

Pepwave Device Connector User Manual

Pepwave Product:

Device Connector Rugged

Pepwave Firmware 1.1

June 2020

Table of Contents

1. Getting Started

- 1.1 What's in the Box
- 1.2 Get to Know Your Device Connector
- 1.3 Access the Web Admin Interface
 - 1.3.1 Connect by Ethernet
 - 1.3.2 Connect by Wi-Fi
- 1.4 Choose Your Connection Mode

2 Configuring the LAN interface(s)

- 2.1 Network Settings
- 2.2 Port Setting

3 Configuring the WAN Interface(s)

- 3.1 Wi-Fi WAN Settings (Wi-Fi Mode Only)
 - 3.1.1 Wireless Networks
 - 3.1.2 Creating Wi-Fi Connection Profiles
- 3.2 WAN Health Check

4 AP

- 4.1 Wireless SSID
- 4.2 Settings

5 System Settings

- 5.1 Admin Security
- 5.2 Operating Mode
- 5.3 Firmware
- 5.4 Time
- 5.5 Schedule
- 5.6 Email Notification
- 5.7 Event Log
- 5.8 SNMP
- 5.9 InControl
- 5.10 Configuration
- 5.11 Feature Add-ons

5.12 Reboot

6 Tools

6.1 Ping

6.2 Traceroute

6.3 Wake-on-LAN

7 PEPVPN

8 Port Forwarding

9 NAT Mappings

10 QoS

10.1 Bandwidth Control

10.2 Application

10.2.1 Application Prioritization

10.2.2 Prioritization for Custom Applications

10.2.3 DSL/Cable Optimization

11 Miscellaneous Settings

11.1 Certificate Manager

12 Status

12.1 Device

12.2 Client List

12.3 PepVPN

12.4 Event Log

12.5 Bandwidth

12.5.1 Real Time

12.5.2 Hourly

12.5.3 Daily

12.5.4 Monthly

Restoration of Factory Defaults

Appendix

1. Getting Started

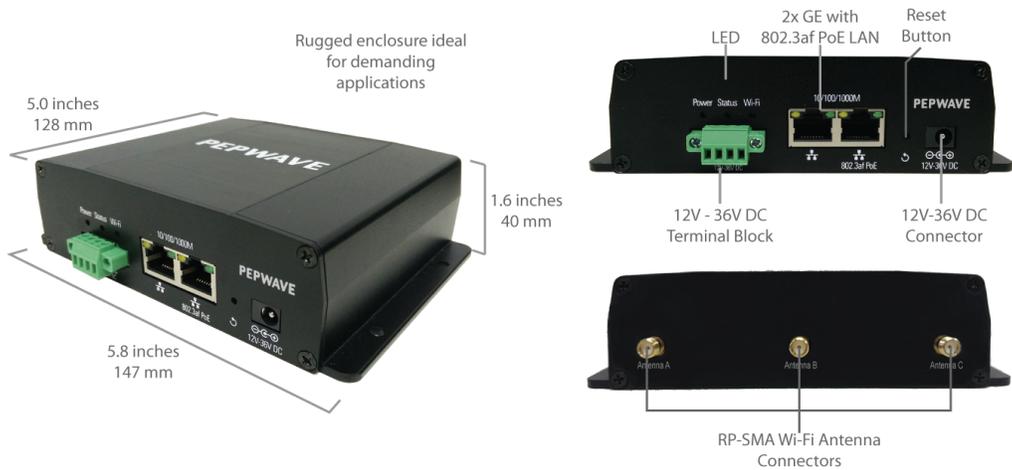
1.1 What's in the Box

DCS-RUG

- 12V power supply
- 3x dual-band 5dBi omni antenna

1.2 Get to Know Your Device Connector

Device Connector Rugged



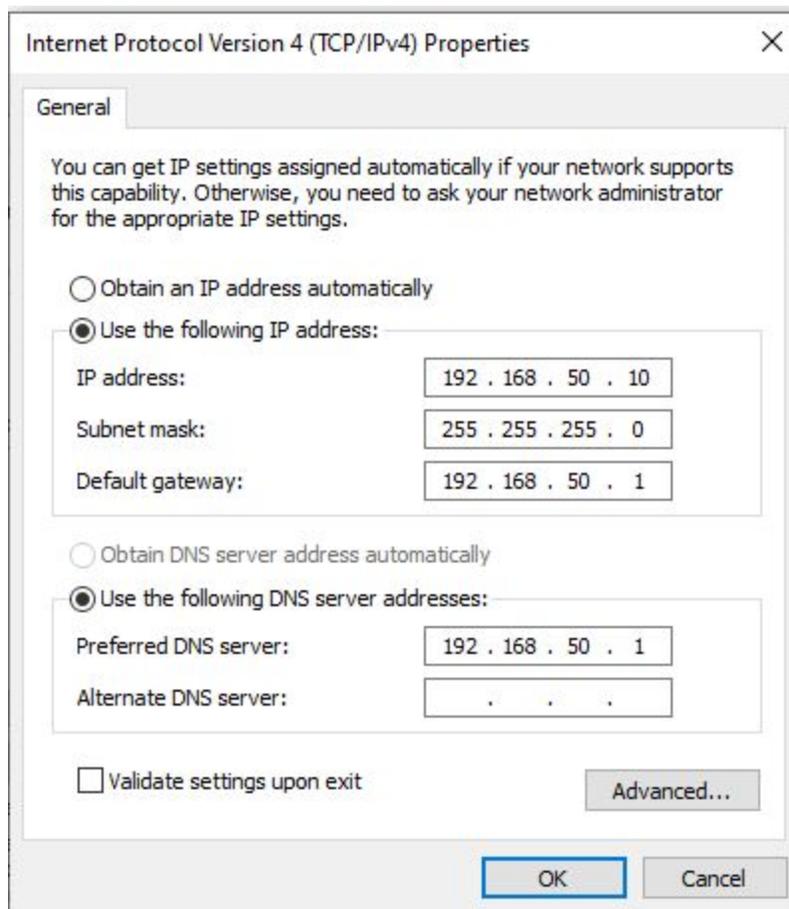
1.3 Access the Web Admin Interface

There are two ways to access the **Web Admin** page.

1.3.1 Connect by Ethernet

To access the Web Admin page by Ethernet, your PC must be in the same subnet as the Device Connector (*i.e.* 192.168.50.X).

Your PC should be set up as follow on the **Internet Protocol (TCP/IP) Properties** or **Network** screen:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address: 192 . 168 . 50 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 50 . 1

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 50 . 1

Alternate DNS server: . . .

Validate settings upon exit

Advanced...

OK Cancel

1.3.2 Connect by Wi-Fi

Connect to the SSID: PEPWAVE_XXX where XXXX represents the last four digits of your device’s serial number (e.g. 7D6E). Passphrase is the last 8 hexadecimal digits of your device’s LAN MAC address (e.g. DDC3CCC0)

Now you are ready to start the first time configuration of the Pepwave Device Connector. On your PC, start a web browser, go to this URL:

<http://192.168.50.1/>

1.4 Choose Your Connection Mode

The Device Connector supports only Wi-Fi connection mode.

After successful login The **dashboard** will be displayed. The **Dashboard** shows current WAN and WI-FI AP.

The screenshot shows the PEPWAVE dashboard with the following sections:

- Navigation:** Dashboard (selected), Network, Advanced, AP, System, Status, Apply Changes.
- WAN Connection Status:**
 - Priority 1 (Highest): Wi-Fi WAN 2 (Scanning...)
 - Priority 2: Wi-Fi WAN 1 (Connected to DCR_2.4GHz)
 - Priority 3: Drag desired (Priority 3) connections here
 - Disabled: Drag desired (Disabled) connections here
- LAN Interface:** Router IP Address: 192.168.50.1
- Wi-Fi AP:** ON (dropdown), Details
- PepVPN:** PepVPN Profile 1 (Starting...)
- Device Information:**
 - Model: Pepwave Device Connector Rugged
 - Firmware: 1.1.0s003 build 2258
 - Uptime: 53 days 5 hours 3 minutes
 - CPU Load: 0%
 - Throughput: 21.0 kbps (down), 22.0 kbps (up)

Copyright © Pepwave. All rights reserved.

2 Configuring the LAN interface(s)

2.1 Network Settings

LAN interface settings are located at **Network>LAN>Network Settings/Port Settings**. Begin setting up your physical LAN by entering IP settings (VLAN configuration will be covered following physical LAN setup).

LAN	VLAN	Network	
LAN	None	172.16.251.1/24	
VLAN1	1	2.2.2.2/24	
VLAN2	2	3.3.3.3/24	

This represents the LAN interfaces that are active on your router (including VLAN). A grey “X” means that the VLAN is used in other settings and cannot be deleted. You can find which settings are using the VLAN by hovering over the grey “X”. Alternatively, a red “X” means that there are no settings using the VLAN. You can delete that VLAN by clicking the red “X”

Clicking any of the existing LAN interfaces will result in the following

IP Settings ?

IP Address

IP Settings

IP Address & Subnet Mask ?

Enter the Device Connector’s IP address and subnet mask values to be used on the LAN. To enable multiple VLANs, press the

DHCP Server Settings			
DHCP Server	<input checked="" type="checkbox"/>	Enable	
IP Range	<input type="text" value="192.168.50.10"/>	-	<input type="text" value="192.168.50.250"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>	(/24)	
Lease Time	<input type="text" value="1"/>	Days	<input type="text" value="0"/> Hours <input type="text" value="0"/> Mins
DNS Servers	<input checked="" type="checkbox"/>	Assign DNS server automatically	
WINS Server	<input checked="" type="checkbox"/>	Assign WINS server	
	<input checked="" type="radio"/>	Built-in	
	<input type="radio"/>	External	
BOOTP	<input checked="" type="checkbox"/>	Server IP Address: <input type="text"/>	
		Boot File: <input type="text"/>	
		Server Name: <input type="text"/> (Optional)	
Extended DHCP Option	<input type="text" value="Option"/>	<input type="text" value="Value"/>	<input type="text"/>
<i>No Extended DHCP Option</i>			
Add			
DHCP Reservation	<input type="text" value="Name"/>	<input type="text" value="MAC Address"/>	<input type="text" value="Static IP"/>
			+

DHCP Server Settings	
DHCP Server	When this setting is enabled, the DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collision on the LAN.
IP Range & Subnet Mask	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.
Lease Time	This setting specifies the length of time throughout which 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 renewal of the IP address assignment will be required.
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If Assign DNS server automatically is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	In addition to standard DHCP options (e.g., DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the Add button, choose the option 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 area input control. Each option can be defined once only.

