Backup KDC Optionally, specify a numerical (non-DNS) IP address and port for a backup KDC. Backup KDCs are referred to as slave servers. The slave server periodically synchronizes its database with the primary (or master) KDC.

Remote KDC Optionally, specify a numerical (non-DNS) IP address and port for a remote KDC. Kerberos implementations can use an administration server allowing remote manipulation of the Kerberos database. This administration server usually runs on the KDC.

Port Specify the ports on which the Primary, Backup and Remote KDCs reside. The default port number for Kerberos Key Distribution Centers is Port 88.

6. Click the **Apply** button to return to the **WLAN** screen to save any changes made within the Kerberos Configuration field of the New Security Policy screen.
7. Click the **Cancel** button to undo any changes made within the Kerberos Configuration field and return to the **WLAN** screen. This reverts all settings for the Kerberos Configuration field to the last saved configuration.

6.5 Configuring 802.1x EAP Authentication

The IEEE 802.1x standard ties the 802.1x EAP authentication protocol to both wired and wireless LAN applications.

The EAP process begins when an unauthenticated supplicant (client device) tries to connect with an authenticator (in this case, the authentication server). The access point passes EAP packets from the client to an authentication server on the wired side of the access point. All other packet types are blocked until the authentication server (typically, a RADIUS server) verifies the MU’s identity.

To configure 802.1x EAP authentication on the access point:

1. Select **Network Configuration** -> **Wireless** -> **Security** from the access point menu tree.

   If security policies supporting 802.1x EAP exist, they appear within the **Security Configuration** screen. These existing policies can be used as is, or their properties edited by clicking the **Edit** button. To configure a new security policy supporting 802.1x EAP, continue to step 2.
2. Click the **Create** button to configure a new policy supporting 802.1x EAP.

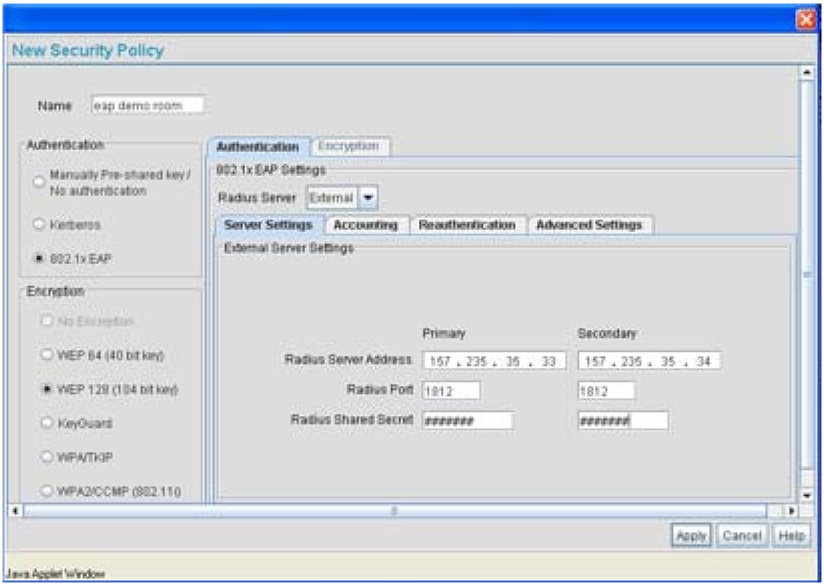
   The **New Security Policy** screen displays with no authentication or encryption options selected.

3. Select the **802.1x EAP** radio button.

   The **802.1x EAP Settings** field displays within the New Security Policy screen.

4. Ensure the **Name** of the security policy entered suits the intended configuration or function of the policy.

5. If using the access point's Internal Radius server, leave the **Radius Server** drop-down menu in the default setting of **Internal**. If an external Radius server is used, select **External** from the drop-down menu.



New Security Policy

Name: eap demo room

Authentication

○ Manually Pre-shared key / No authentication

○ Kerberos

● 802.1x EAP

Encryption

○ No Encryption

○ WEP 64 (40 bit key)

● WEP 128 (104 bit key)

○ KeyGuard

○ WPA/TKIP

○ WPA2/CCMP (802.11i)

Authentication | Encryption

802.1x EAP Settings

Radius Server: External

Server Settings | Accounting | Reauthentication | Advanced Settings

External Server Settings

	Primary	Secondary
Radius Server Address	157 . 235 . 35 . 33	157 . 235 . 35 . 34
Radius Port	1812	1812
Radius Shared Secret	#######	#######

6. Configure the **Server Settings** field as required to define address information for the authentication server. The appearance of the Server Settings field varies depending on whether Internal or External has been selected from the Radius Server drop-down menu.

Radius Server Address

If using an External Radius Server, specify the numerical (non-DNS) IP address of a primary *Remote Dial-In User Service* (Radius) server. Optionally, specify the IP address of a secondary server. The secondary server acts as a failover server if the primary server cannot be contacted. An ISP or a network administrator provides these addresses.

