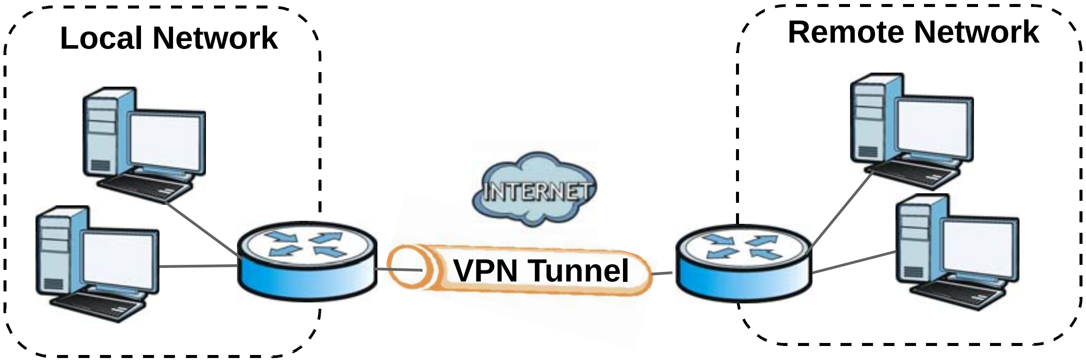
# IPSec VPN

Chapter 16

## 16.1 IPSec VPN

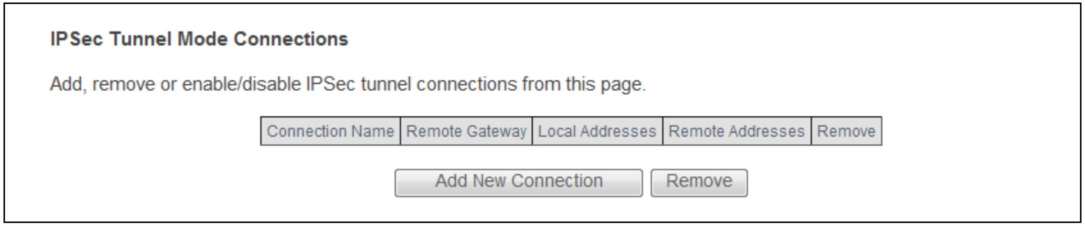
A virtual private network (VPN) provides secure communications over the the Internet. Internet Protocol Security (IPSec) is a standards-based VPN that provides confidentiality, data integrity, and authentication. This chapter shows you how to configure the Router's VPN settings.

**Figure 75** IPSec Fields Summary



Click **Advanced Setup > IPSec VPN** to view and manage your VPN tunnel policies. The following figure helps explain the main fields in the web configurator.

**Figure 76** IPSec VPN



**IPSec Tunnel Mode Connections**

Add, remove or enable/disable IPSec tunnel connections from this page.

| Connection Name | Remote Gateway | Local Addresses | Remote Addresses | Remove |
|---|---|---|---|---|

This screen contains the following fields:

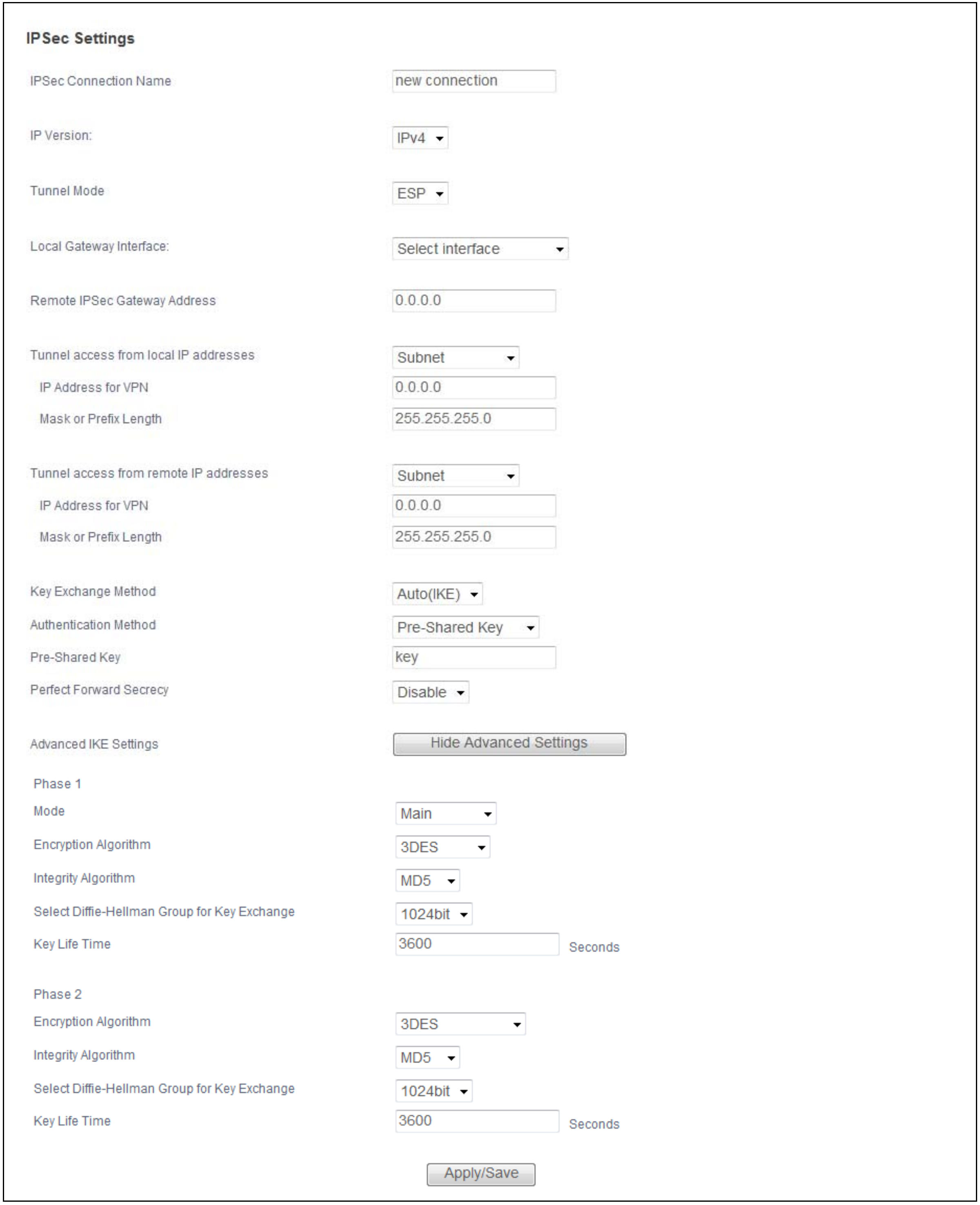
Table 69 IPSec VPN

| LABEL | DESCRIPTION |
|---|---|
| Connection Name | The name of the VPN policy. |
| Remote Gateway | This is the IP address of the remote IPSec router in the IKE SA. |
| Local Addresses | This displays the IP address(es) on the LAN behind your Router. |
| Remote Addresses | This displays the IP address(es) on the LAN behind the remote IPSec's router. |
| Remove | Select entries and click the **Remove** button to delete them. |
| Add New Connection | Click this button to add an item to the list. |

## 16.2 IPSec VPN Add Screen

Use these settings to add IPSec VPN policies. Click the **Add New Connection** button in the **Advanced Setup > IPSec VPN** screen to open this screen as shown next.

**Figure 77** IPSec VPN: Add



**IPSec Settings**

| | |
|---|---|
| IPSec Connection Name | new connection |
| IP Version: | IPv4 ▾ |
| Tunnel Mode | ESP ▾ |
| Local Gateway Interface: | Select interface ▾ |
| Remote IPSec Gateway Address | 0.0.0.0 |
| Tunnel access from local IP addresses | Subnet ▾ |
| IP Address for VPN | 0.0.0.0 |
| Mask or Prefix Length | 255.255.255.0 |
| Tunnel access from remote IP addresses | Subnet ▾ |
| IP Address for VPN | 0.0.0.0 |
| Mask or Prefix Length | 255.255.255.0 |
| Key Exchange Method | Auto(IKE) ▾ |
| Authentication Method | Pre-Shared Key ▾ |
| Pre-Shared Key | key |
| Perfect Forward Secrecy | Disable ▾ |
| Advanced IKE Settings | Hide Advanced Settings |
| Phase 1 | |
| Mode | Main ▾ |
| Encryption Algorithm | 3DES ▾ |
| Integrity Algorithm | MD5 ▾ |
| Select Diffie-Hellman Group for Key Exchange | 1024bit ▾ |
| Key Life Time | 3600 Seconds |
| Phase 2 | |
| Encryption Algorithm | 3DES ▾ |
| Integrity Algorithm | MD5 ▾ |
| Select Diffie-Hellman Group for Key Exchange | 1024bit ▾ |
| Key Life Time | 3600 Seconds |

This screen contains the following fields:

**Table 70** IPSec VPN: Add

| LABEL | DESCRIPTION |
|---|---|
| IPSec Connection Name | Enter the name of the VPN policy. |
| IP Version | Set whether this policy uses IPv4 or IPv6. |
| Tunnel Mode | Select the security protocol to use in the IPSec SA.<br>**AH** (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption.<br>**ESP** (RFC 2406) - provides encryption and the same services offered by AH, but its authentication is weaker. The Router and remote IPSec router must use the same active protocol. |
| Remote IPSec Gateway Address | Enter the IP address of the remote IPSec router in the IKE SA. |
| Tunnel access from local IP addresses | Select **Single Address** to have only one local LAN IP address use the VPN tunnel. Select **Subnet** to specify local LAN IP addresses by their subnet mask. |
| IP Address for VPN | If **Single Address** is selected, enter a (static) IP address on the LAN behind your Router.<br>If **Subnet** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind your Router.  Then enter the subnet mask to identify the network address. |
| Mask or Prefix Length | If **Subnet** is selected, enter the subnet mask (for IPv4) or prefix length (for an IPv6 address) to identify the network address.<br>The IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address. |
| Tunnel access from remote IP addresses | Select **Single Address** to have only one remote LAN IP address use the VPN tunnel. Select **Subnet** to specify remote LAN IP addresses by their subnet mask. |
| IP Address for VPN | If **Single Address** is selected, enter a (static) IP address on the LAN behind the remote IPSec's router.<br>If **Subnet** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind the remote IPSec's router. Then enter the subnet mask to identify the network address. |
| Mask or Prefix Length | If **Subnet** is selected, enter the subnet mask (for IPv4) or prefix length (for an IPv6 address) to identify the network address.<br>The IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address. |

Table 70 IPSec VPN: Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Key Exchange Method | Select the key exchange method:<br>**Auto(IKE)** - Select this to use automatic IKE key management VPN connection policy.<br>**Manual** - Select this option to configure a VPN connection policy that uses a manual key instead of IKE key management. This may be useful if you have problems with IKE key management.<br>Note: Only use manual key as a temporary solution, because it is not as secure as a regular IPSec SA. |
| Authentication Method | Select **Pre-Shared Key** to use a pre-shared key for authentication, and type in your pre-shared key. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.<br>Select **Certificate (X.509)** to use a certificate for authentication. |
| Pre-Shared Key | Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation.<br>Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x” (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself. |
| Perfect Forward Secrecy (PFS) | Select whether or not to enable Perfect Forward Secrecy (PFS). Both routers must enable it or disable it. |
| Advanced IKE Settings | Use the button to show or hide the advanced IKE settings. |
| Phase 1 | |
| Mode | Select the negotiation mode to use to negotiate the IKE SA. Choices are:<br>**Main** - this encrypts the Router’s and remote IPSec router’s identities but takes more time to establish the IKE SA.<br>**Aggressive** - this is faster but does not encrypt the identities.<br>The Router and the remote IPSec router must use the same negotiation mode. |

**Table 70** IPSec VPN: Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Encryption Algorithm | Select which key size and encryption algorithm to use in the IKE SA. Choices are:<br>DES - a 56-bit key with the DES encryption algorithm<br>**3DES** - a 168-bit key with the DES encryption algorithm<br>**AES** - **128** - a 128-bit key with the AES encryption algorithm<br>**AES** - **196** - a 196-bit key with the AES encryption algorithm<br>**AES** - **256** - a 256-bit key with the AES encryption algorithm<br>The Router and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput. |
| Integrity Algorithm | Select which hash algorithm to use to authenticate packet data. Choices are **MD5**, **SHA1**. SHA is generally considered stronger than MD5, but it is also slower. |
| Select Diffie-Hellman Group for Key Exchange | Select which Diffie-Hellman key group you want to use for encryption keys. Choices for number of bits in the random number are: 768, 1024, 1536, 2048, 3072, 4096, 6114, and 8192.<br>The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. |
| Key Life Time | Define the length of time before an IPSec SA automatically renegotiates in this field.<br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| Phase 2 | |
| Encryption Algorithm | Select which key size and encryption algorithm to use in the IKE SA.<br>**DES** - a 56-bit key with the DES encryption algorithm<br>**3DES** - a 168-bit key with the DES encryption algorithm<br>**AES** - **128** - a 128-bit key with the AES encryption algorithm<br>**AES** - **192** - a 196-bit key with the AES encryption algorithm<br>**AES** - **256** - a 256-bit key with the AES encryption algorithm<br>Select **NULL Encryption** to set up a tunnel without encryption. You do not enter an encryption key with this option.<br>The Router and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput. |
| Integrity Algorithm | Select which hash algorithm to use to authenticate packet data. Choices are **MD5** and **SHA1**. SHA is generally considered stronger than MD5, but it is also slower. |

Table 70 IPSec VPN: Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Select Diffie-Hellman Group for Key Exchange | Select which Diffie-Hellman key group you want to use for encryption keys. Choices for number of bits in the random number are: 768, 1024, 1536, 2048, 3072, 4096, 6114, and 8192.<br>The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. |
| Key Life Time | Define the length of time before an IPSec SA automatically renegotiates in this field.<br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| The following fields display if you select **Manual** in the **Key Exchange Method** field. | |
| Perfect Forward Secrecy (PFS) | Select whether or not to enable Perfect Forward Secrecy (PFS). Both routers must enable it or disable it. |
| Encryption Algorithm | Select which key size and encryption algorithm to use in the IKE SA. Choices are:<br>**DES** - a 56-bit key with the DES encryption algorithm<br>**3DES** - a 168-bit key with the DES encryption algorithm<br>**AES** - AES-CBC encryption. CBC creates message authentication code from a block cipher. |
| Encryption Key | This field is applicable when you select an Encryption Algorithm.<br>Enter the encryption key, which depends on the encryption algorithm.<br>**DES** - type a unique key 16 hexadecimal characters long.<br>**3DES** - type a unique key 48 hexadecimal characters long.<br>**AES** - type a unique key 32, 48, or 64 hexadecimal characters long. |
| Authentication Algorithm | Select which hash algorithm to use to authenticate packet data. Choices are **MD5**, **SHA1**. SHA is generally considered stronger than MD5, but it is also slower. |
| Authentication Key | Enter the authentication key, which depends on the authentication algorithm.<br>**MD5** - type a unique key 32 hexadecimal characters long<br>**SHA1** - type a unique key 40 hexadecimal characters long |
| SPI | Type a unique SPI (Security Parameter Index) in hexadecimal characters.<br>The SPI is used to identify the Router during authentication.<br>The Router and remote IPSec router must use the same SPI. |
| Apply/Save | Click this button to save your changes. |

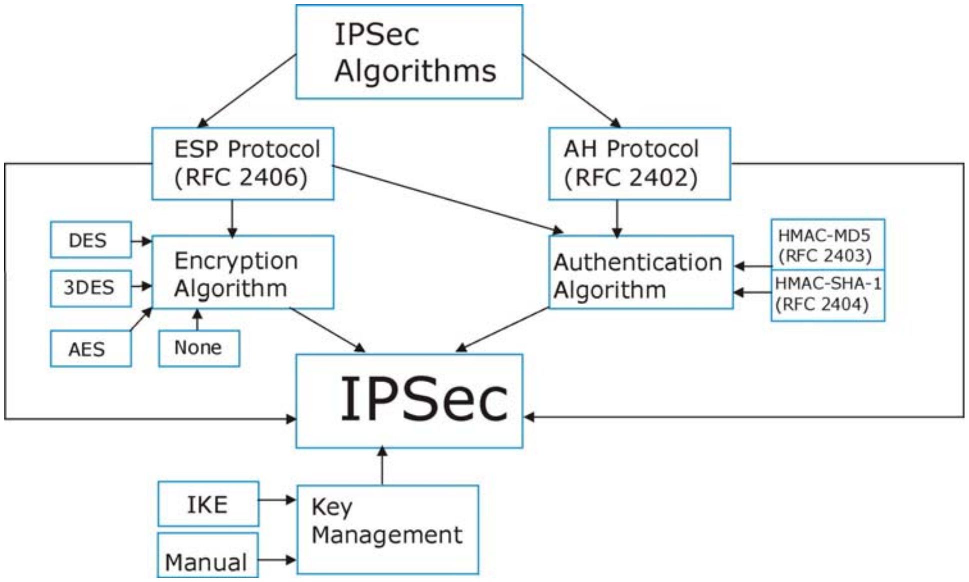
# 16.3 Technical Reference

This section provides some technical background information about the topics covered in this section.

## 16.3.1 IPSec Architecture

The overall IPSec architecture is shown as follows.

**Figure 78** IPSec Architecture



### IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols.

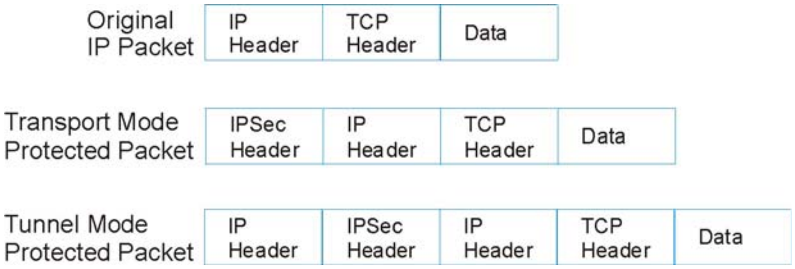
### Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

## 16.3.2 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode. At the time of writing, the Router supports **Tunnel** mode only.

**Figure 79** Transport and Tunnel Mode IPSec Encapsulation



| | | | | | |
|---|---|---|---|---|---|
| Original IP Packet | IP Header | TCP Header | Data | | |
| Transport Mode Protected Packet | IPSec Header | IP Header | TCP Header | Data | |
| Tunnel Mode Protected Packet | IP Header | IPSec Header | IP Header | TCP Header | Data |

### Transport Mode

**Transport** mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

### Tunnel Mode

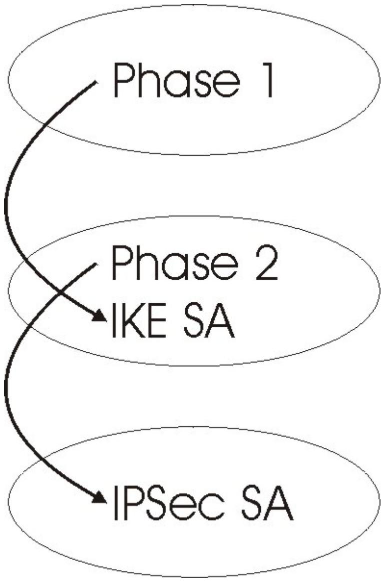
**Tunnel** mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

### 16.3.3 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

**Figure 80** Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The Router automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

## 16.3.4 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

## 16.3.5 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the Router.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

**Tunnel** mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

**Transport** mode **ESP** with authentication is not compatible with NAT.

Table 71 VPN and NAT

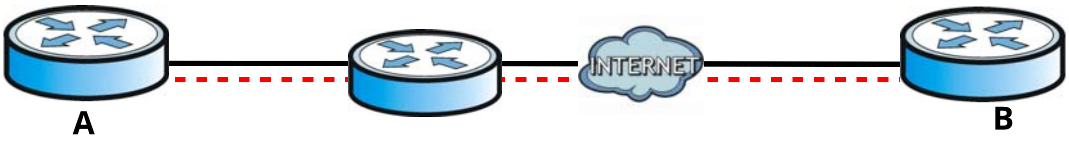
| SECURITY PROTOCOL | MODE | NAT |
|---|---|---|
| AH | Transport | N |
| AH | Tunnel | N |
| ESP | Transport | N |
| ESP | Tunnel | Y |

## 16.3.6 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the Router’s **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

Figure 81 NAT Router Between IPSec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In the above figure, when IPSec router **A** tries to establish an IKE SA, IPSec router **B** checks the UDP port 500 header, and IPSec routers **A** and **B** build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router **A**.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

**Table 72** VPN and NAT

| SECURITY PROTOCOL | MODE | NAT |
|---|---|---|
| AH | Transport | N |
| AH | Tunnel | N |
| ESP | Transport | Y* |
| ESP | Tunnel | Y |

Y* - This is supported in the Router if you enable NAT traversal.

### 16.3.7 ID Type and Content

With aggressive negotiation mode (see Section 16.3.4 on page 124), the Router identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the Router to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses.

Regardless of the ID type and content configuration, the Router does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see Section 16.3.4 on page 124), the ID type and content are encrypted to provide identity protection. In this case the Router can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The Router can distinguish up to 48 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and eight key groups when you configure a VPN rule (see Section 16.1 on page 114). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

**Table 73** Local ID Type and Content Fields

| LOCAL ID TYPE= | CONTENT= |
|---|---|
| IP | Type the IP address of your computer. |
| DNS | Type a domain name (up to 31 characters) by which to identify this Router. |

**Table 73** Local ID Type and Content Fields (continued)

| LOCAL ID TYPE= | CONTENT= |
|---|---|
| E-mail | Type an e-mail address (up to 31 characters) by which to identify this Router. |
| | The domain name or e-mail address that you use in the **Local ID Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. |

#### 16.3.7.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two Routers in this example can complete negotiation and establish a VPN tunnel.

**Table 74** Matching ID Type and Content Configuration Example

| ROUTER A | ROUTER B |
|---|---|
| Local ID type: E-mail | Local ID type: IP |
| Local ID content: tom@yourcompany.com | Local ID content: 1.1.1.2 |
| Remote ID type: IP | Remote ID type: E-mail |
| Remote ID content: 1.1.1.2 | Remote ID content: tom@yourcompany.com |

The two Routers in this example cannot complete their negotiation because Router B's **Local ID Type** is **IP**, but Router A's **Remote ID Type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

**Table 75** Mismatching ID Type and Content Configuration Example

| ROUTER A | ROUTER B |
|---|---|
| Local ID type: IP | Local ID type: IP |
| Local ID content: 1.1.1.10 | Local ID content: 1.1.1.2 |
| Remote ID type: E-mail | Remote ID type: IP |
| Remote ID content: aa@yahoo.com | Remote ID content: 1.1.1.0 |

### 16.3.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 16.3.3 on page 123 for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

### 16.3.9 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

# Certificates

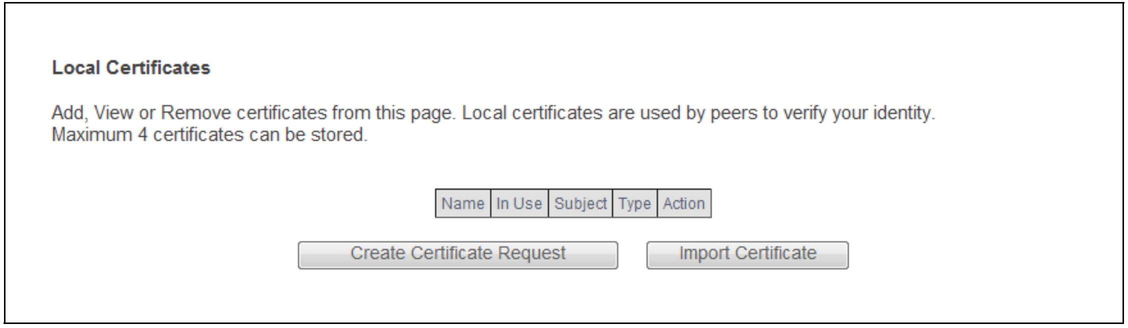
17 Chapter

## 17.1 Local Certificates

The Router can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner’s identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Click **Advanced Setup > Certificates > Local** to manage the Router’s list of certificates and certification requests.

**Figure 82** Local Certificates



**Local Certificates**

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

| Name | In Use | Subject | Type | Action |
|---|---|---|---|---|

**Table 76** Local Certificates

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name. |
| In Use | This field shows whether or not the Router currently uses the certificate. |
| Subject | This field displays identifying information about the certificate’s owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information. |
| Type | This field displays whether the entry is for a certificate or a certificate request. |

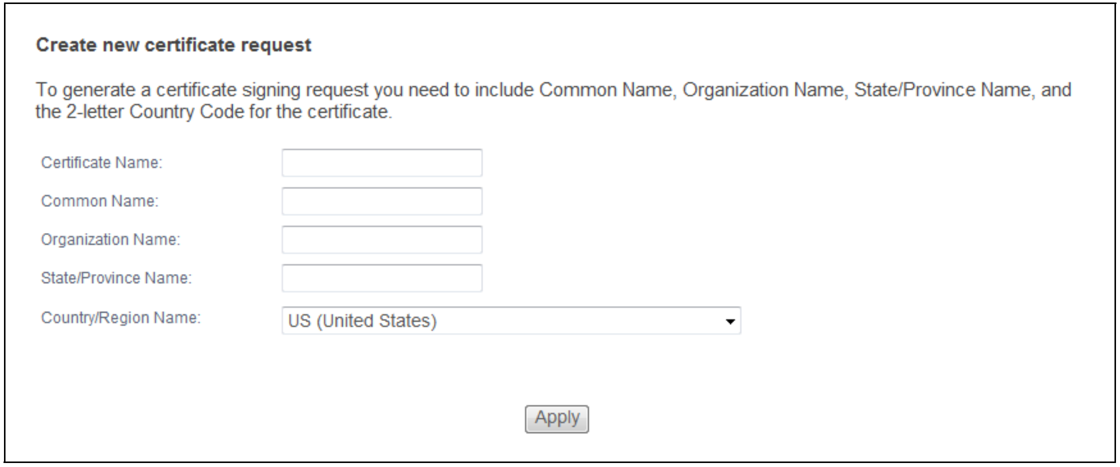
**Table 76** Local Certificates (continued)

| LABEL | DESCRIPTION |
|---|---|
| Action | Click the **View** button to open a screen with an in-depth list of information about the certificate (or certification request).<br>For a certification request, click **Load Signed** to import the signed certificate.<br>Click the **Remove** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use. |
| Create Certificate Request | Click this button to go to the screen where you can have the Router generate a certification request. |
| Import Certificate | Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Router. |

### 17.1.1 Create Certificate Request

Click the **Local Certificates** screen's **Create Certificate Request** button to open the following screen. Use this screen to have the Router generate a certification request.