DHCP Reservation

This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses.

Name (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of **00: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 at **Status>Client List**. For more details, please refer to **Section 22.3**.

Once configuration is complete, click Save to store the changes.

To configure DHCP relay, first click the  button found next to the **DHCP Server** option to display the settings.

DHCP Relay Settings	
DHCP Relay	 <input checked="" type="checkbox"/> Enable
DHCP Server IP Address	 DHCP Server 1: <input type="text"/> DHCP Server 2: <input type="text"/>
DHCP Option 82	 <input type="checkbox"/>

DHCP Relay Settings	
Enable	Check this box to turn on DHCP relay. Click the  icon to disable DHCP relay.
DHCP Server IP Address	Enter the IP addresses of one or two DHCP servers in the provided fields. The DHCP servers entered here will receive relayed DHCP requests from the LAN. For active-passive DHCP server configurations, enter active and passive DHCP server relay IP addresses in DHCP Server 1 and DHCP Server 2 .
DHCP Option 82	DCHP Option 82 includes device information as relay agent for the attached client when forwarding DHCP requests from client to server. This option also embeds the device's MAC address and network name in circuit and remote IDs. Check this box to enable DHCP Option 82.

2.2 Port Setting

Port settings can be accessed at **Network>Port Settings**.

Port Name	Enable	Speed	Advertise Speed
LAN Port 1	<input checked="" type="checkbox"/>	Auto	<input checked="" type="checkbox"/>
LAN Port 2	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>

LAN Physical Settings

Speed This is the port speed of the LAN interface. It should be set to the same speed as the connected device to avoid port negotiation problems. When a static speed is set, you may choose whether to advertise its speed to the peer device. **Auto** is selected by default. You can choose not to advertise the port speed if the port has difficulty negotiating with the peer device.

3 Configuring the WAN Interface(s)

WAN Interface settings are located at Network>WAN. To reorder WAN priority, drag on the appropriate WAN by holding the left mouse button, move it to the desired priority (the first one would be the highest priority, the second one would be lower priority, and so on), and drop it by releasing the mouse button.

Priority	Connection Name	Status	Buttons
Priority 1 (Highest)	Wi-Fi WAN 2	Scanning...	Wireless Networks Details
Priority 2	Wi-Fi WAN 1	Connected to DCR_2.4GHz	Wireless Networks Details
Priority 3	Drag desired (Priority 3) connections here		
Disabled	Drag desired (Disabled) connections here		

To disable a particular WAN connection, drag on the appropriate WAN by holding the left mouse button, move it the Disabled row, and drop it by releasing the mouse button.

You can also set priorities on the Dashboard. Click the Details button in the corresponding row to modify the connection setting.

Important Note

Connection details will be changed and become effective immediately after clicking the **Save and Apply** button.

3.1 Wi-Fi WAN Settings (Wi-Fi Mode Only)

To access Wi-Fi WAN settings, click **Network>WAN**.

3.1.1 Wireless Networks

To see a list of available networks, click inside wireless network. To connect to a displayed network, select it from this list. To access wireless network, click **Network>WAN>Wireless Networks**.

Wireless Networks
✕

Details
^

Network Name (SSID)	Security	Signal	Ch	Action
✔ DCR_2.4GHz	🔒 WPA/WPA2-Personal	📶 -17dBm	11	Disconnect
	🔒 WPA/WPA2-Personal	📶 -26dBm	6	Connect
670 Events	🔒 WPA/WPA2-Personal	📶 -31dBm	6	Connect
680-wifi	🔒 WPA/WPA2-Personal	📶 -47dBm	10	Connect
_Peplink_Guest_2.4G	🔒 WPA/WPA2-Personal	📶 -22dBm	6	Connect
Billy's Dev CP Test5	🔒 WPA/WPA2-Personal	📶 -15dBm	5	Connect
Billy_CP_Mars	🔒 WPA/WPA2-Personal	📶 -23dBm	5	Connect
Billy_Dev_CP_Test4	🔒 WPA/WPA2-Personal	📶 -21dBm	5	Connect

Close

To access detailed WAN settings click, **Network>WAN>Details**.

WAN Connection Settings	
WAN Connection Name	<input type="text" value="Wi-Fi WAN 1"/> <input type="button" value="Default"/>
Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnected
MTU	<input type="radio"/> Auto <input checked="" type="radio"/> Custom Value: <input type="text" value="1500"/> <input type="button" value="Default"/>
Reply to ICMP PING	<input checked="" type="radio"/> Yes <input type="radio"/> No

Wi-Fi Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Standby State	This setting specifies the state of the WAN connection while in standby. The available options are Remain Connected (hot standby) and Disconnect (cold standby).
MTU	This setting specifies the maximum transmission unit. By default, MTU is set to 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 appropriate MTU value will be automatically detected. The auto-detection will run each time the WAN connection establishes
Reply to ICMP PING	If this setting is disabled, the WAN connection will not respond to ICMP ping requests. By default, this setting is enabled.

Wi-Fi WAN Settings	
Channel Width	<input type="text" value="20 MHz"/>
Channel Selection	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
Data Rate	<input checked="" type="radio"/> Auto <input type="radio"/> Fixed
Output Power	<input type="text" value="Max"/> <input type="checkbox"/> Boost
Roaming	<input type="checkbox"/>
Connect to Any Open Mode AP	<input type="radio"/> Yes <input checked="" type="radio"/> No
Beacon Miss Counter	<input type="text" value="5"/>

Wi-Fi WAN Settings	
Channel Width	Available options are 20 MHz, 40 MHz, and Auto (20/40 MHz) . Default is Auto (20/40 MHz), which allows both widths to be used simultaneously.

Channel Selection	Determine whether the channel will be automatically selected. If you select custom, the following table will appear:
Data Rate	This option allows you to select a specific bit rate for data transfer over the device's Wi-Fi network. By default, Auto is selected.
Output Power	This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – Max, High, Mid, and Low. The actual output power will be bound by the regulatory limits of the selected country. Note that selecting the Boost option may cause the MAX's radio output to exceed local regulatory limits.
Roaming	Checking this box will enable Wi-Fi roaming. Click the icon for additional options.
Connect to Any Open Mode AP	This option is to specify whether the Wi-Fi WAN will connect to any open mode access points it finds.
Beacon Miss Counter	This field allows you to set the frequency for the beacon to include delivery traffic indication messages.

Bandwidth Allowance Monitor	
Bandwidth Allowance Monitor	<input checked="" type="checkbox"/> Enable
Action	<input type="checkbox"/> Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification . <input checked="" type="checkbox"/> Disconnect when usage hits 100% of monthly allowance
Start Day	On 1st of each month at 00:00 midnight
Monthly Allowance	<input type="text"/> MB

Bandwidth Allowance Monitor	
Action	<p>If Error! Reference source not found. is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance.</p> <p>If Disconnect when usage hits 100% of monthly allowance is checked, this WAN connection will be disconnected automatically 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.</p>
Start Day	This option allows you to define which day of the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

Health Check Settings	
Health Check Method	? DNS Lookup ▾
Health Check DNS Servers	? Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers <input type="checkbox"/> Include public DNS servers
Timeout	? 5 ▾ second(s)
Health Check Interval	? 5 ▾ second(s)
Health Check Retries	? 3 ▾
Recovery Retries	? 3 ▾

Health Check Settings

Method This setting specifies the health check method for the WAN connection. This value can be configured as Disabled, PING, DNS Lookup, or HTTP. The default method is DNS Lookup. For mobile Internet connections, the value of Method can be configured as Disabled or SmartCheck.

Health Check Disabled

Health Check Settings	
Health Check Method	? Disabled ▾ <small>Health Check disabled. Network problem cannot be detected.</small>

When Disabled is chosen in the Method field, the WAN connection will always be considered as up. The connection will NOT be treated as down in the event of IP routing errors.

Health Check Method: PING

Health Check Method	? PING ▾
PING Hosts	? Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts

ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.

PING Hosts This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. If Use first two DNS servers as Ping Hosts is checked, the target ping host will be the first DNS server for the corresponding WAN connection. Reliable ping hosts with a high uptime should be considered. By default, the first two DNS servers of the WAN connection are used as the ping hosts.

Health Check Method: DNS Lookup

Health Check Method	<input style="float: left; margin-right: 5px;" type="button" value="?"/> DNS Lookup
Health Check DNS Servers	<input style="float: left; margin-right: 5px;" type="button" value="?"/> Host 1: <input style="width: 150px;" type="text"/> Host 2: <input style="width: 150px;" type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers <input type="checkbox"/> Include public DNS servers

DNS lookups will be issued to test connectivity with target DNS servers. The connection will be treated as up if DNS responses are received from one or both of the servers, regardless of whether the result was positive or negative.

Health Check DNS Servers

This field allows you to specify two DNS hosts' IP addresses with which connectivity is to be tested via DNS Lookup.

If Use first two DNS servers as Health Check DNS Servers is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, Host 1 must be filled, while a value for Host 2 is optional.

If Include public DNS servers is selected 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 also 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. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

Health Check Method: HTTP

Health Check Method	<input style="float: left; margin-right: 5px;" type="button" value="?"/> HTTP
URL 1	<input style="float: left; margin-right: 5px;" type="button" value="?"/> http:// <input style="width: 150px;" type="text"/> Matching String: <input type="checkbox"/>
URL 2	<input style="float: left; margin-right: 5px;" type="button" value="?"/> http:// <input style="width: 150px;" type="text"/> Matching String: <input type="checkbox"/>

HTTP connections will be issued to test connectivity with configurable URLs and strings to match.

URL1

WAN Settings>WAN Edit>Health Check Settings>URL1

The URL will be retrieved when performing an HTTP health check. When String to Match is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When String to Match is filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.

URL 2

WAN Settings>WAN Edit>Health Check Settings>URL2

If URL2 is also provided, a health check will pass if either one of the tests passed.

