page. Enter the desired data and click Load to display the Network CO Line Group.

Table 3.1.3.7 Network CO Line Attributes

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Net CO Group	Networking CO group programming for Networking call.	00-24	00
Net CO Line Type	Select network CO Line Type	1:NET 0:PSTN	PSTN

3.1.3.8 Network Numbering Plan Table

Selecting Network Numbering Plan Table will display the Network Numbering Plan Table data entry page.

Table 3.1.3.8 Network Numbering Plan Table

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
System Usage	Select system usage	0:NET 1:PSTN	NET
Numbering Plan Code	'*' means any digits can be inserted between 0 ~ 9. The digits followed by '#' is a internal station number	16 digits	
Numbering Plan CO Group	'00' means an internal net station number.	00-24	. .
CPN Information	Flex 1: ISDN CPN INFORMATION Flex 2: (FLEX BTN 1- 4) 1: 00 CPN INFORMATION 01 2: 00 CPN INFORMATION 02 3: 00 CPN INFORMATION 03 4: 00 CPN INFORMATION 04	16 digits	
Alt Speed Bin	Alternative Dial Number (System SPD Bin) when the networking path has a fatal problem.	200-999 or 2000~4999	

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
MFIM (E) IP Address	IP Address of destination MFIM/E system only when iPECS systems are configured for Voice Networking		0.0.0.0
MFIM(E) Port	Port Number of destination system for Networking.	0000-9999	5588
Digit Repeat	When the number plan code, see above, is for PSTN call or transit-call, this number code can be enveloped in SETUP message or not whether if this field is set or not.	Yes No	No
Net PSTN Enblock	Choose “Transit-out Public Line” as Enblock or Over-lap.	Yes No	No
PSTN CLI Method	NET: Send network station number for CLI PSTN: Send full CLI (eg, 02-450-1000)	NET PSTN	NET
CO Attendant Code CLI	Determine whether if Centralized ATD CLI is sent or not when slave system makes transit call.	On Off	Off
Firewall Routing	Select IP address (Firewall IP address or Non-firewall IP address). If the destination system(VOIM) is in same VPN then Non-firewall IP address should be sent. Otherwise the firewall IP address should be sent. ON : Send firewall IP address OFF : Send Non-firewall(Internal) IP address	On Off	ON
Transit Out Auth COS	When there’s a transit out call request from slave system user by seizing CO line, apply COS according to the authorization code.	Yes No	No
SMDR Dgt Hide	Determine to display dialed digit of transit out call or not at the slave system ; it can contain authorization code.	Yes No	No

3.1.3.9 Network Feature Code Table

Selecting Network Feature Code Table returns the data entry page.

Table 3.1.3.9 Network Feature Code Table

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Net Feature Code	Networking Feature Code programming for Networking paging call.	16 digits	None
Net Feature Destination	INT PAGE ZONE : 1-10 ALL CALL PAGE ZONE : INT(1), ALL(3)	3 digits	N/A

3.1.4 Auto Attendant

3.1.4.1 Voice Mail Group Number

A user can program Voice Mail Group Numbers using this page.

3.1.4.2 System Prompt Upload

A user can upload system prompt information using this page; system prompt can be uploaded with .rom format or .wav format.

1. Prompt Upload menu: upload rom file

??96Wxxxx.rom (?? is nation, i.e., PM, IT, GS, KR, etc.; xxxx indicates the version)

2. Individual Upload menu: upload wave file
   1.wav – 255.wav (system prompt should be G.711 u-law wave file format)

3.1.4.3 Announcement Upload & Download

A user can upload and download announcements with .rom format or .wav format.

1. Individual upload/download: upload .wav file
   1.wav – 72.wav
2. SysGreeting upload/download: upload .rom file
   SGTYPE1.rom

3.1.5 FAX

FAX Configuration page displays the logical station number of SLT port; a user can change FAX utilization of each SLT port and also can make T.38 service enabled for FAX.

3.1.6 Numbering Plan

Feature dial codes for the system can be assigned using the System Flexible Number Plan. Feature codes should be one (1) to four (4) digits in length and must not conflict. For example, Feature codes 53 and 536 represent a conflict. The system will not update the database until correct data is entered. The Table provides a brief description for each feature and default codes.

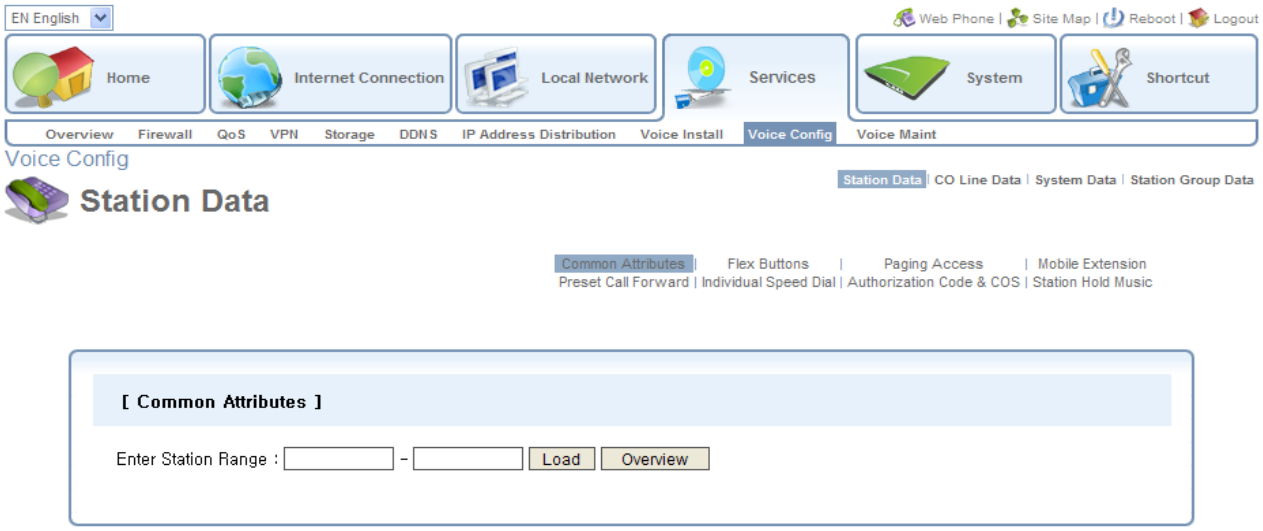
Table 3.1.6 Flexible Numbering Plan

ATTRIBUTE	DESCRIPTION	DEFAULT
Attendant Call	Dial code to call Main Attendant	0
Alarm Reset	Code to reset Alarm contacts	65
Direct Call Pick-Up	Dial code to activate Directed Call Pick-up	7
Group Call Pick-Up	Group Call Pick-up dial code	**
Answering Machine Emulation	Dial code to assign an Answering Machine Emulation Flex button	64
Call Forward	Code to activate Call Forward.	54
Door Open	Dial code to activate Door contact (open door)	#*
Call Coverage Ring	Code for Call Coverage button	*#
Access Random CO Line	Dial code to access the 1st available CO Line in any accessible group	9
CO Line Group Number	Dial code to access a CO Line from a group	801-802
Access Individual CO Line	Dial code to access a specific CO Line/IP Channel	8801-8805
Paging Zones	Page Zone access dial codes	501-510
All Call Paging	All Call Page access dial code	500
Answer Paging (Meet Me)	Meet-Me-Page answer dial code	511
Call Park Locations	Dial code to place/retrieve a call in system Park Orbit	601-610
Group Pilot Number	Station group pilot number	620-631
Do-Not-Disturb (DND)	Dial code to activate Do-Not-Disturb	53
DND/FWD Cancel	Code to cancel DND/FWD	59
Leave Call-Back	Code to activate Message Wait/Call Back	56
Answer Call-Back	Code to return Message Wait/Call Back	57
Camp-On Answer	Dial code to answer a Camped-On call	66

ATTRIBUTE	DESCRIPTION	DEFAULT
Last Number Redial (LNR)	SLT Last number redial feature access dial code	52
Speed Dial Program	SLT Speed Dial programming access code	55
Speed Dial Access	SLT Speed Dial access code	58
CO Line System Hold	Code to place a CO Line call on System Hold	67
Retrieve Any Of Held CO Line	Dial code to access last CO Line or IP channel from Hold	8*
Retrieve Specific Held CO Line	Dial code to access a specific CO Line/IP channel from Hold	8#

3.2 VOICE CONFIGURATION

In this section, user can see or change database for Station, CO Line, System, Station Group (shown).



3.2.1 Station Data

3.2.1.1 Common Attributes

The Common Attributes Table defines features and functions available to the station.

Table 3.2.1.1 Common Attributes

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
CLI Table Index	Default outgoing CLI Table Index.	0-5	1
CLIR Service	CLIR (Calling Line Identification Restriction), an ISDN service, removes the calling party ID sent from the ISDN to the called party with a RESTRICT instruction in the SETUP message. If enabled, the system will send the RESTRICT instruction to the CO when an outgoing ISDN call is placed.	ON OFF	OFF

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
COLR Service	COLR (Connected Line Id Restriction), an ISDN service, removes the connected party ID sent from the ISDN to the calling party with a RESTRICT instruction in the CONNECT message. If enabled, the system will send the restrict instruction to the CO when the station places an ISDN call.	ON OFF	OFF
CO Group Access	Stations can be allowed or denied access to CO group.	1, 2, 3, 4, 5	1, 2, 3, 4, 5
Station Forward No Answer Timer	This timer determines the duration the station will ring prior to Ring-No-Answer Forward. This setting affects both manual and Preset Call Forward and overrides the Call Forward No Answer Timer in System Call Feature Timer	000-600 seconds	000
Active in OOS	If a station is Out-of-Service and has previously forwarded calls, the system will forward the calls if enabled.	ON OFF	OFF
DID Call Wait	When a busy station receives an external call, the call may queue to the station instead of receiving a busy tone. With Call Wait, the caller will hear a Ring-back tone and the CO line LED flashes.	ON OFF	ON
Voice Over	Enables use of Voice Over by station	ENABLE DISABLE	DISABLE
Prime Line	Enables Delayed Prime Line (Idle Line) activation, see Idle Line Selection.	HOT WARM	WARM
Idle Line Selection	When a station goes to an off-hook condition (lifts handset or presses **[speaker]** button), the system normally provides intercom dial tone. In place of dial tone, the station can be programmed to activate Flex button as if pressed, access a CO Line, access CO Group or call a Station	No Selection Flex Button (1-24) CO Line (1-8) CO Group (1-5) Station	No Selection
CO PGM	A station can be permitted to change the CO Line numbers (ports) associated with a CO Line button.	Disable Enable	Disable
Automatic Talk Recording Dest.	When Auto Call recording is defined for a station, the recording Phontage station number or station group number is defined here.	Station Station Grp	
Headset Ring	Selects device to receive incoming ring signals (Speaker, Headset or Both).	Speaker Headset Both	Speaker
Headset or Speaker Mode	Select Speaker or Headset mode for the IP Phone.	Headset Speaker	Speaker
Send SLT CLI Info	When allowed, the system sends CLI information to the SLT	ON OFF	ON

3.2.1.2 Flex Buttons

Each Flex button on a LIP Phone can be assigned a function (TYPE) as listed:

- Empty
- Number Plan
- User Program code
- Station Speed Dial
- System Speed Dial

After selecting the Type for a button, enter the appropriate value (Where applicable).

3.2.1.3 Paging Access

Each LIP Phone is assigned to be able to receive announcements from each Page Zone. A station can be assigned to any, all, or no page zones. The iPECS SBG-1000 system supports up to 10 Internal Page Zones. By default, all stations are assigned to Zone 1.

📖 ***NOTE:*** *A station not assigned to any page zone will not receive any page announcements.*

3.2.1.4 Mobile Extension Table

Selecting Mobile Extension Table will display the Mobile Extension data entry page.
A mobile phone can be used in conjunction with an LIP Phone. The Mobile phone can access system resources available to the user's wired phone and will receive ring for incoming iPECS SBG-1000 calls. The user may be allowed to enable the Mobile extension and define the mobile number. The system can be defined to employ a specific CO Line Group to place calls to the Mobile phone. In addition, the mobile phone can be assigned to receive hunt group calls to the primary extension. Also, parameters for notification of new VSF voice mails can be defined.

Table 3.2.1.4 Mobile Extension Table

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Internal Access	The user may be allowed to access internal call from the mobile extension.	Disable/Enable	Disable
Usage	The user can be allowed to register a Mobile phone number.	Disable Mobile Ext Fail Over	Disable
Hunt Enable	When the paired station is a member of a hunt group (Circular or Terminal), group calls can be sent to the active mobile extension.	Disable Enable	Disable
VSF/VMIM Notify	Enables outbound notification by the system when the VSF has unheard messages.	Not Use Use	Not Use
Notify Retry	Defines the number of attempts the system will make to complete a notification when receiving busy/no-answer.	1 – 9 Times	3 Times
Retry Interval	Defines the time between notification attempts. If a notification fails, the system will retry after the timer expires.	1 – 3 Minute	3 Minute
CO Group	CO group used to call the mobile extension.	0 ~ 5	01
Telephone Number	Telephone number or CLI of the Mobile extension.		Not assigned
CLI Number	When the mobile Telephone number and CLI do not match, the CLI entered here is used to authorize incoming calls from the mobile.		Not assigned

3.2.1.5 Preset Call Forward

Stations can be programmed so that incoming CO and Intercom calls are forwarded to a preset station or station group. This allows an external call or internal call to initially ring at a station and forward to a pre-determined destination. Preset Call Forward can be separately assigned

Unconditional, Internal Busy, Internal No Answer, External Busy or External No Answer preset forwarding to any station, hunt group or system speed dial bin (off-net). As a default, no Preset Call Forward is assigned.

For Transfer Mail-Box, enter the Station Group number of the Voice Mail group; this will permit LIP Phone users to forward calls directly to the desired user's Voice Mail-Box.

3.2.1.6 Individual Speed Dial

Each user can store commonly dialed numbers for easy access using Individual Speed Dial bins. Each station has access to 20 Speed Dial numbers; each Speed Dial number can be up to 23 characters in length and may include special instruction codes.

Special instruction codes available are:

'*' as 1st digit Activate Display Security, do not display number.

LIP Phone users may assign a Flex button for One-Touch access to a specific Speed Dial bin. In addition, the LIP Phone user may assign a Telephone number directly to a Flex button. In this case, the telephone number is allocated to the highest numbered available Individual Speed Dial bin.
Stored speed dial number should not include CO access code.

3.2.1.7 Authorization Code & COS

Authorization codes (up to 12 digits) are used to control access to system resources and facilities. Voice Mail-box and certain Call Forward types may require the input of a valid Authorization code. The Station entries are associated with individual stations.

All stations are assigned a Class-of-Service (COS), which determines the user's ability to dial certain types of calls (refer to Station COS Table). Separate COS assignments are made for Day, Timed and Night Mode operation. As a default, all stations are assigned with a Station COS of 1 for all modes (No restrictions).

Table 3.3.1.7 STATION COS

STATION COS	RESTRICTIONS
1	No restrictions are placed on dialing from the station.
2	The assignments in Exception Table A are monitored for allow and deny numbers.
3	The assignments in Exception Table B are monitored for allow and deny numbers.
4	The assignments in both Exception Tables A & B are monitored for allow and deny numbers.

A station must be allowed Off Net Fwd to forward external incoming calls outside the system or establish a CO-to-CO connection.
If Station Account is set to "ON", the station user must enter an authorization code to access CO lines.

3.2.1.8 Station Hold Music

iPECS SBG-1000 supports two types of Hold Music for Intercom calls. One type of MOH is Hold Tone, and the other type is Record Play. A VSF announcement may be recorded and played as MOH to the connected caller.

3.2.2 CO Line Data

3.2.2.1 Call Routing by Line

This page is enabled only when iPECS SBG-1000 has FXO ports (CSIU, CIU1 or CIU2 option board is installed).

Each CO line is assigned to signal a station or group for an incoming call (Ring). Separate ring assignments are made for Day, Night, and Timed Ring modes. When assigned to ring to a VSF announcement, the call can be dropped automatically after the assigned announcement by checking the “Auto Drop”.

When CO Lines are programmed to Ring to a VSF Group as an Automated Attendant, the Ring signal can be on an immediate or delayed basis allowing other stations/groups to be assigned Ring and answer prior to signaling the AA. The delay is defined in seconds from 00 to 30.

When a call is received, the system may use the ICLID (Incoming Caller ID) to route the call. The system will delay routing a call for ICLID ring timer while awaiting ICLID. If ICLID ring timer is 0, ICLID routing is disabled.

3.2.2.2 Call Routing by Called Number

This page is enabled only when iPECS SBG-1000 has BRI port (BRIU option board is installed).

These characteristics are required for proper operation of the system and BRI incoming call destination selection.

Table 3.2.2.2 Call Routing by Called Number

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Name of Called Number	Name of Called Number		
Route To (Day-Mode Period)	Call routing destination in Day-Mode		Station Group 631
Route To (Night-Mode Period)	Call routing destination in Night-Mode		Station Group 631
Route To (Timed-Mode Period)	Call routing destination in Timed-Mode		Station Group 631
See Caller Number First	Call is routing according to the ‘Call Routing by Caller Number’ if caller number is matched	ON/OFF	OFF

3.2.2.3 Call Routing by Caller Number

The system can employ Incoming Calling Line ID (ICLID) to determine the routing of incoming external calls. The system will compare the received ICLID, and if a match is found, will route the call to the destination defined in the Ring Assignment Table index.

Table 3.2.2.3 Call Routing by Caller Number

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Caller Number	ICLID (Incoming Caller ID) to match for the index. If the Caller ID matches the Table entry, the index is used to select the route.	23 Digits	None
Caller Name	ICLID name that is sent by the system to the destination for the ICLID routed call.	12. Character	None

3.2.2.4 Ring Assignment Table

If the Incoming Caller ID matches an entry in Call Routing by Caller Number, the index from the Table is used to determine the call routing from the Ring Assignment Table. Separate ring assignments are made for Day, Night, and Timed Ring mode for each index, 001 to 250, in this table. When assigned to ring to a VSF announcement, the call can be dropped automatically after the assigned announcement by checking the “Auto Drop”.

When CO Lines are programmed to Ring to a VSF Group as an Automated Attendant, the ring signal can be on an immediate or delayed basis (00-30 sec.) allowing other stations/groups to be assigned ringing and answer prior to signaling the AA.

3.2.2.5 Exceptional Call Routing

When a DID line or DISA user dials an invalid/vacant or busy station number the caller will be sent to the assigned destination. The destination is separately defined for invalid, busy, and No Answer conditions and can be defined as the Attendant, busy tone or a Station Group. For calls on a DID line to a busy station, DID Call Wait can be assigned, refer to Station Common Attributes in section 3.2.1.1.

Also, for DID calls only, announcements (prompts) can be sent from the VSF to the caller for various conditions, busy, error, DND, No Answer, or Attendant Transfer.

3.2.2.6 Call Routing by Auto Attendant

The system incorporates Interactive Voice Response (IVR) capabilities called Customer Call Routing (CCR). After or during a VSF Announcement, the caller may dial digits to select a destination or route for the call. The CCR Table defines the destination type and value associated with the digit dialed by the caller in response to the index, a VSF Announcement (01-70). Up to 70 single-level Audio Text menus may be assigned or, multi-level menu structures (maximum 70 levels) can be established using one menu as a destination for the previous level.

Table 3.3.2.6 Customer Call Routing Auto Attendant Destinations

DESTINATION	VALUE RANGE
Station	10~33
Station Group	620~631
Common Speed Dial	200~999
DVU Announce	01~70
DVU Announce and disconnect	01~70
Paging Zone	01~10
All Call Paging	n/a
Voice Mail	620~631 & 10~33

3.2.2.7 Common Speed Dial

Commonly dialed numbers can be stored by the Attendant or the Administrator in Web Admin. for easy access by stations allowed use of Common Speed Dial bins. Up to 800 Common Speed Dial numbers are available; each Speed Dial number can be up to 23 characters in length and may include special instruction codes.

Special instruction codes available are:

'*' as 1st digit Activate Display Security.

LIP Phone users may assign a Flex button for One-Touch access to a specific Common Speed Dial bin.
Stored speed dial number should not include CO access code.

3.2.2.8 CO Hold Music

iPECS SBG-1000 supports two type of Hold Music for CO Line calls. One type of MOH is Hold Tone, and the other type is Record Play. A VSF announcement may be recorded and played as MOH to the connected caller.

3.2.3 System Data

3.2.3.1 System Attributes

The default codec can be defined as G.711 for decreased bandwidth needs. The codec will be used on all internal communications as well as for other remote devices.
A DISA user is allowed to retry erroneous authentication code entries. DISA Retry Count sets the number of retries before the system disconnects.
When an Authorization code is required, the user may attempt to enter a Valid code up to the maximum value defined in Auth Retry Count.
If Old Auth Code Usage is set to "ON", System Authorization codes must be entered by the user as * and the code. And if it is set to "OFF", codes should be entered as *+ the Auth code index and the code.

If End code(#) usage in System Auth Code is set to “ON”, End code(#) must be entered when system Auto code is entered.
If Station VM Feature Usage is set to “ON”, Station VM feature can be used.
If WAN Fault Alarm Disable is set to “ON”, the WAN Fault Alarm to Attendant will not happen. It will be useful to the site which does not use WAN port.

3.2.3.2 Call Feature Timer

A number of timers can be assigned to control and affect many features and functions.

Table 3.2.3.2 Call Feature Timers

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Attendant Recall Timer	Determines the amount of time the attendant receives recall after which the system will disconnect the call.	00~60 (minutes)	01
Call Park Recall Timer	Determines the amount of time before a parked call will recall the station that parked the call.	000~600 (seconds)	120
Camp-on Recall Timer	When a call is transferred using Camp-On, this entry determines the amount of time before the station that transferred the call receives recall.	000~600 (seconds)	030
Exclusive Hold Recall Timer	Determines the amount of time before a call placed on exclusive hold will recall the station.	000~600 (seconds)	060
I-Hold Recall Timer	Determines the amount of time a call that is recalling the station will recall before also recalling at the attendant.	000~600 (seconds)	030
System Hold Recall Timer	Determines the amount of time before a call placed on system hold will recall the station.	000~600 (seconds)	060
Transfer Recall Timer	Determines the amount of time a transferred call will ring at the receiving station before recalling the station that transferred the call.	000~600 (seconds)	060
ACNR Delay Timer	If the ACNR Pause Timer expires and no CO Line is available for ACNR recall, the delay timer sets the delay before ACNR again attempts to access a CO line. The ACNR retry counter is not affected by this action.	000~300 (seconds)	030
ACNR Pause Timer	This timer establishes the time between ACNR recall attempts (CIS=5-300).	030~300 (seconds)	030
ACNR Retry Counter	This counter sets the number of recall attempts for ACNR before ACNR is abandoned (CIS=1-9).	1~13	03
ACNR Tone Detect Timer	If call progress tones are not available for ACNR, the system will wait this duration after dialing before considering the called party “busy/no answer”.	001~300 (seconds)	30
Automatic CO Release Timer	If a user accesses a CO path and does not take any action, the system will automatically release the CO path when this timer expires.	000~300 (seconds)	030
CCR Inter-digit Timer	Inter-digit timer used with Customer Call Routing function.	000~300 (100 msec)	030
CO Dial Delay Timer	Delay for through connection to prevent illegal dialing when CO/PBX has slow response.	00~99 (100 msec)	05

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
CO Release Guard Timer	When a CO Line is returned to idle, the system will deny access for this time to assure the PSTN returns the CO circuitry to idle.	010~150 (100 msec)	020
CO Ring Off Timer	This timer sets the maximum 'Off' duration of the incoming ring cycle for the Ring Detect circuitry of the system to detect an abandoned call.	001~150 (100 msec)	060
CO Ring ON Timer	This timer sets the 'On' time of the incoming ring cycle for the Ring Detect circuitry of the system to recognize an incoming call.	1~9 (100 msec.)	2
Elapsed Call Timer	Users can receive a periodic tone indicating the length of an outgoing call. This timer sets the time before and between the tones.	060~900 (seconds)	180
Call Forward No Answer Timer	When a user activates No-Answer Forward, calls will ring for this duration before being forward. The Station No Answer timer will take precedence.	000~600 (seconds)	015
DID/DISA No Answer Timer	A DID/DISA call to a busy station will forward to the assigned DID/DISA Destination should this timer expire.	000~255 (seconds)	20
VSF User Maximum Record Timer	This timer sets the maximum duration allowed for the User Greeting in the system's basic Voice Mail.	000~999 (seconds)	60
VSF Valid User Message Timer	This timer sets the minimum duration allowed for a voice mail message in the system's basic Voice Mail. Messages shorter than this duration are not stored.	0~9 (seconds)	1
ICM Dial Tone Timer	If a user goes off-hook on the Intercom and takes no action for this timer, the user will receive error tone.	01~20 (seconds)	10
Inter Digit Timer	This timer sets the maximum time allowed between each user-dialed digit. At expiration, the user will receive error-tone.	01~20 (seconds)	03
MSG Wait Reminder Tone Timer	An LIP Phone user will receive periodic reminder tones of a message waiting at intervals of this timer.	00~60 (minutes)	00
Paging Timeout Timer	Determines the maximum duration of a page after which the caller and Page Zone are released.	000~255 (seconds)	15
Pause Timer	A Timed pause of this duration is used in speed dial and during other automatically dialed digits sent to the PSTN.	1~9 (seconds)	3
SLT Hook Switch Bounce Timer	This timer determines the duration the system considers an actual state change in the hook-switch and not a contact bounce.	01~25 (100 msec.)	01
SLT Maximum Hook Switch Flash Timer	This timer sets the maximum time an SLT user can depress the hook-switch for a Flash signal.	01~25 (100 msec.)	02
SLT Minimum Hook Flash Timer	This time sets the minimum time an SLT user must depress the hook-switch for a Flash signal.	000~250 (10 msec.)	008
Station Auto Release Timer	For an internal call, the system will return a station to idle if the call remains unanswered for this duration.	000~300 (seconds)	060
Prime Line Delay Timer	This timer sets the delay (no action duration) for delayed Prime Line operation.	01~20 (seconds)	05
Enblock Inter Digit Timer	When an ISDN Line is assigned to send digits Enblock, the system will send digits if the user dials "#" or this Enblock inter-digit timer expires.	01~20 (seconds)	3
DTMF Duration Timer	This timer establishes the duration of DTMF tones sent on a CO line.	04~99 (10 msec.)	10

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Flex DID Timer	The system will receive DID digits for this timer. After the timer expires, the system will use the last 2 to 4 digits received as the DID digits.	01~99 (100 msec.)	30
CO Flash Timer	This entry sets the duration of a Flash on the CO Line.	000~300 (10msec)	50
SIP Station Registration Timer	Shorter time will make more traffic. More than 10 minute recommended. 0 means registration timer is disabled.	0, 30~3600 (seconds)	3600

3.2.3.3 Day/Night/Timed Schedule

The system can be programmed to automatically select the Ring and COS mode based on time of day and day of week. Three Ring & COS modes are available: Day, Timed and Night. The Ring assignments are as defined in the Call Routing by Line and Ring Assignments Table. COS assignments are made according to Authorization Code & COS.

The start times for Day, Night and start and end times for Timed modes are programmed for each day of the week. After Timed end time the mode goes to Day if time is less than Night mode. The Attendant can override the Automatic selection and select the desired Mode (Day, Night, or Timed) manually.

3.2.3.4 Toll Exception Table

There are four Toll Restriction Tables arranged in pairs. Each pair consists of an Allow Table and a Deny Table. Each Toll Exception Table permits entry of 50 Allow codes and 50 Deny codes. Each code can contain up to 20 digits including digits 0-9, "#" as a wild card (any digit) and "*" as the end of entry mark.

Based on Table entries, stations or DISA users are allowed or denied dialing specified numbers. The following rules apply to establish restrictions based on the Table entries:

- If entries are only made in the Allow Table, only those numbers entered can be dialed, all other dialed numbers will be restricted.
- If entries are only made in the Deny Table, only those numbers entered will be restricted and all other numbers can be dialed.
- When there are entries in both the Allow and Deny Table pair, if the number is in the Deny Table, the number will be restricted otherwise the number can be dialed without restriction.

3.2.3.5 Emergency Dialing

The Emergency Code Table is used to identify emergency numbers, which when dialed, will override all COS dialing restrictions. An Emergency Code number may be up to fifteen (15) digits in length.

3.2.3.6 SMDR Attributes

Station Message Detail Recording (SMDR), which is output over TCP channel, contains details on both incoming and outgoing calls. Various SMDR attributes can be assigned including; output records for all calls or LD only, call cost per pulse when using call metering, etc. The following Table describes SMDR Attributes:

Table 3.2.3.6 SMDR Attributes

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Call Metering	Selects the call-metering signal from the PSTN to indicate call cost	NONE NPR	NONE
Save Enable	The system can output all outgoing call records (ON), or to allow for PSTN call set-up times, only records for calls that exceed the SMDR Timer (OFF, refer to Start Timer Attribute).	ON OFF	OFF
Print Enable	The system can output SMDR records automatically as they occur (real-time) or only when requested. When this attribute is ON, SMDR output is automatic at call completion.	ON OFF	ON
Record Type	The system can record all outgoing calls or only long distance calls. Long distance calls are identified by the LD digit count and LD codes assigned in “Long Distance Call Digit Counter” and “Long Distance Code” below.	Long Distance All call	All Call
Long Distance Call Digit Counter	Dialed numbers, which exceed the assigned LD digit count are considered long distance calls for SMDR and COS purposes.	07-15	08
Print Incoming Call	The system can output records for Incoming calls as well as outgoing calls. If enabled, incoming as well as outgoing calls are recorded.	ON OFF	OFF
Print Lost Call	When incoming call records are enabled, the system can also provide records for unanswered incoming (abandoned) calls.	ON OFF	ON
Records In Detail	The system can output detailed call records (ON) or summary call information (total number of calls, cost and cost for each station).	ON OFF	ON
Hidden Dialed Digit	For security purposes, digits dialed for an outgoing call can be hidden and replaced with “*”. This field defines the number of digits to hide the trailing digits	3~9	3
SMDR Currency Unit	The unit of currency used for call cost can be identified with 3-characters for easy reference.	Max 3 Characters	EUR
SMDR Cost Per Metering Pulse	When call metering is provided by the PSTN, the cost per metering pulse can be assigned.	6-digits	000000

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
SMDR Decimal Position	This value determines the position of the decimal in the Cost per Pulse entry above, starting from the right most digit.	0~5	2
Record Start Guaranteed Time	To allow for call set-up times through the PSTN, a “Valid call timer” can be set.	000~250 (msec)	000
Long Distance Code	For SMDR and COS purposes, five (5) Long Distance codes of up to two (2) digits each can be assigned. If dialed as the 1st digits, the call is considered an LD call.	5 two digit LD codes, use * as wild card (any digit)	
SMDR CLI or Ring Service I	For incoming calls, the system will send the defined data item for “Field I”. The data item may be CLI, CPN or Ring Service Time. Note the User dialed number is always provided for an outgoing call.	RING CLI CPN	RING
SMDR Ring/CLI/CPN Service II	For incoming calls, the system will send the defined data item for “Field II”. The data item may be CLI, CPN or Ring Service Time.	RING CLI CPN NONE	NONE
Print MSN	Print MSN number Information in SMDR Record	ON OFF	OFF
Print Order No	Print record number as part of SMDR output, will reset to 1 when SMDR capacity is reached or SMDR Mail Auto Delete Set above is enabled.	ON OFF	OFF
LCD Display Priority	Caller ID can be overwritten on Duration or Cost LCD column or not.	Caller ID Duration / Cost	Caller ID
SMDR ICM Save	When enabled, intercom call data is stored as part of the SMDR data.	ON OFF	OFF
SMDR ICM Print	When enabled, intercom call data is printed as part of the On-line SMDR.	ON OFF	OFF
SMDR Disconnect Cause	When enabled, the disconnect cause is stored in Off-line SMDR data and printed as parted of the On-line SMDR.	ON OFF	OFF
SMTP Mail Server Address	SMTP Mail server address to send e-mail SMDR reports.	100 Characters	
SMTP Mail Server ID	This field defines the user’s ID for SMTP Mail server. If user’s ID and password is assigned, SMTP Mail server will check the validation of user ID and password.	Max 40 Characters.	
SMTP Mail Server Password	This field defines the user’s password for SMTP Mail server. If user’s ID and password is assigned, SMTP Mail server will check the validation of user ID and password.	Max 20 Characters.	
SMDR Sender Mail Address	Sender e-mail address to send the SMDR e-mail reports.	40 Characters	-
SMDR Receiver Mail Address	Receiver e-mail address to receive the SMDR e-mail reports.	40 Characters	

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
SMDR Mail Send Weekly Set	Sets day of week to send SMDR data weekly (0 for no weekly data, 1-7 for Monday through Sunday).	N/A day	N/A
SMDR Mail Send Daily Set	Sets time-of-day for SMDR data sent on a daily basis (00 for no daily records, 01-23 for hour of the day).	00~23	00
SMDR Mail Auto Send Set	If the SMDR buffer is full, the system will automatically send a notification e-mail.	ON OFF	OFF
SMDR Mail Auto Delete Set	Delete SMDR records after sending e-mail.	ON OFF	OFF

3.2.3.7 International Call

International call can be restricted by prefix matching. International call prefix, all international call restriction and CO-CO international call restriction can be programmed in this admin. The following Table describes International Call:

Table 3.2.3.7 International Call

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
International Prefix	International prefix is used for classification of international call.	Max 2 digits	00
All International call	All outgoing international call can be restricted by this attribute.	Enable Disable	Enable
CO-CO International call	Transfer or forward to International call can be restricted by this attribute.	Enable Disable	Disable

3.2.3.8 Alarm Attribute

Alarm can be set by this attribute.

Table 3.2.3.8 Alarm Attribute

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Alarm Enable	Alarm Enable	ON/OFF	ON
Alarm Contact Type		Close/Open	Close
Alarm Mode	You can choice Alarm or Door Bell.	Alarm/Door Bell	Alarm
Alarm Signal Mode	How many times repeat?	Repeat/Once	Repeat

3.2.4 Station Group Data

Stations can be grouped so that incoming calls will search (hunt) for an idle station in the group. The iPECS SBG-1000 System supports 7 different hunt processes: Circular, Terminal, Ring, Pick-Up, VSF-Voice Mail, IPCR, Networking Voice Mail.

The Station Group capacities for the iPECS SBG-1000 systems are shown in the Table:

Table 3.2.4 Station Group Data

ITEM	CAPACITY
Number of Groups	12
Stations in a Group	24

Certain types of groups can incorporate announcements, which are given to the calling party. The system's VSF can store up to 70 announcements for use with Station Groups.

📖 ***NOTE:*** *A station can belong to multiple groups if the groups are of the same type. When a Station Group is assigned to a group type, the group attributes revert to the default values.*

3.2.4.1 Station Group Assignment

Under Station Group Assignments the type, members and Pick-Up attributes are assigned.

Table 3.2.4.1 Station Group Assignment

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Group Type	Defines the type of station group.	N/A Circular Terminal Ring Pick-Up VSF-VM IPCR NET-VM	N/A
Pick-up Attribute	Stations can pick-up group calls ringing at other stations in the group. This does not apply to VSF groups.	OFF ON	OFF
Member	Assign stations as members of a station group.		-

3.2.4.2 Station Group Attributes

Each type of group has a different set of available attributes relating to announcements, timers, overflow, etc. The following Tables provide descriptions for the attributes and data entries required.

Table 3.2.4.2-1 Terminal & Circular Group Attributes

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
VSF Announce 1 Timer	If all stations in the group are busy when a call is received, the call may continue to wait (queue) for an available station. If the queue period exceeds the VSF Announce 1 timer, the call is sent to a VSF announcement. If the timer is set to 000, the call will receive the first announcement, in full, prior to the hunt process (guaranteed announcement).	000~999 (seconds)	015
Guar-Annc(Timer 0) Wait If Busy	When a call assigned to receive a guaranteed announcement arrives and all channels are busy, the call may wait with Ringback until a channel is available (ON) or bypass the announcement (OFF).	OFF ON	ON

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
VSF Announce 2 Timer	After the 1st announcement, the 2nd ANNC TMR is activated. At expiration, if the call remains queued to the group, the call is sent to the assigned 2nd VSF announcement.	000~999 (seconds)	000
VSF Announce 1 Location	The Station Group can be assigned an announcement, which is played if the call remains queued beyond the VSF Announce 1 Timer duration. The announcement location is the VSF Announcement number.	00~70	00: none
VSF Announce 1 Auto Drop	If this attribute is selected, the call will drop after the 1st VSF announcement	Check box	
VSF Announce 2 Location	The Station Hunt Group can be assigned a 2nd announcement, which is played if the call remains queued beyond the VSF Announce 2 Timer duration. The announcement location is the VSF Announcement number.	00~70	00: none
VSF Announce 2 Auto Drop	If this attribute is selected, the call will drop after the 2nd VSF announcement	Check box	
VSF Announce 2 Repeat Timer	The 2nd announcement can be repeated to callers that remain in queue at intervals of the announcement 2 repeat timer. Note: VSF Announce 2 Repeat (below) must be “ON”.	000~999 (seconds)	000
VSF Announce 2 Repeat	After the 2nd announcement, if the call remains queued to the group, the 2nd VSF announcement can be repeated at the Announce 2 Repeat Timer interval, defined above.	ON OFF	OFF
Overflow Destination	A call to the group will continue to route through the group until answered or all group members have been tried. The call will remain at the last station or routed to the assigned overflow destination. If VSF Announcement is selected, Auto Drop can be checked.	STA or Hunt Number, VSF Announce, System SPD	
Overflow Timer	A call to the group will remain at the last station in the group or can be sent to the assigned Overflow Destination after expiration of the Overflow Timer.	000~600 (seconds)	180
Warp-Up Timer	After terminating any call, a Group member will be maintained in a busy state for the duration of the Wrap-Up timer.	000~999 (seconds)	002
No Answer Timer	Calls to a station in the group are directed to the station, if unavailable or unanswered in the No Answer Timer, the call can be routed based on the assigned hunt process.	00~99 (seconds)	15
Pilot Hunt	A circular/terminal hunt group can be set so that only calls to the pilot number (station group number) will hunt.	ON OFF	ON
REPT No Member	If a call is received and no members are on-duty, an ICM call will return re-order tone, while a CO call will be routed to the Attendant.	ON OFF	OFF
Music Source	A Music source can be assigned so that calls to the group will receive audio from the assigned source in place of ring-back tone.	Ring-Back Tone Record Play	Ring-Back Tone
Allow Forward Member	A member activating Call forward, may be placed in an unavailable state for hunt group calls (ON). When OFF, group calls are sent to the member as normal.	ON OFF	ON

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
VSF Wait Station	When a call overflows or routes to the VM group, a station number is used to identify the Mailbox for the group messages.	Station Number	
Mail Box Password	The password associated with a group Mailbox is defined here. The password is used in conjunction with the group as with a normal station.	Max 12 digits	
Forced Forward Destination	Calls to a hunt group may forward calls directly to a defined destination.	STA or Hunt grp. VSF Annc SysSpeed	
Forced Forward Dest Usage	Calls to a hunt group may forward calls directly to a defined destination. Forced Forward must be enabled for the group.	OFF ON	OFF
Group Name	An group name can be designated	12 character	
Max Queued Call Counter	When the number of calls queued to the group match this parameter, new calls will receive error tone and be disconnected after the VSF Announcement 1, if assigned, is played.	00-99	99

Table 3.2.4.2-2 Ring Group Attributes

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
VSF Announce 1 Timer	If all stations in the group are busy when a call is received, the call may continue to wait (queue) for an available station. If the queue period exceeds the VSF Announce 1 Timer, the call is sent to a VSF announcement. If the timer is set to 000, the call will receive the first announcement, in full, prior to the hunt process (guaranteed announcement).	000~999 (seconds)	015
Guar-Annc(Timer 0) Wait If Busy	When a call assigned to receive a guaranteed announcement arrives and all channels are busy, the call may wait with Ringback until a channel is available (ON) or bypass the announcement (OFF).	OFF ON	ON
VSF Announce 2 Timer	After the 1st announcement, a 2nd announcement Timer is activated. At expiration, if the call remains queued to the group, the call is sent to the assigned 2nd VSF announcement.	000~999 (seconds)	000
VSF Announce 1 Location	Each Ring Group can be assigned an announcement, which is played if the call remains queued beyond the VSF Announce 1 Timer duration. The announcement location is a VSF Announcement number. An entry of 00 indicates no announcement.	00~20	00: none
VSF Announce 1 Auto Drop	If this attribute is selected, the call will drop after the 1st VSF announcement	Check box	
VSF Announce 2 Location	The Ring Group can be assigned a 2nd announcement, which is played if the call remains queued beyond the VSF Announce 2 Timer duration. The announcement location is a VSF Announcement number. An entry of 00 indicates no announcement.	00~-20	00: none
VSF announce Auto Drop	If this attribute is selected, the call will drop after the 2nd VSF announcement	Check box	

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
VSF Announce 2 Repeat Timer	The 2nd announcement can be repeated to calls that remain in queue at intervals of the VSF Announce 2 Repeat Timer. Note: VSF Announce 2 Repeat below must be “ON”.	000~999 (seconds)	000
VSF Announce 2 Repeat	After the 2nd announcement, if the call remains queued to the group, the 2nd VSF announcement can be repeated at the VSF Announce 2 Repeat Timer interval, defined above.	ON OFF	OFF
Overflow Destination	A call to the group will continue to route through the group until answered or all group members have been tried. The call will remain at the last station or routes to the assigned Overflow Destination. If VSF Announce is assigned, Auto Drop is available.	Station or Group Number, VSF Announce, System SPD	
Overflow Timer	A call to a group will remain at the last station in the group or route to the assigned Overflow Destination after expiration of the Overflow Timer.	000~600 (seconds)	180
Warp-Up Timer	After terminating any call, a Hunt Group member will be maintained in a busy state for the duration of the Wrap-Up Timer.	002~999 (seconds)	002
Music Source	A Music source can be assigned so that calls to the group will receive audio from the assigned source in place of ring-back tone.	Ring-Back Tone Record Play	Ring-Back Tone
Maximum Queued Call Counter	When the number of calls queued to the group match this parameter, new calls will receive an error tone and be disconnected after the VSF AA announcement is played (if assigned).	00-99	99
Allow Forward Member	When a member is forwarded to another station, if this option set OFF, the member receives a incoming hunt call.	OFF : no FWD ON : FWD	ON
Group Name	An group name can be designated	12 character	
VSF Wait Station	When an ring group call overflows or routes to the VM group, a station number is used to identify the Mailbox for the ring group messages.	Station	
Mail Box Password	The password associated with an ring group Mailbox is defined here. The password is used in conjunction with the ring group as with a normal station.	12 digits	
Forced Forward Destination	Calls to a hunt group may forward calls directly to a defined destination.	STA or Hunt grp. VSF Annc SysSpeed	
Forced Forward Dest Usage	Calls to a hunt group may forward calls directly to a defined destination. Forced Forward must be enabled for the group.	OFF ON	OFF

Table 3.2.4.2-3 PICK-UP GROUP ATTRIBUTES

ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Auto Pick Up	If a group member Station is ringing, another member of the Group can Pick-Up the ringing call from their station by simply going Off-hook.	ON OFF	OFF
All Ring	When a call is received to a member of the Pick-Up Group in the Tone Ring mode, all members will ring. Note: Auto Pickup must be set to ON.	ON OFF	OFF

Table 3.2.4.2-4 VSF GROUP ATTRIBUTES

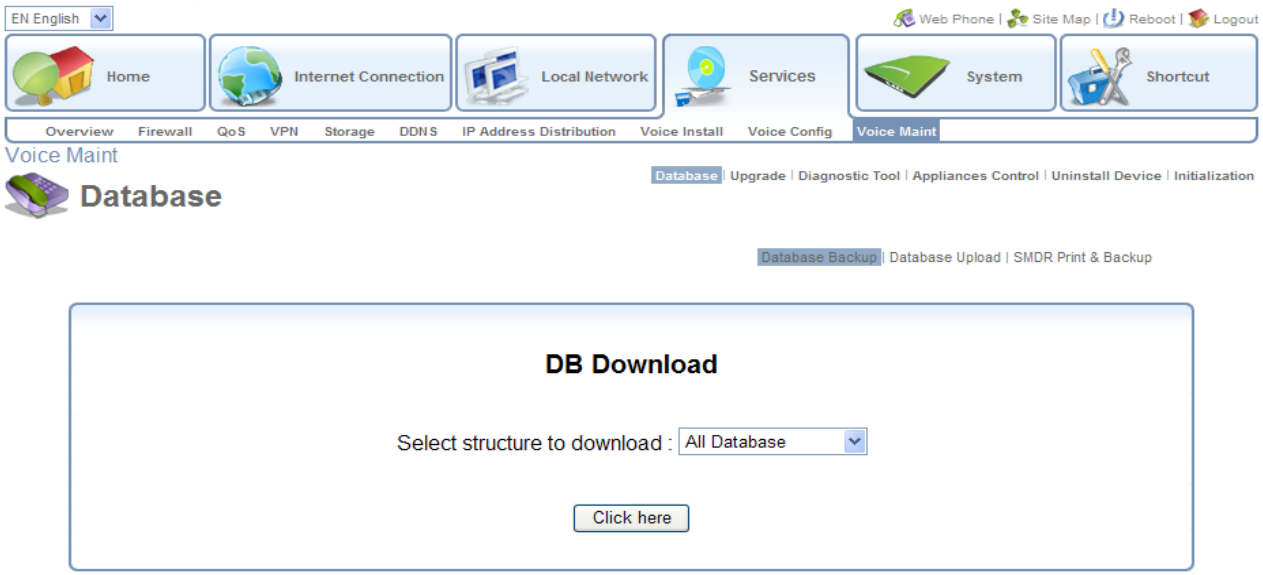
ATTRIBUTE	DESCRIPTION	RANGE	DEFAULT
Time Set (day) *For future use only*	When voice messages are stored in the VSF, the system will maintain (store) the message for the maximum number of days set in this program (1 to 365 days). (Not used currently)	00-99 (day)	0
Time Out (sec): *For future use only*	This timer determines the inter-digit time for a VSF-AA or a VM session. If this timer expires while the VSF AA or VM is awaiting user input, the system will assume the remote party has disconnected and will return the channel to idle. (Not used currently)	00-15 (seconds)	15
Group Name	An group name can be designated	12 character	

3.2.4.3 IPCR Agent

This table used for matching agent ID to station number. If it's done, the station with agent ID is automatically recorded about internal, external call.

3.3 VOICE MAINTENANCE

Selecting Maintenance from the Main menu will display the Maintenance page (shown).



The Maintenance Main menu item permits download of all or portions of the system's database, and downloading and viewing of SMDR data. The user also can set trace direction or target and system logs. Other functions include uninstall registered station, delete voice mail box for each station, and initialize call attributes.

iPECS SBG-1000 User Manual
(DATA Features)

Revision History

ISSUE	DATE	DESCRIPTION OF CHANGES
1.0	2011. August	Initial Release

Table of Contents

1. Accessing the Management Console

This chapter describes how to use iPECS SBG-1000's management console, referred to as the **Web-based Management (WBM)**, which allows you to configure and control all of iPECS SBG-1000's features and system parameters, using a user-friendly graphical interface. This user-friendly approach is also implemented in the WBM's documentation structure, which is based directly on the WBM's structure. You will find it easy to correspondingly navigate through both the WBM and its documentation.

Note: Access to the WBM is restricted to wired clients and Web-authenticated or secured wireless clients. In addition, some of the documented WBM features may appear slightly different or may not be available on certain platforms.

To access the Web-based management:

1. Launch a Web browser on a computer in the LAN.
2. In the address bar, type the gateway's name or IP address. The default name is'http://sbg-1000.home' and the default IP address is 192.168.1.1. The WBM's homepage appears.

1.1 WBM Modes

By default, iPECS SBG-1000's WBM is displayed in read-only basic mode, providing you with the ability to view your features and system parameters. This mode prevents accessing and changing the gateway's settings, misconfiguration of which may harm its performance.

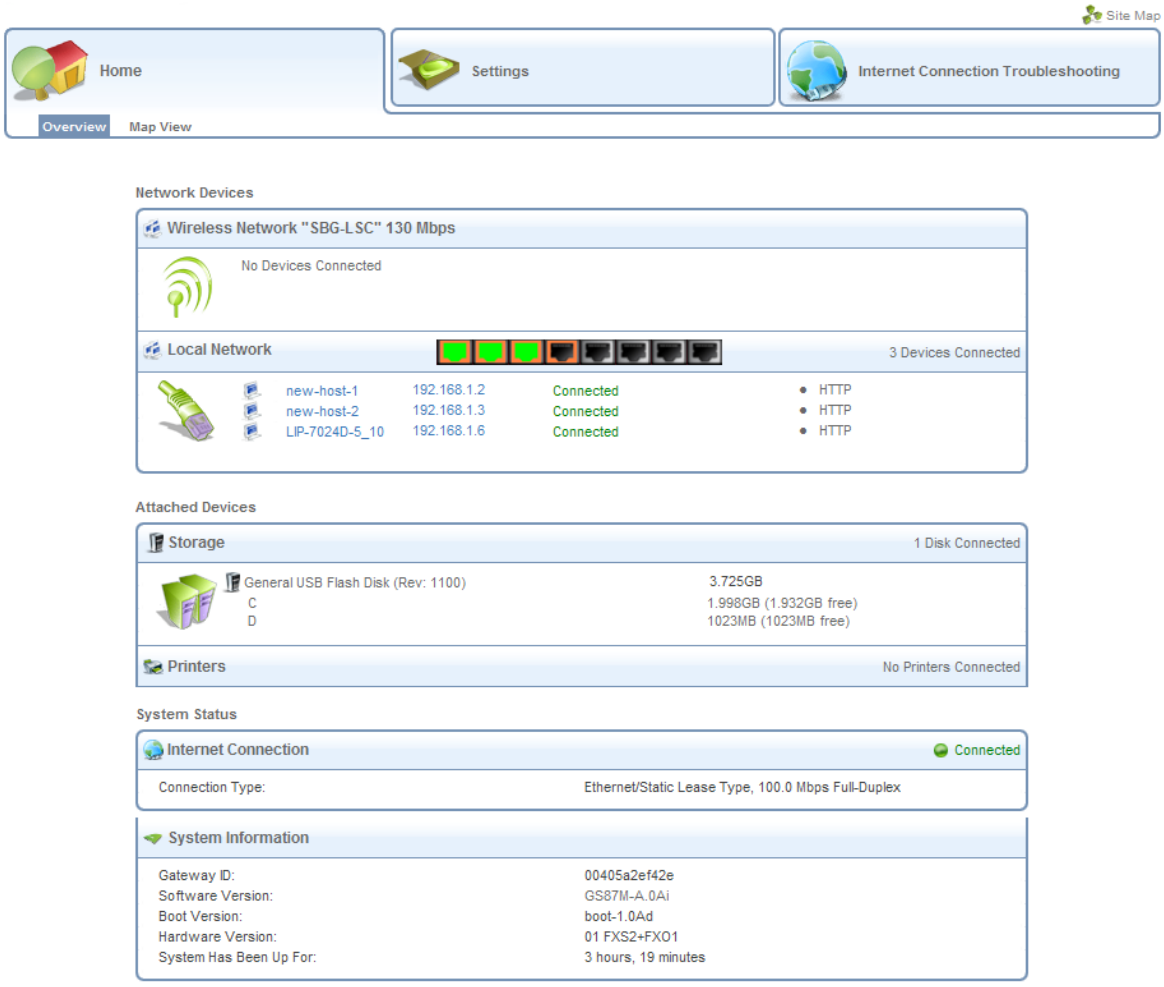


Figure 1.1 WBM – Read Only Basic Mode

To perform configuration actions on your gateway, click the ‘Settings’ tab. You are required to log in.

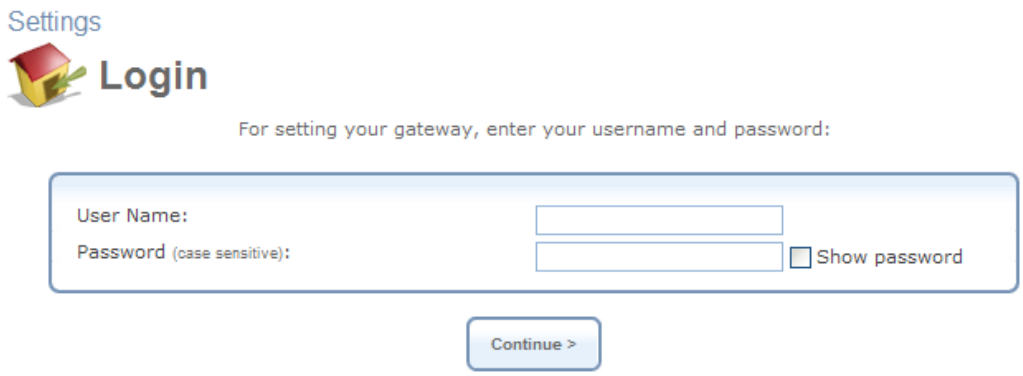


Figure 1.2 Settings Login

Enter your username and password, and click ‘Continue’. The default username is ‘admin’ and the default password is ‘admin’.

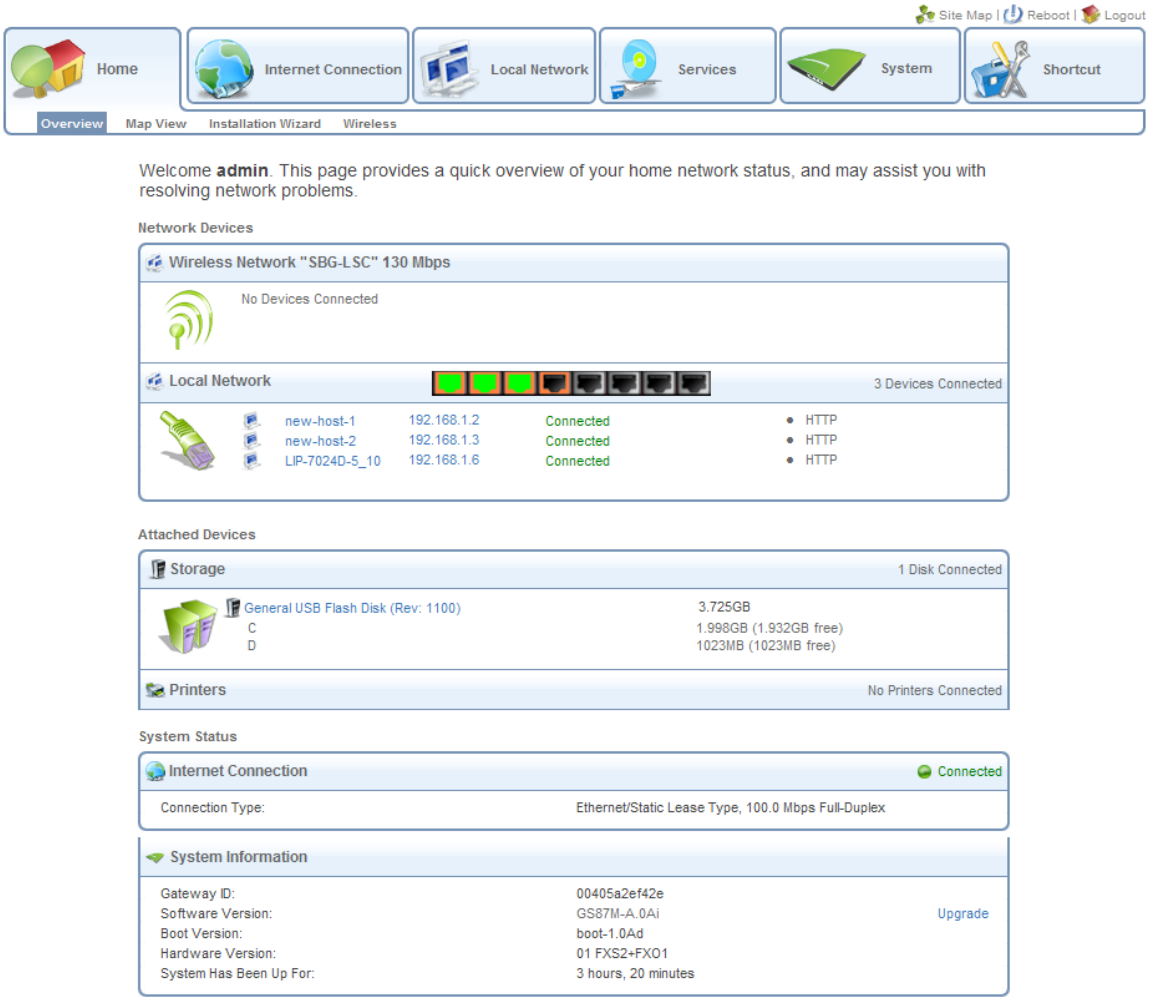


Figure 1.3 WBM – Configuration Mode

By logging in, you have switched from read-only mode to configuration mode. You can now perform various configurations of your gateway, as described in the following sections. To return to read-only mode, click the 'Logout' link located on the top bar.

Note: Prior to changing default settings of any iPECS SBG-1000 feature, it is recommended that you carefully read the relevant instructions provided in this manual.

A login session will automatically time-out after an extended period of inactivity. If you try to operate the WBM after the session has expired, the 'Login' screen will appear. This feature helps to prevent unauthorized users from accessing your session and changing the gateway's settings.

1.2 Navigational Aids

The Web-based management is a user-friendly interface, designed as a Web site that can be explored with any Web browser. This section illustrates the WBM's page structure and describes its navigational components and their hierarchical manner.

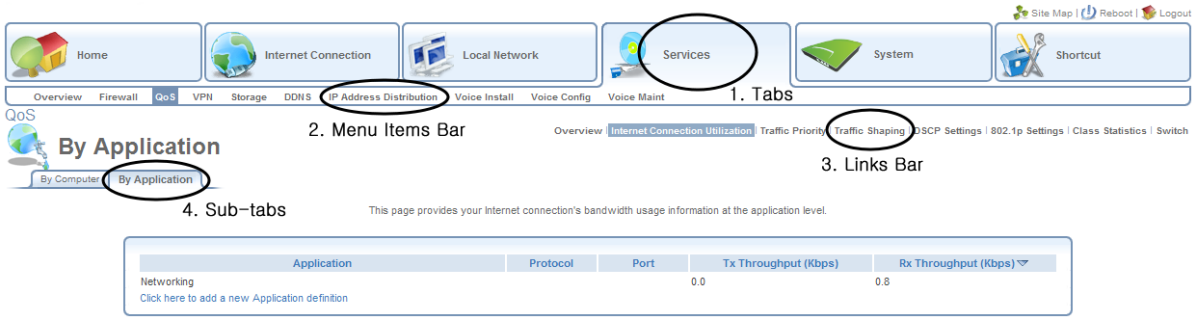


Figure 1.4 Navigation Components

1. The top level navigational aids are the Tabs, grouping the WBM screens into several main subject areas.

Note: The following navigational components are only present in the advanced mode of the WBM.

2. A tab may have a Menu Items bar, listing the different items relevant for the tab.

3. A menu item may have a Links Bar, located at the top-right of the screen. These links further divide the menu item into different subjects.

4. Lastly, a page content, usually a feature's properties page, may have a set of Sub-tabs, providing a division of settings in the form of yet another set of tabs.

Note: For convenience purposes, the entire WBM part of this User Manual has been constructed in accordance with the structure of the WBM—the chapter structure is identical to the tab structure, sections are written after item menus, etc.

In addition, a constant links bar appears at the top of every WBM page, providing shortcuts to information and control actions.

Figure 1.5 Constant Link Bar

The links bar includes:

- **Site Map** – Leads to a screen representing the hierarchial structure of the WBM.
- **Reboot** – Clicking this link initiates a gateway reboot.
- **Logout** – This link can be used to return to read-only basic mode.

1.3 Tables in the WBM

Tables are structures used throughout the Web-based management. They handle user-defined entries relating to elements such as network connections, local servers, restrictions and configurable parameters. The principles outlined in this section apply to all tables in the WBM.

Figure 1.6 Typical Table Structure

Figure 1.6 illustrates a typical table. Each row defines an entry in the table. The following buttons, located in the 'Action' column, enable performing various actions on the table entries.

Use the **Add** action icon to add a row to the table.

Use the **Edit** action icon to edit a row in the table.

Use the **Remove** action icon to remove a row from the table.

Use the **Download** action icon to download a file from the table.

Use the **Copy** action icon to copy an item to the clipboard.

Use the **Move Up** action icon to move a row one step up in the table.

Use the **Move Down** action icon to move a row one step down in the table.

2. Home

2.1 Overview Your Gateway

The ‘Overview’ screen presents the status of iPECS SBG-1000’s various modules in one convenient location. You can quickly and efficiently view important system details such as the status of your Internet connection, wireless and local networks, as well as hardware peripherals.

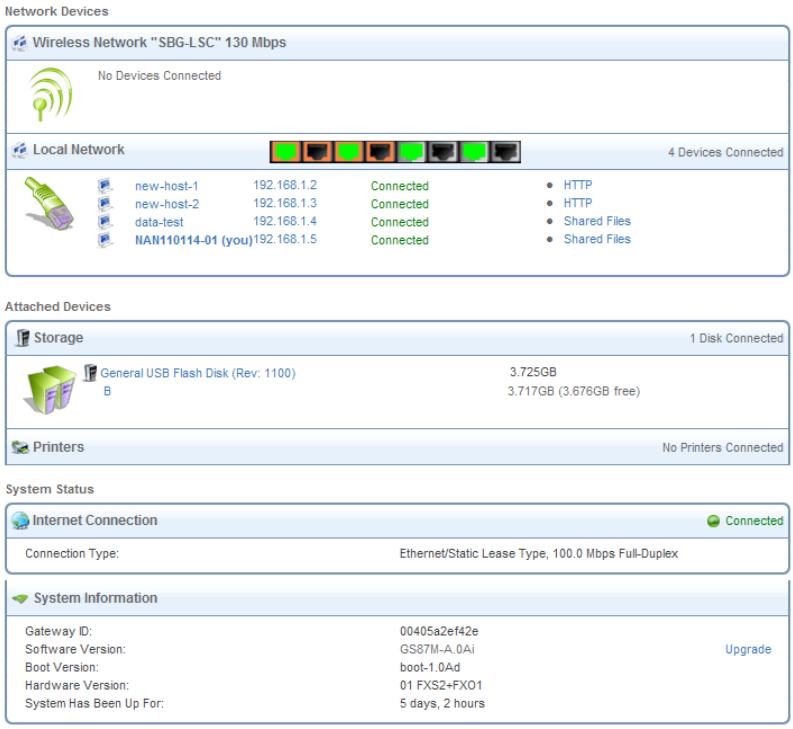


Figure 2.1 Home – Overview

2.1.1 Viewing and Connecting to Your Broadcasted Wireless Network

The ‘Network Devices’ section displays iPECS SBG-1000’s broadcasted wireless network. To connect to this network from a wireless Windows computer, perform the following:

1. In the Windows system tray, click the wireless connection icon.

Figure 2.2 Wireless Icon in the System Tray

The ‘Wireless Network Connection’ screen appears, displaying all available wireless networks (also known as Wi-Fi hotspots) in your vicinity. If your gateway is connected and active, you should see its wireless network displayed in this screen. The default wireless

network name (SSID) is “iPECS SBG-1000 (XXXX)”, where XXXX are the last four characters of the gateway’s MAC address (as printed on the sticker located at the bottom of the gateway).

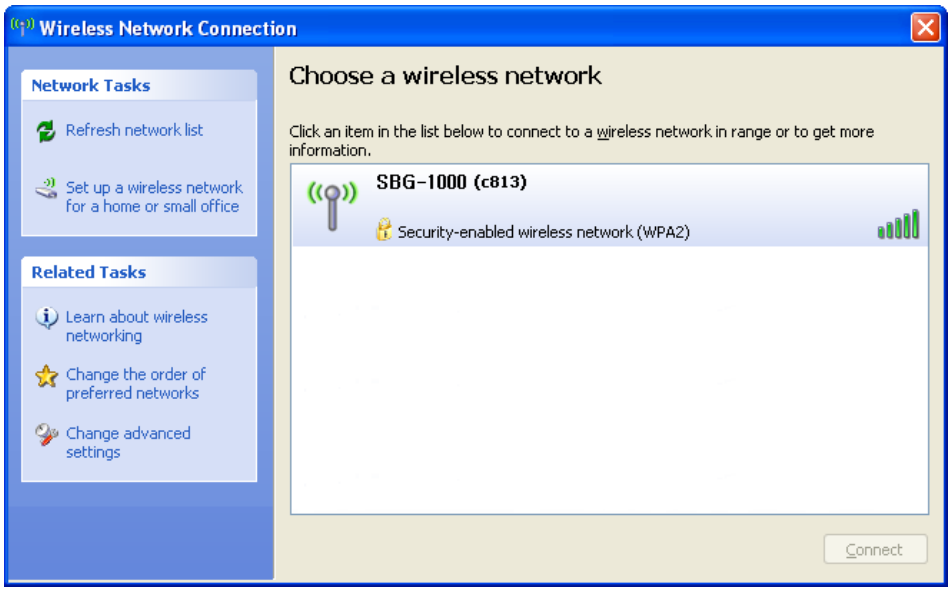


Figure 2.3 Available Wireless Connections

If you do not see your network, refresh the list of detected networks using the ‘Refresh network list’ link.

2. Select the connection and click the ‘Connect’ button at the bottom of the screen. The following window appears, requiring you to provide the WPA password (network key).

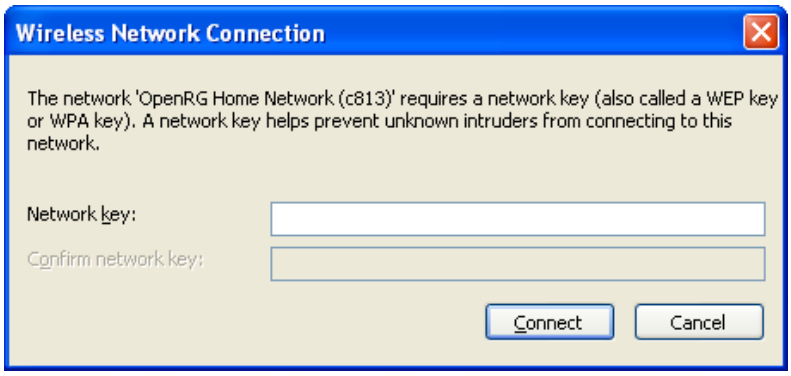


Figure 2.4 WPA Network Key Authentication

Enter the WPA password. This case sensitive password can be found on the sticker located at the bottom of the gateway, and can be changed in the ‘Wireless’ menu item under the ‘Home’ tab. After the connection is established, its status changes to ‘Connected’.

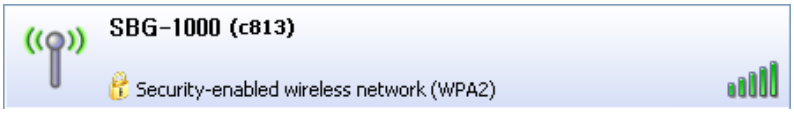


Figure 2.5 Connected Wireless Network

A balloon appears in the notification area, announcing the successful initiation of the wireless connection.

Figure 2.6 Wireless Connection Information

3. If you had selected the default “Medium” security level during the installation wizard, any attempt to browse the Internet will require Web authentication. The following screen appears, requiring you to provide your username and password.

Figure 2.7 Web Authentication

Enter your username and password. You will be redirected to your requested Internet address.

4. Open an Internet browser and browse to any site.

The ‘Home’ screen will now display the connected wireless computer.

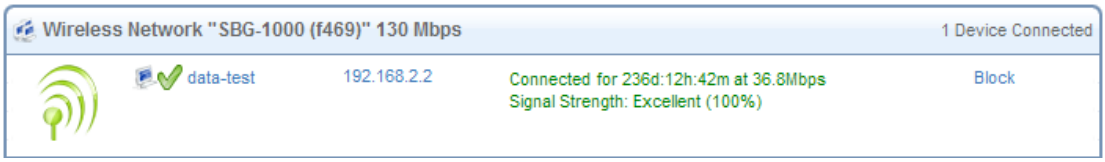


Figure 2.8 Connected Wireless Computer

2.1.2 Authenticating Wireless Network Devices

When attempting to connect to the gateway’s network from a wireless computer, a login session is used for authentication and connection. However, you may wish connect other wireless devices to the gateway, such as gaming devices, cameras, etc., in which a login session in is not possible due to the lack of an interface. In such a case, a simple authentication procedure is required in the ‘Home’ screen.

A preliminary step is to search for the gateway's wireless network from the device itself. Refer to the device's documentation to learn how to perform this search. When iPECS SBG-1000 detects a wireless request, the device is displayed under the relevant wireless connection.

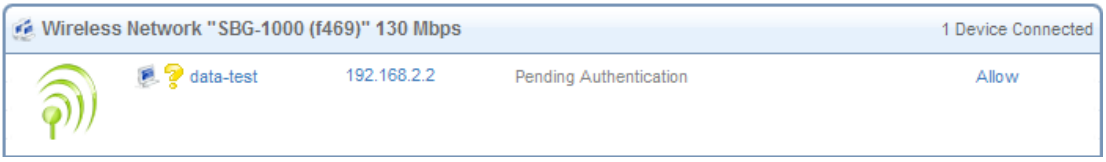


Figure 2.9 Wireless Authentication – Pending

To allow this device to connect to your gateway, click 'Allow'. The screen refreshes, updating the status of the device.

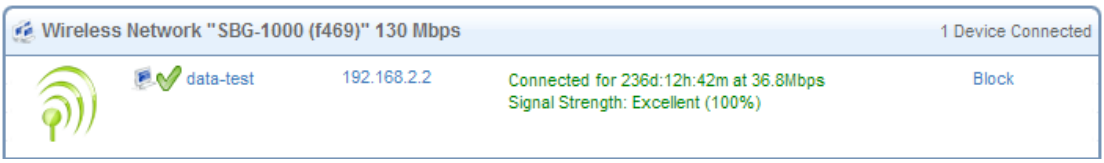


Figure 2.10 Wireless Authentication – Authenticated

The device is now connected. Similarly, you can use the 'Block' link in order to log the device out of your network.

2.1.3 Viewing the Local Network

The 'Network Devices' section also displays iPECS SBG-1000's local network, which includes all computers that have joined the gateway's network, their IP addresses, and connection speed (see Figure 2.1).

To view more information on a specific computer, click its respective link. The 'Host Information' screen appears.

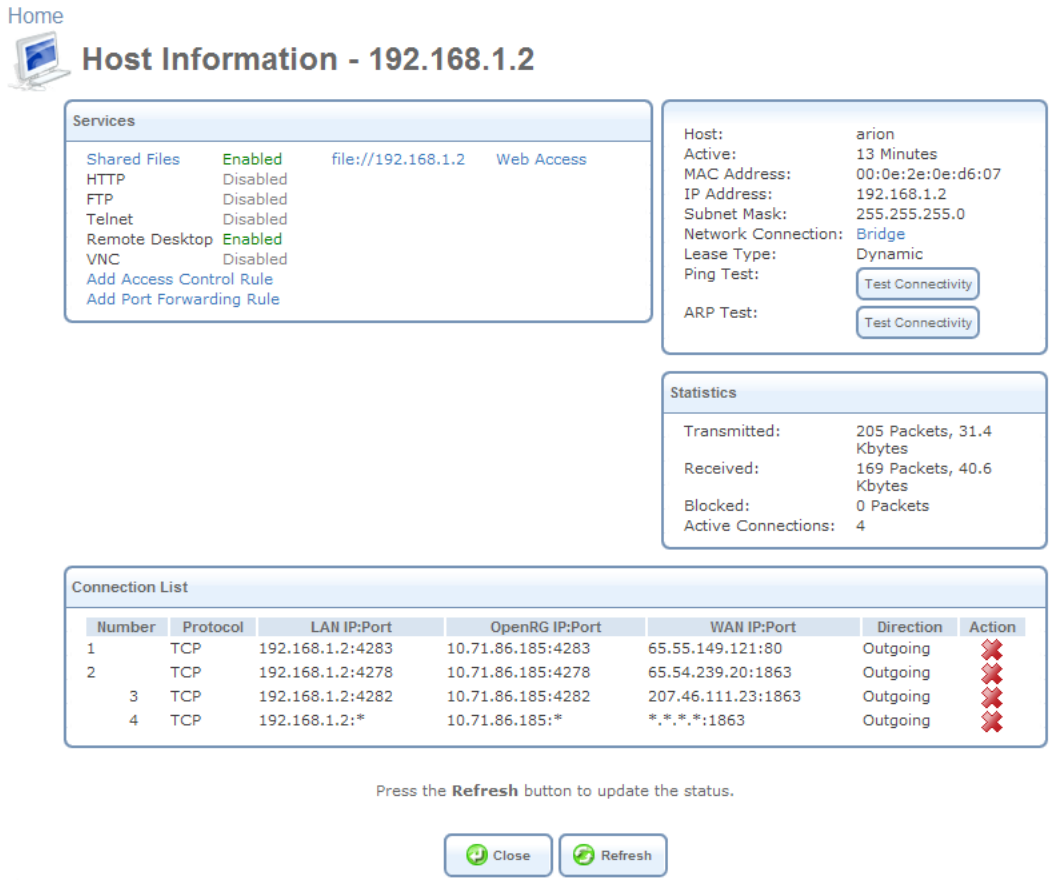


Figure 2.11 Host Information

This screen presents all of the information relevant to the connected computer, such as connection information, available services, and traffic statistics.

Services This section lists the services on the computer that are available to other computers from the LAN. When a service is accessible from the LAN, you can activate it by clicking its name. When a service is accessible via Web access, you can activate it by clicking the 'Web Access' link that appears.

Connection Information This section displays various details regarding the computer's connection settings. In addition, you can run a Ping or ARP test by clicking the respective 'Test Connectivity' button. The tests are performed in the 'Diagnostics' screen (refer to Section 6.8.7).

Statistics This section displays the computer's traffic statistics, such as the number and size of transmitted and received packets.

Connection List This section displays the list of connections opened by the computer on iPECS SBG-1000's firewall. The table displays the computer's source LAN IP address and port, the gateway's IP address and port to which it is translated, and the destination WAN IP address and port.

2.1.4 Viewing Attached Devices

The 'Attached Devices' section displays the peripheral devices connected to your gateway. These may include storage devices and telephones. For example, connect a storage device and refresh the screen.

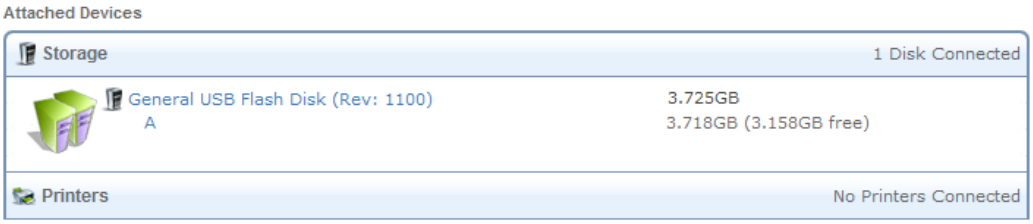


Figure 2.12 Connected Storage Device

To view more details on the connected printer, click its name link. Note that clicking the larger printer icon redirects you to the 'Print Server' screen, which also contains the list of connected printers.
Similarly, this section displays other devices connected to the gateway. For more information on each device type, refer to its respective section of this manual.

2.1.5 Viewing the System Status

The 'System Status' section of the 'Overview' screen (see Figure 2.1) displays the following details:

- The Internet connection's type, speed capability, and data transmission mode. Click the 'Internet Connection' link for more details.
- System information, which includes the gateway's ID, software version and uptime. Click the 'System Information' headline for more details.

2.2 Viewing Your Network with Map View

The 'Map View' screen displays a graphical network map.

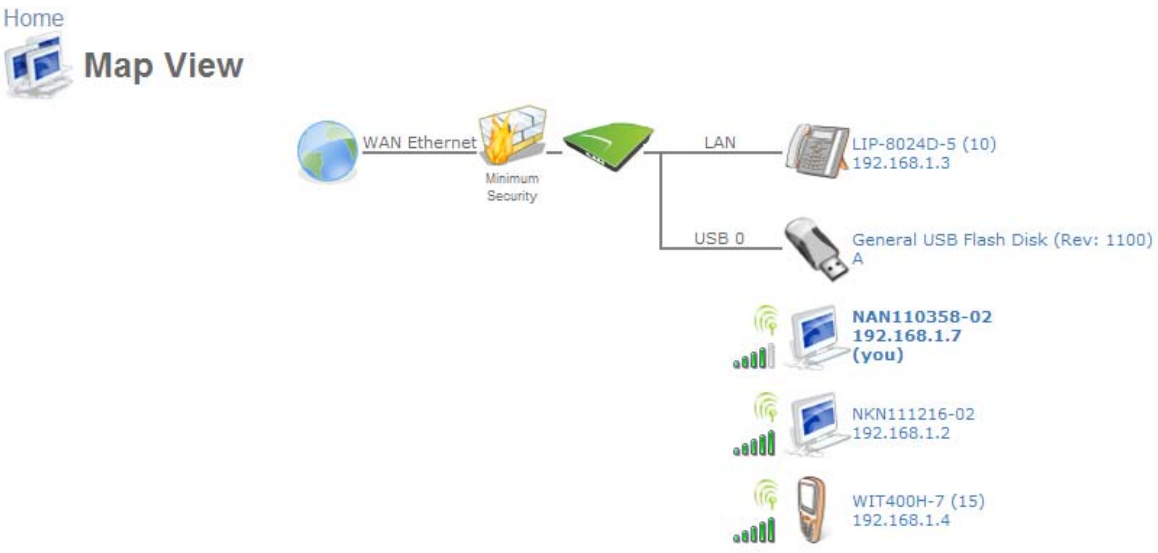


Figure 2.13 Home – Map View

iPECS SBG-1000's standard network map displays devices that the gateway recognized and granted a DHCP lease. The network map depicts the various network elements, such as the Internet connection, firewall, gateway, and local network computers and peripherals.

Represents the Internet

Represents the gateway's Firewall. Click this icon to configure your security settings. For more information, refer to Section 5.2.

Represents your gateway

The network map dynamically represents the network objects connected to your gateway. iPECS SBG-1000 recognizes commercial operating systems and game devices, which are represented by their respective icons.

Represents a wired/wireless computer (host) connected to the gateway. This host is either a DHCP client that has received an IP lease from iPECS SBG-1000, or a host with a static IP address, auto-detected by iPECS SBG-1000. Note that iPECS SBG-1000 will recognize a physically connected host and display it in the Network Map only after network activity from that host has been detected (e.g. trying to browse to the WBM or to surf the Internet). iPECS SBG-1000 will also display incoming connections of types PPTP, L2TP, and IPSec. Click this icon to view network information for the corresponding host.

Represents a host whose DHCP lease has expired and not renewed. The DHCP lease is renewed automatically, unless the host is no longer physically connected to iPECS SBG-1000. The disconnected host's icon will disappear from the network map during the next scheduled IP lease query, performed by iPECS SBG-1000's DHCP server.

Note: This icon also represents a static IP host that has no network activity.

Represents a wireless host connected to your gateway.

Represents a printer connected to your gateway.

Represents an IP-Phone registered to your gateway.

Represents a WiFi Phone registered to your gateway.

Represents a USB storage connected to your gateway.

2.3 Installation Wizard

The installation wizard is the first and foremost configuration procedure, which automatically diagnoses your network environment and configures its components. It is a step-by-step procedure that guides you through establishing an Internet connection, a wireless network, and helps you to subscribe for different services. The wizard progress box, located at the right hand side of the screen, provides a monitoring tool for its steps during the installation progress.

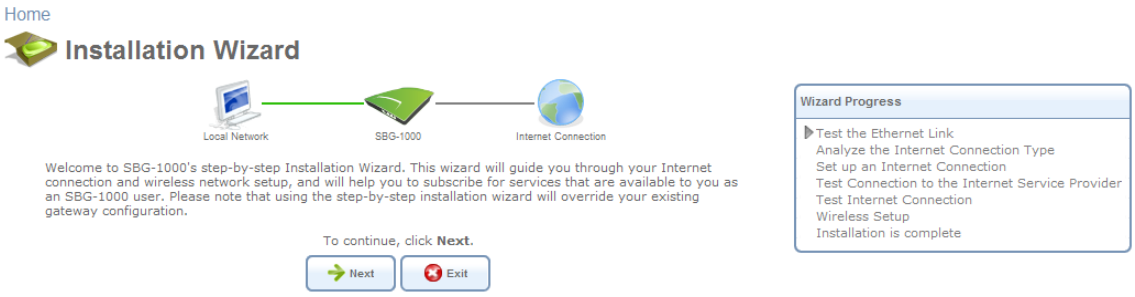


Figure 2.14 Welcome to iPECS SBG-1000 Installation Wizard

1. To start the installation wizard, perform the following:Select the desired language and click ‘Next’ to continue. The ‘Login Setup’ screen appears.

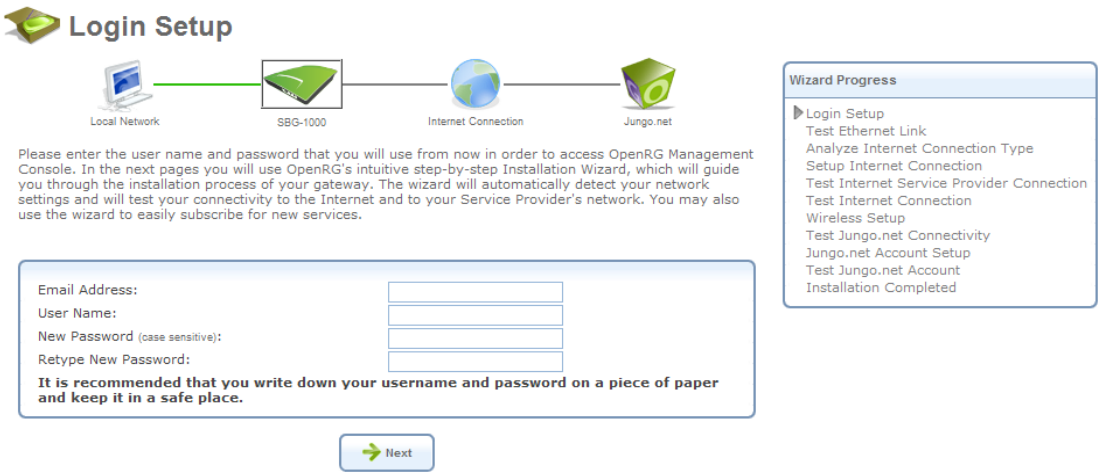


Figure 2.15 Login Setup

2. Enter a valid email address. It will be used by your service provider for sending you important service information.
3. The 'User Name' field is auto-completed by the username part of your email address. You can enter another username, which may only consist of letters and numbers.
4. Enter a password, and retype it in the next field to verify its correctness.

Note: It is recommended to write down your login details on a piece of paper, and store it in a safe place.

5. Click 'Next'. The wizard is now ready to begin your gateway's configuration.

Figure 2.16 Installation Wizard

6. Click 'Next'. The wizard procedure will commence, performing the steps listed in the progress box consecutively, stopping only if a step fails or if input is required. The following sections describe the wizard steps along with their success/failure scenarios. If a step fails, use the 'Retry' or 'Skip' buttons to continue.

Warning: The installation wizard overrides all Internet connection settings, which you may have previously defined.

2.3.1 Step 1: Test Ethernet Link

The first step is a test of the Ethernet connection.

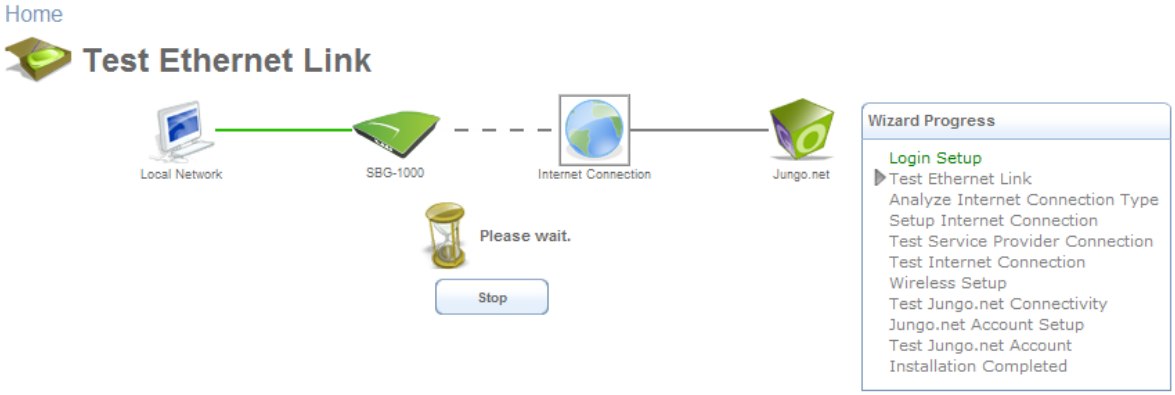


Figure 2.17 Test Ethernet Link

This step may fail if iPECS SBG-1000 cannot detect your Ethernet link (for example, if the cable is unplugged). In this case, the screen changes to the following.

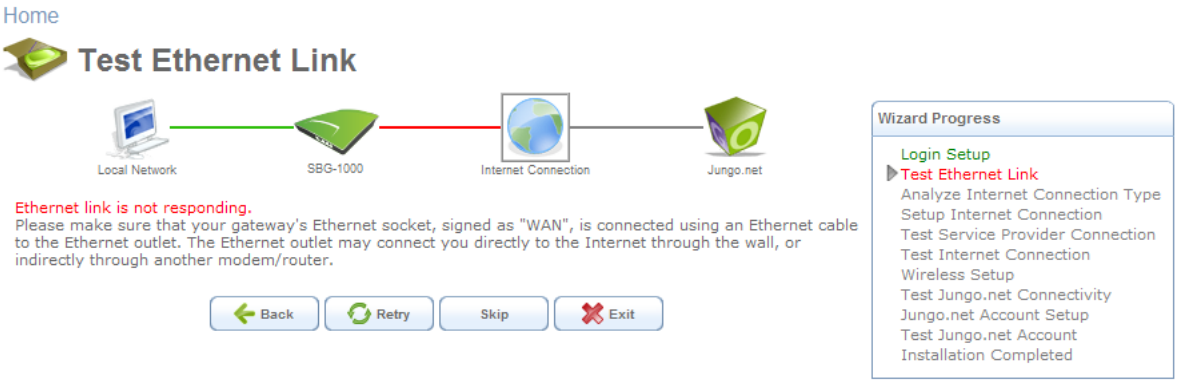


Figure 2.18 Test Ethernet Link – Failure

Verify that your Ethernet/DSL cable is connected properly, and click ‘Retry’.

2.3.2 Step 2: Analyze Internet Connection Type

The next step is an analysis of your Internet connection.

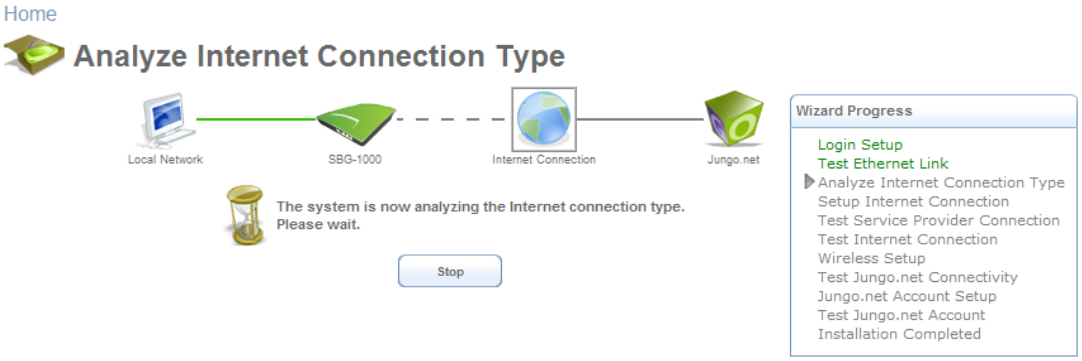


Figure 2.19 Analyze Internet Connection Type

This step may fail if iPECS SBG-1000 is unable to detect your Internet connection type.

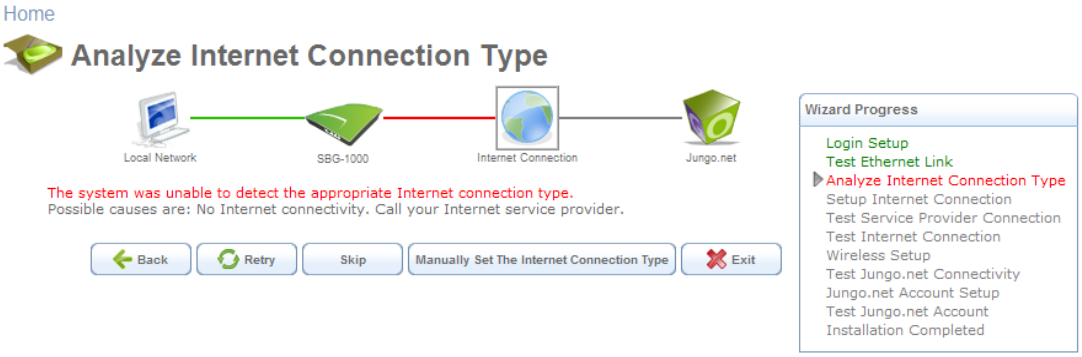


Figure 2.20 Analyze Internet Connection Type – Failure

In this case, you can manually set the Internet connection type, by clicking the corresponding button. The following screen appears.

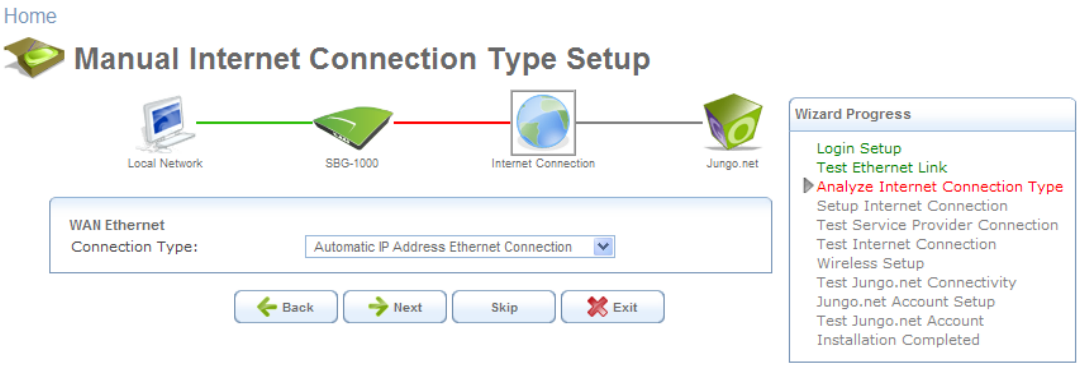


Figure 2.21 Manual Internet Connection Type Setup

To learn about manually configuring your Internet connection, refer to Section 6.4.

2.3.3 Step 3: Setup Internet Connection

If your Internet connection requires login details provided by your Internet Service Provider (ISP) (e.g. when using PPPoE), the following screen appears.

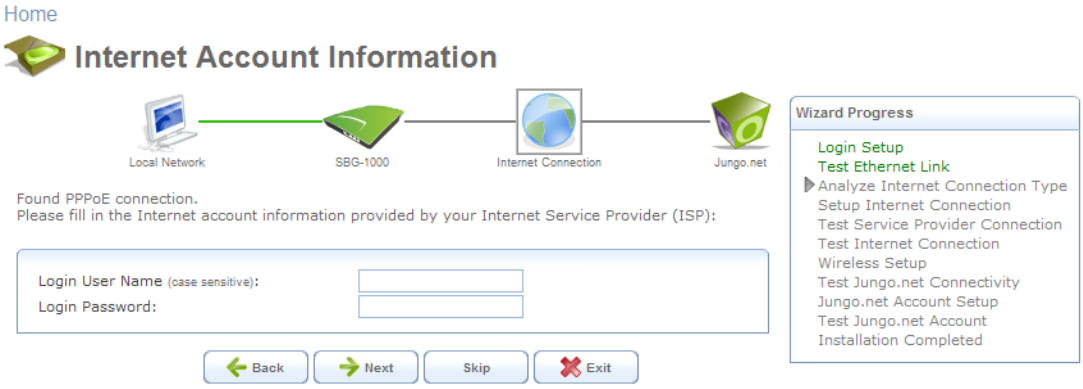


Figure 2.22 Internet Account Information

Enter your user name and password and click ‘Next’. Failure to enter the correct details yields the following message. Click ‘Back’ and try again.

Figure 2.23 Setup Internet Connection

You may have forgotten your login details, issued by your ISP. iPECS SBG-1000 saves the username and password of the PPPoE connection to the ISP, even if it is restored to the factory default settings. When restoring the connection with the installation wizard, iPECS SBG-1000 will offer your old login details.

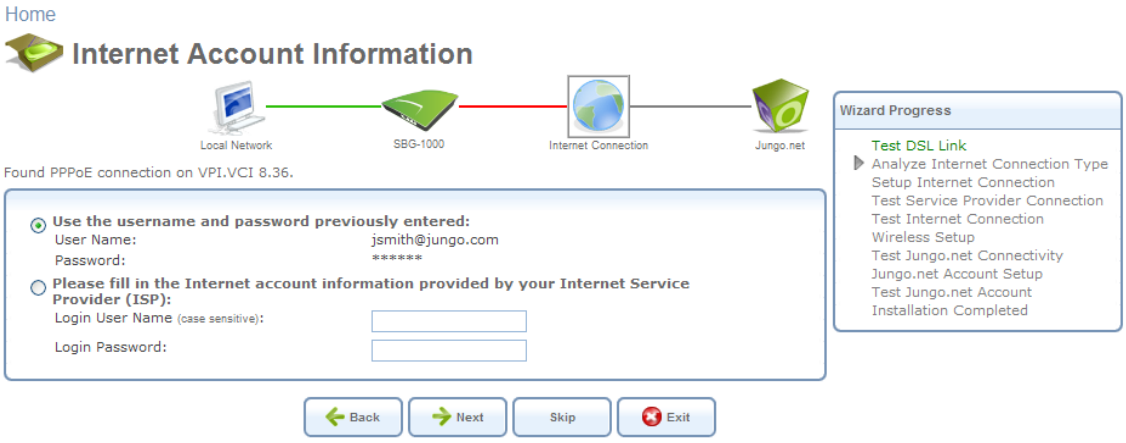


Figure 2.24 Internet Account Information

2.3.4 Step 4: Test Service Provider Connection

This step tests the connectivity to your ISP.

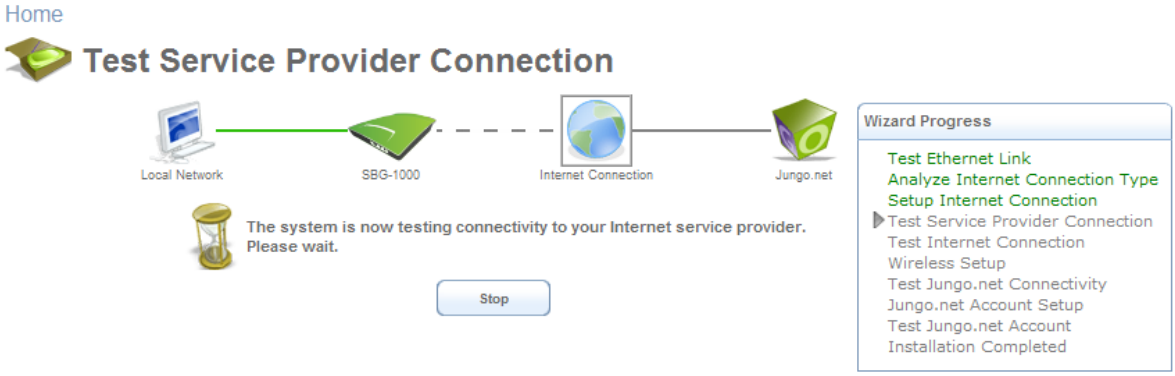


Figure 2.25 Test Service Provider Connection

2.3.5 Step 5: Test Internet Connection

This step tests the connectivity to the Internet.

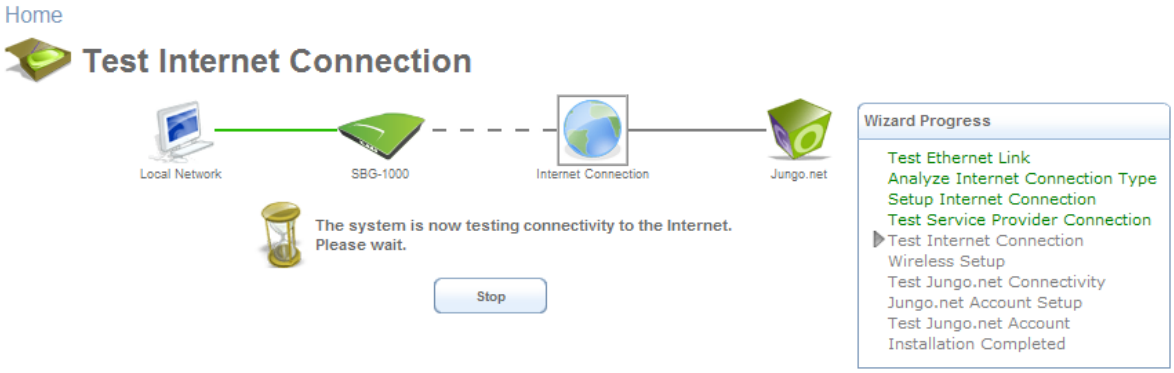


Figure 2.26 Test Internet Connection

2.3.6 Step 6: Wireless Setup

This step enables you to rename your wireless network, as well as change its security level.

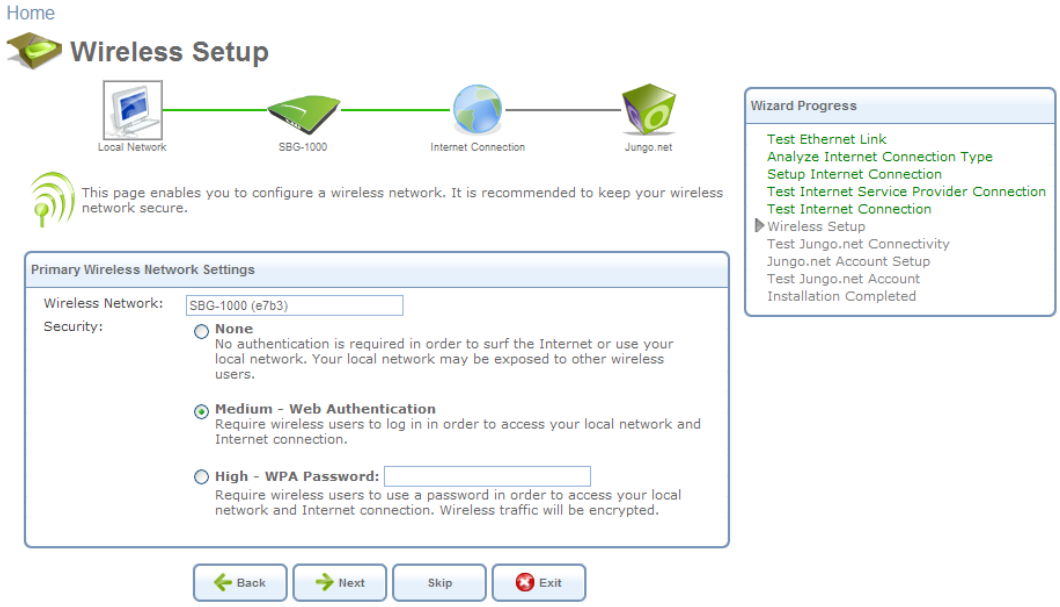


Figure 2.27 Wireless Setup

iPECS SBG-1000 assigns a default name for its wireless network, which you may later change. Select the wireless security level. The default “Medium” level secures your network by requiring users to provide a password in order to connect. “High” level utilizes the Wi-Fi Protected Access (WPA) protocol, requiring a password (network key) as well, but also encrypts the wireless traffic. When selecting this option, enter an eight-character password in the provided field. Click ‘Next’ to continue.

2.3.6.1 Setup via Wireless Connection

If you are running the installation wizard while being connected to iPECS SBG-1000 via a wireless connection, the wizard does not change the default SSID (to prevent you from disconnecting). If you choose to change it manually, the following screen appears, requesting that you re-establish your wireless connection (from your computer) before proceeding with the wizard.

Figure 2.28 Wireless Setup

This screen also appears after selecting the High wireless security level, or after changing the previously entered WPA password (see Figure 2.27).

2.3.6.2 Additional SSIDs with Virtual Access Points

If your gateway supports multiple virtual access points, an additional pre-configured WPA-secured wireless network is displayed in 'Wireless Setup' screen.

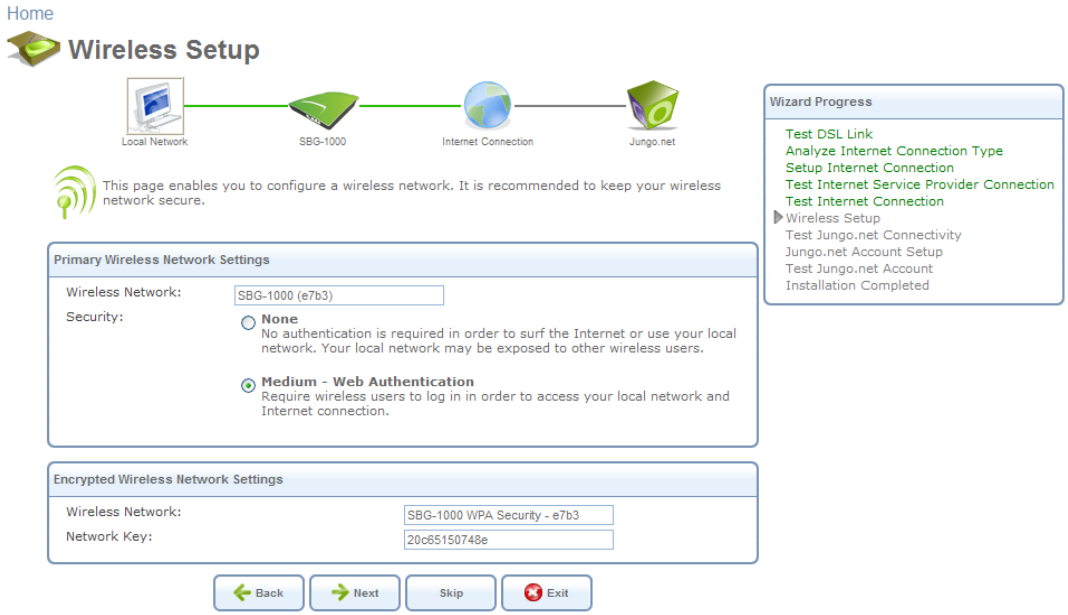


Figure 2.29 Wireless Setup

You can change the default name and network key (password) of this encrypted wireless network in their respective text fields (clicking 'Next' will save the new details). This wireless network will also appear in the 'Network Connections' screen under the 'System' tab, where it can be edited or deleted such as any other network connection.

Figure 2.30 Network Connections

Note: In order to delete this connection, you must first remove it from under the LAN bridge.

2.3.7 Step 7: Installation Completed

This screen provides a summary of all the above Internet connection configuration steps and their results. Click ‘Finish’ to complete the wizard procedure.

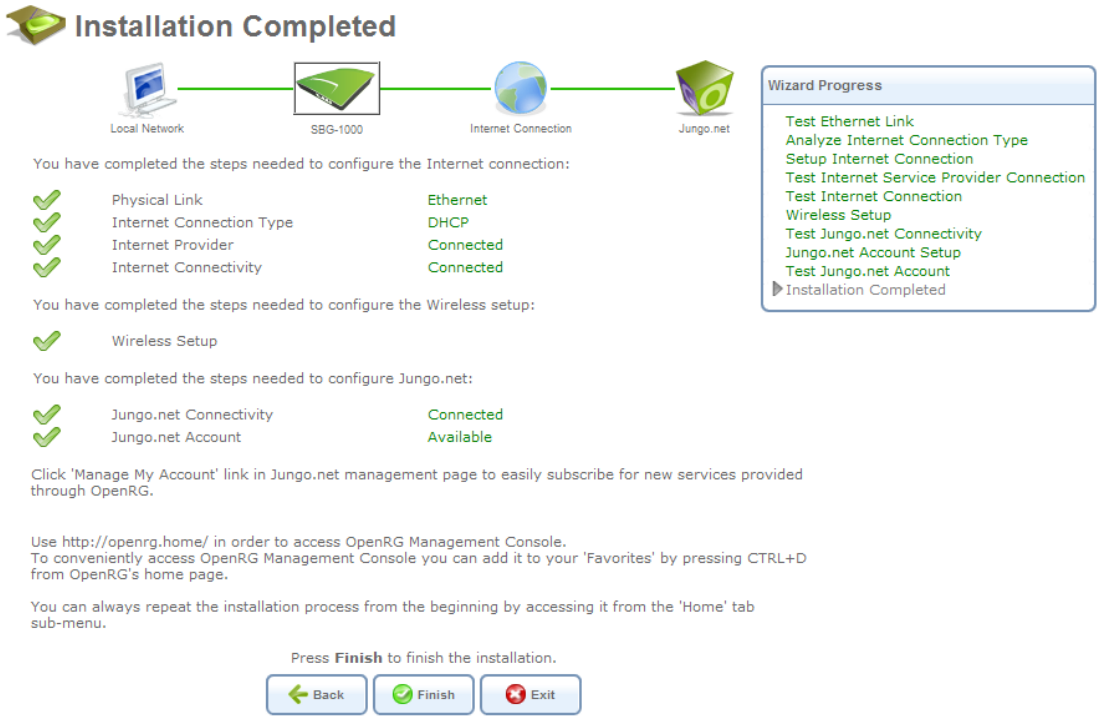


Figure 2.31 Installation Completed

2.4 Configuring Your Wireless Network

The ‘Wireless’ menu item enables you to view and configure the gateway’s ‘Home Network’ and ‘Secured Wireless Network’ wireless access points (the rest can only be configured as described in Section 4.3).

Figure 2.32 Settings – Wireless

The first ‘Enable Wireless’ check box displayed in this screen enables you to activate or deactivate the gateway’s entire wireless interface. The ‘Home Network’ and ‘Secured Wireless Network’ access points are activate by default. You can change their network names (also known as SSIDs) in the respective name fields.
Both access points are secured with a default password (by default “wlpass123”), which you can change in the ‘Global Wireless Password’ field. However, the ‘Secured Wireless Network’ can also be configured with the Wired Equivalent Privacy (WEP) protocol. WEP is a data encryption method utilizing a 13-character security key that is used for authentication of wireless clients. To utilize WEP, select ‘WEP Wireless Network’ from the drop-down menu. The screen refreshes, displaying the ‘Wireless Password’ field, which enables you to define the access point’s WEP security key.

Figure 2.33 Wireless – WEP Security

Enter your personalized security key, and click ‘Apply’ to save the settings.

3. Internet Connection

3.1 Viewing Your Internet Connection Properties

The 'Overview' screen provides general information regarding your Internet connection, such as the connection's status, protocol, speed, duration, as well as the gateway's external IP address and networking parameters. You can use this screen to quickly view your Internet connection status.

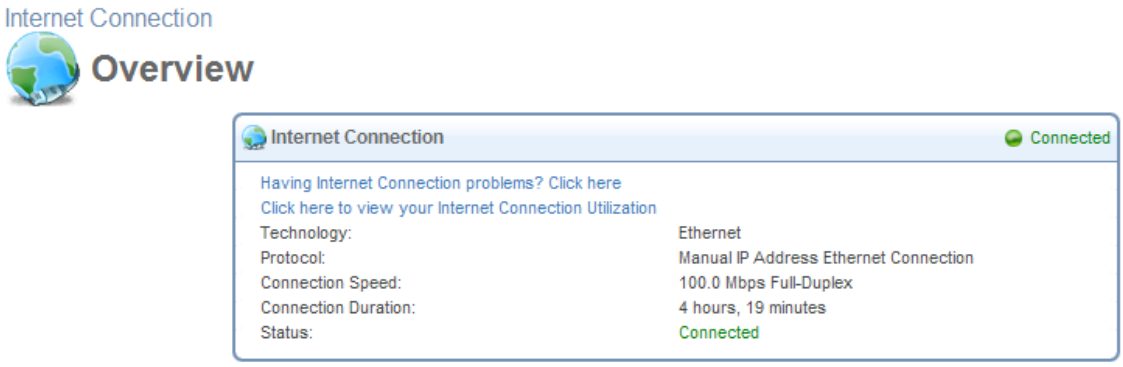


Figure 3.1 Internet Connection – Overview

The following links are available:

- **Have Internet Connection problems? Click here** This link routes you to the 'Troubleshoot' screen, where you can run tests in order to diagnose and resolve Internet connectivity problems.
- **Click Here For Internet Connection Utilization** Click this link to analyze the traffic usage of your WAN connection (for more information, refer to Section 5.3).

In addition, this screen displays iPECS SBG-1000's top bandwidth consuming applications and computers, described in Section 5.3.2.

3.2 Configuring Your Internet Connection

The 'Settings' screen provides basic configuration options for the different types of Internet connections supported by iPECS SBG-1000.

When subscribing to a broadband service, you should be aware of the method by which you are connected to the Internet. Your physical WAN device can be either Ethernet, DSL, or both. Technical information regarding the properties of your Internet connection should be provided by your Internet Service Provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, or what protocols, such as PPTP or PPPoE, you will be using to communicate over the Internet.

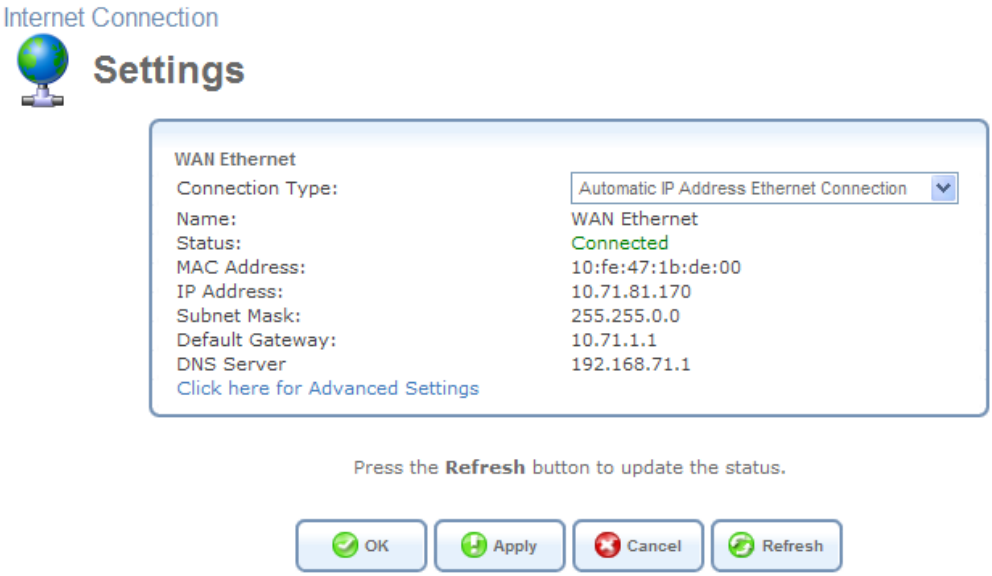


Figure 3.2 Internet Connection – Settings

If you are already connected to the Internet, this screen provides information on your connection. The drop-down menu provides the WAN connection types supported by iPECS SBG-1000, and your WAN connection can be configured using one of the following methods.

- Manual IP Address Ethernet Connection
- Automatic IP Address Ethernet Connection
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Point-to-point protocol over Ethernet (PPPoE)
- No Internet connection

3.2.1 Manual IP Address Ethernet Connection

Select ‘Manual IP Address Ethernet Connection’ from the ‘Connection Type’ drop-down menu.

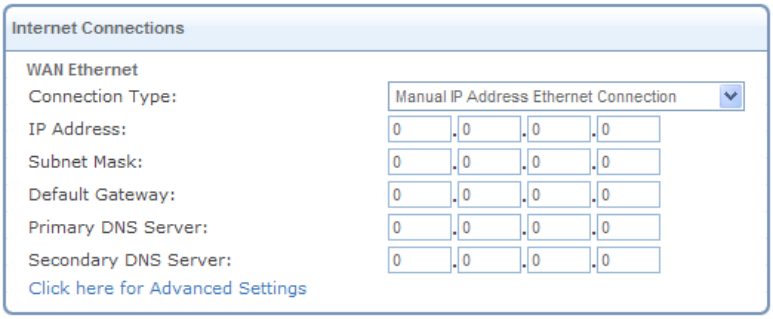


Figure 3.3 Internet Connection – Manual IP Address Ethernet Connection

According to your service provider’s instructions, specify the following parameters:

- IP address

- Subnet mask
- Default gateway
- Primary DNS server
- Secondary DNS server

3.2.2 Automatic IP Address Ethernet Connection

Select ‘Automatic IP Address Ethernet Connection’ from the ‘Connection Type’ drop-down menu. iPECS SBG-1000 will obtain the WAN IP and DNS IP addresses from a DHCP server on the WAN.

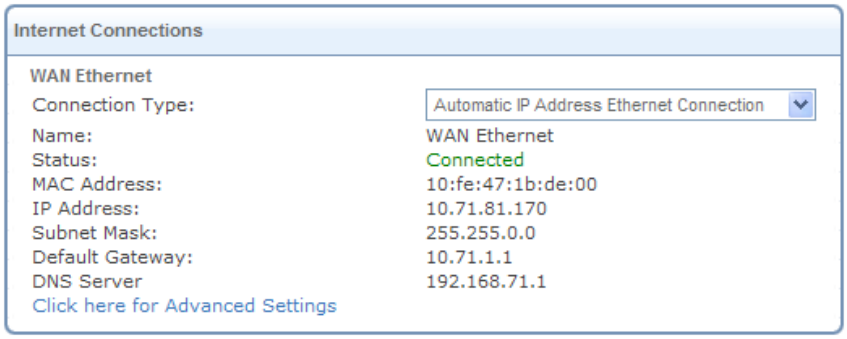


Figure 3.4 Internet Connection – Automatic IP Address Ethernet Connection

3.2.3 Point-to-Point Tunneling Protocol (PPTP)

Select ‘Point-to-Point Tunneling Protocol (PPTP)’ from the ‘Connection Type’ drop-down menu.

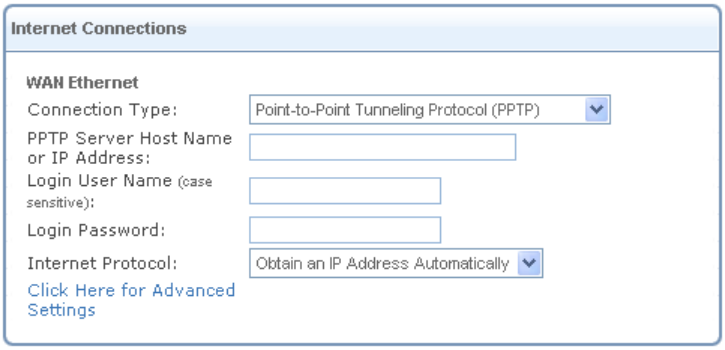


Figure 3.5 Internet Connection – PPTP

Configure the following parameters according to your ISP information:

- PPTP Server Host Name or IP Address
- Login User Name
- Login Password

Select the Internet Protocol:

Most Internet Service Providers (ISPs) provide dynamic IP addresses, hence the default “Obtain

an IP Address Automatically". Should this not be the case, select the "Use the Following IP Address" option. The screen refreshes. Enter the IP Address, Subnet Mask, and Default Gateway provided to you by your ISP.

Figure 3.6 PPTP – Static IP Address

3.2.4 Layer 2 Tunneling Protocol (L2TP)

Select 'Layer 2 Tunneling Protocol (L2TP)' from the 'Connection Type' drop-down menu.

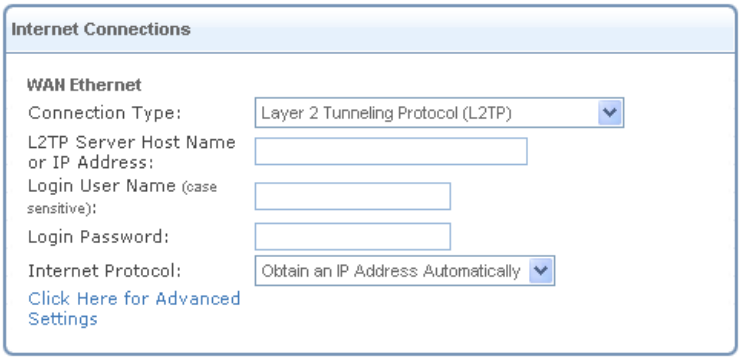


Figure 3.7 Internet Connection – L2TP

Configure the following parameters according to your ISP information:

-
- L2TP Server Host Name or IP Address
- Login User Name
- Login Password

Select the Internet Protocol:

Most Internet Service Providers (ISPs) provide dynamic IP addresses, hence the default "Obtain an IP Address Automatically". Should this not be the case, select the "Use the Following IP Address" option. The screen refreshes. Enter the IP Address, Subnet Mask, and Default Gateway provided to you by your ISP.

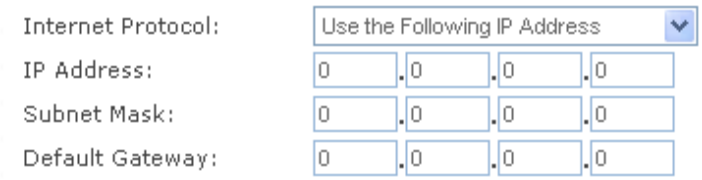


Figure 3.8 L2TP – Static IP Address

3.2.5 Point-to-Point Protocol over Ethernet (PPPoE)

Select 'Point-to-point protocol over Ethernet (PPPoE)' from the 'Connection Type' drop-down menu.

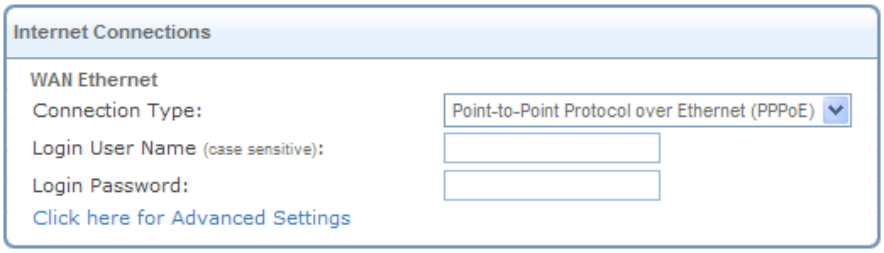


Figure 3.9 Internet Connection – PPPoE

Your Internet Service Provider (ISP) should provide you with the following information:

- Login user name
- Login password

3.2.6 No Internet Connection

Select 'No Internet Connection' from the 'Connection Type' drop-down menu (see Figure 3.10). Choose this connection type if you do not have an Internet connection, or if you want to disable all existing connections.

