BODi rS 1000 Series
WAN Bandwidth on Demand Internet Network Appliance

User Manual

This is a Class A device and is not intended for use in a residential environment.

Sales Office: **+1 (301) 975-1000**
Technical Support: **+1 (301) 975-1007**
E-mail: **support@patton.com**
WWW: **www.patton.com**

Part Number: **07MBD1000-UM, Rev. A**
Revised: **November 28, 2012**

Patton Electronics Company, Inc.
7622 Rickenbacker Drive
Gaithersburg, MD 20879 USA
Tel: +1 (301) 975-1000
Fax: +1 (301) 869-9293
Support: +1 (301) 975-1007
Web: www.patton.com
E-mail: support@patton.com

Copyright © 2012, Patton Electronics Company. All rights reserved.
The information in this document is subject to change without notice. Patton Electronics assumes no liability for errors that may appear in this document.

Important Information

To use virtual private network (VPN) and/or AES/DES/3DES encryption capabilities with the BODi rS, you may need to purchase additional licenses, hardware, software, network connection, and/or service. Contact sales@patton.com or +1 (301) 975-1000 for assistance.

Warranty Information

Patton Electronics warrants all BODi rS components to be free from defects, and will—at our option—repair or replace the product should it fail within one year from the first date of the shipment.

This warranty is limited to defects in workmanship or materials, and does not cover customer damage, abuse or unauthorized modification. If the product fails to perform as warranted, your sole recourse shall be repair or replacement as described above. Under no condition shall Patton Electronics be liable for any damages incurred by the use of this product. These damages include, but are not limited to, the following: lost profits, lost savings and incidental or consequential damages arising from the use of or inability to use this product. Patton Electronics specifically disclaims all other warranties, expressed or implied, and the installation or use of this product shall be deemed an acceptance of these terms by the user.

Summary Table of Contents

Table of Contents

List of Figures

List of Tables

About this guide

This guide describes the BODi rS BD1000 hardware, installation and basic configuration.

Audience

This guide is intended for the following users:

- Operators
- Installers
- Maintenance technicians

Structure

This guide contains the following chapters and appendices:

For best results, read the contents of this guide *before* you install the BODi rS BD1000.

Precautions

Notes, cautions, and warnings, which have the following meanings, are used throughout this guide to help you become aware of potential problems. ***Warnings*** are intended to prevent safety hazards that could result in personal injury. ***Cautions*** are intended to prevent situations that could result in property damage or impaired functioning.

Note A note presents additional information or interesting sidelights.

IMPORTANT

The alert symbol and IMPORTANT heading calls attention to important information.

CAUTION

The alert symbol and CAUTION heading indicate a potential hazard. Strictly follow the instructions to avoid property damage.

CAUTION

The shock hazard symbol and CAUTION heading indicate a potential electric shock hazard. Strictly follow the instructions to avoid property damage caused by electric shock.

WARNING

The alert symbol and WARNING heading indicate a potential safety hazard. Strictly follow the warning instructions to avoid personal injury.

WARNING

The shock hazard symbol and WARNING heading indicate a potential electric shock hazard. Strictly follow the warning instructions to avoid injury caused by electric shock.

Safety when working with electricity


WARNING

- **Do not open the device when the power cord is connected. For systems without a power switch and without an external power adapter, line voltages are present within the device when the power cord is connected.**
- **For devices with an external power adapter, the power adapter shall be a listed *Limited Power Source* The mains outlet that is utilized to power the device shall be within 10 feet (3 meters) of the device, shall be easily accessible, and protected by a circuit breaker in compliance with local regulatory requirements.**
- **For AC powered devices, ensure that the power cable used meets all applicable standards for the country in which it is to be installed.**
- **For AC powered devices which have 3 conductor power plugs (L1, L2 & GND or Hot, Neutral & Safety/Protective Ground), the wall outlet (or socket) must have an earth ground.**
- **For DC powered devices, ensure that the interconnecting cables are rated for proper voltage, current, anticipated temperature, flammability, and mechanical serviceability.**
- **WAN, LAN & PSTN ports (connections) may have hazardous voltages present regardless of whether the device is powered ON or OFF. PSTN relates to interfaces such as telephone lines, FXS, FXO, DSL, xDSL, T1, E1, ISDN, Voice, etc. These are known as "hazardous network voltages" and to avoid electric shock use caution when working near these ports. When disconnecting cables for these ports, detach the far end connection first.**
- **Do not work on the device or connect or disconnect cables during periods of lightning activity**


WARNING

This device contains no user serviceable parts. This device can only be repaired by qualified service personnel.

In accordance with the requirements of council directive 2002/96/EC on Waste of Electrical and Electronic Equipment (WEEE), ensure that at end-of-life you separate this product from other waste and scrap and deliver to the WEEE collection system in your country for recycling.

CAUTION

Always follow ESD prevention procedures when removing and replacing cards.

Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the chassis frame to safely channel unwanted ESD voltages to ground.

To properly guard against ESD damage and shocks, the wrist strap and cord must operate effectively. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

General observations

- Clean the case with a soft slightly moist anti-static cloth
- Place the unit on a flat surface and ensure free air circulation
- Avoid exposing the unit to direct sunlight and other heat sources
- Protect the unit from moisture, vapors, and corrosive liquids

Typographical conventions used in this document

This section describes the typographical conventions and terms used in this guide.

General conventions

The procedures described in this manual use the following text conventions:

Table 1. General conventions

Convention	Meaning
Garamond blue type	Indicates a cross-reference hyperlink that points to a figure, graphic, table, or section heading. Clicking on the hyperlink jumps you to the reference. When you have finished reviewing the reference, click on the **Go to Previous View** button in the Adobe® Acrobat® Reader toolbar to return to your starting point.
Futura bold type	Commands and keywords are in **boldface** font.
Futura bold-italic type	Parts of commands, which are related to elements already named by the user, are in ***boldface italic*** font.
Italicized Futura type	Variables for which you supply values are in *italic* font
Futura type	Indicates the names of fields or windows.
Garamond bold type	Indicates the names of command buttons that execute an action.
< >	Angle brackets indicate function and keyboard keys, such as <SHIFT>, <CTRL>, <C>, and so on.
[ ]	Elements in square brackets are optional.
{a | b | c}	Alternative but required keywords are grouped in braces ({ }) and are separated by vertical bars (|)
`screen`	Terminal sessions and information the system displays are in `screen font`.
node	The leading IP address or nodename of a BODi rS is substituted with ***node*** in ***boldface italic*** font.
SN	The leading **SN** on a command line represents the nodename of the BODi rS
#	An hash sign at the beginning of a line indicates a comment line.

Chapter 1 General Information

Chapter contents

BODi rS BD1000 Overview

Patton's BODi rS ....

Figure 1. BODi rS BD1000

Network Features

The BODi rS BD1000 includes the following key features:

- **WAN**
  - Multiple public IP support (DHCP, PPPoE, Static IP Address)
  - 10/100 Mbps Connection in Full/Half Duplex
  - USB Mobile Connection
  - Network Address Translation (NAT) / Port Address Translation (PAT)
  - Inbound and Outbound NAT mapping
  - Multiple static IP addresses per WAN Connection
  - MAC address clone
  - Customizable MTU and MSS values
  - WAN connection health check
  - Dynamic DNS (Supported service providers: changeip.com, dyndns.org, no-ip.org and tzo.com)
- **LAN**
  - DHCP server on LAN
  - Static routing rules
  - Local DNS

- **VPN**
  - Secure Site-to-Site VPN
  - VPN load balancing and failover among selected WAN connections
  - Site-to-Site VPN bandwidth bonding
  - Ability to route Internet traffic to a remote VPN peer
  - Optional pre-shared key setting
  - Site-to-Site VPN Throughput, Ping and Traceroute Test
  - PPTP server
  - PPTP and IPsec passthrough
- **Inbound Traffic Management**
  - TCP/UDP traffic redirection to dedicated LAN server(s)
- **Outbound Policy**
  - Link load distribution per TCP/UDP service
  - Persistent routing for specified source and/or destination IP addresses per TCP/UDP service
  - Prioritize and route traffic to VPN tunnels with Priority and Enforced algorithms
- **WLAN Controller**
  - Configure and manage AP devices
  - Review the status of connected AP
- **QoS**
  - Quality of Service for different applications and custom protocols
  - User Group classification for different service levels
  - Bandwidth usage control and monitoring on group- and user- level
  - Application Prioritization for custom protocols and DSL optimization
- **Firewall**
  - Outbound (LAN to WAN) firewall rules
  - Inbound (WAN to LAN) firewall rules per WAN connection
  - Intrusion detection and prevention
  - Specification of NAT mappings

- **Other Supported Features**
  - User-friendly web-based administration interface
  - HTTP and HTTPS support for Web Admin Interface
  - Configurable web administration port and administrator password
  - Firmware upgrades, configuration backups, Ping, and Traceroute via Web Admin Interface
  - Remote web based configuration (via WAN and LAN interfaces)
  - Time server synchronization
  - SNMP
  - Email notification
  - Read-only user for Web Admin
  - Authentication and Accounting by RADIUS server for Web Admin
  - Built-in WINS Servers
  - Syslog
  - SIP passthrough
  - PPTP packet passthrough
  - Event Log
  - Active Sessions
  - Client List
  - WINS Client List
  - UPnP / NAT-PMP
  - Real-Time, Daily and Monthly Bandwidth Usage reports and charts

BODi rS BD1000 Panels

Rear Panel

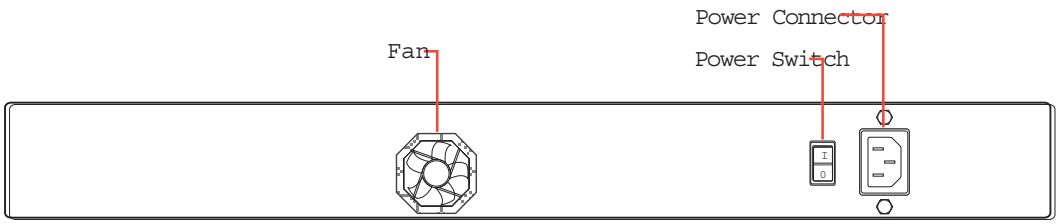


Figure 2. BODi rS rear panel connectors

Front Panel

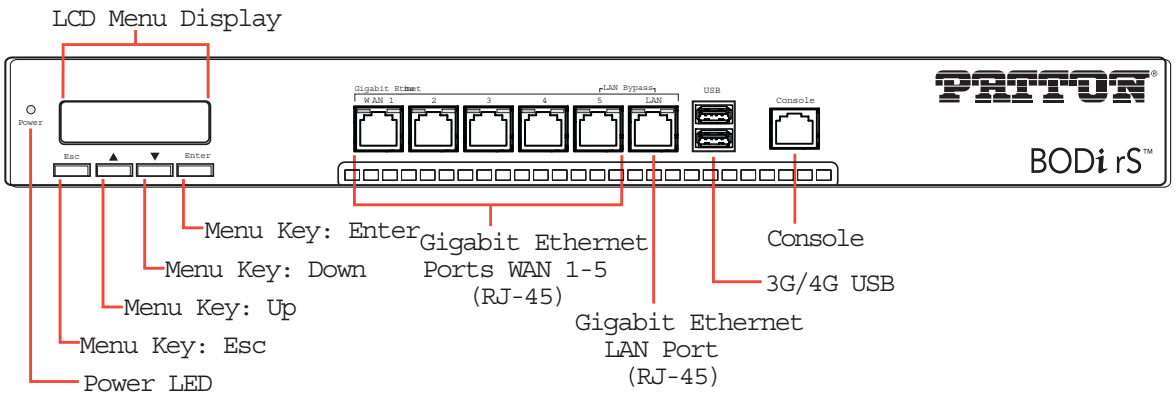


Figure 3. BODi rS front panel connectors

Table 2. BODi rS LEDs

LED	Indication	Description
Power	OFF	System is not connected to a power source
	GREEN	System has a power connection
LAN/WAN Right LED	ORANGE	1000 Mbps
	GREEN	100 Mbps
	OFF	10 Mbps
LAN/WAN Left LED	ON	Port is connected without traffic
	FLASHING	Transferring data
	OFF	Port is not connected

LCD Display Menu

Table 3. LCD Menu

Menu Category		Item	Description
> HA State: Master/Slave		> LAN IP	–
		> VIP	–
> System Status	**> System**	> Firmware Ver.	Shows firmware version
		> Serial Number	Shows serial number
		> System Time	Shows current time
		> System Uptime	Shows system uptime since last reboot
		> CPU Load	Shows current CPU loading 0-100%
		> LAN	–
		> Status	Shows LAN port physical status
		> IP Address	Shows LAN IP address
		> Subnet Mask	Shows LAN subnet mask
	> Link Status	> WAN 1-5...	Shows Connected/Disconnected and IP address list
	> VPN Status	> VPN Profile 1-2...	Shows Connected/Disconnected
	> Link Usage	> Throughput in	Shows transfer rate in Kbps
		> WAN 1-5...	–
		> Throughput out	Shows transfer rate in Kbps
		> WAN 1-5...	–
	> Data Transfer	> WAN 1-5...	Shows volume transferred since last reboot in MB
> Maintenance	**> Reboot**	> Yes/No	Reboot the unit
	> Factory Default	> Yes/No	Restore factory default settings
> LAN Config	**> Port Speed**	> LAN/WAN 1-5...	Shows port speed: Auto,10baseT-FD, 10baseT-HD, 100baseTx-FD, 100baseTx-HD, 1000baseTx-FD

Restoring Factory Default Settings: Use the buttons on the front panel to control the **LCD menu** to go to **Maintenance > Factory Default.** Choose **Yes** to confirm and the factory default settings will be restored.

Note All user settings will be lost after restoring the factory default settings. Backing up the configuration regularly is strongly recommended.

Chapter 2 Installing the BODi rS

Chapter contents

Planning the Installation

Before installing the BODi rS, gather the following information and materials:

- At least one Internet/WAN access account.
- For each network connection, one 10/100BaseT UTP cable with RJ45 connector, or one 1000BaseT Cat5E UTP cable for the Gigabit port or one USB modem for the USB WAN port.
- A computer with TCP/IP network protocol and a web browser installed. Supported browsers include Microsoft Internet Explorer 7.0 or above, Mozilla Firefox 3.0 or above, Apple Safari 3.1.1 or above, and Google Chrome 2.0 or above.

Setting Up the Network

Constructing the Network

At the high level, construct the network according to the following steps:

1. With an Ethernet cable, connect a computer to one of the LAN ports on the BODi rS. Repeat with different cables to connect up to four computers.
2. With another Ethernet cable, connect the WAN/broadband modem to one of the WAN ports on the BODi rS. Repeat using different cables to connect other WAN/broadband connections. Connect a USB modem to the USB WAN port.
3. Connect the power adapter to the power connector on the rear panel of the BODi rS, and then plug into a power outlet.

Figure 4 illustrates the network configuration:

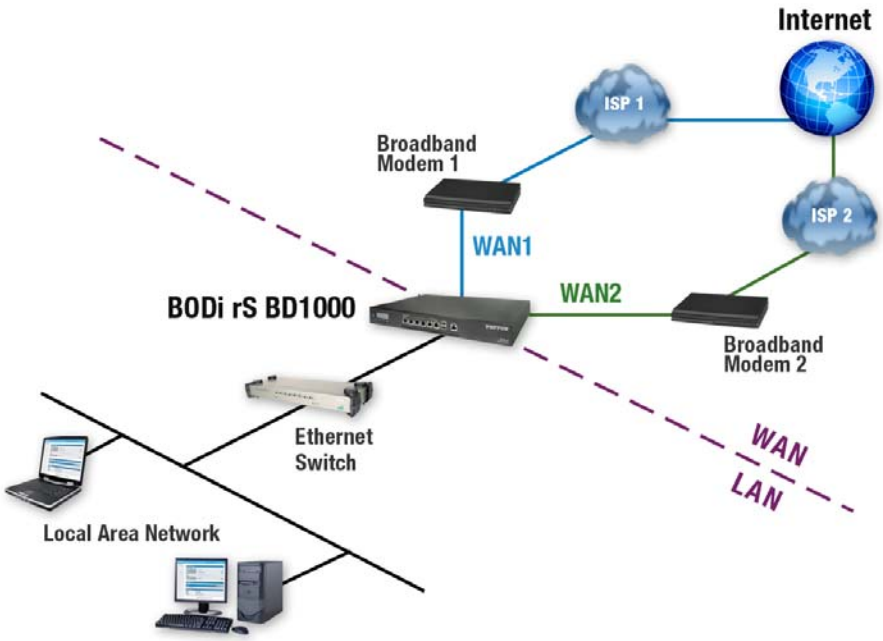


Figure 4. BODi rS Network

Configuring the Network Environment

To ensure that the BODi rS works properly in the LAN environment and can access the Internet via the WAN connections, refer to the following setup procedures:

- To physically connect the LAN and WAN interfaces, refer to "Connecting the BODi rS Interfaces" on page 27.
- To initially configure the LAN and WAN interfaces refer to "Connecting to the Web Admin Interface" on page 28.
- To configure advanced settings for the LAN and WAN interfaces, refer to Chapter 3, "Configuring LAN & WAN Interfaces" on page 32.

Connecting the BODi rS Interfaces

Connecting the Ethernet Interfaces

The BODi rS includes one LAN Ethernet port and five Gigabit Ethernet WAN ports on the front panel. Use a straight-through or cross-over Ethernet cable to connect the Ethernet RJ-45 ports.

Refer to Chapter 3, "Configuring LAN & WAN Interfaces" on page 32 for information about configuring the LAN and WAN interfaces via the Web Admin interface.

Connecting the USB Interfaces

The BODi rS provides two USB 2.0 ports on the front panel. You can use the USB ports to connect cellular modems.

Refer to Chapter 3, "Configuring LAN & WAN Interfaces" on page 32 for information about configuring USB WAN interfaces via the Web Admin interface.

Connecting to the Web Admin Interface

After physically connecting the LAN, you may use the Web Admin interface to configure the BODi rS interfaces. To login to the Web Admin Interface:

1. Start a web browser on a computer that is connected to the BODi rS through the LAN port.
2. Enter the following default LAN IP address in the address field of the web browser: **http://192.168.1.1**
3. Enter the username *admin* and password *admin* to login to the Web Admin Interface. This is the default username and password of the BODi rS. (You may change the Admin and Read-only User Password by clicking on **System > Admin Security** in the Web Admin Interface).
4. After successfully logging in, the **Dashboard** of the Web Admin Interface displays:

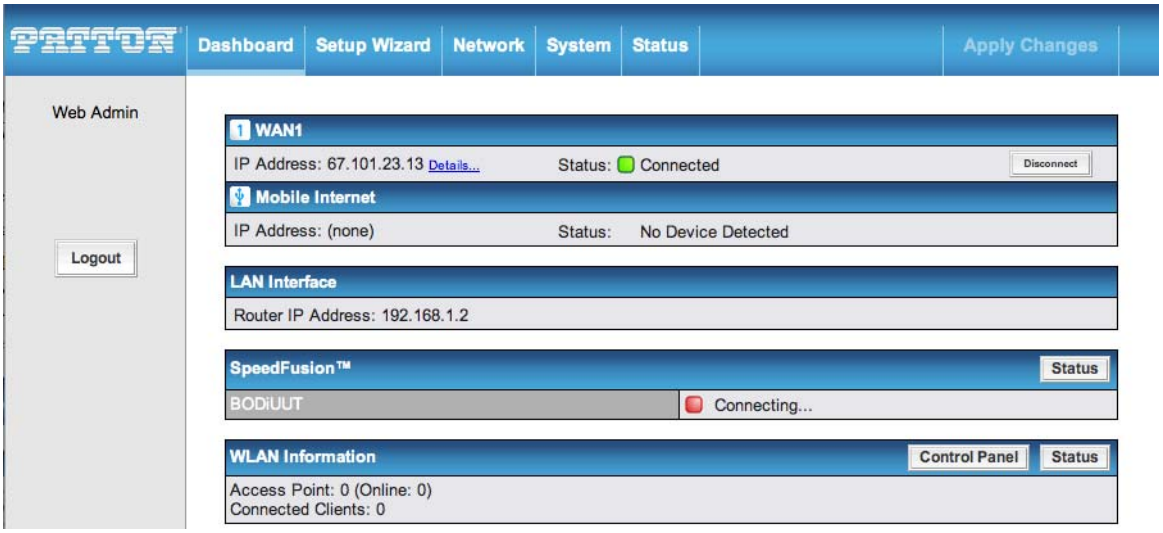


Figure 5. Web Admin Interface home page

The Web Admin Interface **Dashboard** shows the current WAN, LAN, WLAN settings and statuses. The **Dashboard** enables you to change the priority of the WAN connections and switch the Wi-Fi AP connections off or on. For more information about configuring these connections, refer to Chapter 3, "Configuring LAN & WAN Interfaces" on page 32.

The **Device Information** section shows the details about the BODi rS system, including the Firmware version and system uptime. For more information about viewing system status information, refer to Chapter 11, "Managing Status Settings" on page 133.

Note Configuration changes will only take effect after clicking the **Save** button at the bottom of each page. The **Apply Changes** button causes the changes to be saved and applied.

Advanced settings can be configured from the **Network** menu. WAN connections can be configured by entering the corresponding WAN connection information at: **Network > Interfaces > WAN**. For more information about configuring these connections, refer to Chapter 3, "Configuring LAN & WAN Interfaces" on page 32.

Using the Setup Wizard

The Setup Wizard simplifies the task of configuring WAN connection(s) by guiding the configuration process step by step.

1. After logging into the Web Admin Interface, click on the **Setup Wizard** link at the top of the screen. Click **Next** to begin.
2. On the next screen, select **Yes** if you want to set up Drop-in mode in the Setup Wizard.

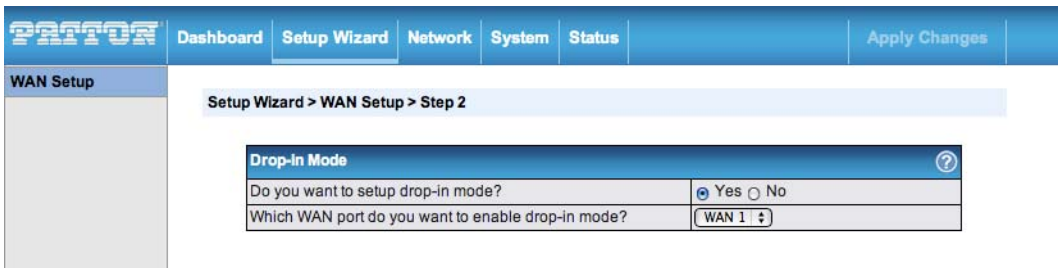


Figure 6. Setup Wizard > Drop-in Mode

3. Click on the appropriate check box(es) to select the WAN connection(s) to be configured. If you have chosen to configure Drop-in mode in Setup Wizard, the box of WAN port that is to be configured in Drop-in mode will be checked by default.

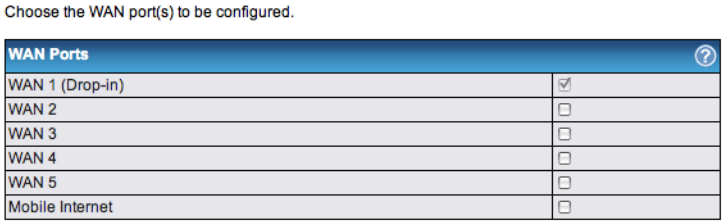


Figure 7. Setup Wizard > WAN Port Selection

4. If Drop-in mode is going to be configured, the Setup Wizard will move on to Drop-in Settings.

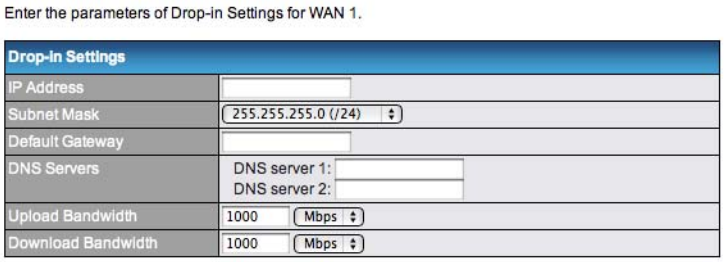


Figure 8. Setup Wizard > Drop-in Mode Configuration

5. Select the connection type for WAN connection(s) from the following screen:

Choose a connection method for WAN 1.

Connection Method	
Method	Select
Static IP	○
DHCP	◉
PPPoE	○
Disable	○

Figure 9. Setup Wizard > Connection Method

Depending on the selection of connection type, further configuration may be needed. For example, PPPoE and Static IP require additional settings for the selected WAN port. Refer to "Configuring the WAN Interface" on page 39 for details on setting up DHCP, Static IP and PPPoE.

6. If **Mobile Internet Connection** is checked, Setup Wizard will move on to Operator settings.

Enter the parameters of Mobile Operator Settings for Mobile Internet.

Mobile Operator Settings	
APN	
Login ID	
Password	
Dial Number	

Figure 10. Setup Wizard > Mobile Internet Operator Settings

7. If **Custom Mobile Operator Settings** is selected, APN parameters are required to be entered. Some service providers may charge a fee for connecting to a different APN. Please consult the service provider for the correct settings.

Select whether Operator Settings for Mobile Internet will be automatically detected or customized.

Operator Settings (for HSPA/EDGE/GPRS only)	
Settings	Select
Auto	○
Custom	◉

Figure 11. Setup Wizard > Custom Mobile Operator Settings

8. Click on the appropriate check box(es) to select the preferred WAN connection(s). Connection(s) not selected in this step will be used as back up only. Click **Next** to continue.

Choose the preferred WAN Port(s) that is to be used as primary connection. The port(s) not selected in this step will only be used when none of the connection of the preferred port is up.

Preferred WAN Port Selection	
Port	Preferred
WAN 1	☑
Mobile Internet	☑

Figure 12. Setup Wizard > Preferred WAN Interfaces

9. Choose the time zone of your Country/Region. Check the box **Show all** to display all time zone options.

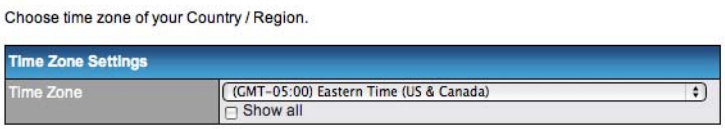


Figure 13. Setup Wizard > Time Zone

10. Check the following screen to make sure all settings have been configured correctly, and then click **Save Settings** to confirm.

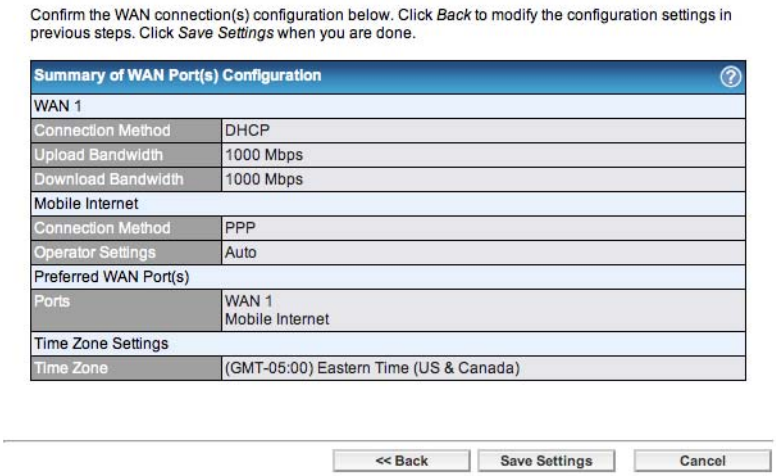


Figure 14. Setup Wizard > Summary

11. After finishing the last step in the Setup Wizard, click **Apply Changes** on the page header to allow the configuration changes to take effect.

Chapter 3 Configuring LAN & WAN Interfaces

Chapter contents

Introduction

This chapter describes setting up Ethernet access through the physical LAN, WAN and USB interfaces. For information about setting up the LAN interface, see "Configuring the LAN Interface" on page 33. For information about setting up the WAN interface, see "Configuring the WAN Interface" on page 39.

Configuring the LAN Interface

This section describes configuring the basic settings and Wi-Fi AP settings for the LAN using the BD1000 Web Admin Interface.

Basic Settings

To configure basic settings for the LAN, click on **Network > Interfaces > LAN** in the Web Interface.

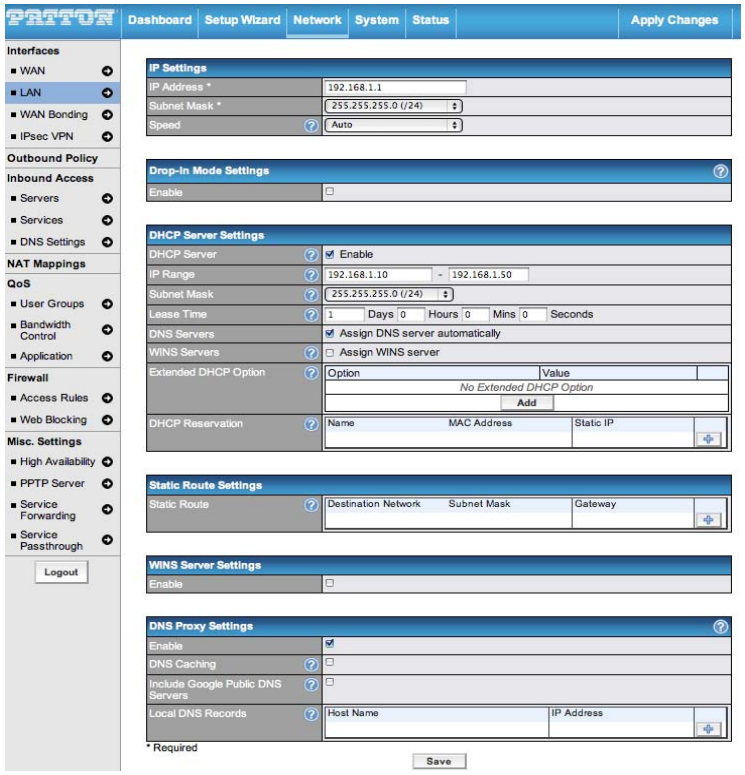


Figure 15. Network > LAN > Basic Settings

The following sections provide information for configuring the LAN on the **Basic Settings** configuration page:

- "IP Settings" on page 34
- "DHCP Server Settings" on page 35
- "Static Route Settings" on page 36
- "WINS Server Settings" on page 36
- "DNS Proxy Settings" on page 36

IP Settings

Table 4. LAN: IP Settings

Field	Description
IP Address	The IP address for the Ethernet LAN management port.
Subnet Mask	The subnet mask for the Ethernet LAN management port.
Speed	The speed of the Ethernet LAN management port. By default, **Auto** is selected and the appropriate data speed is automatically detected by the BD1000. In the event of negotiation issues, the port speed can be manually specified to circumvent the issues. You can also choose whether or not to advertise the speed to the peer by selecting the **Advertise Speed** checkbox.

Drop-in Mode Settings

Note Refer to "Configuring Drop-in Mode" on page 37 for detailed information on using the BD1000 and Drop-in mode.

Table 5. LAN: Drop-in Mode Settings

Field	Description
Enable	Check the box to enable the Drop-in Mode feature. Drop-in Mode eases the installation of the BD1000 on a live network between the existing Firewall and Router, such that no configuration changes are required on existing equipment.
WAN for Drop-in Mode	Select the WAN port to be used for Drop-in mode. If the WAN port for LAN Bypass is selected, High Availability feature will be disabled automatically.
WAN Default Gateway	Enter the WAN router's IP address in this field. If there are more hosts other than the router on the WAN segment, check the box **I have other host(s) on WAN segment** and enter the IP address of the hosts that needs to access LAN devices or to be accessed by others.
WAN DNS Servers	Enter the selected WAN's corresponding DNS server IP addresses.

DHCP Server Settings

Table 6. LAN: DHCP Server Settings

Field	Description
DHCP Server	When enabled, the DHCP server automatically assigns an IP address to each computer that is connected via the LAN and configured to obtain an IP address via DHCP. The DHCP server can prevent IP address collision on LAN.
IP Range & Subnet Mask	Allocates a range of IP addresses that the DHCP Server will assign to LAN computers.
Lease Time	Specifies the length of time that an IP address of a DHCP client remains valid. Upon expiration of the Lease Time, the assigned IP address will no longer be valid and the renewal of the IP address assignment will be required.
DNS Servers	Allows manual input of DNS server addresses to be offered to the DHCP clients. If the **Assign DNS server automatically** option is selected, the BD1000's built-in DNS server address (i.e. LAN IP address) will be offered.
WINS Server	Specifies the Windows Internet Name Service (WINS) server. You may choose to use the Built-in WINS server or External WINS servers. When Site-to-Site VPN is connected, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their DHCP WINS Servers setting. Therefore, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If enabled, you can view a list of WINS clients by clicking **Status > WINS Clients**.
Extended DHCP Option	Specifies the value of additional Extended DHCP Options defined in RFC 2132 (in addition to standard DHCP options like. DNS server address, gateway address, and subnet mask). In this case, you can pass additional configuration information to LAN hosts. To define an Extended DHCP Option, click the **Add** button, choose the option that you want to define and enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text field. You may only define each option one time.
DHCP Reservation	Reserves the assignment of fixed IP addresses for a list of computers on the LAN. The MAC addresses identify the computers that will be assigned fixed IP addresses on the LAN. The fixed IP address assignment is displayed as a cross-reference list between the computers' Name, MAC addresses and fixed IP addresses. The field Name (an optional field) is used to define a name to represent the device. MAC addresses should be in the format of AA:BB:CC:DD:EE Press + to create a new record. Press ✕ to remove a record. Reserved client information can be imported from the Client List, located on the **Status > Client List** configuration page. For more details, refer to Chapter 11, "Managing Status Settings" on page 133.

Static Route Settings

Table 7. LAN: Static Route Settings

Field	Description
Static Route	Defines static routing rules for the LAN segment. A static route consists of the network address, subnet mask and gateway address. The address and subnet mask values are in the format of **w.x.y.z**. The local LAN subnet and subnets behind the LAN will be advertised to the VPN. Remote routes sent over the VPN will also be accepted. Any VPN member will be able to route to the local subnets. Press + to create a new route. Press ✕ to remove a route.

WINS Server Settings

Table 8. LAN: WINS Server Settings

Field	Description
Enable	Check the box to enable the WINS Server. A list of WINS clients display on the **Status > WINS Clients** configuration page.