Other Health Check Settings

Timeout	5 ▾ second(s)
Health Check Interval	5 ▾ second(s)
Health Check Retries	3 ▾
Recovery Retries	3 ▾

Timeout	This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is 5 seconds.
Health Check Interval	This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is 5 seconds.
Health Check Retries	This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Peplink Balance will treat the corresponding WAN connection as down. Default health retries is set to 3. Using the default Health Retries setting of 3, the corresponding WAN connection will be treated as down after three consecutive timeouts.
Recovery Retries	This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before the Peplink Balance treats a previously down WAN connection as up again. By default, Recover Retries is set to 3. Using the default setting, a WAN connection that is treated as down will be considered as up again upon receiving three consecutive successful ping/DNS lookup responses.

3.1.2 Creating Wi-Fi Connection Profiles

You can manually create a profile to connect to a Wi-Fi connection. This is useful for creating a profile for connecting to hidden SSID access points. Click **Network>WAN>Details>Create Profile...** to get started.



Clicking this will open a window similar to the one shown below.

Create Wi-Fi Connection Profile
✕

Wi-Fi Connection

Network Name (SSID)	<input style="width: 90%;" type="text"/>
Security	Open ▾
IP Address	<input checked="" type="radio"/> Obtain an IP address automatically <input type="radio"/> Static

Wi-Fi Connection Profile Settings

Type Select whether the network will connect automatically or manually.

Network Name (SSID) Enter a name to represent this Wi-Fi connection.

Security This option allows you to select which security policy is used for this wireless network. Available options:

- **Open**

Security	Open ▾
----------	--------

- **WEP**

Security	WEP ▾
Encryption Key ?	<input style="width: 90%;" type="text"/>
	<input checked="" type="checkbox"/> Hide Characters

- **WPA/WPA2 – Personal**

Security	WPA/WPA2-Personal ▾
Shared Key ?	<input style="width: 90%;" type="text"/>
	<input checked="" type="checkbox"/> Hide Characters

- **WPA/WPA2 – Enterprise**

Security	WPA/WPA2-Enterprise ▾
Login ID	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
EAP Method	PEAP ▾
EAP Phase 2 Method	EAP/CHAP ▾
EAP outer authentication identity	<input checked="" type="radio"/> Anonymous <input type="radio"/> User Credentials <input type="radio"/> Other: <input type="text"/>

3.2 WAN Health Check

To ensure traffic is routed to healthy WAN connections only, the Pepwave router can periodically check the health of each WAN connection. The health check settings for each WAN connection can be independently configured via **Network>WAN>Details**.

Health Check Settings

Method This setting specifies the health check method for the WAN connection. This value can be configured as **Disabled**, **PING**, **DNS Lookup**, or **HTTP**. The default method is **DNS Lookup**. For mobile Internet connections, the value of **Method** can be configured as **Disabled** or **SmartCheck**.

Health Check Disabled

Health Check Method	<input style="float: left; margin-right: 5px;" type="button" value="?"/> <div style="border: 1px solid #ccc; display: inline-block; padding: 2px;">Disabled ▾</div>
Health Check disabled. Network problem cannot be detected.	

When **Disabled** is chosen in the **Method** field, the WAN connection will always be considered as up. The connection will **NOT** be treated as down in the event of IP routing errors.

Health Check Method: PING

Health Check Method	<input style="float: left; margin-right: 5px;" type="button" value="?"/> <div style="border: 1px solid #ccc; display: inline-block; padding: 2px;">PING ▾</div>				
PING Hosts	<input style="float: left; margin-right: 5px;" type="button" value="?"/> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; border-bottom: 1px solid #ccc;">Host 1:</td> <td style="border-bottom: 1px solid #ccc;"><input style="width: 60%;" type="text"/></td> </tr> <tr> <td style="border-bottom: 1px solid #ccc;">Host 2:</td> <td style="border-bottom: 1px solid #ccc;"><input style="width: 60%;" type="text"/></td> </tr> </table> <input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts	Host 1:	<input style="width: 60%;" type="text"/>	Host 2:	<input style="width: 60%;" type="text"/>
Host 1:	<input style="width: 60%;" type="text"/>				
Host 2:	<input style="width: 60%;" type="text"/>				

ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.

PING Hosts This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. If **Use first two DNS servers as Ping Hosts** is checked, the target ping host will be the first DNS server for the corresponding WAN connection. Reliable ping hosts with a high uptime should be considered. By default, the first two DNS servers of the WAN connection are used as the ping hosts.

Health Check Method: DNS Lookup

Health Check Method	? DNS Lookup ▾
Health Check DNS Servers	Host 1: <input type="text"/>
	Host 2: <input type="text"/>
	<input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers
	<input type="checkbox"/> Include public DNS servers

DNS lookups will be issued to test connectivity with target DNS servers. The connection will be treated as up if DNS responses are received from one or both of the servers, regardless of whether the result was positive or negative.

Health Check DNS Servers

This field allows you to specify two DNS hosts' IP addresses with which connectivity is to be tested via DNS lookup.

If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional.

If **Include public DNS servers** is selected 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 also 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. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

Health Check Method: HTTP

Health Check Method	? HTTP ▾
URL 1	? http:// <input type="text"/> Matching String: <input type="checkbox"/>
URL 2	? http:// <input type="text"/> Matching String: <input type="checkbox"/>

HTTP connections will be issued to test connectivity with configurable URLs and strings to match.

URL 1

WAN Settings>WAN Edit>Health Check Settings>URL1

The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.

URL 2

WAN Settings>WAN Edit>Health Check Settings>URL2

If **URL2** is also provided, a health check will pass if either one of the tests passed.

Timeout		10 ▾ second(s)
Health Check Interval		5 ▾ second(s)
Health Check Retries		3 ▾
Recovery Retries		3 ▾

Other Health Check Settings	
Timeout	This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is 5 seconds .
Health Check Interval	This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is 5 seconds .
Health Check Retries	This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Pepwave router will treat the corresponding WAN connection as down. Default health retries is set to 3 . Using the default Health Retries setting of 3 , the corresponding WAN connection will be treated as down after three consecutive timeouts.
Recovery Retries	This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before the Pepwave router treats a previously down WAN connection as up again. By default, Recover Retries is set to 3 . Using the default setting, a WAN connection that is treated as down will be considered as up again upon receiving three consecutive successful ping/DNS lookup responses.

Automatic Public DNS Server Check on DNS Test Failure

When the health check method is set to **DNS Lookup** and health checks fail, the Pepwave router will automatically perform DNS lookups on public DNS servers. If the tests are successful, the WAN may not be down, but rather the target DNS server malfunctioned. You will see the following warning message on the main page:

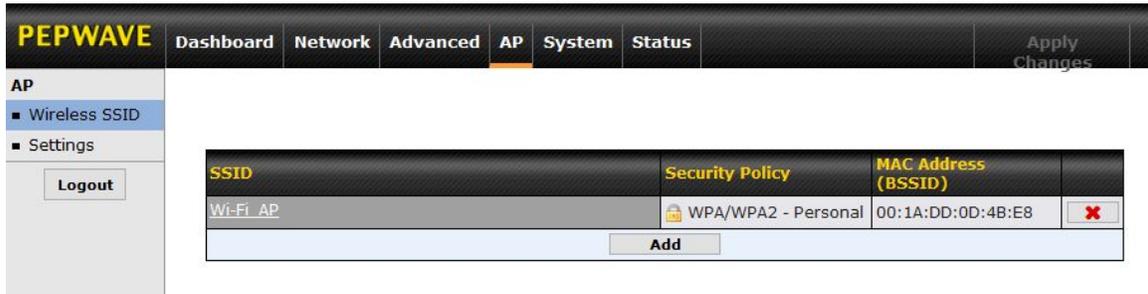
 **Failed to receive DNS response from the health-check DNS servers for WAN connection 3. But public DNS server lookup test via the WAN passed. So please check the DNS server settings.**

4 AP

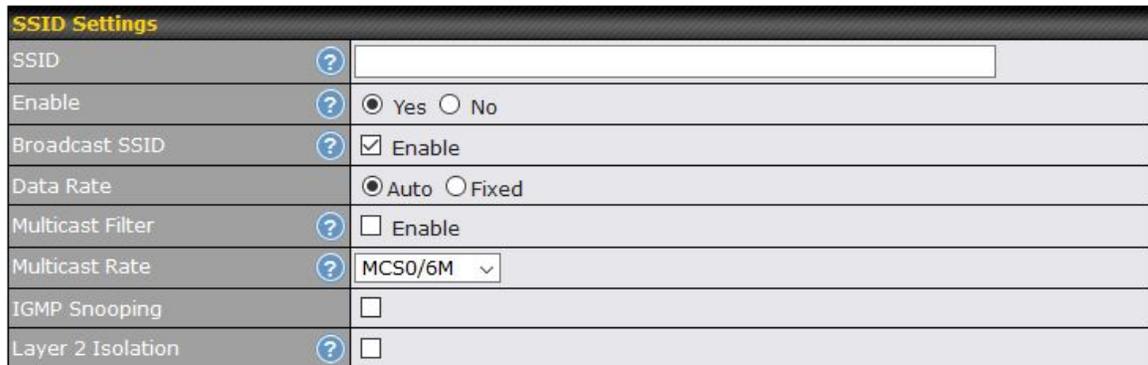
Use the controls on the **AP** tab to set the wireless SSID and AP settings.

4.1 Wireless SSID

Wireless network settings, including the name of the network (SSID) and security policy, can be defined and managed in this section.



Click **ADD** to create a new network profile, or click the existing network profile to modify its settings.



SSID Settings	
SSID	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
Enable	Select Yes to enable the virtual AP.
Broadcast SSID	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. Broadcast SSID is enabled by default.
Data Rate ^A	Select Auto to allow the Pepwave router to set the data rate automatically, or select Fixed and choose a rate from the displayed drop-down menu.
Multicast Filter ^A	This setting enables the filtering of multicast network traffic to the wireless SSID.
Multicast Rate ^A	This setting specifies the transmit rate to be used for sending multicast network traffic. The selected Protocol and Channel Bonding settings will affect the rate options and values available here.

IGMP Snooping ^A	To allow the Pepwave router to listen to internet group management protocol (IGMP) network traffic, select this option.
Layer 2 Isolation ^A	Layer 2 refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to upper communication layer(s). By default, the setting is disabled.

Security Settings	
Security Policy	WPA2 - Personal ▼
Encryption	AES:CCMP
Shared Key	<input type="password" value="••••••••"/> <input checked="" type="checkbox"/> Hide Characters

Security Settings	
Security Policy	This setting configures the wireless authentication and encryption methods. Available options are Open (No Encryption) , WPA/WPA2 - Personal , WPA/WPA2 - Enterprise and Static WEP .