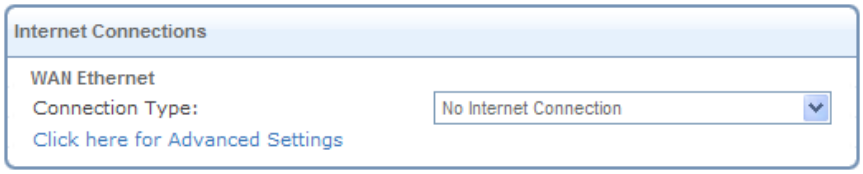


Figure 3.10 Internet Connection – No Internet Connection

4. Local Network

4.1 Overviewing Your Local Network

The ‘Overview’ screen presents iPECS SBG-1000’s network summary. This includes all connected devices: computers, disks, and phones. When this screen is loaded, iPECS SBG-1000 begins the process of automatically detecting the network services available on connected computers (hosts). The screen then refreshes, displaying each computer’s network services.

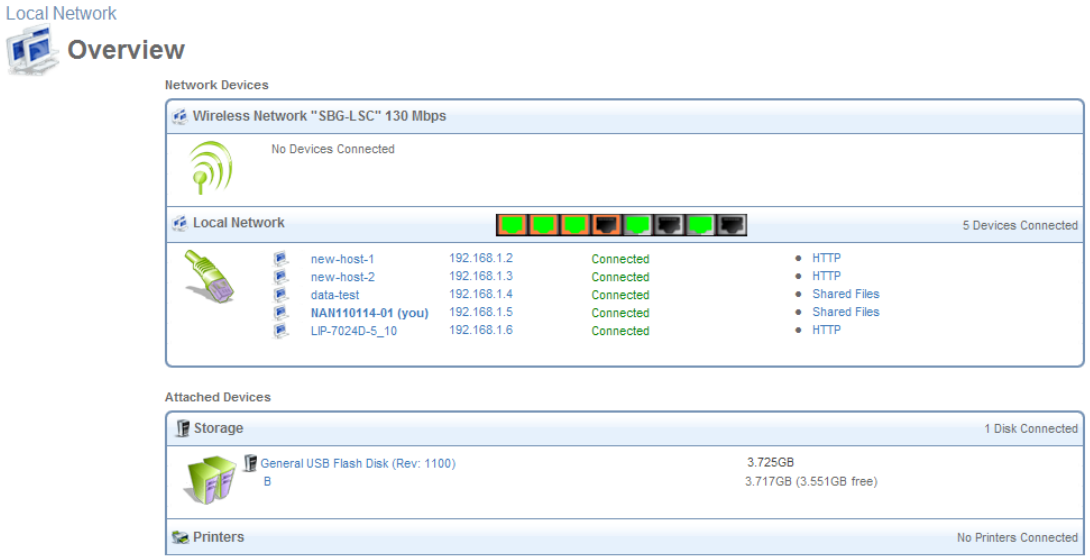


Figure 4.1 Local Network Overview

To view more information on a specific computer, click its respective link. The ‘Host Information’ screen appears.

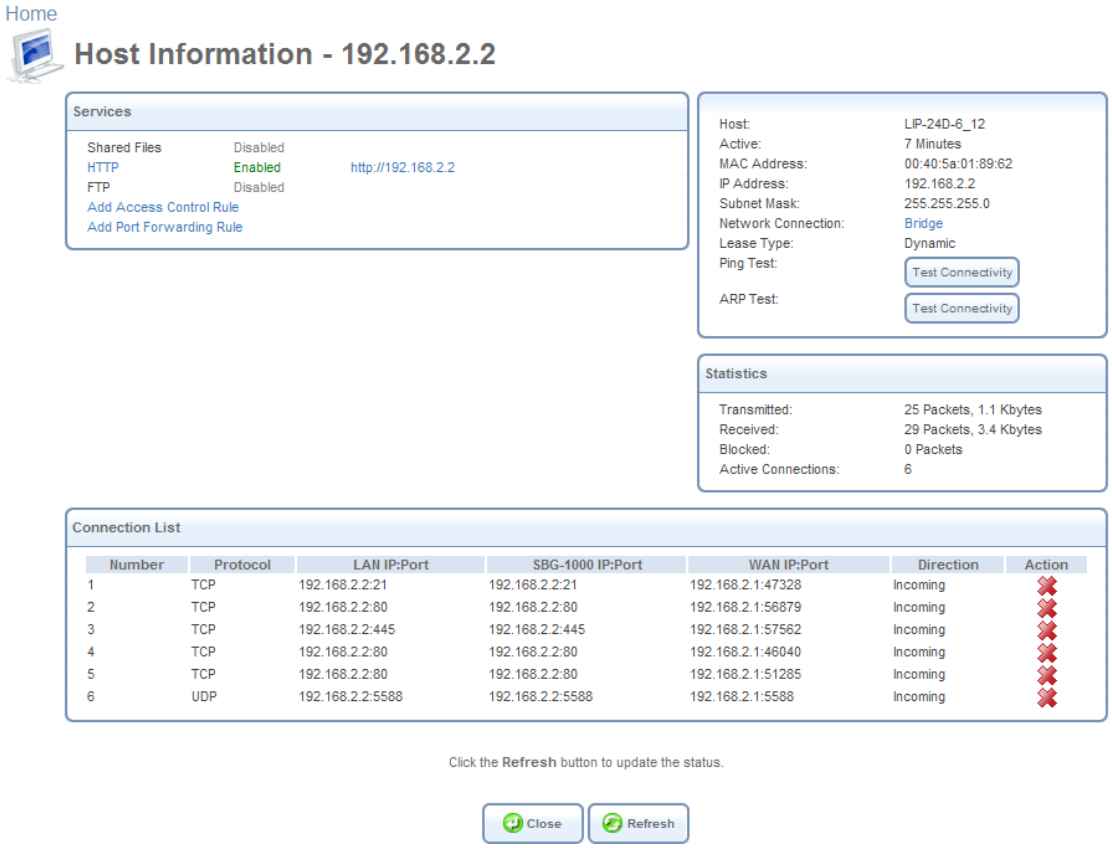


Figure 4.2 Host Information

This screen presents all information that is relevant to the connected computer, such as connection settings, available services, traffic statistics, and connection list. It also enables you to perform connectivity tests with the computer.

Services This section lists the services enabled on the computer that are available to other computers in the LAN, via Web access, or from both. When a service is accessible from the LAN, you can activate it by either clicking its name or the URL that appears (see Figure 4.2). When a service is accessible via Web access, you can activate it by clicking the 'Web Access' link that appears. Available services are:

1 **Shared Files** Access the computer's shared files directory.

- **HTTP** Access the computer's HTTP server (if available).
- **FTP** Open an FTP session with the computer.
- **Add Access Control Rule** Block access to Internet services from the computer, or allow access if the firewall is set to a "High" security level (for more information, refer to Section 5.2.2).
- **Add Port Forwarding Rule** Expose services on the computer to external Internet users (for more information, refer to Section 5.2.3).

Connection Information This section displays various details regarding the computer's connection settings. In addition, you can run a Ping or ARP test by clicking the respective 'Test Connectivity' button. The tests are performed in the 'Diagnostics' screen (refer to Section 6.8.7).

Statistics This section displays the computer's traffic statistics, such as the number and size of

transmitted and received packets.

Connection List This section displays the list of connections opened by the computer on iPECS SBG-1000's firewall. The table displays the computer's source LAN IP address and port, the gateway's IP address and port to which it is translated, and the destination WAN IP address and port.

4.2 Viewing the Gateway's LAN Devices

The 'Device' screen (see Figure 4.3) presents a summary of iPECS SBG-1000's LAN devices, including bridge (if one exists), Ethernet and wireless, and the status of each one (connected/disconnected).

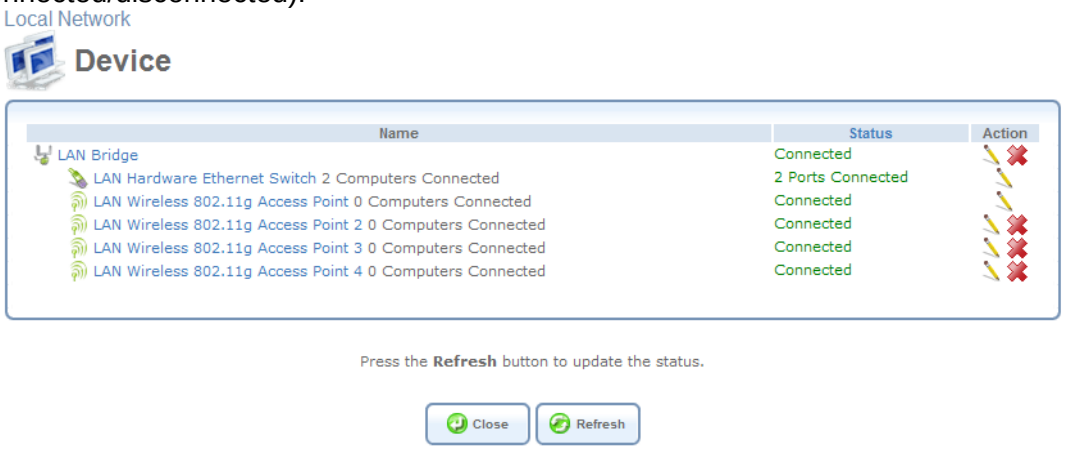


Figure 4.3 Local Network Device View

4.3 Configuring Your Wireless Connection

The 'Wireless' menu item concentrates the wireless LAN settings of your gateway. This screen presents iPECS SBG-1000's wireless connection settings, and enables you to change them according to your needs.

Figure 4.4 Wireless Overview

Enable Wireless Select or deselect this check box to enable or disable the wireless interface.
Channel All devices in your wireless network broadcast on different channels. Leaving this parameter on Automatic ensures that iPECS SBG-1000 continuously scans for the most available wireless channel in your area. It is possible to select a channel manually if you have information regarding the wireless channels used in your vicinity. The channels available depend on the regulatory authority (stated in brackets) to which your gateway conforms. For example, the European regulatory authority (ETSI) has allocated 13 available channels, while the US regulatory authority (FCC) has allocated 11 available channels.
Network Name (SSID) The SSID is the network name shared among all points in a wireless network. It is case-sensitive and must not exceed 32 characters. Note that you may use ASCII characters only. For added security, you may change the default SSID to a unique name.

Type This field shows your wireless security settings.

- **Unsecured -** This option disables security on your wireless connection. Any wireless computer in your area will be able to connect to the Internet using your connection's bandwidth.
- **WPA -** A data encryption method for 802.11 wireless LANs.
- **WPA2 -** An enhanced version of WPA, and defines the 802.11i protocol.
- **WPA and WPA2** - A mixed data encryption method, which utilizes both WPA and WPA2.
- **WEP** - A data encryption method utilizing a statically defined key as the wireless password. Note that the static key must be defined in the wireless Windows client as well.
- **Web Authentication** - With this option, wireless clients attempting to connect to the wireless connection will receive iPECS SBG-1000's main login screen. By logging into the WBM, clients authenticate themselves and are then able to use the connection.

Wireless Password The wireless password required to connect to the gateway's wireless network. You may change the default password in the 'Network Connections' menu item under the 'System' tab. This password must be at least an 8 characters long.

4.4 Managing Your Shared Printers

iPECS SBG-1000 includes a print server that enables your LAN users to share printers attached to the gateway via the USB connection. This eliminates the need to physically connect your printer to a dedicated host, which should be shared and always left on. In addition, the print server offers you such advantages as:

- Support for several print protocols, which enable you to connect Windows, Unix and Mac hosts to the network printer.

- Ability to define printer access permissions for specific LAN users.

4.4.1 Configuring the Print Server

Access the print server settings by clicking the ‘Shared Printers’ menu item under the ‘Local Network’ tab. The ‘Print Server’ screen appears, enabling you to manage your network printer.

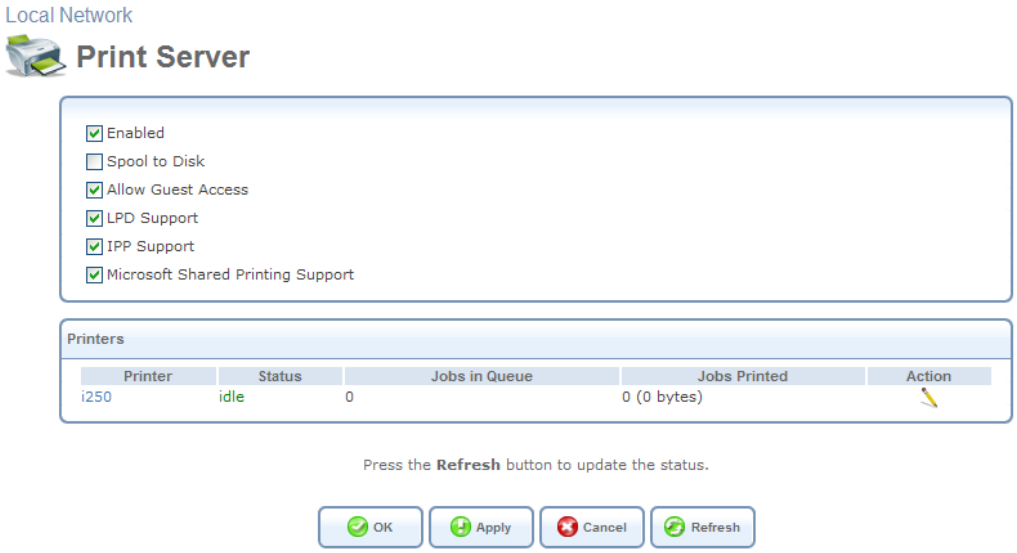


Figure 4.5 Print Server

Enabled Select or deselect this check box to enable or disable this feature.
Spool to Disk Select this check box to temporarily store your print jobs on the disk share, until they are finished. This is especially useful if you would like the printer to process the print job even after you turn the computer off.
The ‘Printers’ section of this screen displays the printer(s) connected to iPECS SBG-1000, the device status, and print job information. Click a printer’s name link to view its details. The ‘Printer’ screen appears.

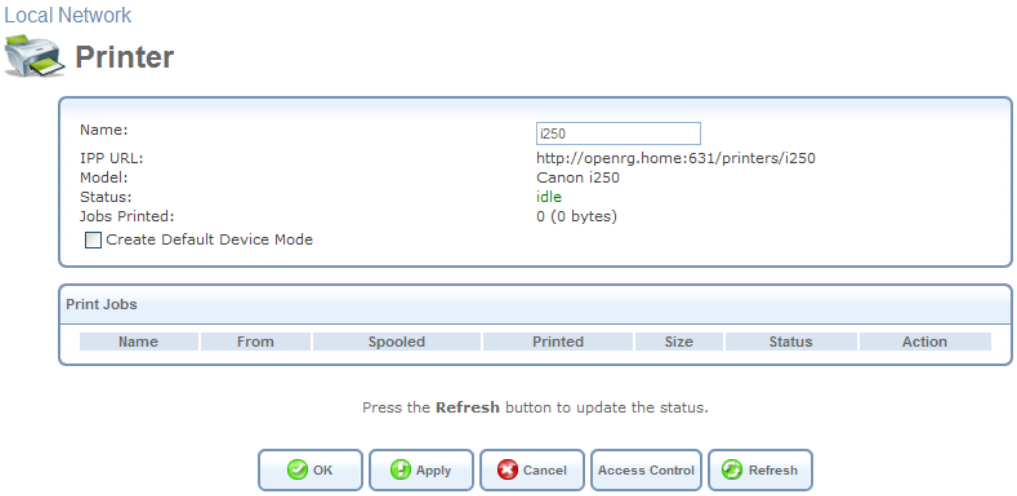


Figure 4.6 Connected Printer

4.5 Managing Your Private Telephony Switching System

iPECS SBG-1000 provide customers state-of the art of LG-Ericsson's Internet Protocol Private Branch Exchange (IP-PBX) features, using the menu in the 'Services' Tab.

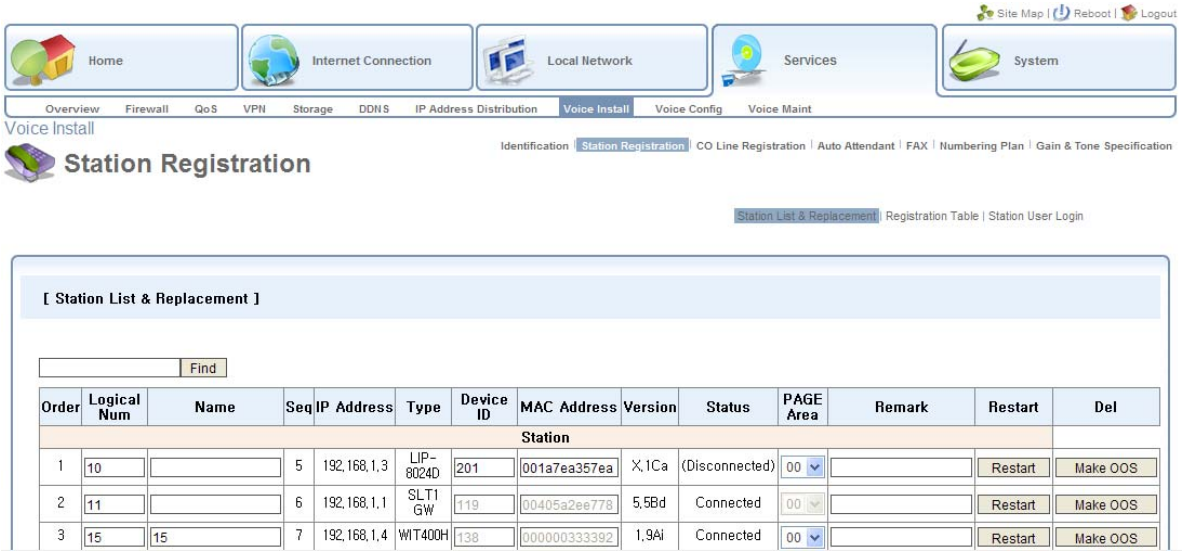


Figure 4.7 IP-PBX Lines

For more information about the IP-PBX features, refer to 'iPECS SBG-1000 IP-PBX Features Manual'.

5. Services

5.1 Overviewing Your Services

The ‘Overview’ screen presents a summary of iPECS SBG-1000’s services and their current status (enabled/disabled, etc.). These services are configurable via their respective menu items under the ‘Services’ tab.

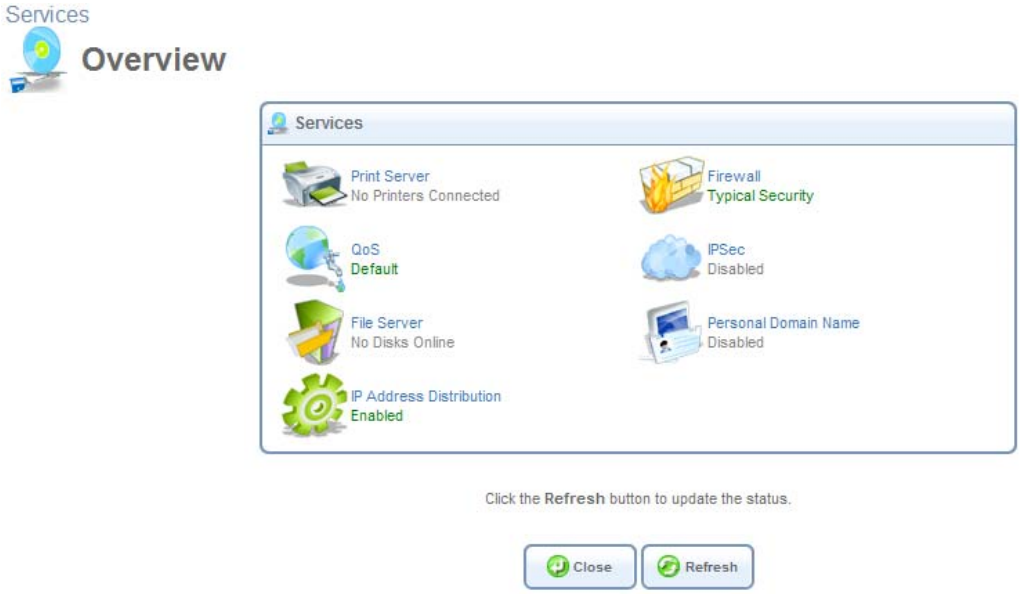


Figure 5.1 Services Overview

5.2 Securing Your Network with the Firewall

iPECS SBG-1000’s gateway security suite includes comprehensive and robust security services: Stateful Packet Inspection Firewall, user authentication protocols and password protection mechanisms. These features together allow users to connect their computers to the Internet and simultaneously be protected from the security threats of the Internet. The firewall has been exclusively tailored to the needs of the residential/office user and has been pre-configured to provide optimum security (see Figure 5.2).

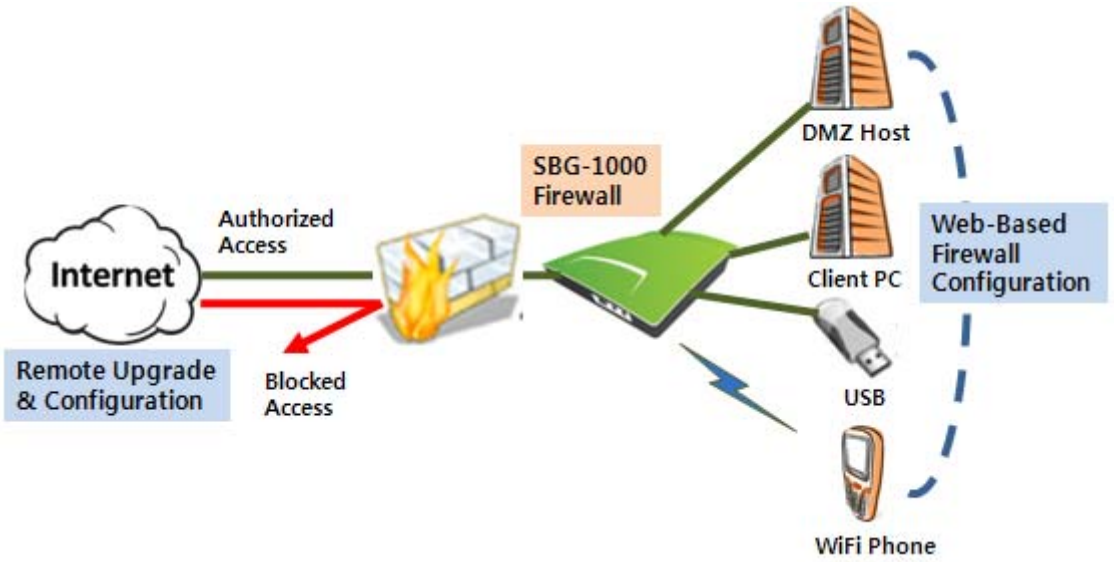


Figure 5.2 iPECS SBG-1000's Firewall in Action

iPECS SBG-1000's firewall provides both the security and flexibility that home and office users seek. It provides a managed, professional level of network security while enabling the safe use of interactive applications, such as Internet gaming and video-conferencing.
Additional features, including browsing restrictions and access control, can also be easily configured locally by the user through a user-friendly Web-based interface, or remotely by a service provider. The iPECS SBG-1000 firewall supports advanced filtering, designed to allow comprehensive control over the firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN network devices.

5.2.1 Configuring Basic Security Settings

The firewall's 'Overview' screen enables you to configure the gateway's basic security settings.

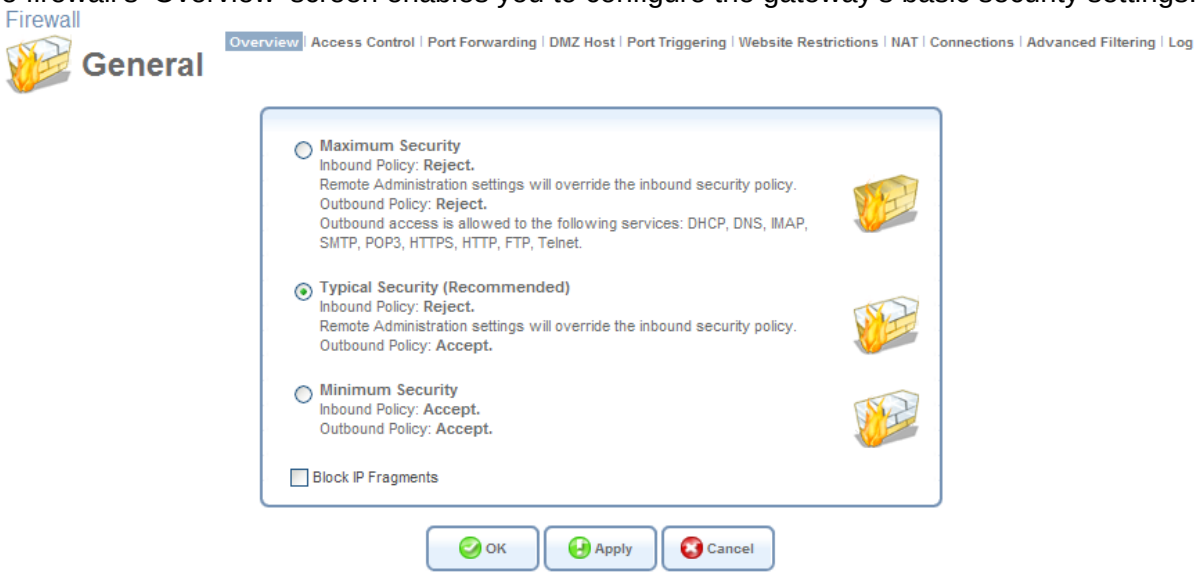


Figure 5.3 Firewall – Overview

You may choose between three pre-defined security levels for iPECS SBG-1000: Minimum, Typical (the default), and Maximum. The following table summarizes iPECS SBG-1000's behavior for each of the three security levels.

Security Level	Requests Originating in the WAN (Incoming Traffic)	Requests Originating in the LAN (Outgoing Traffic)
Maximum Security	*Blocked*: No access to home network from Internet, except as configured in the Port Forwarding, DMZ host and Remote Access screens	*Limited*: Only commonly-used services, such as Web-browsing and e-mail, are permitted. The list of allowed services can be edited in the Access Control screen (refer to Section 5.2.2)
Typical Security (Default)	*Blocked*: No access to home network from Internet, except as configured in the Port Forwarding, DMZ host and Remote Access screens	*Unrestricted*: All services are permitted, except as configured in the Access Control screen
Minimum Security	*Unrestricted*: Permits full access from Internet to home network; all connection attempts permitted	*Unrestricted*: All services are permitted, except as configured in the Access Control screen

Table 5.1 iPECS SBG-1000's Firewall Security Levels

To configure iPECS SBG-1000's basic security settings, perform the following:

1. Choose between the three predefined security levels described in the table above.

   Note: Using the *Minimum Security* setting may expose the home network to significant security risks, and thus should only be used, when necessary, for short periods of time.
2. Check the 'Block IP Fragments' box in order to protect your home network from a common type of hacker attack that could make use of fragmented data packets to sabotage your home network. Note that VPN over IPSec and some UDP-based services make legitimate use of IP fragments. In case of enabling these services, you will need to allow IP fragments to pass into the home network.
3. Click 'OK' to save the settings.

By default, the selected security level affects access to such Internet services as Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SNTP. Note that some programs (such as some Internet messengers and Peer-To-Peer clients) tend to use ports of the above-mentioned services in case they cannot connect using their own default ports. When allowing this behavior, the Internet connection requests of such programs will not be blocked, even at the 'Maximum' security level. After the security level is set, the firewall regulates the flow of data between the home network and the Internet. Both incoming and outgoing data are inspected and then either accepted (allowed to pass through iPECS SBG-1000) or rejected (barred from passing through iPECS SBG-1000), according to a flexible and configurable set of rules. These rules are designed to prevent unwanted

intrusions from the outside, while allowing home users access to the Internet services that they require.
The firewall rules specify what types of services available on the Internet may be accessed from the home network and what types of services available in the home network may be accessed from the Internet. Each request for a service that the firewall receives, whether originating from the Internet or from a computer in the home network, is checked against the set of firewall rules to determine whether the request should be allowed to pass through the firewall. If the request is permitted to pass, then all subsequent data associated with this request (a “session”) will also be allowed to pass, regardless of its direction.
For example, when you point your browser to a Web page, a request is sent to the Internet for retrieving and loading this page. When this request reaches iPECS SBG-1000, its firewall identifies the request’s type and origin. In the Web browsing example, HTTP is the request’s type, and your PC is its origin. Unless you have configured iPECS SBG-1000’s Access Control feature to block requests of this type originating from your PC, the firewall will allow this request to pass out onto the Internet (for more on configuring iPECS SBG-1000’s Access Control, refer to Section 5.2.2). When the Web page is returned from the Web server, the firewall associates it with the current connection and allows it to pass, regardless of whether HTTP access from the Internet to your home network is blocked or permitted. It is the *origin of the request*, not the subsequent responses to this request, that determines whether a connection can be established or not.

5.2.2 Controlling Your Network’s Access to Internet Services

You may want to block specific computers within the home network (or even the whole network) from accessing certain services available on the Internet. For example, you may want to prohibit one computer from browsing the Web, another computer from transferring files using FTP, and the whole network from accessing email (by blocking the *outgoing* requests to POP3 servers on the Internet). The ‘Access Control’ screen enables you to apply restrictions on the types of connection requests that may pass from the home network out to the Internet, and to block the corresponding network traffic in both directions. In addition, this screen can be used for allowing access to specific services when the ‘Maximum’ security is applied (as described in Section 5.2.1).
To block access to a service available on the Internet:

1. Click the ‘Access Control’ link under the ‘Firewall’ menu item. The ‘Access Control’ screen appears.

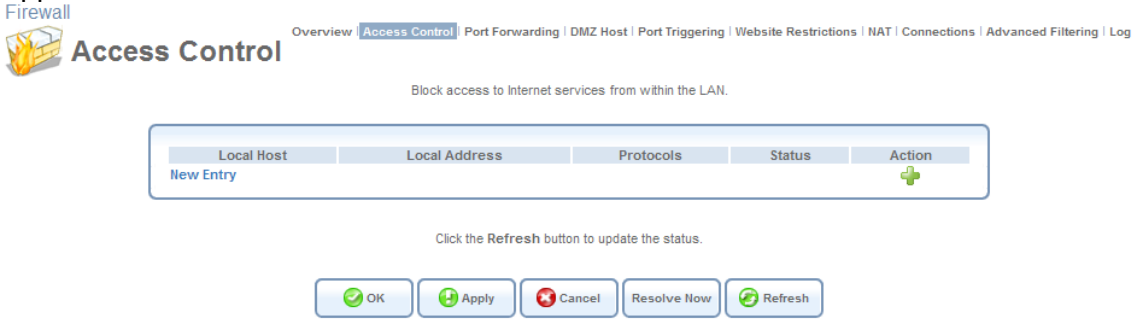


Figure 5.4 Access Control

2. Click the ‘New Entry’ link. The ‘Add Access Control Rule’ screen appears.

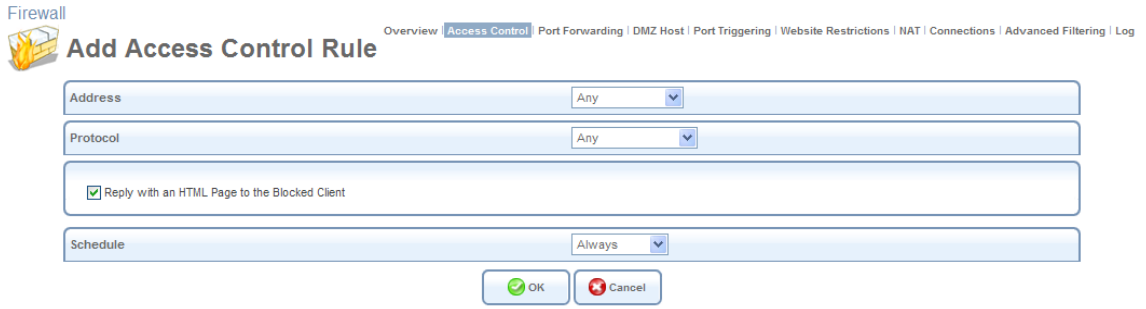


Figure 5.5 Add Access Control Rule

3. From the 'Address' drop-down menu, select an IP address or a computer name from the list in order to apply the rule on the corresponding LAN computer, or 'Any' to apply the rule on all LAN computers. If you wish to add a new LAN address or a range of addresses, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new Network Object, representing the new host. Refer to Section 6.9.2 in order to learn how to do so.
4. From the 'Protocol' drop-down menu, select the type of protocol used by the service. Note that selecting the 'Show All Services' option expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option. This will commence a sequence that will add a new Service, representing the protocol. Refer to Section 6.9.2 in order to learn how to do so.
5. If you selected the HTTP or HTTPS protocol (to deny access to the Internet), you may also wish to enable the feature 'Reply an HTML page to the blocked client'. When its check box is selected, the following message will be displayed in the browser of the blocked LAN computer, when the user attempts to surf the Internet: "Access Denied – this computer is not allowed to surf the Internet. Please contact your admin.". When this check box is deselected, the computer's Internet connection requests are simply ignored and no notification is issued.
6. By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting 'User Defined' from the 'Schedule' drop-down menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.
7. Click 'OK' to save your changes. The 'Access Control' screen displays a summary of the rule that you have just added.

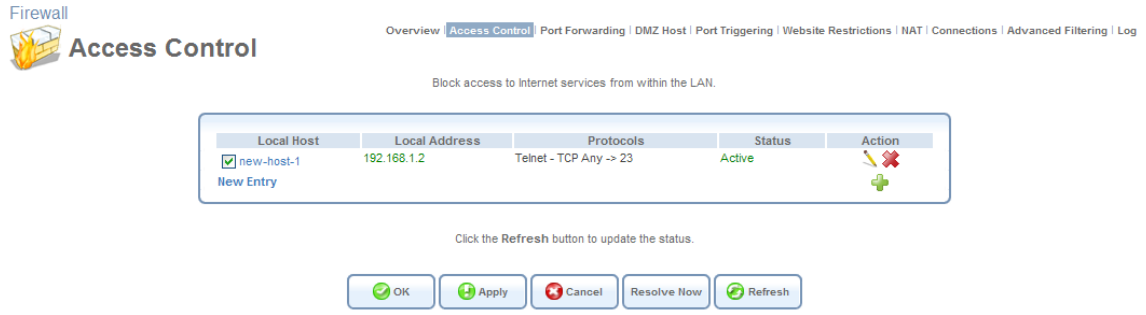


Figure 5.6 Access Control Rule

You may edit the access control rule by modifying its entry displayed under the 'Local Host' column.

- To modify a rule's entry:
  1. Click the rule's action icon. The 'Edit Access Control Rule' screen appears. This screen allows you to edit all the parameters that you configured when creating the access control rule.

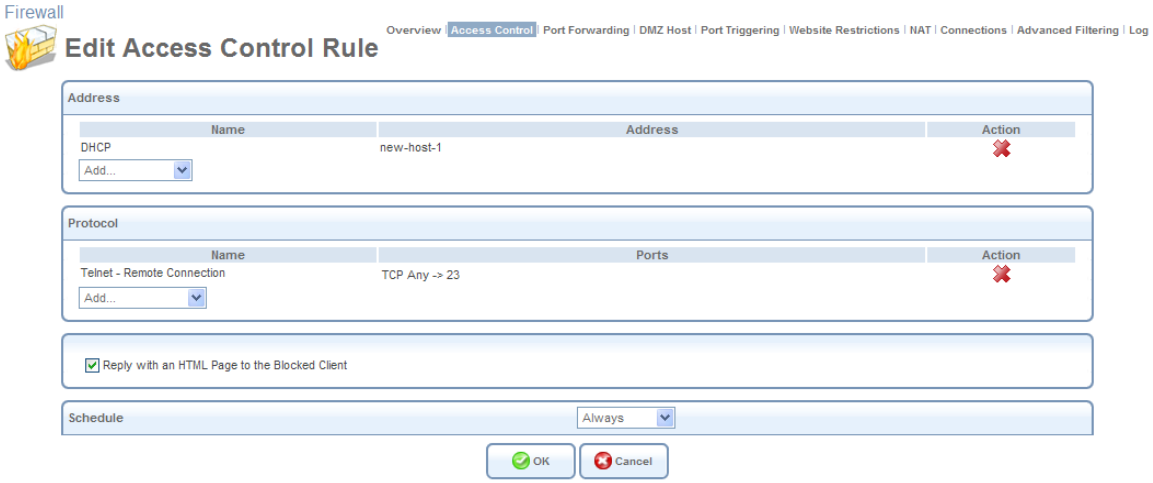


Figure 5.7 Edit Access Control Rule

  2. Click 'OK' to save your changes and return to the 'Access Control' screen.

You can disable an access control rule in order to make the corresponding service available, without having to remove the rule from the 'Access Control' screen. This may be useful if you wish to unblock access to the service only temporarily, intending to reinstate the restriction in the future.

- To temporarily disable a rule, clear the check box next to the service name.
- To reinstate it at a later time, simply reselect the check box.
- To remove a rule, click the service's action icon. The service will be permanently removed.

When the 'Maximum' security level is applied, the 'Access Control' screen also displays a list of automatically generated firewall rules that allow access to specific Internet services from the LAN computers, over pre-defined ports.

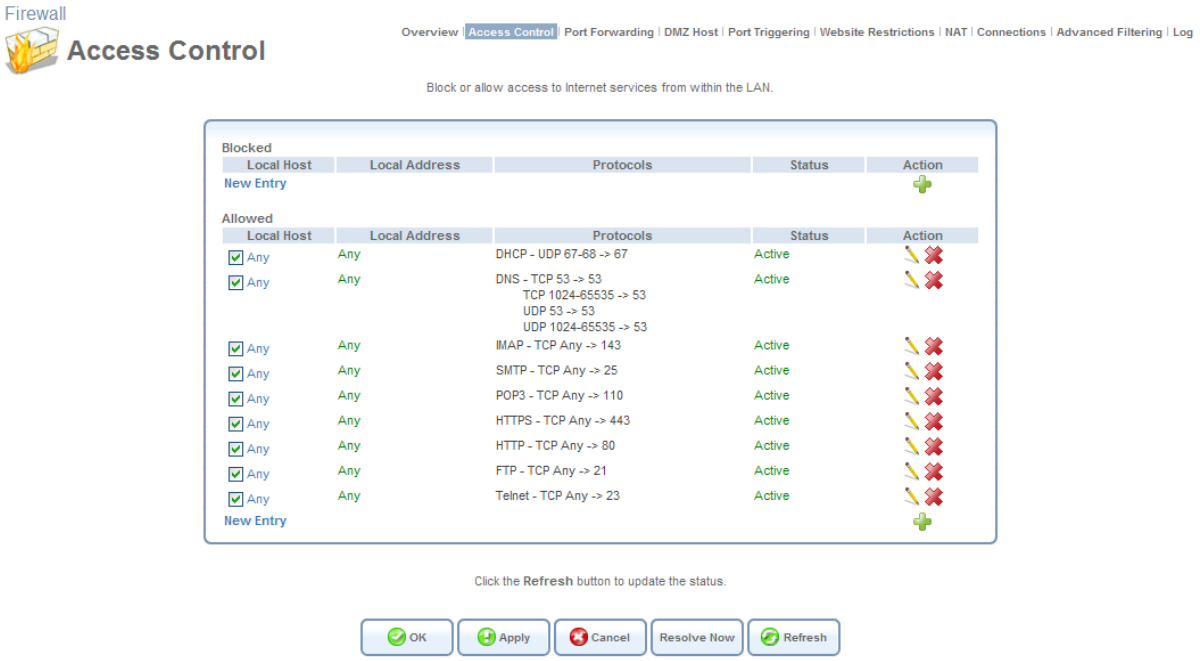


Figure 5.8 Access Control – Allowed Services in Maximum Security Mode

You can manage these access control rules as well as create new ones (allowing access to other services), as described earlier in this section.

5.2.3 Using Port Forwarding

In its default state, iPECS SBG-1000 blocks all external users from connecting to or communicating with your network. Therefore, the system is safe from hackers who may try to intrude into your network and damage it. However, you may wish to expose your network to the Internet in certain limited and controlled ways. iPECS SBG-1000's Port Forwarding feature enables you to do so. If you are familiar with networking terminology and concepts, you may have encountered the Port Forwarding capability referred to as "Local Servers".

The 'Port Forwarding' feature enables you to define applications (for example, Peer-to-Peer, game, voice, or chat programs) that will be allowed a controlled Internet activity. In addition, you may use Port Forwarding to allow external access to specific servers running on your network. For example, if you wish to allow external access to your File Transfer Protocol (FTP) server running on a LAN PC, you would simply create a port forwarding rule, which specifies that all FTP-related data arriving at iPECS SBG-1000 from the Internet will henceforth be forwarded to the specified PC. Another example of utilizing the Port Forwarding feature is hosting a Web site on your own server. When an Internet user points a browser to iPECS SBG-1000's external IP address, the gateway will forward the incoming HTTP request to your Web server, if the corresponding port forwarding rule had been set.

However, there is a limitation that must be considered. With one external IP address (iPECS SBG-1000's main IP address), different applications can be assigned to your LAN computers, however each type of application is limited to use one computer. For example, you can define that FTP will use address X to reach computer A and Telnet will also use address X to reach computer A, but attempting to define FTP to use address X to reach both computer A and B will fail. iPECS SBG-1000 therefore provides the ability to add additional public IP addresses to port forwarding

rules, which you must first obtain from your ISP, and enter into the 'NAT IP Addresses Pool' (refer to Section 5.2.7). You will then be able to define FTP to use address X to reach computer A, and address Y to reach computer B.
Additionally, iPECS SBG-1000's Port Forwarding feature enables you to redirect traffic to a different port instead of the one for which it was designated. For example, if you have a Web server running on your PC on port 8080, you may wish to redirect anyone who browses to iPECS SBG-1000's external IP address (by default, over port 80) to your Web server.

Note: A remote administration service will have precedence over the port forwarding rule created for a local server, when both are configured to utilize the same port. For example, when both the Web server (running on your LAN host) and a remote administration service (utilized by the ISP) are configured to use port 80, iPECS SBG-1000 will grant access to the remote administration traffic. The traffic destined for your Web server will be blocked until you disable the remote administration service or change its dedicated port. For more information about the remote administration services, refer to Section 6.7.3.

Some applications that work with such protocols as FTP, TFTP, PPTP and H.323, require the support of specific Application Level Gateway (ALG) modules in order to work inside the home network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. iPECS SBG-1000 is configured with a robust list of ALG rules in order to enable maximum functionality in the home network. These ALG rules are automatically applied based on the destination ports. You may also create additional ALG rules. To learn how to do so, refer to Section 5.2.8.2).

5.2.3.1 Adding a Port Forwarding Rule

To allow remote access to a service running one a LAN computer, create a corresponding port forwarding rule as follows:

1. Click 'Port Forwarding' under the 'Firewall' menu item. The 'Port Forwarding' screen appears.

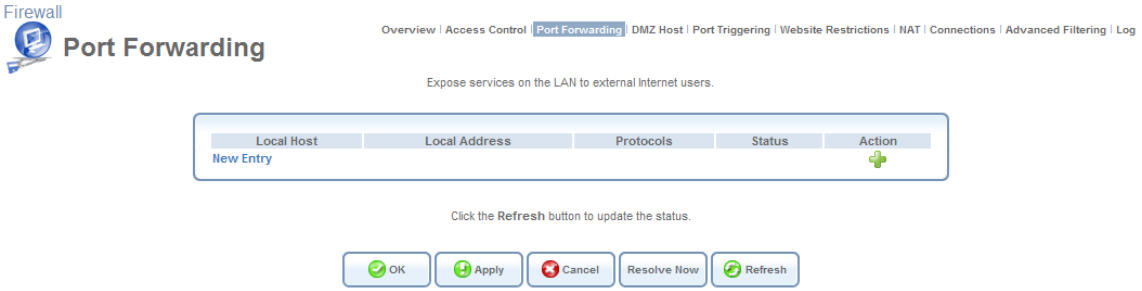


Figure 5.9 Port Forwarding

2. Click the 'New Entry' link. The 'Add Port Forwarding Rule' screen appears.

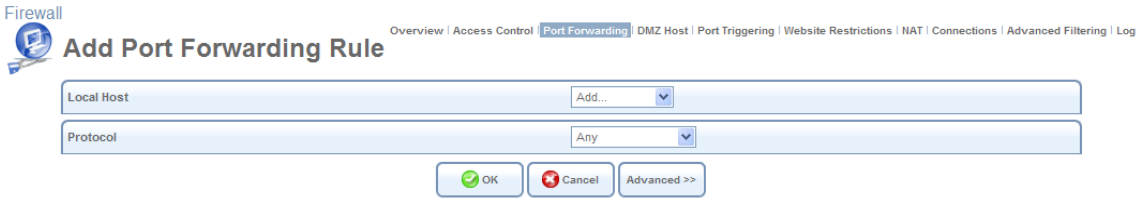


Figure 5.10 Add Port Forwarding Rule – Basic

3. Click the ‘Advanced’ button at the bottom of the screen. The screen expands.

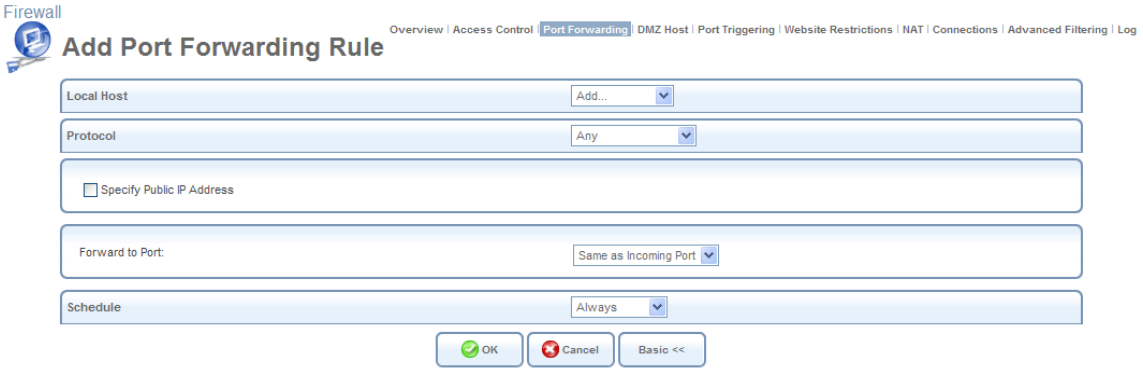


Figure 5.11 Add Port Forwarding Rule – Advanced

4. The ‘Local Host’ drop-down menu lists your available LAN computers. Select a computer that provides the service, to which you wish to grant access over the Internet. If you would like to add a new computer, select the ‘User Defined’ option in the drop-down menu. This will commence a sequence that will add a new Network Object, representing the new host. Refer to Section 6.9.2 in order to learn how to do so. Note that unless an additional external IP address has been added, only one LAN computer can be assigned to provide a specific service or application.
5. From the ‘Protocol’ drop-down menu, select the type of protocol used by the service. Note that selecting the ‘Show All Services’ option expands the list of available protocols. Select a protocol or add a new one using the ‘User Defined’ option. This will commence a sequence that will add a new Service, representing the protocol. Refer to Section 6.9.2 in order to learn how to do so.
6. Click the ‘Advanced’ button at the bottom of the screen. The screen refreshes, displaying the ‘Forward to Port’ and ‘Schedule’ drop-down menus.

Figure 5.12 Add Port Forwarding Rule – Advanced

7. When creating a port forwarding rule, you must ensure that the port used by the selected protocol is not already in use by any other of your local services, which, in this case, may stop functioning. A common example is when using SIP signaling in Voice over IP—the port used by the gateway's VoIP application (5060) is the same port on which port forwarding is set for LAN SIP agents.
8. If you would like to apply this rule on iPECS SBG-1000's non-default IP address (which you can define in the 'NAT' screen, as described in Section 5.2.7), perform the following:
   a. Select the 'Specify Public IP Address' check box. The screen refreshes.

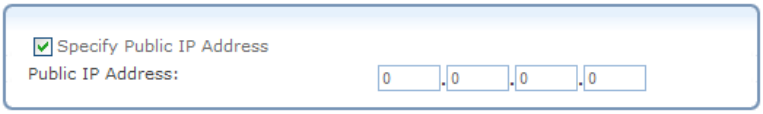


Figure 5.13 Specify Public IP Address

   b. Enter the additional external IP address in the 'Public IP Address' field.
9. By default, iPECS SBG-1000 will forward traffic to the same port as its incoming port. If you wish to redirect traffic to a different port, select the 'Specify' option from the 'Forward to Port' drop-down menu. The screen refreshes, and an additional field appears, enabling you to enter the port number.

Figure 5.14 Forward to a Specific Port

10. By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting 'User Defined' from the 'Schedule' drop-down menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.
11. Click 'OK' to save the settings. The 'Port Forwarding' screen displays a summary of the rule that you have just added.

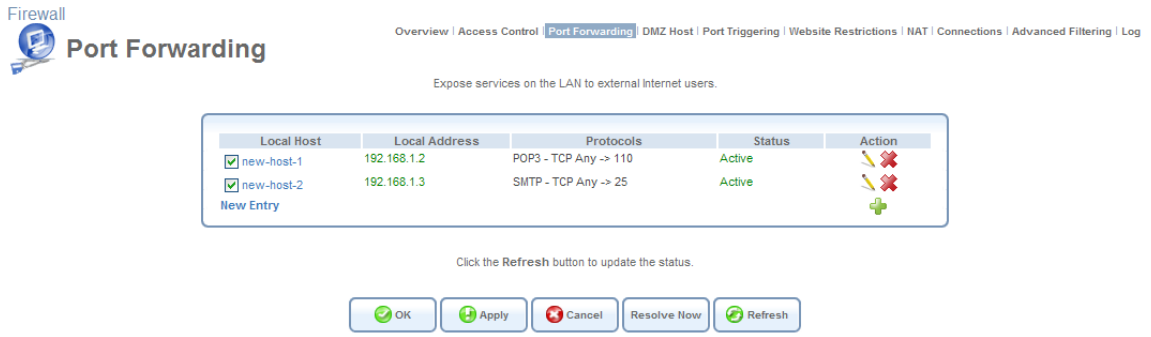


Figure 5.15 Port Forwarding Rule

You may edit the port forwarding rule by clicking its entry under the 'Local Host' column in the 'Port Forwarding' screen. You can also disable the rule in order to make a service unavailable without having to remove the rule from the 'Port Forwarding' screen. This may be useful if you wish to make the service unavailable only temporarily, intending to reinstate it in the future.

- To temporarily disable a rule, clear the check box next to the service name.
- To reinstate it at a later time, simply reselect the check box.
- To remove a rule, click the service's action icon. The service will be permanently removed.

5.2.4 Designating a DMZ Host

The DMZ (Demilitarized) Host feature enables you to expose one local computer to the Internet. Designate a DMZ host when:You wish to use a special-purpose Internet service, such as an on-line game or video-conferencing program, that is not present in the Port Forwarding list, and for which no port range information is available. You are not concerned with security, and wish to expose one computer to all services without restriction.

Warning: A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the home network at risk. When designating a DMZ host, you must consider the security implications, and protect it if necessary

An incoming request for accessing a service in the home network, such as a Web server, is fielded by iPECS SBG-1000. iPECS SBG-1000 will forward this request to the DMZ host if one is designated, unless the service is being provided by another LAN PC (defined in a Port Forwarding rule), in which case that PC will receive the request instead. To designate a local computer as a DMZ Host:

1. Click 'DMZ Host' under the 'Firewall' menu. The 'DMZ Host' screen appears.

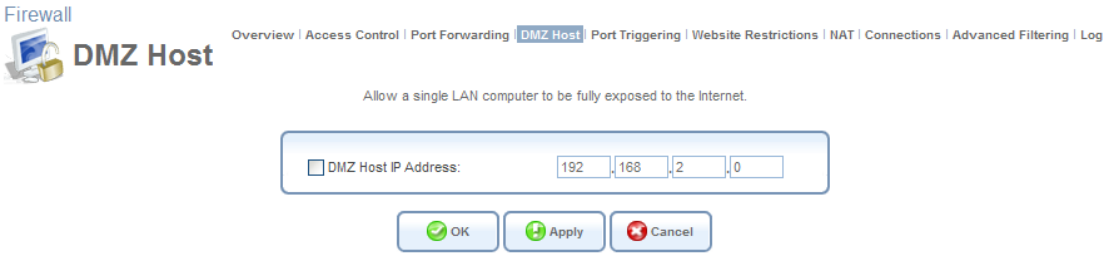


Figure 5.16 DMZ Host

2. Select the check box, and enter the local IP address of the computer that you would like to designate as a DMZ host. Note that only one LAN computer may be a DMZ host at any time.
3. Click 'OK' to save the settings.

You can disable the DMZ host so that it will not be fully exposed to the Internet, but will keep its IP address recorded in the 'DMZ Host' screen. To do so, clear the check box next to the DMZ IP field, and click 'OK'. This may be useful if you wish to temporarily disable the DMZ host, intending to enable it again in the future. To reinstate it at a later time, reselect the check box.

5.2.5 Using Port Triggering

Port triggering is used for setting a dynamic port forwarding configuration. By setting port triggering rules, you can allow inbound traffic to arrive at a specific LAN host, using ports different than those used for the outbound traffic. This is called port triggering since the outbound traffic triggers to which ports inbound traffic is directed.

For example, consider a gaming server that is accessed using the UDP protocol on port 2222. The gaming server responds by connecting the user using UDP on port 3333, when starting gaming sessions. In such a case you must use port triggering, since this scenario conflicts with the following default firewall settings:

- The firewall blocks inbound traffic by default.
- The server replies to iPECS SBG-1000's IP, and the connection is not sent back to your host, since it is not part of a session.

In order to solve this, you need to define a Port Triggering entry, which allows inbound traffic on UDP port 3333 only after a LAN host generated traffic to UDP port 2222. To do so, perform the following:

1. Click the 'Port Triggering' link under the 'Firewall' menu item. The 'Port Triggering' screen appears. This screen will list all of the port triggering entries.

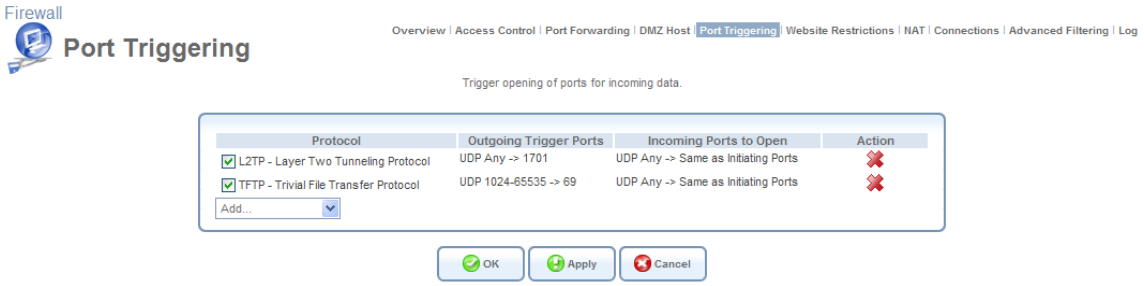


Figure 5.17 Port Triggering

2. Select the ‘User Defined’ option to add an entry. The ‘Edit Port Triggering Rule’ screen appears.

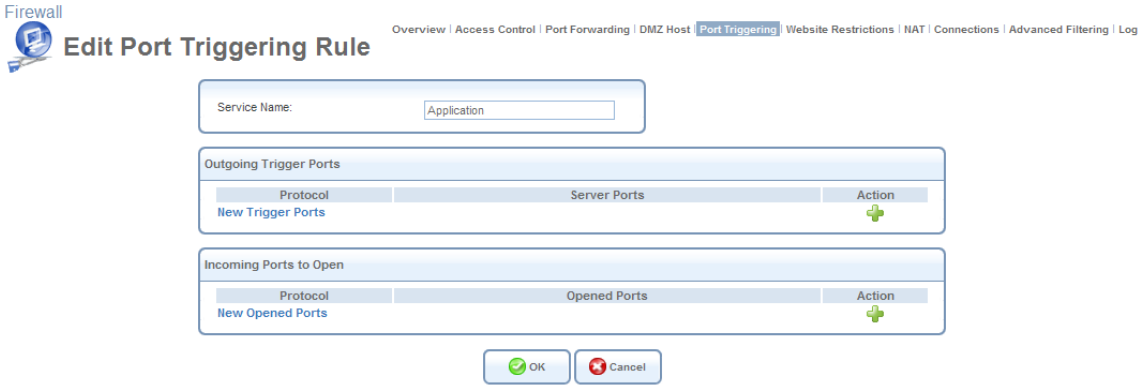


Figure 5.18 Edit Port Triggering Rule

3. Enter a name for the service (e.g. “game_server”), and click the ‘New Trigger Ports’ link. The ‘Edit Service Server Ports’ screen appears.

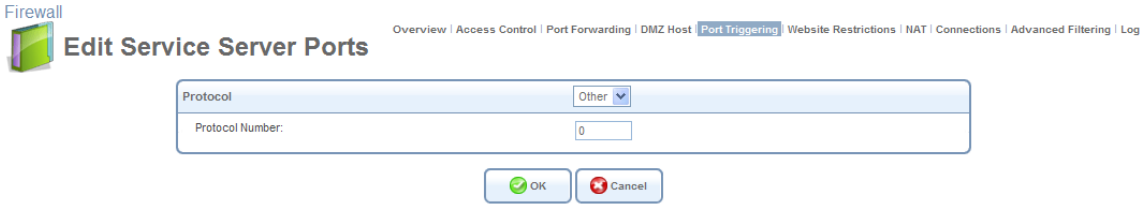


Figure 5.19 Edit Service Server Ports

4. From the ‘Protocol’ drop-down menu, select ‘UDP’. The screen will refresh, providing source and destination port options (see Figure 5.20).
5. Leave the ‘Source Ports’ drop-down menu at its default “Any”. From the ‘Destination Ports’ drop-down menu, select “Single”. The screen will refresh again, providing an additional field in which you should enter “2222” as the destination port.

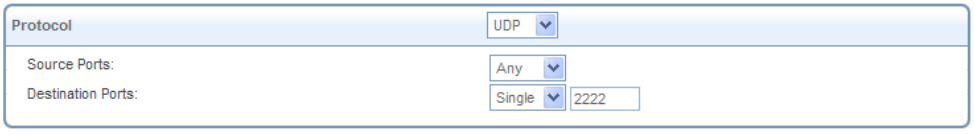


Figure 5.20 Edit Service Server Ports

6. Click ‘OK’ to save the settings.

7. Back in the ‘Edit Port Triggering Rule’ screen (see Figure 5.18), click the ‘New Opened Ports’ link. The ‘Edit Service Opened Ports’ screen appears.

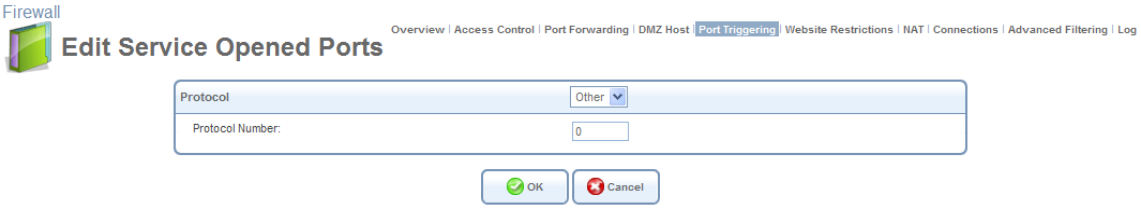


Figure 5.21 Edit Service Opened Ports

8. Select UDP as the protocol, leave the source port at “Any”, and enter a 3333 as the single destination port.

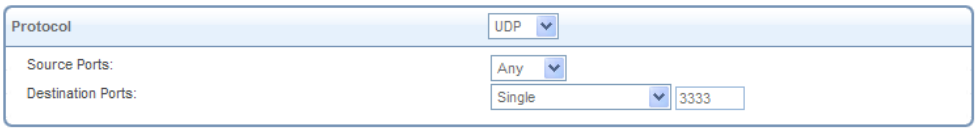


Figure 5.22 Edit Service Opened Ports

9. Click ‘OK’ to save the settings. The ‘Edit Port Triggering Rule’ screen will present your entered information. Click ‘OK’ again to save the port triggering rule. The ‘Port Triggering’ screen will now include the new port triggering entry.

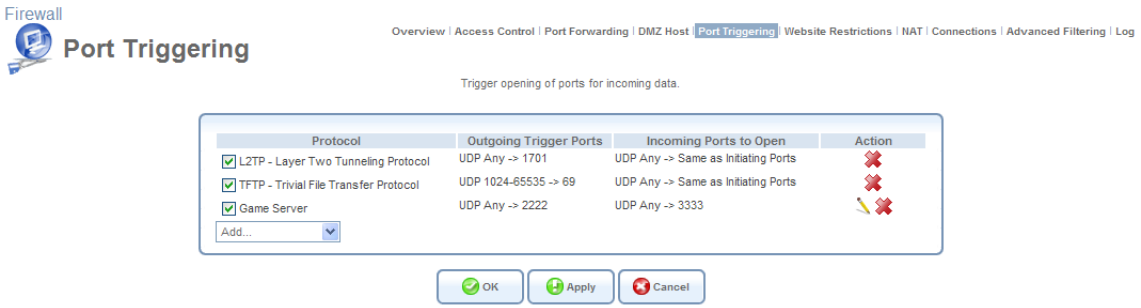


Figure 5.23 New Port Triggering Rule

This will result in accepting the inbound traffic from the gaming server, and sending it back to the LAN Host which originated the outgoing traffic to UDP port 2222.

- To temporarily disable a rule, clear the check box next to the service name.
- To reinstate it at a later time, simply reselect the check box.
- To remove a rule, click the service’s action icon. The service will be permanently removed.

Note: There may be a few default port triggering rules listed when you first access the port triggering screen. Disabling these rules may result in impaired gateway functionality.

5.2.6 Restricting Web Access

You can configure iPECS SBG-1000 to block specific websites so that they cannot be accessed from computers in the home network. Moreover, restrictions can be applied according to a comprehensive and automatically updated list of sites to which access is not recommended.

- To block access to a website:
  1. Click the ‘Website Restrictions’ link under the ‘Firewall’ menu item.

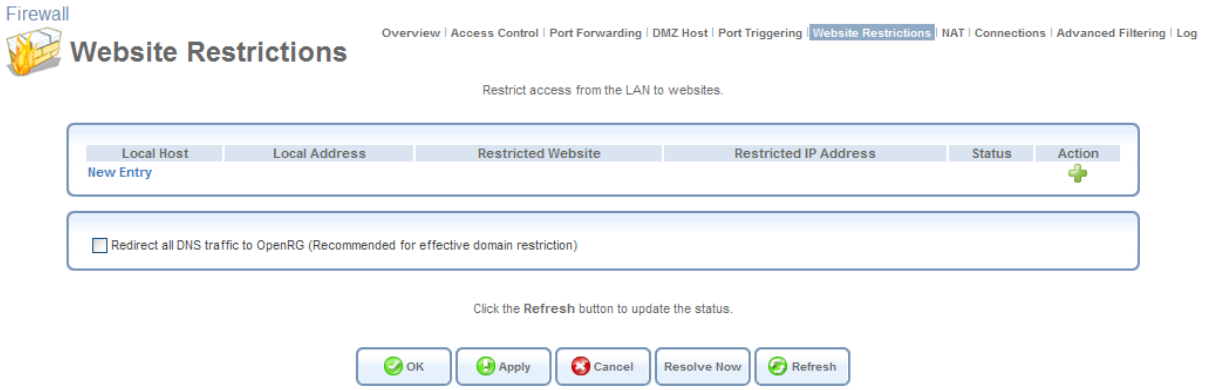


Figure 5.24 Website Restrictions

  2. Click the ‘New Entry’ link. The ‘Restricted Website’ screen appears.

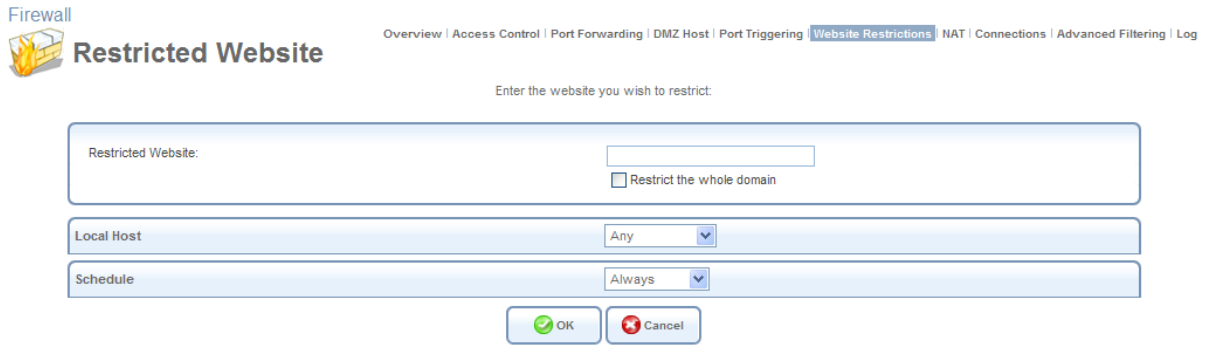


Figure 5.25 Restricted Website

  3. Enter the URL (or part of the URL) that you would like to make inaccessible from your home network (all web pages within this URL will also be blocked). If the URL has multiple IP addresses, iPECS SBG-1000 will resolve all additional addresses and automatically add them to the restrictions table.
  4. The ‘Local Host’ drop-down menu provides you with the ability to specify the computer or group of computers on which you would like to apply the website restriction. Select an address or a name from the list to apply the rule on the corresponding host, or ‘Any’ to apply the rule on all iPECS SBG-1000’s LAN hosts. If you would like to add a new address, select the ‘User Defined’ option in the drop-down menu. This will commence a sequence that will add a new Network Object, representing the new host. Refer to Section 6.9.2 in order to learn how to do so.
  5. By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting ‘User Defined’ from the ‘Schedule’ drop-down

menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

6. Click 'OK' to save the settings. You will be returned to the previous screen, while iPECS SBG-1000 attempts to find the site. 'Resolving...' will appear in the 'Status' column while the site is being located (the URL is 'resolved' into one or more IP addresses).
7. Click the 'Refresh' button to update the status if necessary. If the site is successfully located, then 'Resolved' will appear in the status bar. Otherwise, 'Hostname Resolution Failed' will appear. In case iPECS SBG-1000 fails to locate the website, perform the following:

    a. Use a web browser to verify that the website is available. If it is, then you probably entered the website address incorrectly.

    b. If the website is not available, return to the 'Website Restrictions' screen at a later time and click the 'Resolve Now' button to verify that the website can be found and blocked by iPECS SBG-1000.

You may edit the website restriction by modifying its entry under the 'Local Host' column in the 'Website Restrictions' screen.

- To modify an entry:

    1. Click the  action icon for the restriction. The 'Restricted Website' screen appears (see Figure 5.25). Modify the website address, group or schedule as necessary.
    2. Click the 'OK' button to save your changes and return to the 'Website Restrictions' screen.
- To ensure that all current IP addresses corresponding to the restricted websites are blocked, click the 'Resolve Now' button. iPECS SBG-1000 will check each of the restricted website addresses and ensure that all IP addresses at which this website can be found are included in the IP addresses column.

You can disable a restriction in order to make a website available again without having to remove it from the 'Website Restrictions' screen. This may be useful if you wish to make the website available only temporarily, intending to block it again in the future.

- To temporarily disable a rule, clear the check box next to the service name.
- To reinstate it at a later time, simply reselect the check box.
- To remove a rule, click the service's action icon. The service will be permanently removed.

5.2.7 Using iPECS SBG-1000's Network Address and Port Translation

iPECS SBG-1000 features a configurable Network Address Translation (NAT) and Network Address Port Translation (NAPT) mechanism, allowing you to control the network addresses and ports set in packets routed through your gateway. When enabling multiple computers on your network to access the Internet using a fixed number of public IP addresses, you can statically

define which LAN IP address will be translated to which NAT IP address and/or ports.
By default, iPECS SBG-1000 operates in NAPT routing mode (refer to Section 6.4.6.4.3). However, you can control your network translation by defining static NAT/NAPT rules. Such rules map LAN computers to NAT IP addresses. The NAT/NAPT mechanism is useful for managing Internet usage in your LAN, or complying with various application demands. For example, you can assign your primary LAN computer a single NAT IP address, in order to assure its permanent connection to the Internet. Another example is when an application server to which you would like to connect, such as a security server, requires that packets have a specific IP address—you can define a NAT rule for that address.

5.2.7.1 Configuring the NAT

Click the 'NAT' link under the 'Firewall' menu item. The 'NAT' screen appears.

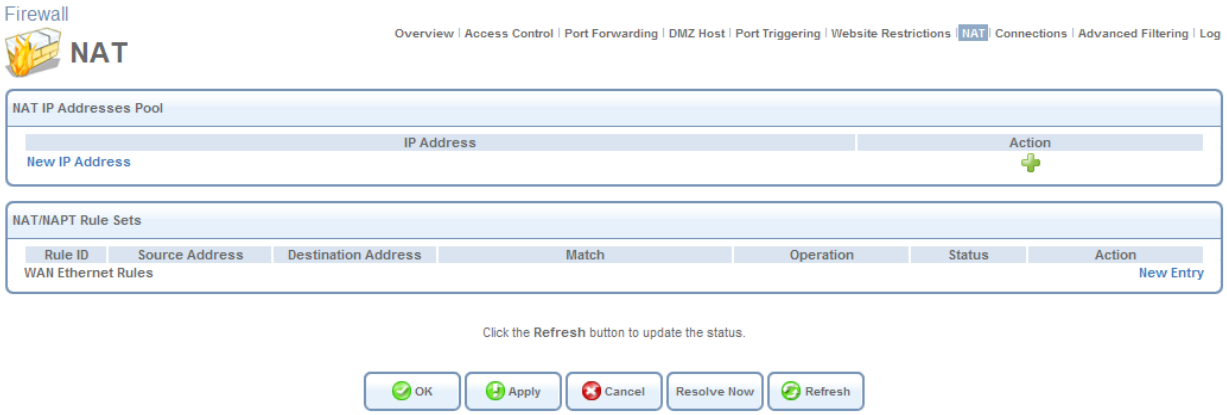


Figure 5.26 Network Address Translation

Before configuring NAT/NAPT rules, you must first enter the additional public IP addresses obtained from your ISP as your NAT IP addresses, in the 'NAT IP Addresses Pool' section.

Note: The primary IP address used by the WAN device for dynamic NAPT should not be added to this table.

To add a NAT IP address, perform the following:

1. Click the 'New IP Address' link. The 'Edit Item' screen appears.

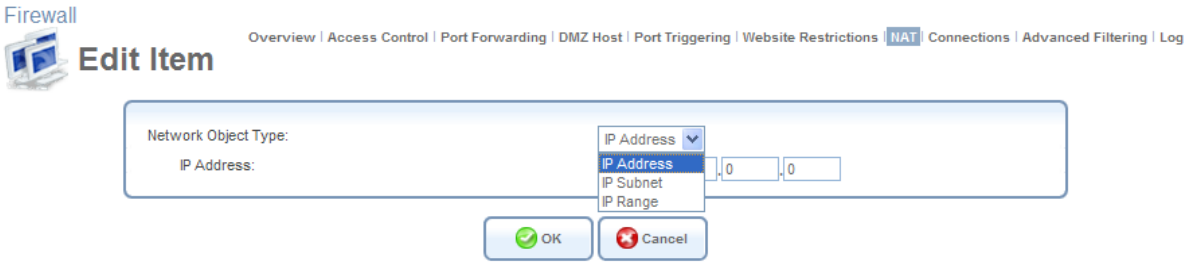


Figure 5.27 Edit Item

2. To add a single public address, select the ‘IP Address’ option from the ‘Network Object Type’ drop-down menu, and enter the IP in the fields that appear.

Figure 5.28 Edit Item

To add a range of public IP addresses, select the ‘IP Range’ option and enter the available IP range.

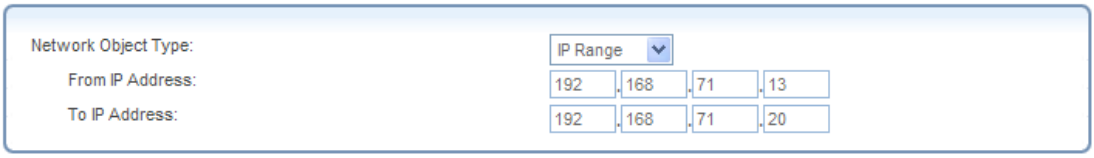


Figure 5.29 Edit Item

3. Click ‘OK’ to save the settings. The new IP addresses are displayed in the ‘NAT IP Addresses Pool’ section.

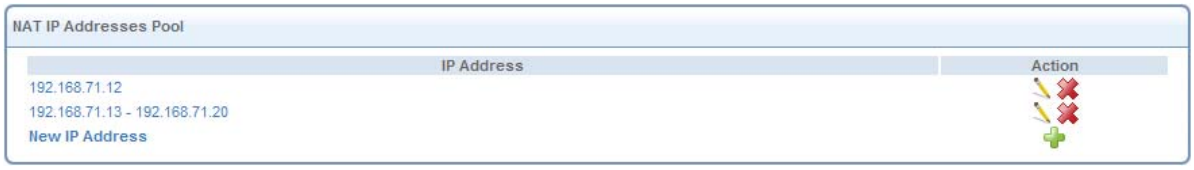


Figure 5.30 NAT IP Addresses

To add a new NAT/NAPT rule, click the ‘New Entry’ link in the ‘NAT/NAPT Rule Sets’ section of the ‘NAT’ screen. The ‘Add NAT/NAPT Rule’ screen appears.

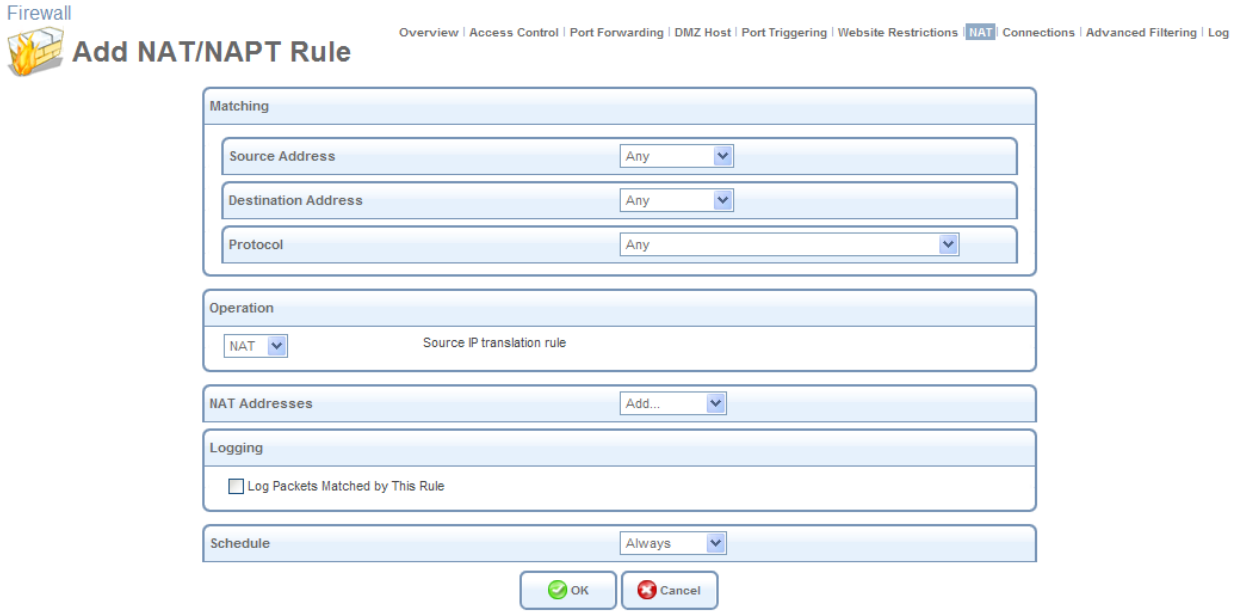


Figure 5.31 Add NAT/NAPT Rule

Matching Use this section to define characteristics of the packets matching the rule.

- **Source Address** The source address of packets sent or received by iPECS SBG-1000. Use this drop-down menu to specify a LAN computer or a group of LAN computers on which you would like to apply the rule. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on all iPECS SBG-1000's LAN hosts. If you would like to add a new address, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new Network Object, representing the new host. Refer to Section 6.9.2 in order to learn how to do so.

- **Destination Address** The destination address of packets sent or received by iPECS SBG-1000. This address can be configured in the same manner as the source address. For example, use this drop-down menu to specify an IP address of a remote application server (such as a security server), which requires that the incoming packets have a specific IP address (e.g., one of those defined in your NAT IP address pool).

- **Protocol** You may also specify a traffic protocol. Selecting the 'Show All Services' option from the drop-down menu expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option. This will commence a sequence that will add a new Service, representing the protocol. Refer to Section 6.9.2 in order to learn how to do so.

Operation Use this section to define the operation that will be applied on the IP addresses matching the criteria defined above. The operations available are NAT or NAPT. Selecting each from the drop-down menu refreshes the screen accordingly.

- **NAT Addresses**

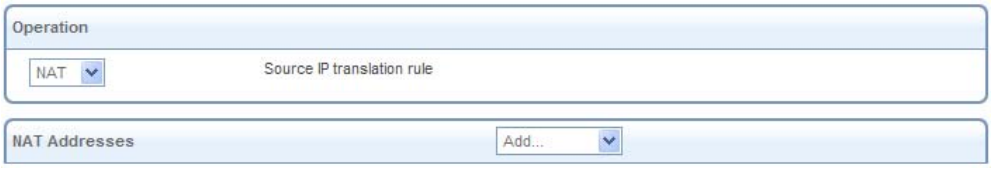


Figure 5.32 Add NAT Rule

This drop-down menu displays all of your available NAT addresses/ranges, from which you can select an entry. If you would like to add a single address or a sub-range from the given pool/range, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new Network Object, representing the new host. Refer to Section 6.9.2 in order to learn how to do so.

- **NAPT Address**

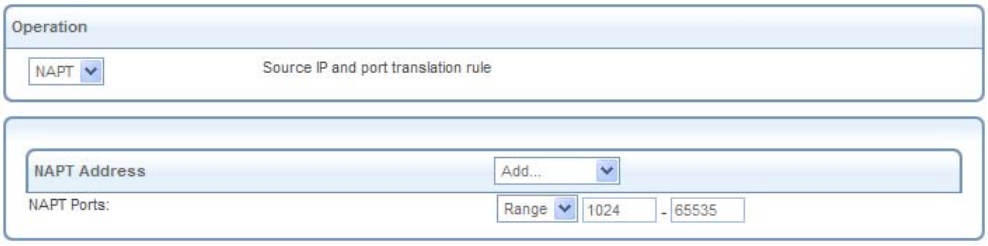


Figure 5.33 Add NAPT Rule

This drop-down menu displays all of your available NAPT addresses/ranges, from which you can select an entry. If you would like to add a single address or a sub-range from the given pool/range, select the 'User Defined' option from the drop-down menu. This will commence a sequence that will add a new Network Object, representing the new host. Refer to Section 6.9.2 in order to learn how to do so. Note, however, that in this case the network object may only be an IP address, as NAPT is port-specific.

- **NAPT Ports** Specify the port(s) for the IP address into which the original IP address will be translated. Enter a single port or select 'Range' in the drop-down menu. The screen refreshes, enabling you to enter a range of ports.

Figure 5.34 Add NAPT Rule

Logging Monitor the rule.

- **Log Packets Matched by This Rule** Select this check box to log the first packet from a connection that was matched by this rule.

Schedule By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting 'User Defined' from the 'Schedule' drop-down menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

5.2.8 Configuring the Advanced Filtering Mechanism

Advanced filtering is designed to allow comprehensive control over the firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN devices.
To view iPECS SBG-1000's advanced filtering options, click the 'Advanced Filtering' link of the 'Firewall' menu item. The 'Advanced Filtering' screen appears.

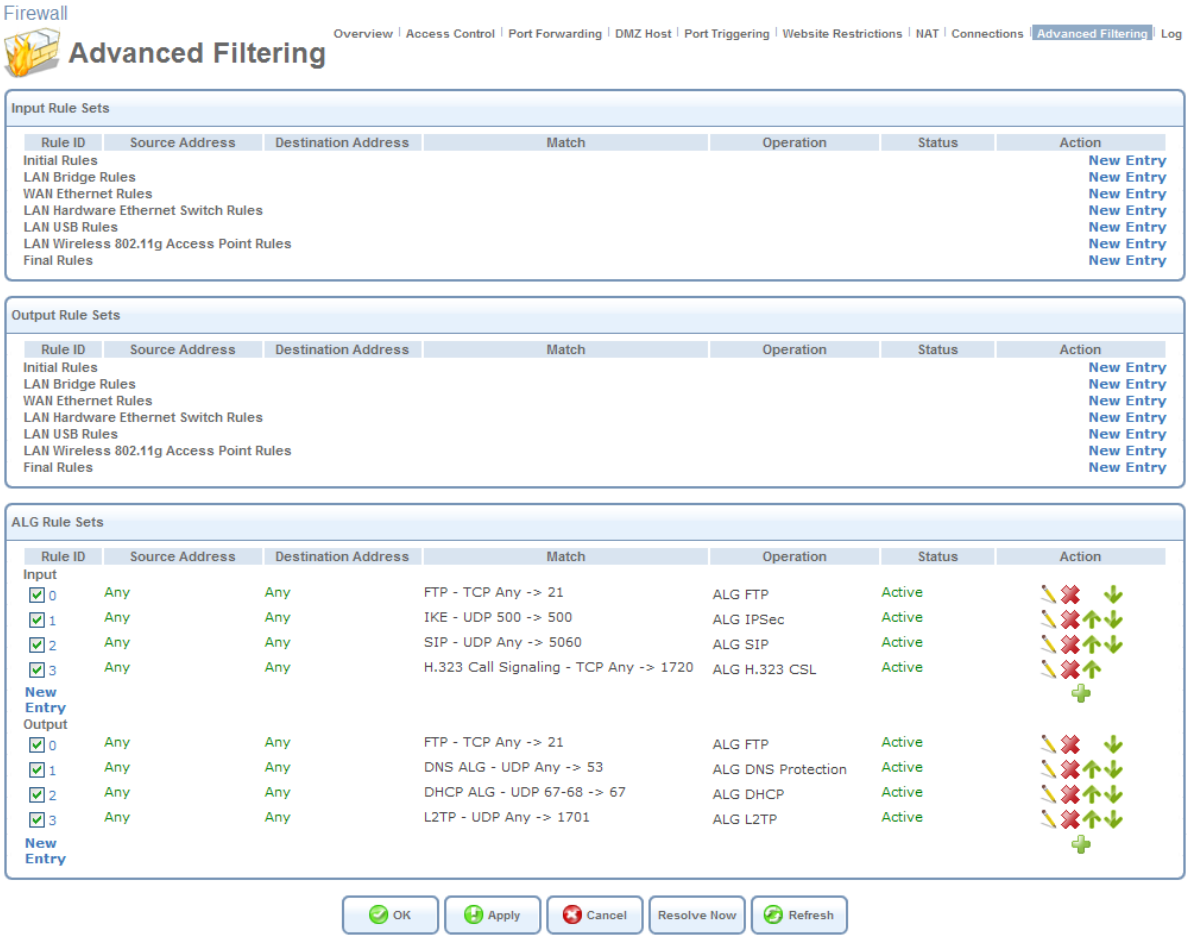


Figure 5.35 Advanced Filtering

5.2.8.1 Adding Input and Output Rules

The first two sections of the ‘Advanced Filtering’ screen—’Input Rule Sets’ and ‘Output Rule Sets’, are designed for configuring inbound and outbound traffic respectively. Each section is comprised of subsets, which can be grouped into three main subjects:

- Initial rules – rules defined here will be applied first, on all gateway devices.
- Network devices rules – rules can be defined per each gateway device.
- Final rules – rules defined here will be applied last, on all gateway devices.

There are numerous rules that are automatically created by the firewall in order to provide improved security and block harmful attacks.
To add an advanced filtering rule, first choose the traffic direction and the device on which to set the rule. Then click the appropriate ‘New Entry’ link. The ‘Add Advanced Filter’ screen appears.

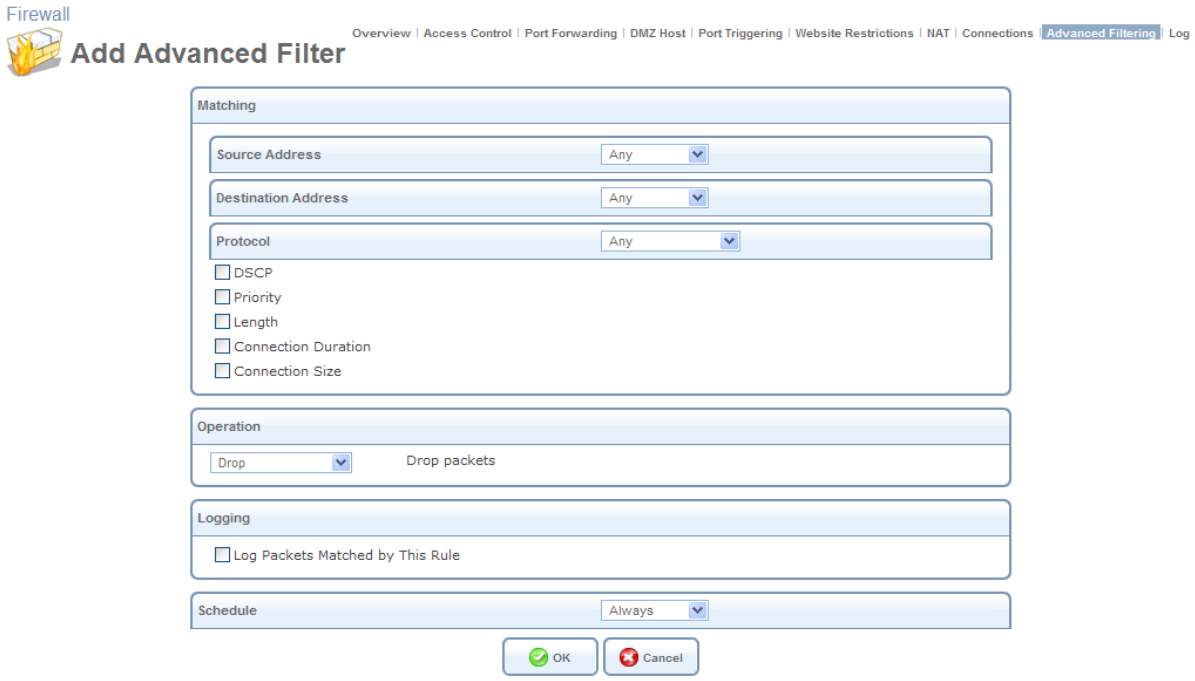


Figure 5.36 Add Advanced Filter

The ‘Matching’ and ‘Operation’ sections of this screen define the operation to be executed when matching conditions apply.

Matching Use this section to define characteristics of the packets matching the rule.

- **Source Address** The source address of packets sent or received by iPECS SBG-1000. Use this drop-down menu to specify the computer or group of computers on which you would like to apply the rule. Select an address or a name from the list to apply the rule on the corresponding host, or ‘Any’ to apply the rule on any host trying to send data. If you would like to add a new address, select the ‘User Defined’ option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to Section 6.9.2 in order to learn how to do so.

- **Destination Address** The destination address of packets sent or received by iPECS SBG-1000. This address can be configured in the same manner as the source address. For example, use this drop-down menu to specify an IP address of a remote application server (such as a security server), which requires that the incoming packets have a specific IP address (e.g., one of those defined in your NAT IP address pool).

- **Protocol** You may also specify a traffic protocol. Selecting the ‘Show All Services’ option from the drop-down menu expands the list of available protocols. Select a protocol or add a new one using the ‘User Defined’ option. This will commence a sequence that will add a new Service, representing the protocol. Refer to Section 6.9.2 in order to learn how to do so.

- **DSCP** Select this check box to display two DSCP fields, which enable you to specify a hexadecimal DSCP value and its mask assigned to the packets matching the priority rule.

For more information, refer to Section 5.3.5.

- **Priority** Select this check box to display a drop-down menu, in which you can select a priority level assigned to the packets matching the priority rule. For more information, refer to Section 5.3.3.

- **Length** Select this check box if you would like to specify the length of packets, or the length of their data portion.

- **Connection Duration** Select this check box to apply the filtering rule only on connections which are open for a certain time period. After selecting the check box, choose whether the duration of connections matching the rule should be greater or less than the time that you specify in the adjacent field.

Figure 5.37 Connection Duration

- **Connection Size** Select this check box to apply the filtering rule only on connections matching a certain data size limit. This option is best used along with the 'Connection Duration' option, enabling you to fine-tune the filtering mechanism according to your needs. After selecting the check box, choose whether the connection's data size should be greater or less than the number of kilobytes that you specify in the adjacent field.

Figure 5.38 Connection Size

Operation Define what action the rule will take, by selecting one of the following radio buttons:

- **Drop** Deny access to packets that match the source and destination IP addresses and service ports defined above.

- **Reject** Deny access to packets that match the criteria defined, and send an ICMP error or a TCP reset to the origination peer.

- **Accept Connection** Allow access to packets that match the criteria defined. The data transfer session will be handled using Stateful Packet Inspection (SPI), meaning that other packets matching this rule will be automatically allowed access.

- **Accept Packet** Allow access to packets that match the criteria defined. The data transfer session will not be handled using SPI, meaning that other packets matching this rule will not be automatically allowed access. This can be useful, for example, when creating rules that allow broadcasting.

Logging Monitor the rule.

- **Log Packets Matched by This Rule** Select this check box to log the first packet from a connection that was matched by this rule.

Schedule By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting 'User Defined' from the 'Schedule' drop-down menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.
The order of the rules' appearance represents both the order in which they were defined and the sequence by which they will be applied. You may change this order after your rules are already defined (without having to delete and then re-add them), by using the action icon and action icon.

Figure 5.39 Move Up and Move Down Action Icons

5.2.8.2 Adding ALG Rules

The 'ALG Rule Sets' section enables you to define address and port processing rules for certain application protocols (such as, FTP, TFTP, SIP, and others), which carry the IP address inside the application data. Most of these protocols will not work with the NAT, unless the NAT is aware of them and does the appropriate translation.
The NAT is application independent, therefore a specific Application Level Gateway (ALG) is required to perform payload monitoring and needed alterations to allow the application's traffic to pass through the firewall. The 'Input' and 'Output' subsections of the 'ALG Rule Sets' feature (see Figure 5.35) are designated to display ALG rules for inbound and outbound traffic respectively. Note that iPECS SBG-1000 is automatically configured with ALG rules for several widespread protocols. You can edit a rule by clicking its respective action icon, or remove it by clicking the action icon.

To create an ALG rule, either inbound or outbound, click the 'New Entry' link that corresponds to the rule type you would like to define. The 'Add ALG Rule' screen appears.

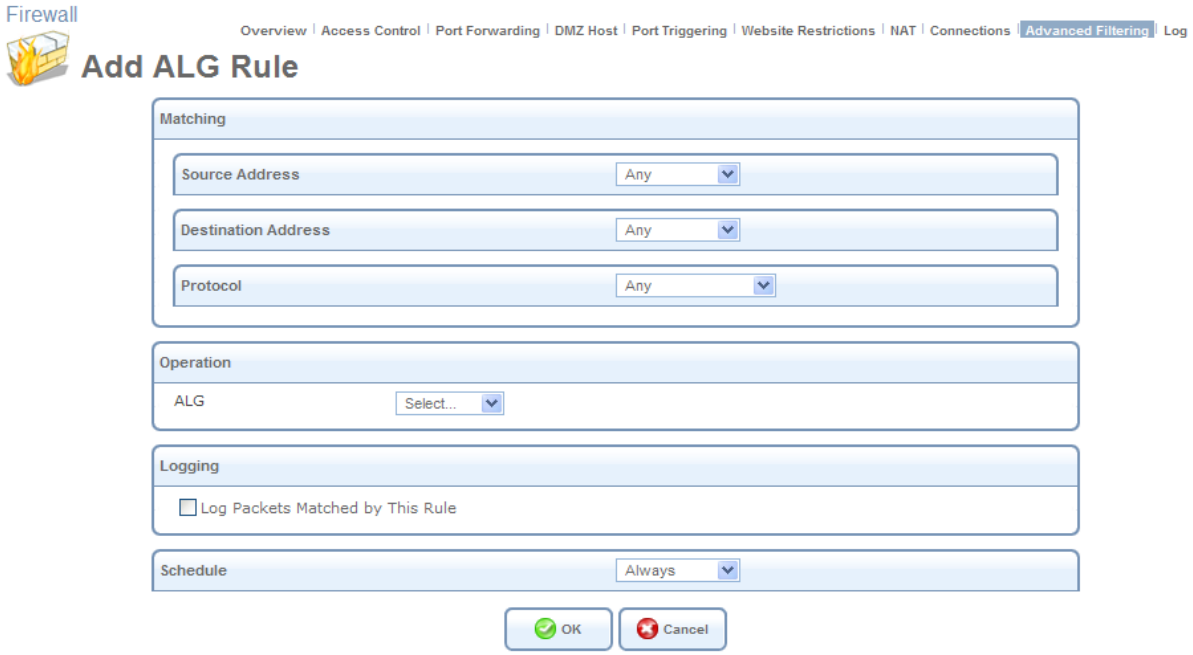


Figure 5.40 Add ALG Rule

The 'Matching' and 'Operation' sections of this screen define the operation to be executed when matching conditions apply.

Matching Use this section to define characteristics of the packets matching the rule.

- **Source Address** The source address of packets sent or received by iPECS SBG-1000. Use this drop-down menu to specify the computer or group of computers on which you would like to apply the rule. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on any host trying to send data. If you would like to add a new address, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new Network Object, representing the new host. Refer to Section 6.9.2 in order to learn how to do so.

- **Destination Address** The destination address of packets sent or received by iPECS SBG-1000. This address can be configured in the same manner as the source address. For example, use this drop-down menu to specify an IP address of a remote application server (such as a security server), which requires that the incoming packets have a specific IP address (e.g., one of those defined in your NAT IP address pool).

- **Protocol** You may also specify a traffic protocol. Selecting the 'Show All Services' option from the drop-down menu expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option. This will commence a sequence that will add a new Service, representing the protocol. Refer to Section 6.9.2 in order to learn how to do so.

Operation Define which ALG will be used, by selecting one from the designated drop-down menu.

Logging Monitor the rule.

- **Log Packets Matched by This Rule** Select this check box to log the first packet from a connection that was matched by this rule.

- **Schedule** By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting 'User Defined' from the 'Schedule' drop-down menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Note: The defined ALG rule will also be applied to the child processes of the application that utilizes the selected protocol.

The order of the rules' appearance represents both the order in which they were defined and the sequence by which they will be applied. You may change this order after your rules are already defined (without having to delete and then re-add them), by using the action icon and action icon.

5.2.9 Viewing the Firewall Log

The 'Firewall Log' screen displays a list of firewall-related events, including attempts to establish inbound and outbound connections, attempts to authenticate through an administrative interface (WBM or Telnet terminal), firewall configuration and system start-up.

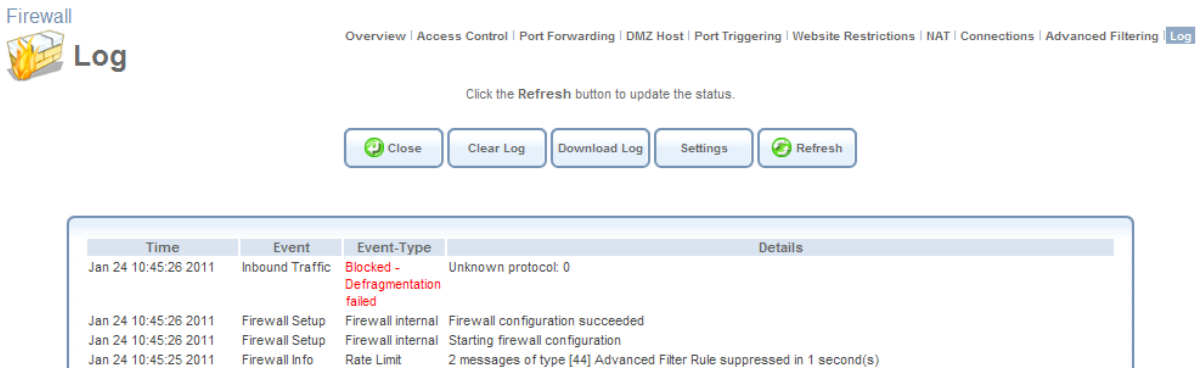


Figure 5.41 Firewall Log

The log's columns are:

Time The time the event occurred.

Event There are five kinds of events:

- Inbound Traffic: The event is a result of an incoming packet.
- Outbound Traffic: The event is a result of outgoing packet.
- Firewall Setup: Configuration message.
- WBM Login: Indicates that a user has logged in to WBM.

- CLI Login: Indicates that a user has logged in to CLI (via Telnet).

Event-Type A textual description of the event:
- Blocked: The packet was blocked. The message is colored red.
- Accepted: The packet was accepted. The message is colored green.

Details More details about the packet or the event, such as protocol, IP addresses, ports, etc.
Use the buttons at the top of the page to:

Close Close the 'Log' screen and return to iPECS SBG-1000's home page.

Clear Log Clear all currently displayed log messages.

Download Log Download the log as a Comma Separated Value (CSV) file, named **firewall.csv**.

Settings View or change the security log settings (explanation follows).

Refresh Refresh the screen to display the latest updated log messages.
To view or change the security log settings:

1. Click the 'Settings' button that appears at the top of the 'Firewall Log' screen. The 'Log Settings' screen appears.

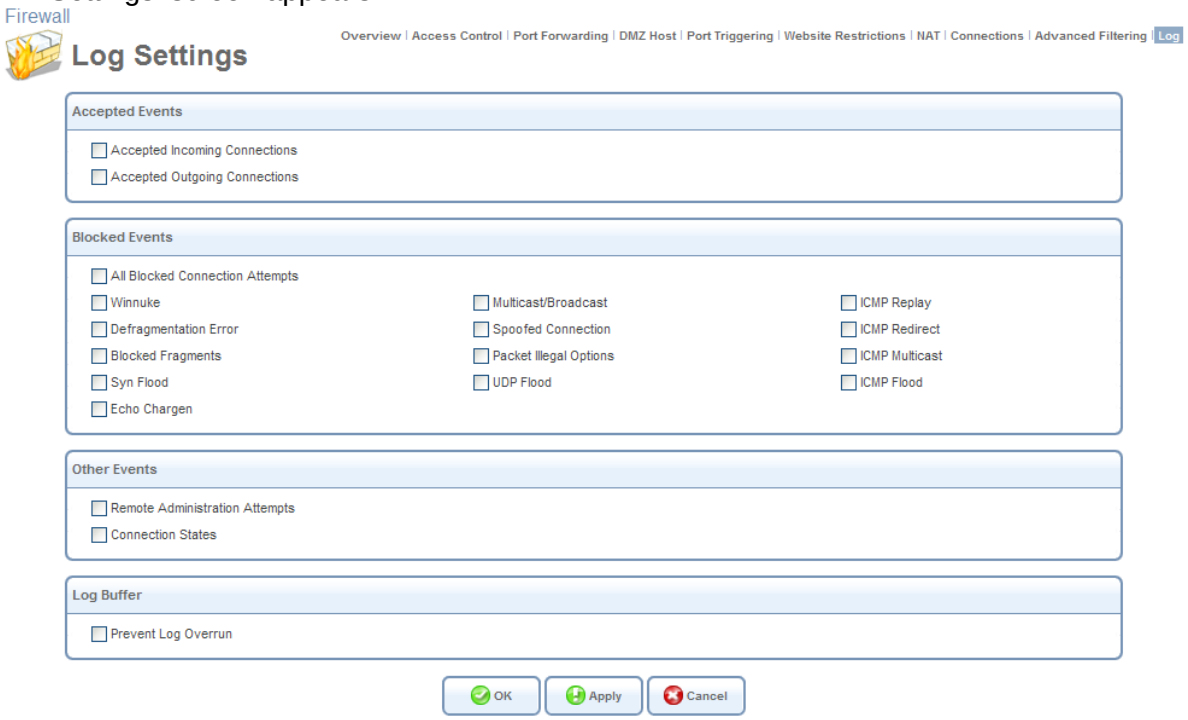


Figure 5.42 Log Settings

2. Select the types of activities for which you would like to have a log message generated

- Accepted Events
  Accepted Incoming Connections Write a log message for each successful attempt to

establish an inbound connection to the home network.
Accepted Outgoing Connections Write a log message for each successful attempt to establish an outgoing connection to the public network.

- Blocked Events
  All Blocked Connection Attempts Write a log message for each blocked attempt to establish an inbound connection to the home network or vice versa. You can enable logging of blocked packets of specific types by disabling this option, and enabling some of the more specific options below it.
  Specific Events Specify the blocked events that should be monitored. Use this to monitor specific event such as SynFlood. A log message will be generated if either the corresponding check box is selected, or the “All Blocked Connection Attempts” check box is selected.

- Other Events
  Remote Administration Attempts Write a log message for each remote administration connection attempt, whether successful or not.
  Connection States Provide extra information about every change in a connection opened by the firewall. Use this option to track connection handling by the firewall and Application Level Gateways (ALGs).

- Log Buffer
  Prevent Log Overrun Select this check box in order to stop logging firewall activities when the memory allocated for the log fills up.

3. Click ‘OK’ to save the settings.

5.2.9.1 The Firewall Event Types

The following are the available event types that can be recorded in the firewall log:

1. Firewall internal – an accompanying explanation from the firewall internal mechanism will be added in case this event–type is recorded.

2. Firewall status changed – the firewall changed status from up to down or the other way around, as specified in the event type description.

3. STP packet – an STP packet has been accepted/rejected.

4. Illegal packet options – the options field in the packet’s header is either illegal or forbidden.

5. Fragmented packet – a fragment has been rejected.

6. WinNuke protection – a WinNuke attack has been blocked.

7. ICMP replay – an ICMP replay message has been blocked.
8. ICMP redirect protection – an ICMP redirected message has been blocked.
9. Packet invalid in connection – a packet has been blocked, being on an invalid connection.
10. ICMP protection – a broadcast ICMP message has been blocked.
11. Broadcast/Multicast protection – a packet with a broadcast/multicast source IP has been blocked.
12. Spoofing protection – a packet from the WAN with a source IP of the LAN has been blocked.
13. DMZ network packet – a packet from a demilitarized zone network has been blocked.
14. Trusted device – a packet from a trusted device has been accepted.
15. Default policy – a packet has been accepted/blocked according to the default policy.
16. Remote administration – a packet designated for iPECS SBG-1000 management has been accepted/blocked.
17. Access control – a packet has been accepted/blocked according to an access control rule.
18. Parental control – a packet has been blocked according to a parental control rule.
19. NAT out failed – NAT failed for this packet.
20. DHCP request – iPECS SBG-1000 sent a DHCP request (depends on the distribution).
21. DHCP response – iPECS SBG-1000 received a DHCP response (depends on the distribution).
22. DHCP relay agent – a DHCP relay packet has been received (depends on the distribution).
23. IGMP packet – an IGMP packet has been accepted.
24. Multicast IGMP connection – a multicast packet has been accepted.
25. RIP packet – a RIP packet has been accepted.
26. PPTP connection – a packet inquiring whether iPECS SBG-1000 is ready to receive a PPTP connection has been accepted.

27. Kerberos key management 1293 – security related, for future use.

28. Kerberos 88 – for future use.

29. AUTH:113 request – an outbound packet for AUTH protocol has been accepted (for maximum security level).

30. Packet-Cable – for future use.

31. IPV6 over IPV4 – an IPv6 over IPv4 packet has been accepted.

32. ARP – an ARP packet has been accepted.

33. PPP Discover – a PPP discover packet has been accepted.

34. PPP Session – a PPP session packet has been accepted.

35. 802.1Q – a 802.1Q (VLAN) packet has been accepted.

36. Outbound Auth1X – an outbound Auth1X packet has been accepted.

37. IP Version 6 – an IPv6 packet has been accepted.

38. iPECS SBG-1000 initiated traffic – all traffic that iPECS SBG-1000 initiates is recorded.

39. Maximum security enabled service – a packet has been accepted because it belongs to a permitted service in the maximum security level.

40. SynCookies Protection – a SynCookies packet has been blocked.

41. ICMP Flood Protection – a packet has been blocked, stopping an ICMP flood.

42. UDP Flood Protection – a packet has been blocked, stopping a UDP flood.

43. Service – a packet has been accepted because of a certain service, as specified in the event type.

44. Advanced Filter Rule – a packet has been accepted/blocked because of an advanced filter rule.

45. Fragmented packet, header too small – a packet has been blocked because after the defragmentation, the header was too small.

46. Fragmented packet, header too big – a packet has been blocked because after the defragmentation, the header was too big.

47. Fragmented packet, drop all – not used.

48. Fragmented packet, bad align – a packet has been blocked because after the defragmentation, the packet was badly aligned.

49. Fragmented packet, packet too big – a packet has been blocked because after the defragmentation, the packet was too big.

50. Fragmented packet, packet exceeds – a packet has been blocked because defragmentation found more fragments than allowed.

51. Fragmented packet, no memory – a fragmented packet has been blocked because there was no memory for fragments.

52. Fragmented packet, overlapped – a packet has been blocked because after the defragmentation, there were overlapping fragments.

53. Defragmentation failed – the fragment has been stored in memory and blocked until all fragments arrived and defragmentation could be performed.
54. Connection opened – usually a debug message regarding a connection.

55. Wildcard connection opened – usually a debug message regarding a connection.

56. Wildcard connection hooked – usually debug message regarding connection.

57. Connection closed – usually a debug message regarding a connection.

58. Echo/Chargen/Quote/Snork protection – a packet has been blocked, protecting from Echo/Chargen/Quote/Snork.

59. First packet in connection is not a SYN packet – a packet has been blocked because of a TCP connection that had started without a SYN packet.

60. Error: No memory – a message notifying that a new connection has not been established because of lack of memory.

61. NAT Error: Connection pool is full – a message notifying that a connection has not been created because the connection pool is full.

62. NAT Error: No free NAT IP – a message notifying that there is no free NAT IP, therefore NAT has failed.

63. NAT Error: Conflict Mapping already exists – a message notifying that there is a conflict since the NAT mapping already exists, therefore NAT has failed.

64. Malformed packet: Failed parsing – a packet has been blocked because it is malformed.

65. Passive attack on ftp-server: Client attempted to open Server ports – a packet has been blocked because of an unauthorized attempt to open a server port.

66. FTP port request to 3rd party is forbidden (Possible bounce attack) – a packet has been blocked because of an unauthorized FTP port request.

67. Firewall Rules were changed – the firewall rule set has been modified.

68. User authentication – a message during login time, including both successful and failed authentication.

69. First packet is Invalid – first packet in connection failed to pass firewall or NAT.

5.3 Managing Your Bandwidth with Quality of Service

Network-based applications and traffic are growing at a high rate, producing an ever-increasing demand for bandwidth and network capacity. For obvious reasons, bandwidth and capacity cannot be expanded infinitely, requiring that bandwidth-demanding services be delivered over existing infrastructure, without incurring additional, expansive investments.

The next logical means of ensuring optimal use of existing resources are Quality of Service (QoS) mechanisms for congestion management and avoidance. Quality of Service refers to the capability of a network device to provide better service to selected network traffic. This is achieved by shaping the traffic and processing higher priority traffic before lower priority traffic.

As Quality of Service is dependent on the “weakest link in the chain”, failure of but a single component along the data path to assure priority packet transmission can easily cause a VoIP call or a Video on Demand (VoD) broadcast to fail miserably. QoS must therefore obviously be addressed end-to-end.

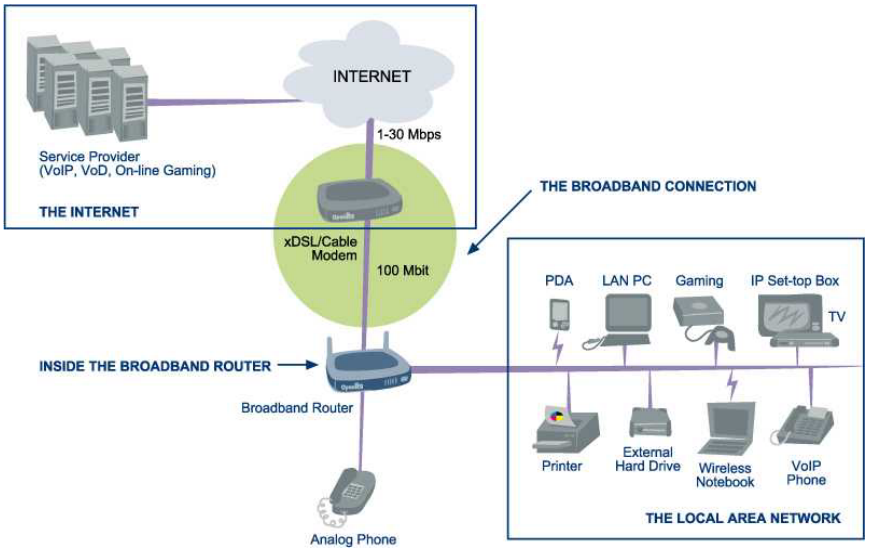


Figure 5.43 End-to-end QoS Challenge Areas

The following are the potential bottleneck areas that need be taken into consideration when implementing an end-to-end QoS-enabled service.

- **The Local Area Network** LANs have finite bandwidth, and are typically limited to 100 Mbps. When given the chance, some applications will consume all available network bandwidth. In business networks, a large number of network-attached devices can lead to congestion. The need for QoS mechanisms is more apparent in wireless LANs (802.11b/g/n), where bandwidth is even more limited (typically no more than 20 Mbps on 802.11g networks).
- **The Broadband Router** All network traffic passes through and is processed by the broadband router. It is therefore a natural focal point for QoS implementation. Lack of sufficient buffer space, memory or processing power, and poor integration among system components can result in highly undesirable real-time service performance. The only way to assure high quality of service is the use of proper and tightly-integrated router operating system software and applications, which can most effectively handle multiple real-time services simultaneously.
- **The Broadband Connection** Typically the most significant bottleneck of the network, this is where the high speed LAN meets limited broadband bandwidth. Special QoS mechanisms must be built into routers to ensure that this sudden drop in connectivity speed is taken into account when prioritizing and transmitting real-time service-related data packets.
- **The Internet** Internet routers typically have a limited amount of memory and bandwidth available to them, so that congestions may easily occur when links are over-utilized, and routers attempt to queue packets and schedule them for retransmission. One must also consider the fact that while Internet backbone routers take some prioritization into account when making routing decisions, all data packets are treated equally under congested conditions.

The following figure depicts iPECS SBG-1000's QoS role and architecture in a network. Many of the terms it contains will become familiar as you read on.

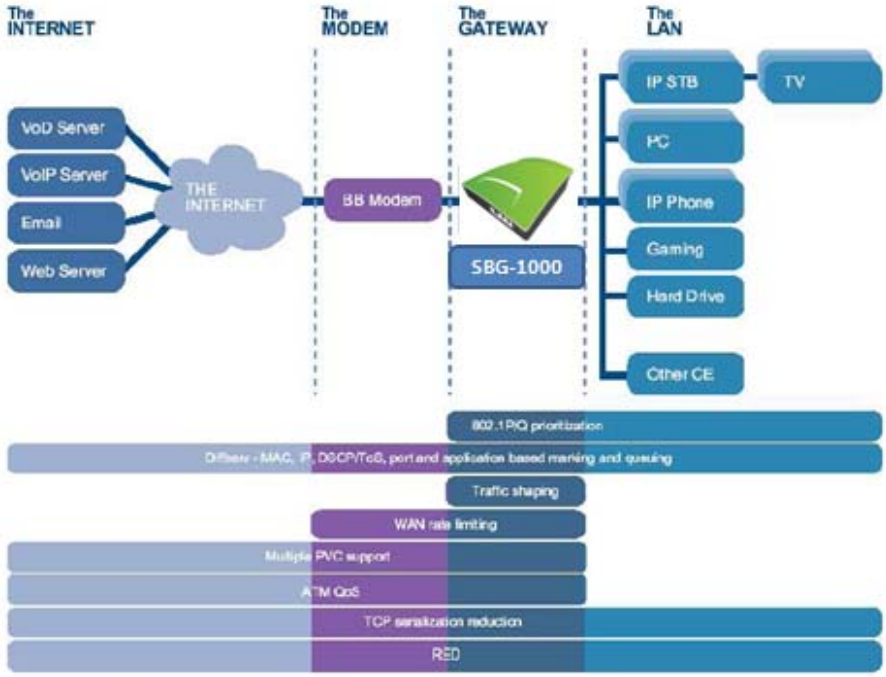


Figure 5.44 iPECS SBG-1000's QoS Architecture

5.3.1 Selecting a QoS Profile

The 'General' screen provides a Quality of Service "wizard", with which you can configure your QoS parameters according to predefined profiles, with just a few clicks. A chosen QoS profile will automatically define QoS rules, which you can view and edit in the rest of the QoS tab screens, described later.

Note: Selecting a QoS profile will cause all previous QoS configuration settings to be **permanently lost**.

Click the QoS tab under 'Services'. The 'General' screen appears with the 'Overview' link being selected.

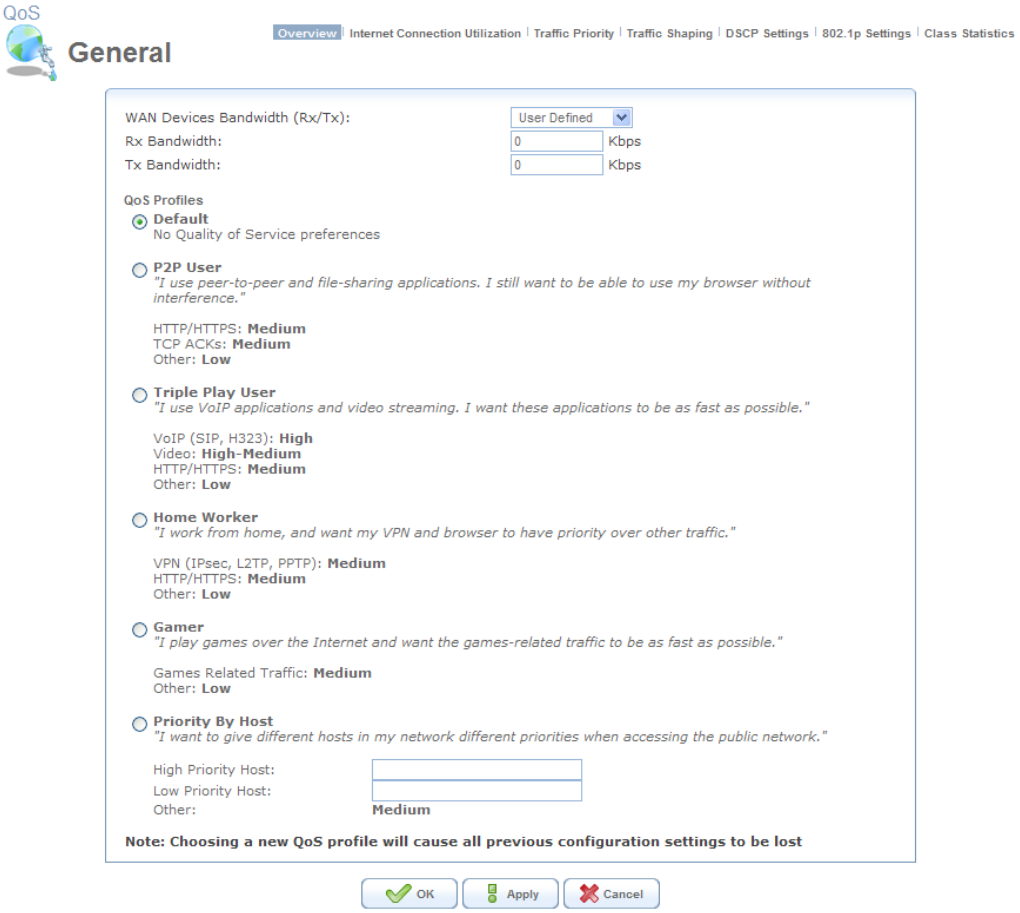


Figure 5.45 General

WAN Devices Bandwidth (Rx/Tx) Before selecting the QoS profile that mostly suits your needs, select your bandwidth from this drop-down menu. If you do not see an appropriate entry, select 'User Defined', and enter your Tx and Rx bandwidths manually.

- **Tx Bandwidth** This parameter defines the gateway's outbound transmission rate. Enter your Tx bandwidth in Kbits per second.
- **Rx Bandwidth** This parameter defines the gateway's Internet traffic reception rate. Enter your Rx bandwidth in Kbits per second.

Note: By default, these parameters are set to 0 Kbps, which means that the bandwidth has not been limited on iPECS SBG-1000. Entering inaccurate Tx/Rx values will cause incorrect behavior of the QoS module. It is important to set these values as accurately as possible.

If you wish to restore the default bandwidth settings, select 'Unlimited' from the drop-down menu, and click 'Apply'. Note that you can also set the desired bandwidth on the WAN (or any other) device in the 'Traffic Shaping' screen (to learn how to do so, refer to Section 5.3.4.1).

QoS Profiles Select the profile that mostly suits your bandwidth usage. Each profile entry displays a quote describing what the profile is best used for, and the QoS priority levels granted to

each bandwidth consumer in this profile.

- Default – No QoS profile, however the device is limited by the requested bandwidth, if specified.
- P2P User – Peer-to-peer and file sharing applications will receive priority.
- Triple Play User – VoIP and video streaming will receive priority.
- Home Worker – VPN and browsing will receive priority.
- Gamer – Game-related traffic will receive priority.
- Priority By Host – This entry provides the option to configure which computer in your LAN will receive the highest priority and which the lowest. If you have additional computers, they will receive medium priority.
  High Priority Host Enter the host name or IP address of the computer to which you would like to grant the highest bandwidth priority.
  Low Priority Host Enter the host name or IP address of the computer to which you would like to grant the lowest bandwidth priority.

5.3.2 Viewing Your Bandwidth Utilization

The 'Internet Connection Utilization' screen provides detailed real-time information regarding the usage of your Internet connection's bandwidth. At any time, you can view an up-to-date bandwidth usage report on both the application and computer level.

5.3.2.1 Application View

The 'Utilization by Application' table displays the following information fields. You can sort the table according to these fields (ascending or descending), by clicking the fields' names. Note that you can stop the screen's refreshing by using the 'Automatic Refresh Off' button at the bottom of the screen.