DNS Proxy Settings

Table 9. LAN: DNS Proxy Settings

Field	Description
Enable	Check the box to enable the DNS Proxy feature.
DNS Caching	Enables DNS Caching on the built-in DNS proxy server. When enabled, queried DNS replies will be cached until the records' Time To Live (TTL) limit has been reached. This feature can help improve the DNS lookup time. However, it cannot return the most updated result for frequently updated DNS records. Default = **Disabled**.
Use Google DNS Server as Backup	Check the box to enable the Google DNS feature, and the BD1000 will automatically use the Google DNS Server as a backup DNS server. The DNS proxy server will forward DNS requests to Google's Public DNS Servers in case all of the WAN connections' DNS servers become unavailable. Default = **Disabled**.
Local DNS Records	Defines custom local DNS records. A static local DNS record consists of a Host Name and an IP Address. When looking up the Host Name from the LAN to LAN IP of the BD1000, the corresponding IP Address will be returned. Press + to create a new record. Press ✕ to remove a record.

Configuring Drop-in Mode

Drop-in Mode (or transparent bridging mode) eases the installation of the BD1000 on a live network between the firewall and router, such that changes to the settings of existing equipment are not required. The following diagram illustrates the Drop-in Mode setup:

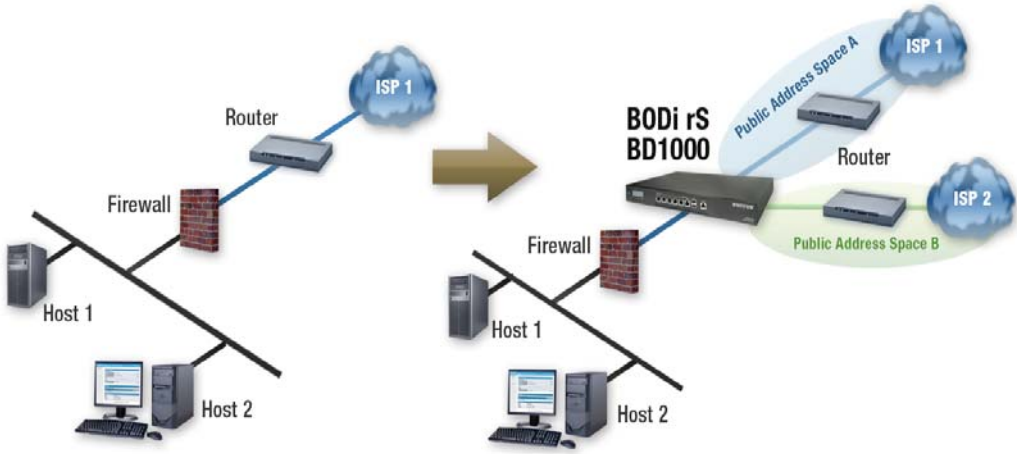


Figure 16. Drop-in Mode Application Diagram (1)

Check the box to **Enable** the Drop-in Mode. After enabling this feature and selecting the WAN for Drop-in mode, various settings including the WAN's connection method and IP address will be automatically updated.

When Drop-in Mode is enabled, the LAN and the WAN for Drop-in Mode ports will be bridged. Traffic going in between the LAN hosts and WAN router will be forwarded to each other. In this case, the hosts on both sides will not notice any IP or MAC address change.

After successfully setting up the BD1000 as part of the network via Drop-in Mode, a BD1000 will accommodate four additional WAN connections.

Note The PPTP server will be disabled under Drop-in Mode.

To enable Drop-in Mode, use the following steps:

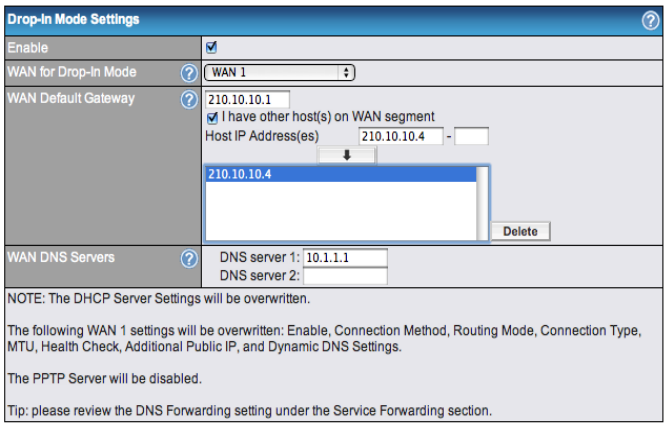


Figure 17. Network > Interfaces > LAN > Drop-in Mode

1. Click on **Network > Interfaces > LAN** and check the **Enable** box in the Drop-in Mode section. (After checking the **Enable** box, most network settings for WAN1 will be hidden from the Web Administration Interface.)
2. Enter the IP address of the WAN1 router in the **WAN Default Gateway** field. Ensure that the BD1000 IP subnet is the same as the Firewall's WAN port and the Router's LAN port.
3. If there are hosts other than the router existing on the WAN segment of the BD1000, check the box for **I have other host(s) on WAN segment**, enter the IP address(es) of the host(s), and then click the down-arrow to add the hosts.

The figure below illustrates the BD1000 in Drop-in mode:

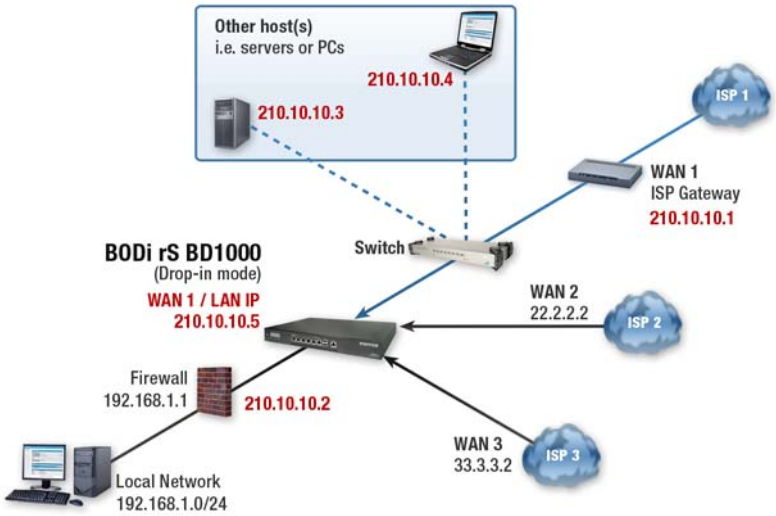


Figure 18. Drop-in Mode Application Diagram (2)

Configuring the WAN Interface

This section describes managing the WAN settings using the BD1000 Web Admin Interface. From the **Dashboard**, click on **Network** > **Interfaces** > **WAN Bonding** to reach the main WAN configuration page.

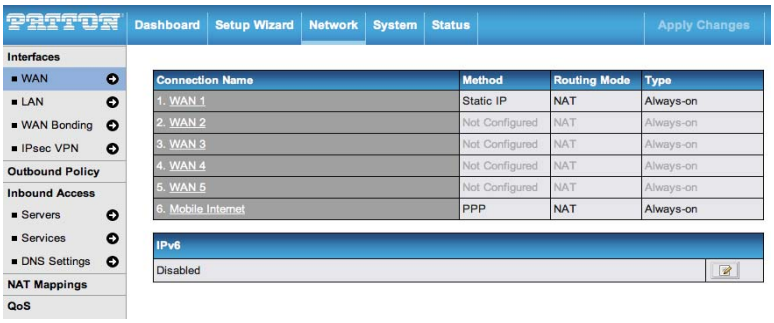


Figure 19. Network > Interfaces > WAN

Table 10. WAN: General Connection Settings

Field	Description
WAN Connection Name	Defines a unique name to represent the WAN connection.
Enable	Select **Yes** to enable the connection; select **No** to disable.
Connection Method	Available connection methods for Ethernet WAN: • DHCP: See "DHCP Settings" on page 40 • Static IP: "Static IP Settings" on page 41 • PPPoE: "PPPoE Settings" on page 42 • Mobile Internet:
Routing Mode	Select to apply Network Address Translation (**NAT**) to the traffic routing.
Connection Type	Specifies the utilization of the WAN connection. The **Always-on** option should be used whenever it is available. If **Backup Priority** and a priority group are selected, the WAN connection is treated as a backup connection and is used only in the absence of available Always-on WAN connection(s) and higher priority backup connection(s). Default (recommended) = **Always-on**
Reply to ICMP Ping	When disabled, the WAN connection will not respond to ICMP PING requests. Default = **Enabled**
Upload Bandwidth	Specifies the data bandwidth in the outbound direction from the LAN through the WAN interface. This value is provided by the ISP and should reflect the actual speed of the WAN. This value is referenced when default weight is chosen for outbound traffic and traffic prioritization. A correct value can result in effective traffic prioritization and efficient use of upload bandwidth.
Download Bandwidth	Specifies the data bandwidth in the inbound direction from the WAN interface to the LAN. This value is provided by the ISP and should reflect the actual speed of the WAN. This value is referenced as the default weight value when using the custom rule default (**Auto**), the algorithm **Least Used**, or the algorithm **Persistence (Auto)** in Outbound Policy with **Managed by Custom Rules** chosen (see "Creating Custom Rules for the Outbound Policy" on page 61).

Connection Methods

There are five possible WAN connection methods: DHCP, Static IP, PPPoE or Mobile Internet.

DHCP Settings

The DHCP connection method is suitable if the ISP provides an IP address automatically by DHCP (e.g. via Satellite Modem, WiMAX Modem, Cable, Metro Ethernet, etc.).

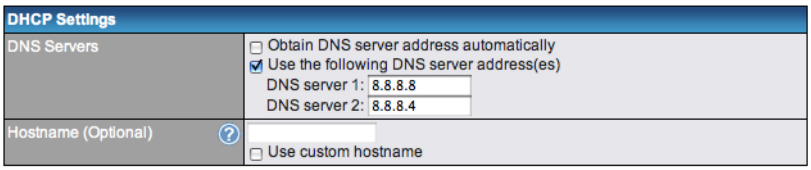


Figure 20. Network > WAN > Ethernet WAN Settings > DHCP Connection

Table 11. WAN: DHCP Settings

Field	Description
DNS Servers	Specifies the DNS (Domain Name System) Servers to be used when a DNS lookup is routed through this connection. Each ISP may provide a set of DNS servers for DNS lookups. Selecting **Obtain DNS server address automatically** allows the WAN DHCP Server to assign the DNS Servers used for outbound DNS lookups over the connection. (The DNS Servers are obtained along with the WAN IP address assigned from the DHCP server.) When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS server 1** and **DNS server 2** fields.
Hostname (Optional)	If your service provider's DHCP server requires you to supply a hostname value upon acquiring an IP address, you may enter the value in the **Hostname** field. If your service provider does not provide you with the value, you can safely bypass this option.

Static IP Settings

The Static IP connection method is suitable if the ISP provides a static IP address to connect directly.

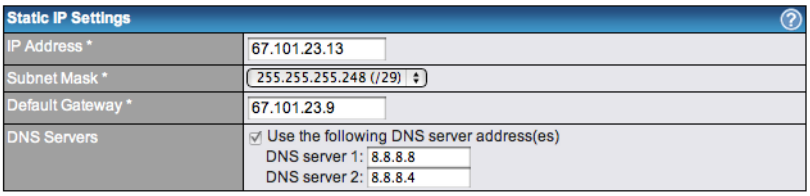


Figure 21. Network > WAN > Ethernet WAN Settings > Static IP Connection

Table 12. WAN: Static IP Settings

Field	Description
IP Address	Specifies a fixed IP address to connect to the Internet. The ISP typically provides this information.
Subnet Mask	Specifies the subnet mask for the IP address. The ISP typically provides this information.
Default Gateway	Specifies the default gateway to connect to the Internet. The ISP typically provides this information.
DNS Servers	Specifies the DNS (Domain Name System) Servers to be used when a DNS lookup is routed through this connection. Each ISP may provide a set of DNS servers for DNS lookups. You may enter the DNS server addresses provided by the ISP into the **DNS server 1** and **DNS server 2** fields. If no address is entered, this link will not be used for DNS lookups.

PPPoE Settings

The PPPoE connection method is suitable if the ISP provides the login ID /password to connect via PPPoE.

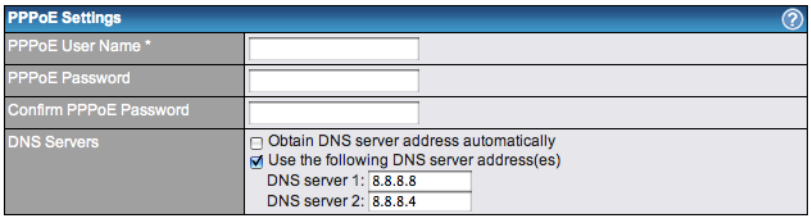


Figure 22. Network > WAN > Ethernet WAN Settings > PPPoE Connection

Table 13. WAN: PPPoE Settings

Field	Description
PPPoE Username / Password	Enter the username and password to connect to the ISP via the PPPoE server. The ISP typically provides this information.
Confirm PPPoE Password	Enter the password again for verification.
Service Name	Specifies the Service Name. The ISP typically provides this information. **Note:** Leave this field blank unless it is provided by your ISP.
DNS Servers	Specifies the DNS (Domain Name System) Servers to be used when a DNS lookup is routed through this connection. Each ISP may provide a set of DNS servers for DNS lookups. Selecting **Obtain DNS server address automatically** allows the PPPoE Server to assign the DNS Servers used for outbound DNS lookups over the WAN connection. (The DNS Servers are obtained along with the WAN IP address assigned from the PPPoE server.) When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS server 1** and **DNS server 2** fields.

Mobile Internet Settings

The Mobile Internet Connection method is suitable for USB modem mobile connection such as 3G, WiMAX, LTE, EVDO, EDGE, and GPRS, etc. Currently, it only applies to USB mobile WAN port.

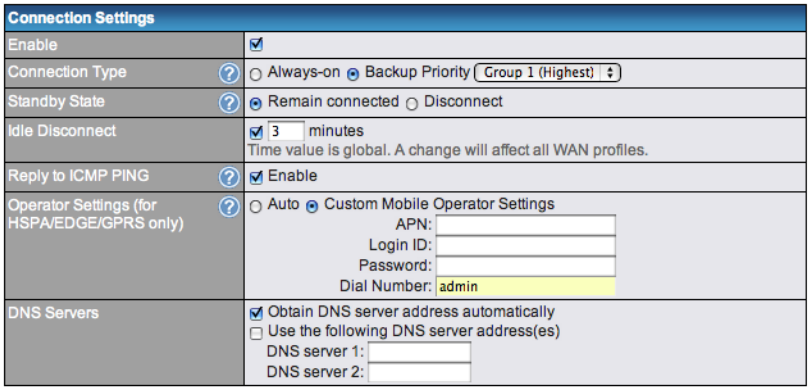


Figure 23. Network > WAN > Ethernet WAN Settings > Mobile Internet Connection

Table 14. WAN: Mobile Internet Settings

Field	Description
Enable	Select **Yes** to enable the connection; select **No** to disable.
Connection Type	Specifies the utilization of the WAN connection.The **Always-on** option should be used whenever it is available. If **Backup Priority** and a priority group are selected, the WAN connection is treated as a backup connection and is used only in the absence of available Always-on WAN connection(s) and higher priority backup connection(s). Default (recommended) = **Always-on**
Standby State	Select to remain connected or to disconnect when this WAN connection is no longer in the highest priority and has entered the standby state. When **Remain connected** is chosen, upon bringing up this WAN connection to active, it will be immediately available for use.
Idle Disconnect	When enabled, an idle connection will be disconnected after a specified amount of time. This time value is global and will affect all WAN profiles. The mobile connection will re-establish on demand.
GRE	Select to enable Generic Routing Encapsulation.
Reply to ICMP Ping	When disabled, the WAN connection will not respond to ICMP PING requests. Default = **Enabled**
Operator Settings	*Applies to 3G / EDGE / GPRS modem only. It does not apply to EVDO / EVDO Rev. A modem. Configures the APN settings of the WAN connection. Select **Auto** to detect the mobile operator automatically. Select **Custom** to enter the carrier's PN, Login, Password, and Dial Number settings manually. You may obtain this information from your carrier. Default/Recommended Setting = **Auto**
SIM PIN (optional)	Optional field to use if there is SIM lock for your SIM card service.

Table 14. WAN: Mobile Internet Settings

Field	Description
DNS Servers	Specifies the DNS (Domain Name System) Servers to be used when a DNS lookup is routed through this connection. Each ISP may provide a set of DNS servers for DNS lookups. Selecting **Obtain DNS server address automatically** allows the PPPoE Server to assign the DNS Servers used for outbound DNS lookups over the WAN connection. (The DNS Servers are obtained along with the WAN IP address assigned from the PPPoE server.) When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS server 1** and **DNS server 2** fields.

Modem Specific Custom Settings. The following settings may be available depending on the modem model. The example below is for a 3G modem.

Table 15. WAN: Modem Specific Custom Settings

Field	Description
Modem Model	Displays the Manufacturer name of the connected mobile modem.
ESN (WiMAX only)	Displays the modem's electronic serial number (ESN).
SIM Card IMSI	Displays the International Mobile Subscriber Identity (IMSI) associated with the SIM inside the mobile modem.
Network Type	Specifies the preference for using the 4G, 3G and/or 2G networks. 4G networks include WiMAX; 3G networks include HSPA / UMTS; 2G networks include EDGE / GPRS. Select **3G only** or **2G only** to use the HSPA / UMTS or EDGE / GPRS network, respectively. If the chosen network is not available, no other network will be used regardless of its availability. The modem connection will remain offline. Select **3G preferred** or **2G preferred** to use the chosen network when it is available. If the chosen network is not available, the other network will be used where available. Default = **3G preferred** (The example above uses a Huawei 3G modem).
GSM Frequency Band	Specifies which GSM frequency band to use. Select **GSM1900** for use in the United States, Canada, and many other countries in the Americas. Select **GSM900 / GSM1800 / GSM2100** for use in Europe, Middle East, Africa, Asia, Oceania, and Brazil. Select **All Bands** to automatically use the appropriate frequency band. Default = **All Bands**

Physical Interface Settings

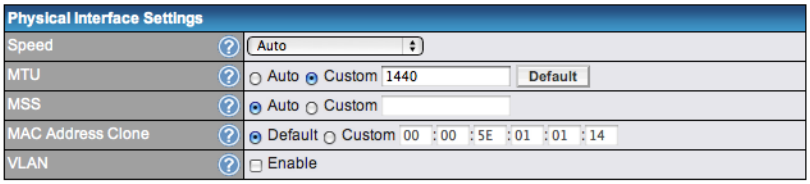


Figure 24. Network > WAN > Physical Interfaces

Table 16. WAN: Physical Interface Settings

Field	Description
Speed	Specifies the speed and duplex configurations of the WAN Port. By default, **Auto** is selected and the BD1000 automatically detects the appropriate data speed. In the event of negotiation issues, the port speed can be manually specified to circumvent the issues. You can also choose whether or not to advertise the speed to the peer by selecting the **Advertise Speed** checkbox.
MTU	Specifies the Maximum Transmission Unit. Default = **Custom 1440** You may adjust the MTU value by editing the text field. Click **Default** to restore the default MTU value. Select **Auto** and the BD1000 will automatically detect the appropriate MTU value. The auto-detection will run each time the WAN connection establishes.
MSS	Configures the maximum payload size that the local system can handle. The MSS (Maximum Segment Size) is computed from the MTU minus 40 bytes for TCP over IPv4. If MTU is set to Auto, the MSS will also be set automatically. Default = **Auto**
MAC Address Clone	Specifies the MAC address. Some service providers (e.g. cable providers) identify the client's MAC address and require the client to always use the same MAC address to connect to the network. In these cases, use the **MAC Address Clone** field to change the WAN's MAC address to the original client PC's MAC address. The default MAC Address is a unique value assigned at the factory. In most cases, the default value is sufficient. Click the **Default** button to restore the MAC Address to the default value.
VLAN	Some service providers require the router to enable VLAN tagging for Internet traffic. If it is required by your service provider, you can enable this field and enter the VLAN ID that the provider requires. Default = **Disabled**

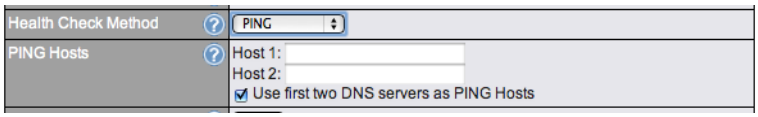
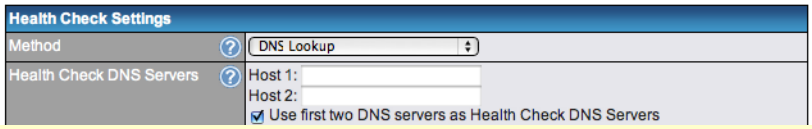
WAN Health Check

To ensure that traffic is routed only to healthy WAN connections, the BD1000 provides the functionality to periodically check the health of each WAN connection. The Health Check settings for each WAN connection can be independently configured. To configure WAN Health Check settings, click on **Network > Interfaces > WAN** in the Web Admin Interface. Then, click on the **Details** button in the row of the desired WAN connection in the **WAN Connection Status** table. The configuration page for that WAN connection displays, which includes the **Health Check** options.

Health Check Methods

The **Health Check** drop-down menu specifies the health check method for the WAN connection. Available methods include **Disabled**, **Ping**, or **DNS Lookup**. The default value is **DNS Lookup**.

Table 17. WAN: Health Check Methods

Method	Description
Disabled	Select the **Disabled** option so that the WAN connection will always be considered as "up." The connection will not be treated as down in the event of IP routing errors.
Ping	 Select the **Ping** method to issue ICMP PING packets to test the connectivity of a target IP address or hostname. A WAN connection is considered "up" if PING responses are received from either one or both of the PING Hosts. The **Ping Hosts** field specifies the IP addresses or hostnames to test with the ICMP PING method for connectivity. If you select the **Use first two DNS servers as Ping Hosts** box, the target PING Host will be the first DNS server for the corresponding WAN connection.
DNS Lookup	 Select the **DNS Lookup** method to test the connectivity with target DNS servers. The connection will be treated as "up" if DNS responses are received from either one or both of the servers, regardless of whether the result was positive or negative. The **Health Check DNS Servers** field allows you to specify two DNS hosts' IP address with which connectivity is to be tested via DNS Lookup. If you select the **Use first two DNS servers as Health Check DNS Servers** box, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, field Host 1 must be filled and field Host 2 is optional. If you select the **Include public DNS servers** box and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as "down" only if there is no response received from the public DNS servers. Connections will be considered as "up" if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result.

Additional Health Check Settings

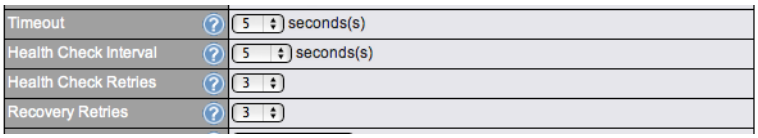


Figure 25. Network > WAN > Details > Other Health Check Settings

Table 18. WAN: Other Health Check Settings

Method	Description
Timeout	Specifies the timeout, in seconds, for ping/DNS lookup requests. Default = **5 seconds**
Health Check Interval	Specifies the time interval, in seconds, between ping or DNS lookup requests. Default = **5 seconds**
Health Check Retries	Specifies the number of consecutive ping/DNS lookup timeouts to try before the BD1000 marks the corresponding WAN connection as "down." Default = **3 retries** For example, with the default Health Retries setting of 3, after 3 consecutive timeouts, the corresponding WAN connection will be treated as "down."
Recovery Retries	Specifies the number of consecutive successful ping/DNS lookup responses that must be received before the BD1000 considers a previously down WAN connection to be "up" again. Default = **3 retries** For example, a WAN connection that is treated as "down" will be considered to be up again after receiving 3 consecutive successful ping/DNS lookup responses.

Note When the health check method is set to **DNS Lookup** and the corresponding health checks fail, the BD1000 will automatically perform DNS lookups on some public DNS servers. If the tests are successful, the WAN may not be considered as "down": however, the target DNS server may malfunction. If a malfunction occurs, the following warning displays on the main page:

Bandwidth Allowance Monitor

The Bandwidth Allowance Monitor feature tracks network usage for the BD1000. The Bandwidth Allowance settings for each WAN connection can be independently configured.

To configure the Bandwidth Allowance Monitor, click on **Network > WAN** in the Web Admin Interface. Then, click on the **Details** button in the row of the desired WAN connection in the **WAN Connection Status** table. The configuration page for that WAN connection displays, which includes the **Bandwidth Allowance Monitor** option. Select the box to enable and configure Bandwidth Allowance settings.

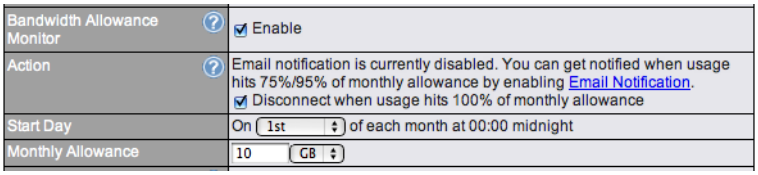


Figure 26. Network > WAN > Details > Bandwidth Allowance Monitor

Table 19. WAN: Bandwidth Allowance Monitor

Method	Description
Action	Enable the **Email Notification** feature to be notified through email when network usage hits 75% and 95% of the monthly allowance. Select the **Disconnect when usage hits 100% of monthly allowance** box to automatically disconnect this WAN service when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off, or the usage has been reset when a new billing cycle starts.
Start Day	Defines which day in the month each billing cycle begins.
Monthly Allowance	Defines the maximum bandwidth usage allowed for the WAN connection each month.

Dynamic DNS Settings

The BD1000 provides the functionality to register the domain name relationships to dynamic DNS service providers. Through registration with dynamic DNS service provider(s), the default public Internet IP address of each WAN connection can be associated with a hostname. When the IP address is changed or 23 days have passed without a link reconnection, the BD1000 will connect to the dynamic DNS service provider to perform an IP address update within the provider's records.

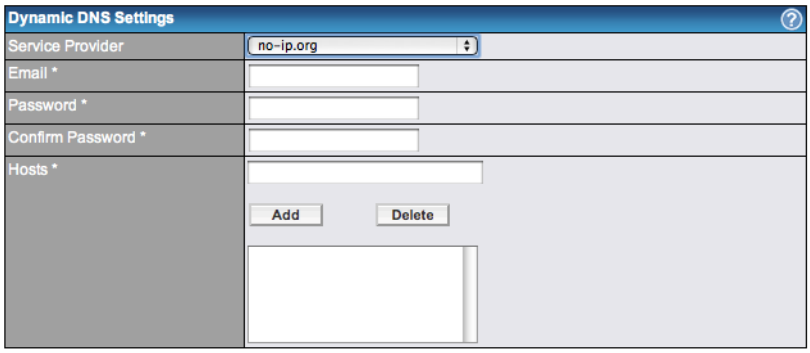


Figure 27. Network > WAN > Ethernet WAN Settings > Dynamic DNS

Table 20. WAN: Dynamic DNS Settings

Field	Description
Service Provider	Specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: • hangeip.com • dyndns.org • no-ip.org • zo.com Select **Disabled** to disable this feature.
User ID	Specifies the registered username for the dynamic DNS service.
Password	Specifies the password for the dynamic DNS service.
Hosts	Specifies a list of hostnames or domains to be associated with the WAN connection's public Internet IP address. You may use the Enter key to add more than one host.

Note In order to use dynamic DNS services, appropriate hostname registration(s) as well as a valid account with a supported dynamic DNS service provider are required.
A dynamic DNS update is performed whenever a WAN's IP address changes (e.g. IP is changed after a DHCP IP refresh, reconnection, etc...).
Due to dynamic DNS service providers' policy, a dynamic DNS host will automatically expire if the host record has not been updated for a long time. The BD1000 performs an update every 23 days even if a WAN's IP address has not changed.

Chapter 4 Configuring the WAN

Chapter contents

Introduction

This chapter describes setting up and managing the WAN Bonding functionality for the BD1000. The WAN Bonding functionality securely connects the BD1000 in a different branch to another BD1000. The data, voice or video communications between these locations are kept confidential across the public Internet.

The WAN Bonding of the BD1000 is specifically designed for a multi-WAN enviroment. The BD1000 can aggregate the bandwidth for all WAN connections to route Site-to-Site VPN traffic. Unless all of the VPN connections of one site are down, the BD1000 can still keep the VPN up and running. With VPN Bandwidth Bonding, all available bandwidth will be utilized to establish the VPN tunnel, and all traffic will be load balanced at packet level across all links. VPN Bandwidth Bonding is enabled by default.

Note You can define firewall rules to control access within the VPN network. Outbound traffic can be redirected to VPN tunnels with custom outbound policies (see Chapter 5, "Managing Outbound Traffic to the WAN" on page 59).

Configuring WAN Bonding Settings

To configure WAN Bonding options for the BD1000, click on **Network > WAN Bonding** in the Web Admin Interface. The **BD1000 WAN Bonding** configuration page displays:

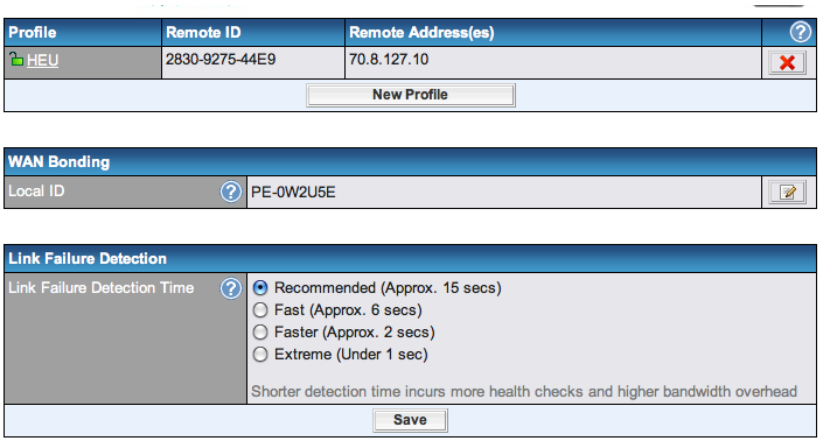


Figure 28. Network > WAN Bonding

Refer to the following sections for details about configuring and managing Site-to-Site VPN connections:

- "Configuring a WAN Bonding Profile" on page 52
- "Managing Link Failure Detection Settings" on page 54
- "Configuring a NAT Router Behind the BD1000 for VPN Connections" on page 55
- "Viewing the WAN Bonding Status" on page 55

Configuring a WAN Bonding Profile

The BD1000 supports making two Site-to-Site VPN connections with a remote BD1000 unit. The BD1000 that supports multiple WAN connections can act as a central hub which connects branch offices. For example, branch office A and branch office B make VPN connections to headquarters C, both branch offices' LAN subnet and subnets behind it (i.e. static routes) will also be advertised to the headquarters C and the other branches. So branch office A will be able to access branch office B via headquarters C in this case.

The local LAN subnet and subnets behind the LAN (defined in the "Static Route Settings" on page 36) will be advertised to the VPN. All VPN members (branch offices and headquarters) will be able to route to the local subnets.

Note All LAN subnets and subnets behind the LAN must be unique. Otherwise, the VPN members will not be able to access each other.

All data can be routed over the VPN with 256-bit AES encryption standard.

To configure a new WAN connection, click on **Network > WAN Bonding** in the Web Admin Interface, and click the **New Profile** button to create a new WAN profile. The **WAN Profile** configuration page displays:

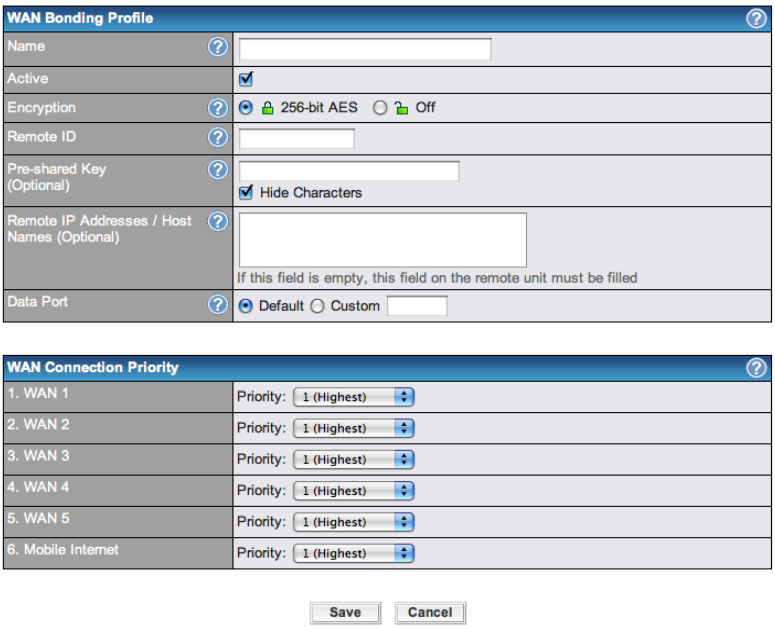


Figure 29. Network > WAN Bonding > Add WAN Connection

This section describes the following settings for creating a new VPN profile:

- VPN Settings (see "VPN Settings" on page 53)
- WAN Connection Priority Settings (see "WAN Connection Priority Settings" on page 53)

VPN Settings

Table 21. Site-to-Site VPN: New VPN Connection Settings

Field	Description
VPN Connection Name	Specifies a name to represent this VPN connection profile.
Active	Check this box to enable the VPN connection.
Encryption	By default, VPN traffic is encrypted with 256-bit AES standard. If the Off option is selected on both sides of a VPN connection, no encryption will be applied.
Peer Serial Number	The BD1000 only establishes a VPN connection with a remote peer that has a serial number specified in this **Peer Serial Number** field. If the remote peer is in a high availability setup, select the **Remote client is set up in high availability mode** option, and enter the second unit's serial number into the second text box.
Pre-Shared Key	Defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match.
Peer IP Addresses / Host Names	(Optional) Enter the remote peer's WAN IP address(es) or host name(s) in the **Peer IP Addresses** field. Enter one IP address or host name per line. The BD1000 also accepts Dynamic-DNS host names. When you provide the peer details, the BD1000 will initiate a connection to each of the remote IP addresses until they connect successfully. If the field is empty, the BD1000 will wait for a connection from the remote peer. Therefore, at least one side of the two VPN peers has to have this peer field filled. Otherwise, a VPN connection cannot be established.