Access Control	
Restricted Mode	Deny all except listed ▼
MAC Address List	<input type="text"/>

Access Control	
Restricted Mode	The settings allow administrator to control access using MAC address filtering. Available options are None , Deny all except listed
MAC Address List	Connection coming from the MAC addresses in this list will be either denied or accepted based the option selected in the previous field.

4.2 Settings

Navigating to **AP>Settings** displays a screen similar to the one shown below:

Wi-Fi Radio Settings	
Operating Country	United States <input type="button" value="v"/>
SSID	2.4GHz <input checked="" type="checkbox"/> 5GHz <input checked="" type="checkbox"/> Wi-Fi_AP

Wi-Fi AP Settings ?	
Protocol	802.11ng <input type="button" value="v"/> 802.11ac <input type="button" value="v"/>
Channel Width	20 MHz <input type="button" value="v"/> 80 MHz <input type="button" value="v"/>
Channel	1 (2.412 GHz) <input type="button" value="v"/> Auto <input type="button" value="v"/> <input type="button" value="Edit"/> Channels: 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 149 153 157 161
Output Power	Max <input type="button" value="v"/> <input type="checkbox"/> Boost Max <input type="button" value="v"/> <input type="checkbox"/> Boost
Maximum number of clients	0 (0: Unlimited)
Client Signal Strength Threshold	0 -95 dBm (0: Unlimited)
Beacon Rate	? 1 Mbps <input type="button" value="v"/>
Beacon Interval	? 100 ms <input type="button" value="v"/>
DTIM	? 1 <input type="button" value="Default"/>
RTS Threshold	0 <input type="button" value="Default"/>
Fragmentation Threshold	0 (0: Disable) <input type="button" value="Default"/>
Distance / Time Converter	<input type="range" value="4050"/> 4050 m Note: Input distance for recommended values
Slot Time	? <input type="radio"/> Auto <input checked="" type="radio"/> Custom 9 <input type="button" value="μs"/> <input type="button" value="Default"/>
ACK Timeout	? 48 <input type="button" value="μs"/> <input type="button" value="Default"/>
Frame Aggregation	<input type="checkbox"/>

Wi-Fi Radio Settings	
Operating Country	This option sets the country whose regulations the Pepwave router follows.
Wi-Fi Antenna	Choose from the router's internal or optional external antennas, if so equipped.

Important Note

Per FCC regulations, the country selection is not available on all models marketed in the US. All US models are fixed to US channels only.

Wi-Fi AP Settings

Protocol	This option allows you to specify which client association requests will be accepted. By default, 802.11ng is selected.
Channel Width	Auto (20/40 MHz) and 20 MHz are available. The default setting is Auto (20/40 MHz) , which allows both widths to be used simultaneously. Auto (80 MHz) and (20/40 MHz) are available. The default setting is 80 MHz . The two default settings are for 802.11ng and 802.11ac accordingly?
Channel	This option allows you to select which 802.11 RF channel will be used.
Output Power	This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – Max, High, Mid, and Low . The actual output power will be bound by the regulatory limits of the selected country.
Maximum number of clients	Enter the maximum number of clients that can simultaneously connect to the wireless network or enter 0 to allow an unlimited number of connections.
Client Signal Strength Threshold^A	This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts.
Beacon Rate^A	This option is for setting the transmit bit rate for sending a beacon. By default, 1Mbps is selected.
Beacon Interval^A	This option is for setting the time interval between each beacon. By default, 100ms is selected.
DTIM^A	This field allows you to set the frequency for the beacon to include a delivery traffic indication message. The interval is measured in milliseconds. The default value is set to 1 ms .
RTS Threshold	Set the minimum packet size for your access point to send an RTS using the RTS/CTS handshake. Setting 0 disables this feature.
Fragmentation Threshold^A	Determines the maximum size (in bytes) that each packet fragment will be broken down into. Set 0 to disable fragmentation.

Distance/Time Converter^A	Select the distance you want your Wi-Fi to cover in order to adjust the below parameters. Default values are recommended.
Slot Time^A	This field is for specifying the wait time before the Device Connector transmits a packet. By default, this field is set to 9 μs .
ACK Timeout^A	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to 48 μs .
Frame Aggregation^A	This option allows you to enable frame aggregation to increase transmission throughput.

5 System Settings

5.1 Admin Security

There are two types of user accounts available for accessing the web admin: admin and user. They represent two user levels: the admin level has full administration access, while the user level is read-only. The user level can access only the device's status information; users cannot make any changes on the device

PEPWAVE Dashboard Network Advanced AP System Status Apply Changes

WAN Connection Status

Priority 1 (Highest)

Wi-Fi WAN 2 Scanning... Wireless Networks Details

Priority 2

Wi-Fi WAN 1 Connected to DCR_2.4GHz Wireless Networks Details

Priority 3

Drag desired (Priority 3) connections here

Disabled

Drag desired (Disabled) connections here

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP ON Details

Wi-Fi_AP

PepVPN Status

PepVPN Profile 1 Starting...

Device Information

Model: Pepwave Device Connector Rugged
 Firmware: 1.1.0s003 build 2258
 Uptime: 56 days 10 hours 3 minutes
 CPU Load: 10%
 Throughput: 8.0 kbps ↓ 17.0 kbps ↑

Logout

Copyright © Pepwave. All rights reserved.

Admin Account UI

The screenshot displays the PEPWAVE web interface with the following sections:

- WAN Connection Status:**
 - Priority 1 (Highest): WI-FI WAN 2 (Connected to DCR_5GHz)
 - Priority 2: WI-FI WAN 1 (Standby)
- LAN Interface:** Router IP Address: 192.168.50.1
- Wi-Fi AP:** Status is ON.
- PepVPN:** PepVPN Profile 1 (Starting...)
- Device Information:**
 - Model: Pepwave Device Connector Rugged
 - Firmware: 1.1.0s003 build 2258
 - Uptime: 59 days 18 hours 45 minutes
 - CPU Load: 16%
 - Throughput: 17.0 kbps (down), 50.0 kbps (up)

A yellow warning banner at the bottom states: "You logged in as a read-only user". A "Logout" button is visible in the left sidebar.

Copyright © Pepwave. All rights reserved.

User Account UI

A web login session will be logged out automatically when it has been idle longer than the **Web Session Timeout**. Before the session expires, you may click the **Logout** button in the web admin to exit the session.

0 hours 0 minutes signifies an unlimited session time. This setting should be used only in special situations, as it will lower the system security level if users do not log out before closing the browser. The **default** is 4 hours, 0 minutes.

For security reasons, after logging in to the web admin Interface for the first time, it is recommended to change the administrator password. Configuring the administration interface to be accessible only from the LAN can further improve system security. Administrative settings configuration is located at **System>Admin Security**.

Admin Settings ?	
Router Name	DCS-956A hostname: dcs-956a ⚙️ This configuration is being managed by InControl .
Admin User Name	admin
Admin Password	••••••••
Confirm Admin Password	••••••••
Read-only User Name	user
User Password	
Confirm User Password	
Web Session Timeout	? 4 Hours 0 Minutes
Authentication by RADIUS	? <input checked="" type="checkbox"/> Enable
Auth Protocol	MS-CHAP v2 ▼
Auth Server	<input type="text"/> Port 1812 Default
Auth Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
Auth Timeout	3 seconds
Accounting Server	<input type="text"/> Port 1813 Default
Accounting Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
CLI SSH & Console	? <input checked="" type="checkbox"/> Enable
CLI SSH Port	8822 Default
CLI SSH Access	LAN Only ▼
Security	HTTP ▼
Web Admin Port	80 Default
Web Admin Access	LAN Only ▼

Admin Settings	
Router Name	This field allows you to define a name for this Pepwave router. By default, Router Name is set as DCS_XXXX , where XXXX refers to the last 4 digits of the unit's serial number.
Admin User Name	Admin User Name is set as <i>admin</i> by default, but can be changed, if desired.
Admin Password	This field allows you to specify a new administrator password.
Confirm Admin Password	This field allows you to verify and confirm the new administrator password.

Read-only User Name	Read-only User Name is set as <i>user</i> by default, but can be changed, if desired.
User Password	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.
Confirm User Password	This field allows you to verify and confirm the new user password.
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to 4 hours .
Authentication by RADIUS	With this box is checked, the web admin will authenticate using an external RADIUS server. Authenticated users are treated as either "admin" with full read-write permission or "user" with read-only access. 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. Additional authentication options will be available once this box is checked.
Auth Protocol	This specifies the authentication protocol used. Available options are MS-CHAP v2 and PAP .
Auth Server	This specifies the access address and port of the external RADIUS server.
Auth Server Secret	This field is for entering the secret key for accessing the RADIUS server.
Auth Timeout	This option specifies the time value for authentication timeout.
Accounting Server	This specifies the access address and port of the external accounting server.
Accounting Server Secret	This field is for entering the secret key for accessing the accounting server.
CLI SSH & Console	The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI.
CLI SSH Port	This field determines the port on which clients can access CLI SSH.
CLI SSH Access	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.
Security	This option is for specifying the protocol(s) through which the web admin interface can be accessed: <ul style="list-style-type: none"> <input checked="" type="radio"/> HTTP

	<ul style="list-style-type: none"> ● HTTPS ● HTTP/HTTPS
Web Admin Port	This field is for specifying the port number on which the web admin interface can be accessed.
Web Admin Access	<p>This option is for specifying the network interfaces through which the web admin interface can be accessed:</p> <ul style="list-style-type: none"> ● LAN only ● LAN/WAN <p>If LAN/WAN is chosen, the WAN Connection Access Settings form will be displayed.</p>

5.2 Operating Mode

Operating Mode can be accessed at **System>Operating Mode**. The operating mode can be changed between **Router or Bridge Mode**.

Operating Mode

Select the operating mode you want to use for this device:

Router mode

Bridge mode

Save and Apply

Operating Mode

Operating Mode Your device can act as a bridge or as a router, depending on your selection here.

5.3 Firmware

Pepwave router firmware is upgradeable through the web admin interface. Firmware upgrade functionality is located at **System>Firmware**.

Firmware Upgrade ?

Current firmware version: 1.1.0
No update available

Check for Firmware

Manual Firmware Upgrade ?

Firmware Image No file selected.

Manual Upgrade

There are two ways to upgrade the unit. The first method is through an online download. The second method is to upload a firmware file manually.