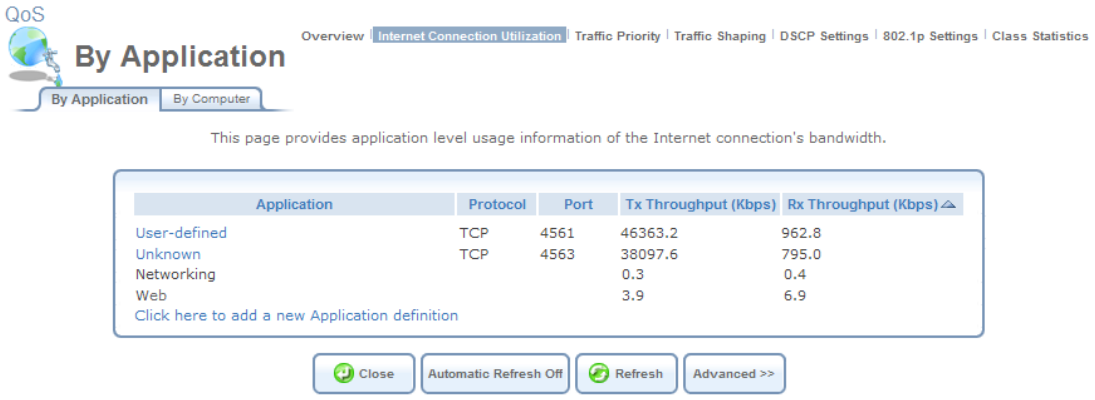


Figure 5.46 Utilization by Application

Application A list of categories of applications that are currently using the bandwidth. This section may also display user-defined or unknown applications that had not been identified by iPECS SBG-1000 as belonging to one of the pre-defined categories. In this case, their names will appear as links, which you can click to view their details.
Protocol The application's network protocol.
Port The port through which traffic is transferred.
Tx Throughput The transmission bit rate in kilo-bits per second.
Rx Throughput The reception bit rate in kilo-bits per second.
iPECS SBG-1000 does not recognize all possible applications running on LAN computers, and marks such an application as "Unknown". You can define an unknown application by clicking the 'Click Here to Add a New Application Definition' link at the bottom of the table. The 'Protocols' screen appears, in which you can define the application by adding it as a new service entry. To learn more about adding protocols, refer to Section 6.9.1.

To view the applications that underlie the displayed categories, click the 'Advanced' button.

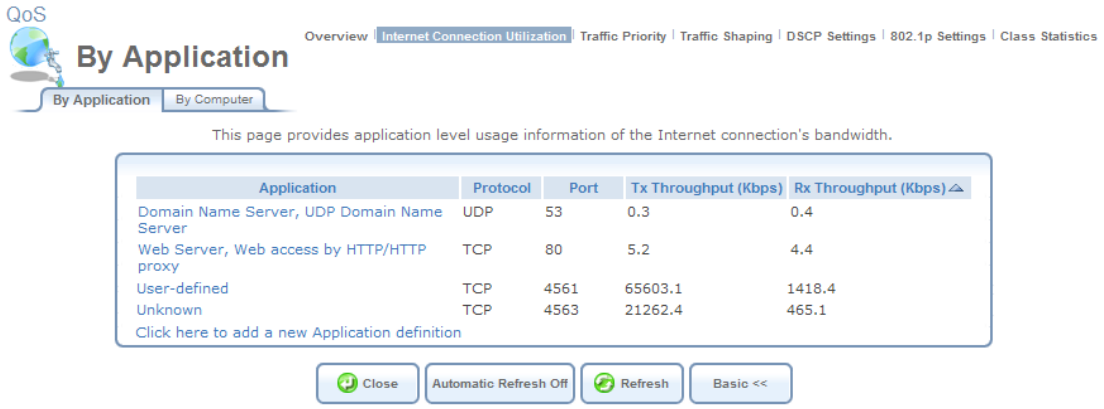
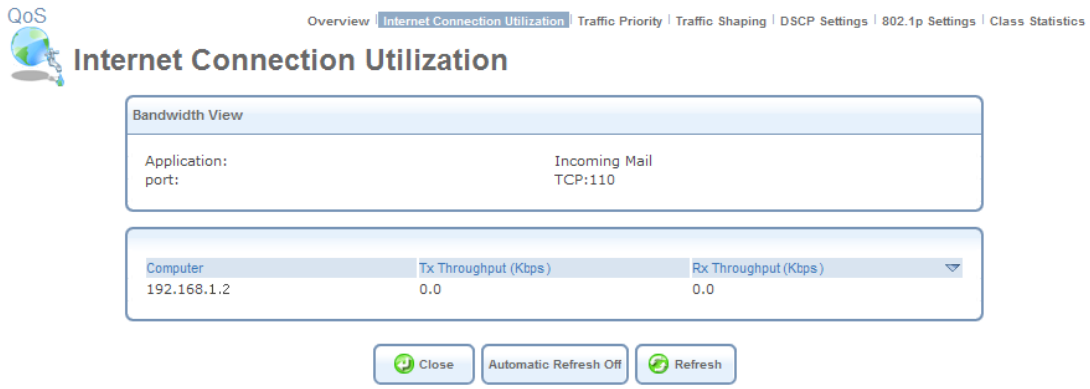


Figure 5.47 Utilization by Application – Advanced View

In this view, you can click each application's name to view its details, particularly which LAN computer is running it.



`

Figure 5.48 A Specific Application

5.3.2.2 Computer View

The 'Utilization by Computer' table displays the sum of bandwidth used by each LAN computer. The fields displayed are the computer's IP address and the Tx and Rx throughput.

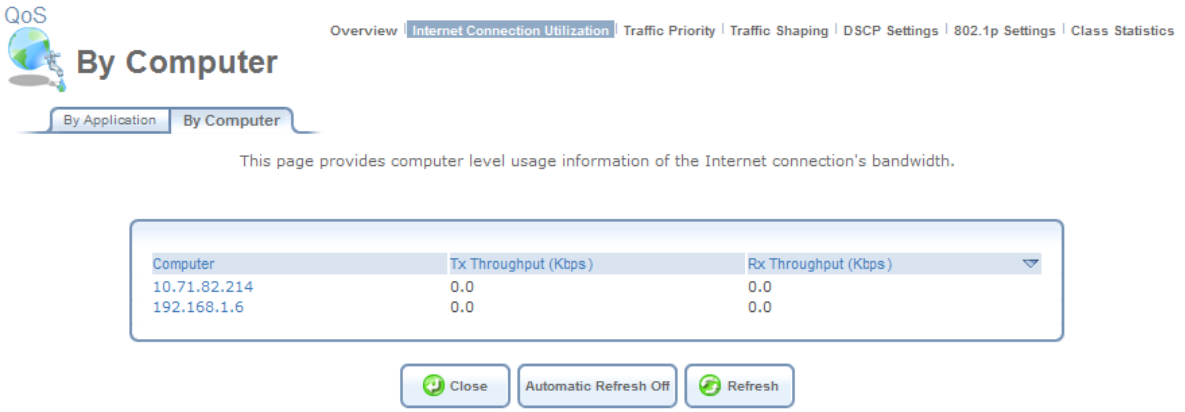


Figure 5.49 Utilization by Computer

Click a computer's IP address to view the bandwidth-consuming applications running on that computer.

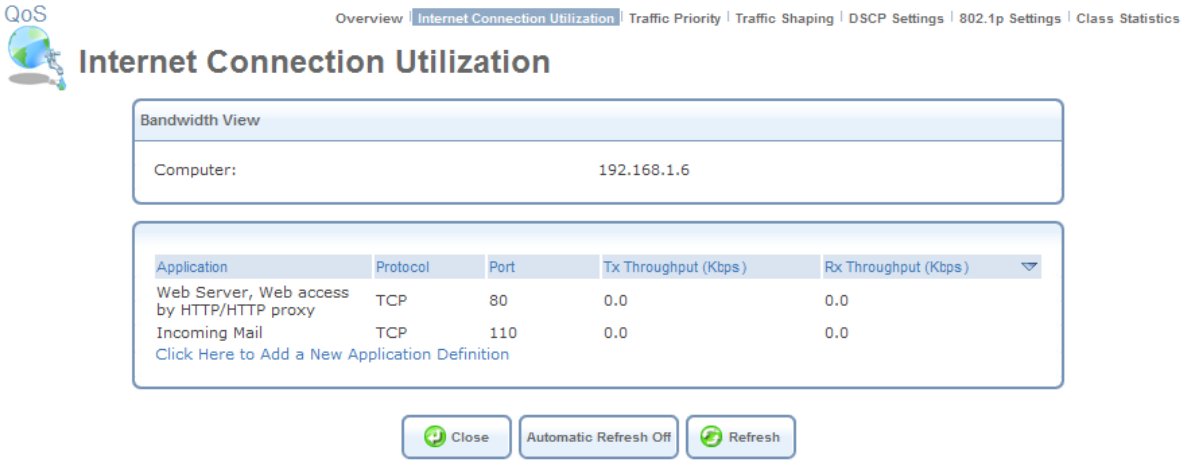


Figure 5.50 A Specific Computer

In this example, computer 192.168.1.6 is running the applications "Web Server" and "Incoming Mail". This screen provides a combined computer and application view, by displaying a computer-specific application table.

5.3.3 Defining Traffic Priority Rules

Traffic Priority allows you to manage and avoid traffic congestion by defining inbound and outbound priority rules for each device on your gateway. These rules determine the priority that packets, traveling through the device, will receive. QoS parameters (DSCP marking and packet priority) are set per packet, on an application basis. You can set QoS parameters using flexible

rules, according to the following parameters:

- Source/destination IP address, MAC address or host name
- Device
- Source/destination ports
- Limit the rule for specific days and hours

iPECS SBG-1000 supports two priority marking methods for packet prioritization:

- DSCP (refer to Section 5.3.5).
- 802.1p Priority (refer to Section 5.3.6).

The matching of packets by rules is connection-based, known as Stateful Packet Inspection (SPI), using the same connection-tracking mechanism used by iPECS SBG-1000's firewall. Once a packet matches a rule, all subsequent packets with the same attributes receive the same QoS parameters, both inbound and outbound. A packet can match more than one rule. Therefore:

- The first class rule has precedence over all other class rules (scanning is stopped once the first rule is reached).
- The first traffic-priority (classless) rule has precedence over all other traffic-priority rules.
- There is no prevention of a traffic-priority rule conflicting with a class rule. In this case, the priority and DSCP setting of the class rule (if given) will take precedence.

Connection-based QoS also allows inheriting QoS parameters by some of the applications that open subsequent connections. For instance, you can define QoS rules on SIP, and the rules will apply to both control and data ports (even if the data ports are unknown). This feature applies to all applications that have ALG in the firewall, such as:

- SIP
- MSN Messenger/Windows Messenger
- TFTP
- FTP
- MGCP
- H.323
- Port Triggering applications (refer to Section 5.2.5)
- PPTP
- IPSec

To set traffic priority rules:

1. Under the 'QoS' menu item, click 'Traffic Priority'. The 'Traffic Priority' screen appears (see Figure 5.51). This screen is divided into two identical sections, one for 'QoS input rules' and the other for 'QoS output rules', which are for prioritizing inbound and outbound traffic, respectively. Each section lists all the gateway devices on which rules can be set. You can set rules on all devices at once, using the 'All devices' entry.

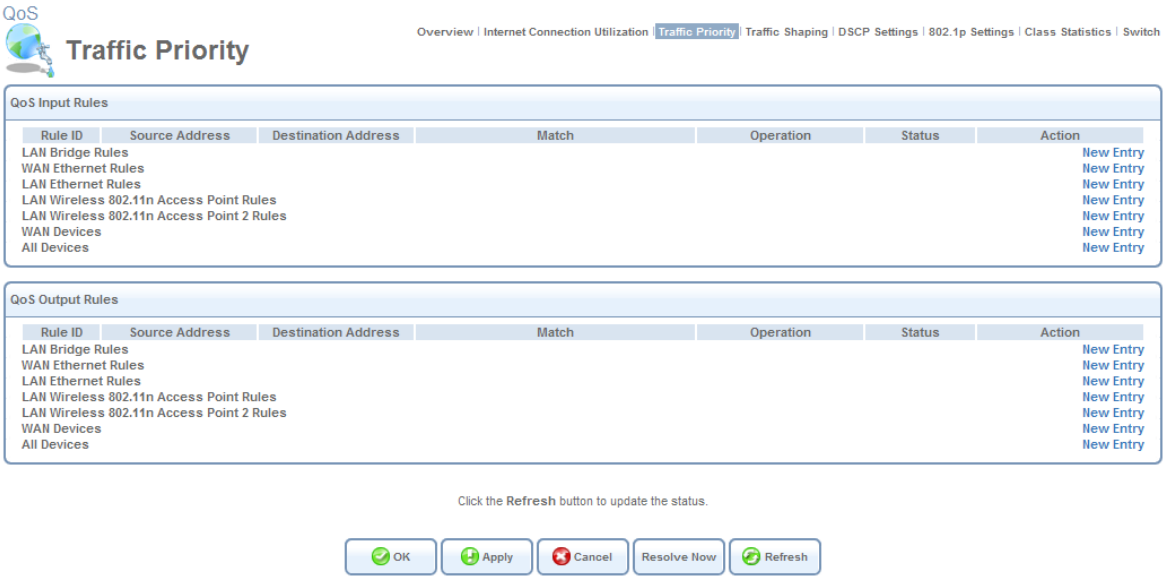


Figure 5.51 Traffic Priority

2. After choosing the traffic direction and the device on which to set the rule, click the appropriate ‘New Entry’ link. The ‘Add Traffic Priority Rule’ screen appears.

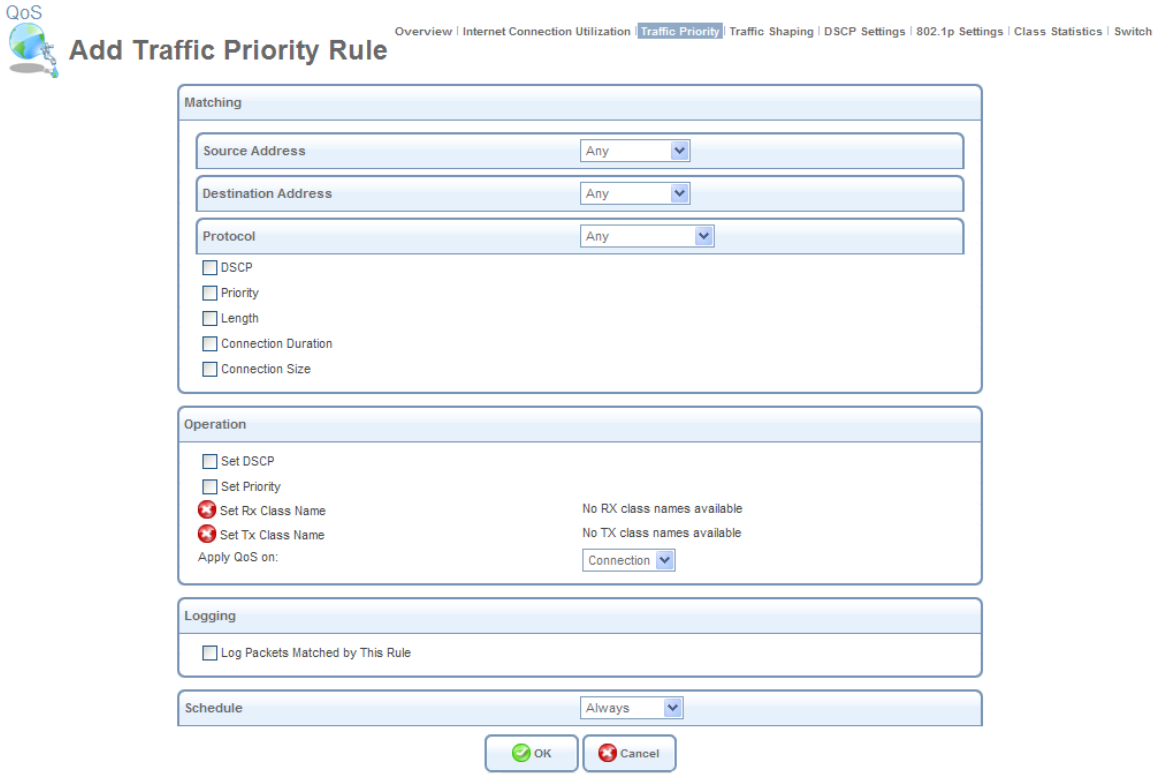


Figure 5.52 Add Traffic Priority Rule

This screen is divided into two main sections, ‘Matching’ and ‘Operation’, which are for defining the operation to be executed when matching conditions apply.

Matching Use this section to define characteristics of the packets matching the rule.

- **Source Address** The source address of packets sent or received by iPECS SBG-1000. Use this drop-down menu to specify the computer or group of computers on which you would like to apply the rule. Select an address or a name from the list to apply the rule on the corresponding host, or ‘Any’ to apply the rule on any host trying to send data. If you would like to add a new address, select the ‘User Defined’ option in the drop-down menu. This will commence a sequence that will add a new Network Object, representing the new host. Refer to Section 6.9.2 in order to learn how to do so.

- **Destination Address** The destination address of packets sent or received by iPECS SBG-1000. This address can be configured in the same manner as the source address. For example, use this drop-down menu to specify an IP address of a remote application server (such as a security server), which requires that the incoming packets have a specific IP address (e.g., one of those defined in your NAT IP address pool).

- **Protocol** You may also specify a traffic protocol. Selecting the ‘Show All Services’ option from the drop-down menu expands the list of available protocols. Select a protocol or add a new one using the ‘User Defined’ option. This will commence a sequence that will add a new **Service**, representing the protocol. Refer to Section 6.9.2 in order to learn how to do so.

  Using a protocol requires observing the relationship between a client and a server, in order to distinguish between the source and destination ports. For example, let’s assume you have an FTP server in your LAN, serving clients inquiring from the WAN. You want to apply a QoS rule on incoming packets from any port on the WAN (clients) trying to access FTP port 21 (your server), and the same for outgoing packets from port 21 trying to access any port on the WAN. Therefore, you must set the following Traffic Priority rules:

  - In the ‘Matching’ section of ‘QoS Input Rules’, select ‘FTP’ from the ‘Protocol’ drop-down menu. The ‘TCP Any -> 21’ setting appears under ‘Ports’.
  - Define a priority in the ‘Operation’ section.
  - Click ‘OK’ to save the settings.
  - Define a QoS output rule in the same way as the input rule.

- **DSCP** Select this check box to display two DSCP fields, which enable you to specify a hexadecimal DSCP value and its mask assigned to the packets matching the priority rule. For more information, refer to Section 5.3.5.

- **Priority** Select this check box to display a drop-down menu, in which you can select a priority level assigned to the packets matching the priority rule.

- **Device** Select this check box to display a drop-down menu, in which you can select a network device on which the packet-rule matching will be performed. This option is relevant in case you have previously selected the ‘All Devices’ option in the ‘Traffic Priority’ screen (see Figure 5.51).

- **Length** Select this check box if you would like to specify the length of packets, or the length of their data portion.

Note: The following two options are applicable only if the Fastpath feature is disabled in the 'Routing' menu item under 'System'. Depending on your gateway's model, the feature's name may appear as 'Software Acceleration' or 'Hardware Acceleration'.

- **Connection Duration** Select this check box to apply the priority rule only on connections which are open for a certain time period. This option is especially useful if you would like to accelerate your Web browsing by lowering the speed of concurrently running download jobs, or vice versa. After selecting the check box, choose whether the duration of connections matching the rule should be greater or less than the time that you specify in the adjacent field.

Figure 5.53 Connection Duration

For example, if you define the connection duration as less than 10 seconds, you will notice acceleration of your Web browsing and small file downloads, but slowing down of your large file downloads. The reason for this is that when a connection passes the specified time limit (as in case of a large file download), its priority is lowered, thereby giving more priority to shorter connections.

- **Connection Size** Select this check box to apply the priority rule only on connections matching a certain data size limit. This option is best used along with the 'Connection Duration' option, enabling you to fine-tune the gateway's traffic priority mechanism according to your needs. After selecting the check box, choose whether the connection's data size should be greater or less than the number of kilobytes that you specify in the adjacent field.

Figure 5.54 Connection Size

For example, if you define the connection size as less than 400 kilobytes, you will notice acceleration of Web browsing, and lowering of your file download speed. The reason for this is that when a connection exceeds the specified data size limit, its priority is lowered, thereby giving more priority to connections with a smaller data size.

Operation Perform the following operations on packets that match the priority rule.

- **Set DSCP** Select this check box if you would like to change the DSCP value on packets matching the rule, prior to routing them further. The screen refreshes (see Figure 5.55), enabling you to enter the hexadecimal DSCP value in its respective field that appears.

Figure 5.55 Set DSCP Rule

- **Set Priority** Select this check box if you would like to change a priority of the packets matching the rule. The screen refreshes (see Figure 5.56), enabling you to select between one of eight priority levels, zero being the lowest and seven the highest. Each priority level is assigned a default queue number, where Queue 0 has the lowest priority. iPECS SBG-1000's QoS supports up to four queues.

Figure 5.56 Set Priority with Queuing

The matching between a priority level and a queue number can be edited in the '802.1p Settings' screen (for more information, refer to Section 5.3.6).

- **Apply QoS on** Select whether to apply QoS on a connection or just the first packet. When applying on a connection, the data transfer session will be handled using Stateful Packet Inspection (SPI). This means that other packets matching this rule will be automatically allowed to access, and the same QoS scheme will be applied to them.

Logging Monitor the rule.

- **Log Packets Matched by This Rule** Select this check box to log the first packet from a connection that was matched by this rule.
- **Schedule** By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting 'User Defined' from the 'Schedule' drop-down menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

3. Click 'OK' to save the settings.

The order of the rules' appearance represents both the order in which they were defined and the sequence by which they will be applied. You may change this order after your rules are already defined (without having to delete and then re-add them), by using the action icon and action icon.

Figure 5.57 Move Up and Move Down Action Icons

5.3.4 Avoiding Congestion with Traffic Shaping

Traffic Shaping is the solution for managing and avoiding congestion where a high speed LAN meets limited broadband bandwidth. In the scenario of a 100 Mbps Ethernet LAN with a 100 Mbps

WAN interface gateway, the gateway may have to communicate with the ISP using a modem with a bandwidth of 2Mbps. This typical configuration makes the modem, having no QoS module, the bottleneck.
Instead of sending traffic as fast as it is received, iPECS SBG-1000's QoS algorithms perform traffic shaping, limiting the bandwidth of the gateway, thus artificially forcing it to become the bottleneck. A traffic shaper is essentially a regulated queue that accepts uneven and/or bursty flows of packets and transmits them in a steady, predictable stream so that the network is not overwhelmed with traffic. While Traffic Priority allows basic prioritization of packets, Traffic Shaping provides more sophisticated definitions, such as:

- Bandwidth limit for each device
- Bandwidth limit for classes of rules
- Prioritization policy
- TCP serialization on a device

Additionally, you can define QoS traffic shaping rules for a default device. These rules will be used on a device that has no definitions of its own. This enables the definition of QoS rules on Default WAN, for example, and their maintenance even if the PPP or bridge device over the WAN is removed.

5.3.4.1 Shaping the Traffic of a Device

To shape the traffic of a device, perform the following:

1. Click 'Traffic Shaping' under the QoS tab in the 'Services' screen. The 'Traffic Shaping' screen appears.

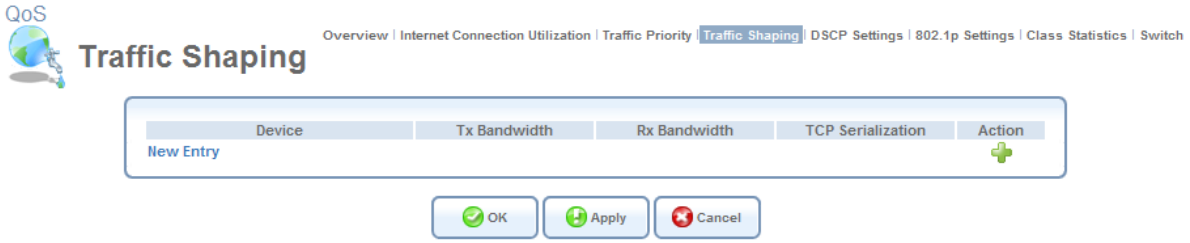


Figure 5.58 Traffic Shaping

2. Click the 'New Entry' link. The 'Add Device Traffic Shaping' screen appears (see Figure 5.59).

3. Select the device for which you would like to shape the traffic. The drop-down menu includes all your gateway's devices, and you can select either a specific device for which to shape the traffic, or 'All Devices' to add a traffic class to all devices. In this example, select the WAN Ethernet option.

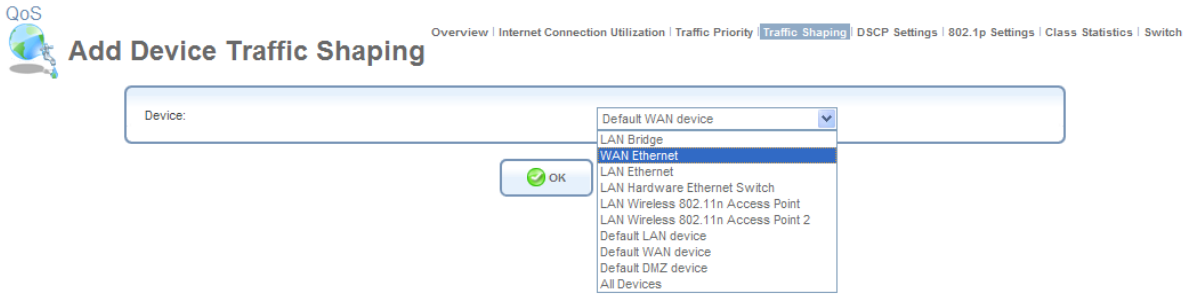


Figure 5.59 Add Device Traffic Shaping

If you would like to configure iPECS SBG-1000's LAN traffic transmission/reception rate, select the relevant LAN device. If you would like to apply the settings on all LAN devices, select the 'Default LAN Device' entry

4. Click 'OK'. The 'Edit Device Traffic Shaping' screen appears.

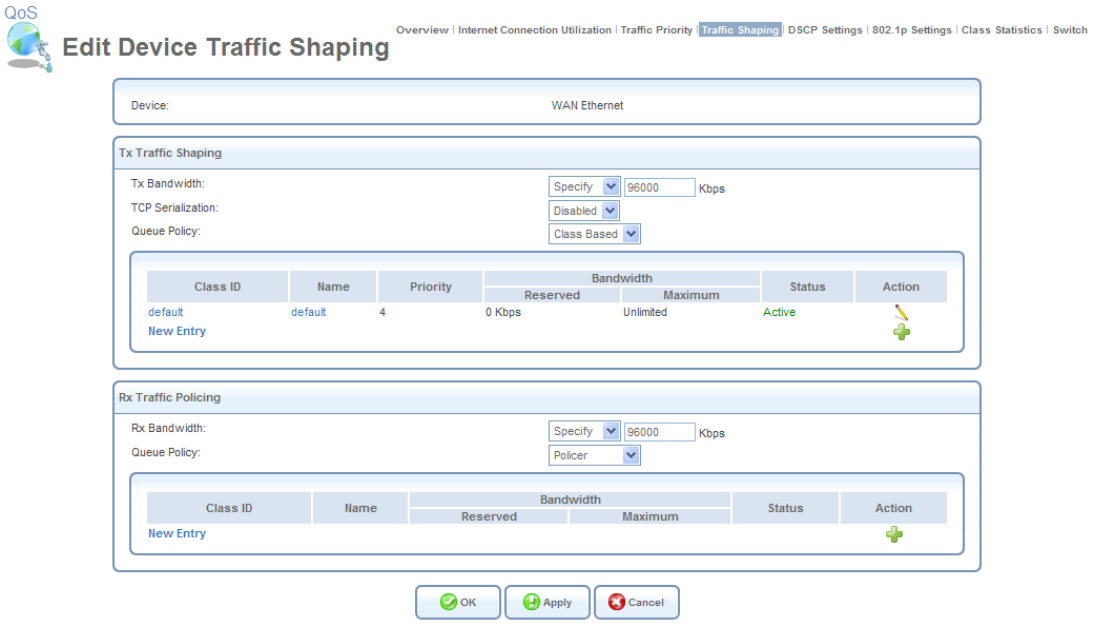


Figure 5.60 Edit Device Traffic Shaping

5. Configure the following fields:

Tx Bandwidth This parameter limits the gateway's bandwidth transmission rate. The purpose is to limit the bandwidth of the WAN device to that of the weakest outbound link, for instance, the DSL speed provided by the ISP. This forces iPECS SBG-1000 to be the network bottleneck, where sophisticated QoS prioritization can be performed. If the device's bandwidth is not limited correctly, the bottleneck will be in an unknown router or modem on the network path, rendering iPECS SBG-1000's QoS useless.

TCP Serialization You can enable TCP Serialization in its drop-down menu, either for active voice calls only or for all traffic. The screen will refresh, adding a 'Maximum Delay' field (see Figure 5.61). This function allows you to define the maximal allowed transmission time frame (in milliseconds) of a single packet. Any packet that requires a longer time to be transmitted will be fragmented to smaller sections. This avoids transmission of large, bursty packets that

may cause delay or jitter for real-time traffic such as VoIP. If you insert a delay value in milliseconds, the delay in number of bytes will be automatically updated on refresh.

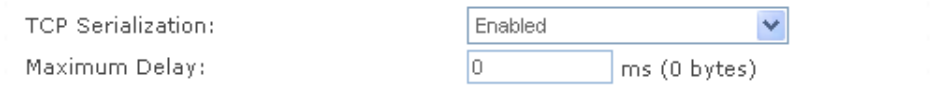


Figure 5.61 TCP Serialization – Maximum Delay

Queue Policy Tx traffic queueing can be based on a traffic class (see the following explanations) or on the pre-defined priority levels (refer to Section 5.3.3). Note that when it is based on a traffic class, the class's bandwidth requirements will be met regardless of the priority, and only excess bandwidth will be given to traffic with a higher priority. However, when unlimited bandwidth is selected for the Tx traffic, the queue policy can only be based on the pre-defined priority levels.

5.3.4.2 Creating a Traffic Shaping Class

The bandwidth of a device can be divided in order to reserve constant portions of bandwidth to predefined traffic types. Such a portion is known as a *Traffic Shaping Class*. When not used by its predefined traffic type, or owner (for example VoIP), the bandwidth will be available to all other traffic. However when needed, the entire class is reserved solely for its owner.
Moreover, you can limit the maximum bandwidth that a class can use even if the entire bandwidth is available. When a traffic class is first defined for a specific traffic type, two classes are created. The second class is the 'Default Class', which is responsible for all the packets that *do not* match the defined traffic class, or any other classes that may be defined on the device. You can also define **wildcard** devices, such as all WAN devices. This can be viewed in the 'Class Statistics' screen (see Figure 5.71).
To define a new traffic shaping class, perform the following:

1. In the 'Edit Device Traffic Shaping' screen (see Figure 5.60), click the 'New Entry' link in the 'Tx Traffic Shaping' section. The 'Add Shaping Class' screen appears.

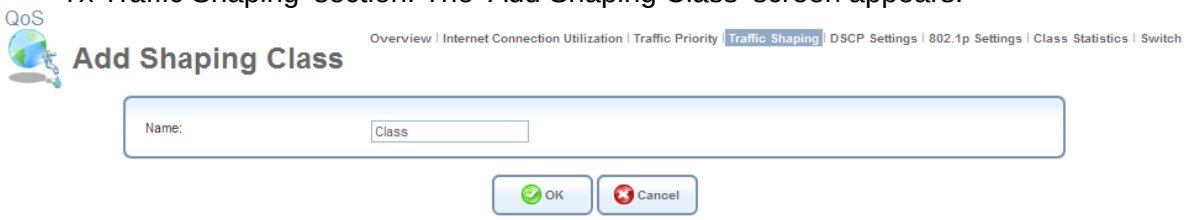


Figure 5.62 Add Shaping Class

2. Name the new class and click 'OK' to save the settings, e.g. Class A.

3. Back in the 'Edit Device Traffic Shaping' screen, click the class name to edit the traffic class. Alternatively, click its action icon. The 'Edit Shaping Class' screen appears.

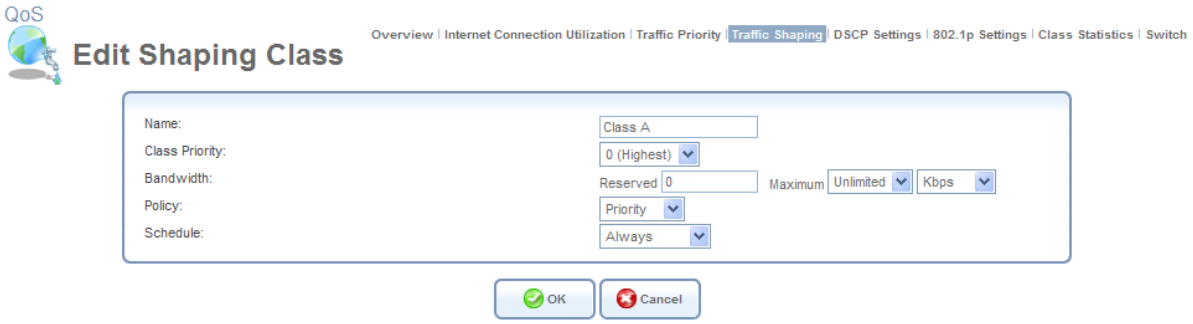


Figure 5.63 Edit Shaping Class

4. Configure the following fields:

Name The name of the class.

Class Priority The class can be granted one of eight priority levels, zero being the highest and seven the lowest (note the obversion when compared to the rules priority levels). This level sets the priority of a class in comparison to other classes on the device.

Bandwidth The reserved transmission bandwidth in kilo-bits per second. You can limit the maximum allowed bandwidth by selecting the 'Specify' option in the drop-down menu. The screen will refresh, adding another Kbits/s field.

Figure 5.64 Specify Maximum Bandwidth

Policy The class policy determines the policy of routing packets inside the class. Select one of the four options:

- **Priority** Priority queuing utilizes multiple queues, so that traffic is distributed among queues based on priority. This priority is defined according to packet's priority, which can be defined explicitly, by a DSCP value (refer to Section 5.3.5), or by a 802.1p value (refer to Section 5.3.6).

- **FIFO** The "First In, First Out" priority queue. This queue ignores any previously-marked priority that packets may have.

- **Fairness** The fairness algorithm ensures no starvation by granting all packets a certain level of priority.

- **RED** The Random Early Detection algorithm utilizes statistical methods to drop packets in a "probabilistic" way before queues overflow. Dropping packets in this way slows a source down enough to keep the queue steady and reduces the number of packets that would be lost when a queue overflows and a host is transmitting at a high rate.

- **WRR** Weighted Round Robin utilizes a process scheduling function that prioritizes traffic according to the pre-defined 'Weight' parameter of a traffic's class. This level of prioritizing provides more flexibility in distributing bandwidth between traffic types, by defining additional classes within a parent class.

Schedule By default, the class will always be active. However, you can configure scheduler rules in order to define time segments during which the class may be active. To learn how to configure scheduler rules, refer to the 'Defining Scheduler Rules' section of the iPECS SBG-1000 Administrator Manual.

5.3.4.3 Setting an Incoming Traffic Policy

When shaping the traffic for a device, you must also determine a policy for incoming traffic. In the 'Edit Device Traffic Shaping' screen (see Figure 5.60), configure the following fields in the 'Rx Traffic Policing' section:

Rx Bandwidth This parameter limits the device's bandwidth reception rate. In this example, the purpose is to limit the bandwidth that the WAN device can receive from the ISP.

Queue Policy Similar to Tx traffic, Rx traffic queueing can be based on a traffic class or on strict priority (unless unlimited bandwidth is selected). By default, however, the queue policy is set to Policer, which is a relatively simple method of bandwidth control. With the policer option, you can dedicate a portion of the bandwidth to a certain traffic type. This portion will always remain available to its traffic type, even when not in use. This is a simpler method, as priority is not used at all.

When selecting a class-based queue policy, you must define an Rx Traffic Policy Class, which is identical to defining a Tx Traffic Shaping Class, described earlier. However if you select the policer as your queue policy, defining a policing class is even simpler, as it lacks the priority setup.

To define an Rx traffic policy class, perform the following:

1. In the 'Edit Device Traffic Shaping' screen (see Figure 5.60), click the 'New Entry' link in the 'Rx Traffic Policing' section. The 'Add Policing Class' screen appears.

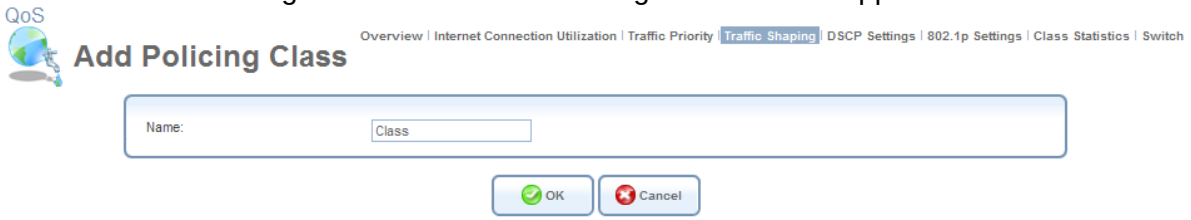


Figure 5.65 Add Policing Class

2. Name the new class and click 'OK' to save the settings, e.g. Class B.

3. Back in the 'Edit Device Traffic Shaping' screen, click the class name to edit the traffic class. Alternatively, click its action icon. The 'Edit Policing Class' screen appears.

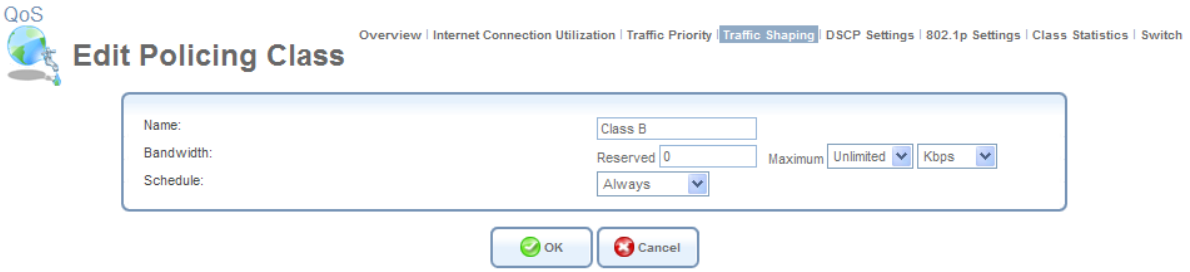


Figure 5.66 Edit Policing Class

4. Configure the following fields:

Name The name of the class.

Bandwidth The reserved reception bandwidth in kilo-bits per second. You can limit the maximum allowed bandwidth by selecting the 'Specify' option in the combo box. The screen refreshes, adding yet another Kbps field.

Figure 5.67 Specify Maximum Bandwidth

Schedule By default, the class will always be active. However, you can configure scheduler rules in order to define time segments during which the class may be active. To learn how to configure scheduler rules, refer to the 'Defining Scheduler Rules' section of the Manual.

5.3.5 Prioritizing Traffic with DSCP

In order to understand what Differentiated Services Code Point (DSCP) is, one must first be familiarized with the *Differentiated Services* model. Differentiated Services (Diffserv) is a Class of Service (CoS) model that enhances best-effort Internet services by differentiating traffic by users, service requirements and other criteria. Packets are specifically marked, allowing network nodes to provide different levels of service, as appropriate for voice calls, video playback or other delay-sensitive applications, via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows.

Diffserv defines a field in IP packet headers referred to as DSCP. Hosts or routers passing traffic to a Diffserv-enabled network will typically mark each transmitted packet with an appropriate DSCP. The DSCP markings are used by Diffserv network routers to appropriately classify packets and to apply particular queue handling or scheduling behavior. iPECS SBG-1000 provides a table of predefined DSCP values, which are mapped to 802.1p priority marking method (refer to Section 5.3.6).

You can edit or delete any of the existing DSCP setting, as well as add new entries.

1. Under the QoS menu item, click 'DSCP Settings'. The following screen appears.

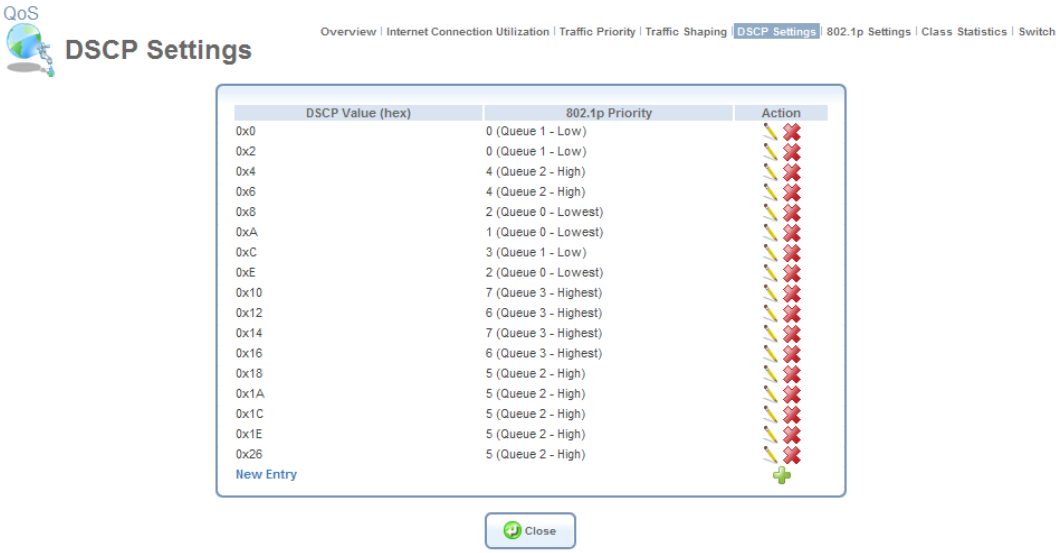


Figure 5.68 DSCP--Traffic Priority Matching

Each DSCP value is assigned a default queue number as a part of its 802.1p priority settings. iPECS SBG-1000's QoS supports up to four queues, where Queue 0 has the lowest priority.

2. To edit an existing entry, click its action icon. To add a new entry, click the 'New Entry' link. In both cases, the 'Edit DSCP Settings' screen appears.

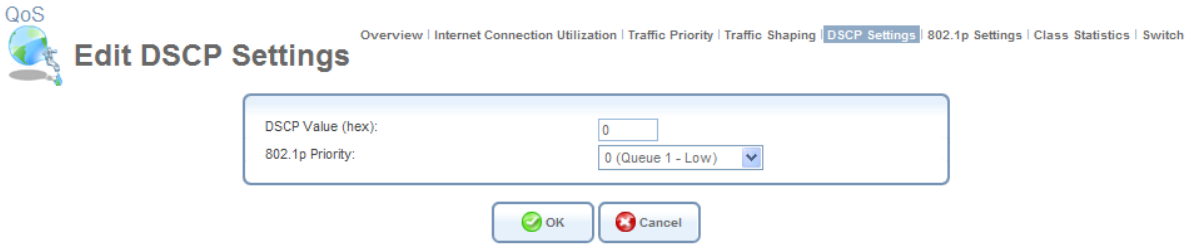


Figure 5.69 Edit DSCP Settings

3. Configure the following fields:

   DSCP Value (hex) Enter a hexadecimal number that will serve as the DSCP value.

   802.1p Priority Select a 802.1p priority level from the drop-down menu (each priority level is mapped to lowest/low/high/highest priority).

4. Click 'OK' to save the settings.

Note: The DSCP value overriding the priority of incoming packets with an unassigned value (priority 0, assumed to be a no-priority-set) is "0x0".

5.3.6 Configuring 802.1p Priority Values

The IEEE 802.1p priority marking method is a standard for prioritizing network traffic at the data link/MAC sub-layer. 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established. The 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority (0-7), where level 7 is the highest one. In addition, iPECS SBG-1000 maps these eight levels to priority queues, where Queue 0 has the lowest priority.
iPECS SBG-1000's QoS supports up to four queues. By default, the higher the level and queue values, the more priority they receive. Therefore, the more critical the traffic is, the higher priority level and queue number it should receive. To change the mapping between a priority value and a queue value, perform the following:

1. Under the 'QoS' menu item, click '802.1p Settings'. The following screen appears.

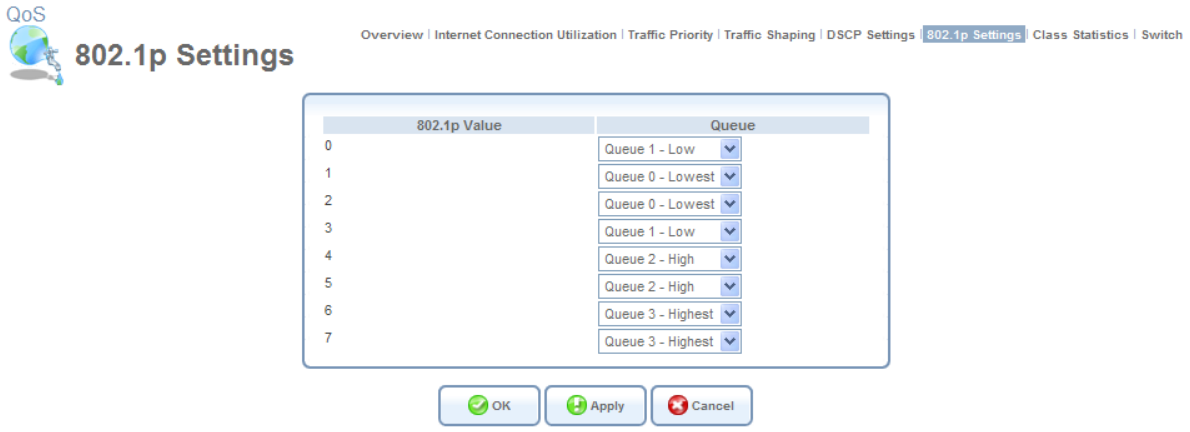


Figure 5.70 Traffic Queuing in 802.1p Settings

2. From the corresponding drop-down menu, select a desired value.

3. Click 'OK' to save the settings.

5.3.7 Viewing Traffic Statistics

iPECS SBG-1000 provides you with accurate, real-time information on the traffic moving through your defined device classes. For example, the amount of packets sent, dropped or delayed, are just a few of the parameters that you can monitor per each shaping class. To view your class statistics, click 'Class Statistics' under the QoS menu item. The following screen appears.

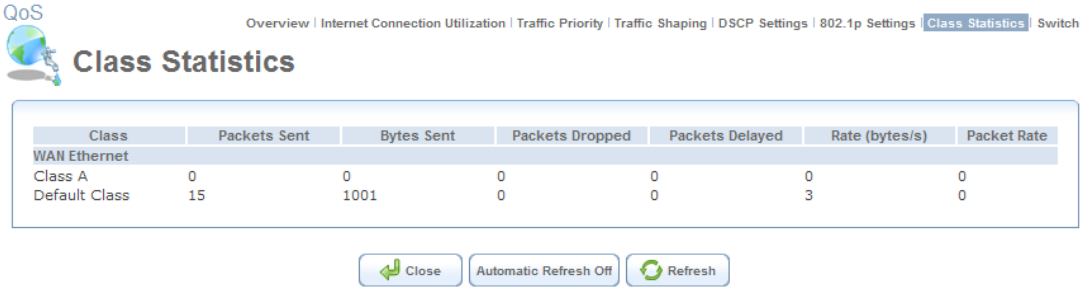


Figure 5.71 Class Statistics

Note that class statistics will only be available after defining at least one class (otherwise the screen will not present any information).

5.4 Virtual Private Network

5.4.1 Internet Protocol Security

Internet Protocol Security (IPSec) is a series of guidelines for the protection of Internet Protocol (IP) communications. It specifies procedures for securing private information transmitted over public networks. The IPSec protocols include:

- AH (Authentication Header) provides packet-level authentication.
- ESP (Encapsulating Security Payload) provides encryption and authentication.
- IKE (Internet Key Exchange) negotiates connection parameters, including keys, for the other two services.

Services supported by the IPSec protocols (AH, ESP) include confidentiality (encryption), authenticity (proof of sender), integrity (detection of data tampering), and replay protection (defense against unauthorized resending of data). IPSec also specifies methodologies for key management. Internet Key Exchange (IKE), the IPSec key management protocol, defines a series of steps to establish keys for encrypting and decrypting information; it defines a common language on which communications between two parties is based. Developed by the Internet Engineering Task Force (IETF), IPSec and IKE together standardize the way data protection is performed, thus making it possible for security systems developed by different vendors to interoperate.

5.4.1.1 Technical Specifications

- Security architecture for the Internet Protocol
- IP Security Document Roadmap
- Connection type: Tunnel, Transport
- Use of Internet Security Association and Key Management Protocol (ISAKMP) in main and aggressive modes
- Key management: Manual, Automatic (Internet Key Exchange)
- NAT Traversal Negotiation for resolution of NATed tunnel endpoint scenarios
- Dead Peer Detection for tunnel disconnection in case the remote endpoint ceases to operate

- Gateway authentication: X.509, RSA signatures and pre-shared secret key
- IP protocols: ESP, AH
- Encryption: AES, 3DES, DES, NULL, HW encryption integration (platform dependent)
- Authentication: MD5, SHA-1
- IP Payload compression
- Interoperability: VPNC Certified IPSec, Windows 2000, Windows NT, FreeS/WAN, FreeBSD, Checkpoint Firewall-1, Safenet SoftRemote, NetScreen, SSH Sentinel

5.4.1.2 IPSec Settings

Access this feature either from the 'VPN' menu item under the 'Services' tab, or by clicking its icon in the 'Shortcut' screen. The 'Internet Protocol Security (IPSec)' screen appears.

Figure 5.72 Internet Protocol Security (IPSec)

This screen enables you to configure the following settings:

Block Unauthorized IP Select the 'Enabled' check box to block unauthorized IP packets to iPECS SBG-1000. Specify the following parameters:

- **Maximum Number of Authentication Failures** The maximum number of packets to authenticate before blocking the origin's IP address.
- **Block Period (in seconds)** The timeframe during which iPECS SBG-1000 will drop packets from an unauthorized IP address.

Enable Anti-Replay Protection Select this option to enable dropping of packets that are recognized (by their sequence number) as already been received.

Connections This section displays the list of IPSec connections. To learn how to create an IPSec connection, refer to Section 6.4.12.

5.4.1.2.1 Public Key Management

The 'Settings' button in the 'Internet Protocol Security (IPSec)' screen enables you to manage iPECS SBG-1000's public keys.

1. Click the 'Settings' button (see Figure 5.72) to view iPECS SBG-1000's public key. If necessary, you can copy the public key from the screen that appears.

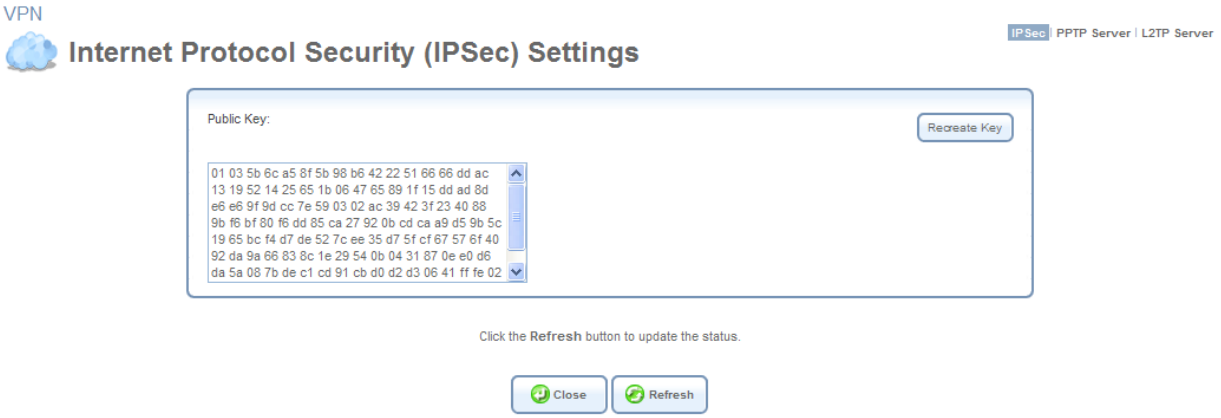


Figure 5.73 Internet Protocol Security (IPSec) Settings

2. Click the ‘Recreate Key’ button to recreate the public key, or the ‘Refresh’ button to refresh the key displayed in this screen.

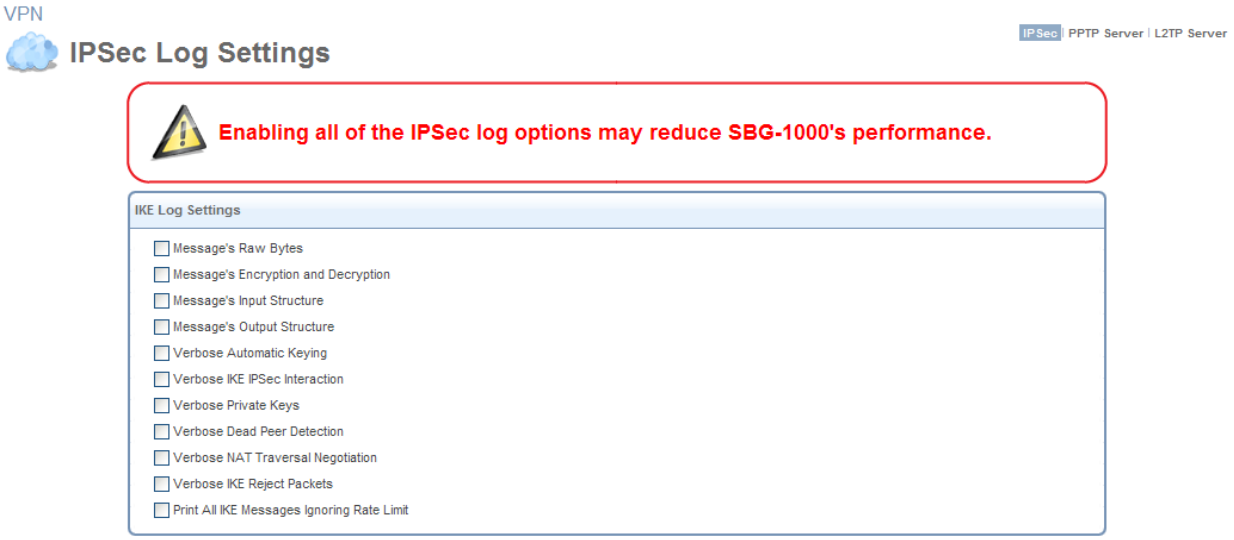
5.4.1.2.2 Log Settings

The IPSec Log can be used to identify and analyze the history of the IPSec package commands, attempts to create connections, etc. The IPSec activity, as well as that of other iPECS SBG-1000 modules, are displayed together in this view.

1. Click the ‘Log Settings’ button. The ‘IPSec Log Settings’ screen appears (see Figure 5.74).

2. Select the check boxes relevant to the information you would like the IPSec log to record.

3. Click ‘OK’ to save the settings.



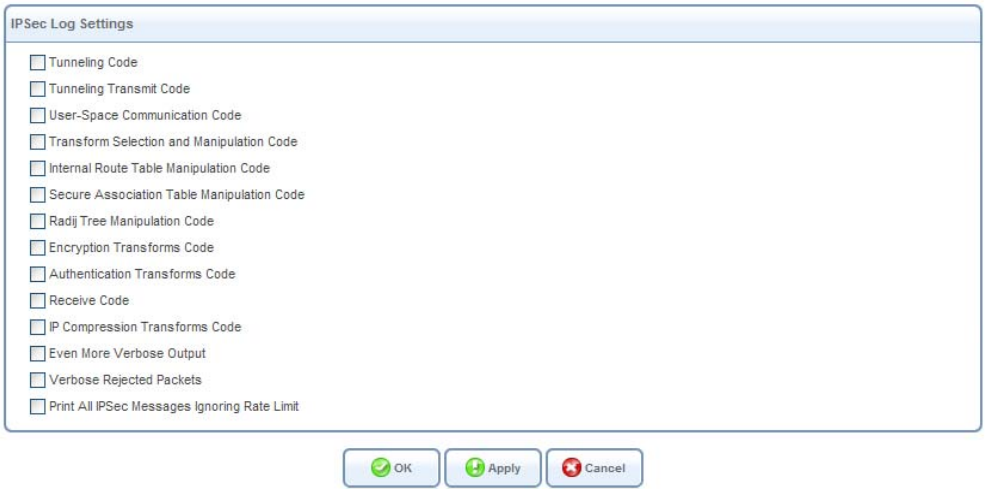


Figure 5.74 IPSec Log Settings

5.4.1.3 IPSec Connection Settings

The IPSec connections are displayed under the 'Connections' section of the 'Internet Protocol Security (IPSec)' screen (see Figure 5.72), in addition to the general 'Network Connections' screen (refer to Section 6.4). To configure an IPSec connection settings, perform the following:

1. Click the connection's action icon. The 'VPN IPSec Properties' screen appears, displaying the 'General' sub-tab.

Figure 5.75 VPN IPSec Properties – General

2. Click the 'Settings' sub-tab, and configure the following settings:

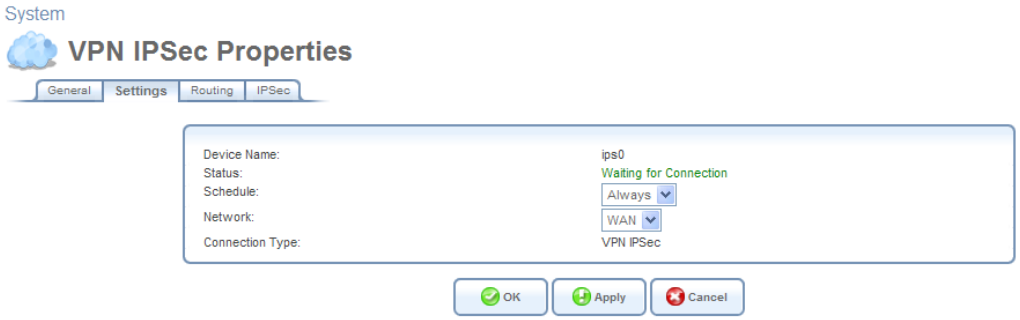


Figure 5.76 VPN IPSec Properties – Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind iPECS SBG-1000.

3. Click the 'Routing' sub-tab, and define the connection's routing rules. To learn how to create routing rules, refer to Section 6.6.

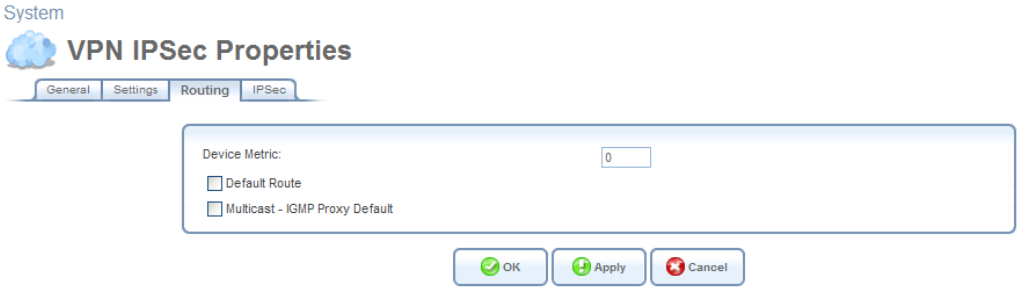


Figure 5.77 VPN IPSec Properties – Routing

4. Click the 'IPSec' sub-tab, and configure the following settings.

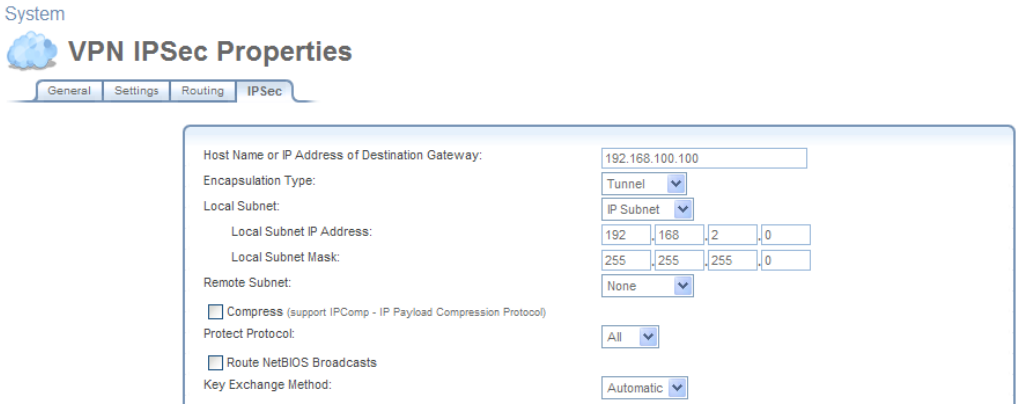


Figure 5.78 VPN IPSec Properties – IPSec

Host Name or IP Address of Destination Gateway The IP address of your IPSec peer. If your connection is an IPSec Server, this field will display “Any Remote Gateway”.

Encapsulation Type Select between ‘Tunneling’ or ‘Transport’ encapsulation. ‘Transport’ encapsulation is performed between two gateways (no subnets), and therefore needs no explicit configuration. ‘Tunneling’ requires that you configure the following parameters:

- **Local Subnet** Define your local endpoint, by selecting one of the following options:

  IP Subnet (default) Enter iPECS SBG-1000’s Local Subnet IP Address and Local Subnet Mask.

  IP Range Enter the ‘From’ and ‘To’ IP addresses, forming the endpoints range of the local subnet(s).

  IP Address Enter the Local IP Address to define the endpoint as a single host.

  None Select this option if you do not want to define a local endpoint. The endpoint will be set to the gateway.

- **Remote Subnet** This section is identical to the ‘Local Subnet’ section above, but is for defining the remote endpoint.

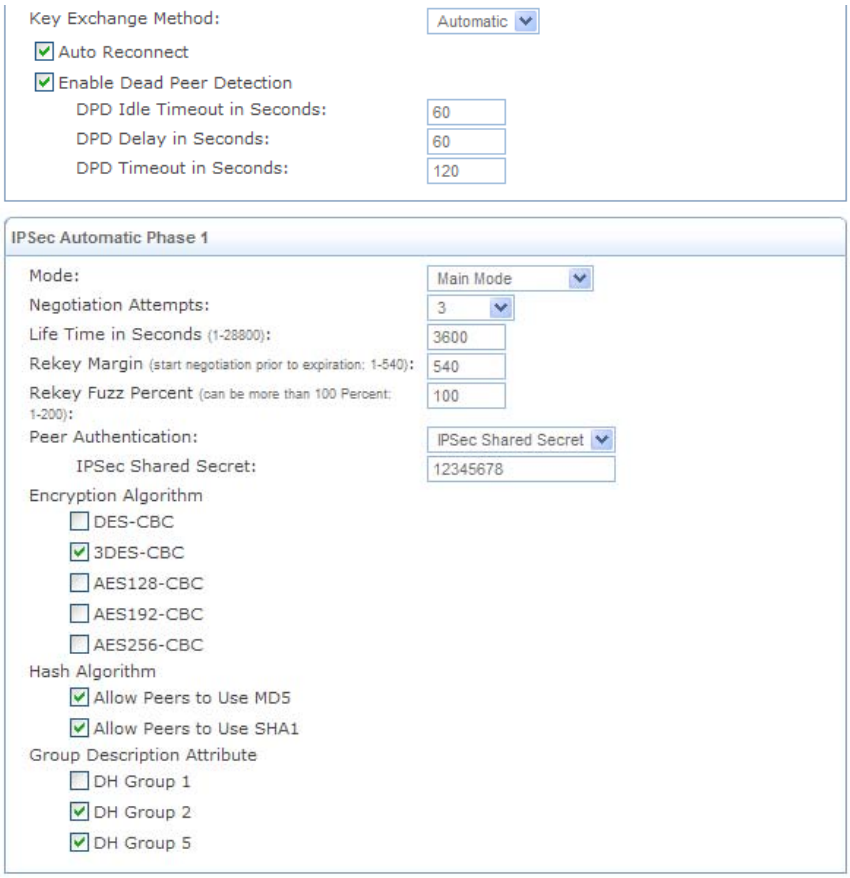
  Compress (Support IPComp protocol) Select this check box to compress packets during encapsulation with the IP Payload Compression protocol. Please note that this reduces performance (and is therefore unchecked by default).

Protect Protocol Select the protocols to protect with IPSec: All, TCP, UDP, ICMP or GRE. When selecting TCP or UDP, additional source port and destination port drop-down menus will appear, enabling you to select ‘All’ or to specify ‘Single’ ports in order to define the protection of specific packets. For example, in order to protect L2TP packets, select UDP and specify 1701 as both single source and single destination ports.

Route NetBIOS Broadcasts Select this option to allow NetBIOS packets through the IPSec tunnel, which otherwise would not meet the routing conditions specified.

Key Exchange Method The IPSec key exchange method can be 'Automatic' (the default) or 'Manual'. Selecting one of these options will alter the rest of the screen.

1. Automatic key exchange settings:



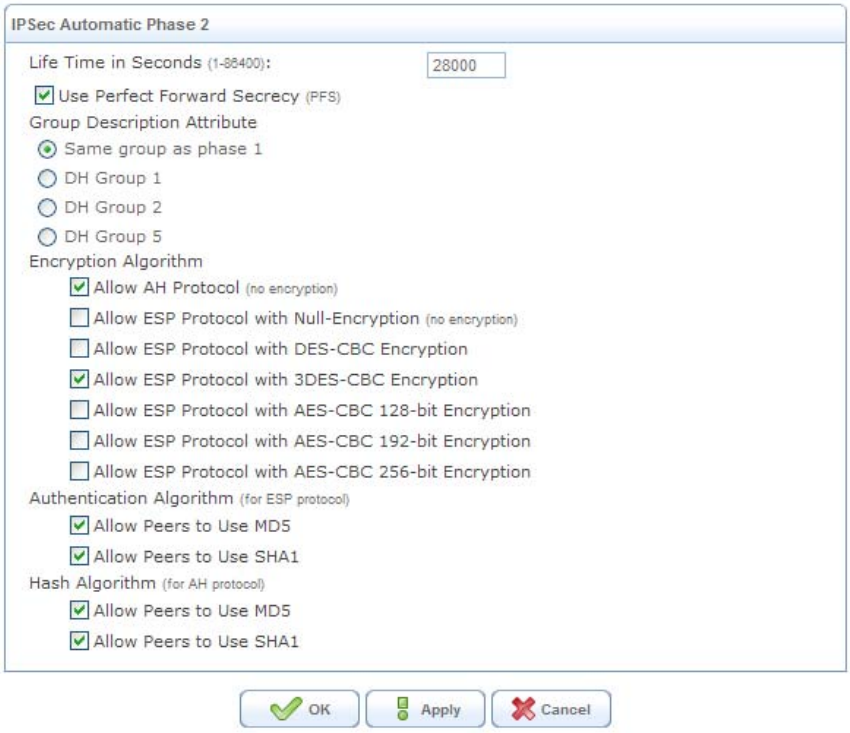


Figure 5.79 Automatic Key Exchange Settings

Auto Reconnect The IPSec connection will reconnect automatically if disconnected for any reason.

Enable Dead Peer Detection iPECS SBG-1000 will detect whether the tunnel endpoint has ceased to operate, in which case will terminate the connection. Note that this feature will be functional only if the other tunnel endpoint supports it. This is determined during the negotiation phase of the two endpoints.

- **DPD Idle Timeout in Seconds** Defines how long the IPSec tunnel can be idle before iPECS SBG-1000 sends the first DPD message to the remote peer, in order to check if it is alive.

- **DPD Delay in Seconds** Defines how long iPECS SBG-1000 will wait for the peer's response to the DPD message, before sending an additional message (in case of response failure).

- **DPD Timeout in Seconds** Defines how long iPECS SBG-1000 will try to contact the peer, before it declares the peer dead and terminates the connection.

IPSec Automatic Phase 1 – Peer Authentication

- **Mode** Select the IPSec mode – either 'Main Mode' or 'Aggressive Mode'. Main mode is a secured but slower mode, which presents negotiable propositions according to the authentication algorithms that you select in the check boxes. Aggressive Mode is faster but less secured. When selecting this mode, the algorithm check boxes are replaced by radio buttons, presenting strict propositions according to your selections.

- **Negotiation attempts** Select the number of negotiation attempts to be performed in the automatic key exchange method. If all attempts fail, iPECS SBG-1000 will wait for a negotiation request.

- **Life Time in Seconds** The timeframe in which the peer authentication will be valid.

- **Rekey Margin** Specifies how long before connection expiry should attempts to negotiate a replacement begin. It is similar to that of the key life time and is given as an integer denoting seconds.

- **Rekey Fuzz Percent** Specifies the maximum percentage by which Rekey Margin should be randomly increased to randomize re-keying intervals.

- **Peer Authentication** Select the method by which iPECS SBG-1000 will authenticate your IPSec peer.
  . IPSec Shared Secret – Enter the IPSec shared secret.
  . RSA Signature – Enter the peer's RSA signature (based on iPECS SBG-1000's public key), as described in Section 5.8.1.5.3.
  . Certificate – If a certificate exists on iPECS SBG-1000, it will appear when you select this option. Enter the certificate's local ID and peer ID. To learn how to add certificates to iPECS SBG-1000, refer to Section 6.9.4.

- **Encryption Algorithm** Select the encryption algorithms that iPECS SBG-1000 will attempt to use when negotiating with the IPSec peer.

- **Hash Algorithm** Select the hash algorithms that iPECS SBG-1000 will attempt to use when negotiating with the IPSec peer.
- **Group Description Attribute** Select the Diffie-Hellman (DH) group description(s). Diffie-Hellman is a public-key cryptography scheme that allows two parties to establish a shared secret over an insecure communications channel.

IPSec Automatic Phase 2 – Key Definition

- **Life Time in Seconds** The length of time before a security association automatically performs renegotiation.

- **Use Perfect Forward Secrecy (PFS)** Select whether Perfect Forward Secrecy of keys is required on the connection's keying channel (with PFS, penetration of the key-exchange protocol does not compromise keys negotiated earlier). Deselecting this option will hide the next parameter.
  Group Description Attribute Select whether to use the same group chosen in phase 1, or reselect specific groups.

- **Encryption Algorithm** Select the encryption algorithms that iPECS SBG-1000 will

attempt to use when negotiating with the IPSec peer.

- **Authentication Algorithm (for ESP protocol)** Select the authentication algorithms that iPECS SBG-1000 will attempt to use when negotiating with the IPSec peer.

- **Hash Algorithm (for AH protocol)** Select the hash algorithms that iPECS SBG-1000 will attempt to use when negotiating with the IPSec peer.

2. Manual key definition:

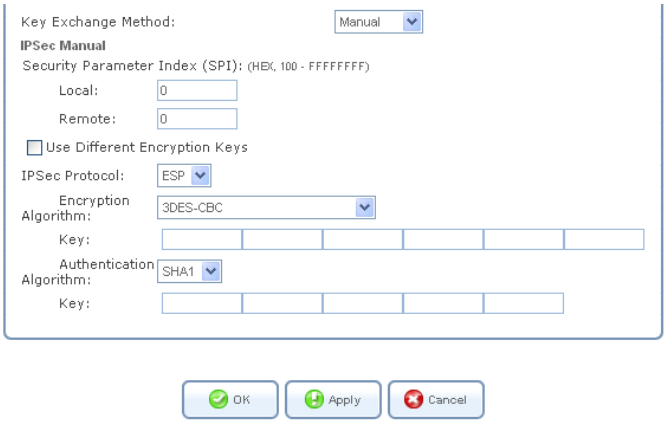


Figure 5.80 Manual Key Definition

Security Parameter Index (SPI): (HEX, 100 - FFFFFFFF) A 32 bit value that together with an IP address and a security protocol, uniquely identifies a particular security association. The local and remote values must be coordinated with their respective values on the IPSec peer.
Use Different Encryption Keys Selecting this option allows you to define both local and remote algorithm keys when defining the IPSec protocol (in the next section).
IPSec Protocol Select between the ESP and AH IPSec protocols. The screen will refresh accordingly:

- **ESP –** Select the encryption and authentication algorithms, and enter the algorithm keys in hexadecimal representation.
- **AH –** Select the hash algorithm, and enter the algorithm key in hexadecimal representation.

5. Click ‘OK’ to save the settings.

5.4.1.4 IPSec Gateway-to-Host Connection Scenario

In order to create an IPSec connection between iPECS SBG-1000 and a Windows host, you need to configure both the gateway and the host. This section describes both iPECS SBG-1000’s configuration and a Windows XP client configuration.

5.4.1.4.1 Configuring IPSec on iPECS SBG-1000

1. Under the ‘System’ tab, click the ‘Network Connections’ menu item. The ‘Network

Connections' screen appears.

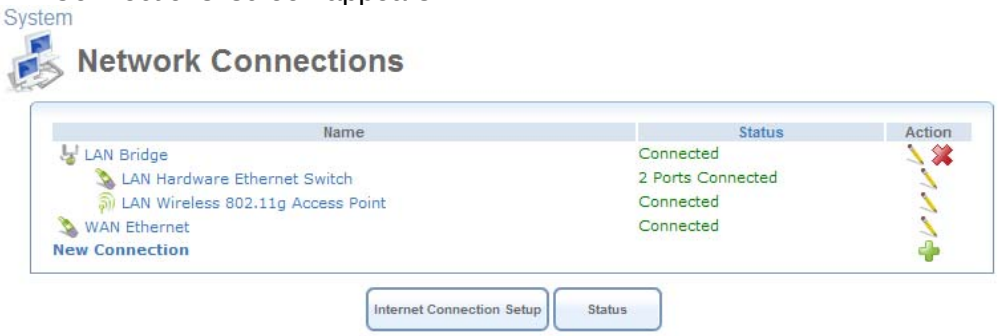


Figure 5.81 Network Connections

2. Click the 'New Connection' link. The 'Connection Wizard' screen appears.

Figure 5.82 Connection Wizard

3. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears.

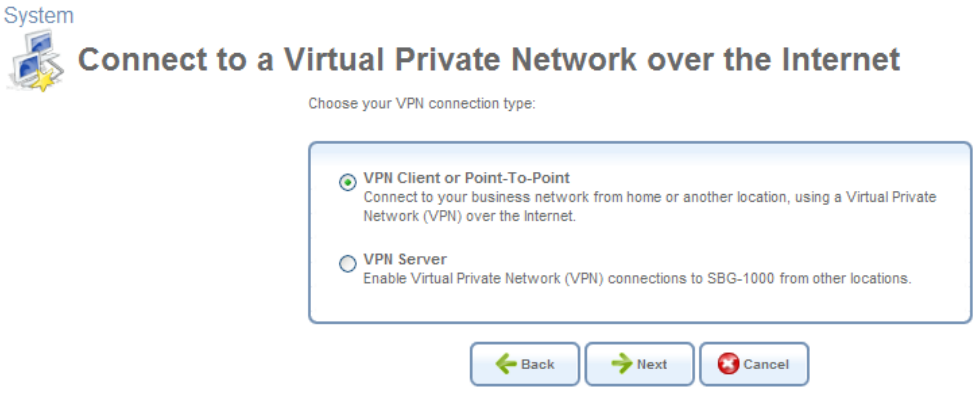


Figure 5.83 Connect to a Virtual Private Network over the Internet

4. Select the 'VPN Client or Point-To-Point' radio button and click 'Next'. The 'VPN Client or Point-To-Point' screen appears.

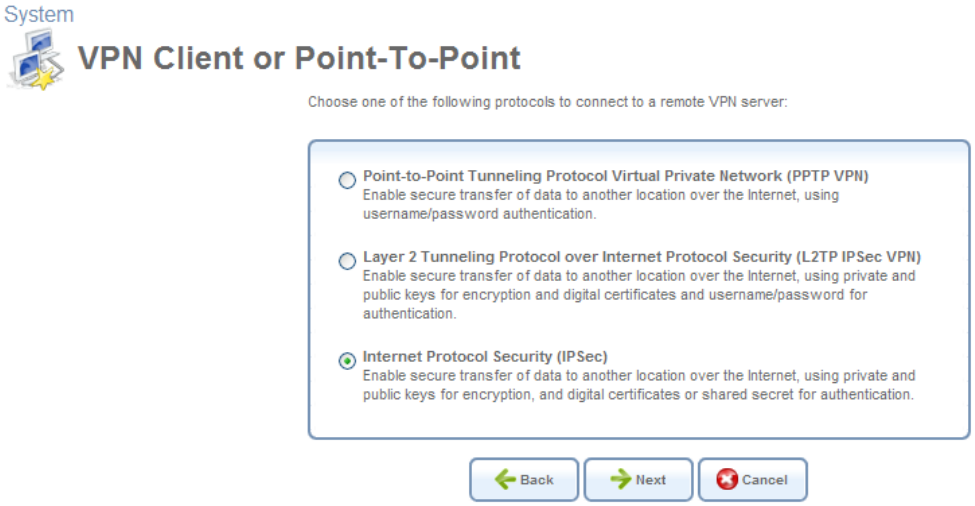


Figure 5.84 VPN Client or Point-To-Point

5. Select the 'Internet Protocol Security (IPSec)' radio button and click 'Next'. The 'Internet Protocol Security (IPSec)' screen appears.

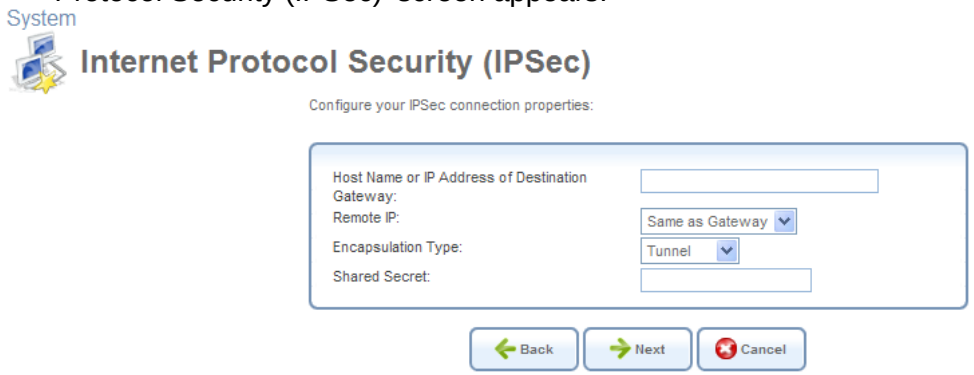


Figure 5.85 Internet Protocol Security (IPSec)

6. Specify the following parameters:

- **Host Name or IP Address of Destination Gateway** Specify 22.23.24.25
- **Remote IP** Select "Same as Gateway".
- **Encapsulation Type** Select "Tunnel".
- **Shared Secret** Enter "hr5x".

7. Click 'Next'. The 'Connection Summary' screen appears.

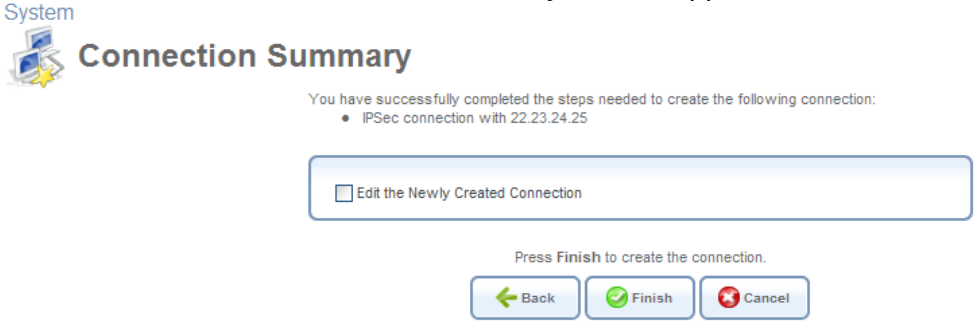


Figure 5.86 Connection Summary

8. Click ‘Finish’. The ‘Network Connections’ screen displays the newly created IPSec connection.

Figure 5.87 New VPN IPSec Connection

5.4.1.4.2 Configuring IPSec on the Windows Host

The following IP addresses are needed for the host configuration:

- Windows IP address – referred to as <windows_ip>.
- iPECS SBG-1000 WAN IP address – referred to as <iPECS SBG-1000_wan_ip>.
- iPECS SBG-1000 LAN Subnet address – referred to as <iPECS SBG-1000_lan_subnet>.

The configuration sequence:

1. Creating the IPSec Policy:

   a. Click the Start button and select Run. Type “secpol.msc” and click ‘OK’. The ‘Local Security Settings’ window appears.

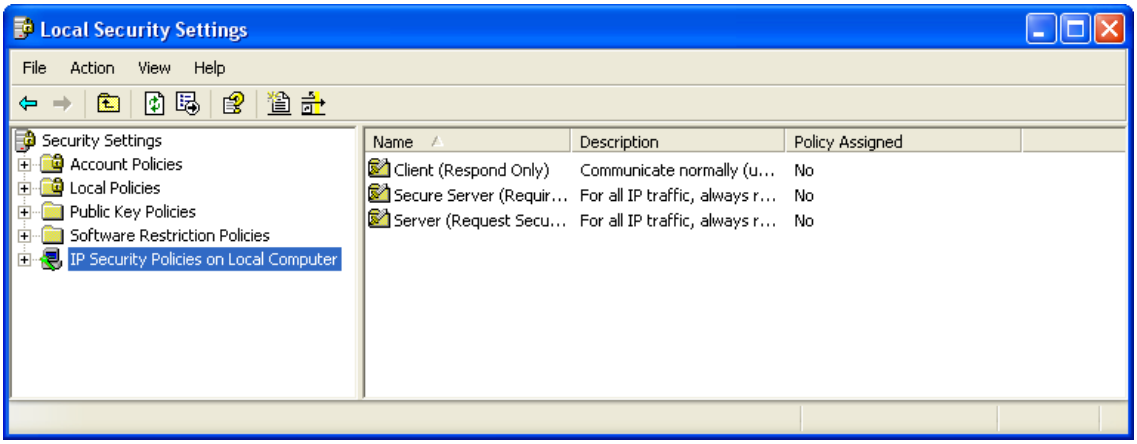


Figure 5.88 Local Security Settings

   b. Right-click the ‘IP Security Policies on Local Computer’ and choose ‘Create IP Security Policy...’. The IP Security Policy Wizard appears.

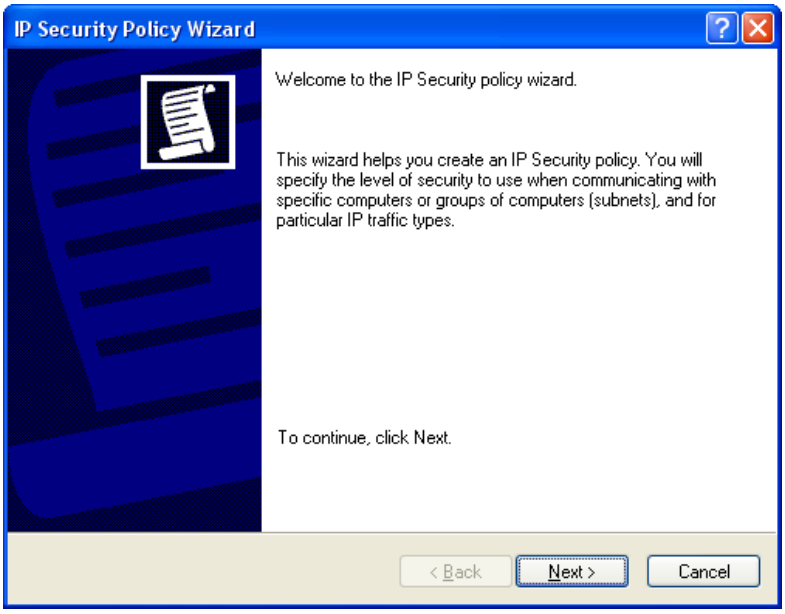


Figure 5.89 IP Security Policy Wizard

c. Click ‘Next’ and type a name for your policy, for example “iPECS SBG-1000 Connection”.

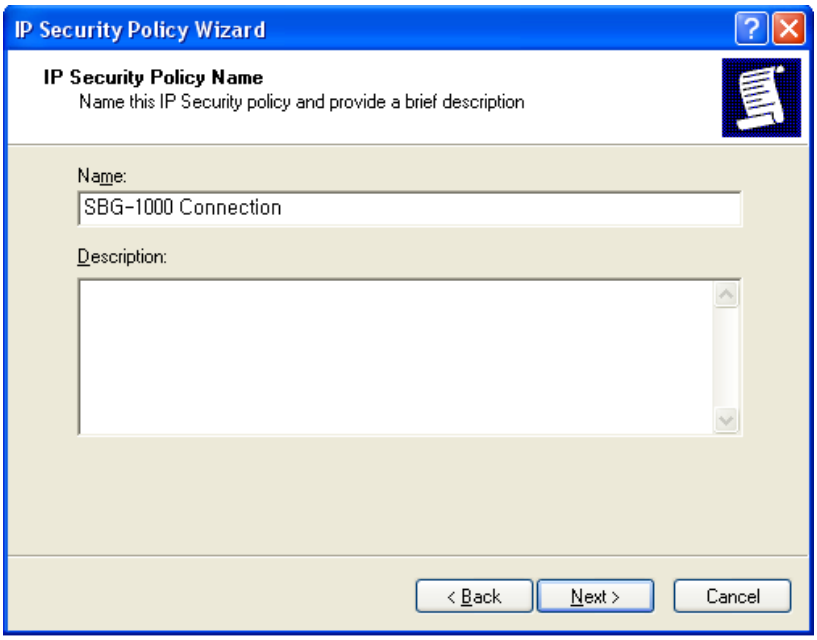


Figure 5.90 IP Security Policy Name

d. Click ‘Next’. The ‘Requests for Secure Communication’ screen appears.

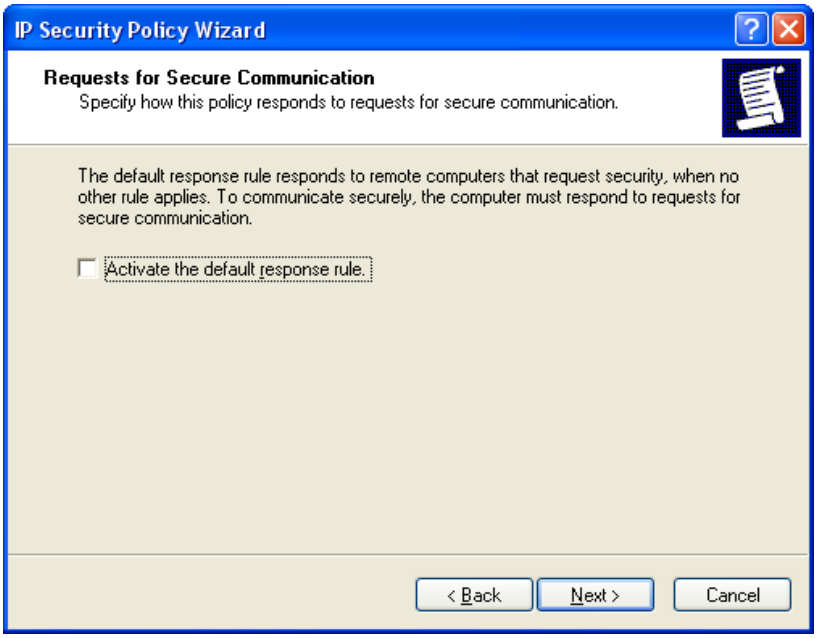


Figure 5.91 Requests for Secure Communication

e. Deselect the 'Activate the default response rule' check box, and click 'Next'. The 'Completing the IP Security Policy Wizard' screen appears.

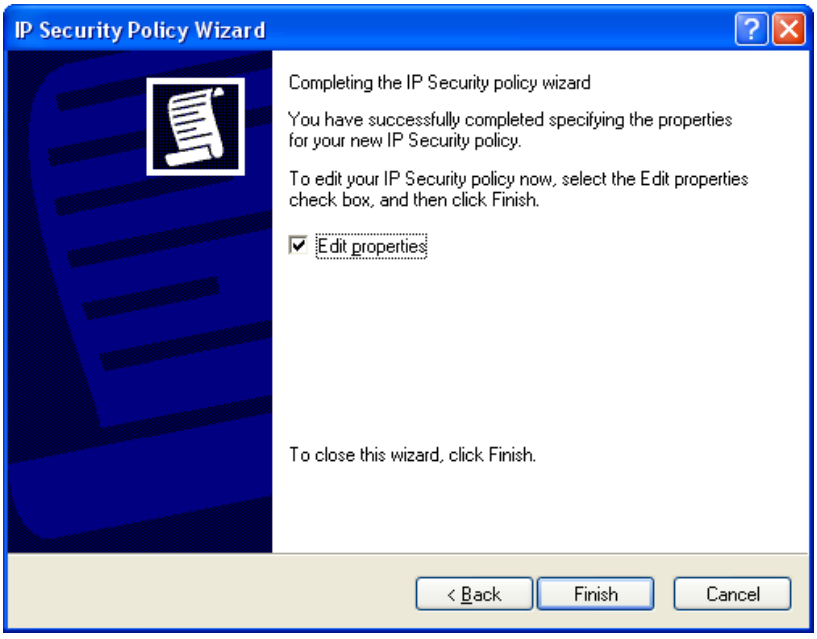


Figure 5.92 Completing the IP Security Policy Wizard

f. Make sure that the 'Edit Properties' check box is selected, and click 'Finish'. The 'iPECS SBG-1000 Connection Properties' window appears.

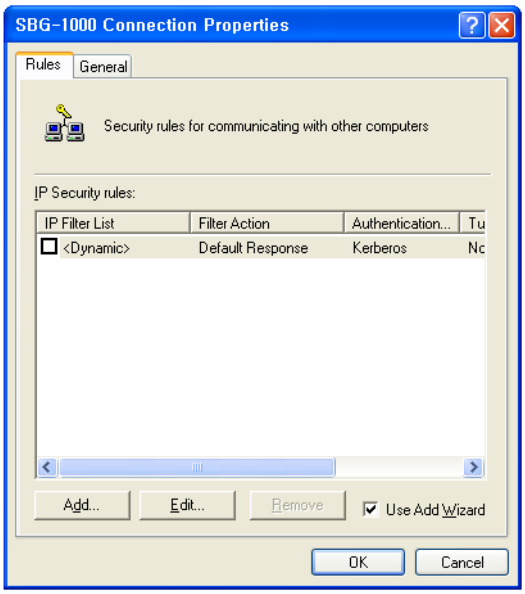


Figure 5.93 iPECS SBG-1000 Connection Properties

g. Click ‘OK’.

2. Building Filter List 1 – Windows XP to iPECS SBG-1000:

a. In the ‘Local Security Settings’ window, right-click the new ‘iPECS SBG-1000 Connection’ policy, created in the previous step, and select Properties. The Properties window appears (see Figure 5.93).

b. Deselect the ‘Use Add Wizard’ check box and click the ‘Add’ button to create a new IP Security rule. The ‘New Rule Properties’ window appears.

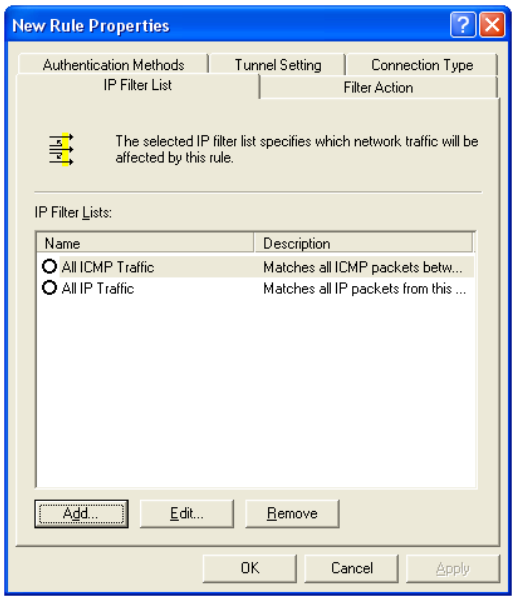


Figure 5.94 New Rule Properties

c. Under the IP Filter List tab, click the ‘Add’ button. The ‘IP Filter List’ window appears.

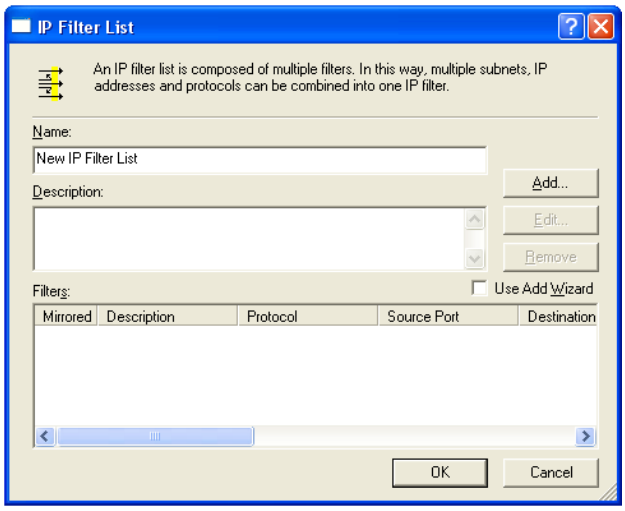


Figure 5.95 IP Filter List

d. Enter the name “Windows XP to iPECS SBG-1000” for the filter list, and deselect the ‘Use Add Wizard’ check box. Then, click the ‘Add’ button. The ‘Filter Properties’ window appears.

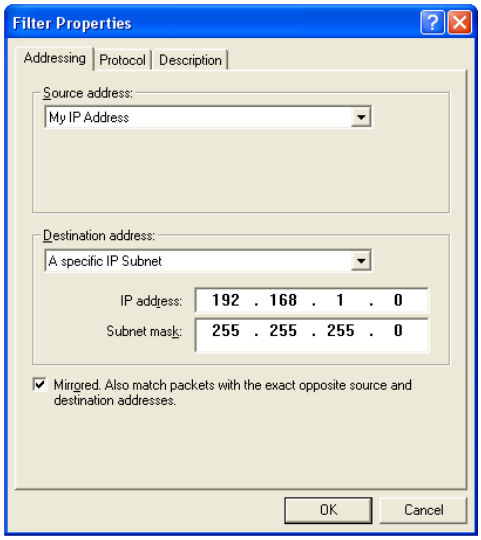


Figure 5.96 Filter Properties

e. In the ‘Source address’ drop-down menu, select ‘My IP Address’.

f. In the ‘Destination address’ drop-down menu, select ‘A Specific IP Subnet’. In the ‘IP Address’ field, enter the LAN Subnet (<iPECS SBG-1000_lan_subnet>), and in the ‘Subnet mask’ field enter 255.255.255.0.

g. Click the ‘Description’ tab if you would like to enter a description for your filter.

h. Click the ‘OK’ button. Click ‘OK’ again in the ‘IP Filter List’ window to save the settings.

3. Building Filter List 2 – iPECS SBG-1000 to Windows XP:

a. Under the IP Filter List tab of the ‘New Rule Properties’ window, click the ‘Add’ button. The ‘IP Filter List’ window appears (see Figure 5.95).

b. Enter the name “iPECS SBG-1000 to Windows XP” for the filter list, deselect the ‘Use Add Wizard’ check box, and click the ‘Add’ button. The ‘Filter Properties’ window appears.

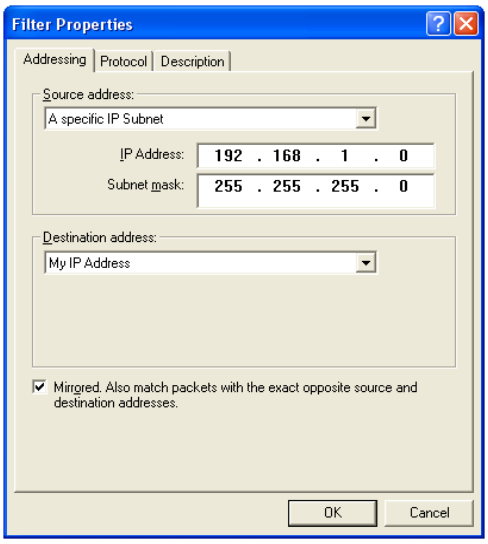


Figure 5.97 Filter Properties

c. In the ‘Source address’ drop-down menu, select ‘A Specific IP Subnet’. In the ‘IP Address’ field enter the LAN Subnet (<iPECS SBG-1000_lan_subnet>), and in the ‘Subnet mask’ field enter 255.255.255.0.

d. In the ‘Destination address’ drop-down menu, select ‘My IP Address’.

e. Click the ‘Description’ tab if you would like to enter a description for your filter.

f. Click the ‘OK’ button. Click ‘OK’ again in the ‘IP Filter List’ window to save the settings.

4. Configuring Individual Rule of Tunnel 1 (Windows XP to iPECS SBG-1000):

a. Under the ‘IP Filter List’ tab of the ‘New Rule Properties’ window, select the ‘Windows XP to iPECS SBG-1000’ radio button.

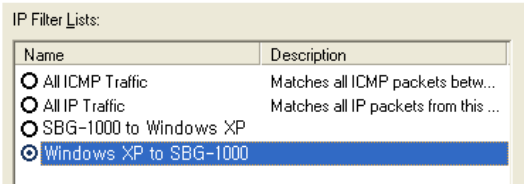


Figure 5.98 IP Filter List

b. Click the ‘Filter Action’ tab.

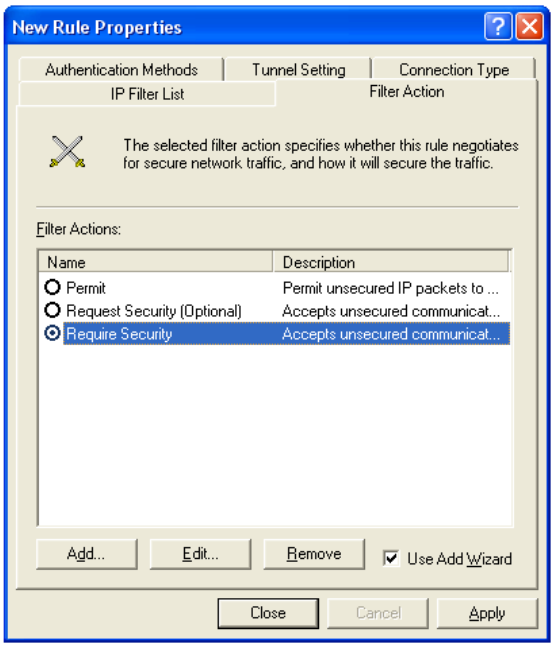


Figure 5.99 Filter Action

c. Select the ‘Require Security’ radio button, and click the ‘Edit’ button. The ‘Require Security Properties’ window appears.

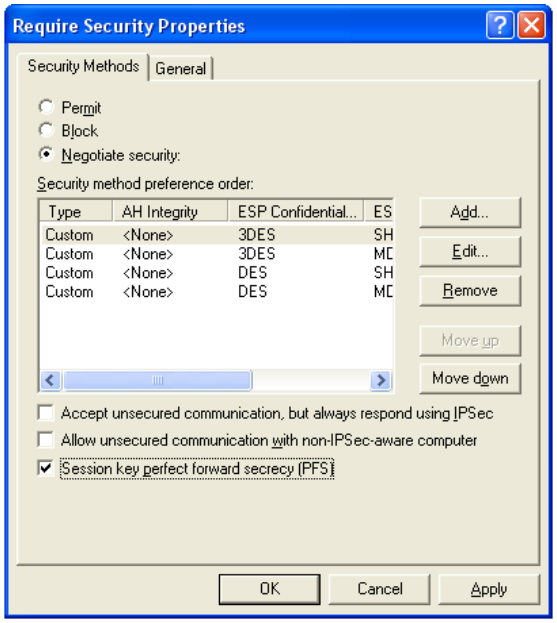


Figure 5.100 Require Security Properties

d. Verify that the ‘Negotiate security’ option is enabled, and deselect the ‘Accept unsecured communication, but always respond using IPSec’ check box. Select the ‘Session key Perfect Forward Secrecy (PFS)’ (the PFS option must be enabled on iPECS SBG-1000), and click the OK button.

e. Under the ‘Authentication Methods’ tab, click the Edit button. The ‘Edit Authentication

Method Properties' window appears.

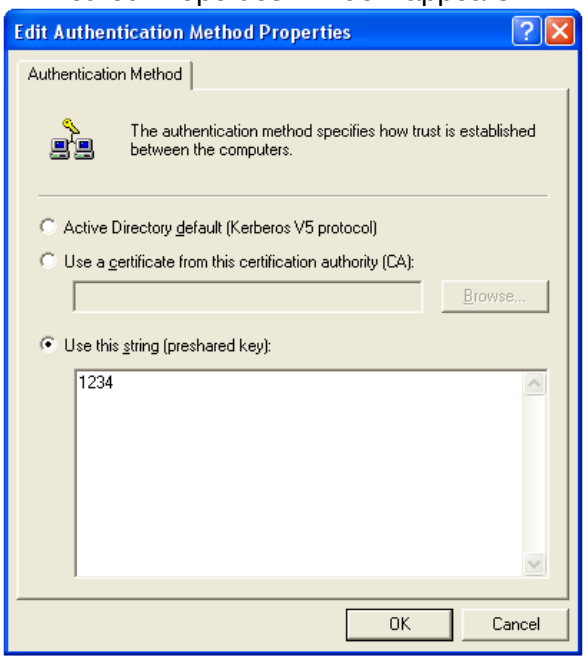


Figure 5.101 Edit Authentication Method Properties

f. Select the 'Use this string (preshared key)' radio button, and enter a string that will be used as the key (for example, 1234). Click the 'OK' button.

g. Under the 'Tunnel Setting' tab, select the 'The tunnel endpoint is specified by this IP Address' radio button, and enter <iPECS SBG-1000_wan_ip>.

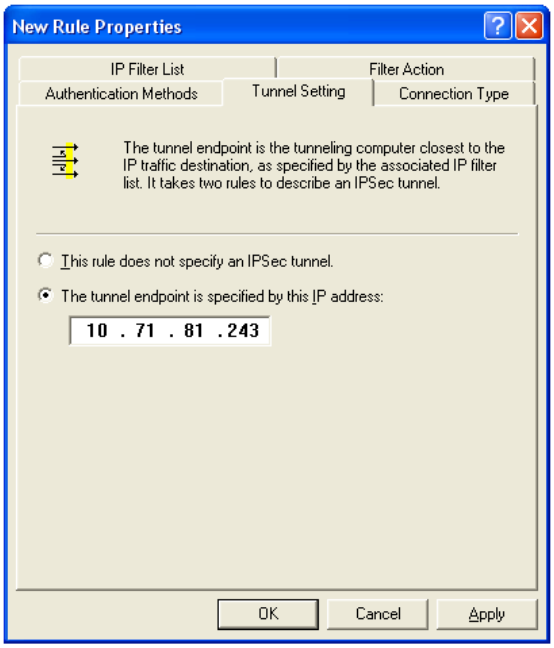


Figure 5.102 Tunnel Setting

h. Under the 'Connection Type' tab, verify that 'All network connections' is selected.

i. Click the ‘Apply’ button and then click the ‘OK’ button to save this rule.

5. Configuring Individual Rule of Tunnel 2 (iPECS SBG-1000 to Windows XP):

a. Under the ‘IP Filter List’ tab of the ‘New Rule Properties’ window, select the ‘iPECS SBG-1000 to Windows XP’ radio button.

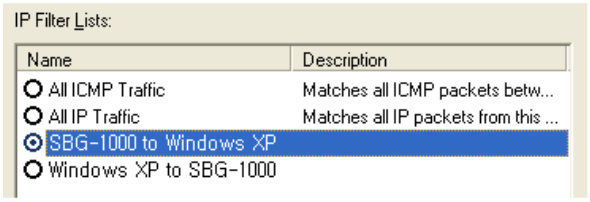


Figure 5.103 IP Filter List

b. Click the ‘Filter Action’ tab (see Figure 5.99).

c. Select the ‘Require Security’ radio button, and click the ‘Edit’ button. The ‘Require Security Properties’ window appears (see Figure 5.100).

d. Verify that the ‘Negotiate security’ option is enabled, and deselect the ‘Accept unsecured communication, but always respond using IPSec’ check box. Select the ‘Session key Perfect Forward Secrecy (PFS)’ (the PFS option must be enabled on iPECS SBG-1000), and click the OK button.

e. Under the ‘Authentication Methods’ tab, click the Edit button. The ‘Edit Authentication Method Properties’ window appears (see Figure 5.101).

f. Select the ‘Use this string (preshared key)’ radio button, and enter a string that will be used as the key (for example, 1234). Click the ‘OK’ button.

g. Under the ‘Tunnel Setting’ tab, select the ‘The tunnel endpoint is specified by this IP Address’ radio button, and enter <windows_ip>.

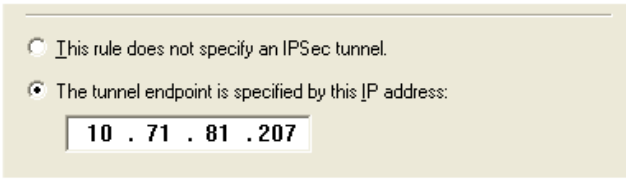


Figure 5.104 Tunnel Setting

h. Under the ‘Connection Type’ tab, verify that ‘All network connections’ is selected.

i. Click the ‘Apply’ button and then click the ‘OK’ button to save this rule.

j. Back on the ‘iPECS SBG-1000 Connection Properties’ window, note that the two new rules have been added to the ‘IP Security rules’ list.

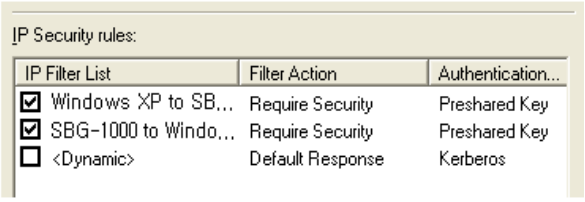


Figure 5.105 iPECS SBG-1000 Connection Properties

Click 'Close' to go back to the 'Local Security Settings' window (see Figure 5.88).

6. Assigning the New IPSec Policy: In the 'Local Security Settings' window, right-click the 'iPECS SBG-1000 Connection' policy, and select 'Assign'. A small green arrow will appear on the policy's folder icon and its status under the 'Policy Assigned' column will change to 'Yes'.

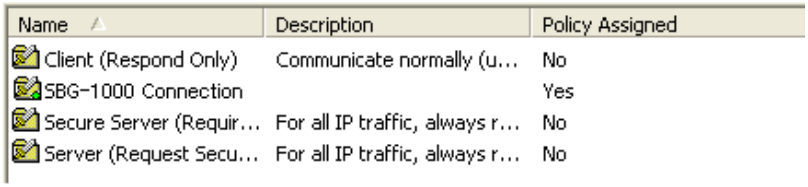


Figure 5.106 Local Security Settings

5.4.1.5 IPSec Gateway-to-Gateway Connection Scenario

Establishing an IPSec tunnel between Gateways A and B creates a transparent and secure network for clients from subnets A and B, who can communicate with each other as if they were inside the same network.

This section describes how to create a gateway to gateway IPSec tunnel with the following authentication methods:

- **Pre-shared Secret** – Developed by the VPN Consortium (VPNC). iPECS SBG-1000's VPN feature is VPNC certified.
- **RSA Signature** – A method using an RSA signature that is based on iPECS SBG-1000's public key.
- **Peer Authentication of Certificates** – A method using a Certificate Authority (CA).

This section describes the network configuration of both gateways, followed by the IPSec tunnel setup methods. The configurations of both gateways are identical, except for their IP addresses and the use of these addresses when creating the tunnel—the default gateway address of each gateway should be the WAN IP address of the other gateway.

Note: This section describes the configuration of Gateway A only. The same configuration must be performed on Gateway B, with the exceptions that appear in the note admonitions.

The following figure describes the IPSec tunnel setup, and contains all the IP addresses involved. Use it as a reference when configuring your gateways.

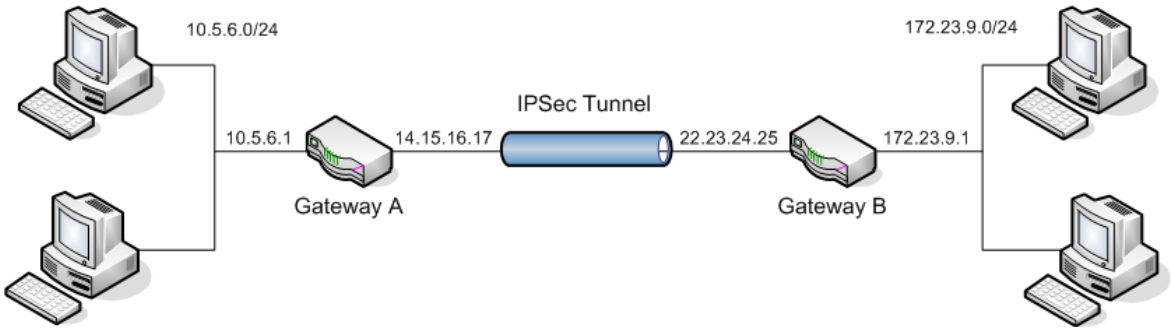


Figure 5.107 Configuration Diagram

5.4.1.5.1 Network Configuration

Before you can set up an IPSec connection, you must configure both of the gateways' LAN and WAN interface settings. This example contains specific IP addresses, which you can either use or substitute with your own.

- **LAN Interface Settings**

1. Under the 'System' tab, click the 'Network Connections' menu item. The 'Network Connections' screen appears.

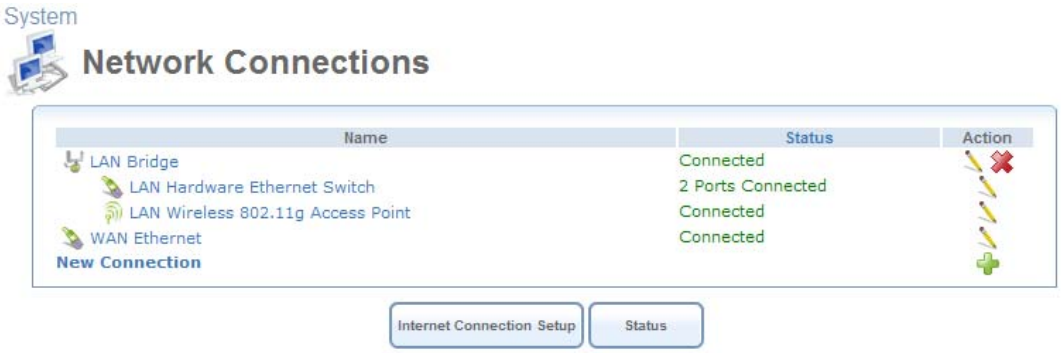


Figure 5.108 Network Connections

2. If your LAN Ethernet connection is bridged, click the 'LAN Bridge' link (as depicted in this example). Otherwise, click the 'LAN Ethernet' link. The 'LAN Bridge Properties' screen appears.

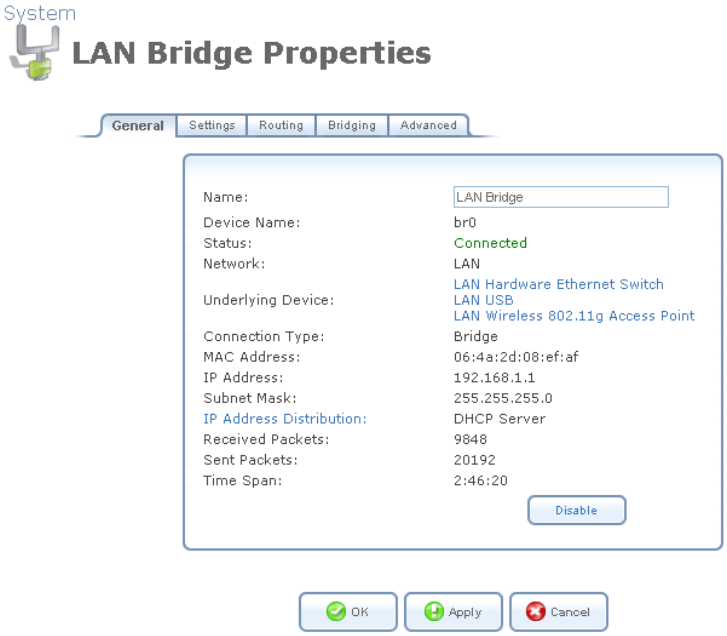


Figure 5.109 LAN Bridge Properties – General

3. Press the 'Settings' tab, and configure the following settings:

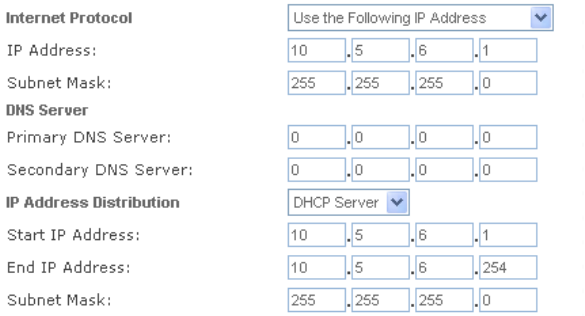


Figure 5.110 LAN Bridge Properties – Settings

Internet Protocol Select "Use the Following IP Address"
IP Address Specify 10.5.6.1
Subnet Mask Specify 255.255.255.0
IP Address Distribution Select "DHCP Server"
Start IP Address Specify 10.5.6.1
End IP Address Specify 10.5.6.254
Subnet Mask Specify 255.255.255.0

Note: When configuring Gateway B, the IP address should be 172.23.9.1, according to the example depicted here.

4. Click 'OK' to save the settings.

- **WAN Interface Settings**

1. Under the ‘System’ tab, click the ‘Network Connections’ menu item. The ‘Network Connections’ screen appears.

Figure 5.111 Network Connections

2. Click the ‘WAN Ethernet’ link, the ‘WAN Ethernet Properties’ screen appears.

Figure 5.112 WAN Ethernet Properties – General

3. Press the ‘Settings’ tab, and configure the following settings:

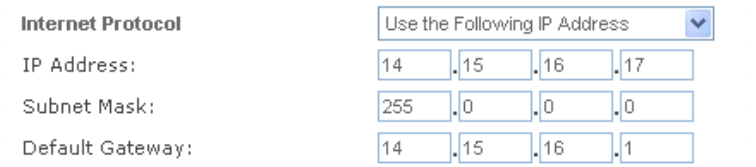


Figure 5.113 WAN Ethernet Properties – Settings

Internet Protocol Select “Use the Following IP Address”

IP Address Specify 14.15.16.17

Subnet Mask Specify the appropriate subnet mask, i.e 255.0.0.0

Default Gateway Specify the appropriate Default Gateway in order to enable IP routing, i.e 14.15.16.1


Note: When configuring Gateway B, the IP address should be 22.23.24.25, and the default gateway 22.23.24.1, according to the example depicted here.

4. Click ‘OK’ to save the settings.

5.4.1.5.2 Gateway-to-Gateway with Pre-shared Secrets

A typical gateway-to-gateway VPN uses a pre-shared secret for authentication. Gateway A connects its internal LAN 10.5.6.0/24 to the Internet. Gateway A’s LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17. Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B’s WAN (Internet) interface has the address 22.23.24.25. The Internet Key Exchange (IKE) Phase 1 parameters used are:

- Main mode
- 3DES (Triple DES)
- SHA-1
- MODP group 2 (1024 bits)
- Pre-shared secret of “hr5x”
- SA lifetime of 28800 seconds (eight hours)

The IKE Phase 2 parameters used are:

- 3DES (Triple DES)
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for re-keying
- SA lifetime of 3600 seconds (one hour)
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

To set up Gateway A for this scenario, follow these steps:

1. Under the ‘System’ tab, click the ‘Network Connections’ menu item. The ‘Network Connections’ screen appears.

Figure 5.114 Network Connections

2. Click the 'New Connection' link. The 'Connection Wizard' screen appears.

Figure 5.115 Connection Wizard

3. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears.

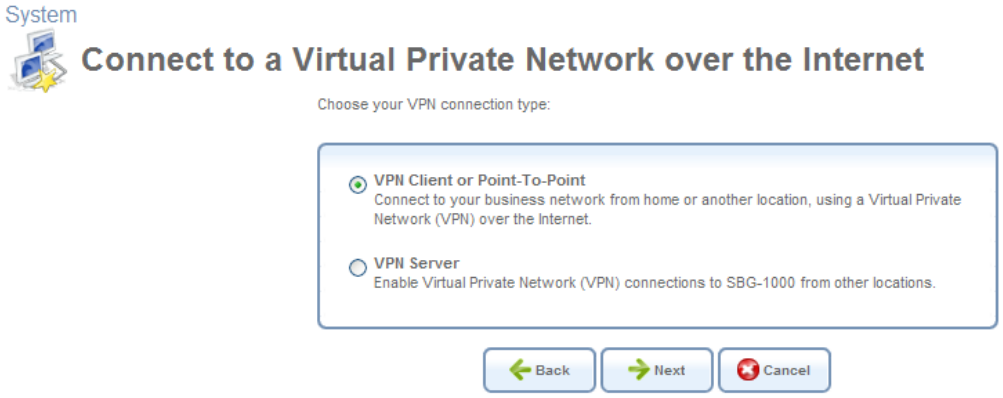


Figure 5.116 Connect to a Virtual Private Network over the Internet

4. Select the 'VPN Client or Point-To-Point' radio button and click 'Next'. The 'VPN Client or Point-To-Point' screen appears.

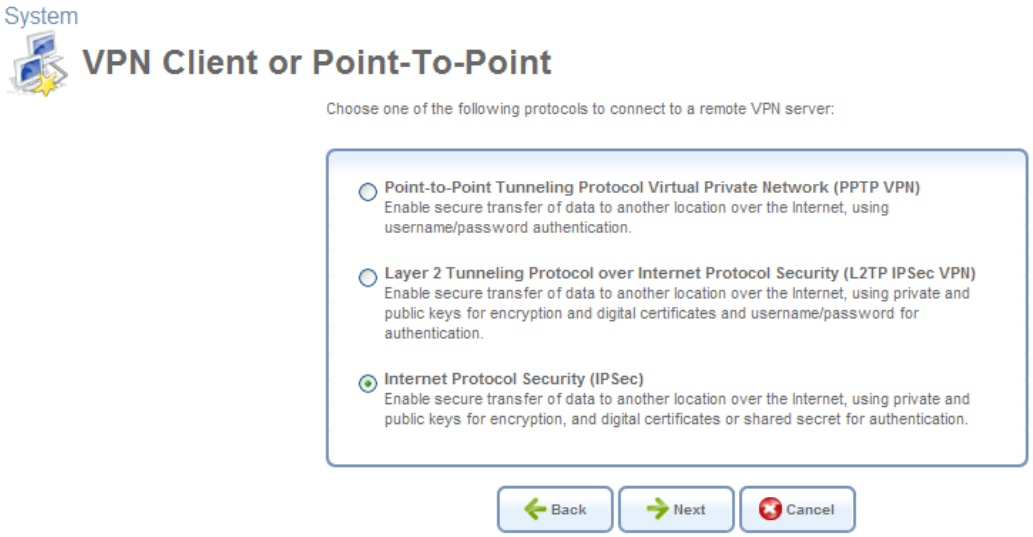


Figure 5.117 VPN Client or Point-To-Point

5. Select the 'Internet Protocol Security (IPSec)' radio button and click 'Next'. The 'Internet Protocol Security (IPSec)' screen appears.