**Figure 83** Create Certificate Request



**Create new certificate request**

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

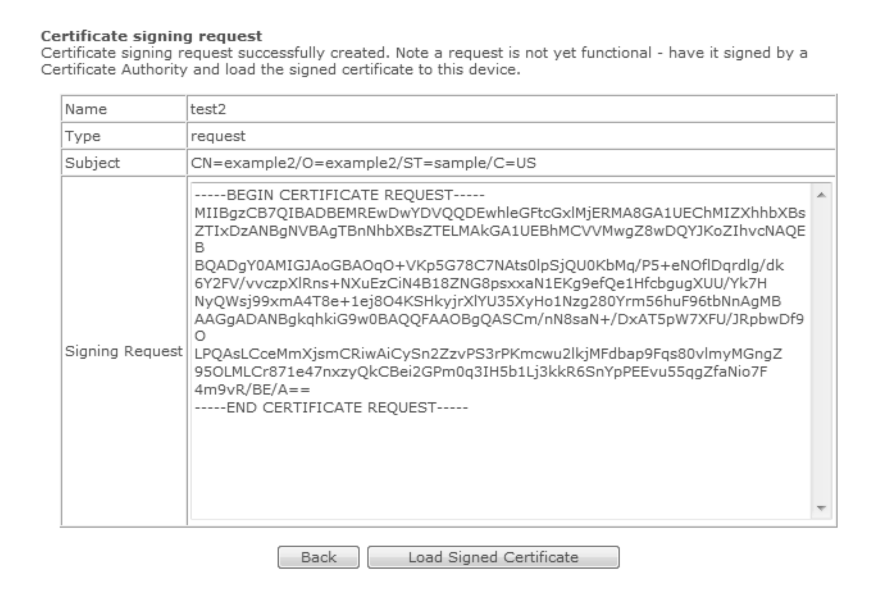
| | |
|---|---|
| Certificate Name: | |
| Common Name: | |
| Organization Name: | |
| State/Province Name: | |
| Country/Region Name: | US (United States) |

**Table 77** Create Certificate Request

| LABEL | DESCRIPTION |
|---|---|
| Certificate Name | Type up to 63 ASCII characters (not including spaces) to identify this certificate. |
| Common Name | Select **Auto** to have the Router configure this field automatically. Or select **Customize** to enter it manually.<br>Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 63 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string. |
| Organization Name | Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the Router drops trailing spaces. |
| State/Province Name | Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the Router drops trailing spaces. |
| Country/Region Name | Select a country to identify the nation where the certificate owner is located. |
| Apply | Click **Apply** to save your changes. |

After you click **Apply**, the following screen displays to notify you that you need to get the certificate request signed by a Certificate Authority. If you already have, click **Load_Signed** to import the signed certificate into the Router. Otherwise click **Back** to return to the **Local Certificates** screen.

**Figure 84** Certificate Request Created



**Certificate signing request**

Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

| | |
|---|---|
| Name | test2 |
| Type | request |
| Subject | CN=example2/O=example2/ST=sample/C=US |
| Signing Request | (see below) |

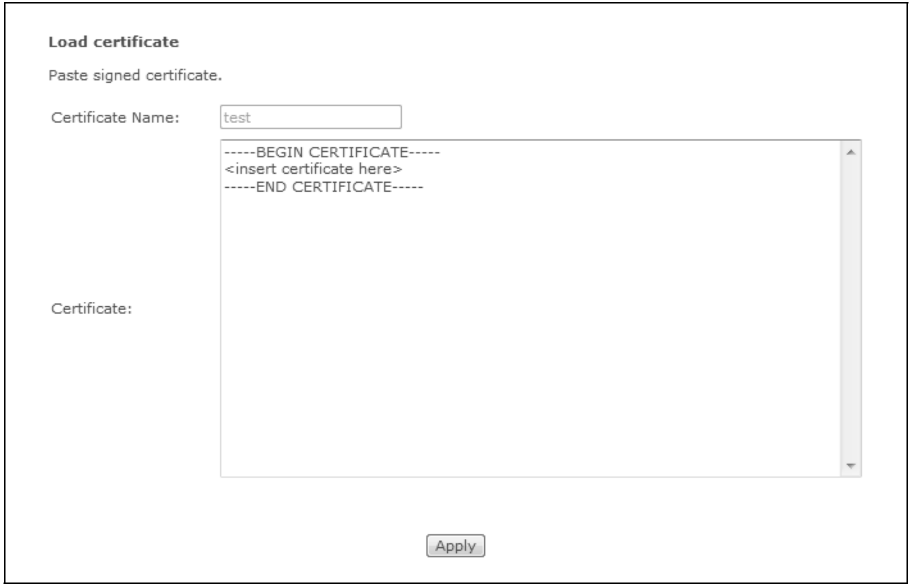
```
-----BEGIN CERTIFICATE REQUEST-----
MIIBgzCB7QIBADBEMREwDwYDVQQDEwhleGFtcGxlMjERMA8GA1UEChMIZXhhbXBs
ZTIxDzANBgNVBAgTBnNhbXBsZTELMAkGA1UEBhMCVVMwgZ8wDQYJKoZIhvcNAQE
B
BQADgY0AMIGJAoGBAOqO+VKp5G78C7NAts0lpSjQU0KbMq/P5+eNOflDqrdlg/dk
6Y2FV/vvczpXlRns+NXuEzCiN4B18ZNG8psxxaN1EKg9efQe1HfcbgugXUU/Yk7H
NyQWsj99xmA4T8e+1ej8O4KSHkyjrXlYU35XyHo1Nzg280Yrm56huF96tbNnAgMB
AAGgADANBgkqhkiG9w0BAQQFAAOBgQASCm/nN8saN+/DxAT5pW7XFU/JRpbwDf9
O
LPQAsLCceMmXjsmCRiwAiCySn2ZzvPS3rPKmcwu2lkjMFdbap9Fqs80vlmyMGngZ
95OLMLCr871e47nxzyQkCBei2GPm0q3IH5b1Lj3kkR6SnYpPEEvu55qgZfaNio7F
4m9vR/BE/A==
-----END CERTIFICATE REQUEST-----
```

### 17.1.2 Load Signed Certificate

After you create a certificate request and have it signed by a Certificate Authority, in the **Local Certificates** screen click the certificate request's **Load Signed** button to import the signed certificate into the Router.

ⓘ You must remove any spaces from the certificate's filename before you can import it.

**Figure 85** Load Signed Certificate



Load certificate

Paste signed certificate.

Certificate Name: test

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

**Table 78** Load Signed Certificate

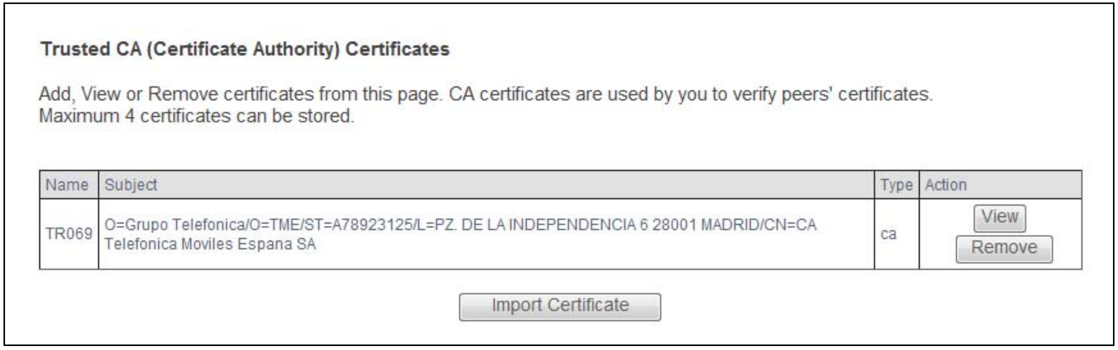
| LABEL | DESCRIPTION |
|---|---|
| Certificate Name | This is the name of the signed certificate. |
| Certificate | Copy and paste the signed certificate into the text box to store it on the Router. |
| Apply | Click **Apply** to save your changes. |

## 17.2 Trusted CA

Use the **Trusted CA** screen to view a summary list of certificates of the certification authorities that you have set the Router to accept as trusted. The Router accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Click **Advanced Setup > Certificates > Trusted CA** to open the **Trusted CA** screen.

**Figure 86** Trusted CA



**Trusted CA (Certificate Authority) Certificates**

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.

| Name | Subject | Type | Action |
|---|---|---|---|
| TR069 | O=Grupo Telefonica/O=TME/ST=A78923125/L=PZ. DE LA INDEPENDENCIA 6 28001 MADRID/CN=CA Telefonica Moviles Espana SA | ca | View<br>Remove |

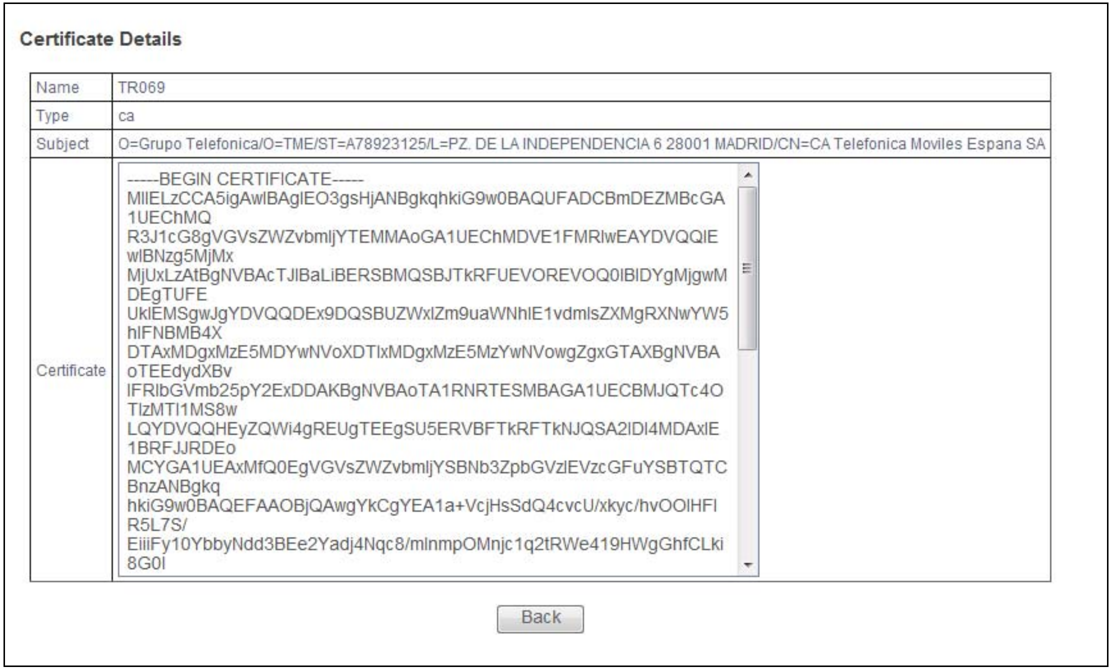
**Table 79** Trusted CA

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the name used to identify this certificate. |
| Subject | This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information. |
| Type | This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate. |
| Action | Click the **View** button to open a screen with an in-depth list of information about the certificate (or certification request).<br>Click the **Remove** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use. |
| Import Certificate | Click this button to open a screen where you can save the certificate of a certification authority that you trust to the Router. |

### 17.2.1 View Trusted CA Certificate

Click the **View** icon in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority’s certificate.

**Figure 87** Trusted CA: View



**Certificate Details**

| | |
|---|---|
| Name | TR069 |
| Type | ca |
| Subject | O=Grupo Telefonica/O=TME/ST=A78923125/L=PZ. DE LA INDEPENDENCIA 6 28001 MADRID/CN=CA Telefonica Moviles Espana SA |
| Certificate | -----BEGIN CERTIFICATE-----<br>MIIELzCCA5igAwIBAgIEO3gsHjANBgkqhkiG9w0BAQUFADCBmDEZMBcGA<br>1UEChMQ<br>R3J1cG8gVGVsZWZvbmljYTEMMAoGA1UEChMDVE1FMRIwEAYDVQQIE<br>wIBNzg5MjMx<br>MjUxLzAtBgNVBAcTJlBaLiBERSBMQSBJTkRFUEVOREVOQ0lBIDYgMjgwM<br>DEgTUFE<br>UklEMSgwJgYDVQQDEx9DQSBUZWxlZm9uaWNhIE1vdmlsZXMgRXNwYW5<br>hIFNBMB4X<br>DTAxMDgxMzE5MDYwNVoXDTIxMDgxMzE5MzYwNVowgZgxGTAXBgNVBA<br>oTEEdydXBv<br>IFRlbGVmb25pY2ExDDAKBgNVBAoTA1RNRTESMBAGA1UECBMJQTc4O<br>TIzMTI1MS8w<br>LQYDVQQHEyZQWi4gREUgTEEgSU5ERVBFTkRFTkNJQSA2IDI4MDAxIE<br>1BRFJJRDEo<br>MCYGA1UEAxMfQ0EgVGVsZWZvbmljYSBNb3ZpbGVzIEVzcGFuYSBTQTC<br>BnzANBgkq<br>hkiG9w0BAQEFAAOBjQAwgYkCgYEA1a+VcjHsSdQ4cvcU/xkyc/hvOOlHFI<br>R5L7S/<br>EiiiFy10YbbyNdd3BEe2Yadj4Nqc8/mlnmpOMnjc1q2tRWe419HWgGhfCLki<br>8G0I |

The following table describes the fields in this screen.

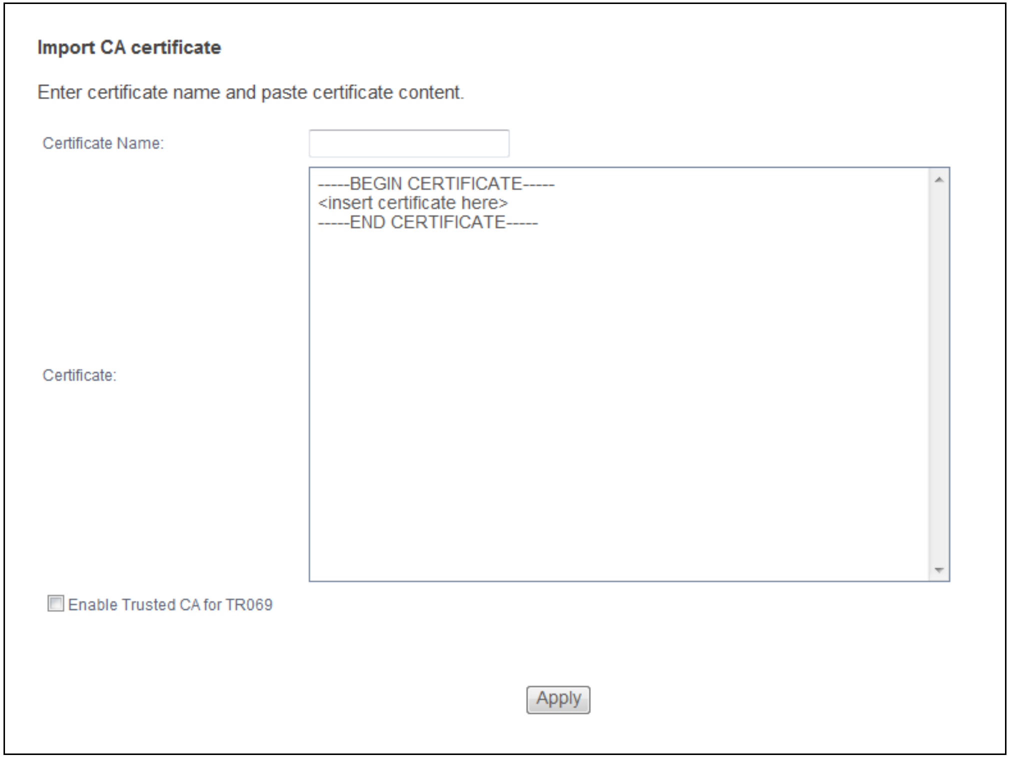
**Table 80** Trusted CA: View

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the identifying name of this certificate. |
| Type | This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate. |
| Subject | This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C). |
| Certificate | This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form.<br>You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example). |
| Back | Click **Back** to return to the previous screen. |

### 17.2.2 Import Trusted CA Certificate

Click the **Trusted CA** screen's **Import Certificate** button to open the following screen. The Router trusts any valid certificate signed by any of the imported trusted CA certificates.

**Figure 88** Trusted CA: Import Certificate



**Import CA certificate**

Enter certificate name and paste certificate content.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

□ Enable Trusted CA for TR069

The following table describes the fields in this screen.

**Table 81** Trusted CA: Import Certificate

| LABEL | DESCRIPTION |
|---|---|
| Certificate Name | Type a name for the signed certificate. |
| Certificate | Copy and paste the certificate into the text box to store it on the Router. |
| Enable Trusted CA for TR069 | Select this to have the Router use this trusted CA certificate to authenticate TR069 connections. |
| Apply | Click this to save your changes. |

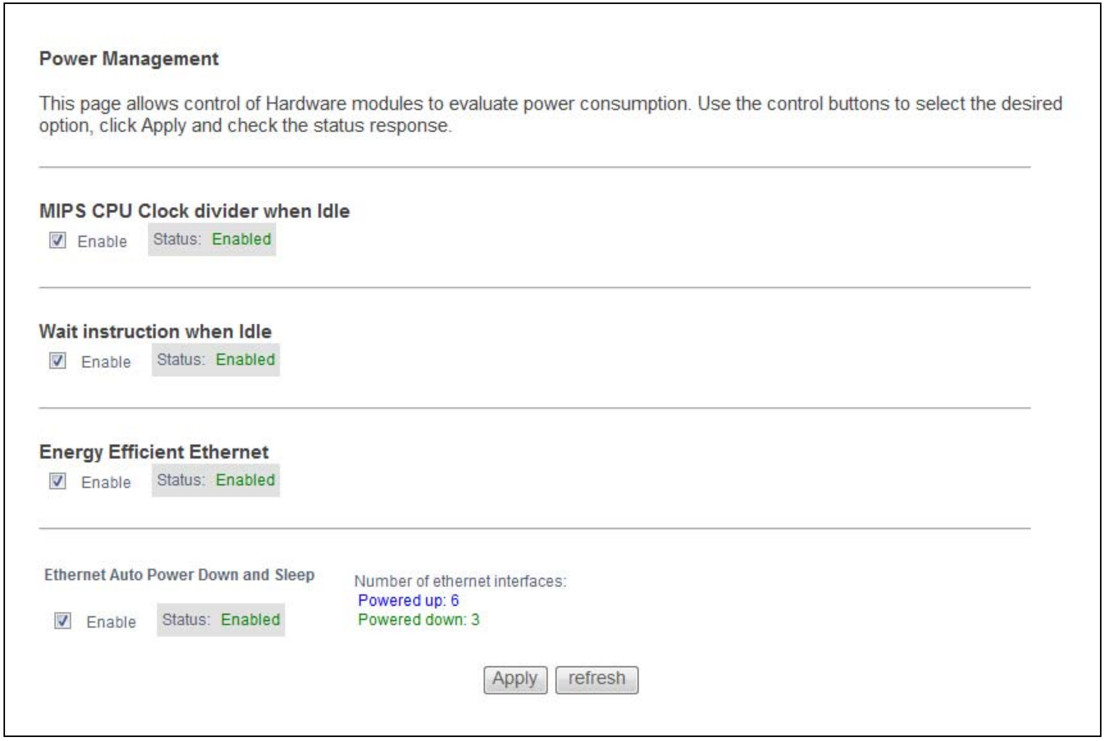
# Power Management

# 18 Chapter

## 18.1 Power Management

Click **Advanced Setup > Power Management** to control hardware modules to reduce power consumption. Use the control buttons to select the desired option, click **Apply** and check the status response.

Figure 89 Power Management



Power Management

This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the status response.

MIPS CPU Clock divider when Idle

☑ Enable Status: Enabled

Wait instruction when Idle

☑ Enable Status: Enabled

Energy Efficient Ethernet

☑ Enable Status: Enabled

Ethernet Auto Power Down and Sleep

☑ Enable Status: Enabled

Number of ethernet interfaces:
Powered up: 6
Powered down: 3

Table 82 Power Management

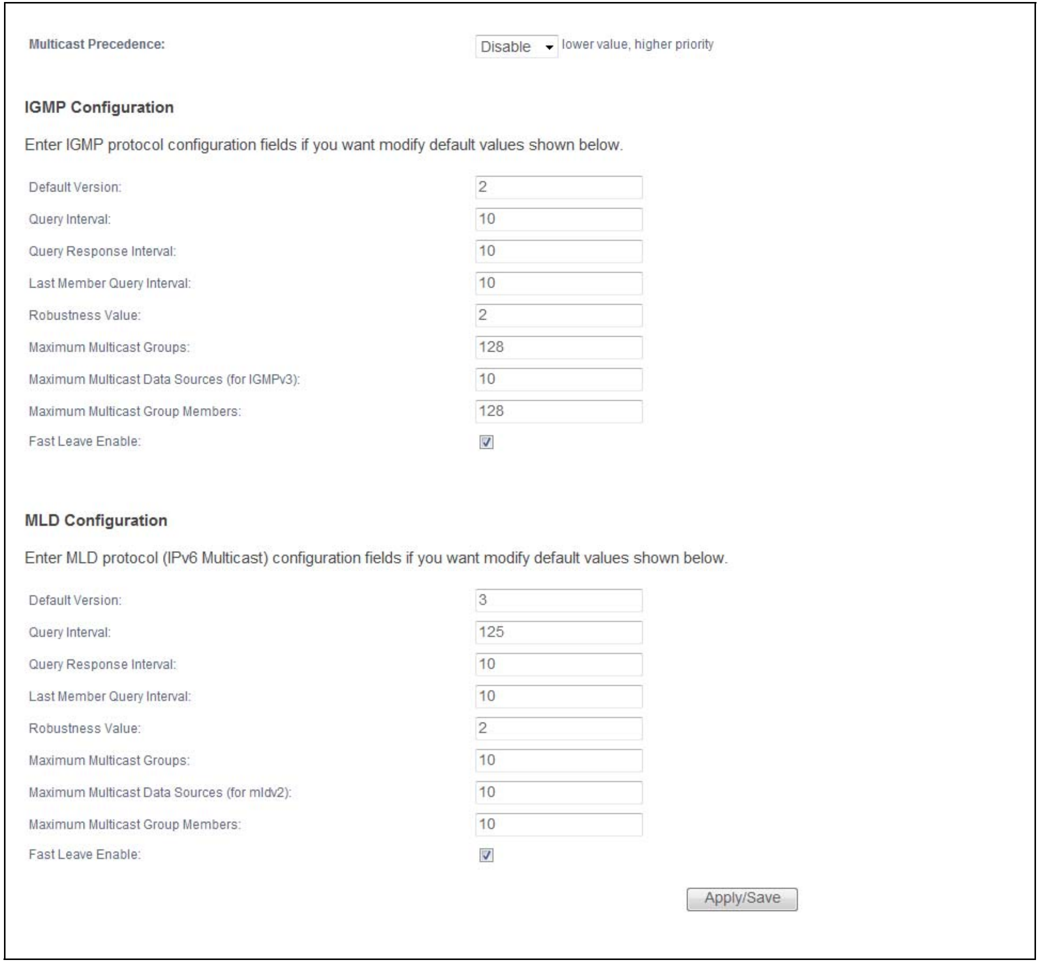
| LABEL | DESCRIPTION |
|---|---|
| MIPS CPU Clock divider when Idle | Select **Enable** to reduce the MIPS CPU’s clock  when idle to reduce power usage. Clear this to always run the MIPS CPU at full speed. |
| Wait instruction when Idle | Select **Enable** to put the CPU to sleep when idle to reduce power usage. Clear this to always keep the CPU running. |
| Energy Efficient Ethernet | Select **Enable** to set the Ethernet interfaces to power saving mode. Clear this to turn off power saving on the Ethernet interfaces. |
| Ethernet Auto Power Down and Sleep | Select **Enable** to power down Ethernet interfaces when idle to reduce power usage. Clear this to keep the Ethernet interfaces always on.<br>The screen shows how many Ethernet interfaces are running and how many are powered down. |
| Apply | Click this button to save and apply your changes. |
| Refresh | Click this button to update the display in this screen. |

# Multicast

## 19.1 Multicast

Click **Advanced Setup > Multicast** to configure multicast and IGMP and MLD group settings.

**Figure 90** Multicast



| | |
|---|---|
| **Multicast Precedence:** | Disable ▾ lower value, higher priority |

**IGMP Configuration**

Enter IGMP protocol configuration fields if you want modify default values shown below.

| | |
|---|---|
| Default Version: | 2 |
| Query Interval: | 10 |
| Query Response Interval: | 10 |
| Last Member Query Interval: | 10 |
| Robustness Value: | 2 |
| Maximum Multicast Groups: | 128 |
| Maximum Multicast Data Sources (for IGMPv3): | 10 |
| Maximum Multicast Group Members: | 128 |
| Fast Leave Enable: | ☑ |

**MLD Configuration**

Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

| | |
|---|---|
| Default Version: | 3 |
| Query Interval: | 125 |
| Query Response Interval: | 10 |
| Last Member Query Interval: | 10 |
| Robustness Value: | 2 |
| Maximum Multicast Groups: | 10 |
| Maximum Multicast Data Sources (for mldv2): | 10 |
| Maximum Multicast Group Members: | 10 |
| Fast Leave Enable: | ☑ |

**Table 83** Multicast

| LABEL | DESCRIPTION |
|---|---|
| Multicast Precedence | Set the Router’s multicast precedence (1 to 9) or disable multicast on the Router. The lower the number, the higher the Router’s multicast priority. |
| IGMP/MLD Configuration | |
| Default Version | Enter the version of IGMP (1~3) and MLD (1~2) that you want the Router to use on the WAN. |
| Query Interval | Specify how many seconds since the last query the Router waits before it queries all directly connected networks to gather multicast group membership. |
| Query Response Interval | Enter the maximum number of seconds the Router can wait to receive a General Query message.  Multicast routers use general queries to learn which multicast groups have members. |
| Last Member Query Interval | Enter the maximum number of seconds the Router can wait for receiving a response to a Group-Specific Query message. Multicast routers use group-specific queries to learn whether any member remains in a specific multicast group. |
| Robustness Value | Enter the number of times (1~7) the Router can resend a packet if packet loss occurs due to network congestion. |
| Maximum Multicast Groups | Enter a number to limit the number of multicast groups an interface on the Router is allowed to join. Once a multicast member is registered in the specified number of multicast groups, any new IGMP or MLD join report frames are dropped by the interface. |
| Maximum Multicast Data Sources | Enter a number to limit the number of multicast data sources (1-24) a multicast group is allowed to have. Note: The setting only works for IGMPv3 and MLDv2. |
| Maximum Multicast Group Members | Enter a number to limit the number of multicast members a multicast group can have. |
| Fast Leave Enable | Select this option to set the Router to remove a port from the multicast tree immediately (without sending an IGMP or MLD membership query message) once it receives an IGMP or MLD leave message. This is helpful if a user wants to quickly change a TV channel (multicast group change) especially for IPTV applications. |
| Apply/Save | Click this button to save your changes. |

# Wireless

# 20 Chapter

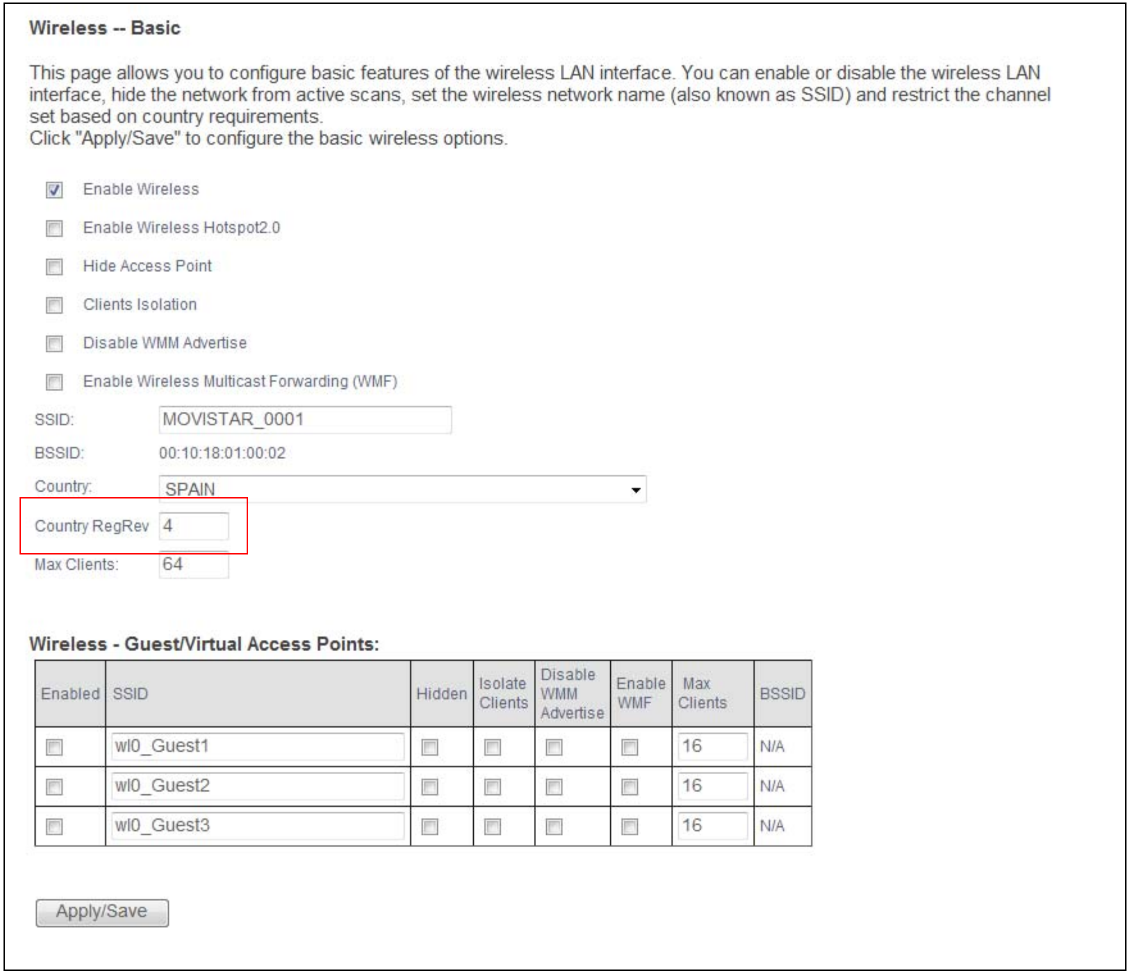
## 20.1 Wireless Basic

Use the **Advanced Setup > Wireless** screens to configure the 2.4 GHz wireless network.