To perform an online download, click on the **Check for Firmware** button. The Pepwave router will check online for new firmware. If new firmware is available, the Pepwave router will automatically download the firmware. The rest of the upgrade process will be automatically initiated.

You may also download a firmware image from the Peplink website and update the unit manually. To update using a firmware image, click **Choose File** to select the firmware file from the local computer, and then click **Manual Upgrade** to send the firmware to the Pepwave router. It will then automatically initiate the firmware upgrade process.

Please note that all Peplink devices can 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.

Important Note

The firmware upgrade process may not necessarily preserve the previous configuration, and the behavior varies on a case-by-case basis. Consult the release notes for the particular firmware version before installing. Do not disconnect the power during firmware upgrade process. Do not attempt to upload a non-firmware file or a firmware file that is not supported by Peplink. Upgrading the Pepwave router with an invalid firmware file will damage the unit and may void the warranty.

Important Note

If the firmware is rolled back from 5.x to 4.x, the configurations will be lost.

5.4 Time

Time Settings enables the system clock of the Pepwave router to be synchronized with a specified time server. Time settings are located at **System>Time**.

Time Settings	
Time Zone	(GMT+07:00) Krasnoyarsk <input type="checkbox"/> Show all
Time Server	0.peplink.pool.ntp.org <input type="button" value="Default"/>

Time Settings	
Time Zone	This specifies the time zone (along with the corresponding Daylight Savings Time scheme). The Time Zone value affects the time stamps in the Pepwave router's event log and e-mail notifications. Check Show all to show all time zone options.
Time Server	This setting specifies the NTP network time server to be utilized by the Pepwave router.

5.5 Schedule

Enable and disable different functions (such as WAN connections, outbound policy, and firewalls at different times, based on a user-scheduled configuration profile. The settings for this are located at **System > Schedule**

Schedule

Enabled ✎

Name	Time	Used by	
Weekdays Only	Weekdays only	-	✖

New Schedule

Edit schedule profile ✕

Schedule Settings

Enable The schedule function of those associated features will be lost if profile is disabled.

Name

Schedule

Used by You may go to supported feature settings page and set this profile as scheduler.

Schedule Map

	Midnight	4am	8am	Noon	4pm	8pm
Sunday	x	x	x	x	x	x
Monday	✓	✓	✓	✓	✓	✓
Tuesday	✓	✓	✓	✓	✓	✓
Wednesday	✓	✓	✓	✓	✓	✓
Thursday	✓	✓	✓	✓	✓	✓
Friday	✓	✓	✓	✓	✓	✓
Saturday	x	x	x	x	x	x

Save
Cancel

Edit Schedule Profile	
Enabling	Click this checkbox to enable this schedule profile. Note that if this is disabled, then any associated features will also have their scheduling disabled.
Name	Enter your desired name for this particular schedule profile.
Schedule	Click the drop-down menu to choose pre-defined schedules as your starting point. Please note that upon selection, previous changes on the schedule map will be deleted.

5.6 Email Notification

Email notification functionality provides a system administrator with up-to-date information on network status. The settings for configuring email notifications are found at System>Email Notification.

Email Notification Setup	
Email Notification	<input checked="" type="checkbox"/> Enable
SMTP Server	<input type="text"/> <input type="checkbox"/> Require authentication
SSL Encryption	<input type="checkbox"/> (Note: any server certificate will be accepted)
SMTP Port	25 Default
Sender's Email Address	<input type="text"/>
Recipient's Email Address	<input type="text"/>

Test Email Notification **Save**

Email Notification Settings	
Email Notification	This setting specifies whether or not to enable email notification. If Enable is checked, the Pepwave router will send email messages to system administrators when the WAN status changes or when new firmware is available. If Enable is not checked, email notification is disabled and the Pepwave router will not send email messages.
SMTP Server	This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check Require authentication .

SSL Encryption	Check the box to enable SMTPS. When the box is checked, SMTP Port will be changed to 465 automatically.
SMTP Port	This field is for specifying the SMTP port number. By default, this is set to 25 ; when SSL Encryption is checked, the default port number will be set to 465 . You may customize the port number by editing this field. Click Default to restore the number to its default setting.
SMTP User Name / Password	This setting specifies the SMTP username and password while sending email. These options are shown only if Require authentication is checked in the SMTP Server setting.
Confirm SMTP Password	This field allows you to verify and confirm the new administrator password.
Sender's Email Address	This setting specifies the email address the Pepwave router will use to send reports.
Recipient's Email Address	This setting specifies the email address(es) to which the Pepwave router will send email notifications. For multiple recipients, separate each email addresses using the enter key.

After you have finished setting up email notifications, you can click the **Test Email Notification** button to test the settings before saving. After **Test Email Notification** is clicked, you will see this screen to confirm the settings:

Test Email Notification	
SMTP Server	smtp.mycompany.com
SMTP Port	465
SMTP UserName	smtpuser
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

Click **Send Test Notification** to confirm. In a few seconds, you will see a message with detailed test results.

Test email sent. Email notification settings are not saved, it will be saved after clicked the 'Save' button.

Test Result

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

5.7 Event Log

Event log functionality enables event logging at a specified remote syslog server. The settings for configuring the remote system log can be found at **System>Event Log**.

Send Events to Remote Syslog Server	
Remote Syslog	<input checked="" type="checkbox"/>
Remote Syslog Host	<input type="text"/>
Push Events to Mobile Devices	
Push Events	<input checked="" type="checkbox"/>

Event Log Settings	
Remote Syslog	This setting specifies whether or not to log events at the specified remote syslog server.
Remote Syslog Host	This setting specifies the IP address or hostname of the remote syslog server.
Push Events	<p>The Pepwave router can also send push notifications to mobile devices that have our Mobile Router Utility installed. Check the box to activate this feature.</p> <p>For more information on the Router Utility, go to: www.peplink.com/products/router-utility</p>

5.8 SNMP

SNMP or simple network management protocol is an open standard that can be used to collect information about the Pepwave router. SNMP configuration is located at **System>SNMP**.

SNMP Settings	
SNMP Device Name	DCS-956A
SNMP Port	161 <input type="button" value="Default"/>
SNMPv1	<input type="checkbox"/> Enable
SNMPv2c	<input type="checkbox"/> Enable
SNMPv3	<input type="checkbox"/> Enable
SNMP Trap	<input type="checkbox"/> Enable
<input type="button" value="Save"/>	

Community Name	Allowed Source Network	Access Mode
No SNMPv1 / SNMPv2c Communities Defined		
<input type="button" value="Add SNMP Community"/>		

SNMPv3 User Name	Authentication / Privacy	Access Mode
No SNMPv3 Users Defined		
<input type="button" value="Add SNMP User"/>		

SNMP Settings	
SNMP Device Name	This field shows the router name defined at System>Admin Security .
SNMP Port	This option specifies the port which SNMP will use. The default port is 161 .
SNMPv1	This option allows you to enable SNMP version 1.
SNMPv2	This option allows you to enable SNMP version 2.
SNMPv3	This option allows you to enable SNMP version 3.

5.9 InControl

InControl Management	
InControl Management <input style="float: left; margin-right: 5px;" type="button" value="?"/>	<input checked="" type="checkbox"/> Allow InControl Management
Privately Host InControl	<input type="checkbox"/>

InControl is a cloud-based service which allows you to manage all of your Peplink and Pepwave devices with one unified system. With it, you can generate reports, gather statistics, and configure your devices automatically. All of this is now possible with InControl.

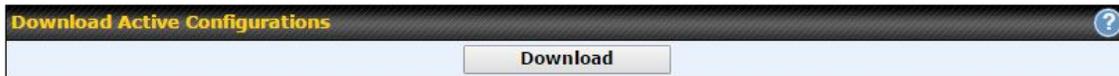
When this check box is checked, the device's status information will be sent to the Peplink InControl system. This device's usage data and configuration will be sent to the system if you enable the features in the system.

Alternately, you could also privately host InControl. Simply check the box beside the "Privately Host InControl" open, and enter the IP Address of your InControl Host.

You can sign up for an InControl account at <https://incontrol2.peplink.com/>. You can register your devices under the account, monitor their status, see their usage reports, and receive offline notifications

5.10 Configuration

Backing up Pepwave router settings immediately after successful completion of initial setup is strongly recommended. The functionality to download and upload Pepwave router settings is found at **System>Configuration**. Note that available options vary by model.



Configuration	
Restore Configuration to Factory Settings	The Restore Factory Settings button is to reset the configuration to factory default settings. After clicking the button, you will need to click the Apply Changes button on the top right corner to make the settings effective.
Download Active Configurations	Click Download to backup the current active settings.
Upload Configurations	To restore or change settings based on a configuration file, click Choose File to locate the configuration file on the local computer, and then click Upload . The new settings can then be applied by clicking the Apply Changes button on the page header, or you can cancel the procedure by pressing discard on the main page of the web admin interface.

5.11 Feature Add-ons

Pepwave devices have features that can be activated upon purchase. Once the purchase is complete, you will receive an activation key. Enter the key in the **Activation Key** field, click **Activate**, and then click **Apply Changes**

5.12 Reboot

This page provides a reboot button for restarting the system. For maximum reliability, the Pepwave router can equip with two copies of firmware. Each copy can be a different version. You can select the firmware version you would like to reboot the device with. The firmware marked with **(Running)** is the current system boot up firmware.

Please note that a firmware upgrade will always replace the inactive firmware partition.

6 Tools

6.1 Ping

The ping test tool sends pings through a specified Ethernet interface or a VPN connection. You can specify the number of pings in the field Number of times, to a maximum number of 10 times. Packet Size can be set to a maximum of 1472 bytes. The ping utility is located at **System>Tools>Ping**, illustrated below:

Ping	
Connection	Wi-Fi WAN 1 ▾
Destination	<input type="text"/>
Packet Size	<input type="text" value="56"/>
Number of times	Times 5 

Results	Clear Log
(Empty)	

Tip

A system administrator can use the ping utility to manually check the connectivity of a particular LAN/WAN connection.

6.2 Traceroute

The traceroute test tool traces the routing path to the destination through a particular Ethernet interface or a SpeedFusion™ connection. The traceroute test utility is located at **System>Tools>Traceroute**.

