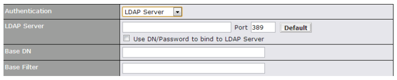
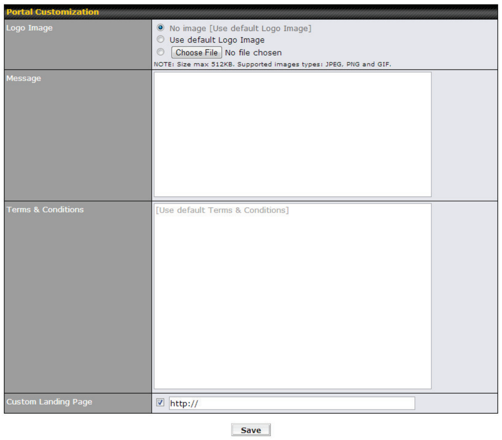
LDAP Server	This authenticates your clients through a LDAP server. Upon selecting this option, you will see the following fields:  Authentication: LDAP Server LDAP Server: Port 389 Default □ Use DN/Password to bind to LDAP Server Base DN Base Filter Fill in the necessary information to complete your connection to the server and enable authentication.
Access Quota	Set a time and data cap to each user's Internet usage.
Quota Reset Time	This menu determines how your usage quota resets. Setting it to **Daily** will reset it at a specified time every day. Setting a number of **minutes after quota reached** establish a timer for each user that begins after the quota has been reached.
Allowed Networks	To whitelist a network, enter the domain name / IP address here and click ➕. To delete an existing network from the list of allowed networks, click the ✖ button next to the listing.
Splash Page	Here, you can choose between using the Pepwave router's built-in captive portal and redirecting clients to a URL you define.

The **Portal Customization** menu has two options: Preview and ✎. Clicking Preview displays a pop-up previewing the captive portal that your clients will see. Clicking ✎ displays the following menu:



Portal Customization

Logo Image: ● No image [Use default Logo Image] ○ Use default Logo Image ○ Choose File No file chosen

NOTE: Size max 512KB. Supported images types: JPEG, PNG and GIF.

Message

Terms & Conditions: [Use default Terms & Conditions]

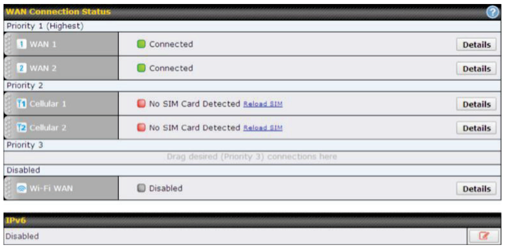
Custom Landing Page: ☑ http://

Save

Portal Customization	
Logo Image	Click the **Choose File** button to select a logo to use for the built-in portal.
Message	If you have any additional messages for your users, enter them in this field.
Terms & Conditions	If you would like to use your own set of terms and conditions, please enter them here. If left empty, the built-in portal will display the default terms and conditions.
Custom Landing Page	Fill in this field to redirect clients to an external URL.

10 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.



WAN Connection Status

Priority 1 (Highest)

1 WAN 1	🟩 Connected	Details
2 WAN 2	🟩 Connected	Details

Priority 2

1 Cellular 1	🟥 No SIM Card Detected Reload SIM	Details
2 Cellular 2	🟥 No SIM Card Detected Reload SIM	Details

Priority 3

Drag desired (Priority 3) connections here

Disabled

Wi-Fi WAN	Disabled	Details

IPv6

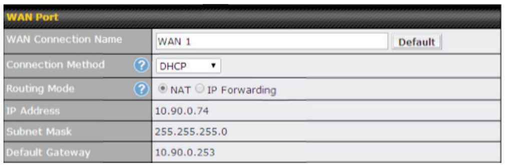
Disabled

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.

10.1 Ethernet WAN

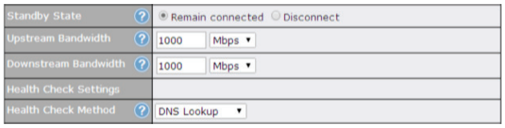
From **Network>WAN,** choose a WAN connection and then click **Details**.



WAN Port

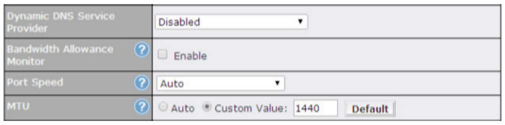
WAN Connection Name	WAN 1 Default
Connection Method	DHCP
Routing Mode	● NAT ○ IP Forwarding
IP Address	10.90.0.74
Subnet Mask	255.255.255.0
Default Gateway	10.90.0.253

WAN Port (Section 1)	
WAN Connection Name	Enter a name to represent this WAN connection.
Connection Method	There are three possible connection methods for Ethernet WAN: • **DHCP** • **Static IP** • **PPPoE** The connection method and details are determined by, and can be obtained from, the ISP. See the following sections for details on each connection method.
Routing Mode	This field shows that **NAT** (network address translation) will be applied to the traffic routed over this WAN connection. **IP Forwarding** is available when you click the link in the help text.
IP Address/Subnet Mask/Default Gateway	Enter the WAN IP address and subnet mask, as well as the IP address of the default gateway, in these fields.



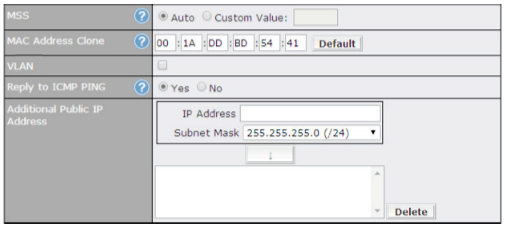
Standby State	● Remain connected ○ Disconnect
Upstream Bandwidth	1000 Mbps
Downstream Bandwidth	1000 Mbps
Health Check Settings	
Health Check Method	DNS Lookup

WAN Port (Section 2)	
Standby State	This setting specifies the standby state of the WAN connection. The available options are **Remain connected** and **Disconnect**. The default state is **Remain Connected**.
Upstream Bandwidth	This setting specifies the data bandwidth in the outbound direction from the LAN through the WAN interface.
Downstream Bandwidth	This setting specifies the data bandwidth in the inbound direction from the WAN interface to the LAN. This value is referenced as the default weight value when using the algorithm **Least Used** or the algorithm **Persistence (Auto)** in outbound policy with **Managed by Custom Rules** chosen (see **Section 15.2**).
Health Check Method	This setting specifies the health check method for the WAN connection. The value of method can be configured as **Disabled**, **Ping**, **DNS Lookup**, or **HTTP**. The default method is **Disabled**. See **Section 10.4** for configuration details.



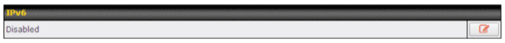
Dynamic DNS Service Provider	Disabled
Bandwidth Allowance Monitor	□ Enable
Port Speed	Auto
MTU	○ Auto ● Custom Value: 1440 Default

WAN Port (Section 3)	
Dynamic DNS Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: • changeip.com • dyndns.org • no-ip.org • tzo.com • DNS-O-Matic Select **Disabled** to disable this feature. See **Section 9.5** for configuration details.
Bandwidth Allowance Monitor	This option enables bandwidth usage monitoring on this WAN connection for each billing cycle. When this setting is not enabled, each month's bandwidth usage is tracked, but no action will be taken.
Port Speed	This setting specifies port speed and duplex configurations of the WAN port. By default, **Auto** is selected and the appropriate data speed is automatically detected by the Pepwave router. In the event of negotiation issues, the port speed can be manually specified. You can also choose whether or not to advertise the speed to the peer by selecting the **Advertise Speed** checkbox.
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. Auto-detection will run each time the WAN connection establishes.