Click **Advanced Setup > Wireless** to enable  or disable the 2.4 GHz Wireless LAN and configure basic settings.

ⓘ If you are configuring the Router from a computer connected to the wireless LAN and you change the Router’s SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the Router’s new settings.

**Figure 91** Wireless Basic



**Wireless -- Basic**

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.
Click "Apply/Save" to configure the basic wireless options.

☑ Enable Wireless

□ Enable Wireless Hotspot2.0

□ Hide Access Point

□ Clients Isolation

□ Disable WMM Advertise

□ Enable Wireless Multicast Forwarding (WMF)

| | |
|---|---|
| SSID: | MOVISTAR_0001 |
| BSSID: | 00:10:18:01:00:02 |
| Country: | SPAIN |
| Country RegRev | 4 |
| Max Clients: | 64 |

**Wireless - Guest/Virtual Access Points:**

| Enabled | SSID | Hidden | Isolate Clients | Disable WMM Advertise | Enable WMF | Max Clients | BSSID |
|---|---|---|---|---|---|---|---|
| □ | wl0_Guest1 | □ | □ | □ | □ | 16 | N/A |
| □ | wl0_Guest2 | □ | □ | □ | □ | 16 | N/A |
| □ | wl0_Guest3 | □ | □ | □ | □ | 16 | N/A |

**Table 84** Wireless Basic

| LABEL | DESCRIPTION |
|---|---|
| Enable Wireless | Select this check box to activate the wireless LAN. |
| Enable Wireless Hotspot2.0 | |
| Hide Access Point | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. |
| Clients Isolation | Select this to keep the wireless clients in this SSID from communicating with each other directly through the Router. |
| Disable WMM Advertise | WMM (Wifi MultiMedia) automatically prioritizes services according to the ToS value in the IP header of packets. Turn off WMM if your wireless clients are not able to associate with an AP using WMM. |

Table 84 Wireless Basic (continued)

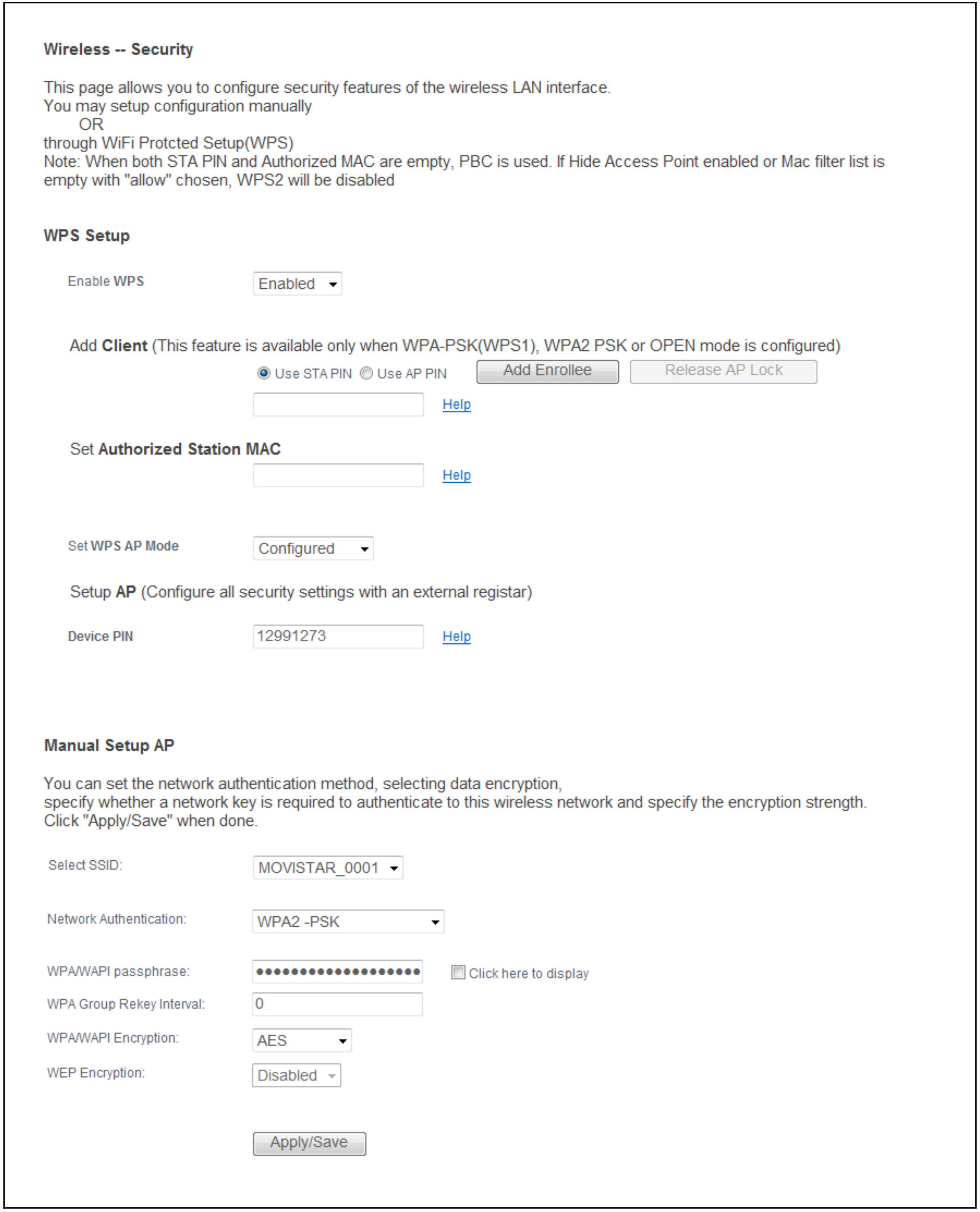
| LABEL | DESCRIPTION |
|---|---|
| Enable Wireless Multicast Forwarding | Select this check box to have the Router convert wireless multicast traffic (IGMP version 2 or 3) into wireless unicast traffic to reduce the traffic load. This function can improve the transmission quality of video services (for example, IPTV). |
| SSID | Enter a descriptive name for the wireless LAN. |
| BSSID | This shows the MAC address of the wireless interface on the Device when wireless LAN is enabled. |
| Country | Select the country you have the Router in. This has the Router use the correct frequency bands. |
| Country RegRev | Specify the sub-revision of the regulatory locale table for the country code. |
| Max Clients | Set a limit for how many wireless clients can connect to the Router at a time. |
| Wireless Guest/ Virtual Access Points | Use this section to enable and configure multiple wireless networks on the Router. |
| Enabled | Select this to activate the wireless network. |
| SSID | The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.<br>Note: If you are configuring the Router from a computer connected to the wireless LAN and you change the Router's SSID or WEP settings, you will lose your wireless connection when you press **Save/Apply** to confirm. You must then change the wireless settings of your computer to match the Router's new settings. |
| Hidden | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. |
| Isolate Clients | Select this to isolate wireless clients from accessing others in the same wireless network. |
| Enable WMF | Select this check box to improve the wireless transmission quality for multicast frames. It is recommended to select this for video streaming application. |
| Max Clients | Set a limit for how many wireless clients can connect to the wireless network at a time. |
| BSSID | This shows the MAC address of the wireless network on the Device when the wireless network is enabled. |
| Apply/Save | Click this button to save your changes. |

## 20.2 Wireless Security

Click **Wireless > Security** to open the **Security** screen. Set **Network Authentication** to **Open** and **WEP Encryption** to **Disabled** to allow wireless stations to communicate with the Router without any data encryption or authentication.

ⓘ If you do not enable any wireless security on your Router, your network is accessible to any wireless networking device that is within range.

**Figure 92** Wireless Security



**Wireless -- Security**

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protcted Setup(WPS)
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

**WPS Setup**

Enable **WPS**: Enabled

Add **Client** (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)

● Use STA PIN ○ Use AP PIN

Set **Authorized Station MAC**

Set **WPS AP Mode**: Configured

Setup **AP** (Configure all security settings with an external registar)

**Device PIN**: 12991273

**Manual Setup AP**

You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID: MOVISTAR_0001

Network Authentication: WPA2 -PSK

WPA/WAPI passphrase: ••••••••••••••••••• □ Click here to display

WPA Group Rekey Interval: 0

WPA/WAPI Encryption: AES

WEP Encryption: Disabled

Table 85 Wireless Security

| LABEL | DESCRIPTION |
|---|---|
| Enable WPS | Use WiFi Protected Setup (WPS) to quickly set up a wireless network without having to manually configure settings. Set up each WPS connection between two devices at a time. |
| Add Client | Use this section to add a wireless client to the wireless network.<br>Select **Use STA PIN** to add a client by entering the client's Personal Identification Number (PIN) in the field that displays when you select this option.<br>Select **Use AP PIN** to add a client by entering the AP's PIN from the **Device PIN** field in the client's WPS configuration. |
| Add Enrollee | Click this to use WPS to add a wireless client to your wireless network.<br>Note: You must also activate WPS on the client within two minutes. |
| Release AP Lock | Click this to unlock the Router's AP function if WPS locked it due to unauthorized wireless access attempts. |
| Set Authorized Station MAC | If you select **Enter STA PIN** as your method to add a client, you may enter the MAC address of an authorized wireless client here. |
| Set WPS AP Mode | **Configured** uses the Router's current wireless security settings for WPS.<br>**Unconfigured** has the Router change its wireless security settings when you do one of the following:<br>• Add a wireless enrollee. The Router automatically uses WPA2-PSK and a random key. The **WPS AP Mode** automatically changes to **Configured**.<br>• Use **Setup AP** to have an external registrar (like Windows Vista) configure the Router's wireless security settings. The **WPS AP Mode** automatically changes to **Configured**.<br>• Manually configure the Router's wireless security settings. Then you can manually set the **WPS AP Mode** to **Configured**. |
| Device PIN | This shows the Router's PIN. Enter this PIN in the external registrar within two minutes of clicking **Generate PIN**.<br>Enter this PIN in the client's WPS configuration if you selected **Use AP PIN**. |
| Select SSID | Select an SSID for which to configure wireless security settings. |
| Network Authentication | Use the strongest authentication method that the wireless clients all support.<br>**WPA2-PSK** uses a common password for all clients.<br>**Mixed WPA2/WPA -PSK** supports WPA2-PSK and WPA-PSK simultaneously. While WPA2-PSK offers stronger security, more wireless clients support WPA-PSK.<br>**Shared** - encrypts the wireless communications using a shared (WEP) password.<br>Choose **Open** to allow all wireless connections without authentication. |

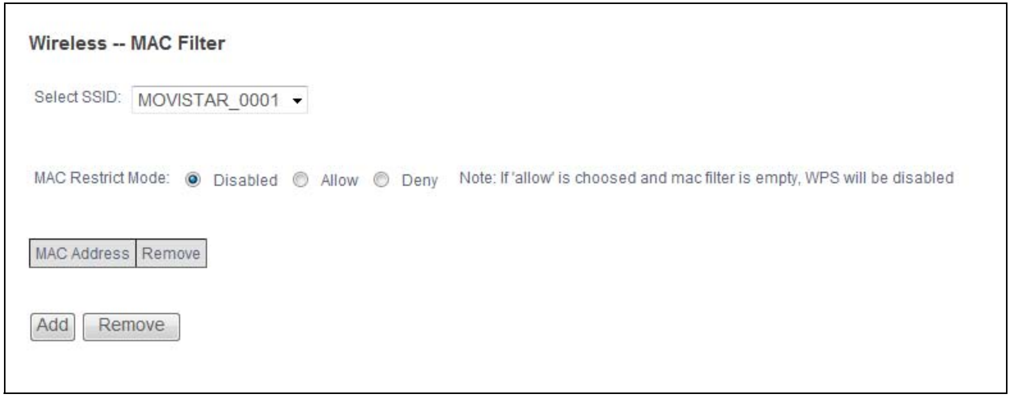
**Table 85** Wireless Security

| LABEL | DESCRIPTION |
|---|---|
| WPA/WAPI passphrase | This field displays when you select WPA2-PSK or Mixed WPA2/WPA -PSK.<br>Use the automatically generated password or enter 16 to 63 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive. Click the link to display the password. |
| WPA Group Rekey Interval | Set the rate at which the AP (if using WPA2/WPA-PSK key management) or RADIUS server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. |
| WPA/WAPI Encryption | Select the encryption type (**AES** or **TKIP+AES**) for data encryption.<br>Select **AES** if your wireless clients can all use AES.<br>Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES. |
| WEP Encryption | This field displays when you set **Network Authentication** to **Open**. Enable WEP encryption to scramble the wireless data transmissions between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.<br>Note: WEP is extremely insecure. Attackers can break it using widely-available software. It is strongly recommended that you use a more effective security mechanism. |
| Encryption Strength | If you are using WEP encryption, select **64-bit** or **128-bit** to set the length of the encryption key. |
| Current Network Key | This field displays when you enable WEP encryption. Configure up to four 64-bit or 128-bit WEP keys. Use this field to select which one the network uses. |
| Network Key 1~4 | These fields display when you enable WEP encryption. WEP uses a network key to encrypt data. The Router and wireless clients must use the same network key (password).<br>If you chose **64-bit** WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").<br>If you chose **128-bit** WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").<br>You must configure at least one password. |
| Apply/Save | Click this button to save your changes. |

## 20.3 Wireless MAC Filter

Click **Wireless > MAC Filter** to open the **MAC Filter** screen. This screen allows you to configure the Router to give exclusive access to specific devices **(Allow)** or exclude specific devices from accessing the Router **(Deny)**. Every Ethernet device has a unique MAC (Media Access Control) address assigned at the factory. It consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

**Figure 93** Wireless MAC Filter



Wireless -- MAC Filter

Select SSID: MOVISTAR_0001

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

| MAC Address | Remove |
|---|---|

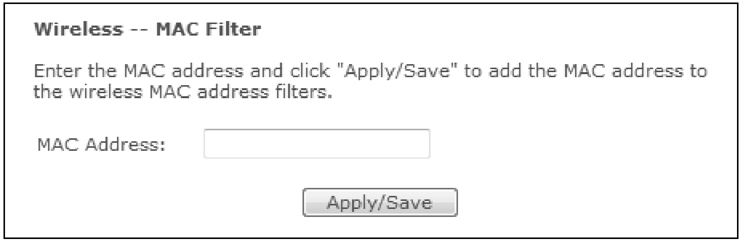
**Table 86** Wireless MAC Filter

| LABEL | DESCRIPTION |
|---|---|
| Select SSID | Select an SSID for which to configure MAC filter settings. |
| MAC Restrict Mode | Define the filter action for the list of MAC addresses in the **MAC Address** table.<br>Select **Disabled** to turn off MAC filtering.<br>Select **Allow** to permit access to the Router. MAC addresses not listed will be denied access to the Router.<br>Select **Deny** to block access to the Router. MAC addresses not listed will be allowed to access the Router. |
| MAC Address | This displays the MAC addresses of the wireless devices that are allowed or denied access to the Router. |
| Remove | Select entries and click the **Remove** button to delete them. |
| Add | Click this to add a new MAC address entry to the table. |

### 20.3.1 Wireless MAC Filter Add

Use this screen to add MAC address entries. Click **Wireless > MAC Filter > Add** to open the following screen.

**Figure 94** Wireless MAC Filter Add



**Wireless -- MAC Filter**

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address:

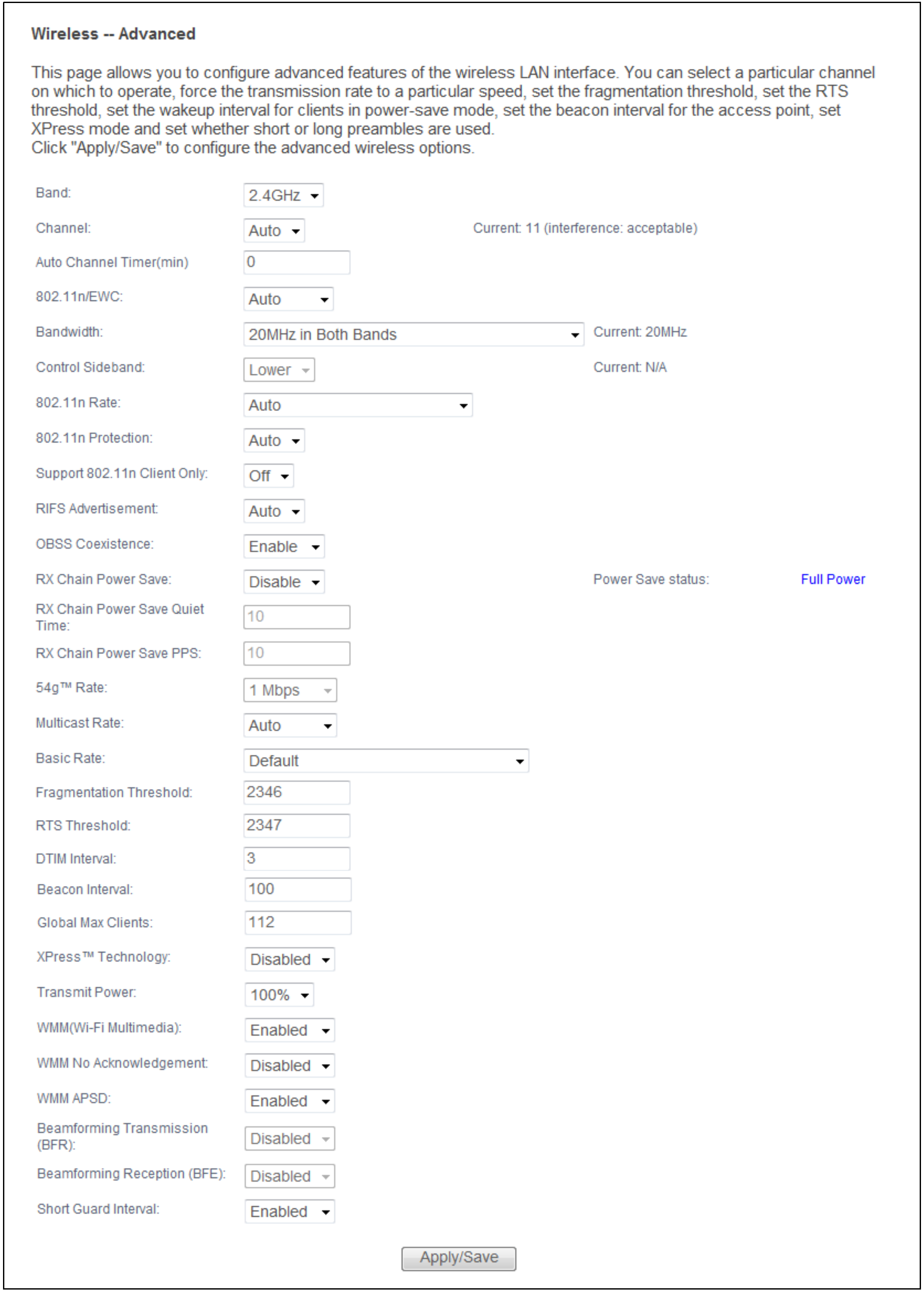
**Table 87** Wireless MAC Filter Add

| LABEL | DESCRIPTION |
|---|---|
| MAC Address | Enter the MAC address of the wireless device that is to be allowed or denied access to the Router. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. |
| Save/Apply | Click this button to save the changes and have the Router start using them. |

## 20.4 Wireless Advanced

Click **Wireless > Advanced** to configure advanced wireless settings.

**Figure 95** Wireless Advanced



**Wireless -- Advanced**

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.
Click "Apply/Save" to configure the advanced wireless options.

| | | | |
|---|---|---|---|
| Band: | 2.4GHz | | |
| Channel: | Auto | Current: 11 (interference: acceptable) | |
| Auto Channel Timer(min) | 0 | | |
| 802.11n/EWC: | Auto | | |
| Bandwidth: | 20MHz in Both Bands | Current: 20MHz | |
| Control Sideband: | Lower | Current: N/A | |
| 802.11n Rate: | Auto | | |
| 802.11n Protection: | Auto | | |
| Support 802.11n Client Only: | Off | | |
| RIFS Advertisement: | Auto | | |
| OBSS Coexistence: | Enable | | |
| RX Chain Power Save: | Disable | Power Save status: | Full Power |
| RX Chain Power Save Quiet Time: | 10 | | |
| RX Chain Power Save PPS: | 10 | | |
| 54g™ Rate: | 1 Mbps | | |
| Multicast Rate: | Auto | | |
| Basic Rate: | Default | | |
| Fragmentation Threshold: | 2346 | | |
| RTS Threshold: | 2347 | | |
| DTIM Interval: | 3 | | |
| Beacon Interval: | 100 | | |
| Global Max Clients: | 112 | | |
| XPress™ Technology: | Disabled | | |
| Transmit Power: | 100% | | |
| WMM(Wi-Fi Multimedia): | Enabled | | |
| WMM No Acknowledgement: | Disabled | | |
| WMM APSD: | Enabled | | |
| Beamforming Transmission (BFR): | Disabled | | |
| Beamforming Reception (BFE): | Disabled | | |
| Short Guard Interval: | Enabled | | |

**Table 88** Wireless Advanced

| LABEL | DESCRIPTION |
|---|---|
| Band | Select an operating band to use. |
| Channel | Select an operating channel to use. The choices depend on your particular region. Either select a channel or use **Auto** to have the Router automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. |
| Auto Channel Timer | If you set the channel to **Auto**, specify the interval in minutes for how often the Router scans for the best channel. Enter 0 to disable the periodical scan. |
| 802.11n/EWC | Select whether to enable (**Auto**) or disable (**Disabled**) the use of the wireless 802.11n modes defined by the Enhanced Wireless Consortium (EWC). These modes can enhance speeds although the wireless clients must also support the EWC modes. |
| Bandwidth | **20MHz in Both Bands** uses a single radio channel in the 2.4 GHz band and a single radio channel in the 5.0 GHz band. Use this if the wireless clients do not support channel bonding.<br>**40MHz in Both Bands** bonds two adjacent radio channels in the 2.4 GHz band and two adjacent radio channels in the 5.0 GHz band.<br>40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.<br>**20MHz in 2.4G Band and 40MHz in 5G Band** uses a single radio channel in the 2.4 GHz band and bonds two adjacent radio channel in the 5.0 GHz band. Use this if you have IEEE 802.11b and/or g clients that do not support 40 MHz and IEEE 802.11n clients that do. |
| Control Sideband | This is available for some regions when you select a specific channel and set the **Bandwidth** field to **40MHz in Both Bands**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands. |
| 802.11n Rate | Select a fixed transmission rate or select **Auto** to have the system configure it automatically. |
| 802.11n Protection | Enable this feature to help prevent collisions in mixed-mode networks (networks with both IEEE 802.11n and IEEE 802.11g traffic).<br>Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11n performance.<br>Select **Off** to disable IEEE 802.11n protection. The transmission rate of your Router might be reduced in a mixed-mode network. |
| Support 802.11n Client Only | Select this to only allow IEEE 802.11n wireless clients to connect to the Router. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the Router. |
| RIFS Advertisement | Select **Auto** to enable the Reduced Inter-frame Spacing (RIFS) feature. It improves the Router’s performance by reducing the amount of dead time required between OFDM transmissions. |

Table 88 Wireless Advanced (continued)

| LABEL | DESCRIPTION |
|---|---|
| OBSS Co-Existance | Select **Enable** to allow coexistence between 20 MHZ and 40 MHZ Overlapping Basic Service Sets (OBSS) in wireless local area networks. |
| RX Chain Power Save | Select **Enable** to activate the RX Chain Power Save feature. It turns off one of the Receive chains to save power. |
| RX Chain Power Save Quiet Time | Specify the number of seconds the traffic must be below the PPS value before the Rx Chain Power Save feature is activated. |
| RX Chain Power Save PPS | Specify the maximum number of packets per second that can be processed by the WLAN interface for a time period (specified in the **RX Chain Power Save Quiet Time** field) before the Rx Chain Power Save feature is activated. |
| 54g™ Rate | This field is available when **802.11n/EWC** is set to **Disabled**.<br>Select a fixed wireless transmission rate or let the Router and the wireless client automatically select a rate. |
| Multicast Rate | Select a data rate at which the Router transmits wireless multicast traffic.<br>If you select a high rate, multicast traffic may occupy all the bandwidth and cause network congestion. |
| Basic Rate | Select a minimum transmission rate. |
| Fragmentation Threshold | This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432. |
| RTS Threshold | Use CTS/RTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions).<br>A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS equal to or higher than the fragmentation threshold to turn RTS off. |
| DTIM Interval | Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with<br>the network. This value can be set from 1 to 100. |
| Beacon Interval | When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again.<br>The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 20ms to 1000ms. A high value helps save current consumption of the access point. |
| Global Max Clients | Specify the maximum number (from 1 to 64) of the wireless stations that may connect to the Router. |
| XPress™ Technology | Select this for higher speeds, especially if you have both IEEE 802.11b and IEEE 802.11g wireless clients. The wireless clients do not have to support XPress™ Technology, although the performance enhancement is greater if they do. |

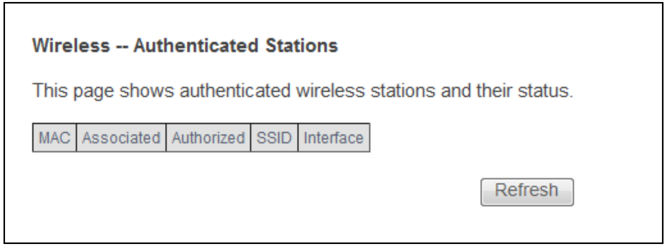
Table 88 Wireless Advanced (continued)

| LABEL | DESCRIPTION |
|---|---|
| Transmit Power | Set the output power of the Router. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. |
| WMM (Wi-Fi Multimedia) | Use WMM (Wifi MultiMedia) to prioritize services in wireless traffic.<br>Select **Auto** to automatically prioritize services according to the ToS value in the IP header of packets.<br>Select **Enable** to prioritize services according to the Router's Quality of Service settings.<br>Select **Disable** to not prioritize services in wireless traffic. |
| WMM No Acknowledgement | When using WMM, you can enable this to have the Router not re-send data if an error occurs. This can increase throughput speed but may also increase errors, especially in an environment with a lot of Radio Frequency (RF) noise. Otherwise leave it disabled. |
| WMM APSD | When using WMM, enable APSD (Automatic Power Save Delivery) to have the Router manage radio usage to help increase battery life for battery-powered wireless clients. APSD uses a longer beacon interval when transmitting traffic that does not require a short packet exchange interval. For example, web browsing or using e-mail does not require a short packet exchange interval but Voice Over IP (VoIP) does. The wireless client must also support APSD for there to be any affect on the battery life. |
| Beamforming Transmission | Enable beamforming to have the Router focus the wireless signal and aim it directly at the wireless clients. Clear this option to disable beamforming. You may need to do this if beamforming causes issues with IEEE 802.11 N, G, or B devices. |
| Short Guard Interval | Enable short guard interval option to set the Router to use a reduced guard interval. This increases throughput at the cost of an increased error rate in certain network environments with greater radio interference. |
| Apply/Save | Click this to save your changes back to the Router. |

## 20.5 Wireless Station Info

The station monitor displays the connection status of the wireless clients connected to (or trying to connect to) the Router. To open the station monitor, click **Wireless** > **Station Info**. The screen appears as shown.