Peplink routers can send magical Packets

Traceroute	
Connection	WAN 1
Destination	64.233.189.99
<input type="button" value="Start"/> <input type="button" value="Stop"/>	

Results	Clear Log
<pre> Traceroute to 64.233.189.99 (64.233.189.99), 30 hops max, 90 bytes packet size 0 10.0.0.1 [10.0.0.1] 0.700 ms 0.472 ms 0.287 ms 1 10.0.0.254 [10.0.0.254] 0.000 ms 0.000 ms 0.000 ms 2 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms 3 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms 4 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms 5 10.0.0.254 [10.0.0.254] 0.000 ms 0.000 ms 0.000 ms 6 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms 7 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms 8 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms 9 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms 10 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms 11 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms 12 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms 13 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms 14 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms </pre>	

Tip

A system administrator can use the traceroute utility to analyze the connection path of a LAN/WAN connection.

6.3 Wake-on-LAN

Peplink routers can send special “magic packets” to any client specified from the Web UI. To access this feature, navigate to **System>Tools>Wake-on-LAN**.

Wake-on-LAN	
Wake-on-LAN Target	<input type="text" value="Custom MAC Address..."/> <input type="text" value="00:00:00:00:00:00"/> <input type="button" value="Send"/>

Select a client from the drop-down list and click **Send** to send a “magic packet”.

7 PEPVPN

To configure PepVPN and SpeedFusion, navigate to **Advanced>PepVPN**

Profile	Remote ID	Remote Address(es)	
PepVPN Profile 1	Remote_ID		
<input type="button" value="New Profile"/>			

Send All Traffic To
No PepVPN profile selected

Rules Drag and drop rows to change rule order					
Service	Algorithm	Source	Destination	Protocol / Port	
PepVPN Routes					
(Auto)					
<input type="button" value="Add Rule"/>					

Expert Mode
Enabled

PepVPN Local ID
Local ID DCS_956A

PepVPN Settings	
Link Failure Detection Time	<input checked="" type="radio"/> Recommended (Approx. 15 secs) <input type="radio"/> Fast (Approx. 6 secs) <input type="radio"/> Faster (Approx. 2 secs) <input type="radio"/> Extreme (Under 1 sec) Shorter detection time incurs more health checks and higher bandwidth overhead
<input type="button" value="Save"/>	

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

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

All data can be routed over the VPN using the 256-bit AES encryption standard. To configure, navigate to **Advanced>PepVPN** and click the **New Profile** button to create a new VPN profile (you may have to first save the displayed default profile in order to access the **New Profile** button). Each profile specifies the settings for making VPN connection with one remote Pepwave or Peplink device.

Click the **Save** button to create and save a new VPN connection profile for making a VPN connection.

PepVPN Profile Settings	
Name	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ().
Active	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
Encryption	By default, VPN traffic is encrypted with 256-bit AES . If Off is selected on both sides of a VPN connection, no encryption will be applied.

Authentication	Select from By Remote ID Only , Preshared Key . When selecting By Remote ID Only , be sure to enter a unique peer ID number in the Remote ID field.
Remote ID / Pre-shared Key	This optional field becomes available when Remote ID / Pre-shared Key is selected as the Peplink Balance's VPN Authentication method, as explained above. 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. When the peer is running firmware 5.0+, this setting will be ignored.
NAT Mode	Check this box to allow the local DHCP server to assign an IP address to the remote peer. When NAT Mode is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.
Remote IP Address / Host Names (Optional)	If NAT Mode is not enabled, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted. This field is optional. With this field filled, the Peplink Balance will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Peplink Balance will wait for connection from the remote peer. Therefore, at least one of the two VPN peers must specify this value. Otherwise, VPN connections cannot be established.
Data Port	This field is used to specify a UDP port number for transporting outgoing VPN data. If Default is selected, UDP port 4500 will be used. Port 32015 will be used if the remote unit uses Firmware prior to version 5.4 or if port 4500 is unavailable. If Custom is selected, enter an outgoing port number from 1 to 65535.
Bandwidth Limit	Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above.
Cost	Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10

8 Port Forwarding

pepwave device connector can act as a firewall that blocks, by default, all inbound access from the internet. By using port forwarding, Internet users can access servers behind the pepwave router. Inbound port forwarding rules can be defined at **Advanced>Port Forwarding**.

Service	IP Address(es)	Server	Protocol
No Services Defined			
<input type="button" value="Add Service"/>			

To define a new service, click **Add Service**.

Port Forwarding ✕

Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Service Name	<input type="text"/>		
IP Protocol	<input type="text" value="TCP"/>	←	<input type="text" value=":: Protocol Selection Tool ::"/>
Port	<input type="text" value="Any Port"/>		
Inbound IP Address(es) (Require at least one IP address)	<div style="border: 1px solid black; padding: 2px;"> <p>Connection / IP Address(es) All Clear</p> <p><input type="checkbox"/> Wi-Fi WAN 1</p> <p><input type="checkbox"/> Wi-Fi WAN 2</p> <p><input type="checkbox"/> PepVPN</p> </div>		
Server IP Address	<input type="text"/>		

Port Forwarding Settings	
Enable	This setting specifies whether the inbound service takes effect. When Enable is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Pepwave router disregards the other parameters of the rule.
Service Name	This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore “_” characters.
IP Protocol	The IP Protocol setting, along with the Port setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Pepwave router via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the Servers setting. Please see below for details on the Port and Servers settings. Alternatively, the Protocol Selection Tool drop-down menu can be used 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, the protocol and port number remain manually modifiable.
Port	<p>The Port setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:</p> <p>Any Port, Single Port, Port Range, Port Map, and Range Mapping</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> Port <input type="text" value="Any Port"/> </div> <p>Any Port: all traffic that is received by the Pepwave router 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.</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> Port <input type="text" value="Single Port"/> Service Port: 80 </div> <p>Single Port: traffic that is received by the Pepwave router via the specified protocol at the specified port is forwarded via the same port to the servers specified by the Servers</p>

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	Port Range	Service Ports: 80 - 88
------	------------	------------------------

Port Range: traffic that is received by the Pepwave router 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 **Port Range** and **Service Ports** 80-88, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports.

Port	Port Mapping	Service Port: 80	Map to Port: 88
------	--------------	------------------	-----------------

Port Mapping: traffic that is received by Pepwave router 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 Mapping**, **Service Port** 80, and **Map to Port** 88, TCP traffic on port 80 is forwarded to the configured servers via port 88.

(Please see below for details on the **Servers** setting.)

Port	Range Mapping	Service Ports: 80 - 88	Map to Ports: 88 - 96
------	---------------	------------------------	-----------------------

Range Mapping: traffic that is received by the Pepwave router 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 Address(es)	This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.
Server IP Address	This setting specifies the LAN IP address of the server that handles the requests for the service.

9 NAT Mappings

NAT mappings allow IP address mapping of all inbound and outbound NAT traffic to and from an internal client IP address. Settings to configure NAT mappings are located at **Advanced>NAT Mappings**.

LAN Clients	Inbound Mappings	Outbound Mappings
No NAT Mappings Defined		
Add NAT Rule		

To add a rule for NAT mappings, click **Add NAT Rule**.

NAT Mappings ✕

LAN Client(s) ?	IP Address ▼					
Address ?	<input style="width: 100%;" type="text"/>					
Inbound Mappings ?	<div style="background-color: #333; color: #fff; padding: 2px;">Connection / Inbound IP Address(es)</div> <input type="checkbox"/> Wi-Fi WAN 1 <input type="checkbox"/> Wi-Fi WAN 2 <input type="checkbox"/> PepVPN					
Outbound Mappings ?	<div style="background-color: #333; color: #fff; padding: 2px;">Connection / Outbound IP Address</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%;">Wi-Fi WAN 1</td> <td>192.168.98.16 (Interface IP) ▼</td> </tr> <tr> <td>Wi-Fi WAN 2</td> <td>Interface IP ▼</td> </tr> </table>		Wi-Fi WAN 1	192.168.98.16 (Interface IP) ▼	Wi-Fi WAN 2	Interface IP ▼
Wi-Fi WAN 1	192.168.98.16 (Interface IP) ▼					
Wi-Fi WAN 2	Interface IP ▼					

NAT Mapping Settings	
LAN Client(s)	NAT mapping rules can be defined for a single LAN IP Address, an IP Range, or an IP Network.
Address	This refers to the LAN host's private IP address. The system maps this address to a number of public IP addresses (specified below) in order to facilitate inbound and outbound traffic. This option is only available when IP Address is selected.
Inbound Mappings	This setting specifies the WAN connections and corresponding WAN-specific Internet IP addresses on which the system should bind. 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 in the LAN Client(s) field.
Outbound Mappings	This setting specifies the WAN IP addresses that should be used 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).

10 QoS

10.1 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).

Individual Bandwidth Limit					
Enable	<input checked="" type="checkbox"/>				
User Bandwidth Limit	Download		Upload		
	Manager: Unlimited		Unlimited		
	Staff:	0 Mbps	0 Mbps	(0: unlimited)	
	Guest:	0 Mbps	0 Mbps	(0: unlimited)	

10.2 Application

10.2.1 Application Prioritization

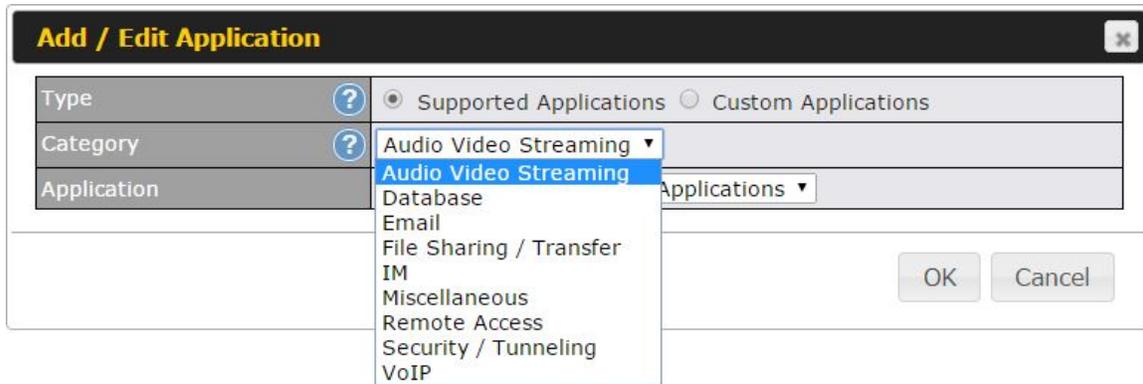
Three application priority levels can be set: **↑High**, **—Normal**, and **↓Low**. Pepwave device connectors can detect various application traffic types by inspecting the packet content. Select an application by choosing a supported application, or by defining a custom application manually. The priority preference of supported applications is placed at the top of the table. Custom applications are at the bottom.