Radius is a client/server protocol and software enabling remote-access clients to communicate with a server used to authenticate users and authorize access to the requested system or service. This setting is not available if Internal has been selected from the Radius Server drop-down menu.

RADIUS Port

If using an External Radius Server, specify the port on which the primary Radius server is listening. Optionally, specify the port of a secondary (failover) server. Older Radius servers listen on ports 1645 and 1646. Newer servers listen on ports 1812 and 1813. Port 1645 or 1812 is used for authentication. Port 1646 or 1813 is used for accounting. The ISP or a network administrator needs to confirm the appropriate primary and secondary port numbers for authentication. This setting is not available if Internal has been selected from the Radius Server drop-down menu.

RADIUS Shared Secret

Specify a shared secret for authentication on the Internal or Primary Radius server (External Radius Server only). The shared secret is required to match the shared secret on the Radius server. Optionally, specify a shared secret for a secondary (failover) server. Use shared secrets to verify Radius messages (with the exception of the Access-Request message) sent by a Radius enabled device configured with the same shared secret.

Apply the qualifications of a well-chosen password to the generation of a shared secret. Generate a random, case-sensitive string using letters, numbers and symbols. Verify the shared secret is at least 22 characters to protect the Radius server from brute-force attacks. An example of a strong and secure shared secret is: 8d#>9fq4bV)H7%a3-zE13sW.

7. Select the **Accounting** tab as required to define a timeout period and retry interval Syslog for MUs interoperating with the access point and EAP authentication server. The items within this tab could be enabled or disabled depending on whether internal or External has been selected from the Radius Server drop-down menu.

Internal/External Accounting — If using an Internal Radius server, select **Disabled** (no Internal Accounting), **Internal Only** or **Both Internal and External**. Selecting Both Internal and External displays additional parameters for configuring the External Radius Server.

If using an External Radius server, simply select **Enable** or **Disable** to allow or deny external accounting with the external Radius server.

External Radius Server Address — Specify the IP address of the external Radius server used to provide Radius accounting.

External Radius Port — Specify the port on which the Radius server is listening.

External Radius Shared Secret — Specify a shared secret for authentication. The shared secret is required to match the shared secret on the Radius server.

MU Timeout — Specify the time (in seconds) for the access point's retransmission of EAP-Request packets. The default is 10 seconds. If this time is exceeded, the authetnication session is terminated.

Retries — Specify the number of retries for the MU to retransmit a missed frame to the Radius server before it times out of the authentication session. The default is 2 retries.

Enable Syslog — Select the **Enable Syslog** checkbox to enable syslog messages relating to EAP events to be written to the specified syslog server.

Syslog Server IP Address — Enter the IP address of the destination syslog server to be used to log EAP events.

8. Select the **Reauthentication** tab as required to define authentication connection policies, intervals and maximum retries. The items within this tab are identical regardless of whether Internal or External is selected from the Radius Server drop-down menu.

Enable Reauthentication — Select the **Enable Reauthentication** checkbox to configure a wireless connection policy so MUs are forced to reauthenticate periodically. Periodic repetition of the EAP process provides ongoing security for current authorized connections.

Period (30-9999) secs Set the EAP reauthentication period to a shorter time interval (at least 30 seconds) for tighter security on the WLAN's connections. Set the EAP reauthentication period to a longer time interval (at most, 9999 seconds) to relax security on wireless connections. The reauthentication period setting does not affect wireless connection throughput. The default is 3600 seconds.

Max. Retries (1-99) retries Define the maximum number of MU retries to reauthenticate after failing to complete the EAP process. Failure to reauthenticate in the specified number of retries results in a terminated connection. The default is 2 retries.

9. Select the **Advanced Settings** tab as required to specify a MU quiet period, timeout interval, transmit period, and retry period for MUs and the authentication server. The items within this tab are identical regardless of whether Internal or External is selected from the Radius Server drop-down menu.

MU Quiet Period (1-65535) secs Specify an idle time (in seconds) between MU authentication attempts, as required by the authentication server. The default is 10 seconds.

MU Timeout (1-255) secs Define the time (in seconds) for the access point’s retransmission of EAP-Request packets. The default is 10 seconds.

MU Tx Period (1-65635) secs Specify the time period (in seconds) for the access point's retransmission of the EAP Identity Request frame. The default is 5 seconds.

MU Max Retries (1-10) retries Specify the maximum number of times the access point retransmits an EAP-Request frame to the client before it times out the authentication session. The default is 2 retries.

Server Timeout (1-255) secs Specify the time (in seconds) for the access point's retransmission of EAP-Request packets to the server. The default is 5 seconds. If this time is exceeded, the authetnication session is terminated.

Server Max Retries (1-255 retries) Specify the maximum number of times for the access point to retransmit an EAP-Request frame to the server before it times out the authentication session. The default is 2 retries.