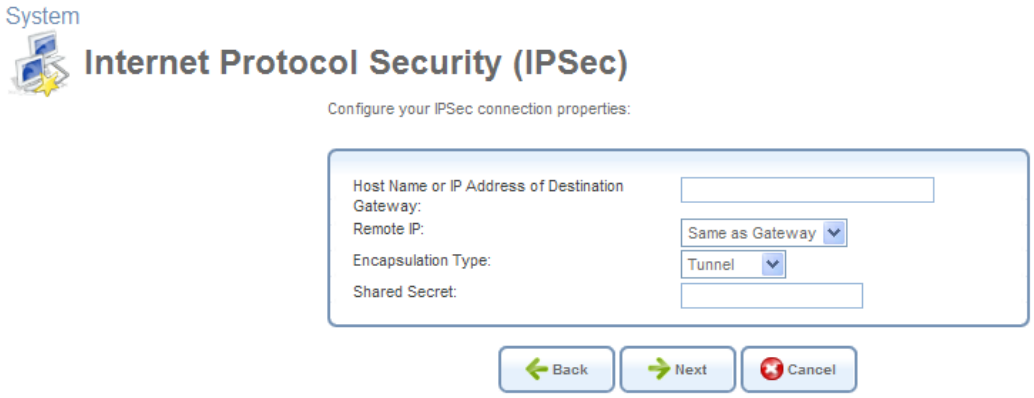


Figure 5.118 Internet Protocol Security (IPSec)

6. Specify the following parameters, as depicted in Figure 5.119.

Host Name or IP Address of Destination Gateway Specify 22.23.24.25

Remote IP Select "IP Subnet"

Remote Subnet IP Address Specify 172.23.9.0

Remote Subnet Mask Specify 255.255.255.0

Shared Secret Specify "hr5x"

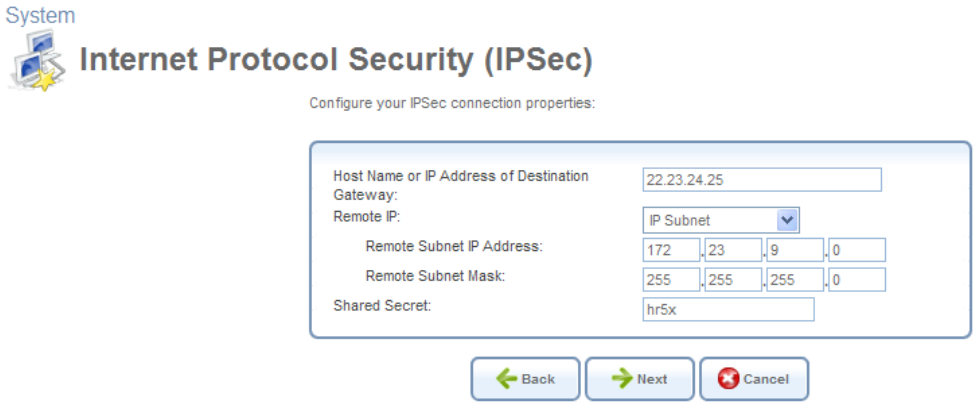


Figure 5.119 Internet Protocol Security (IPSec)

Note: When configuring Gateway B, the IP Address of Destination Gateway should be 14.15.16.17, and the Remote Subnet IP Address should be 10.5.6.0, according to the example depicted here.

7. Click ‘Next’, the ‘Connection Summary’ screen appears.

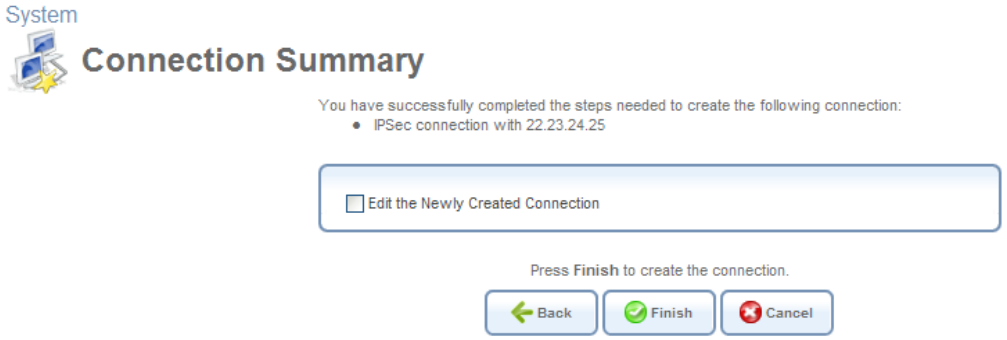


Figure 5.120 Connection Summary

8. Select the ‘Edit the Newly Created Connection’ check box, and click ‘Finish’. The ‘VPN IPSec Properties’ screen appears, displaying the ‘General’ tab.

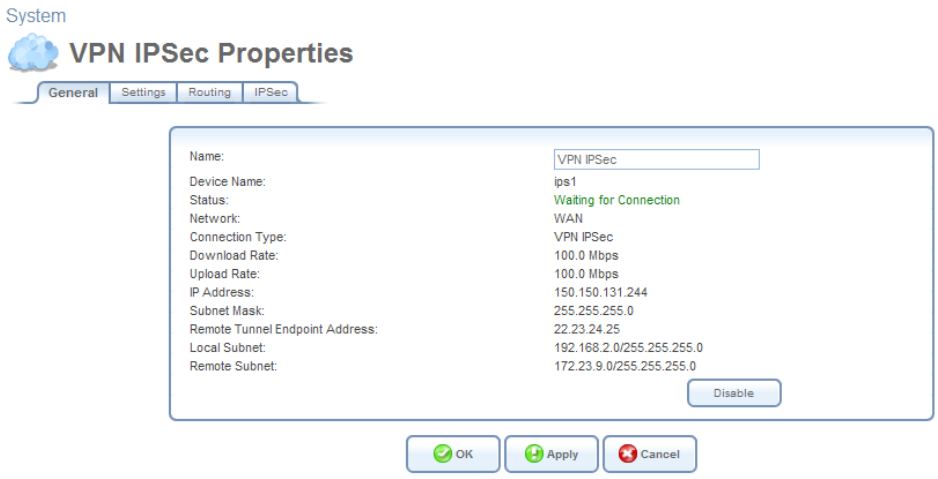


Figure 5.121 VPN IPSec Properties – General

9. Click the ‘IPSec’ tab, and configure the following settings:
   - Deselect the ‘Compress’ check box.
   - Under ‘Hash Algorithm’, deselect the ‘Allow Peers to Use MD5’ check box.
   - Under ‘Group Description Attribute’, deselect the ‘DH Group 5’ check box.
   - Under ‘Encryption Algorithm’, deselect the ‘Allow AH Protocol (No Encryption)’ check box.
10. Click ‘OK’ to save the settings.

Perform the same procedure on Gateway B with its respective parameters. When done, the IPSec connection’s status should change to “Connected”.

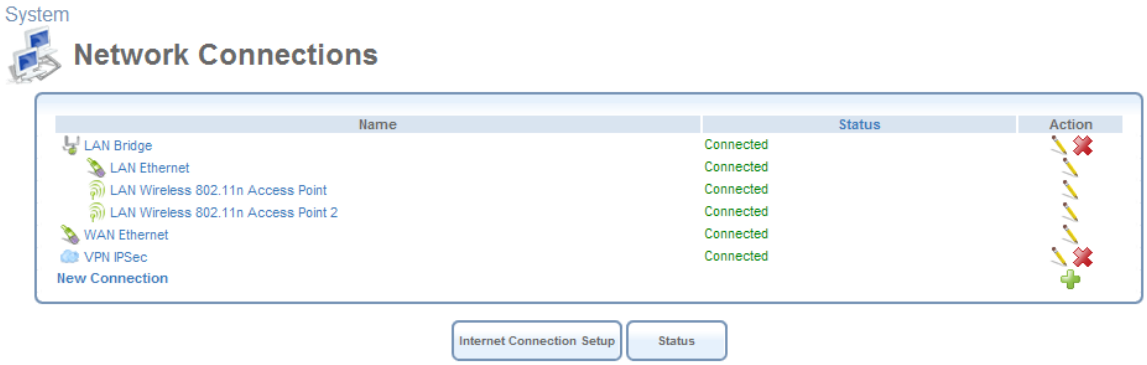


Figure 5.122 Connected VPN IPSec Connection

5.4.1.5.3 Gateway-to-Gateway with an RSA Signature

The RSA signature, which is part of the RSA encryption mechanism, is an additional method available on iPECS SBG-1000 for providing peer authentication in a VPN IPSec connection. The RSA signature can be created in iPECS SBG-1000 on the basis of its public key. When using this method, the two gateways must be configured with each other’s RSA signature, as further explained in this section.

To enable the gateway-to-gateway VPN IPSec connection using the RSA signature, perform the following:

1. Create a VPN IPSec connection on each gateway as described in Section 5.8.1.5.2.
2. In iPECS SBG-1000 A, go to the ‘Shortcut’ screen, and click the ‘IPSec’ icon. The ‘Internet Protocol Security (IPSec)’ screen appears.

Figure 5.123 Internet Protocol Security (IPSec)

3. Click the ‘Settings’ button. The ‘Internet Protocol Security (IPSec) Settings’ screen appears, displaying iPECS SBG-1000’s public key.

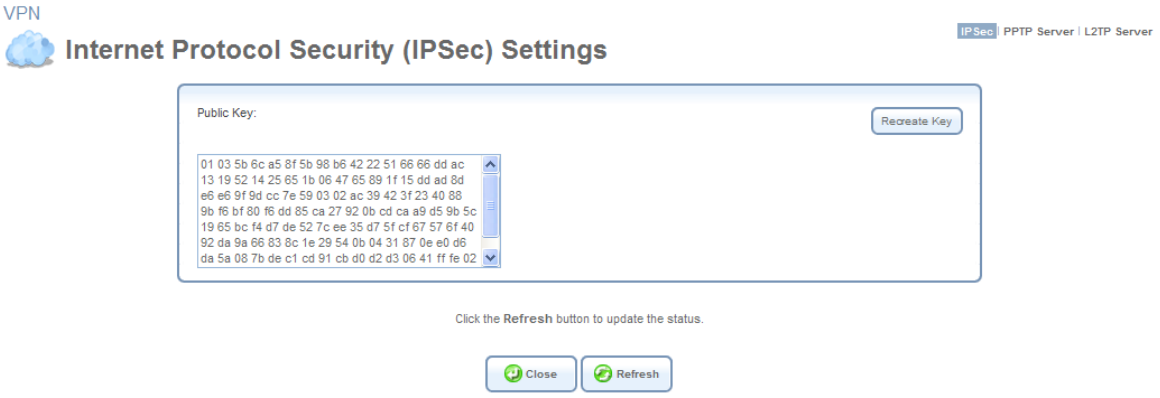


Figure 5.124 Internet Protocol Security (IPSec) Settings

4. Copy the public key and paste it into a text editor.

5. Remove all spaces from the public key so that it will appear as one string.

6. In iPECS SBG-1000 B, click the ‘VPN’ menu item under the ‘Services’ tab. The ‘Internet Protocol Security (IPSec)’ screen appears, displaying the VPN IPSec connection you have created (see Figure 5.123).

7. Click the connection’s action icon, and select the ‘IPSec’ sub-tab of the ‘VPN IPSec Properties’ screen that appears (see Figure 5.121).

8. From the ‘Peer Authentication’ drop-down menu, select the ‘RSA Signature’ option. The screen refreshes, displaying the ‘RSA Signature’ text field.

9. In the text field, type 0x and paste the public key string from the text editor.

10. Repeat the same procedure for configuring iPECS SBG-1000 A with the RSA signature of iPECS SBG-1000 B. When done, the IPSec connection’s status on both gateways should change to ‘Connected’.

5.4.1.5.4 Gateway-to-Gateway with Certificate-based Peer Authentication

An additional authentication method for a gateway-to-gateway VPN is peer authentication of certificates. Authentication is performed when each gateway presents a certificate, signed by a mutually agreed upon Certificate Authority (CA), to the other gateway.

For testing purposes, Linux provides a mechanism for creating self-signed certificates, thus eliminating the need to acquire them from the CA. This section provides a description for this procedure, after which you will be able to use these certificates for authentication of the gateway-to-gateway VPN connection.

To create a self-signed certificate, perform the following:

1. Running as root, install the OpenSSL Debian package:

```
# apt-get install openssl
```

2. Switch back to a regular user, and create a directory for the certificates:

```
$ cd ~
$ mkdir cert_create
$ cd cert_create/
```

3. Use the Linux ‘CA.sh’ utility. Note that only the required fields are listed below. For the rest, you may simply press Enter.

```
$ /usr/lib/ssl/misc/CA.sh -newca
    Enter PEM pass phrase: <enter a password>
    Common Name: <enter your CA name>
    Enter pass phrase for ./demoCA/private/./cakey.pem: <enter a password>
```

   For more information about this script, run ‘man CA.pl’ (CA.pl and CA.sh are the same).

4. Copy the certificates from the /demoCA directory under which they were created, providing them with your CA name.

```
$ cp demoCA/cacert.pem <your CA name>_cacert.pem
$ cp demoCA/careq.pem <your CA name>_careq.pem
```

5. Load the new certificates to both gateways:

   a. Browse to the ‘Shortcut’ tab and click the ‘Certificates’ icon.

   b. Select the ‘CA’s’ sub-tab and click ‘Upload Certificate’. The ‘Load CA’s Certificate’ screen appears.

   c. Browse for the location of the certificate, which is ~**/cert_create/<your CA name>_cacert.pem**, and click ‘Upload’.

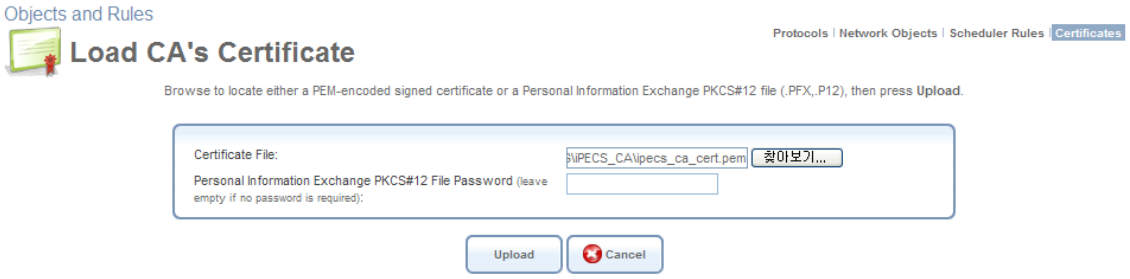


Figure 5.125 Load CA's Certificate

6. Generate a certificate request from both gateways:

   a. Browse to the 'Shortcut' tab and click the 'Certificates' icon.

   b. In the 'iPECS SBG-1000's Local' sub-tab, click 'Create Certificate Request'. The 'Create X509 Request' screen appears.

   c. In the 'Certificate Name' field, enter "iPECS SBG-1000-1" (and "iPECS SBG-1000-2" on the other gateway, respectively).

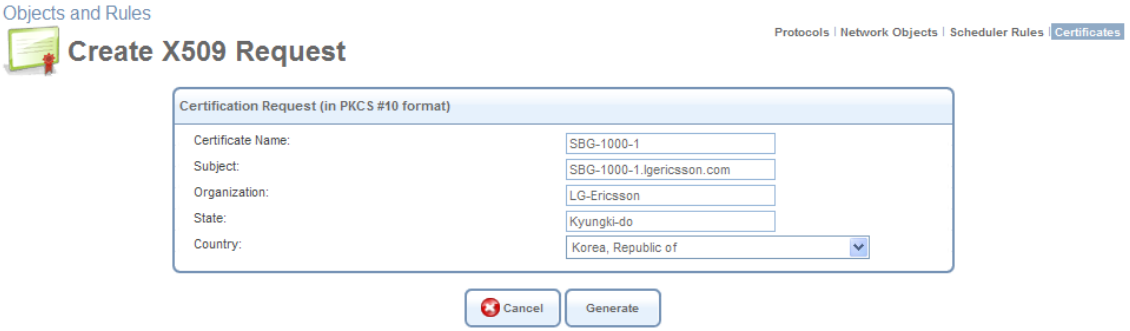


Figure 5.126 Create X509 Request

   d. Click 'Generate' and then 'Refresh'. The 'New X509 Request' screen appears.

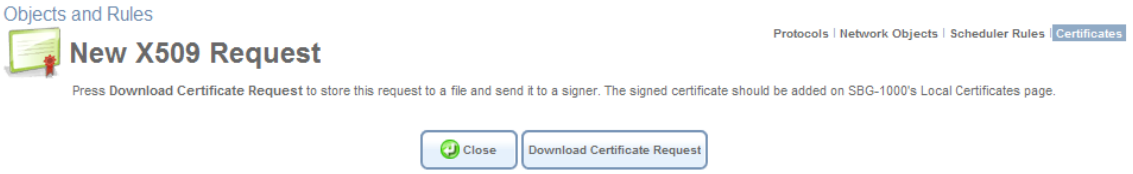


Figure 5.127 New X509 Request

   e. Click 'Download Certificate Request', and save the file under **~/cert_create/iPECS SBG-1000-1/2.csr.**

Note: Do not delete the empty certificate that now appears under the 'iPECS SBG-1000's Local' sub-tab, as this is the request itself. If you delete it, the certificate will not be accepted by iPECS SBG-1000.

7. Sign the certificate request using the 'CA.sh' script on both gateways:

```
$ mv <iPECS SBG-1000-1>.csr newreq.pem
$ /usr/lib/ssl/misc/CA.sh -sign
      Enter pass phrase for ./demoCA/private/cakey.pem: <enter a password>
      Sign the certificate? [y/n]: <choose y>
      1 out of 1 certificate requests certified, commit? [y/n] <choose y>
$ mv newcert.pem <iPECS SBG-1000-1>_newcert.pem
$ mv newreq.pem <iPECS SBG-1000-1>_newreq.pem

<Repeat the above for iPECS SBG-1000-2>
```

8. Load the certificates to both gateways:
   a. Browse to the ‘Shortcut’ tab and click the ‘Certificates’ icon.

   b. In the ‘iPECS SBG-1000’s Local’ sub-tab, click ‘Upload Certificate’. The ‘Load iPECS SBG-1000’s Local Certificate’ screen appears.

   c. Browse to the location of the certificate, which is **~/cert_create/<iPECS SBG-1000-1/2>_newcert.pem**, and click ‘Upload’.

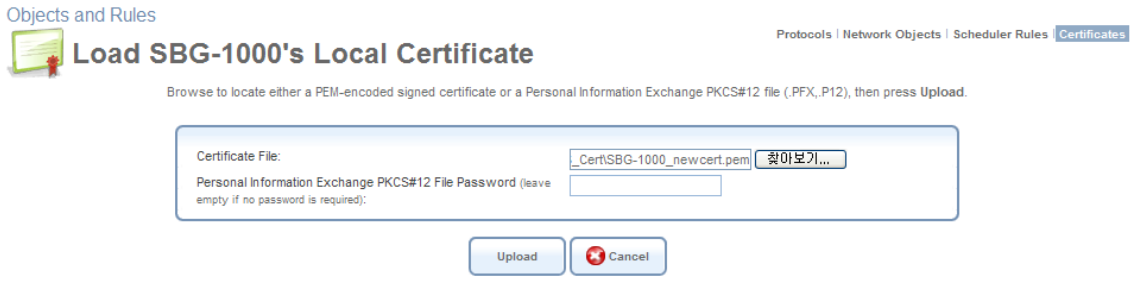


Figure 5.128 Load iPECS SBG-1000’s Local Certificate

To authenticate the VPN connection with the created certificates, perform the following:

1. Click the ‘VPN IPSec’ link in the ‘Network Connections’ screen, and then click the ‘IPSec’ sub-tab.

2. In the ‘IPSec Automatic Phase 1’ section, in the ‘Peer Authentication’ drop-down menu, select “Certificate”. The screen refreshes, providing additional settings.

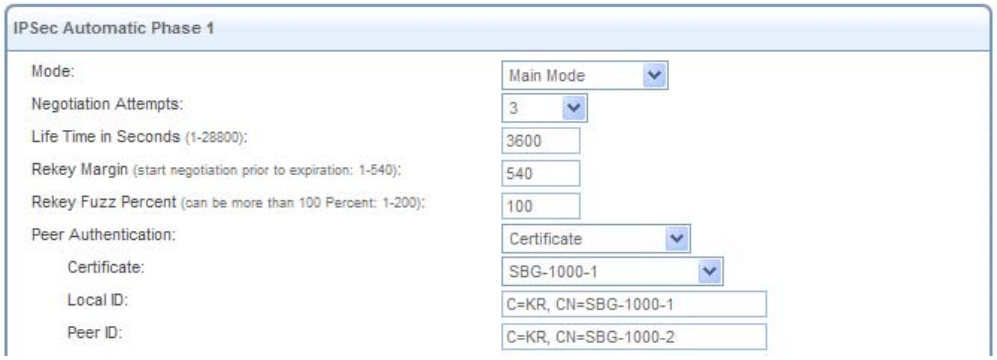


Figure 5.129 VPN IPSec Properties

3. In the ‘Certificate’ drop-down menu, select Gateway A’s newly added certificate.

4. In the ‘Local ID’ field, enter Gateway A’s certificate details. You can copy these details from the ‘Certificates’ screen under the ‘Shortcut’ tab. Click the certificate and copy the details from the subject field, for example “C=KR, CN=iPECS SBG-1000-1”.

5. In the ‘Peer ID’ field, enter Gateway B’s certificate details, for example “C=KR, CN=iPECS SBG-1000-2”.

6. Click ‘OK’ to save the settings.

Perform the same procedure on Gateway B with its respective parameters. When done, the IPSec connection’s status should change to “Connected”.

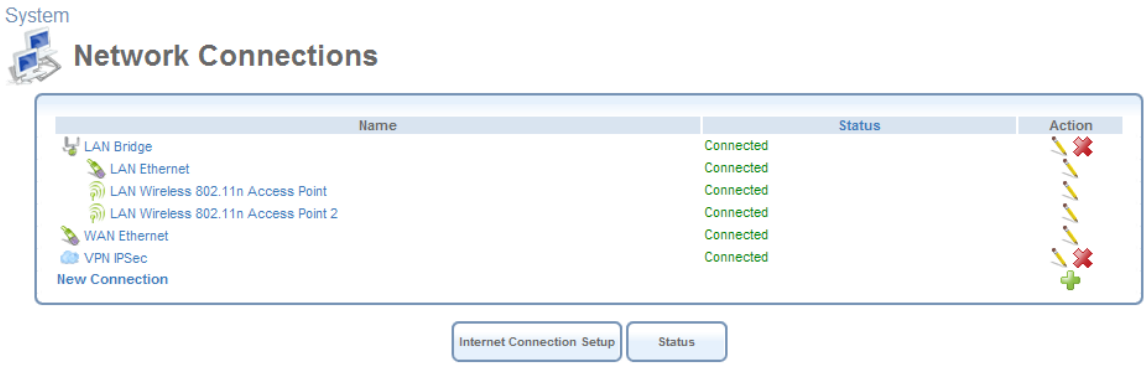


Figure 5.130 Connected VPN IPSec Connection

5.4.2 Point-to-Point Tunneling Protocol Server

iPECS SBG-1000 can act as a Point-to-Point Tunneling Protocol Server (PPTP Server), accepting PPTP client connection requests.

5.4.2.1 Configuring the PPTP Server

Access this feature either from its link in the ‘VPN’ tab under the ‘Services’ screen, or by clicking the ‘PPTP Server’ icon in the ‘Shortcut’ screen. The ‘Point-to-Point Tunneling Protocol Server (PPTP Server)’ screen appears:

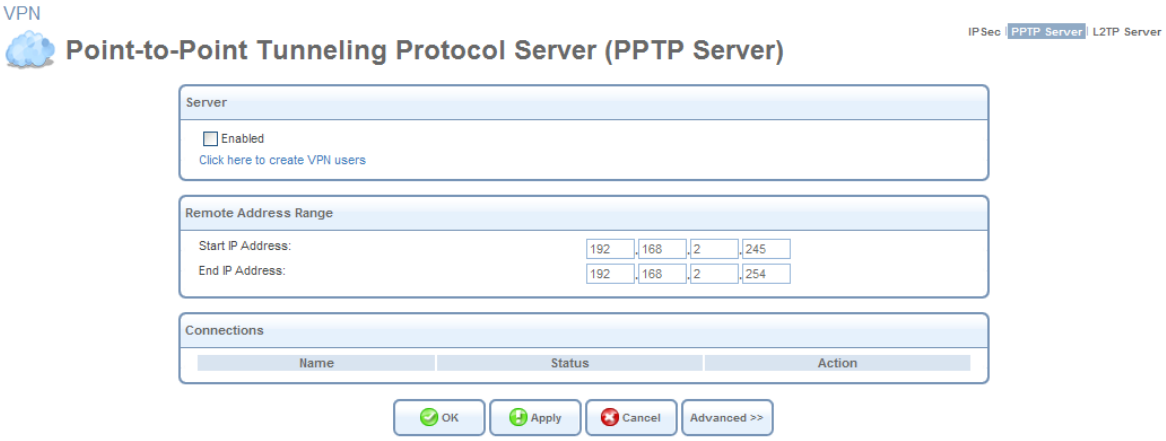


Figure 5.131 Point-to-Point Tunneling Protocol Server (PPTP Server)

This screen enables you to configure:

Enabled Select or deselect this check box to enable or disable this feature.

Note that checking this box creates a PPTP server (if not yet created with the wizard), but does not define remote users.

Click Here to Create VPN Users Click this link to define remote users that will be granted access to your home network. Refer to Section 6.3 to learn how to define and configure users.

Remote Address Range Use the 'Start IP Address' and 'End IP Address' fields to specify the range of IP addresses that will be granted by the PPTP server to the PPTP client.

5.4.2.2 Advanced PPTP Server Settings

To configure advanced PPTP server settings press the 'Advanced' button on the PPTP screen (see Figure 5.131). The screen expands, offering additional settings:

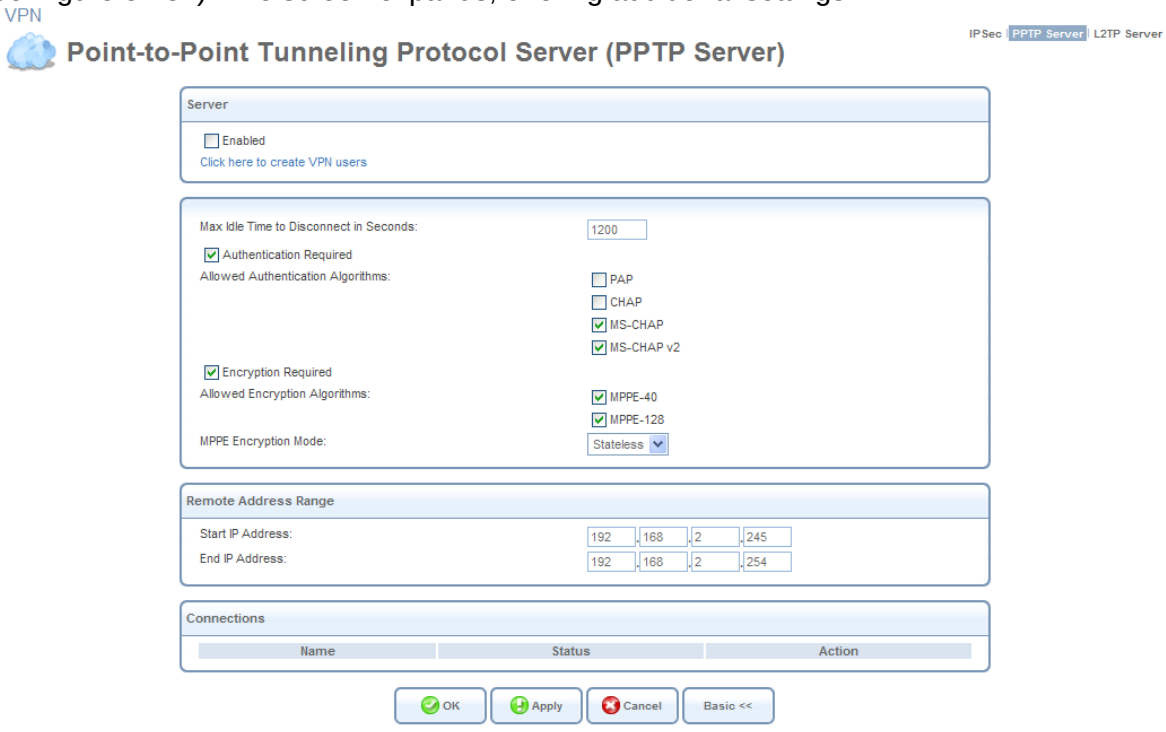


Figure 5.132 Advanced PPTP Server Parameters

Maximum Idle Time to Disconnect in Seconds Specify the amount of idle time (during which no data is sent or received) that should elapse before the gateway disconnects a PPTP connection.
Authentication Required Select whether PPTP will use authentication.
Allowed Authentication Algorithms Select the algorithms the server may use when authenticating its clients.
Encryption Required Select whether PPTP will use encryption.
Allowed Encryption Algorithms Select the algorithms the server may use when encrypting data.
MPPE Encryption Mode Select the Microsoft Point-to-Point Encryption mode: stateless or stateful.

Note that the server settings must be in tune with the client settings, described in Section 6.4.10.

5.4.3 Layer 2 Tunneling Protocol Server

iPECS SBG-1000 can act as a Layer 2 Tunneling Protocol Server (L2TP Server), accepting L2TP client connection requests.

5.4.3.1 Configuring the L2TP Server

Access this feature either from the 'VPN' menu item under the 'Services' tab, or by clicking the 'L2TP Server' icon in the 'Shortcut' screen. The 'Layer 2 Tunneling Protocol Server (L2TP Server)' screen appears.

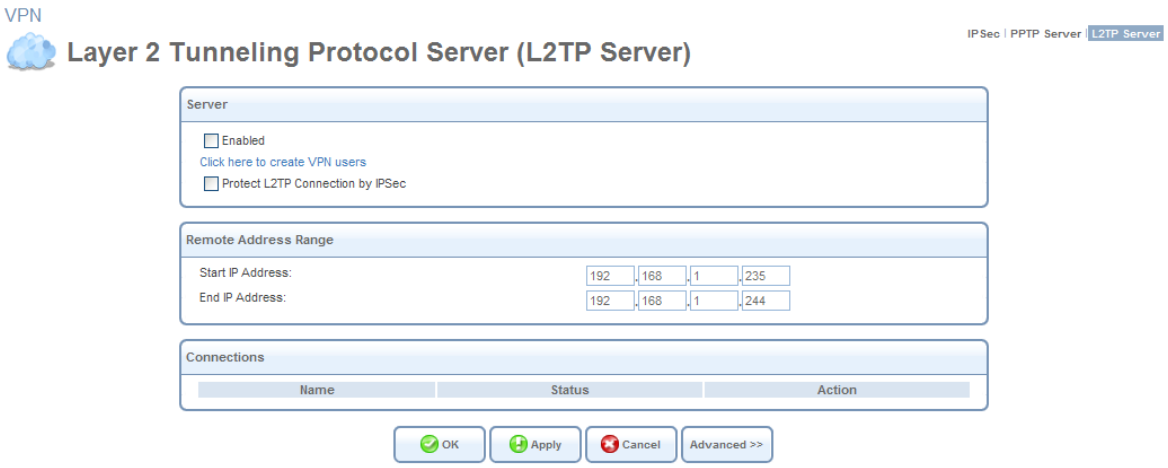


Figure 5.133 Layer 2 Tunneling Protocol Server (L2TP Server)

This screen enables you to configure the following connection settings:
Enabled Select or deselect this check box to enable or disable this feature.
Note that selecting this box creates an L2TP server (if not yet created with the wizard), but does not define remote users.
Click Here to Create VPN Users Click this link to define remote users that will be granted access to your home network. Refer to Section 6.3 to learn how to define and configure users.
Protect L2TP Connection by IPSec By default, the L2TP connection is not protected by the IP

Security (IPSec) protocol. Select this option to enable this feature. When enabled, the following entry appears.

Create Default IPSec Connection When creating an L2TP Server with the connection wizard, a default IPSec connection is created to protect it. If you wish to disable this feature, uncheck this option. However, note that if L2TP protection is enabled by IPSec (see previous entry), you must provide an alternative, active IPSec connection in order for users to be able to connect. When this feature is enabled, the following entry appears.

L2TP Server IPSec Shared Secret You may change the IPSec shared secret, provided when the connection was created, in this field.

Remote Address Range Use the 'Start IP Address' and 'End IP Address' fields to specify the range of IP addresses that will be granted by the L2TP server to the L2TP client.

5.4.3.2 Advanced L2TP Server Settings

To configure advanced L2TP server settings, click the 'Advanced' button in the L2TP Server screen (see Figure 5.133). The screen expands, offering additional settings.

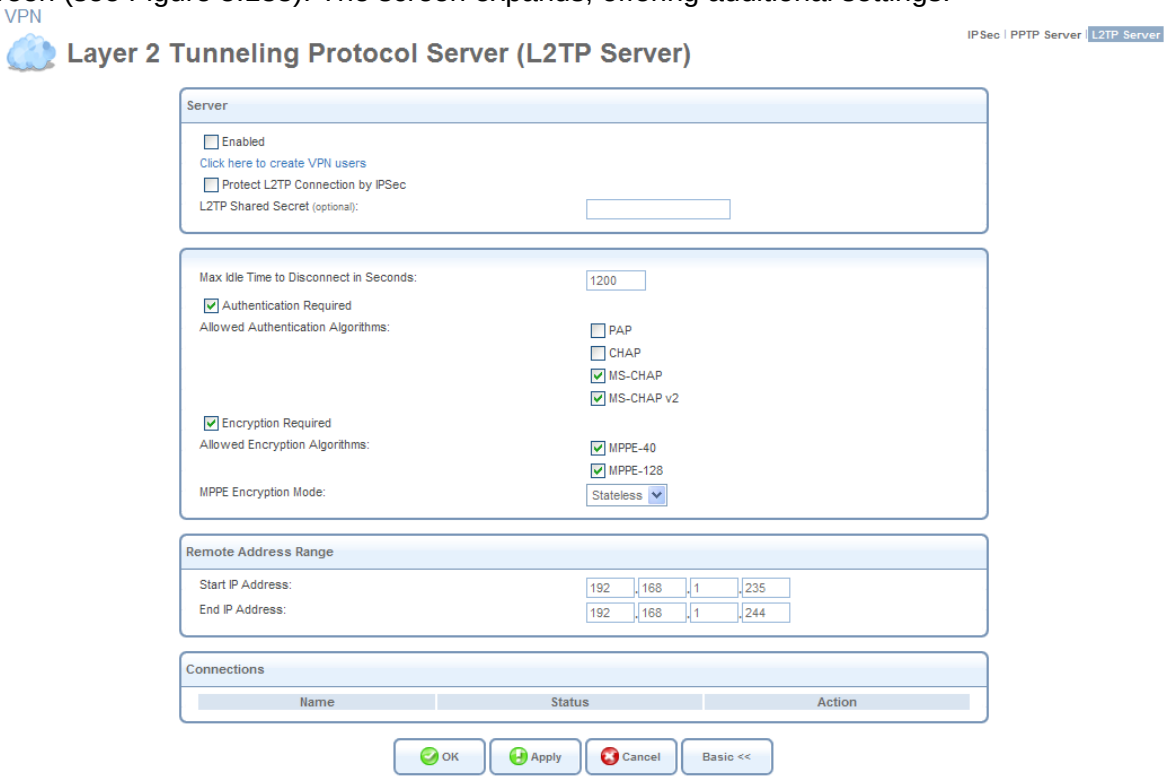


Figure 5.134 Advanced L2TP Server Parameters

L2TP Shared Secret (optional) Use this optional field to define a shared secret for the L2TP connection, for added security.

Maximum Idle Time to Disconnect in Seconds Specify the amount of idle time (during which no data is sent or received) that should elapse before the gateway disconnects the L2TP connection.

Authentication Required Select whether L2TP will use authentication.

Allowed Authentication Algorithms Select the algorithms the server may use when authenticating its clients.

Encryption Required Select whether L2TP will use encryption.
Allowed Encryption Algorithms Select the algorithms the server may use when encrypting data.
MPPE Encryption Mode Select the Microsoft Point-to-Point Encryption mode: stateless or stateful.

5.4.3.3 Configuring an L2TP over IPSec VPN Client

If you wish to connect to iPECS SBG-1000's L2TP server (with the default IPSec configuration) using the Windows IPSec client, configure your host's L2TP connection with the following:

- Your login credentials (for more information, refer to Section 6.3)
- The L2TP server's IPSec shared secret (for more information, refer to Section 5.4.3.1).
- The L2TP server's IP address (iPECS SBG-1000's WAN address)

In case you wish to use a third-party IPSec client (for example, Netscreen) with your L2TP connection, configure the client with the following parameters. Note that these parameters match the gateway's default IPSec VPN connection parameters.

Remote Party's Identity
- **ID Type** Select 'IP Address', and specify iPECS SBG-1000's WAN IP address.
- **Protocol** Select UDP.
- **Port** Select L2TP 1701.

My Identity
- **ID Type** Select 'IP Address'.
- **Port** Select L2TP 1701.

Security Policy Select the 'Main' mode.

Phrase 1 Negotiation Mode
- Select 'IPSec Shared Secret' as the peer authentication method, and enter the shared secret defined in the L2TP server's IPSec VPN settings.
- Define the encryption algorithm—by default, iPECS SBG-1000 supports the 3DES-CBC algorithm.
- Define the hash algorithm—iPECS SBG-1000 supports both the MD5 and SHA1 algorithms.
- Define the Key group—by default, iPECS SBG-1000 supports Diffie-Hellman (DH) Group 2 and Group 5.

Phrase 2 Negotiation Mode
- Enable the 'Encapsulation Protocol' option.
- Define the encryption and hash algorithms exactly as in Phase 1.
- Set the encapsulation method to 'Transport'.

5.5 Storage

5.5.1 Managing Your File Server

iPECS SBG-1000 provides a file server utility, allowing you to perform various tasks on your files, such as manage file server shares and define access control lists. When a mass storage device is connected to the gateway, all disk partitions are automatically shared by default.
Access the file server settings by clicking the ‘Storage’ menu item under the ‘Services’ tab. The ‘File Server’ screen appears.

Figure 5.135 File Server

Enabled Select or deselect this check box to enable or disable this feature.
NetBIOS Workgroup iPECS SBG-1000’s workgroup name that will be displayed in the Windows network map of LAN hosts. All computers connected to iPECS SBG-1000’s network will appear in this workgroup.
Automatically Share All Partitions A partitioned storage device connected to iPECS SBG-1000 is automatically displayed and shared by all LAN computers. This feature is enabled by default.
Allow Guest Access From the drop-down menu, select a permission level, according to which the LAN users will access the share:

Read/Write Every LAN user can read and write the shared files without authentication.
Read Only Every LAN user can only read the shared files.
Disabled LAN users must authenticate themselves, in order to access the share. They will be able to use the share according to their permissions defined in iPECS SBG-1000’s ‘User Settings’ screen.

File Server Shares Define file shares on your disk partitions, as depicted in the following sections.

5.5.1.1 Sharing Specific Partitions with Microsoft File Sharing

By default, all partitions are automatically displayed shared among all users. Figure 5.135 depicts such a scenario, where share entries appear in the ‘File Server Shares’ section as soon as a partitioned and formatted storage device is connected to the gateway. However, if you only wish to share specific partitions, you can disable automatic file sharing and manually define file shares using the ‘Microsoft File Sharing Protocol’. Note that this protocol requires associating specific users with the shares.

To share a specific partition only, perform the following sequence. First, enable Microsoft File Sharing for users you would like to have access to the share:

1. Click the ‘Users’ menu item under the ‘System’ tab. The ‘Users’ screen appears.

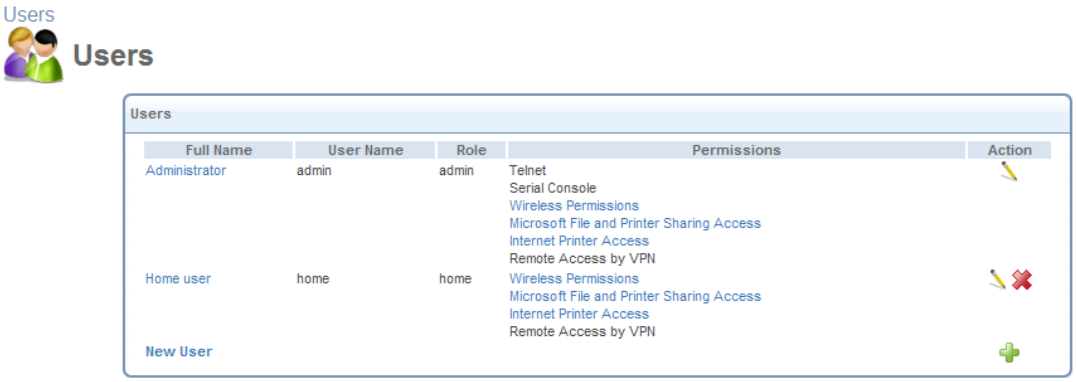


Figure 5.136 Users

2. Click the name of the user for whom you wish to enable file sharing.

3. In the ‘User Settings’ screen that appears, check the “Microsoft File and Printer Sharing Access” check box in the ‘Permissions’ section.

Figure 5.137 User Settings

4. Click ‘OK’ to save the settings.

Next, define the specific file share:

1. In the ‘File Server’ screen (see Figure 5.135), deselect the ‘Automatically Share All Partitions’ option and click ‘Apply’. The list of all automatically shared partitions disappears.

2. Click the ‘New Entry’ link. In the ‘File Server Share Settings’ that appears:
   a. Enter a name for the share in the ‘Name’ field.

Note: The default name “share” can be changed to another one. The share’s name is not case sensitive. Even if entered in upper-case letters, the name will be displayed in lower case, after saving the setting.

   b. Enter a valid partition path (e.g. A, B/my_documents) in the ‘Path’ field.

Note: If a drive’s sub directory does not exist yet, you will have to create it as soon as the share is defined and accessible.

   c. You may add a comment in the ‘Comment’ field.

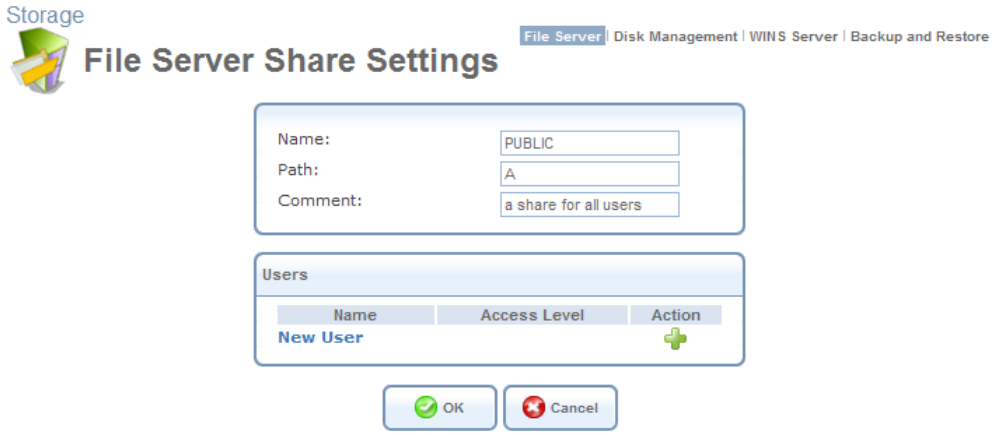


Figure 5.138 File Server Share Settings

   d. In the ‘Users’ section, click the ‘New User’ link to allow a user to use the share.

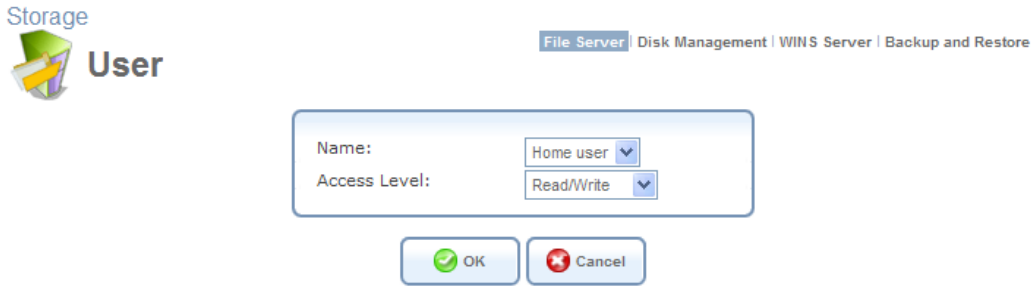


Figure 5.139 User

   e. Select the user and the allowed access level in the drop-down menus, and click ‘OK’.

3. Click ‘OK’ to save the settings. The ‘File Server’ screen reappears, displaying the share in the ‘File Server Shares’ section.

Figure 5.140 File Server Shares Section

However, note that access to a file share is different for FAT32, NTFS, and EXT2/3 formatted partitions. FAT32 has no restrictions—any user can access any share for both reading and writing.

In addition, shares defined on EXT2/3 partitions are only readable to non-administrator users (even with writing permissions), with the following exceptions:

- The user will be able to write to the share's root directory (e.g. A\ , my_share\ ).
- The user will be able to write to the directory that had been created for that user.

Moreover, to create new directories that will be writable for users, you must be logged in as a user, not an administrator. Any directories created by an administrator will only be writable to the administrator.

To access the new share, you must be logged in with a user associated with share (in this example, user 'home'). Perform the following:

1. Click the share's link under the 'Name' column in the 'File Server Shares' section (see Figure 5.140).

Note: If the share is not available, for example if the disk has been removed, the link will not be clickable and appear as plain text.

A Windows login dialog box appears.

Figure 5.141 Login Dialog

2. Enter your WBM username and password to login. The share opens in a new window.

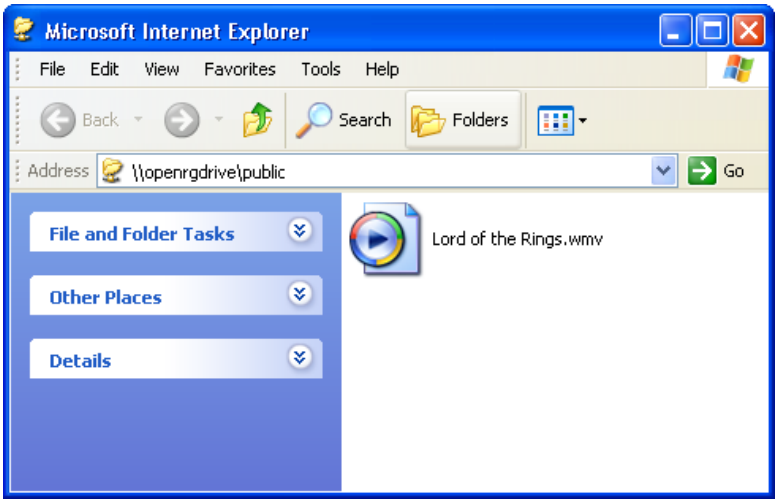


Figure 5.142 File Share

Once logged into a share, Windows remembers your username and password, and automatically re-logins with the same user. To logout and re-login with a different user (for example, to switch between an administrator and a user), logout and re-login to Windows.

Users with appropriate permissions can access file shares from any PC on the LAN using the following standard methods:

- From iPECS SBG-1000's Web-based management as described above.

- Browsing to the share itself by simply typing its path (for example, iPECS SBG-1000\ A) in a browser address line or in the command line.
- Mapping the share using Window's 'Map Network Drive' utility.

All of these methods require an initial username and password login, as described above. The share content will be displayed in a new window. If the share is the partition configured to serve as the system storage area, it will contain automatically-generated system folders. Otherwise, it will either be empty or contain pre-loaded files.

5.5.1.2 Viewing and Modifying Access Control Lists

The Windows operating system boasts an extensive file permission scheme. When you right-click a file and choose Properties, you can see under the Security tab that file permissions can be defined for any number of users and groups. Each user and group may be allowed or denied several levels of access, ranging from Full Control to Read only.

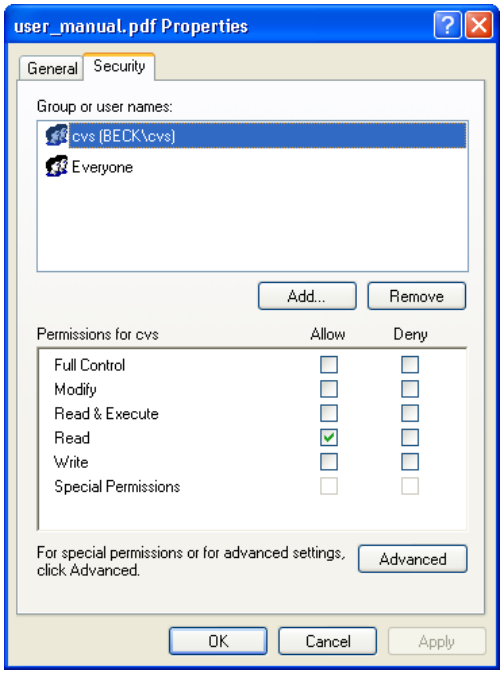


Figure 5.143 File Properties

Linux, on the other hand, has a very limited file permissions scheme, offering the basic Read (r), Write (w) and Execute (x) permissions to the file owner and his group only. Access Control Lists (ACLs) are an extension of the common Linux permission scheme. ACLs allow granting the aforementioned permissions not only to the file owner and his group, but to any number of users and groups. The need for ACLs in iPECS SBG-1000 is mainly to support permissions defined by a Windows client connected to the file server. This connection is done via the 'Microsoft File and Printer Sharing Protocol', which is supported on iPECS SBG-1000 and allows interoperability between Linux/Unix servers and Windows-based clients. The basic user and group file permissions in Windows are: Full control, Modify, Read and Execute, Read, and Write. Each permission can be allowed or denied. Linux supports Read, Write and Execute only, and does not support the Allow/Deny mechanism. When you modify a file's permissions on a Windows client, iPECS SBG-1000 uses a "best effort" algorithm to translate the ACLs to Linux r/w/x bits, making the file compatible with Linux clients.

To view a file's access control list on a Windows client connected to iPECS SBG-1000's file server, perform the following:

1. Click the file share link in the 'File Server Shares' section (see Figure 5.140) of the 'File Server' screen to open the file share (login with a valid user for the share if a login prompt appears).

2. Create a file on the share.

3. Right-click the file and choose "Properties".

4. Click the Security tab to view the file ACLs (see Figure 5.143).

Under the Security tab you can view the permissions of the file owner, the owner's group and the group "Everyone", for all other users. If you have more users (or groups) defined on iPECS SBG-1000, you can add them to the file's ACL and grant them permissions. To modify a file's access control list, perform the following:

1. Click the 'Add' button in the Security tab window to view the users and groups list.

2. In the 'Select Users or Groups' window that appears (see Figure 5.144), press the 'Advanced' button.

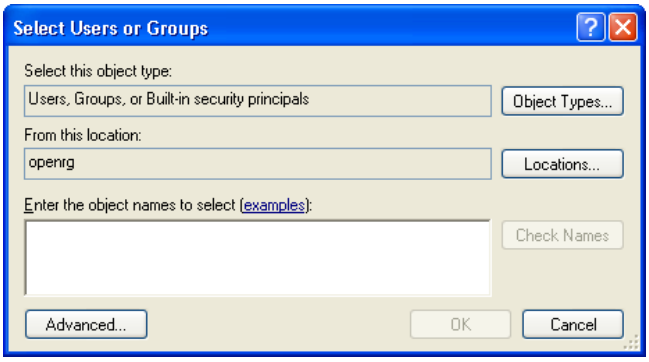


Figure 5.144 Select Users or Groups

3. In the advanced window (see Figure 5.145) press the 'Find Now' button.

4. A login prompt will appear. Log in with the same share user. A list of both iPECS SBG-1000 users and system default users will be displayed.

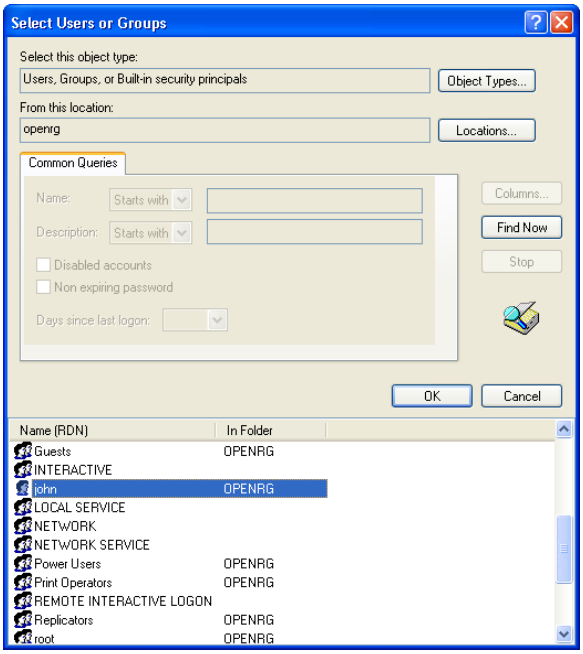


Figure 5.145 Users or Groups List

5. Select an iPECS SBG-1000 user from the list and click 'OK'. Click 'OK' again in the initial 'Select Users or Groups' window to save the settings. The selected user will be added to

the groups and users list on the Security tab, with the default ACLs.

6. Check or uncheck the different permissions to allow or deny the user of the permissions.

7. Click ‘OK’ to save the settings.

In the same manner, you can remove a user or a group using the ‘Remove’ button in the Security window.

5.5.1.3 Using the File Server with Mac

In order to connect to iPECS SBG-1000’s file server with a Mac computer, perform the following:

1. On your Mac computer connected to iPECS SBG-1000, click “Connect to Server” from the “Go” menu. The ‘Connect to Server’ screen appears.

Figure 5.146 Connect to Server

2. In the server address field, enter smb://192.168.1.1 , and click the ‘Connect’ button. A new window appears, displaying the available file shares.

Figure 5.147 Connect to Server

3. Select the share to which you would like to connect. If prompted, enter a valid username and password, and click ‘OK’. When a connection is established, the share content appears.

Figure 5.148 Connect to Server

5.5.2 WINS Server

iPECS SBG-1000 can operate as a Windows Internet Naming Service (WINS) server, handling name registration requests from WINS clients and registering their names and IP addresses. WINS is a name resolution software from Microsoft that converts NetBIOS names to IP addresses. Windows machines that are named as PCs in a workgroup rather than in a domain use NetBIOS names, which must be converted to IP addresses if the underlying transport protocol is TCP/IP. Windows machines identify themselves to the WINS server, so that other Windows machines can query the server to find the IP address. Since the WINS server itself is contacted by IP address, which can be routed across subnets, WINS allows Windows machines on one LAN segment to locate Windows machines on other LAN segments by name. When a host connects to the LAN, it is assigned an IP address by iPECS SBG-1000's DHCP (refer to Section 5.7). The WINS database is automatically updated with its NetBIOS name and the assigned IP address. iPECS SBG-1000's WINS server also responds to name queries from WINS clients by returning the IP address of the name being queried (assuming the name is registered with the WINS server). The "Internet" in the WINS name refers to the enterprise Internet (LAN), not the public Internet. To configure iPECS SBG-1000's WINS server settings, perform the following:

1. Access the WINS Server settings either from its link in the 'Storage' tab under the 'Services' screen, or by clicking the 'WINS Server' icon in the 'Shortcut' screen. The 'WINS Server' screen will appear (see Figure 5.149). By default, iPECS SBG-1000's WINS server is disabled.

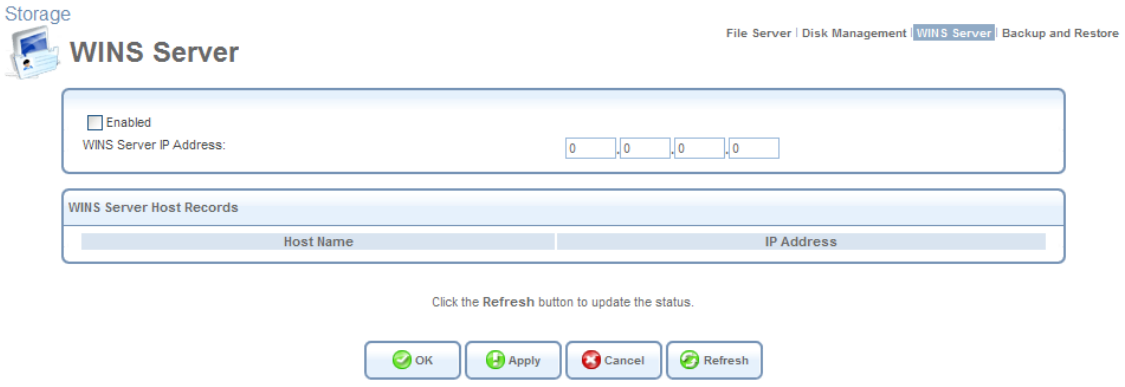


Figure 5.149 WINS Server

2. If you would like to use an external WINS server, enter its IP address and click 'OK'.

3. If you would like to use iPECS SBG-1000's WINS server, select the 'Enabled' check-box. The screen will refresh, omitting the IP address field (see Figure 5.150).

Figure 5.150 WINS Server

4. Select the 'Domain Master Browser' check box if you would like iPECS SBG-1000 to act as a domain master in the Windows NetBIOS protocol.

5. Click 'OK' to save the settings.

Hosts connected to the LAN will register their names and IP addresses with either the specified remote WINS server or with iPECS SBG-1000's WINS server, depending on the configuration above. In both cases, the registered hosts will be added to the 'WINS Server Host Records' table in this screen.

5.5.3 Backup and Restore

iPECS SBG-1000's backup facility allows backing up data, stored in the system storage area, to external USB disks. You may specify backups to run automatically at scheduled times. Two preliminary conditions must be met before enabling the backup mechanism:

- The file server feature must be activated and configured (refer to Section 5.5.1).
- The file server must be consisted of at least two disks.

Please note that the backup is done at the directory level, meaning that it is not possible to backup a single stand-alone file.

5.5.3.1 Backing Up Your Data

To backup your data:

1. Access the Backup settings either from its link in the 'Storage' tab under the 'Services' screen, or by clicking the 'Backup and Restore' icon in the 'Shortcut' screen. The 'Backup and Restore' screen appears:

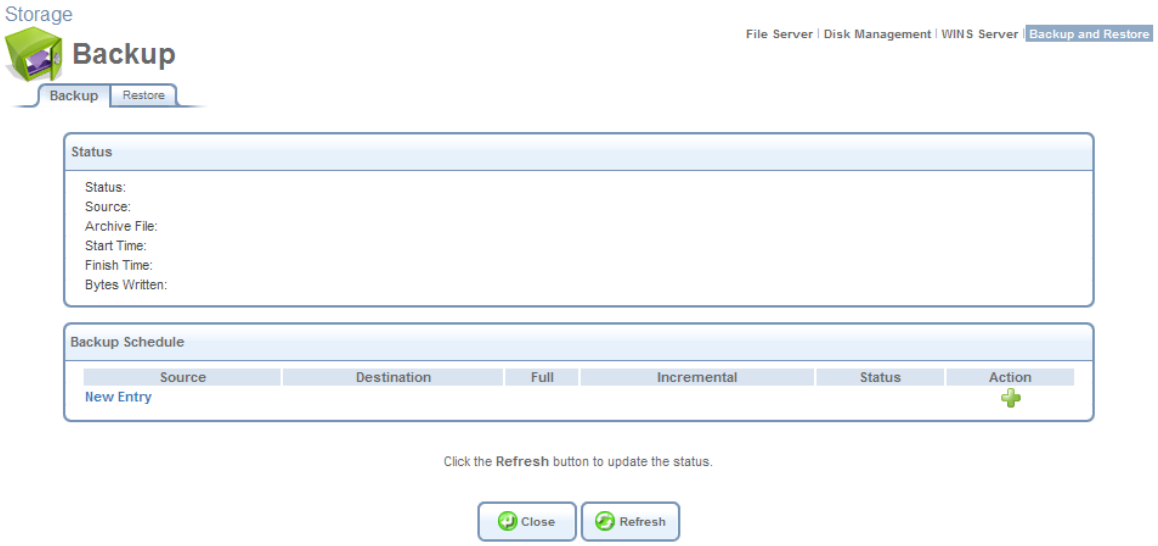


Figure 5.151 Backup and Restore

2. Click the ‘New Entry’ link in the ‘Backup Schedule’ section.
3. In the ‘Edit Backup’ screen that appears (see Figure 5.152), configure the following parameters:
   a. Type the source to backup. For example, { A/homes }.
   b. Type the destination of the backup files. For example, { B/backups }. It is recommended that the destination be an external storage device.
   c. Choose between full backup, incremental backup, or both, by scheduling a time for the backup operation. You can choose between daily, weekly or monthly backups in the ‘Schedule’ combo boxes.
4. Press ‘OK’ to save the schedule settings.
5. Press ‘Backup Now’ to run the backup operation immediately. When backing up, the screen will display the status and progress of the operation.

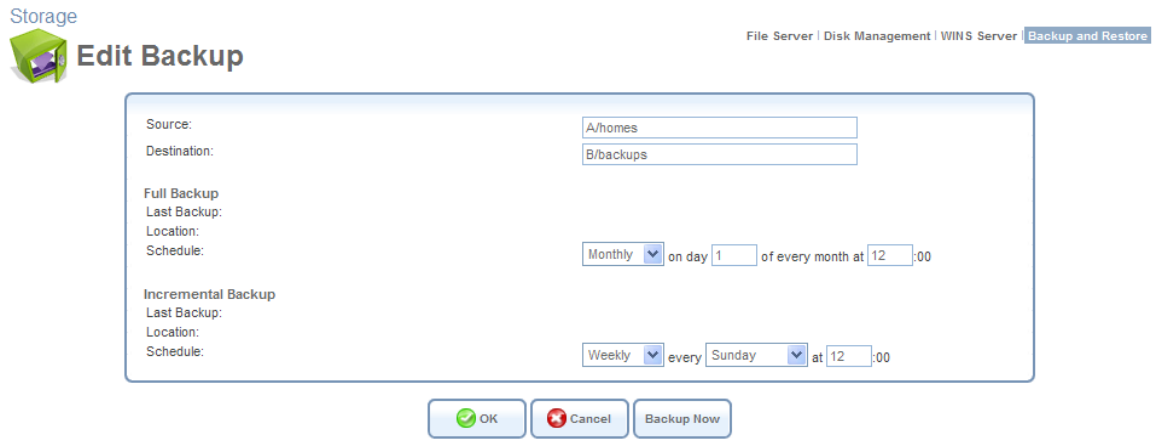


Figure 5.152 Edit Backup

Note: Do not schedule a monthly backup on the 31st, as backups will not run on months with 30 days.

5.5.3.2 Restoring Your Data

To restore your data:

1. Press the ‘Backup and Restore’ icon in the ‘Shortcut’ screen of the WBM. The ‘Backup and Restore’ screen appears (see Figure 5.151).

2. Press the ‘Restore’ tab.

3. In the ‘Restore’ screen that appears (see Figure 5.153), configure the following parameters:
   a. Type the source to restore in the ‘Source Archive’ field. For example, { B/backups/2011_Apr_16_15_34_11.full.tar} .

   b. Choose whether to restore the entire archive or only a sub directory, in the ‘Restore Option’ combo box. If you choose sub directory, a second field appears in which you must enter the name of the sub directory, relative to the source archive. For example, to restore { A/homes/john}, type { john} as the sub directory.

   c. Choose a destination for which to restore the archive. You can choose between the original location or any other directory. If you choose another directory, a second field appears in which you must enter the name of the directory. Note that the path of the restored directory will be created under the path of the destination directory. For example, if you specify the directory { A/restore_dir} , the result will be { A/restore_dir/A/homes/john} .

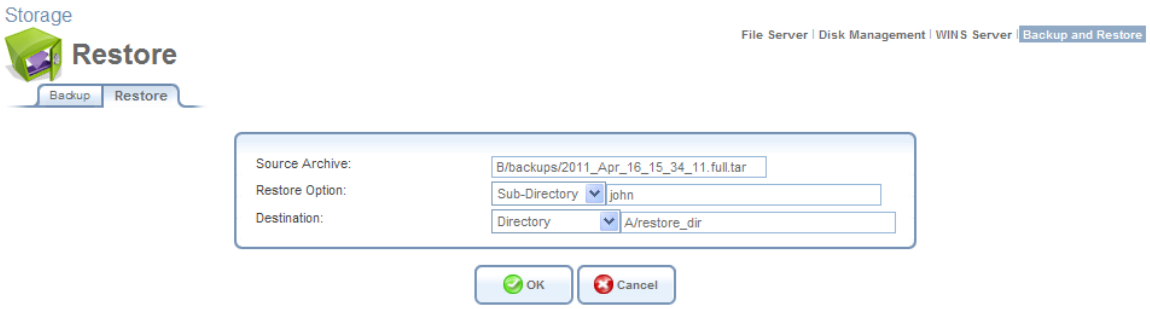


Figure 5.153 Edit Restore

5.5.4 Managing Your Disks

The ‘Storage’ menu item provides access to the ‘Disk Management’ screen, which enables you to view and manage your storage devices.

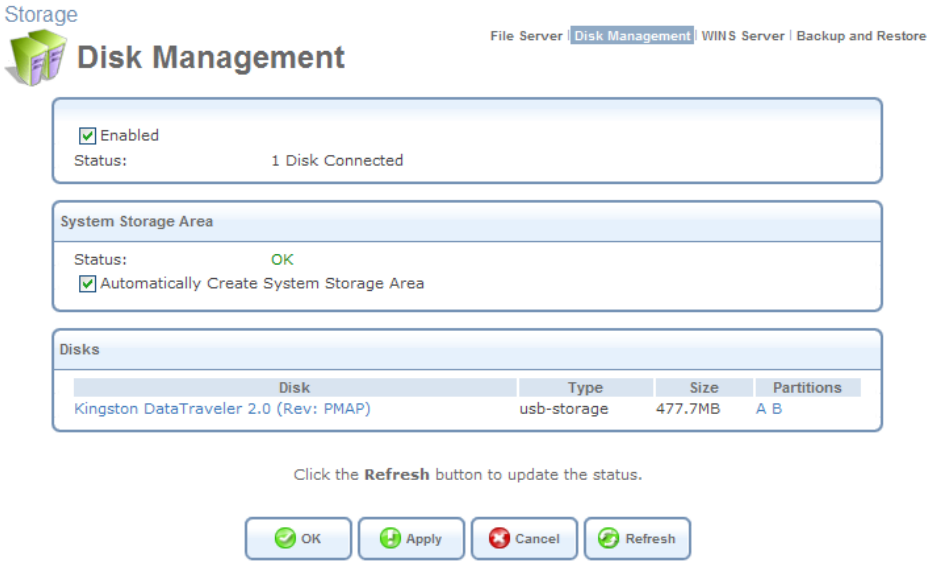


Figure 5.154 Disk Management

Enabled Select or deselect this check box to enable or disable this feature.

System Storage Area iPECS SBG-1000 automatically defines a specific location on the storage device for storing data used by its various services. This setting is valid until the storage device is disconnected. When reconnected, iPECS SBG-1000 may select another partition for this purpose.

Disks This section provides details about the attached storage device. Click the name of the disk. The 'Disk Information' screen appears, providing all available information regarding the disk and its partitions.

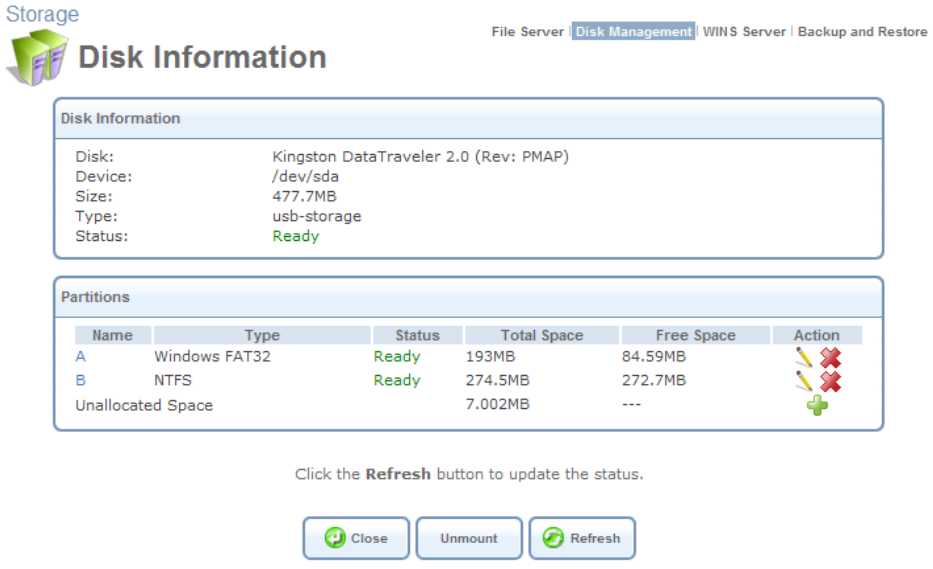


Figure 5.155 Disk Information

5.5.4.1 Managing Disk Partitions

A disk partition can be formatted, checked, or deleted. The following sections describe each of these operations.

Warning: When applying administrative changes to storage devices, services using these devices are stopped (for more information about such services, refer to Section 5.5).

5.5.4.1.1 Adding and Formatting a Partition

In order to be used, a mass storage device must first be partitioned and formatted. However, partitioning can only be performed on unallocated disk space. If your device is already partitioned, you may not be able to add a partition, unless unallocated space is available.

To add a Windows formatted partition, perform the following:

1. Click the ‘Storage’ menu item under the ‘Services’ tab. The ‘Disk Management’ screen appears.

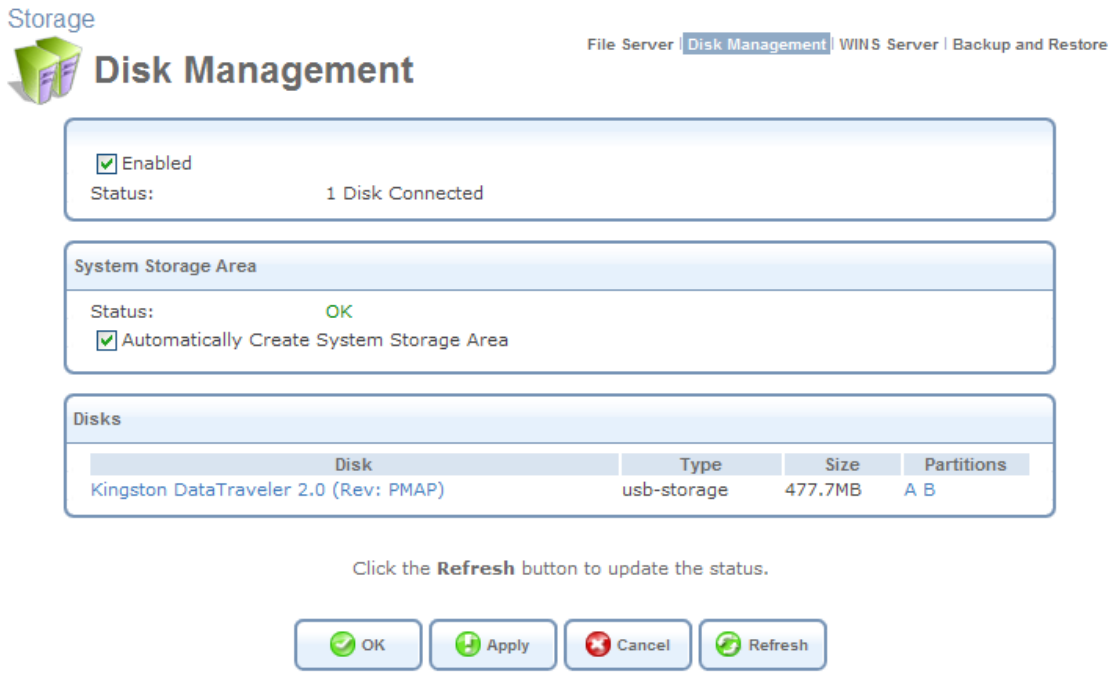


Figure 5.156 Disk Management

2. In the ‘Disks’ section, displaying your connected storage devices, click the disk’s link. The ‘Disk Information’ screen appears.

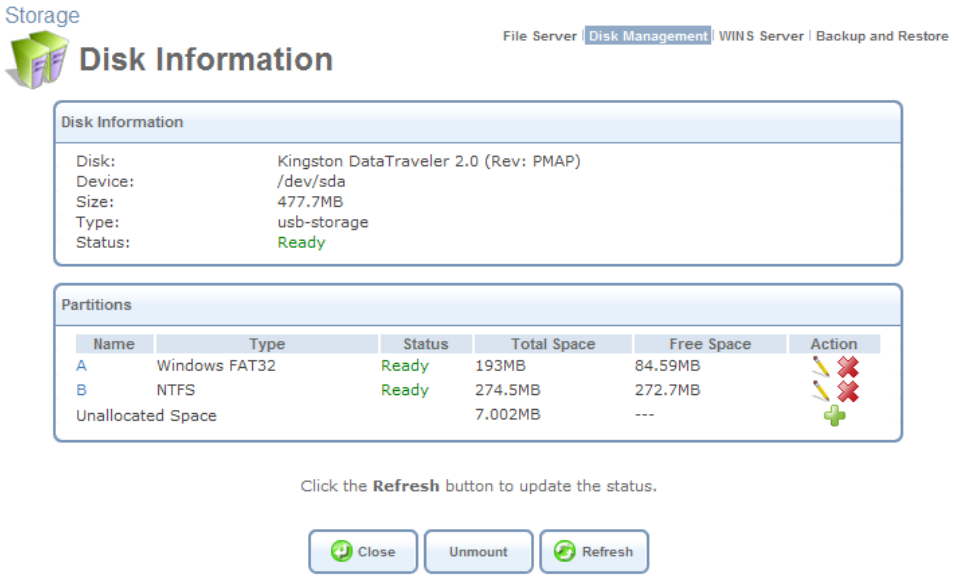


Figure 5.157 Disk Information

3. In the 'Partitions' section, click the action icon. The 'Partition Type' screen appears.

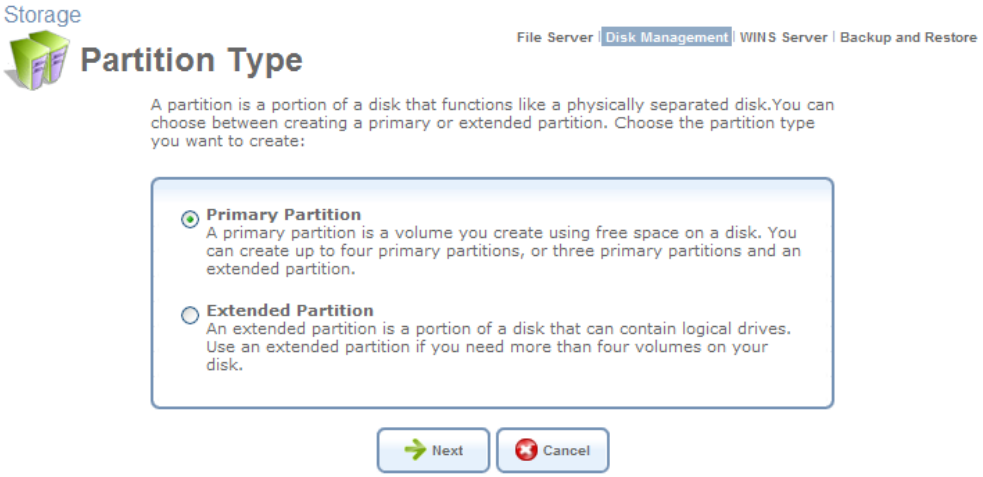


Figure 5.158 Partition Type

4. Select 'Primary Partition', and click 'Next'. The 'Partition Size' screen appears.

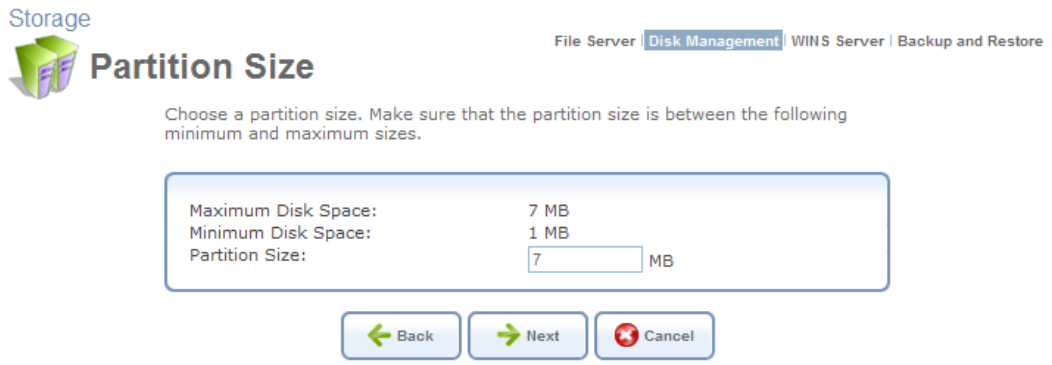


Figure 5.159 Partition Size

5. Enter a volume for the new partition (in mega bytes) and click ‘Next’. The ‘Partition Format’ screen appears.

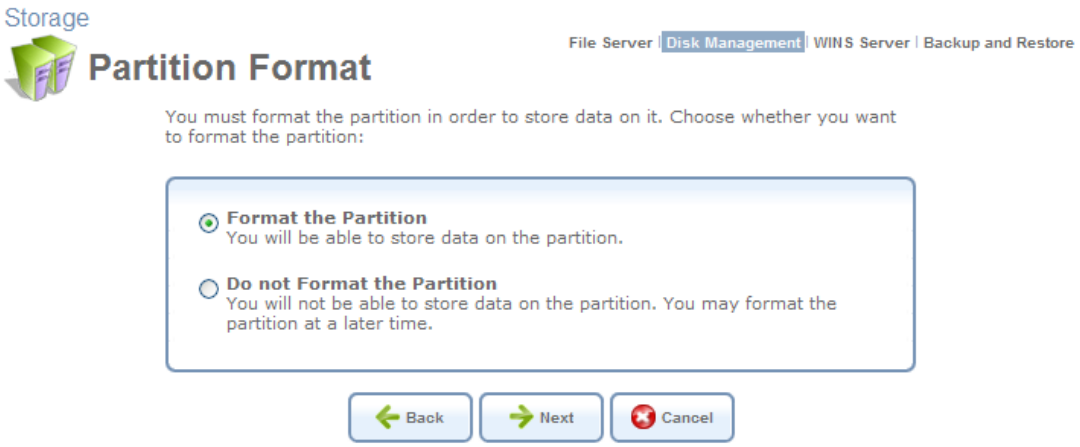


Figure 5.160 Partition Format

6. Select ‘Format the Partition’, and click ‘Next’. The ‘Partition File System’ screen appears.

Figure 5.161 Partition File System

7. Select ‘Windows (FAT32) (LBA)’ as the file system for the partition and click ‘Next’. The ‘Partition Summary’ screen appears.

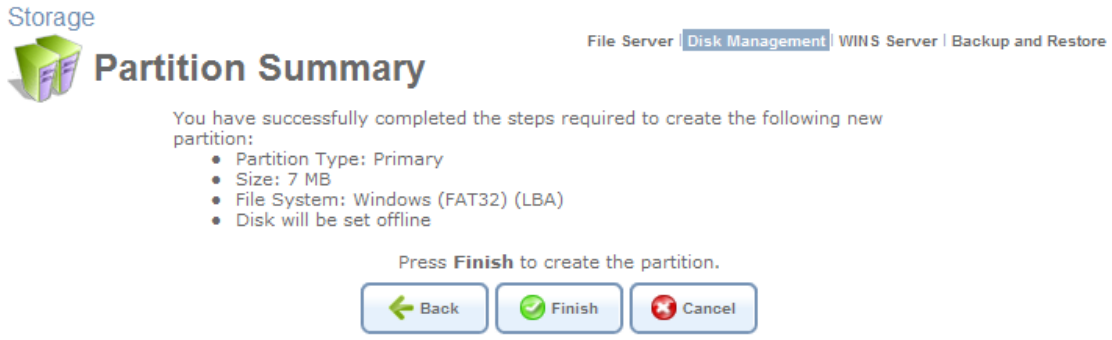


Figure 5.162 Partition Summary

8. Click ‘Finish’ to create the new partition. The ‘Disk Information’ screen reappears, refreshing as the partition formatting progresses, until the status changes to ‘Ready’.

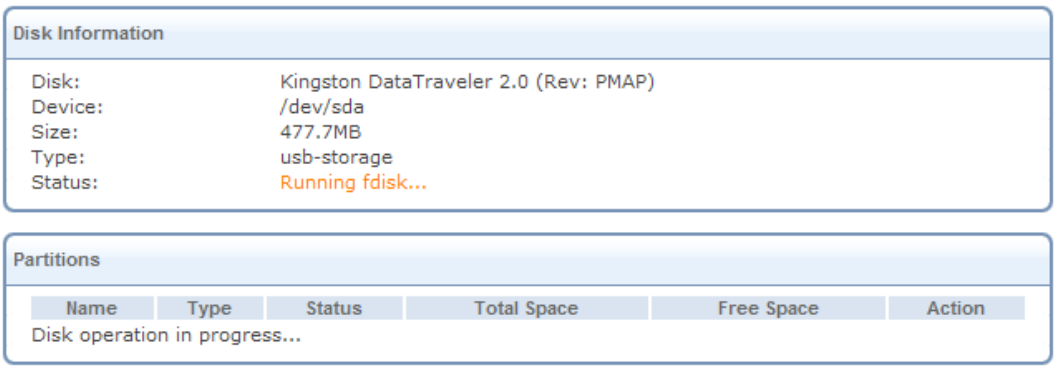


Figure 5.163 Partition Formatting in Progress

The new partition path names are designated as “A”, “B”, etc.

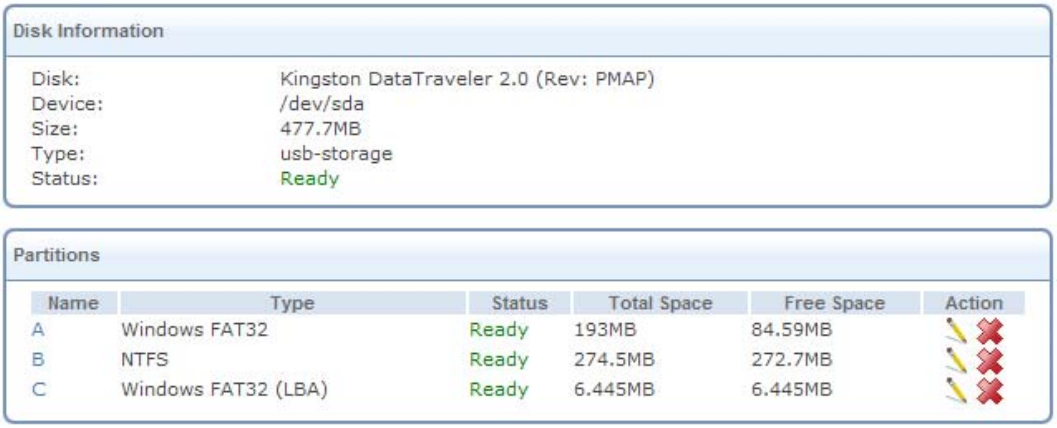


Figure 5.164 Formatting Complete – Partition Ready

To learn about additional operations you can perform on your storage device, refer to the ‘Shared Storage’ section of the iPECS SBG-1000 Manual.

5.5.4.1.2 Checking a Partition

Periodically, you should check the disk’s partitions for the presence of bad sectors, to maintain the disk’s health and prevent data loss.

To check a partition:

1. In the ‘Disks’ section of the ‘Disk Management’ screen, click the disk’s link. The ‘Disk Information’ screen appears.

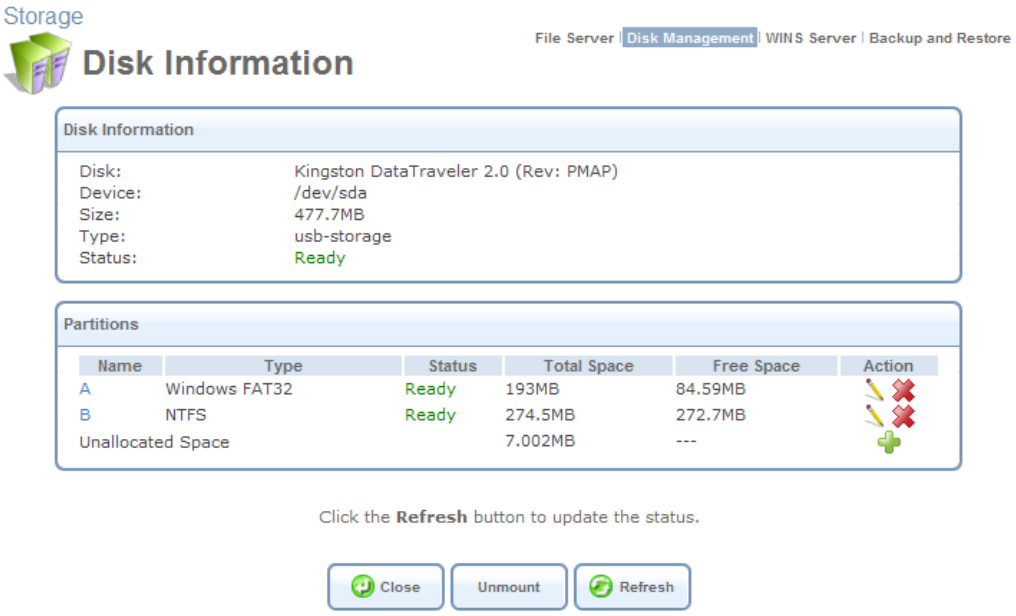


Figure 5.165 Disk Information

2. In the ‘Partitions’ section, click the action icon of the partition you would like to check. The ‘Partition Properties’ screen appears.

Figure 5.166 Partition Properties

3. Click the ‘Check Partition’ button. The ‘Partition Check’ screen appears.

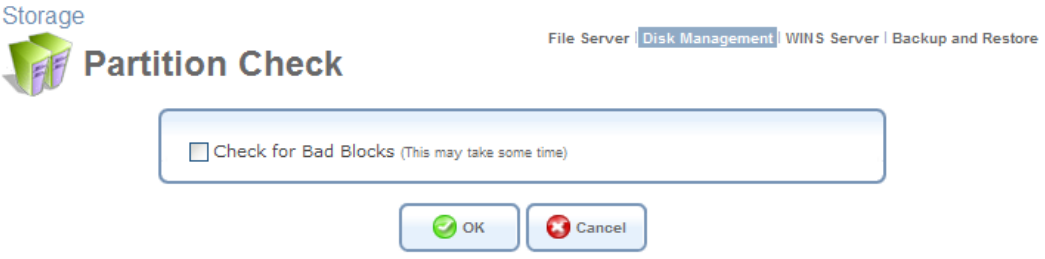


Figure 5.167 Partition Check

This screen enables you to check a partition for presence of bad blocks prior to the regular file system checkup. To do so, select the ‘Check for Bad Blocks’ check box.

4. Click ‘OK’. A warning screen appears, alerting you that the partition will be set to offline.

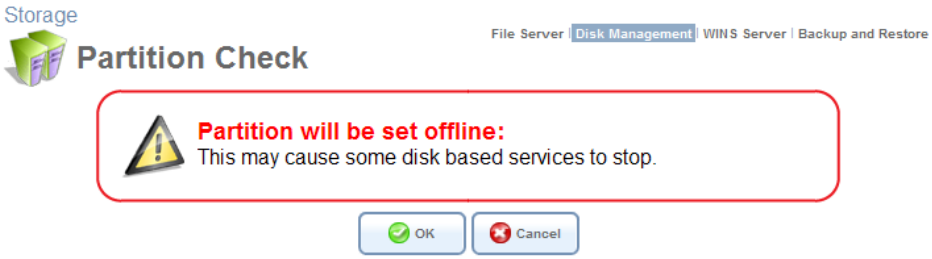


Figure 5.168 Offline Partition Warning

5. Click ‘OK’ to check the partition. The screen refreshes as the partition checking progresses.

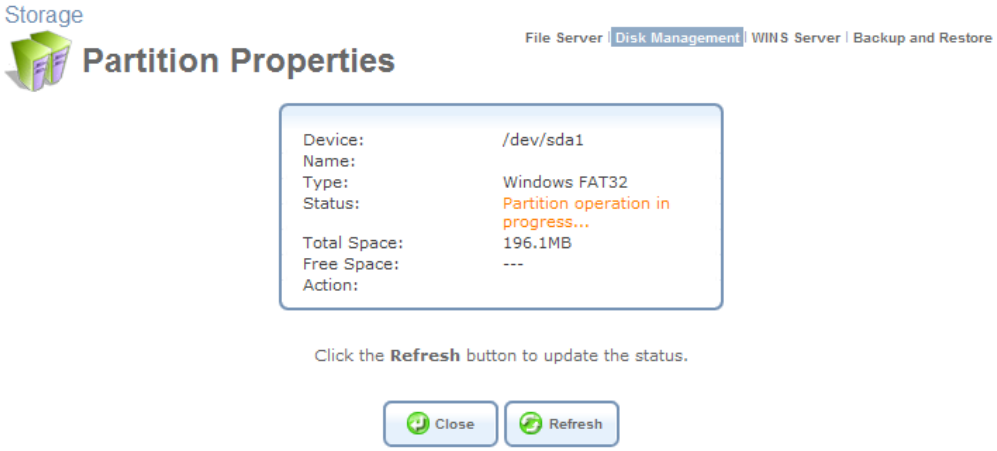


Figure 5.169 Partition Checking in Progress

When the check is complete, the status changes to ‘Ready’.

Figure 5.170 Checking Complete – Partition Ready

5.5.4.1.3 Reformatting a Partition

In addition to formatting a newly created partition, you can reformat an existing partition with either EXT2, EXT3, FAT32, or NTFS file systems, allowing both *Read* and *Write* access.

Note: For security reasons, it is recommended to format disk partitions with the EXT2 or EXT3 file system.

To reformat a partition:

1. In the 'Disks' section of the 'Disk Management' screen, click the disk's link. The 'Disk Information' screen appears.

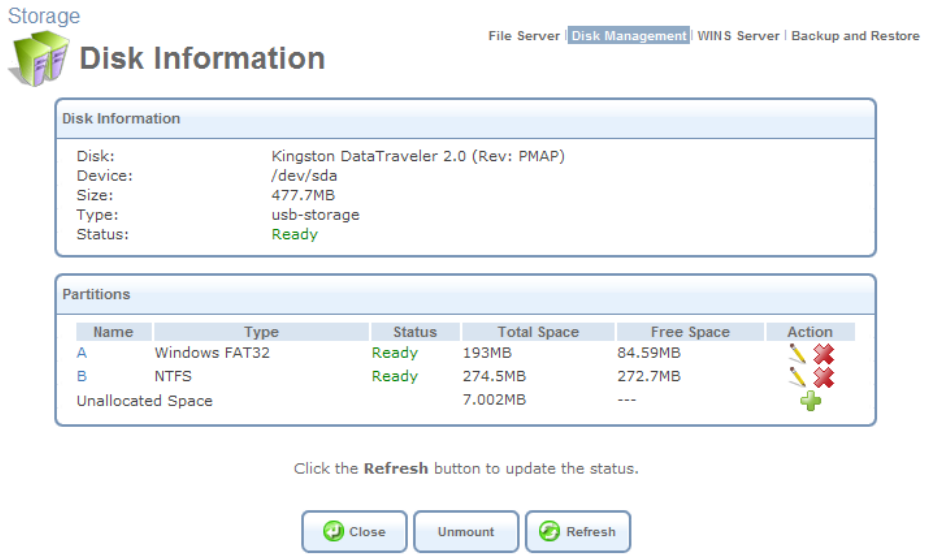


Figure 5.171 Disk Information

2. In the 'Partitions' section, click the action icon of the partition you would like to edit. The 'Partition Properties' screen appears.

Figure 5.172 Partition Properties

3. Click the 'Format Partition' button. The 'Partition Format' screen appears.

Figure 5.173 Partition Format

Note: You can also instruct iPECS SBG-1000 to check the disk for bad blocks prior to formatting it, by selecting the corresponding check box. Only the disk space consisting of healthy blocks will be formatted. Bad blocks will be ignored.

4. Select a file system for the partition and click ‘OK’. A warning screen appears, alerting you that all the data on the partition will be lost.

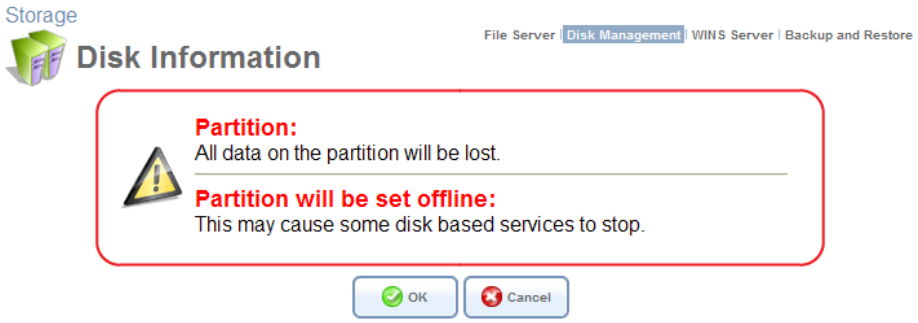


Figure 5.174 Lost Data Warning

5. Click ‘OK’ to format the partition. The screen refreshes as the partition formatting progresses.

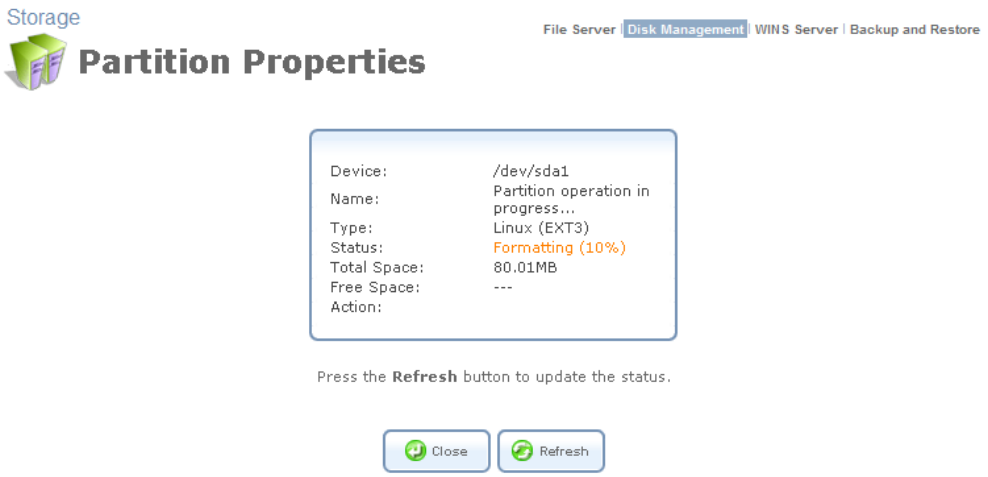


Figure 5.175 Partition Formatting in Progress

When the format is complete, the status changes to ‘Ready’.

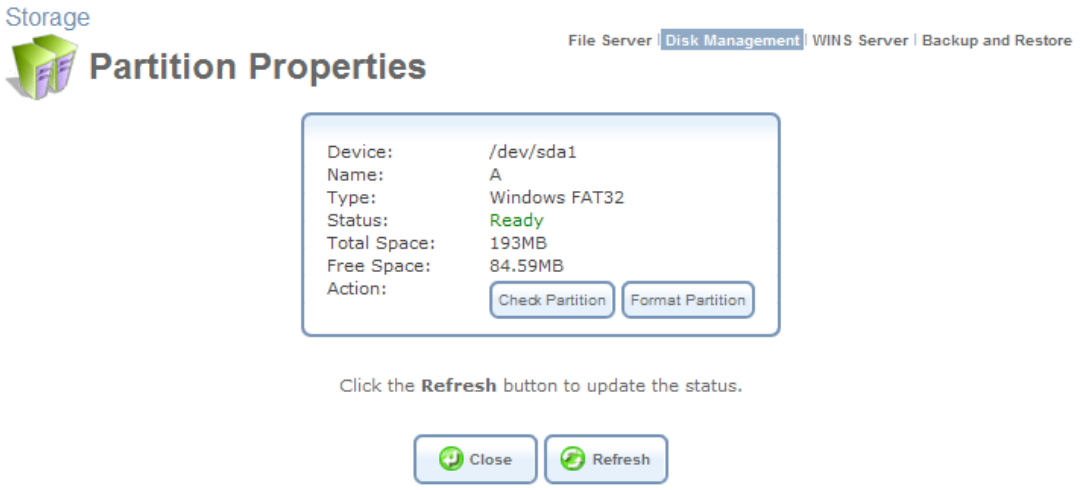


Figure 5.176 Formatting Complete – Partition Ready

5.5.4.1.4 Deleting a Partition

If you would like to delete a partition on your storage device, perform the following:

1. In the 'Disks' section of the 'Disk Management' screen, click the disk's link. The 'Disk Information' screen appears.

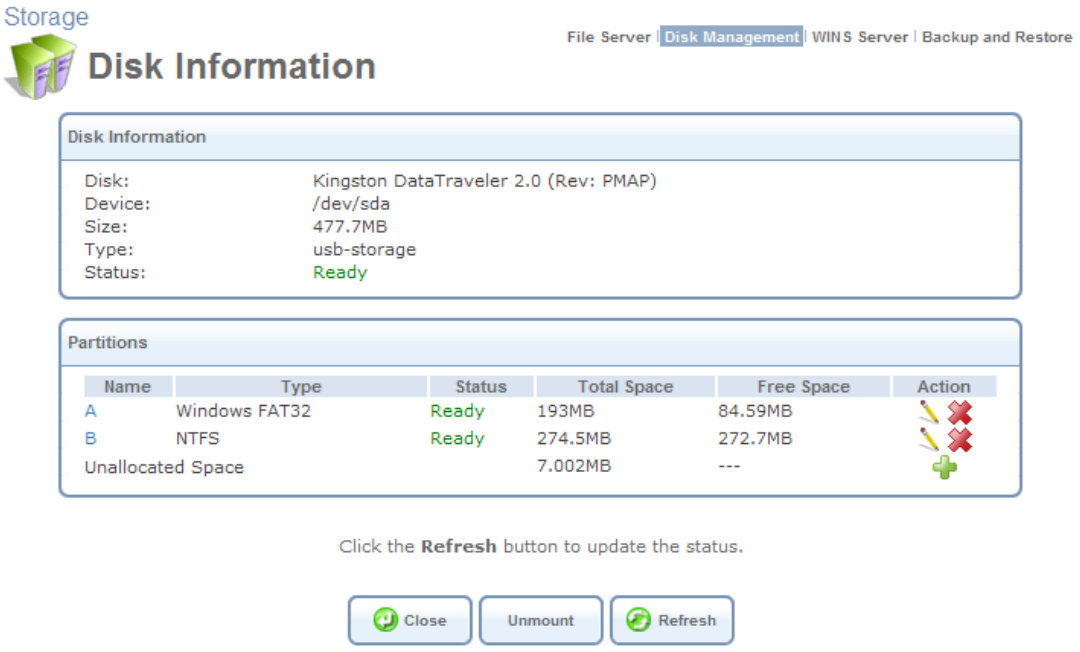


Figure 5.177 Disk Information

2. In the 'Partitions' section, click the action icon of the partition you would like to delete. A warning screen appears, alerting you that all the data on the partition will be lost.

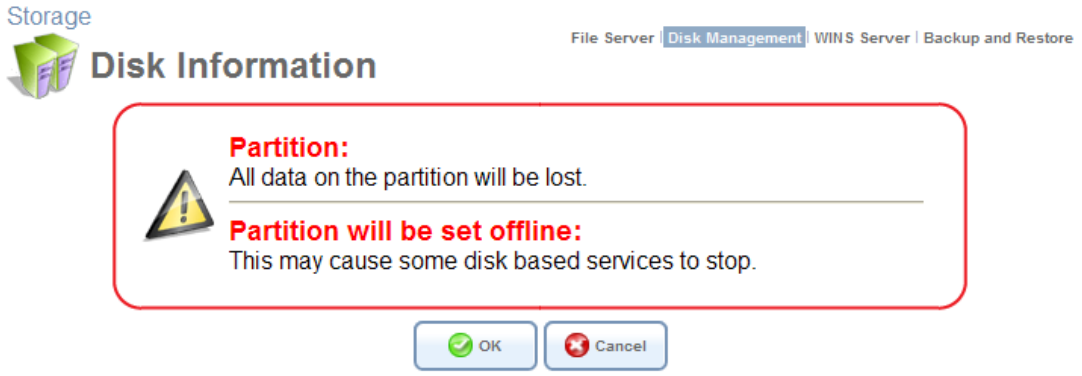


Figure 5.178 Lost Data Warning

3. Click ‘OK’ to delete the partition.

5.5.4.2 Changing the System Storage Area Location

iPECS SBG-1000 uses a specific location on a storage device for storing data used by its various services. The following services use the system storage area:

- Printer spool and drivers
- Users’ directories

If you would like to set a specific partition as the location for the system storage area, perform the following:

1. Deselect the ‘Automatically Create System Storage Area’ check box. The screen refreshes displaying the ‘System Storage Area’ field (containig the auto-selected partition).

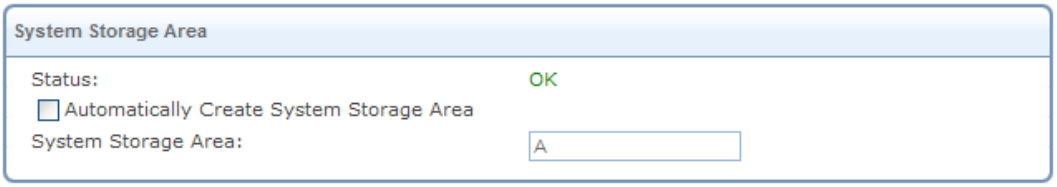


Figure 5.179 Manually Defined System Storage Area

2. Enter the letter of the partition to which you would like to set the system storage area.

3. Click ‘OK’ to save the settings.

If you wish to view the system directories, verify that the system storage area is shared (refer to Section 5.5.1.1). Then, browse to \ \ sbg-1000drive\ <PARTITION LETTER> (use Windows Explorer if you are using a browser other than Internet Explorer).

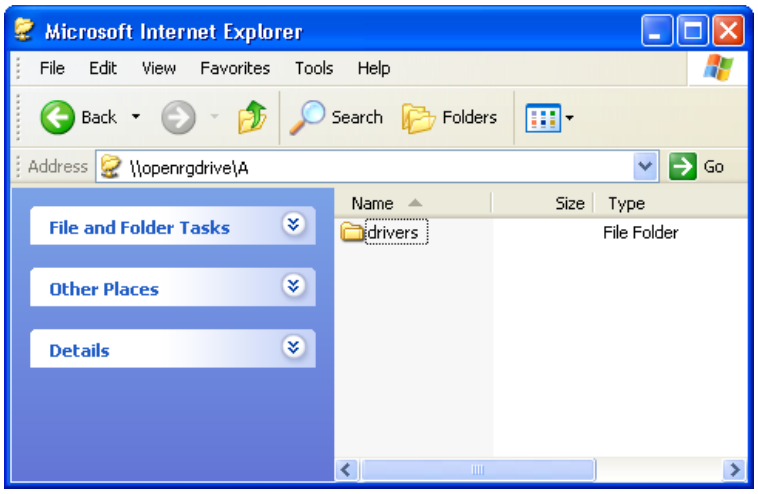


Figure 5.180 System Storage Area Directories

5.6 Accessing Your Network Using a Domain Name

iPECS SBG-1000's Dynamic DNS (DDNS) service enables you to define a unique domain name for your gateway's Internet connection, thereby allowing you to access the gateway or your home network's services just by pointing the browser to this name. When using this feature, you will not need to check and remember your gateway's Internet IP address, which may change in case of a disconnection from the ISP's network.

5.6.1 Opening a Dynamic DNS Account

In order to use the DDNS feature, you must first obtain a DDNS account. iPECS SBG-1000 provides a list of DDNS servers on which you may create such an account. To view this list, perform the following:

1. Access this feature either from the 'DDNS' menu item under the 'Services' tab, or by clicking the 'Personal Domain Name (Dynamic DNS)' icon in the 'Shortcut' screen. The 'Personal Domain Name (Dynamic DNS)' screen appears.

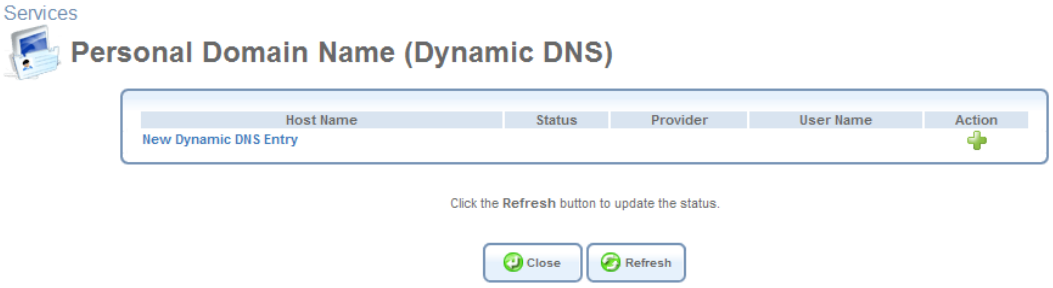


Figure 5.181 Personal Domain Name (Dynamic DNS)

2. Click the 'New Dynamic DNS Entry' link to add a new DDNS entry. The following screen appears.

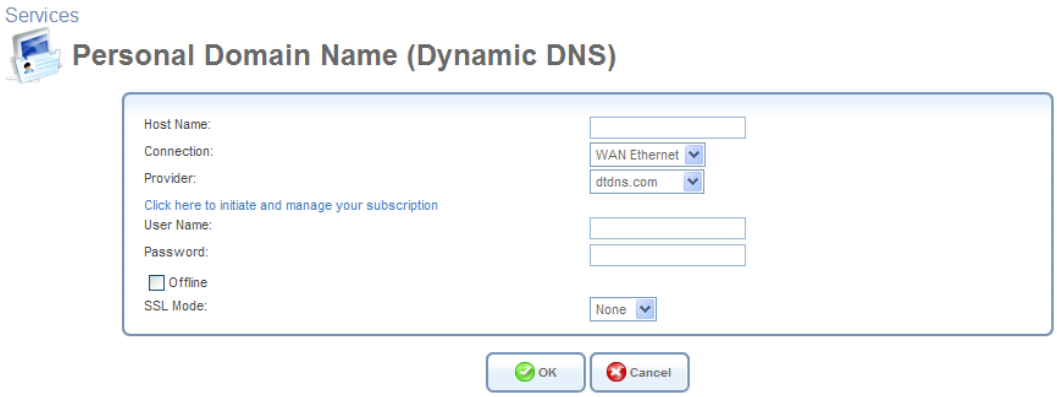


Figure 5.182 Dynamic DNS Entry

3. Specify the DDNS parameters:

Host Name Enter your full DDNS domain name.

Connection You can couple the DDNS service with your WAN Ethernet connection, and the DDNS service will only use the chosen device.

Provider Select your DDNS service provider. The screen will refresh, displaying the parameters required by each provider. The provider depicted herein is dyndns.org, which includes all available parameters.

Click Here to Initiate and Manage your Subscription Clicking this link will open the selected provider's account creation Web page. For example, when dyndns.org is selected, the following page will open: http://www.dyndns.com/account/.

User Name Enter your DDNS user name.
Password Enter your DDNS password.

Wildcard Select this check-box to enable use of special links such as http://www.<your host>.dyndns.com.

Mail Exchanger Enter your mail exchange server address, to redirect all e-mails arriving at your DDNS address to your mail server.

Backup MX Select this check box to designate the mail exchange server to be a backup server.

Offline If you wish to temporarily take your site offline (prevent traffic from reaching your DDNS domain name), select this check box to enable redirection of DNS requests to an alternative URL, predefined in your DDNS account. The availability of this feature depends on your account's level and type of service.

SSL Mode With iPECS SBG-1000 versions that support Secure Socket Layer (SSL),

secured DDNS services are accessed using HTTPS. Upon connection, iPECS SBG-1000 validates the DDNS server's certificate. Use this entry to choose the certificate's validation method.

None Do not validate the server's certificate.

Chain Validate the entire certificate chain. When selecting this option, the screen will refresh (see Figure 5.183), displaying an additional drop-down menu for selecting whether to validate the certificate's expiration time. Choose 'Ignore' or 'Check' respectively. If the certificate has expired, the connection will terminate immediately.

Figure 5.183 SSL Mode

Direct Ensure that the server's certificate is directly signed by the root certificate. This option also provides the 'Validate Time' drop-down menu for validation of the certificate's expiration time, as described above.

5.7 Configuring Your Gateway's IP Address Distribution

iPECS SBG-1000's Dynamic Host Configuration Protocol (DHCP) server enables you to easily add computers that are configured as DHCP clients to the home network. It provides a mechanism for allocating IP addresses and delivering network configuration parameters to such computers. iPECS SBG-1000's DHCP server for wired and wireless connections is the LAN bridge.
The host can choose to renew an expiring lease or let it expire. If it chooses to renew a lease then it will also receive current information about network services, as it did with the original lease, allowing it to update its network configurations to reflect any changes that may have occurred since it first connected to the network. If the host wishes to terminate a lease before its expiration it can send a release message to the DHCP server, which will then make the IP address available for use by others.

Your gateway's DHCP server:

- Displays a list of all DHCP host devices connected to iPECS SBG-1000
- Defines the range of IP addresses that can be allocated in the LAN
- Defines the length of time for which dynamic IP addresses are allocated
- Provides the above configurations for each LAN device and can be configured and enabled/disabled separately for each LAN device
- Enables you to assign a static IP lease to a LAN computer, so that the computer will receive

the same IP address each time it connects to the network, even if this IP address is within the range of addresses that the DHCP server may assign to other computers

- Provides the DNS server with the host name and IP address of each computer that is connected to the LAN

5.7.1 Viewing and Configuring the DHCP Settings

Access this feature either from the 'IP Address Distribution' menu item under the 'Services' tab, or by clicking the 'IP Address Distribution' icon in the 'Shortcut' screen. The 'IP Address Distribution' screen appears, displaying the available network interfaces and their DHCP settings.

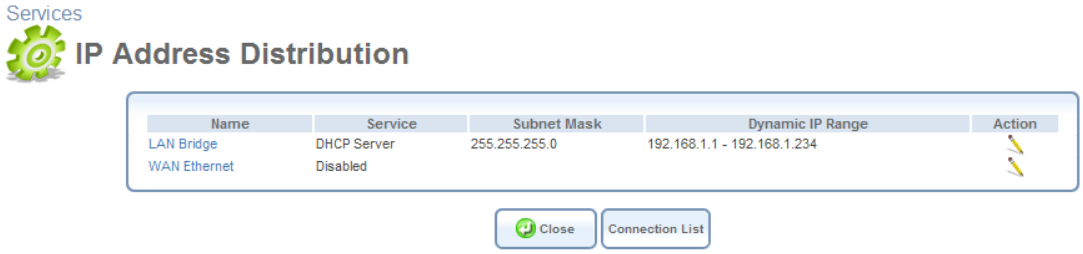


Figure 5.184 IP Address Distribution

To edit the DHCP server settings for a device:

1. Click the device's action icon. The DHCP settings screen for this device appears.

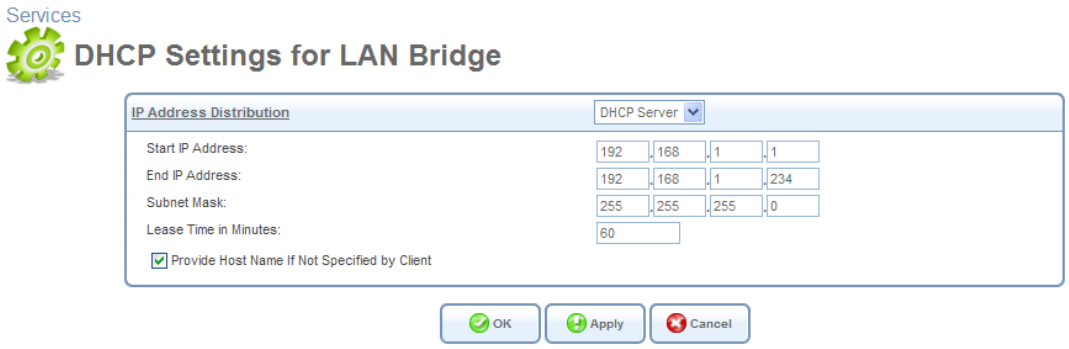


Figure 5.185 DHCP Settings for LAN Bridge

2. Select the DHCP service:
   Disabled Disable the DHCP server for this device.
   DHCP Server Enable the DHCP server for this device.

3. In case you have chosen DHCP Server, complete the following fields:
   Start IP Address The first IP address that may be assigned to a LAN host. Since the LAN interface's default IP address is 192.168.1.1, it is recommended that the first address assigned to a LAN host will be 192.168.1.2 or greater.
   End IP Address The last IP address in the range that can be used to automatically assign IP addresses to LAN hosts.

Subnet Mask A mask used to determine to what subnet an IP address belongs. An example of a subnet mask value is 255.255.255.0.
Lease Time In Minutes Each device will be assigned an IP address by the DHCP server for this amount of time, when it connects to the network. When the lease expires the server will determine if the computer has disconnected from the network. If it has, the server may reassign this IP address to a newly-connected computer. This feature ensures that IP addresses that are not in use will become available for other computers on the network.
Provide Host Name If Not Specified by Client If the DHCP client does not have a host name, the gateway will automatically assign one for it.

4. Click 'OK' to save the settings.

5.7.2 DHCP Connections

To view a list of computers currently recognized by the DHCP server, click the 'Connection List' button that appears at the bottom of the 'IP Address Distribution' screen (see Figure 5.184). The 'DHCP Connections' screen appears.

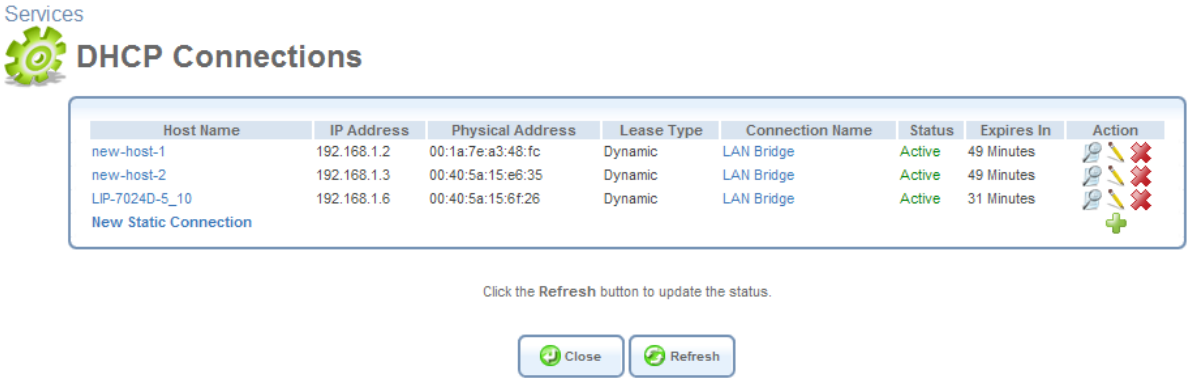


Figure 5.186 DHCP Connections

To define a new connection with a fixed IP address:

1. Click the 'New Static Connection' link. The 'DHCP Connection Settings' screen appears:

Figure 5.187 DHCP Connection Settings

2. Enter a host name for this connection.

3. Enter the fixed IP address that you would like to have assigned to the computer.

4. Enter the MAC address of the computer's network card.

Note: A device's fixed IP address is actually assigned to the specific network card's (NIC) MAC address installed on the LAN computer. If you replace this network card then you must update the device's entry in the DHCP Connections list with the new network card's MAC address.

5. Click 'OK' to save the settings.

The 'DHCP Connections' screen will reappear (see Figure 5.188), displaying the defined static connection. This connection can be edited or deleted using the standard action icons.

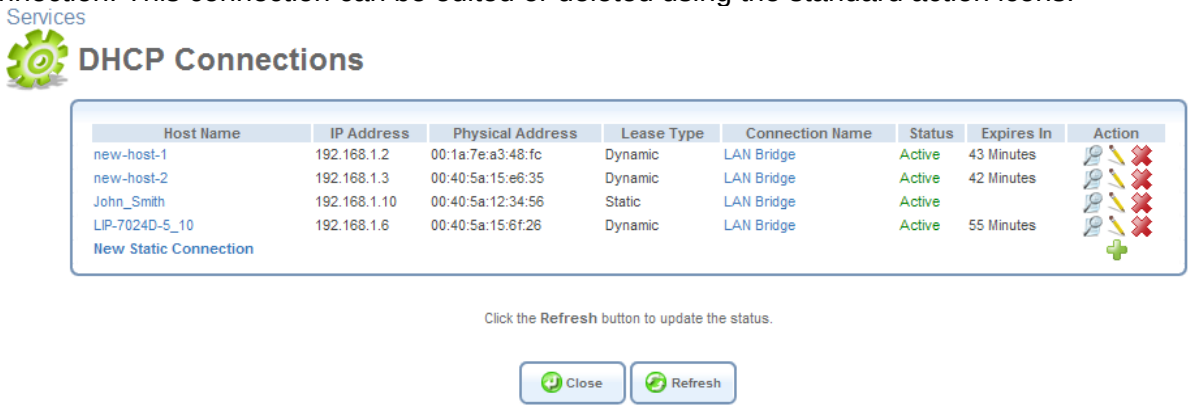


Figure 5.188 DHCP Connections

5.8 Advanced

5.8.1 DNS Server

Domain Name System (DNS) provides a service that translates domain names into IP addresses and vice versa. The gateway's DNS server is an auto-learning DNS, which means that when a new computer is connected to the network the DNS server learns its name and automatically adds it to the DNS table. Other network users may immediately communicate with this computer using either its name or its IP address. In addition your gateway's DNS:

- Shares a common database of domain names and IP addresses with the DHCP server.
- Supports multiple subnets within the LAN simultaneously.
- Automatically appends a domain name to unqualified names.
- Allows new domain names to be added to the database using iPECS SBG-1000's WBM.
- Permits a computer to have multiple host names.
- Permits a host name to have multiple IPs (needed if a host has multiple network cards).

The DNS server does not require configuration. However, you may wish to view the list of computers known by the DNS, edit the host name or IP address of a computer on the list, or manually add a new computer to the list.

5.8.1.1 Viewing and Modifying the DNS Table

Access this feature either from the ‘DNS Server’ menu item under the ‘Services’ tab, or by clicking the ‘DNS Server’ icon in the ‘Shortcut’ screen. The DNS table will be displayed (see Figure 5.189).