WAN Connection Priority Settings

Table 22. Site-to-Site VPN: WAN Connection Priority Settings

Field	Description
WAN Connection Priority	You can specify the priority level of the WAN connections used for making VPN connections. WAN connections set to **OFF** will never be used. Only available WAN connections with the highest priority will be utilized.

Managing Link Failure Detection Settings

To configure Link Failure Detection settings for the BD1000, click on **Network > WAN Bonding** in the Web Admin Interface. The **BD1000 Wan Bonding** configuration page displays, including the **Link Failure Detection** section:

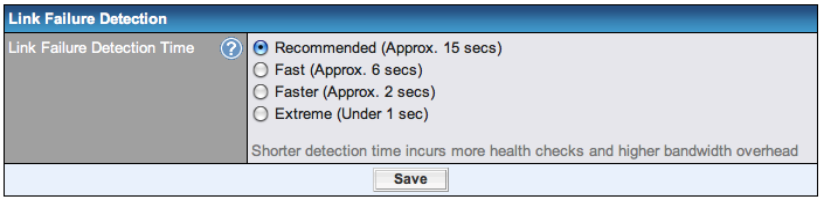


Figure 30. Network > WAN Bonding > Link Failure Detection

The bonded Site-to-Site VPN can detect routing failures on the path between two sites over each WAN connection. Failed WAN connections will not be used to route VPN traffic. Health check packets are sent to the peer to detect any failure. Checking the status more frequently leads to a shorter detection time, but higher bandwidth overhead will be consumed.

Table 23. Site-to-Site VPN: Link Failure Detection

Link Failure Detection Time	Description
Recommended[a]	Select the **Recommended** option to send a health check packet every 5 seconds. The expected detection time is 15 seconds.
Fast	Select the **Fast** option to send a health check packet every 3 seconds. The expected detection time is 6 seconds.
Faster	Select the **Faster** option to send a health check packet every 1 second. The expected detection time is 2 seconds.
Extreme	Select the **Extreme** option to send a health check packet every 0.1 second. The expected detection time is under 1 second.

a. **Recommended** is the default setting for the Link Failure Detection Time.

Note The BD1000 Site-to-Site VPN feature uses TCP and UDP port 32015 for establishing VPN connections. If you have a firewall in front of the devices, you will need to add firewall rules for these ports and protocols that will allow inbound and outbound traffic to pass through the firewall.

Configuring a NAT Router Behind the BD1000 for VPN Connections

The BD1000 supports establishing Site-to-Site VPN over WAN connections that are behind a NAT (Network Address Translation) router. In order for a WAN connection behind a NAT router to accept VPN connections, you can configure the NAT router in front of the WAN connection to forward to TCP port 32015.

If one or more WAN connections on **Router A** can accept VPN connections (by means of port forwarding or not) while none of the WAN connections on the peer **Router B** can, you should put all public IP addresses or host names of the **Router A** in the **Router B** on **Router B**. Leave the **Peer IP Addresses / Host Names** field on **Router A** empty. With these settings in place, the BD1000 can set up a site-to-site VPN connection and all WAN connections on both sides can be used. For example, see Figure 31 below:

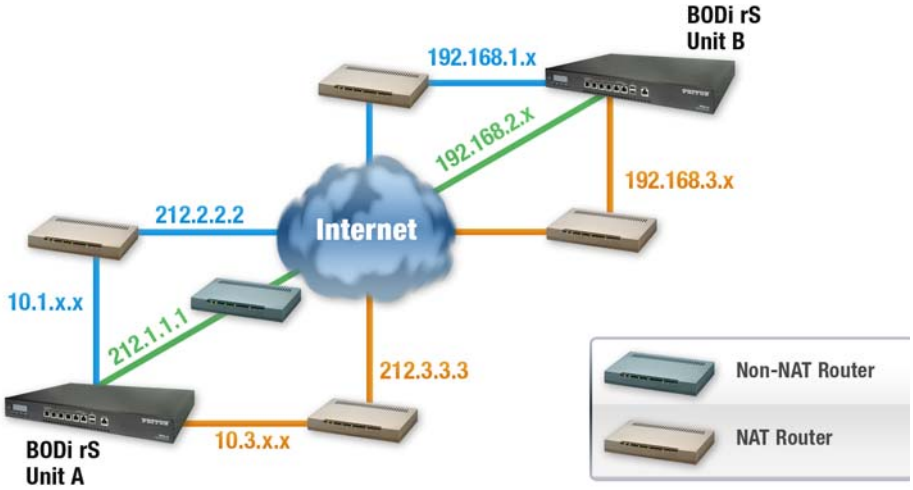


Figure 31. BD1000 Behind a NAT Router Application

One of the WAN connections of **Router A** is not using NAT (*212.1.1.1*). The rest of the WAN connections on **Router A** and all of the WAN connections on **Router B** are using NAT. In this case, the **Peer IP Addresses / Host Names** field in **Router B** should be filled with all of the **Router A**'s host names or public IP addresses (i.e. *212.1.1.1*, *212.2.2.2* and *212.3.3.3*), and the field in **Router A** can be left blank. The two NAT routers on WAN1 and WAN3 of **Router A** should forward inbound traffic through TCP port 32015 to **Router A** so that all of the WAN connections can be utilized to establish the VPN connection.

Viewing the WAN Bonding Status

To view the status of VPN connections, click on the **Dashboard** in the Web Admin Interface. The **WAN Bonding** section shows the connection status of each connection profile. To view more details about a VPN connection status, click the **Status** button in the top-right hand corner of the **WAN Bonding** table. The **Status > WAN Bonding** page display provides the subnet and WAN connection information of each VPN peer. Refer to "Viewing Site-to-Site VPN Connection Details" on page 136 for more information.

Note **IP Subnets must be unique among VPN peers.**
The entire inter-connected WAN Bonding network is one single non-NAT IP network. No two subnets in two sites can be duplicated. Otherwise, the BD1000 will experience connectivity problems in accessing those subnets.

Configuring IPsec VPN Settings

The BD1000 IPsec VPN functionality securely connects one or more branch offices to your company's main headquarters or to other branches. The data, voice or video communications between these locations are thus kept safe and confidential across the public Internet.

The IPsec VPN of the BD1000 is especially designed for a multi-WAN environment. For instance, a user sets up multiple IPsec profiles for his multi- WAN1 ~ WAN3 environment, if WAN1 is connected and its health check returns as good, the IPsec traffic will go through this link. However, should unforeseen problems (e.g. physically unplugged or ISP problems) arise and cause WAN1 to go down, our IPsec implementation will make use of WAN2 and WAN3 accordingly, as failover purposes.

Setting Up an IPsec VPN Connection

To configure IPsec VPN settings for the BD1000, click on **Network > IPsec VPN** in the Web Admin Interface. The **BD1000 IPsec VPN** page displays:

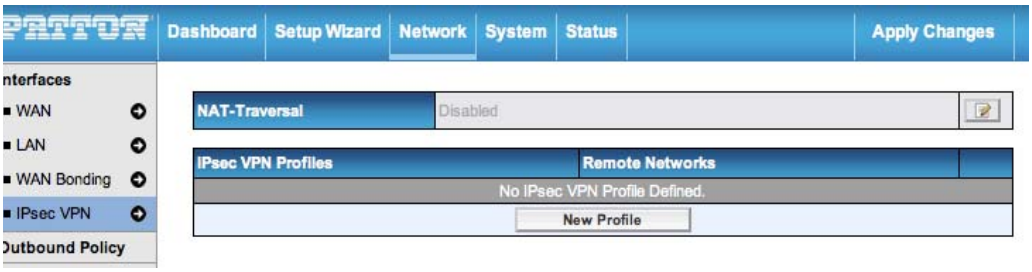


Figure 32. Network > IPsec VPN Profiles

Note All LAN subnets and subnets behind the LAN must be unique. Otherwise, the VPN members will not be able to access each other.

All data can be routed over the VPN with a selected encryprion standard: 3DES, AES-128, and AES-256.

The NAT-Traversal option should be enabled if your system is behind a NAT router. Click the **New Profile** button to create new IPsec VPN profiles that make VPN connections to remote BD1000, Cisco or Juniper Routers via the available WAN connections. To edit any of the profiles, click on its associated connection name in the far left column.The **IPsec VPN Profile** configuration page displays (Figure 33 on page 57).

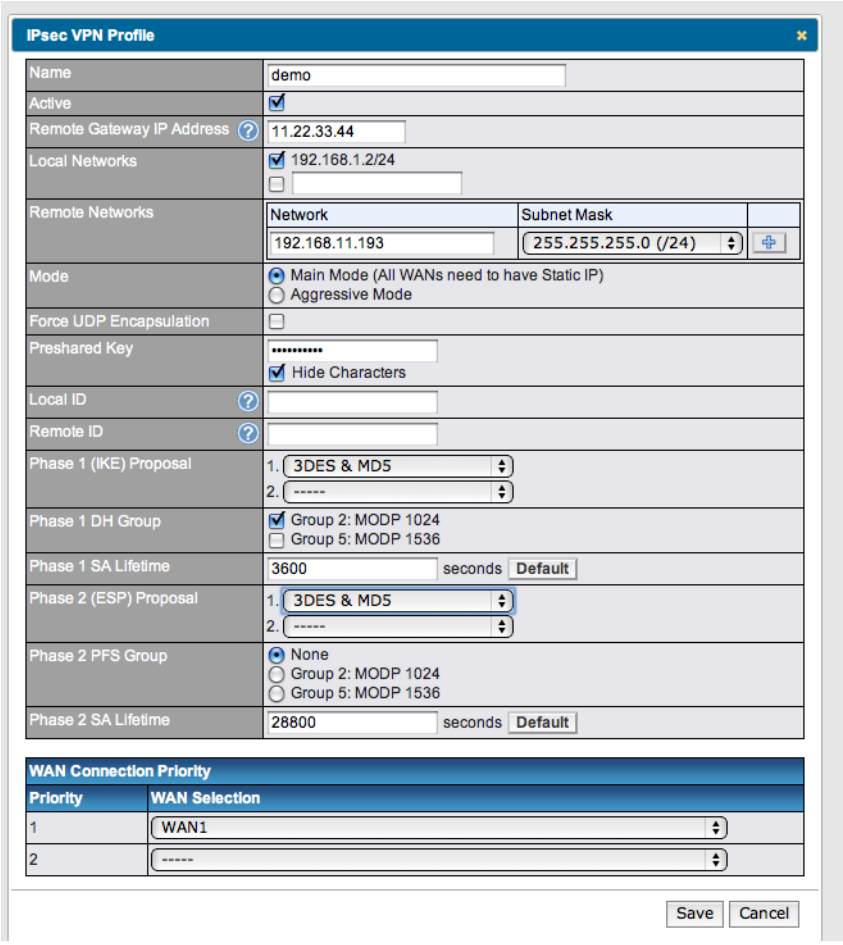


Figure 33. Network > New IPsec VPN Connection

Table 24. IPsec VPN: New Connection Settings

Field	Description
Name	Specifies a name to represent this VPN connection profile.
Active	Check this box to enable the VPN connection.
Remote Gateway IP	Enter the remote peer's public IP address. For Aggressive Mode, this is optional.
Local Networks	Enter the local LAN subnets here. If you have defined "static routes," they will be shown here too.
Remote Networks	Enter the LAN and subnets that are located at the remote site here.
Main Mode	Choose this Main Mode if both IPsec peers use static IP addresses.
Aggressive Mode	Choose this Aggressive Mode if one of the IPsec peers uses dynamic IP addresses.
Force UDP Encapsulation	Check this box for UDP encapsulation to be forced regardless of the NAT-Traversal.

Table 24. IPsec VPN: New Connection Settings

Field	Description
Pre-Shared Key	Defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match.
Local ID	Under Main Mode, this field can be left blank. Under Aggressive Mode, if Remote Gateway IP Address field is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
Remote ID	Under Main Mode, this field can be left blank. Under Aggressive Mode, if Remote Gateway IP Address field is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
Phase 1 (IKE) Proposal	Under Main Mode, this allows the setting of up to 6 encryption standards, in descending order of priority, to be used in the initial connection key negotiations. For Aggressive Mode, only one selection is permitted.
Phase 1 DH Group	This is the Diffie-Hellman group used within IKE. This allows two parties to establish a shared secret over an insecure communications channel. The larger the group number, the higher the security. • Group 2 - 1024-bit is the default value. • Group 5 - 1536-bit is the alternative option.
Phase 1 SA Lifetime	Specifies the lifetime limit of this Phase 1 Security Association. Default = 3600 seconds
Phase 2 (ESP) Proposal	Under Main Mode, this allows the setting of up to 6 encryption standards, in descending order of priority, to be used for the IP data that is being transferred. For Aggressive Mode, only one selection is permitted.
Phase 2 PFS Group	The Perfect Forward Secrecy (PFS) ensures that if a key was compromised, the attacker will be able to access only the data protected by that key but not any other data. • None - Do not request for PFS when initiating connection. However, since there is no valid reason to refuse PFS, the system will allow the connection to use PFS if requested by the remote peer. This is the default value. • Group 2 - 1024-bit Diffie-Hellman group. The larger the group number, the higher the security. • Group 5 - 1536-bit is the third option.
Phase 2 SA Lifetime	Specifies the lifetime limit of this Phase 2 Security Association. Default = 28800 seconds

Viewing the IPsec Status

The **IPsec Status** section shows the current connection status of each connection profile. To view more details about a VPN connection status, navigate to the **Status > IPsec** page.

Chapter 5 Managing Outbound Traffic to the WAN

Chapter contents

Introduction

The BD1000 provides the functionality to flexibly manage and balance the load of outbound traffic among the WAN connections. To manage outbound traffic and load balancing, click on **Network > Outbound Policy** in the Web Admin Interface.

Note The **Outbound Policy** is only applied when more than one WAN connection is active.

Selecting the Outbound Policy

The BD1000 provides three policy options for managing outbound traffic: High Application Compatibility, Normal Application Combatibility (Default) and Custom Rules.

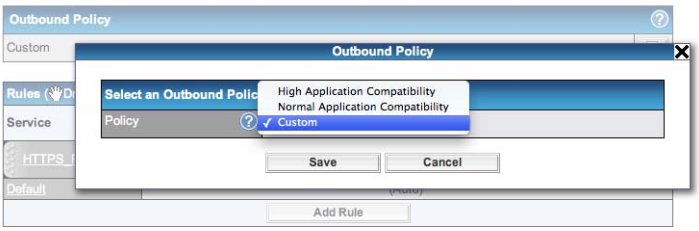


Figure 34. Network > Outbound Policy > Select Policy

Table 25. Outbound Policy: Options

Field	Description
High Application Compatibility	Select this policy to route outbound traffic from a source LAN device through the same WAN connection, regardless of the destination IP address and protocol. This option provides the highest application compatibility.
Normal Application Compatibility[a]	Select this policy to persistently route outbound traffic from a source LAN device to the same destination IP address via the same WAN connection, regardless of the protocol. This option provides high compatibility to most applications, and users still benefit from WAN link load balancing when multiple Internet servers are accessed.
Custom	Select this policy to manually define custom rules to manage outbound traffic behavior. Rules can be defined in a custom rule table. A default rule can be defined for connections that cannot be matched with any one of the rules.

a. The default policy is **Normal Application Compatibility**.

Creating Custom Rules for the Outbound Policy

To configure custom rules for the outbound policy, click on the **Pencil icon** in the Outbound Policy window. Select the **Custom** option in the drop-down menu, then press **Save**. The **Custom Rules** section displays.

Click on the **Default** rule listing at the bottom of the table. You may edit this rule to change the device's default method of controlling outbound traffic for all connections, as long as it does not match any of the rules above it in the table. Drag and drop a row to rearrange the preferred priority level of an outbound rule:

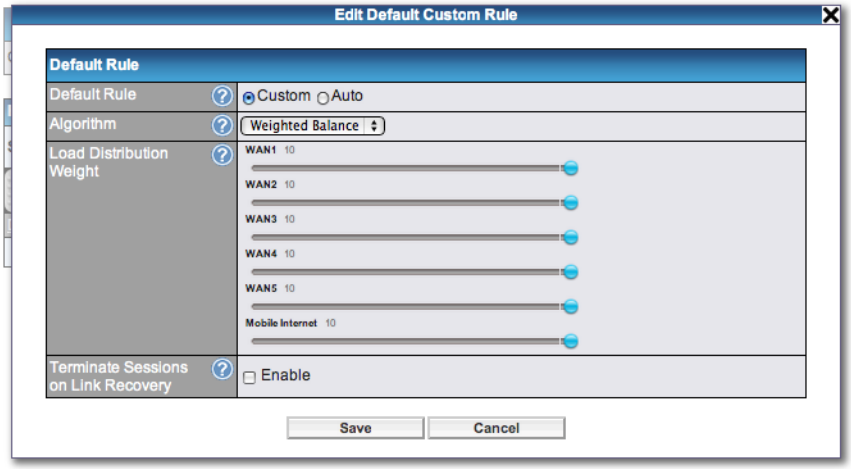


Figure 35. Outbound Policy > Edit Default Custom Rule

By default, **Auto** is the selected setting for the **Default Rule**. Click on **Custom** to change the **Algorithm** used to define the rule. To create a custom rule, click **Add Rule** at the bottom of the table. The **Add a New Custom Rule** window displays:

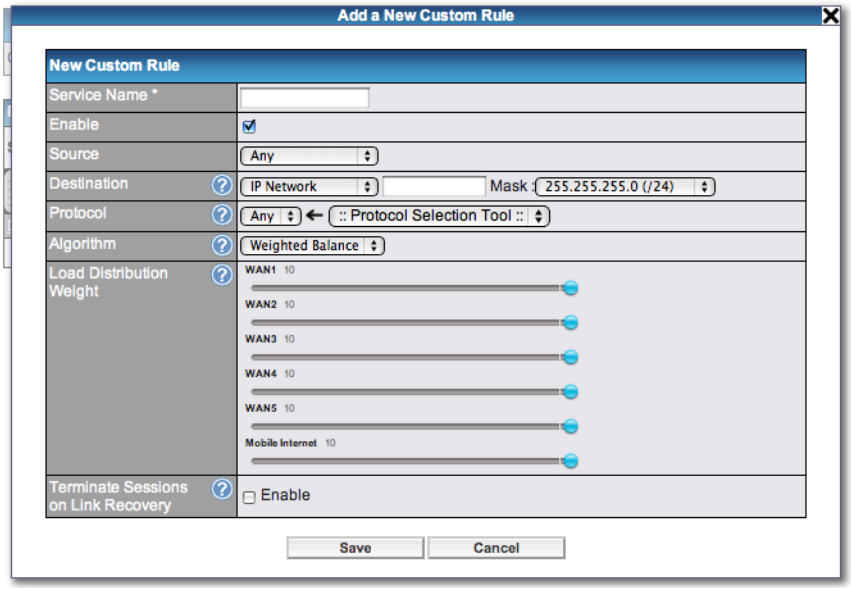


Figure 36. Outbound Policy > Add New Custom Rule

New Custom Rule Settings

Table 26. Outbound Policy: Custom Rule Settings

Field	Description
Service Name	Specifies the name of the custom rule.
Enable	Specifies whether the outbound traffic rule takes effect. Click **Yes** to enable the outbound traffic rule. When enabled, the BD1000 matches traffic and takes action based on the other parameters of the rule. Click **No** to disable the outbound traffic rule. When disabled, the BD1000 disregards the other parameters of the rule.
Source	Specifies the source IP Address, IP Network or MAC Address for outbound traffic that matches the rule.
Destination	Specifies the destination IP Address or IP Network for outbound traffic that matches the rule.
Protocol and Port	Specifies the IP Protocol and Port of outbound traffic that matches this rule. Click the drop-down menu for the **Protocol Selection Tool** to choose a common protocol.
Algorithm	Specifies the behavior of the BD1000 for the custom rule. Available options: • **Weighted Balance** (see "Algorithm: Weighted Balance" on page 63) • **Persistence** (see "Algorithm: Persistence" on page 63) • **Enforced** (see "Algorithm: Enforced" on page 65) • **Priority** (see "Algorithm: Priority" on page 65) • **Overflow** (see "Algorithm: Overflow" on page 66) • **Least Used** (see "Algorithm: Least Used" on page 66) • **Lowest Latency** (see "Algorithm: Lowest Latency" on page 67)
Terminate Sessions on Link Recovery	Specifies whether to terminate existing IP sessions on a less preferred WAN connection in the event that a more preferred WAN connection is recovered. This setting only applies to the **Weighted Balance**, **Persistence** and **Priority** options. By default, this option is disabled. When disabled, all existing IP sessions will not be terminated or affected when any other WAN connection is recovered. When enabled, existing IP sessions may be terminated when another WAN connection is recovered, so that only the preferred healthy WAN connection(s) are used at any point in time.

Algorithm: Weighted Balance

The Weighted Balance Algorithm specifies the ratio of WAN connection usage to be applied on the specified IP Protocol and Port. These settings only apply when the Algorithm is set to **Weighted Balance** (shown in Figure 36 on page 61).

The amount of matching traffic that is distributed to a WAN connection is proportional to the weight of the WAN connection relative to the total weight. Use the sliders to change the weight for each WAN.

For example, the weight settings in the bulleted list have these results:

- **WAN1:** 10
- **WAN2:** 10
- **WAN3:** 5

The total weight is 25 = (10 + 10 + 5)

Matching traffic distributed to WAN1 is 40% = (10 / 25) x 100%

Matching traffic distributed to WAN2 is 40% = (10 / 25) x 100%

Matching traffic distributed to WAN3 is 20% = (5 / 25) x 100%

Algorithm: Persistence

The Persistence Algorithm provides solutions to fix undesirable link load distribution for Internet services.

For example, many e-banking and other secure websites, for security reasons, terminate the session when the client computer's Internet IP address changes during the session.

In general, different Internet IP addresses represent different computers. The security concern is that an IP address change during a session may be the result of an unauthorized intrusion attempt. Therefore, to prevent damages from the potential intrusion, the session is terminated upon the detection of an IP address change.

The BD1000 can be configured to distribute data traffic across multiple WAN connections. Also, the Internet IP depends on the WAN connections where communication actually takes place. As a result, a LAN client computer behind the BD1000 may communicate using multiple Internet IP addresses. For example, a LAN client computer behind an BD1000 with three WAN connections may communicate on the Internet using three different IP addresses.

When using the **Persistence** Algorithm with the BD1000 (Figure 37 on page 64), rules can be configured to enable client computers to persistently utilize the same WAN connections for e-banking and other secure websites. As a result, a client computer will communicate with the other end using one IP address to eliminate the issues.

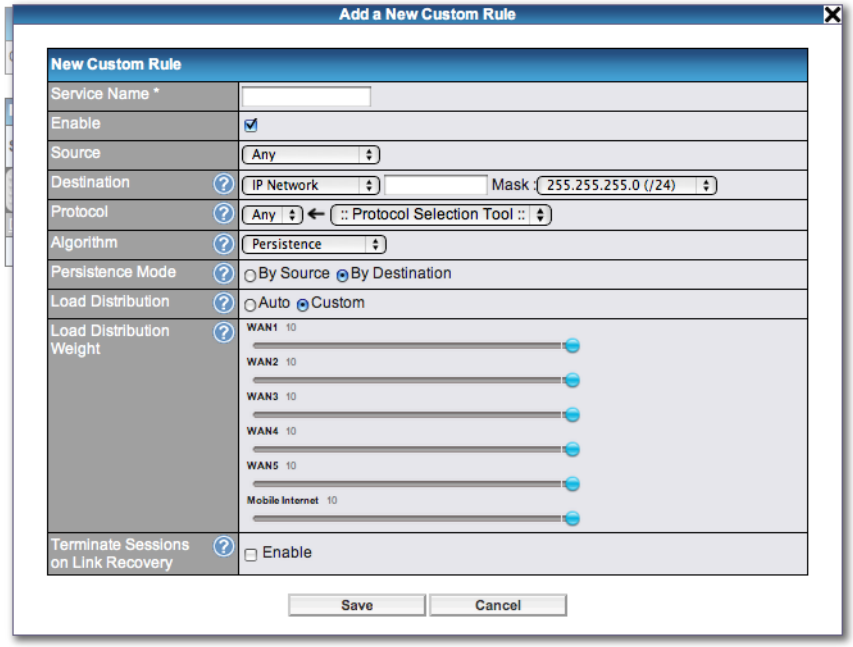


Figure 37. Outbound Policy > Custom Rule > Persistence

The **Persistence** Algorithm provides two options: **By Source** or **By Destination**.

Table 27. Persistence Algorithm: Persistence Mode Options

Mode	Description
By Source[a]	The same WAN connection will be used for traffic matching the rule and originating from the same machine regardless of its destination. This option will provide the highest level of application compatibility.
By Destination	The same WAN connection will be used for traffic matching the rule, originating from the same machine, and going to the same destination. This option can better distribute load to WAN connections when there are only a few client machines.

a. Default Persistence Mode

When there are multiple client requests, they can be distributed (persistently) to WAN connections with a weight. Select **Auto** for the **Load Distribution** setting to automatically adjust weights according to each WAN's Downstream Bandwidth specified in the WAN settings page (see "Configuring the WAN Interface" on page 39). Alternatively, select **Custom** to manually set the weight of each WAN using the sliders.

Algorithm: Enforced

The Enforced Algorithm specifies the WAN connection usage to be applied on the specified IP Protocol and Port. These settings only apply when the Algorithm is set to **Enforced**:

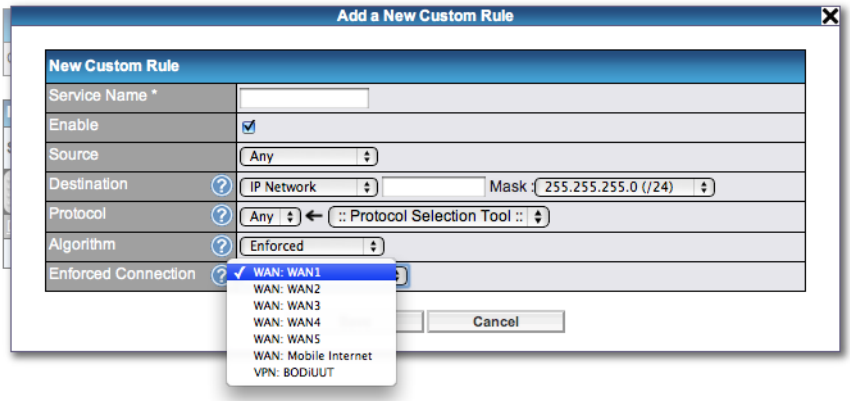


Figure 38. Outbound Policy > Custom Rule > Enforced

Matching traffic will be routed through the specified WAN connection regardless of the connection's health check status. Outbound traffic can be enforced to go through a specified Site-to-Site VPN connection.

Algorithm: Priority

The Priority Algorithm specifies the priority of the WAN connections to be utilized to route the specified network service. The highest priority WAN connection available will always be used for routing the specified type of traffic. A lower priority WAN connection will be used only when all higher priority connections have become unavailable.

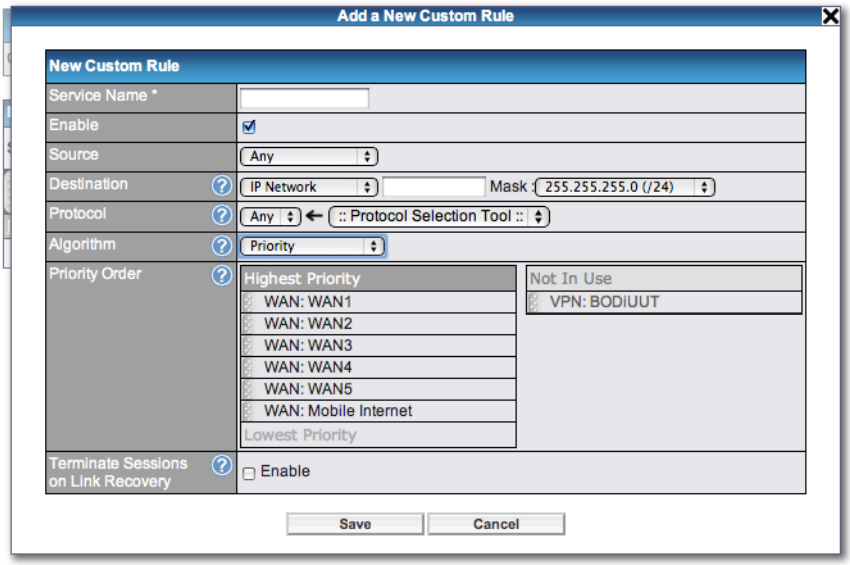


Figure 39. Outbound Policy > Custom Rule > Priority

Outbound traffic can be prioritized to go through a specified Site-to-Site VPN connection. You may configure multiple distribution rules to accommodate different kinds of services.

Algorithm: Overflow

The Overflow Algorithm manages traffic by routing through the healthy WAN connection that has the highest priority and is not fully loaded. When this connection becomes saturated, new sessions will be routed to the next healthy WAN connection that is available.

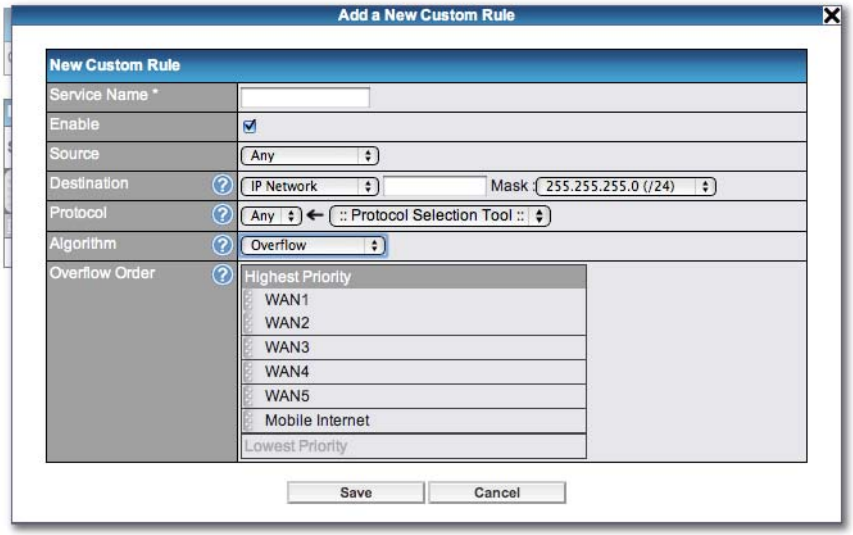


Figure 40. Outbound Policy > Custom Rule > Overflow

Drag and drop to specify the order of WAN connections to be used for routing traffic. Only the highest priority healthy connection that is not in full load will be utilized.

Algorithm: Least Used

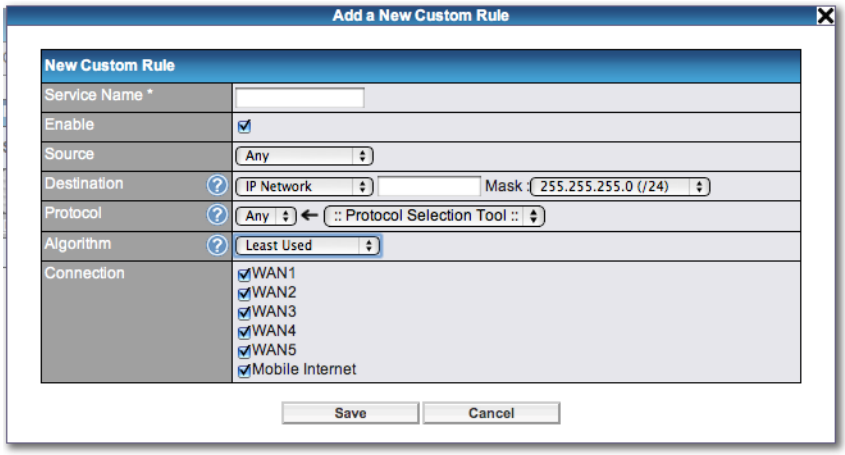


Figure 41. Outbound Policy > Custom Rule > Least Used

The Least Used Algorithm manages traffic by routing through the healthy WAN connection that is selected in the **Connection** field and has the most available downstream bandwidth. The available downstream bandwidth of a WAN connection is calculated from the total downstream bandwidth specified in the WAN settings page and the current downstream usage. The available bandwidth and WAN selection is determined every time an IP session is made.

Algorithm: Lowest Latency

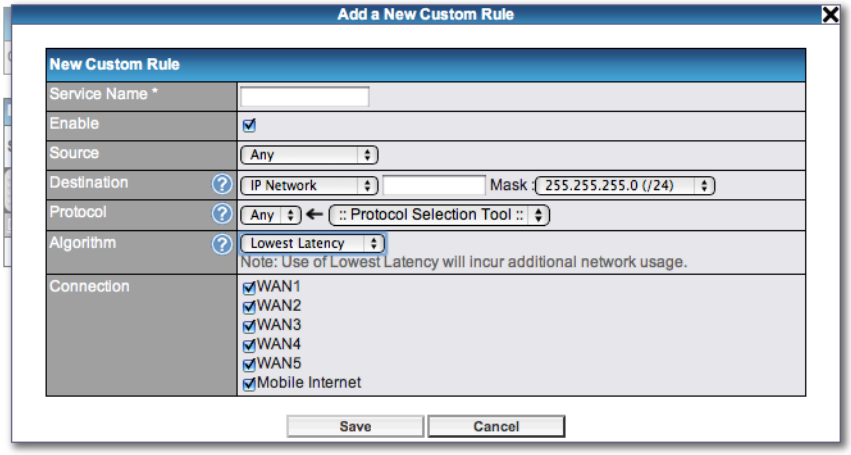


Figure 42. Outbound Policy > Custom Rule > Lowest Latency

The Lowest Latency Algorithm manages traffic by routing through the healthy WAN connection that is selected in the **Connection** field and has the lowest latency. Latency checking packets are issued periodically to a nearby router of each WAN connection to determine its latency value. The latency of a WAN is the packet round trip time of the WAN connection. Additional network usage may be incurred as a result.

The round trip time of a "6M down / 640k up" link can be higher than that of a "2M down / 2M up" link. This occurs because the overall round trip time is lengthened by its lower upstream bandwidth, despite the higher downlink speed. This algorithm is ideal for the following two scenarios:

- All WAN connections are symmetric.
- A latency sensitive application must be routed through the lowest latency WAN, regardless the WAN's available bandwidth.