10. Click the **Apply** button to save any changes made within the 802.1x EAP Settings field (including all 5 selectable tabs) of the New Security Policy screen.

11. Click the **Cancel** button to undo any changes made within the 802.1x EAP Settings field and return to the **WLAN** screen. This reverts all settings for the 802.1x EAP Settings field to the last saved configuration.

6.6 Configuring WEP Encryption

Wired Equivalent Privacy (WEP) is a security protocol specified in the *IEEE Wireless Fidelity (Wi-Fi)* standard. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN.

WEP may be all that a small-business user needs for the simple encryption of wireless data. However, networks that require more security are at risk from a WEP flaw. The existing 802.11 standard alone offers administrators no effective method to update keys.

To configure WEP on the access point:

1. Select **Network Configuration** -> **Wireless** -> **Security** from the access point menu tree.

   If security policies supporting WEP exist, they appear within the **Security Configuration** screen. These existing policies can be used as is, or their properties edited by clicking the **Edit** button. To configure a new security policy supporting WEP, continue to step 2.

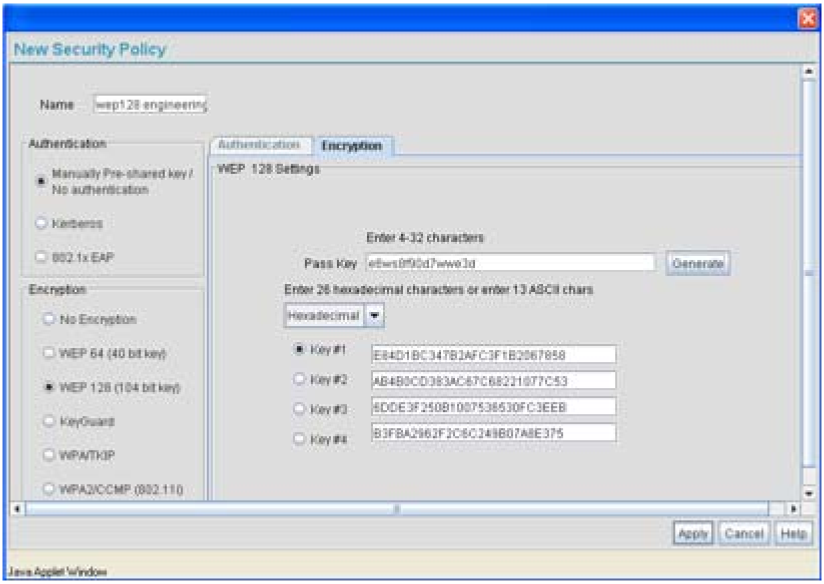
2. Click the **Create** button to configure a new policy supporting WEP.

   The **New Security Policy** screen displays with no authentication or encryption options selected.

3. Select either the **WEP 64 (40 bit key)** or **WEP 128 (104 bit key)** radio button.

   The **WEP 64 Settings** or **WEP 128 Settings** field displays within the New Security Policy screen.

4. Ensure the **Name** of the security policy entered suits the intended configuration or function of the policy.



New Security Policy

Name: wep128 engineering

Authentication
- ● Manually Pre-shared key / No authentication
- ○ Kerberos
- ○ 802.1x EAP

Encryption
- ○ No Encryption
- ○ WEP 64 (40 bit key)
- ● WEP 128 (104 bit key)
- ○ KeyGuard
- ○ WPA/TKIP
- ○ WPA2/CCMP (802.11i)

WEP 128 Settings

Enter 4-32 characters

Pass Key: e8ws0f90d7wwe3d

Enter 26 hexadecimal characters or enter 13 ASCII chars

Hexadecimal

- ● Key #1 E84D1BC347B2AFC3F1B2067858
- ○ Key #2 AB4B0CD383AC67C68221077C53
- ○ Key #3 6DDE3F250B1007536530FC3EEB
- ○ Key #4 B3FBA2962F2C6C249B07A8E375

5. Configure the **WEP 64 Settings** or **WEP 128 Settings** field as required to define the Pass Key used to generate the WEP keys. These keys must be the same between the access point and its MU to encrypt packets between the two devices.

Pass Key	Specify a 4 to 32 character pass key and click the **Generate** button. The pass key can be any alphanumeric string. The access point, other proprietary routers and Symbol MUs use the algorithm to convert an ASCII string to the same hexadecimal number. MUs without Symbol adapters need to use WEP keys manually configured as hexadecimal numbers.
Keys #1-4	Use the **Key #1-4** areas to specify key numbers. The key can be either a hexadecimal or ASCII depending on which option is selected from the drop-down menu. For WEP 64 (40-bit key), the keys are 10 hexadecimal characters in length or 5 ASCII characters. For WEP 128 (104-bit key), the keys are 26 hexadecimal characters in length or 13 ASCII characters. Select one of these keys for activation by clicking its radio button.