Figure 96 Wireless Station Info



Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

| MAC | Associated | Authorized | SSID | Interface |
|---|---|---|---|---|

The following table describes the labels in this menu.

Table 89 Wireless Station Info

| LABEL | DESCRIPTION |
|---|---|
| MAC | This displays the MAC address (in XX:XX:XX:XX:XX:XX format) of a connected wireless station. |
| Associated | This is the time that the wireless client associated with the Router. |
| Authorized | This is the time that the wireless client’s connection to the Router was authorized. |
| SSID | This is the name of the wireless network on the Router to which the wireless client is connected. |
| Interface | This is the name of the wireless LAN interface on the Router to which the wireless client is connected. |
| Refresh | Click this button to update the information in the screen. |

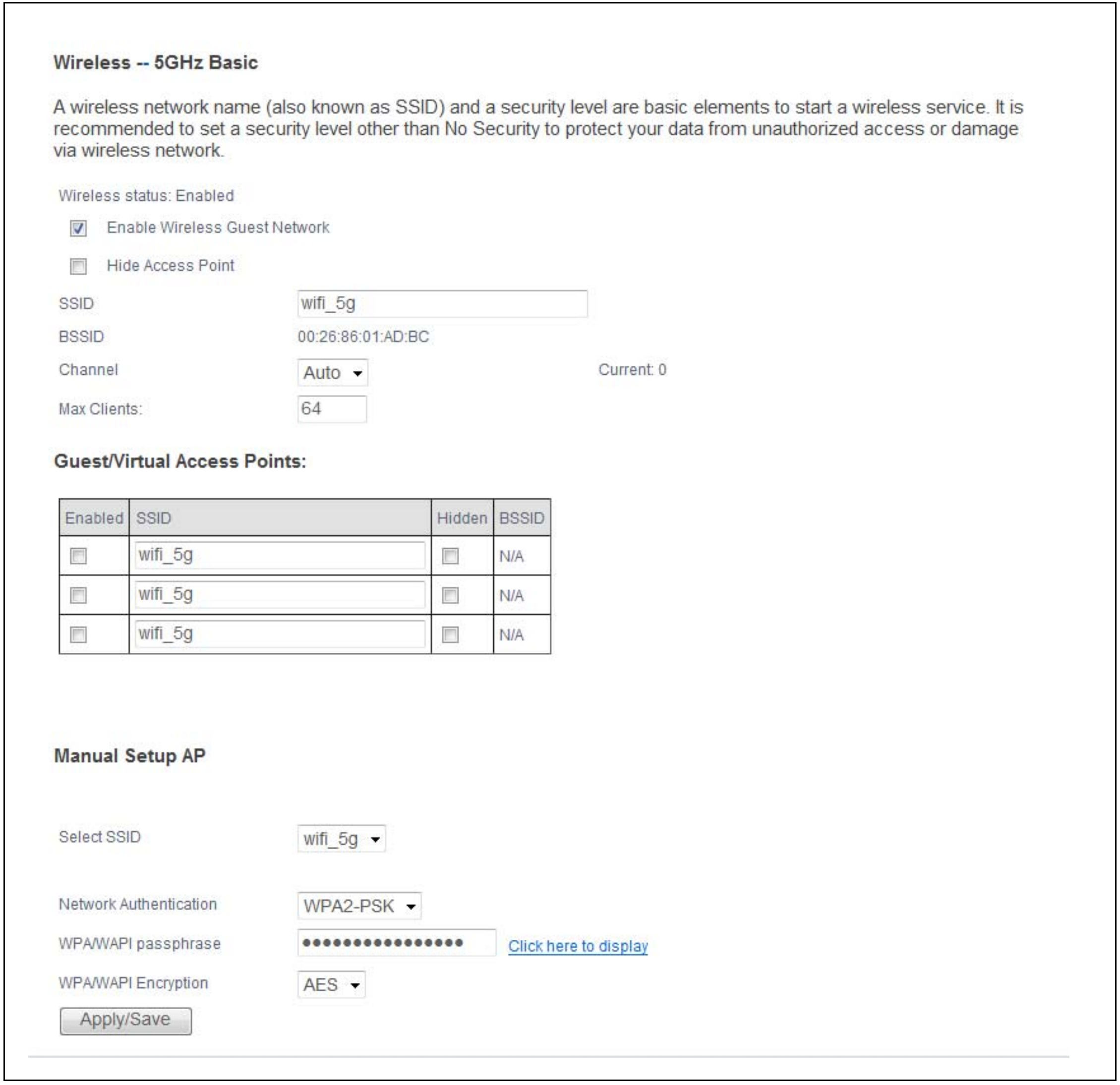
## 20.6 Wireless 5GHz Basic

Use the **Advanced Setup > Wireless 5GHz** screens to configure the 5 GHz wireless network.

Click **Advanced Setup > Wireless 5GHz** to enable the 5 GHz Wireless LAN and set the wireless security.

ⓘ If you are configuring the Router from a computer connected to the wireless LAN and you change the Router’s SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the Router’s new settings.

**Figure 97** Wireless 5GHz Basic



**Wireless -- 5GHz Basic**

A wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than No Security to protect your data from unauthorized access or damage via wireless network.

Wireless status: Enabled

☑ Enable Wireless Guest Network

□ Hide Access Point

SSID: wifi_5g

BSSID: 00:26:86:01:AD:BC

Channel: Auto ▾ Current: 0

Max Clients: 64

**Guest/Virtual Access Points:**

| Enabled | SSID | Hidden | BSSID |
|---|---|---|---|
| □ | wifi_5g | □ | N/A |
| □ | wifi_5g | □ | N/A |
| □ | wifi_5g | □ | N/A |

**Manual Setup AP**

Select SSID: wifi_5g ▾

Network Authentication: WPA2-PSK ▾

WPA/WAPI passphrase: ●●●●●●●●●●●●●●●● Click here to display

WPA/WAPI Encryption: AES ▾

**Table 90** Wireless 5GHz Basic

| LABEL | DESCRIPTION |
|---|---|
| Enable Wireless Guest Network | Select this check box to activate the guest wireless LAN. |
| Hide Access Point | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. |

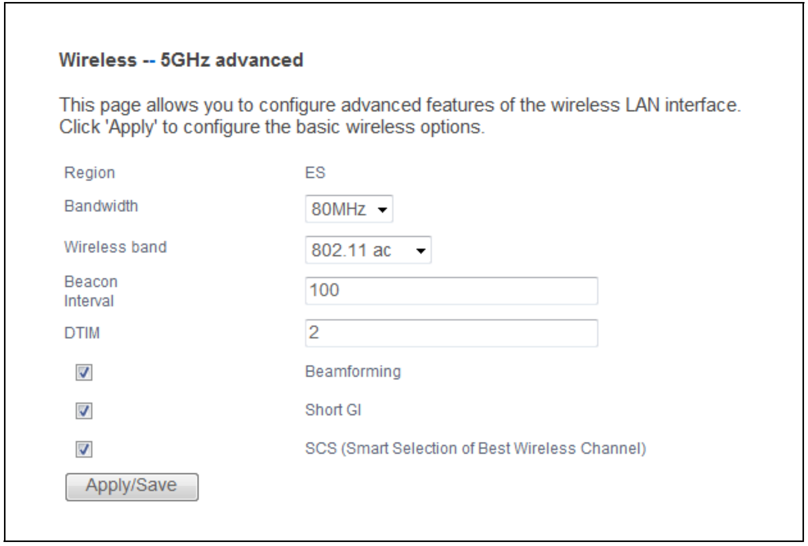
**Table 90** Wireless 5GHz Basic (continued)

| LABEL | DESCRIPTION |
|---|---|
| SSID | Enter a descriptive name for the wireless LAN. |
| BSSID | This shows the MAC address of the wireless interface on the Device when wireless LAN is enabled. |
| Country | Select the country you have the Router in. This has the Router use the correct frequency bands. |
| Channel | Select an operating channel to use. The choices depend on your particular region. Either select a channel or use **Auto** to have the Router automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. |
| Max Clients | Set a limit for how many wireless clients can connect to the Router at a time. |
| Guest/Virtual Access Points | Use this section to enable and configure multiple wireless networks on the Router. |
| Enabled | Select this to activate the wireless network. |
| SSID | The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.<br>Note: If you are configuring the Router from a computer connected to the wireless LAN and you change the Router's SSID or WEP settings, you will lose your wireless connection when you press **Save/Apply** to confirm. You must then change the wireless settings of your computer to match the Router's new settings. |
| Hidden | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. |
| BSSID | This shows the MAC address of the wireless network on the Device when the wireless network is enabled. |
| Select SSID | Select an SSID for which to configure wireless security settings. |
| Network Authentication | Use the strongest authentication method that the wireless clients all support.<br>**WPA2-PSK** uses a common password for all clients. While WPA2-PSK offers stronger security, more wireless clients support WPA-PSK.<br>Choose **Open** to allow all wireless connections without authentication. |
| WPA/WAPI passphrase | This field displays when you select WPA2-PSK<br>Use the automatically generated password or enter 16 to 63 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive. Click the link to display the password. |
| WPA/WAPI Encryption | Select the encryption type for data encryption.<br>Select **AES** if your wireless clients can all use AES. |
| Apply/Save | Click this button to save your changes. |

## 20.7 Wireless 5GHz Advanced Screen

Click **Wireless 5GHz > Advanced** to configure advanced 5 GHz wireless settings.

**Figure 98** Wireless 5GHz Advanced



**Wireless -- 5GHz advanced**

This page allows you to configure advanced features of the wireless LAN interface.
Click 'Apply' to configure the basic wireless options.

| | |
|---|---|
| Region | ES |
| Bandwidth | 80MHz |
| Wireless band | 802.11 ac |
| Beacon Interval | 100 |
| DTIM | 2 |
| ☑ | Beamforming |
| ☑ | Short GI |
| ☑ | SCS (Smart Selection of Best Wireless Channel) |

**Table 91** Wireless 5GHz Advanced

| LABEL | DESCRIPTION |
|---|---|
| Region | Select an operating band to use. |
| Bandwidth | Select whether the Device uses a wireless channel width of 20MHz, 40MHz, or 80MHz.<br>A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps, and a 80MHz channel uses only one channel and offers speeds of up to 433 Mbps.<br>A wider band enables higher transmission rates. A 40MHz (channel bonding or dual channel) channel bonds two adjacent radio channels to increase throughput. An 80MHz channel bonds two adjacent 40 MHz channels to get even higher data rates. The wireless clients must also support 40 MHz or 80 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.<br>Select **20MHz** to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. |
| Wireless band | Select whether to use IEEE 802.11 ac or IEEE 802.11 ac and IEEE 802.11n wireless. |
| Beacon Interval | When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again.<br>The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 20ms to 1000ms. A high value helps save current consumption of the access point. |

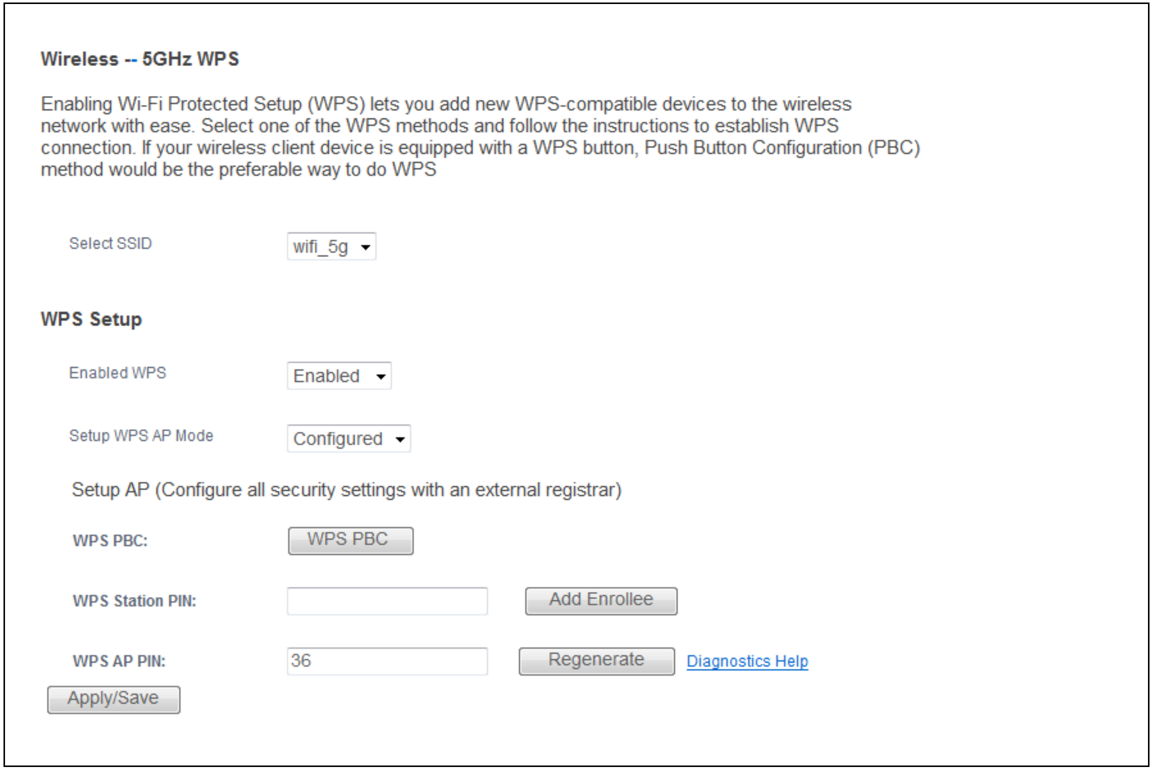
**Table 91** Wireless 5GHz Advanced (continued)

| LABEL | DESCRIPTION |
|---|---|
| DTIM | Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with<br>the network. This value can be set from 1 to 100. |
| Beamforming | Select this option to have the Router focus the wireless signal and aim it directly at the wireless clients. Clear this option to disable beamforming. You may need to do this if beamforming causes issues with IEEE 802.11 N, G, or B devices. |
| Short GI | Select this option to set the Router to use a reduced guard interval. This increases throughput at the cost of an increased error rate in certain network environments with greater radio interference. |
| SCS | Select this to have the Router automatically determine and select the most suitable wireless channel. |
| Apply/Save | Click this to save your changes back to the Router. |

## 20.8 Wireless 5GHz WPS

Click **Wireless 5GHz > WPS** to open the **WPS** screen. Enabling Wi-Fi Protected Setup (WPS) lets you add new WPS-compatible devices to the wireless network with ease.

**Figure 99** Wireless 5GHz WPS



**Wireless -- 5GHz WPS**

Enabling Wi-Fi Protected Setup (WPS) lets you add new WPS-compatible devices to the wireless network with ease. Select one of the WPS methods and follow the instructions to establish WPS connection. If your wireless client device is equipped with a WPS button, Push Button Configuration (PBC) method would be the preferable way to do WPS

Select SSID: wifi_5g

**WPS Setup**

Enabled WPS: Enabled

Setup WPS AP Mode: Configured

Setup AP (Configure all security settings with an external registrar)

WPS PBC:

WPS Station PIN:

WPS AP PIN: 36

**Table 92** Wireless 5GHz WPS

| LABEL | DESCRIPTION |
|---|---|
| Enable WPS | Use WiFi Protected Setup (WPS) to quickly set up a wireless network without having to manually configure settings. Set up each WPS connection between two devices at a time. |
| Add Client | Use this section to add a wireless client to the wireless network.<br>Select **Use STA PIN** to add a client by entering the client's Personal Identification Number (PIN) in the field that displays when you select this option.<br>Select **Use AP PIN** to add a client by entering the AP's PIN from the **Device PIN** field in the client's WPS configuration. |
| Add Enrollee | Click this to use WPS to add a wireless client to your wireless network.<br>Note: You must also activate WPS on the client within two minutes. |
| Release AP Lock | Click this to unlock the Router's AP function if WPS locked it due to unauthorized wireless access attempts. |
| Set Authorized Station MAC | If you select **Enter STA PIN** as your method to add a client, you may enter the MAC address of an authorized wireless client here. |

Table 92 Wireless 5GHz WPS (continued)

| LABEL | DESCRIPTION |
|---|---|
| Select SSID | Select an SSID for which to configure security settings. |
| Enabled WPS | Use WiFi Protected Setup (WPS) to quickly set up a wireless network without having to manually configure settings. Set up each WPS connection between two devices at a time. WPS is not available when using WPA or WPA 2. |
| Setup WPS AP Mode | Use an external registrar (like Windows Vista) configure the Router's wireless security settings. The **WPS AP Mode** automatically changes to **Configured**. |
| WPS PBC | Click this to initiate push button configuration. Use PBC on each WPS-enabled device, and allow them to connect automatically. See Section 20.8.1 on page 159 for details. |
| WPS Station PIN | Add a client to the wireless network by entering the client's Personal Identification Number (PIN) in the field and clicking the **Add Enrollee** button.<br>Note: You must also activate WPS on the client within two minutes. |
| WPS AP PIN | Add a client by entering the AP's PIN from this field in the client's WPS configuration. Click **Regenerate** to refresh it. |
| Apply/Save | Click this button to save your changes. |

## 20.8.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1 Ensure that the two devices you want to set up are within wireless range of one another.

2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this).

3 Press the button on one of the devices (it doesn't matter which). For the Router you must press the WPS button for more than three seconds.

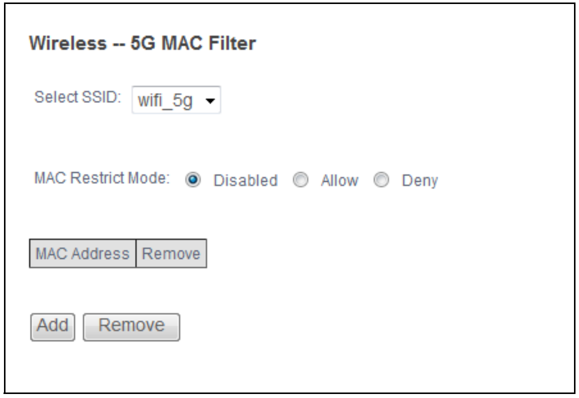
4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

## 20.9 Wireless 5GHz MAC Filter

Click **Wireless 5GHz > MAC Filter** to open the **MAC Filter** screen. This screen allows you to configure the Router to give exclusive access to specific devices **(Allow)** or exclude specific devices from accessing the Router **(Deny)**. Every Ethernet device has a unique MAC (Media Access Control) address assigned at the factory. It consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

**Figure 100** Wireless 5GHz MAC Filter



Wireless -- 5G MAC Filter

Select SSID: wifi_5g

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

| MAC Address | Remove |
|---|---|

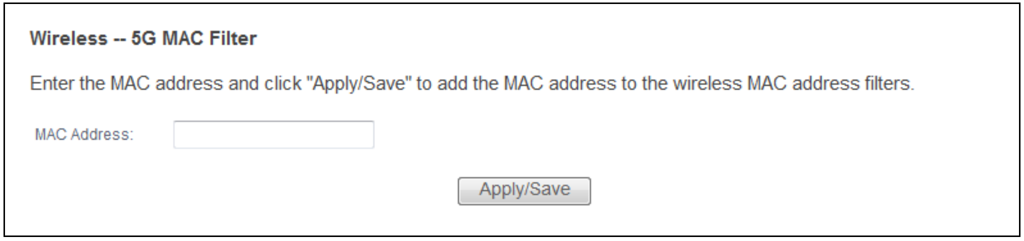
**Table 93** Wireless 5GHz MAC Filter

| LABEL | DESCRIPTION |
|---|---|
| Select SSID | Select an SSID for which to configure MAC filter settings. |
| MAC Restrict Mode | Define the filter action for the list of MAC addresses in the **MAC Address** table.<br>Select **Disabled** to turn off MAC filtering.<br>Select **Allow** to permit access to the Router. MAC addresses not listed will be denied access to the Router.<br>Select **Deny** to block access to the Router. MAC addresses not listed will be allowed to access the Router. |
| MAC Address | This displays the MAC addresses of the wireless devices that are allowed or denied access to the Router. |
| Remove | Select entries and click the **Remove** button to delete them. |
| Add | Click this to add a new MAC address entry to the table. |

### 20.9.1 Wireless MAC Filter Add

Use this screen to add MAC address entries. Click **Wireless > MAC Filter > Add** to open the following screen.

**Figure 101** Wireless MAC Filter Add



Wireless -- 5G MAC Filter

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

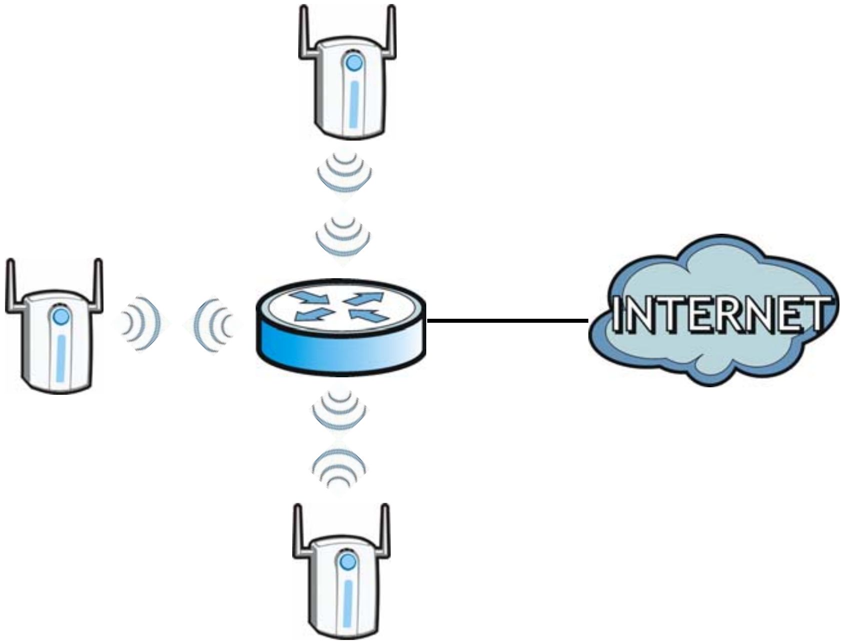
**Table 94** Wireless MAC Filter Add

| LABEL | DESCRIPTION |
|---|---|
| MAC Address | Enter the MAC address of the wireless device that is to be allowed or denied access to the Router. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. |
| Save/Apply | Click this button to save the changes and have the Router start using them. |

## 20.10 Wireless 5GHz Bridge

The Router can function as a wireless network bridge to wirelessly connect two or more APs.

**Figure 102** Connecting Wireless Networks Using WDS



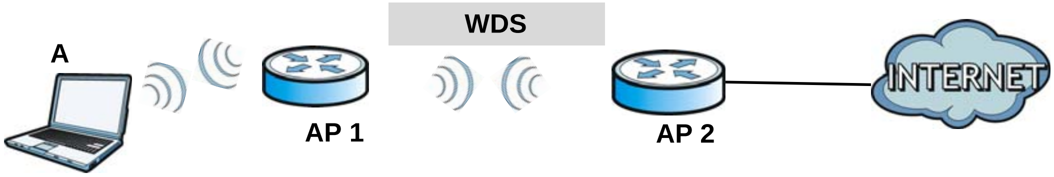
Use this screen to set up your Wireless Distribution System (WDS) links between the Router and other wireless APs. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between devices is made.

### Wireless Bridge Limitations

- At the time of writing, WDS is compatible with other APs of the same brand only. Not all models support WDS links.

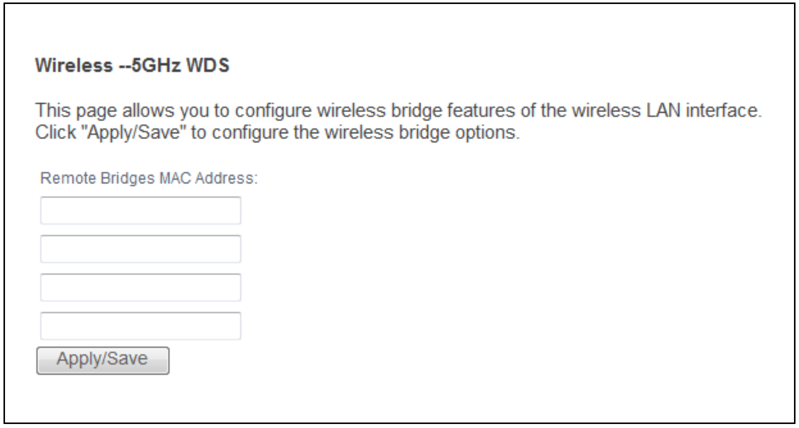
The following figure illustrates how WDS link works between APs. Notebook computer **A** is a wireless client connecting to access point **AP 1**. **AP 1** has no wired Internet connection, but can establish a WDS link with access point **AP 2**, which does. When **AP 1** has a WDS link with **AP 2**, the notebook computer can access the Internet through **AP 2**.

**Figure 103** WDS Link Example



Click **Wireless 5GHz > Wireless Bridge** to display the following screen.

**Figure 104** Wireless 5GHz Bridge



**Wireless --5GHz WDS**

This page allows you to configure wireless bridge features of the wireless LAN interface.
Click "Apply/Save" to configure the wireless bridge options.