Expert Mode Settings

The **Expert Mode** is available for advanced users to configure custom rules. Click the **?** Help circle at the top of the **Custom Rules** window, and click the link to **turn on Expert Mode**.

Under Expert Mode, a special rule, "**Site-to-Site VPN Routes,**" is available in the Custom Rules table. This option represents all Site-to-Site VPN routes learned from remote VPN peers. By default, this bar is on the top of all custom rules. That means traffic for remote VPN subnets will be routed to its corresponding VPN peer.

You can create custom **Priority** or **Enforced** rules and move them above the bar to override the Site-to-Site VPN Routes.

When disabled, all of the rules above the **Expert Mode** bar will be deleted.

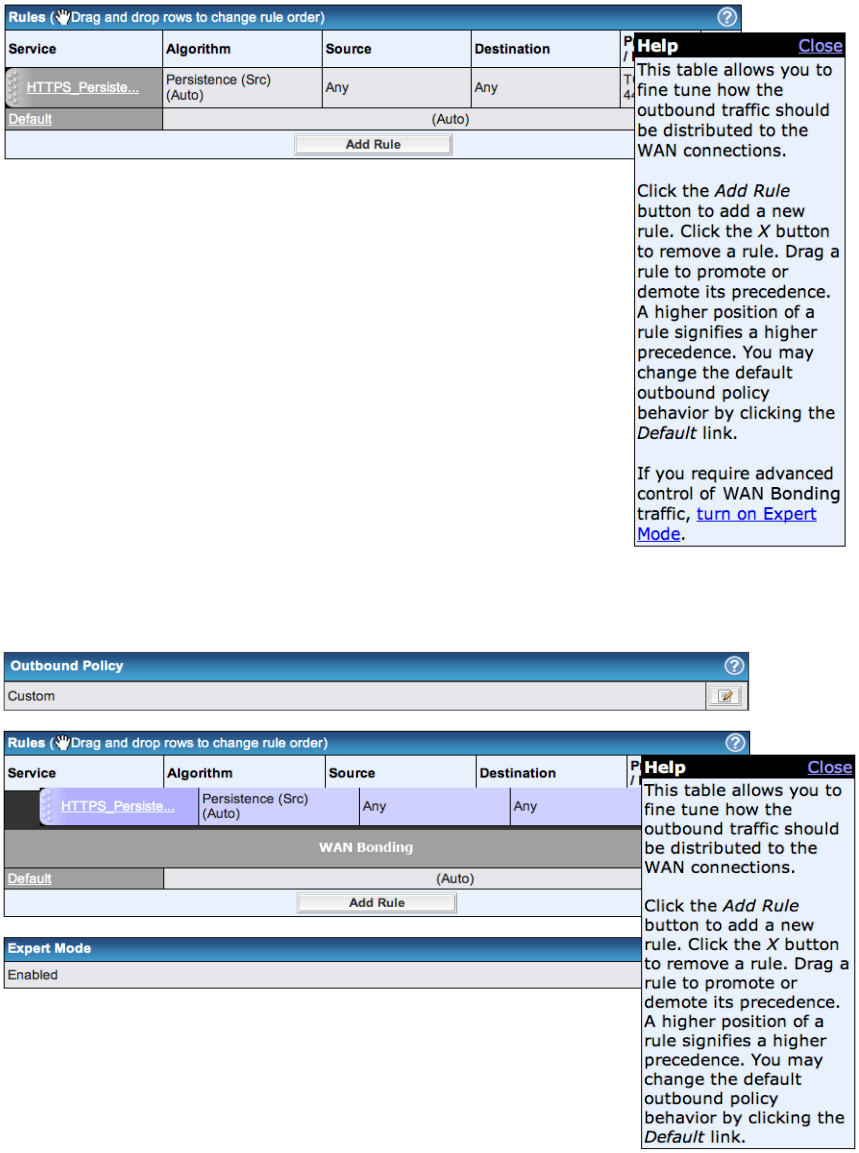


Figure 43. Outbound Policy > Custom Rule > Expert Mode

Chapter 6 Configuring Inbound Access & NAT Mappings

Chapter contents

Introduction

This chapter describes setting up inbound access services (also known as inbound port address translation) and NAT mappings.

For information about setting up inbound access, see "Configuring Inbound Access Rules" on page 70.

For information about setting up NAT mappings, see "Configuring NAT Mappings" on page 93.

Configuring Inbound Access Rules

Inbound Access is also known as inbound port address translation. On a NAT WAN connection, all inbound traffic to the server behind the BD1000 requires Inbound Access rules. By the custom definition of servers and services for inbound access, Internet users can access the servers behind the BD1000. Advanced configurations allow inbound access to be distributed among multiple servers on the LAN.

Note Inbound Access applies only to WAN connections that operate under NAT mode. For WAN connections that operate under drop-in mode or IP forwarding, inbound traffic is forwarded to the LAN by default.

This section describes the following settings for managing inbound access features using the BD1000 Web Admin Interface:

Port Forwarding Service Settings

The BD1000 can act as a firewall that blocks all inbound access from the Internet by default. By using the port forwarding, Internet users can access the servers behind the BD1000. To configure inbound port forwarding rules, click on **Network > Inbound Access > Port Forwarding** in the Web Admin Interface.

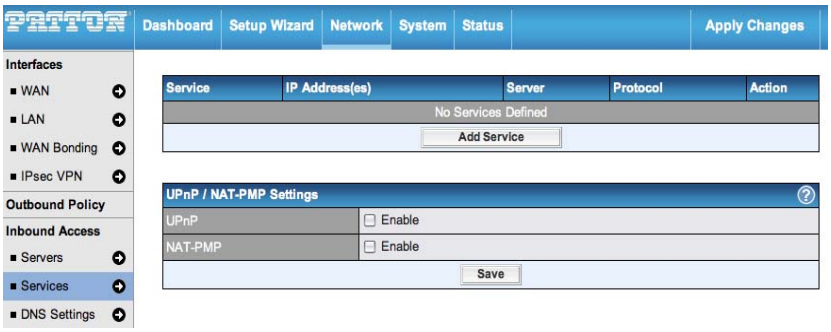


Figure 44. Network > Inbound Access > Port Forwarding

To define a new service, click the **Add Service** button and the following window displays:

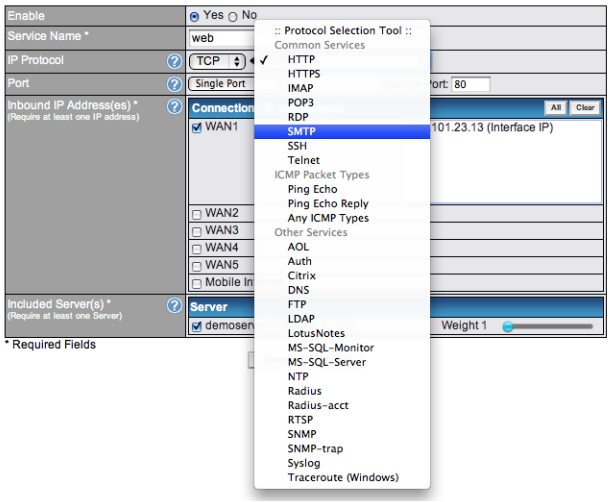


Figure 45. Network > Inbound Access > Port Forwarding > Add Service

Table 28. Port Forwarding Service: New Service Settings

Field	Description
Enable	Specifies whether the inbound service rule takes effect. Select **Yes** for the inbound service rule to take effect. If the inbound traffic matches the specified IP Protocol and Port, the BD1000 will take action based on the other parameters of the rule. Select **No** to disable the inbound service rule. The BD1000 will disregard the other parameters of the rule.
Service Name	Identifies the service to the System Administrator. Valid values for this setting consist only of alphanumeric and the underscore "_" characters.

Table 28. Port Forwarding Service: New Service Settings

Field	Description
IP Protocol	Specifies the protocol of the service as TCP, UDP, ICMP or IP. Traffic that is received by the BD1000 via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the **Servers** setting. (See below for details on the **Port** and **Servers** settings.) Alternatively, use the **Protocol Selection Tool** drop-down menu to automatically fill in the **Protocol** and a single **Port** number of common Internet services (e.g. HTTP, HTTPS, etc.). After selecting an item from the **Protocol Selection Tool** drop-down menu, you may still manually modify the **Protocol** and **Port** settings.
Port	Specifies the port(s) that correspond to the service, and can be configured to behave in one of the following ways: • **Any Port:** All traffic that is received by the BD1000 via the specified protocol is forwarded to the servers specified by the **Servers** setting. – For example, with IP Protocol set to **TCP** and Port set to **Any Port**, all TCP traffic is forwarded to the configured servers. • **Single Port:** Traffic that is received by the BD1000 via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting. – For example, with IP Protocol set to **TCP** and Port set to **Single Port** and **Service Port 80**, TCP traffic received on Port 80 is forwarded to the configured servers via Port 80. • **Port Range:** Traffic that is received by the BD1000 via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Servers** setting. – For example, with IP Protocol set to **TCP** and Port set to **Single Port** and **Service Port 80-88**, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports. • **Port Mapping:** Traffic that is received by the BD1000 via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Servers** setting. – For example, with IP Protocol set to **TCP** and Port set to **Port Map Service Port 80** and **Map to Port 88**, TCP traffic on Port 80 is forwarded to the configured servers via Port 88. • **Range Mapping:** Traffic that is received by the BD1000 via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the **Servers** setting.
Inbound IP Addresses	Specifies the WAN connections and Internet IP address(es) from which the service can be accessed. It is required to select at least one IP address.
Server IP Address	Specifies the LAN IP address of the server that handles the service requests.

Inbound Access LAN Servers

To configure settings for servers on the LAN, click on **Network > Inbound Access > Servers**. Inbound connections from the Internet will be forwarded to the specified Inbound IP Address(es) based on the protocol and port number. When more than one server is defined, requests will be distributed to the servers in the weight ratio specified for each server.

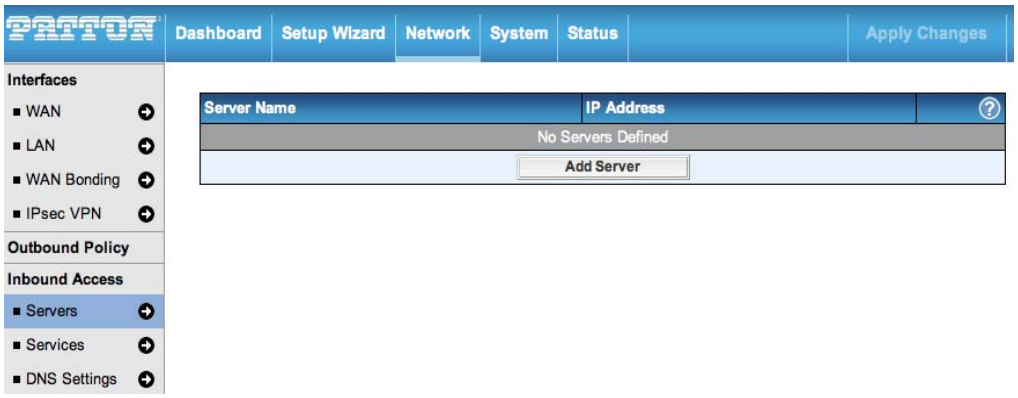


Figure 46. Network > Inbound Access > Servers

To define a new server, click the **Add Server** button to show the following window:

Figure 47. Network > Inbound Access > New Server

Enter a valid server name, and its corresponding LAN IP address.

Click **Save** to keep the new server information. The updated Server List page displays.

To define additional servers, click the **Add Server** button and repeat the above steps.

Inbound Access Services

To configure inbound access services, click on **Network > Inbound Access > Services**. At least one server must be defined before services can be added.

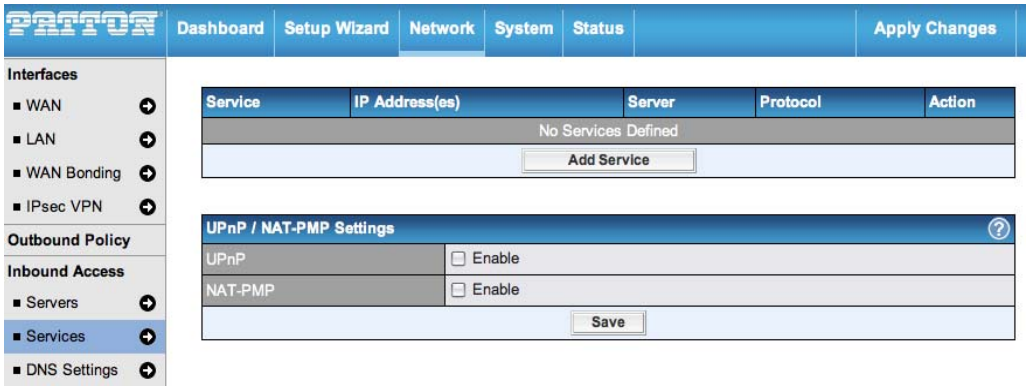


Figure 48. Network > Inbound Access > Services

To define a new service, click the **Add Service** button to show the following window:

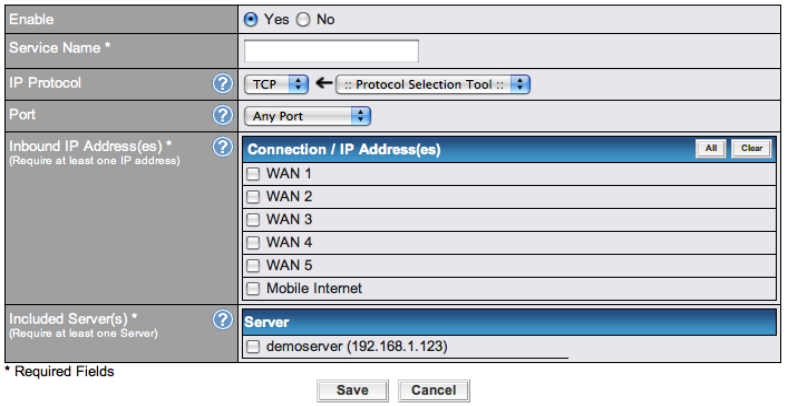


Figure 49. Network > Inbound Access > New Service

Table 29. Inbound Access Services: New Service Settings

Field	Description
Enable	Specifies whether the inbound service rule takes effect. Select **Yes** for the inbound service rule to take effect. If the inbound traffic matches the specified IP Protocol and Port, the BD1000 will take action based on the other parameters of the rule. Select **No** to disable the inbound service rule. The BD1000 will disregard the other parameters of the rule.
Service Name	Identifies the service to the System Administrator. Valid values for this setting consist only of alphanumeric and the underscore "_" characters.

Table 29. Inbound Access Services: New Service Settings

Field	Description
IP Protocol	Specifies the protocol of the service as TCP, UDP, ICMP or IP. Traffic that is received by the BD1000 via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the **Servers** setting. (See below for details on the **Port** and **Servers** settings.) Alternatively, use the **Protocol Selection Tool** drop-down menu to automatically fill in the **Protocol** and a single **Port** number of common Internet services (e.g. HTTP, HTTPS, etc.). After selecting an item from the **Protocol Selection Tool** drop-down menu, you may still manually modify the **Protocol** and **Port** settings.
Port	Specifies the port(s) that correspond to the service, and can be configured to behave in one of the following ways: • **Any Port:** All traffic that is received by the BD1000 via the specified protocol is forwarded to the servers specified by the **Servers** setting. – For example, with IP Protocol set to **TCP** and Port set to **Any Port**, all TCP traffic is forwarded to the configured servers. • **Single Port:** Traffic that is received by the BD1000 via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting. – For example, with IP Protocol set to **TCP** and Port set to **Single Port** and **Service Port 80**, TCP traffic received on Port 80 is forwarded to the configured servers via Port 80. • **Port Range:** Traffic that is received by the BD1000 via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Servers** setting. – For example, with IP Protocol set to **TCP** and Port set to **Single Port** and **Service Port 80-88**, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports. • **Port Mapping:** Traffic that is received by the BD1000 via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Servers** setting. – For example, with IP Protocol set to **TCP** and Port set to **Port Map Service Port 80** and **Map to Port 88**, TCP traffic on Port 80 is forwarded to the configured servers via Port 88. • **Range Mapping:** Traffic that is received by the BD1000 via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the **Servers** setting.
Inbound IP Addresses	Specifies the WAN connections and Internet IP address(es) from which the service can be accessed. It is required to select at least one IP address.

Table 29. Inbound Access Services: New Service Settings

Field	Description
Included Server(s)	Specifies the LAN servers that manage the service requests and the relative weight values. The amount of traffic that is distributed to a server is proportional to the weight value assigned to the server relative to the total weight. **Example:** With the following weight settings on a BD1000: demo_server_1: 10 demo_server_2: 5 The total weight is 15 = (10 + 5) Matching traffic distributed to demo_server_1: 67% = (10 / 15) x 100% Matching traffic distributed to demo_server_2: 33% = (5 / 15) x 100%

UPnP/NAT-PMP Settings

Universal Plug and Play (UPnP) and NAT Port Mapping Protocol (NAT-PMP) are network protocols that allow a computer on the LAN to automatically configure the router to allow parties on the WAN to connect to itself. In this way, the process of inbound port forwarding is automated.

When a computer creates a rule using these protocols, the specified TCP/UDP port of all WAN connections of the default IP address will be forwarded.

Check the corresponding box(es) to enable UPnP and/or NAT-PMP. Only enable these features if you trust the computers on the LAN.

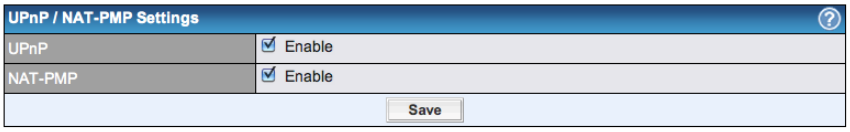


Figure 50. Status > UPnP/NAT-PMP

When enabled, click on **Status > UPnP/NAT-PMP** to view a list of the forwarded ports controlled via UPnP or NAT-PMP.

DNS Records

The built-in DNS Server functionality of the BD1000 facilitates inbound load balancing. With the presence of the functionality, NS/SOA DNS records for a domain name can be delegated to Internet IP address(es) of the BD1000. Upon receiving a DNS query, the BD1000 supports returning, as an "A" record, the corresponding IP address for the domain name on the most appropriate healthy WAN connection. It also supports acting as a generic DNS server for hosting "A," "CNAME," "MX," "TXT" and "NS" records.

For example (for illustration only; the actual resolution that takes place in implementation will likely vary):

The DNS resolution of the domain name www.mycompany.com is delegated to the WAN2 Internet IP addresses of the BD1000. Upon receiving the DNS query, the BD1000 returns, as an "A" record, the IP address for www.mycompany.com on WAN1 because WAN1 is the most appropriate healthy link.

The settings for defining the DNS records to be hosted by the BD1000 are located at: **Network > Inbound Access > DNS Settings**.

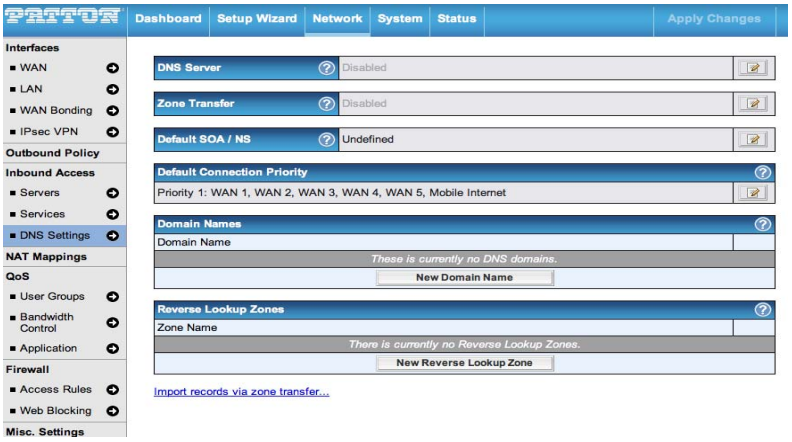


Figure 51. Network > Inbound Access > DNS Settings

Table 30. Inbound Access: DNS Records

Field	Description
DNS Server	Specifies the WAN IP addresses on which the DNS server of the BD1000 should listen. If no addresses are selected, the Inbound Link Load Balancing feature will be disabled; the BD1000 will not respond to DNS requests. To specify and/or modify the IP addresses on which the DNS Server should listen, click the **Edit** button that corresponds to **DNS Server Listens on**. To specify the IP addresses on which the DNS Server should listen, select the WAN connection by checking the appropriate boxes and the IP addresses associated with the WAN connections by highlighting the appropriate items in the list. (Multiple items in the list can be selected by holding CTRL and clicking on the items.) Click **Save** to keep the settings when configuration is complete.
Zone Transfer	Specifies the IP address(es) of secondary DNS server(s) that are to be allowed to retrieve zone records from the DNS server of the BD1000.The zone transfer server of the BD1000 listens on TCP Port 53. The BD1000 serves both the clients that are accessing from the specified IP addresses, and the clients that are accessing from the LAN Interface (of the BD1000 unit).
Default SOA/NS	Click the Pencil icon to define a default SOA / NS record for all Domain Names. For configuration details, refer to "SOA Records" on page 80. For defining a default SOA record, the field Name Server IP Address is optional. If left blank, the Address (A) record for the same server should be defined manually in each domain. For defining default NS records, the host [domain] indicates that this record is for the domain name itself, without a sub-domain prefix. To add a secondary NS server, just create a second NS record with the Host field empty. When the entered Name Server is a FQDN, the IP Address field will be disabled.
Default Connection Priority	Defines the default priority group of each WAN connection in resolving A records. It applies to A records which have the Connection Priority set to **Default**. For configuration details, refer to "CNAME Records" on page 82. The WAN connection(s) with the highest priority (smallest number) will be chosen. Those with lower priorities will not be chosen in resolving A records unless the higher priority ones become unavailable. To specify the Primary and Backup connections, click the Pencil icon that corresponds to **Default Connection Priority**. Each WAN connection is associated with a priority number. Click **Save** to keep the settings when configuration is complete.
Domain Name	Displays a list of domain names to be hosted by the BD1000. Each domain can have its "NS", "MX" and "TXT" records, and its or its sub-domains' "A" and "CNAME" records. Add a new record by clicking the **New Domain Name** button. Click on a domain name to edit. Press the X button to remove a domain name.

The settings for creating new DNS records for a domain are located at: **Network > Inbound Access > DNS Settings**. In the **Domain Name** field, enter a name for the new entry. Click on the newly created link to display the following screen. This page defines the domain's SOA, NS, MX, CNAME, A, TXT and SRV records. Seven tables are presented in this page for defining the five types of records.

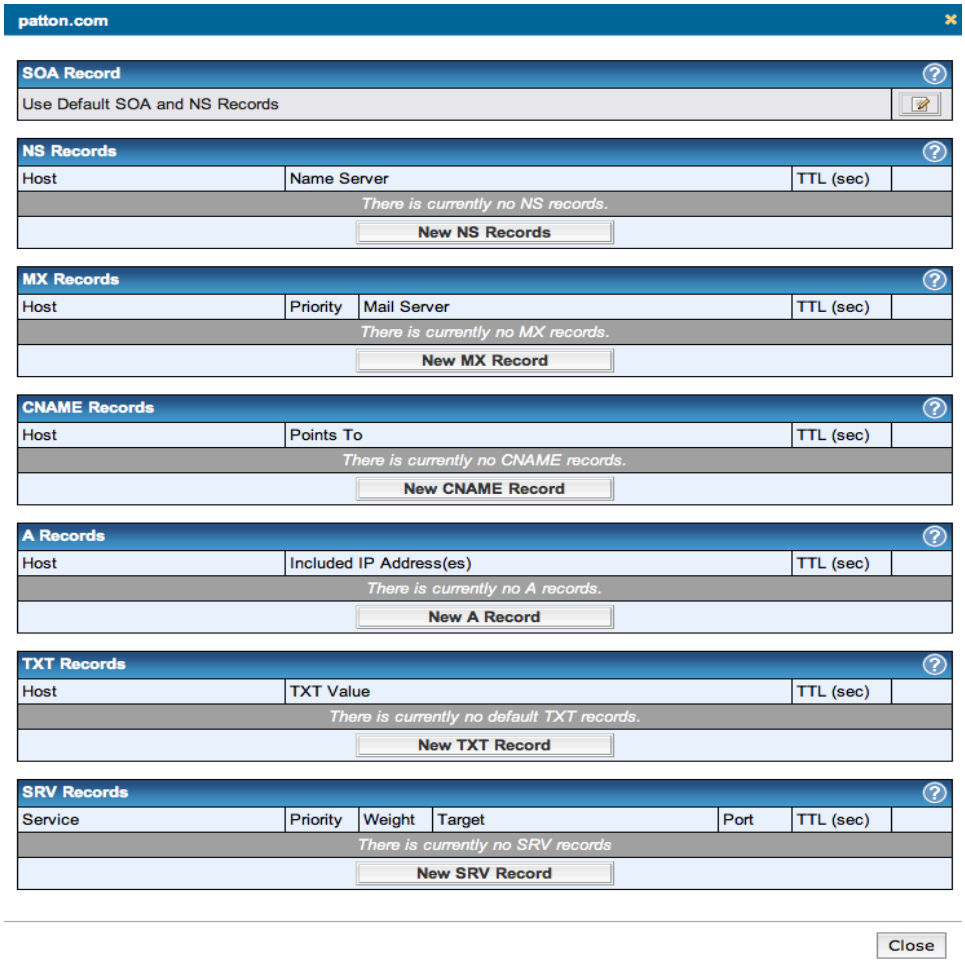


Figure 52. Network > Inbound Access > DNS Settings

Refer to the following sections for information about the types of DNS records:

- Start Of Authority Records - "SOA Records" on page 80
- Name Server Records - "NS Records" on page 81
- Mail Exchange Records - "MX Records" on page 81
- Cononical Name Records - "CNAME Records" on page 82
- Address Records - "A Records" on page 82
- Pointer Records - "PTR Records" on page 84
- Text Records - "TXT Records" on page 84
- Service Locator Records - "SRV Records" on page 85

SOA Records

Click on the Pencil icon to choose whether to use the pre-defined Default SOA Record and NS Records. If the option's Default SOA and NS Records is selected, any changes made in the Default SOA / NS Records will be applied to this domain automatically. Otherwise, select the SOA Record option to customize this domain's SOA and NS records.

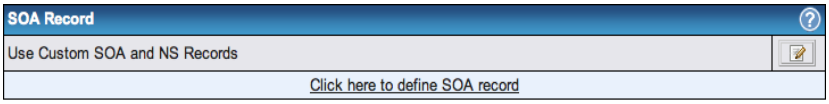


Figure 53. DNS > SOA Record

The table in the figure above displays the current SOA record. When the option **Customize SOA Record for this domain** is selected, you can click the link **Click here to define SOA record** to create, or click on the **Name Server** field to edit the SOA record.

In the SOA record, you must fill out the fields for: *Name Server, Name Server IP Address (optional), Email, Refresh, Retry, Expire, Min Time*, and *TTL*.

Default values are set for SOA and NS records.

- **Name Server IP Address (optional):** This is the IP address of the authoritative name server. If the Balance is the authoritative name server of the domain, this field's value should be the WAN connection's name server IP address that is registered in the DNS registrar. If this field is entered, a corresponding A record for the name server will be created automatically. If it is left blank, the A record for the name server must be created manually.
- **E-mail:** Defines the E-mail address of the person responsible for this zone. Note: Format should be mail-box-name.domain.com, e.g. hostmaster.example.com
- **Refresh:** Indicates the length of time (in seconds) when the slave will try to refresh the zone from the master.
- **Retry:** Defines the duration (in seconds) between retries if the slave (secondary) fails to contact the master when refresh (above) has expired.
- **Expire:** Indicates the time (in seconds) when the zone data is no longer authoritative. This option applies to Slaves DNS servers only.
- **Min Time:** Sets the negative caching time that defines the time (in seconds) after an error record is cached.
- **TTL (Time-to-Live):** Defines the duration (in seconds) that the record may be cached.

NS Records

The NS Record table shows the NS servers and TTL that correspond to the domain. The NS record of the name server defined in the SOA record is automatically added here. To add a new NS record, click the **New NS Records** button in the **NS Records** box. Then, the table will expand to look like the following:

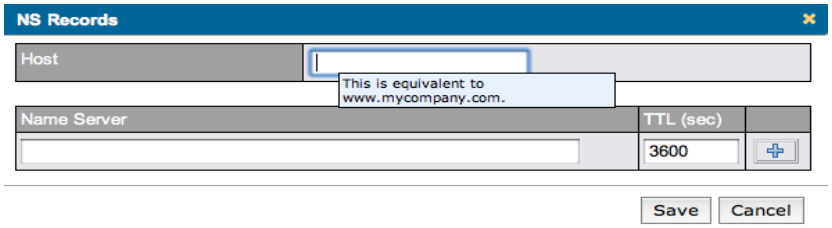


Figure 54. DNS > NS Record

When creating an NS record for the domain itself (not a sub-domain), the **Host** field should be left blank. Enter a name server host name and its IP address into the corresponding boxes. The host name can be a non-FQDN (Fully Qualified Domain Name). (Please be sure that a corresponding A record is created.)

Click the + button to complete the entry and add the other Name Server. After finishing adding NS records, click the **Save** button. (If you have *not* clicked the **Save** button, all NS record changes are not yet saved to the BD1000.)

MX Records

The MX Record table shows the domain's MX records. To add a new MX record, click the **New MX Records** button in the **MX Records** box. Then, the table will expand to look like the following:

Figure 55. DNS > MX Record

When creating an MX record for the domain itself (not a sub-domain), the **Host** field should be left blank.

For each record, **Priority** and **Mail Server** name must be entered. **Priority** typically ranges from 10 to 100. Smaller numbers have a higher a priority.

After finishing adding MX records, click the **Save** button.

CNAME Records

The CNAME Record table shows the domain's CNAME records. To add a new CNAME record, click the **New CNAME Records** button in the **CNAME Records** box. Then, the table will expand to look like the following:

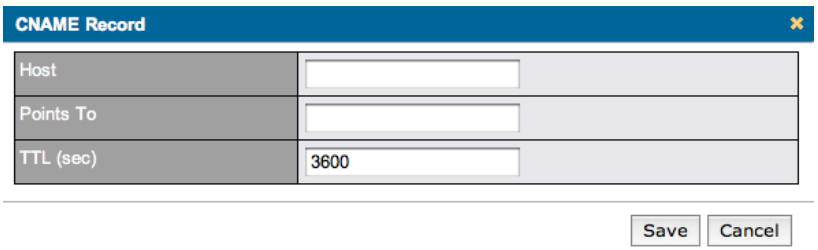


Figure 56. DNS > CNAME Record

When creating a CNAME record for the domain itself (not a sub-domain), the **Host** field should be left blank.

The wildcard character "*" is supported in the **Host** field. The Reference of "*.*omain.name*" will be returned for every name ending with ".*domain.name*" except names that have their own records.

The **TTL** field tells the time-to-live of the record in external DNS caches.

A Records

This table shows the A records of the domain name.

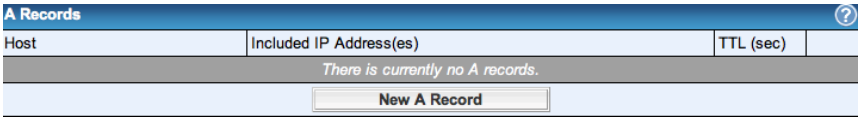


Figure 57. DNS > A Record

To add an A record, click the **New A Record** button. The following screen displays:

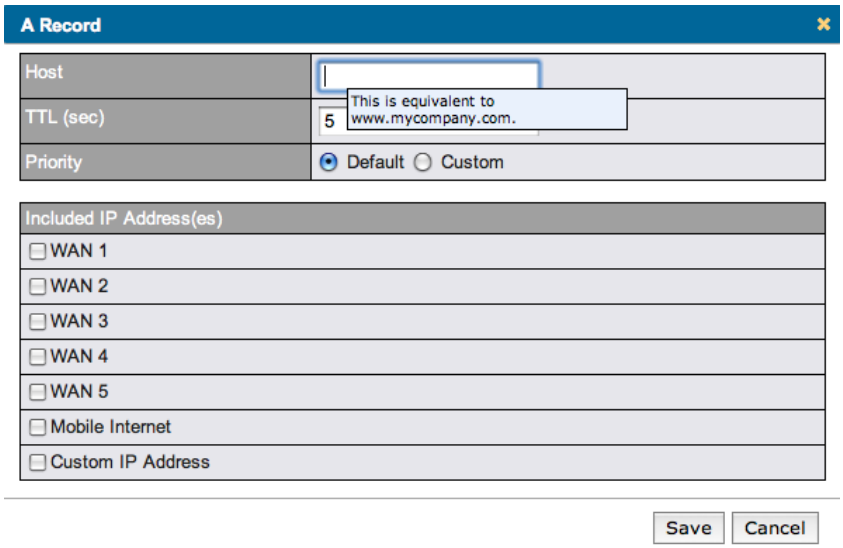


Figure 58. DNS > A Record

An A record may be automatically added for the SOA records with a Name Server IP Address provided.

Table 31. DNS: A Records

Field	Description
Host Name	Specifies the A record of this sub-domain to be served by the BD1000. The wildcard character "*" is supported. The IP addresses of *".domain.name"* will be returned for every name ending with "*domain.name"* except names that have their own records.
TTL	Specifies the time-to-live of this record in external DNS caches. In order to reflect any dynamic changes on the IP addresses in case of link failure and recovery, this value should be set to a smaller value. E.g. 5 secs, 60 secs, etc.
Priority	Specifies the priority of different connections. Select the **Default** option to apply the **Default Connection Priority** (refer to the main DNS Settings page) to an A record. To customize priorities, choose the Custom option and a priority selection table will be shown at the bottom.
Included IP Address(es)	Specifies the WAN-specific Internet IP addresses that are candidates to be returned when the BD1000 responds to DNS queries for the domain name specified by Host Name. The IP addresses listed in each box as **default** are the Internet IP addresses associated with each of the WAN connections. Static IP addresses that are not associated with any WAN can be entered into the Custom IP list. A PTR record is also created for each Custom IP. For WAN connections that operate under Drop-in mode, there may be other routable IP addresses in addition to the **default** IP address. Therefore, the BD1000 allows custom Internet IP addresses to be added manually via filling the text box on the right-hand side and clicking the + button. Only the checked IP addresses in the lists are candidates to be returned when responding to a DNS query. In case a WAN connection is down, the corresponding set of IP addresses will not be returned. However, the IP addresses in the Custom IP field will always be returned. If the Connection Priority field is set to **Custom**, you can also specify the priority of the use of each WAN connection. Only selected IP address(es) of available connection(s) with the highest priority, and also Custom IP addresses will be returned. By default, the Connection Priority is set to **Default**.