MSS	● Auto ○ Custom Value:
MAC Address Clone	00 : 1A : DD : BD : 54 : 41 Default
VLAN	□
Reply to ICMP PING	● Yes ○ No
Additional Public IP Address	IP Address Subnet Mask 255.255.255.0 (/24) ↓ Delete

WAN Port (Section 4)	
MSS	This setting should be configured based on 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. By default, MSS is set to **Auto**.
MAC Address Clone	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 such cases, change the WAN interface's MAC address to the original client PC's MAC address via this field. The default MAC address is a unique value assigned at the factory. In most cases, the default value is sufficient. Clicking **Default** restores the MAC address to the default value.
VLAN	Click the square if you wish to enable VLAN functionality and enable multiple broadcast domains. Once you enable VLAN, you will be able to enter a name for your network.
Reply to ICMP PING	If this field is disabled, the WAN connection will not respond to ICMP ping requests. By default, this is **enabled**.
Additional Public IP Address	The **IP Address** list represents the list of fixed Internet IP addresses assigned by the ISP, in the event that more than one Internet IP address is assigned to this WAN connection. Enter the fixed Internet IP addresses and the corresponding subnet mask, and then click the **Down Arrow** button to populate IP address entries to the **IP Address** List.



IPv6
Disabled

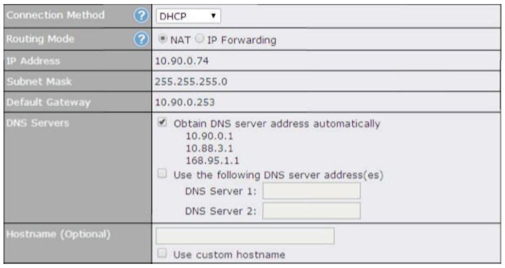
IPv6	
IPv6	IPv6 support can be enabled on one of the available Ethernet WAN ports. On this screen, you can choose which WAN will support IPv6. To enable IPv6 support on a WAN, the WAN router must respond to stateless address auto configuration advertisements and DHCPv6 requests. IPv6 clients on the LAN will acquire their IPv6, gateway, and DNS server addresses from it. The device will also acquire an IPv6 address for performing ping/traceroute checks and accepting web admin accesses. Note: This feature is only available on the Pepwave MAX 700, HD2, and HD2 IP67.

10.1.1 DHCP Connection

There are three possible connection methods:

1. DHCP
2. Static IP
3. PPPoE

The DHCP connection method is suitable if the ISP provides an IP address automatically using DHCP (e.g., satellite modem, WiMAX modem, cable, Metro Ethernet, etc.).



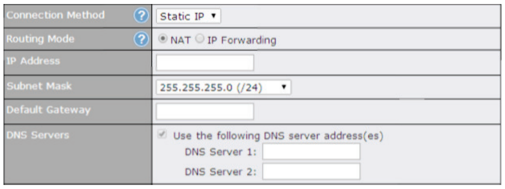
Connection Method	DHCP
Routing Mode	● NAT ○ IP Forwarding
IP Address	10.90.0.74
Subnet Mask	255.255.255.0
Default Gateway	10.90.0.253
DNS Servers	☑ Obtain DNS server address automatically 10.90.0.1 10.88.3.1 168.95.1.1 □ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
Hostname (Optional)	□ Use custom hostname

DHCP Connection Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
IP Address/ Subnet Mask/ Default	This information is obtained from the ISP automatically.

Gateway	
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be 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 here. If your service provider does not provide you with the value, you can safely bypass this option.

10.1.2 Static IP Connection

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

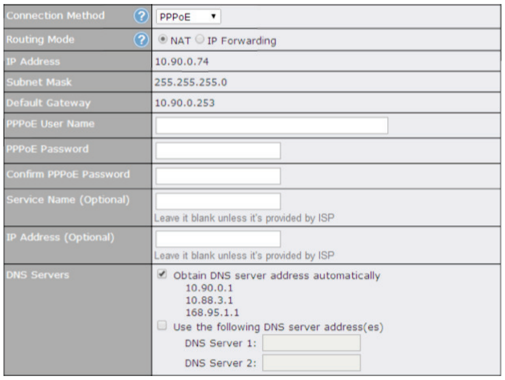


Connection Method	Static IP ▾
Routing Mode	● NAT ○ IP Forwarding
IP Address	
Subnet Mask	255.255.255.0 (/24) ▾
Default Gateway	
DNS Servers	☑ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

Static IP Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
IP Address / Subnet Mask / Default Gateway	These settings allow you to specify the information required in order to communicate on the Internet via a fixed Internet IP address. The information is typically determined by and can be obtained from the ISP.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be 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.

10.1.3 PPPoE Connection

This connection method is suitable if your ISP provides a login ID/password to connect via PPPoE.



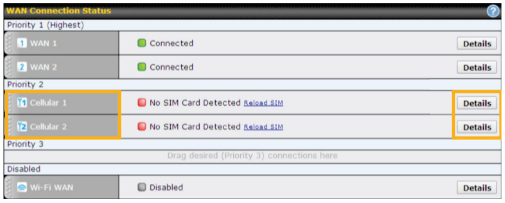
Connection Method	PPPoE ▾
Routing Mode	● NAT ○ IP Forwarding
IP Address	10.90.0.74
Subnet Mask	255.255.255.0
Default Gateway	10.90.0.253
PPPoE User Name	
PPPoE Password	
Confirm PPPoE Password	
Service Name (Optional)	Leave it blank unless it's provided by ISP
IP Address (Optional)	Leave it blank unless it's provided by ISP
DNS Servers	☑ Obtain DNS server address automatically 10.90.0.1 10.88.3.1 168.95.1.1 ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

PPPoE Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
IP Address / Subnet Mask / Default Gateway	This information is obtained from the ISP automatically.
PPPoE User Name / Password	Enter the required information in these fields in order to connect via PPPoE to the ISP. The parameter values are determined by and can be obtained from the ISP.
Confirm PPPoE Password	Verify your password by entering it again in this field.
Service Name (Optional)	Service name is provided by the ISP. **Note: Leave this field blank unless it is provided by your ISP**.
IP Address (Optional)	If your ISP provides a PPPoE IP address, enter it here. **Note: Leave this field blank unless it is provided by your ISP**.

DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be 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.

10.2 Cellular WAN

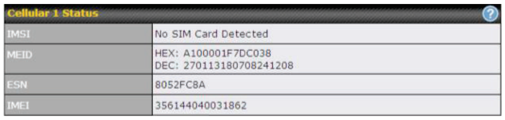
To access cellular WAN settings, click **Network>WAN>Details**.



WAN Connection Status

Priority 1 (Highest)		
1 WAN 1	🟩 Connected	Details
2 WAN 2	🟩 Connected	Details
Priority 2		
1 Cellular 1	🟥 No SIM Card Detected Reload SIM	Details
2 Cellular 2	🟥 No SIM Card Detected Reload SIM	Details
Priority 3		
	Drag desired (Priority 3) connections here	
Disabled		
Wi-Fi WAN	■ Disabled	Details

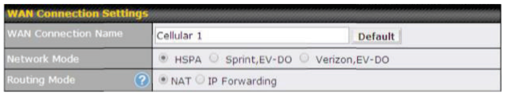
(**Available on the Pepwave MAX BR1, HD2, and HD2 IP67 only)**



Cellular 1 Status

IMSI	No SIM Card Detected
MEID	HEX: A100001F7DC038 DEC: 270113180708241208
ESN	8052FC8A
IMEI	356144040031862

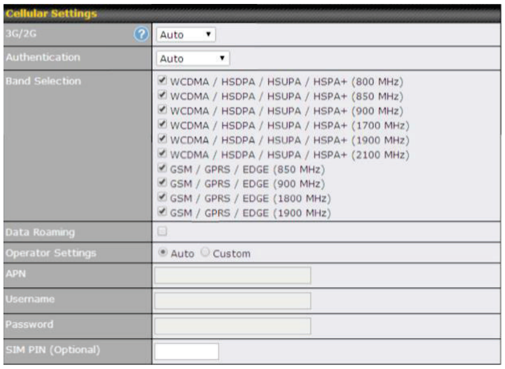
Cellular Status	
IMSI	This is the International Mobile Subscriber Identity which uniquely identifies the SIM card. This is applicable to 3G modems only.
MEID	Some Pepwave routers support both HSPA and EV-DO. For Sprint or Verizon Wireless EV-DO users, a unique MEID identifier code (in hexadecimal format) is used by the carrier to associate the EV-DO device with the user. This information is presented in hex and decimal format.
ESN	This serves the same purpose as MEID HEX but uses an older format.
IMEI	This is the unique ID for identifying the modem in GSM/HSPA mode.