Remote Bridges MAC Address:

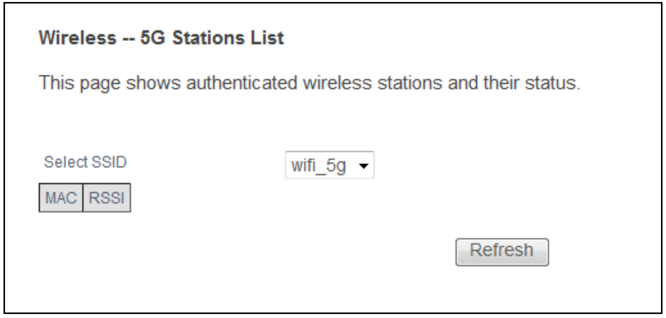
**Table 95** Wireless Bridge

| LABEL | DESCRIPTION |
|---|---|
| Remote Bridges MAC Address | Type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc). |
| Apply/Save | Click this to save and apply your changes. |

## 20.11 Wireless 5GHz Station Info

The station monitor displays the connection status of the wireless clients connected to (or trying to connect to) the Router. To open the station monitor, click **Wireless 5GHz** > **Station Info** to display this screen.

**Figure 105** Wireless 5GHz Station Info



**Wireless -- 5G Stations List**

This page shows authenticated wireless stations and their status.

Select SSID wifi_5g

| MAC | RSSI |
|---|---|

The following table describes the labels in this menu.

Table 96 Wireless 5GHz Station Info

| LABEL | DESCRIPTION |
|---|---|
| Select SSID | Select an SSID for which to display the authenticated wireless stations and their status. |
| MAC | This displays the MAC address (in XX:XX:XX:XX:XX:XX format) of a connected wireless station. |
| RSSI | This displays the Received Signal Strength Indication of the wireless station’s connection to the 5 GHz network. |
| Refresh | Click this button to update the information in the screen. |

# Voice

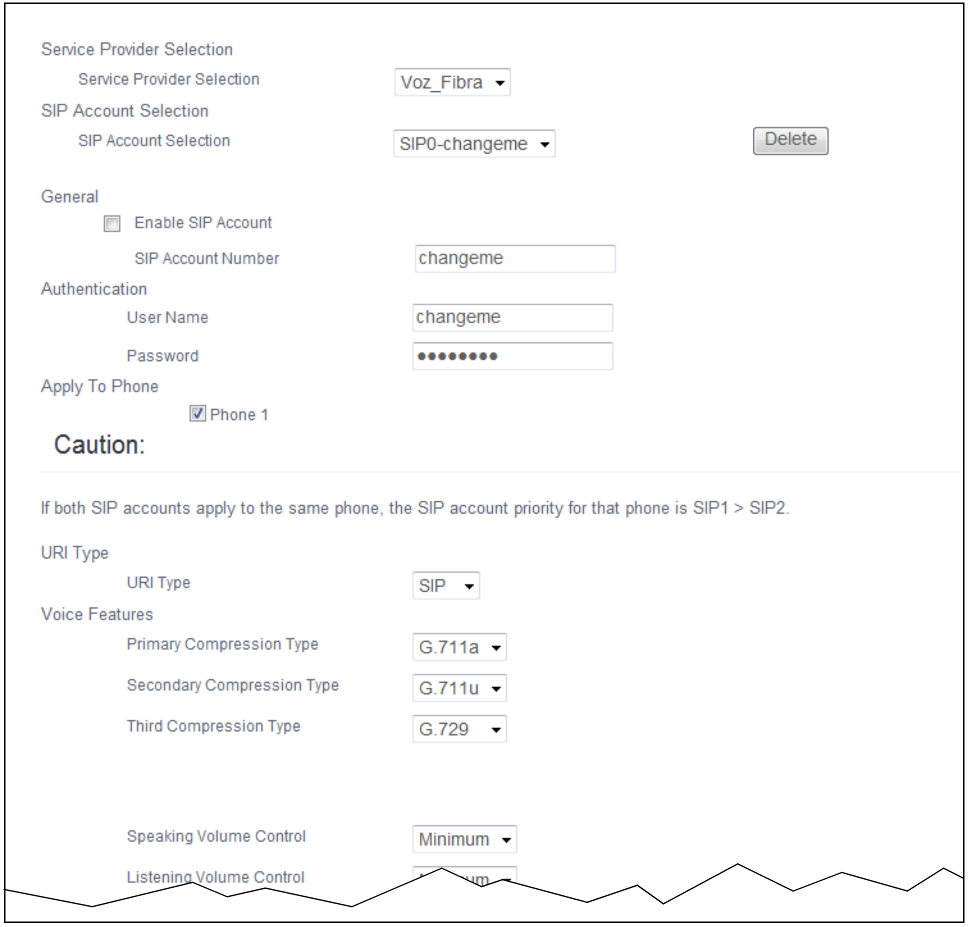
Chapter 21

## 21.1 SIP Account

The Router uses a SIP account to make outgoing VoIP calls and check if an incoming call’s destination number matches your SIP account’s SIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account, and map it to a phone port. The SIP account contains information that allows your Router to connect to your VoIP service provider.

Use this screen to maintain information about each SIP account. You can also enable and disable each SIP account. To access this screen, click **Voice > SIP Account**.

**Figure 106** SIP Account



Service Provider Selection

Service Provider Selection: Voz_Fibra

SIP Account Selection

SIP Account Selection: SIP0-changeme

Delete

General

☐ Enable SIP Account

SIP Account Number: changeme

Authentication

User Name: changeme

Password: ●●●●●●●●

Apply To Phone

☑ Phone 1

Caution:

If both SIP accounts apply to the same phone, the SIP account priority for that phone is SIP1 > SIP2.

URI Type

URI Type: SIP

Voice Features

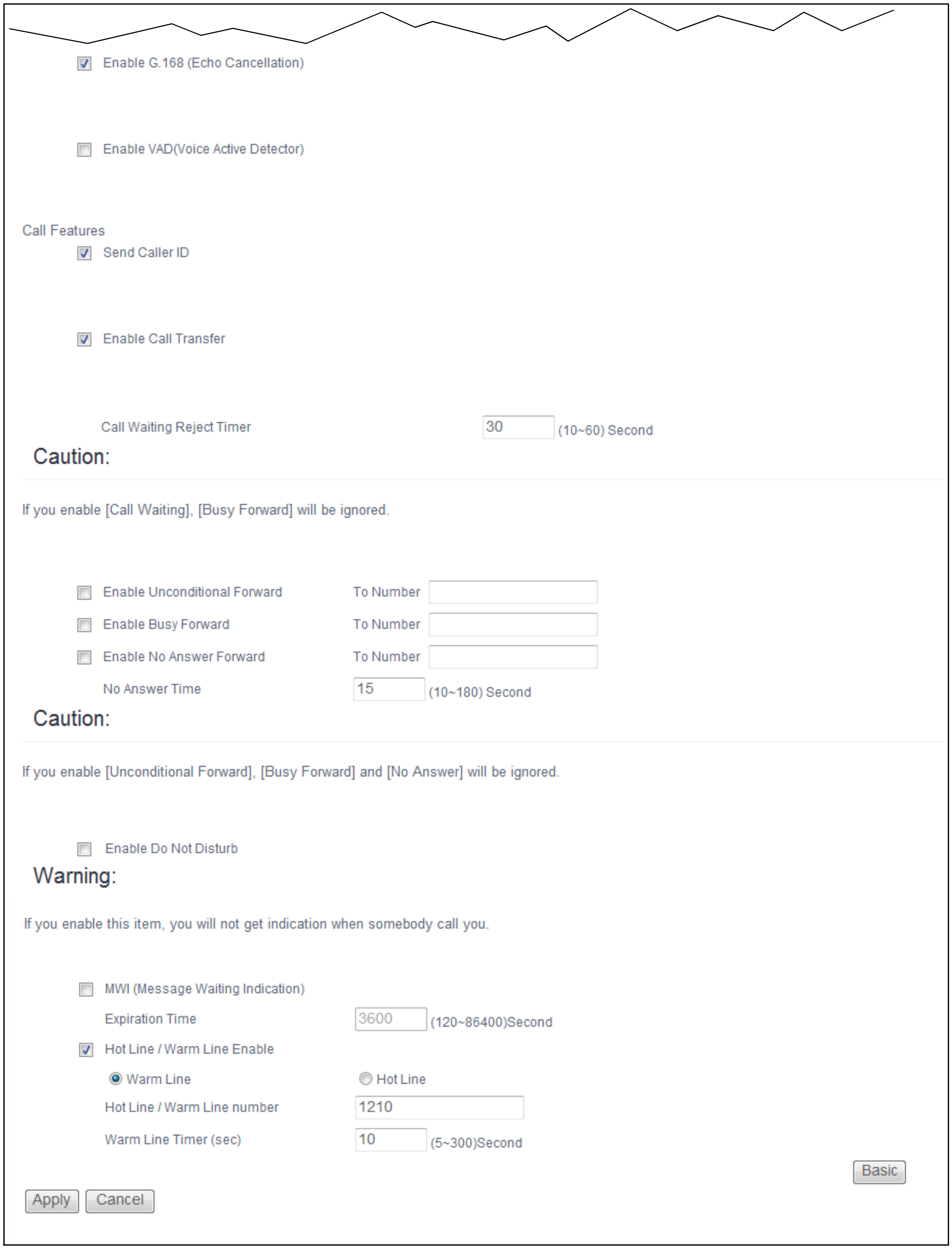
Primary Compression Type: G.711a

Secondary Compression Type: G.711u

Third Compression Type: G.729

Speaking Volume Control: Minimum

Listening Volume Control



☑ Enable G.168 (Echo Cancellation)

☐ Enable VAD(Voice Active Detector)

Call Features

☑ Send Caller ID

☑ Enable Call Transfer

Call Waiting Reject Timer 30 (10~60) Second

Caution:

If you enable [Call Waiting], [Busy Forward] will be ignored.

|  |  |
|---|---|
| ☐ Enable Unconditional Forward | To Number |
| ☐ Enable Busy Forward | To Number |
| ☐ Enable No Answer Forward | To Number |
| No Answer Time | 15 (10~180) Second |

Caution:

If you enable [Unconditional Forward], [Busy Forward] and [No Answer] will be ignored.

☐ Enable Do Not Disturb

Warning:

If you enable this item, you will not get indication when somebody call you.

|  |  |
|---|---|
| ☐ MWI (Message Waiting Indication) |  |
| Expiration Time | 3600 (120~86400)Second |
| ☑ Hot Line / Warm Line Enable |  |
| ● Warm Line | ○ Hot Line |
| Hot Line / Warm Line number | 1210 |
| Warm Line Timer (sec) | 10 (5~300)Second |

Each field is described in the following table.

Table 97 SIP Account

| LABEL | DESCRIPTION |
|---|---|
| Service Provider Selection | Select the SIP service provider profile you want to use for the SIP account you configure in this screen. If you change this field, the screen automatically refreshes. |
| SIP Account Selection | Select the SIP account you want to see in this screen. If you change this field, the screen automatically refreshes.<br>Select **ADD_NEW** to create a new SIP account on the Router. |
| Delete | Click this button to remove the SIP account selected in the **SIP Account Selection** field.<br>This button is not available when you select **ADD_NEW** in the **SIP Account Selection** field. |
| General | |
| Enable SIP Account | Select this if you want the Router to use this account. Clear it if you do not want the Router to use this account. |
| SIP Account Number | Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters. |
| Authentication | |
| User Name | Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters. |
| Password | Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII Extended set characters. |
| Apply To Phone | Select a phone port on which you want to make or receive phone calls for this SIP account.<br>If you map a phone port to more than one SIP account, there is no way to distinguish between the SIP accounts when you receive phone calls. The Router uses the most recently registered SIP account first when you make an outgoing call.<br>If a phone port is not mapped to a SIP account, you cannot receive or make any calls on the phone connected to this phone port. |
| Advanced/Basic | Click **Advanced** to display and edit more information for the SIP account. Click **Basic** to display and configure the basic SIP account settings. |
| URI Type | Select whether or not to include the SIP service domain name when the Router sends the SIP number.<br>**SIP** - include the SIP service domain name.<br>**TEL** - do not include the SIP service domain name. |
| Voice Features | |

Table 97 SIP Account (continued)

| LABEL | DESCRIPTION |
|---|---|
| Primary Compression Type<br>Secondary Compression Type<br>Third Compression Type | Select the type of voice coder/decoder (codec) that you want the Router to use.<br>G.711 provides high voice quality but requires more bandwidth (64 kbps). G.711 is the default codec used by phone companies and digital handsets.<br>• **G.711a** is typically used in Europe.<br>• **G.711u** is typically used in North America and Japan.<br>• **G.711a_VBD** is used in fax transmission. If both sides support the Voice Band Data (VBD) codec defined in ITU-T Recommendation V.152, they automatically use it instead of T.38.<br>**G.722** is a 7 KHz wideband voice codec that operates at 48, 56 and 64 kbps. By using a sample rate of 16 kHz, G.722 can provide higher fidelity and better audio quality than narrowband codecs like G.711, in which the voice signal is sampled at 8 KHz.<br>**G.726** operates at **24** or **32** kbps.<br>The Router must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec.<br>Select the Router's first choice for voice coder/decoder.<br>Select the Router's second choice for voice coder/decoder. Select **None** if you only want the Router to accept the first choice.<br>Select the Router's third choice for voice coder/decoder. Select **None** if you only want the Router to accept the first or second choice. |
| Speaking Volume Control | Enter the loudness that the Router uses for speech that it sends to the peer device.<br>**Minimum** is the quietest, and **Maximum** is the loudest. |
| Listening Volume Control | Enter the loudness that the Router uses for speech that it receives from the peer device.<br>**Minimum** is the quietest, and **Maximum** is the loudest. |
| Enable G.168 (Echo Cancellation) | Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk. |
| Enable VAD (Voice Active Detector) | Select this if the Router should stop transmitting when you are not speaking. This reduces the bandwidth the Router uses. |
| Call Features | |
| Send Caller ID | Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification. |
| Enable Call Transfer | Select this to enable call transfer on the Router. This allows you to transfer an incoming call (that you have answered) to another phone. |
| Call Waiting Reject Timer | Specify a time of seconds that the Router waits before rejecting the second call if you do not answer it. |

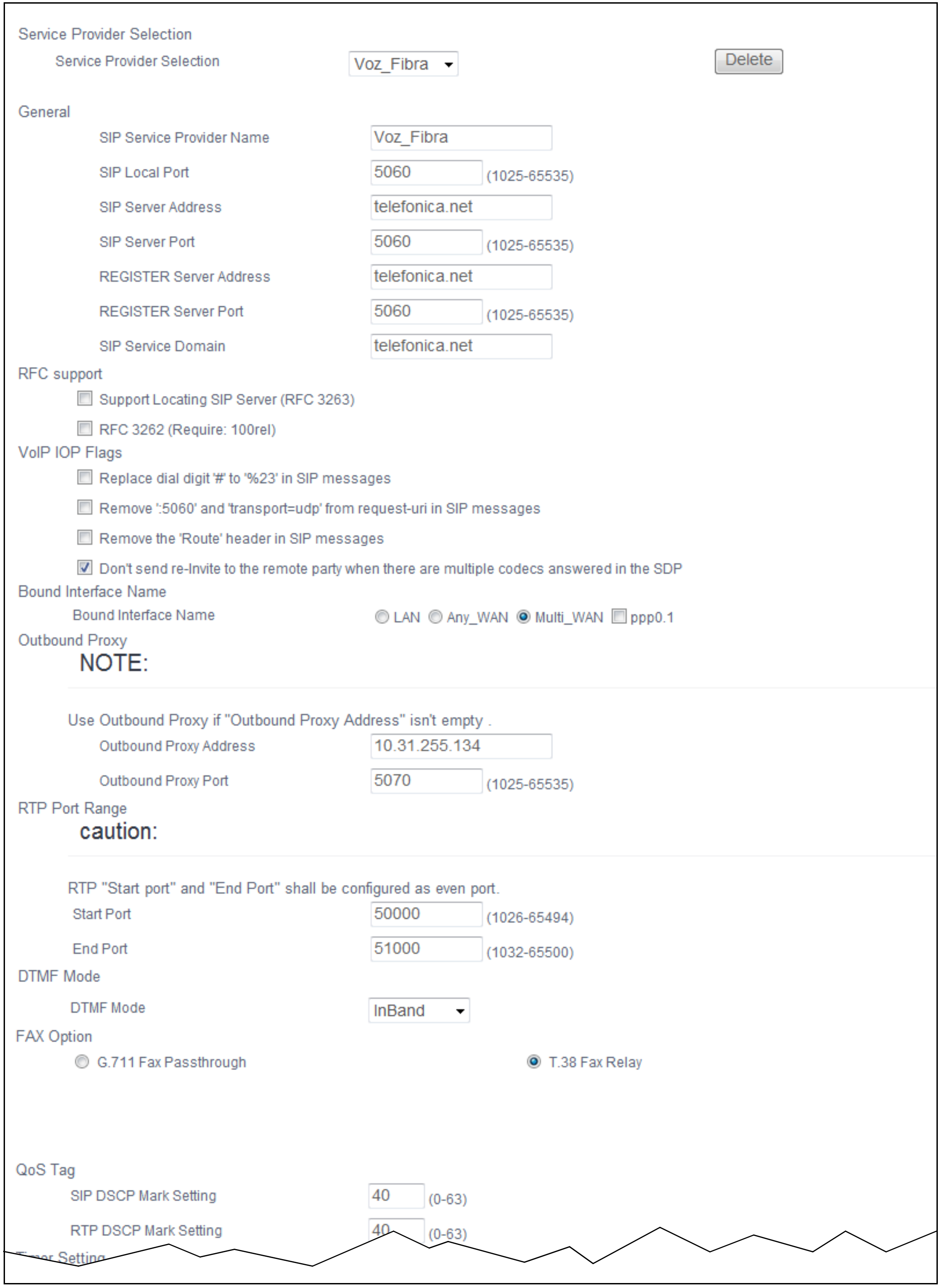
**Table 97** SIP Account (continued)

| LABEL | DESCRIPTION |
|---|---|
| Enable Unconditional Forward | Select this if you want the Router to forward all incoming calls to the specified phone number.<br>Specify the phone number in the **To Number** field on the right. |
| Enable Busy Forward | Select this if you want the Router to forward incoming calls to the specified phone number if the phone port is busy.<br>Specify the phone number in the **To Number** field on the right.<br>If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call. |
| Enable No Answer Forward | Select this if you want the Router to forward incoming calls to the specified phone number if the call is unanswered. (See **No Answer Time**.)<br>Specify the phone number in the **To Number** field on the right. |
| No Answer Time | This field is used by the **Active No Answer Forward** feature.<br>Enter the number of seconds the Router should wait for you to answer an incoming call before it considers the call is unanswered. |
| Enable Do Not Disturb | Select this to set your phone to not ring when someone calls you. |
| MWI (Message Waiting Indication) | Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature. |
| Expiration Time | Keep the default value for this field, unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the Router subscribes to the service. Before this time passes, the Router automatically subscribes again. |
| Hot Line / Warm Line Enable | Select this to enable the hot line or warm line feature on the Router. |
| Warm Line | Select this to have the Router dial the specified warm line number after you pick up the telephone and do not press any keys on the keypad for a period of time. |
| Hot Line | Select this to have the Router dial the specified hot line number immediately when you pick up the telephone. |
| Hot Line / Warm Line number | Enter the number of the hot line or warm line that you want the Router to dial. |
| Warm Line Timer | Enter a number of seconds that the Router waits before dialing the warm line number if you pick up the telephone and do not press any keys on the keypad. |
| Apply | Click this to save your changes and to apply them to the Router. |
| Cancel | Click this to set every field in this screen to its last-saved value. |

## 21.2 SIP Server

Click **Voice > SIP Server** to open the **SIP Server** screen. Use this screen to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions, and dialing plan.

**Figure 107** SIP Server



Service Provider Selection

| | | |
|---|---|---|
| Service Provider Selection | Voz_Fibra ▾ | Delete |

General

| | | |
|---|---|---|
| SIP Service Provider Name | Voz_Fibra | |
| SIP Local Port | 5060 | (1025-65535) |
| SIP Server Address | telefonica.net | |
| SIP Server Port | 5060 | (1025-65535) |
| REGISTER Server Address | telefonica.net | |
| REGISTER Server Port | 5060 | (1025-65535) |
| SIP Service Domain | telefonica.net | |

RFC support

□ Support Locating SIP Server (RFC 3263)

□ RFC 3262 (Require: 100rel)

VoIP IOP Flags

□ Replace dial digit '#' to '%23' in SIP messages

□ Remove ':5060' and 'transport=udp' from request-uri in SIP messages

□ Remove the 'Route' header in SIP messages

☑ Don't send re-Invite to the remote party when there are multiple codecs answered in the SDP

Bound Interface Name

Bound Interface Name ○ LAN ○ Any_WAN ● Multi_WAN □ ppp0.1

Outbound Proxy

NOTE:

Use Outbound Proxy if "Outbound Proxy Address" isn't empty .

| | | |
|---|---|---|
| Outbound Proxy Address | 10.31.255.134 | |
| Outbound Proxy Port | 5070 | (1025-65535) |

RTP Port Range

caution:

RTP "Start port" and "End Port" shall be configured as even port.

| | | |
|---|---|---|
| Start Port | 50000 | (1026-65494) |
| End Port | 51000 | (1032-65500) |

DTMF Mode

DTMF Mode InBand ▾

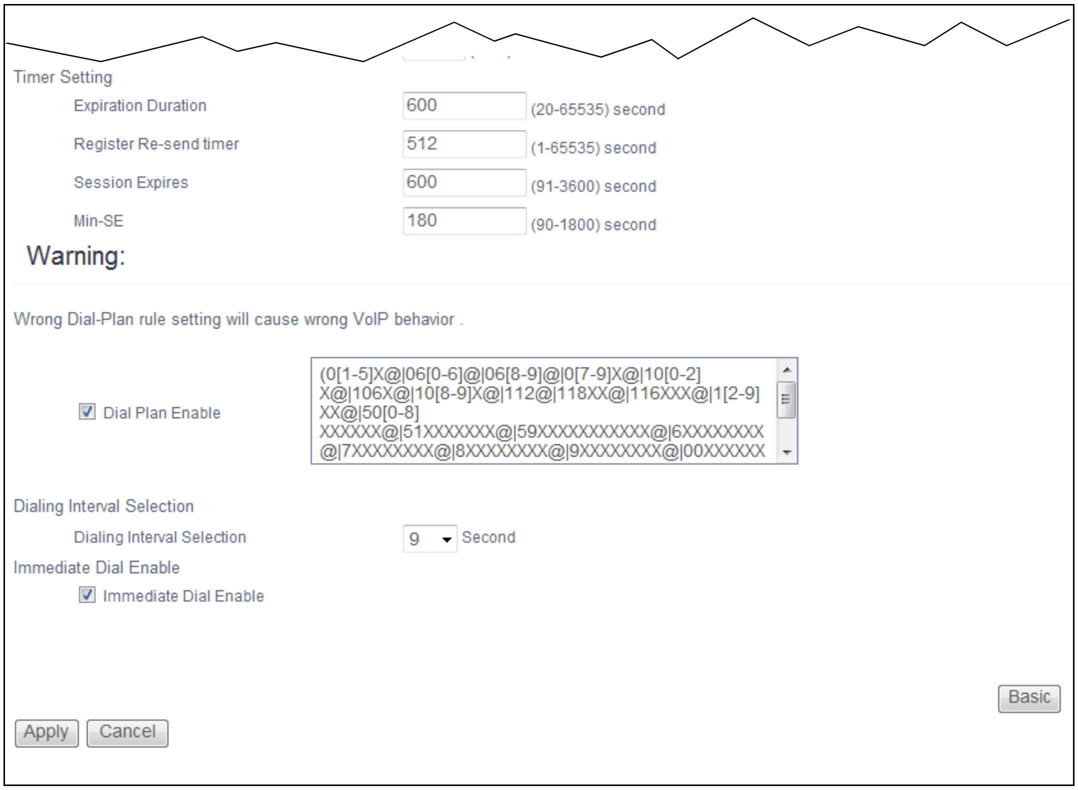
FAX Option

○ G.711 Fax Passthrough ● T.38 Fax Relay

QoS Tag

| | | |
|---|---|---|
| SIP DSCP Mark Setting | 40 | (0-63) |
| RTP DSCP Mark Setting | 40 | (0-63) |

Timer Setting



Timer Setting

| | | |
|---|---|---|
| Expiration Duration | 600 | (20-65535) second |
| Register Re-send timer | 512 | (1-65535) second |
| Session Expires | 600 | (91-3600) second |
| Min-SE | 180 | (90-1800) second |

Warning:

Wrong Dial-Plan rule setting will cause wrong VoIP behavior .

☑ Dial Plan Enable

```
(0[1-5]X@|06[0-6]@|06[8-9]@|0[7-9]X@|10[0-2]
X@|106X@|10[8-9]X@|112@|118XX@|116XXX@|1[2-9]
XX@|50[0-8]
XXXXXX@|51XXXXXXX@|59XXXXXXXXXXX@|6XXXXXXXX
@|7XXXXXXXX@|8XXXXXXXX@|9XXXXXXXX@|00XXXXXX
```

Dialing Interval Selection

Dialing Interval Selection: 9 Second

Immediate Dial Enable

☑ Immediate Dial Enable

Each field is described in the following table.