Application	Priority			Action
	Manager	Staff	Guest	
All Supported Streaming Applications	↑ High	— Normal	↑ High	✘
All Email Protocols	↑ High	↑ High	↑ High	✘
MySQL	↑ High	— Normal	↓ Low	✘
SIP	↑ High	↓ Low	↓ Low	✘
Add				

10.2.2 Prioritization for Custom Applications

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

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



10.2.3 DSL/Cable Optimization

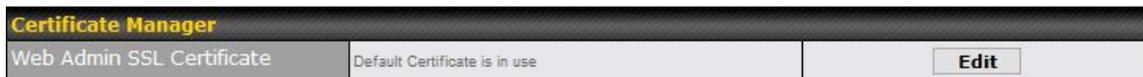
DSL/cable-based WAN connections have lower upload bandwidth and higher download bandwidth. When a DSL/cable circuit's uplink is congested, the download bandwidth will be affected. Users will not be able to download data at full speed until the uplink becomes less congested. **DSL/Cable Optimization** can relieve such an issue. When it is enabled, the download speed will become less affected by the upload traffic. By default, this feature is enabled.



11 Miscellaneous Settings

11.1 Certificate Manager

This section allows you to assign certificates for web admin SSL. The local keys will not be transferred to another device by any means.



12 Status

12.1 Device

System information is located at **Status>Device**

System Information	
Router Name	DCS-956A
Model	Pepwave Device Connector Rugged
Product Code	DCS-RUG
Hardware Revision	1
Serial Number	2933-243F-956A
Firmware	1.1.0s003 build 2258
PepVPN Version	5.0.0
Host Name	dcs-956a
Uptime	54 days 12 hours 43 minutes
System Time	Wed Jan 18 21:26:44 UTC 2017
SpeedFusion WAN Smoothing & Link Load Balancing	Activate
Diagnostic Report	Download
Remote Assistance	Turn on

System Information	
Router Name	This is the name specified in the Router Name field located at System>Admin Security .
Model	This shows the model name and number of this device.
Product Code	If your model uses a product code, it will appear here.
Hardware Revision	This shows the hardware version of this device.
Serial Number	This shows the serial number of this device.
Firmware	This shows the firmware version this device is currently running.
PepVPN Version	This shows the current PepVPN version.
Hostname	The host name assigned to the Pepwave router appears here.
Uptime	This shows the length of time since the device has been rebooted.
System Time	This shows the current system time.

Diagnostic Report	The Download link is for exporting a diagnostic report file required for system investigation.
Remote Assistance	Click Turn on to enable remote assistance.

Interface	MAC Address
LAN	00:1A:DD:0D:4B:E0
Wi-Fi WAN 1	00:1A:DD:0D:4B:E4
Wi-Fi WAN 2	00:1A:DD:0D:4B:E8

The second table shows the MAC address of each LAN/WAN interface connected. To view your device’s End User License Agreement (EULA), click .

Important Note

If you encounter issues and would like to contact the Pepwave Support Team (<http://www.pepwave.com/contact/>), please download the diagnostic report file and attach it along with a description of your issue.

12.2 Client List

The client list table is located at **Status>Client List**. It lists DHCP and online client IP addresses, names (retrieved from the DHCP reservation table or defined by users), current download and upload rate, and MAC address.

Clients can be imported into the DHCP reservation table by clicking the button on the right. You can update the record after import by going to **Network>LAN**.

Filter Online Clients Only DHCP Clients Only

Client List ?					
IP Address ▲	Name	Download (kbps)	Upload (kbps)	MAC Address	Import
192.168.1.100		0	0	00:50:56:99:E1:76	

Scale: kbps Mbps

12.3 PepVPN

PepVPN - Remote Peer Details Show disconnected profiles

Search

Remote Peer ▲	Profile	Information
No information		

Current PepVPN status information is located at **Status>PepVPN**. Click on the corresponding peer name to explore the WAN connection(s) status and subnet information of each VPN peer. Click the button for a chart displaying real-time throughput, latency, and drop-rate information for each WAN connection

12.4 Event Log

Event log information is located at **Status>EventLog**

Device Event Log

Device Event Log		<input checked="" type="checkbox"/> Auto Refresh
Jan 24 18:24:13	WAN: Wi-Fi WAN 2 disconnected	
Jan 24 18:24:13	WAN: Wi-Fi WAN 1 connected to DCR_2.4GHz (192.168.98.16)	
Jan 24 14:02:32	WAN: Wi-Fi WAN 2 connected to DCR_5GHz (192.168.98.12)	
Jan 24 14:02:32	WAN: Wi-Fi WAN 1 standby (192.168.98.16)	
Jan 24 14:02:12	WAN: Wi-Fi WAN 2 disconnected	
Jan 24 14:02:12	WAN: Wi-Fi WAN 1 connected to DCR_2.4GHz (192.168.98.16)	
Jan 24 14:02:03	WAN: Wi-Fi WAN 2 connected to DCR_5GHz (192.168.98.12)	
Jan 24 14:02:03	WAN: Wi-Fi WAN 1 standby (192.168.98.16)	
Jan 24 14:01:37	WAN: Wi-Fi WAN 2 disconnected	
Jan 24 14:01:37	WAN: Wi-Fi WAN 1 connected to DCR_2.4GHz (192.168.98.16)	
Jan 24 14:01:03	WAN: Wi-Fi WAN 2 connected to DCR_5GHz (192.168.98.12)	
Jan 24 14:01:03	WAN: Wi-Fi WAN 1 standby (192.168.98.16)	
Jan 24 14:00:47	WAN: Wi-Fi WAN 2 disconnected	
Jan 24 14:00:47	WAN: Wi-Fi WAN 1 connected to DCR_2.4GHz (192.168.98.16)	
Jan 24 03:28:25	WAN: Wi-Fi WAN 2 connected to DCR_5GHz (192.168.98.12)	
Jan 24 03:28:25	WAN: Wi-Fi WAN 1 standby (192.168.98.16)	
Jan 24 03:28:00	WAN: Wi-Fi WAN 2 disconnected	
Jan 24 03:28:00	WAN: Wi-Fi WAN 1 connected to DCR_2.4GHz (192.168.98.16)	
Jan 24 03:26:20	System: Changes applied	
Jan 24 03:26:18	WAN: Wi-Fi WAN 2 connected to DCR_5GHz (192.168.98.12)	
Jan 24 03:26:18	WAN: Wi-Fi WAN 1 standby (192.168.98.16)	

The log section displays a list of events that has taken place on the Pepwave router. Check **Auto Refresh** to refresh log entries automatically. Click the **Clear Log** button to clear the log.

12.5 Bandwidth

This section shows bandwidth usage statistics and is located at **Status>Bandwidth**. Bandwidth usage at the LAN while the device is switched off (e.g., LAN bypass) is neither recorded nor shown.

12.5.1 Real Time

The **Data transferred since installation** table indicates how much network traffic has been processed by the device since the first bootup. The **Data transferred since last reboot** table indicates how much network traffic has been processed by the device since the last boot up.

Data transferred since installation (Sun Oct 10 05:56:02 PST 2010)

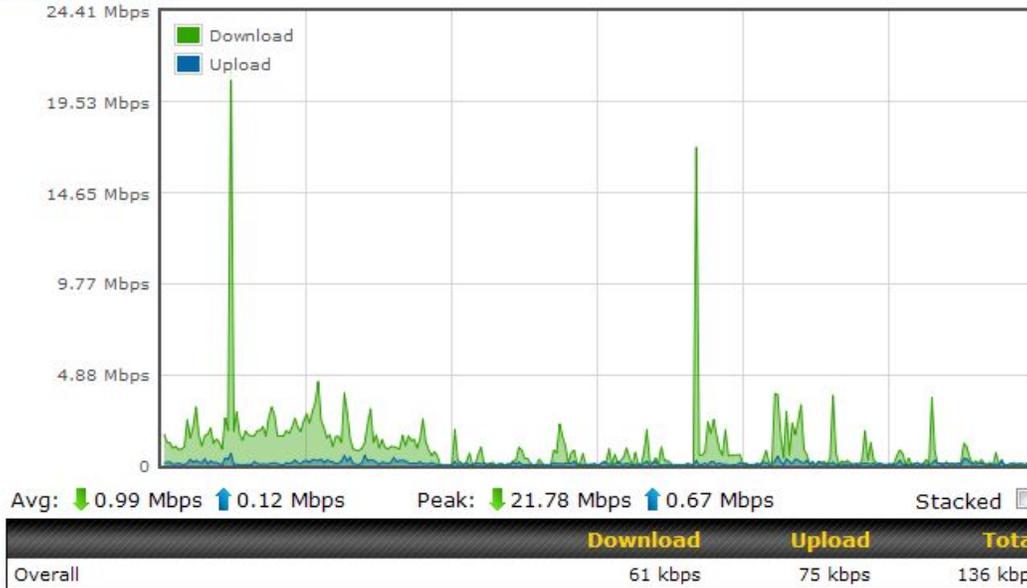
	Download	Upload	Total
All WAN Connections	216.68 GB	91.70 GB	308.38 GB

Data transferred since last reboot

[\[Hide Details \]](#)

	Download	Upload	Total
All WAN Connections	0.74 GB	0.63 GB	1.37 GB
WAN1	0.67 GB	0.61 GB	1.28 GB
WAN2	0.07 GB	0.02 GB	0.09 GB

Aggregated Transfer



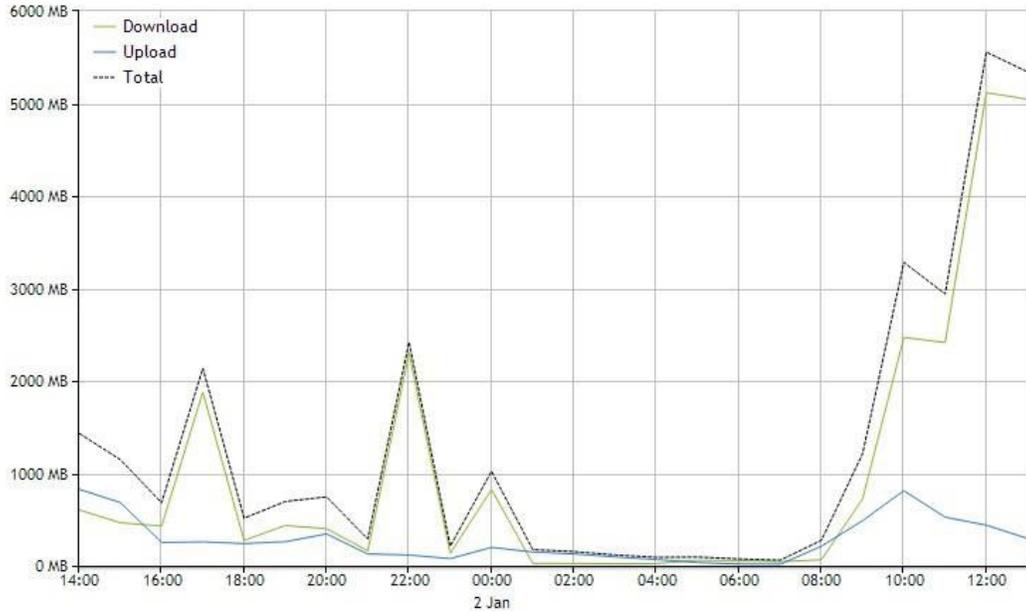
12.5.2 Hourly

This page shows the hourly bandwidth usage for all WAN connections, with the option of viewing each individual connection. Select the desired connection to check from the drop-down menu.