WAN Connection Settings

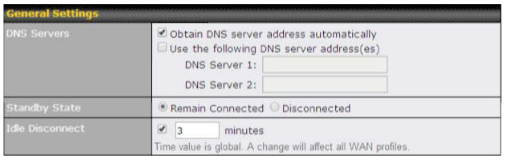
WAN Connection Name	Cellular 1 Default
Network Mode	● HSPA ○ Sprint,EV-DO ○ Verizon,EV-DO
Routing Mode	● NAT ○ IP Forwarding

WAN Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Network Mode	Users have to specify the network they are on accordingly.
Routing Mode	This option allows you to select the routing method to be used in routing IP frames via the WAN connection. The mode can be either **NAT** (network address translation) or **IP Forwarding**. Click the ? button to enable IP forwarding.



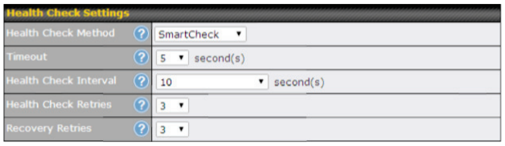
Cellular Settings	
3G/2G	Auto ▾
Authentication	Auto ▾
Band Selection	☑ WCDMA / HSDPA / HSUPA / HSPA+ (800 MHz) ☑ WCDMA / HSDPA / HSUPA / HSPA+ (850 MHz) ☑ WCDMA / HSDPA / HSUPA / HSPA+ (900 MHz) ☑ WCDMA / HSDPA / HSUPA / HSPA+ (1700 MHz) ☑ WCDMA / HSDPA / HSUPA / HSPA+ (1900 MHz) ☑ WCDMA / HSDPA / HSUPA / HSPA+ (2100 MHz) ☑ GSM / GPRS / EDGE (850 MHz) ☑ GSM / GPRS / EDGE (900 MHz) ☑ GSM / GPRS / EDGE (1800 MHz) ☑ GSM / GPRS / EDGE (1900 MHz)
Data Roaming	□
Operator Settings	● Auto ○ Custom
APN	
Username	
Password	
SIM PIN (Optional)	

Cellular Settings	
3G/2G	This drop-down menu allows restricting cellular to particular band. Click the ? button to enable the selection of specific bands.
Authentication	Choose from **PAP Only** or **CHAP Only** to use those authentication methods exclusively. Select **Auto** to automatically choose an authentication method.
Data Roaming	This checkbox enables data roaming on this particular SIM card. Please check your service provider's data roaming policy before proceeding.
Operator Settings	This setting applies to 3G/EDGE/GPRS modems only. It does not apply to EVDO/EVDO Rev. A modems. This allows you to configure the APN settings of your connection. If **Auto** is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making connection, you may select **Custom** to enter your carrier's **APN**, **Login**, **Password**, and **Dial Number** settings manually. The correct values can be obtained from your carrier. The default and recommended setting is **Auto**.
APN / Login / Password / SIM PIN	When **Auto** is selected, the information in these fields will be filled automatically. Select **Custom** to customize these parameters. The parameter values are determined by and can be obtained from the ISP.



General Settings	
DNS Servers	☑ Obtain DNS server address automatically □ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
Standby State	● Remain Connected ○ Disconnected
Idle Disconnect	☑ 3 minutes Time value is global. A change will affect all WAN profiles.

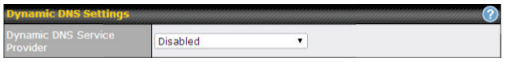
General Settings	
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be 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.
Standby State	This option allows you to choose whether to remain connected or disconnected when this WAN connection is no longer in the highest priority and has entered the standby state. When **Remain connected** is chosen, bringing up this WAN connection to active makes it immediately available for use.
Idle Disconnect	When Internet traffic is not detected within the user-specified timeframe, the modem will automatically disconnect. Once the traffic is resumed by the LAN host, the connection will be re-activated.



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

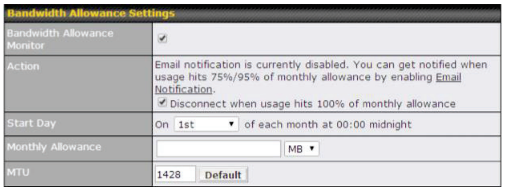
Health Check Settings	
Heath Check Method	This setting allows you to specify the health check method for the cellular connection. Available options are **Disabled**, **Ping**, **DNS Lookup**, **HTTP**, and **SmartCheck**. The default method is **DNS Lookup**. See **Section 10.4** for configuration details.
Timeout	If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.
Health Check	This is the time interval between each health check test.

Interval	
Health Check Retries	This is the number of consecutive check failures before treating a connection as down.
Recovery Retries	This is the number of responses required after a health check failure before treating a connection as up again.



Dynamic DNS Settings	
Dynamic DNS Service Provider	Disabled ▾

Dynamic DNS Settings	
Dynamic DNS Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: • changeip.com • dyndns.org • no-ip.org • tzo.com • DNS-O-Matic Select **Disabled** to disable this feature. See **Section 9.5** for configuration details.



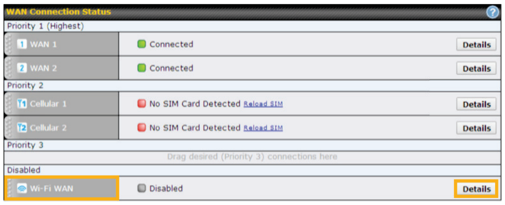
Bandwidth Allowance Settings	
Bandwidth Allowance Monitor	☑
Action	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification. ☑ Disconnect when usage hits 100% of monthly allowance
Start Day	On 1st ▾ of each month at 00:00 midnight
Monthly Allowance	MB ▾
MTU	1428 Default

Bandwidth Allowance Settings	
Bandwidth Allowance Monitor	This option allows you to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this is not enabled, bandwidth usage of each month is still being tracked, but no action will be taken.
Action	If email notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If **Disconnect when usage hits 100% of monthly allowance** is checked, this WAN connection will be disconnected automatically when the usage hits the

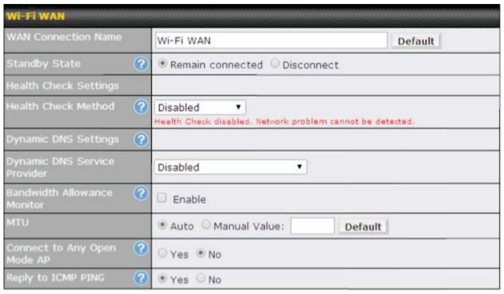
	monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.
Start Day	This option allows you to define which day of the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.
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.

10.3 Wi-Fi WAN

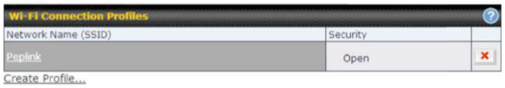
To access Wi-Fi WAN settings, click **Network>WAN>Details**.