PTR Records

PTR records are created along with A records pointing to Custom IPs (see "A Records" on page 82). For example, if you created an A record *www.mydomain.com* pointing to *11.22.33.44*, then a PTR record *44.33.22.11.in-addr.arpa* pointing to *www.mydomain.com* will also be created.

When there are multiple host names pointing to the same IP address, only one PTR record for the IP address will be created.

In order to have the PTR records working, you will also have to create NS records for the PTR records. For example, if the IP address range *11.22.33.0* to *11.22.33.255* is delegated to the DNS server on the BD1000, you will also have to create a domain *33.22.11.in-addr.arpa* and have its NS records pointing to your DNS server's (the BD1000) public IP addresses.

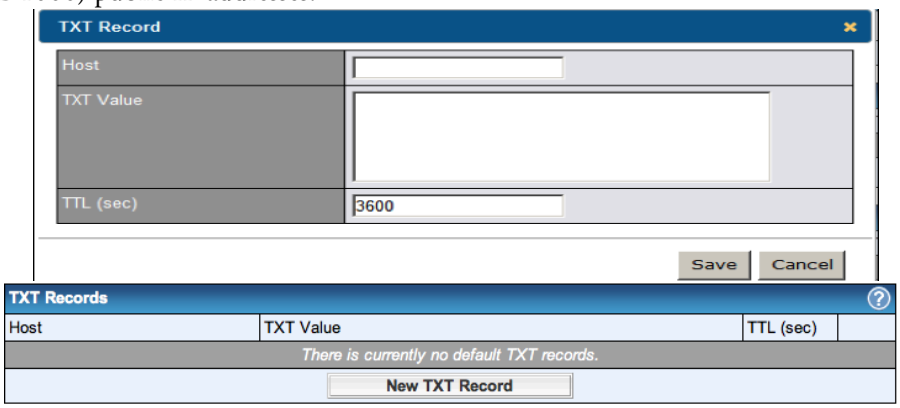


Figure 59. DNS > PTR Record

With the above records created, the PTR record creation is complete.

TXT Records

This table shows the TXT record of the domain name.

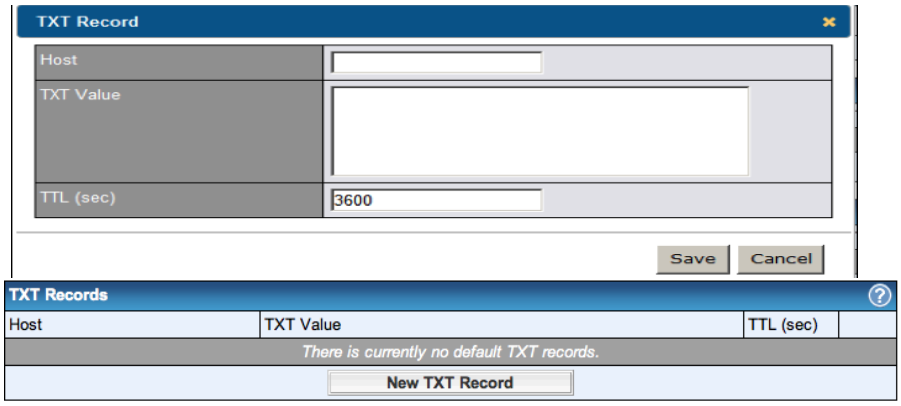


Figure 60. DNS > TXT Record

To add a new TXT record, click the **New TXT Record** button in the **TXT Records** box. Click the **Edit** button to edit the record. The time-to-live value and the TXT record's value can be entered. Click the **Save** button to complete the entry.

When creating a TXT record for the domain itself (not a sub-domain), the **Host** field should be left blank.

The maximum size of the TXT Value is 255 bytes.

After you are done editing the types of record, you can simply leave the page by going to another section of the Web Admin Interface.

SRV Records

To add a new SRV record, click the **New SRV Record** button in the **SRV Records** box.

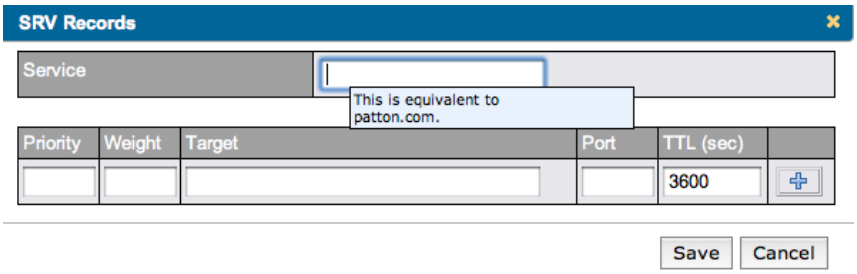


Figure 61. DNS > SRV Record

- **Service:** The symbolic name of the desired service.
- **Priority:** Indicates the priority of the Target; the smaller the value, the higher the priority.
- **Weight:** A relative weight for records with the same priority.
- **Target:** The canonical hostname of the machine providing the service.
- **Port:** Enter the TCP or UDP port number on which the service is to be found.

Domain Delegation

Follow the steps below if you host your domain at your ISP or a domain registrar and want to delegate a sub-domain to be resolved and managed at the BD1000.

1. Click **New Domain Name** button to add a domain name. e.g. *www.mycompany.com*. Click the corresponding domain name to view and edit record details.

Figure 62. DNS > Domain Delegation: New Domain Name

2. Create SOA / NS records named *ns1, ns2, etc*. The IP addresses are the BD1000 DNS server addressess.

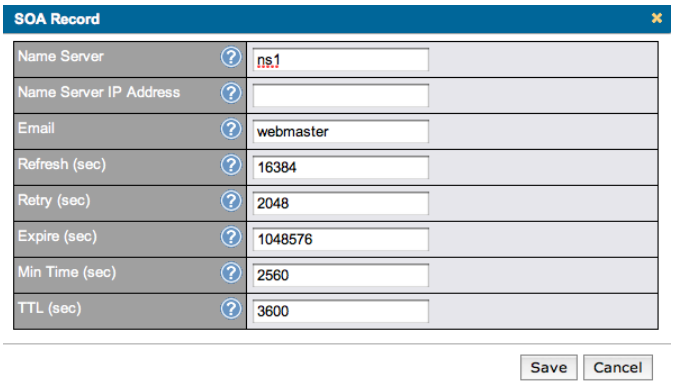


Figure 63. DNS > Domain Delegation: Create SOA/NS Records

3. Create an A record with an empty host name:

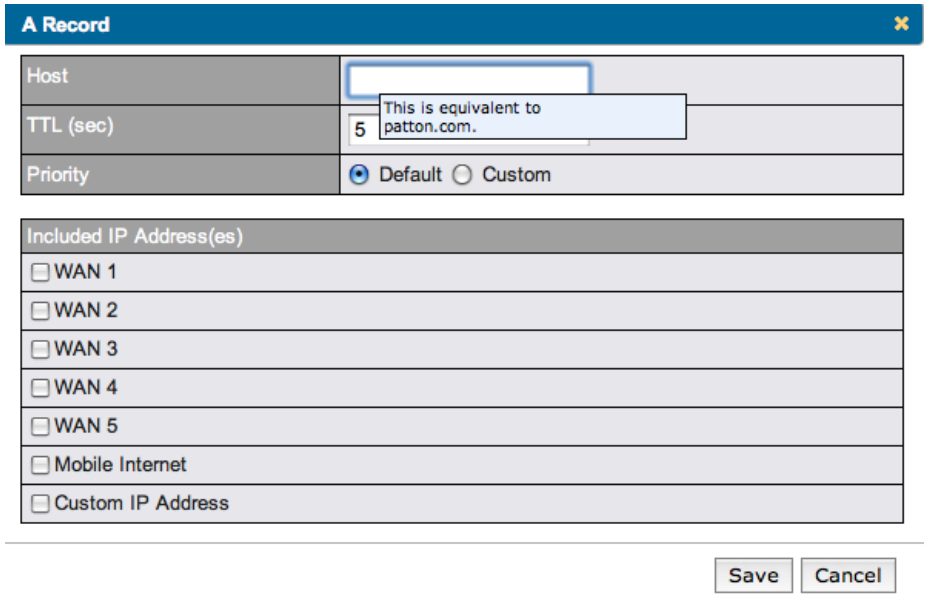


Figure 64. DNS > Domain Delegation: Create A Record

If ISC BIND 8 or 9 is being utilized in the zone file *mycompany.com*, then the addition of the following lines suffice:

www	*IN*	*NS*	*bd1000wan1*
www	*IN*	*NS*	*bd1000wan2*
bd1000wan1	*IN*	*A*	*202.153.122.108*
bd1000wan2	*IN*	*A*	*67.38.212.18*

Testing the DNS Configuration

To test the DNS configuration, use an IP address of the BD1000 and **nslookup** to search for the corresponding host name of a host on the Internet. Check the information that is returned for the expected results.

An example with **nslookup** in Windows follows:

```
:\Documents and Settings\User Name>nslookup
Default Server:  ns1.myisp.com
Address:  147.22.11.2
> server 202.153.122.108(This is the BD100 WAN IP address.)
Default Server:  balance.mycompany.com
Address:  202.153.122.108
> www.mycompany.com(This is the hostname to look up.)
Default Server:  balance.mycompany.com
Address:  202.153.122.108
Name:    www.mycompany.com
Address:  202.153.122.109, 67.38.212.19
```

The values of the IP addresses are fictitious and for illustration only; the actual IP addresses in implementation will likely be different.

Reverse Lookup Zones

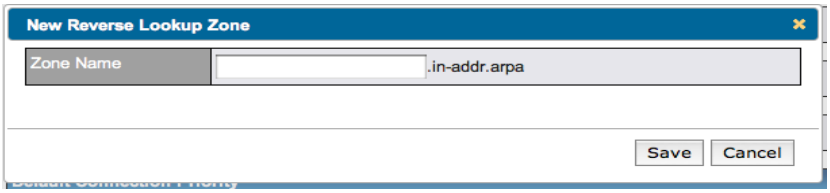


Figure 65. DNS > New Reverse Lookup Zone

Reverse Lookup refers to performing a DNS query to find one or more DNS names associated with a given IP address. The DNS stores IP addresses in the form of specially formatted names as pointer (PTR) records using special domains/zones. The zone is *in-addr.arpa*.

To enable DNS clients to perform a Reverse Lookup for a host, perform two steps:

1. Create a Reverse Lookup Zone that corresponds to the subnet network address of the host.
2. In the Reverse Lookup Zone, add a pointer (PTR) resource record that maps the host IP address to the host name.
3. Click the **New Reverse Lookup Zone** button and enter a Reverse Lookup Zone Name. If you are delegating the subnet 11.22.33.0/24, the Zone Name should be *11.33.22.11.in-arpa.addr*. PTR records for

11.22.33.1, 11.22.33.2, ... 11.22.33.254 should be defined in this zone where the Host IP Numbers are 1, 2, ... 254 respectively.

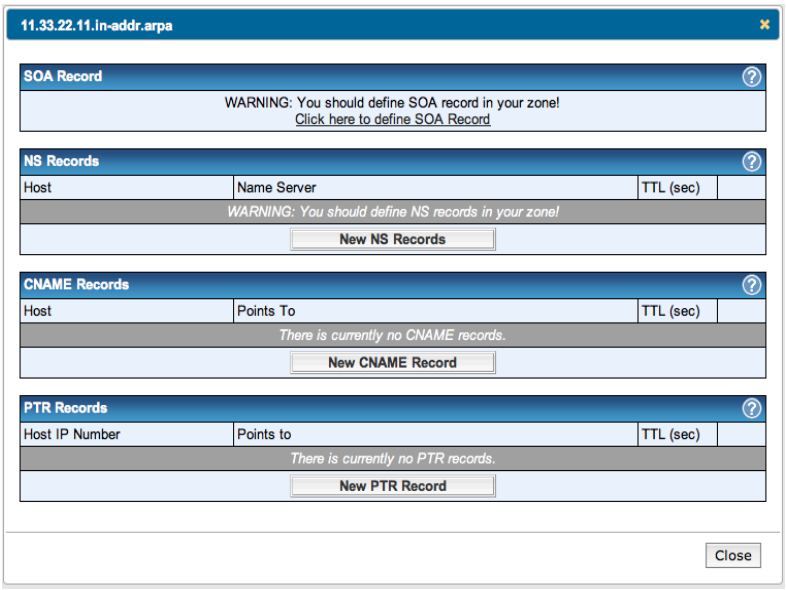


Figure 66. DNS > Reverse Lookup Zone Configuration

SOA Records

Click the link **Click here to define SOA record** to create or click on the Name Server field to edit the SOA record:

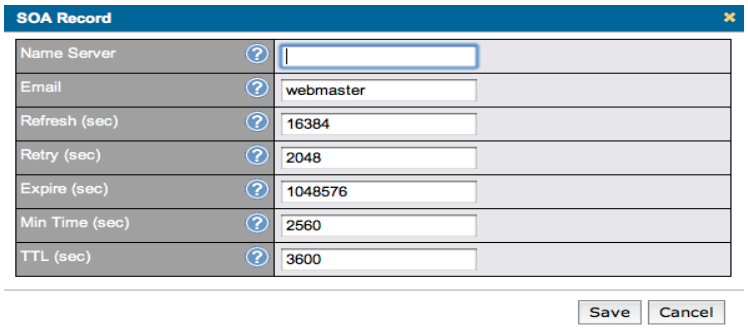


Figure 67. DNS > Reverse Lookup Zone > SOA Record

In the SOA record, you must fill out the fields for: *Name Server, Name Server IP Address (optional), Email, Refresh, Retry, Expire, Min Time*, and *TTL*

- **Name Server**: Enter the NS record's FQDN server name.

  For example:
  "ns1.mydomain.com" (equivalent to "www.1stdomain.com.")
  "ns2.mydomain.com."

- **Email, Refresh, Retry, Expire, Min Time,** and **TTL** are the same as that in the forward zone.

  Refer to "SOA Records" on page 80 for more information.

NS Records

The NS record of the name server defined in the SOA record is automatically added here. To create a new NS record, click the **New NS Records** button.

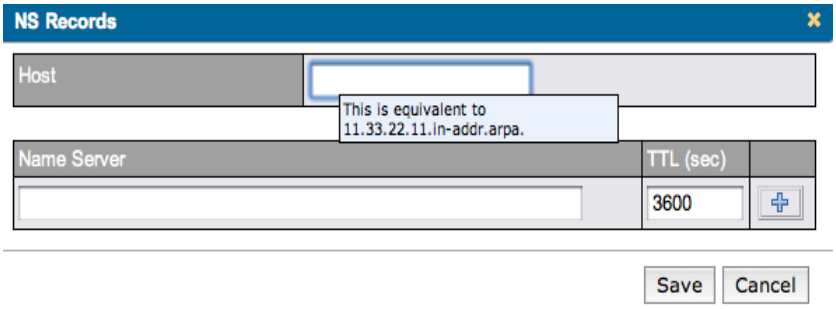


Figure 68. DNS > Reverse Lookup Zone > NS Record

When creating an NS record for the **Reverse Lookup Zone** itself (not a sub-domain or dedicated zone), the **Host** field should be left blank. The **Name Server** must be a FQDN (Fully Qualified Domain Name).

CNAME Records

To add a new CNAME record, click the **New CNAME Records** button.

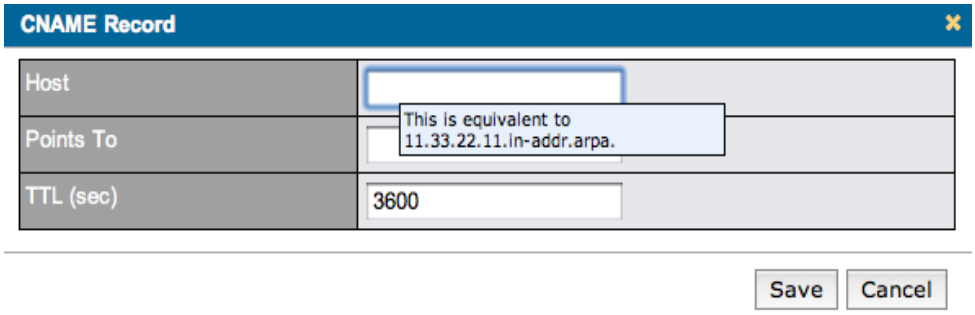


Figure 69. DNS > Reverse Lookup Zone > CNAME Record

CNAME records are typically used for defining classless reverse lookup zones. Subnetted reverse lookup zones are further described in RFC 2317, "Classless IN-ADDR.ARPA delegation."

PTR Records

To add a new PTR record, click the **New PTR Records** button.

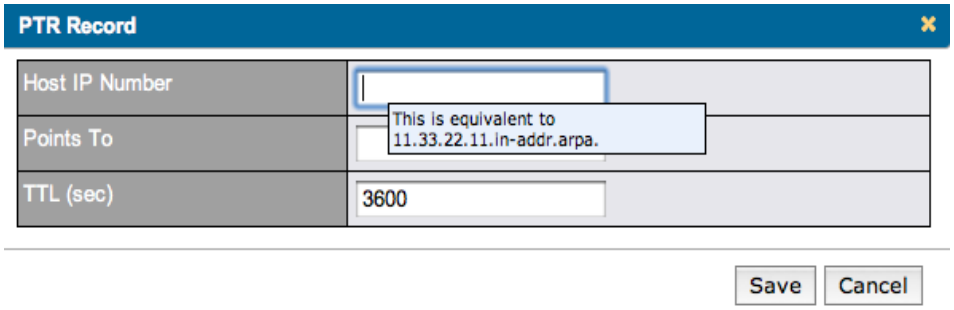


Figure 70. DNS > Reverse Lookup Zone > PTR Record

The **Host IP Number** field is the last integer in the IP address of a PTR record. E.g. for the IP address 22.33.44 where the Reverse Lookup Zone is *11.22.11.in-arpa.addr*, the Host IP Number should be *44*.

The **Points To** field defines the host name that the PTR record should direct to. It must be a FQDN (Fully Qualified Domain Name).

DNS Record Import Wizard

At the bottom of the page of DNS Settings, there is a link to **Import records via zone transfer…** that is used to access the DNS Record Import Wizard.

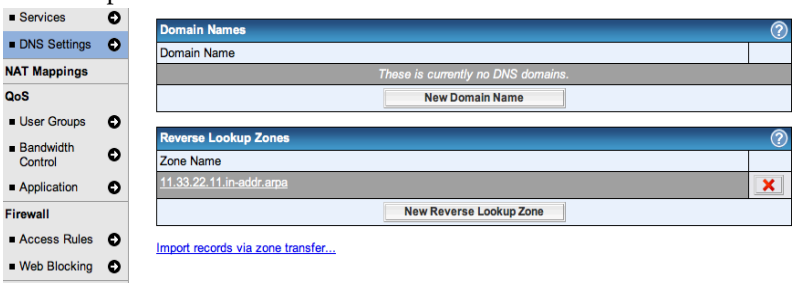


Figure 71. DNS > DNS Record Import Wizard (1)

1. From the Import Wizard introduction screen, click **Next >>** to continue.

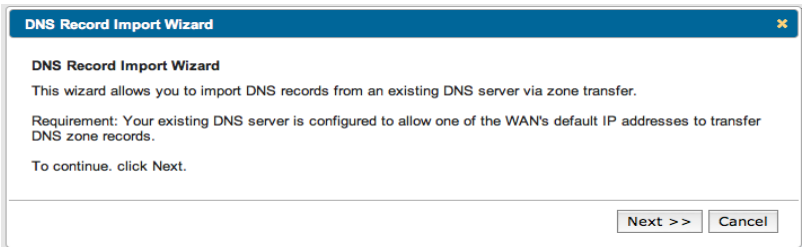


Figure 72. DNS > DNS Record Import Wizard (2)

2. In the **Target DNS Server IP Address** field, enter the IP address of the DNS server. In the **Transfer via…**field, choose the connection you would like to transfer through. Click **Next >>** to continue.

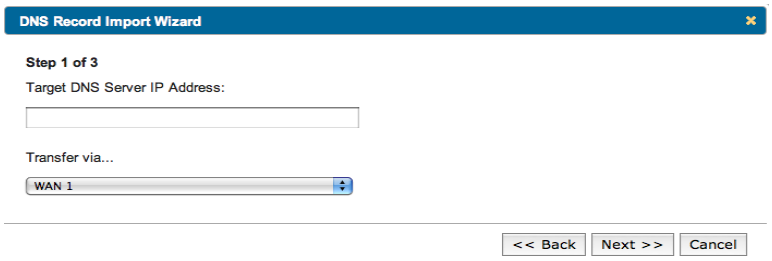


Figure 73. DNS > DNS Record Import Wizard (3)

3. In the blank space, enter the **Domain Names (Zones)** that you would like to assign with the IP address entered in the previous step. Enter one domain name per line. Click **Next >>** to continue.

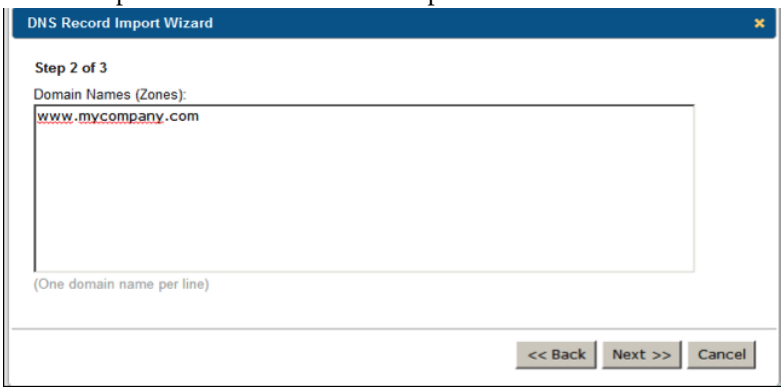


Figure 74. DNS > DNS Record Import Wizard (4)

Configuring NAT Mappings

This section describes how to set up NAP Mappings on the BD1000. A NAT Mapping configuration allows the BD1000 to map IP addresses of all inbound and outbound NAT traffic to and from an internal client IP address. To configure NAT Mappings, click on **Network > NAT Mappings** in the Web Admin Interface.

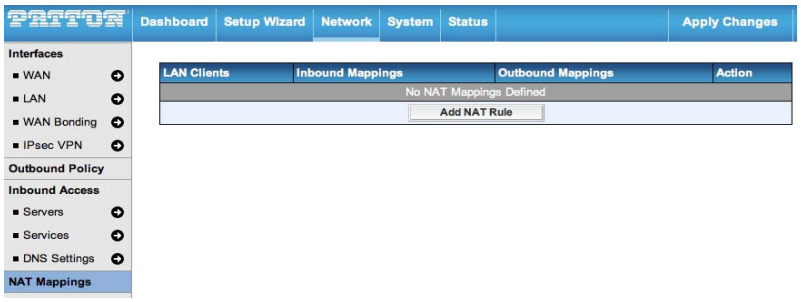


Figure 75. Network > NAT Mappings

To add a rule for NAT Mappings, click **Add NAT Rule** and the following window displays:

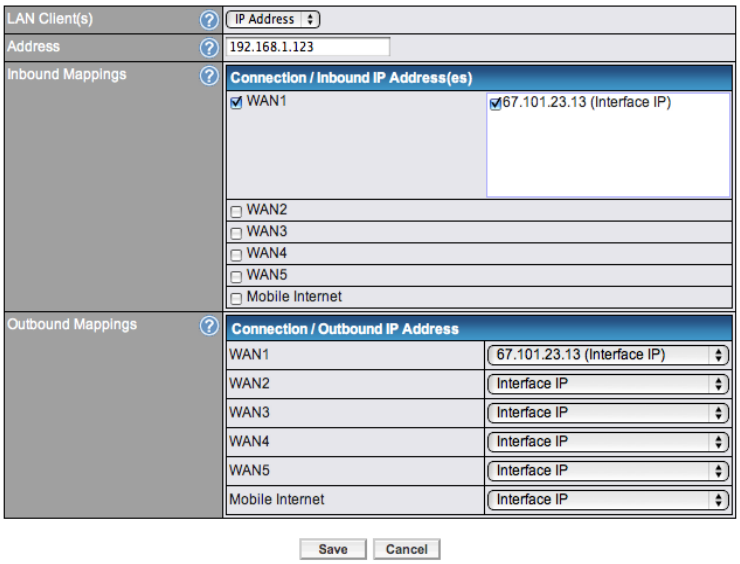


Figure 76. NAT Mappings > Add NAT Rule

Table 32 on page 94 explains the new NAT rule settings.

Table 32. NAT Mappings: New Rule Settings

Field	Description
LAN Client(s)	Specifies where the new rule applies: a single **LAN IP Address**, an **IP Range** or an **IP Network**.
Address	Refers to the LAN host's private IP address. The system maps this address to a number of specified public IP addresses in order to facilitate inbound and outbound traffic. *This option is only available when **IP Address** is selected as the **LAN Client**.
Range	Refers to a contiguous group of private IP addresses used by the LAN host. The system maps these addresses to a number of specified public IP addresses to facilitate outbound traffic. *This option is only available when **IP Range** is selected as the **LAN Client**.
Network	Refers to all private IP addresses and ranges managed by the LAN host. The system maps these addresses to a number of specified public IP addresses to facilitate outbound traffic. *This option is only available when **IP Network** is selected as the **LAN Client**.
Inbound Mappings	Specifies the system to bind on these WAN connections and corresponding WAN-specific IP addresses. Any access to the specified WAN connection(s) and IP address(es) will be forwarded to the LAN Host. *This option is only available when **IP Address** is selected as the **LAN Client**. **Note** Inbound Mapping is not needed for WAN connections in drop-in or IP forwarding mode. **Note** Each WAN IP address can be associated to one NAT Mapping only.
Outbound Mappings	Specifies which WAN IP addresses to use when an IP connection is made from a LAN host to the Internet. Each LAN host in an IP range or IP network will be evenly mapped to one of each selected WAN's IP addresses (for better IP address utilization) in a persistent manner (for better application compatibility). **Note** If you do not want to use a specific WAN for outgoing accesses, you should select the **Default** option, then customize the outbound access rule in the **Outbound Policy** section. **Note** WAN connections in drop-in or IP forwarding mode are not shown.

Click **Save** to save the new configuration.

Note Inbound firewall rules override the Inbound Mapping settings.

Chapter 7 Configuring Quality of Service

Chapter contents

Introduction

This chapter describes managing Quality of Service (QoS) settings for the BD1000. To configure QoS settings, click on **Network > QoS** in the Web Admin Interface. There are three services that you can manage under QoS: User Groups (page 96), Bandwidth Control (page 97), and Applications (page 98).

Managing User Groups

LAN and PPTP clients can be categorized into three user groups—**Manager**, **Staff** and **Guest**. The **User Group** table allows you to define rules and assign client IP addresses or subnets to a user group. You can apply different bandwidth and traffic prioritization policies on each user group in the **Bandwidth Control** and **Application** sections.

The table is automatically sorted and the table order signifies the rules' precedence. The smaller and more specific subnets are put towards the top of the table and have higher precedence; larger and less specific subnets are placed towards the bottom.

Click the **Add** button to define clients and their user group. Click ✖ to remove the defined rule.

Two default rules are pre-defined and located at the bottom of the table. They include **All DHCP reservation clients** and **Everyone**; these rules cannot be removed from the table. **All DHCP reservation clients** represent the LAN clients defined in the **DHCP Reservation** table in the **LAN settings** page. **Everyone** represents all clients that are not defined in any rule above. Click on a rule to change its group.

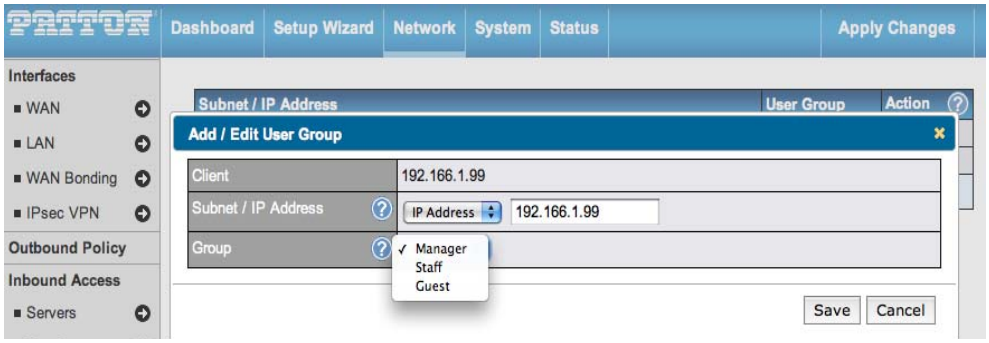


Figure 77. Network > QoS > User Groups

Table 33. QoS: User Group Settings

Field	Description
Subnet / IP Address	Select an option from the drop-down menu to define the client via **Subnet** or **IP Address**. Select **IP Address** to enter a name defined in the **DHCP Reservation** table or a LAN client's IP address. Select **Subnet** to enter a subnet address and specify a subnet mask.
Group	Defines the **User Group** for the specified **Subnet / IP Address**.

Once users have been assigned to a user group, their Internet traffic will be restricted by the rules defined for that particular group. For more information on setting these rules, refer to "Setting Up Bandwidth Control" on page 97 and "Configuring Applications" on page 98.

Setting Up Bandwidth Control

This section defines how much minimum bandwidth will be reserved to each user group when a WAN connection is in **full load**. When this feature is enabled, a slider with two indicators will be shown. You can move the indicators to adjust each group's weight. The lower part of the table shows the corresponding reserved download and upload bandwidth value of each connection.

By default, **50%** of bandwidth has been reserved for Manager, **30%** for Staff, and **20%** for Guest.

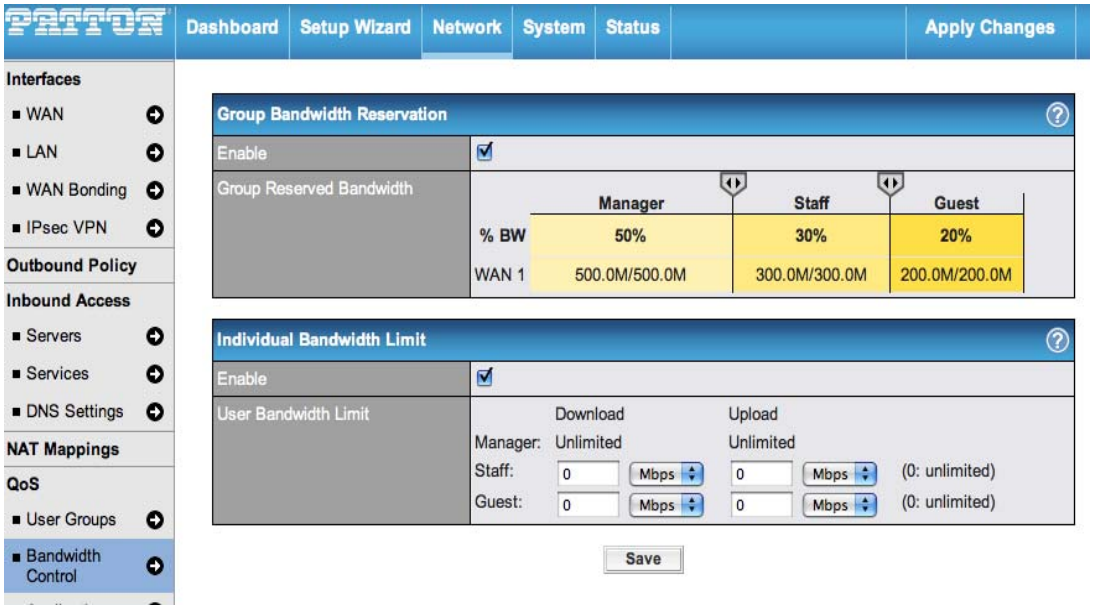


Figure 78. Network > QoS > Bandwidth Control

You can define a maximum download speed (over all WAN connections) and upload speed (for each WAN connection) that each individual Staff and Guest member can consume. No limit can be imposed on individual Manager members.

By default, Download and Upload Bandwidth Limits are set to unlimited (set as **0**).l

Configuring Applications

You may use the **Application** section of the QoS page for prioritizing and optimizing Application services.

Application Prioritization

You can choose whether to apply the same Prioritization settings to all user groups or customize the settings for each group.

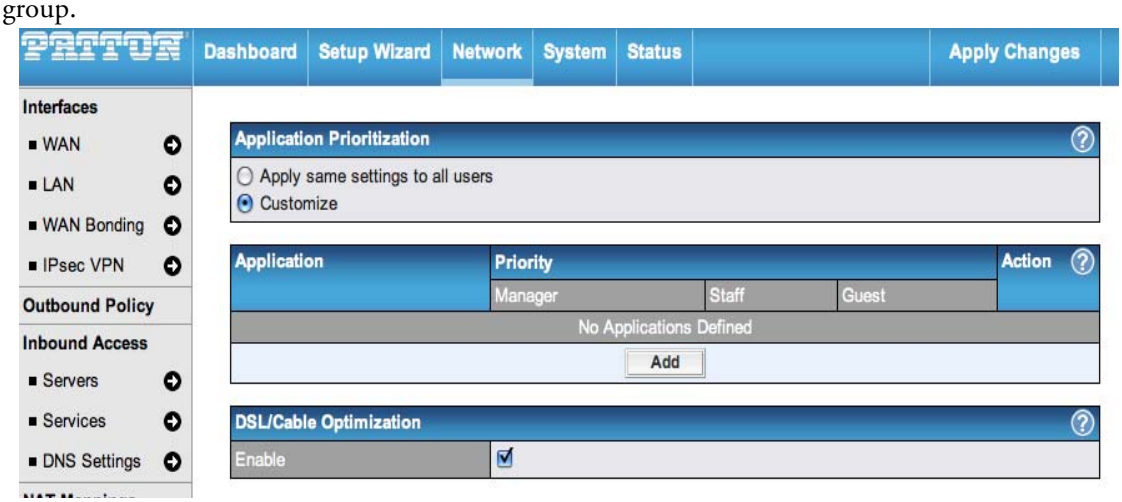


Figure 79. Network > QoS > Application Prioritization

You may choose from three priority levels for application prioritization—↑**High**, –**Normal** and ↓**Low**. The BD1000 supports various application traffic by inspecting the packets' content. Select an application by choosing a supported application, or by defining a custom application manually. The priority preference of supported applications is placed at the top of the table. Custom applications are at the bottom.