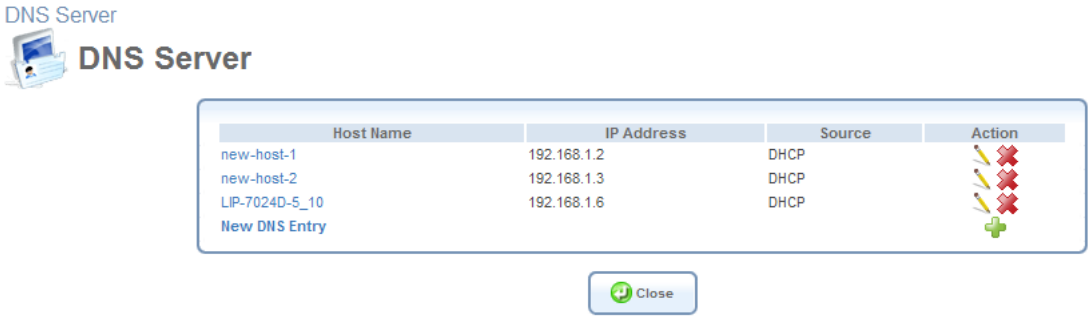


Figure 5.189 DNS Table

To add a new entry to the list:

1. Click the ‘New DNS Entry’ button. The ‘DNS Entry’ screen will appear (see Figure 5.190).

2. Enter the computer’s host name and IP address.

3. Click ‘OK’ to save the settings.

Figure 5.190 Add or Edit a DNS Entry

To edit the host name or IP address of an entry:

1. Click the ‘Edit’ button that appears in the Action column. The ‘DNS Entry’ screen appears (see Figure 5.190).

2. If the host was manually added to the DNS Table then you may modify its host name and/or IP address, otherwise you may only modify its host name.

3. Click ‘OK’ to save the settings.

To remove a host from the DNS table:

1. Click the ‘Delete’ button that appears in the Action column. The entry will be removed from the table.

6. System

6.1 Viewing the System Information

The ‘Overview’ screen (see Figure 6.1) displays the gateway’s software and hardware characteristics, as well as its uptime.

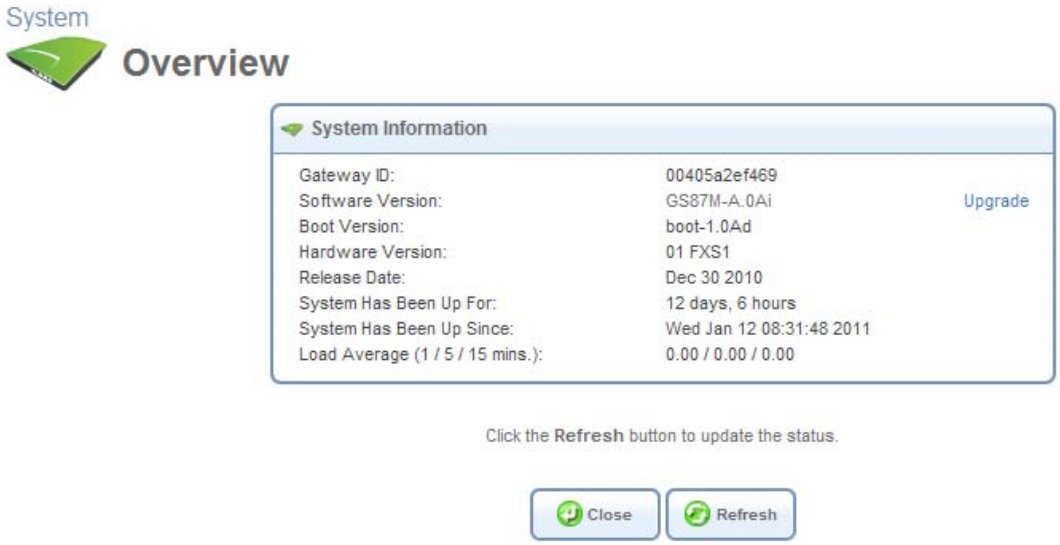


Figure 6.1 System Overview

6.2 Settings

6.2.1 Overviewing and Configuring System Settings

The ‘System Settings’ screen enables you to configure various system and management parameters.

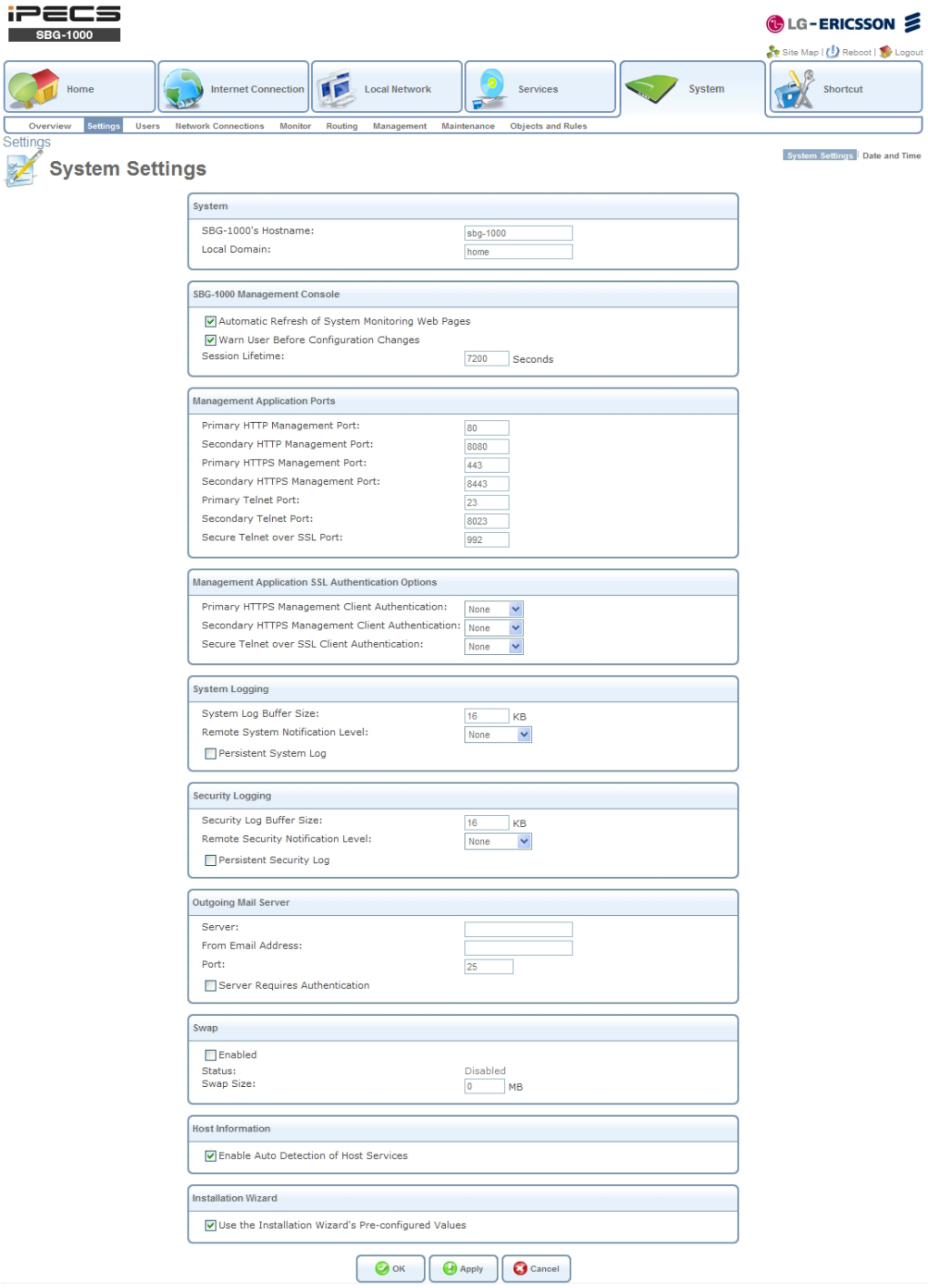


Figure 6.2 System Settings

System Configure general system parameters.

iPECS SBG-1000's Hostname Specify the gateway's host name. The host name is the gateway's URL address.

Local Domain Specify your network's local domain.

iPECS SBG-1000 Management Console Configure Web-based management settings.

Automatic Refresh of System Monitoring Web Pages Select this check-box to enable the automatic refresh of system monitoring web pages.

Warn User Before Network Configuration Changes Select this check-box to activate user warnings before network configuration changes take effect.

Session Lifetime The duration of idle time (in seconds) in which the WBM session will remain active. When this duration times out, the user will have to re-login.

User Interface Theme You can select an alternative GUI theme from the list provided.

Management Application Ports Configure the following management application ports:

1. Primary/secondary HTTP ports
2. Primary/secondary HTTPS ports
3. Primary/secondary Telnet ports
4. Secure Telnet over SSL port


Note: You can selectively enable these management application ports in the ‘Remote Administration’ screen (for more information, refer to Section 6.7.3).

Management Application SSL Authentication Options Configure the remote client authentication settings, for each of the following iPECS SBG-1000 management options:

1. Primary HTTPS Management Client Authentication
2. Secondary HTTPS Management Client Authentication
3. Secure Telnet over SSL Client Authentication

The applied authentication settings can be either of the following:

None The client is not authenticated during the SSL connection. Therefore, the client does not need to have a certificate recognized by iPECS SBG-1000, which can be used for authentication (for more information about certificates, refer to Section 6.9.4). This is the default setting for all of the mentioned management options.

Required The client is required to have a valid certificate, which is used instead of the regular login procedure. If the client does not have such a certificate, the connection is terminated.

Optional If the client has a valid certificate, it may be used for authentication instead of the regular login procedure. This means that in case of the HTTPS management session, the user, having a valid certificate, directly accesses the ‘Network Map’ screen of iPECS SBG-1000’s WBM.

In case of the secure Telnet connection, the user, having a valid certificate, directly accesses iPECS SBG-1000’s CLI prompt. To learn how to establish a secure Telnet connection to iPECS SBG-1000, refer to Section 6.7.3. Note that the ‘Common Name’ (**CN**) parameter in the **Subject**

field of a client's certificate should contain an existing username, to which administrative permissions are assigned.

System Logging Configure system logging parameters. You can view the system log in the 'System Log' screen under 'Monitor' (refer to Section 6.5.3).

System Log Buffer Size Set the size of the system log buffer in Kilobytes.

Remote System Notification Level By default, the 'None' option is selected, which means that iPECS SBG-1000 will not send notifications to a remote host. To activate the feature, select one of the following notification types:

- Error
- Warning
- Information

The screen refreshes, displaying the 'Remote System Host IP Address' field.

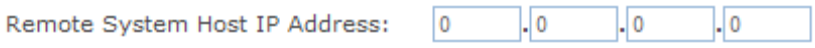


Figure 6.3 Remote System Host IP Address

Enter the remote host's IP address and click 'Apply'.

Note: If you would like to view iPECS SBG-1000's system logs on a LAN host, you must first install and run the syslog server.

Persistent System Log Select this check box to save the system log to the Flash---the gateway's permanent memory. This will prevent the system log from being erased when the gateway reboots. Note that by default, this check box is deselected.

Security Logging Configure security logging parameters.

Security Log Buffer Size Set the size of the security log buffer in Kilobytes.

Remote Security Notification Level The remote security notification level can be one of the following:

- None
- Error
- Warning
- Information

Persistent Security Log Select this check box to save the security log to the Flash. This will prevent the security log from being erased when the gateway reboots. Note that by default, this check box is deselected.

Note: Do not leave the persistent logging feature enabled permanently, as continuous writing of the log files to the Flash reduces gateway's performance.

Outgoing Mail Server Configure outgoing mail server parameters.

Server Enter the hostname of your outgoing (SMTP) server in the 'Server' field.

From Email Address Each email requires a 'from' address and some outgoing servers refuse to forward mail without a valid 'from' address for anti-spam considerations. Enter a 'from' email address in the 'From Email Address' field.

Port Enter the port that is used by your outgoing mail server.

Server Requires Authentication If your outgoing mail server requires authentication check the 'Server Requires Authentication' check-box and enter your user name and password in the 'User Name' and 'Password' fields respectively.

Swap This feature enables you to free a portion of the RAM by creating a swap file on the storage device connected to iPECS SBG-1000. This is especially useful for platforms with a small RAM. To activate this feature:

1. Verify that a storage device is connected to iPECS SBG-1000.
2. Select the 'Enabled' check box.
3. In the 'Swap Size' field, enter a swap file size in megabytes.
4. Click 'Apply'. A swap file is created on the storage device, and the feature's status changes to 'Ready'.

Host Information iPECS SBG-1000 can auto-detect its LAN hosts' properties, available services, traffic statistics, and connections (for more information refer to Section 4.1). To enable this feature, select its check box.

Installation Wizard Select the 'Use Installation Wizard Pre-configured Values' check box to have the wizard skip the steps for which parameters had been preconfigured and saved in factory settings file (**rg_factory**).

6.2.2 Setting the Date and Time

The 'Date and Time' menu item enables you to configure your gateway's time, date, time zone and daylight saving (summer time) settings.

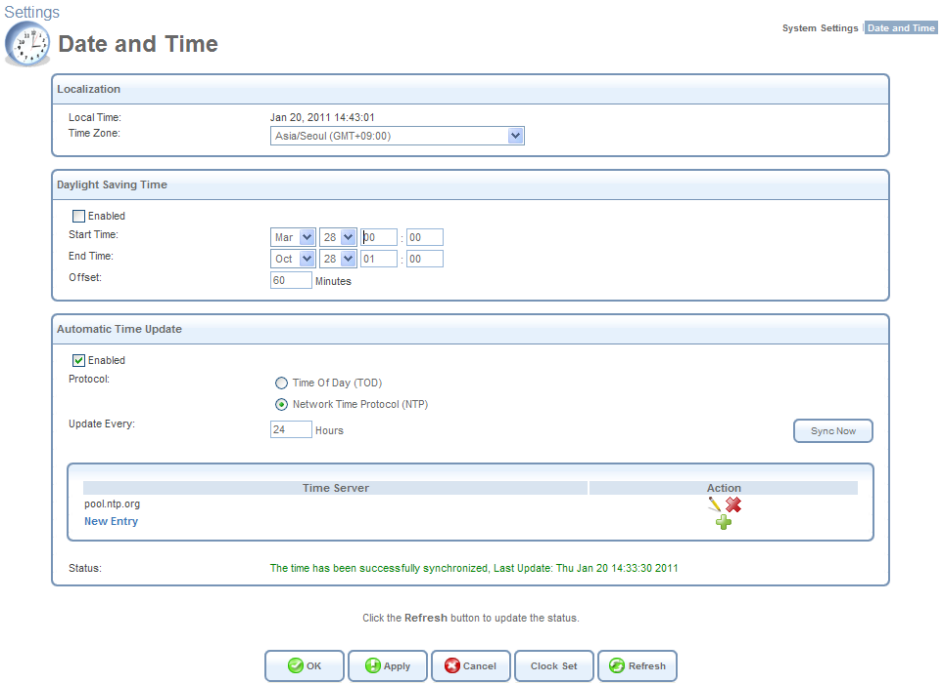


Figure 6.4 Date and Time Settings

Setting Your Local Time Zone

From the 'Time Zone' drop-down menu, select a time zone that corresponds to your current location. If you wish to manually define your time zone settings, select the 'Other' option. The screen refreshes, displaying the 'GMT Offset' field.

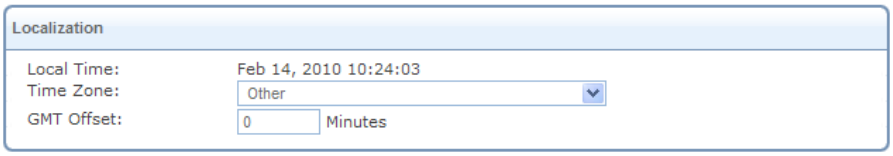


Figure 6.5 Local Time Zone – GMT Offset

This field enables you to manually adjust your local time's offset from the Greenwich Mean Time (GMT).

Configuring the Daylight Saving Settings

iPECS SBG-1000 automatically detects the daylight saving settings of a large number of time zones, by using its internal time zone database. There are several time zones, however, for which the daylight saving settings have not been preset on iPECS SBG-1000, as they may vary occasionally. In case the daylight saving settings of your selected time zone may periodically vary, the following fields appear, enabling you to manually configure your local daylight saving time.

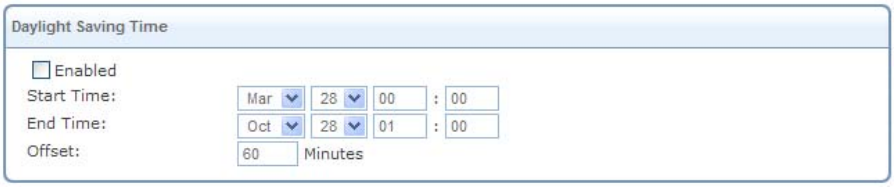


Figure 6.6 Daylight Saving Settings

Enabled Select this check box to automatically enable the daylight saving mode during the period specified below.
Start A date and time when your time zone's daylight saving period starts.
End A date and time when your time zone's daylight saving period ends.
Offset A daylight saving time offset from the standard (winter) time.

If you want the gateway to periodically perform an automatic time update, proceed as follows:

1. Select the 'Enabled' check box under the 'Automatic Time Update' section.

2. Select the protocol to be used to perform the time update by selecting either the 'Time of Day' or 'Network Time Protocol' radio button.

3. In the 'Update Every' field, specify the frequency of performing the update.

4. By default, iPECS SBG-1000 is configured with NTP Pool Project server for testing purposes only. You can define another time server address by clicking the 'New Entry' link at the bottom of the 'Automatic Time Update' section. You can find a list of time server addresses sorted by region at http://www.pool.ntp.org.

If you wish to manually set the local time and current date, perform the following:

1. Click the 'Clock Set' button. The 'Clock Set' screen appears.

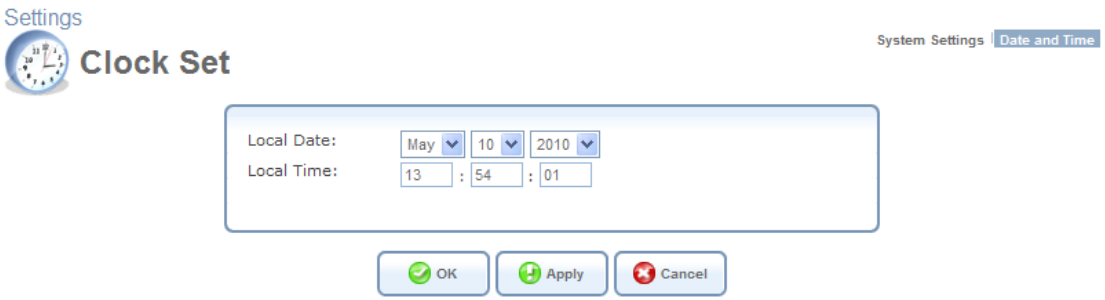


Figure 6.7 Clock Set

2. Adjust the settings as necessary and click 'OK'. You are redirected back to the 'Date and Time' screen.

6.3 Managing Users

The 'Users' menu item enables you to view and edit the defined user accounts.

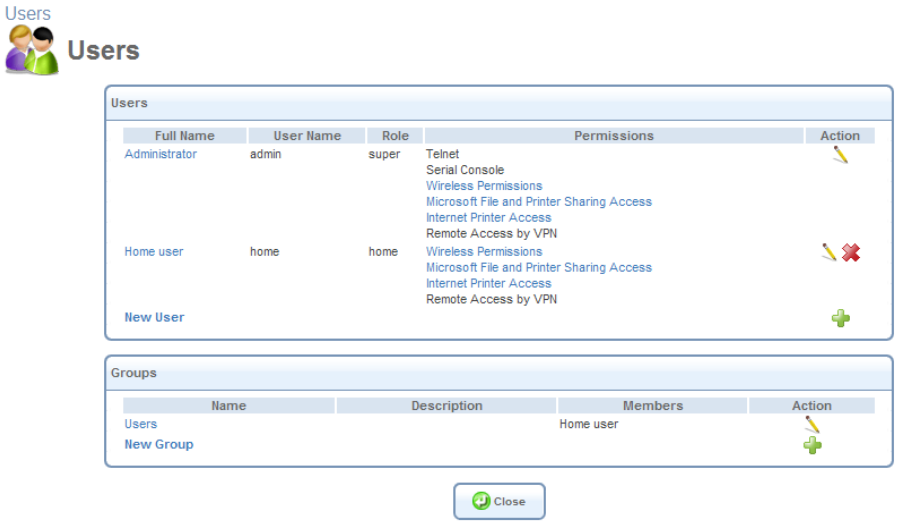


Figure 6.8 Users

By default, only one user account (Admin) is available.

6.3.1 Editing a User's Profile

To edit a user's profile (for example, change the assigned permissions or password), click the user's link or the corresponding action icon (see Figure 6.8). The 'User Settings' screen appears.

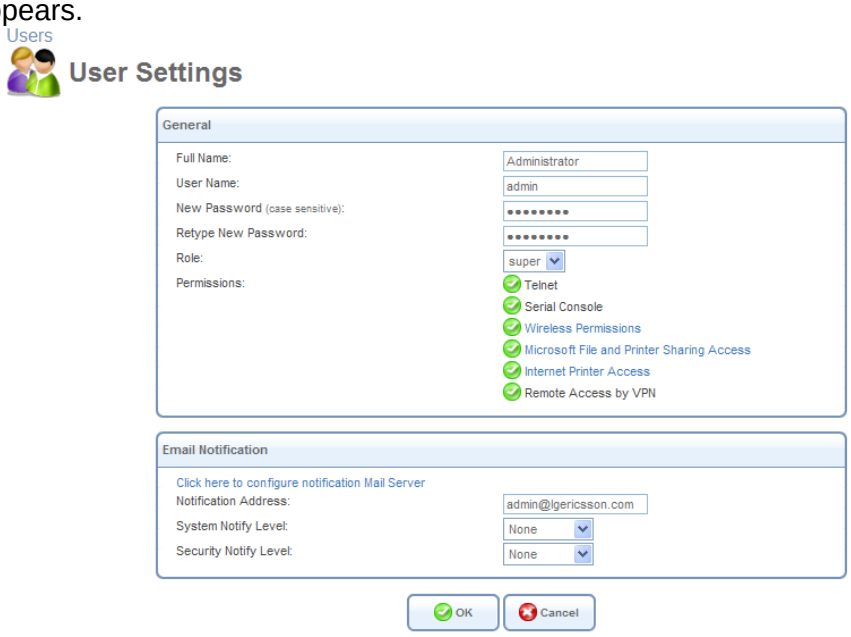


Figure 6.9 User Settings

After making necessary changes, click 'OK' to save them.

Important Note: Selecting the 'guest' role and applying this setting disables the user's permission to access iPECS SBG-1000's WBM, until the gateway is restored to defaults. After making the necessary changes, click 'OK' to save them.

6.3.2 Disk Management

Enable User Home Directory By default, this option is selected. When activated, it creates a directory for the user in the 'Home' directory of the system storage area. This directory is necessary when using various applications, such as the mail server. For more information, refer to Section 5.5.4.2.

6.3.3 E-Mail Notification

You can use email notification to receive indications of system events for a predefined severity classification. The available types of events are 'System' or 'Security' events. The available severity of events are 'Error', 'Warning' and 'Information'.
If the 'Information' level is selected, the user will receive notification of the 'Information', 'Warning' and 'Error' events. If the 'Warning' level is selected, the user will receive notification of the 'Warning' and 'Error' events etc.

To configure email notification for a specific user:

- Make sure you have configured an outgoing mail server in 'System Settings'. A click on the 'Configure Mail Server' link will display the 'System Settings' screen where you can configure the outgoing mail server.
- Enter the user's email address in the 'Address' field of the 'Email' section.
- Select the 'System' and 'Security' notification levels in the 'System Notify Level' and 'Security Notify Level' drop-down menu respectively.

6.3.4 Creating User Groups

You may assemble your defined users into different groups, based on different criteria—for example, home users versus office users. By default, new users will be added to the default group "Users". To add a new group, click the 'New Group' link. The 'Group Settings' screen appears.

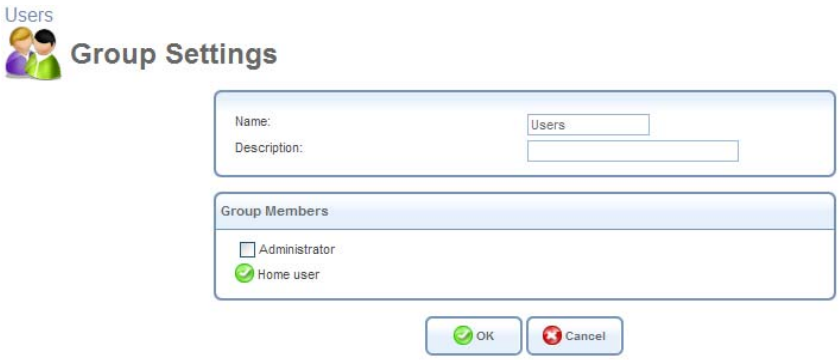


Figure 6.10 Group Settings

Name Enter a name for the group of users.
Description You may also enter a short description for the group.
Group Members Select the users that will belong to this group. All users defined are presented in this section. A user can belong to more than one group.

6.4 Network Connections

This chapter describes the different network connections available with iPECS SBG-1000, as well as the connection types that you can create. iPECS SBG-1000 supports both physical and logical network connections. When clicking the 'Network Connections' menu item under 'System', the 'Network Connections' screen appears, enabling you to configure the various parameters of your physical connections (the LAN and WAN), and create new connections, using tunneling protocols over existing connections (such as PPP and VPN).

Figure 6.11 Network Connections

iPECS SBG-1000's physical network connections are:

LAN – Creating a home/SOHO network

- LAN Bridge (refer to Section 6.4.4).
- LAN Ethernet (refer to Section 6.4.3).
- LAN Wireless 802.11n Access Point (refer to Section 6.4.5).

WAN – Internet Connection

- WAN Ethernet (refer to Section 6.4.6).

The logical network connections available with iPECS SBG-1000 are:

WAN – Internet Connection

- Point-to-Point Protocol over Ethernet (refer to Section 6.4.7).
- Point-to-Point Tunneling Protocol (refer to Section 6.4.10).
- Layer 2 Tunneling Protocol (refer to Section 6.4.8).
- WAN-LAN Bridge (refer to Section 6.4.14).

Virtual Private Network over the Internet

- Layer 2 Tunneling Protocol over Internet Protocol Security (refer to Section 6.4.8).
- Layer 2 Tunneling Protocol Server (refer to Section 6.4.9).
- Point-to-Point Tunneling Protocol Virtual Private Network (refer to Section 6.4.10).
- Point-to-Point Tunneling Protocol Server (refer to Section 6.4.11).
- Internet Protocol Security (refer to Section 6.4.12).
- Internet Protocol Security Server (refer to Section 6.4.13).

Advanced Connections

- Network Bridging (refer to Section 6.4.4 and Section 6.4.14).
- VLAN Interface (refer to Section 6.4.17).
- Internet Protocol over Internet Protocol (refer to Section 6.4.15).
- General Routing Encapsulation (refer to Section 6.4.16).

6.4.1 Network Types

Every network connection in iPECS SBG-1000 can be configured to operate in one of three modes: WAN, LAN or DMZ. This provides high flexibility and increased functionality. For example, you may define that a LAN Ethernet connection on iPECS SBG-1000 will operate as a WAN network. This means that all hosts in this LAN will be referred to as WAN computers, both by computers outside iPECS SBG-1000 and by iPECS SBG-1000 itself. WAN and firewall rules may be applied as on any other WAN network.
Another example is a network connection that is defined as a DMZ (Demilitarized) network. Although this network is physically inside iPECS SBG-1000, it will function as an unsecured, independent network, for which iPECS SBG-1000 merely acts as a router.

6.4.2 Using the Connection Wizard

The logical network connections can be easily created using the Connection Wizard. This wizard consists of a series of management screens, intuitively structured to gather all the information needed to create a logical connection.

6.4.2.1 Creating Connections on an Ethernet Gateway

To initiate a connection setup using the wizard, click the ‘New Connection’ link in the ‘Network Connections’ screen (see Figure 6.11). The ‘Connection Wizard’ screen appears.

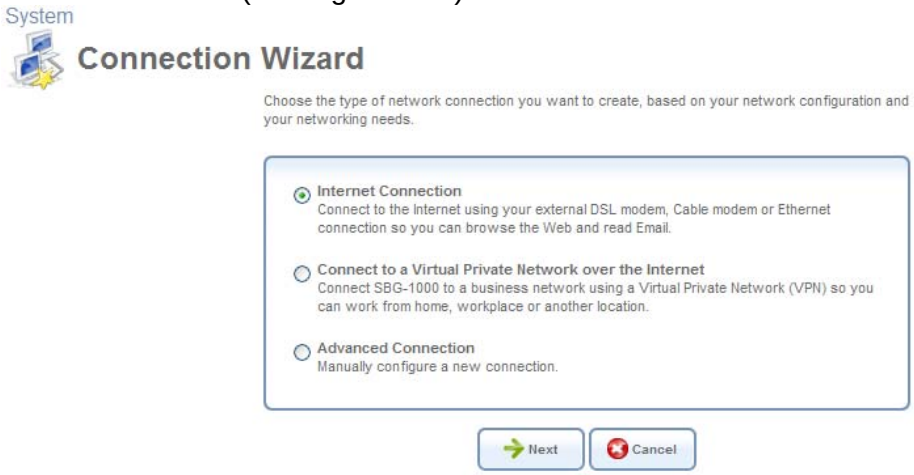


Figure 6.12 Connection Wizard

This screen presents you with the main connection types. Each option that you choose will lead you to further options, adding more information with each step and narrowing down the parameters towards the desired network connection.

Internet Connection – Selecting this option takes you to the 'Internet Connection' screen, enabling you to set up your Internet connection, in one of the available methods.

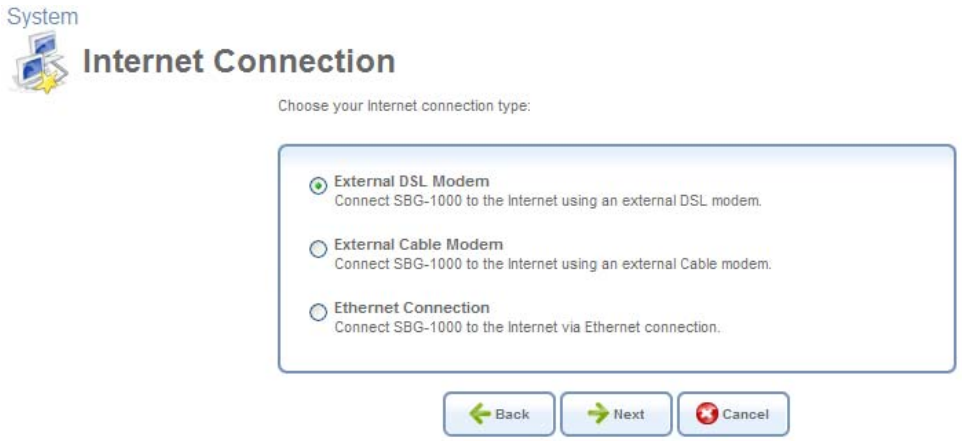


Figure 6.13 Internet Connection Wizard Screen

The Internet connection setup options are depicted in Figure 6.14, where rectangles represent the steps/screens to be taken and ellipses represent the available connections.

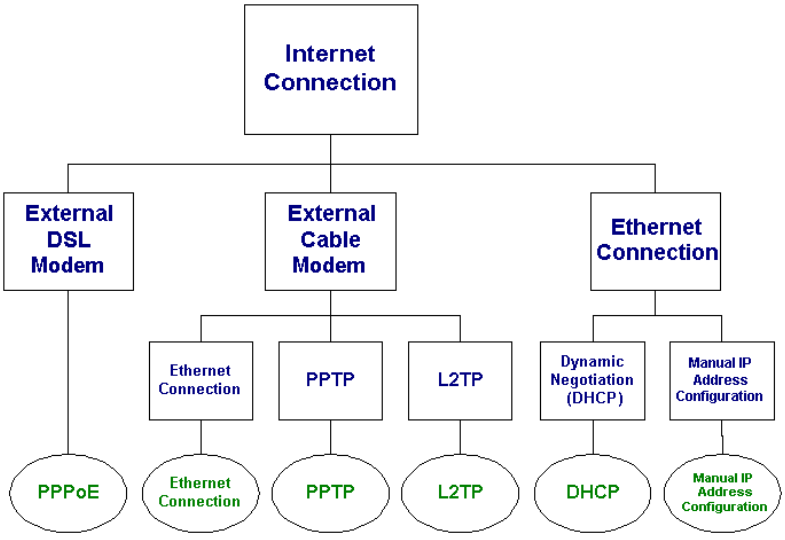


Figure 6.14 Internet Connection Wizard Tree

Connect to a Virtual Private Network over the Internet – Selecting this option takes you to the 'Connect to a Virtual Private Network over the Internet' screen, enabling you to securely connect iPECS SBG-1000 to a business network using a Virtual Private Network (VPN).

Figure 6.15 VPN Wizard Screen

The VPN setup options are depicted in Figure 6.16, assisting you in choosing a VPN setup mode that suits your needs—either a VPN client or a server.

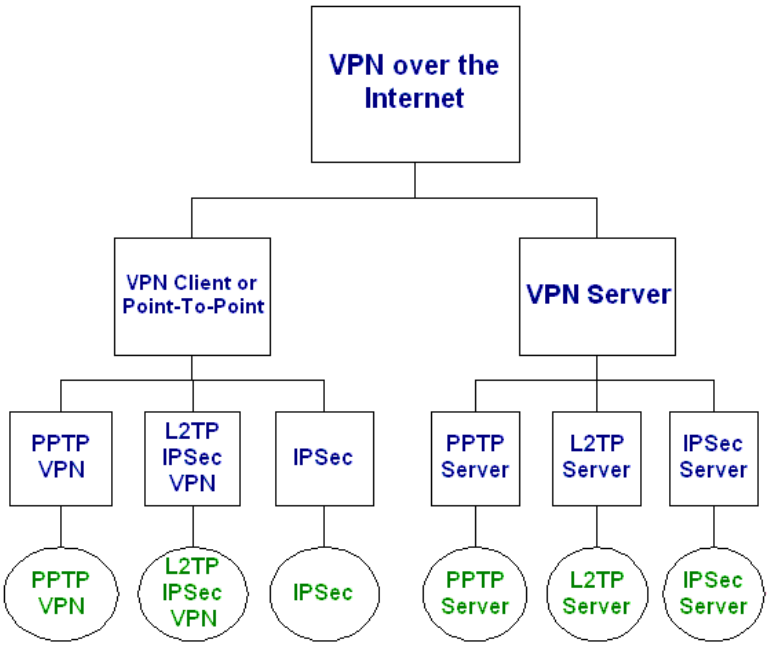


Figure 6.16 VPN Wizard Tree

Advanced Connection – Selecting this option takes you to the 'Advanced Connection' screen, enabling you to select a type of logical network connection setup that you would like to initiate. In addition, it provides a wizard for creating the Network Bridge and VLAN Interface connections.

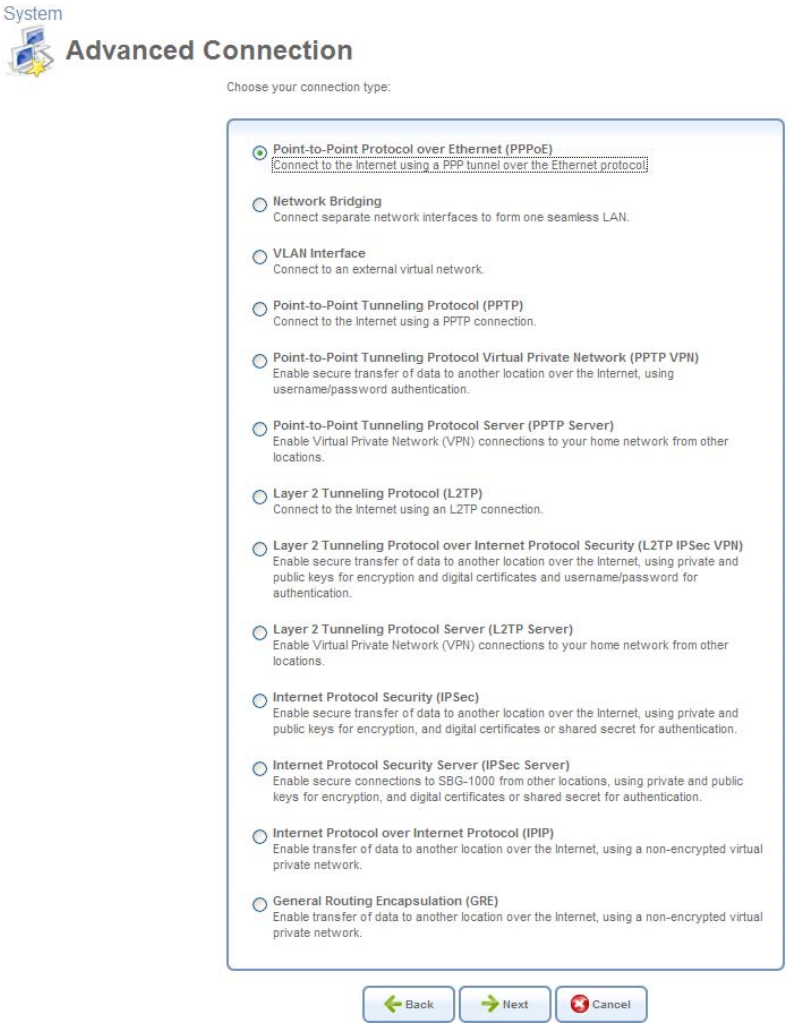


Figure 6.17 Advanced Connection Wizard Screen

The Advanced Connection options are depicted in Figure 6.18.

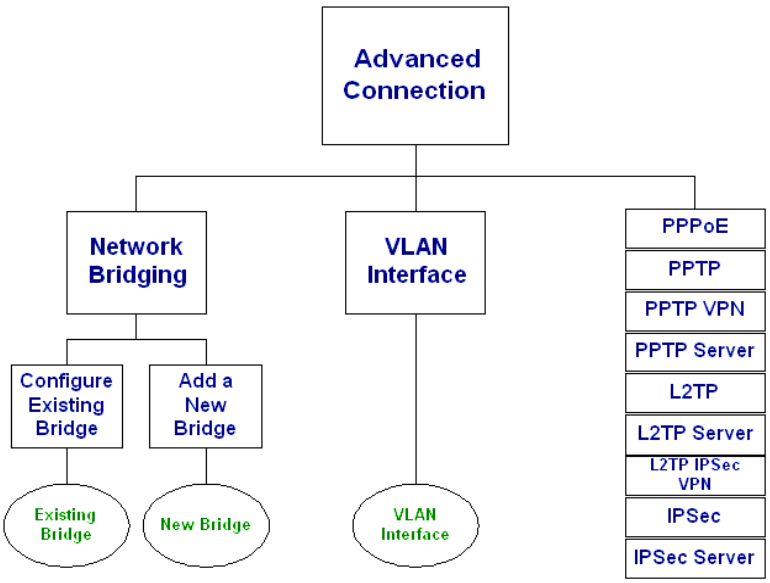


Figure 6.18 Advanced Connection Wizard Tree

6.4.3 Configuring the LAN Ethernet Settings

The LAN Ethernet interface represents all of iPECS SBG-1000's LAN ports. To view and modify the LAN Ethernet settings, click the 'LAN Ethernet' link in the 'Network Connections' screen (see Figure 6.11). The 'LAN Ethernet Properties' screen appears.

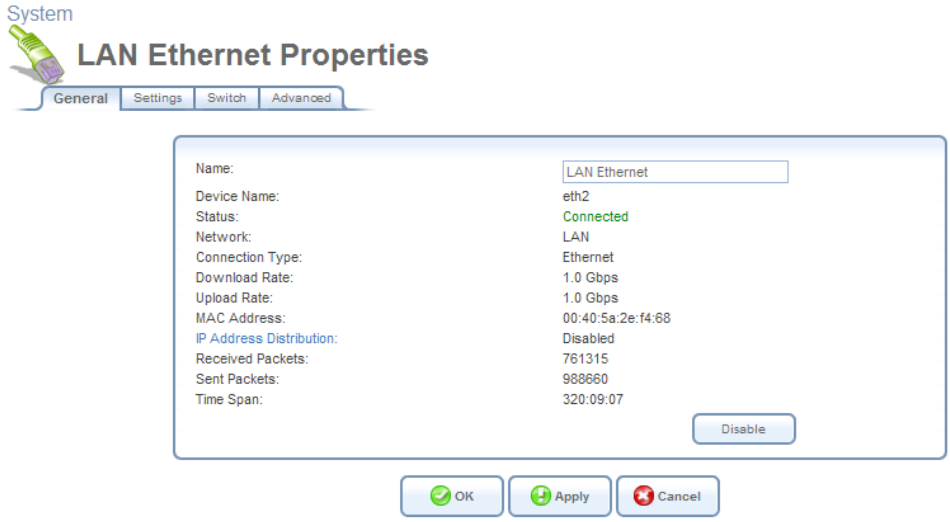


Figure 6.19 LAN Ethernet Properties

6.4.3.1 General

This sub-tab enables you to view the LAN Hardware Ethernet Switch settings (see Figure 6.19). These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.3.2 Settings

This sub-tab displays the connection's general parameters. It is recommended not to change the default values unless you are familiar with the networking concepts they represent. Since your gateway is configured to operate with the default values, no parameter modification is necessary.

Figure 6.20 Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a

scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind iPECS SBG-1000.

Physical Address The physical address of the network interface for your network. Some interfaces allow you to change this address.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

6.4.3.3 Switch

This sub-tab displays the hardware switch ports properties. The switch ports are physical sockets on the board, to which different cables connect. The table in this screen consists of a list of all available ports, their status, and the VLANs of which they are members. Untagged packets (packets with no VLAN tag) that arrive in a port, will be tagged with the VLAN number that appears under the Port VLAN Identifier (PVID) column.

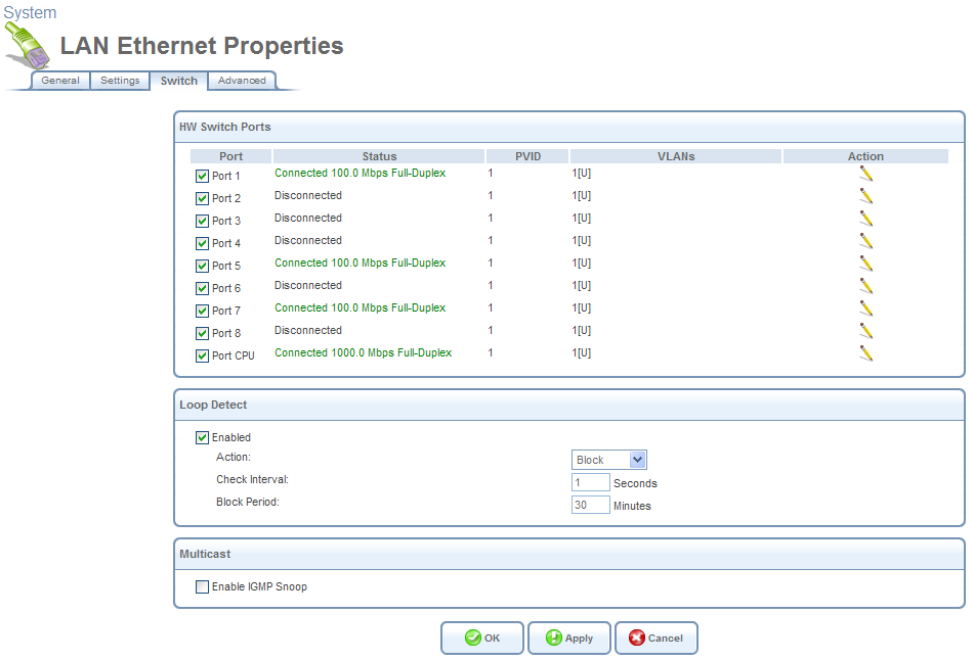


Figure 6.21 Switch

You can edit the configuration of each port. To do so, click a connected port's action icon. The 'Port LAN Settings' screen appears.

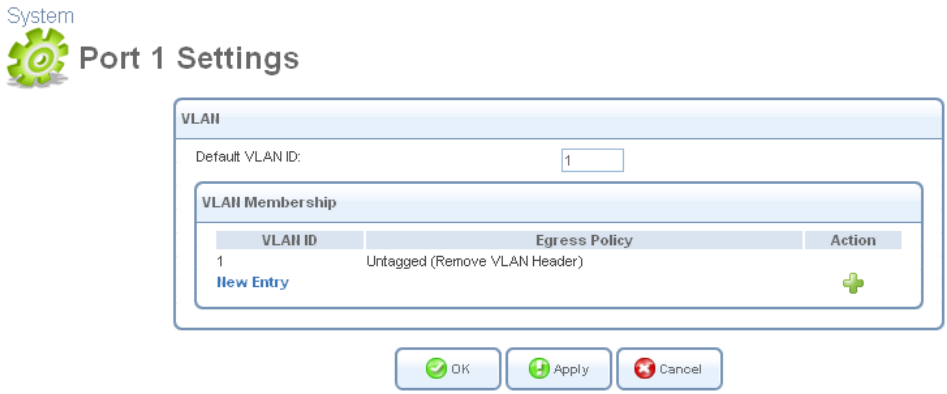


Figure 6.22 Port LAN Settings

Default VLAN ID The port's VLAN identifier. You may add additional identifiers to the VLAN by clicking 'New Entry'.
Refer Section 6.4.17 VLAN configuration for detail information.

6.4.3.4 Advanced

This sub-tab enables you to configure the following advanced switch settings.
Internet Connection Firewall Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

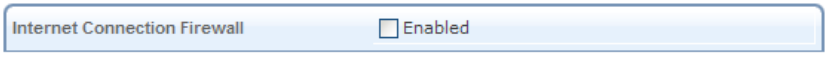


Figure 6.23 Internet Connection Firewall

Additional IP Addresses You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1 and the http://sbg-1000.home.

Figure 6.24 Additional IP Addresses

6.4.4 Setting Up a LAN Bridge

The LAN bridge connection is used to combine several LAN devices under one virtual network. For example, creating one network for LAN Ethernet and LAN wireless devices. Note that when a bridge is removed, its formerly underlying devices inherit the bridge's DHCP settings. For example,

the removal of a bridge that is configured as DHCP client, automatically configures the LAN devices formerly constituting the bridge as DHCP clients, with the exact DHCP client configuration.

6.4.4.1 Creating a LAN Bridge Connection

To create a new bridge or configure an existing one, perform the following:

1. In the ‘Network Connections’ screen under ‘System’ (see Figure 6.11), click the ‘New Connection’ link. The ‘Connection Wizard’ screen appears (see Figure 6.12).

2. Select the ‘Advanced Connection’ radio button and click ‘Next’. The ‘Advanced Connection’ screen appears.

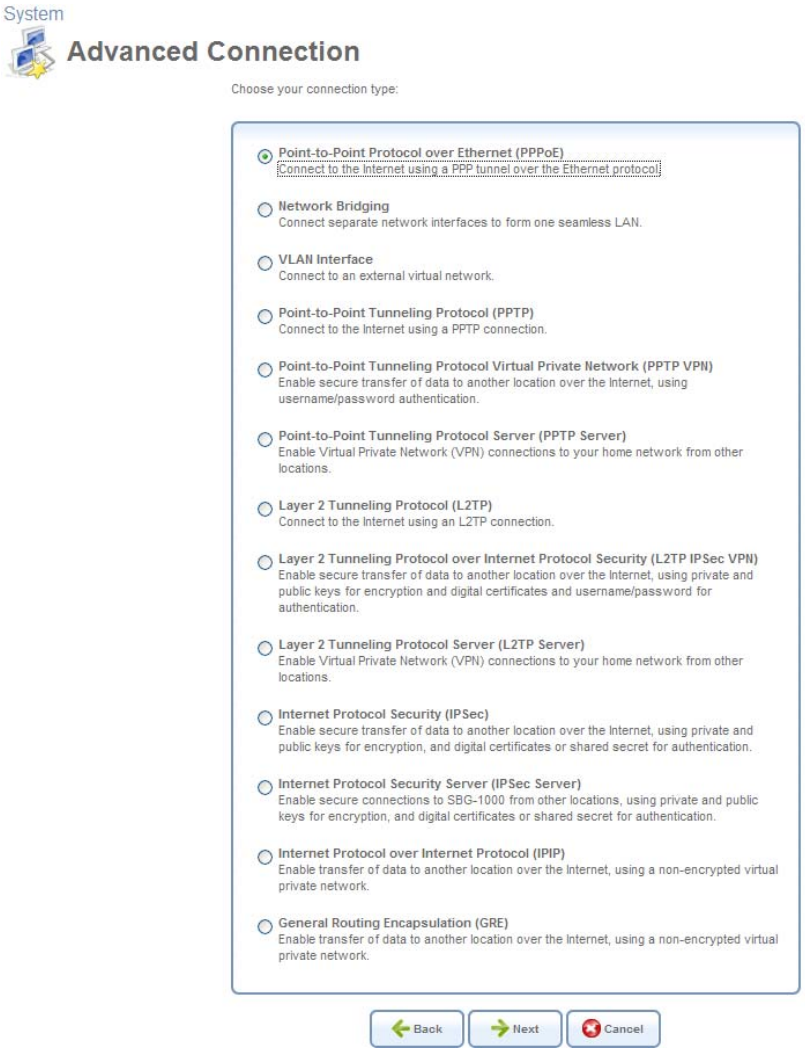


Figure 6.25 Advanced Connection Wizard

3. Select the ‘Network Bridging’ radio button and click ‘Next’. The ‘Bridge Options’ screen appears.

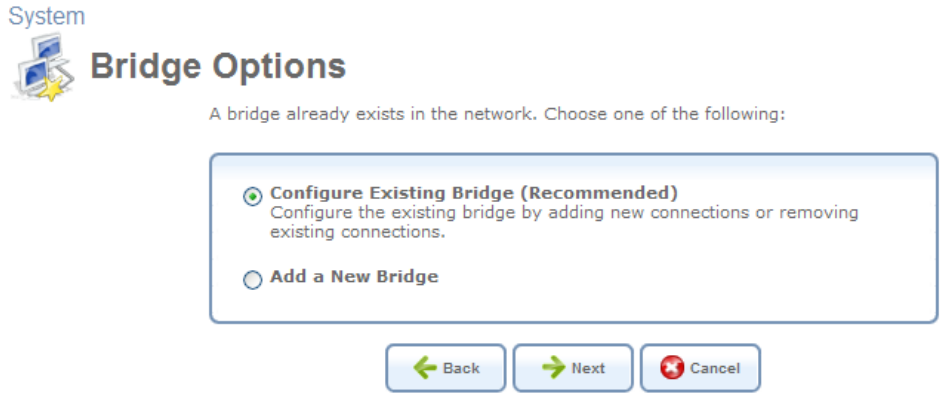


Figure 6.26 Bridge Options

4. Select whether to configure an existing bridge (this option will only appear if a bridge exists) or to add a new one:

   a. **Configure Existing Bridge** Select this option and click ‘Next’. The ‘Network Bridging’ screen appears allowing you to add new connections to the bridge or remove existing ones, by selecting or deselecting their respective check boxes. For example, to create a WAN-LAN bridge, select the WAN connection’s check box.

Figure 6.27 Network Bridging – Configure Existing Bridge

   b. **Add a New Bridge** Select this option and click ‘Next’. A different ‘Network Bridging’ screen appears allowing you to add a bridge over the unbridged connections, by selecting their respective check boxes.

Figure 6.28 Network Bridging – Add a New Bridge

5. Click ‘Next’. The ‘Connection Summary’ screen appears, corresponding to your changes.

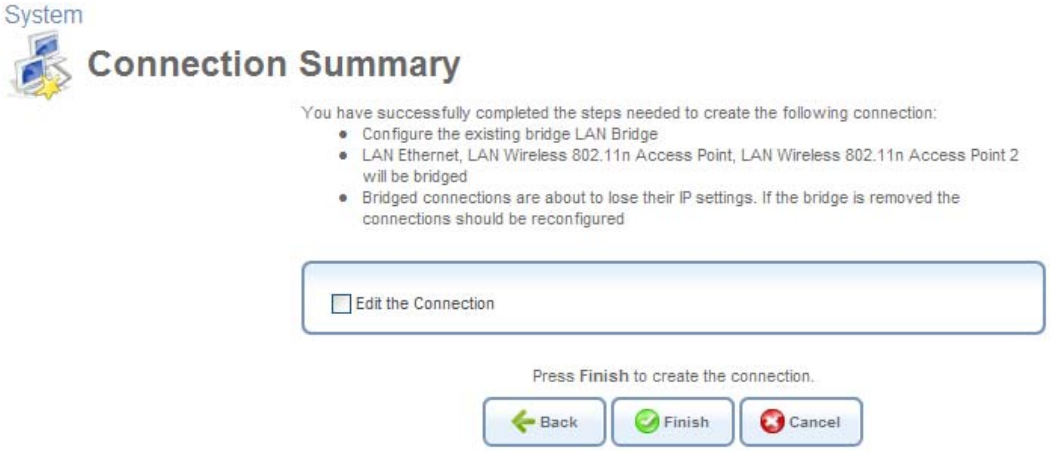


Figure 6.29 Connection Summary – Configure Existing Bridge

6. Select the ‘Edit the Newly Created Connection’ check box if you wish to be routed to the new connection’s configuration screen after clicking ‘Finish’. This screen is described later in this chapter.

7. Click ‘Finish’ to save the settings. The new bridge will be added to the network connections list, and it will be configurable like any other bridge.

The new bridge will be added to the network connections list, and it will be configurable like any other bridge.

Note: Creating a WAN-LAN bridge disables iPECS SBG-1000’s DHCP server. This means that LAN hosts may only receive an IP address from a DHCP server on the WAN. If you configure a host with a static IP address from an alias subnet of the bridge (192.168.1.X), you will be able to access iPECS SBG-1000 but not the WAN, as NAT is not performed in the WAN-LAN bridge mode.

6.4.4.2 Viewing and Editing the LAN Bridge Settings

After creating a bridge, you can view or modify its settings by clicking the bridge's entry in the 'Network Connections' screen. The 'LAN Bridge Properties' screen appears.

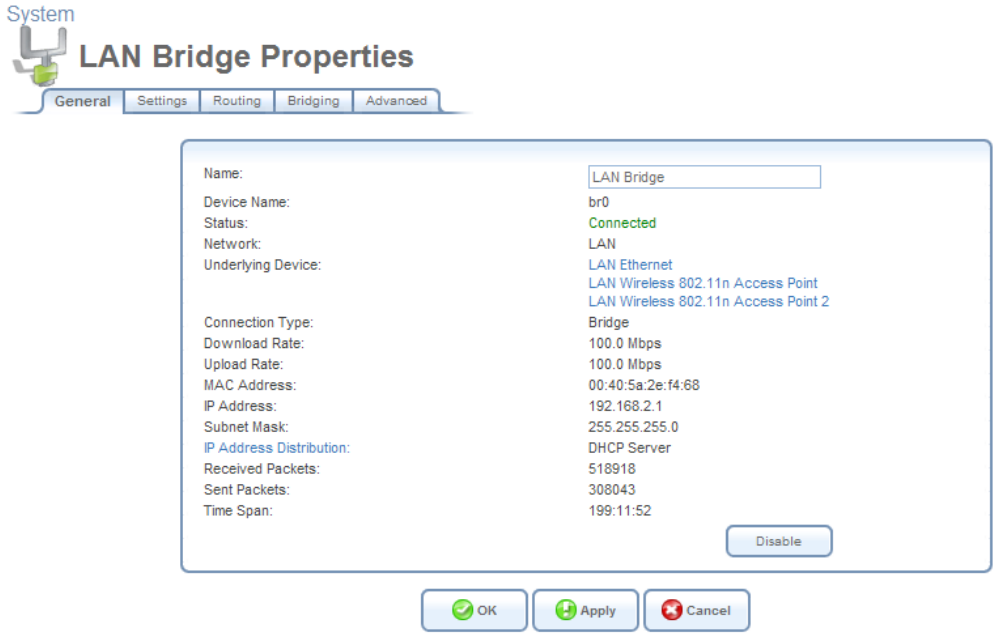


Figure 6.30 LAN Bridge Properties

6.4.4.2.1 General

This sub-tab enables you to view the LAN bridge connection settings (see Figure 6.30). These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.4.2.2 Settings

This sub-tab enables you to edit the following LAN bridge settings.

General This section displays the connection's general parameters. It is recommended not to change the default values unless you are familiar with the networking concepts they represent. Since your gateway is configured to operate with the default values, no parameter modification is necessary.

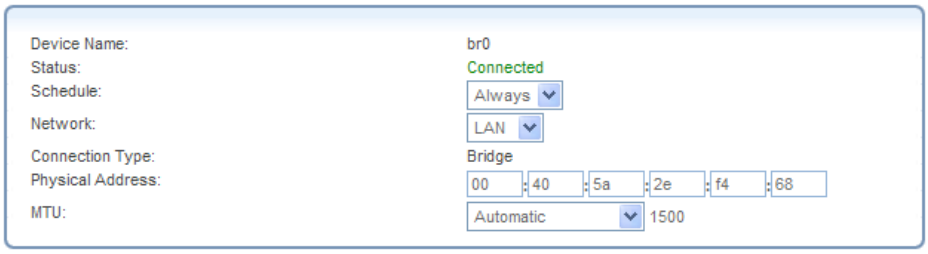


Figure 6.31 General Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a

scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind iPECS SBG-1000.

Physical Address The physical address of the network interface for your network. Some interfaces allow you to change this address.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen will refresh to display relevant configuration settings according to your choice.

No IP Address Select 'No IP Address' if you require that your gateway have no IP address. This can be useful if you are working in an environment where you are not connected to other networks, such as the Internet.

Figure 6.32 Internet Protocol – No IP Address

Obtain an IP Address Automatically Your connection is configured by default to act as a DHCP client. You should keep this configuration in case your service provider supports DHCP, or if you are connecting using a dynamic IP address. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead. You can click the 'Release' button to release the current leased IP address. Once the address has been released, the button text changes to 'Renew'. Use the 'Renew' button to renew the leased IP address.

Figure 6.33 Internet Protocol – Automatic IP

Use the Following IP Address Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

Figure 6.34 Internet Protocol – Static IP

DNS Server Domain Name System (DNS) is the method by which Web site domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

Figure 6.35 DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

Figure 6.36 DNS Server – Static IP

To learn more about this feature, refer to Section 5.8.1.

IP Address Distribution The 'IP Address Distribution' section allows you to configure the gateway's Dynamic Host Configuration Protocol (DHCP) server parameters. The DHCP automatically assigns IP addresses to network PCs. If you enable this feature, make sure that you also configure your network PCs as DHCP clients. For a comprehensive description of this feature, refer to Section 5.7. Select one of the following options from the 'IP Address Distribution' drop-down menu:

- **DHCP Server**

In case you have chosen DHCP Server, complete the following fields:

Start IP Address The first IP address that may be assigned to a LAN host. Since the LAN

interface's default IP address is 192.168.1.1, it is recommended that the first address assigned to a LAN host will be 192.168.1.2 or greater.

End IP Address The last IP address in the range that can be used to automatically assign IP addresses to LAN hosts.

Subnet Mask A mask used to determine to what subnet an IP address belongs. An example of a subnet mask value is 255.255.255.0.

Lease Time In Minutes Each device will be assigned an IP address by the DHCP server for this amount of time, when it connects to the network. When the lease expires the server will determine if the computer has disconnected from the network. If it has, the server may reassign this IP address to a newly-connected computer. This feature ensures that IP addresses that are not in use will become available for other computers on the network.

Provide Host Name If Not Specified by Client If the DHCP client does not have a host name, the gateway will automatically assign one for it.

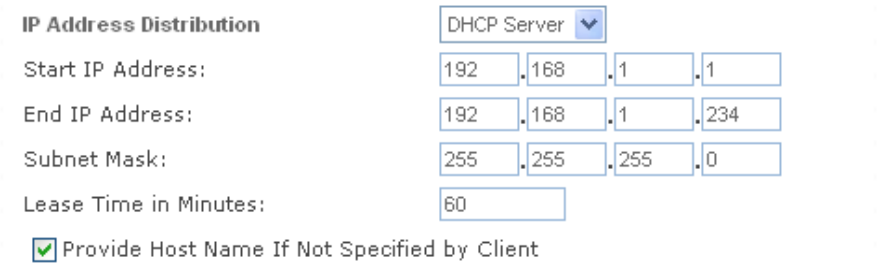


Figure 6.37 IP Address Distribution – DHCP Server

- **Disabled** Select 'Disabled' from the drop-down menu if you would like to statically assign IP addresses to your network computers.

Figure 6.38 IP Address Distribution – Disable DHCP

6.4.4.2.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

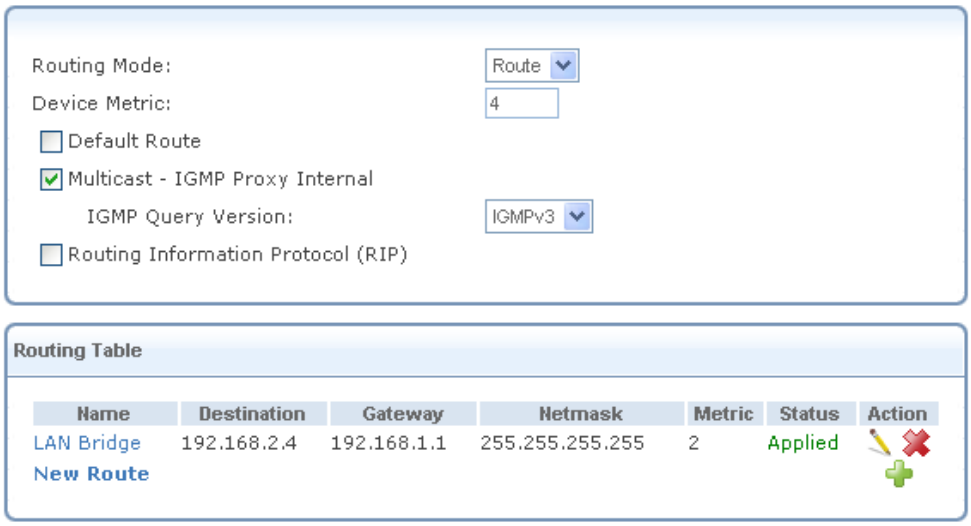


Figure 6.39 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

Route Use route mode if you want your gateway to function as a router between two networks.

NAPT Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default iPECS SBG-1000 serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version iPECS SBG-1000 supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- Listen to RIP messages—select either ‘None’, ‘RIPv1’, ‘RIPv2’ or ‘RIPv1/2’.

- Send RIP messages—select either ‘None’, ‘RIPv1’, ‘RIPv2-broadcast’ or ‘RIPv2-multicast’.

Routing Table Allows you to add or modify routes when this device is active. Use the ‘New Route’ button to add a route or edit existing routes. To learn more about routing, refer to Section 6.6.

6.4.4.2.4 Bridging

This sub-tab enables you to specify the devices that you would like to join under the network bridge.

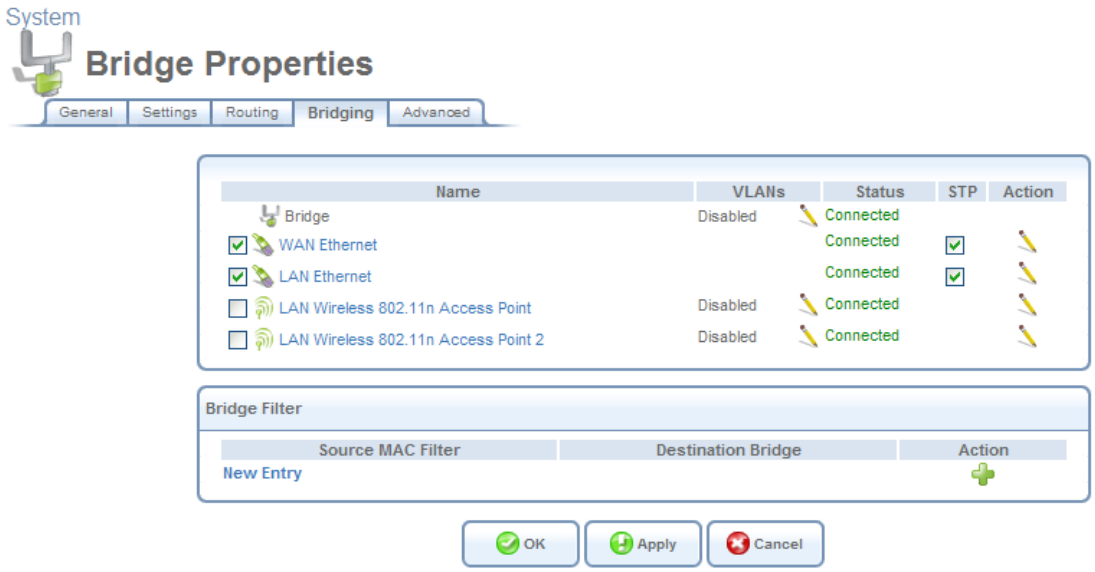


Figure 6.40 Bridge Settings

If you wish to assign the network connections to specific virtual LANS (VLANs), click the action icon under the ‘VLANs’ column.

Note: If you would like to logically partition your Ethernet-based network, you can set up a VLAN bridge as described in Section 6.4.17.5.

Select the ‘STP’ check box to enable the Spanning Tree Protocol on the device. Use this feature to ensure that there are no loops in your network configuration, especially in case your network consists of multiple switches, or other bridges apart from those created by the gateway. By blocking redundant connections, STP enables a single data path between LAN hosts. If a device or a link failure causes this path to become unusable, STP will enable an alternative path. Note that iPECS SBG-1000 also supports the Rapid Spanning Tree Protocol (RSTP), which provides a faster response to changes in your local network topology than STP.

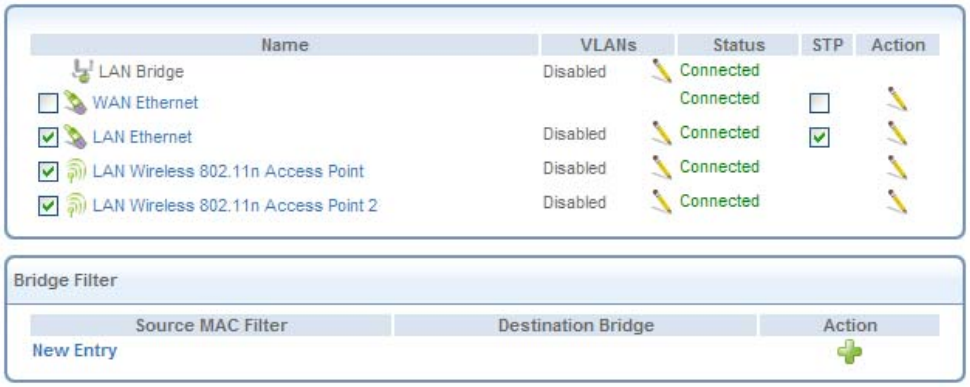


Figure 6.41 LAN Bridge Settings

Bridge Filter This section is used for creating a traffic filtering rule on the bridge, in order to enable direct packet flow between the WAN and the LAN. Such an example is when setting up a hybrid bridging mode (refer to Section 6.4.14.2).

Bridge Hardware Acceleration Select this check box to utilize the **Fastpath** algorithm for enhancing packet flow through the bridge. Note that this feature must be supported and enabled on the bridge's underlying devices in order to work properly.

6.4.4.2.5 Advanced

This sub-tab enables you to configure the advanced LAN bridge settings.

Internet Connection Firewall Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

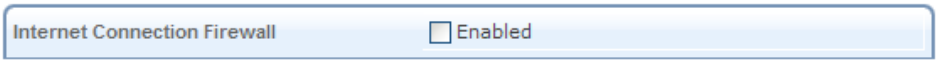


Figure 6.42 Internet Connection Firewall

Additional IP Addresses You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1 and the http://sbg-1000.home.

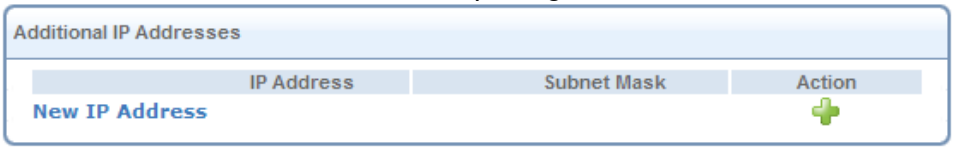


Figure 6.43 Additional IP Addresses

6.4.5 Setting Up a LAN Wireless Network

iPECS SBG-1000 provides broadband customer premise equipment (CPE) manufacturers with a complete software solution for developing feature-rich CPE with wireless connectivity over the 802.11 **b**, **g**, and **n** standards. The solution is vertically integrated and includes an operating system, communication protocols, routing, advanced wireless and broadband networking security, remote management and home networking applications.
iPECS SBG-1000 integrates multiple layers of wireless security. These include the IEEE 802.1x port-based authentication protocol, RADIUS client, EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, Wi-Fi Protected Access (WPA), WPA2, WPA and WPA2 (mixed mode), as well as industry-leading iPECS SBG-1000 Firewall and VPN applications. In addition, iPECS SBG-1000's built-in authentication server enables home/SOHO users to define authorized wireless users without the need for an external RADIUS server.

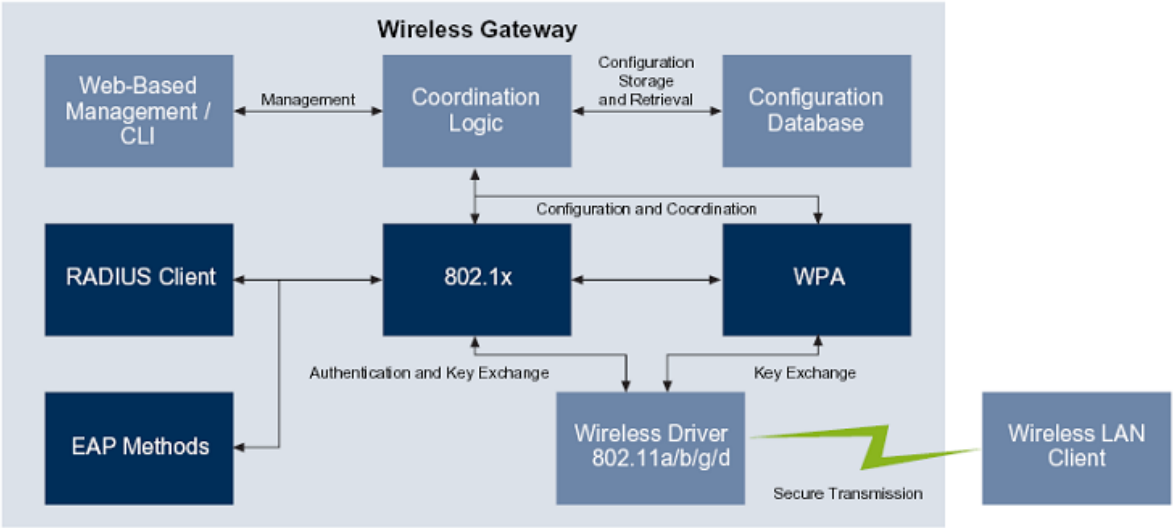


Figure 6.44 iPECS SBG-1000 for Wireless Gateways – Authentication and Encryption Components

6.4.5.1 Enabling iPECS SBG-1000's Wireless Network Interface

To enable iPECS SBG-1000's wireless network interface, perform the following:

1. Click the 'LAN Wireless 802.11n Access Point' link in the 'Network Connections' screen (see Figure 6.11). The 'LAN Wireless 802.11n Access Point Properties' screen appears.

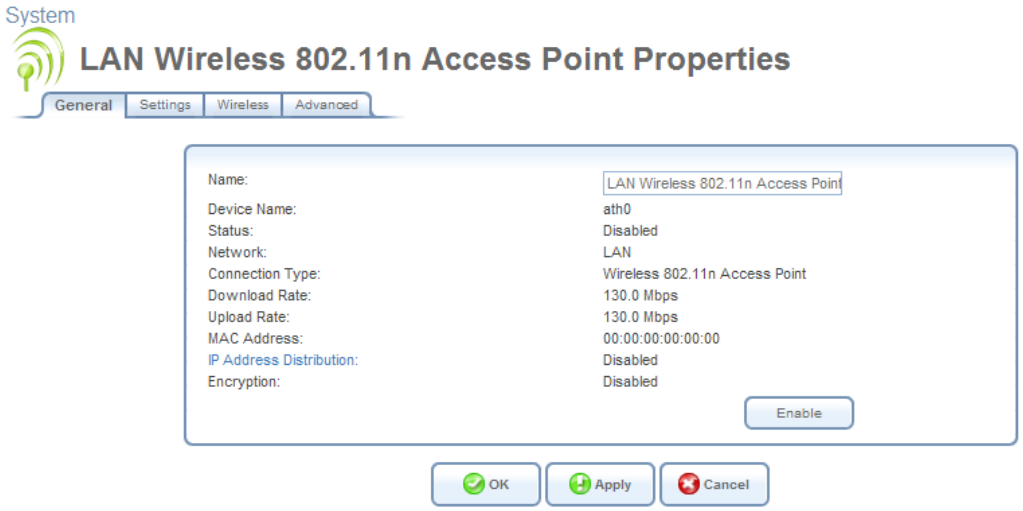


Figure 6.45 LAN Wireless 802.11n Access Point Properties – Disabled

2. Click the 'Enable' button (this button is displayed only if a wireless card is available on the gateway). The screen refreshes, and the connection status changes to "Connected".

3. Click the 'Wireless' sub-tab.

4. In the 'SSID' field, you may change the broadcasted name of your wireless network from the default to a more unique name.

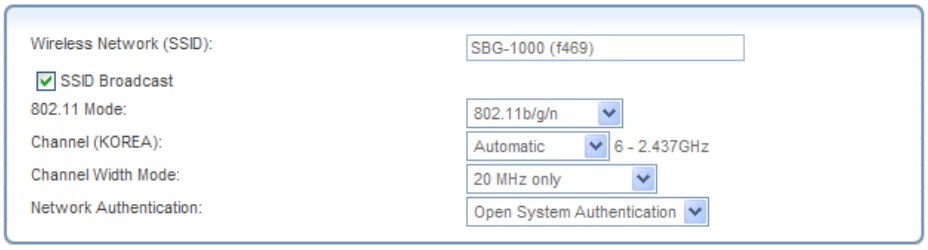


Figure 6.46 Wireless Access Point

5. Click 'OK' to save the settings.

Note: In order to connect a wireless PC to the gateway, you may also need to configure the PC, as described in the 'Connecting Your PC' section of the iPECS SBG-1000 User Manual.

By default, only HTTP authentication protects the wireless network from unauthorized users. Consider securing the wireless network using other methods as described in Section 6.4.5.3. You can perform basic configuration of the gateway's wireless interface using the installation wizard, as described in Section 2.3. The following sections will familiarize you with iPECS SBG-1000's wireless connection settings.

6.4.5.2 Passing Web Authentication

Prior to wireless authentication and encryption, the Web authentication feature protects your

wireless network from unauthorized wireless clients. When wireless clients attempt to connect to iPECS SBG-1000's WAN, they are prompted to enter a user name and password (see Figure 6.47). Note that all other attempts to use the wireless network prior to the authentication will fail (Telnet, FTP, ping).

Figure 6.47 Web Authentication

As a wireless user, enter your user name and password and click 'OK'. Once authentication has been performed, you may proceed to use iPECS SBG-1000's wireless network from the configured PC, for example to browse the Internet.

Figure 6.48 Web Authentication – Enabled Browsing

Note: Web authentication is available only after you first perform an initial configuration using the 'Quick Setup' screen and have an active WAN connection.

As the gateway's administrator, you can control the access that wireless users will have, via the WBM. In the 'Overview' screen under the 'Home' tab, you can allow or block wireless users in the 'Local Network' section, by clicking the respective links (the same section appears in the 'Overview' screen under the 'Local Network' tab).

Figure 6.49 Home Overview – Local Network

Figure 6.49 depicts a connected wireless user (that can be blocked), and a user that has not been authenticated yet (hence, the yellow question mark appears). This user can be authenticated either by entering correct login details in the Web authentication screen, or by the gateway's administrator from this screen. Click 'Allow' to authenticate the user or 'Block' to reject. The screen will refresh and present the relevant action(s) that can be performed.

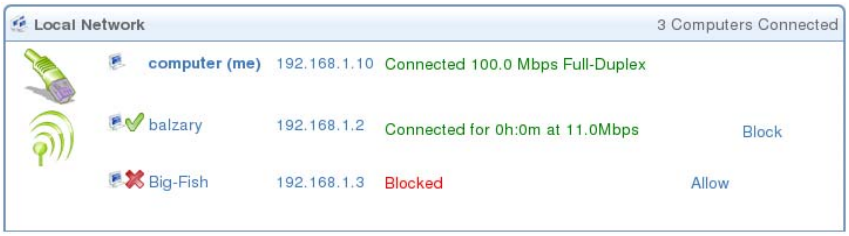


Figure 6.50 Home Overview – Local Network

6.4.5.3 Securing Your Wireless Network

iPECS SBG-1000's wireless network is ready for operation with its default values. The following section describes how to secure your wireless connection using the **Wi-Fi Protected Access** (WPA) security protocol. The Wi-Fi Alliance created the WPA security protocol as a data encryption method for 802.11 wireless local area networks (WLANs). WPA is an industry-supported, pre-standard version of 802.11i utilizing the Temporal Key Integrity Protocol (TKIP), which fixes the problems of Wired Equivalent Privacy (WEP), including the use of dynamic keys.

6.4.5.3.1 Securing with WPA

To secure your wireless network with WPA, perform the following:

1. Click the 'LAN Wireless 802.11n Access Point' link in the 'Network Connections' screen. The 'LAN Wireless 802.11n Access Point Properties' screen appears:

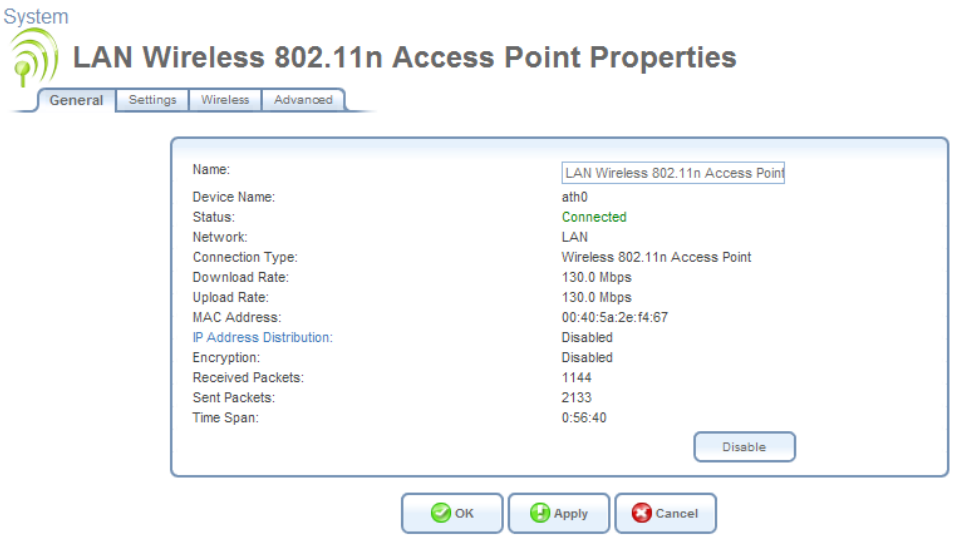


Figure 6.51 LAN Wireless 802.11n Access Point Properties – Enabled

2. Click the 'Wireless' tab.

3. Enable the 'Wireless Security' feature by selecting its 'Enabled' check box. The screen will refresh, displaying the wireless security options (see Figure 6.52).

4. From the 'Stations Security Type' drop-down menu, select "WPA". Note that when selecting

WPA, both WPA and WPA2 are supported.

5. Verify that the selected authentication method is “Pre-Shared Key”.

6. In the ‘Pre-Shared Key’ text field, enter at least 8 characters. Verify that “ASCII” is selected in the associated drop-down menu.

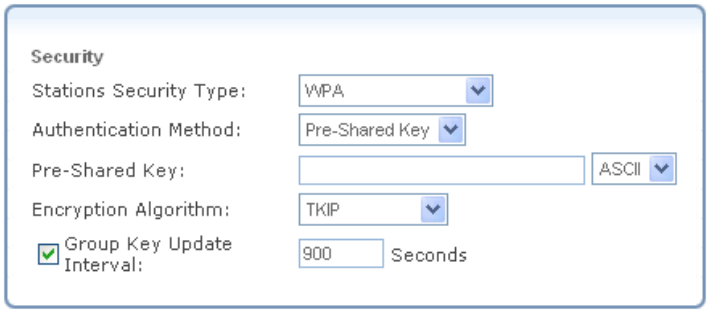


Figure 6.52 WPA Wireless Security Parameters

7. Click ‘OK’. The following ‘Attention’ screen appears.

Figure 6.53 Wireless Client Disconnection Warning

8. Click ‘OK’ to save the settings.

6.4.5.3.2 Connecting a Wireless Windows Client

If your PC has wireless capabilities, Microsoft Windows™ will automatically recognize this and display a wireless connection icon in the system tray (alternatively, this icon is displayed in the Windows ‘Network Connections’ screen, accessed from the Control Panel). Click this icon to search for and connect to your gateway’s wireless network.
Alternatively, you can use the wireless client software supplied with your wireless hardware to connect to your wireless networks.

To manually establish a wireless connection between your PC and the gateway, perform the following:

1. Double-click the wireless connection icon that appears in the system tray. The ‘Wireless Network Connection’ screen appears, displaying iPECS SBG-1000’s wireless connection. Note that the connection is defined as “Security-enabled wireless network (WPA)”.

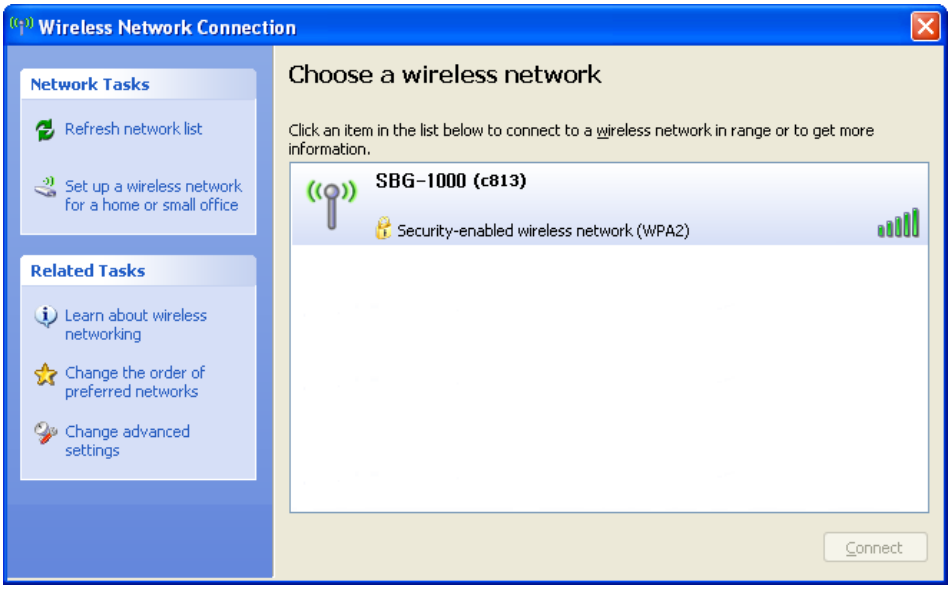


Figure 6.54 Available Wireless Connections

2. Click the connection once to mark it, and then click the ‘Connect’ button at the bottom of the screen. The following login window appears, asking for a ‘Network Key’, which is the pre-shared key you have configured.

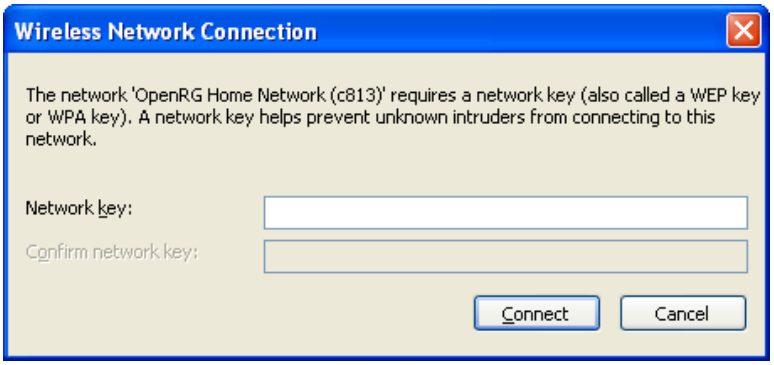


Figure 6.55 Wireless Network Connection Login

3. Enter the pre-shared key in both fields and click the ‘Connect’ button. After the connection is established, its status will change to ‘Connected’.

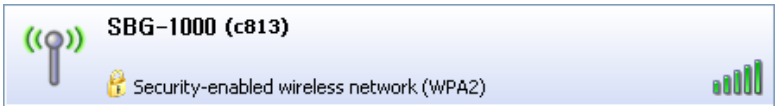


Figure 6.56 Connected Wireless Network

An icon will appear in the notification area, announcing the successful initiation of the wireless connection.

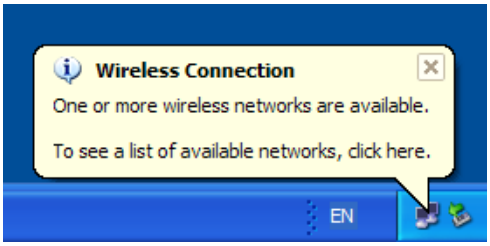


Figure 6.57 Wireless Connection Information

4. Test the connection by disconnecting all other networks and by browsing the Internet.

Should the login window above not appear and the connection attempt fail, configure the wireless connection manually:

1. Click the connection once to mark it, and then click the ‘Change advanced settings’ link in the ‘Related Tasks’ box on the left part of the window (see Figure 6.54). The ‘Wireless Network Connection Properties’ window appears.

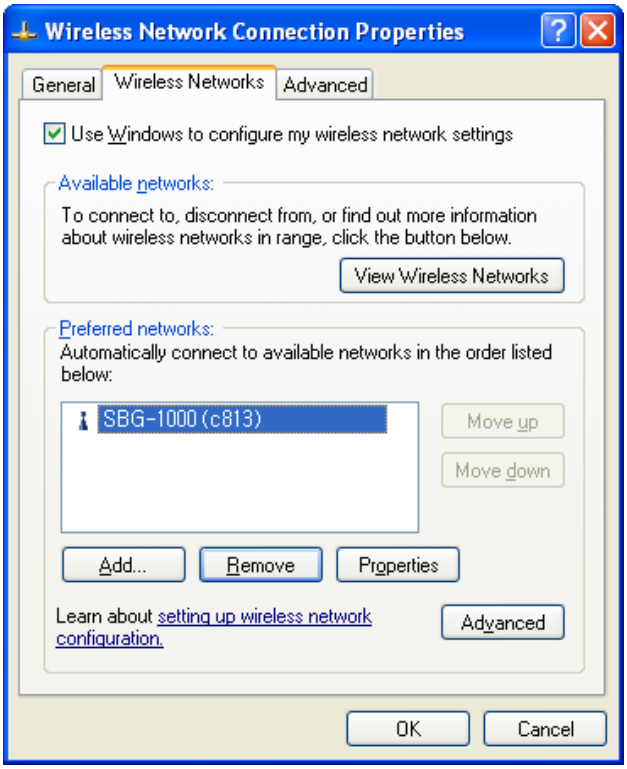


Figure 6.58 Wireless Network Connection Properties

2. Select the ‘Wireless Networks’ tab (see Figure 6.58).

3. Click your connection to highlight it, and click the ‘Properties’ button. Your connection’s properties window appears.

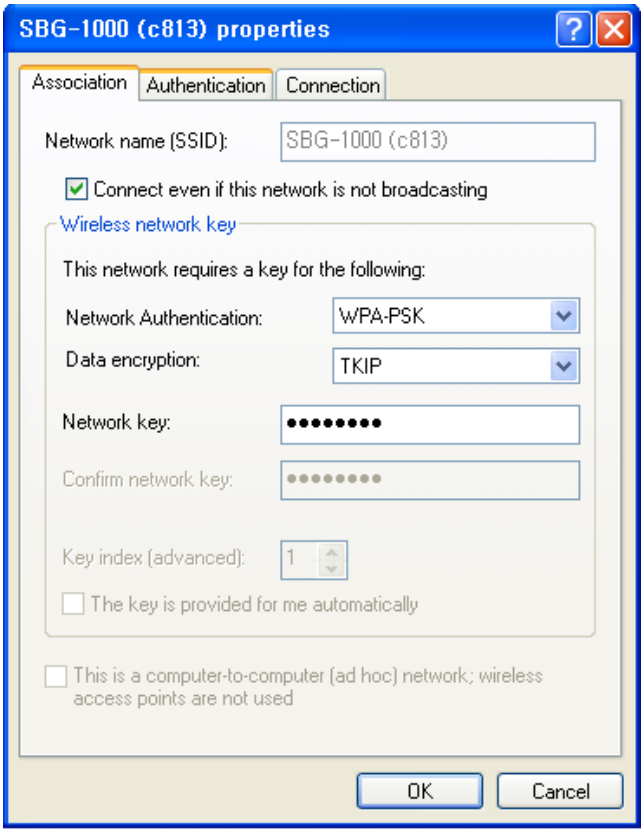


Figure 6.59 Connection Properties Configuration

a. From the ‘Network Authentication’ drop-down menu, select “WPA-PSK”.

b. From the ‘Data Encryption’ drop-down menu, select “TKIP”.

c. Enter your pre-shared key in both the ‘Network key’ and the ‘Confirm network key’ fields.

4. Click ‘OK’ in both windows to save the settings.

5. When attempting to connect to the wireless network, the login window will appear, pre-filled with the pre-shared key. Click the ‘Connect’ button to connect.

Since your network is now secured, only users that know the pre-shared key will be able to connect. The WPA security protocol is similar to securing network access using a password.

6.4.5.4 Configuring General Wireless Parameters

The ‘LAN Wireless 802.11n Access Point Properties’ screen displays a detailed summary of the wireless connection’s parameters, under the ‘General’ sub-tab.

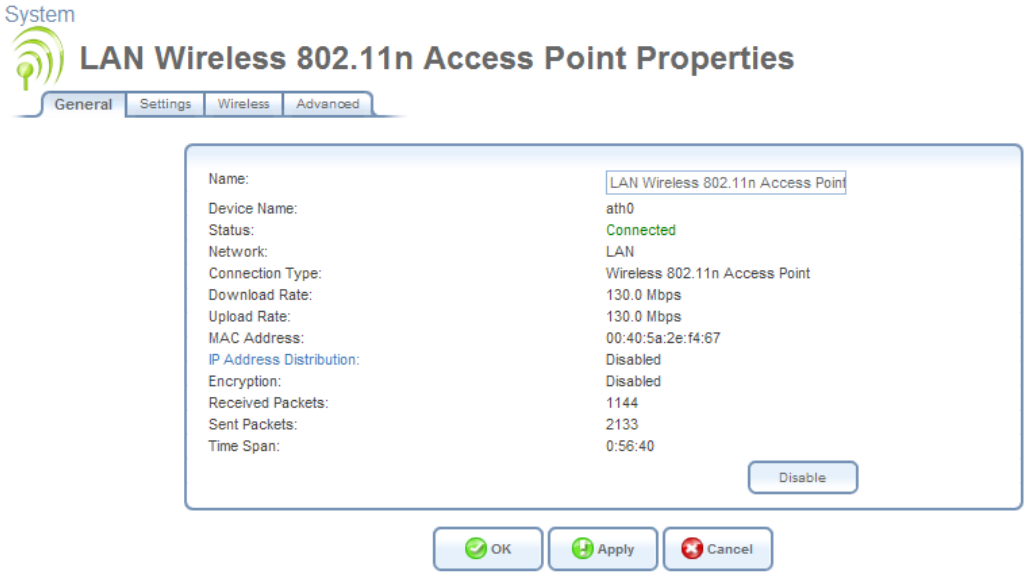


Figure 6.60 LAN Wireless 802.11n Access Point Properties – Enabled

Use the 'Settings' sub-tab to edit these parameters.

General This section displays the connection's general parameters. It is recommended not to change the default values unless you are familiar with the networking concepts they represent. Since your gateway is configured to operate with the default values, no parameter modification is necessary.

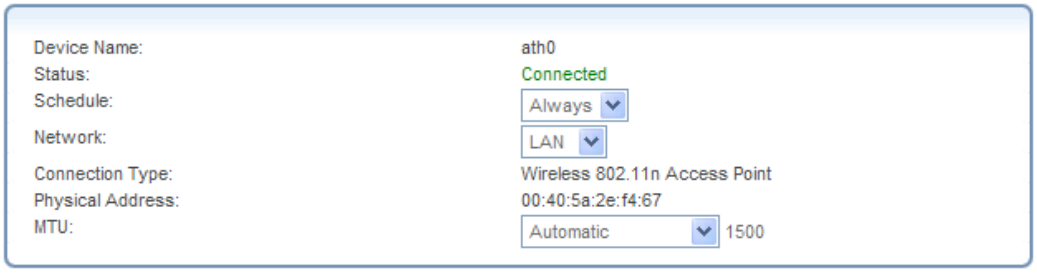


Figure 6.61 General Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.

- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind iPECS SBG-1000.

Physical Address The physical address of the network interface for your network. Some interfaces allow you to change this address.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

6.4.5.5 Defining Advanced Wireless Access Point Settings

The 'Wireless' and 'Advanced' sub-tabs enable you to perform advanced configuration of your wireless access point.

6.4.5.5.1 Wireless Network

Use this section to define the basic wireless access point settings.

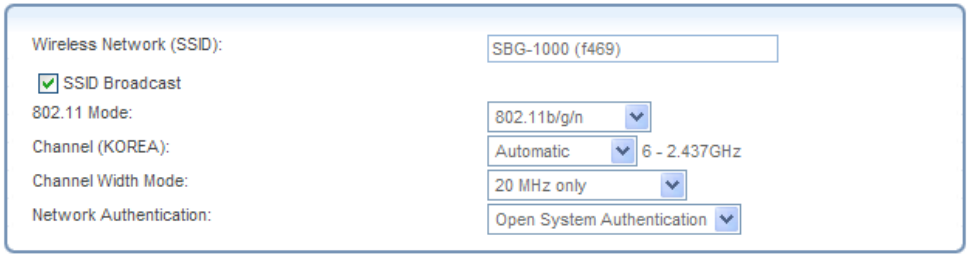


Figure 6.62 Wireless Access Point

SSID Broadcast By default, iPECS SBG-1000 broadcasts the name of its wireless network (SSID). For security reasons, you may choose to hide your wireless network by deselecting this check box. Wireless clients will only be able to connect by manually typing the SSID in their wireless client applications (whether Windows or a third party application), rather than choosing it from the list of available wireless networks.

802.11 Mode The modes available in this drop-down menu are the wireless communication standards supported by your gateway's wireless card. Select the 802.11 mode that is compatible with your network's wireless clients. Only clients of this mode will be able to communicate with the gateway. Note that 802.11b legacy devices are not compatible with modes 802.11g/n and 802.11g Only.

Channel All devices in your wireless network must broadcast on different channels in order to function correctly. It is best to leave this parameter on Automatic. This ensures that iPECS SBG-1000 continuously scans for the most available wireless channel in the vicinity. It is possible to select a channel manually if you have information regarding the wireless channels used in your vicinity. The channels available depend on the regulatory authority (stated in brackets) to which your gateway conforms. For example, the European regulatory authority (ETSI) has allocated 13 available channels, while the US regulatory authority (FCC) has allocated 11 available channels.

Channel Width Mode This option appears on platforms supporting 802.11n only. Select the MHz width of the wireless channel, depending on your selected communication standard. For b and g, select either “20 MHz only” or “20/40 MHz (dynamic)”. For 802.11n any mode may be selected.

Network Authentication The WPA network authentication method is ‘Open System Authentication’, meaning that a network key is not used for authentication. When using the 802.1X WEP or Non-802.1X WEP security protocols, this field changes to a drop-down menu, offering the ‘Shared Key Authentication’ method (which uses a network key for authentication), or both methods combined.

MAC Filtering Mode You can filter wireless users according to their MAC address, either allowing or denying access. Choose the action to be performed by selecting it from the drop-down menu.

6.4.5.5.2 MAC Filtering Table

Use this section to define advanced wireless access point settings. Click ‘New MAC Address’ to define filtering of MAC addresses. The ‘MAC Filtering Settings’ screen appears.

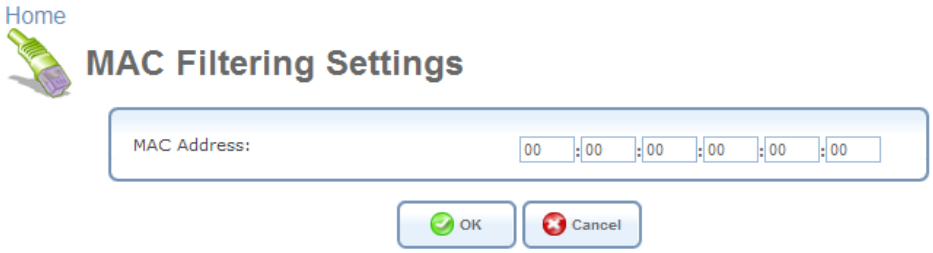


Figure 6.63 MAC Filtering Settings

Enter the MAC address to be filtered and click ‘OK’ button. A MAC address list appears, upon which the selected filtering action (allow/deny) will be performed.

Figure 6.64 MAC Filtering Table

6.4.5.5.3 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is a method for simplifying the security setup and management of wireless networks. This feature is available on iPECS SBG-1000, but is disabled by default. By enabling it, you can control the setup of your wireless security, which is defined in the following ‘Security’ section of the screen (refer to Section 6.4.5.5.4). Note that WPS only supports the WPA security protocol, therefore when enabling this feature, all other types of protocols are disabled (and are no longer available in the ‘Security’ section drop-down menu).
To enable WPS, click the ‘Enabled’ check box. The screen refreshes.

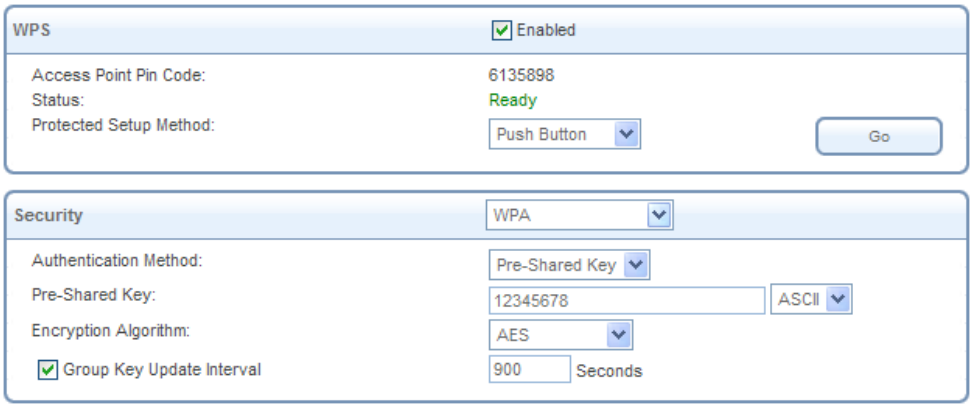


Figure 6.65 Enabled WPS

You can enter/change the value of pre-shared key at anytime by typing a different one in the field, as well as change the type of the value to ASCII using the provided drop-down menu.
Status Indicates the WPS status. “Ready” means that the system is ready to negotiate with incoming wireless clients, or “enrollees”.

Protected Setup Method iPECS SBG-1000 supports two setup methods, “Push Button” (the default) and “Pin Code”. These are the methods used by wireless clients when seeking an access point.

Push Button – The enrollment is initiated by either pressing a physical button on the wireless client or through its software. After initiating the enrollment, click ‘Go’ for the devices to establish a connection.

Pin Code – The enrollment is initiated by the wireless client’s software, which also provides a pin code. To comply with this method, select this option from the drop-down menu. The screen refreshes to provide a field for entering the pin code:

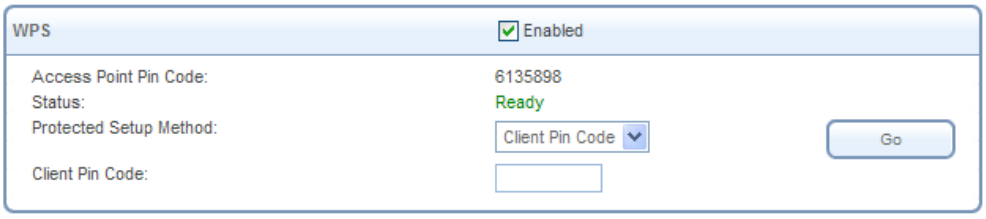


Figure 6.66 Protected Setup Method – Pin Code

In this field, enter the eight digit pin code provided by the wireless client’s software. Click ‘Go’ for the devices to establish a connection.

When attempting to connect a wireless client to iPECS SBG-1000, you must be aware of its setup method. A connection attempt will time out after two minutes if no connection is established. If a connection is established, the ‘Status’ field will change to reflect that.

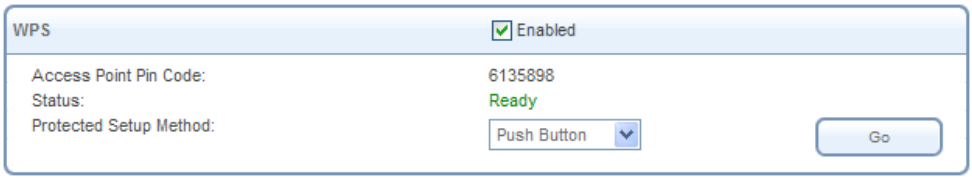


Figure 6.67 Successful Enrollee Registration

6.4.5.5.4 Security

Use this section to configure your wireless security settings. Select the type of security protocol in the 'Stations Security Type' drop-down menu. The screen refreshes, presenting each protocol's configuration respectively.

- **None** Selecting this option disables security on your wireless connection.

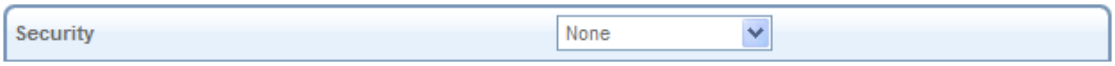


Figure 6.68 Disabled Wireless Security

- **WPA** WPA is a data encryption method for 802.11 wireless LANs (refer to Section 6.4.5.3).

  Authentication Method Select the authentication method you would like to use. You can choose between Pre-Shared Key and 802.1x.

  Pre-Shared Key This entry appears only if you had selected this authentication method. Enter your encryption key in the 'Pre-Shared Key' field. You can use either an ASCII or a Hex value by selecting the value type in the drop-down menu provided.

  Encryption Algorithm Select between Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) for the encryption algorithm.

  Group Key Update Interval Defines the time interval in seconds for updating a group key.

  Inter Client Privacy Select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

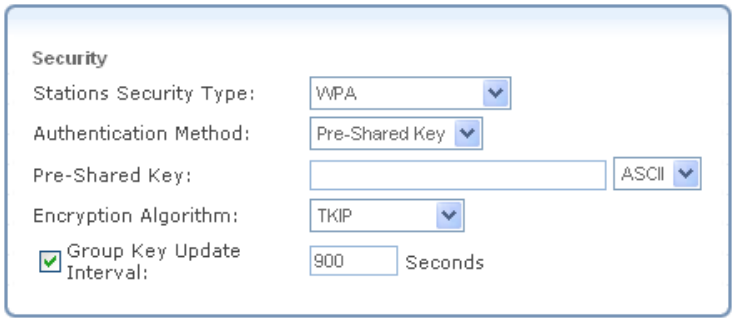


Figure 6.69 WPA Wireless Security Parameters

- **WPA2** WPA2 is an enhanced version of WPA, and defines the 802.11i protocol.

  Authentication Method Select the authentication method you would like to use. You can choose between Pre-Shared Key and 802.1x.

  Pre-Shared Key This entry appears only if you had selected this authentication method. Enter your encryption key in the 'Pre-Shared Key' field. You can use either an ASCII or a Hex value by selecting the value type in the drop-down menu provided.

  Pre Authentication When selecting the 802.1x authentication method, these two entries appear (see Figure 6.70). Select this option to enable iPECS SBG-1000 to accept RADIUS authentication requests from computers connected to other access points. This enables roaming from one wireless network to another.

  PMK Cache Period The number of minutes before deletion (and renewal) of the Pairwise Master Key used for authentication.

Figure 6.70 802.1x Authentication Method

  Encryption Algorithm The encryption algorithm used for WPA2 is the Advanced Encryption Standard (AES).

  Group Key Update Interval Defines the time interval in seconds for updating a group key.

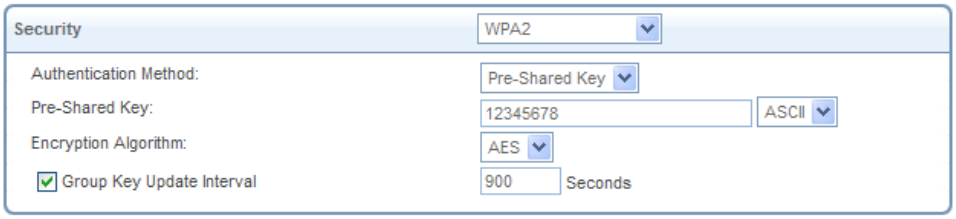


Figure 6.71 WPA2 Wireless Security Parameters

- **WPA and WPA2** Mixed Mode WPA and WPA2 is a mixed data encryption method.

  Authentication Method Select the authentication method you would like to use. You can choose between Pre-Shared Key and 802.1x.

  Pre-Shared Key This entry appears only if you had selected this authentication method. Enter your encryption key in the 'Pre-Shared Key' field. You can use either an ASCII or a Hex value by selecting the value type in the drop-down menu provided.

Pre Authentication When selecting the 802.1x authentication method, these two entries appear (see Figure 6.72). Select this option to enable iPECS SBG-1000 to accept RADIUS authentication requests from computers connected to other access points. This enables roaming from one wireless network to another.

PMK Cache Period The number of minutes before deletion (and renewal) of the Pairwise Master Key used for authentication.

Figure 6.72 802.1x Authentication Method

Encryption Algorithm The encryption algorithm used for WPA and WPA2 is a either the Temporal Key Integrity Protocol (TKIP) or the Advanced Encryption Standard (AES).

Group Key Update Interval Defines the time interval in seconds for updating a group key.

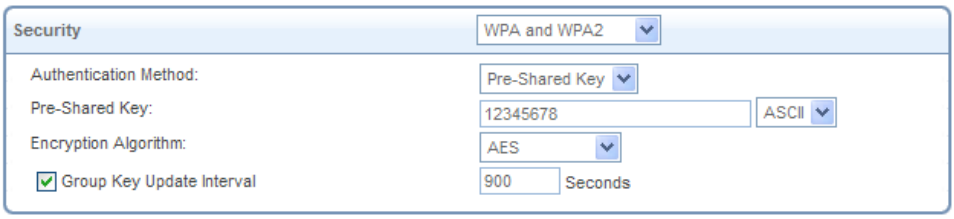


Figure 6.73 WPA and WPA2 Wireless Security Parameters

- **802.1x WEP** 802.1x WEP is a data encryption method utilizing an automatically defined key for wireless clients that use 802.1x for authentication and WEP for encryption.

  Inter Client Privacy Select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

  RADIUS Server Configure the RADIUS Server parameters.
  - **a. Server IP** Enter the RADIUS server's IP address.
  - **b. Server Port** Enter the RADIUS server's port.
  - **c. Shared Secret** Enter your shared secret.

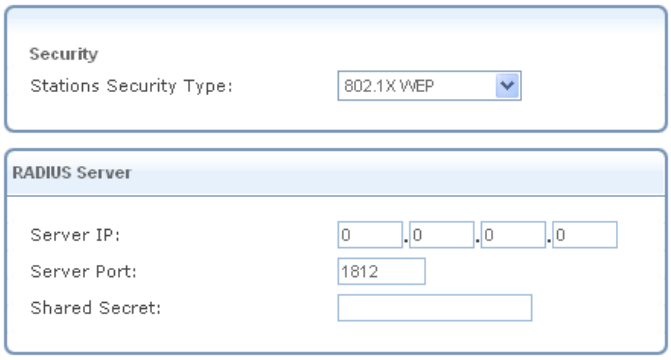


Figure 6.74 802.1x WEP Wireless Security Parameters

- **Non-802.1x WEP** Non-802.1x WEP is a data encryption method utilizing a statically defined key for wireless clients that do not use 802.1x for authentication, but use WEP for encryption. You may define up to four keys but use only one at a time. Note that the static key must be defined in the wireless Windows client as well.

  Inter Client Privacy Select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

  Active Select the encryption key to be activated.

  Encryption Key Type the encryption key until the entire field is filled. The key cannot be shorter than the field's length.

  Entry Method Select the character type for the key: ASCII or HEX.

  Key Length Select the key length in bits: 40 or 104 bits.

Figure 6.75 Non-802.1x WEP Wireless Security Parameters

The encryption key must be defined in the wireless Windows client as well. This is done in the Connection Properties Configuration window (to learn how to reach this window, refer to Section 6.4.5.3.2).

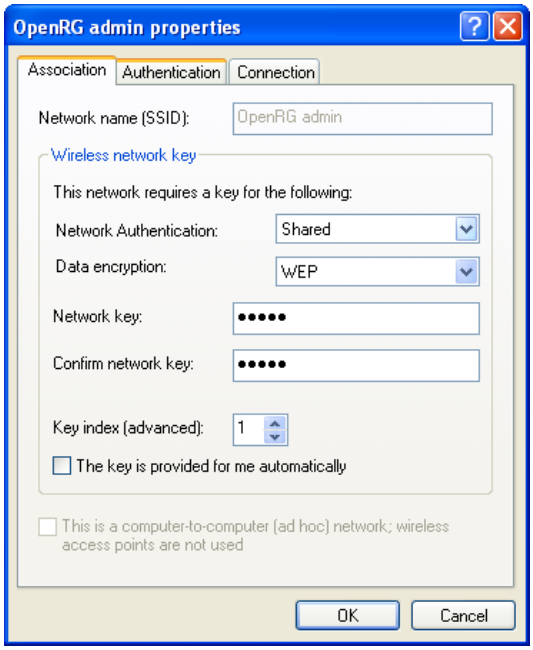


Figure 6.76 Connection Properties Configuration

1. In the 'Network Authentication' drop-down menu, select "Shared".
2. In the 'Data Encryption' drop-down menu, select "WEP".
3. Enter your encryption key in both the 'Network key' and the 'Confirm network key' fields.

- **Web Authentication** When selecting this option, wireless clients attempting to connect to the wireless connection will receive iPECS SBG-1000's main login screen, along with the following attention message:

Figure 6.77 Web Authentication Needed

By logging into the WBM, clients authenticate themselves and are then able to use the connection. iPECS SBG-1000 keeps record of authenticated clients. To clear this list, click the 'Clean Mac List' button. Clients will have to re-authenticate themselves in order to use the wireless connection.

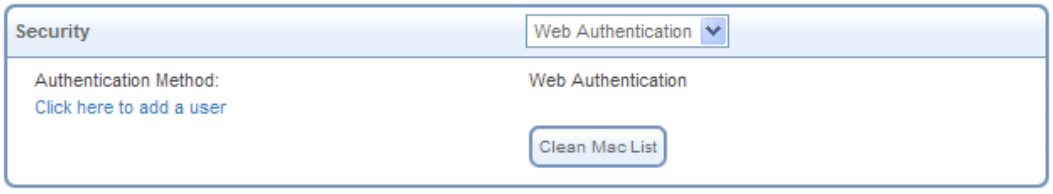


Figure 6.78 Authentication Only Wireless Security Parameters

6.4.5.5.5 Wireless QoS (WMM)

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance certification, based on the IEEE 802.11e draft standard. It provides basic Quality of Service (QoS) features to IEEE 802.11 networks. If your gateway's wireless card supports WMM, you can enable this feature by checking its 'Enabled' check box. The screen refreshes.

Figure 6.79 Wireless QoS (WMM)

Note: When working in 802.11n mode, this feature's check box is not available as WMM is already enabled..

6.4.5.5.6 Transmission Properties

Use this section to define the wireless transmission settings.

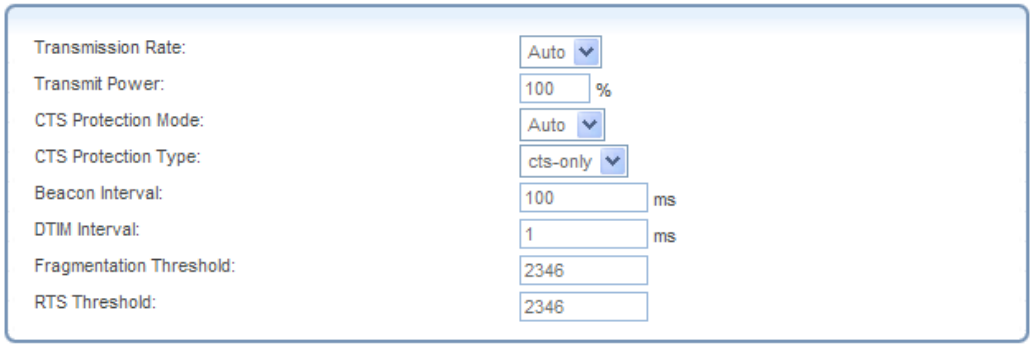


Figure 6.80 Transmission Properties

Transmission Rate The transmission rate is set according to the speed of your wireless connection. Select the transmission rate from the drop-down menu, or select 'Auto' to have iPECS SBG-1000 automatically use the fastest possible data transmission rate (the only option when using 802.11ng). Note that if your wireless connection is weak or unstable, it is best to select a low transmission rate.

Transmit Power The percentage of maximum transmission power.

CTS Protection Mode CTS Protection Mode boosts your gateway's ability to intercept 802.11g and 802.11b transmissions. Conversely, CTS Protection Mode decreases performance. Leave this feature disabled unless you encounter severe communication difficulties between the gateway and 802.11g products. If enabling, select "Always". Select "Auto" to have iPECS SBG-1000 automatically decide whether or not to use this feature.

CTS Protection Type Select the type of CTS protection—cts-only or rts-cts.

Beacon Interval A beacon is a packet broadcast by iPECS SBG-1000 to synchronize the wireless network. The Beacon Interval value indicates how often the beacon is sent.

DTIM Interval The Delivery Traffic Indication Message (DTIM) is a countdown value that informs wireless clients of the next opportunity to receive multicast and broadcast messages. This value ranges between 1 and 16384.

Fragmentation Threshold Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.

RTS Threshold iPECS SBG-1000 sends Request to Send (RTS) packets to the wireless client in order to negotiate the dispatching of data. The wireless client responds with a Clear to Send (CTS) packet, signaling that transmission can commence. In case packets are smaller than the preset threshold, the RTC/CTS mechanism is not active. If you encounter inconsistent data flow, try a minor reduction of the RTS threshold size.

6.4.5.5.7 Virtual Access Points

You can set up multiple virtual wireless LANs on iPECS SBG-1000 up to four connections. Such virtual wireless LANs are referred to as “Virtual APs” (virtual access points).

The ‘Virtual APs’ section appears under the ‘Wireless’ sub-tab of the ‘LAN Wireless 802.11n Access Point Properties’ screen, and displays iPECS SBG-1000’s physical wireless access point, on top of which virtual connections may be created.

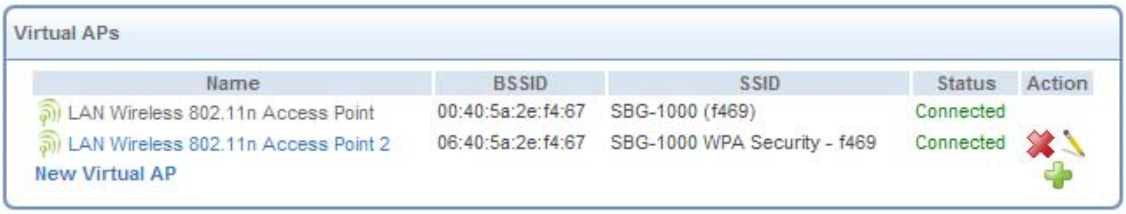


Figure 6.81 Virtual APs

To create a virtual connection, click the ‘New Virtual AP’ link. The screen refreshes, displaying the new virtual connection.

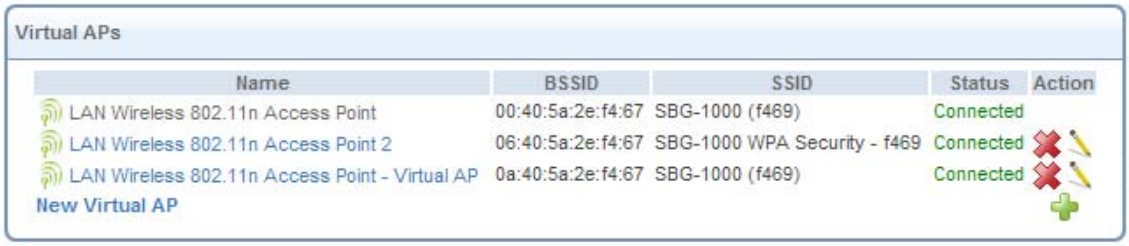


Figure 6.82 New Virtual Access Point

The new connection will also be added to the network connections list, and will be configurable like any other connection.

Figure 6.83 Network Connections

You can edit the new virtual access point's properties by clicking its action icon. The 'LAN Wireless 802.11n Access Point - Virtual AP Properties' screen appears. For example, change the connection's default name by changing the SSID value in the 'Wireless' sub-tab.

Figure 6.84 LAN Wireless 802.11n Access Point – Virtual AP Properties

A usage example for this virtual connection is to dedicate it for guest access. Through this connection, guests will be able to access the WAN, but they will be denied access to other wireless LANs provided by iPECS SBG-1000. To do so, perform the following:

1. Set a firewall rule that blocks access to all other iPECS SBG-1000 LANs.

Figure 6.85 Firewall Rule

To learn how to do so, refer to Section 5.2.8.

2. Back in the virtual connection's 'LAN Wireless 802.11n Access Point - Virtual AP Properties' screen:

   a. In the 'Internet Protocol' section under the 'Settings' sub-tab, enter an IP address for the connection by selecting 'Use the Following IP Address'.

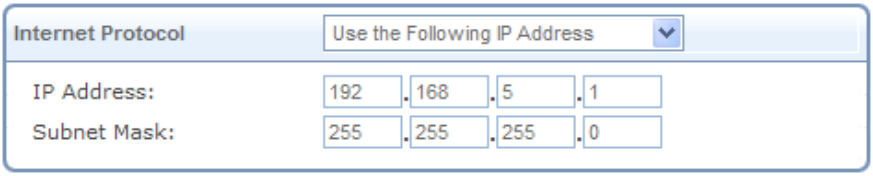


Figure 6.86 Internet Protocol

b. In the 'IP Address Distribution' section, select 'DHCP Server' and enter the IP range from which IP addresses will be granted to wireless guests.