WAN Connection Status		
Priority 1 (Highest)		
1 WAN 1	🟩 Connected	Details
2 WAN 2	🟩 Connected	Details
Priority 2		
1 Cellular 1	🟥 No SIM Card Detected Reload SIM	Details
2 Cellular 2	🟥 No SIM Card Detected Reload SIM	Details
Priority 3		
	Drag desired (Priority 3) connections here	
Disabled		
Wi-Fi WAN	■ Disabled	Details



Wi-Fi WAN	
WAN Connection Name	Wi-Fi WAN [Default]
Standby State	● Remain connected ○ Disconnect
Health Check Settings	
Health Check Method	Disabled ▾ Health Check disabled. Network problem cannot be detected.
Dynamic DNS Settings	
Dynamic DNS Service Provider	Disabled ▾
Bandwidth Allowance Monitor	□ Enable
MTU	● Auto ○ Manual Value: [Default]
Connect to Any Open Mode AP	○ Yes ● No
Reply to ICMP PING	● Yes ○ No



Wi-Fi Connection Profiles		
Network Name (SSID)	Security	
Peplink	Open	✕

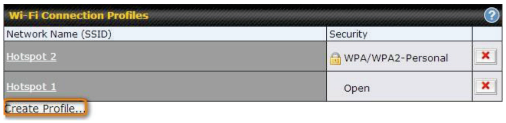
Create Profile...

Wi-Fi WAN 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).
Health Check Method	This setting allows you to specify the health check method for the WAN connection. The available options are **Disabled**, **Ping**, **DNS Lookup**, and **HTTP**. The default method is **Disabled**. See **Section 10.4** for configuration details.
Dynamic DNS Settings/Dynamic DNS Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: • changeip.com • dyndns.org • no-ip.org • tzo.com • DNS-O-Matic Select **Disabled** to disable this feature. See **Section 9.5** for configuration details.
Bandwidth	This option allows you to enable bandwidth usage monitoring on this WAN connection for

Allowance Monitor	each billing cycle. When this is not enabled, bandwidth usage each month is still being tracked, but no action will be taken.
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
Connect to Any Open Mode AP	This option is to specify whether the Wi-Fi WAN will connect to any open mode access point it finds. By default, this is disabled.
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.

10.3.1 Creating Wi-Fi Connection Profiles

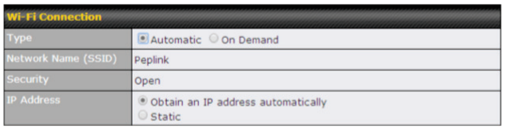
You can manually create a profile to connect to a Wi-Fi connection. This is useful for creating a profile for connecting to hidden-SSID access points. Click **Network>WAN>Details>Create Profile…** to get started.



Wi-Fi Connection Profiles		
Network Name (SSID)	Security	
Hotspot 2	WPA/WPA2-Personal	✕
Hotspot 1	Open	✕

Create Profile...

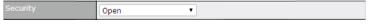
This will open a window similar to the one shown below:



Wi-Fi Connection	
Type	● Automatic ○ On Demand
Network Name (SSID)	Peplink
Security	Open
IP Address	● Obtain an IP address automatically ○ Static

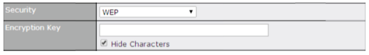
Wi-Fi Connection Profile Settings	
Type	Select whether the network will connect automatically or manually.
Network Name (SSID)	Enter a name to represent this Wi-Fi connection.
Security	This option allows you to select which security policy is used for this wireless network. Available options:

- **Open**



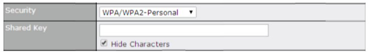
Security	Open ▾

- **WEP**



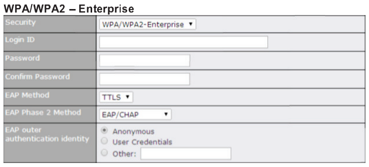
Security	WEP ▾
Encryption Key	☑ Hide Characters

- **WPA/WPA2 – Personal**



Security	WPA/WPA2-Personal ▾
Shared Key	☑ Hide Characters

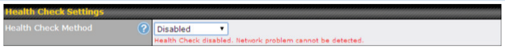
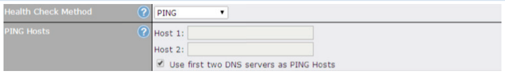
- **WPA/WPA2 – Enterprise**

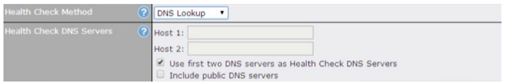
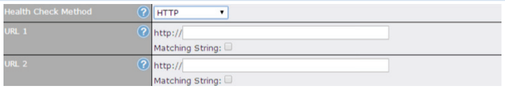


Security	WPA/WPA2-Enterprise ▾
Login ID	
Password	
Confirm Password	
EAP Method	TTLS ▾
EAP Phase 2 Method	EAP/CHAP ▾
EAP outer authentication identity	● Anonymous ○ User Credentials ○ Other:

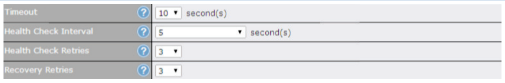
10.4 WAN Health Check

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 Settings Health Check Method: Disabled ▾ 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: PING ▾ PING Hosts: Host 1: Host 2: ☑ 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: DNS Lookup ▾ Health Check DNS Servers: Host 1: Host 2: ☑ Use first two DNS servers as Health Check DNS Servers □ 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:// Matching String: □ URL 2: http:// Matching String: □ 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	10 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 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.**

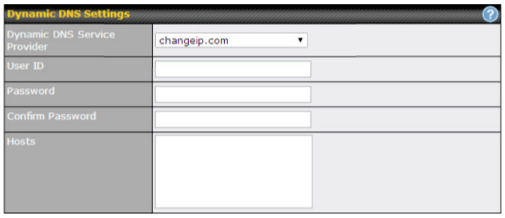
10.5 Dynamic DNS Settings

Pepwave routers are capable of registering 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 host name. With dynamic DNS service enabled for a WAN connection, you can connect to your WAN's IP address from the external, even if its IP address is dynamic. You must register for an account from the listed dynamic DNS service providers before enabling this option.

If the WAN connection's IP address is a reserved private IP address (i.e., behind a NAT router), the public IP of each WAN will be automatically reported to the DNS service provider.

Either upon a change in IP addresses or every 23 days without link reconnection, the Pepwave router will connect to the dynamic DNS service provider to perform an IP address update within the provider's records.

The settings for dynamic DNS service provider(s) and the association of hostname(s) are configured via **Network>WAN>Details>Dynamic DNS Service Provider/Dynamic DNS Settings**.



Dynamic DNS Settings

Dynamic DNS Service Provider	changeip.com
User ID	
Password	
Confirm Password	
Hosts	

Dynamic DNS Settings

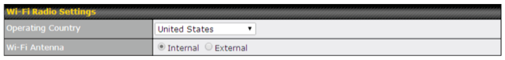
Dynamic DNS	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: • changeip.com • dyndns.org • no-ip.org • tzo.com • DNS-O-Matic Select **Disabled** to disable this feature.
Account Name / Email Address	This setting specifies the registered user name for the dynamic DNS service.
Password / TZO Key	This setting specifies the password for the dynamic DNS service.
Hosts / Domain	This field allows you to specify a list of host names or domains to be associated with the public Internet IP address of the WAN connection. If you need to enter more than one host, use a carriage return to separate them.

Important Note

In order to use dynamic DNS services, appropriate host name registration(s) and 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., the 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. Therefore the Pepwave router performs an update every 23 days, even if a WAN's IP address has not changed.

11 Advanced Wi-Fi Settings

Wi-Fi settings can be configured at **Advanced>Wi-Fi Settings** (or **AP>Settings** on some models). Note that menus displayed can vary by model.