Prioritization for Custom Applications

Click the **Add** button to define a custom application. Click ✕ in the **Action** column to delete the custom application in the corresponding row.

When **Supported Applications** is selected, the BD1000 will inspect network traffic and prioritize the selected application. Alternatively, select **Custom Applications** to define the application by providing the protocol, scope, port number and DSCP value.

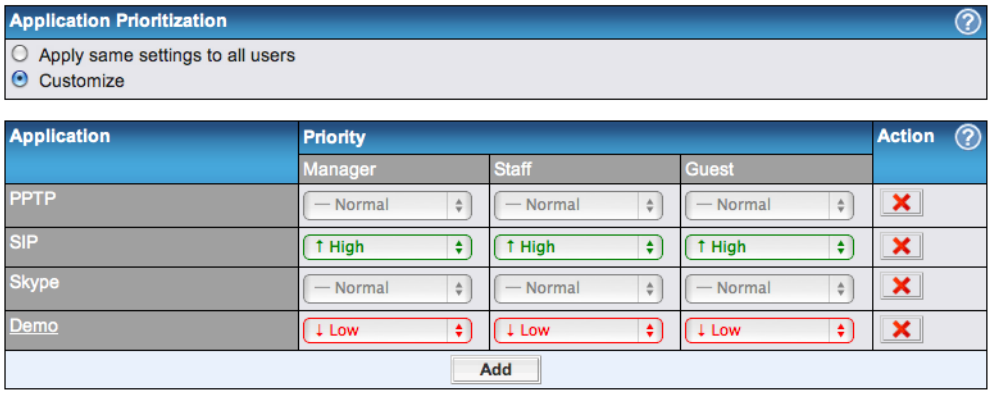


Figure 80. Network > QoS > Custom Applications Prioritization

DSL/Cable Optimization

A DSL/Cable-based WAN connection sets the upload bandwidth lower than the download bandwidth. With **DSL/Cable Optimization** option enabled, the download bandwidth of the WAN can be fully utilized in any situation.

When a DSL/Cable circuit's uplink is congested, the download bandwidth will be affected. Users will not be able to download data in full speed until the uplink becomes less congested. The **DSL/Cable Optimization** feature can relieve issues with this case. When enabled, the download speed will become less affected by the upload traffic.

By default, this feature is **Enabled**.

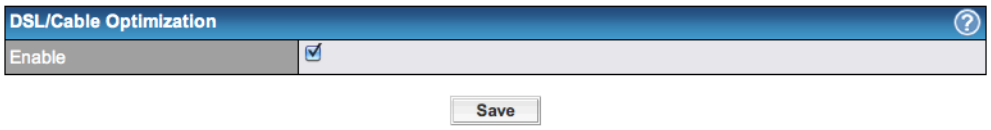


Figure 81. Network > QoS > DSL/Cable Optimization

Chapter 8 Configuring Firewall Settings

Chapter contents

Introduction

This chapter describes managing Firewall settings for the BD1000. A firewall is a mechanism that selectively filters data traffic between the WAN side (the Internet) and the LAN side of the network. It can protect the local network from potential hacker attacks, offensive Web sites and/or other inappropriate uses.

The firewall functionality of the BD1000 supports the selective filtering of data traffic in both directions:

- Outbound (LAN to WAN)
- Inbound (WAN to LAN)
- Intrusion Detection and DoS Prevention
- Web Blocking

With Site-to-Site VPN enabled (see Chapter 4, "Configuring the WAN" on page 50), the firewall rules also apply to VPN tunneled traffic.

Configuring Outbound and Inbound Firewall Rules

You may configure outbound and inbound firewall settings for "Access Rules" (see page 101) and for "Intrusion Detection and DoS Prevention" (see page 105).

Access Rules

To configure the outbound and inbound firewall settings, click on **Network > Firewall > Access Rules**.

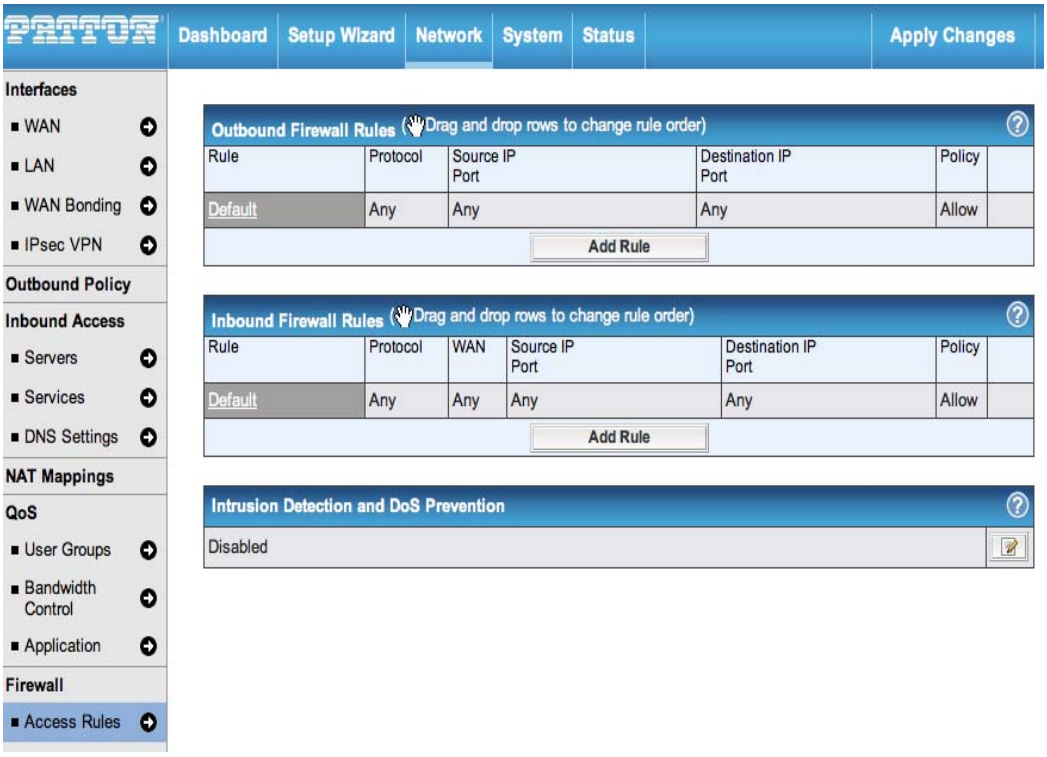


Figure 82. Network > Firewall > Outbound and Inbound Firewall Rules

After clicking **Add Rule**, the following configuration window displays:

Figure 83. Network > Firewall > Add Firewall Rule

Table 34 describes the settings for configuring a new firewall rule.

Table 34. Firewall: Inbound/Outbound Firewall Settings

Field	Description
Rule Name	Specifies a name for the firewall rule.
Enable	Specifies whether the firewall rule should take effect. Select **Yes** for the firewall rule to take effect. If the traffic matches the specified Protocol/IP/Port, the BD1000 will take action based on the other parameters of the rule. Select **No** to disable the firewall rule. The BD1000 will disregard the other parameters of the rule.
WAN Connection (*Only applies to inbound)	Specifies the WAN connections for the rule. Available options include: • Any (applies to all WAN connections) • WAN 1 • WAN 2 • WAN 3 • WAN 4 • WAN 5 • Mobile Internet

Table 34. Firewall: Inbound/Outbound Firewall Settings

Field	Description
Protocol	Specifies the protocol for the rule. Select one of the following protocols from the drop-down menu: • TCP • UDP • ICMP • IP Alternatively, you may use the **Protocol Selection Tool** drop-down menu to automatically fill in the Protocol and Port number of common Internet services (e.g. HTTP, HTTPS, etc.). After selecting an item from the Protocol Selection Tool drop-down menu, you may still modify the Protocol and Port number manually.
Source IP & Port	Specifies the source IP address(es) and port number(s) to match with the firewall rule. You may specify a single address or network, and a single port or a range of ports.
Destination IP & Port	Specifies the destination IP address(es) and port number(s) to match with the firewall rule. You may specify a single address or network, and a single port or a range of ports.
Action	Specifies what the BD1000 should do upon encountering traffic that matches the Source IP & Port or Destination IP & Port. Select **Allow** to let the matching traffic pass through the BD1000 (to be routed to the destination). Select **Deny** to disable the matching traffic from passing through the BD1000.
Event Logging	Specifies whether or not to log matched firewall events. You may view logged messages by clicking on **Status > Event** Log. The following shows a sample log message: `Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1 DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80` • **CONN:** The connection specified in the log entry • **SRC:** Source IP address • **DST:** Destination IP address • **LEN:** Packet length • **PROTO:** Protocol • **SPT:** Source port • **DPT:** Destination port

Click **Save** to add the new rule to the **Firewall Rules** table. To reorder the rules in the table, hold the left mouse button on the desired rule, drag it to the new position, and release the mouse button:

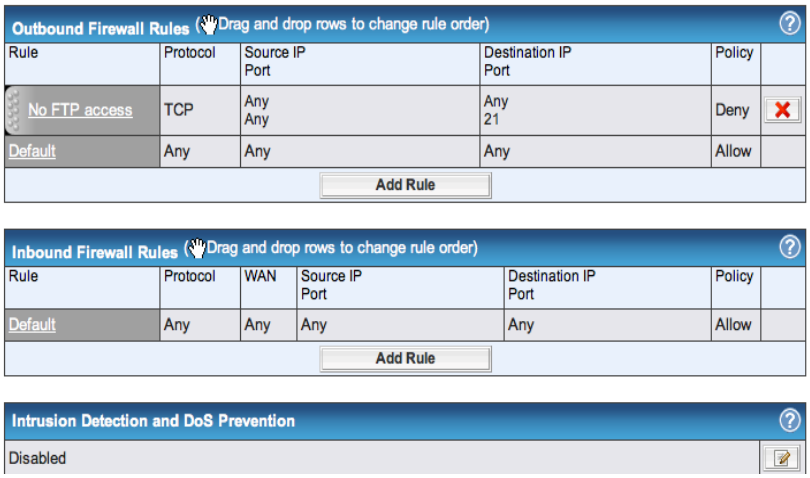


Figure 84. Network > Firewall > Reorder Rules List

To delete a rule from the table, click ✖. Rules are matched from top to bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules match the connection, the BD1000 will apply the **Default** rule. The **Default** rule is set to **Allow** for both outbound and inbound access.

Note If the default inbound rule is set to **Allow** for NAT-enabled WANs, no inbound allowed firewall rules will be required for inbound Port Forwarding and inbound NAT Mapping rules. However, if the default inbound rule is set to **Deny,** a corresponding **Allow** firewall rule will be required.

Intrusion Detection and DoS Prevention

The BD1000 supports detecting and preventing intrusions and Denial-of-Service (DoS) attacks from the Internet. To turn on this feature, click and check **Enable** for Intrusion Detection and DoS Prevention. Click **Save** to apply the setting.

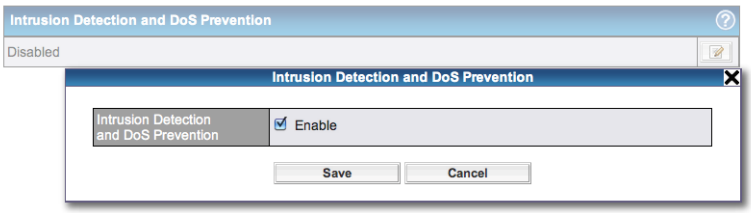


Figure 85. Network > Firewall > Intrusion Detection and DoS Prevention

When enabled, the BD1000 will detect and protect the network from the following kinds of intrusions and denial-of-service attacks:

- **Port Scan:**
  - NMAP FIN/URG/PSH
  - Xmas Tree
  - Another Xmas Tree
  - Null Scan
  - SYN/RST
  - SYN/FIN
- **SYN Flood Prevention**
- **Ping Flood Attack Prevention**

Setting Up Web Blocking

Enter an appropriate website address and the BD1000 will block and disallow LAN/PPTP/Site-to-Site VPN peer clients to access these websites.

You may enter the wild card ".*" at the end of a domain name to block any web site with a host name having the domain name in the middle. For example, If you enter "foobar.*," then "www.foobar.com," "www.foobar.co.jp," or "foobar.co.uk" will be blocked. Placing the wild card in any other position is not supported.

The BD1000 will inspect and look for blocked domain names on all HTTP traffic. Secure web (HTTPS) traffic is not supported.

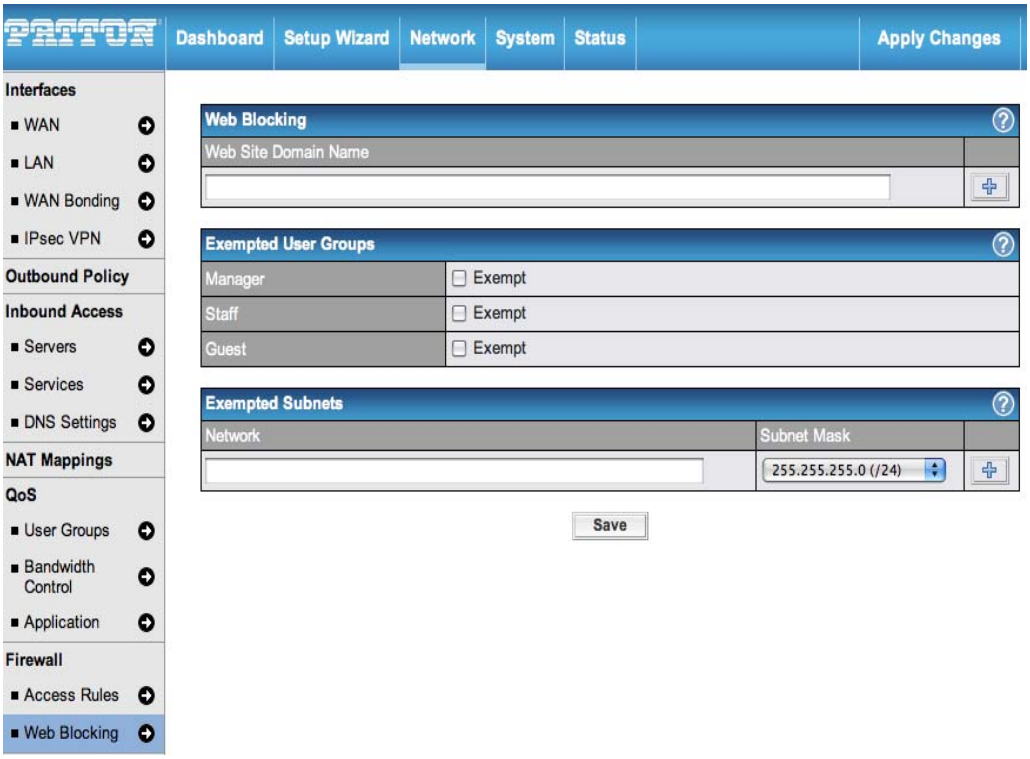


Figure 86. Network > Firewall > Web Blocking

- **Exempted User Group:** Check and select pre-defined user group(s) who can exempt from the access blocking rules. User groups can be defined at **QoS > User Group** section. Refer to "Managing User Groups" (see page 96) for more information.
- **Exempted Subnets:** With the subnet defined in the field, clients on the particular subnet(s) can exempt from the access blocking rules.

Chapter 9 Configuring Miscellaneous Services

Chapter contents

Introduction

To configure High Availability, the PPTP Server, Service Forwarding and Service Passthrough, click on **Network > Miscellaneous Settings** in the Web Admin Interface.

Setting Up High Availability Configurations

The BD1000 supports High Availability (HA) configurations via an open standard Virtual Router Redundancy Protocol (VRRP, RFC 3768).

In an HA configuration, two BODi rS units provide redundancy and failover in a master-slave arrangement. From a high level, in the event that the Master Unit is down, the Slave Unit becomes active.

High Availability will be disabled automatically where there is a Drop-in connection configured on a LAN Bypass port. The following diagram illustrates an HA configuration with two BD1000 units and two Internet connections:

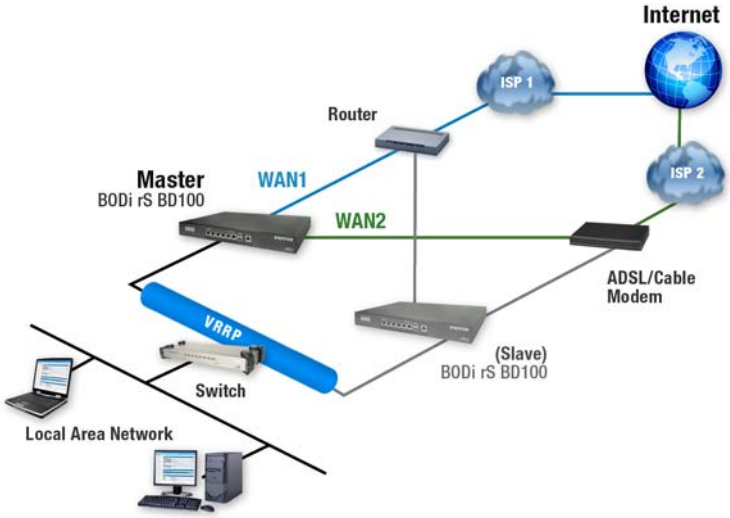


Figure 87. High Availability Application

In the diagram, the WAN ports on each BD1000 unit connect to the router and modem; and the BD1000 unit connects to the same LAN switch via a LAN port. The points below explain the technical details of the implementation, by the BD1000, of Virtual Router Redundancy Protocol (VRRP):

- In an HA configuration, the two BD1000 units communicate with each other using VRRP over the LAN.
- The two BD1000 units broadcast heartbeat signals to the LAN at a frequency of one heartbeat signal per second.
- In the event that no heartbeat signal from the Master BD1000 unit is received in 3 seconds (or longer) since the last heartbeat signal, the Slave BD1000 unit becomes active.
- The Slave BD1000 unit initiates the WAN connections, and binds to a previously configured LAN IP address.
- At a subsequent point when the Master BD1000 unit recovers, it will once again become active.

To configure High Availability settings, click **Network > Misc. Settings > High Availability**.

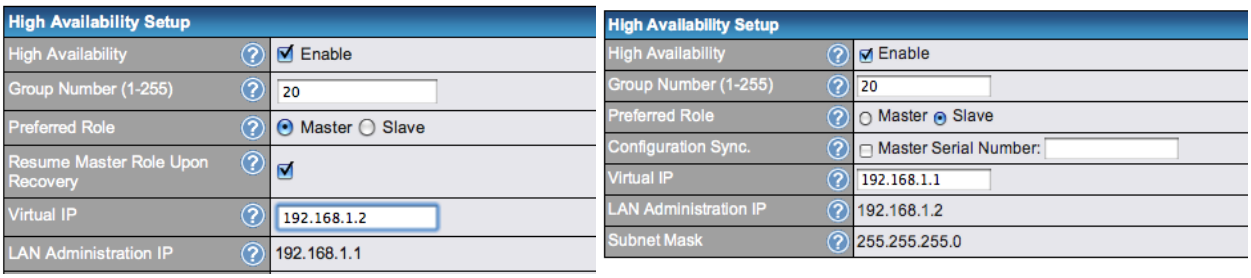


Figure 88. Network > Miscellaneous Settings > High Availability

Table 35. Misc. Settings: HA Configurations

Field	Description
High Availability (HA)	Check this box to specify that the BD1000 is part of an HA configuration.
Group Number	Specifies a number that identifies a pair of BD1000 units that operate in a High Availability configuration. The two BD1000 units in the pair must have the same Group Number value.
Preferred Role	Specifies whether the BD1000 unit operates in Master or Slave mode. Click the corresponding radial button to set the role of the unit. One of the units in the pair must be configured as the Master and the other unit must be configured as the Slave.
Resume Master Role Upon Recovery	Displays when **Master** mode is selected as the Preferred Role. When enabled, once the device has recovered from an outage, it will take over and resume its **Master** role from the slave unit.
Configuration Sync	Displays when **Slave** mode is selected as the Preferred Role. When **enabled** and the **Master Serial Number** matches with the actual master unit, the master unit will automatically transfer the configuration to this unit. **Note** Confirm that the the LAN IP Address and Subnet Mask fields are set correctly in the LAN Settings page. Refer to the **Event Log** for the configuration synchronization status.
Master Serial Number	Enter the required serial number of the Master unit to use when the **Configuration Sync.** option is enabled.
Virtual IP	Specifies the LAN IP address where the active BD1000 listens. The value of Virtual IP represents a LAN IP address that is shared among the Master and Slave units; however, at any time, only one of the two units will listen on the IP address. If the WAN is configured in NAT mode, the Default Gateway of the clients on the LAN should be set to the virtual IP. These configurations are not required when the WAN is configured in Drop-in mode.
LAN Administration IP	Specifies a LAN IP address to use for accessing administration functionality. This address should be unique within the LAN.
Subnet Mask	Specifies the subnet mask of the LAN.

Note For the BD1000 in NAT mode, the VIP should be set as the default gateway for all hosts sitting on the LAN segment. For example, a firewall sitting behind the BD1000 should set its default gateway as the VIP instead of the IP of the Master BD1000.

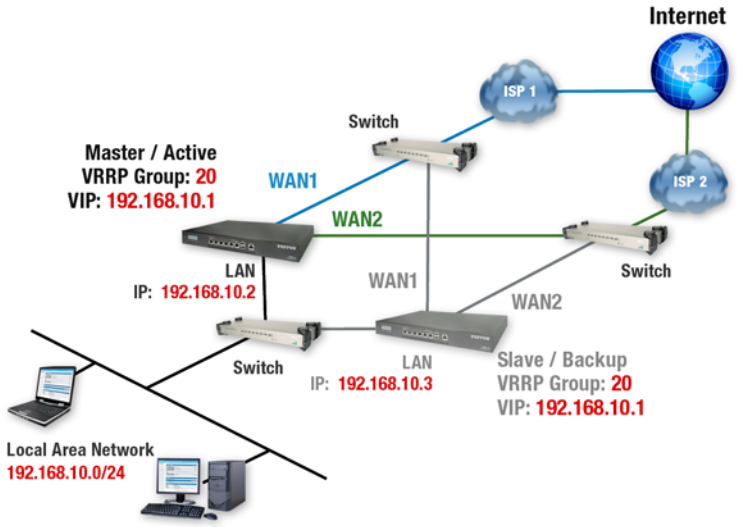


Figure 89. High Availability Application: VIP Default Gateway

In Drop-in mode, no other configuration needs to be set.

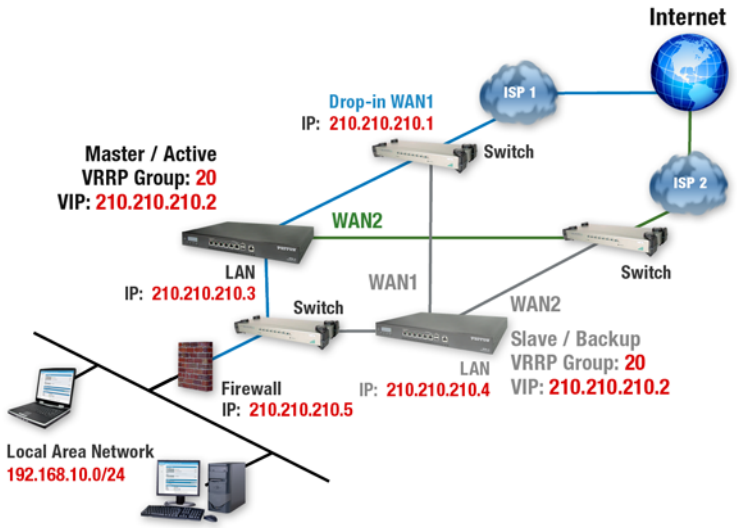


Figure 90. High Availability Application: Drop-In Mode

Note Drop-in WAN cannot be configured in LAN Bypass port when it is configuring High Availability.

Enabling the PPTP Server

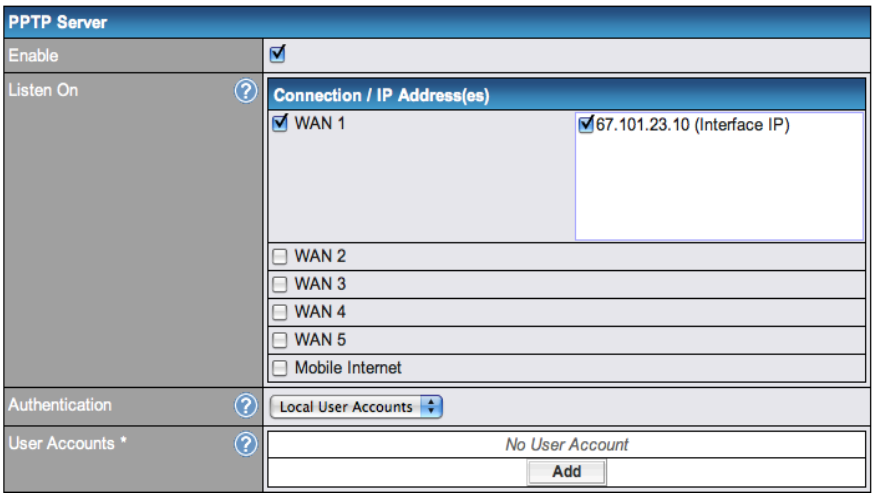


Figure 91. PPTP Server Application

The BD1000 has a built-in PPTP Server that enables remote computers to conveniently and securely access the local network. To configure the PPTP server settings, click **Network > Misc. Settings > PPTP Server**. Check the **Enable** box to turn on the PPTP server function. To view all connected PPTP sessions, click on **Status > Client List** (see "Viewing the Client List" on page 135).

Table 36. Misc Settings: PPTP Server

Field	Description
Listen On	Specifies the WAN connection(s) and IP address(es) where the PPTP server should listen.
Authentication	Specifies the source of user database for PPTP authentication. Available options include: • **Local User Accounts**: User accounts are stored in the BD1000. You can add/modify/delete the accounts in the User Accounts table. • **LDAP Server**: Authenticate with an external LDAP server. Tested with OpenLDAP server where passwords are NTLM hashed. Active Directory is not supported. (You can opt to use RADIUS to authenticate with a Windows Server.) • **RADIUS Server:** Authenticate with an external RADIUS server. Tested with Microsoft Windows Internet Authentication Service and FreeRADIUS servers where passwords are NTLM hashed or in plain text.
User Accounts	Defines the PPTP User Accounts. Click **Add** to enter a username and password to create an account. After adding the user accounts, you can click on a username to edit the account password. Click ✖ to delete a corresponding account.

Note The PPTP server will be disabled automatically if the BD1000 is deployed in Drop-in mode.

Enabling Service Forwarding

To configure Service Forwarding settings, click on **Network > Misc. Settings > Service Forwarding** in the Web Admin Interface. The following section displays:

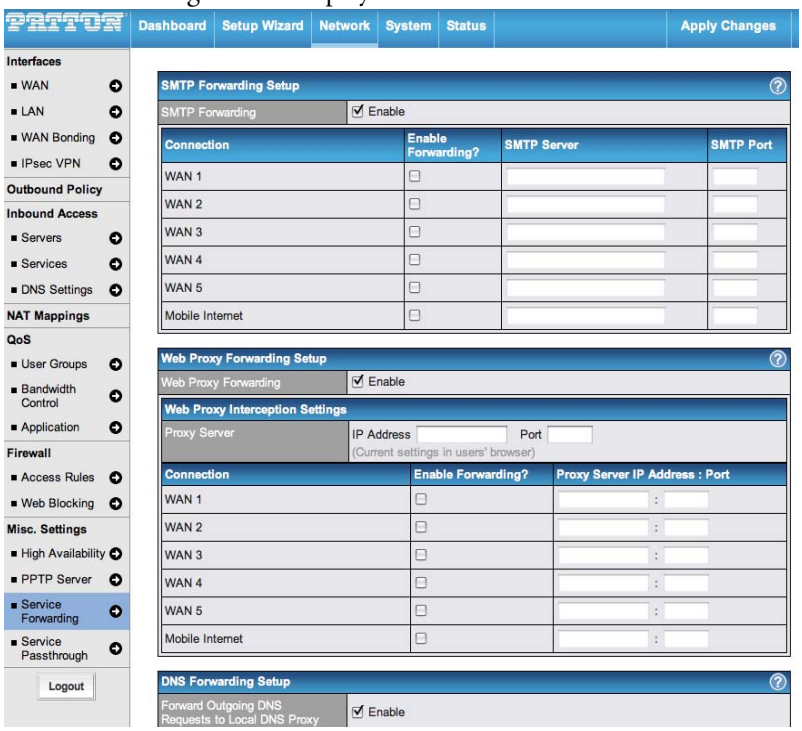


Figure 92. Network > Miscellaneous Settings > Service Forwarding

Table 37. Misc. Settings: Service Forwarding

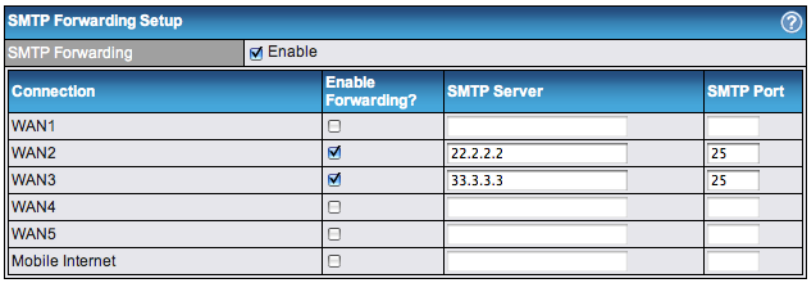
Field	Description
SMTP Forwarding	Click **Enable** to intercept all outgoing SMTP connections destined for any host at **TCP Port 25**. These connections will be redirected to a specified SMTP server and port number. SMTP server settings for each WAN can be specified after selecting **Enable**. For more information, see "SMTP Forwarding" on page 114.
Web Proxy Forwarding	Click **Enable** to intercept all outgoing connections destined for the proxy server specified in **Web Proxy Interception Settings**. These connections will be redirected to a specified web proxy server and port number. Web Proxy Interception Settings and proxy server settings for each WAN can be specified after selecting **Enable**. For more information, see "Web Proxy Forwarding Settings" on page 115.

Table 37. Misc. Settings: Service Forwarding

Field	Description
DNS Forwarding	Click **Enable** to intercept all outgoing DNS lookups to the built-in DNS name server. If any LAN device is using DNS name servers of a WAN connection, you may want to enable this option to enhance the DNS availability without modifying the DNS server setting of the clients. The built-in DNS name server will distribute DNS lookups to corresponding DNS servers of all available WAN connections. In this case, DNS service will not be interrupted even if any WAN connection is down. For more information, see "DNS Forwarding Settings" on page 115.

SMTP Forwarding

Some ISPs require their users to send e-mails via the ISP's SMTP server. All outgoing SMTP connections are blocked except for those connecting to the ISPs. The BD1000 supports intercepting and redirecting all outgoing SMTP connections (destined for TCP port 25) via a WAN connection to the WAN's corresponding SMTP server:



SMTP Forwarding Setup

SMTP Forwarding ☑ Enable

Connection	Enable Forwarding?	SMTP Server	SMTP Port
WAN1	☐		
WAN2	☑	22.2.2.2	25
WAN3	☑	33.3.3.3	25
WAN4	☐		
WAN5	☐		
Mobile Internet	☐		

Figure 93. Miscellaneous Settings > Service Forwarding > SMTP Forwarding

To turn on SMTP forwarding, select the **Enable** check box under **SMTP Forwarding Setup**, then select the boxes for the WAN connections in the **Enable Forwarding** column that require forwarding. Enter the ISP's e-mail server address and TCP port number for each WAN service.

The BD1000 will intercept SMTP connections, select a WAN with reference to the Outbound Policy and then forward the connection to the forwarded SMTP server if the chosen WAN has enabled forwarding. If the forwarding is disabled for a WAN connection, the BD1000 will forward the SMTP connections to the connection's original destination.

Note To route all SMTP connections only to specific WAN connection(s), create a rule in **Outbound Policy** (see "Creating Custom Rules for the Outbound Policy" on page 61).

Web Proxy Forwarding Settings

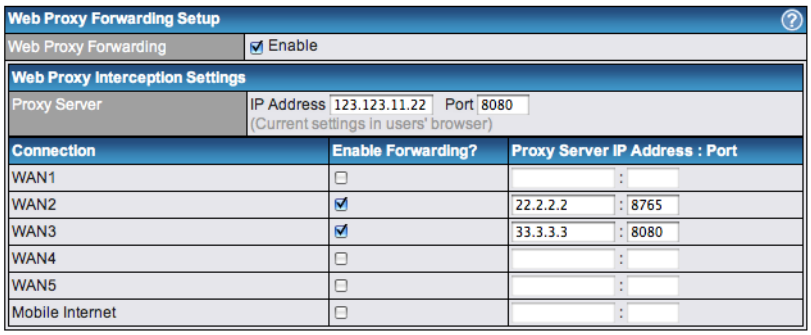


Figure 94. Miscellaneous Settings > Service Forwarding > Web Proxy Forwarding

To turn on Web Proxy Forwarding, select the **Enable** check box under **Web Proxy Forwarding Setup**. When enabled, the BD1000 will: 1) intercept all outgoing connections destined for the proxy server specified in the **Web Proxy Interception Settings**, 2) choose a WAN connection with reference to the Outbound Policy and 3) forward them to the specified web proxy server and port number.

You may configure the redirected server settings for each WAN in the **Web Proxy Interception Settings** section. If forwarding is disabled for a WAN, the BD1000 will forward the web proxy connections for the WAN to the connection's original destination.

DNS Forwarding Settings

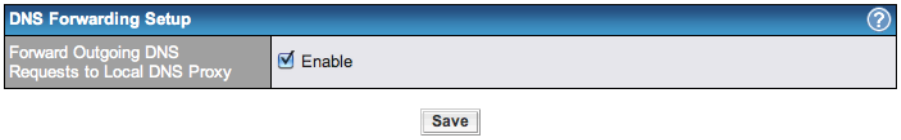


Figure 95. Miscellaneous Settings > Service Forwarding > DNS Forwarding

To turn on DNS Forwarding, select the **Enable** check box under **DNS Forwarding Setup**. When enabled, the BD1000 will intercept all clients' outgoing DNS requests and forward them to the built-in DNS proxy server.