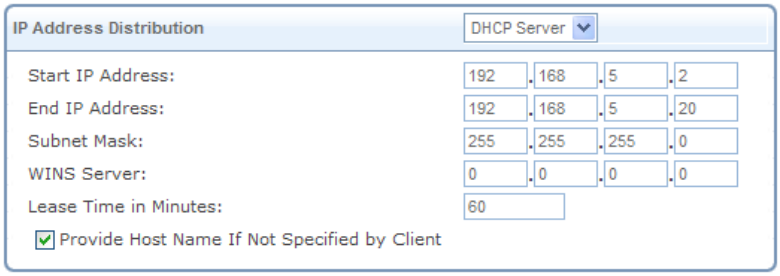


Figure 6.87 IP Address Distribution

c. Click 'OK' to save the settings.

After going through this procedure, you have secured all of your wireless connections. A guest will only be able to connect to the "Guests" wireless LAN, from which only the WAN access will be granted.

6.4.5.5.8 Advanced

Use the 'Advanced' sub-tab to configure the following parameters.

Internet Connection Firewall Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

Figure 6.88 Internet Connection Firewall

Additional IP Addresses You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1 and the http://sbg-1000.home.

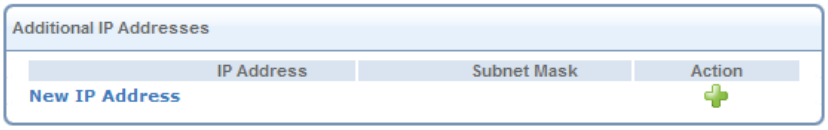


Figure 6.89 Additional IP Addresses

6.4.6 Setting Up a WAN Ethernet Connection

The WAN Ethernet connection enables you to connect iPECS SBG-1000 to another network either directly or via an external modem. The Connection Wizard provides a number of methods for quick establishment of this connection.

6.4.6.1 Using the Ethernet Connection Wizard

The Ethernet Connection wizard utility is the most basic method for establishing a WAN Ethernet connection. This method is intended for connections that do not require username and password in order to connect to the Internet.

To establish a new Ethernet connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.11). The 'Connection Wizard' screen appears (see Figure 6.12).

2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see Figure 6.13).

3. Select the 'External Cable Modem' radio button and click 'Next'. The 'Internet Cable Modem Connection' screen appears.

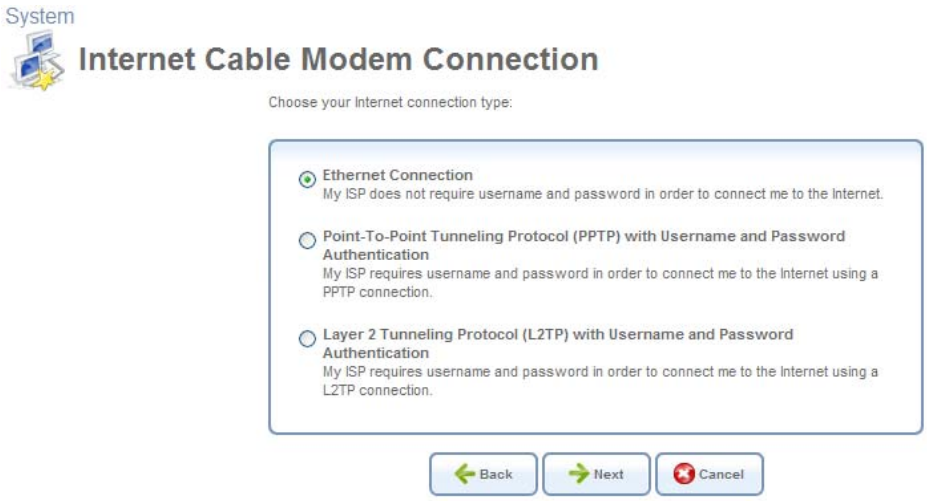


Figure 6.90 Internet Cable Modem Connection

4. Select the 'Ethernet Connection' radio button and click 'Next'. The 'Connection Summary' screen appears.

Figure 6.91 Connection Summary

5. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

6. Click 'Finish' to save the settings.

The WAN Ethernet connection will be configured accordingly. Refer to Section 6.4.6.4 to learn how to view and edit the connection's settings.

6.4.6.2 Using the Dynamic Host Configuration Protocol (DHCP) Wizard

The Dynamic Host Configuration Protocol (DHCP) connection wizard utility is a dynamic negotiation method for establishing a WAN Ethernet connection. When using this method, the client obtains an IP address automatically from the service provider when connecting to the Internet.

To create a new WAN DHCP-based connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.11). The 'Connection Wizard' screen appears (see Figure 6.12).

2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see Figure 6.13).

3. Select the 'Ethernet Connection' radio button and click 'Next'. The 'Ethernet Connection' screen appears.

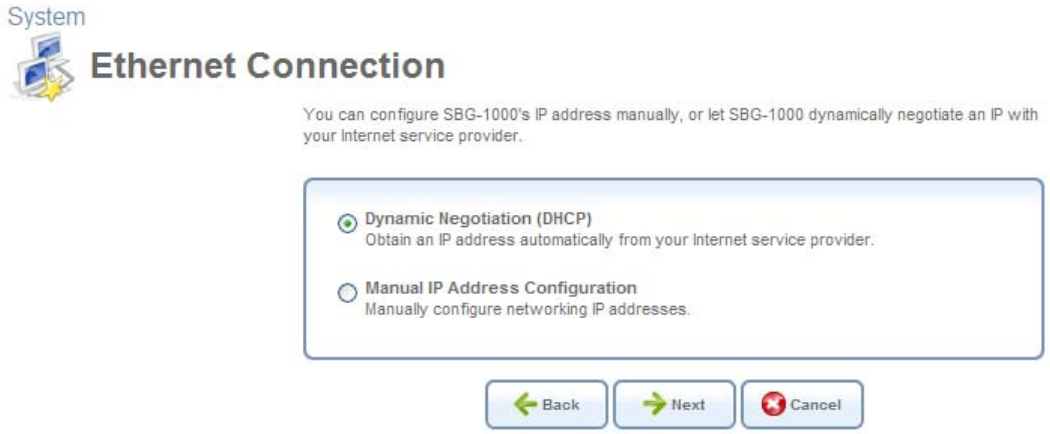


Figure 6.92 Ethernet Connection

4. Select the 'Dynamic Negotiation (DHCP)' radio button and click 'Next'. The 'Connection Summary' screen appears.

Figure 6.93 Connection Summary

5. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

6. Click 'Finish' to save the settings.

The WAN Ethernet connection will be configured to obtain an IP address using a DHCP. Refer to Section 6.4.6.4 to learn how to view and edit the connection's settings.

Note: If your WAN connection is set to DHCP when there is no DHCP server available, and a PPPoE server is available instead, the device status will show: "Waiting for DHCP Lease – PPPoE server found, consider configuring your WAN connection to PPPoE". If you select this option, refer to Section 6.4.7.

6.4.6.3 Using the Manual IP Address Configuration Wizard

The Manual IP Address Configuration wizard utility is used to manually configure the WAN interface's IP addresses when connecting to the Internet.

To manually configure the IP addresses, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.11). The 'Connection Wizard' screen appears (see Figure 6.12).

2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see Figure 6.13).

3. Select the 'Ethernet Connection' radio button and click 'Next'. The 'Ethernet Connection' screen appears.

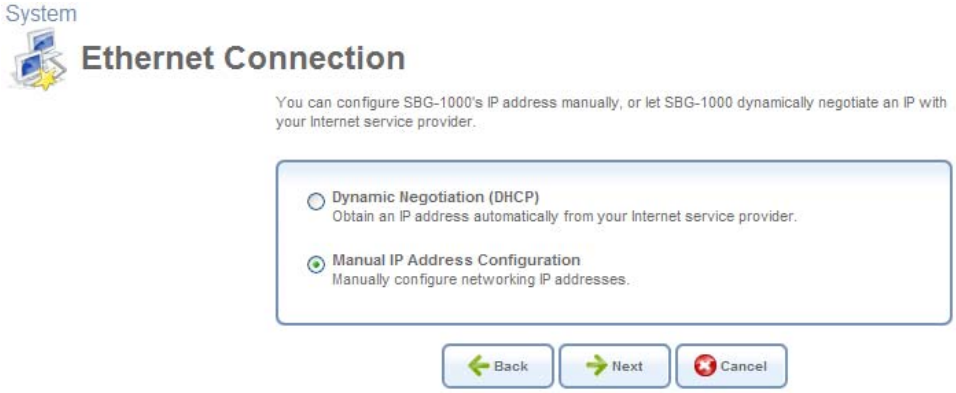


Figure 6.94 Ethernet Connection

4. Select the 'Manual IP Address Configuration' radio button and click 'Next'. The 'Manual IP Address Configuration' screen appears.

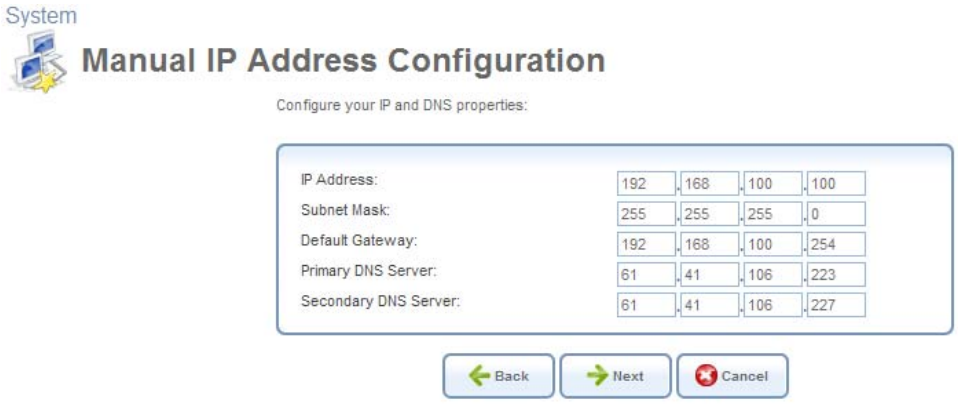


Figure 6.95 Manual IP Address Configuration

5. Enter the IP address, subnet mask, default gateway, and DNS server addresses in their respective fields. These values should either be provided to you by your ISP or configured by your system administrator.

6. Click ‘Next’. The ‘Connection Summary’ screen appears.

Figure 6.96 Connection Summary

7. Select the ‘Edit the Newly Created Connection’ check box if you wish to be routed to the new connection’s configuration screen after clicking ‘Finish’. This screen is described later in this chapter.

8. Click ‘Finish’ to save the settings.

The WAN Ethernet connection will be configured with the new settings. Refer to Section 6.4.6.4 to learn how to view and edit the connection’s settings.

6.4.6.4 Viewing and Editing the Connection’s Settings

To view and edit the WAN Ethernet connection settings, click the ‘WAN Ethernet’ link in the ‘Network Connections’ screen (see Figure 6.11). The ‘WAN Ethernet Properties’ screen appears.

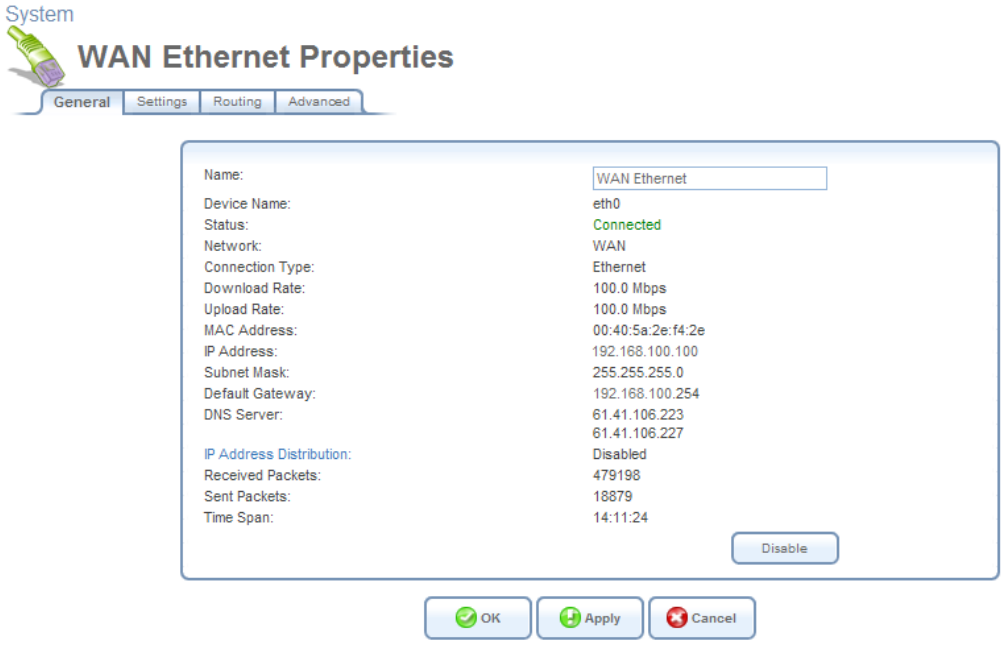


Figure 6.97 WAN Ethernet Properties

6.4.6.4.1 General

This sub-tab enables you to view the WAN Ethernet connection settings (see Figure 6.97). These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.6.4.2 Settings

This sub-tab enables you to configure the following WAN Ethernet settings:

General It is recommended not to change the default values unless you are familiar with the networking concepts they represent. Since your gateway is configured to operate with the default values, no parameter modification is necessary.

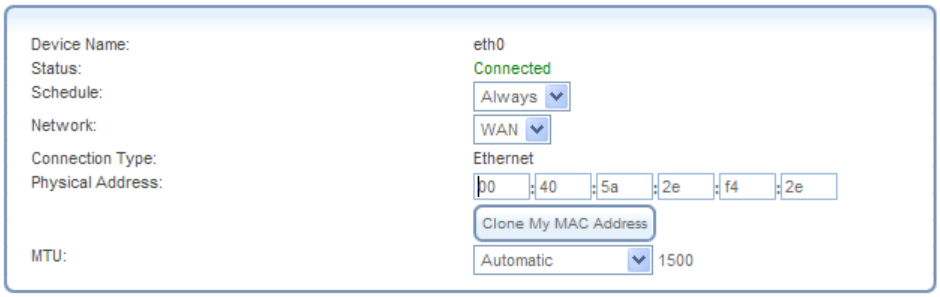


Figure 6.98 General

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind iPECS SBG-1000.

Physical Address The physical address of the network interface for your network. Some interfaces allow you to change this address.

Clone My MAC Address Press this button to copy your PC's current MAC address to the board.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen will refresh to display relevant configuration settings according to your choice.

No IP Address Select 'No IP Address' if you require that your gateway have no IP address. This can be useful if you are working in an environment where you are not connected to other networks, such as the Internet.

Figure 6.99 Internet Protocol – No IP Address

Obtain an IP Address Automatically Your connection is configured by default to act as a DHCP client. You should keep this configuration in case your service provider supports DHCP, or if you are connecting using a dynamic IP address. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead. You can click the 'Release' button to release the current leased IP address. Once the address has been released, the button text changes to 'Renew'. Use the 'Renew' button to renew the leased IP address.

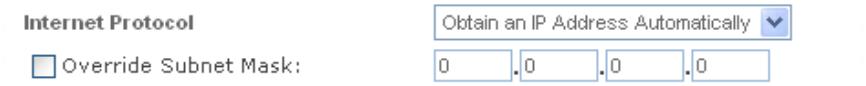


Figure 6.100 Internet Protocol Settings – Automatic IP

Use the Following IP Address Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

Figure 6.101 Internet Protocol – Static IP

DNS Server Domain Name System (DNS) is the method by which Web site domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by

your ISP. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

Figure 6.102 DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

Figure 6.103 DNS Server – Static IP

To learn more about this feature, refer to Section 5.8.1.

IP Address Distribution The 'IP Address Distribution' section allows you to configure the gateway's Dynamic Host Configuration Protocol (DHCP) server parameters. The DHCP automatically assigns IP addresses to network PCs. If you enable this feature, make sure that you also configure your network PCs as DHCP clients. For a comprehensive description of this feature, refer to Section 5.7. Select one of the following options from the 'IP Address Distribution' drop-down menu:

- **DHCP Server**

In case you have chosen DHCP Server, complete the following fields:

Start IP Address The first IP address that may be assigned to a LAN host. Since the LAN interface's default IP address is 192.168.1.1, it is recommended that the first address assigned to a LAN host will be 192.168.1.2 or greater.

End IP Address The last IP address in the range that can be used to automatically assign IP addresses to LAN hosts.

Subnet Mask A mask used to determine to what subnet an IP address belongs. An example of a subnet mask value is 255.255.255.0.

Lease Time In Minutes Each device will be assigned an IP address by the DHCP server for this amount of time, when it connects to the network. When the lease expires the server will determine if the computer has disconnected from the network. If it has, the server may reassign this IP address to a newly-connected computer. This feature ensures that IP addresses that are not in use will become available for other computers on the network.

Provide Host Name If Not Specified by Client If the DHCP client does not have a host name, the gateway will automatically assign one for it.

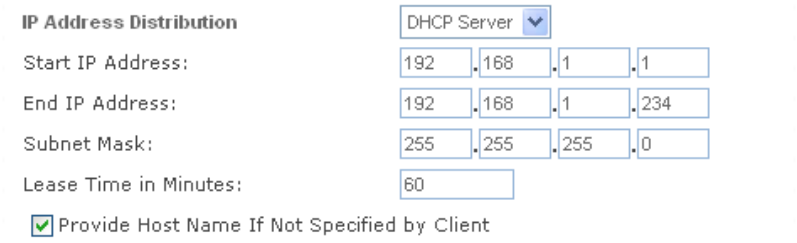


Figure 6.104 IP Address Distribution – DHCP Server

- **Disabled** Select 'Disabled' from the drop-down menu if you would like to statically assign IP addresses to your network computers.

Figure 6.105 IP Address Distribution – Disable DHCP

6.4.6.4.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

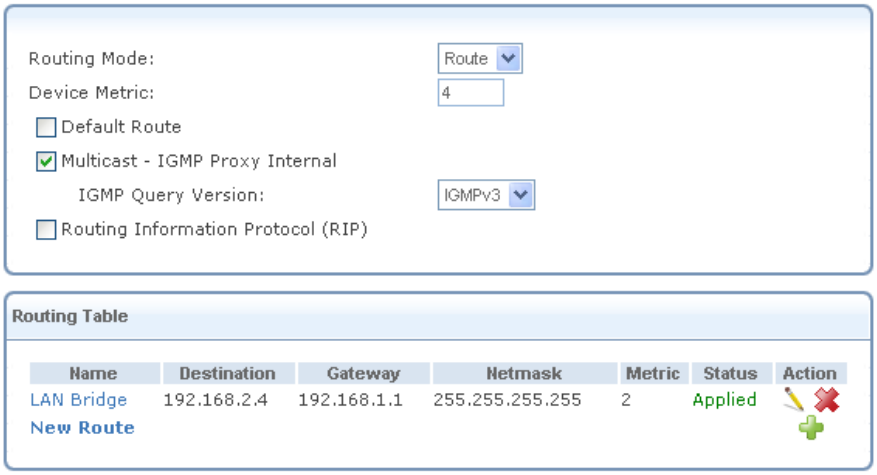


Figure 6.106 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

Route Use route mode if you want your gateway to function as a router between two networks.

NAPT Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default iPECS SBG-1000 serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version iPECS SBG-1000 supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages—**select either ‘None’, ‘RIPv1’, ‘RIPv2’ or ‘RIPv1/2’.
- **Send RIP messages—**select either ‘None’, ‘RIPv1’, ‘RIPv2-broadcast’ or ‘RIPv2-multicast’.

Routing Table Allows you to add or modify routes when this device is active. Use the ‘New Route’ button to add a route or edit existing routes.
To learn more about routing, refer to Section 6.6.

6.4.6.4.4 Advanced

This sub-tab enables you to configure the advanced WAN Ethernet settings.

Internet Connection Firewall Your gateway’s firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the ‘Enabled’ check box. To learn more about your gateway’s security features, refer to Section 5.2.

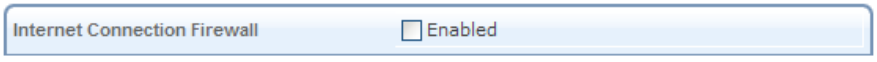


Figure 6.107 Internet Connection Firewall

Additional IP Addresses You can add alias names (additional IP addresses) to the gateway by clicking the ‘New IP Address’ link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1 and the http://sbg-1000.home.

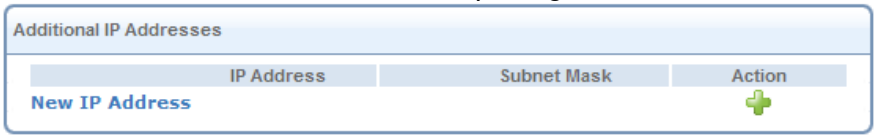


Figure 6.108 Additional IP Addresses

6.4.7 Setting Up a PPPoE Connection

Point-to-Point Protocol over Ethernet (PPPoE) relies on two widely accepted standards, PPP and Ethernet. PPPoE enables your home network PCs that communicate on an Ethernet network to exchange information with PCs on the Internet. PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point connection to be established in the multipoint architecture of Ethernet. A discovery process in PPPoE determines the Ethernet MAC address of the remote device in order to establish a session.

6.4.7.1 Creating a PPPoE Connection

To create a PPPoE connection, perform the following:

1. Click the ‘New Connection’ link in the ‘Network Connections’ screen (see Figure 6.11). The ‘Connection Wizard’ screen appears (see Figure 6.12).

2. Select the ‘Advanced Connection’ radio button and click ‘Next’. The ‘Advanced Connection’ screen appears (see Figure 6.13).

3. Select the ‘Point-to-Point Protocol over Ethernet’ radio button and click ‘Next’. The ‘Point-to-Point Protocol over Ethernet’ screen appears.

Figure 6.109 Point-to-Point Protocol over Ethernet

4. Enter the username and password provided by your Internet Service Provider (ISP), and click ‘Next’. The ‘Connection Summary’ screen appears.

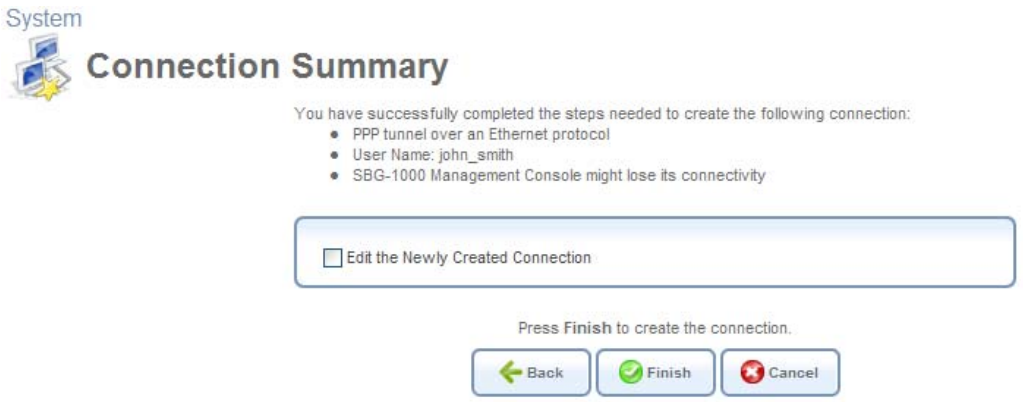


Figure 6.110 Connection Summary

5. Select the ‘Edit the Newly Created Connection’ check box if you wish to be routed to the new connection’s configuration screen after clicking ‘Finish’. This screen is described later in this chapter.

6. Click ‘Finish’ to save the settings.

The new PPPoE connection will be added to the network connections list, and will be configurable like any other connection.

Note: If your WAN connection is set to PPPoE when there is no PPPoE server available, and a DHCP server is available instead, the device status will show: “In Progress – DHCP server found, consider configuring your WAN connection to Automatic”

6.4.7.2 Viewing and Editing the Connection’s Settings

To view and edit the PPPoE connection settings, click the ‘WAN PPPoE’ link in the ‘Network Connections’ screen (see Figure 6.11). The ‘WAN PPPoE Properties’ screen appears.

Figure 6.111 WAN PPPoE Properties

6.4.7.2.1 General

This sub-tab enables you to view the PPPoE connection settings (see Figure 6.111). These settings can be edited in the rest of the screen’s sub-tabs, as described in the following sections.

6.4.7.2.2 Settings

This sub-tab enables you to edit the following PPPoE connection settings:

General This section displays the connection’s general parameters.

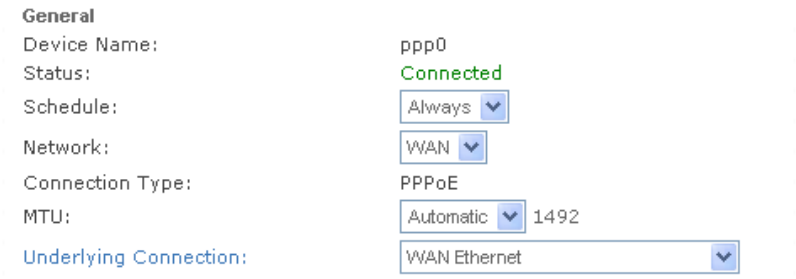


Figure 6.112 General PPPoE Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind iPECS SBG-1000.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Underlying Connection Specify the underlying connection above which the protocol will be initiated.

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' combo-box:

- Unnumbered
- Obtain an IP Address Automatically
- Use the Following IP Address

Please note that the screen will refresh to display relevant configuration settings according to your choice.

Unnumbered Select this option to assign a predefined LAN address as iPECS SBG-1000's WAN address. This is useful when iPECS SBG-1000 operates in routing mode. Before selecting this option, configure the 'Internet Protocol' of your LAN device (or bridge, in case the LAN device is under a bridge) to use a permanent (static) IP address from the range of IP addresses

provided by your ISP (instead of 192.168.1.1).

Figure 6.113 Internet Protocol – Unnumbered

Obtain an IP Address Automatically Your connection is configured by default to obtain an IP automatically. You should change this configuration in case your service provider requires it. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead.

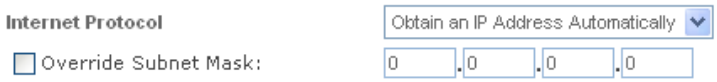


Figure 6.114 Internet Protocol – Automatic IP

Use the Following IP Address Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

Figure 6.115 Internet Protocol – Static IP

DNS Server Domain Name System (DNS) is the method by which Web site domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

Figure 6.116 DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

Figure 6.117 DNS Server – Static IP

To learn more about this feature, refer to Section 5.8.1.

6.4.7.2.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

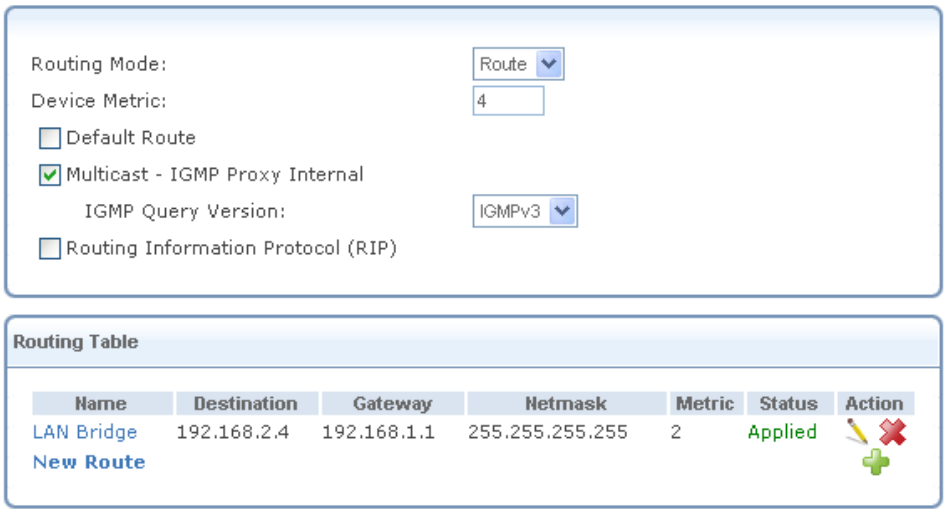


Figure 6.118 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

Route Use route mode if you want your gateway to function as a router between two networks.

NAPT Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default iPECS SBG-1000 serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version iPECS SBG-1000 supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages**—select either 'None', 'RIPv1', 'RIPv2' or 'RIPv1/2'.
- **Send RIP messages**—select either 'None', 'RIPv1', 'RIPv2-broadcast' or 'RIPv2-multicast'.

Routing Table Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.
To learn more about routing, refer to Section 6.6.

6.4.7.2.4 Advanced

This sub-tab enables you to edit the advanced PPPoE connection settings.

Internet Connection Firewall Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

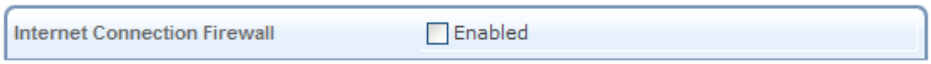


Figure 6.119 Internet Connection Firewall

6.4.8 Setting Up an L2TP Connection

Layer 2 Tunneling Protocol (L2TP) is an extension to the PPP protocol, enabling your gateway to create VPN connections. Derived from Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer 2 Forwarding (L2F) technology, L2TP encapsulates PPP frames into IP packets either at the remote user's PC or at an ISP that has an L2TP Remote Access Concentrator (LAC). The LAC transmits the L2TP packets over the network to the L2TP Network Server (LNS) at the corporate side. With iPECS SBG-1000, L2TP is targeted at serving two purposes:

1. Connecting iPECS SBG-1000 to the Internet when it is used as a cable modem, or when using an external cable modem. Such a connection is established by authenticating your username and password.

2. Connecting iPECS SBG-1000 to a remote network using a Virtual Private Network (VPN) tunnel over the Internet. This enables secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates, and user name and password for authentication.

6.4.8.1 Creating an L2TP Connection

To create a new L2TP connection, perform the following:

1. Click the ‘New Connection’ link in the ‘Network Connections’ screen (see Figure 6.11). The ‘Connection Wizard’ screen appears (see Figure 6.12).

2. Select the ‘Internet Connection’ radio button and click ‘Next’. The ‘Internet Connection’ screen appears (see Figure 6.13).

3. Select the ‘External Cable Modem’ radio button (this option is for both internal and external cable modems) and click ‘Next’. The ‘Internet Cable Modem Connection’ screen appears.

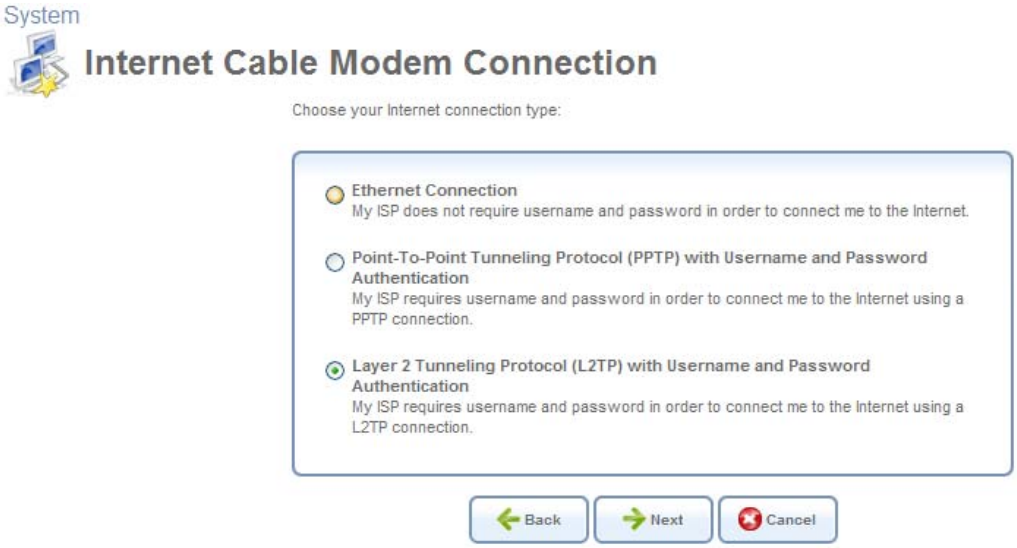


Figure 6.120 Internet Cable Modem Connection

4. Select the ‘Layer 2 Tunneling Protocol (L2TP) with the ‘User Name and Password Authentication’ radio button and click ‘Next’. The ‘Layer 2 Tunneling Protocol (L2TP)’ screen appears.

Figure 6.121 Layer 2 Tunneling Protocol (L2TP)

5. Enter the username and password provided by your Internet Service Provider (ISP).

6. Enter the L2TP server host name or IP address provided by your ISP.

7. Select whether to obtain an IP address automatically or specify one. This option is described in detail in Internet Protocol.

8. Click ‘Next’. The ‘Connection Summary’ screen appears.

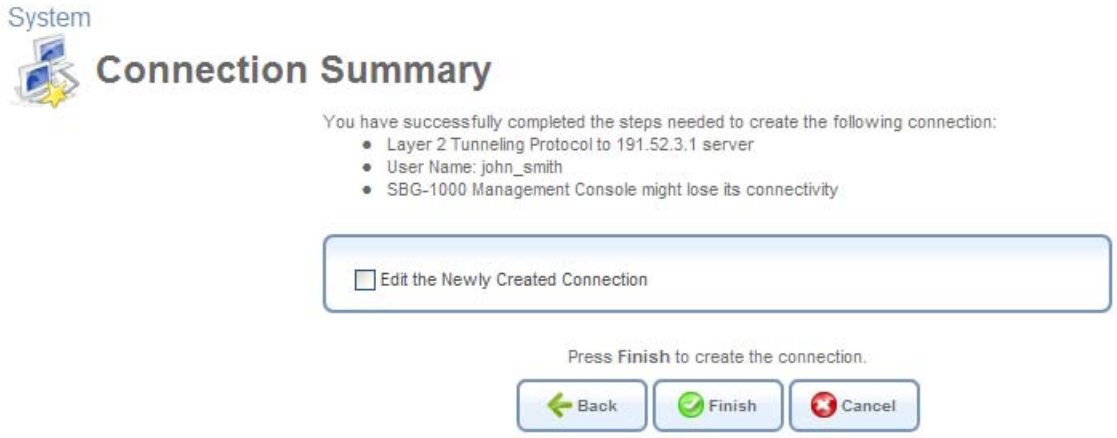


Figure 6.122 Connection Summary

9. Select the ‘Edit the Newly Created Connection’ check box if you wish to be routed to the new connection’s configuration screen after clicking ‘Finish’. This screen is described later in this chapter.

10. Click ‘Finish’ to save the settings.

The new L2TP connection will be added to the network connections list, and will be configurable like any other connection.

6.4.8.2 Creating an L2TP IPSec VPN Connection

To create an L2TP IPSec VPN connection, perform the following:

1. Click the ‘New Connection’ link in the ‘Network Connections’ screen (see Figure 6.11). The ‘Connection Wizard’ screen appears (see Figure 6.12).

2. Select the ‘Connect to a Virtual Private Network over the Internet’ radio button and click ‘Next’. The ‘Connect to a Virtual Private Network over the Internet’ screen appears (see figure ‘Connect to a Virtual Private Network over the Internet’).

3. Select the ‘VPN Client or Point-To-Point’ radio button and click ‘Next’. The ‘VPN Client or Point-To-Point’ screen appears.

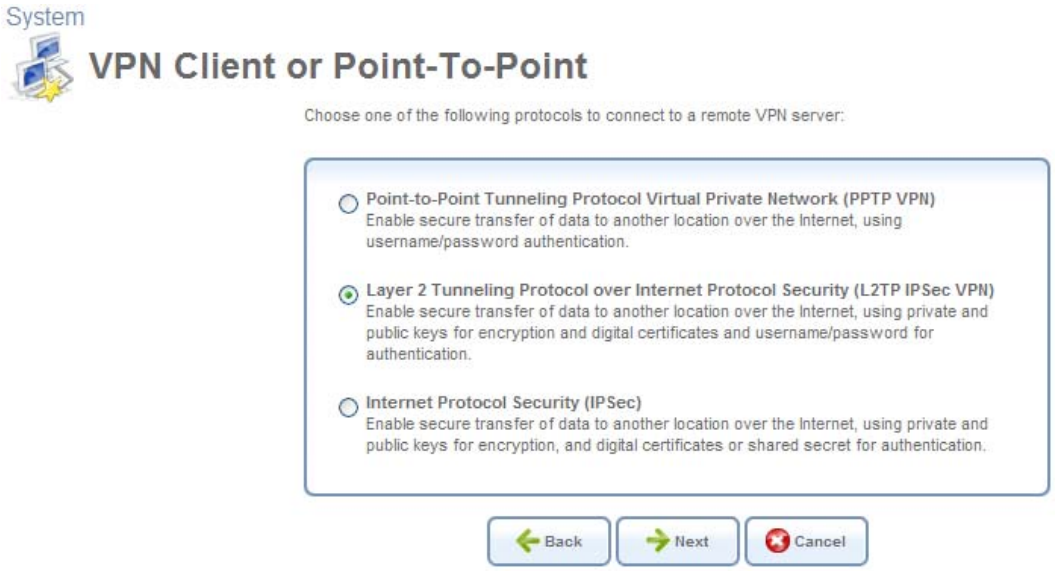


Figure 6.123 VPN Client or Point-To-Point

4. Select the 'Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)' radio button and click 'Next'. The 'Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)' screen appears.

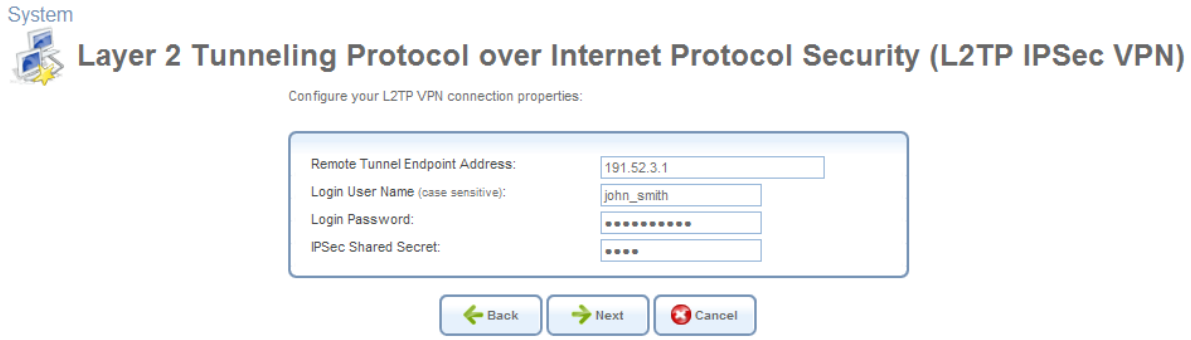


Figure 6.124 L2TP IPSec VPN

5. Enter the username and password provided by the administrator of the network you are trying to access.

6. Enter the IPSec shared secret, which is the encryption key jointly decided upon with the network you are trying to access.

7. Enter the remote tunnel endpoint address. This would be the IP address or domain name of the remote network computer, which serves as the tunnel's endpoint.

8. Click 'Next'. The 'Connection Summary' screen appears.

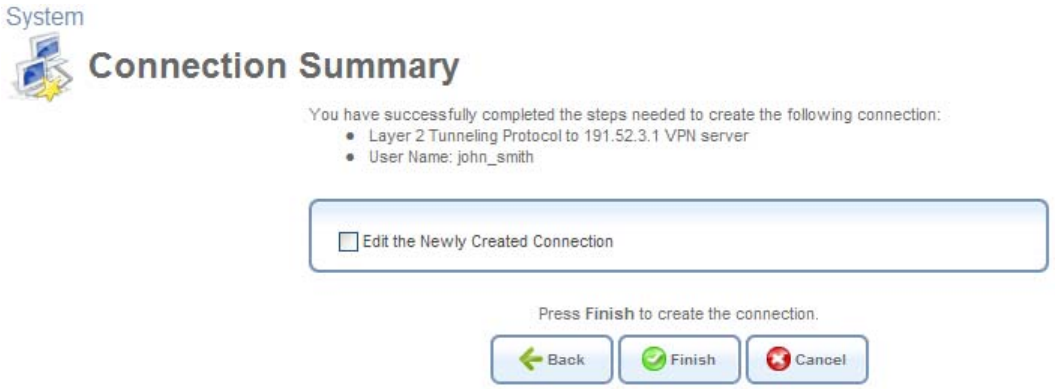


Figure 6.125 Connection Summary

9. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

10. Click 'Finish' to save the settings.

The new L2TP IPSec VPN connection will be added to the network connections list, and will be configurable like any other connection.

6.4.8.3 Viewing and Editing the Connection's Settings

To view and edit the L2TP connection settings, click the 'L2TP' link in the 'Network Connections' screen (see Figure 6.11). The 'L2TP Properties' screen appears.

Figure 6.126 L2TP Properties

6.4.8.3.1 General

This sub-tab enables you to view a detailed summary of the connection's settings. These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.8.3.2 Settings

This sub-tab enables you to edit the following L2TP connection settings:

General This section displays the connection's general parameters.

Figure 6.127 General L2TP Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind iPECS SBG-1000.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen refreshes to display relevant configuration settings according to your choice.

Obtain an IP Address Automatically Your connection is configured by default to obtain an IP

automatically. You should change this configuration in case your service provider requires it. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead.

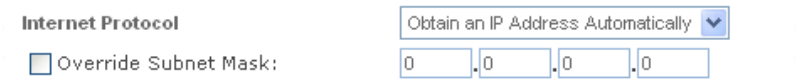


Figure 6.128 Internet Protocol – Automatic IP

Use the Following IP Address Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

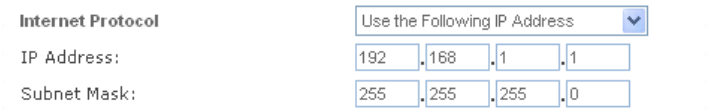


Figure 6.129 Internet Protocol – Static IP

DNS Server Domain Name System (DNS) is the method by which Web site domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

Figure 6.130 DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

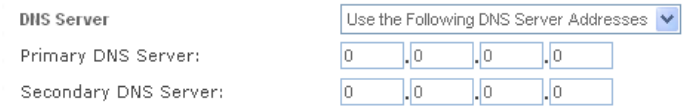


Figure 6.131 DNS Server – Static IP

To learn more about this feature, refer to Section 5.8.1.

6.4.8.3.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

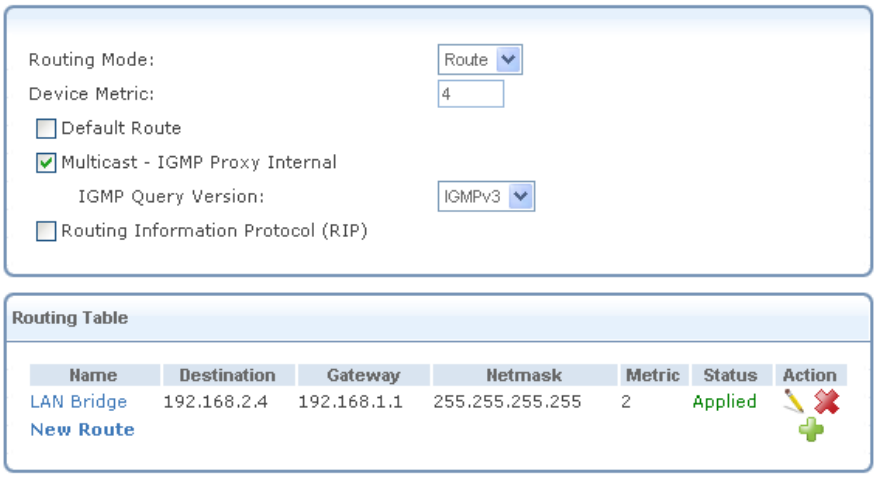


Figure 6.132 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

Route Use route mode if you want your gateway to function as a router between two networks.

NAPT Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default iPECS SBG-1000 serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version iPECS SBG-1000 supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages**—select either ‘None’, ‘RIPv1’, ‘RIPv2’ or ‘RIPv1/2’.
- **Send RIP messages**—select either ‘None’, ‘RIPv1’, ‘RIPv2-broadcast’ or ‘RIPv2-multicast’.

Routing Table Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.
To learn more about routing, refer to Section 6.6.

6.4.8.3.4 L2TP

This sub-tab enables you to edit the following L2TP settings.

L2TP Define your ISP's server parameters.

- **L2TP Server Host Name or IP Address** Enter the connection's host name or IP address obtained from your ISP.
- **Shared Secret** Enter the shared secret value obtained from your ISP.

Figure 6.133 L2TP Configuration

6.4.8.3.5 Advanced

This sub-tab enables you to edit the advanced L2TP settings.

Internet Connection Firewall Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

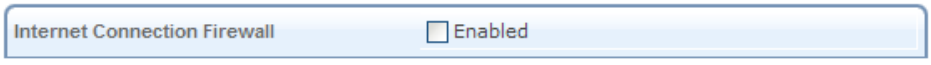


Figure 6.134 Internet Connection Firewall

6.4.9 Setting Up an L2TP Server

iPECS SBG-1000 can act as a Layer 2 Tunneling Protocol Server (L2TP Server), accepting L2TP client connection requests.

To set up a new L2TP Server, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.11). The 'Connection Wizard' screen appears (see Figure 6.12).

2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').

3. Select the 'VPN Server' radio button and click 'Next'. The 'VPN Server' screen appears.

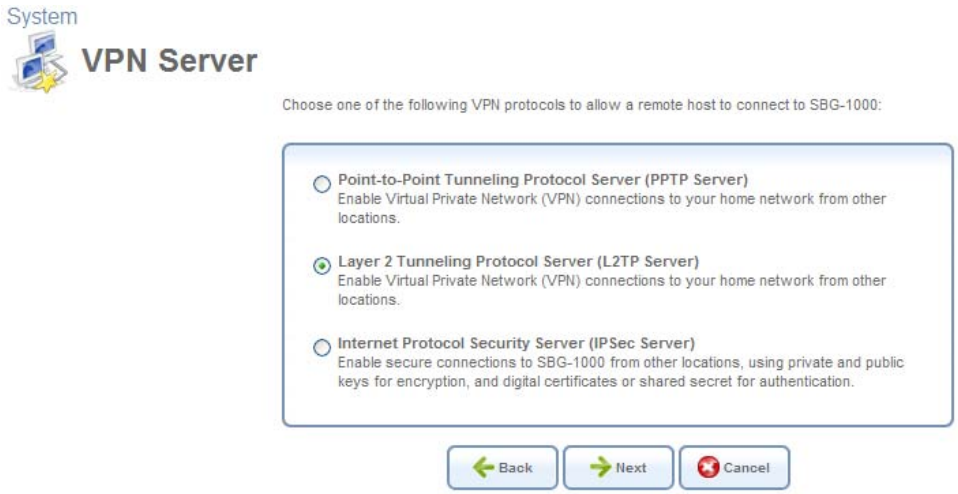


Figure 6.135 VPN Server

4. Select the 'Layer 2 Tunneling Protocol Server (L2TP Server)' radio button and click 'Next'. The 'Layer 2 Tunneling Protocol (L2TP)' screen appears.

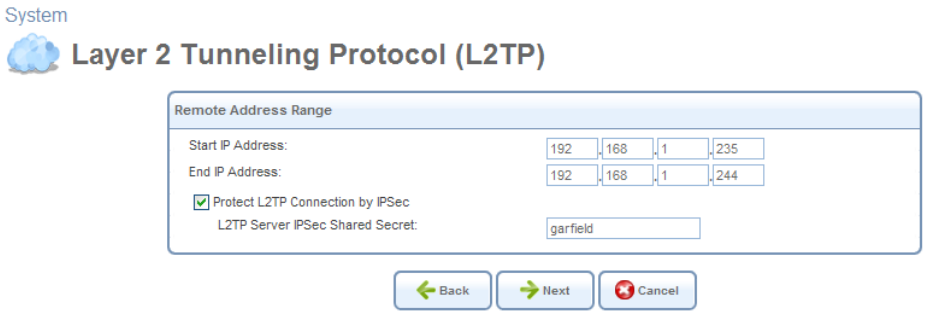


Figure 6.136 Layer 2 Tunneling Protocol (L2TP)

5. In this screen, perform the following:

   a. Specify the address range that iPECS SBG-1000 will reserve for remote users. You

may use the default values as depicted in Figure 6.136.

b. By default, the L2TP connection is protected by the IP Security (IPSec) protocol (the option is selected). However, if you wish to keep this setting, you must provide a string that will serve as the 'L2TP Server IPSec Shared Secret'. Alternatively, deselect this option to disable L2TP protection by IPSec.

6. Click 'Next'. The 'Connection Summary' screen appears (see Figure 6.137). Note the attention message alerting that there are no users with VPN permissions.

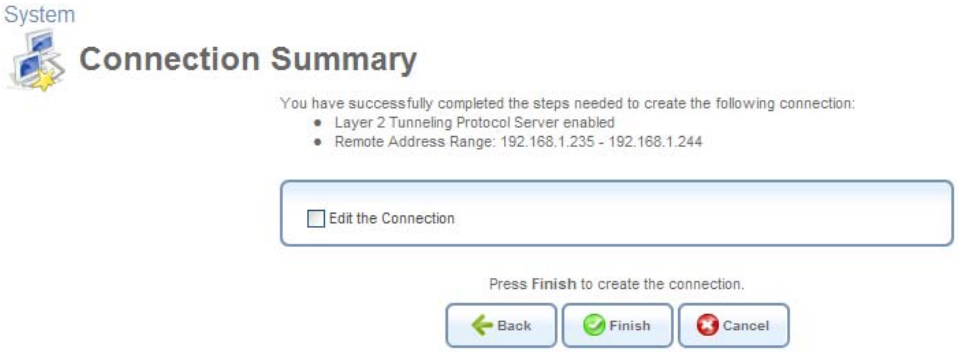


Figure 6.137 Connection Summary

7. Check the 'Edit the Connection' check box and click 'Finish'. The 'Layer 2 Tunneling Protocol Server (L2TP Server)' screen appears.

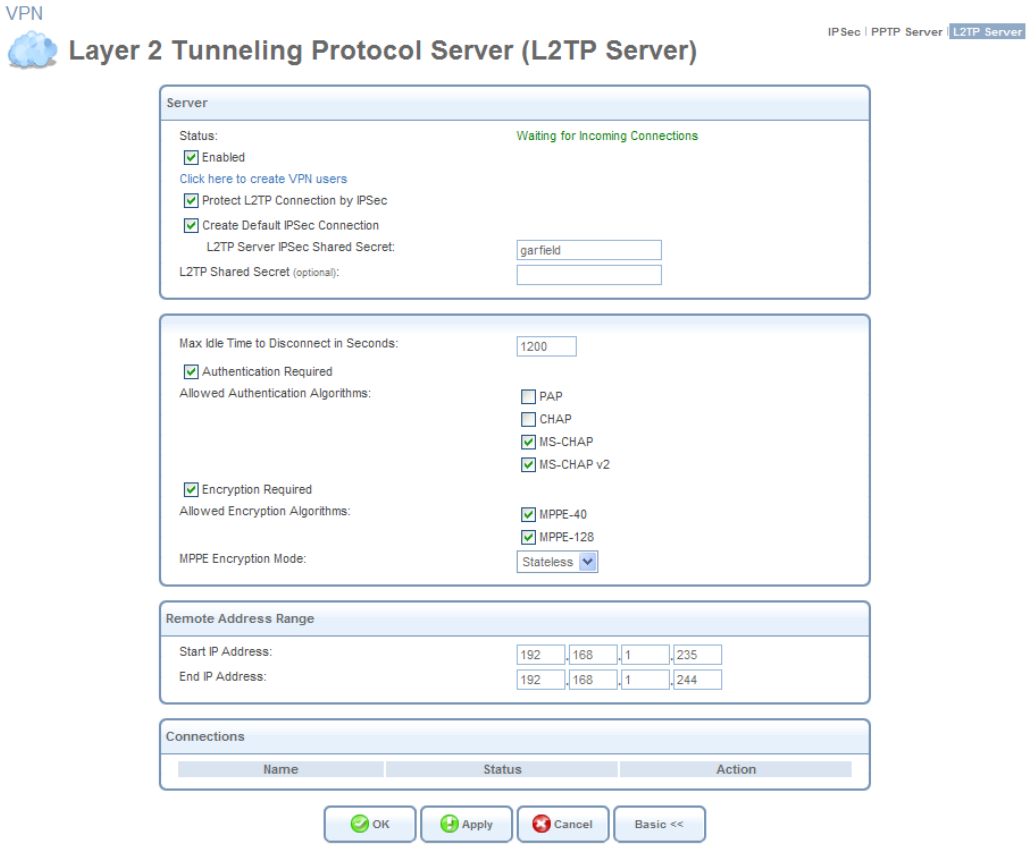


Figure 6.138 Advanced L2TP Server Parameters

8. Click the ‘Click Here to Create VPN Users’ link to define remote users that will be granted access to your home network. Refer to Section 6.3 to learn how to define and configure users.

9. Click ‘OK’ to save the settings.

The new L2TP Server will be added to the network connections list, and will be configurable like any connection. Unlike other connections, it is also accessible via the iPECS SBG-1000’s ‘Shortcut’ screen. Note that the connection wizard automatically creates a default IPSec connection in order to protect the L2TP connection. To learn more, refer to Section 5.4.3.
To learn how to configure your L2TP and IPSec clients in order to connect to the L2TP server, refer to Section 5.4.3.3.

6.4.10 Setting Up a PPTP Connection

Point-to-Point Tunneling Protocol (PPTP) is a protocol developed by Microsoft targeted at creating VPN connections over the Internet. This enables remote users to access the gateway via any ISP that supports PPTP on its servers. PPTP encapsulates network traffic, encrypts content using Microsoft’s Point-to-Point Encryption (MPPE) protocol that is based on RC4, and routes using the generic routing encapsulation (GRE) protocol. With iPECS SBG-1000, PPTP is targeted at serving the following purposes:

1. Connecting iPECS SBG-1000 to the Internet when it is used as a cable modem, or when using an external cable modem. Such a connection is established by authenticating your user name and password.

2. Connecting iPECS SBG-1000 to a remote network using a Virtual Private Network (VPN) tunnel over the Internet. This enables secure transfer of data to another location over the Internet, by authenticating your username and password.

6.4.10.1 Creating a PPTP Connection

To create a new PPTP connection, perform the following:

1. Click the ‘New Connection’ link in the ‘Network Connections’ screen (see Figure 6.11). The ‘Connection Wizard’ screen appears (see Figure 6.12).

2. Select the ‘Internet Connection’ radio button and click ‘Next’. The ‘Internet Connection’ screen appears (see Figure 6.13).

3. Select the ‘External Cable Modem’ radio button (this option is for both internal and external cable modems) and click ‘Next’. The ‘Internet Cable Modem Connection’ screen appears.

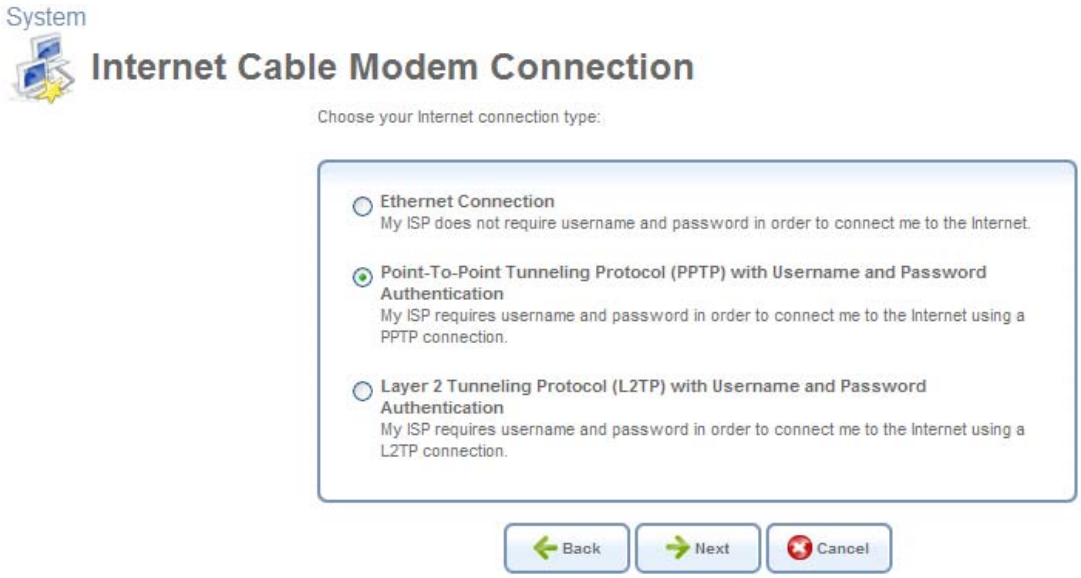


Figure 6.139 Internet Cable Modem Connection

4. Select the 'Point-To-Point Tunneling Protocol (PPTP) with User Name and Password Authentication' radio button and click Next. The 'Point-to-Point Tunneling Protocol (PPTP)' screen appears.

Figure 6.140 Point-to-Point Tunneling Protocol

5. Enter the username and password provided by your Internet Service Provider (ISP).

6. Enter the PPTP server's host name or IP address provided by your ISP.

7. Select whether to obtain an IP address automatically or specify one. This option is described in Section 6.4.10.3.2.

8. Click 'Next'. The 'Connection Summary' screen appears.

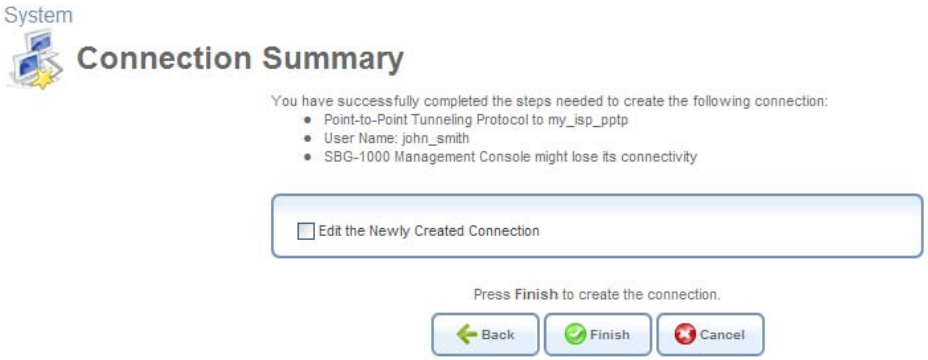


Figure 6.141 Connection Summary

9. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

10. Click 'Finish' to save the settings.

The new PPTP connection is added to the network connections list, and is configurable like any other connection.

6.4.10.2 Creating a PPTP VPN Connection

To create a new PPTP VPN connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.11). The 'Connection Wizard' screen appears (see Figure 6.12).

2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').

3. Select the 'VPN Client or Point-To-Point' radio button, and click 'Next'. The 'VPN Client or Point-To-Point' screen appears.

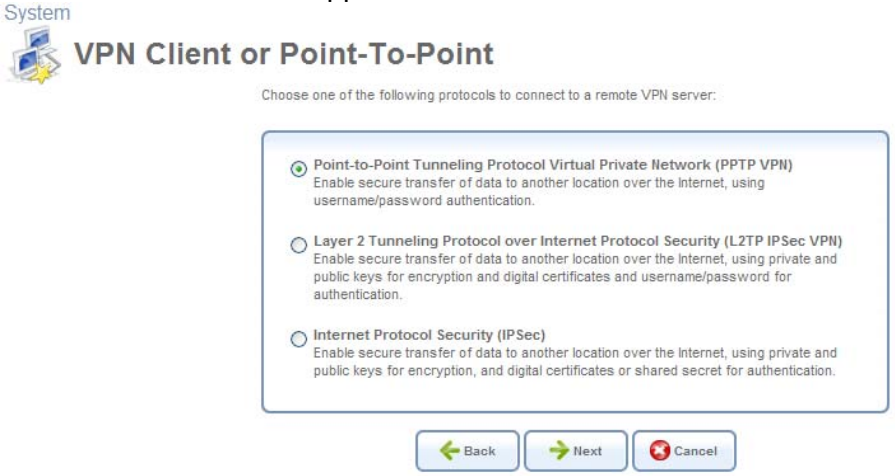


Figure 6.142 VPN Client or Point-To-Point

4. Select the ‘Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)’ radio button and click ‘Next’. The ‘Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)’ screen appears.

Figure 6.143 PPTP VPN

5. Enter the username and password provided by the administrator of the network you are trying to access.

6. Enter the remote tunnel endpoint address. This would be the IP address or domain name of the remote network computer, which serves as the tunnel’s endpoint.

7. Click ‘Next’. The ‘Connection Summary’ screen appears.

Figure 6.144 Connection Summary

8. Select the ‘Edit the Newly Created Connection’ check box if you wish to be routed to the new connection’s configuration screen after clicking ‘Finish’. This screen is described later in this chapter.

9. Click ‘Finish’ to save the settings.

The new PPTP VPN connection is added to the network connections list, and is configurable like any other connection.

6.4.10.3 Viewing and Editing the Connection's Settings

To view and edit the PPTP connection settings, click the 'PPTP' link in the 'Network Connections' screen (see Figure 6.11). The 'PPTP Properties' screen appears.

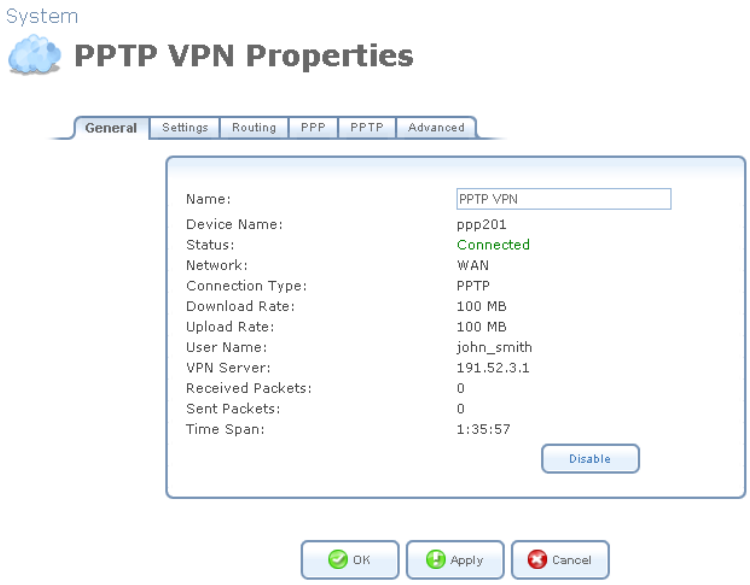


Figure 6.145 PPTP Properties

6.4.10.3.1 General

This sub-tab enables you to view a detailed summary of the connection's settings. These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.10.3.2 Settings

This sub-tab enables you to edit the following PPTP connection settings:

General This section displays the connection's general parameters.

Figure 6.146 General PPTP Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information,

refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- •Remove the connection from under a bridge, if that is the case.
- •Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- •Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind iPECS SBG-1000.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen refreshes to display relevant configuration settings according to your choice.

Obtain an IP Address Automatically Your connection is configured by default to obtain an IP automatically. You should change this configuration in case your service provider requires it. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead.

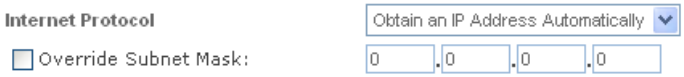


Figure 6.147 Internet Protocol – Automatic IP

Use the Following IP Address Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

Figure 6.148 Internet Protocol – Static IP

DNS Server Domain Name System (DNS) is the method by which Web site domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

Figure 6.149 DNS Server – Automatic IP

To manually configure DNS server addresses, select ‘Use the Following DNS Server Addresses’ from the ‘DNS Server’ drop down menu (see figure ‘DNS Server -- Static IP’). Specify up to two different DNS server address, one primary, another secondary.

Figure 6.150 DNS Server – Static IP

To learn more about this feature, refer to Section 5.8.1.

6.4.10.3.3 Routing

This sub-tab enables you to configure the connection’s routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

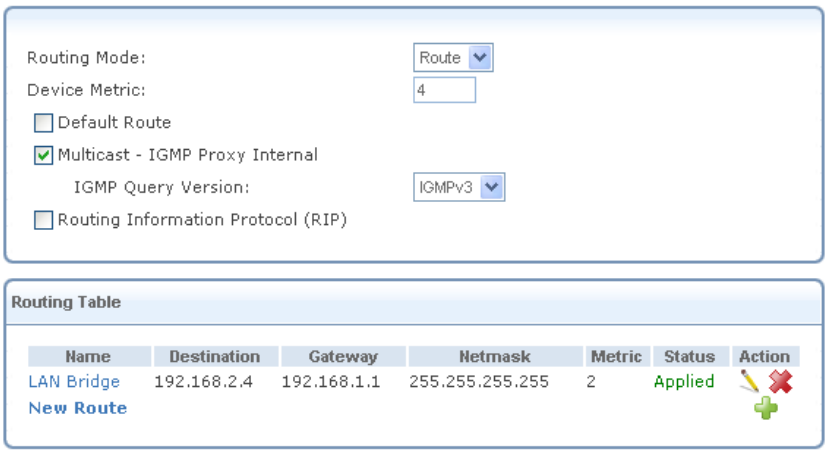


Figure 6.151 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

Route Use route mode if you want your gateway to function as a router between two networks.

NAPT Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default iPECS SBG-1000 serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections

by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version iPECS SBG-1000 supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages**—select either 'None', 'RIPv1', 'RIPv2' or 'RIPv1/2'.
- **Send RIP messages**—select either 'None', 'RIPv1', 'RIPv2-broadcast' or 'RIPv2-multicast'.

Routing Table Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.
To learn more about routing, refer to Section 6.6.

6.4.10.3.4 PPTP

This sub-tab enables you to edit the following PPTP settings.

PPTP Define your ISP's server parameters.
PPTP Server Host Name or IP Address Enter the connection's host name or IP address obtained from your ISP.

Figure 6.152 PPTP Configuration

6.4.10.3.6 Advanced

This sub-tab enables you to edit the advanced PPTP settings.

Internet Connection Firewall Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

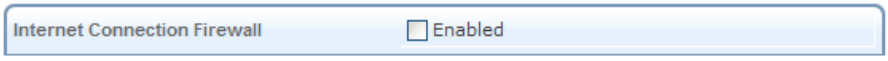


Figure 6.153 Internet Connection Firewall

6.4.11 Setting Up a PPTP Server

iPECS SBG-1000 can act as a Point-to-Point Tunneling Protocol (PPTP) Server, accepting PPTP client connection requests.

To set up a PPTP Server, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.11). The 'Connection Wizard' screen appears (see Figure 6.12).
2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').

3. Select the 'VPN Server' radio button and click 'Next'. The 'VPN Server' screen appears.

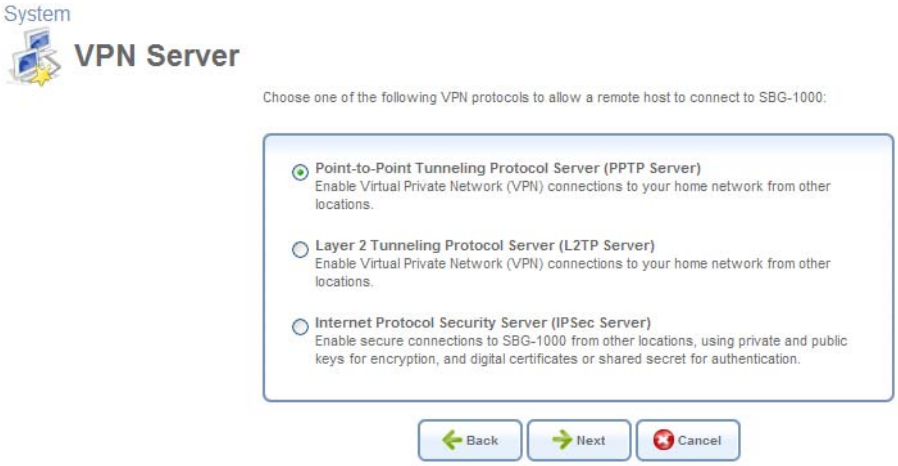


Figure 6.154 VPN Server

4. Select the 'Point-to-Point Tunneling Protocol Server (PPTP Server)' radio button and click 'Next'. The 'Point-to-Point Tunneling Protocol (PPTP)' screen appears.

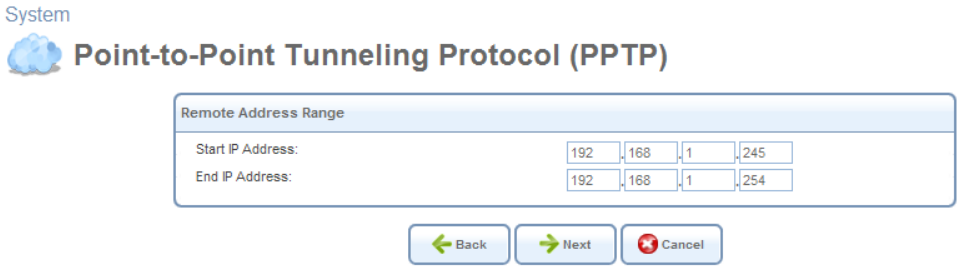


Figure 6.155 Point-to-Point Tunneling Protocol (PPTP)

5. Specify the address range that iPECS SBG-1000 will reserve for remote users. You may use the default values as depicted in Figure 6.155.

6. Click 'Next'. The 'Connection Summary' screen appears (see Figure 6.156). Note the attention message alerting that there are no users with VPN permissions.

Figure 6.156 Connection Summary

7. Check the 'Edit the Newly Created Connection' check box and click 'Finish'. The 'Point-to-Point Tunneling Protocol Server (PPTP Server)' screen appears.

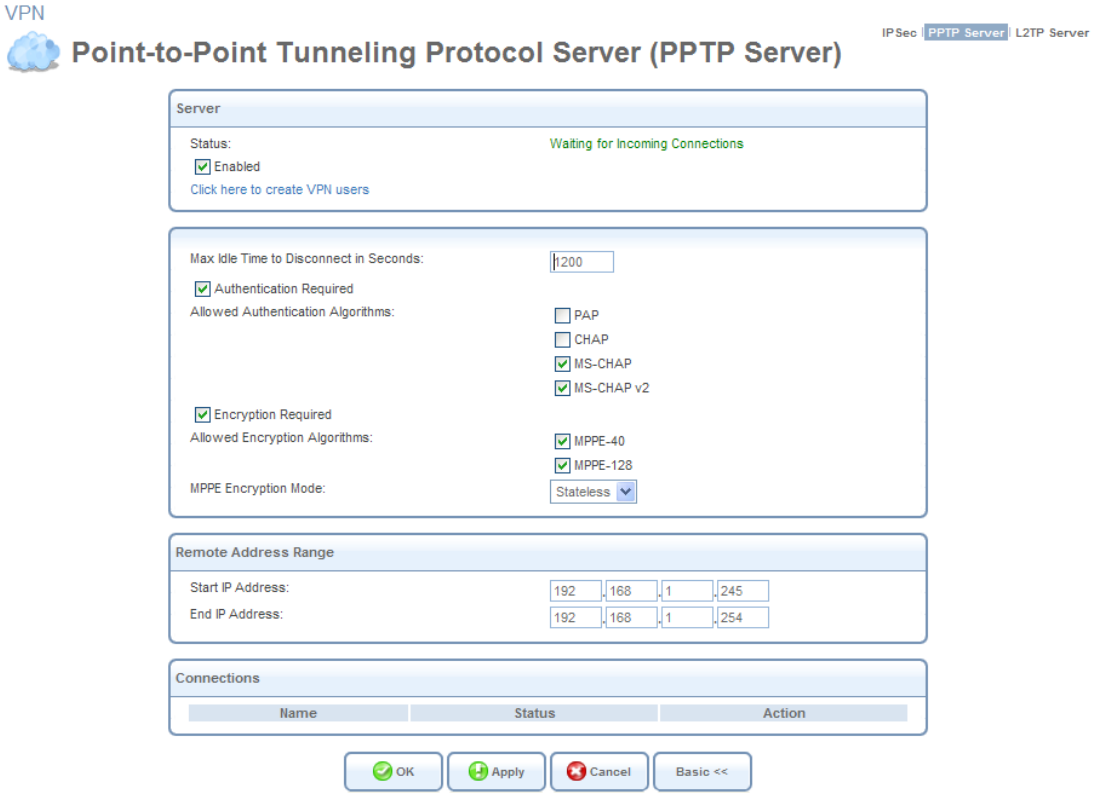


Figure 6.157 Advanced PPTP Server Parameters

8. Click the 'Click Here to Create VPN Users' link to define remote users that will be granted access to your home network. Refer to Section 6.3 to learn how to define and configure users.
9. Click 'OK' to save the settings.

The new PPTP Server will be added to the network connections list, and will be configurable like any connection. Unlike other connections, it is also accessible via the iPECS SBG-1000's 'Shortcut' screen. To learn more about the configuration of a PPTP server, refer to Section 5.4.2.

6.4.12 Setting Up an IPSec Connection

Internet Protocol Security (IPSec) is a series of guidelines for the protection of Internet Protocol (IP) communications. It specifies procedures for securing private information transmitted over public networks.

To set up an IPSec connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.11). The 'Connection Wizard' screen appears (see Figure 6.12).

2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').

3. Select the 'VPN Client or Point-To-Point' radio button and click 'Next'. The 'VPN Client or Point-To-Point' screen appears.

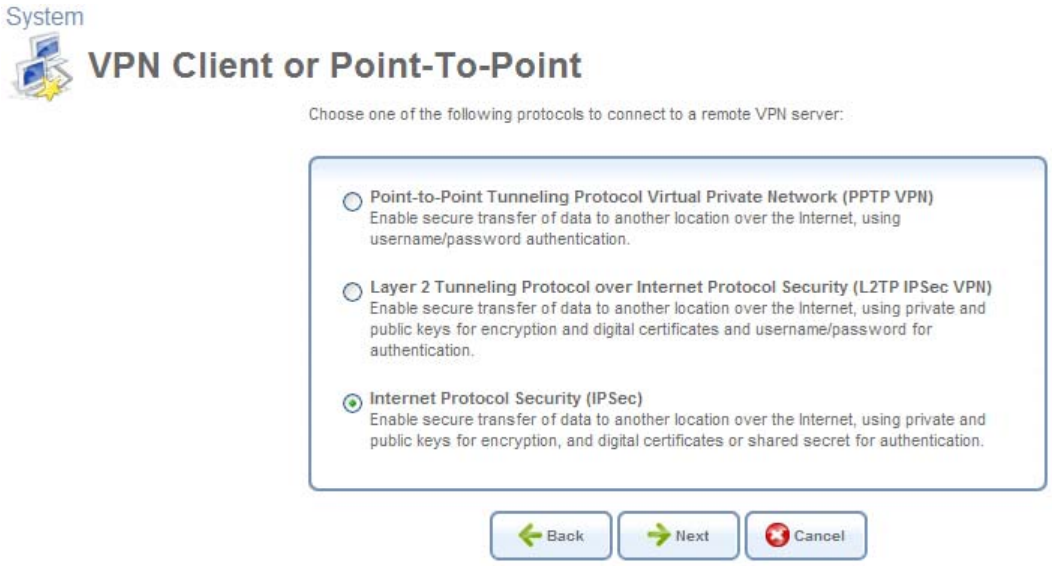


Figure 6.158 VPN Client or Point-To-Point

4. Select the 'Internet Protocol Security (IPSec)' radio button and click 'Next'. The 'Internet Protocol Security (IPSec)' screen appears.

Figure 6.159 Internet Protocol Security (IPSec)

5. Enter the host name or IP address of the destination gateway.

6. Select a method for specifying the remote IP address, which serves as the tunnel's endpoint. Use "Same as Gateway" when connecting your LAN to a remote gateway. When connecting your LAN to a remote network (a group of computers beyond a gateway), use one of the remaining options. Also, use the transport encapsulation type in a gateway-to-gateway scenario only. Upon selection of an option, the screen refreshes providing you with the appropriate fields for entering the data.
   a. **Same as Gateway** – The default option that uses the gateway IP entered above. When selecting this option, you must also select the encapsulation type, tunnel or transport, from its drop-down menu.
   b. **IP Address** – The 'Remote IP Address' field appears. Specify the IP address.
   c. **IP Subnet** – The 'Remote Subnet IP Address' and 'Remote Subnet Mask' fields appear. Specify these parameters.
   d. **IP Range** – The 'From IP Address' and 'To IP Address' fields will appear. Specify the IP range.

7. Enter the IPSec shared secret, which is the encryption key jointly decided upon with the network you are trying to access.

8. Click 'Next'. The 'Connection Summary' screen appears.

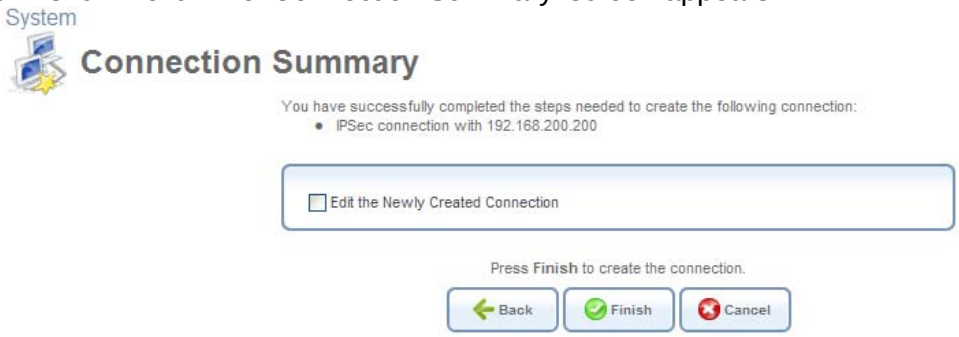


Figure 6.160 Connection Summary

9. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

10. Click ‘Finish’ to save the settings.

The new IPSec connection will be added to the network connections list, and will be configurable like any connection. Unlike other connections, it is also accessible via the iPECS SBG-1000’s ‘Shortcut’ screen. To learn more about the configuration of an IPSec connection, refer to Section 5.4.1.

6.4.13 Setting Up an IPSec Server

To set up an Internet Protocol Security (IPSec) Server, perform the following:

1. Click the ‘New Connection’ link in the ‘Network Connections’ screen (see Figure 6.11). The ‘Connection Wizard’ screen appears (see Figure 6.12).

2. Select the ‘Connect to a Virtual Private Network over the Internet’ radio button and click ‘Next’. The ‘Connect to a Virtual Private Network over the Internet’ screen appears (see figure ‘Connect to a Virtual Private Network over the Internet’).

3. Select the ‘VPN Server’ radio button and click ‘Next’. The ‘VPN Server’ screen appears.

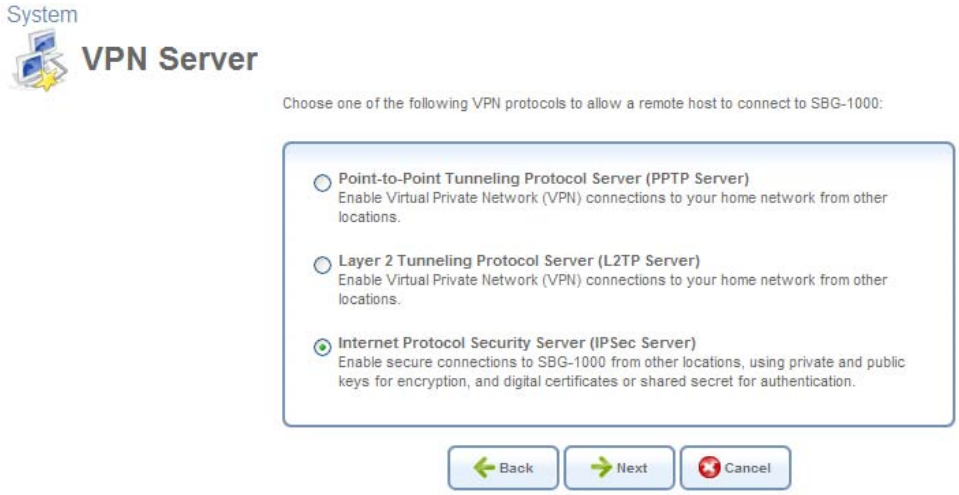


Figure 6.161 VPN Server

4. Select the ‘Internet Protocol Security Server (IPSec Server)’ radio button and click ‘Next’. The ‘Internet Protocol Security Server (IPSec Server)’ screen appears.

Figure 6.162 Internet Protocol Security Server (IPSec Server)

5. Enter the IPSec shared secret, which is the encryption key jointly decided upon with the

network you are trying to access.

6. Click ‘Next’. The ‘Connection Summary’ screen appears.

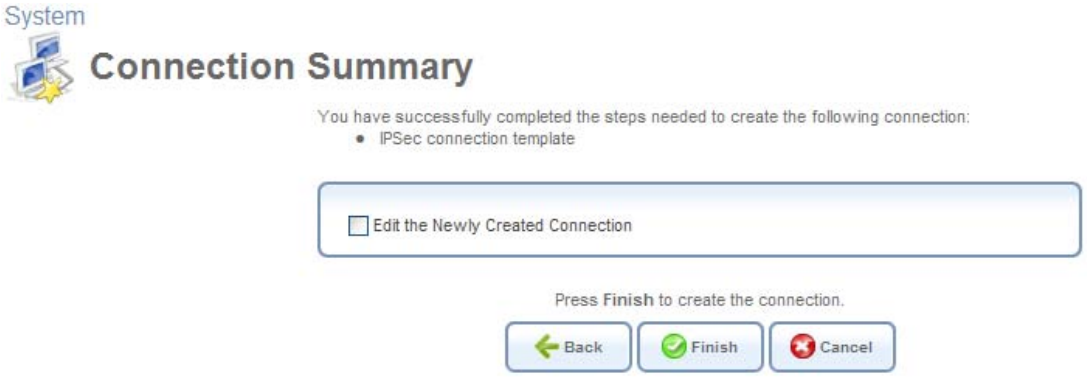


Figure 6.163 Connection Summary

7. Select the ‘Edit the Newly Created Connection’ check box if you wish to be routed to the new connection’s configuration screen after clicking ‘Finish’. This screen is described later in this chapter.

8. Click ‘Finish’ to save the settings.

The new IPSec Server will be added to the network connections list, and will be configurable like any other connection. To learn more about the configuration of an IPSec server, refer to Section 5.4.1.

6.4.14 Setting up a WAN-LAN Bridge

A WAN-LAN bridge is a bridge over WAN and LAN devices. This way computers on the iPECS SBG-1000 LAN side can get IP addresses that are known on the WAN side.

6.4.14.1 Creating a WAN-LAN Bridge Connection

To create a new bridge or configure an existing one, perform the following:

1. In the ‘Network Connections’ screen under ‘System’ (see Figure 6.11), click the ‘New Connection’ link. The ‘Connection Wizard’ screen appears (see Figure 6.12).

2. Select the ‘Advanced Connection’ radio button and click ‘Next’. The ‘Advanced Connection’ screen appears.

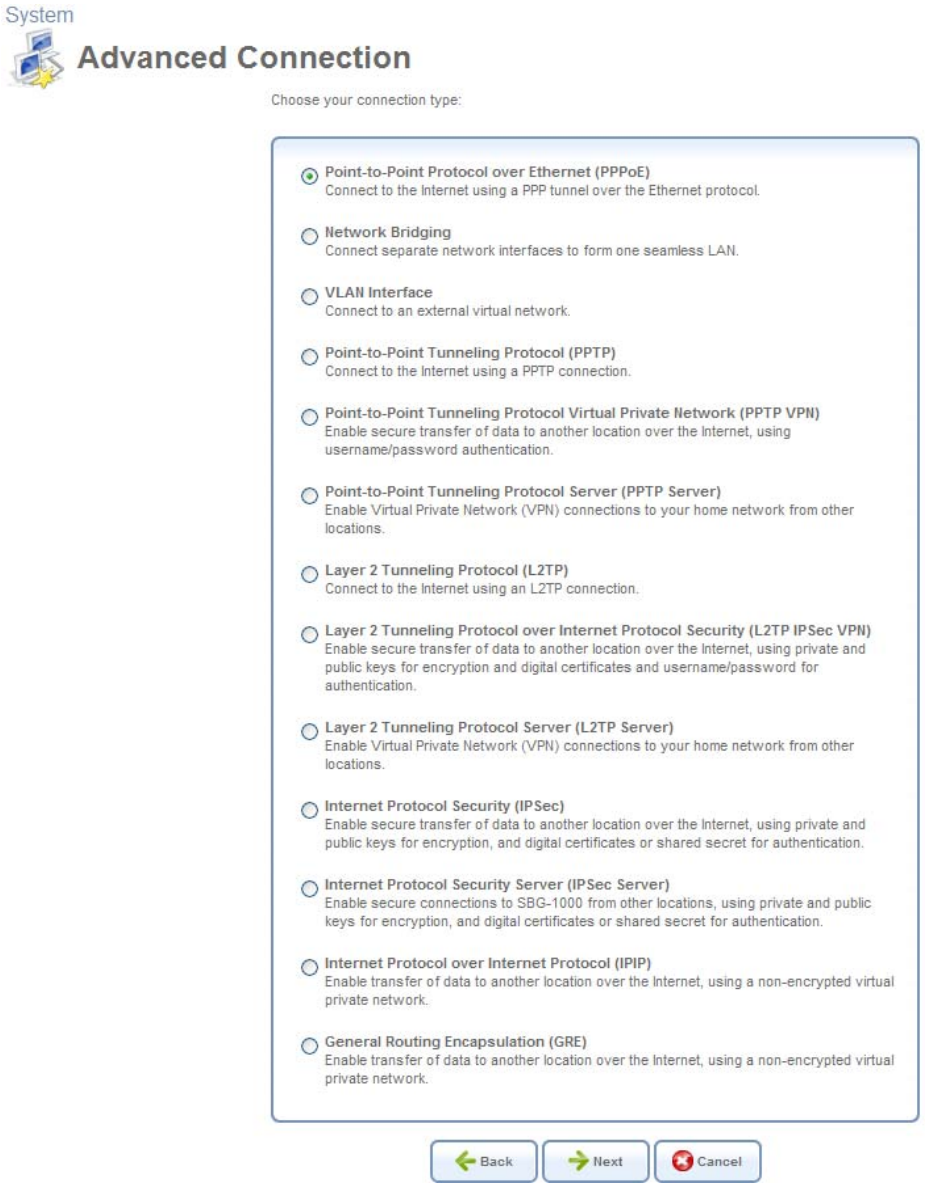


Figure 6.164 Advanced Connection Wizard

3. Select the ‘Network Bridging’ radio button and click ‘Next’. The ‘Bridge Options’ screen appears.

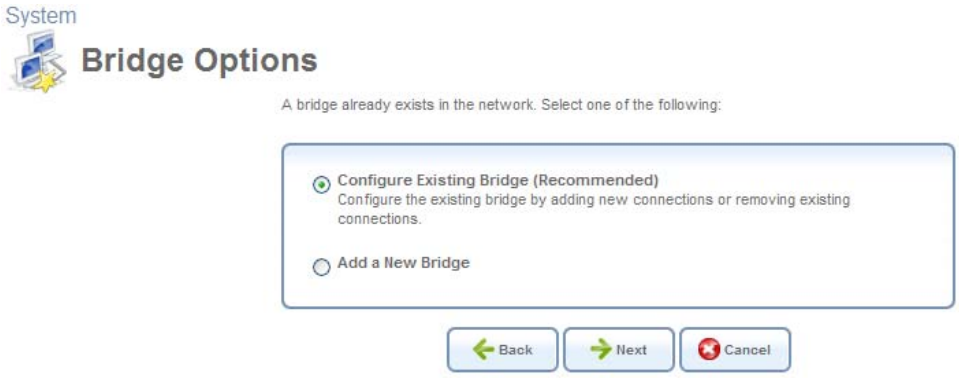


Figure 6.165 Bridge Options

4. Select whether to configure an existing bridge (this option will only appear if a bridge exists) or to add a new one:

   a. **Configure Existing Bridge** Select this option and click ‘Next’. The ‘Network Bridging’ screen appears allowing you to add new connections to the bridge or remove existing ones, by selecting or deselecting their respective check boxes. For example, to create a WAN-LAN bridge, select the WAN connection’s check box.

Figure 6.166 Network Bridging – Configure Existing Bridge

   b. **Add a New Bridge** Select this option and click ‘Next’. A different ‘Network Bridging’ screen appears allowing you to add a bridge over the unbridged connections, by selecting their respective check boxes.

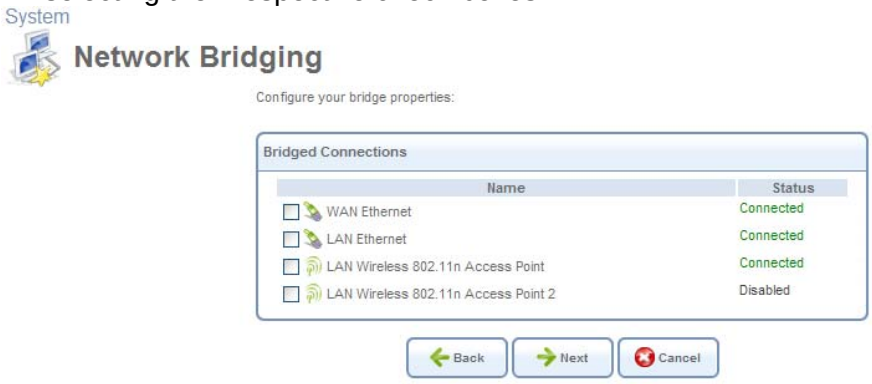


Figure 6.167 Network Bridging – Add a New Bridge

5. Click ‘Next’. The ‘Connection Summary’ screen appears, corresponding to your changes.

Figure 6.168 Connection Summary – Configure Existing Bridge

6. Select the ‘Edit the Newly Created Connection’ check box if you wish to be routed to the new connection’s configuration screen after clicking ‘Finish’. This screen is described later in this chapter.

7. Click ‘Finish’ to save the settings. The new bridge will be added to the network connections list, and it will be configurable like any other bridge.

The new bridge will be added to the network connections list, and it will be configurable like any other bridge.

Note: Creating a WAN-LAN bridge disables iPECS SBG-1000’s DHCP server. This means that LAN hosts may only receive an IP address from a DHCP server on the WAN. If you configure a host with a static IP address from an alias subnet of the bridge (192.168.1.X), you will be able to access iPECS SBG-1000 but not the WAN, as NAT is not performed in the WAN-LAN bridge mode.

After creating a WAN-LAN bridge, you must also disable the IGMP Proxy on this connection. To do so, perform the following:

1. In the ‘Network Connections’ screen under ‘System’, click the ‘LAN Bridge’ link. The ‘LAN Bridge Properties’ screen appears.

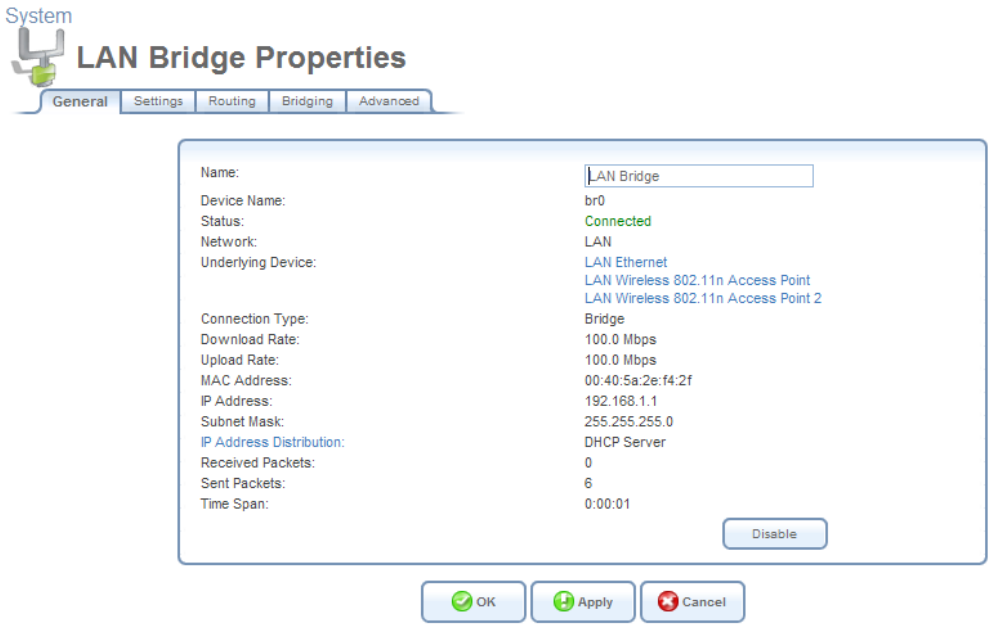


Figure 6.169 LAN Bridge Properties

2. Select the ‘Routing’ sub-tab, and disable the ‘Multicast - IGMP Proxy Default’ option (to learn more about this option, refer to Section 6.4.14.3.3).

3. Click ‘OK’ to save the settings.

6.4.14.2 Enabling the Hybrid Bridging Mode

iPECS SBG-1000 enables you to bridge certain bandwidth-consuming and traffic-sensitive LAN hosts, such as IPTV Set Top Boxes, directly to the WAN. Such a network connection scheme does not interfere with iPECS SBG-1000's routing mode, in which all traffic usually passes through the NAT, and is checked by the firewall. These two modes can work simultaneously, if you have two bridges under iPECS SBG-1000's LAN network device:

LAN bridge Receives its IP address from iPECS SBG-1000's DHCP server. The traffic passing through the LAN on its way to the WAN is inspected by iPECS SBG-1000's firewall, and assigned a public address by the NAT.

WAN-LAN bridge Receives its IP address from the WAN DHCP server, thereby enabling direct communication with the WAN.
iPECS SBG-1000 based on Linux 2.6 supports direct communication between devices placed under the two bridges. For example, if you connect your IPTV Set Top Box with a Personal Video Recorder (PVR) to iPECS SBG-1000's WAN-LAN bridge, you will be able to access the content recorded on the PVR from any home computer connected to iPECS SBG-1000's LAN.
This network configuration is called *Hybrid Bridging*. iPECS SBG-1000 detects LAN hosts that should be bridged to the WAN according to their MAC address or a specific DHCP option (either **Vendor Class ID**, **Client ID** or **User Class ID**). Once detected, these LAN hosts are placed under the WAN-LAN bridge, which you must add and configure for the hybrid bridging mode beforehand. To add the WAN-LAN bridge, follow the Connection Wizard steps described in Section 6.4.14.1. In the final step, check the 'Edit the Newly Created Connection' check box, and click 'Finish'. The 'Bridge Properties' screen appears.

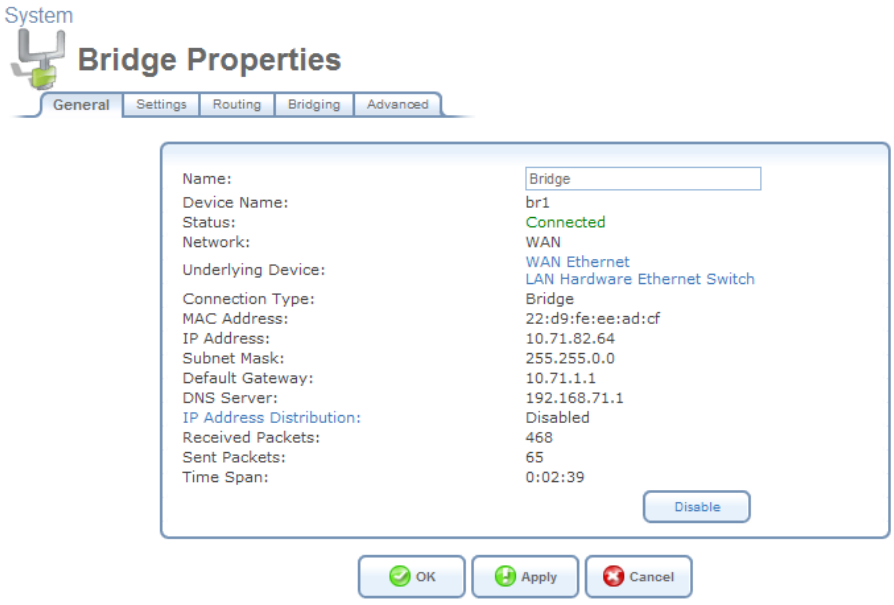


Figure 6.170 Bridge Properties

To configure the WAN-LAN bridge for the hybrid bridging mode, perform the following:

1. In the 'Bridge Properties' screen, click the 'Routing' tab. The following screen appears.

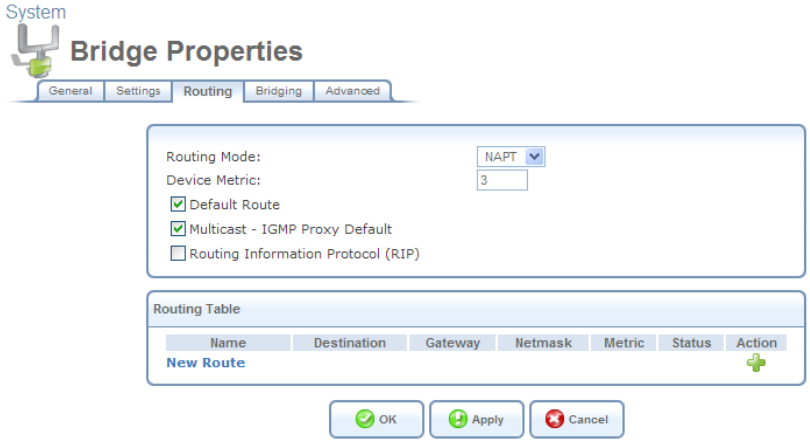


Figure 6.171 WAN-LAN Bridge Routing Settings

2. From the 'Routing Mode' drop-down menu, select 'Route' and click 'Apply'. The following warning screen appears.

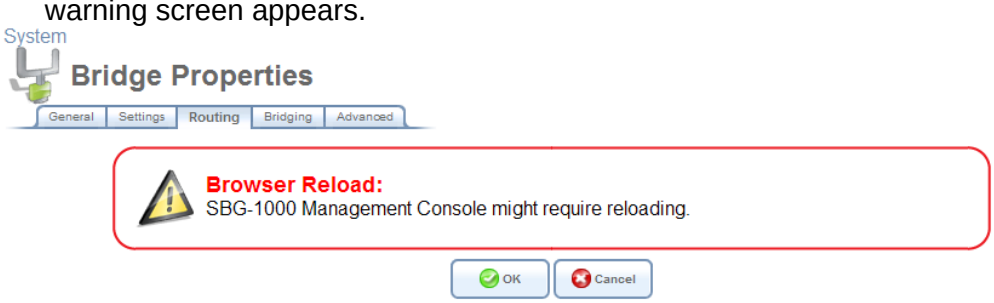


Figure 6.172 Browser Reload Warning Message

3. Click 'OK'. The page refreshes while saving the new settings, and returns to the previous screen.

4. Click the 'Bridging' tab. The following screen appears.

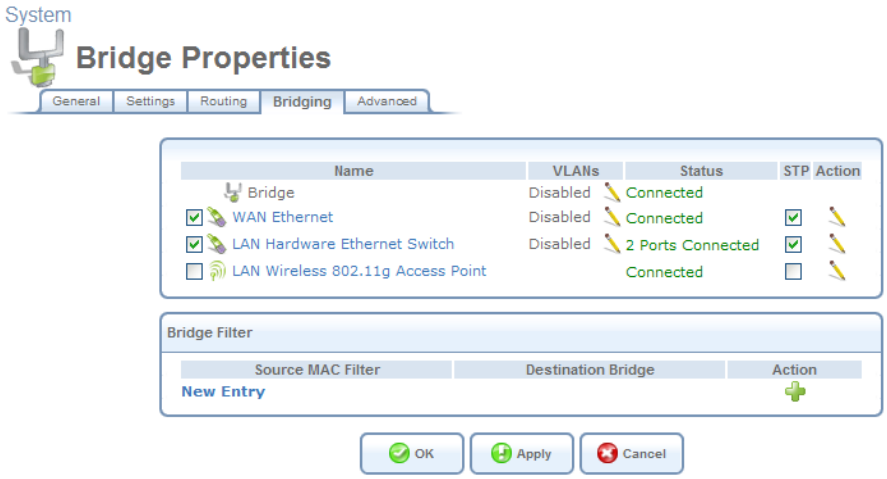


Figure 6.173 WAN-LAN Bridging Settings

5. In the 'Bridge Filter' section, click the 'New Entry' link. The following screen appears.

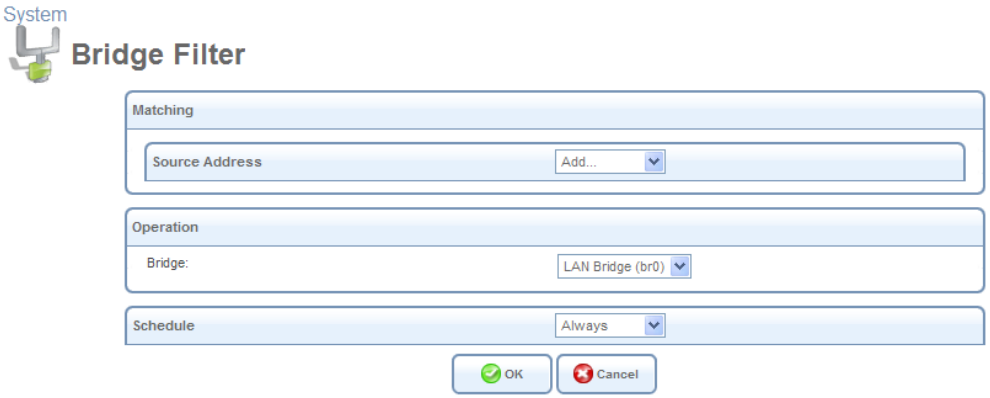


Figure 6.174 Bridge Filter Settings

6. From the drop-down menu in the ‘Operation’ section, select the WAN-LAN bridge. If not renamed, its default entry appears as “Bridge (br1)”.

7. From the ‘Source Address’ drop-down menu, select ‘User Defined’. The ‘Edit Network Object’ screen appears.

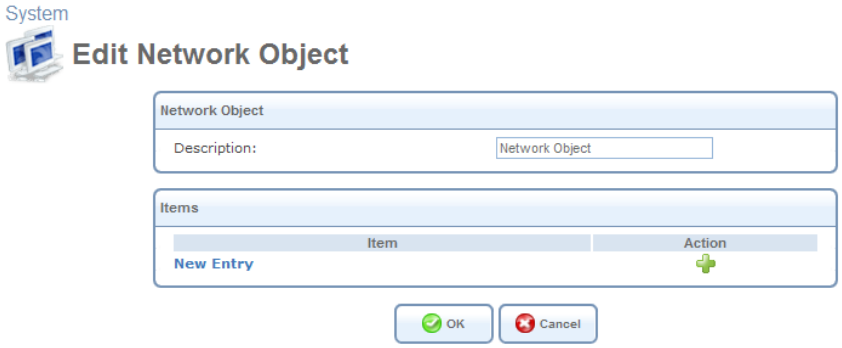


Figure 6.175 Edit Network Object

8. Click the ‘New Entry’ link. The ‘Edit Item’ screen appears.

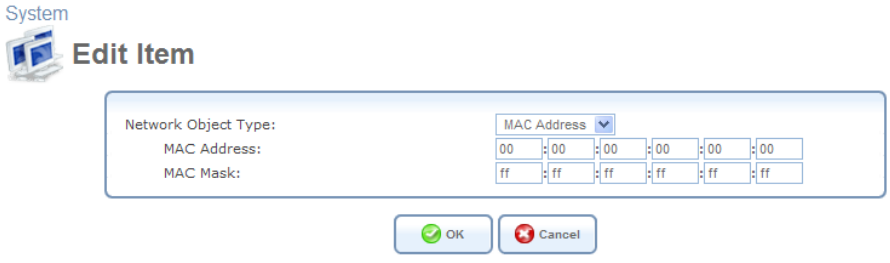


Figure 6.176 Edit Item – MAC Address

This screen enables you to create a traffic filtering rule, which enables direct packet flow between the WAN and the LAN host that will be placed under the WAN-LAN bridge. This filtering rule can be based on either a LAN host’s MAC address or one of its DHCP options mentioned earlier.

9. If you wish to base this rule on the MAC address, enter the MAC address and the MAC mask in their respective fields. Otherwise, perform the following:

a. From the ‘Network Object Type’ drop-down menu, select ‘DHCP Option’. The screen refreshes, changing to the following.

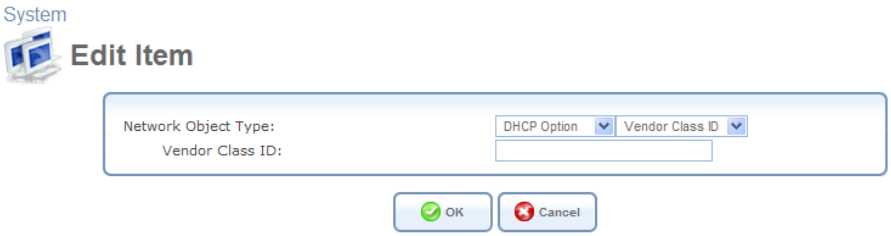


Figure 6.177 Edit Item – DHCP Options

b. From the designated drop-down menu, select one of the DHCP options. The field below changes accordingly.
c. Enter a relevant value for the DHCP option (should be supplied by your service provider).

10. Click ‘OK’ to save the settings.

6.4.14.3 Viewing and Editing the Connection’s Settings

To view and edit the WAN-LAN bridge connection settings, click the ‘Bridge’ link in the ‘Network Connections’ screen. The ‘Bridge Properties’ screen appears.

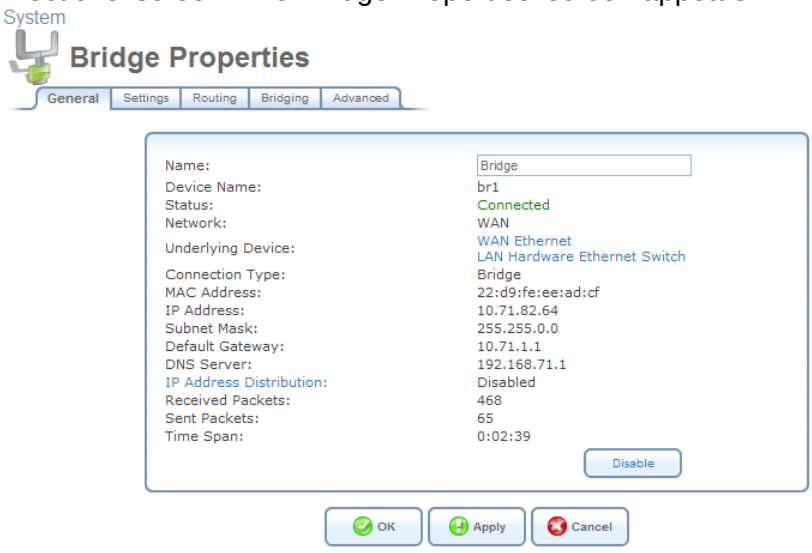


Figure 6.178 Bridge Properties

6.4.14.3.1 General

This sub-tab enables you to view a detailed summary of the WAN-LAN bridge connection settings. These settings can be edited in the rest of the screen’s sub-tabs, as described in the following sections.

6.4.14.3.2 Settings

This sub-tab enables you to edit the following WAN-LAN bridge connection settings.

General This section displays the connection’s general parameters.

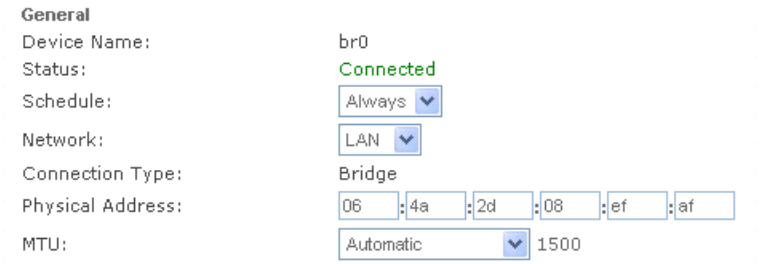


Figure 6.179 General Bridge Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind iPECS SBG-1000.

Physical Address The physical address of the network interface for your network. Some interfaces allow you to change this address.

Clone My MAC Address Press this button to copy your PC's current MAC address to the board.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen will refresh to display relevant configuration settings according to your choice.

No IP Address Select 'No IP Address' if you require that your gateway have no IP address. This can be useful if you are working in an environment where you are not connected to other networks, such as the Internet.

Figure 6.180 Internet Protocol – No IP Address

Obtain an IP Address Automatically Your connection is configured by default to act as a DHCP client. You should keep this configuration in case your service provider supports DHCP, or if you are connecting using a dynamic IP address. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead. You can click the 'Release' button to release the current leased IP address. Once the address has been released, the button text changes to 'Renew'. Use the 'Renew' button to renew the leased IP address.

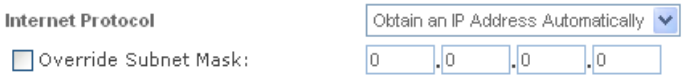


Figure 6.181 Internet Protocol Settings – Automatic IP

Use the Following IP Address Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

Figure 6.182 Internet Protocol – Static IP

DNS Server Domain Name System (DNS) is the method by which Web site domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

Figure 6.183 DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

Figure 6.184 DNS Server – Static IP

To learn more about this feature, refer to Section 5.8.1.

IP Address Distribution In general, the 'IP Address Distribution' section enables you to configure the DHCP server parameters. However, in the WAN-LAN bridge configuration, the DHCP server must be disabled.

6.4.14.3.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

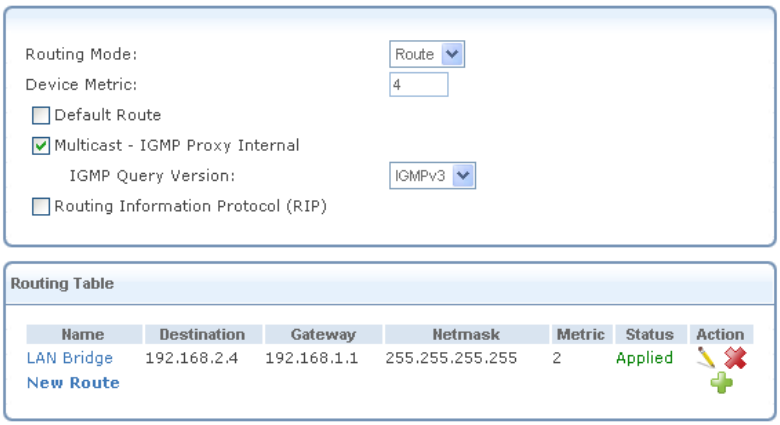


Figure 6.185 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

Route Use route mode if you want your gateway to function as a router between two networks.

NAPT Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default iPECS SBG-1000 serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version iPECS SBG-1000 supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages**—select either ‘None’, ‘RIPv1’, ‘RIPv2’ or ‘RIPv1/2’.
- **Send RIP messages**—select either ‘None’, ‘RIPv1’, ‘RIPv2-broadcast’ or ‘RIPv2-multicast’.

Routing Table Allows you to add or modify routes when this device is active. Use the ‘New Route’ button to add a route or edit existing routes.
To learn more about routing, refer to Section 6.6.

6.4.14.3.4 Bridging

This sub-tab enables you to specify the devices that you would like to join under the network bridge.

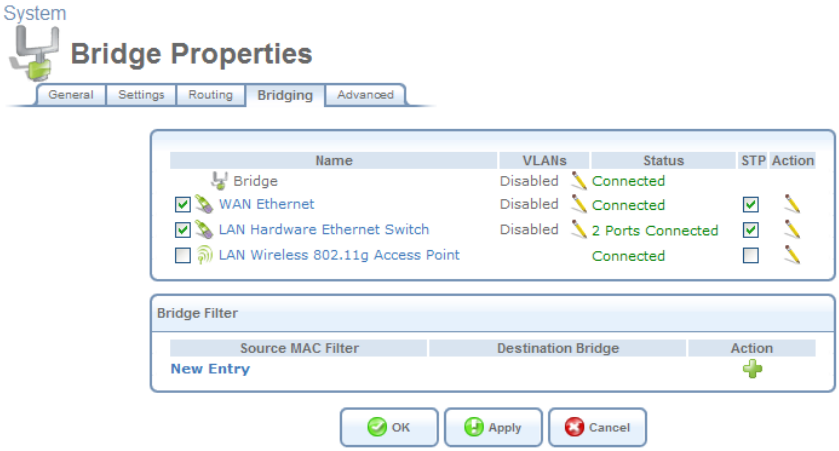


Figure 6.186 Bridge Settings

If you wish to assign the network connections to specific virtual LANS (VLANs), click the action icon under the ‘VLANs’ column.

Note: If you would like to logically partition your Ethernet-based network, you can set up a VLAN bridge as described in Section 6.4.17.5.

Select the ‘STP’ check box to enable the Spanning Tree Protocol on the device. Use this feature to ensure that there are no loops in your network configuration, especially in case your network consists of multiple switches, or other bridges apart from those created by the gateway. By blocking redundant connections, STP enables a single data path between LAN hosts. If a device or a link failure causes this path to become unusable, STP will enable an alternative path. Note that iPECS SBG-1000 also supports the Rapid Spanning Tree Protocol (RSTP), which provides a faster response to changes in your local network topology than STP.

6.4.14.3.5 Advanced

This sub-tab enables you to edit the connection’s advanced settings.

- **Internet Connection Firewall** Your gateway’s firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the ‘Enabled’ check box. To learn more about your gateway’s security features, refer to Section 5.2.

Figure 6.187 Internet Connection Firewall

- **Additional IP Addresses** You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1 and the http://sbg-1000.home.

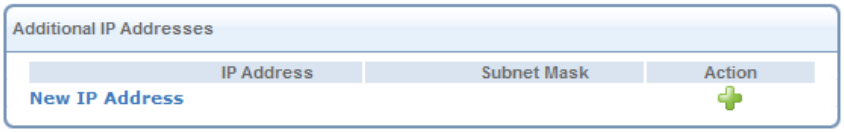


Figure 6.188 Additional IP Addresses

6.4.15 Setting Up an IPIP Tunnel

iPECS SBG-1000 allows you to create an Internet Protocol over Internet Protocol (IPIP) tunnel to another router, by encapsulating IP packets in IP. This tunnel can be managed as any other network connection. Supported by many routers, this protocol enables using multiple network schemes. Note, however, that IPIP tunnels are not secured.

6.4.15.1 Creating an IPIP Tunnel

To create a new IPIP tunnel, perform the following:

1. In the 'Network Connections' screen under 'System' (see Figure 6.11), click the 'New Connection' link. The 'Connection Wizard' screen appears (see Figure 6.12).

2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears.

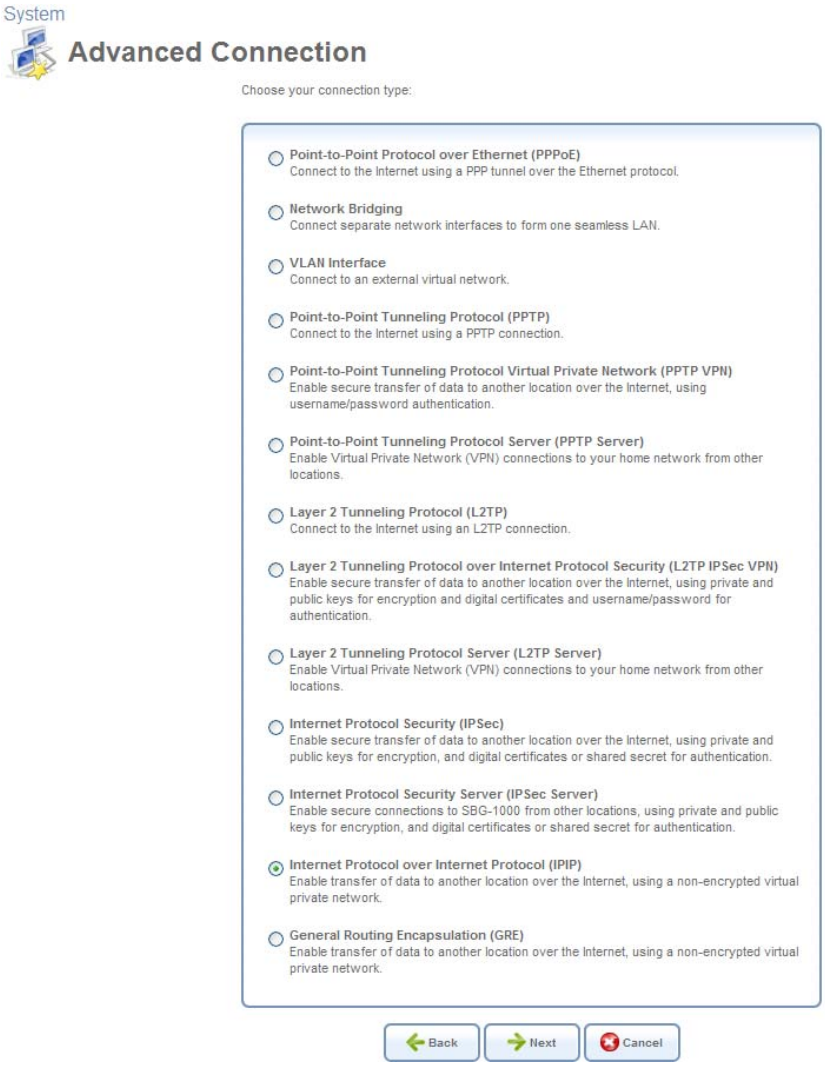


Figure 6.189 Advanced Connection Wizard

3. Select the ‘Internet Protocol over Internet Protocol (IPIP)’ radio button and click ‘Next’. The ‘Internet Protocol over Internet Protocol (IPIP)’ screen appears.

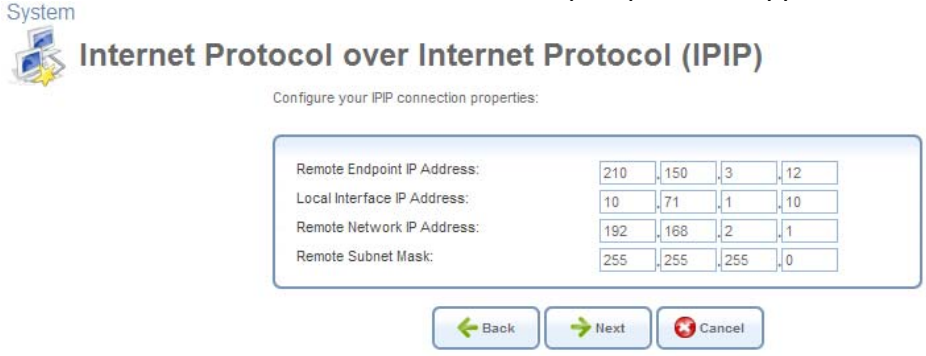


Figure 6.190 Internet Protocol over Internet Protocol (IPIP)

4. Enter the tunnel’s remote endpoint IP address.

5. Enter the local IP address for the interface.

6. Enter the IP address and subnet mask of the remote network that will be accessed via the tunnel, and click ‘Next’. The ‘Connection Summary’ screen appears.