Default (hexadecimal) keys for WEP 64 include:

Key 1	1011121314
Key 2	2021222324
Key 3	3031323334
Key 4	4041424344

Default (hexadecimal) keys for WEP 128 include:

Key 1	101112131415161718191A1B1C
Key 2	202122232425262728292A2B2C
Key 3	303132333435363738393A3B3C
Key 4	404142434445464748494A4B4C

6. Click the **Apply** button to save any changes made within the WEP 64 Setting or WEP 128 Setting field of the New Security Policy screen.
7. Click the **Cancel** button to undo any changes made within the WEP 64 Setting or WEP 128 Setting field and return to the **WLAN** screen. This reverts all settings to the last saved configuration.

6.7 Configuring KeyGuard Encryption

KeyGuard is a proprietary encryption method developed by Symbol Technologies. KeyGuard is Symbol's enhancement to WEP encryption, and was developed before the finalization of WPA-TKIP. This encryption implementation is based on the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i.

WPA2-CCMP (not KeyGuard) offers the highest level of security among the encryption methods available with the access point.

1. Select **Network Configuration** -> **Wireless** -> **Security** from the access point menu tree.

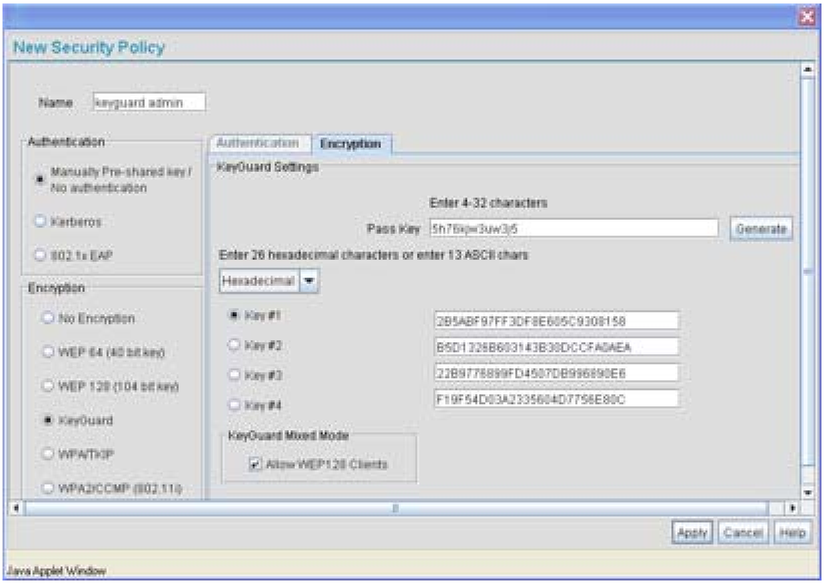
   If security policies supporting KeyGuard exist, they appear within the **Security Configuration** screen. These existing policies can be used as is, or their properties edited by clicking the **Edit** button. To configure a new security policy supporting KeyGuard, continue to step 2.
2. Click the **Create** button to configure a new policy supporting KeyGuard.

   The **New Security Policy** screen displays with no authentication or encryption options selected.

3. Select the **KeyGuard** radio button.

   The **KeyGuard Settings** field displays within the New Security Policy screen.

4. Ensure the **Name** of the security policy entered suits the intended configuration or function of the policy.



New Security Policy

Name: keyguard admin

Authentication
- ● Manually Pre-shared key / No authentication
- ○ Kerberos
- ○ 802.1x EAP

Encryption
- ○ No Encryption
- ○ WEP 64 (40 bit key)
- ○ WEP 128 (104 bit key)
- ● KeyGuard
- ○ WPA/TKIP
- ○ WPA2/CCMP (802.11i)

Authentication | Encryption

KeyGuard Settings

Enter 4-32 characters

Pass Key: 5h7bipw3uw3j5 [Generate]

Enter 26 hexadecimal characters or enter 13 ASCII chars

Hexadecimal

- ● Key #1: 2B5ABF97FF3DF8E605C9308158
- ○ Key #2: B5D1326B603143B30DCCFA0AEA
- ○ Key #3: 22B9776899FD4507DB996890E6
- ○ Key #4: F19F54D03A2335604D7756E80C

KeyGuard Mixed Mode

☑ Allow WEP128 Clients

5. Configure the **KeyGuard Settings** field as required to define the Pass Key used to generate the WEP keys used with the KeyGuard algorithm. These keys must be the same between the access point and its MU to encrypt packets between the two devices

   Pass Key Specify a 4 to 32 character pass key and click the **Generate** button. The pass key can be any alphanumeric string. The access point, other proprietary routers, and Symbol MUs use the algorithm to convert an ASCII string to the same hexadecimal number. MUs without Symbol adapters need to use WEP keys manually configured as hexadecimal numbers.

   Keys #1-4 Use the **Key #1-4** areas to specify key numbers. The key can be either a hexadecimal or ASCII depending on which option is selected from the drop-down menu. The keys are 26 hexadecimal characters in length or 13 ASCII characters. Select one of these keys for activation by clicking its radio button.