Enabling Service Passthrough

To configure Service Passthrough settings, click on **Network > Misc. Settings > Service Passthrough** in the Web Admin Interface. The following section displays:

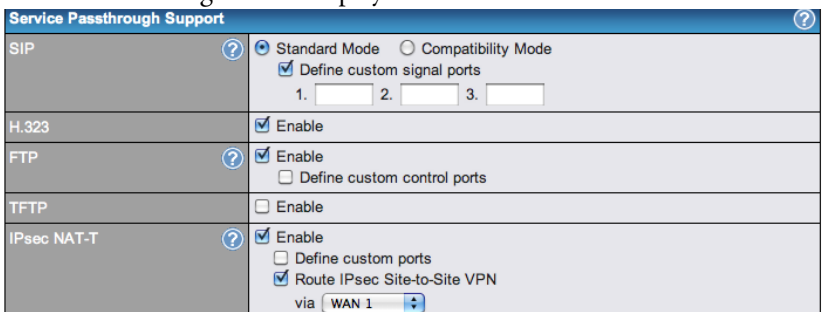


Figure 96. Network > Miscellaneous Settings > Service Passthrough

Some Internet services require special handling in a multi-WAN environment. The BD1000 supports handling these services so that that Internet applications do not notice it is behind a multi-WAN router.

Table 38. Misc. Settings: Service Passthrough Support

Field	Description
SIP	With Voice-over-IP (VoIP) Session Initiation Protocol (**SIP**), the BD1000 acts as a SIP Application Layer Gateway (ALG) that binds connections for the same SIP session to the same WAN connection, and translates the IP address in the SIP packets correctly in NAT mode. This type of passthrough support is always enabled. Available options include **Standard Mode** and **Compatibility Mode**. If your SIP server's signal port number is non-standard, check the box **Define custom signal ports** and enter the port numbers into the text boxes.
H.323	With **H.323** enabled, the BD1000 defines protocols that provide audio-visual communication sessions on any packet network to passthrough the BD1000.
FTP	**FTP** sessions consist of two TCP connections—one for control and one for data. In multi-WAN situations, FTP sessions must be binded to the same WAN connection. Otherwise, problems will arise when transferring files. By default, the BD1000 monitors TCP control connections on port 21 for any FTP connections and binds TCP connections of the same FTP session to the same WAN. If you have an FTP server listening on a port number other than 21, check the box **Define custom control ports** and enter the port numbers into the text boxes.
TFTP	The BD1000 monitors outgoing **TFTP** connections and routes any incoming TFTP data packets back to the client. Select **Enable** if you want to turn on **TFTP Passthrough** support.
IPSec NAT-T	With **IPsec NAT-T Passthrough** enabled, the BD1000 monitors UDP ports 500, 4500 and 10000 by default. Select the box **Define custom ports** to add more custom data ports for your IPsec system. If the VPN contains IPsec Site-to-Site VPN traffic, you must check the box **Route IPsec Site-to-Site VPN** and select the **WAN connection** to route traffic. If you have **IPsec Site-to-Site VPN** traffic routed, check the **Route IPsec Site-to-Site VPN** option and select a **WAN** to force routing traffic to the specified WAN.

Chapter 10 Managing System Settings

Chapter contents

Introduction

This chapter describes setting up and managing general system administration utilities, including security, upgrades, time, notifications, logs, SNMP and connection tests.

Configuring Administration Security Settings

This section describes the following settings for managing account and connection access via the BD1000 Web Admin Interface: user account settings (see "Admin Settings" on page 118) and connection access settings (see "WAN Connection Access Settings" on page 121).

Admin Settings

The BD1000 provides two user accounts for accessing the Web Admin—**admin** and **user**. The **admin** account has full administration access, while **user** is a read-only account. The **user** account can only access the device's status information and cannot make any changes to the configuration.

Web login sessions will log out automatically after being idle for longer than the specified **Web Session Timeout**. The default timeout is 4 hours. Before the session expires, click the **Logout** button in the Web Admin Interface to close the session.

For security reasons, you should change the administrator password after logging into the **admin** account for the first time. You may also configure access to the **admin** account from the LAN only to improve system security.

To configure user accounts and sessions, click on **System > Admin Security** in the Web Admin Interface (Figure 97 on page 119).

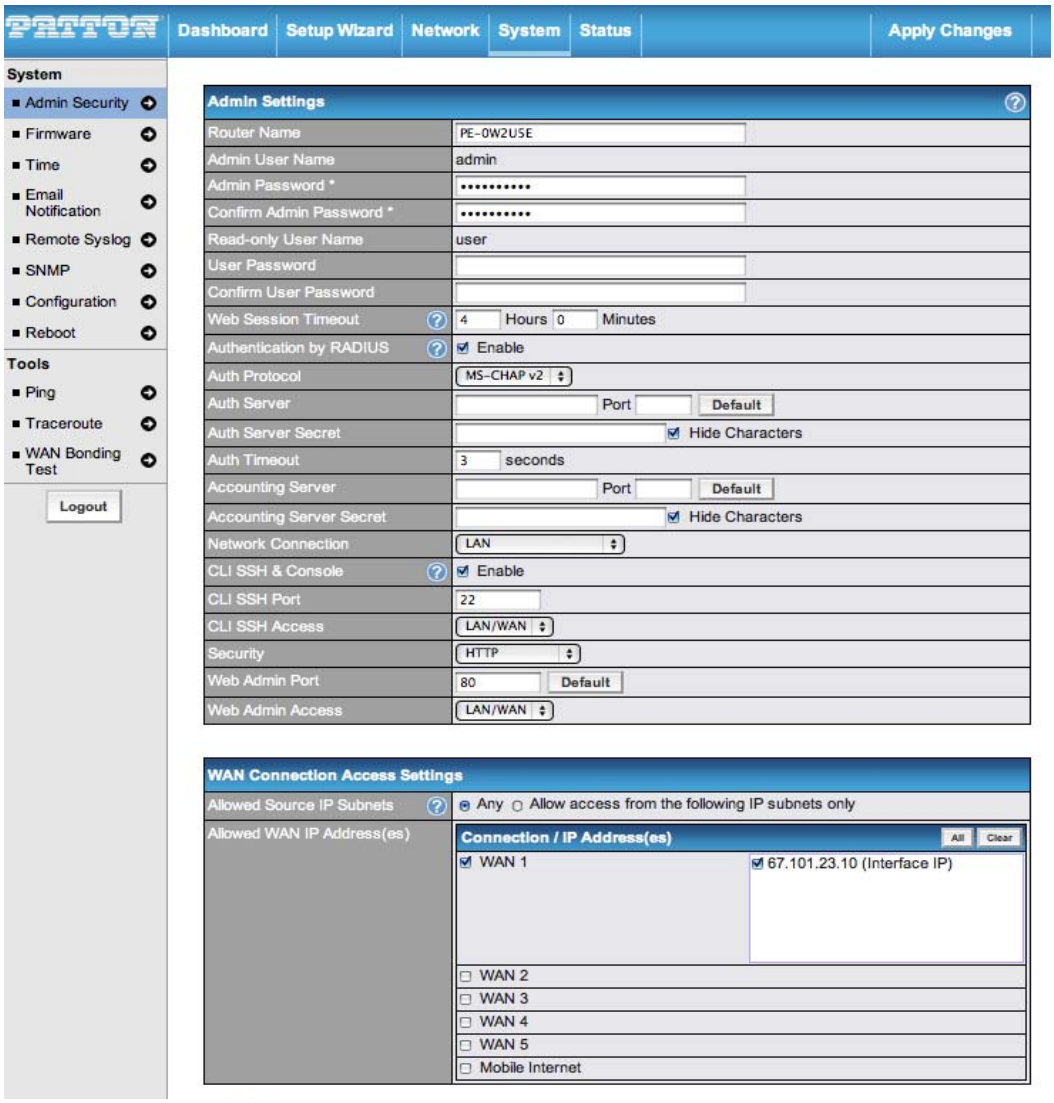


Figure 97. System > Admin Security

Table 39. System: Admin Security Settings

Field	Description
Router Name	Defines a name for this specific BD1000 unit.
Admin User Name	*Non-configurable; set as **admin** by default.
Admin Password	Specifies a new password for the **admin** account.
Confirm Admin Password	Verifies and confirms the new password for the **admin** account.
Read-only User Name	*Non-configurable; set as **user** by default.
User Password	Specifies a new password for the **user** account. When confirmed, the user account will be available for read-only use.
Confirm User Password	Verifies and confirms the password for the **user** account.

Table 39. System: Admin Security Settings

Field	Description
Web Session Timeout	Specifies the number of hours and minutes that a web session can remain idle before the BD1000 terminates the session. Default = 4 hours
Authentication by RADIUS	Select the **Authentication by RADIUS** option to authenticate access using an external RADIUS server. The BD1000 treats authenticated users as **admin** users with full read-write permissions. Local "admin" and "user" accounts will be disabled. When the device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access. *Authentication options will be available once this box is checked.
Auth Protocol	Specifies the authentication protocol used. Available options include: **MS-CHAP v2** and **PAP**.
Auth Server	Specifies the access address of the external RADIUS server.
Auth Server Secret	Defines the secure password phrase for accessing the RADIUS server.
Auth Timeout	Specifies the time value for authentication timeout.
Accounting Server	Specifies the access address of the external Accounting server.
Accounting Server Secret	Defines the secure password phrase for accessing the Accounting server.
Network Connection	Specifies the network connection that the BD1000 will use for the authentication connection. Select an option from LAN, WAN and VPN connections.
Security	Specifies the authorized protocol(s) for accessing the Web Admin Interface: • **HTTP** • **HTTPS** • **HTTP/HTTPS**
Web Admin Port	Specifies the port number to use to access the Web Admin Interface.
Web Admin Access	Specifies the authorized network interfaces for accessing the Web Admin Interface: • **LAN only** • **LAN/WAN** (see "WAN Connection Access Settings" on page 121)

WAN Connection Access Settings

To configure **WAN Connection Access** settings, select **LAN/WAN** as the **Web Admin Access** option in the **Admin Settings** section.

Table 40. System: WAN Connection Access Settings

Field	Description
Allowed Source IP Subnets	Specifies authorized IP subnets that may access the Web Admin Interface. Available options include: • **Any:** Allow web admin access from any location, without IP address restrictions. • **Allow access from the following IP subnets only:** Only the defined IP subnets may access the Web Admin Interface. When selected, this option displays a text field that allows you to enter the authorized IP subnet addresses. Each IP subnet must be in form of **w.x.y.z/m**, where: – *w.x.y.z* is an IP address (e.g. 192.168.0.0) – */m* is the subnet mask in CIDR format, which is between 0 and 32 inclusively. (e.g.168.0.0/24) To define multiple subnets, enter only one IP subnet on each line. For example: *168.0.0/24* *10.8.0.0/16*
Allowed WAN IP Addresses	Specifies the WAN IP address(es) where the web server should listen for activity.

Upgrading the Firmware

This section describes how to upgrade the firmware for the BD1000 through the Web Admin Interface. To reach the Firmware page, click on **System > Firmware**:

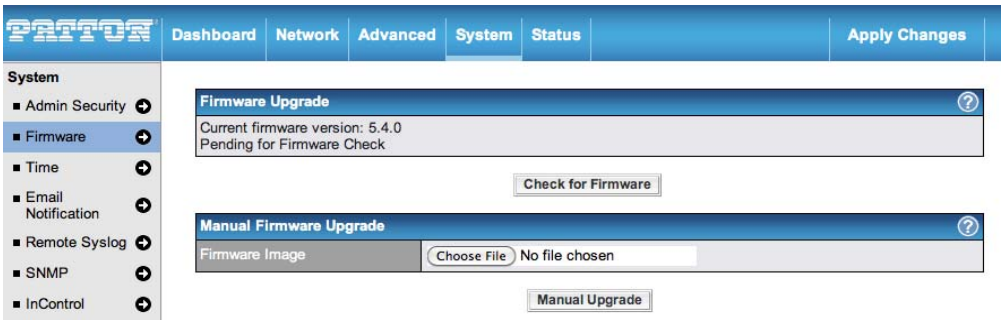


Figure 98. System > Firmware

There are two ways to upgrade the unit—online or manually. To upgrade the firmware online, the system can Check, Download and Upgrade over the Internet. To manually upgrade the firmware, you may browse and select a firmware file to upload.

To use the **online** upgrade option, click on the **Check Again** button in the **Firmware Upgrade** section of the screen. With this option, the BD1000 checks online for new firmware. If a new firmware update is available, the BD1000 will automatically download the new firmware file. The BD1000 will automatically initiate the upgrade process after downloading the new firmware file.

To use the **manual** upgrade option, go to **www.patton.com/support/upgrades** and select the BODi BD1000 from the **Model Number** drop-down menu. Then, click the **Download** hyperlink for the desired software release. In the BD1000 Web Admin Interface, click **Browse...** to select the firmware file from the local computer, and then click **Manual Upgrade** to send the firmware to the unit. The BD1000 will automatically initiate the upgrade process after downloading the new firmware file.

The BD1000 has the ability to store two different firmware versions in two different partitions. A firmware upgrade will always replace the inactive partition. If you want to keep the inactive firmware, you can simply reboot your device with the inactive firmware, and then perform the firmware upgrade.

Firmware Upgrade Status

During the firmware upgrade, the **Status** LED on the front of the unit shows the upgrade process:

- **OFF**: Firmware upgrade in progress (DO NOT disconnect the power)
- **Red:** The BD1000 is rebooting
- **Green:** The firmware upgrade is successfully completed.

Note

- The firmware upgrade process may not necessarily preserve the previous configuration, and the behavior varies on a case-by-case basis.
- Do not disconnect the power during the firmware upgrade process.
- Do not attempt to upload a non-firmware file or a firmware file that is not supported by the BD1000. Upgrading a BD1000 with an invalid firmware file will damage the unit, and may void the warranty.

Configuring the Time Server

The Time Server functionality enables the system clock of the BD1000 to synchronize with a specified Time Server. To configure the time server settings, click on **System > Time** in the Web Admin Interface.

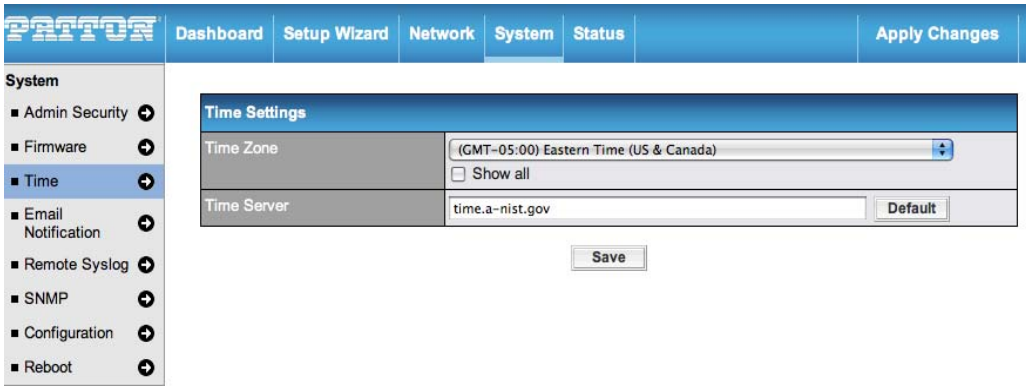


Figure 99. System > Time

Table 41. System: Time Server Settings

Field	Description
Time Zone	Specifies the time zone (along with the corresponding Daylight Savings Time scheme) for the BD1000. The Time Zone value affects the time stamps in the Event Log of BD1000 and E-mail notifications. Select the box for **Show all** to view all available time zone options.
Time Server	Specifies the NTP network time server to be utilized by the BD1000.

Configuring Email Notifications

The Email Notification functionality of the BD1000 sends the System Administrator up-to-date information on the network status. To configure notification settings, click on **System > Email Notification** in the Web Admin Interface.

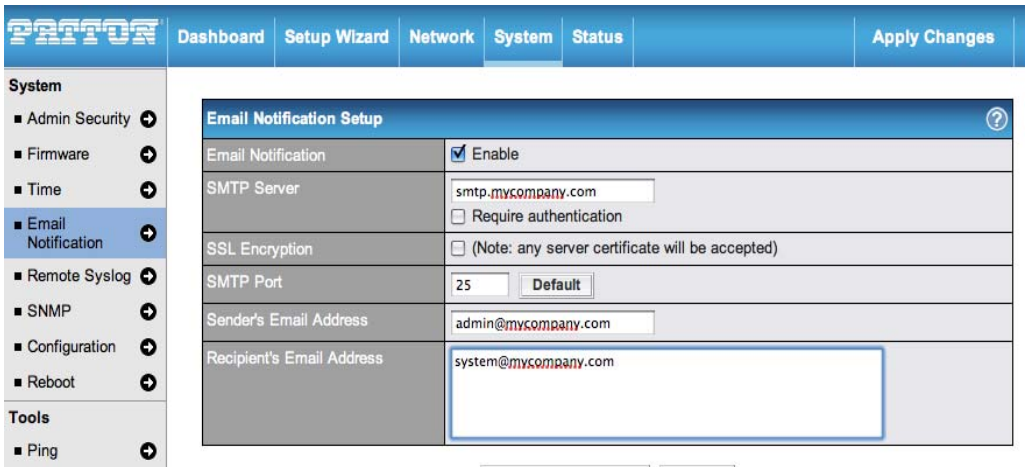


Figure 100. System > Email Notification

Table 42. System: Email Notification Settings

Field	Description
Email Notification	Select **Enable** to allow the BD1000 to send email messages to a System Administrator when the WAN status changes, or when new firmware is available. If the Enable box is not checked, the BD1000 will not send email messages about the system.
SMTP Server	Specifies the SMTP server used for sending email. If the server requires authentication, select **Require authentication**.
SSL Encryption	Select the box to **Enable SMTPS**. When enabled, the **SMTP Port** field will change to **465** automatically.
SMTP Port	Specifies the SMTP Port number; by default, this is set to **25**. Select the **SSL Encryption** box to automaticaly change the port to **465**. You may also enter a new port number, or you may click **Default** to restore the default port setting.
SMTP Username/ Password	Specifies the **SMTP username** and **password** while sending email. Select **Require authentication** in the **SMTP Server** field to view these options.
Confirm SMTP Password	Verifies and confirms the new administrator password.
Sender's Email Address	Specifies the sender email address shown on the email notifciations sent by the BD1000.
Recipient's Email Address	Specifies the email addresses where the BD1000 may send notifications to the administrator(s). You may enter multiple recipients' email addresses in this field.

After you have completed the settings, click the **Test Email Notification** button to test the settings before saving. The following screen displays to confirm the settings:

Test Email Notification	
SMTP Server	smtp.mycompany.com
SMTP Port	25
SMTP User Name	smtpuser
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

Send Test Notification | Cancel

Figure 101. Test Email Notification

Click **Yes** to confirm. Wait a few seconds, and a window displays with detailed test results:

Test Result

```
[INFO] Try email through connection #3
[<-] 220 ESMTP
[->] EHLO balance
[<-] 250-smtp Hello balance [210.210.210.210]
250-SIZE 100000000
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
```

Figure 102. Test Email Result

Setting Up the Remote System Log

The Remote Syslog functionality of the BD1000 enables event logging at a specified remote Syslog server. To configure the remote system log settings, click on **System > Remote Syslog** in the Web Admin Interface.

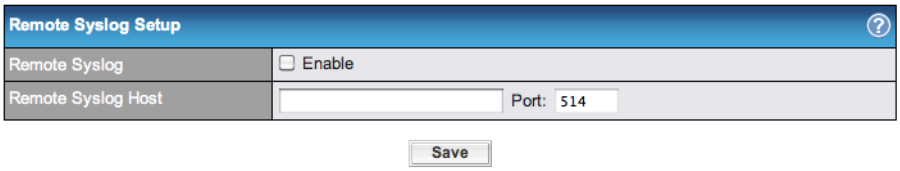


Figure 103. System > Remote Syslog

Table 43. System: Remote Syslog Setup

Field	Description
Remote Syslog	Specifies whether or not to log events at the specified remote Syslog server.
Remote Syslog Host	Specifies the IP address or host name of the remote Syslog server.
Remote Syslog Host Port	Specifies the port number of the remote Syslog service. Default = **514**

Configuring Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is an open standard that can be used to collect information from the BD1000. To configure SNMP settings, click on **System > SNMP** in the Web Admin Interface.

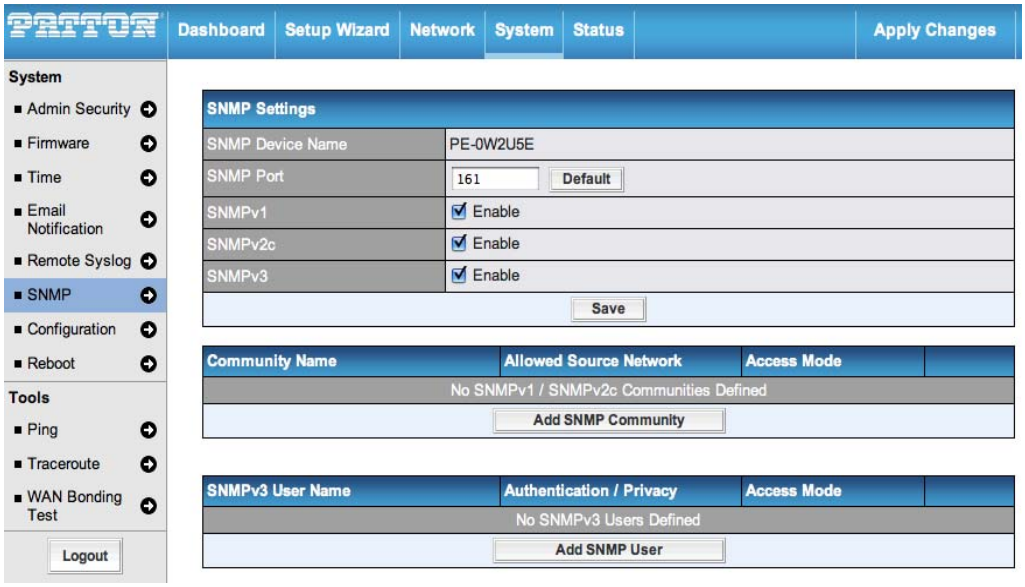


Figure 104. System > SNMP

General SNMP Settings

Table 44. System: SNMP Settings

Field	Description
SNMP Device Name	Displays the router name defined in ***System > Admin Security***.
SNMP Port	Specifies the SNMP port to use. Default = **161**.
SNMPv1	Select the box to **Enable SNMP version 1**.
SNMPv2	Select the box to **Enable SNMP version 2**.
SNMPv3	Select the box to **Enable SNMP version 3**.

SNMP Community Settings

To add a community for either SNMPv1 or SNMPv2, click the **Add SNMP Community** button in the **Community Name** table. The following screen displays:

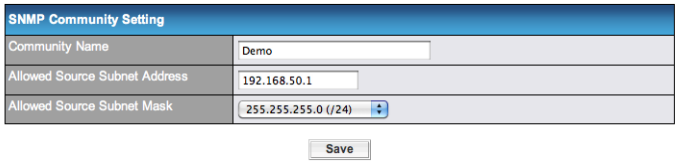


Figure 105. System > SNMP Community

Table 45. System: SNMP Community Settings

Field	Description
Community Name	Specifies a unique name for the SNMP Community.
Allowed Source Subnet Address	Enter a subnet address where the SNMP Server will allow access.
Allowed Source Subnet Mask	Specifies the subnet mask that corresponds with the Allowed Source Subnet Address *(e.g. 255.255.255.0)*.

SNMPv3 User Settings

To define a user name for SNMPv3, click **Add SNMP User** in the **SNMPv3 User Name** table. The following screen displays:

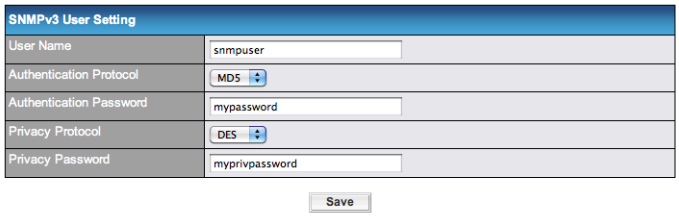


Figure 106. System > SNMPv3 User

Table 46. System: SNMP Community Settings

Field	Description
User Name	Specifies an account name to use with SNMPv3.
Authentication Protocol	Select an authentication protocol from the drop-down menu. Available options include: • **NONE** • **MD5** • **SHA**
Authentication Password	Specifies the authentication password (only applies to **MD5** or **SHA**).
Privacy Protocol	Select a privacy protocol from the drop-down menu. Available options include: • **NONE** • **DES**
Privacy Password	Specifies the privacy password (only applies to **DES**).

Managing the Reporting Server

The Reporting functionality enables the BD1000 to post traffic data and other information periodically to a Reporting Server for generating detailed historical usage reports of the device. To configure Reporting Server settings, click on **System > Reporting Server** in the Web Admin Interface.

Table 47. System: Reporting Server Settings

Field	Description
Post Data to Server	Specifies whether or not the BD1000 should periodically and automatically post traffic data to Reporting Server.
Reporting Server	Specifies the Internet IP address or host name of the Reporting Server. Default = report.bd1000.com.
Create a Login link	Click the link to register a login ID on the Reporting Server. Each login ID can associate with multiple BODi rS devices. If you already have a login ID on the server, you can skip this step.
Specify link	Click on the link to display the Reporting Server Registration window. Fill in the "User Account" field to specify the login ID on the Reporting Server to allow access to the report of this BD1000 device.
View Reports link	Click the link to view link usage reports from the Reporting Server (login required).

Note The registration process will establish contact to the Reporting Server to associate the BD1000 unit with the specified user account on the server.

Prior to registration, please ensure that the user account to be entered is valid.

Importing and Exporting System Configuration Files

Backing up the BD1000 settings immediately after successful completion of the initial setup is strongly recommended. To configure the settings for uploading and downloading system files, click on **System > Configuration** in the Web Admin Interface.

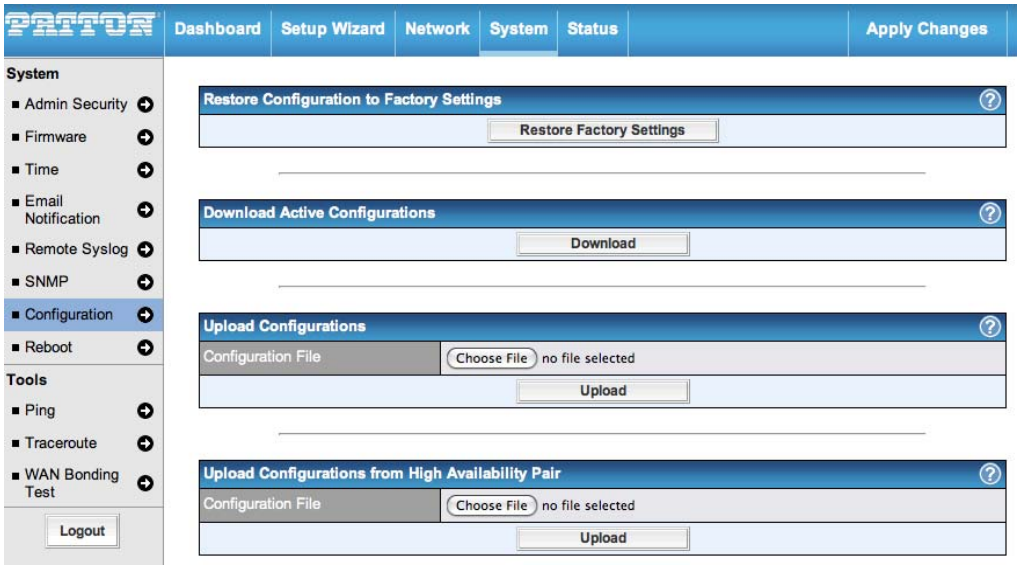


Figure 107. System > Configuration

Restore Configuration to Factory Settings

Use the **Restore Factory Settings** button to reset the BD1000 to the factory default settings. You must click the **Apply Changes** button for the new settings to take effect.

Downloading Active Configurations

Use the **Download** button to back up the current active settings and save the configuration file.

Uploading Configurations

To restore or change settings based on a configuration file, click **Browse…** to locate the configuration file on the local computer, and then click **Upload**. You must click the **Apply Changes** button for the new settings to take effect.

Uploading Configurations from High Availability Pair

In a High Availability (HA) configuration, click the **Upload** button to quickly load the configuration of the BD1000's HA counterpart onto this BD1000 unit. After loading the settings, configure the LAN IP address of the BD1000 unit to be different from the HA counterpart.

Rebooting the System

For the highest reliability, the BD1000 provides two copies of the firmware in different versions. The firmware marked **(Running)** is the current system firmware file used for booting up.

Note A firmware upgrade always replaces the inactive firmware partition.

To restart the BD1000, click on **System > Reboot System** in the Web Admin Interface. Select a firmware file, then click the **Reboot** button.

Figure 108. System > Reboot

Testing System Connections

You may test the health of connections from the BD1000 using built-in system utilities. To access the setup screens for these tests, click on **System > Tools** in the Web Admin Interface.

- Use the **Ping Test** (see "Ping Test" on page 131) to view the connectivity of a WAN or VPN link.
- Use the **Traceroute Test** (see "Traceroute Test" on page 132) to view the connection path of a WAN or VPN link.
- Use the **VPN Test** (see "VPN Test" on page 132) to view the throughput between different VPN peers.

Ping Test

The BD1000 provides a **Ping Test** tool that checks the connection of a specified Ethernet interface or a Site-to-Site VPN link. A System Administrator can use the Ping utility to manually check the connectivity of a particular LAN/WAN connection. You can specify the number of pings in the **Number of Times** field (to a maximum of 10 times), and you may specify the **Packet Size** (to a maximum of **1472** bytes).

To run a ping test on a BD1000 connection, click on **System > Tools > Ping** in the Web Admin Interface. Select an option from the **Connection** drop-down menu. If desired, adjust the packet size and number of times for the connection test to run, then click the **Start** button. Click **Stop** to end the ping test.

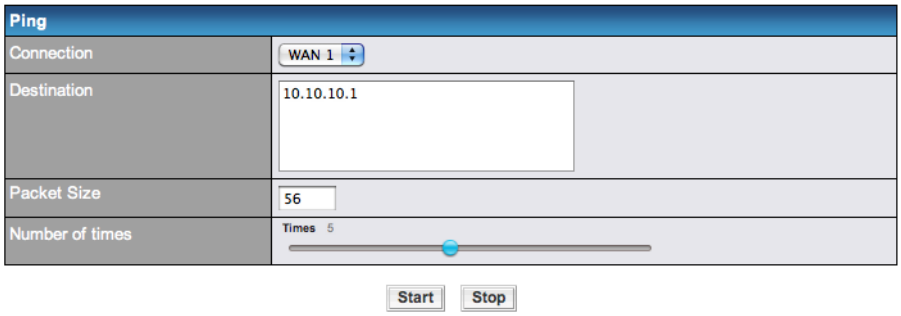


Figure 109. System > Tools > Ping Test

Traceroute Test

The BD1000 provides a **Traceroute Test** tool that follows and reports the routing path to the destination through a particular Ethernet interface or a Site-to-Site VPN connection. A System Administrator can use the Traceroute utility to analyze the connection path of a LAN/WAN connection.

To run a traceroute test on a BD1000 connection, click on **System > Tools > Traceroute** in the Web Admin Interface. Select an option from the **Connection** drop-down menu, then click the **Start** button. Click **Stop** to end the traceroute test.

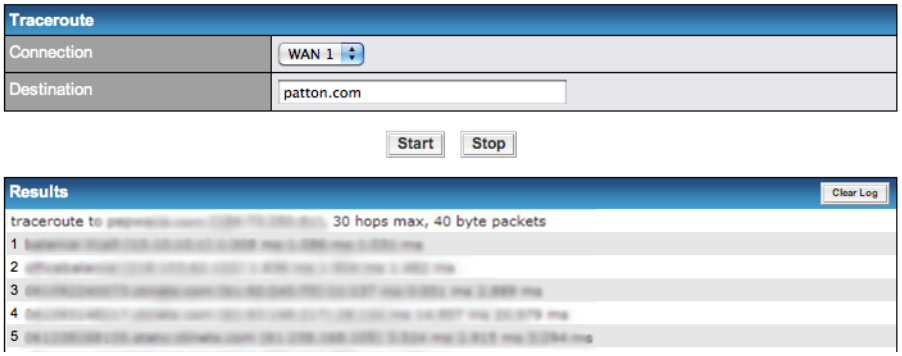


Figure 110. System > Tools > Traceroute Test

VPN Test

The BD1000 provides a **VPN Test** tool that tracks the throughout between different VPN peers. To run a VPN test on a BD1000 connection, click on **System > Tools > VPN** in the Web Admin Interface. Select an option from the **VPN Profile** drop-down menu, and select the **Test Type** and **Direction**. Enter the length of time for the test (in seconds), then click the **Go!** button.

Chapter 11 Managing Status Settings

Chapter contents

Introduction

This chapter describes viewing system information for the BD1000, including active sessions, the client list, the WINS client list, Site-to-Site VPN connections, UPnP/NAT-PMP information, events and bandwidth statistics.