Hourly Usage

Connection: All WAN

Scale: MB GB



Date	Download	Upload	Total
13:00	5 047 MB	295 MB	5 342 MB
12:00	5 117 MB	439 MB	5 556 MB
11:00	2 414 MB	526 MB	2 940 MB
10:00	2 470 MB	812 MB	3 282 MB
09:00	725 MB	488 MB	1 213 MB
08:00	64 MB	211 MB	275 MB

12.5.3 Daily

This page shows the daily bandwidth usage for all WAN connections, with the option of viewing each individual connection.

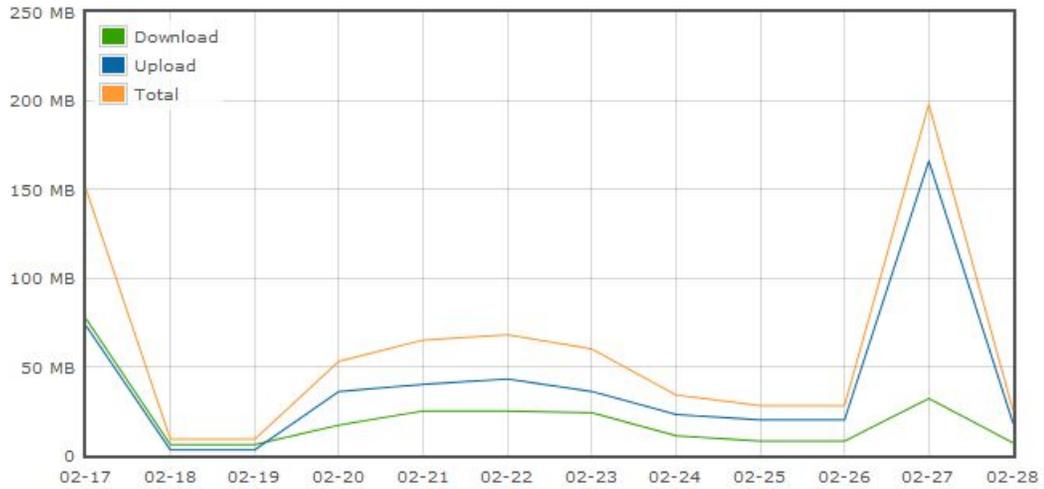
Select the connection to check from the drop-down menu. If you have enabled the **Bandwidth Monitoring** feature, the **Current Billing Cycle** table for that WAN connection will be displayed.

Click on a date to view the client bandwidth usage of that specific date. This feature is not available if you have selected to view the bandwidth usage of only a particular WAN connection. The scale of the graph can be set to display megabytes (**MB**) or gigabytes (**GB**).

Daily Usage

Connection: All WAN

Scale: MB GB

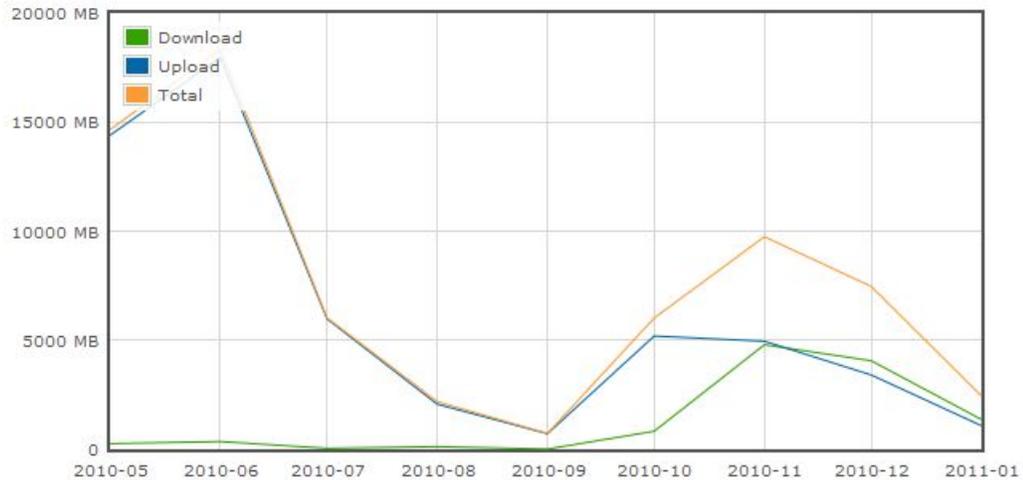


Date	Download	Upload	Total
2012-02-28	7 MB	18 MB	25 MB
2012-02-27	32 MB	166 MB	198 MB
2012-02-26	8 MB	20 MB	28 MB
2012-02-25	8 MB	20 MB	28 MB
2012-02-24	11 MB	23 MB	34 MB
2012-02-23	24 MB	36 MB	60 MB
2012-02-22	25 MB	43 MB	68 MB
2012-02-21	25 MB	40 MB	65 MB
2012-02-20	17 MB	36 MB	53 MB
2012-02-19	6 MB	3 MB	9 MB
2012-02-18	6 MB	3 MB	9 MB
2012-02-17	77 MB	73 MB	150 MB

Current Month	
Down	249 MB
Up	489 MB
Total	738 MB

12.5.4 Monthly

Monthly Usage	
Connection	All WAN
Scale	<input checked="" type="radio"/> MB <input type="radio"/> GB



Date	Download	Upload	Total
2011-01-01 to now	1 367 MB	1 081 MB	2 448 MB
2010-12-01 to 2010-12-31	4 059 MB	3 408 MB	7 467 MB
2010-11-01 to 2010-11-30	4 792 MB	4 952 MB	9 744 MB
2010-10-01 to 2010-10-31	825 MB	5 183 MB	6 008 MB

Client Bandwidth Usage (2010-12-01 to 2010-12-31)				
IP Address	Type	Download	Upload	Total
10.10.10.103	LAN Client	1.54 MB	1 412.51 MB	1 414.05 MB
192.168.50.150	LAN Client	490.46 MB	20.87 MB	511.33 MB
59.115.100.40	LAN Client	0.00 MB	141.63 MB	141.63 MB
203.186.47.43	LAN Client	0.00 MB	131.22 MB	131.22 MB
91.189.92.170	LAN Client	0.00 MB	58.04 MB	58.04 MB

All WAN Monthly Bandwidth Usage

Restoration of Factory Defaults

To restore the factory default settings on a Pepwave Device Connector Rugged, follow the steps below:

1. Locate the reset button on the front or back panel of the Pepwave Device Connector Rugged router.
2. With a paperclip, press and keep the reset button pressed.

Note: There is a dual function to the reset button.

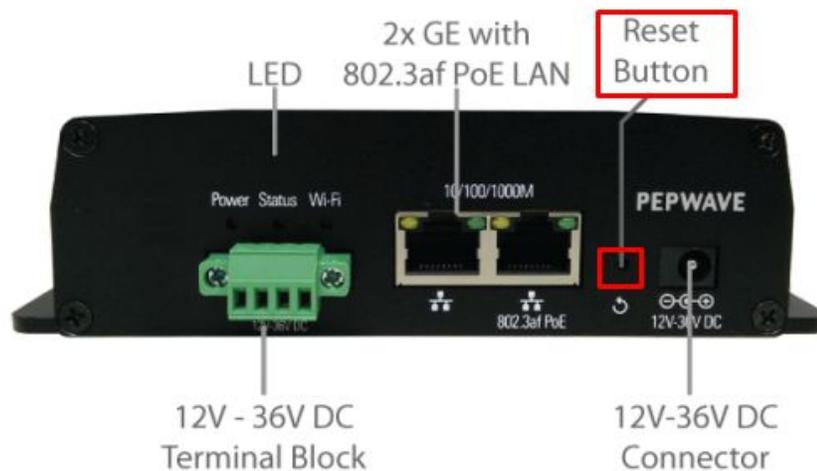
Hold for 5-10 seconds for admin password reset (Note: The LED status light blinks in RED 2 times and release the button, green status light starts blinking)

Hold for approximately 20 seconds for factory reset (Note: The LED status light blinks in RED 3 times and release the button, all WAN/LAN port lights start blinking)

After the Pepwave Device Connector Rugged finishes rebooting, the factory default settings will be restored.

Important Note

All previous configurations and bandwidth usage data will be lost after restoring factory default settings. Regular backup of configuration settings is strongly recommended.



Appendix

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- 1) Reorient or relocate the receiving antenna.
- 2) Increase the separation between the equipment and receiver.
- 3) Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4) Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE: FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Taiwan NCC Statement

經型式認證合格之低功率射頻電機,非經許可,公司、商號或使用者均不得擅自 變更 頻率、加大功率或變更原設計之特性及功能
低功率射頻電機之使用不得影響飛航安全及干擾合法通信;經發現有干擾現象時,應改善至無干擾時方得繼續使用。前項合法通信,指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Copyright

Copyright © 2016 Peplink

The content of this documentation may not be reproduced in any part or as a whole without the prior written permission of Peplink.

Disclaimer

Peplink does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent right nor the patent rights of others. Peplink further reserves the right to make changes in any products described herein without notice. This documentation is subject to change without notice.