Wi-Fi Radio Settings

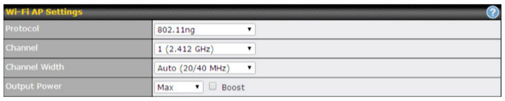
Operating Country	United States
Wi-Fi Antenna	● Internal ○ External

Wi-Fi Radio Settings

Operating Country	This drop-down menu specifies the national/regional regulations which the Wi-Fi radio should follow. • If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW). • If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). NOTE: Users are required to choose an option suitable to local laws and regulations.
Wi-Fi Antenna	This setting determines whether the Wi-Fi radio will use its internal antenna or rely on an outside one installed on its SMA or Type-N connectors.

Important Note

Per FCC regulation, 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

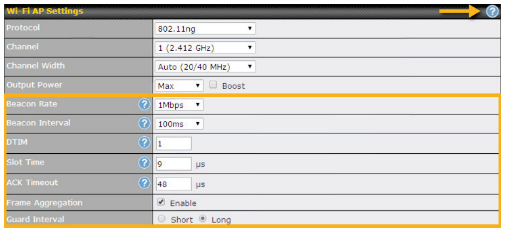
Protocol	802.11ng
Channel	1 (2.412 GHz)
Channel Width	Auto (20/40 MHz)
Output Power	Max □ Boost

Wi-Fi AP Settings

Protocol	This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are **802.11ng** and **802.11na**. By default, **802.11ng** is selected.
Channel	This option allows you to select which 802.11 RF channel will be utilized. **Channel 1 (2.412 GHz)** is selected by default.
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.
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.

Advanced Wi-Fi AP settings can be displayed by clicking the ? on the top right-hand

corner of the **Wi-Fi AP Settings** section, which can be found at **AP>Settings**. Other models will display a separate section called **Wi-Fi AP Advanced Settings**, which can be found at **Advanced>Wi-Fi Settings**.



Wi-Fi AP Settings

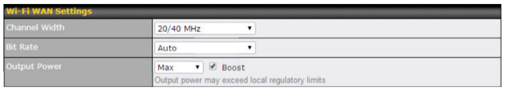
Protocol	802.11ng
Channel	1 (2.412 GHz)
Channel Width	Auto (20/40 MHz)
Output Power	Max □ Boost
Beacon Rate	1Mbps
Beacon Interval	100ms
DTIM	1
Slot Time	9 μs
ACK Timeout	48 μs
Frame Aggregation	☑ Enable
Guard Interval	○ Short ● Long

Wi-Fi AP Advanced Settings

Beacon Rate	This option is for setting the transmit bit rate for sending a beacon. By default, **1Mbps** is selected.
Beacon Interval	This option is for setting the time interval between each beacon. By default, **100ms** is selected.
DTIM	This field allows you to set the frequency for the beacon to include delivery traffic indication messages. The interval is measured in milliseconds. The default value is set to **1 ms**.
Slot Time	This field is for specifying the unit wait time before transmitting a packet. By default, this field is set to **9 μs**.
ACK Timeout	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	This option allows you to enable frame aggregation to increase transmission throughput.
Guard Interval	This is where you opt for a short or long guard period interval for your transmissions.

Wi-Fi WAN settings can be configured at **Advanced>Wi-Fi Settings** (or

Advanced>Wi-Fi WAN or some models).



Wi-Fi WAN Settings	
Channel Width	20/40 MHz ▾
Bit Rate	Auto ▾
Output Power	Max ▾ ☑ Boost Output power may exceed local regulatory limits

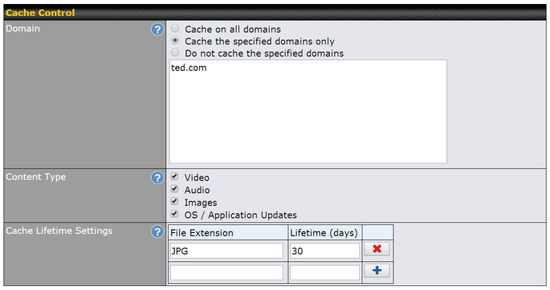
Wi-Fi WAN Settings	
Channel Width	Available options are **20/40 MHz** and **20 MHz**. Default is **20/40 MHz**, which allows both widths to be used simultaneously.
Bit Rate	This option allows you to select a specific bit rate for data transfer over the device's Wi-Fi network. By default, **Auto** is 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.

12 MediaFast Configuration

MediaFast settings can be configured from the **Network** menu.

12.1 Setting Up MediaFast Content Caching

To access MediaFast content caching settings, select **Advanced>Cache Control**.

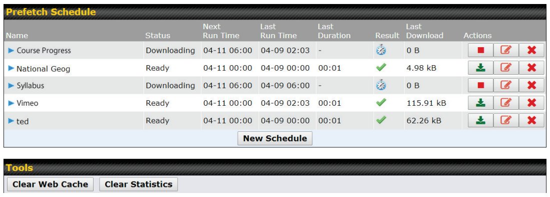


Cache Control	
Domain	○ Cache on all domains ● Cache the specified domains only ○ Do not cache the specified domains ted.com
Content Type	☑ Video ☑ Audio ☑ Images ☑ OS / Application Updates
Cache Lifetime Settings	File Extension: JPG — Lifetime (days): 30 ✖ +

Cache Control Settings	
Domain	Choose to **Cache on all domains**, or enter domain names and then choose either **Cache the specified domains only** or **Do not cache the specified domains**.
Content Type	Check these boxes to cache the listed content types or leave boxes unchecked to disable caching for the listed types.
Cache Lifetime Settings	Enter a file extension, such as JPG or DOC. Then enter a lifetime in days to specify how long files with that extension will be cached. Add or delete entries using the controls on the right.

12.2 Scheduling Content Prefetching

Content prefetching allows you to download content on a schedule that you define, which can help to preserve network bandwidth during busy times and keep costs down. To access MediaFast content prefetching settings, select **Advanced >Prefetch Schedule**.



Prefetch Schedule

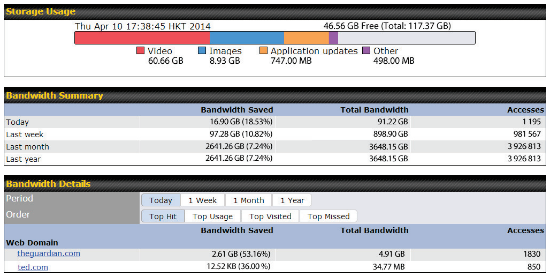
Name	Status	Next Run Time	Last Run Time	Last Duration	Result	Last Download	Actions
▶ Course Progress	Downloading	04-11 06:00	04-09 02:03	-	⏱	0 B	■ ✎ ✖
▶ National Geog	Ready	04-11 00:00	04-09 00:00	00:01	✓	4.98 kB	⬇ ✎ ✖
▶ Syllabus	Downloading	04-11 06:00	04-09 06:00	-	⏱	0 B	■ ✎ ✖
▶ Vimeo	Ready	04-11 00:00	04-09 02:03	00:01	✓	115.91 kB	⬇ ✎ ✖
▶ ted	Ready	04-11 00:00	04-09 00:00	00:01	✓	62.26 kB	⬇ ✎ ✖

Prefetch Schedule Settings	
Name	This field displays the name given to the scheduled download.
Status	Check the status of your scheduled download here.
Next Run Time/Last Run Time	These fields display the date and time of the next and most recent occurrences of the scheduled download.
Last Duration	Check this field to ensure that the most recent download took as long as expected to complete. A value that is too low might indicate an incomplete download or incorrectly specified download target, while a value that is too long could mean a download with an incorrectly specified target or stop time.
Result	This field indicates whether downloads are in progress (⏱) or complete (✓).
Last Download	Check this field to ensure that the most recent download file size is within the expected range. A value that is too low might indicate an incomplete download or incorrectly specified download target, while a value that is too long could mean a download with an incorrectly specified target or stop time. This field is also useful for quickly seeing which downloads are consuming the most storage space.
Actions	To begin a scheduled download immediately, click ⬇. To cancel a scheduled download, click ■. To edit a scheduled download, click ✎. To delete a scheduled download, click ✖.
New Schedule	To begin creating a new scheduled download, click this button.