Viewing General Device Information

To view system status information, click on **Status > Device** in the Web Admin Interface:

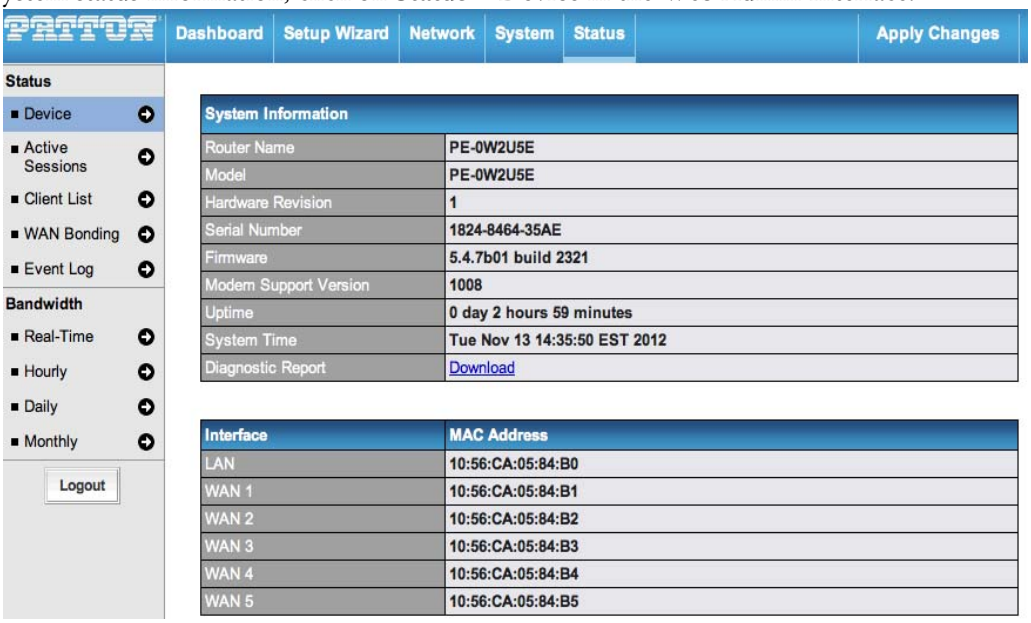


Figure 111. Status > Device

Table 48. Status: System Information

Field	Description
Router Name	Displays the name specified for this specific BD1000 device in the Router Name field located in ***System > Admin Security***.
Model	Shows the model name and number of this specific BD1000 device.
Hardware Revision	Shows the hardware version of this specific BD1000 device.
Serial Number	Shows the serial number of this specific BD1000 device.
Firmware	Shows the firmware version that the BD1000 is currently running.
Uptime	Shows the length of time since the BD1000 has rebooted.
System Time	Shows the current system time.
Diagnostic Report	Use the **Download** button to export a diagnostic report file of system statistics.

The second table on the **Device** status page shows the MAC address of each LAN/WAN interface connected to the BD1000.

Viewing Details of Active Sessions

The **Active Sessions** section displays the active inbound / outbound and UDP / TCP sessions of each WAN connection on the BD1000. To view information about current sessions that are currently active on the BD1000, click on **Status > Active Sessions** in the Web Admin Interface. A filter is available to help sort the active session information. Enter a keyword in the field or check one of the WAN connection boxes for filtering:

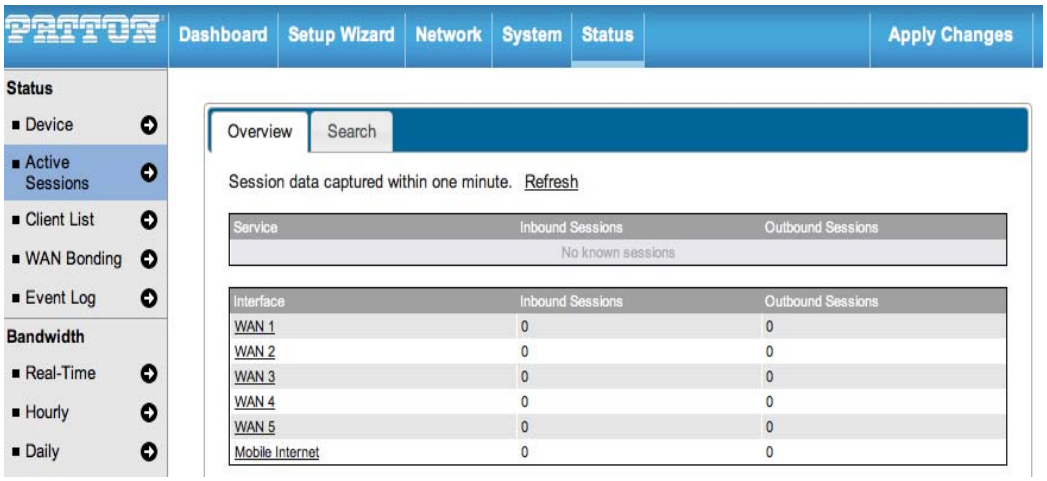


Figure 112. Status > Active Sessions

Viewing the Client List

The **Client List** section shows DHCP clients associated with the BD1000 since it has powered up. To view information about DHCP clients, click on **Status > Client List** in the Web Admin Interface.

The table lists the DHCP client **IP Addresses**, their **Names** (retrieved from DHCP reservation table or defined by users), current **Download** and **Upload** rates and **MAC addresses**. The Network Name (SSID) and Signal refers to the information about Wi-Fi AP, which is the name of the Network and its signal strength. Clients can be imported into the DHCP Reservation table by clicking the arrow button in the far right column. To update the record after importing clients, go to **Network > LAN**.

If you have enabled the PPTP Server (see "Enabling the PPTP Server" on page 111), you may see the corresponding connection name listed in the Name field of the Client List:

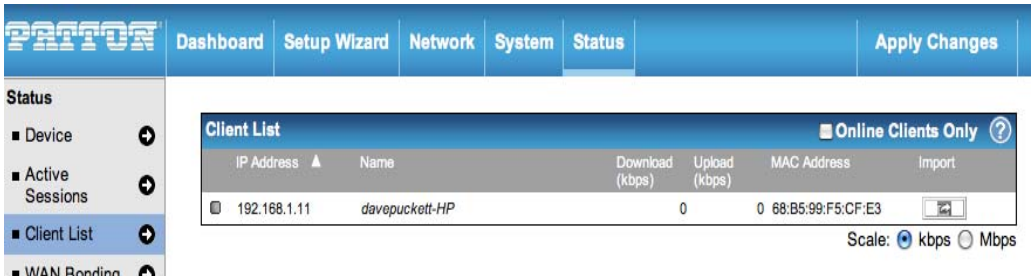


Figure 113. Status > Client List

Viewing Access Points

The **Access Point** section shows connected AP devices associated with the BD1000 since it has powered up. To view information about access points, click on **Status > Access Point** in the Web Admin Interface.

The table lists all connected or detected BODi rS access point devices and their IP address, firmware version, assigned AP profile, number of connected clients and broadcasting channel.

The broadcasting channel followed by a "*" shows that the channel is automatically chosen and selected by the BD1000.

Viewing the WINS Client List

The **WINS Client** section shows Windows Internet Name Service (WINS) clients associated with the BD1000. This section is only available if you have enabled the WINS Server (see "WINS Server Settings" on page 36). To view information about WINS clients, click on **Status > WINS Client** in the Web Admin Interface.

The table lists the names of clients retrieved and automatically matched with the DHCP Client List (see "Viewing the Client List" on page 135). Click the button **Flush All** to clear the table of all WINS client records.

Viewing Site-to-Site VPN Connection Details

The **Site-to-Site VPN** section shows the current status and details of all VPN peers. To view details about peer WAN connections, click on **Status > Site-to-Site VPN** in the Web Admin Interface.

Viewing IPsec VPN Connection Details

The **IPsec VPN** section shows the current status of IPsec VPN profiles. To view details about IPsec VPN connections, click on **Status > IPsec VPN** in the Web Admin Interface.

Viewing UPnP and NAT-PMP Connection Details

The **UPnP/NAT-PMP** section shows forwarded ports using UPnP and NAT-PMP protocols. This section is only available if you have enabled UNnP/NAT-PMP functions (see "UPnP/NAT-PMP Settings" on page 77). To view details about these connections, click on **Status > UPnP/NAT-PMP** in the Web Admin Interface.

Click the **X** button to delete a single UPnP/NAT-PMP record in its corresponding row. To delete all records, click the **Delete All** button below the table. UPnP/NAT-PMP records are deleted immediately without confirmation.

Viewing Event Log Details

The **Event Log** section displays a list of events that have taken place on the BD1000. To view log details, click on **Status > Event Log** in the Web Admin Interface.

Device Event Log

Click the **Refresh** button to update the list of log entries. Click the **Clear Log** button to remove all of the log entries. Select the number of entries to show in the log screen at a time—**50**, **100**, or **all**.

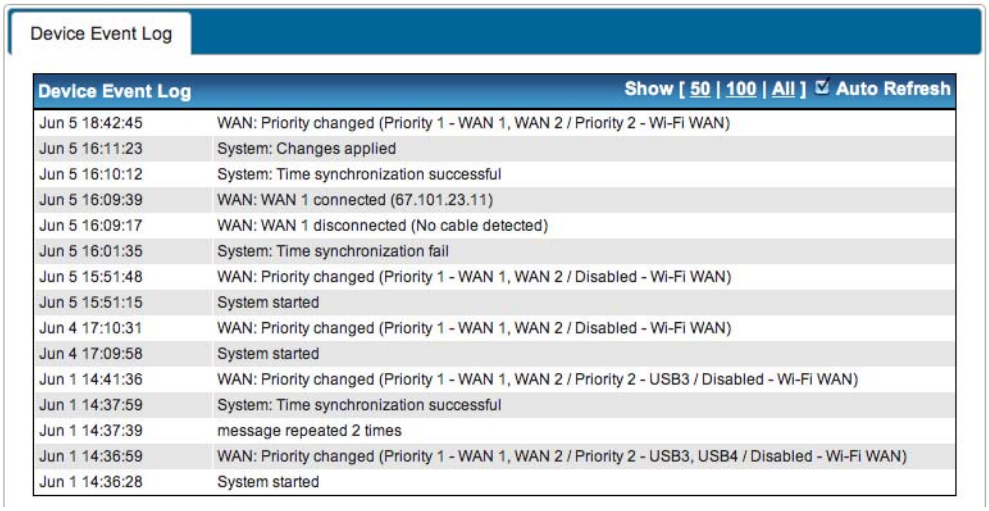


Figure 114. Status > Device Event Log

AP Event Log

This section displays a list of events that has taken place on the connected / detected BODi rS access point devices. Select the number of entries to show in the log screen at a time—**50**, **100**, or **all**.

Viewing Bandwidth Usage Statistics

The **Bandwidth** section shows bandwidth usage statistics for the BD1000, including details about real-time, daily and monthly bandwidth usage. To view bandwidth statistics, click on **Status > Bandwidth** in the Web Admin Interface.

- "Real-Time Bandwidth Usage" on page 137
- "Daily Bandwidth Usage" on page 139
- "Monthly Bandwidth Usage" on page 140

Real-Time Bandwidth Usage

The **Data Transferred since installation** table shows you how much network traffic has been processed by the BD1000 since the first bootup.

Click the **Show Details** link in the top right corner of each table to display the details of transferred data. Select the **Stacked** box below the data transferred graph to show the aggregated transferred rate of both traffic directions.

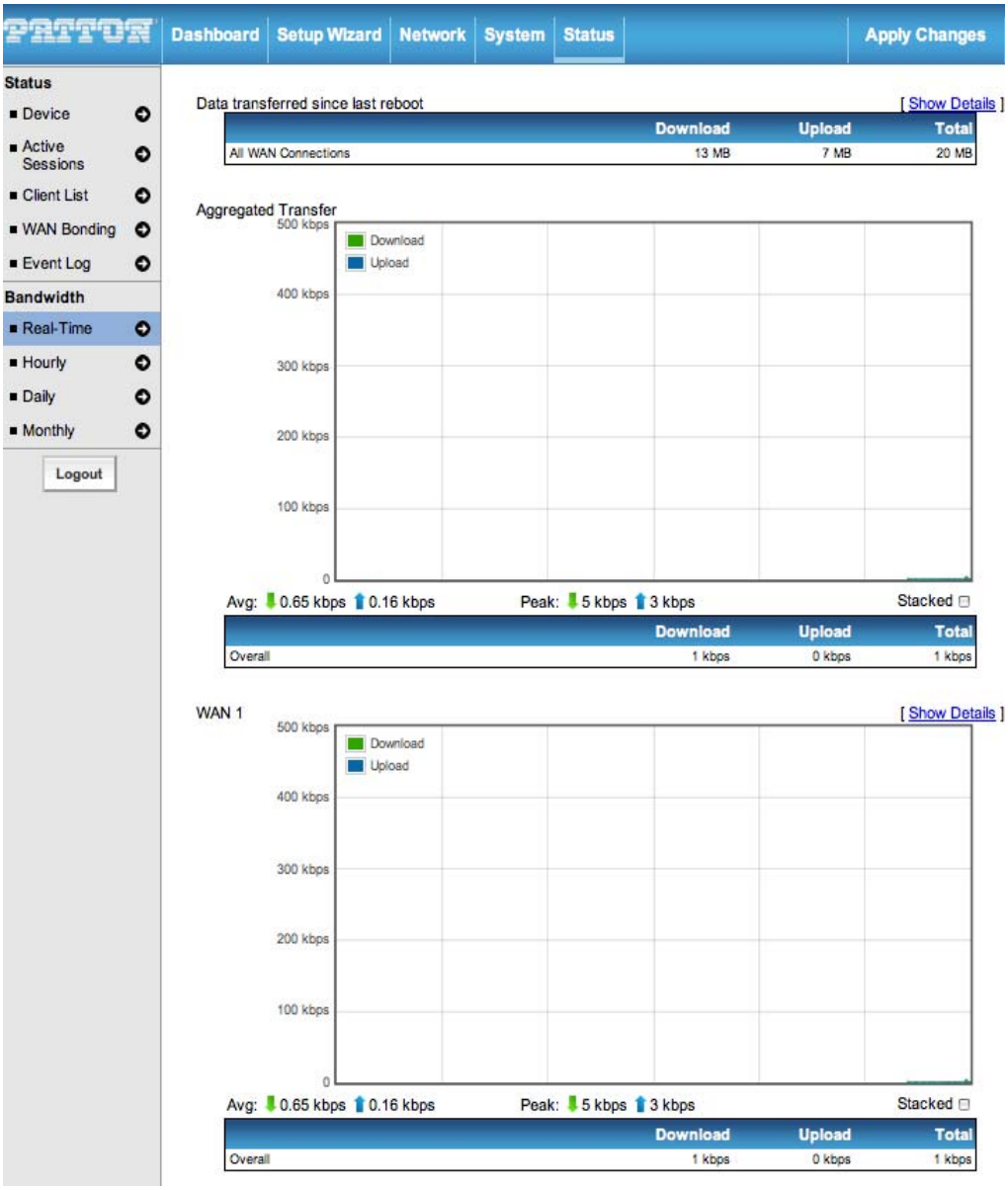


Figure 115. Real-Time Bandwidth Usage

Daily Bandwidth Usage

The **Daily Bandwidth** status page shows the daily bandwidth usage for all WAN connections and for each specific WAN connection.

From the drop-down menu, select theWAN connection to display its bandwidth information. If you have enabled the **Bandwidth Monitoring** feature (see "Bandwidth Allowance Monitor" on page 48), the BD1000 will display the **Current Billing Cycle** table for that specific WAN connection.

In the **Client Bandwidth Usage** table, click on a date hyperlink to view the client bandwidth usage for that specific date. This feature is not available if you have selected to view the bandwidth usage of one specific WAN connection.

In the **Daily Usage** table, you may select to show the scale of the graph in **Megabytes (MB)** or **Gigabytes (GB).**

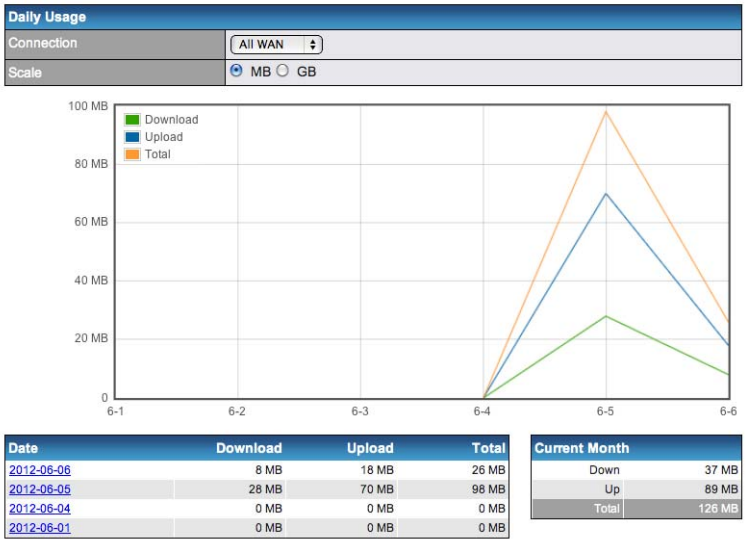


Figure 116. Daily Bandwidth Usage

Monthly Bandwidth Usage

The **Monthly Bandwidth** status page shows the bandwidth usage for each month for each specific WAN connection.

From the drop-down menu, select a specific WAN connection to display its monthly bandwidth usage information. If you have enabled the **Bandwidth Monitoring** feature (see "Bandwidth Allowance Monitor" on page 48), the BD1000 will display the **Billing Cycle** or **Calendar Month** for that specific WAN connection.

In the **Client Bandwidth Usage** table, click on the first or second row to view the client bandwidth usage for the current month. This feature is not available if you have selected to view the bandwidth usage of one specific WAN connection.

In the **Monthly Usage** table, you may select to show the scale of the graph in **Megabytes (MB)** or **Gigabytes (GB).**

Note By default, the scale of data size is in **MB**. 1GB equals 1024MB.

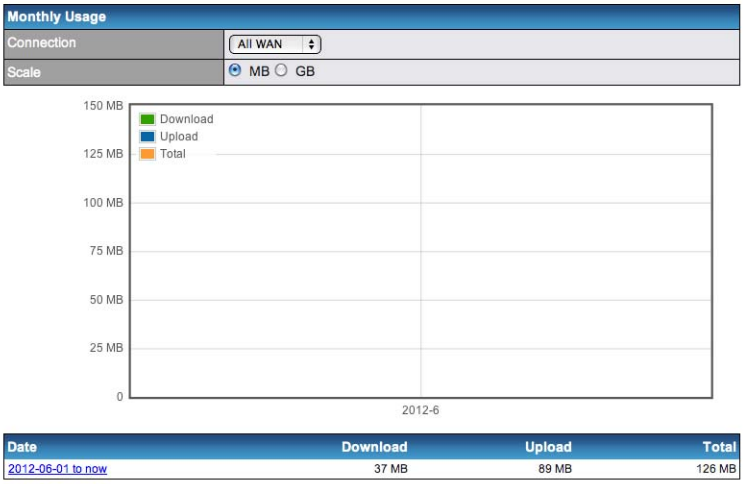


Figure 117. Monthly Bandwidth Usage

Chapter 12 **Troubleshooting**

Chapter contents

Outbound Load

- **Problem:** Outbound load is only distributed over one WAN connection.
- **Solution:** Outbound load can only be distributed evenly to the WAN connection if many outbound connections are made. If there is only one user on the LAN and only one download session is made from his/her browser, the WAN connections cannot be fully utilized.

  For a single user, download manager applications are recommended. The applications can split a file into pieces and download the pieces simultaneously. For example: DownThemAll (Firefox Extension), iGetter (MAC), etc.

  If the outbound traffic is going across the Site-to-Site VPN tunnel, i.e. transferring a file to a VPN peer, all WAN connections will be bonded by our Site-to-Site VPN technology. In this case, all bandwidth will be utilized and a file will be transferred across all available WAN connections.

Download Speed

- **Problem:** I am using a download manager program (e.g. Download Accelerator Plus, DownThemAll etc.). Why is the download speed still in single link's speed?
- **Solution:** First, check whether the WAN connections are up.

  Second, ensure your download manager application has split the file into 3 parts or more.

  It is also possible that all of 2 or even 3 download sessions were being distributed to the same link by chance.

Public IP Address

- **Problem:** I am using some websites to lookup my public IP address, e.g. www.whatismyip.com. When I keep pressing the browser's Refresh button, the server almost always returns the same address. The IP address is supposed to be changing for every refresh.
- **Solution:** The web server has enabled the **Keep Alive** function such that you were using the same TCP session to query the server.

  Try to test with a website that does not enable **Keep Alive**.

  For example, try http://private.dnsstuff.com/tools/aboutyou.ch (This third-party website is provided only for reference. Patton has no association with the site and does not guarantee the site's validity or availability.)

LAN Connection

- **Problem:** What can I do if I suspect a problem on my LAN connection?
- **Solution:** You can test the LAN connection using **Ping**.

  For example, if you are using DOS/Windows, at the Command Prompt, type: ***ping 192.168.1.1***

  This pings the BODi device (provided that BD1000 device's IP is 192.168.1.1) to test whether the connection to BD1000 is OK.

WAN Connection

- **Problem:** What can I do if I suspect a problem on my Internet/WAN connection?
- **Solution:** You can test the WAN connection using **Ping**.

  As we want to isolate the problems from the LAN, **Ping** will be performed from the BD1000. By using the **Ping/Traceroute** tests in the **Status** tab on the Web Admin Interface, you may be able to find out the source of problem.

File Upload/Transfer

- **Problem:** When I upload files to a server via ftp, the transfer stalls after a few kilobytes of data are sent. What should I do?
- **Solution:** The Maximum Transmission Unit (MTU) or MSS setting may need to be adjusted.

  By default, the MTU is set at 1440. Choose mtu for all of your WAN connections. If it does not solve the problem, you may try the MTU 1492 if a connection is a DSL. If problem still persists, change the size to smaller values until your problem is resolved (e.g. 1462, 1440, 1420, 1400, etc).

Chapter 13 Contacting Patton for assistance

Chapter contents

Introduction

This chapter contains the following information:

- "Contact information"—describes how to contact Patton technical support for assistance.
- "Warranty Service and Returned Merchandise Authorizations (RMAs)"—contains information about the warranty and obtaining a return merchandise authorization (RMA).

Contact information

Patton Electronics offers a wide array of free technical services. If you have questions about any of our other products we recommend you begin your search for answers by using our technical knowledge base. Here, we have gathered together many of the more commonly asked questions and compiled them into a searchable database to help you quickly solve your problems.

Patton support headquarters in the USA

- Online support: available at **www.patton.com**
- E-mail support: e-mail sent to **support@patton.com** will be answered within 1 business day
- Telephone support: standard telephone support is available five days a week—from **8:00 am** to **5:00 pm EST** (**1300** to **2200 UTC/GMT**)—by calling **+1 (301) 975-11000**
- Fax: **+1 (301) 869-9293**

Alternate Patton support for Europe, Middle East, and Africa (EMEA)

- Online support: available at **www.patton.com**
- E-mail support: e-mail sent to **support@patton.com** will be answered within 1 business day
- Telephone support: standard telephone support is available five days a week—from **9:00 am** to **5:30 pm CET** (**0800** to **1630 UTC/GMT**)—by calling **+41 (0)31 985 25 55**
- Fax: **+41 (0)31 985 25 26**

Warranty Service and Returned Merchandise Authorizations (RMAs)

Patton Electronics is an ISO-9001 certified manufacturer and our products are carefully tested before shipment. All of our products are backed by a comprehensive warranty program.

Note If you purchased your equipment from a Patton Electronics reseller, ask your reseller how you should proceed with warranty service. It is often more convenient for you to work with your local reseller to obtain a replacement. Patton services our products no matter how you acquired them.

Warranty coverage

Our products are under warranty to be free from defects, and we will, at our option, repair or replace the product should it fail within one year from the first date of shipment. Our warranty is limited to defects in workmanship or materials, and does not cover customer damage, lightning or power surge damage, abuse, or unauthorized modification.

Out-of-warranty service

Patton services what we sell, no matter how you acquired it, including malfunctioning products that are no longer under warranty. Our products have a flat fee for repairs. Units damaged by lightning or other catastrophes may require replacement.

Returns for credit

Customer satisfaction is important to us, therefore any product may be returned with authorization within 30 days from the shipment date for a full credit of the purchase price. If you have ordered the wrong equipment or you are dissatisfied in any way, please contact us to request an RMA number to accept your return. Patton is not responsible for equipment returned without a Return Authorization.

Return for credit policy

- Less than 30 days: No Charge. Your credit will be issued upon receipt and inspection of the equipment.
- 30 to 60 days: We will add a 20% restocking charge (crediting your account with 80% of the purchase price).
- Over 60 days: Products will be accepted for repairs only.

RMA numbers

RMA numbers are required for all product returns. You can obtain an RMA by doing one of the following:

- Completing a request on the RMA Request page in the *Support* section at **www.patton.com**
- By calling **+1 (301) 975-11000** and speaking to a Technical Support Engineer
- By sending an e-mail to **returns@patton.com**

All returned units must have the RMA number clearly visible on the outside of the shipping container. Please use the original packing material that the device came in or pack the unit securely to avoid damage during shipping.

Shipping instructions

The RMA number should be clearly visible on the address label. Our shipping address is as follows:

Patton Electronics Company
RMA#: xxxx
7622 Rickenbacker Dr.
Gaithersburg, MD 20879-4773 USA

Patton will ship the equipment back to you in the same manner you ship it to us. Patton will pay the return shipping costs.

Appendix A **Compliance Information**

Chapter contents

Compliance

EMC

- EN55022, Class A
- EN55024

Low-Voltage Directive (Safety)

- IEC/EN60950-1, 2nd edition

CE Declaration of Conformity

Patton Electronics, Inc declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2004/108/EC relating to electromagnetic compatibility and Directive 2006/95/EC relating to electrical equipment designed for use within certain voltage limits. The Declaration of Conformity may be obtained from Patton Electronics, Inc at www.patton.com/certifications.

The safety advice in the documentation accompanying this device shall be obeyed. The conformity to the above directive is indicated by CE mark on the device.

Authorized European Representative

D R M Green

European Compliance Services Limited.

Avalon House, Marcham Road

Abingdon,

Oxon OX14 1UD, UK

Appendix B **Specifications**

Chapter contents

WAN Interface

5 x Fast Ethernet Ports

2x USB interfaces

Dual 802.11b/g/n Wi-Fi Modem

Support for PPPoE, Static IP, DHCP

WAN Link Health Check

Bandwidth Allowance Monitor

LAN Interface

1-Port Gigabit Ethernet Switch

Extended DHCP Options

DHCP Reservation

Support for Dynamic DNS services

DNS Proxy for LAN Clients

VPN

Complete VPN Solution

Site-to-Site VPN Bonding

Bandwidth Aggregation

Intelligent Failover

256-bit AES Encryption

Pre-shared Key Authentication

Dynamic Routing PPTP VPN Server

RADIUS, LDAP Authentication

IPsec VPN (Network-to-Network)

Load Balancing

Intelligent Failover

Session Persistence

Per-Service Load Distribution

Multiple Algorithms

Networking

NAT and IP Forwarding

Static Routes

Port Forwarding

Many to One, One to One NAT

NAT Pool

SIP ALG, H.323 ALG

UPnP, NAT-PMP

WINS Server

Advanced QoS

User Groups

Bandwidth Reservation

Individual Bandwidth Limit

Custom Application QoS

Application Prioritization

Device Management

Web Administrative Interface

Email Notification

Active Client & Session Lists

Bandwidth Usage Statistics

Web Reporting Services

Syslog Service

SNMP v1, v2c and v3

Physical

Dimensions: 10.2W x 5.7H x 1.6D inch (260W x 143H x 39.5D mm)

Weight: 4 lbs

Operating temperature:

Appendix C **Applications**

Chapter contents

Routing under DHCP, Static IP, and PPPoE

The information in this section only applies to situations where the BD1000 operates with to a WAN connection under DHCP, Static IP and PPPoE.

Routing via Network Address Translation (NAT)

When the BD1000 is operating under NAT mode, the source IP addresses of outgoing IP packets are translated to the WAN IP address of the BD1000. Therefore, with NAT, all LAN devices share the same WAN IP address to access the Internet (i.e. the WAN IP address of the BD1000). Operating the BD1000 in NAT mode requires only one WAN (Internet) IP address. In addition, operating in NAT mode also has security advantages because LAN devices are hidden behind the BD1000, not directly accessible from the Internet and hence, less vulnerable to attacks. The following figure shows the packet flow in NAT mode:

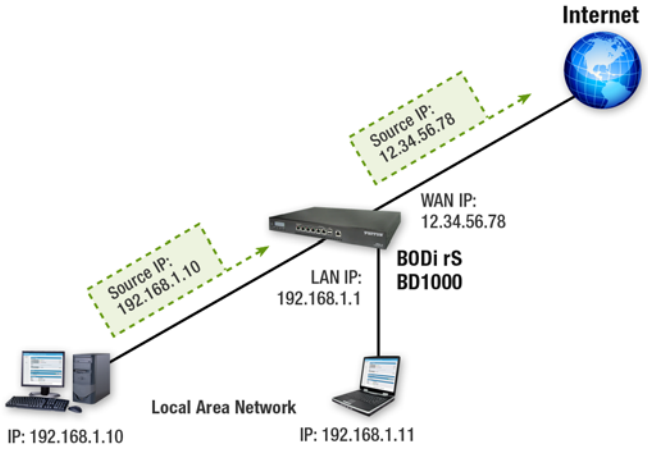


Figure 118. Routing via NAT Application

Routing via IP Forwarding

When the BD1000 is operating under IP Forwarding mode, the IP addresses of IP packets are unchanged; the BD1000 forwards both inbound and outbound IP packets without changing their IP addresses. The following figure shows the packet flow in IP Forwarding mode:

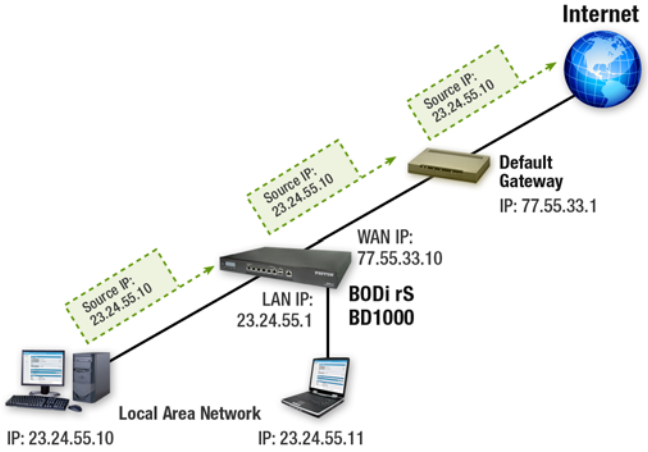


Figure 119. Routing via NAT Application

Performance Optimization

Scenario

In this scenario, email and web browsing are the two main Internet services used by the LAN users. The mail server is external to the network. The connections are ADSL (with slow uplink and fast downlink) and Metro Ethernet (symmetric).

Solution

The solution is to individually set the WAN loading balance according to the service.

- Web browsing mainly downloads data; sending e-mails mainly consumes upload bandwidth.
- Both connections offer good download speeds; WAN2 offers good upload speeds.
- Define WAN1 and WAN2's inbound and outbound bandwidths to be 3M/512k and 4M/4M respectively.
- For HTTP, set the weight to 3 : 4.
- For SMTP, set the weight to 1 : 8, such that users will have a greater chance to be routed via WAN2 when sending e-mail.

Settings

- Add a new outbound traffic rule for HTTP.
- Add a new outbound traffic rule for SMTP.

Maintaining the Same IP Address throughout a Session

Scenario

Some client IP address sensitive websites (for example, Internet banking) use both client IP address and cookies matching for session identification. Since different IP addresses are used during the load balancing, the session is dropped when a mismatching IP is detected.

Solution

Make use of the Persistence functionality of the BD1000.

With Persistence configured and the option **By Destination** selected, the BD1000 uses a consistent WAN connection for source-destination pairs of IP addresses, and prevents sessions from being dropped.

With Persistence configured and the option **By Source** selected, the BD1000 uses a consistent WAN connection for same source IP addresses. This option offers even higher application compatibility, but the outbound traffic load will be distributed more evenly only if more users use the Internet.

Settings

- Set persistence in: **Network > Outbound Policy > Managed by Custom Rules**.
- Click **Add Rule**, select **HTTP** (TCP port 80) for web service,and select **Persistence**.

Note A network administrator can use the Traceroute utility to manually analyze the connection path of a particular WAN connection.

Bypassing the Firewall to Access Hosts on LAN

Scenario

There are times when remote access to computers on the LAN is desirable; for example, when hosting websites, online businesses and FTP download and upload areas, etc. In such cases, it may be appropriate to create an inbound NAT mapping for the network to allow some hosts on the LAN to be accessible from outside of the firewall.

Solution

Web Admin Interface can be used for adding an inbound NAT Mapping to a host and to bind the host to the WAN connections, via **Network > NAT Mappings > Add NAT Rule**. For example, you may add the host, with IP address 192.168.1.102 to an Inbound Mapping, and bind the host to the default IP and 211.123.123.100 of WAN1.

Inbound Access Restriction

Scenario

A firewall is required to protect the network from potential hacker attacks and other Internet security threats.

Solution

Firewall functionality is built into the BD1000. By default, inbound access is unrestricted. Enabling a basic level of protection involves setting up firewall rules. For example, to set up a firewall rule between the Internet and the private network that monitors Web access from the Internet, click the **Add Rule** button in the **Inbound Firewall Rules** table. Use the following settings for the new rule:

- **Protocol:** TCP <- HTTP
- **Source IP & Port:** Any Address, Any Port
- **Destination IP & Port:** Any Address, Single Port, Port 80
- **Action:** Allow

After the fields have been entered, click **Save** to add the rule. Then, change the default inbound rule to **Deny** by clicking the **Default** rule in the **Inbound Firewall Rules** table.

Outbound Access Restriction

Scenario

For security reasons, it may be appropriate to disallow LAN users to use ftp to transfer files to and from the Internet, or otherwise restrict outbound access. This can easily be achieved by setting up an outbound firewall rule with the BD1000.

Solution

To set up a firewall rule between the Internet and the private network for outbound access, click the **Add Rule** button in the **Outbound Firewall Rules** table. Use the following settings for the new rule:

- **Protocol:** TCP <- HTTP
- **Source IP & Port:** Any Address, Any Port
- **Destination IP & Port:** Any Address, Single Port, Port 21
- **Action:** Deny

After the fields have been entered, click **Save** to add the rule.

Appendix D **Terms**

Chapter contents

Abbreviations

Abbreviation	Meaning
3G	3rd Generation standards for wireless communications (e.g. HSDPA)
4G	4th Generation standards for wireless communications (e.g. WiMAX, LTE)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EVDO	Evolution-Data Optimized
HSDPA	High-Speed Downlink Packet Access
GRE	Generic Routing Encapsulation
HTTP	Hyper-Text Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
MAC Address	Media Access Control Address
MTU	Maximum Transmission Unit
MSS	Maximum Segment Size
NAT	Network Address Translation
PPPoE	Point to Point Protocol over Ethernet
QoS	Quality of Service
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WINS	Windows Internet Name Service
WLAN	Wireless Local Area Network