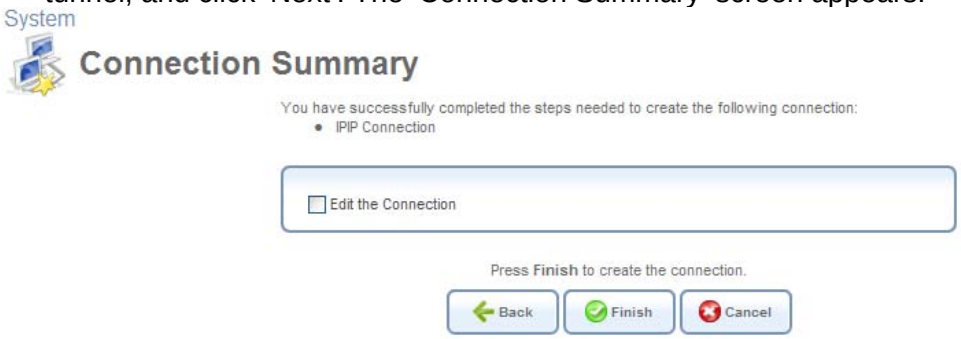


Figure 6.191 Connection Summary

7. Select the ‘Edit the Newly Created Connection’ check box if you wish to be routed to the new connection’s configuration screen after clicking ‘Finish’. This screen is described later in this chapter.

8. Click ‘Finish’ to save the settings.

The new IPIP tunnel will be added to the network connections list, and will be configurable like any other connection.

6.4.15.2 Viewing and Editing the Tunnel Settings

To view and edit the IPIP tunnel settings, click the ‘WAN IPIP’ link in the ‘Network Connections’ screen (see Figure 6.11). The ‘WAN IPIP Properties’ screen appears.

Figure 6.192 WAN IPIP Properties

6.4.15.2.1 General

This sub-tab enables you to view a detailed summary of the IPIP tunnel settings (see Figure 6.192). These settings can be edited in the rest of the screen’s sub-tabs, as described in the following sections.

6.4.15.2.2 Settings

This sub-tab enables you to edit the following IPIP tunnel settings.

General This section displays the tunnel's general parameters.

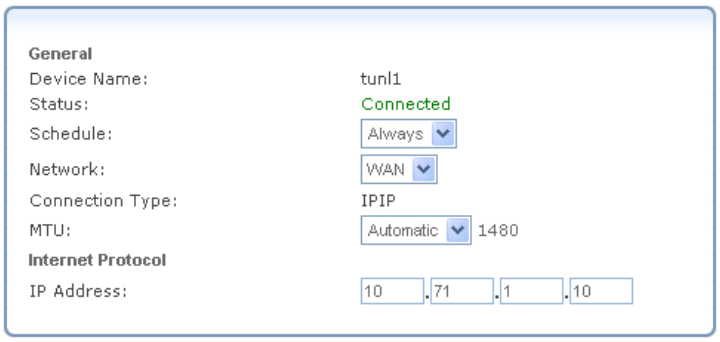


Figure 6.193 General WAN IPIP Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind iPECS SBG-1000.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol The local IP address for the interface.

6.4.15.2.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

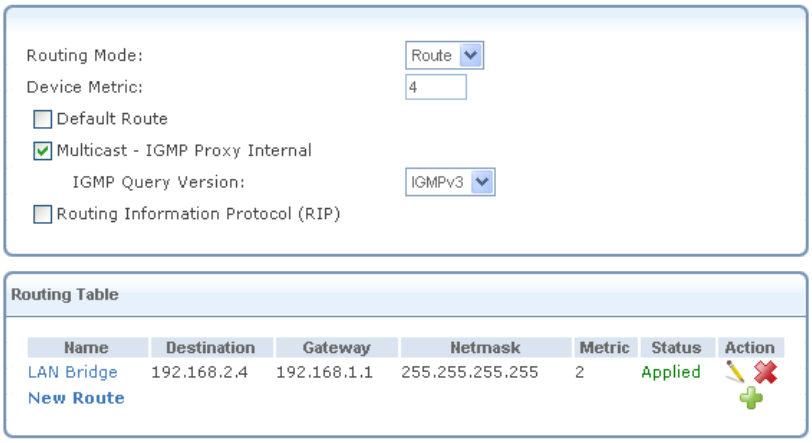


Figure 6.194 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

Route Use route mode if you want your gateway to function as a router between two networks.

NAPT Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default iPECS SBG-1000 serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version iPECS SBG-1000 supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages**—select either ‘None’, ‘RIPv1’, ‘RIPv2’ or ‘RIPv1/2’.
- **Send RIP messages**—select either ‘None’, ‘RIPv1’, ‘RIPv2-broadcast’ or ‘RIPv2-multicast’.

Routing Table Allows you to add or modify routes when this device is active. Use the ‘New Route’ button to add a route or edit existing routes.
To learn more about routing, refer to Section 6.6.

6.4.15.2.4 IPIP

This sub-tab enables you to edit the tunnel's remote endpoint IP address.

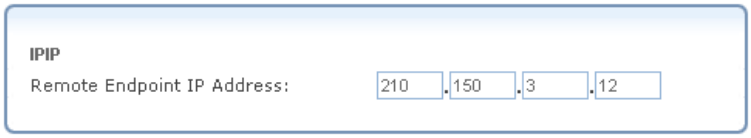


Figure 6.195 IPIP

6.4.15.2.5 Advanced

This sub-tab enables you to edit the tunnel's advanced settings.

Internet Connection Firewall Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

Figure 6.196 Internet Connection Firewall

6.4.16 Setting Up a GRE Tunnel

iPECS SBG-1000 allows you to create a General Routing Encapsulation (GRE) tunnel in order to transport multicast traffic, in addition to other existing tunneling capabilities (for example, IPIP, L2TP, PPTP).

6.4.16.1 Creating a GRE Tunnel

To create a new GRE tunnel, perform the following:

1. In the 'Network Connections' screen under 'System' (see Figure 6.11), click the 'New Connection' link. The 'Connection Wizard' screen appears (see Figure 6.12).

2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears.

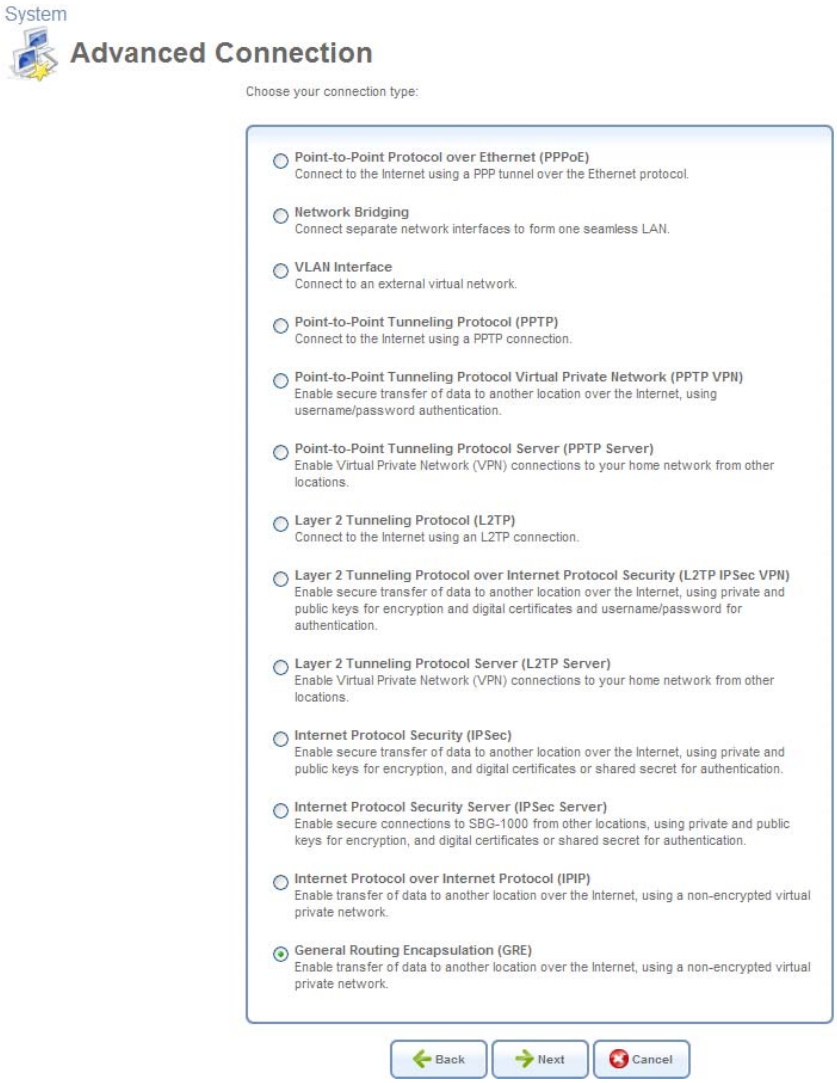


Figure 6.197 Advanced Connection Wizard

3. Select the ‘General Routing Encapsulation (GRE)’ radio button and click ‘Next’. The ‘General Routing Encapsulation (GRE)’ screen appears.

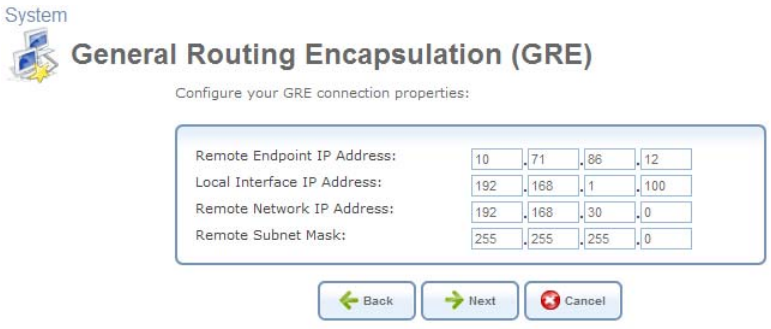


Figure 6.198 General Routing Encapsulation (GRE)

4. Enter the tunnel’s remote endpoint IP address.

5. Enter the local IP address of the gateway’s GRE interface.

6. Enter the IP address and subnet mask of the remote network that will be accessed via the tunnel, and click ‘Next’. The ‘Connection Summary’ screen appears.

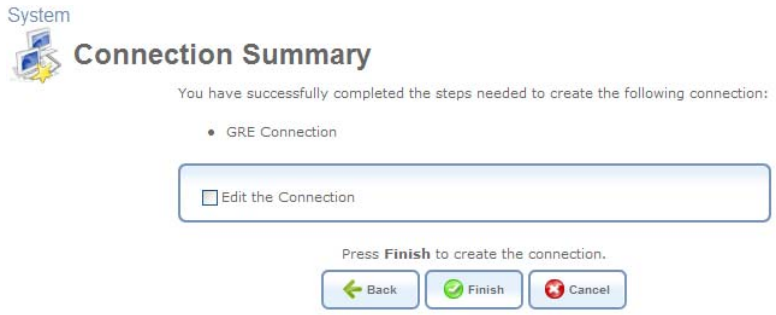


Figure 6.199 Connection Summary

7. Select the ‘Edit the Newly Created Connection’ check box if you wish to be routed to the new connection’s configuration screen after clicking ‘Finish’. This screen is described later in this chapter.

8. Click ‘Finish’ to save the settings.

The new GRE tunnel will be added to the network connections list, and will be configurable like any other connection.

6.4.16.2 Viewing and Editing the Tunnel Settings

To view and edit the GRE connection settings, click the ‘WAN GRE’ link in the ‘Network Connections’ screen (see Figure 6.11). The ‘WAN GRE Properties’ screen appears.

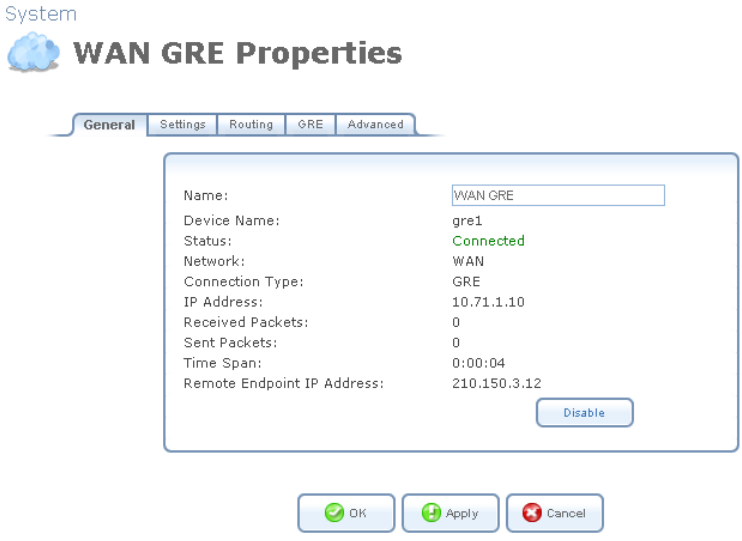


Figure 6.200 WAN GRE Properties

6.4.16.2.1 General

This sub-tab enables you to view a detailed summary of the GRE tunnel settings (see Figure 6.200). These settings can be edited in the rest of the screen’s sub-tabs, as described in the following sections.

6.4.16.2.2 Settings

This sub-tab enables you to edit the following GRE tunnel settings.

General This section displays the connection's general parameters.

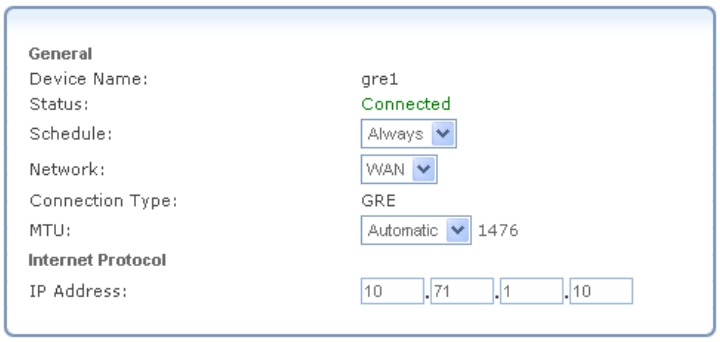


Figure 6.201 General WAN GRE Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind iPECS SBG-1000.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol The local IP address for the interface.

6.4.16.2.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

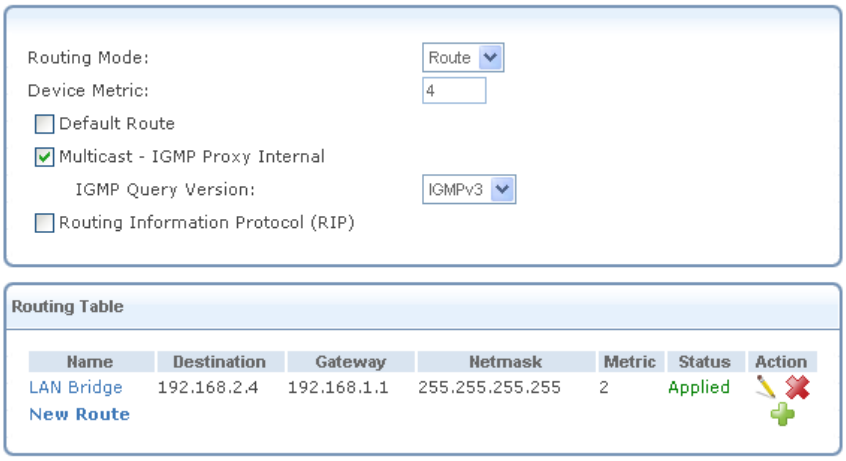


Figure 6.202 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

Route Use route mode if you want your gateway to function as a router between two networks.

NAPT Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default iPECS SBG-1000 serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version iPECS SBG-1000 supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages**—select either ‘None’, ‘RIPv1’, ‘RIPv2’ or ‘RIPv1/2’.
- **Send RIP messages**—select either ‘None’, ‘RIPv1’, ‘RIPv2-broadcast’ or ‘RIPv2-multicast’.

Routing Table Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.
To learn more about routing, refer to Section 6.6.

6.4.16.2.4 GRE

This sub-tab enables you to edit the tunnel's remote endpoint IP address.

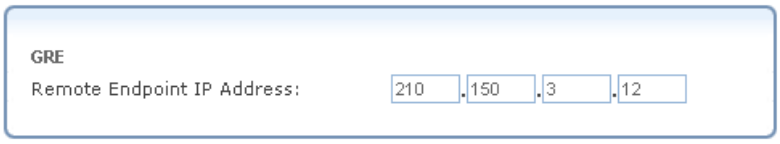


Figure 6.203 GRE

6.4.16.2.5 Advanced

This sub-tab enables you to edit the tunnel's advanced settings.

Internet Connection Firewall Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

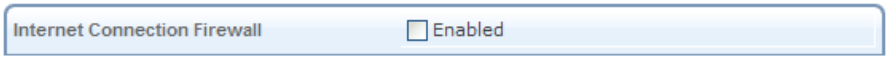


Figure 6.204 Internet Connection Firewall

6.4.17 Setting Up a VLAN Interface

A Virtual LAN (VLAN) interface enables you to group workstations together into one broadcast domain, even if they are not located on the same LAN segment. iPECS SBG-1000 allows you to create virtual Ethernet-based networks according to the IEEE 802.1Q standard. If you would like your VLANs to communicate with the same network node without communicating with each other, use iPECS SBG-1000's VLAN bridging capability as described in Section 6.4.17.5.3.

6.4.17.1 Understanding internal device architecture of iPECS SBG-1000

Before explaining how to set up VLAN interface, you should understand internal device architecture of iPECS SBG-1000. As below figure, iPECS SBG-1000 consists of CPU, 8 ports Ethernet switch and WiFi chip. The CPU is connected with the switch and WiFi chip. If you want to configure VLAN between WAN and user ports on LAN side, you must set VLAN configurations on CPU and Switch each other.

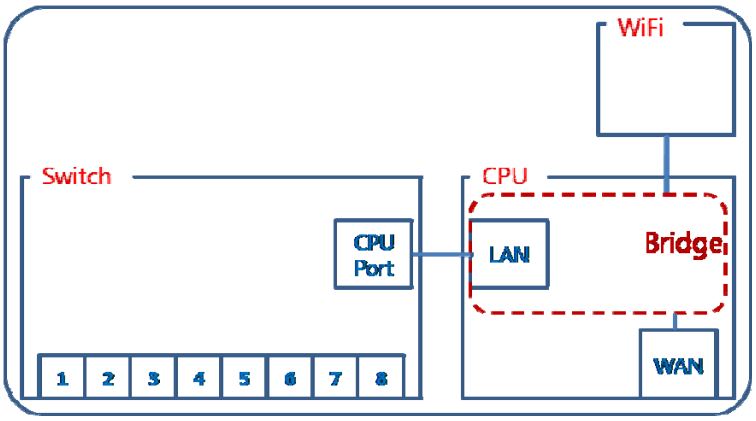


Figure 6.205 iPECS SBG-1000 internal architecture

The switch of iPECS SBG-1000 has 9 ports including CPU port. The port has a PVID (Port VLAN ID) and can set VLAN IDs up to 4094 and egress policy. When ingress untagged packets are received, the PVID is used to handle by default VLAN ID membership.

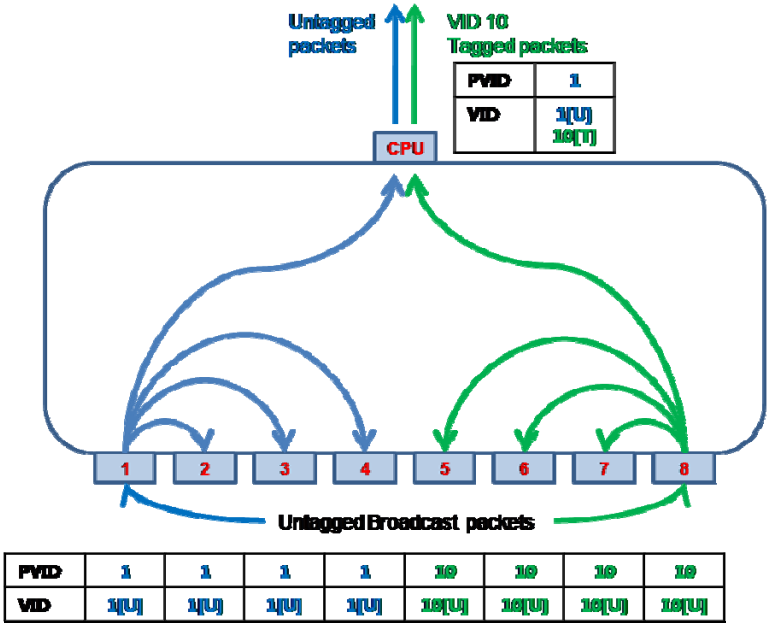


Figure 6.206 Example of two VLAN configuration

Figure 6.206 is an example of configuration separated by VLAN. The ports 1-4 and CPU have default PVID 1 and the ports 5-8 have PVID 10. When broadcast packets are input in port 1, the packets will be forwarded to port 2, 3, 4 and CPU because of same VLAN domain. When the packets are input in port 8, the packets will be forwarded to port 5, 6 and 7. If the port CPU has VLAN ID 10 with egress tagged policy, the packets will be transmitted with VLAN header with VLAN ID 10.

You can find explanations as described in Section 6.4.17.2 for CPU part and Section 6.4.17.4 for Switch part.

6.4.17.2 Creating a VLAN Interface

To create a new VLAN interface, perform the following:

- In the ‘Network Connections’ screen under ‘System’ (see Figure 6.11), click the ‘New Connection’ link. The ‘Connection Wizard’ screen appears (see Figure 6.12).
- Select the ‘Advanced Connection’ radio button and click ‘Next’. The ‘Advanced Connection’ screen appears.

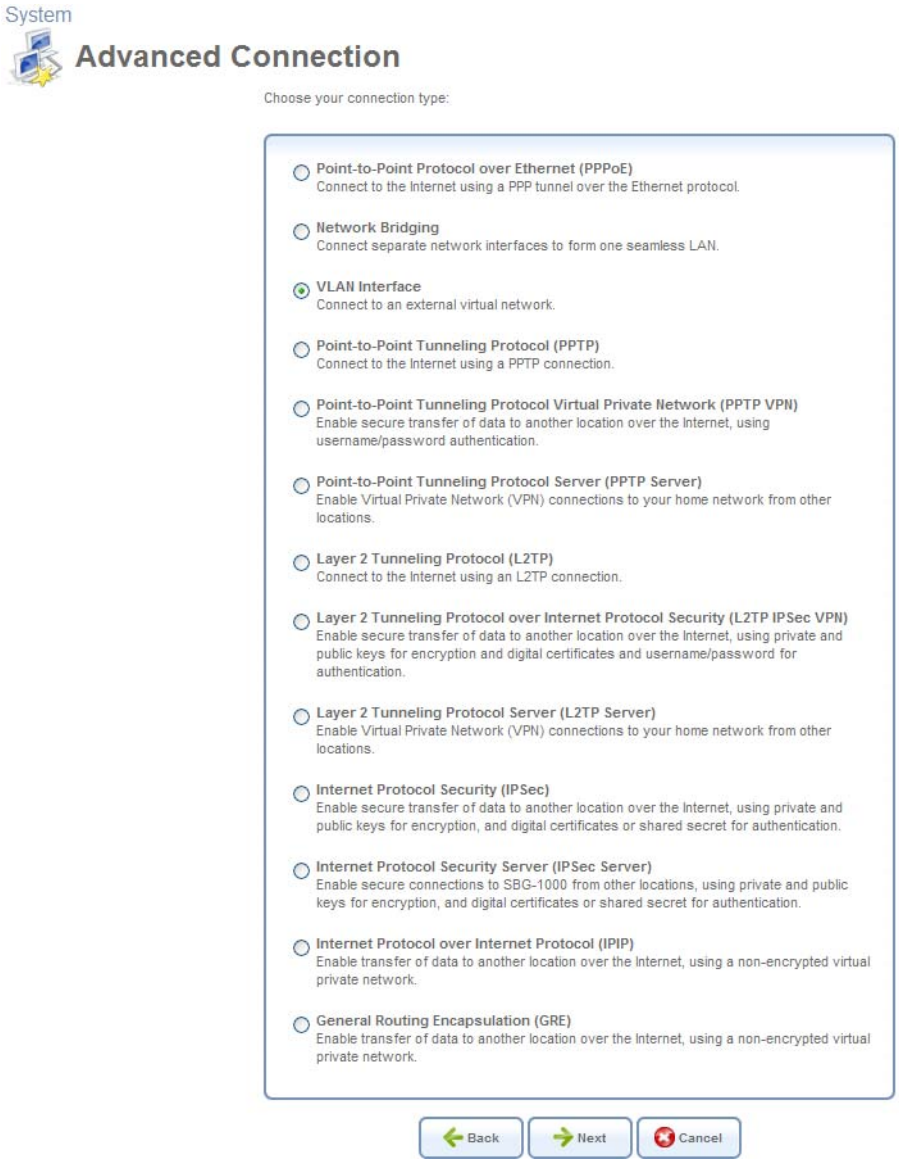


Figure 6.207 Advanced Connection Wizard

Select the ‘VLAN Interface’ radio button and click ‘Next’. The ‘VLAN Interface’ screen appears.

Figure 6.208 VLAN Interface

Note: By default, all of the gateway's physical LAN devices are enslaved by iPECS SBG-1000's LAN bridge. A VLAN cannot be created over an enslaved network device. Therefore, remove a device from the bridge prior to creating a VLAN over it. To learn how to do so, refer to Section 6.4.4.1.

Select the underlying device for this interface. The drop-down menu will display iPECS SBG-1000's Ethernet connections.
Enter a value that will serve as the VLAN ID, and click 'Next'. If you choose to create the VLAN over the LAN bridge, the following screen appears.

Figure 6.209 VLAN over LAN Bridge

Tagging This feature enables you to select whether to add a *tag header* (a 32-bit label serving as a VLAN ID) to the frames transferred over the VLAN. When the 'Untagged' option is selected, the VLAN is determined based on other information, such as the ID of a port on which the data arrived (PVID). Select the relevant setting from the designated drop-down menu. If the created virtual network is intended for VLAN-unaware hosts, it is recommended that you select the 'Untagged' option. And if the "Tagged" option is selected and "LAN Ethernet" port is checked, you must configure switch VLAN configuration as described in Section 6.4.17.4.

VLAN Ports You can select the LAN bridge ports on which you would like to enable the VLAN. To enable the VLAN on a specific device port, select its check box. You can also select or

deselect all of the ports by clicking the corresponding buttons.

After setting the VLAN parameters, click ‘Next’. The ‘Connection Summary’ screen appears.

Figure 6.210 Connection Summary

Select the ‘Edit the Newly Created Connection’ check box if you wish to be routed to the new connection’s configuration screen after clicking ‘Finish’. This screen is described later in this chapter.

Click ‘Finish’ to save the settings.

The new VLAN interface will be added to the network connections list, and will be configurable like any other connection.

6.4.17.3 Viewing and Editing the VLAN Interface Settings

To view and edit the VLAN interface settings, click its link. For example, click the ‘WAN Ethernet’ link in the ‘Network Connections’ screen. The ‘WAN Ethernet Properties’ screen appears.

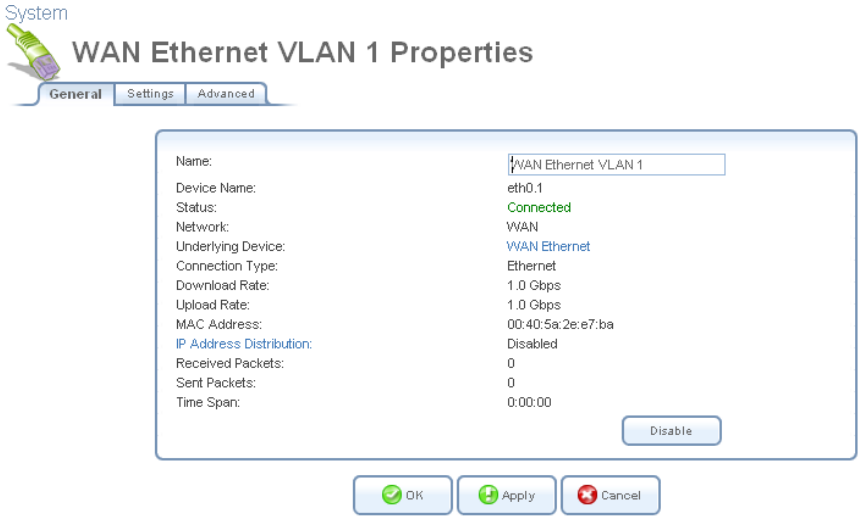


Figure 6.211 WAN Ethernet VLAN 1 Properties

6.4.17.3.1 General

This sub-tab enables you to view a detailed summary of the VLAN interface settings (see Figure 6.211). These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.17.3.2 Settings

This sub-tab enables you to edit the following VLAN interface settings.

General This section displays the connection's general parameters.

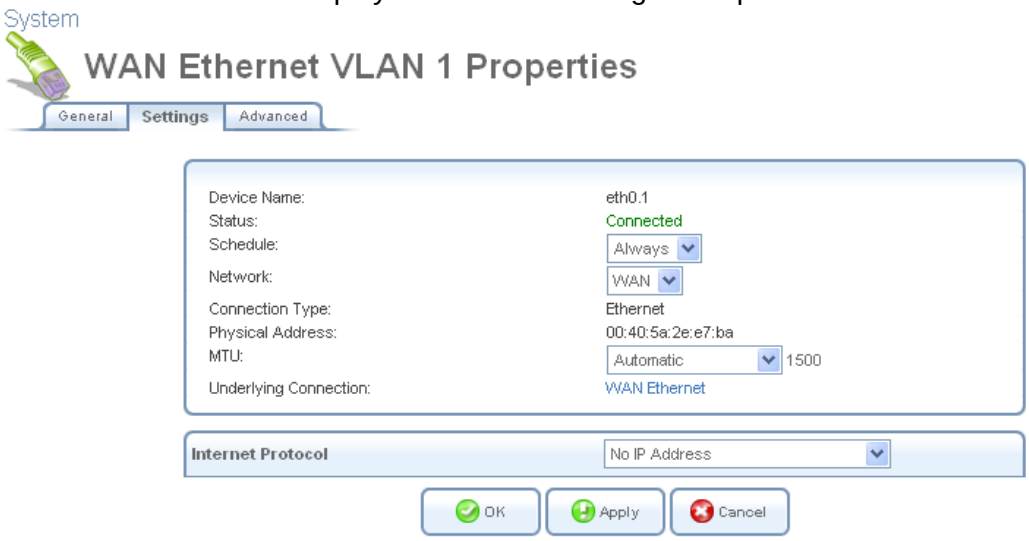


Figure 6.212 General VLAN Interface Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:Remove the connection from under a bridge, if that is the case.
Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind iPECS SBG-1000.

Physical Address The physical address of the network interface for your network. Some interfaces allow you to change this address.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Underlying Connection The Ethernet device over which the connection is implemented.

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

No IP Address Select 'No IP Address' if you require that your gateway have no IP address. This can be useful if you are working in an environment where you are not connected to other networks, such as the Internet. When this menu is selected, routing tab is disappeared because this interface doesn't use IP.

Figure 6.213 Internet Protocol – No IP Address

Obtain an IP Address Automatically Your connection is configured by default to act as a DHCP client. You should keep this configuration in case your service provider supports DHCP, or if you are connecting using a dynamic IP address. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead. You can click the 'Release' button to release the current leased IP address. Once the address has been released, the button text changes to 'Renew'. Use the 'Renew' button to renew the leased IP address.

Figure 6.214 Internet Protocol Settings – Automatic IP

Use the Following IP Address Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

Figure 6.215 Internet Protocol – Static IP

6.4.17.3.3 Advanced

This sub-tab enables you to edit the VLAN's advanced settings.

Internet Connection Firewall Your gateway's firewall helps protect your computer by

preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

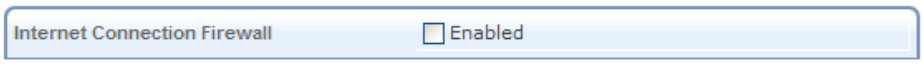


Figure 6.216 Internet Connection Firewall

Additional IP Addresses You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1 and the http://sbg-1000.home.

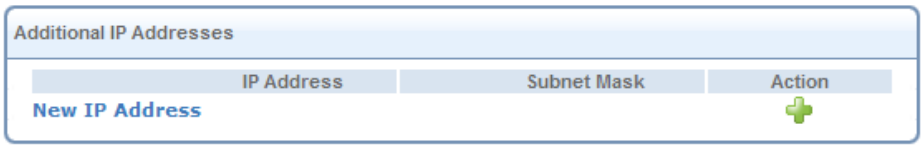


Figure 6.217 Additional IP Addresses

6.4.17.3.4 DSCP Remark According to 802.1p CoS

When creating a VLAN interface over a LAN connection, it is possible to determine the IP header's Differentiated Services Code Point (DSCP) priority value according to the VLAN header's 802.1p Class of Service (CoS) tag. The DSCP value can then be used for Quality of Service (Qos) traffic prioritization. For more information, refer to Section 5.3.

Figure 6.218 DSCP Remark According to 802.1p CoS

Select the 'Enabled' check-box. The screen refreshes, displaying the following table.

Figure 6.219 DSCP Remarks Table

Click the 'New DSCP Remark' link. The following screen appears.

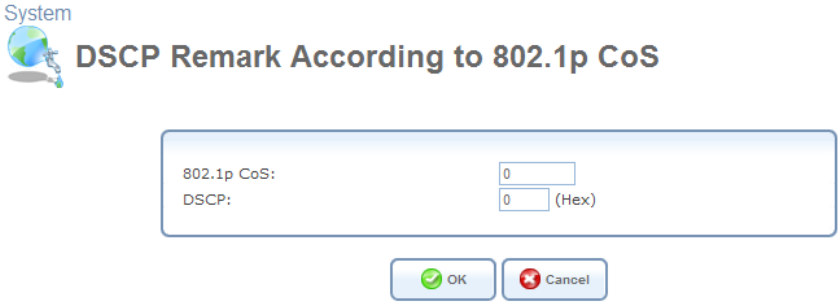


Figure 6.220 DSCP Remark Entry Settings

Enter the 802.1p CoS and DSCP values to be associated, and click ‘OK’. The new pair of values will appear in the table.

Click ‘OK’ to save the settings.

6.4.17.4 Switch configuration

As described in Section 6.4.17.1, switch device is connected with ‘LAN Ethernet’ device. Therefore, you must properly set up switch configuration according to ‘LAN Ethernet’ settings. First of all, you should find ‘LAN Ethernet’ page for switch settings. You can find the page in ‘Network Connections’ of ‘System’. Click ‘System’ on top of menu and ‘Network Connections’. The following screen appears.

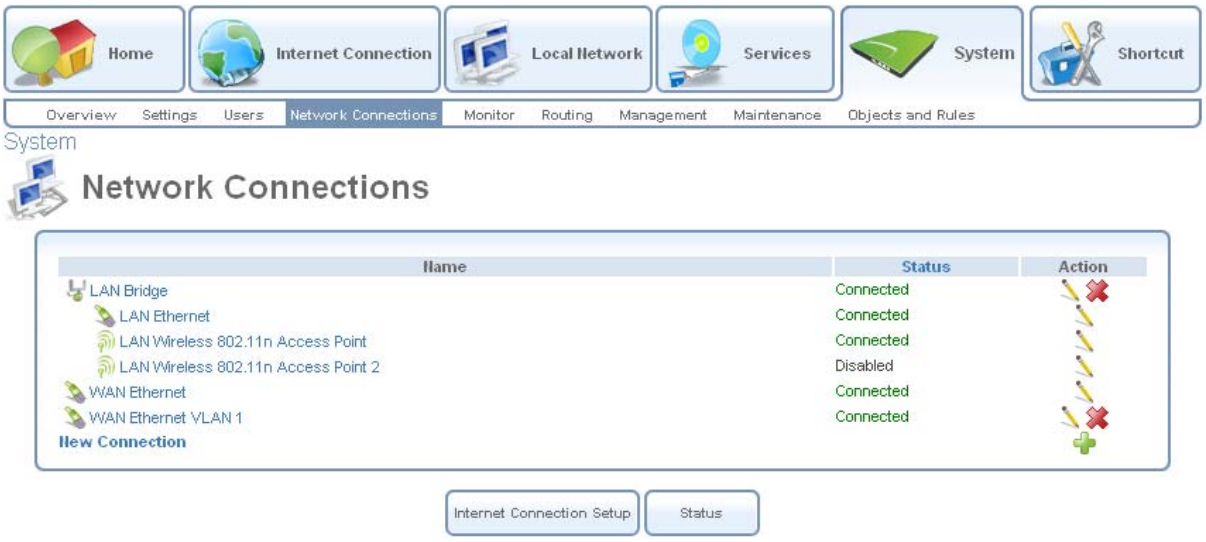


Figure 6.221 Network Connections list

Click the ‘LAN Ethernet’ link and select ‘Switch’. The following screen appears.

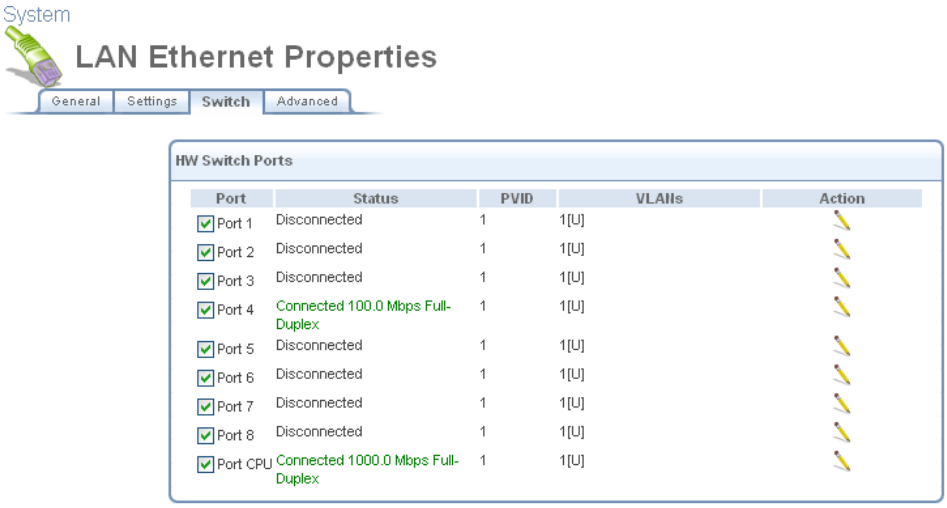


Figure 6.222 Switch Ports Properties

You can see switch ports information such as status, PVID and VLANs with egress policy([U] is egress untagged and [T] is egress tagged sign.) Click the action icon that corresponds to the port you would like to configure. The 'Port Settings' screen appears.

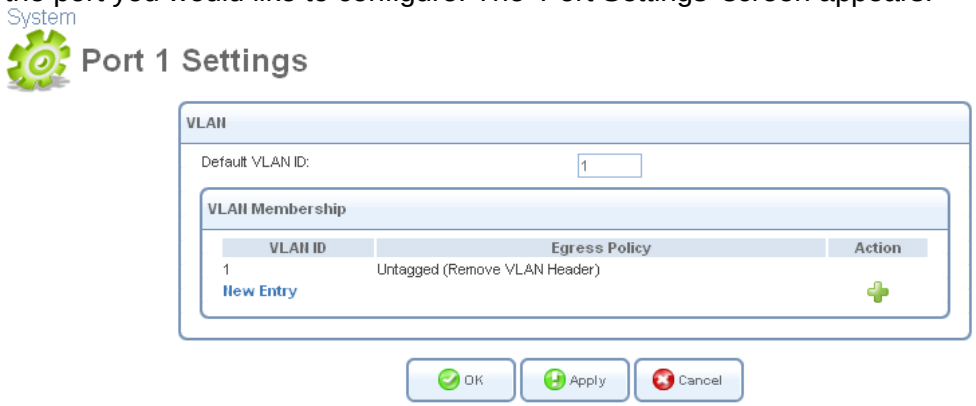


Figure 6.223 Switch port Settings

Enter an ID of the VLAN used for default VLAN. The incoming (ingress) untagged frames will be forwarded according to this ID. And the incoming tagged frames with this ID will be forwarded. If you would like to add more VLAN IDs to this port, click 'New Entry' link. The 'Add Port to a VLAN' screen appears.

Figure 6.223 VLAN settings per port

Enter an ID you want. And from the 'Egress Policy' drop-down menu, select the 'Untagged' or 'Tagged'. The 'Untagged' is action that VLAN header will be removed from egress packets if the packets have VLAN header. On the contrary, the 'Tagged' is action that VLAN header will be

added to egress packets with the VLAN ID.
Click ‘OK’ to save the settings. iPECS SBG-1000 will request browser reloading.

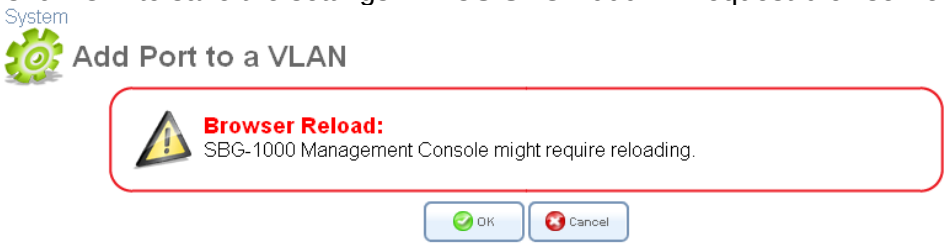


Figure 6.224 VLAN Settings – Browser Reloading

Click ‘OK’ to proceed. After the ‘Port Settings’ screen is back, the added VLAN ID appears in the VLAN ID entries table.

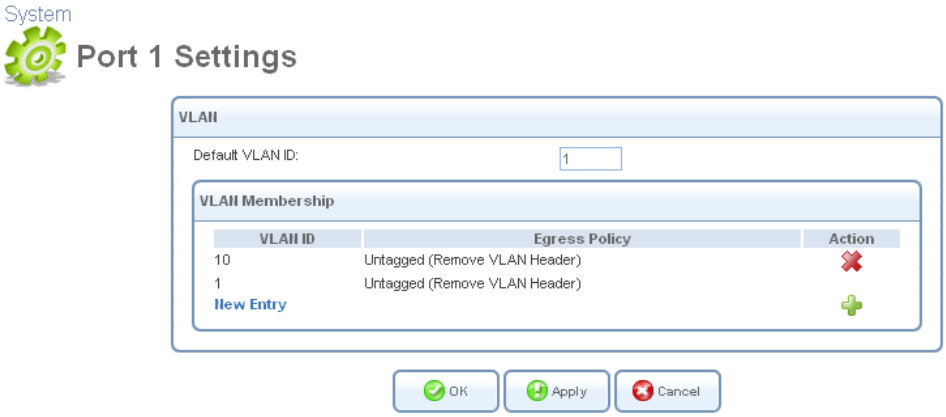


Figure 6.225 Switch port Settings

Click ‘OK’ to proceed. You are redirected back to the ‘LAN Ethernet Properties’ screen, in which the configured port’s VLAN ID is displayed.

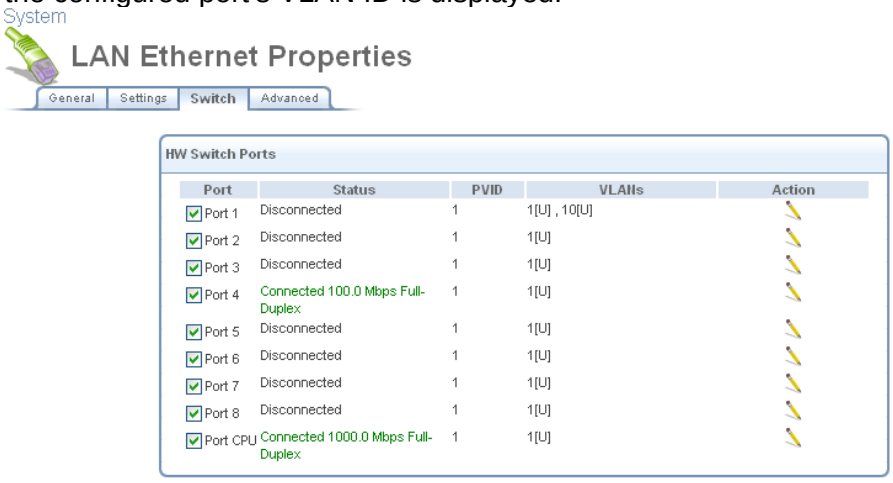


Figure 6.226 Switch Ports Properties

You can see added VLAN ID from the table. If you would like to add more VLAN ID to any ports, try again from Section 6.4.17.2. ***Especially ‘Port CPU’ must be set properly for connection on the WAN side hosts or devices because the port is connected with CPU (including WAN).***

6.4.17.5 VLAN Use Case

iPECS SBG-1000 enables you to partition an Ethernet-based network by creating segregated virtual networks. You can divide LAN ports per VLAN and insert VLAN header to egress packets. WAN also. In this Section, how to configure VLAN is described per case.

6.4.17.5.1 How to use VLAN tag on WAN device

If you would like to add VLAN header to egress packets and handle ingress packets with VLAN header like below figure, perform these following steps. This procedure was described based on default configuration.

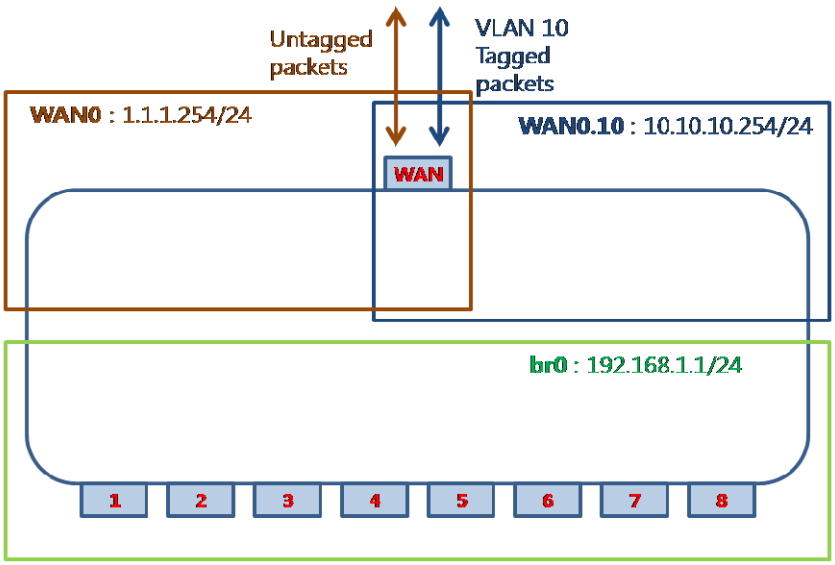


Figure 6.227 VLAN tagging use case on WAN

Create new VLAN interface on WAN with VLAN ID 10 and set IP address to 10.10.10.1/24. Refer to Section 6.4.17.2 Creating a VLAN Interface. In the ‘Network Connections’ screen under ‘System’ (see Figure 6.11), click the ‘New Connection’ link. The ‘Connection Wizard’ screen appears (see Figure 6.12). Select the ‘Advanced Connection’ radio button and click ‘Next’. The ‘Advanced Connection’ screen appears. Select the ‘VLAN Interface’ radio button and click ‘Next’. The ‘VLAN Interface’ screen appears.

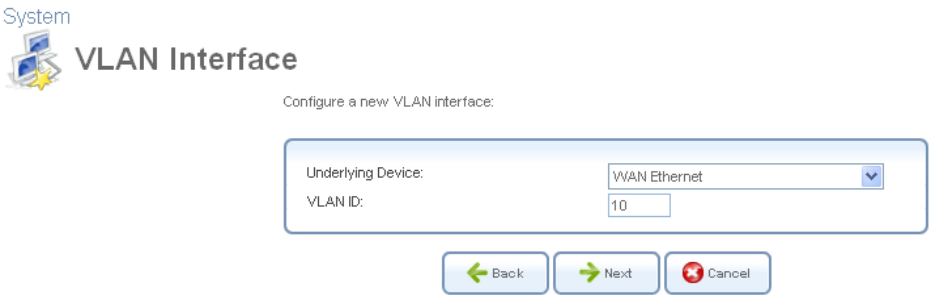


Figure 6.228 VLAN Interface setting

Enter a value that will serve as the VLAN ID, and click ‘Next’. The following screen appears.

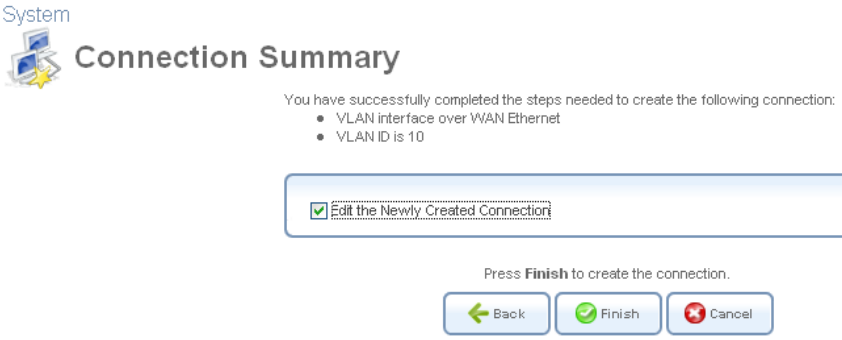


Figure 6.229 Connection Summary

Select the 'Edit the Newly Created Connection' check box for editing IP Address. Click 'Finish' to save the settings. The following screen appears.

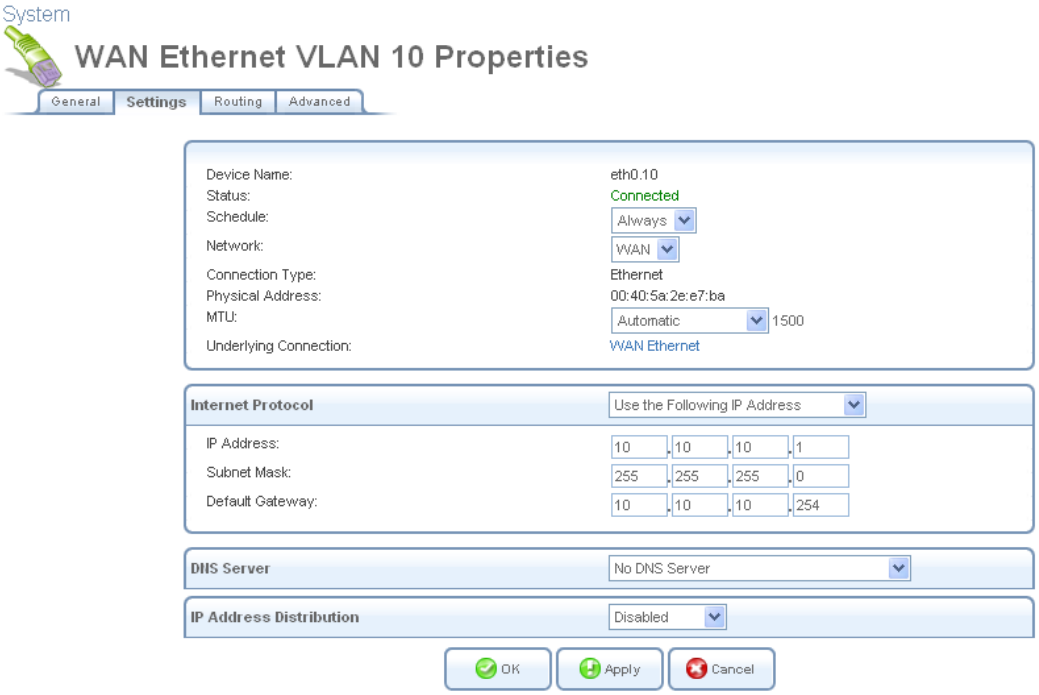


Figure 6.230 WAN Ethernet VLAN Properties

Select 'Use the Following IP Address' from the 'Internet Protocol' drop-down menu. If you have DHCP server using VLAN ID 10 on the WAN side, select 'Obtain an IP Address Automatically' if you want. And fill 'Internet Protocol' contents. Click 'OK' to save the settings. The following screen appears. Refer to Section 6.4.17.3 (Viewing and Editing the VLAN Interface Settings) for detailed information.

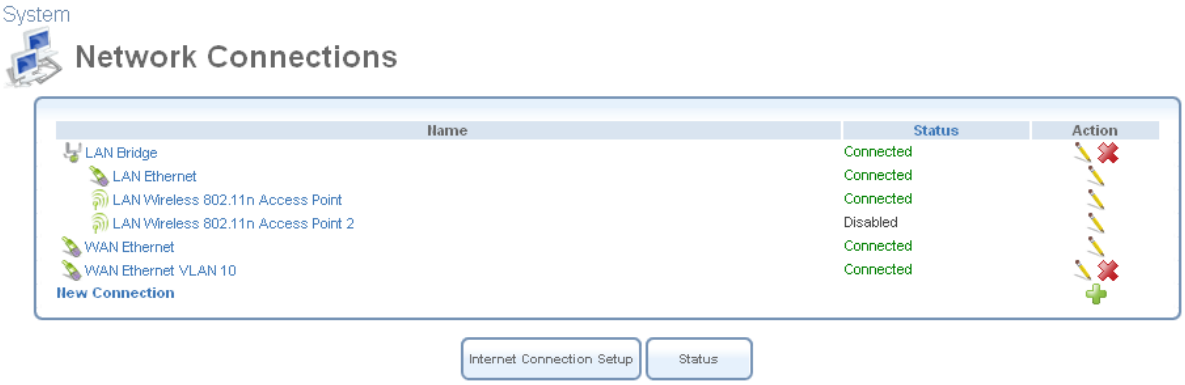


Figure 6.231 Network Connection list

You can see new interface 'WAN Ethernet VLAN 10'. When SIP (source IP) of packets is included 10.10.10.0/24, those packets will be transmitted via WAN with VLAN ID 10. And when DIP (destination IP) of packets belonging to 10.10.10.0/24 is received from WAN, WAN will check VLAN ID. If the packet doesn't have VLAN ID 10, the packet will be discarded.

6.4.17.5.2 How to divide LAN ports in two VLAN

If you would like to divide LAN ports into two VLAN like below figure, perform these following steps. This example is started from Section Section 6.4.17.5.1 'How to use VLAN tag on WAN device'. If you don't want VLAN interface on the WAN side, you can ignore interface WAN0.10 configuration.

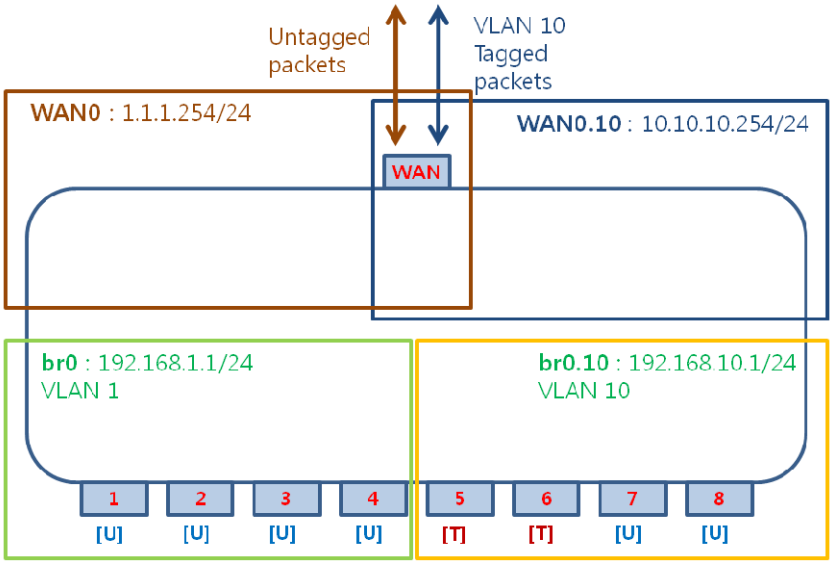


Figure 6.232 Dividing LAN ports use case

Create new VLAN interface on 'LAN Bridge' with VLAN ID 10 and set IP address 192.168.10.1/24.

Refer to Section 6.4.17.2 Creating a VLAN Interface. In the 'Network Connections' screen under 'System' (see Figure 6.11), click the 'New Connection' link. The 'Connection Wizard' screen appears (see Figure 6.12). Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears. Select the 'VLAN Interface' radio button and click 'Next'. The 'VLAN Interface' screen appears.

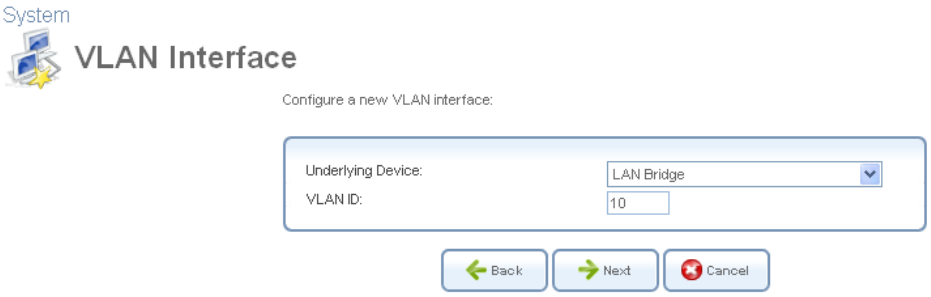


Figure 6.233 VLAN Interface setting

Enter a value that will serve as the VLAN ID, and click ‘Next’. The following screen appears.

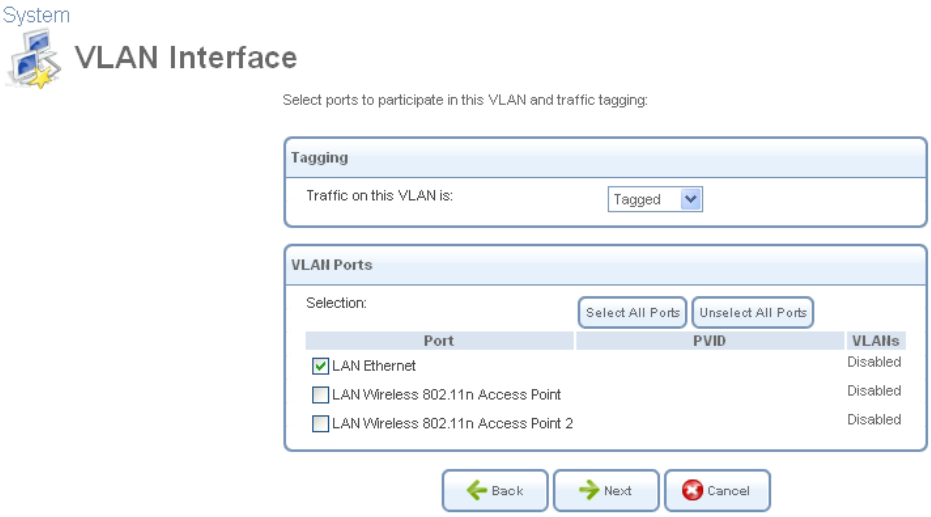


Figure 6.234 VLAN over LAN Bridge

Select ‘Tagged’ from ‘Traffic on this VLAN is’ and select ‘LAN Ethernet’ check box. These settings make tagged interface on the LAN side of CPU. The egress packets to ‘LAN Ethernet’ will be tagged VLAN header with VLAN ID 10.
If you select ‘Untagged’ and ‘LAN Ethernet’ when Default Bridge (br0) is exist, the ingress untagged packets will be handled by this VLAN interface. Therefore the interface br0 will not handle the untagged packets any more.

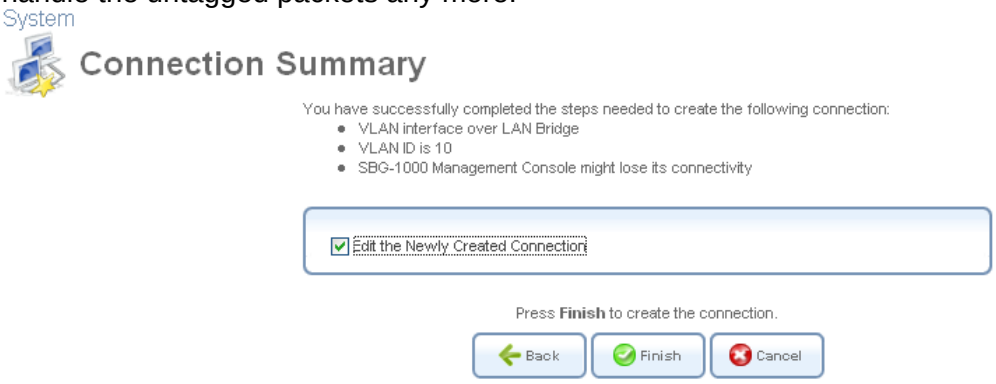


Figure 6.235 Connection Summary

Select the ‘Edit the Newly Created Connection’ check box for editing IP Address. Click ‘Finish’ to

save the settings.

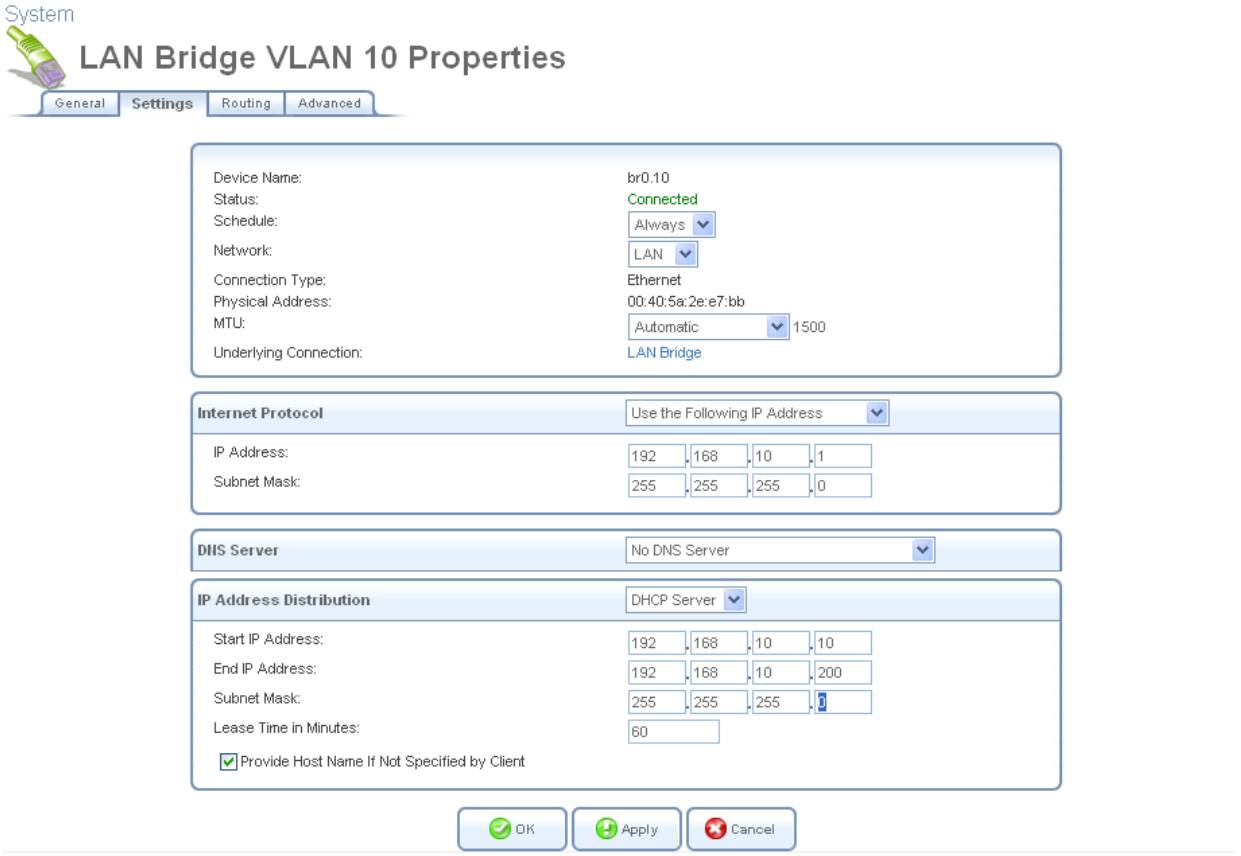


Figure 6.236 LAN Bridge VLAN 10 Properties

Edit ‘Internet Protocol’ properly. And set ‘IP Address Distribution’ if you need. Click ‘OK’ to save the settings.

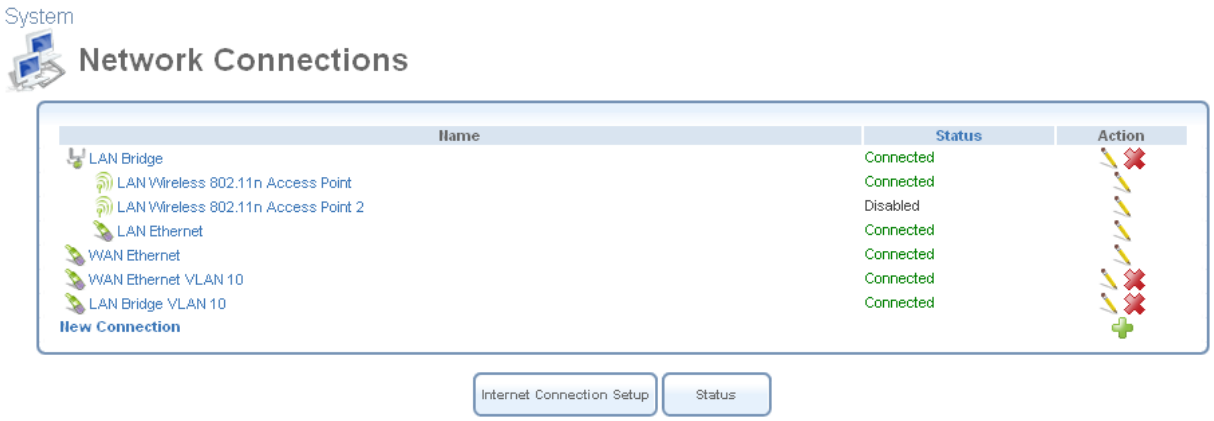


Figure 6.237 Network Connections after Settings

You can see new ‘LAN Bridge VLAN 10’ interface. If you would like to change settings, click and edit. The next step is ‘Switch’ configuration. As described above, when you want to use ‘LAN Bridge’ for tagged port, you must configure ‘Switch’ settings.

Refer to Section 6.4.17.4 Switch configuration. In the ‘Network Connections’ screen under ‘System’, click the ‘LAN Ethernet’ link. The ‘LAN Ethernet Properties’ screen appears. Select the ‘Switch’ tab. The ‘HW Switch Ports’ screen appears.

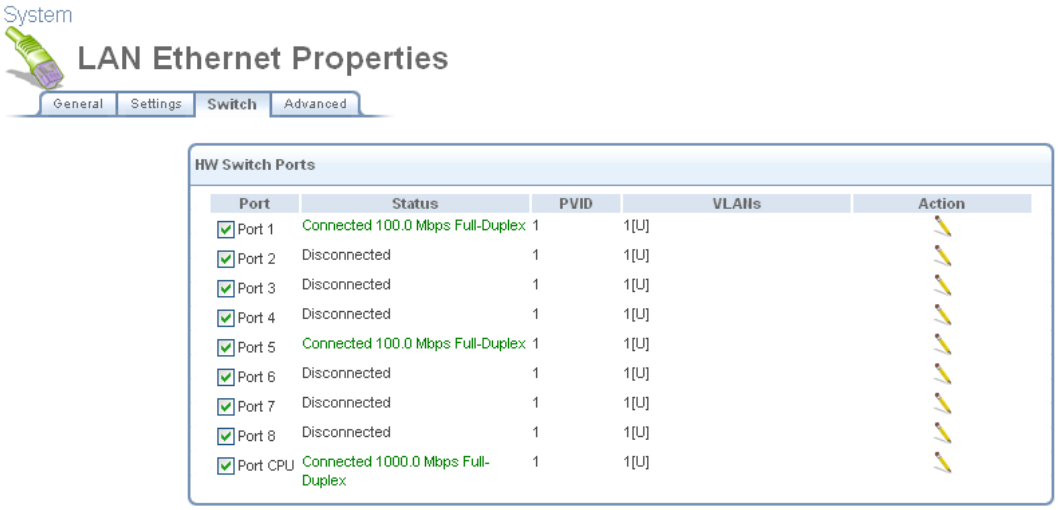


Figure 6.238 Switch tab of LAN Ethernet Properties

The switch ports 1-4 will not be changed because they belong to the default bridge (br0). The ports 5-8 must be changed to VLAN ID 10 and be set ‘Tagged’ or ‘Untagged’ port if you want egress packets to tag VLAN header with ID 10. Finally, you must configure ‘Port CPU’. The ‘Port CPU’ is connected with ‘LAN Bridge VLAN 10’. The egress packets to ‘LAN Bridge VLAN 10’ must have VLAN header with ID 10 to handle by the interface. If the egress packets have no VLAN ID (untagged), the packets will be handled by the default bridge (br0). Click of ‘Port CPU’ to edit VLAN ID. The following screen appears.

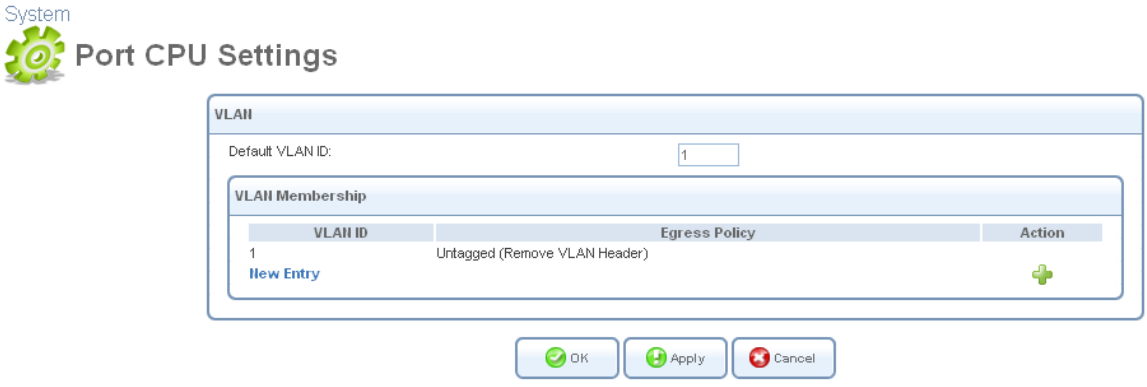


Figure 6.239 LAN Switch Port CPU Settings

In this case, ‘Default VLAN ID’ will be used ‘1’. Click ‘New Entry’ to add port to a VLAN. The ‘Add Port to a VLAN’ screen appears.

Figure 6.240 VLAN settings per port

Edit ‘VLAN ID’ to 10 and select ‘Tagged’ from ‘Egress Policy’ drop-down menu. And click ‘OK’. iPECS SBG-1000 will request browser reloading.

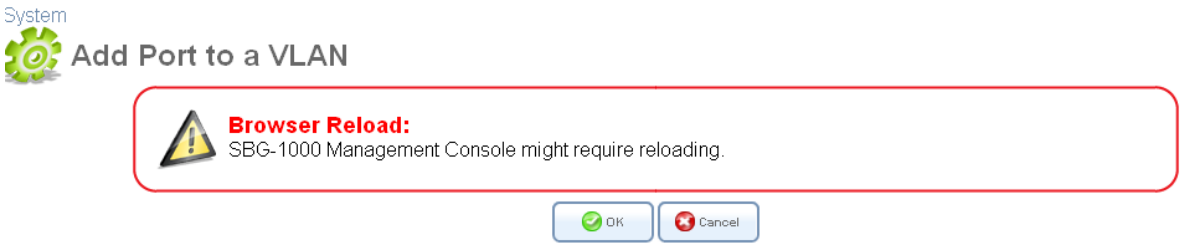


Figure 6.241 VLAN Settings – Browser Reloading

Click ‘OK’ to proceed. After the ‘Port CPU Settings’ screen is back, the added VLAN ID appears in the VLAN ID entries table.

Figure 6.242 LAN Switch Port CPU Settings

Click ‘OK’ to proceed. You are redirected back to the ‘LAN Ethernet Properties’ screen after ‘Browser Reload’ screen.

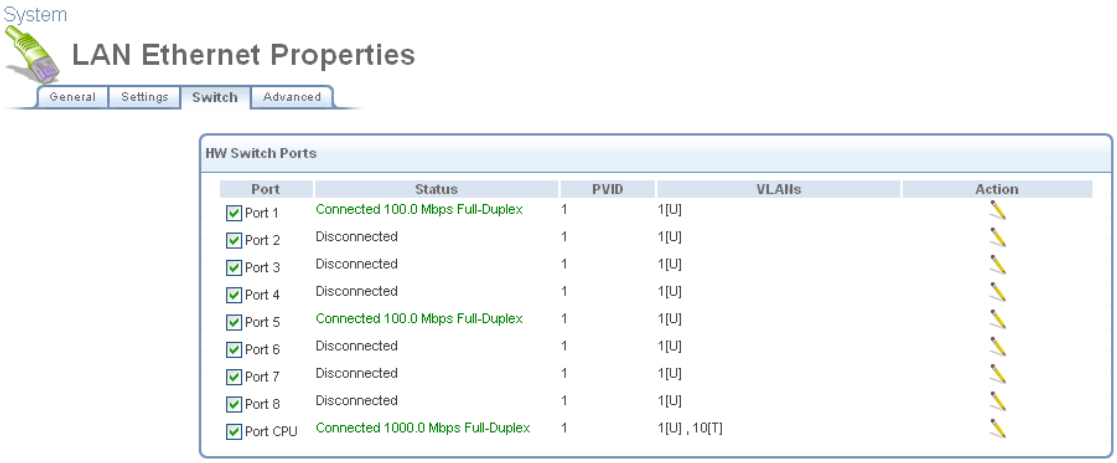


Figure 6.243 Switch tab of LAN Ethernet Properties

You can see added VLAN ID from the table. The egress packets to 'CPU' will be tagged VLAN header with VLAN ID 10. And click  of 'Port 5' to edit VLAN ID. The following screen appears.

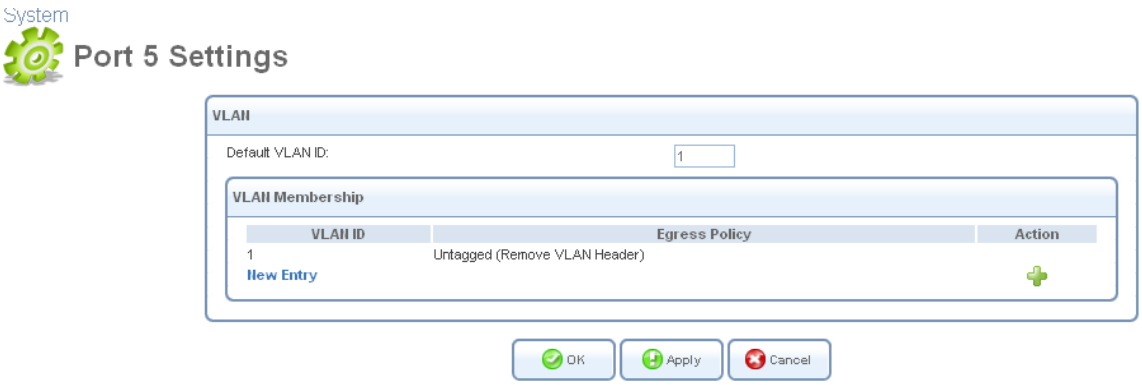


Figure 6.244 LAN Switch Port 5 Settings

Change 'Default VLAN ID' value from 1 to 10. Click 'OK' to save the settings. iPECS SBG-1000 will request browser reloading.

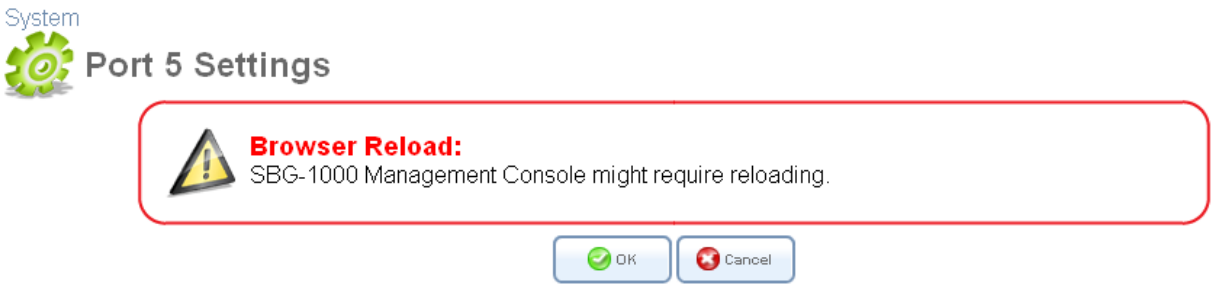


Figure 6.245 LAN Switch Port 5 Settings – Browser Reloading

Click 'OK'. The following screen appears.

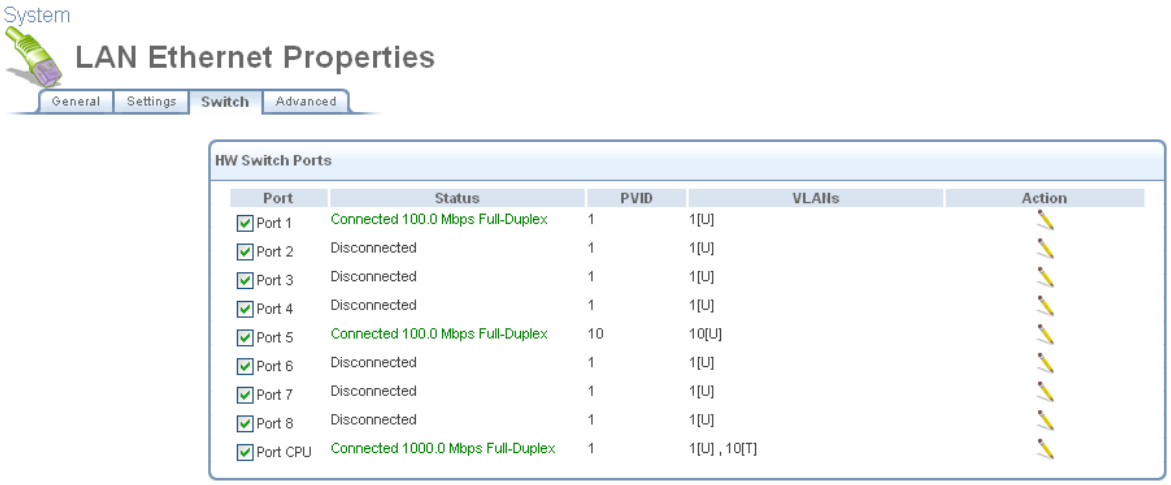


Figure 6.246 Switch tab of LAN Ethernet Properties

The ‘Port 5’ was set to VLAN 10. The ingress packets from ‘Port 5’ will be forwarded to VLAN ID 10 membership ports such as ‘Port CPU’. The egress packets will be transmitted with no VLAN header. If you want to attach VLAN header to egress packets, configure the port to tagged port. Click and ‘New Entry’. The following screen appears.

Figure 6.247 VLAN settings per port

Edit ‘VLAN ID’ to 10 and select ‘Tagged’ from ‘Egress Policy’ drop-down menu. And click ‘OK’. You are redirected back to the ‘Port 7 Settings’ screen after ‘Browser Reload’ screen

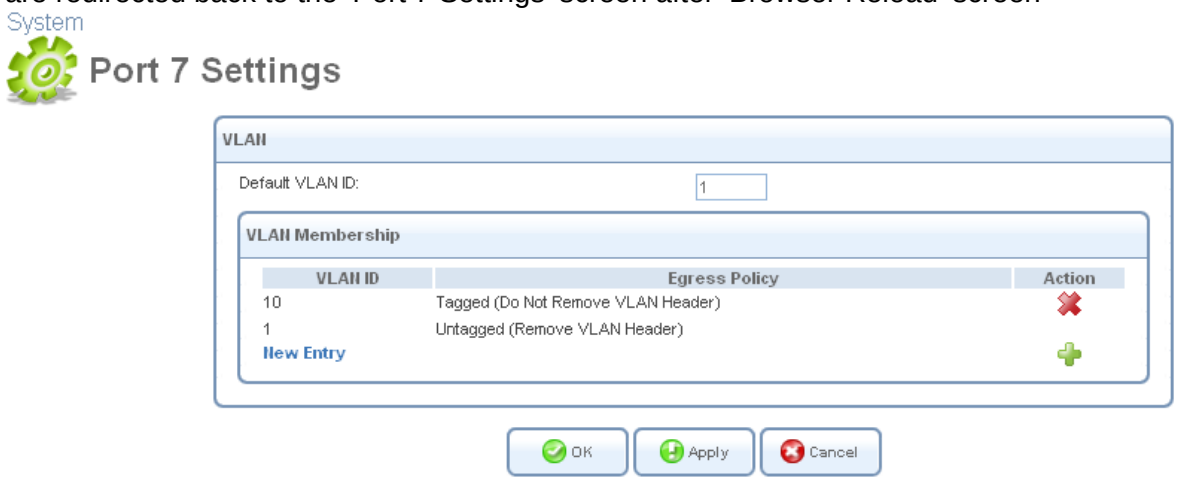


Figure 6.248 Switch port Settings

Click ‘OK’ to proceed. You are redirected back to the ‘LAN Ethernet Properties’ screen after ‘Browser Reload’ screen.

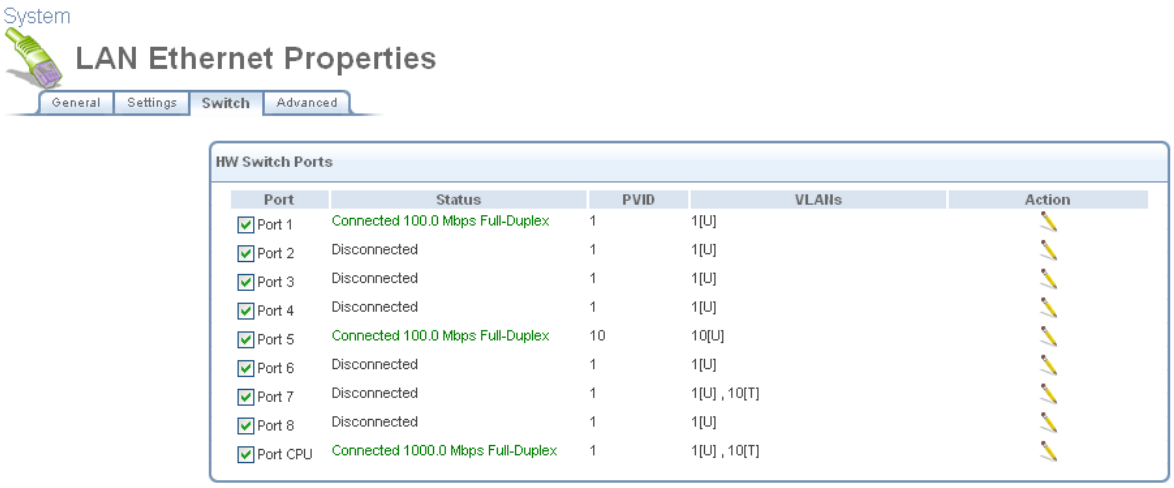


Figure 6.249 Switch tab of LAN Ethernet Properties

The ‘Port 7’ was set to VLAN 10. The ingress packets with VLAN ID 10 from ‘Port 5’ will be forwarded to VLAN ID 10 membership ports such as ‘Port 5’ and ‘Port CPU’. The egress packets will be transmitted with VLAN header VLAN ID 10 if the packets are included VLAN membership 10. If the ingress packets with no VLAN header, they will be handled by VLAN 1.

6.4.17.5.3 How to use VLAN on LAN Bridge

If you would like to create VLAN interface on LAN Bridge with WAN like below figure, perform these following steps.

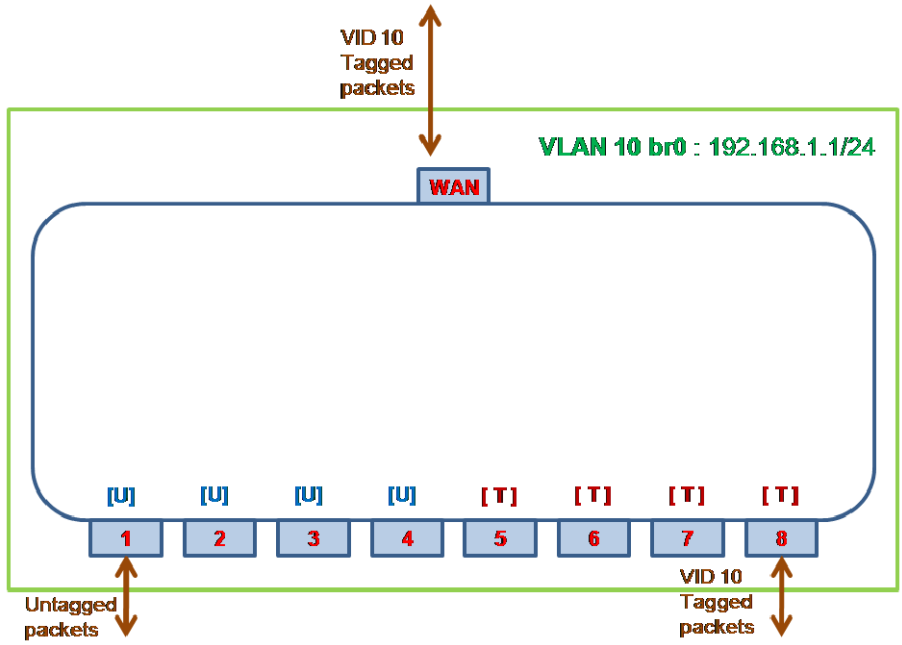


Figure 6.250 Example of LAN Bridge VLAN

First, you must insert ‘WAN Ethernet’ to LAN Bridge. Refer to Section 6.4.14 Setting up a WAN-LAN Bridge. In the ‘Network’ Connections’ screen under ‘System’, click ‘LAN Bridge’ and ‘Bridging’. The ‘LAN Bridge Properties’ screen appears. You must check ‘WAM Ethernet’ to insert to ‘LAN Bridge’. Click ‘Apply’. The following screen appears.

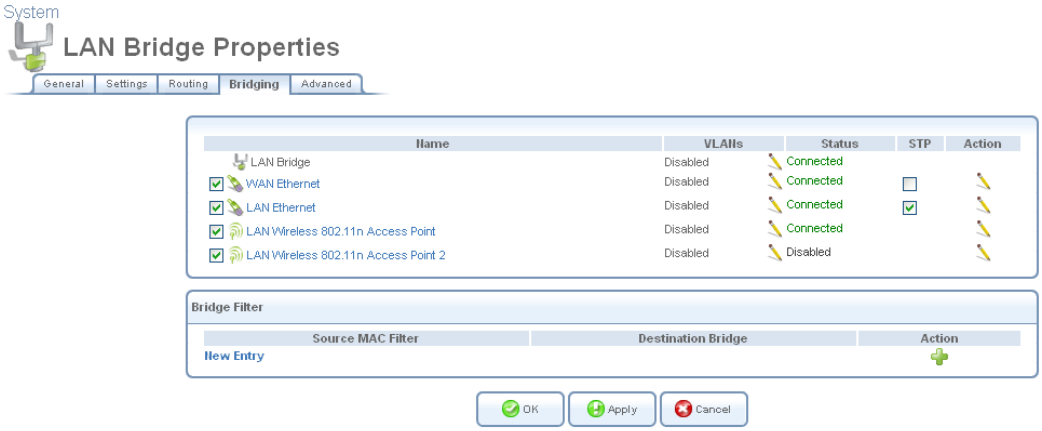


Figure 6.251 Bridging tab of LAN Bridge Properties

Refer to Section 6.4.17.2 Creating a VLAN Interface. In the ‘Network Connections’ screen under ‘System’ (see Figure 6.11), click the ‘New Connection’ link. The ‘Connection Wizard’ screen appears (see Figure 6.12). Select the ‘Advanced Connection’ radio button and click ‘Next’. The ‘Advanced Connection’ screen appears. Select the ‘VLAN Interface’ radio button and click ‘Next’. The ‘VLAN Interface’ screen appears.

Figure 6.252 VLAN Interface setting

Enter a value that will serve as the VLAN ID, and click ‘Next’. The following screen appears.

Figure 6.253 VLAN over LAN Bridge

Select ‘Tagged’ from ‘Tagging’ menu and select ‘LAN Ethernet and WAN Ethernet’ from ‘VLAN Ports’ menu. Click ‘Next’. The following screen appears.

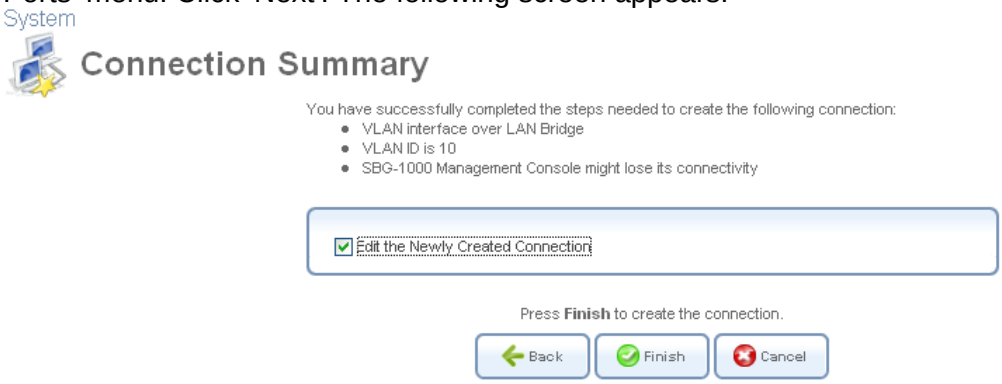


Figure 6.254 Connection Summary

Select the ‘Edit the Newly Created Connection’ check box for editing IP Address. Click ‘Finish’ to save the settings.

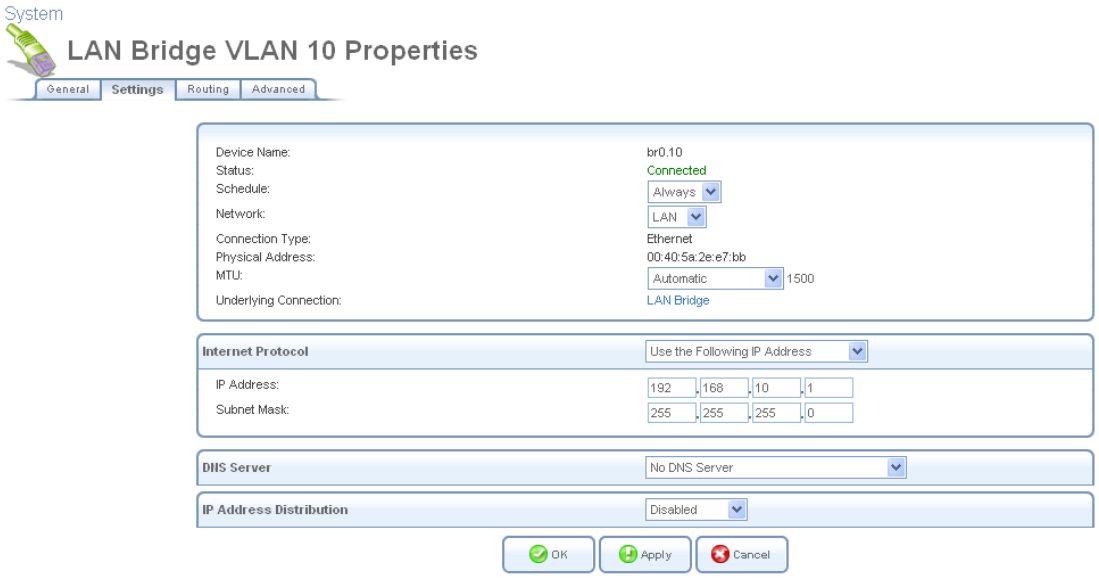


Figure 6.255 LAN Bridge VLAN 10 Properties

Edit ‘Internet Protocol’ properly and click ‘OK’ to save the settings.

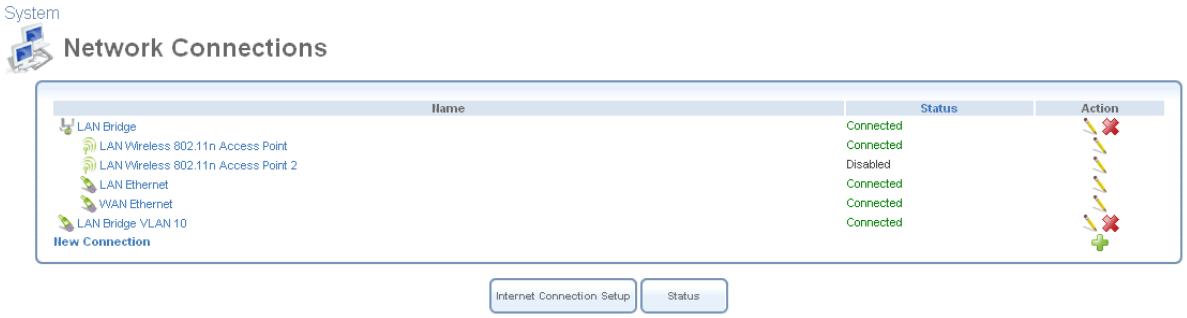


Figure 6.256 Network Connections after Settings

The next step is ‘Switch’ configuration. As described above, when you want to use ‘LAN Bridge’ for tagged port, you must configure ‘Switch’ settings.
Refer to Section 6.4.17.4 Switch configuration. In the ‘Network Connections’ screen under ‘System’, click the ‘LAN Ethernet’ link. The ‘LAN Ethernet Properties’ screen appears. Select the ‘Switch’ tab. The ‘HW Switch Ports’ screen appears.

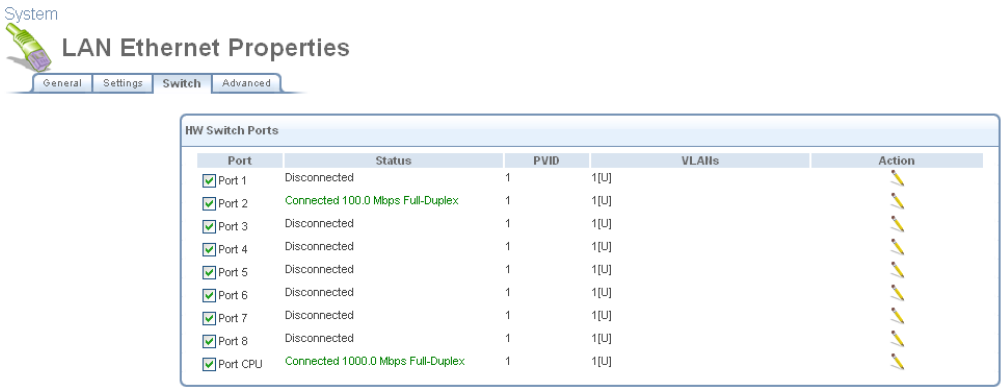


Figure 6.257 Switch tab of LAN Ethernet Properties

The switch ports 1-4 will be used untagged port with VLAN ID 10. The ports 5-8 must be changed to VLAN ID 10 and be set ‘Tagged’ port. Finally, you must configure ‘Port CPU’. The ‘Port CPU’ is connected with ‘LAN Bridge VLAN 10’. The egress packets to ‘LAN Bridge VLAN 10’ must have VLAN header with ID 10 to handle by the interface. Click of ‘Port CPU’ to edit VLAN ID. The following screen appears.

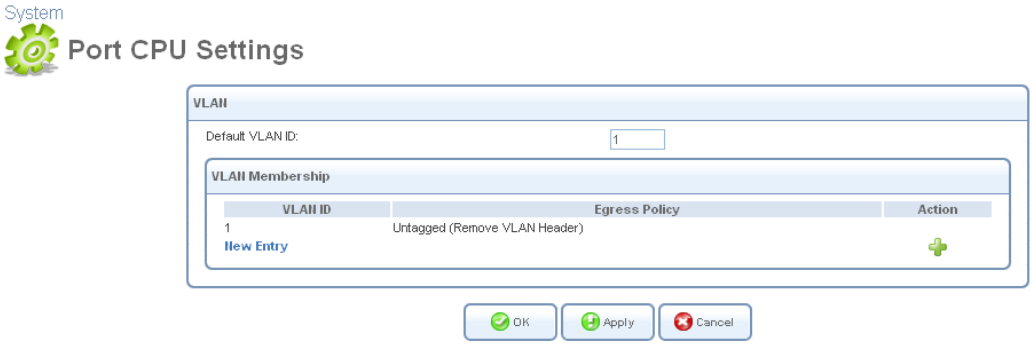


Figure 6.258 LAN Switch Port CPU Settings

In this case, ‘Default VLAN ID’ will be used ‘1’. Click ‘New Entry’ to add port to a VLAN. The ‘Add Port to a VLAN’ screen appears.

Figure 6.259 VLAN settings per port

Edit ‘VLAN ID’ to 10 and select ‘Tagged’ from ‘Egress Policy’ drop-down menu. And click ‘OK’. iPECS SBG-1000 will request browser reloading.

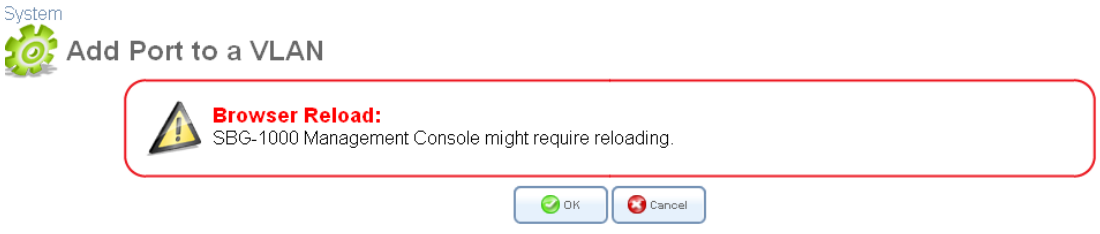


Figure 6.260 VLAN Settings – Browser Reloading

Click ‘OK’ to proceed. After the ‘Port CPU Settings’ screen is back, the added VLAN ID appears in the VLAN ID entries table.

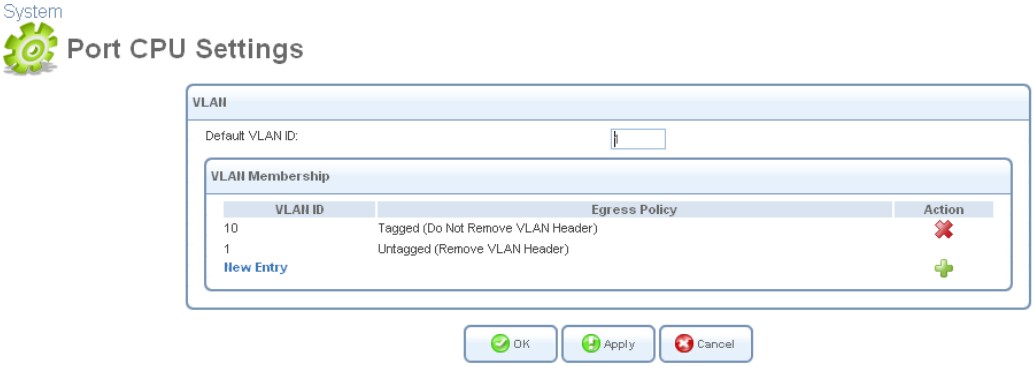


Figure 6.261 Switch port Settings

Click ‘OK’ to proceed. You are redirected back to the ‘LAN Ethernet Properties’ screen after ‘Browser Reload’ screen.

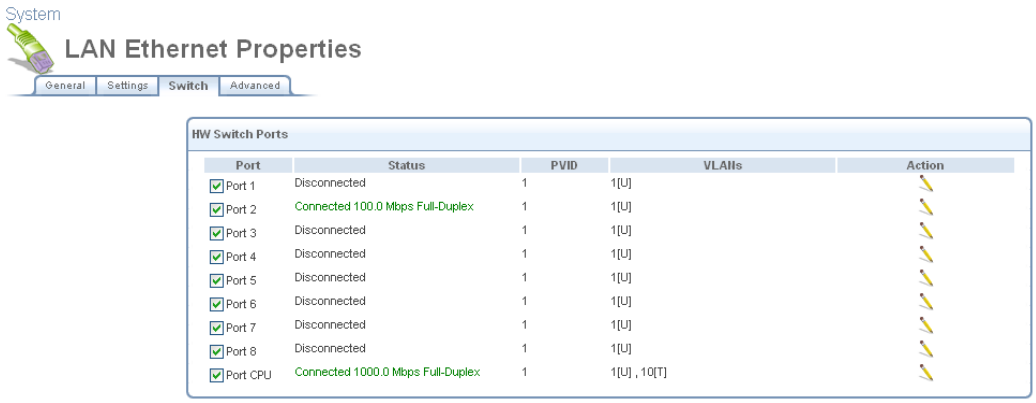


Figure 6.262 Switch Ports Properties

You can see added VLAN ID from the table. The egress packets to ‘CPU’ will be tagged VLAN header with VLAN ID 10. And click  of ‘Port 1’ to edit PVID. The following screen appears.

Figure 6.263 Switch port Settings

Edit ‘Default VLAN ID’ to 10 for changing PVID and click ‘OK’ to save.

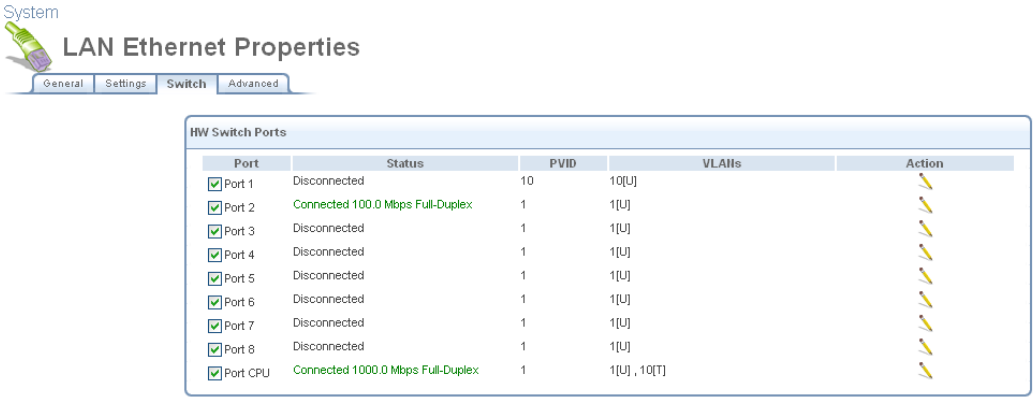


Figure 6.264 Switch Ports Properties

You can see added VLAN ID from the table. The egress packets to 'Port 1' will be untagged. Repeat to 'Port 4'. And click  of 'Port 5' and 'New Entry' to set tagging port. The following screen appears.

Figure 6.265 VLAN settings per port

Edit 'VLAN ID' to 10 and select 'Tagged' from 'Egress Policy' drop-down menu. And click 'OK'. You are redirected back to the 'Port 5 Settings' screen after 'Browser Reload' screen

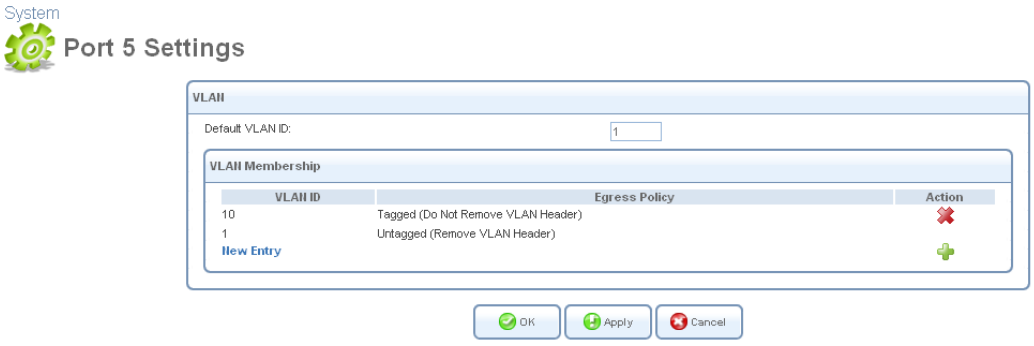


Figure 6.266 Switch port Settings

Click 'OK' to proceed. You are redirected back to the 'LAN Ethernet Properties' screen after 'Browser Reload' screen.

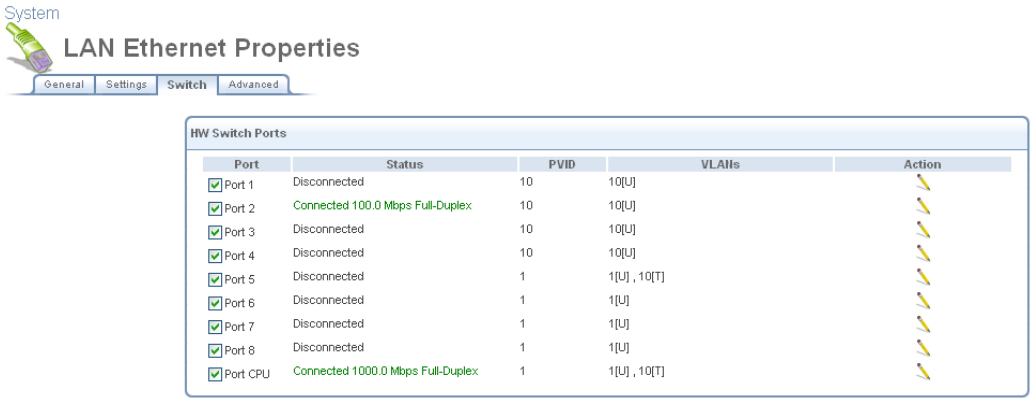


Figure 6.267 Switch Ports Properties

You can see added VLAN ID from the table. The egress packets to 'Port 8' will be tagged VLAN header with VLAN ID 10. Repeat to 'Port 8'.

6.5 Monitor

6.5.1 Monitoring Your Network Connections

The 'Network Connections' screen displays a table summarizing the monitored connection data (see Figure 6.268). iPECS SBG-1000 constantly monitors traffic within the local network and between the local network and the Internet. You can view statistical information about data received from and transmitted to the Internet (WAN) and to computers in the local network (LAN).

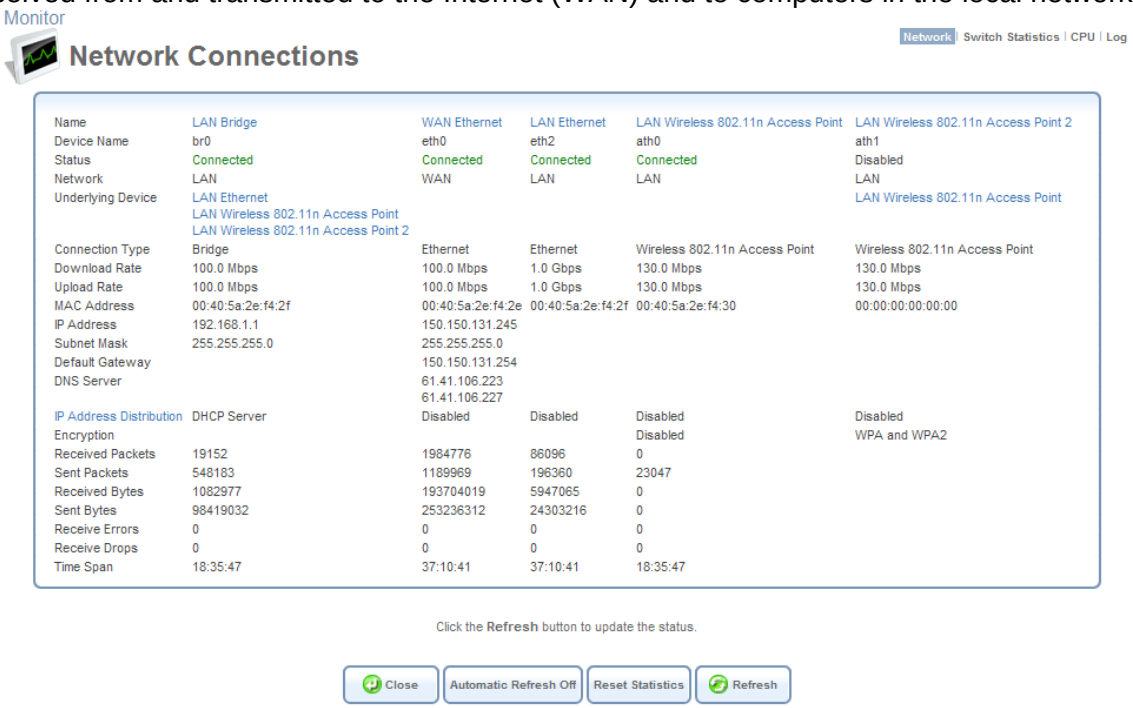


Figure 6.268 Monitoring Connections

Click the 'Refresh' button to update the display, or the 'Automatic Refresh On' button to constantly update the displayed parameters.

6.5.2 Monitoring the CPU Load

Click the ‘CPU’ link in the links bar to view the gateway’s CPU status. The ‘CPU’ screen displays a real-time report about the CPU’s status and load.

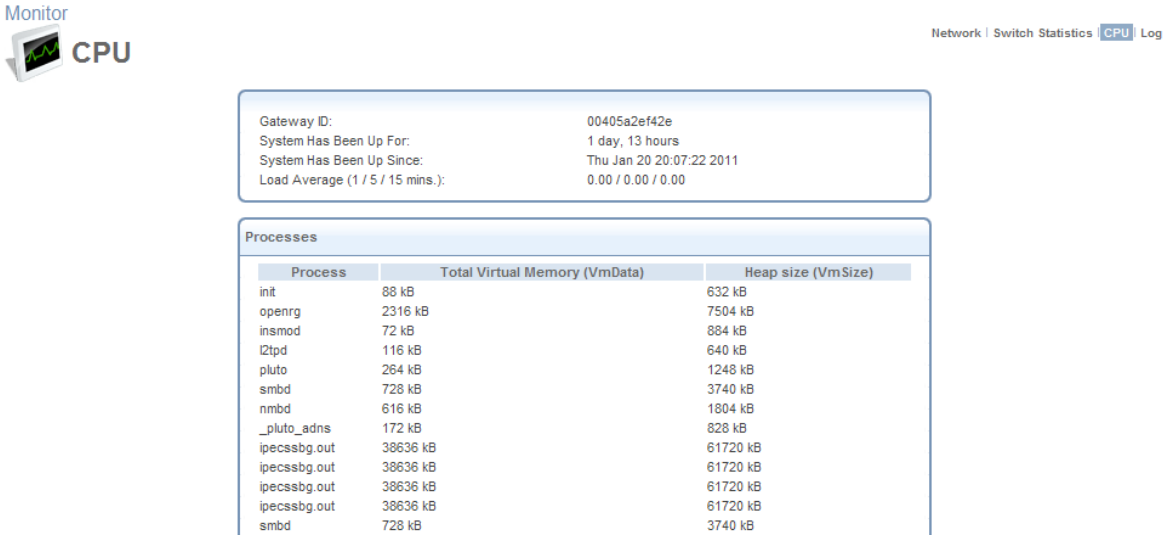


Figure 6.269 CPU Monitoring

System Has Been Up For The amount of time that has passed since the system was last started.

Load Average (1 / 5 / 15 mins.) The average number of processes that are either in a runnable or uninterruptible state. A process in the runnable state is either using the CPU or waiting to use the CPU. A process in the uninterruptible state is waiting for I/O access, e.g. waiting for the disk. The averages are taken over the three time intervals. The meaning of the load average value varies according to the number of CPUs in the system. This means for example, that a load average of 1 on a single-CPU system means that the CPU was loaded all the time, while on a 4-CPU system this means that the CPU was idle 75% of the time.

Processes A list of processes currently running on iPECS SBG-1000, and their virtual memory usage. The amount of memory granted for each process is presented with the help of the following parameters:

- **Total Virtual Memory (VmData)** The amount of memory currently utilized by the running process.

- **Heap size (VmSize)** The total amount of memory allocated for the running process.

Note: Some processes have several child processes. The child processes may be displayed under the same name as the parent one, and use the same memory address space.

This screen is automatically refreshed by default, though you may change this by clicking ‘Automatic Refresh Off’.

6.5.3 Viewing the System Log

Click the ‘Log’ link in the links bar to view your system’s log. The ‘System Log’ screen displays a list of recent activities that has taken place on iPECS SBG-1000.

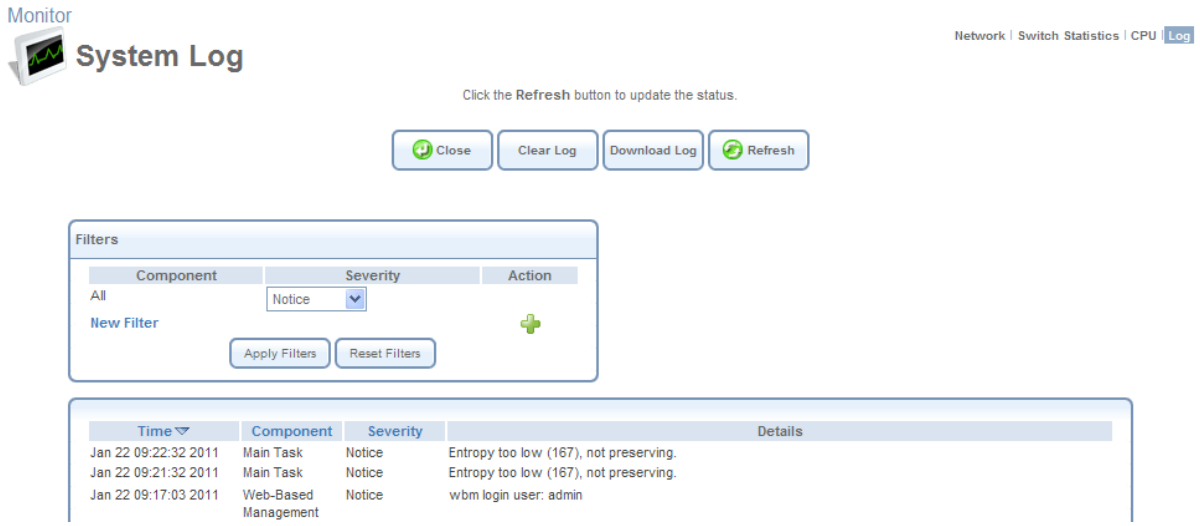


Figure 6.270 System Log

Use the buttons at the top of the page to:
Close Close the ‘Log’ screen and return to iPECS SBG-1000’s home page.
Clear Log Clear all currently displayed log messages.
Download Log Download the log as a Comma Separated Value (CSV) file, named **sbg-1000_log.csv**.
Refresh Refresh the screen to display the latest updated log messages.
By default, all log messages are displayed one after another, sorted by their order of posting by the system (newest on top). You can sort the messages according to the column titles—Time, Component, or Severity. This screen also enables you to filter the log messages by the component that generated them, or by their severity, providing a more refined list. This ability is useful mainly for software developers debugging iPECS SBG-1000.

By default, the screen displays log messages with ‘debug’ severity level and higher, for all components (see default filter in Figure 6.270). You may change the severity level for this filter. To add a new filter, click the ‘New Filter’ link or its corresponding action icon. The screen refreshes.

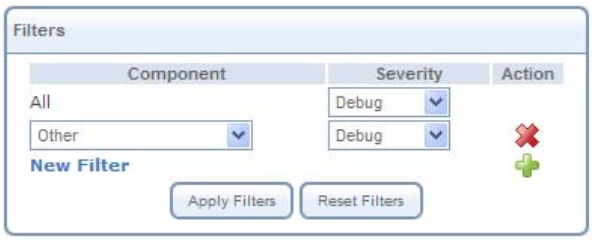


Figure 6.271 System Log Filters

Using the drop-down menus, select the component and severity level by which to sort the log messages. Click ‘Apply Filters’ to display the messages in your specified criteria. You can add more filters in the same way, or delete filters using their respective action icons. Defined filters override the default filter that displays all messages.

Note: Clicking “Reset Filters” deletes all the defined filters without a warning.

Note that if you would like to view iPECS SBG-1000’s system log in your host’s command prompt, you must install and run the syslog server. Then, configure iPECS SBG-1000 with your host’s IP address as described in Section 6.2.

6.6 Routing

6.6.1 Managing the Routing Table

The ‘Routing’ screen enables you to add, edit, or delete routing rules from iPECS SBG-1000’s routing table.

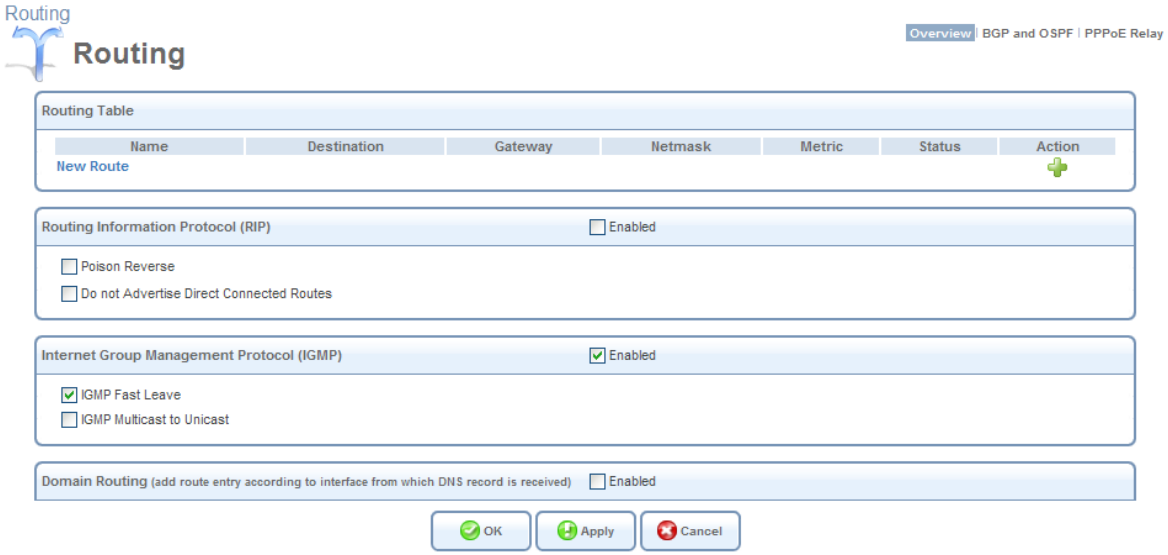


Figure 6.272 Routing

Note that this table only displays routing rules that you define manually using the WBM, and does not display dynamic rules applied by iPECS SBG-1000’s network connection interfaces, such as IPSec, OSPF, RIP, etc..

6.6.1.1 Adding a Routing Rule

To add a routing rule, click the ‘New Route’ link or the action icon. The ‘Route Settings’ screen appears.