Clear Web Cache	To clear all cached content, click this button. Note that this action cannot be undone.
Clear Statistics	To clear all prefetch and status page statistics, click this button.

12.3 Viewing MediaFast Statistics

To get details on storage and bandwidth usage, select **Status>MediaFast**.



Storage Usage

Thu Apr 10 17:38:45 HKT 2014 — 46.56 GB Free (Total: 117.37 GB)

🟥 Video	🟦 Images	🟧 Application updates	🟪 Other
60.66 GB	8.93 GB	747.00 MB	498.00 MB

Bandwidth Summary

	Bandwidth Saved	Total Bandwidth	Accesses
Today	16.90 GB (18.53%)	91.22 GB	1 195
Last week	97.28 GB (10.82%)	898.90 GB	981 567
Last month	2641.26 GB (7.24%)	3648.15 GB	3 926 813
Last year	2641.26 GB (7.24%)	3648.15 GB	3 926 813

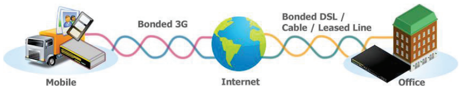
Bandwidth Details

Period: Today | 1 Week | 1 Month | 1 Year

Order: Top Hit | Top Usage | Top Visited | Top Missed

Web Domain	Bandwidth Saved	Total Bandwidth	Accesses
theguardian.com	2.61 GB (53.16%)	4.91 GB	1830
ted.com	12.52 KB (36.00 %)	34.77 MB	850

13 Bandwidth Bonding SpeedFusion™ / PepVPN

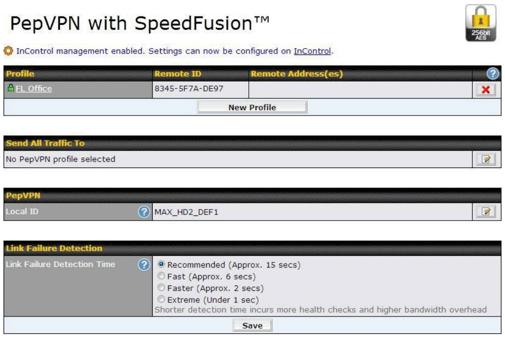


Pepwave bandwidth bonding SpeedFusion™ functionality securely connects your Pepwave router to another Pepwave or Peplink device (Peplink Balance 210/310/380/580/710/1350 only). Data, voice, or video communications between these locations are kept confidential across the public Internet.

Bandwidth bonding SpeedFusion™ is specifically designed for multi-WAN environments. Pepwave routers can aggregate all WAN connections' bandwidth for routing SpeedFusion™ traffic. Unless all the WAN connections of one site are down, Pepwave routers can keep the VPN up and running.

VPN bandwidth bonding is supported in Firmware 5.1 or above. 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.

13.1 PepVPN



PepVPN with SpeedFusion™

InControl management enabled. Settings can now be configured on InControl.

Profile	Remote ID	Remote Address(es)
FL Office	8345-5F7A-DE97	

New Profile

Send All Traffic To
No PepVPN profile selected

PepVPN
Local ID: MAX_HD2_DEF1

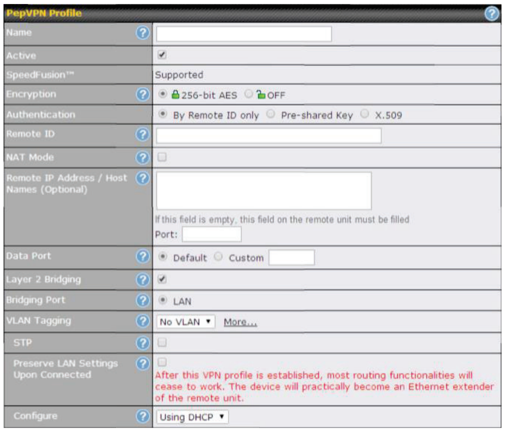
Link Failure Detection
Link Failure Detection Time:
● Recommended (Approx. 15 secs)
○ Fast (Approx. 6 secs)
○ Faster (Approx. 2 secs)
○ Extreme (Under 1 sec)
Shorter detection time incurs more health checks and higher bandwidth overhead

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>SpeedFusion™** or **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 acesss the **New Profile** button). Each profile specifies the settings for making VPN connection with one remote Pepwave or Peplink device. Note that available settings vary by model.



PepVPN Profile

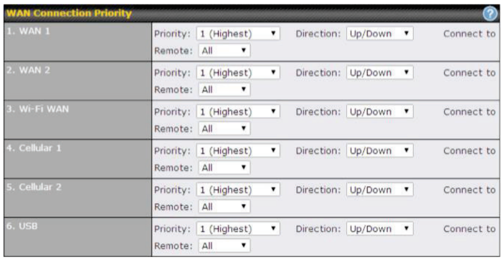
Name	
Active	☑
SpeedFusion™	Supported
Encryption	● 256-bit AES ○ OFF
Authentication	● By Remote ID only ○ Pre-shared Key ○ X.509
Remote ID	
NAT Mode	☐
Remote IP Address / Host Names (Optional)	If this field is empty, this field on the remote unit must be filled Port:
Data Port	● Default ○ Custom
Layer 2 Bridging	☑
Bridging Port	● LAN
VLAN Tagging	No VLAN ▾ More...
STP	☐
Preserve LAN Settings Upon Connected	☐ After this VPN profile is established, most routing functionalities will cease to work. The device will practically become an Ethernet extender of the remote unit.
Configure	Using DHCP ▾

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.
SpeedFusion™	This field indicates whether this device supports SpeedFusion or not.
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**, or **X.509** to specify the method the

	Pepwave router will use to authenticate peers. When selecting **By Remote ID Only**, be sure to enter a unique peer ID number in the **Remote ID** field.
Remote ID	To allow the Pepwave router to establish a VPN connection with a specific remote peer using a unique identifying number, enter the peer's ID or serial number here.
Pre-shared Key	This optional field becomes available when **Pre-shared Key** is selected as the Pepwave router'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. If you would like to prevent the display of the pre-shared key, check **Hide Characters**.
Remote ID/Remote Certificate	These optional fields become available when **X.509** is selected as the Pepwave router's VPN authentication method, as explained above. To authenticate VPN connections using X.509 certificates, copy and paste certificate details into these fields. To get more information on a listed X.509 certificate, click the **Show Details** link below the field.
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 Pepwave router will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Pepwave router 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.
Layer 2 Bridging^{A}	To make this option visible, click the question mark icon appearing at the top right of the **PepVPN Profile** settings section, and then click the displayed link. When this check box is unchecked, traffic between local and remote networks will be IP forwarded. To bridge the Ethernet network of an Ethernet port on a local and remote network, select **Layer 2 Bridging**. When this check box is selected, the two networks will become a single LAN, and any broadcast (e.g., ARP requests) or multicast traffic (e.g., Bonjour) will be sent over the VPN.
Bridging Port^{A}	When Layer 2 bridging is enabled, this field specifies the port to be bridged to the remote site. If you choose **WAN**, the selected WAN will be dedicated to bridging with the remote site and will be disabled for WAN purposes. The LAN port will remain unchanged.
VLAN Tagging^{A}	This field specifies the VLAN ID with which the VPN's traffic should be tagged before sending the traffic to the bridge port. If no VLAN tagging is needed, select **No VLAN**. To define a new VLAN ID, click **More**... and input the VLAN ID. VLAN IDs that are not referenced by any VPN profiles will be removed from the list automatically. The default value for this field is **No VLAN**.