**Table 98** SIP Server

| LABEL | DESCRIPTION |
|---|---|
| Service Provider Selection | Select the SIP service provider profile you want to see in this screen. If you change this field, the screen automatically refreshes.<br>Select **ADD_NEW** to create a new SIP service provider profile on the Router. |
| Delete | Click this button to remove the SIP service provider profile selected in the **Service Provider Selection** field.<br>This button is not available when you select **ADD_NEW** in the **Service Provider Selection**. |
| General | |
| SIP Service Provider Name | Enter a descriptive name of up to 63 printable characters for this SIP service provider profile. Spaces are not allowed. |
| SIP Local Port | Enter the Router’s listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value. |
| SIP Server Address | Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server. |
| SIP Server Port | Enter the SIP server’s listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value. |

**Table 98** SIP Server (continued)

| LABEL | DESCRIPTION |
|---|---|
| REGISTER Server Address | Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **SIP Server Address** field. You can use up to 95 printable ASCII characters. |
| REGISTER Server Port | Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the **SIP Server Port** field. |
| SIP Service Domain | Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters. |
| RFC support | |
| Support Locating SIP Server (RFC 3263) | Select this option to have the Router use DNS procedures to resolve the SIP domain and find the SIP server's IP address, port number and supported transport protocol(s).<br>The Router first uses DNS Name Authority Pointer (NAPTR) records to determine the transport protocols supported by the SIP server. It then performs DNS Service (SRV) query to determine the port number for the protocol. The Router resolves the SIP server's IP address by a standard DNS address record lookup.<br>The **SIP Server Port** and **REGISTER Server Port** fields are grayed out and not applicable and the **Transport Type** can also be set to **AUTO** if you select this option. |
| RFC 3262 | RFC 3262 defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method.<br>Select this to have the Router include a SIP Require/Supported header field with the option tag 100rel in all INVITE requests. When the Router receives a SIP response message indicating that the phone it called is ringing, the Router sends a PRACK message to have both sides confirm the message is received.<br>If you select this option, the peer device should also support the option tag 100rel to send provisional responses reliably. |
| VoIP IOP Flags | Use this section to modify the header or some information in SIP messages in order to resolve interoperability issues with some SIP servers. |
| Replace dial digit '#' to '%23' in SIP messages | Replace a dial digit "#" with "%23" in the INVITE messages. |
| Remove ':5060' and 'transport=udp' from request-uri in SIP messages | Remove ":5060" and "transport=udp" from the "Request-URI" string in the REGISTER and INVITE packets. |
| Remove the 'Route' header in SIP messages | Remove the 'Route' header in SIP packets. |

**Table 98** SIP Server (continued)

| LABEL | DESCRIPTION |
|---|---|
| Don't send re-Invite to the remote party when there are multiple codecs answered in the SDP | Do not send a re-Invite packet to the remote party when the remote party answers that it can support multiple codecs?? |
| Bound Interface Name | |
| Bound Interface Name | If you select **LAN** or **Any_WAN**, the Router automatically activates the VoIP service when any LAN or WAN connection is up.<br>If you select **Multi_WAN**, you also need to select the pre-configured WAN connections. The VoIP service is activated only when one of the selected WAN connections is up. |
| Outbound Proxy | |
| Outbound Proxy Address | Enter the IP address or domain name of the SIP outbound proxy server if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the Router to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the Router to keep it from re-translating the IP address (since this is already handled by the outbound proxy server). |
| Outbound Proxy Port | Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value. |
| RTP Port Range | |
| Start Port<br>End Port | Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values.<br>To enter one port number, enter the port number in the **Start Port** and **End Port** fields.<br>To enter a range of ports,<br>• enter the port number at the beginning of the range in the **Start Port** field.<br>• enter the port number at the end of the range in the **End Port** field. |
| DTMF Mode | |
| DTMF Mode | Control how the Router handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses.<br>**RFC2833** - send the DTMF tones in RTP packets.<br>**InBand** - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones.<br>**SIPInfo** - send the DTMF tones in SIP messages. |

**Table 98** SIP Server (continued)

| LABEL | DESCRIPTION |
|---|---|
| FAX Option | This field controls how the Router handles fax messages.<br>Select **G.711 Fax Passthrough** to have the  use G.711 to send fax messages. The peer devices must also use G.711.<br>Select **T.38 Fax Relay** to have the Router send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38. |
| QoS Tag | |
| SIP DSCP Mark Setting | Enter the DSCP (DiffServ Code Point) number for SIP voice transmissions. The Router creates Class of Service (CoS) priority tags with this number to voice traffic that it transmits. |
| RTP DSCP Mark Setting | Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The Router creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits. |
| Timer Setting | |
| Expiration Duration | Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The Router automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.) |
| Register Re-send timer | Enter the number of seconds the Router waits before it tries again to register the SIP account, if the first try failed or if there is no response. |
| Session Expires | Enter the number of seconds the Router lets a SIP session remain idle (without traffic) before it automatically disconnects the session. |
| Min-SE | Enter the minimum number of seconds the Router lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the Router accepts. |
| Phone Key Config | |
| Call Return | Specify the key combinations that you can enter to place a call to the last number that called you. |
| One Shot Caller Display Call | Specify the key combinations that you can enter to activate caller ID for the next call only. |
| One Shot Caller Hidden Call | Specify the key combinations that you can enter to deactivate caller ID for the next call only. |
| One Shot Call Waiting Enable | Specify the key combinations that you can enter to put a call on hold when you are answering another. |
| Call Waiting Enable | Specify the key combinations that you can enter to turn on the call waiting function. |
| Call Waiting Disable | Specify the key combinations that you can enter to turn off the call waiting function. |

**Table 98** SIP Server (continued)

| LABEL | DESCRIPTION |
|---|---|
| Internal Call | Specify the key combinations that you can enter to call the phone(s) connected to the Router. |
| Call Transfer | Specify the key combinations that you can enter to transfer a call to another phone. |
| Unconditional Call Forward Enable | Specify the key combinations that you can enter to forward all incoming calls to the phone number you specified in the **SIP > SIP Account** screen. |
| Unconditional Call Forward Disable | Specify the key combinations that you can enter to turn the unconditional call forward function off. |
| No Answer Call Forward Enable | Specify the key combinations that you can enter to forward incoming calls to the phone number you specified in the **SIP > SIP Account** screen if the calls are unanswered. |
| No Answer Call Forward Disable | Specify the key combinations that you can enter to turn the no answer call forward function off. |
| Call Forward When Busy Enable | Specify the key combinations that you can enter to forward incoming calls to the phone number you specified in the **SIP > SIP Account** screen if the phone port is busy. |
| Call Forward When Busy Disable | Specify the key combinations that you can enter to turn the busy forward function off. |
| One Shot Call Waiting Disable | Specify the key combinations that you can enter to deactivate call waiting on the next call only. |
| Do Not Disturb Enable | Specify the key combinations that you can enter to set your phone not to ring when someone calls you. |
| Do Not Disturb Disable | Specify the key combinations that you can enter to turn this function off. |
| Call Completion on Busy Subscriber (CCBS) Deactivate | Specify the key combinations that you can enter to disable CCBS on a call. |
| Outgoing SIP | Specify the key combinations that you can enter to select the SIP account that you use to make outgoing calls.<br>If you enter #12(by default)<SIP account index number>#<the phone number you want to call>, #1201#12345678 for example, the Router uses the first SIP account to call 12345678. |
| Dial Plan | |
| Dial Plan Enable | Select this to activate the dial plan rules you specify in the text box provided. See Section 21.2.1 on page 176 for how to set up a rule. |

**Table 98** SIP Server (continued)

| LABEL | DESCRIPTION |
|---|---|
| Dialing Interval Selection | |
| Dialing Interval Selection | Enter the number of seconds the Router should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers.<br>If you select **Immediate Dial Enable**, you can press the pound key (#) to tell the Router to make the phone call immediately, regardless of this setting. |
| Immediate Dial Enable | |
| Immediate Dial Enable | Select this if you want to use the pound key (#) to tell the Router to make the phone call immediately, instead of waiting the number of seconds you selected in the **Dialing Interval Selection** field.<br>If you select this, dial the phone number, and then press the pound key. The Router makes the call immediately, instead of waiting. You can still wait, if you want. |
| Apply | Click this to save your changes and to apply them to the Router. |
| Cancel | Click this to set every field in this screen to its last-saved value. |

### 21.2.1 Dial Plan Rules

A dial plan defines the dialing patterns, such as the length and range of the digits for a telephone number. It also includes country codes, access codes, area codes, local numbers, long distance numbers or international call prefixes. For example, the dial plan ([2-9]xxxxxx) does not allow a local number which begins with 1 or 0.

Without a dial plan, users have to manually enter the whole callee's number and wait for the specified dialing interval to time out or press a terminator key (usually the pound key on the phone keypad) before the Router makes the call.

The Router initializes a call when the dialed number matches any one of the rules in the dial plan. Dial plan rules follow these conventions:

- The collection of rules is in parentheses ().
- Rules are separated by the | (bar) symbol.
- "x" stands for a wildcard and can be any digit from 0 to 9.
- A subset of keys is in a square bracket []. Ranges are allowed.

  For example, [359] means a number matching this rule can be 3, 5 or 9. [26-8*] means a number matching this rule can be 2, 6, 7, 8 or *.
- The dot "." appended to a digit allows the digit to be ignored or repeated multiple times. Any digit (0~9, *, #) after the dot will be ignored.

  For example, (01.) means a number matching this rule can be 0, 01, 0111, 01111, and so on.

- <dialed-number:translated-number> indicates the number after the colon replaces the number before the colon in an angle bracket <>. For example,

  (<:1212> xxxxxxx) means the Router automatically prefixes the translated-number "1212" to the number you dialed before making the call. This can be used for local calls in the US.

  (<9:> xxx xxxxxxx) means the Router automatically removes the specified prefix "9" from the number you dialed before making the call. This is always used for making outside calls from an office.

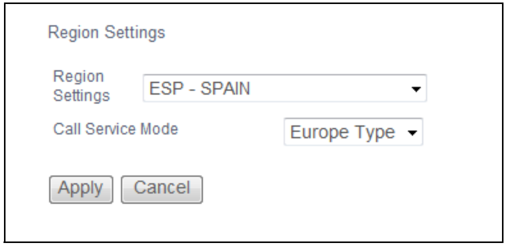
  (xx<123:456>xxxx) means the Router automatically translates "123" to "456" in the number you dialed before making the call.
- Calls with a number followed by the exclamation mark "!" will be dropped.
- Calls with a number followed by the termination character "@" will be made immediately. Any digit (0~9, *, #) after the @ character will be ignored.

In this example dial plan (0 | [49]11 | 1 [2-9]xx xxxxxxx | 1 947 xxxxxxx !), you can dial "0" to call the local operator, call 411 or 911, or make a long distance call with an area code starting from 2 to 9 in the US. The calls with the area code 947 will be dropped.

## 21.3 Phone Region

Use this screen to maintain settings that depend on which region of the world the Router is in. To access this screen, click **Voice > Phone**.

**Figure 108** Phone Region



Region Settings

Region Settings: ESP - SPAIN

Call Service Mode: Europe Type

Each field is described in the following table.

**Table 99** Phone Region

| LABEL | DESCRIPTION |
|---|---|
| Region Settings | Select the place in which the Router is located. |
| Call Service Mode | Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports.<br>**Europe Type** - use supplementary phone services in European mode<br>**USA Type** - use supplementary phone services American mode<br>You might have to subscribe to these services to use them. Contact your VoIP service provider. |

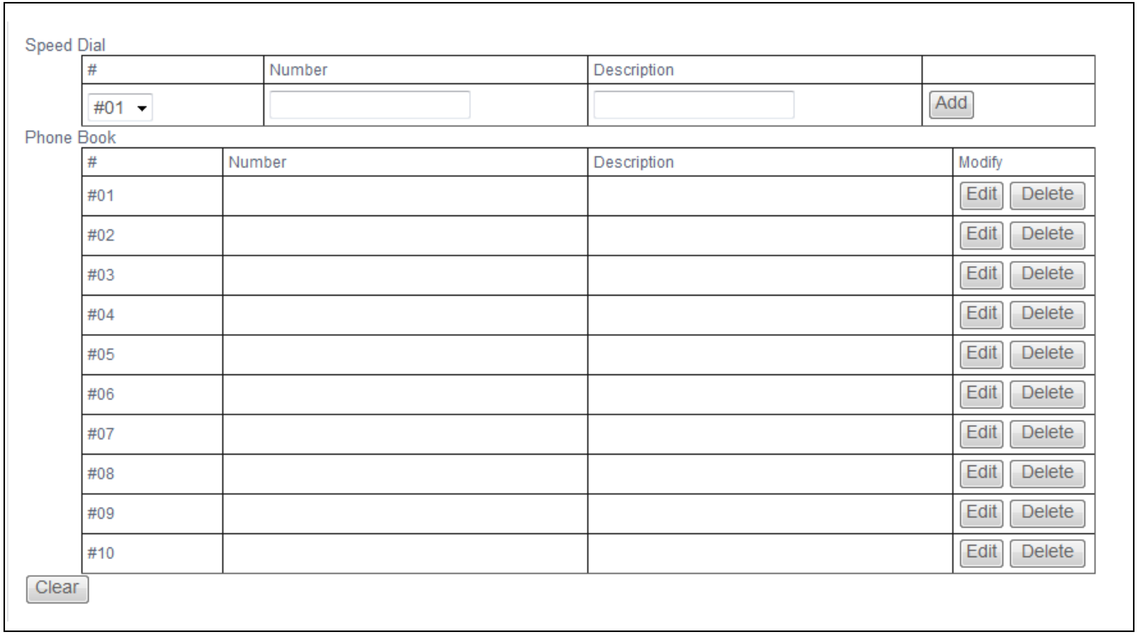
**Table 99** Phone Region

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click this to save your changes and to apply them to the Router. |
| Cancel | Click this to set every field in this screen to its last-saved value. |

## 21.4 Call Rule

Click **Voice > Call Rule** to manage speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number.

**Figure 109** Call Rule



Speed Dial

| # | Number | Description | |
|---|---|---|---|
| #01 ▾ | | | Add |

Phone Book

| # | Number | Description | Modify |
|---|---|---|---|
| #01 | | | Edit Delete |
| #02 | | | Edit Delete |
| #03 | | | Edit Delete |
| #04 | | | Edit Delete |
| #05 | | | Edit Delete |
| #06 | | | Edit Delete |
| #07 | | | Edit Delete |
| #08 | | | Edit Delete |
| #09 | | | Edit Delete |
| #10 | | | Edit Delete |

Each field is described in the following table.

**Table 100** Call Rule

| LABEL | DESCRIPTION |
|---|---|
| Speed Dial | Use this section to create or edit speed-dial entries. |
| # | Select the speed-dial number you want to use for this phone number. |
| Number | Enter the SIP number you want the Router to call when you dial the speed-dial number. |

**Table 100** Call Rule

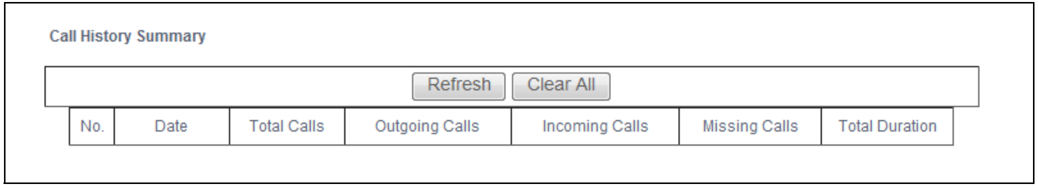
| LABEL | DESCRIPTION |
|---|---|
| Description | Enter a name to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters. |
| Add | Click this to use the information in the **Speed Dial** section to update the **Phone Book** section. |
| Phone Book | Use this section to look at all the speed-dial entries and to erase them. |
| # | This field displays the speed-dial number you should dial to use this entry. |
| Number | This field displays the SIP number the Router calls when you dial the speed-dial number. |
| Description | This field displays the name of the party you call when you dial the speed-dial number. |
| Modify | Use this field to edit or erase the speed-dial entry.<br>Click the **Edit** button to copy the information for this speed-dial entry into the **Speed Dial** section, where you can change it.<br>Click the **Delete** button to erase this speed-dial entry. |
| Clear | Click this to erase all the speed-dial entries. |

## 21.5 Call History Summary

The Router logs calls from or to your SIP numbers. This screen allows you to view the summary of received, dialed and missed calls.

Click **Voice > Summary**. The following screen displays.

**Figure 110** Call History Summary



Call History Summary

| No. | Date | Total Calls | Outgoing Calls | Incoming Calls | Missing Calls | Total Duration |
|---|---|---|---|---|---|---|

Each field is described in the following table.

**Table 101** Call History Summary

| LABEL | DESCRIPTION |
|---|---|
| Refresh | Click this button to renew the call history list. |
| Clear All | Click this button to remove all entries from the call history list. |

Table 101 Call History Summary

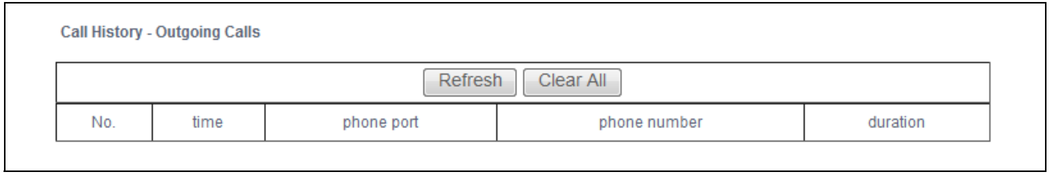
| LABEL | DESCRIPTION |
|---|---|
| No. | This is a read-only index number. |
| Date | This is the date when the calls were made. |
| Total Calls | This displays the total number of calls from or to your SIP numbers that day. |
| Outgoing Calls | This displays how many calls originated from you that day. |
| Incoming Calls | This displays how many calls you received that day. |
| Missing Calls | This displays how many incoming calls were not answered that day. |
| Total Duration | This displays how long all calls lasted that day. |

## 21.6 Outgoing Calls

Use this screen to see detailed information for each outgoing call you made.

Click **Voice > Outgoing**. The following screen displays.

**Figure 111** Outgoing Calls



Call History - Outgoing Calls

| No. | time | phone port | phone number | duration |
|---|---|---|---|---|

Each field is described in the following table.

Table 102 Outgoing Calls

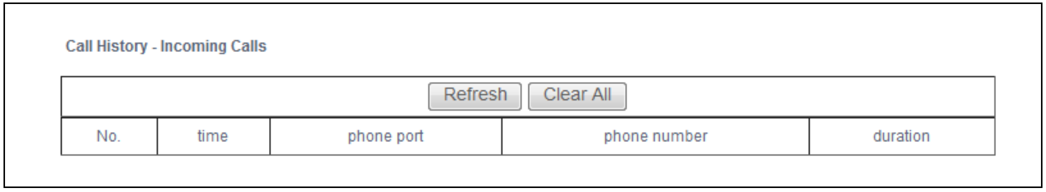
| LABEL | DESCRIPTION |
|---|---|
| Refresh | Click this button to renew the dialed call list. |
| Clear All | Click this button to remove all entries from the dialed call list. |
| No. | This is a read-only index number. |
| time | This is the date and time when the call was made. |
| phone port | This is the phone port on which you made the call. |
| phone number | This is the SIP number you called. |
| duration | This displays how long the call lasted. |

## 21.7 Incoming Calls

Use this screen to see detailed information for each incoming call from someone calling you.

Click **Voice > Incoming**. The following screen displays.

**Figure 112** Incoming Calls



Call History - Incoming Calls

| No. | time | phone port | phone number | duration |
|---|---|---|---|---|

Each field is described in the following table.

**Table 103** Incoming Calls

| LABEL | DESCRIPTION |
|---|---|
| Refresh | Click this button to renew the received call list. |
| Clear All | Click this button to remove all entries from the received call list. |
| No. | This is a read-only index number. |
| time | This is the date and time when the call was made. |
| phone port | This is the phone port on which you received the call.<br>**Missed** means the call was unanswered. |
| phone number | This is the SIP number that called you. |
| duration | This displays how long the call lasted. |

# 21.8 Technical Reference

This section contains background material relevant to the **VoIP** screens.

### VoIP

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

### SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

#### SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

#### SIP Number

The SIP number is the part of the SIP URI that comes before the “@” symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

#### SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then “VoIP-provider.com” is the SIP service domain.

#### SIP Registration

Each Router is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

A SIP user agent has to register with the SIP registrar and must provide information about the users it represents, as well as its current IP address (for the routing of incoming SIP requests). After successful registration, the SIP server knows that the users (identified by their dedicated SIP URIs) are represented by the UA, and knows the IP address to which the SIP requests and responses should be sent.

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the Router). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

A SIP registration has a limited lifespan. The User Agent Client must renew its registration within this lifespan. If it does not do so, the registration data will be deleted from the SIP registrar's database and the connection broken.

The Router attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the Router attempts to register the port immediately.

### Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated via a challenge / response system using the HTTP digest mechanism (as detailed in RFC 3261, "SIP: Session Initiation Protocol").

### SIP Servers

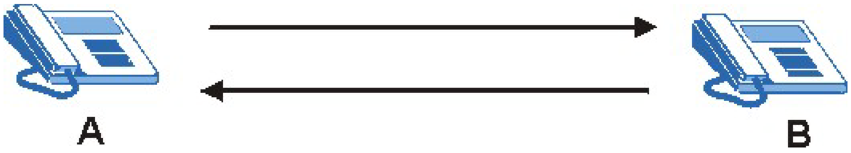
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

### SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either **A** or **B** can act as a SIP user agent client to initiate a call. **A** and **B** can also both act as a SIP user agent to receive the call.

**Figure 113** SIP User Agent



### SIP Proxy Server

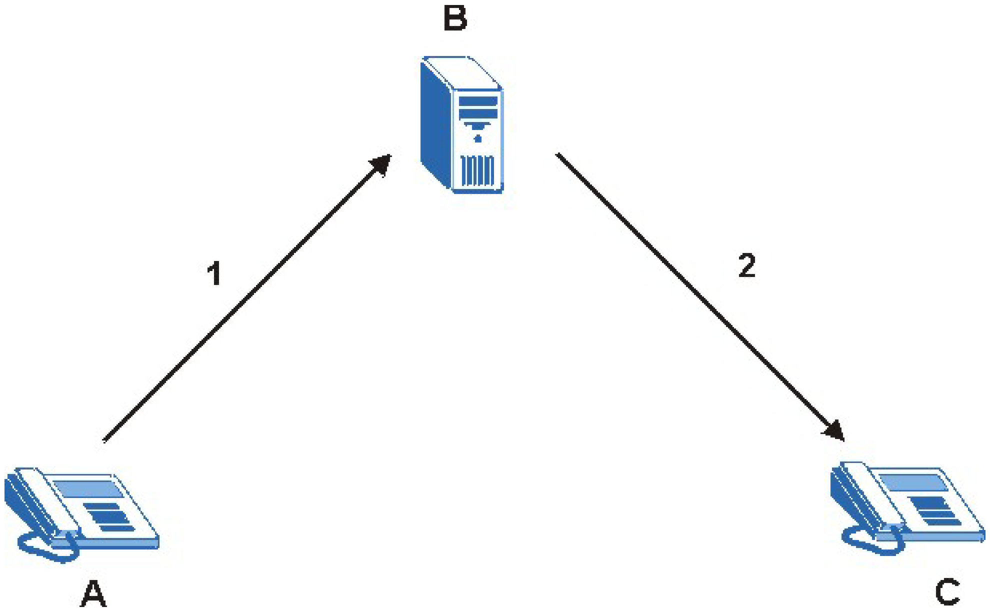
A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device **A** to call someone who is using client device C.

1 The client device (**A** in the figure) sends a call invitation to the SIP proxy server (**B**).

2 The SIP proxy server forwards the call invitation to **C**.

**Figure 114** SIP Proxy Server



### SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

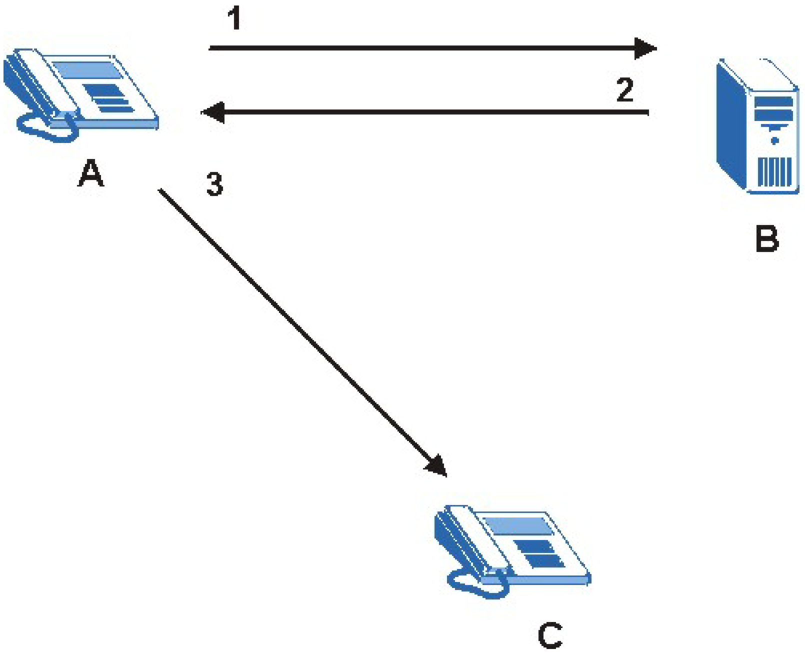
In the following example, you want to use client device **A** to call someone who is using client device **C**.

1 Client device **A** sends a call invitation for **C** to the SIP redirect server (**B**).

2 The SIP redirect server sends the invitation back to **A** with **C**’s IP address (or domain name).

3 Client device **A** then sends the call invitation to client device **C**.

**Figure 115** SIP Redirect Server



### SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

### RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

### Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

### SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

**Table 104** SIP Call Progression

| A | | B |
|---|---|---|
| 1. INVITE | → | |
| | ← | 2. Ringing |

**Table 104** SIP Call Progression (continued)

| A | | B |
|---|---|---|
| | ← | 3. OK |
| 4. ACK | → | |
| | 5.Dialogue (voice traffic) | |
| 6. BYE | → | |
| | ← | 7. OK |

1 **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.

2 **B** sends a response indicating that the telephone is ringing.

3 **B** sends an OK response after the call is answered.

4 **A** then sends an ACK message to acknowledge that **B** has answered the call.

5 Now **A** and **B** exchange voice media (talk).

6 After talking, **A** hangs up and sends a BYE request.

7 **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

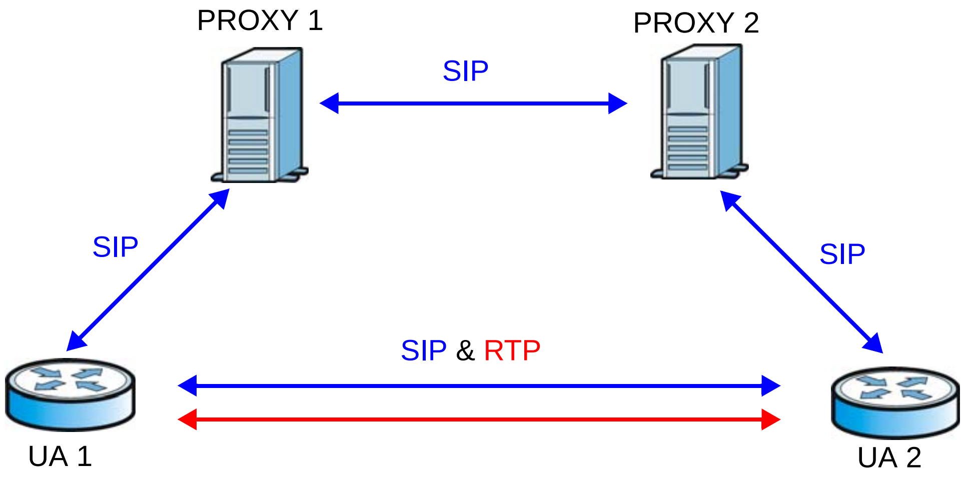
### SIP Call Progression Through Proxy Servers

Usually, the SIP UAC sets up a phone call by sending a request to the SIP proxy server. Then, the proxy server looks up the destination to which the call should be forwarded (according to the URI requested by the SIP UAC). The request may be forwarded to more than one proxy server before arriving at its destination.

The response to the request goes to all the proxy servers through which the request passed, in reverse sequence. Once the session is set up, session traffic is sent between the UAs directly, bypassing all the proxy servers in between.

The following figure shows the SIP and session traffic flow between the user agents (**UA 1** and **UA 2**) and the proxy servers (this example shows two proxy servers, **PROXY 1** and **PROXY 2**).

**Figure 116** SIP Call Through Proxy Servers



The following table shows the SIP call progression.

**Table 105** SIP Call Progression

| UA 1 | PROXY 1 | PROXY 2 | UA 2 |
|---|---|---|---|
| Invite → | | | |
| | Invite → | | |
| ← | 100 Trying | Invite → | |
| | ← | 100 Trying | |
| | | ← | 180 Ringing |
| | ← | 180 Ringing | |
| ← | 180 Ringing | | |
| | | ← | 200 OK |
| | ← | 200 OK | |
| ← | 200 OK | | |
| ACK → | → | → | |
| RTP ↔ | ↔ | ↔ | RTP |

**Table 105** SIP Call Progression

| UA 1 | PROXY 1 | PROXY 2 | UA 2 |
|---|---|---|---|
| | ←———————— | ———————— | BYE |
| 200 OK | ———————— | ————————→ | |

1 **User Agent 1** sends a SIP INVITE request to **Proxy 1**. This message is an invitation to **User Agent 2** to participate in a SIP telephone call. **Proxy 1** sends a response indicating that it is trying to complete the request.