Default (hexadecimal) keys for KeyGuard include:

Key 1	101112131415161718191A1B1C
Key 2	202122232425262728292A2B2C
Key 3	303132333435363738393A3B3C
Key 4	404142434445464748494A4B4C

6. Select the **Allow WEP128 Clients** checkbox (from within the **KeyGuard Mixed Mode** field) to enable WEP128 clients to associate with an access point's KeyGuard supported WLAN. The WEP128 clients must use the same keys as the KeyGuard clients to interoperate within the access point's KeyGuard supported WLAN.
7. Click the **Apply** button to save any changes made within the KeyGuard Setting field of the New Security Policy screen.
8. Click the **Cancel** button to undo any changes made within the KeyGuard Setting field and return to the **WLAN** screen. This reverts all settings to the last saved configuration.

6.8 Configuring WPA Using TKIP

Wi-Fi Protected Access (WPA) is a robust encryption scheme specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i. WPA provides more sophisticated data encryption than WEP. WPA is designed for corporate networks and small-business environments where more wireless traffic allows quicker discovery of encryption keys by an unauthorized person.

WPA's encryption method is *Temporal Key Integrity Protocol (TKIP).* TKIP addresses WEP's weaknesses with a re-keying mechanism, a per-packet mixing function, a message integrity check, and an extended initialization vector. WPA also provides strong user authentication based on 802.1x EAP. To configure WPA-TKIP encryption on the access point:

1. Select **Network Configuration** -> **Wireless** -> **Security** from the access point menu tree.

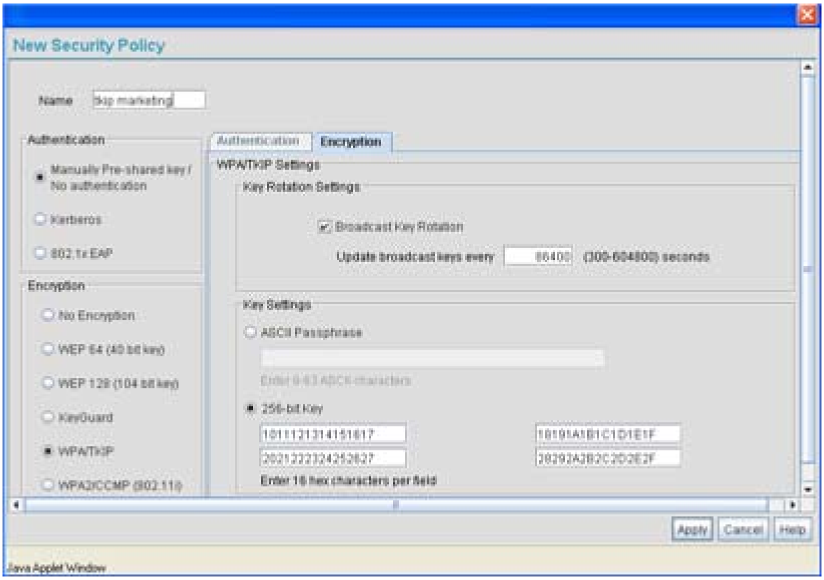
   If security policies supporting WPA-TKIP exist, they appear within the **Security Configuration** screen. These existing policies can be used as is, or their properties edited by clicking the **Edit** button. To configure a new security policy supporting WPA-TKIP, continue to step 2.
2. Click the **Create** button to configure a new policy supporting WPA-TKIP.

   The **New Security Policy** screen displays with no authentication or encryption options selected.

3. Select the **WPA/TKIP** radio button.

   The **WPA/TKIP Settings** field displays within the New Security Policy screen.

4. Ensure the **Name** of the security policy entered suits the intended configuration or function of the policy.



New Security Policy

Name: tkip marketing

Authentication
- ● Manually Pre-shared key / No authentication
- ○ Kerberos
- ○ 802.1x EAP

Encryption
- ○ No Encryption
- ○ WEP 64 (40 bit key)
- ○ WEP 128 (104 bit key)
- ○ KeyGuard
- ● WPA/TKIP
- ○ WPA2/CCMP (802.11i)

WPA/TKIP Settings

Key Rotation Settings

☑ Broadcast Key Rotation

Update broadcast keys every 86400 (300-604800) seconds

Key Settings

○ ASCII Passphrase

Enter 8-63 ASCII characters

● 256-bit Key

1011121314151617 18191A1B1C1D1E1F
2021222324252627 28292A2B2C2D2E2F

Enter 16 hex characters per field

5. Configure the **Key Rotation Settings** area as needed to broadcast encryption key changes to MUs and define the broadcast interval.

   Broadcast Key Rotation Select the **Broadcast Key Rotation** checkbox to enable or disable the broadcasting of encryption-key changes to MUs. Only broadcast key changes when required by associated MUs to reduce the transmissions of sensitive key information. This value is disabled by default.