STP^{A}	Checking this box enables spanning tree protocol, used to prevent loops in bridged Ethernet LANs.
Preserve LAN Settings Upon Connected^{A}	The LAN port is chosen as the bridge port. Selecting this option preserves LAN settings (e.g., LAN port IP address, DHCP server, etc.) when the Layer 2 VPN is connected. Uncheck this option if the LAN IP address and gateway will use remote LAN settings. Check this option if the LAN IP address and local DHCP server should remain unchanged after the VPN is up. If you choose not to preserve LAN settings when the VPN is connected, the device will not act as a router and most Layer 3 routing functions will cease to work.
Configure^{A}	This setting specifies how a management IP address is acquired for the bridge port in the specified VLAN (if defined) when the Layer 2 bridge is connected. Choosing **As None** will result in no IP address being assigned to the bridge port for the Layer 2 connection.

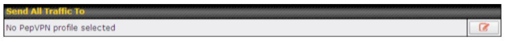
^{A} - Advanced feature, please click the ? button on the top right-hand corner to activate.



WAN Connection Priority

1. WAN 1	Priority: 1 (Highest) ▾	Remote: All ▾	Direction: Up/Down ▾	Connect to
2. WAN 2	Priority: 1 (Highest) ▾	Remote: All ▾	Direction: Up/Down ▾	Connect to
3. Wi-Fi WAN	Priority: 1 (Highest) ▾	Remote: All ▾	Direction: Up/Down ▾	Connect to
4. Cellular 1	Priority: 1 (Highest) ▾	Remote: All ▾	Direction: Up/Down ▾	Connect to
5. Cellular 2	Priority: 1 (Highest) ▾	Remote: All ▾	Direction: Up/Down ▾	Connect to
6. USB	Priority: 1 (Highest) ▾	Remote: All ▾	Direction: Up/Down ▾	Connect to

WAN Connection Priority	
WAN Connection Priority	If your device supports it, you can specify the priority of WAN connections to be used for making VPN connections. WAN connections set to **OFF** will never be used. Only available WAN connections with the highest priority will be used. To enable connection mapping to remote WANs, click the ? button.

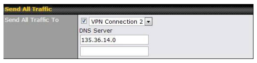


Send All Traffic To

No PepVPN profile selected

Send All Traffic To

This feature allows you to redirect all traffic to a specified PepVPN connection. Click the button to select your connection and the following menu will appear:



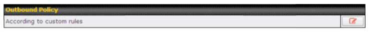
Send All Traffic

Send All Traffic To ☑ VPN Connection 2
DNS Server
135.36.14.0

You could also specify a DNS server to resolve incoming DNS requests. Note that this feature can be found at **Advanced>PepVPN>Outbound Policy>** on some Pepwave routers.

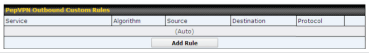
Outbound Policy/PepVPN Outbound Custom Rules

Some models allow you to set outbound policy and custom outbound rules from **Advanced>PepVPN**. See **Section 14** for more information on outbound policy settings.



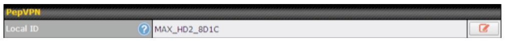
Outbound Policy

According to custom rules



PepVPN Outbound Custom Rules

Service	Algorithm	Source	Destination	Protocol
(Auto)				

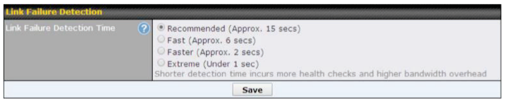


PepVPN

Local ID: MAX_HD2_8D1C

PepVPN Local ID

The local ID is a text string to identify this local unit when establishing a VPN connection. When creating a profile on a remote unit, this local ID must be entered in the remote unit's **Remote ID** field. Click the icon to edit **Local ID**.



Link Failure Detection

Link Failure Detection Time
● Recommended (Approx. 15 secs)
○ Fast (Approx. 6 secs)
○ Faster (Approx. 2 secs)
○ Extreme (Under 1 sec)
Shorter detection time incurs more health checks and higher bandwidth overhead

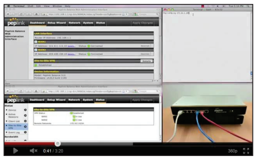
Link Failure Detection	
Link Failure Detection Time	The bonded VPN can detect routing failures on the path between two sites over each WAN connection. Failed WAN connections will not be used to route VPN traffic. Health check packets are sent to the remote unit to detect any failure. The more frequently checks are sent, the shorter the detection time, although more bandwidth will be consumed. When **Recommended** (default) is selected, a health check packet is sent every five seconds, and the expected detection time is 15 seconds. When **Fast** is selected, a health check packet is sent every three seconds, and the expected detection time is six seconds. When **Faster** is selected, a health check packet is sent every second, and the expected detection time is two seconds. When **Extreme** is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second.

Important Note

Peplink proprietary SpeedFusion^{TM} uses TCP port 32015 and UDP port 4500 for establishing VPN connections. If you have a firewall in front of your Pepwave devices, you will need to add firewall rules for these ports and protocols to allow inbound and outbound traffic to pass through the firewall.

Tip

Want to know more about VPN sub-second session failover? Visit our YouTube Channel for a video tutorial!



http://youtu.be/TLQgdpPSY88

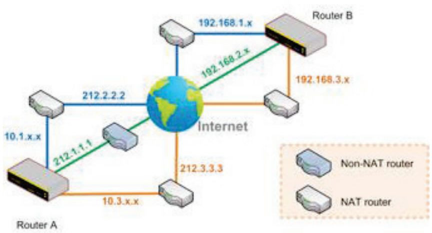
13.2 The Pepwave Router Behind a NAT Router

Pepwave routers support establishing SpeedFusion^{TM} over WAN connections which are behind a NAT (network address translation) router.

To enable a WAN connection behind a NAT router to accept VPN connections, you can configure the NAT router in front of the WAN connection to inbound port-forward TCP port 32015 to the Pepwave router.

If one or more WAN connections on Unit A can accept VPN connections (by means of port forwarding or not), while none of the WAN connections on the peer Unit B can do so, you should enter all of Unit A's public IP addresses or hostnames into Unit B's **Remote IP Addresses / Host Names** field. Leave the field in Unit A blank. With this setting, a SpeedFusion^{TM} connection can be set up and all WAN connections on both sides will be utilized.

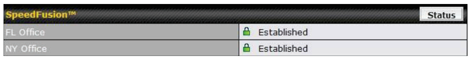
See the following diagram for an example of this setup in use:



One of the WANs connected to Router A is non-NAT'd (*212.1.1.1*). The rest of the WANs connected to Router A and all WANs connected to Router B are NAT'd. In this case, the **Peer IP Addresses / Host Names** field for Router B should be filled with all of Router A's hostnames 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 connected to Router A should inbound port-forward TCP port 32015 to Router A so that all WANs will be utilized in establishing the VPN.

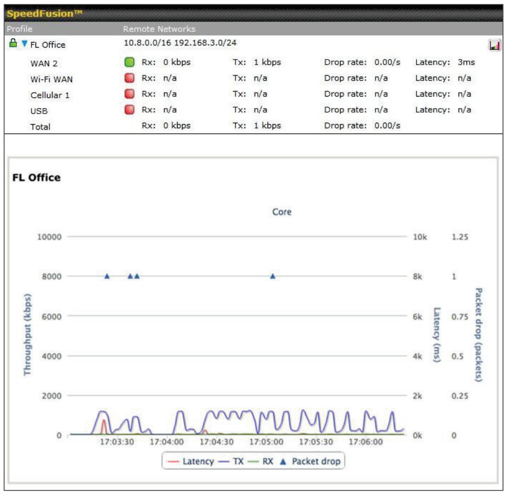
13.3 SpeedFusion^{TM} Status

SpeedFusion^{TM} status is shown in the **Dashboard**. The connection status of each connection profile is shown as below.