2 **Proxy 1** sends a SIP INVITE request to **Proxy 2**. **Proxy 2** sends a response indicating that it is trying to complete the request.

3 **Proxy 2** sends a SIP INVITE request to **User Agent 2**.

4 **User Agent 2** sends a response back to **Proxy 2** indicating that the phone is ringing. The response is relayed back to **User Agent 1** via **Proxy 1**.

5 **User Agent 2** sends an OK response to **Proxy 2** after the call is answered. This is also relayed back to **User Agent 1** via **Proxy 1**.

6 **User Agent 1** and **User Agent 2** exchange RTP packets containing voice data directly, without involving the proxies.

7 When **User Agent 2** hangs up, he sends a BYE request.

8 **User Agent 1** replies with an OK response confirming receipt of the BYE request, and the call is terminated.

### Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The Router supports the following codecs.

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.
- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

### Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the Router reduce the bandwidth that a call uses by not transmitting “silent packets” when you are not speaking.

### Comfort Noise Generation

When using VAD, the Router generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

### Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

### MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

### Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the Router. The Router allows you to record custom tones for the **Early Media** and **Music On Hold** functions. The same recordings apply to both the caller ringing and on hold tones.

**Table 106** Custom Tones Details

| LABEL | DESCRIPTION |
|---|---|
| Total Time for All Tones | 900 seconds for all custom tones combined |
| Maximum Time per Individual Tone | 180 seconds |
| Total Number of Tones Recordable | 5<br>You can record up to 5 different custom tones but the total time must be 900 seconds or less. |

### Recording Custom Tones

Use the following steps if you would like to create new tones or change your tones:

1 Pick up the phone and press “****” on your phone’s keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1101~1105 on your phone followed by the “#” key.

3 Play your desired music or voice recording into the receiver’s mouthpiece. Press the “#” key.

4 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

**Listening to Custom Tones**

Do the following to listen to a custom tone:

1 Pick up the phone and press “****” on your phone’s keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1201~1208 followed by the “#” key to listen to the tone.

3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

**Deleting Custom Tones**

Do the following to delete a custom tone:

1 Pick up the phone and press “****” on your phone’s keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1301~1308 followed by the “#” key to delete the tone of your choice. Press 14 followed by the “#” key if you wish to clear all your custom tones.

You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

## 21.8.1 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

**Type of Service (ToS)**

Network traffic can be classified by setting the ToS (Type of Service) values at the data source (for example, at the Router) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

**DiffServ**

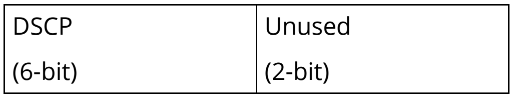
DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCP) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.[1]

### DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

**Figure 117** DiffServ: Differentiated Service Field



| DSCP<br>(6-bit) | Unused<br>(2-bit) |
|---|---|

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

## 21.8.2 Phone Services Overview

Supplementary services such as call hold, call waiting, and call transfer. are generally available from your VoIP service provider. The Router supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding
- Three-Way Conference
- Internal Calls
- Call Park and Pickup
- Do not Disturb

To take full advantage of the supplementary phone services available through the Router's phone ports, you may need to subscribe to the services from your VoIP service provider.

[1] The Router does not support DiffServ at the time of writing.

### 21.8.2.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the Router.

You can invoke all the supplementary services by using the flash key.

### 21.8.2.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

**Table 107** European Flash Key Commands

| COMMAND | SUB-COMMAND | DESCRIPTION |
|---|---|---|
| Flash | | Put a current call on hold to place a second call.<br>Switch back to the call (if there is no second call). |
| Flash | 0 | Drop the call presently on hold or reject an incoming call which is waiting for answer. |
| Flash | 1 | Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold. |
| Flash | 2 | 1. Switch back and forth between two calls.<br>2. Put a current call on hold to answer an incoming call.<br>3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold). |
| Flash | 3 | Create three-way conference connection. |
| Flash | *98# | Transfer the call to another phone. |

#### European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then “2” to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then “0” to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then “1” to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

### European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.

  Press the flash key and then press “0”.
- Disconnect the first call and answer the second call.

  Either press the flash key and press “1”, or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.

  Press the flash key and then “2”.

### European Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial “*98#” followed by the number to which you want to transfer the call.
3. After you hear the ring signal or the second party answers it, hang up the phone.

### European Three-Way Conference

Use the following steps to make three-way conference calls.

1. When you are on the phone talking to someone, press the flash key to put the caller on hold and get a dial tone.
2. Dial a phone number directly to make another call.
3. When the second call is answered, press the flash key and press “3” to create a three-way conversation.
4. Hang up the phone to drop the connection.
5. If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press “2”.

### 21.8.2.3 USA Type Supplementary Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

**Table 108** USA Flash Key Commands

| COMMAND | SUB-COMMAND | DESCRIPTION |
|---|---|---|
| Flash | | Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call.<br>Put a current call on hold to answer an incoming call. |
| Flash | *98# | Transfer the call to another phone. |

**USA Call Hold**

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller **A** and **B** by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

**USA Call Waiting**

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

**USA Call Transfer**

Do the following to transfer an incoming call (that you have answered) to another phone.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial “*98#” followed by the number to which you want to transfer the call.
3. After you hear the ring signal or the second party answers it, hang up the phone.

**USA Three-Way Conference**

Use the following steps to make three-way conference calls.

1 When you are on the phone talking to someone (party A), press the flash key to put the caller on hold and get a dial tone.

2 Dial a phone number directly to make another call (to party B).

3 When party B answers the second call, press the flash key to create a three-way conversation.

4 Hang up the phone to drop the connection.

5 If you want to separate the activated three-way conference into two individual connections (with party A on-line and party B on hold), press the flash key.

6 If you want to go back to the three-way conversation, press the flash key again.

7 If you want to separate the activated three-way conference into two individual connections again, press the flash key. This time the party B is on-line and party A is on hold.

## 21.8.2.4 Phone Functions Summary

The following table shows the key combinations you can enter on your phone's keypad to use certain features.

**Table 109** Phone Functions Summary

| ACTION | FUNCTION | DESCRIPTION |
|---|---|---|
| *98# | Call transfer | Transfer a call to another phone. See Section 21.8.2.2 on page 192 (Europe type) and Section 21.8.2.3 on page 194 (USA type). |
| *66# | Call return | Place a call to the last person who called you. |
| *95# | Enable Do Not Disturb | Use these to set your phone not to ring when someone calls you, or to turn this function off. |
| #95# | Disable Do Not Disturb | |
| *41# | Enable Call Waiting | Use these to allow you to put a call on hold when you are answering another, or to turn this function off. |
| #41# | Disable Call Waiting | |
| **** | IVR | Use these to set up Interactive Voice Response (IVR). IVR allows you to record custom caller ringing tones (the sound a caller hears before you pick up the phone) and on hold tones (the sound someone hears when you put their call on hold). |
| #### | Internal Call | Call the phone(s) connected to the Router. |
| *82 | One Shot Caller Display Call | Activate or deactivate caller ID for the next call only. |
| *67 | One Shot Caller Hidden Call | |

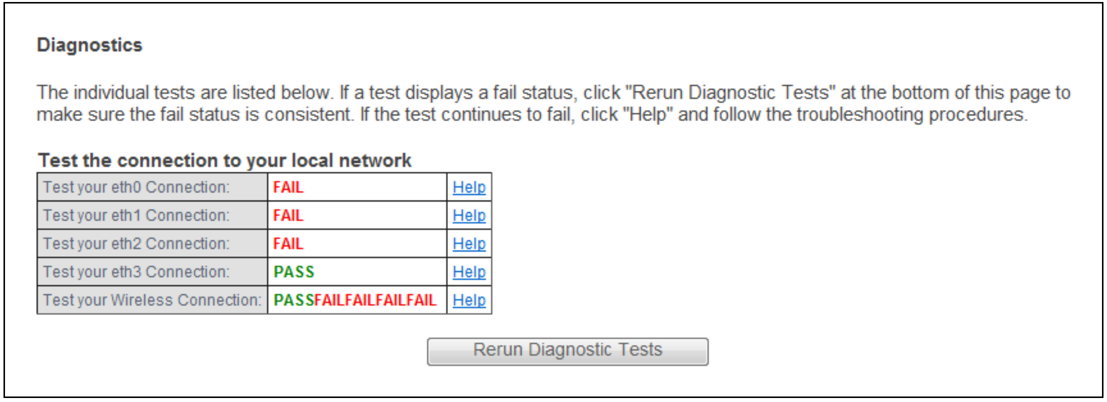
# Diagnostics

# 22 Chapter

## 22.1 Diagnostics

Click **Diagnostics** to test the Router's connections.

**Figure 118** Diagnostics



**Diagnostics**

The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

**Test the connection to your local network**

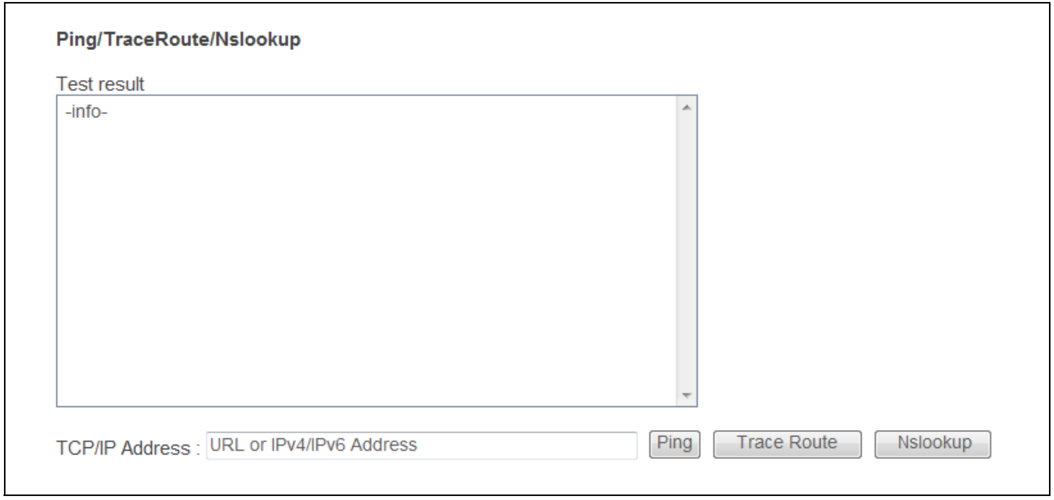
| | | |
|---|---|---|
| Test your eth0 Connection: | FAIL | Help |
| Test your eth1 Connection: | FAIL | Help |
| Test your eth2 Connection: | FAIL | Help |
| Test your eth3 Connection: | PASS | Help |
| Test your Wireless Connection: | PASSFAILFAILFAILFAIL | Help |

Click **Rerun Diagnostic Tests** to perform the tests again.

## 22.2 Ping/TraceRoute/Nslookup

Ping, traceroute, and nslookup help check availability of remote hosts and also help troubleshoot network or Internet connections. Click **Diagnostics > Ping&TraceRoute&Nslookup** to open the screen shown next.

**Figure 119** Ping/TraceRoute/Nslookup



**Ping/TraceRoute/Nslookup**

Test result

```
-info-
```

TCP/IP Address : URL or IPv4/IPv6 Address

**Table 110** Ping/TraceRoute/Nslookup

| LABEL | DESCRIPTION |
|---|---|
| Ping | Type an IPv4 or IPv6 address to which to test a connection. Click **Ping** and the ping statistics will show in the diagnostic. |
| TraceRoute | Click this to show the path that packets take from the system to the IP address that you entered. |
| Nslookup | Click this button to perform a DNS lookup on the IP address that you entered. |

# Settings

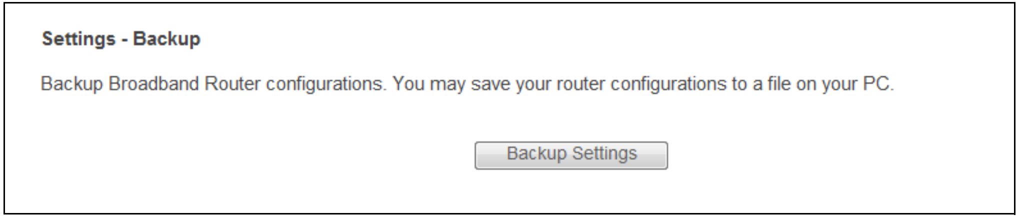
23 Chapter

This chapter describes how to manage your Router’s configuration.

## 23.1 Backup Configuration Using the Web Configurator

Click **Management > Settings > Backup** to open the following screen. Use this screen to back up (save) the Router’s current configuration to a file on your computer. Once your Router is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

**Figure 120** Settings: Backup



Settings - Backup

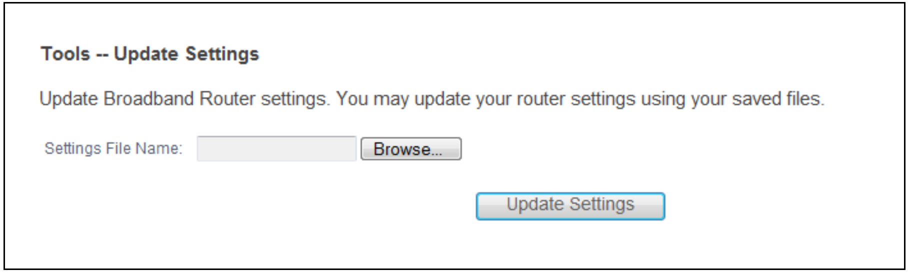
Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

Click **Backup Settings** to save the Router’s current configuration to your computer.

## 23.2 Restore Configuration Using the Web Configurator

Click **Management > Settings > Update** to open the following screen. Use this screen to upload a new or previously saved configuration file from your computer to your Router.

**Figure 121** Settings: Update



Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name:

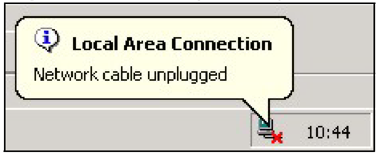
**Table 111** Settings: Update

| LABEL | DESCRIPTION |
|---|---|
| Settings File Name | Type in the location of the file you want to upload in this field or click **Browse...** to find it. |
| Browse... | Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them. |
| Update Settings | Click this to begin the upload process. |

Do not turn off the Router while configuration file upload is in progress

You must then wait before logging into the Router again. The Router automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 122** Temporarily Disconnected



Local Area Connection

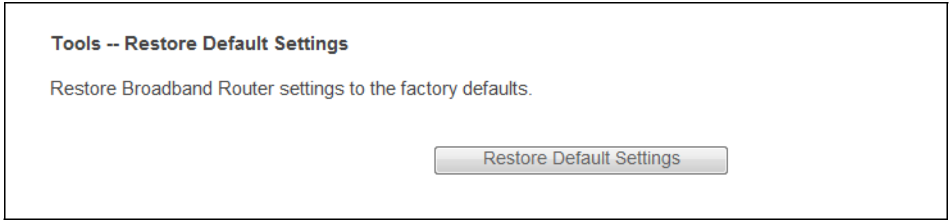
Network cable unplugged

You may need to change the IP address of your computer to be in the same subnet as that of the Router's IP address (192.168.1.1). See the appendix for details on how to set up your computer's IP address.

## 23.3 Restoring Factory Defaults

Click **Management > Settings > Restore Default** to open the following screen.

Figure 123 Management > Settings > Restore Default



Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

Click **Restore Default Settings** to clear all user-entered configuration information and return the Router to its factory defaults.

You can also press the **RESET** button on the rear panel to reset the factory defaults of your Router.

You may need to change the IP address of your computer to be in the same subnet as that of the default Router IP address (192.168.1.1). See the appendix for details on how to set up your computer's IP address.

# Logs

24 Chapter

## 24.1 Logs

The Web Configurator allows you to choose which categories of events and/or alerts to have the Router log and then display the logs or have the Router send them to an administrator (as e-mail) or to a syslog server.

### 24.1.1 What You Need To Know

The following terms and concepts may help as you read this chapter.

**Alerts and Logs**

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

**Syslog Overview**

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

**Table 112** Syslog Severity Levels

| CODE | SEVERITY |
|---|---|
| 0 | Emergency: The system is unusable. |
| 1 | Alert: Action must be taken immediately. |
| 2 | Critical: The system condition is critical. |
| 3 | Error: There is an error condition on the system. |
| 4 | Warning: There is a warning condition on the system. |
| 5 | Notice: There is a normal but significant condition on the system. |

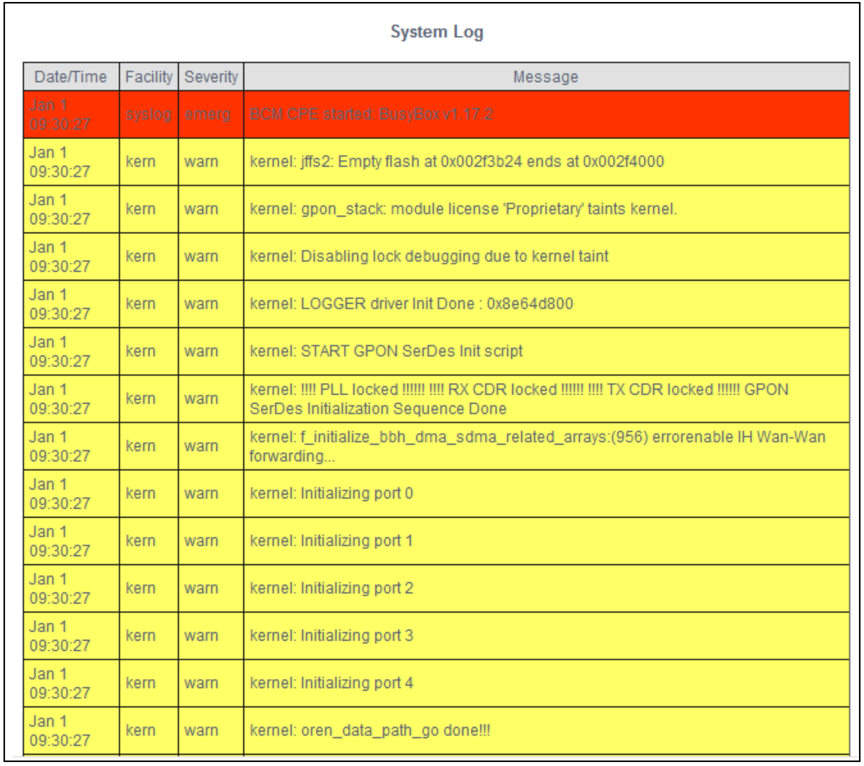
Table 112 Syslog Severity Levels (continued)

| CODE | SEVERITY |
|---|---|
| 6 | Informational: The syslog contains an informational message. |
| 7 | Debug: The message is intended for debug-level purposes. |

## 24.2 System Log

Use the **System Log** screen to see the system logs. Click **Management > System Log > View System Log** to open the **System Log** screen.

**Figure 124** System Log



System Log

| Date/Time | Facility | Severity | Message |
|---|---|---|---|
| Jan 1<br>09:30:27 | syslog | emerg | BCM CPE started: BusyBox v1.17.2 |
| Jan 1<br>09:30:27 | kern | warn | kernel: jffs2: Empty flash at 0x002f3b24 ends at 0x002f4000 |
| Jan 1<br>09:30:27 | kern | warn | kernel: gpon_stack: module license 'Proprietary' taints kernel. |
| Jan 1<br>09:30:27 | kern | warn | kernel: Disabling lock debugging due to kernel taint |
| Jan 1<br>09:30:27 | kern | warn | kernel: LOGGER driver Init Done : 0x8e64d800 |
| Jan 1<br>09:30:27 | kern | warn | kernel: START GPON SerDes Init script |
| Jan 1<br>09:30:27 | kern | warn | kernel: !!!! PLL locked !!!!!! !!!! RX CDR locked !!!!!! !!!! TX CDR locked !!!!!! GPON SerDes Initialization Sequence Done |
| Jan 1<br>09:30:27 | kern | warn | kernel: f_initialize_bbh_dma_sdma_related_arrays:(956) errorenable IH Wan-Wan forwarding... |
| Jan 1<br>09:30:27 | kern | warn | kernel: Initializing port 0 |
| Jan 1<br>09:30:27 | kern | warn | kernel: Initializing port 1 |
| Jan 1<br>09:30:27 | kern | warn | kernel: Initializing port 2 |
| Jan 1<br>09:30:27 | kern | warn | kernel: Initializing port 3 |
| Jan 1<br>09:30:27 | kern | warn | kernel: Initializing port 4 |
| Jan 1<br>09:30:27 | kern | warn | kernel: oren_data_path_go done!!! |

The following table describes the fields in this screen.

Table 113 System Log

| LABEL | DESCRIPTION |
|---|---|
| Date/Time | This field displays when the log was recorded. |
| Facility | The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Severity | This field displays the severity level of the logs that the device is to send to this syslog server. |

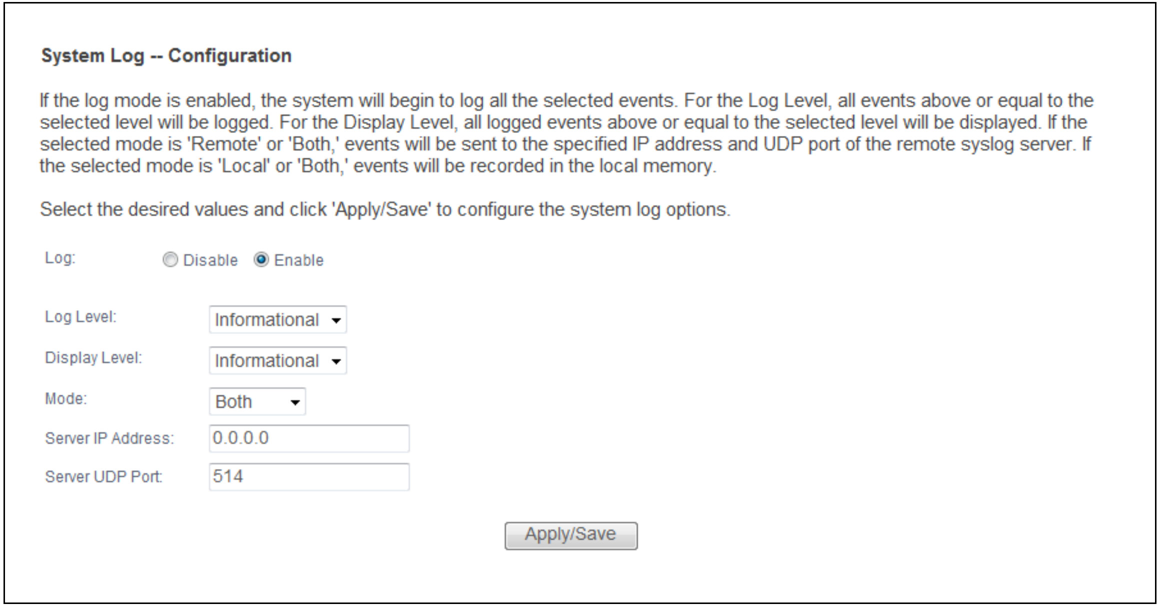
**Table 113** System Log (continued)

| LABEL | DESCRIPTION |
|---|---|
| Messages | This field states the reason for the log. |
| Refresh | Click this to renew the log screen. |
| Close | Click this to close the log screen. |

## 24.3 System Log Configuration

To change your Router's log settings, click **Management > System Log > Configure System Log**. The screen appears as shown.

**Figure 125** System Log Configuration



**System Log -- Configuration**

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: ○ Disable ● Enable

Log Level: Informational

Display Level: Informational

Mode: Both

Server IP Address: 0.0.0.0

Server UDP Port: 514

The following table describes the fields in this screen.

**Table 114** System Log Configuration

| LABEL | DESCRIPTION |
|---|---|
| Log | Select **Enable** to have the Router log events. |
| Log Level | Select the severity level of events to log. |
| Display Level | Select the severity level of events to display in the log. |
| Mode | Select the syslog destination from the drop-down list box.<br>Select **Remote**, the log(s) to send logs only to a remote syslog server. Select **Local** to save the logs in a local file. To send the log(s) to a remote syslog server and save it in a local file, select **Both**. |

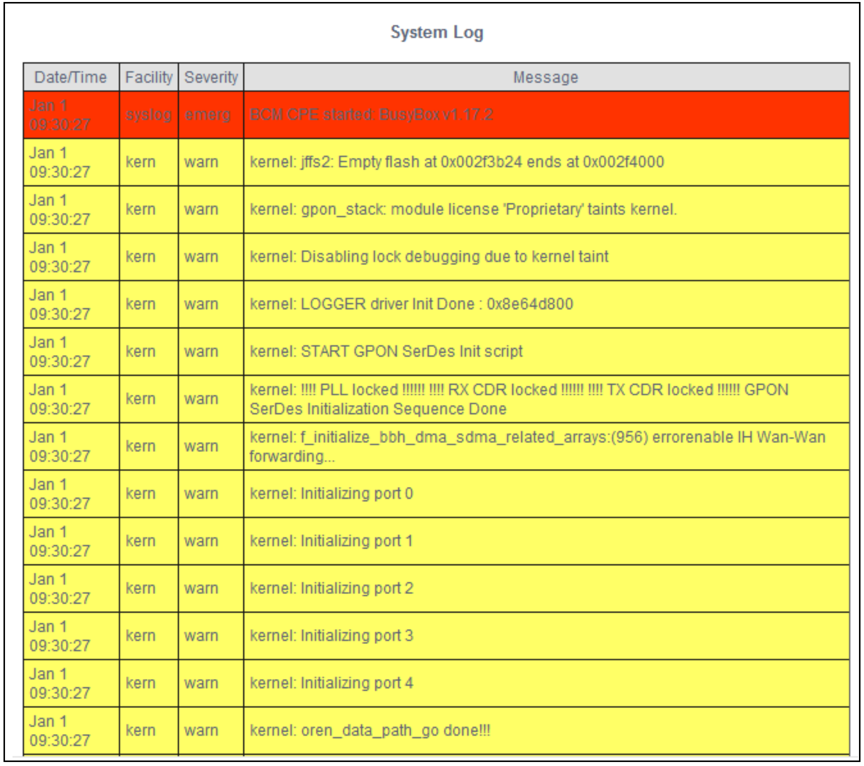
Table 114 System Log Configuration (continued)

| LABEL | DESCRIPTION |
|---|---|
| Server IP Address | Enter the IP address of the syslog server that will log the selected categories of logs. |
| Server UDP Port | Enter the port number used by the syslog server. |
| Apply/Save | Click this button to save your changes. |

## 24.4 Security Log

Use the **Security Log** screen to see the system logs. Click **Management > Security Log > View** to open the **Security Log** screen.

**Figure 126** Security Log



System Log

| Date/Time | Facility | Severity | Message |
|---|---|---|---|
| Jan 1 09:30:27 | syslog | emerg | BCM CPE started: BusyBox v1.17.2 |
| Jan 1 09:30:27 | kern | warn | kernel: jffs2: Empty flash at 0x002f3b24 ends at 0x002f4000 |
| Jan 1 09:30:27 | kern | warn | kernel: gpon_stack: module license 'Proprietary' taints kernel. |
| Jan 1 09:30:27 | kern | warn | kernel: Disabling lock debugging due to kernel taint |
| Jan 1 09:30:27 | kern | warn | kernel: LOGGER driver Init Done : 0x8e64d800 |
| Jan 1 09:30:27 | kern | warn | kernel: START GPON SerDes Init script |
| Jan 1 09:30:27 | kern | warn | kernel: !!!! PLL locked !!!!!! !!!! RX CDR locked !!!!!! !!!! TX CDR locked !!!!!! GPON SerDes Initialization Sequence Done |
| Jan 1 09:30:27 | kern | warn | kernel: f_initialize_bbh_dma_sdma_related_arrays:(956) errorenable IH Wan-Wan forwarding... |
| Jan 1 09:30:27 | kern | warn | kernel: Initializing port 0 |
| Jan 1 09:30:27 | kern | warn | kernel: Initializing port 1 |
| Jan 1 09:30:27 | kern | warn | kernel: Initializing port 2 |
| Jan 1 09:30:27 | kern | warn | kernel: Initializing port 3 |
| Jan 1 09:30:27 | kern | warn | kernel: Initializing port 4 |
| Jan 1 09:30:27 | kern | warn | kernel: oren_data_path_go done!!! |

The following table describes the fields in this screen.