   Update broadcast keys every (300-604800 seconds) Specify a time period in seconds for broadcasting encryption-key changes to MUs. Set key broadcasts to a shorter time interval (at least 30 seconds) for tighter security on the WLAN's wireless connections. Set key broadcasts to a longer time interval (at most, 80000 seconds) to extend the key times for wireless connections. Default is 86,400 seconds.

6. Configure the **Key Settings** area as needed to set an ASCII Passphrase and key values.

ASCII Passphrase To use an ASCII passphrase (and not a hexadecimal value), select the checkbox and enter an alphanumeric string of 8 to 63 characters. The alphanumeric string allows character spaces. The access point converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

256-bit Key To use a hexadecimal value (and not an ASCII passphrase), select the checkbox and enter 16 hexadecimal characters into each of the four fields displayed.

Default (hexadecimal) 256-bit keys for WPA/TKIP include:

1011121314151617

18191A1B1C1D1E1F

2021222324252627

28292A2B2C2D2E2F

7. Click the **Apply** button to save any changes made within the WPA/TKIP Settings field of the New Security Policy screen.
8. Click the **Cancel** button to undo any changes made within the WPA/TKIP Settings field and return to the **WLAN** screen. This reverts all settings to the last saved configuration.

6.9 Configuring WPA2-CCMP (802.11i)

WPA2 is a newer 802.11i standard that provides even stronger wireless security than Wi-Fi Protected Access (WPA) and WEP. CCMP is the security standard used by the *Advanced Encryption Standard (AES).* AES serves the same function TKIP does for WPA-TKIP. CCMP computes a *Message Integrity Check (MIC)* using the proven *Cipher Block Chaining (CBC)* technique. Changing just one bit in a message produces a totally different result.

WPA2/CCMP is based on the concept of a *Robust Security Network (RSN),* which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the keys the administrator provides are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The end result is an encryption scheme as secure as any the access point provides.

To configure WPA2-CCMP on the access point:

1. Select **Network Configuration** -> **Wireless** -> **Security** from the access point menu tree.

If security policies supporting WPA2-CCMP exist, they appear within the **Security Configuration** screen. These existing policies can be used as is, or their properties edited by clicking the **Edit** button. To configure a new security policy supporting WPA2-CCMP, continue to step 2.

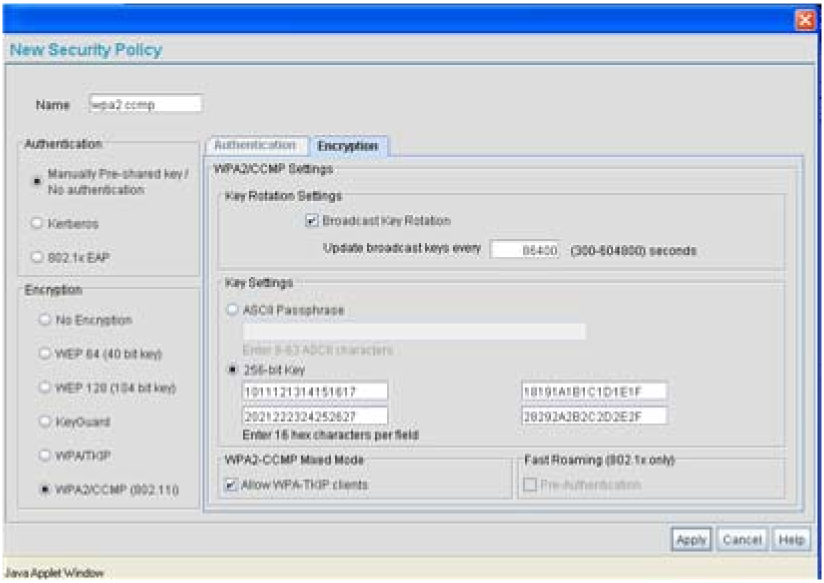
2. Click the **Create** button to configure a new policy supporting WPA2-CCMP.

   The **New Security Policy** screen displays with no authentication or encryption options selected.

3. Select the **WPA2/CCMP (802.11i)** checkbox.

   The **WPA2/CCMP Settings** field displays within the New Security Policy screen.

4. Ensure the **Name** of the security policy entered suits the intended configuration or function of the policy.



New Security Policy

Name: wpa2 ccmp

Authentication
- ● Manually Pre-shared key / No authentication
- ○ Kerberos
- ○ 802.1x EAP

Encryption
- ○ No Encryption
- ○ WEP 64 (40 bit key)
- ○ WEP 128 (104 bit key)
- ○ KeyGuard
- ○ WPA/TKIP
- ● WPA2/CCMP (802.11i)

WPA2/CCMP Settings

Key Rotation Settings
- ☑ Broadcast Key Rotation
- Update broadcast keys every 86400 (300-604800) seconds

Key Settings
- ○ ASCII Passphrase
- Enter 8-63 ASCII characters
- ● 256-bit Key
- 1011121314151617 18191A1B1C1D1E1F
- 2021222324252627 28292A2B2C2D2E2F
- Enter 16 hex characters per field

WPA2-CCMP Mixed Mode
- ☑ Allow WPA-TKIP clients

Fast Roaming (802.1x only)
- ☐ Pre-Authentication

5. Configure the **Key Rotation Settings** field as required to set Broadcast Key Rotation and the update interval.

Broadcast Key Rotation

Select the **Broadcast Key Rotation** checkbox to enable or disable the broadcasting of encryption key changes to MUs. Only broadcast key changes when required by associated MUs to reduce the transmissions of sensitive key information. This option is disabled by default.