SpeedFusion™	Status
FL Office	Established
NY Office	Established

After clicking the **Status** button at the top right corner of the SpeedFusion^{TM} table, you will be forwarded to **Status>SpeedFusion^{TM}**, where you can view subnet and WAN connection information for each VPN peer. Please refer to **Section 23.5** for details.



SpeedFusion™

Profile	Remote Networks			
FL Office	10.8.0.0/16 192.168.3.0/24			
WAN 2	🟩 Rx: 0 kbps	Tx: 1 kbps	Drop rate: 0.00/s	Latency: 3ms
Wi-Fi WAN	🟥 Rx: n/a	Tx: n/a	Drop rate: n/a	Latency: n/a
Cellular 1	🟥 Rx: n/a	Tx: n/a	Drop rate: n/a	Latency: n/a
USB	🟥 Rx: n/a	Tx: n/a	Drop rate: n/a	Latency: n/a
Total	Rx: 0 kbps	Tx: 1 kbps	Drop rate: 0.00/s	

IP Subnets Must Be Unique Among VPN Peers

The entire interconnected SpeedFusion^{TM} network is a single non-NAT IP network. Avoid duplicating subnets in your sites to prevent connectivity problems when accessing those subnets.

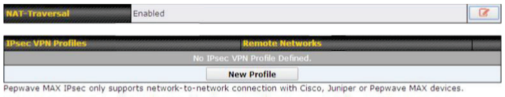
14 IPsec VPN (for Pepwave MAX only)

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

IPsec VPN on Pepwave routers is specially designed for multi-WAN environments. For instance, if a user sets up multiple IPsec profiles for a multi-WAN environment and WAN1 is connected and healthy, IPsec traffic will go through this link. However, should unforeseen problems (e.g., unplugged cables or ISP problems) cause WAN1 to go down, our IPsec implementation will make use of WAN2 and WAN3 for failover.

14.1 IPsec VPN Settings

Many Pepwave products can make multiple IPsec VPN connections with Peplink, Pepwave, Cisco, and Juniper routers. 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 with a selection of encryption standards, such as 3DES, AES-128, and AES-256. To configure IPsec VPN on Pepwave devices that support it, navigate to **Advanced>IPsec VPN.**

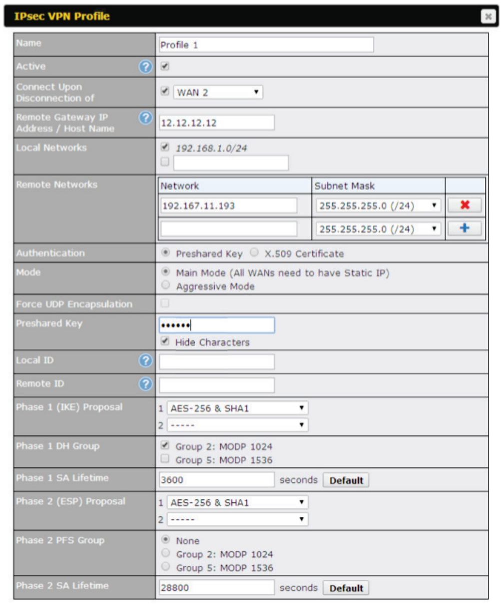


NAT-Traversal	Enabled

IPsec VPN Profiles	Remote Networks
No IPsec VPN Profile Defined.	

Pepwave MAX IPsec only supports network-to-network connection with Cisco, Juniper or Pepwave MAX devices.

A **NAT-Traversal** option and list of defined **IPsec VPN** profiles will be shown. **NAT-Traversal** 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 Pepwave, Cisco, or Juniper routers via available WAN connections. To edit any of the profiles, click on its associated connection name in the leftmost column.



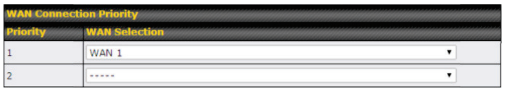
IPsec VPN Profile

Name	Profile 1
Active	☑
Connect Upon Disconnection of	☑ WAN 2 ▾
Remote Gateway IP Address / Host Name	12.12.12.12
Local Networks	☑ *192.168.1.0/24* ☐
Remote Networks	Network: 192.167.11.193 — Subnet Mask: 255.255.255.0 (/24) ▾ ✖ Network: — Subnet Mask: 255.255.255.0 (/24) ▾ +
Authentication	● Preshared Key ○ X.509 Certificate
Mode	● Main Mode (All WANs need to have Static IP) ○ Aggressive Mode
Force UDP Encapsulation	☐
Preshared Key	•••••• ☑ Hide Characters
Local ID	
Remote ID	
Phase 1 (IKE) Proposal	1 AES-256 & SHA1 ▾ 2 ----- ▾
Phase 1 DH Group	☑ Group 2: MODP 1024 ☐ Group 5: MODP 1536
Phase 1 SA Lifetime	3600 seconds Default
Phase 2 (ESP) Proposal	1 AES-256 & SHA1 ▾ 2 ----- ▾
Phase 2 PFS Group	● None ○ Group 2: MODP 1024 ○ Group 5: MODP 1536
Phase 2 SA Lifetime	28800 seconds Default

IPsec VPN Settings	
Name	This field is for specifying a local name to represent this connection profile.
Active	When this box is checked, this IPsec VPN connection profile will be enabled. Otherwise, it will be disabled.
Connect Upon Disconnection of	Check this box and select a WAN to connect to this VPN automatically when the specified WAN is disconnected.
Remote Gateway IP	Enter the remote peer's public IP address. For **Aggressive Mode**, this is optional.

Address / Host Name	
Local Networks	Enter the local LAN subnets here. If you have defined static routes, they will be shown here.
Remote Networks	Enter the LAN and subnets that are located at the remote site here.
Authentication	To access your VPN, clients will need to authenticate by your choice of methods. Choose between the **Preshared Key** and **X.509 Certificate** methods of authentication.
Mode	Choose **Main Mode** if both IPsec peers use static IP addresses. Choose **Aggressive Mode** if one of the IPsec peers uses dynamic IP addresses.
Force UDP Encapsulation	For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.
Pre-shared Key	This defines the peer authentication pre-shared key used to authenticate this VPN connection. The connection will be up only if the pre-shared keys on each side match.
Remote Certificate (pem encoded)	Available only when **X.509 Certificate** is chosen as the **Authentication** method, this field allows you to paste a valid X.509 certificate.
Local ID	In **Main Mode**, this field can be left blank. In **Aggressive Mode**, if **Remote Gateway IP Address** 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	In **Main Mode**, this field can be left blank. In **Aggressive Mode**, if **Remote Gateway IP Address** 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	In **Main Mode**, this allows setting up to six encryption standards, in descending order of priority, to be used in initial connection key negotiations. In **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	This setting specifies the lifetime limit of this Phase 1 Security Association. By default, it is set at **3600** seconds.
Phase 2 (ESP) Proposal	In **Main Mode**, this allows setting up to six encryption standards, in descending order of priority, to be used for the IP data that is being transferred. In **Aggressive Mode**, only one selection is permitted.
Phase 2 PFS Group	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. **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	This setting specifies the lifetime limit of this Phase 2 Security Association. By default, it is set at **28800** seconds.



WAN Connection Priority

Priority	WAN Selection
1	WAN 1 ▾
2	----- ▾

WAN Connection Priority	
WAN Connection	Select the appropriate WAN connection from the drop-down menu.