**Table 115** Security Log

| LABEL | DESCRIPTION |
|---|---|
| Date/Time | This field displays when the log was recorded. |
| Facility | The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Severity | This field displays the severity level of the logs that the device is to send to this syslog server. |
| Messages | This field states the reason for the log. |
| Refresh | Click this to renew the log screen. |
| Close | Click this to close the log screen. |

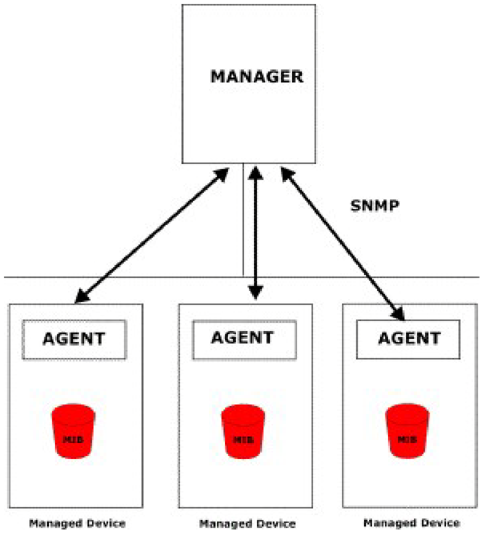
# SNMP

25 Chapter

## 25.1 SNMP Agent

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Router supports SNMP agent functionality, which allows a manager station to manage and monitor the Router through the network. The Router supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

**Figure 127** SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the Router). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

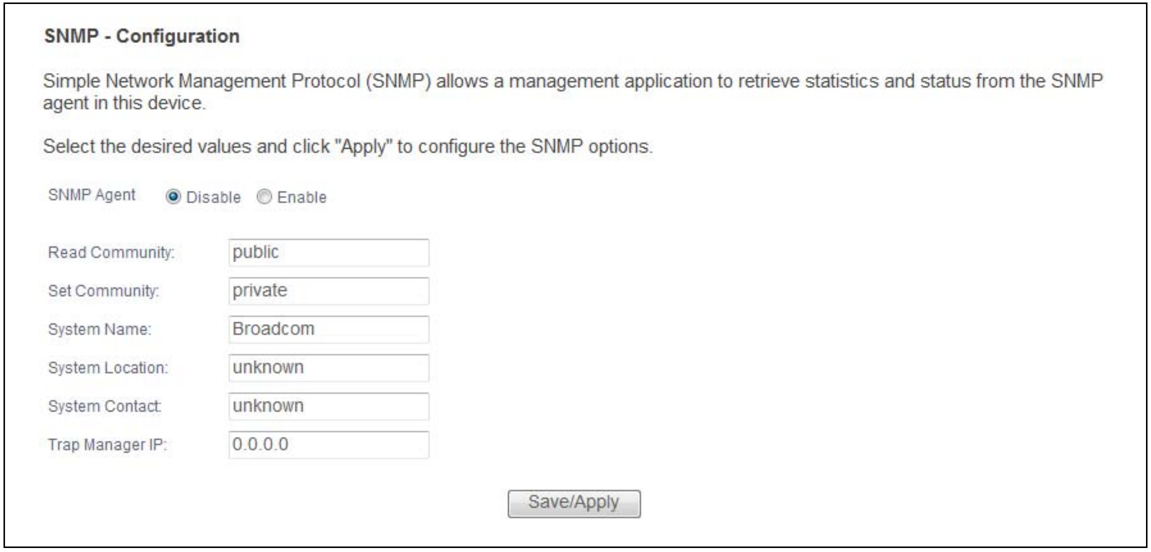
The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

Click **Management > SNMP Agent** to open the following screen. Use this screen to configure the Router SNMP settings.

**Figure 128** Management > SNMP Agent



**SNMP - Configuration**

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent ● Disable ○ Enable

| | |
|---|---|
| Read Community: | public |
| Set Community: | private |
| System Name: | Broadcom |
| System Location: | unknown |
| System Contact: | unknown |
| Trap Manager IP: | 0.0.0.0 |

The following table describes the fields in this screen.

**Table 116** Management > SNMP Agent

| LABEL | DESCRIPTION |
|---|---|
| SNMP Agent | Select **Enable** to let the Router act as an SNMP agent, which allows a manager station to manage and monitor the Device through the network. Select **Disable** to turn this feature off. |
| Read Community | Enter the **Read Community**, which is the password for the incoming Get and GetNext requests from the management station. |
| Set Community | Enter the **Set community**, which is the password for incoming Set requests from the management station. |
| System Name | Enter the SNMP system name. |
| System Location | Enter the SNMP system location. |

Table 116 Management > SNMP Agent (continued)

| LABEL | DESCRIPTION |
|---|---|
| System Contact | Enter the SNMP system contact. |
| Trap Manager IP | Type the IP address of the station to send your SNMP traps to. |
| Save/Apply | Click this to save your changes back to the Router. |

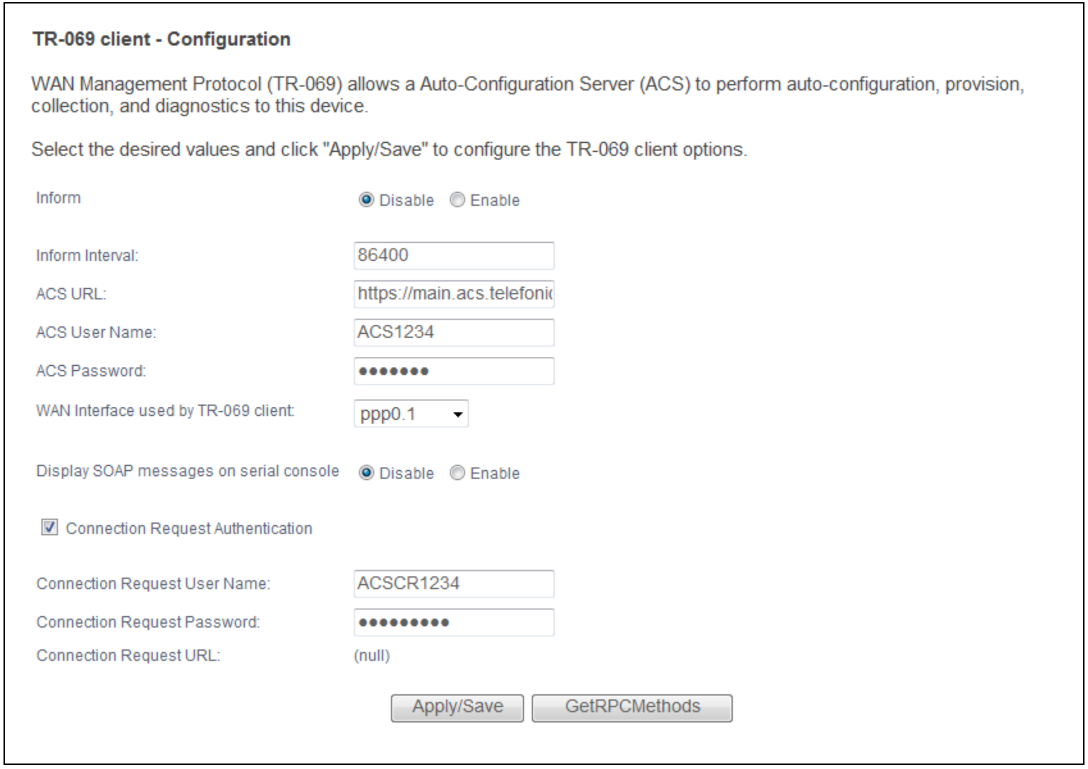
# TR-069 Client

# 26 Chapter

## 26.1 TR-069 Client

Click **Management > TR-069 Client** to open the following screen. Use this screen to configure your Router to be managed by an ACS (Auto Configuration Server).

**Figure 129** TR-069 Client



**TR-069 client - Configuration**

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

| | |
|---|---|
| Inform | ● Disable ○ Enable |
| Inform Interval: | 86400 |
| ACS URL: | https://main.acs.telefoni |
| ACS User Name: | ACS1234 |
| ACS Password: | ●●●●●●● |
| WAN Interface used by TR-069 client: | ppp0.1 |
| Display SOAP messages on serial console | ● Disable ○ Enable |
| ☑ Connection Request Authentication | |
| Connection Request User Name: | ACSCR1234 |
| Connection Request Password: | ●●●●●●●●● |
| Connection Request URL: | (null) |

**Table 117** TR-069 Client

| LABEL | DESCRIPTION |
|---|---|
| Inform | Select **Enable** for the Router to send periodic inform via TR-069 on the WAN. Otherwise, select **Disable**. |
| Inform Interval | Enter the time interval (in seconds) at which the Router sends information to the auto-configuration server. |
| ACS URL | Enter the URL or IP address of the auto-configuration server. |

**Table 117** TR-069 Client (continued)

| LABEL | DESCRIPTION |
|---|---|
| ACS User Name | Enter the TR-069 user name for authentication with the auto-configuration server. |
| ACS Password | Enter the TR-069 password for authentication with the auto-configuration server. |
| WAN Interface used by TR-069 client | Select a WAN interface through which the TR-069 traffic passes.<br>If you select **Any_WAN**, you should also select the pre-configured WAN connection(s). |
| Display SOAP messages on serial console | Select **Enable** to show the SOAP messages on the console. |
| Connection Request Authentication | Select this option to enable authentication when there is a connection request from the ACS. |
| Connection Request User Name | Enter the connection request user name. When the ACS makes a connection request to the Router, this user name is used to authenticate the ACS. |
| Connection Request Password | Enter the connection request password. When the ACS makes a connection request to the Router, this password is used to authenticate the ACS. |
| Connection Request URL | This shows the connection request URL. The ACS can use this URL to make a connection request to the Router. |
| Apply/Save | Click this button to save your changes. |
| GetRPCMethods | In TR-069, a Remote Procedure Call (RPC) mechanism is used for bidirectional communication between a CPE and the auto-configuration server. The RPC method is used to initiate the transfer (download or upload) between them. Click this button to discover the method supported by the ACS, such as Inform, TransferComplete or RequestDownload. |

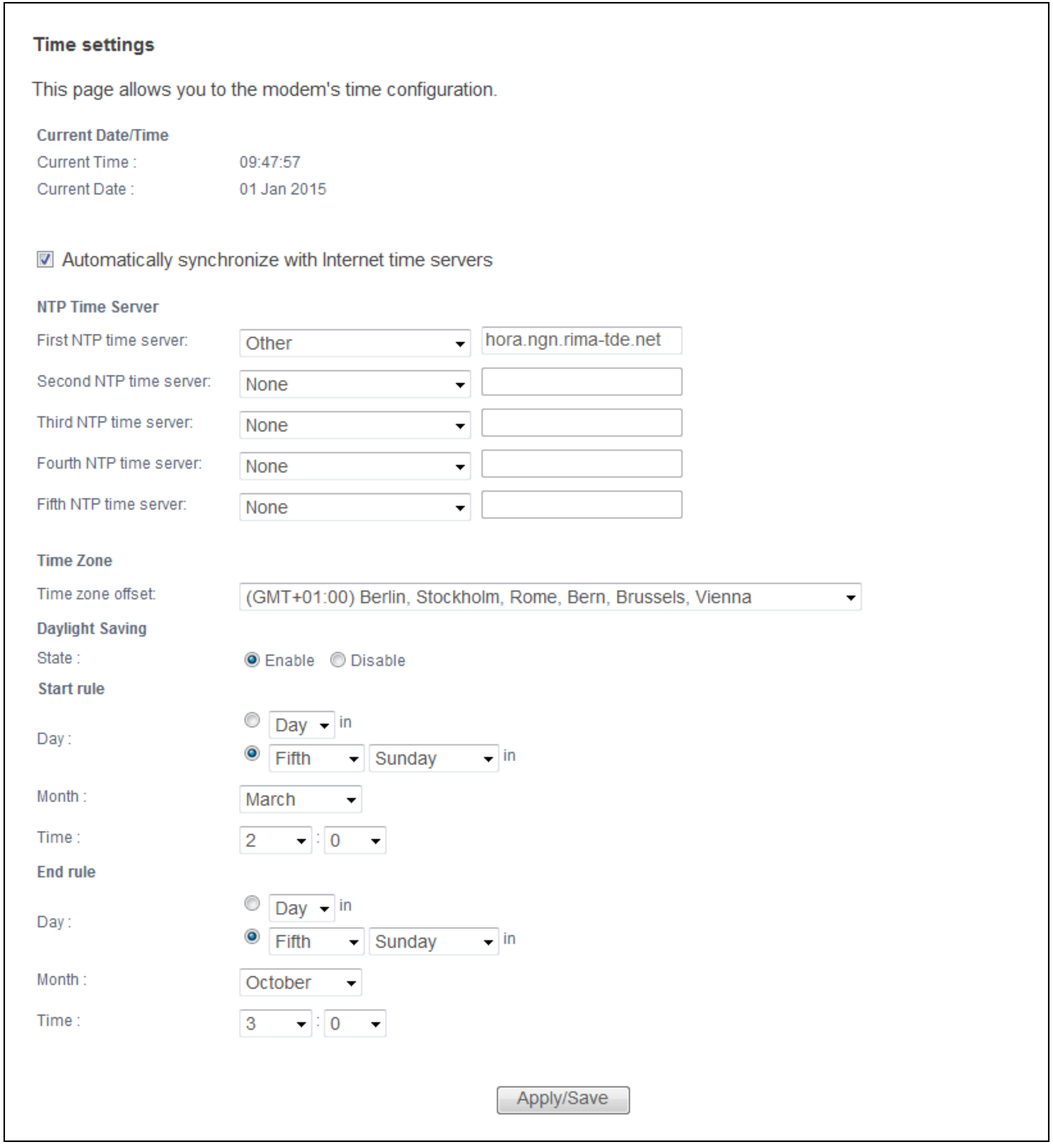
# Internet Time

27 Chapter

## 27.1 Internet Time

Click **Management > Internet Time** to configure the Router to get the time from time servers on the Internet.

**Figure 130** Internet Time



**Time settings**

This page allows you to the modem's time configuration.

**Current Date/Time**

| | |
|---|---|
| Current Time : | 09:47:57 |
| Current Date : | 01 Jan 2015 |

☑ Automatically synchronize with Internet time servers

**NTP Time Server**

| | | |
|---|---|---|
| First NTP time server: | Other | hora.ngn.rima-tde.net |
| Second NTP time server: | None | |
| Third NTP time server: | None | |
| Fourth NTP time server: | None | |
| Fifth NTP time server: | None | |

**Time Zone**

Time zone offset: (GMT+01:00) Berlin, Stockholm, Rome, Bern, Brussels, Vienna

**Daylight Saving**

State : ● Enable ○ Disable

**Start rule**

Day : ○ Day in<br>● Fifth Sunday in

Month : March

Time : 2 : 0

**End rule**

Day : ○ Day in<br>● Fifth Sunday in

Month : October

Time : 3 : 0

The following table describes the fields in this screen.

Table 118 Internet Time

| LABEL | DESCRIPTION |
|---|---|
| Automatically synchronize with Internet time servers | Select this to have the Router get the time from the specified Internet time servers. |
| First ~ Fifth NTP time server | Select an NTP time server from the drop-down list box.<br>Otherwise, select **Other** and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server.<br>Select **None** if you don’t want to configure the time server.<br>Check with your ISP/network administrator if you are unsure of this information. |
| Time zone offset | Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). |
| Daylight Savings | Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time. |
| Start/End Date | Configure the day and time when Daylight Saving Time starts/ends if you enabled daylight saving. The **Time** fields use the 24 hour format. |
| Apply/Save | Click this button to save your changes. |

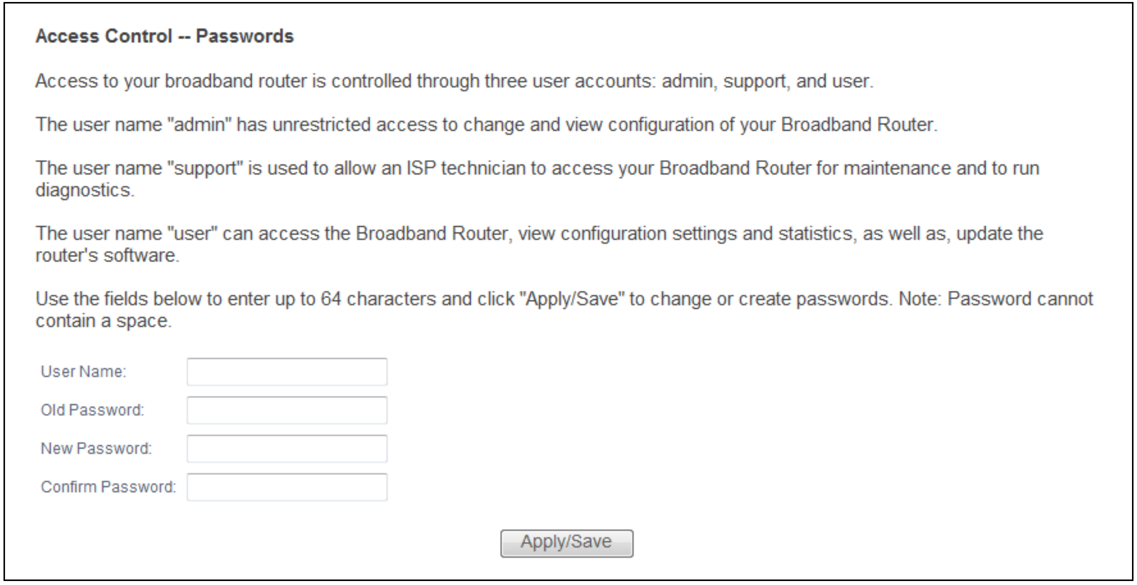
# User Passwords

28 Chapter

## 28.1 User Passwords

Click **Management > Access Control > Passwords** to change the login password.

**Figure 131** Use Passwords



**Access Control -- Passwords**

Access to your broadband router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.

The user name "support" is used to allow an ISP technician to access your Broadband Router for maintenance and to run diagnostics.

The user name "user" can access the Broadband Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 64 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

| | |
|---|---|
| User Name: | |
| Old Password: | |
| New Password: | |
| Confirm Password: | |

**Table 119** User Passwords

| LABEL | DESCRIPTION |
|---|---|
| User Name | Enter the name of one of the Router system accounts. |
| Old Password | Type the account’s default password or existing password. |
| New Password | Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Router. |
| Retype to confirm | Type the new password again for confirmation. |
| Apply/Save | Click this button to save your changes. |

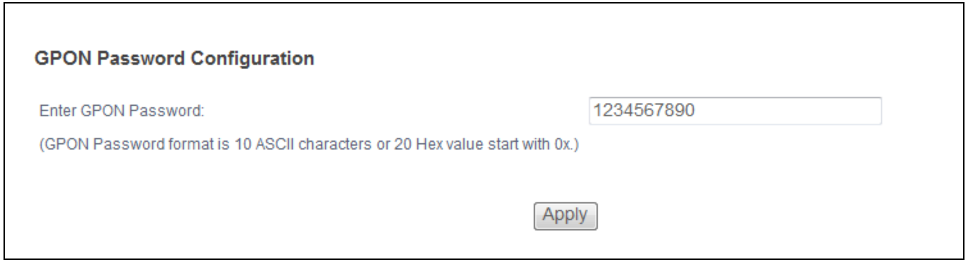
# GPON Password

Chapter 29

## 29.1 GPON Password

Click **Management > GPON Password** to enter the password for your GPON Internet access account.

**Figure 132** GPON Password



GPON Password Configuration

Enter GPON Password: 1234567890

(GPON Password format is 10 ASCII characters or 20 Hex value start with 0x.)

**Table 120** GPON Password

| LABEL | DESCRIPTION |
|---|---|
| Enter GPON Password | Enter the password for your GPON Internet access account. |
| Apply | Click this button to save and apply your changes. |

# Update Software

30 Chapter

## 30.1 Update Software

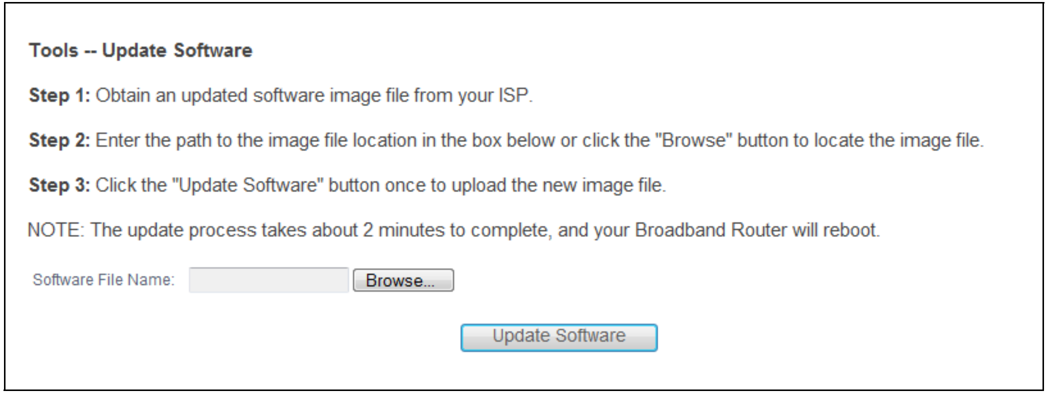
Click **Management > Update Software** to open the following screen where you can upload new software to your Router. You can download new software releases from your ISP to use to upgrade your device’s performance.

Only use software for your device’s specific model. Refer to the label on the bottom of your Router.

The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Do NOT turn off the Router while software upload is in progress!

**Figure 133** Update Software



**Tools -- Update Software**

**Step 1:** Obtain an updated software image file from your ISP.

**Step 2:** Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

**Step 3:** Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Software File Name:

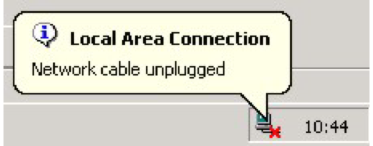
**Table 121** Update Software

| LABEL | DESCRIPTION |
|---|---|
| Software File Name | Type in the location of the file you want to upload in this field or click **Browse ...** to find it. |
| Browse... | Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them. |
| Update Software | Click this to begin the upload process. This process may take up to two minutes. |

After you see the software updating screen, wait two minutes before logging into the Router again.

The Router automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 134 Network Temporarily Disconnected



**Local Area Connection**

Network cable unplugged

After two minutes, log in again and check your new software version in the **Device Info** screen.

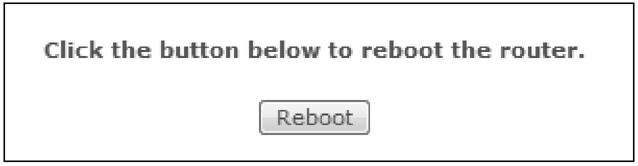
# Reboot

31 Chapter

## 31.1 Restart Using the Web Configurator

Click **Management > Reboot** to open the following screen. Use this screen to restart the .

**Figure 135** Reboot



Click the button below to reboot the router.

# Troubleshooting

32 Chapter

## 32.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Router Access and Login
- Internet Access
- Wireless Internet Access
- Phone Calls and VoIP
- UPnP

## 32.2 Power, Hardware Connections, and LEDs

The Router does not turn on. None of the LEDs turn on.

1. Make sure the Router is turned on.
2. Make sure you are using the power adaptor or cord included with the Router.
3. Make sure the power adaptor or cord is connected to the Router and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the Router off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.3 on page 11.
2. Check the hardware connections. See Section 1.2 on page 9.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4. Turn the Router off and on.

5. If the problem continues, contact the vendor.

## 32.3 Router Access and Login

### I forgot the IP address for the Router.

1. The default IP address is 192.168.1.1.

2. If you changed the IP address and have forgotten it, you might get the IP address of the Router by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Router (it depends on the network), so enter this IP address in your Internet browser.

3. If this does not work, you have to reset the device to its factory defaults. See Section 1.2 on page 9.

### I forgot the password.

1. The default password is random. Please refer to the label sticker at the bottom of the device.

2. If you can’t remember the password, you have to reset the device to its factory defaults. See Section 1.2 on page 9.

### I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.1.
   - If you changed the IP address (Section 4.1 on page 46), use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Router.

2. Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.2 on page 9.

3. Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled.

4. Reset the device to its factory defaults, and try to access the Router with the default IP address. See Section 1.2 on page 9.

5. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

**Advanced Suggestions**

- Try to access the Router using another service, such as Telnet. If you can access the Router, check the remote management settings and firewall rules to find out why the Router does not respond to HTTP.
- If your computer is connected wirelessly, use a computer that is connected to a **ETHERNET** port.

### I can see the **Login** screen, but I cannot log in to the Router.

1 Make sure you have entered the user name and password correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the Router. Log out of the Router in the other session, or ask the person who is logged in to log out.

3 Turn the Router off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 32.2 on page 219.

### I cannot Telnet to the Router.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

### I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

## 32.4 Internet Access

### I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.3 on page 11.

2 Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.

4. If you are trying to access the Internet wirelessly, make sure you have enabled the wireless LAN by the **Wifi/WPS** button or the **Network Setting > Wireless > General** screen.

5. Disconnect all the cables from your device, and follow the directions in Section 1.2 on page 9. again.

6. If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the Router), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.3 on page 11.

2. Turn the Router off and on.

3. If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.3 on page 11. If the Router is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2. Turn the Router off and on.

3. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

**Advanced Suggestions**

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

## 32.5 Wireless Internet Access

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

### What wireless security modes does my Router support?

Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network.

The available security modes in your Router are as follows:

- **WPA2-PSK:** (recommended) This uses a pre-shared key with the WPA2 standard.
- **WPA-PSK:** This has the device use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.
- **WPA2:** WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. It requires the use of a RADIUS server and is mostly used in business networks.
- **WPA:** Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. It requires the use of a RADIUS server and is mostly used in business networks.
- **WEP:** Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.

## 32.6 Phone Calls and VoIP

### The telephone port won’t work or the telephone lacks a dial tone.

1 Check the telephone connections and telephone wire.

### I can access the Internet, but cannot make VoIP calls.

1 The **Telf** light should come on. Make sure that your telephone is connected to the **Telf1** port.

2 You can also check the VoIP status in the **System Info** screen.

3 If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you can make a call using speed dial, there may be something wrong with the SIP server, contact your VoIP service provider.

## 32.7 UPnP

### When using UPnP and the Router reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

1 Disconnect the Ethernet cable from the Router’s LAN port or from your computer.

2 Re-connect the Ethernet cable.

### The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

### I cannot open special applications such as white board, file transfer and video when I use the MSN messenger.

1 Wait more than three minutes.

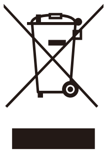
2 Restart the applications.

# Safety Warnings

Appendix A

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- This product is for indoor use only (utilisation intérieure exclusivement).

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



**Federal Communications Commission (FCC) 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 generate, 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:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 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.

**RF exposure warning**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be collocated or operating in conjunction with any other antenna or transmitter.