Update broadcast keys every (300-604800 seconds)

Specify a time period in seconds for broadcasting encryption key changes to MUs. Set key broadcasts to a shorter interval (at least 30 seconds) for tighter security on the WLAN's wireless connections. Set key broadcasts to a longer interval to extend the key times for wireless connections. Default is 86,400 seconds.

6. Configure the **Key Settings** area as needed to set an ASCII Passphrase and 128-bit key.

ASCII Passphrase

To use an ASCII passphrase (and not a hexadecimal value), select the checkbox enter an alphanumeric string of 8 to 63 characters. The string allows character spaces. The access point converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

256-bit Key

To use a hexadecimal value (and not an ASCII passphrase), select the checkbox and enter 16 hexadecimal characters into each of the four fields displayed.

Default (hexadecimal) 256-bit keys for WP2A/CCMP include:

1011121314151617

18191A1B1C1D1E1F

2021222324252627

28292A2B2C2D2E2F

7. Configure the **WPA2-CCMP Mixed Mode** field as needed to allow TKIP and WPA2 client interoperation.

Allow WPA-TKIP clients

WPA2-CCMP Mixed Mode enables WPA2-CCMP and WPA-TKIP clients to operate together on the network. Enabling this option allows backwards compatibility for clients that support WPA-TKIP but do not support WPA2-CCMP. Symbol recommends enabling this feature if WPA-TKIP supported MUs operate within a WLAN populated by WPA2-CCMP enabled clients.

8. Configure the **Fast Roaming (802.1x only)** field as required to enable additional access point roaming and key caching options. This feature is applicable only when using 802.1x EAP authentication with WPA2/CCMP.

Pre-Authentication	Selecting this option enables an associated MU to carry out an 802.1x authentication with another access point before it roams to it. The access point caches the keying information of the client until it roams to the other access point. This enables the roaming client to start sending and receiving data sooner by not having to do 802.1x authentication after it roams. This feature is only supported when 802.1x EAP authentication is enabled.

9. Click the **Apply** button to save any changes made within the WPA2/CCMP Settings field of the New Security Policy screen.
10. Click the **Cancel** button to undo any changes made within the WPA2/CCMP Settings field and return to the **WLAN** screen. This reverts all settings to the last saved configuration.

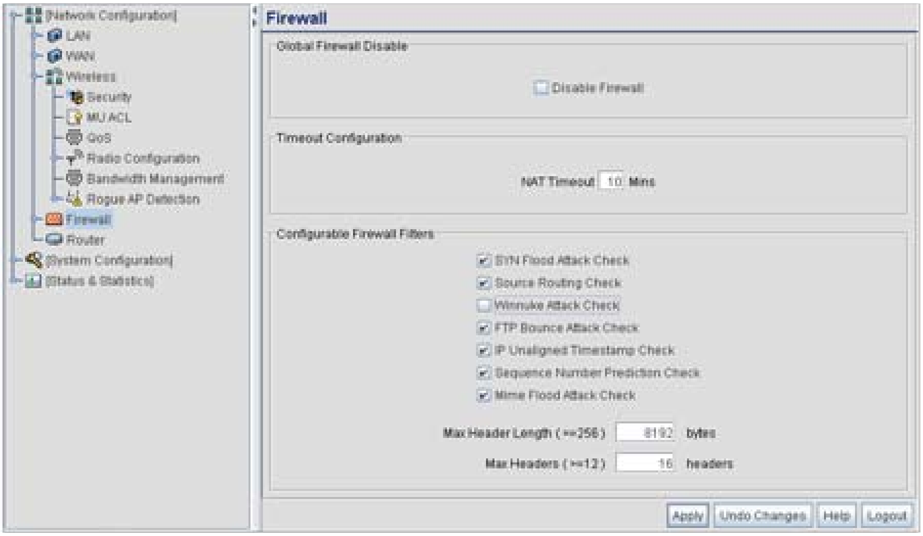
6.10 Configuring Firewall Settings

The access point's firewall is a set of related programs located in the gateway on the WAN side of the access point. The firewall uses a collection of filters to screen information packets for known types of system attacks. Some of the access point's filters are continuously enabled, others are configurable.