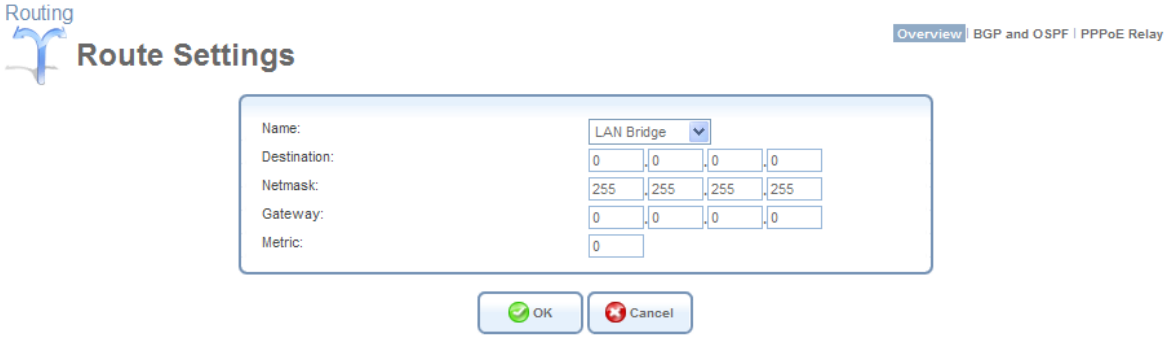


Figure 6.273 Route Settings

Specify the following:

Name Select the network device.

Destination Enter the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.

Netmask The network mask is used in conjunction with the destination to determine when a route is used.

Gateway Enter the gateway's IP address.

Metric A measurement of a route's preference. Typically, the lowest metric is the most preferred route. If multiple routes have the same metric value, the default route will be the first in the order of appearance.

6.6.1.2 Supported Routing Protocols

Routing Information Protocol (RIP) Select this check box in order to enable connections previously defined to use RIP. If this check box is not selected, RIP will be disabled for all connections, including those defined to use RIP.

- **Poison Reverse** iPECS SBG-1000 will advertise acquired route information with a high metric, in order for other routers to disregard it.

- **Do not Advertise** Direct Connected Routes iPECS SBG-1000 will not advertise the route information to the same subnet device from which it was obtained.

Internet Group Management Protocol (IGMP) iPECS SBG-1000 provides support for the IGMP multicasting. When a host sends out a request to join a multicast group, iPECS SBG-1000 will listen and intercept the group's traffic, forwarding it to the subscribed host. iPECS SBG-1000 keeps record of subscribed hosts. When a host requests to cancel its subscription, iPECS SBG-1000 queries for other subscribers and stops forwarding the multicast group's traffic after a short timeout.

- **Enable IGMP Fast Leave** If a host is the only subscriber, iPECS SBG-1000 will stop forwarding traffic to it immediately upon request (there will be no query delay).

- **IGMP Multicast to Unicast** Enables iPECS SBG-1000 to convert the incoming multicast data stream into unicast format, in order to route it to the specific LAN host that had requested the data. In this way, iPECS SBG-1000 will prevent flooding the rest of the LAN hosts with

irrelevant multicast traffic.

Domain Routing When iPECS SBG-1000's DNS server receives a reply from an external DNS server, it will add a routing entry for the IP address of the reply through the device from which it arrived. This means that future packets from this IP address will be routed through the device from which the reply arrived.

6.6.2 BGP and OSPF

The 'BGP and OSPF' feature is an implementation of two routing protocols used to deliver up-to-date routing information to a network or a group of networks, called *Autonomous System*.

Border Gateway Protocol (BGP) The main routing protocol of the Internet. It is used to distribute routing information among Autonomous Systems (for more information, refer to the protocol's RFC at http://www.ietf.org/rfc/rfc1771.txt).

Open Shortest Path First Protocol (OSPF) An Interior Gateway Protocol (IGP) used to distribute routing information within a single Autonomous System (for more information, refer to the protocol's RFC at http://www.ietf.org/rfc/rfc2328.txt).

The feature's routing engine is based on the *Quagga* GNU routing software package. By using the BGP and OSPF protocols, this routing engine enables iPECS SBG-1000 to exchange routing information with other routers within and outside an Autonomous System. To enable this feature, perform the following:

1. In the 'Routing' screen, click the 'BGP and OSPF' link. The 'BGP and OSPF' screen appears.

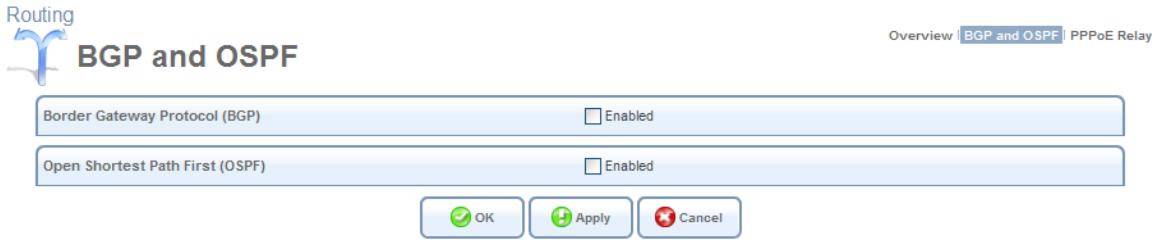


Figure 6.274 BGP and OSPF

Note: Depending on its purpose of use, iPECS SBG-1000 may support both of the protocols or only one of them.

2. Select the 'Enabled' check box of the supported protocol(s). For example, enable OSPF. The screen refreshes, changing to the following.

Figure 6.275 Enabled OSPF

To activate the routing engine, you need to create a configuration file for the protocol daemon, and also for *Zebra*. Zebra is Quagga's IP routing management daemon, which provides kernel routing table updates, interface lookups, and redistribution of routes between the routing protocols.

Note: To view examples of the configuration files, browse to http://www.quagga.net/docs/quagga.pdf.

3. Enter the configuration files into their respective code fields. Alternatively, click the 'Set Default Values' button to the right of each code field. The default values, displayed in a field are the following:

   • **BGP :**
   !router bgp <AS number> The exclamation mark is Quagga's comment character. The router bgp string is a command that activates the BGP daemon. The exclamation mark emphasizes that the command must be followed by an exact Autonomous System's ID number.
   log syslog A command that instructs the daemon to send its log messages to the system log.

   • **OSPF :**
   router ospf A command that activates the OSPF daemon.
   log syslog See the explanation under BGP.

   • **Zebra**
   interface ixp1 Instructs the daemon to query and update routing information via a specific WAN device. It is important that you change the default ixp1 value to your WAN device name.

log syslog See the explanation under BGP.

4. Click ‘OK’ to save the settings.

If the OSPF daemon is activated, iPECS SBG-1000 starts sending the ‘Hello’ packets to other routers to create adjacencies. After determining the shortest path to each of the neighboring routers, Zebra updates the routing table according to the network changes. If the BGP deamon is activated, iPECS SBG-1000 starts to advertise routes it uses to other BGP-enabled network devices located in the neighboring Autonomous System(s). The BGP protocol uses TCP as its transport protocol. Therefore, iPECS SBG-1000 first establishes a TCP connection to routers with which it will communicate. *KeepAlive* messages are sent periodically to ensure the liveness of the connection. When a change in the routing table occurs, iPECS SBG-1000 advertises an *Update* message to its peers. This update message adds a new route or removes the unfeasible one from their routing table.

6.6.3 Enabling PPPoE Relay

PPPoE Relay enables iPECS SBG-1000 to relay packets on PPPoE connections, while keeping its designated functionality for any additional connections. The PPPoE Relay screen (see Figure 6.276) displays a check-box that enables PPPoE Relay.

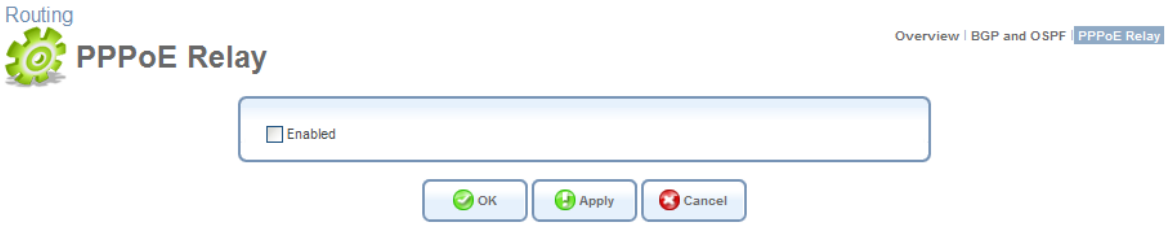


Figure 6.276 PPPoE Relay

6.7 Performing Advanced Management Operations

6.7.1 Utilizing iPECS SBG-1000’s Universal Plug and Play Capabilities

Universal Plug-and-Play (UPnP) is a networking technology that provides compatibility among networking equipment, software, and peripherals. This technology leverages existing standards and technologies, including TCP/IP, HTTP 1.1 and XML, facilitating the incorporation of Universal Plug-and-Play capabilities into a wide range of networked products for the home.
Your gateway is at the forefront of this technology, offering a complete software platform for UPnP devices. This means that any UPnP-enabled LAN device can dynamically join your network, obtain an IP address, and exchange information about its capabilities and those of other devices on your home network. All this happens automatically, providing a truly zero-configuration network.
The most widespread and trivial example of utilizing iPECS SBG-1000’s UPnP feature is connecting a PC to iPECS SBG-1000. If your PC is running an operating system that supports

UPnP, such as Windows XP™, you will only need to connect it to one of the gateway's LAN sockets. The PC is automatically recognized and added to the local network.
Likewise, you can add any other UPnP-enabled device (for example, a media streamer, digital picture frame, etc.) to your home network.

6.7.1.1 Configuring iPECS SBG-1000's UPnP Settings

iPECS SBG-1000's UPnP feature is enabled by default. You can access the UPnP settings from the 'Management' menu item, by clicking the 'Universal Plug and Play' link, or by clicking the 'Universal Plug and Play' icon in the 'Shortcut' screen. The 'Universal Plug and Play' settings screen appears.

Figure 6.277 Universal Plug and Play

Allow Other Network Users to Control iPECS SBG-1000's Network Features Selecting this check-box enables the UPnP feature. This will allow you to define local services on any of the LAN hosts, and to make the services available to computers on the Internet, as described in Section 6.7.1.2.
Enable Automatic Cleanup of Old Unused UPnP Services When this check box is selected, iPECS SBG-1000 periodically checks the availability of the LAN computers that have been configured to provide the local services. In case the DHCP lease granted to such a host has expired and the host does not appear in the ARP table, iPECS SBG-1000 removes the port forwarding rule that enables access to the corresponding local service (for more information about port forwarding rules, refer to Section 5.2.3).
WAN Connection Publication By default, iPECS SBG-1000 will publish only its main WAN connection, which will be controllable by UPnP entities. However, you may select the 'Publish All WAN Connections' option if you wish to grant UPnP control over all of iPECS SBG-1000's WAN connections.

6.7.1.2 Granting Remote Access to Your LAN Services Using UPnP

You may also make the services provided by your LAN computers available to computers on the Internet. For example, you may designate a UPnP-enabled Windows PC in your home network to act as a Web server, allowing computers on the Internet to request pages from it. Another example is a game that you may wish to play with other people over the Internet. Some online games require that specific ports be opened to allow communication between your PC and other online players.

- To make your local services available to computers on the Internet:
  1. On your PC (which provides the service), open the 'Network Connections' window.

2. Right-click ‘Internet Connection’ and choose ‘Properties’. The ‘Internet Connection Properties’ window appears.

Figure 6.278 Internet Connection Properties

3. Click the ‘Settings’ button. The ‘Advanced Settings’ window appears.

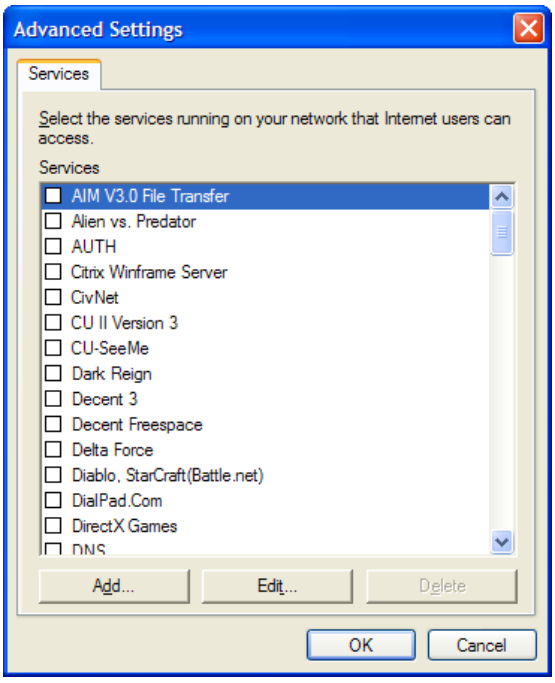


Figure 6.279 Advanced Settings

4. Select a local service that you would like to make available to computers on the Internet. The ‘Service Settings’ window will automatically appear.

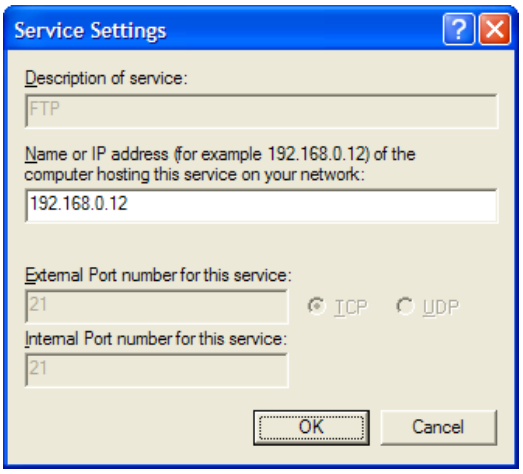


Figure 6.280 Service Settings: Edit Service

5. Enter the PC's local IP address and click 'OK'.

6. Select other services as desired, and repeat the previous step for each.

7. Click 'OK' to save the settings.

- To add a local service that is not listed in the 'Advanced Settings' window:

1. Follow steps 1-3 above.

2. Click the 'Add...' button. The 'Service Settings' window appears.

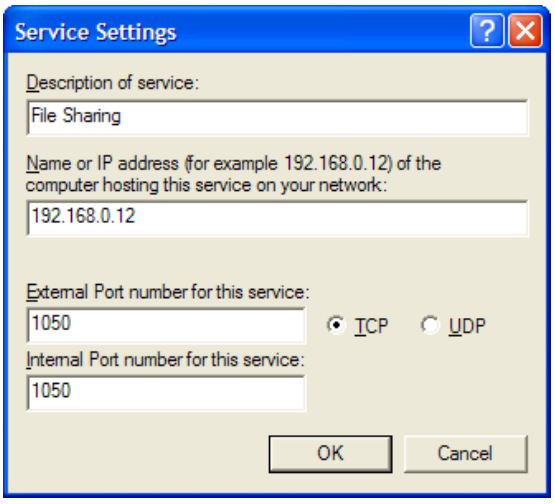


Figure 6.281 Service Settings: Add Service

3. Complete the fields as indicated in the window.

4. Click 'OK' to close the window and return to the 'Advanced Settings' window. The service will be selected.

5. Click 'OK' to save the settings.

6.7.2 Simple Network Management Protocol

Simple Network Management Protocol (SNMP) enables network management systems to remotely configure and monitor iPECS SBG-1000. Your Internet Service Provider (ISP) may use SNMP in order to identify and resolve technical problems. Technical information regarding the properties of iPECS SBG-1000's SNMP agent should be provided by your ISP. To configure iPECS SBG-1000's SNMP agent, perform the following:

1. Access this feature either from the 'Management' menu item under the 'System' tab, or by clicking its icon in the 'Shortcut' screen. The 'SNMP' screen appears:

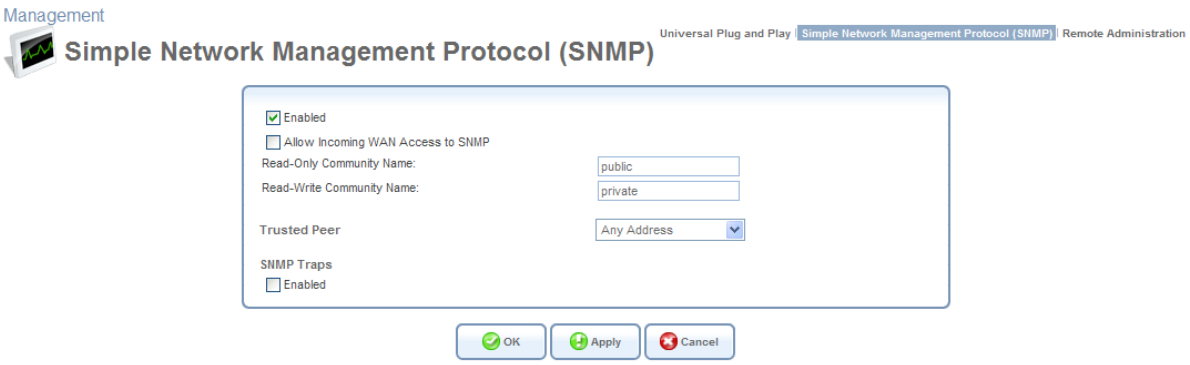


Figure 6.282 SNMP Management

2. Specify the SNMP parameters, as provided by your Internet service provider:
   Allow Incoming WAN Access to SNMP Select this check box to allow access to iPECS SBG-1000's SNMP over the Internet.
   Read-only/Write Community Names SNMP community strings are passwords used in SNMP messages between the management system and iPECS SBG-1000. A read-only community allows the manager to monitor iPECS SBG-1000. A read-write community allows the manager to both monitor and configure iPECS SBG-1000.
   Trusted Peer The IP address, or subnet of addresses, that identify which remote management stations are allowed to perform SNMP operations on iPECS SBG-1000.
   SNMP Traps Messages sent by iPECS SBG-1000 to a remote management station, in order to notify the manager about the occurrence of important events or serious conditions. iPECS SBG-1000 supports both SNMP version 1 and SNMP version 2c traps. Check the Enabled check box to enable this feature. The screen refreshes, displaying the following fields.

Figure 6.283 SNMP Traps

- **Version** Select between version SNMP v1 and SNMP v2c.
- **Destination** The remote management station's IP address.
- **Community** Enter the community name that will be associated with the trap messages.

6.7.2.1 Defining an SNMPv3 User Account

Simple Network Management Protocol version 3 (SNMPv3) enables you to perform certain management and monitoring operations on iPECS SBG-1000 outside its WBM. Information is exchanged between a management station and iPECS SBG-1000's SNMP agent in the form of an SNMP message. The advantage of the third version of SNMP over the previous versions is that it provides user authentication, privacy, and access control.

SNMPv3 specifies a User Security Model (USM) that defines the need to create an SNMP user account, in order to secure the information exchange between the management station and the SNMP agent. The following example demonstrates how to define an SNMPv3 user account in iPECS SBG-1000. Let's assume that you want to add a new SNMPv3 user called "admin". For this purpose, perform the following steps:

1. Add the SNMPv3 user account to the USM table.

2. Associate the user with a new or an existing group.

3. Associate the group with specific views.

4. Create the group views.

Step 1 is performed from iPECS SBG-1000's CLI. Steps 2–4 are performed from a Linux shell, as in the following example.

1. Add the new user (admin) to the USM table, by running the following conf set commands from iPECS SBG-1000's CLI:

```
iPECS SBG-1000> conf set
 /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
 .79.65.5.97.100.109.105.110/name admin

 iPECS SBG-1000> conf set
 /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
 .79.65.5.97.100.109.105.110/security_name admin

 iPECS SBG-1000> conf set
 /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
 .79.65.5.97.100.109.105.110/public “”

 iPECS SBG-1000> conf set
 /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
 .79.65.5.97.100.109.105.110/auth_protocol 1.3.6.1.6.3.10.1.1.1

 iPECS SBG-1000> conf set
 /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
 .79.65.5.97.100.109.105.110/priv_protocol 1.3.6.1.6.3.10.1.2.1
```

```
iPECS SBG-1000> conf set
/snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/storage_type 3

iPECS SBG-1000> conf set
/snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/row_status 1

iPECS SBG-1000> conf set
/snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/clone_from 0.0

iPECS SBG-1000> conf set
/snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/engine_id <ENGINE_ID>
```

The sub-OID 13.128.0.42.47.128.242.184.29.85.234.15.79.65 stands for the engine ID (with length of 13 octets). The decimal values of each engine ID are permanent. The sub-OID 5.97.100.109.105.110 stands for “admin” (5 octets, according to the word length). The decimal values of the user name appear as defined in the ASCII table. The <ENGINE_ID> parameter should be taken from the engine ID in the output of the following command:

```
iPECS SBG-1000> conf print /snmp/persist_conf
```

 Note You should copy the engine ID without the “0x” prefix.

After the commands specified above are issued, the authentication protocol is set to usmNoAuthProtocol (which has OID 1.3.6.1.6.3.10.1.1.1), and the privacy protocol is set to usmNoPrivProtocol (which has OID 1.3.6.1.6.3.10.1.2.1).

2. Associate the user with a group. The associated group can be either a new group or an existing group. For example, to add a new group called “admin_group” and associate it with the user “admin”, run the following SNMP SET commands from a Linux shell:

```
$ snmpset -v2c -c private <iPECS SBG-1000’s IP address>
 vacmSecurityToGroupStatus.3.5.97.100.109.105
 .110 i createAndWait

 $ snmpset -v2c -c private <iPECS SBG-1000’s IP address>
 vacmGroupName.3.5.97.100.109.105.110 s
 admin_group

 $ snmpset -v2c -c private <iPECS SBG-1000’s IP address>
 vacmSecurityToGroupStorageType.3.5.97.100
 .109.105.110 i nonVolatile
```

```
$ snmpset -v2c -c private <iPECS SBG-1000's IP address>
vacmSecurityToGroupStatus.3.5.97.100.109.105
.110 i active
```

The sub-OID 5.97.100.109.105.110 stands for "admin" (with length of 5 octets). These commands populate vacmSecurityToGroupTable with a new group called "admin_group".

3. Associate between the group and its views. For example, suppose you want to associate "admin_group" with a view called "admin_view" for reading, writing and notifications, with security level of noAuthNoPriv. You can do this by running the following SNMP SET commands from a Linux shell:

```
$ snmpset -v2c -c private <iPECS SBG-1000's IP address>
 vacmAccessStatus.11.97.100.109.105.110.95
 .103.114.111.117.112.0.3.1 i createAndWait

 $ snmpset -v2c -c private <iPECS SBG-1000's IP address>
 vacmAccessContextMatch.11.97.100.109.105.110
 .95.103.114.111.117.112.0.3.1 i exact

 $ snmpset -v2c -c private <iPECS SBG-1000's IP address>
 vacmAccessReadViewName.11.97.100.109.105.110
 .95.103.114.111.117.112.0.3.1 s admin_view

 $ snmpset -v2c -c private <iPECS SBG-1000's IP address>
 vacmAccessWriteViewName.11.97.100.109.105
 .110.95.103.114.111.117.112.0.3.1 s admin_view

 $ snmpset -v2c -c private <iPECS SBG-1000's IP address>
 vacmAccessNotifyViewName.11.97.100.109.105
 .110.95.103.114.111.117.112.0.3.1 s admin_view

 $ snmpset -v2c -c private <iPECS SBG-1000's IP address>
 vacmAccessStorageType.11.97.100.109.105.110
 .95.103.114.111.117.112.0.3.1 i nonVolatile

 $ snmpset -v2c -c private <iPECS SBG-1000's IP address>
 vacmAccessStatus.11.97.100.109.105.110.95
 .103.114.111.117.112.0.3.1 i active
```

The sub-OID 11.97.100.109.105.110.95.103.114.111.117.112 stands for "admin_group" (with length of 11 octets).

4. Create the needed views. For example, suppose you want to define "admin_view" as a view that includes all the 1.3 subtree. You can do this by running the following SNMP SET

commands:

```
$ snmpset -v2c -c private <iPECS SBG-1000's IP address>
vacmViewTreeFamilyStatus.10.97.100.109.105
.110.95.118.105.101.119.2.1.3 i createAndWait

$ snmpset -v2c -c private <iPECS SBG-1000's IP address>
vacmViewTreeFamilyType.10.97.100.109.105.110
.95.118.105.101.119.2.1.3 i included

$ snmpset -v2c -c private <iPECS SBG-1000's IP address>
vacmViewTreeFamilyStorageType.10.97.100.109
.105.110.95.118.105.101.119.2.1.3 i nonVolatile

$ snmpset -v2c -c private <iPECS SBG-1000's IP address>
vacmViewTreeFamilyStatus.10.97.100.109.105
.110.95.118.105.101.119.2.1.3 i active
```

The sub-OID 10.97.100.109.105.110.95.118.105.101.119 stands for "admin_view".

After completing these steps, you will have an SNMPv3 user account defined in iPECS SBG-1000. The following is a sample SNMPv3 query issued to iPECS SBG-1000's SNMP agent:

```
$ snmpwalk -v 3 -u admin -l noAuthNoPriv 192.168.1.1
```

6.7.3 Enabling Remote Administration

It is possible to access and control iPECS SBG-1000 not only from within the home network, but also from the Internet. This allows you, for example, to view or change your gateway's settings while travelling. It also enables you to allow your ISP to remotely view your gateway's settings and help you troubleshoot functionality and network communication issues.

Remote access to iPECS SBG-1000 is blocked by default to ensure the security of your home network. However, remote access can be provided via the services described further in this section.

To view and configure iPECS SBG-1000's remote administration options, click the 'Remote Administration' link under the 'Management' menu item. Alternatively, click the 'Remote Administration' icon in the 'Shortcut' screen. The 'Remote Administration' screen appears.

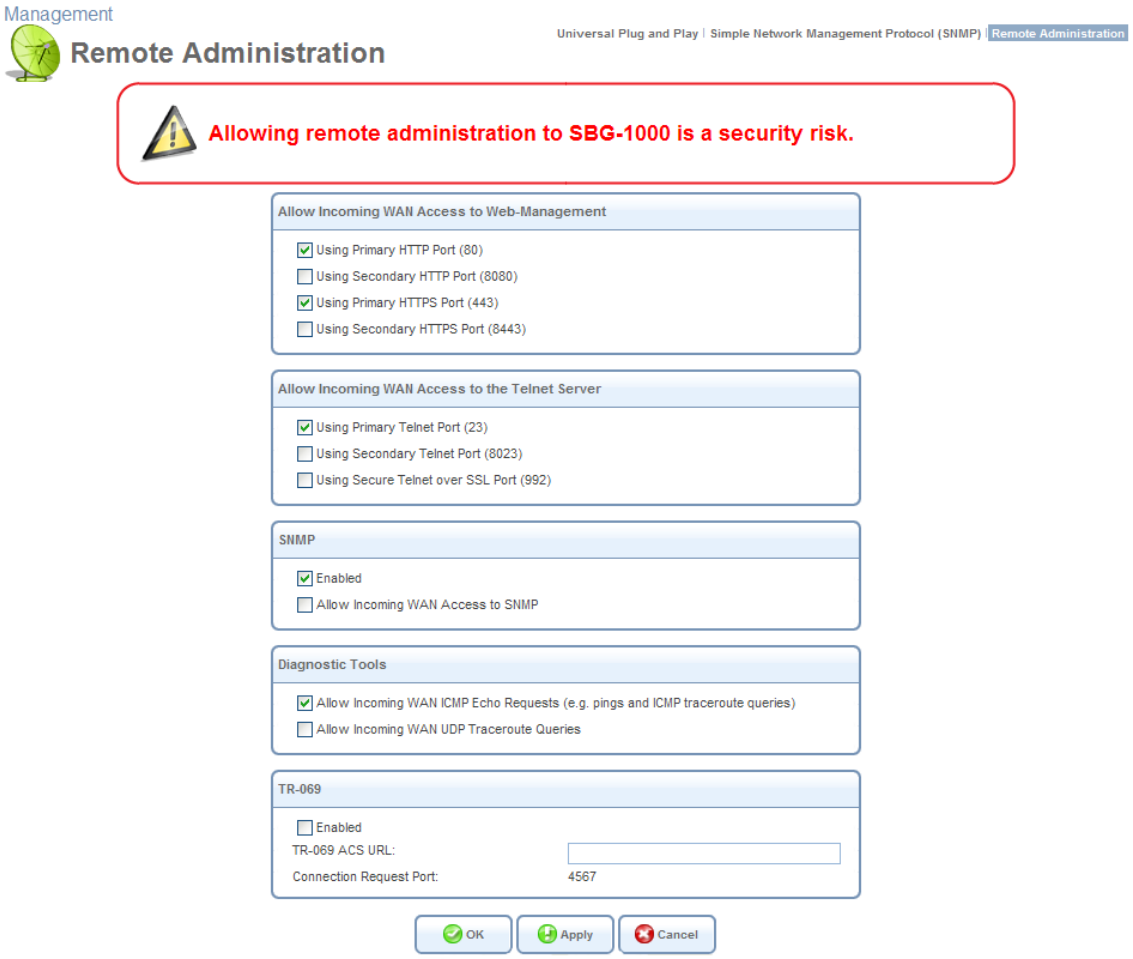


Figure 6.284 Remote Administration

Note that the following management application ports can be configured in the 'System Settings' screen (for more information, refer to Section 6.2).

Allow Incoming Access to Web-Management Used to allow remote access to the WBM via a browser over the selected port(s). Both the secure (HTTPS) and non-secure (HTTP) access can be enabled.

Note that if you select a port other than 80 (which browsers use by default), you will have to specify the port in iPECS SBG-1000's address when trying to access it. For example, after selecting port 443, you will be able to reach iPECS SBG-1000's WBM by browsing to:
https://<iPECS SBG-1000's Internet IP>:443.

Allow Incoming Access to the Telnet Server Used to allow remote access to iPECS SBG-1000's Telnet server over the selected port(s).

Note: Web Management and Telnet may be used to modify settings of the firewall or disable it. The remote user may also change local IP addresses and other settings, making it difficult or impossible to access the gateway from the home network. Therefore, remote access to Telnet or Web services should only be permitted **when it is absolutely necessary**.

Allow SNMP Control and Diagnostic Requests Used to allow Simple Network Management Protocol (SNMP) requests to remotely configure and monitor iPECS SBG-1000. For more information, refer to Section 6.7.2.
Diagnostic Tools Used to allow the Ping and Traceroute utilities on a remote computer to communicate with iPECS SBG-1000 in order to test its connectivity.
TR-069 TR-069 is a WAN management protocol intended for communication between Customer Premise Equipment (CPE) and an Auto-Configuration Server (ACS). It defines a mechanism that encompasses secure auto configuration of a CPE, and also incorporates other CPE management functions into a common framework.

To allow remote access to iPECS SBG-1000's administrative services:

1. Select the services that you would like to make available to computers on the Internet. The following should be taken into consideration:
   - Although the Telnet service is password-protected, it is not considered a secured protocol. When allowing incoming access to a Telnet server, if port forwarding is configured to use port 23, select port 8023 to avoid conflicts.

   - When allowing incoming access to the WBM, if one of your port forwarding rules is configured to use port 80, select port 8080 to avoid conflicts.

     Note: A remote administration service will have precedence over the port forwarding rule created for a local server, when both are configured to utilize the same port. For example, when both the Web server (running on your LAN host) and a remote administration service (utilized by the ISP) are configured to use port 80, iPECS SBG-1000 will grant access to the remote administration traffic. The traffic destined for your Web server will be blocked until you disable the remote administration service or change its dedicated port. For more information about the port forwarding rules created for local servers, refer to Section 5.2.3.

2. Click 'OK' to save the settings.

The encrypted remote administration over the Web, which is performed using a secure (SSL) connection, requires an SSL certificate. When accessing iPECS SBG-1000 for the first time using encrypted remote administration, you will encounter a warning message generated by your browser regarding certificate authentication. This is due to the fact that iPECS SBG-1000's SSL certificate is self-generated. When encountering this message under these circumstances, ignore it and continue.
It should be noted that even though this message appears, the self-generated certificate is safe, and provides you with a secure SSL connection. It is also possible to assign a user-defined certificate to iPECS SBG-1000. To learn about certificates, refer to Section 6.9.4.

If you wish to securely administrate iPECS SBG-1000 via its CLI, establish a Telnet over SSL connection to the gateway by performing the following:

1. Select the 'Using Secure Telnet over SSL Port' check box (see Figure 6.284). By default,

the secure Telnet over SSL port is 992. You can change the port number in the 'System Settings' screen, as described in Section 6.2.

2. Install a Telnet SSL client on your PC.

3. Connect to iPECS SBG-1000 via Telnet SSL. For example, if you are using a Linux host, enter the following command in a shell:
   $ telnet-ssl -z ssl 192.168.1.1 992

   Unless you have a digital certificate recognized by iPECS SBG-1000, you will be requested to enter iPECS SBG-1000's username and password.

   Note: If iPECS SBG-1000's 'Telnet over SSL Client Authentication' option is set to 'Required' (refer to Section 6.2), it is important that the CN field of the certificate contain the name of the iPECS SBG-1000 user, which has administrator rights. Otherwise, iPECS SBG-1000 will deny access to its CLI.

6.8 Performing System Maintenance

6.8.1 About iPECS SBG-1000

The 'About iPECS SBG-1000' screen presents various details about iPECS SBG-1000's software version, such as version number, type of platform and list of features.

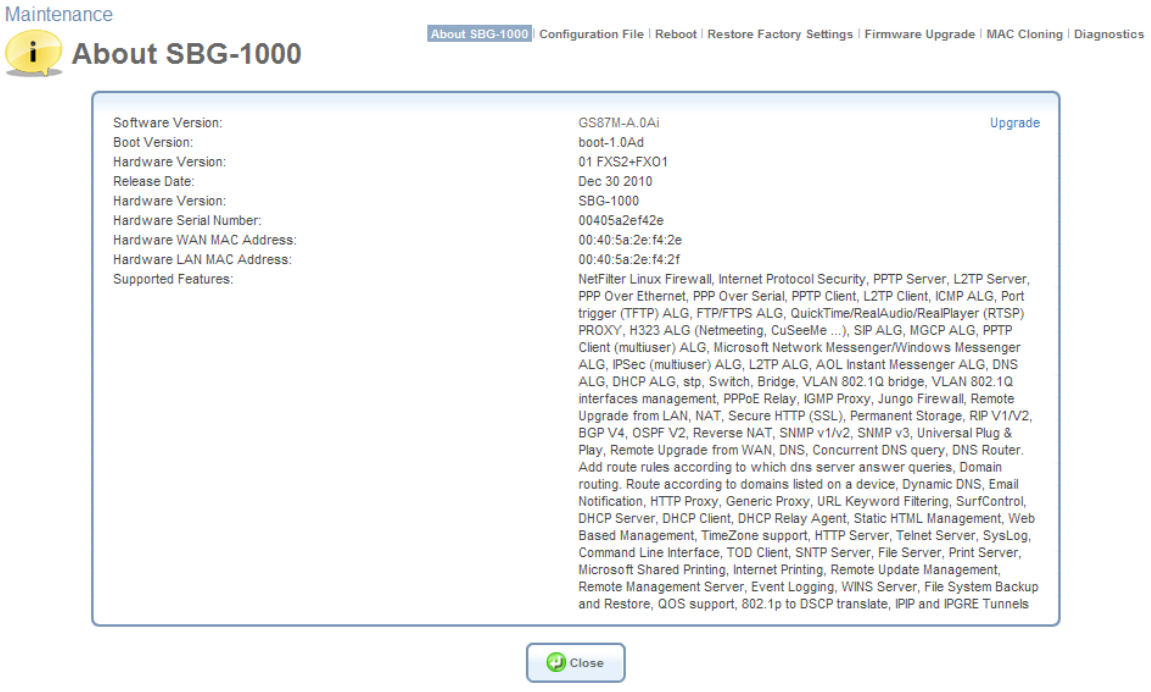


Figure 6.285 About iPECS SBG-1000

6.8.2 Accessing the Configuration File

iPECS SBG-1000 enables you to view, save and load its configuration file in order to backup and restore your gateway's current configuration. Click the 'Configuration File' link in the links bar to view this file. You can also access it by clicking its icon in the 'Shortcut' screen. The 'Configuration File' screen appears, displaying the complete contents of iPECS SBG-1000's configuration file.

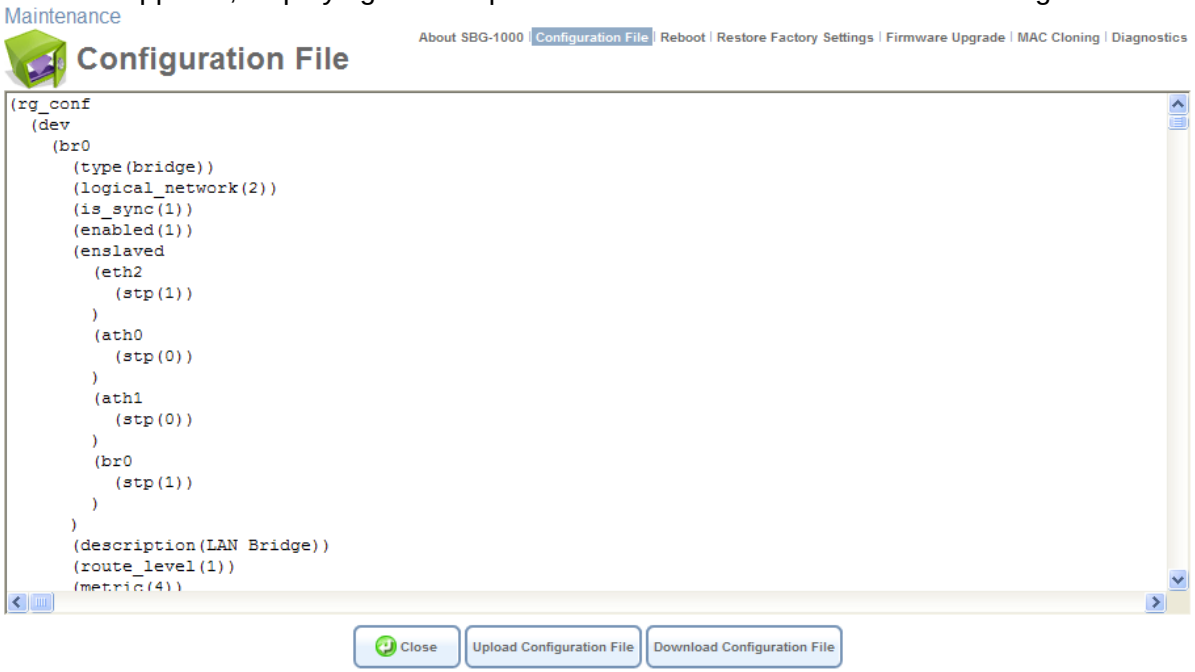


Figure 6.286 Configuration File

Click 'Download Configuration File' to save a copy of your current configuration file on a PC connected to the gateway. Click 'Upload Configuration File' to restore your configuration from a saved file and restart iPECS SBG-1000.

Note: Upon reboot, iPECS SBG-1000 restores the settings from its configuration file. However, if reboot attempts fail five times consecutively, iPECS SBG-1000 will reset the configuration file by restoring factory defaults before attempting to reboot.

6.8.3 Rebooting Your Gateway

If you wish to reboot your gateway, click the 'Reboot' link under the 'Maintenance' menu item. The 'Reboot' screen appears.

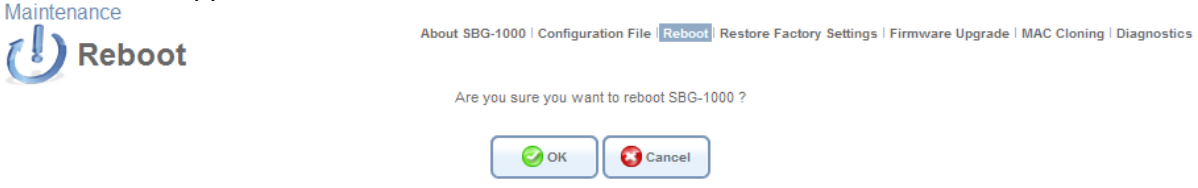


Figure 6.287 Reboot

Click 'OK' to reboot iPECS SBG-1000. This may take up to two minute. To re-enter the WBM after the gateway is up, click the browser's 'Refresh' button, or browse to iPECS SBG-1000's local address.

6.8.4 Restoring Factory Settings

Restoring iPECS SBG-1000's factory settings removes all of the configuration changes made to iPECS SBG-1000 (including the created user accounts). This is useful, for example, when you wish to build your home network from the beginning, and wish to go back to the default configuration.
Click the 'Restore Factory Settings' link under the 'Maintenance' menu item. The 'Restore Factory Settings' appears.

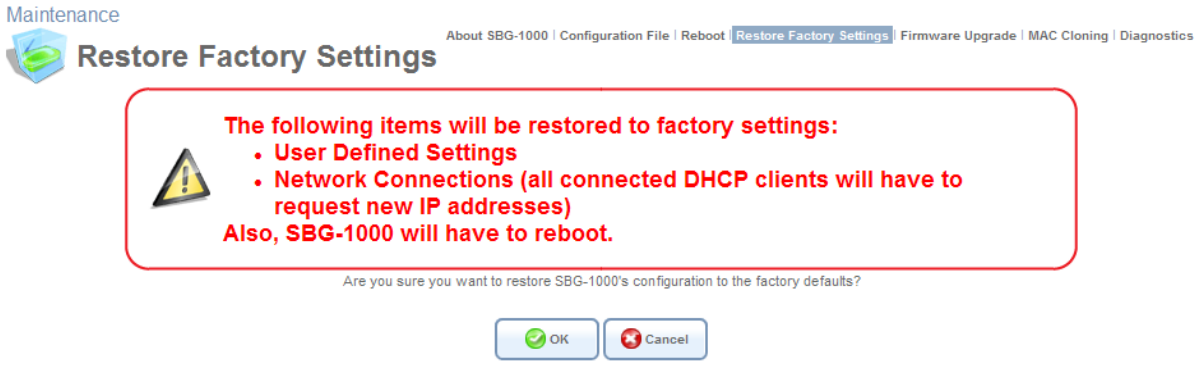


Figure 6.288 Restore Defaults

Click 'OK' to proceed. iPECS SBG-1000 removes all of your personal settings, and then reboots.

6.8.5 Upgrading the Gateway's Firmware

Click the 'iPECS SBG-1000 Firmware Upgrade' link in the links bar. The 'iPECS SBG-1000 Firmware Upgrade' screen appears.

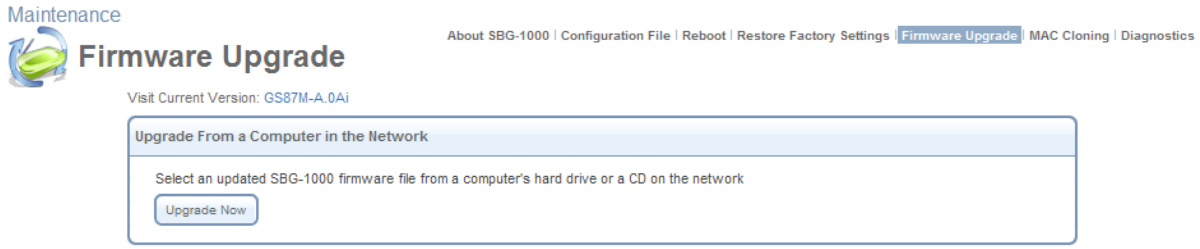


Figure 6.289 iPECS SBG-1000 Firmware Upgrade

- iPECS SBG-1000 offers a built-in mechanism for upgrading its software image, without losing any of your custom configurations and settings.

6.8.5.1 Upgrading From a Computer in the Network

To upgrade iPECS SBG-1000's software image using a locally available **.rms** file, perform the following:

1. In the 'Upgrade From a Computer in the Network' section, click the 'Upgrade Now' button. The 'Upgrade From a Computer in the Network' screen appears.

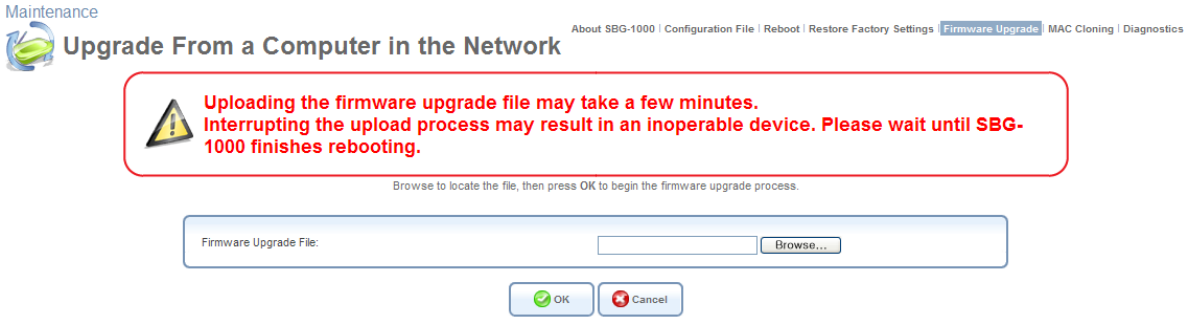


Figure 6.290 Upgrade From a Computer in the Network

2. Enter the path of the software image file, or click the 'Browse' button to browse for the file on your PC, and click 'OK'.

Note: You can only use files with an '**rms**' extension when performing the firmware upgrade procedure.

The file will start loading from your PC to the gateway, and the following upgrade meesage will be displayed while the system is being upgraded.

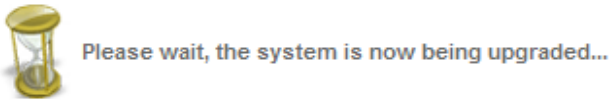


Figure 6.291 Upgrade Message

3. When the upgrade process ends, iPECS SBG-1000 automatically reboots, and the login screen of the updated image is displayed. The new software maintains your custom configurations and settings.

6.8.6 Replacing iPECS SBG-1000's MAC Address

Click the 'MAC Cloning' link in the links bar. The 'MAC Cloning' screen appears.

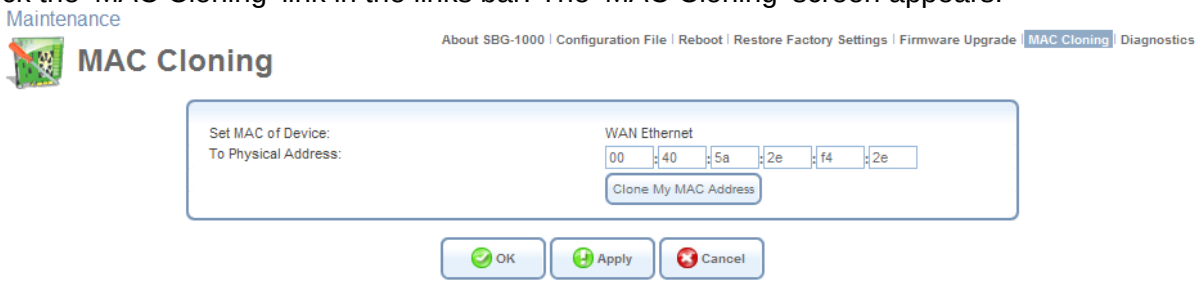


Figure 6.292 MAC Cloning Settings

A Media Access Control (MAC) address is the numeric code that identifies a device on a network, such as a modem or a PC network card. After connecting iPECS SBG-1000, you can replace its MAC address with that of the modem or network card. This is useful, for example, if you are using a static IP address service provided by your ISP. The ISP uses the MAC address to identify the device to which it grants the static IP address. If iPECS SBG-1000 is identified by the replaced MAC address, you can continue receiving the service uninterrupted, and without having to inform

your ISP of your newly installed equipment.
To override iPECS SBG-1000's MAC address with that of the currenly connected modem or network card, click 'Clone My MAC Address'. The MAC address of device connected to iPECS SBG-1000 will replace iPECS SBG-1000's original one. Click 'OK' to save the changes.
You may also replace iPECS SBG-1000's MAC address manually, by typing any valid MAC address in the provided fields and clicking 'OK'.

6.8.7 Diagnosing Network Connectivity

Click the 'Diagnostics' link in the links bar. The 'Diagnostics' screen appears.

Figure 6.293 Maintenance – Diagnostics

This screen can assist you in testing network connectivity and viewing statistics, such as the number of packets transmitted and received, round-trip time and success status.

Note: The test tools described in this section are platform-dependent, and therefore may not all be available at once.

6.8.7.1 Performing a Ping Test

Use the 'Ping (ICMP Echo)' section to to run a Ping test:

1. In the 'Destination' field, enter the IP address or URL to be tested.
2. Enter the number of pings you would like to run.
3. Click 'Go'.

After a few moments, diagnostic statistics will be displayed. If no new information is displayed, click 'Refresh'.

6.8.7.2 Performing an ARP Test

The Address Resolution Protocol (ARP) test is used to query the physical address (MAC) of a host. Use the 'ARP' section to run an ARP test:

1. In the 'Destination' field, enter the IP address of the target host.

2. Click 'Go'.

After a few moments, diagnostic statistics will be displayed. If no new information is displayed, click 'Refresh'.

6.8.7.3 Performing a Traceroute Test

Use the 'Traceroute' section to run a traceroute test:

1. In the 'Destination' field, enter the IP address or URL to be tested.

2. Click 'Go'. The traceroute test commences, constantly refreshing the screen.

3. To stop the test and view the results, click 'Cancel'.

6.9 Objects and Rules

6.9.1 Viewing and Defining Protocols

The Protocols feature incorporates a list of preset and user-defined applications and common port settings. You can use protocols in various security features such as Access Control and Port Forwarding (refer to Section 5.2.2 and Section 5.2.3 respectively). You may add new protocols to support new applications or edit existing ones according to your needs.
To view the basic protocols list, click the 'Objects and Rules' menu item under the 'System' tab. The 'Protocols' screen appears.

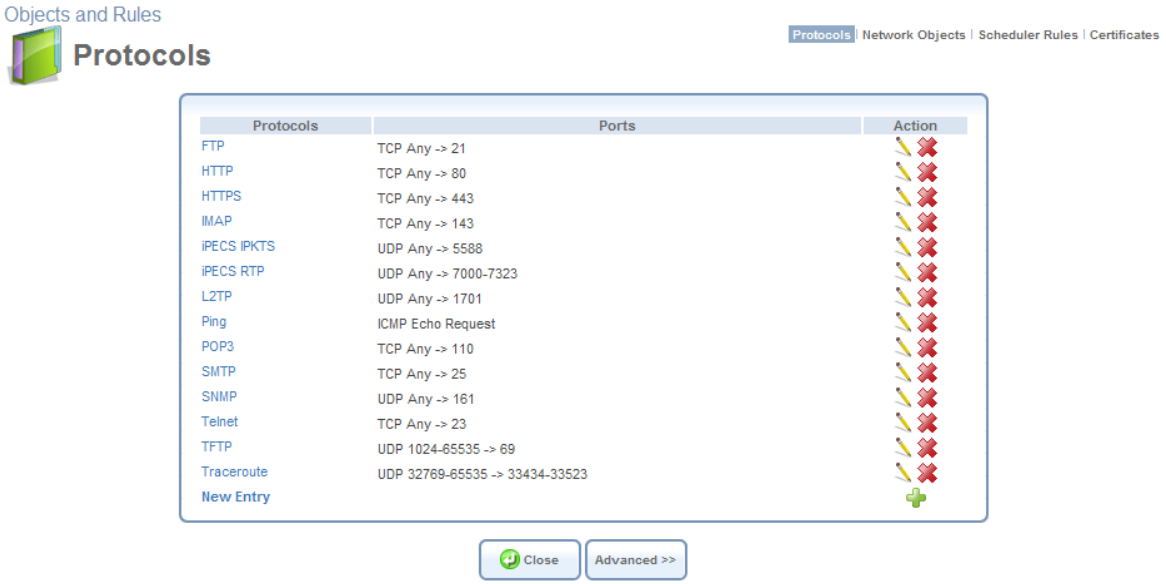


Figure 6.294 Protocols

Click the ‘Advanced’ button at the bottom of this screen for the full list of protocols supported by iPECS SBG-1000.

Note that toggling this view between ‘Basic’ and ‘Advanced’ is reflected throughout the WBM wherever the protocols list is displayed, and can be set back with ‘Show All Services’ and ‘Show Basic Services’, respectively.

To define a protocol:

1. Click the ‘New Entry’ link in the ‘Protocols’ screen. The ‘Edit Service’ screen appears:

Figure 6.295 Edit Service

2. Name the service in the ‘Service Name’ field, and click the ‘New Server Ports’ link. The ‘Edit Service Server Ports’ screen appears (see Figure 6.296). You may choose any of the protocols available in the drop-down menu, or add a new one by selecting ‘Other’. When selecting a protocol from the drop-down menu, the screen refreshes, presenting the respective fields by which to enter the relevant information.

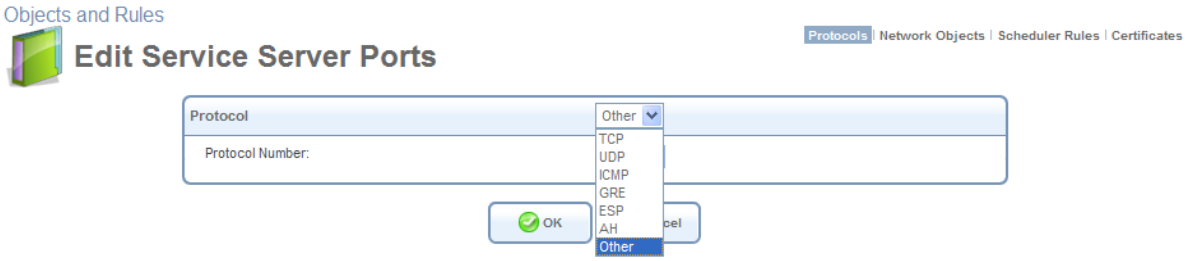


Figure 6.296 Edit Service Server Ports

3. Select a protocol and enter the relevant information.

4. Click ‘OK’ to save the settings.

6.9.2 Defining Network Objects

Click the ‘Network Objects’ link in the links bar. The ‘Network Objects’ screen appears.

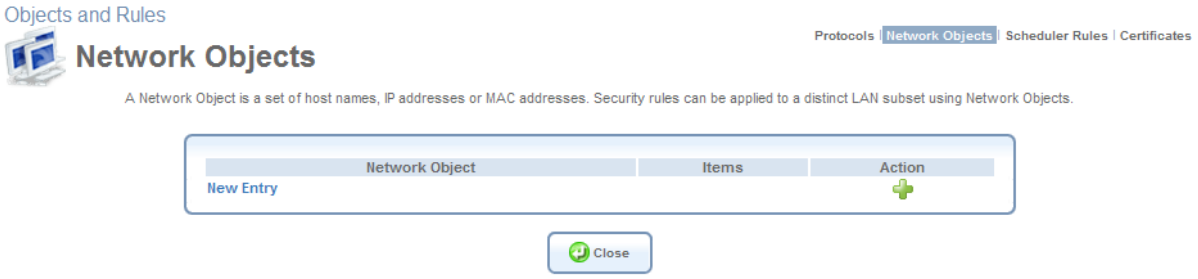


Figure 6.297 Network Objects

Network Objects is a method used to abstractly define a set of LAN hosts, according to specific criteria, such as MAC address, IP address, or host name. Defining such a group can assist when configuring system rules. For example, network objects can be used when configuring iPECS SBG-1000’s security filtering settings such as IP address filtering, host name filtering or MAC address filtering. You can use network objects in order to apply security rules based on host names instead of IP addresses. This may be useful, since IP addresses change from time to time. It is also possible to define network objects according to MAC addresses, making rule application more persistent against network configuration settings. Moreover, iPECS SBG-1000 supports several DHCP options—60, 61, and 77, enabling the gateway to apply security and QoS rules on a network object according to its unique vendor, client, or user class ID, respectively. For example, a Dell iPECS SBG-1000™ IP telephone can be identified and applied with specific QoS priority rules.

To define a network object:

1. In the ‘Network Objects’ screen, click the ‘New Entry’ link. The ‘Edit Network Object’ screen appears.

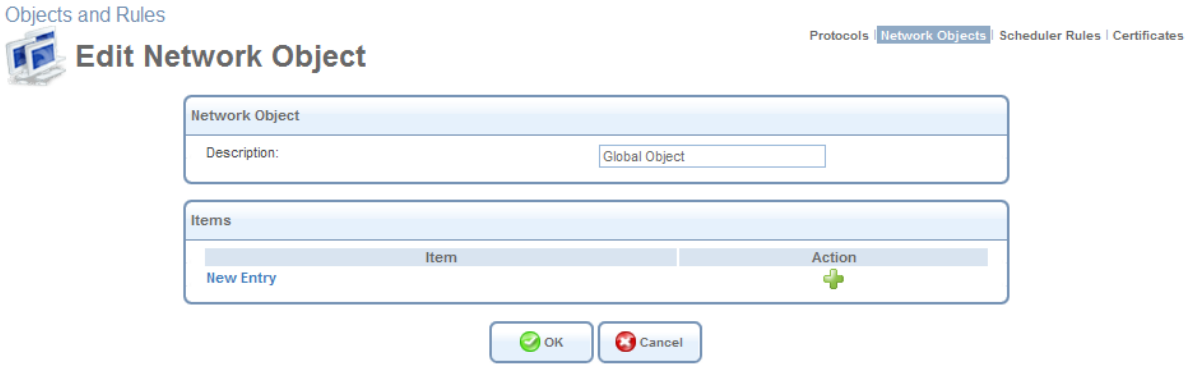


Figure 6.298 Edit Network Object

2. Name the network object in the 'Description' field, and click 'New Entry' to create it. The 'Edit Item' screen appears.

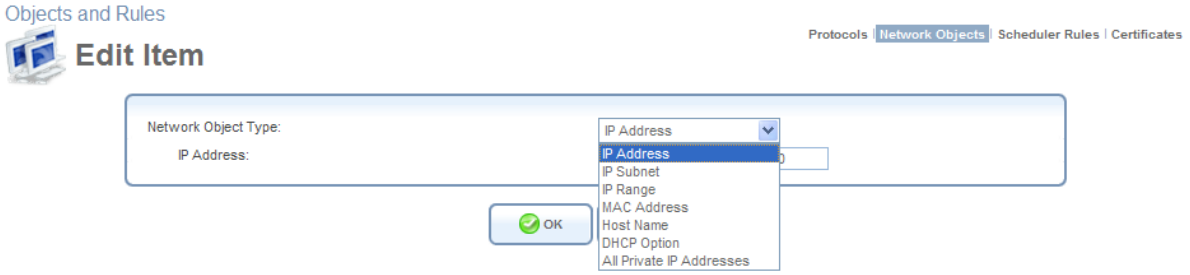


Figure 6.299 Edit Item

When selecting a method from the 'Network Object Type' drop-down menu, the screen refreshes presenting the respective fields for entering the relevant information. The group definition can be according to one of the following methods:

IP Address Enter an IP address common to the group.

IP Subnet Enter a subnet IP address and a subnet mask.

IP Range Enter first and last IP addresses in the range.

MAC Address Enter a MAC address and mask.

Host Name Enter a host name common to the group.

DHCP Option Enter either a vendor class ID (option 60), client ID (option 61), or user class ID (option 77), supplied by your service provider. Note that DHCP clients must also be configured with one of those IDs, in order to be associated with this network object.

3. Select a method and enter the source address accordingly.

4. Click 'OK' to save the settings.

6.9.3 Defining Scheduler Rules

Click the ‘Scheduler Rules’ link in the links bar. The ‘Scheduler Rules’ screen appears.

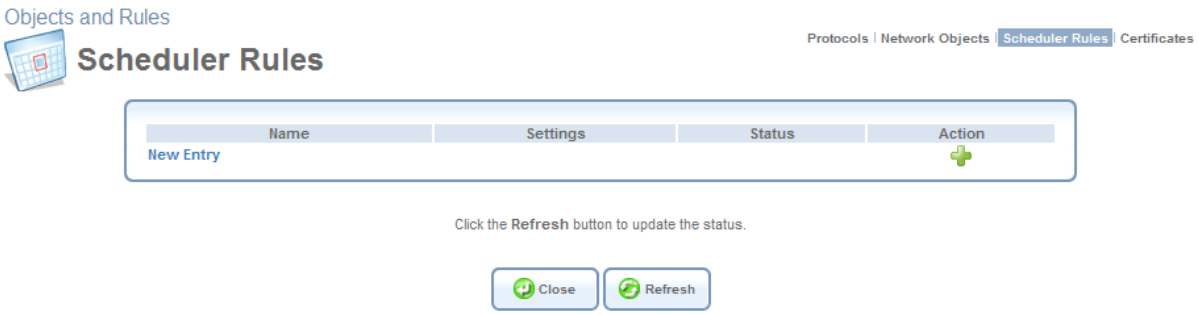


Figure 6.300 Scheduler Rules

Scheduler rules are used for limiting the activation of Firewall rules to specific time periods, specified in days of the week, and hours. To define a rule, perform the following:

1. In the ‘Scheduler Rules’ screen, click the ‘New Entry’ link. The ‘Edit Scheduler Rule’ screen appears.

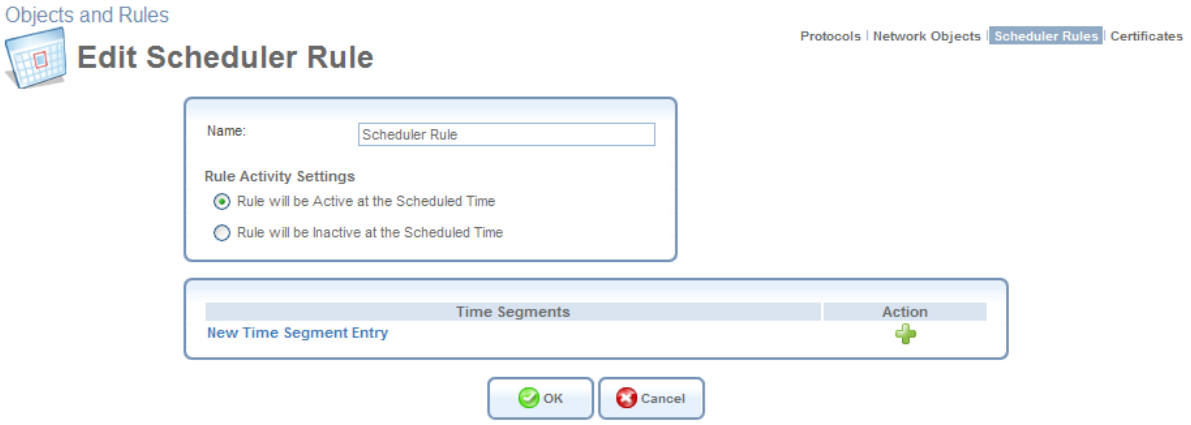


Figure 6.301 Edit Scheduler Rule

2. Specify a name for the rule in the ‘Name’ field.

3. Click the ‘New Time Segment Entry’ link to define the time segment to which the rule will apply. The ‘Edit Time Segment’ screen appears.

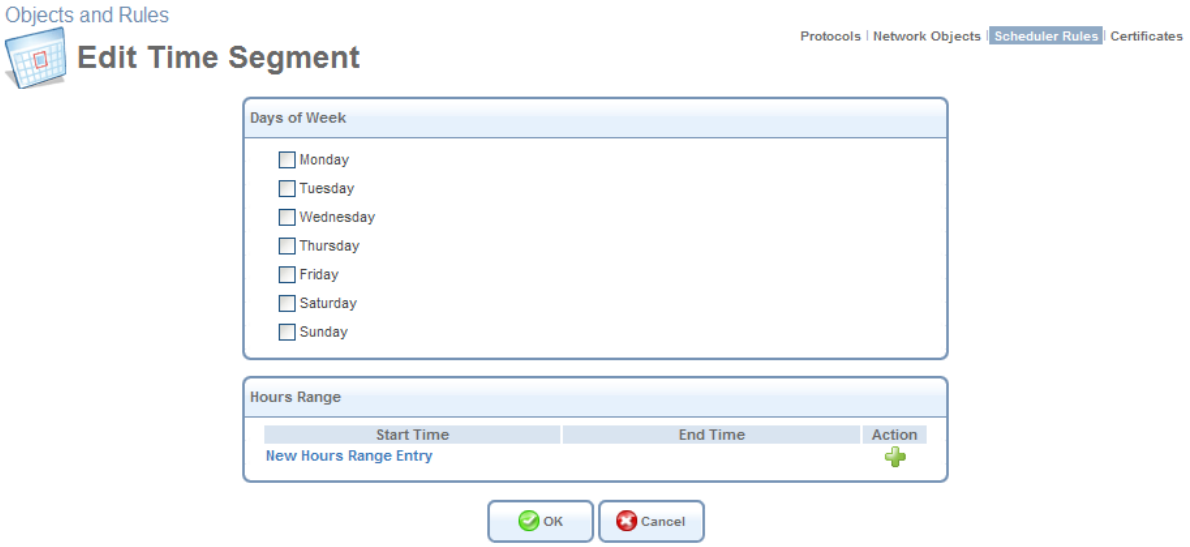


Figure 6.302 Edit Time Segment

a. Select the day(s) of the week, on which the rule will be activated or deactivated.

b. Click the 'New Hours Range Entry' to narrow the time segment to a specific hour range. The 'Edit Hour Range' screen appears.

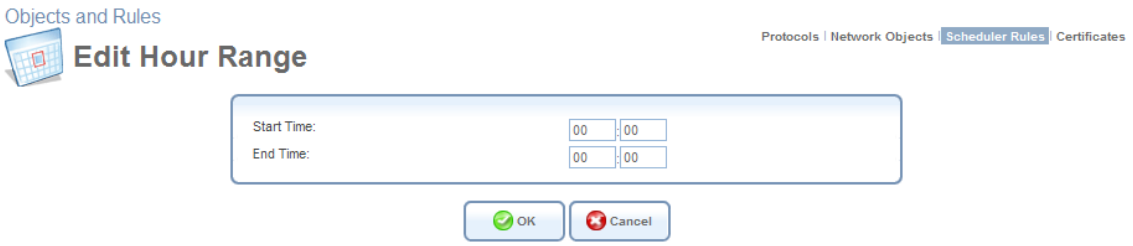


Figure 6.303 Edit Hour Range

c. Enter the desired start and end time values.

Note: The defined start and end time will be applied to all days of the week you have selected. In addition, if you choose the hour range 21:00-08:00, for example, the rule will be activated on the selected day, and deactivated the next day at 8 o'clock in the morning.

4. Click 'OK' to save the settings. The 'Edit Scheduler Rule' screen appears with the defined time segment.

5. Specify if the rule will be active/inactive during the designated time period, by selecting the appropriate 'Rule Activity Settings' radio button.

6. Click 'OK' to return to the 'Scheduler Rules' screen.

6.9.4 Creating and Loading Digital Certificates

6.9.4.1 Overview

Public-key cryptography uses a pair of keys: a public key and a corresponding private key. These keys can play opposite roles, either encrypting or decrypting data. Your public key is made known to the world, while your private key is kept secret. The public and private keys are mathematically associated; however it is computationally infeasible to deduce the private key from the public key. Anyone who has the public key can encrypt information that can only be decrypted with the matching private key. Similarly, the person with the private key can encrypt information that can only be decrypted with the matching public key.
Technically, both public and private keys are large numbers that work with cryptographic algorithms to produce encrypted material. The primary benefit of public-key cryptography is that it allows people who have no preexisting security arrangement to authenticate each other and exchange messages securely. iPECS SBG-1000 makes use of public-key cryptography to encrypt and authenticate keys for the encryption of Wireless and VPN data communication, the Web Based Management (WBM) utility, and secured telnet.

6.9.4.1.1 Digital Certificates

When working with public-key cryptography, you should be careful and make sure that you are using the correct person's public key. Man-in-the-middle attacks pose a potential threat, where an ill-intending 3rd party posts a phony key with the name and user ID of an intended recipient. Data transfer that is intercepted by the owner of the counterfeit key can fall in the wrong hands.
Digital certificates provide a means for establishing whether a public key truly belongs to the supposed owner. It is a digital form of credential. It has information on it that identifies you, and an authorized statement to the effect that someone else has confirmed your identity. Digital certificates are used to foil attempts by an ill-intending party to use an unauthorized public key.
A digital certificate consists of the following:

A public key An encryption key that is published and available to anyone.

Certificate information The "identity" of the user, such as name, user ID and so on.

Digital signatures A statement stating that the information enclosed in the certificate has been vouched for by a Certificate Authority (CA).

Binding this information together, a certificate is a public key with identification forms attached, coupled with a stamp of approval by a trusted party.

6.9.4.1.2 X.509 Certificate Format

iPECS SBG-1000 supports X.509 certificates that comply with the ITU-T X.509 international standard. An X.509 certificate is a collection of a standard set of fields containing information about a user or device and their corresponding public key. The X.509 standard defines what information goes into the certificate, and describes how to encode it (the data format). All X.509 certificates have the following data:
The certificate holder's public key the public key of the certificate holder, together with an algorithm identifier that specifies which cryptosystem the key belongs to and any associated key parameters.
The serial number of the certificate the entity (application or person) that created the certificate is responsible for assigning it a unique serial number to distinguish it from other certificates it

issues. This information is used in numerous ways; for example when a certificate is revoked, its serial number is placed on a Certificate Revocation List (CRL).
The certificate holder's unique identifier this name is intended to be unique across the Internet. A DN consists of multiple subsections and may look something like this: CN=John Smith, EMAIL=sbg-1000@lgericsson.com, OU=R&D, O=LG-Ericsson, C=US (These refer to the subject's Common Name, Organizational Unit, Organization, and Country.)
The certificate's validity period the certificate's start date/time and expiration date/time; indicates when the certificate will expire.
The unique name of the certificate issuer the unique name of the entity that signed the certificate. This is normally a CA. Using the certificate implies trusting the entity that signed this certificate. (Note that in some cases, such as root or top-level CA certificates, the issuer signs its own certificate.)
The digital signature of the issuer the signature using the private key of the entity that issued the certificate.
The signature algorithm identifier identifies the algorithm used by the CA to sign the certificate.

6.9.4.2 iPECS SBG-1000 Certificate Stores

iPECS SBG-1000 maintains two certificate stores:

1. iPECS SBG-1000 Local Store This store contains a list of approved certificates that are used to identify iPECS SBG-1000 to its clients. The list also includes certificate requests that are pending a CA's endorsement. You can obtain certificates for iPECS SBG-1000 using the following methods:

    - Requesting an X509 Certificate – This method creates both a private and a matching public key. The public key is then sent to the CA to be certified.

    - Creating a Self-Signed Certificate – This method is the same as requesting a certificate, only the authentication of the public key does not require a CA. This is mainly intended for use within small organizations.

    - Loading a PKCS#12 Format Certificate – This method loads a certificate using an already available and certified set of private and public keys.

2. Certificate Authority (CA) Store This store contains a list of the trusted certificate authorities, which is used to check certificates presented by iPECS SBG-1000 clients.

6.9.4.2.1 Requesting an X509 Certificate

To obtain an X509 certificate, you must ask a CA to issue you one. You provide your public key, proof that you possess the corresponding private key, and some specific information about yourself. You then digitally sign the information and send the whole package (the certificate request) to the CA. The CA then performs some due diligence in verifying that the information you provided is correct and, if so, generates the certificate and returns it. You might think of an X509 certificate as looking like a standard paper certificate with a public key taped to it. It has your name and some information about you on it, plus the signature of the person who issued it to you.

To request an X509 certificate, perform the following:

1. Access this feature either from the ‘Objects and Rules’ menu item under the ‘System’ tab, or by clicking its icon in the ‘Shortcut’ screen. The ‘iPECS SBG-1000’s Local’ sub-tab of the ‘Certificates’ screen appears.

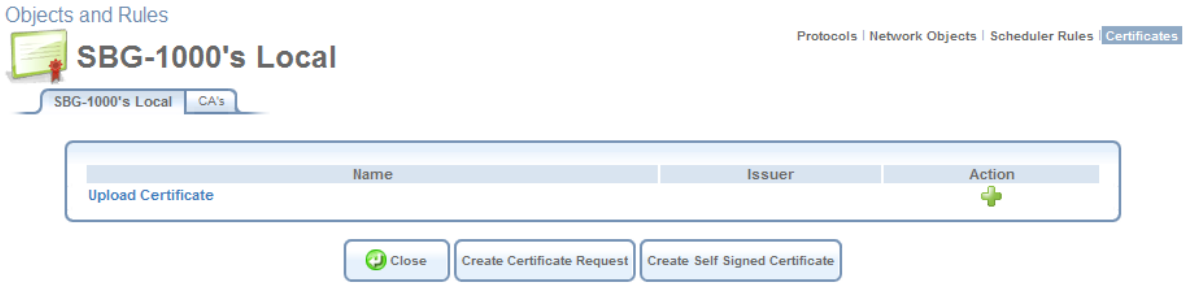


Figure 6.304 Certificate Management

2. Click the ‘Create Certificate Request’ button. The ‘Create X509 Request’ screen appears:

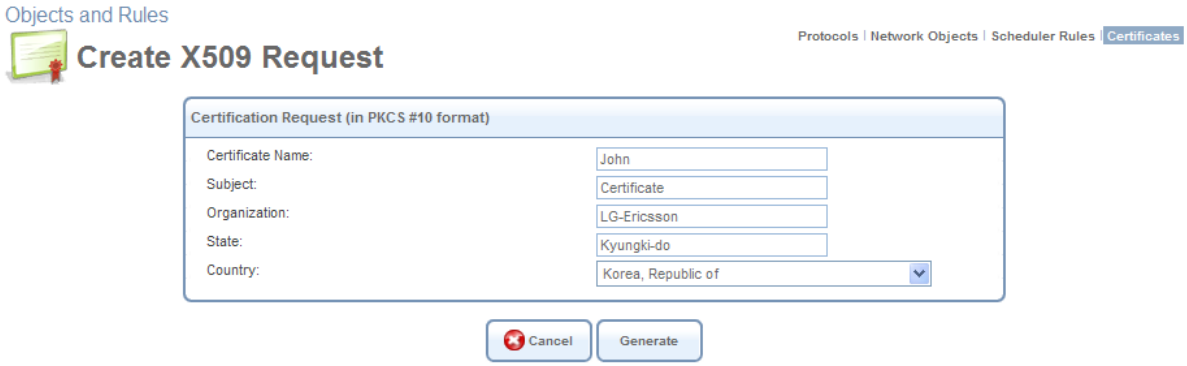


Figure 6.305 Create X509 Request

3. Enter the following certification request parameters:
   - Certificate Name
   - Subject
   - Organization
   - State
   - Country

4. Click the ‘Generate’ button. A screen appears, stating that the certification request is being generated.

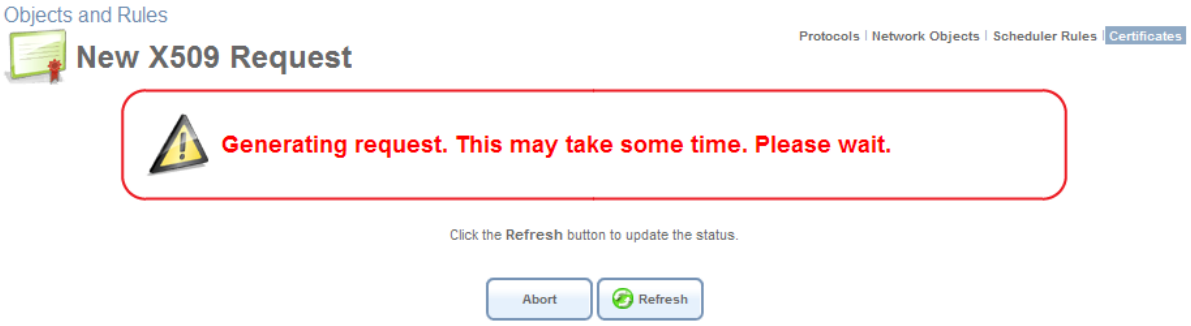


Figure 6.306 Generating a Request

5. After a short while, click the 'Refresh' button, until the 'Download Certificate Request' screen appears.

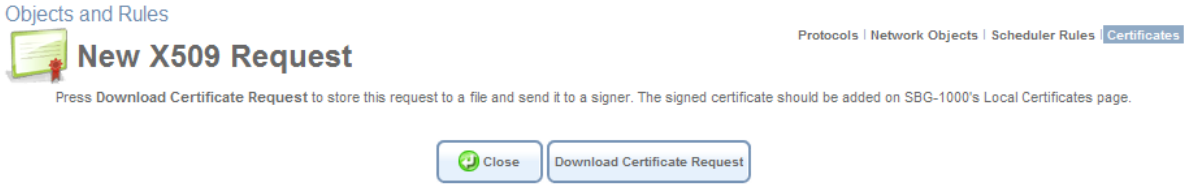


Figure 6.307 Save Certificate Request

6. Click the 'Download Certificate Request' button, and save the request to a file.
7. Click the 'Close' button. The main certificate management screen reappears, listing your certificate as "Unsigned". In this state, the request file may be opened at any time by clicking the  action icon and then 'Open' in the dialogue box (Windows only).

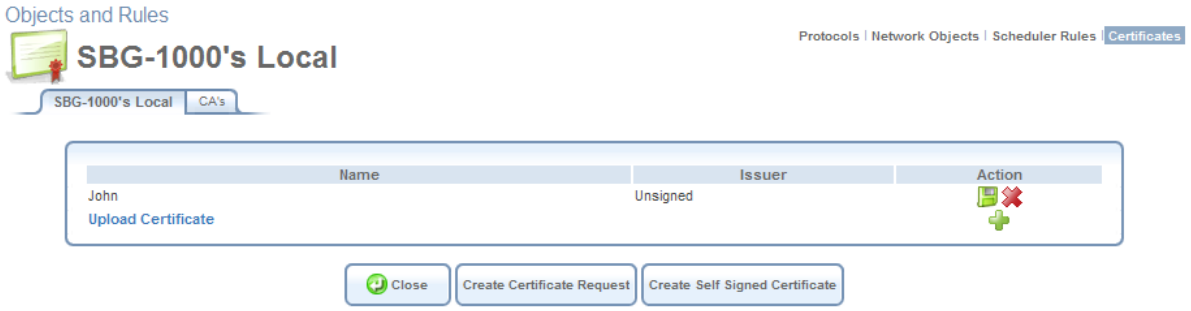


Figure 6.308 Unsigned Certification Request

8. After receiving a reply from the CA in form of a '.pem' file, click the 'Upload Certificate' link. The 'Load iPECS SBG-1000's Local Certificate' screen appears.

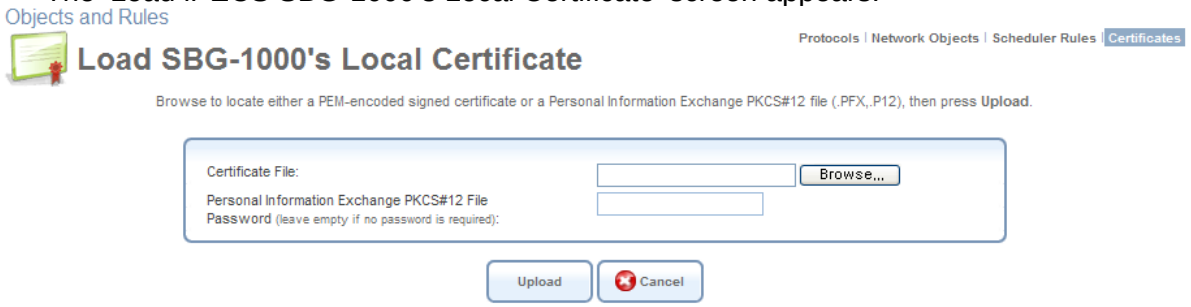


Figure 6.309 Load Certificate

9. Click the ‘Browse’ button to browse to the signed certificate ‘.pem’ file. Leave the password entry empty and click “Upload” to load the signed certificate. The certificate management screen appears, displaying the certificate name and issuer.

Figure 6.310 Loaded Certificate

10. Click the  action icon and then the ‘Open’ button in the dialogue box to view the ‘Certificate’ window (Windows only).

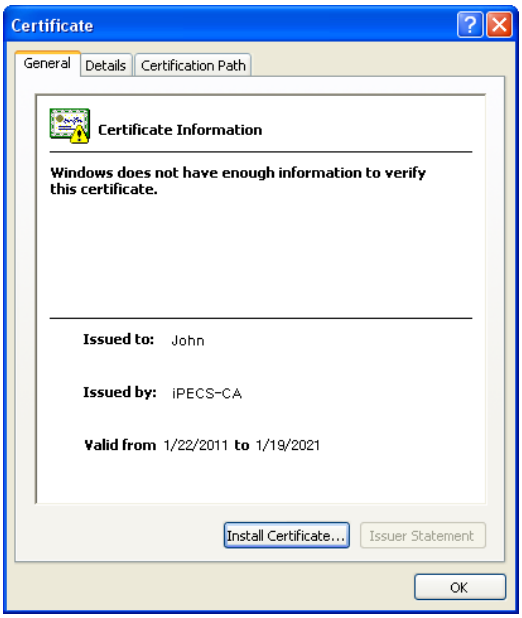


Figure 6.311 Certificate Window

Alternatively, click ‘Save’ in the dialogue box to save the certificate to a file.

11. You can also click the  action icon to view the ‘Certificate Details’ screen.

Figure 6.312 Certificate Details

6.9.4.2.2 Creating a Self-Signed Certificate

A default self-signed certificate is included in iPECS SBG-1000, in order to enable certificate demanding services such as HTTPS.

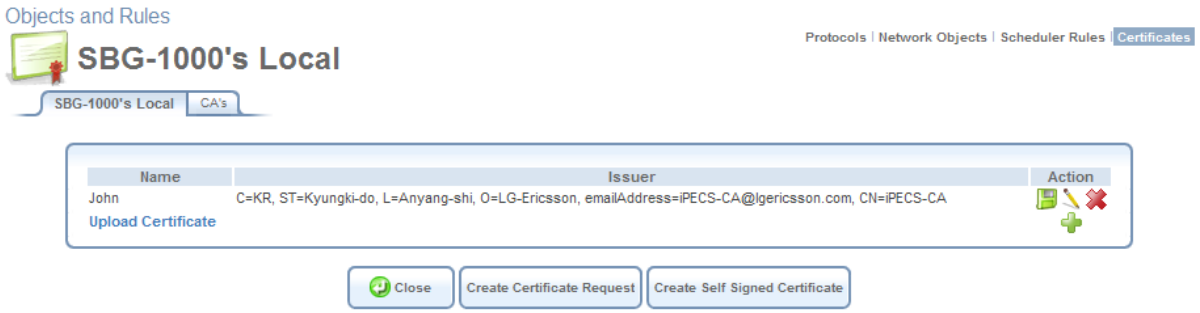


Figure 6.313 Certificates

Note that if deleted, this certificate is restored when iPECS SBG-1000's Restore Defaults operation is run (refer to Section 6.8.4).

To create a self-signed certificate, perform the following:

1. In the 'iPECS SBG-1000's Local' sub-tab of the 'Certificates' screen, click the 'Create Self Signed Certificate' button. The 'Create Self Signed X509 Certificate' screen appears.

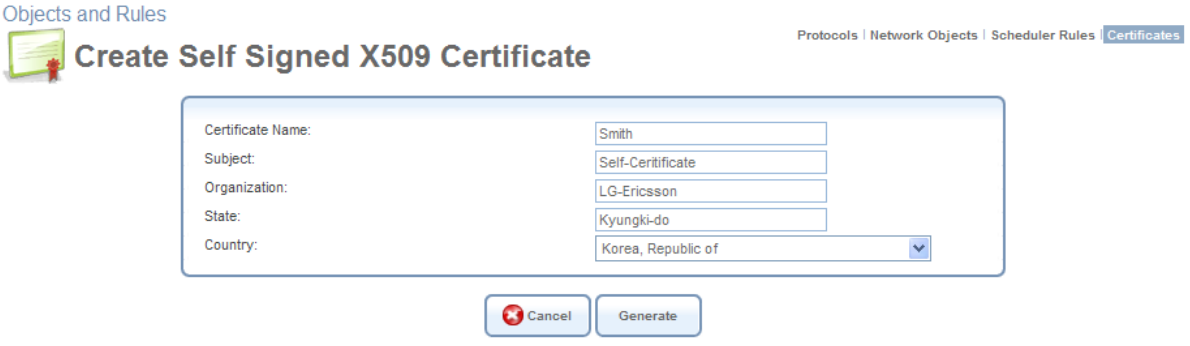


Figure 6.314 Create Self Signed X509 Certificate

2. Enter the following certification request parameters:

- Certificate Name
- Subject
- Organization
- State
- Country

3. Click the ‘Generate’ button. A screen appears, stating that the certificate is being generated (see Figure 6.315).

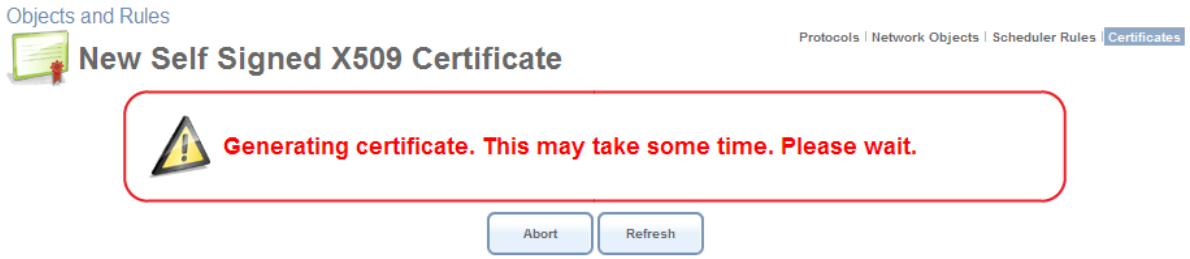


Figure 6.315 Generating a Self-Signed X509 Certificate

4. After a short while, click the ‘Refresh’ button, until the ‘New Self Signed X509 Certificate’ screen appears.

Figure 6.316 New Self Signed X509 Certificate

5. Click the ‘OK’ button. The main certificate management screen reappears, displaying the certificate name and issuer (see Figure 6.317).

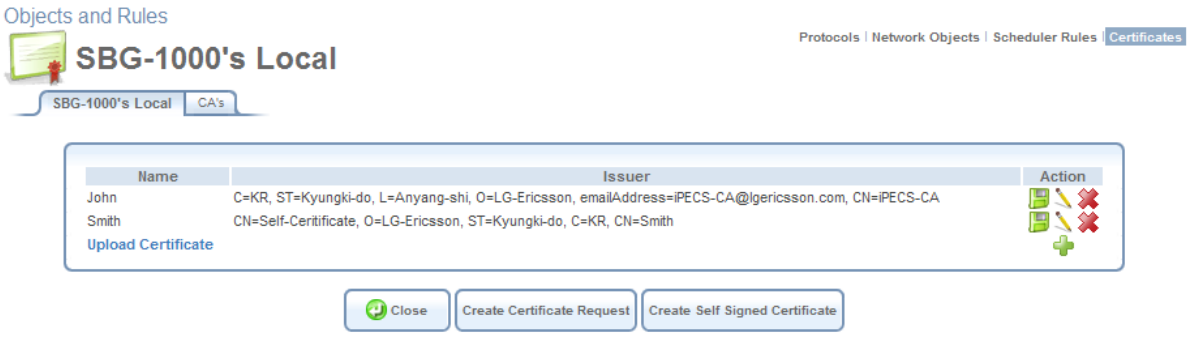


Figure 6.317 Loaded Certificate

6. Click the action icon and then the ‘Open’ button in the dialogue box to view the ‘Certificate’ window (Windows only).

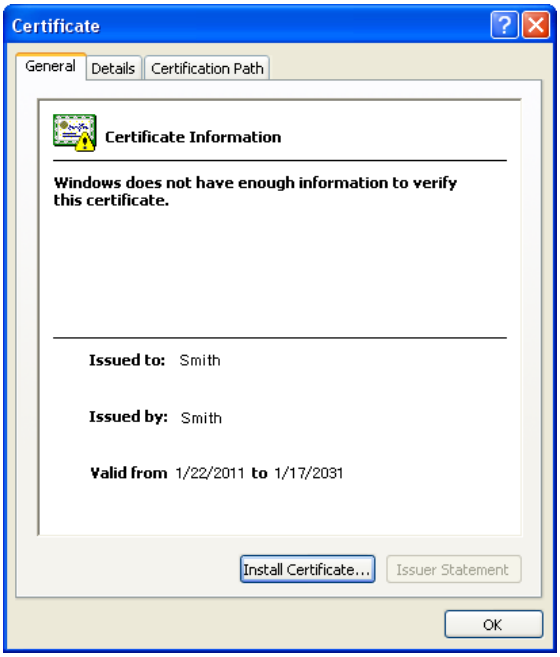


Figure 6.318 Certificate Window

Alternatively, click ‘Save’ in the dialogue box to save the certificate to a file.

7. You can also click the action icon to view the ‘Certificate Details’ screen.

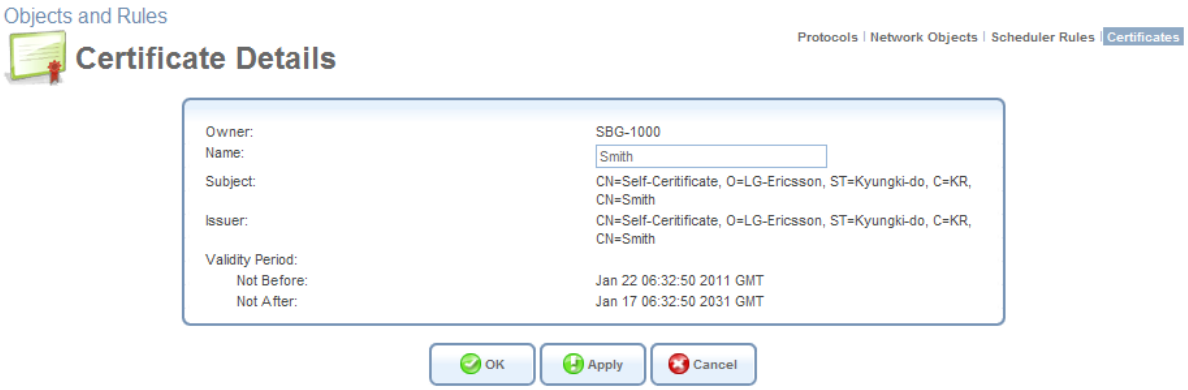


Figure 6.319 Certificate Details

6.9.4.2.3 Loading a PKCS#12 Format Certificate

You can load certificates in PKCS#12 format (usually stored in .p12 files) to iPECS SBG-1000’s certificate store. To do so, you must first obtain the ‘.p12’ file, containing the private and public keys and optional CA certificates. Then, perform the following:

1. In the ‘iPECS SBG-1000’s Local’ sub-tab of the ‘Certificates’ screen, click the ‘Upload Certificate’ link. The ‘Load iPECS SBG-1000’s Local Certificate’ screen appears.

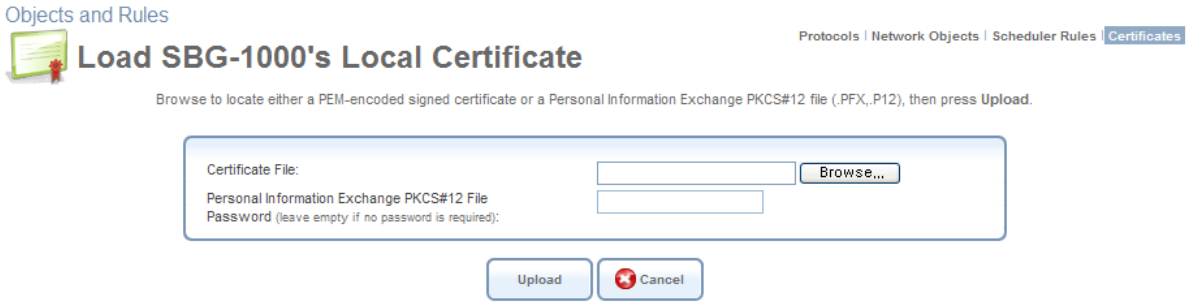


Figure 6.320 Load Certificate

2. Click the 'Browse' button to browse to the '.p12' file. If the private key is encrypted using a password, type it in the password entry (otherwise leave the entry empty), and click "Upload" to load the certificate. The certificate management screen appears, displaying the certificate name and issuer.

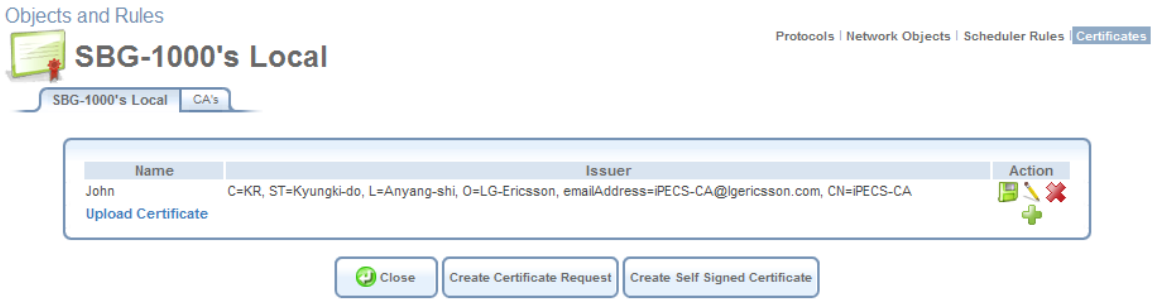


Figure 6.321 Loaded Certificate

If the '.p12' file contained any CA certificates, they will be displayed in the CA store (click the 'CA's' tab to view the CA certificates).

3. Click the  action icon and then the 'Open' button in the dialogue box to view the 'Certificate' window (Windows only).

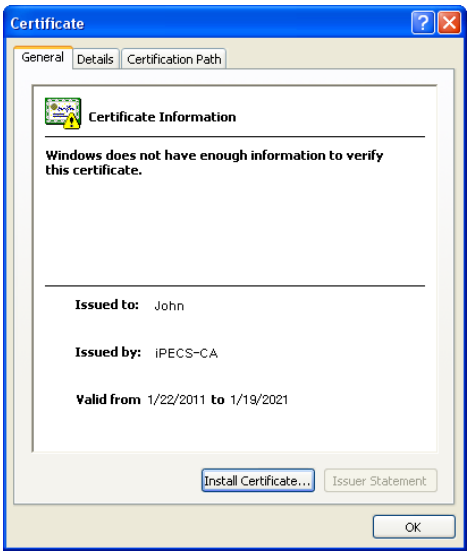


Figure 6.322 Certificate Window

Alternatively, click ‘Save’ in the dialogue box to save the certificate to a file.

4. You can also click the action icon to view the ‘Certificate Details’ screen.

Figure 6.323 Certificate Details

6.9.4.2.4 Loading a CA’s Certificate

Before you can load a CA’s certificate, you must obtain a signed certificate ‘.pem’ or ‘.p12’ file. Then, perform the following:

1. In the ‘Certificates’ screen, click the ‘CA’s’ sub-tab. The ‘CA’s’ screen appears, displaying a list of certificates.

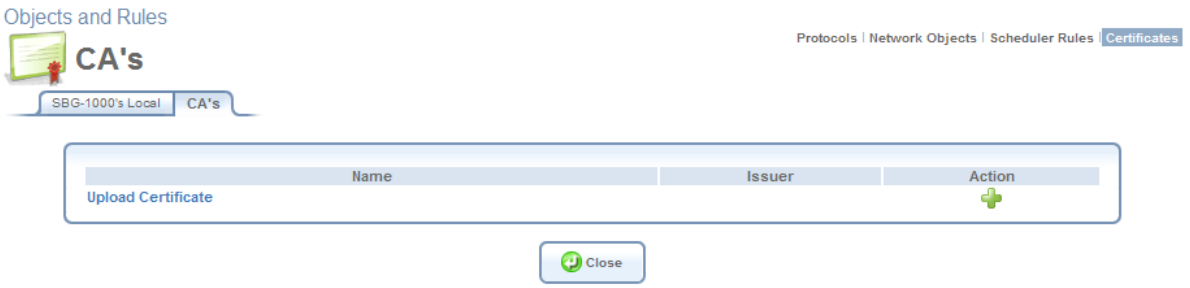


Figure 6.324 CA’s Certificates

2. Click the ‘Upload Certificate’ link. The ‘Load CA’s Certificate’ screen appears.

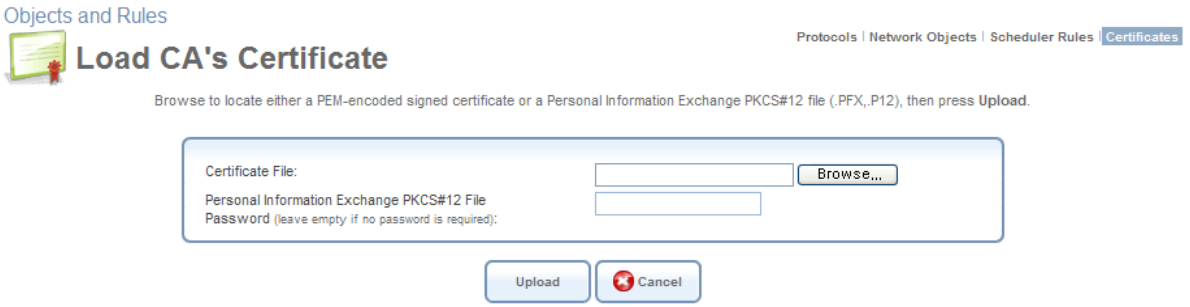


Figure 6.325 Load CA’s Certificate

3. Click the ‘Browse’ button to browse to the ‘.pem’ or ‘.p12’ file. Leave the password entry

empty and click “Upload” to load the certificate. The CA Certificates screen reappears (see Figure 6.324), displaying the trusted certificate authority at the bottom of the list.

4. Click the action icon and then the ‘Open’ button in the dialogue box to view the ‘Certificate’ window (Windows only).

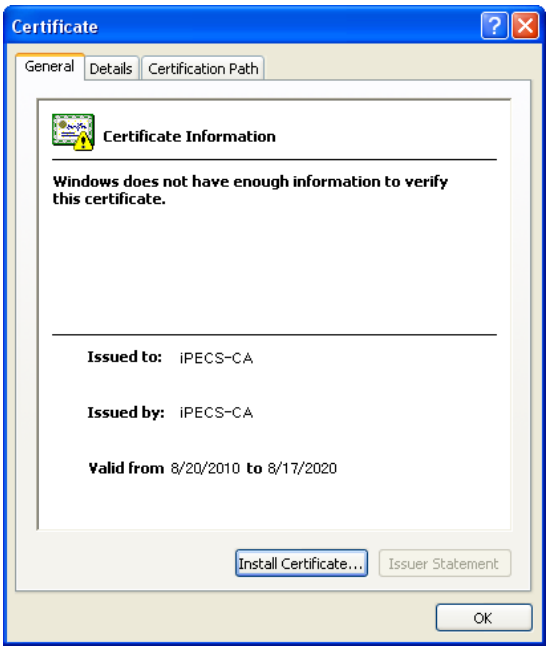


Figure 6.326 Certificate Window

Alternatively, click ‘Save’ in the dialogue box to save the certificate to a file.

5. You can also click the action icon to view the ‘Certificate Details’ screen.

Figure 6.327 Certificate Details

7. Configuring a Computer's Network Interface

In most cases, a computer's network interface is configured by default to automatically obtain an IP address. However, a computer with a statically defined IP address and DNS address, for example, may fail to connect to iPECS SBG-1000. In this case, configure the computer's network interface to obtain its IP and DNS server IP settings automatically. The configuration principle is identical but performed differently on different operating systems. Following are TCP/IP configuration instructions for all supported operating systems.

Windows XP

1. Access 'Network Connections' from the Control Panel.
2. Right-click the Ethernet connection icon, and select 'Properties'.
3. Under the 'General' tab, select the 'Internet Protocol (TCP/IP)' component, and press the 'Properties' button.
4. The 'Internet Protocol (TCP/IP)' properties window will be displayed.
    a. Select the 'Obtain an IP address automatically' radio button.
    b. Select the 'Obtain DNS server address automatically' radio button.
    c. Click 'OK' to save the settings.

Linux

1. Login into the system as a super-user, by entering "su" at the prompt.
2. Type "ifconfig" to display the network devices and allocated IP addresses.
3. Type "pump -i <dev>", where <dev> is the network device name.
4. Type "ifconfig" again to view the new allocated IP address.
5. Make sure no firewall is active on device <dev>.

8. List of Acronyms

Acronym	Definition
ALG	Application-Level Gateway
API	Application Programming Interface
CPE	Customer Premise Equipment
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specification
DSL	Digital Subscriber Line
FTP	File Transfer Protocol
HomePNA	Home Phoneline Network Alliance
HTTP	HyperText Transport Protocol
IAD	Integrated Access Device
ICMP	Internet Control Message Protocol
IGMP	Internet Group Multicast Protocol
IP	Internet Protocol
IPSec	IP Security
LAN	Local Area Network
MAC	Media Access Control
MTU	Maximum Transmission Unit
NAPT	Network Address Port Translation
OAM	Operations and Maintenance
OEM	Original Equipment Manufacturer
PDA	Personal Digital Assistant
POP3	Post Office Protocol 3
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RG	Residential Gateway
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
SPI	Stateful Packet Inspection

Acronym	Definition
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Universal Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network

9. Glossary

PAP Password Authentication Protocol, the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. The Basic Authentication feature built into the HTTP protocol uses PAP.
CHAP Challenge Handshake Authentication Protocol, a type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. The sender and peer must share a predefined secret.
Authentication The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.
Encryption The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.
MPPE Microsoft Point to Point Encryption (MPPE) is a means of representing Point to Point Protocol (PPP) packets in an encrypted form.
Broadcast Broadcasting sends a message to everyone on the network whereas multicasting sends a message to a select list of recipients.
Multicast To transmit a single message to a select group of recipients. A simple example of multicasting is sending an e-mail message to a mailing list. Teleconferencing and videoconferencing also use multicasting, but require more robust protocols and networks.
PPTP Point-to-Point Tunneling Protocol, a technology for creating Virtual Private Networks (VPNs). Because the Internet is essentially an open network, the PPTP is used to ensure that messages transmitted from one VPN node to another are secure. With PPTP, users can dial in to their corporate network via the Internet.
PPTP IP Security, a set of protocols developed to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs).
VPN A Virtual Private Network (VPN) is a private Network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling Protocol and security procedures.
100Base-T Also known as "Fast Ethernet," an Ethernet cable standard with a data transfer rate of up to 100 Mbps.
10Base-T An older Ethernet cable standard with a data transfer rate of up to 10 Mbps.
802.11, 802.11b A family of IEEE (Institute of Electrical and Electronics Engineers)-defined specifications for wireless networks. Includes the 802.11b standard, which supports high-speed (up to 11 Mbps) wireless data transmission.
802.3 The IEEE - defined specification that describes the characteristics of Ethernet (wired) connections.
Access point A device that exchanges data between computers on a network. An access point typically does not have any Firewall or NAT capabilities.
Ad hoc network A solely wireless computer-to-computer network. Unlike an infrastructure network,

an ad hoc network does not include a gateway router.
Adapter Also known as a “network interface card” (NIC). An expansion card or other device used to provide network access to a computer, printer, or other device.
Administrator A person responsible for planning, configuring, and managing the day-to-day operation of a computer network. The duties of an administrator include installing new workstations and other devices, adding and removing individuals from the list of authorized users, archiving files, overseeing password protection and other security measures, monitoring usage of shared resources, and handling malfunctioning equipment.
Bandwidth The amount of information, or size of file, that can be sent through a network connection at one time. A connection with more bandwidth can transfer information more quickly.
Bridge A device that forwards packets of information from one segment of a network to another. A bridge forwards only those packets necessary for communication between the segments.
Broadband connection A high-speed connection, typically 256 Kbps or faster. Broadband services include cable modems and DSL.
Broadband modem A device that enables a broadband connection to access the Internet. The two most common types of broadband modems are cable modems, which rely on cable television infrastructure, and DSL modems, which rely on telephone lines operating at DSL speeds.
Bus A set of hardware lines used for data transfer among the components of a computer system. A bus essentially allows different parts of the system to share data. For example, a bus connects the disk-drive controller, memory, and input/output ports to the microprocessor.
Cable modem A device that enables a broadband connection to access the Internet. Cable modems rely on cable television infrastructure, in other words, the data travels on the same lines as you cable television.
CAT 5 cable Abbreviation for “Category 5 cable.” A type of Ethernet cable that has a maximum data rate of 100 Mbps.
Channel A path or link through which information passes between two devices.
Client Any computer or program that connects to, or requests the services of, another computer or program on a network. For a local area network or the Internet, a client is a computer that uses shared network resources provided by a server.
Client/server network A network of two or more computers that rely on a central server to mediate the connections or provide additional system resources. This dependence on a server differentiating a client/server network from a peer-to-peer network.
Computer name A name that uniquely identifies a computer on the network so that all its shared resources can be accessed by other computers on the network. One computer name cannot be the same as any other computer or domain name on the network.
Crossover cable A type of cable that facilitates network communications. A crossover cable is a cable that is used to interconnect two computers by “crossing over” (reversing) their respective pin contacts.
DHCP Acronym for `Dynamic Host Configuration Protocol’. A TCP/IP protocol that automatically assigns temporary IP addresses to computers on a local area network (LAN). iPECS SBG-1000 supports the use of DHCP. You can use DHCP to share one Internet connection with multiple computers on a network.
Dial-up connection An Internet connection of limited duration that uses a public telephone network rather than a dedicated circuit or some other type of private network.
DMZ Acronym for `demilitarized zone’. A collection of devices and subnets placed between a

private network and the Internet to help protect the private network from unauthorized Internet users.
DNS Acronym for `Domain Name System'. A data query service chiefly used on the Internet for translating host names into Internet addresses. The DNS database maps DNS domain names to IP addresses, so that users can locate computers and services through user-friendly names.
Domain In a networked computer environment, a collection of computers that share a common domain database and security policy. A domain is administered as a unit with common rules and procedures, and each domain has a unique name.
Domain name An address of a network connection that identifies the owner of that address in a hierarchical format: server.organization.type. For example, http://www.whitehouse.gov identifies the Web server at the WhiteHouse, which is part of the U.S. government.
Drive An area of storage that is formatted with a file system and has a drive letter. The storage can be a floppy disk (which is often represented by drive A), a hard disk (usually drive C), a CD-ROM (usually drive D), or another type of disk. You can view the contents of a drive by clicking the drive's icon in Windows Explorer or My Computer. Drive C (also known as the hard disk), contains the computer's operating system and the programs that have been installed on the computer. It also has the capacity to store many of the files and folders that you create.
Driver Within a networking context, a device that mediates communication between a computer and a network adapter installed on that computer.
DSL Acronym for `Digital Subscriber Line'. A constant, high-speed digital connection to the Internet that uses standard copper telephone wires.
DSL modem A device that enables a broadband connection to access the Internet. DSL modems rely on telephone lines that operate at DSL speeds.
Duplex A mode of connection. Full-duplex transmission allows for the simultaneous transfer of information between the sender and the receiver. Half-duplex transmission allows for the transfer of information in only one direction at a time.
Dynamic IP address The IP address assigned (using the DHCP protocol) to a device that requires it. A dynamic IP address can also be assigned to a gateway or router by an ISP.
Edge computer The computer on a network that connects the network to the Internet. Other devices on the network connect to this computer. The computer running the most current, reliable operating system is the best choice to designate as the edge computer.
Ethernet A networking standard that uses cables to provide network access. Ethernet is the most widely-installed technology to connect computers together.
Ethernet cable A type of cable that facilitates network communications. An Ethernet cable comes in a couple of flavors. there is twisted pair, and coax Ethernet cables. Each of these allow data to travel at 10Mbit per second.
Firewall A security system that helps protect a network from external threats, such as hacker attacks, originating outside the network. A hardware Firewall is a connection routing device that has specific data checking settings and that helps protect all of the devices connected to it.
Firmware Software information stored in nonvolatile memory on a device.
Flash memory A type of memory that does not lose data when power is removed from it. Flash memory is commonly used as a supplement to or replacement for hard disks in portable computers. In this context, flash memory either is built in to the unit or, more commonly, is available as a PC Card that can be plugged in to a PCMCIA slot.
FTP Acronym for `File Transfer Protocol'. The standard Internet protocol for downloading, or

transferring, files from one computer to another.
Gateway A device that acts as a central point for networked devices, receives transmitted messages, and forwards them. iPECS SBG-1000 can link many computers on a single network, and can share an encrypted Internet connection with wired and wireless devices.
Gateway address The IP address you use when you make a connection outside your immediate network.
Hexadecimal A numbering system that uses 16 rather than 10 as the base for representing numbers. It is therefore referred to as a base-16 numbering system. The hexadecimal system uses the digits 0 through 9 and the letters A through F (uppercase or lowercase) to represent the decimal numbers 0 through 15. For example, the hexadecimal letter D represents the decimal number 13. One hexadecimal digit is equivalent to 4 bits, and 1 byte can be expressed by two hexadecimal digits.
HomePNA An industry standard that ensures that through existing telephone lines and a registered jack, computer users on a home network can share resources (such as an Internet connection, files, and printers) without interfering with regular telephone service. HomePNA currently offers data transmission speeds of up to 10 Mbps.
HomeRF An industry standard that combines 802.11b and portable phone standards for home networking. It uses frequency hopping (switching of radio frequencies within a given bandwidth to reduce the risk of unauthorized signal interception). HomeRF offers data transmission speeds of up to 1.6 Mbps at distances of up to 150 feet.
Host name The DNS name of a device on a network, used to simplify the process of locating computers on a network.
Hub A device that has multiple ports and that serves as a central connection point for communication lines from all devices on a network. When data arrives at one port, it is copied to the other ports.
IEEE Acronym for `Institute of Electrical and Electronics Engineers'. A society of engineering and electronics professionals that develops standards for the electrical, electronics, computer engineering, and science-related industries. The IEEE (Eye-triple-E) is a non-profit, technical professional association of more than 377,000 individual members in 150 countries. The full name is the Institute of Electrical and Electronics Engineers, Inc., although the organization is most popularly known and referred to by the letters I-E-E-E.
Infrastructure network A network configuration in which wireless devices connect to a wireless access point (such as iPECS SBG-1000) instead of connecting to each other directly.
Internet domain In a networked computer environment, a collection of computers that share a common domain database and security policy. A domain is administered as a unit with common rules and procedures, and each domain has a unique name.
Intranet A network within an organization that uses Internet technologies (such a Web browser for viewing information) and protocols (such as TCP/IP), but is available only to certain people, such as employees of a company. Also called a private network. Some intranets offer access to the Internet, but such connections are directed through a Firewall.
IP Acronym for `Internet Protocol'. The protocol within TCP/IP that is used to send data between computers over the Internet. More specifically, this protocol governs the routing of data messages, which are transmitted in smaller components called packets.
IP address Acronym for `Internet Protocol' address. IP is the protocol within TCP/IP that is used to send data between computers over the Internet. An IP address is an assigned number used to

identify a computer that is connected to a network through TCP/IP. An IP address consists of four numbers (each of which can be no greater than 255) separated by periods, such as 192.168.1.1.
ISO/OSI reference model Abbreviation for “International Organization for Standardization Open Systems Interconnection” reference model. An architecture that standardizes levels of service and types of interaction for computers that exchange information through a communications network. The ISO/OSI reference model separates computer-to-computer communications into seven protocol layers, or levels; each builds on and relies on the standards contained in the levels below it. The lowest of the seven layers deals solely with hardware links; the highest deals with software interactions at the program level. It is a fundamental blueprint designed to help guide the creation of hardware and software for networks.
ISP Acronym for `Internet service provider’. A company that provides individuals or companies access to the Internet.
Kbps Abbreviation of `kilobits per second’. Data transfer speed, as through a modem or on a network, measured in multiples of 1,000 bits per second.
LAN Acronym for `local area network’. A group of computers and other devices dispersed over a relatively limited area (for example, a building) and connected by a communications link that enables any device to interact with any other on the network.
MAC address Abbreviation for `media access control’ address. The address that is used for communication between network adapters on the same subnet. Each network adapter is manufactured with its own unique MAC address.
MAC layer Abbreviation for `media access control’ layer. The lower of two sub layers that make up the data-link layer in the ISO/OSI reference model. The MAC layer manages access to the physical network, so a protocol like Ethernet works at this layer.
mapping A process that allows one computer to communicate with a resource located on another computer on the network. For example, if you want to access a folder that resides on another computer, you “map to” that folder, as long as the computer that holds the folder has been configured to share it.
Mbps Abbreviation of `megabits per second’. A unit of bandwidth measurement that defines the speed at which information can be transferred through a network or Ethernet cable. One megabyte is roughly equivalent to eight megabits.
Modem A device that transmits and receives information between computers.
NAT Acronym for `network address translation’. The process of converting between IP addresses used within a private network and Internet IP addresses. NAT enables all of the computers on a network to share one IP address.
Network A collection of two or more computers that are connected to each other through wired or wireless means. These computers can share access to the Internet and the use of files, printers, and other equipment.
Network adapter Also known as a `network interface card’ (NIC). An expansion card or other device used to provide network access to a computer, printer, or other device.
Network name The single name of a grouping of computers that are linked together to form a network.
Network printer A printer that is not connected directly to a computer, but is instead connected directly to a network through a wired or wireless connection.
Packet A unit of information transmitted as a whole from one device to another on a network.
PC Card A peripheral device that adds memory, mass storage, modem capability, or other

networking services to portable computers.
PCI Acronym for `Peripheral Component Interconnect'. A specific bus type designed to be used with devices that have high bandwidth requirements.
PCI card A card designed to fit into a PCI expansion slot in a personal computer. PCI cards provide additional functionality; for example, two types of PCI cards are video adapters and network interface cards. See PCI.
PCI expansion slot A connection socket designed to accommodate PCI cards.
PCMCIA Acronym for `Personal Computer Memory Card International Association'. A nonprofit organization of manufacturers and vendors formed to promote a common technical standard for PC Card-based peripherals and the slot designed to hold them, primarily on portable computers and intelligent electronic devices.
Peer-to-peer network A network of two or more computers that communicate without using a central server. This lack of reliance on a server differentiates a peer-to-peer network from a client/server network.
PING A protocol for testing whether a particular computer is connected to the Internet by sending a packet to the computer's IP address and waiting for a response.
Plug and Play A set of specifications that allows a computer to automatically detect and configure various peripheral devices, such as monitors, modems, and printers.
Port A physical connection through which data is transferred between a computer and other devices (such as a monitor, modem, or printer), a network, or another computer. Also, a software channel for network communications.
PPPoE Acronym for `Point-to-Point Protocol over Ethernet'. A specification for connecting users on an Ethernet network to the Internet by using a broadband connection (typically through a DSL modem).
Profile A computer-based record that contains an individual network's software settings and identification information.
Protocol A set of rules that computers use to communicate with each other over a network.
Resource Any type of hardware (such as a modem or printer) or software (such as an application, file, or game) that users can share on a network.
Restore factory defaults The term used to describe the process of erasing your iPECS SBG-1000's current settings to restore factory settings. You accomplish this by holding 'Reset to Default' button for five or more seconds. Note that this is different from resetting the iPECS SBG-1000.
RJ-11 connector An attachment used to join a telephone line to a device such as a modem or the external telephone lines.
RJ-45 connector An attachment found on the ends of all Ethernet cables that connects Ethernet (wired) cables to other devices and computers
Server A computer that provides shared resources, such as storage space or processing power, to network users.
Shared folder A folder (on a computer) that has been made available for other people to use on a network.
Shared printer A printer (connected to a computer) that has been made available for other people to use on a network.
Sharing To make the resources associated with one computer available to users of other computers on a network.

SNTP Acronym for `Simple Network Time Protocol'. A protocol that enables client computers to synchronize their clocks with a time server over the Internet.
SSID Acronym for `Service Set Identifier', also known as a "wireless network name." An SSID value uniquely identifies your network and is case sensitive.
Static IP address A permanent Internet address of a computer (assigned by an ISP).
Straight-through cable A type of cable that facilitates network communications. An Ethernet cable comes in a couple of flavors. There is twisted pair, and coax Ethernet cables. Each of these allow data to travel at 10Mbit per second. Unlike the Crossover cable, straight-through cable has the same order of pin contacts on each end-plug of the cable.
Subnet A distinct network that forms part of a larger computer network. Subnets are connected through routers and can use a shared network address to connect to the Internet.
Subnet mask Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address. Similar in form to an IP address and typically provided by an ISP. An example of a subnet mask value is 255.255.0.0.
Switch A central device that functions similarly to a hub, forwarding packets to specific ports rather than broadcasting every packet to every port. A switch is more efficient when used on a high-volume network.
Switched network A communications network that uses switching to establish a connection between parties.
Switching A communications method that uses temporary rather than permanent connections to establish a link or to route information between two parties. In computer networks, message switching and packet switching allow any two parties to exchange information. Messages are routed (switched) through intermediary stations that together serve to connect the sender and the receiver.
TCP/IP Acronym for `Transmission Control Protocol/Internet Protocol'. A networking protocol that allows computers to communicate across interconnected networks and the Internet. Every computer on the Internet communicates by using TCP/IP.
Throughput The data transfer rate of a network, measured as the number of kilobytes per second transmitted.
USB Acronym for `universal serial bus'. USB (Universal Serial Bus) is a plug-and-play interface between a computer and add-on devices (such as audio players, joysticks, keyboards, telephones, scanners, and printers). With USB, a new device can be added to your computer without having to add an adapter card or even having to turn the computer off.
USB adapter A device that connects to a USB port.
USB connector The plug end of the USB cable that is connected to a USB port. It is about half an inch wide, rectangular and somewhat flat.
USB port A rectangular slot in a computer into which a USB connector is inserted.
UTP Acronym for `unshielded twisted pair'. A cable that contains one or more twisted pairs of wires without additional shielding. It's more flexible and takes less space than a shielded twisted pair (STP) cable, but has less bandwidth.
Virtual server One of multiple Web sites running on the same server, each with a unique domain name and IP address.
WAN Acronym for `wide area network'. A geographically widespread network that might include

many linked local area networks.
Wi-Fi A term commonly used to mean the wireless 802.11b standard.
Wireless Refers to technology that connects computers without the use of wires and cables. Wireless devices use radio transmission to connect computers on a network to one another. Radio signals can be transmitted through walls, ceilings, and floors, so you can connect computers that are in different rooms in the house without physically attaching them to one another.
Wireless access point A device that exchanges data between wireless computers or between wireless computers and wired computers on a network.
Wireless network name The single name of a grouping of computers that are linked together to form a network.
Wireless security A wireless network encryption mechanism that helps to protect data transmitted over wireless networks.
WLAN Acronym for “wireless local area network.” A network that exclusively relies on wireless technology for device connections.

10. Licensing Acknowledgement and Source Code Offering

The iPECS SBG-1000 product may contain code that is subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), and BSD (BSDS) license.
Those parts of iPECS SBG-1000 software are based on Jungo's OpenRG Solution, and detailed information on licenses and code request is provided on Jungo's Open Source Web page (http://www.jungo.com/openrg/sp_os.html). The Web page contains:

- With respect to GPL/LGPL: the code package names, license types and locations for the license files, and
- With respect to BSD (BSDS): the code package names with the license texts.

To receive the source code of the GPL/LGPL packages, please refer to Jungo's GNU Code Requests Web page (http://www.jungo.com/openrg/download_gpl.html).