Use the access point’s **Firewall** screen to enable or disable the configurable firewall filters. Enable each filter for maximum security. Disable a filter if the corresponding attack does not seem a threat in order to reduce processor overhead. Use the WLAN Security screens (WEP, Kerberos etc.) as required for setting user authentication and data encryption parameters.

To configure the access point firewall settings:

1. Select **Network Configuration** -> **Firewall** from the access point menu tree.



Firewall

Global Firewall Disable

□ Disable Firewall

Timeout Configuration

NAT Timeout 10 Mins

Configurable Firewall Filters

☑ SYN Flood Attack Check
☑ Source Routing Check
□ Winnuke Attack Check
☑ FTP Bounce Attack Check
☑ IP Unaligned Timestamp Check
☑ Sequence Number Prediction Check
☑ Mime Flood Attack Check

Max Header Length (>=256) 8192 bytes

Max Headers (>=12) 16 headers

2. Refer to the **Global Firewall Disable** field to enable or disable the access point firewall.

Disable Firewall	Select the **Disable Firewall** checkbox to disable all firewall functions on the access point. This includes firewall filters, NAT, VPN, content filtering, and subnet access. Disabling the access point firewall makes the access point vulnerable to data attacks and is not recommended during normal operation if using the WAN port.

3. Refer to the **Timeout Configuration** field to define a timeout interval to terminate IP address translations.

NAT Timeout	*Network Address Translation (NAT)* converts an IP address in one network to a different IP address or set of IP addresses in a different network. Set a **NAT Timeout** interval (in minutes) the access point uses to terminate the IP address translation process if no translation activity is detected after the specified interval.

4. Refer to the **Configurable Firewall Filters** field to set the following firewall filters:

SYN Flood Attack Check	A SYN flood attack requests a connection and then fails to promptly acknowledge a destination host's response, leaving the destination host vulnerable to a flood of connection requests.

Source Routing Check A source routing attack specifies an exact route for a packet's travel through a network, while exploiting the use of an intermediate host to gain access to a private host.

Winnuke Attack Check A "Win-nuking" attack uses the IP address of a destination host to send junk packets to its receiving port.

FTP Bounce Attack Check An FTP bounce attack uses the PORT command in FTP mode to gain access to arbitrary ports on machines other than the originating client.

IP Unaligned Timestamp Check An IP unaligned timestamp attack uses a frame with the IP timestamp option, where the timestamp is not aligned on a 32-bit boundary.

Sequence Number Prediction Check A sequence number prediction attack establishes a three-way TCP connection with a forged source address. The attacker guesses the sequence number of the destination host response.

Mime Flood Attack Check A MIME flood attack uses an improperly formatted MIME header in "sendmail" to cause a buffer overflow on the destination host.

Max Header Length Use the **Max Header Length** field to set the maximum allowable header length (at least 256 bytes).

Max Headers Use the **Max Headers** field to set the maximum number of headers allowed (at least 12 headers).

5. Click **Apply** to save any changes to the Firewall screen. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.
6. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Firewall screen to the last saved configuration.
7. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

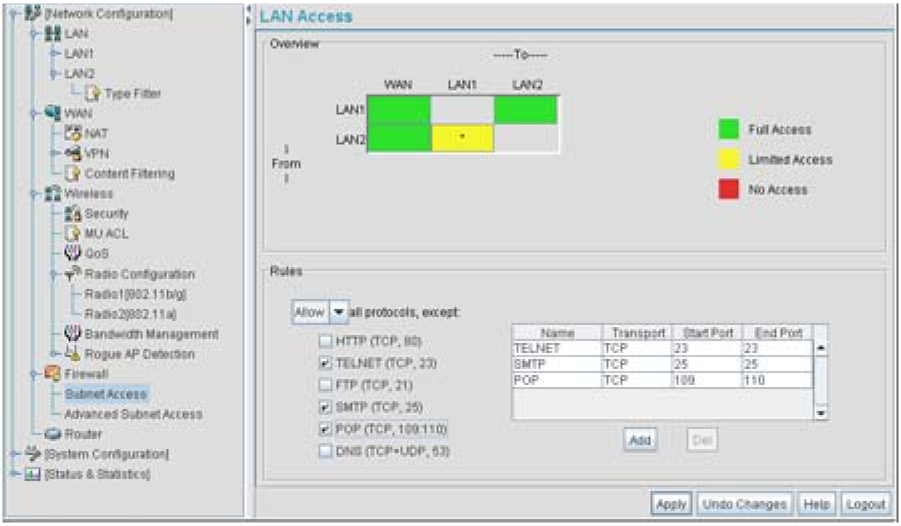
6.10.1 Configuring LAN to WAN Access

The access point LAN can be configured to communicate with the WAN side of the access point. Use the **Subnet Access** screen to allow/deny access to the access point WAN protocols, specify names and properties for existing protocols and enable pre-configured protocols (FTP, TFTP, Telnet ect.).

To configure access point subnet access:

1. Select **Network Configuration** -> **Firewall** -> **Subnet Access** from the access point menu tree.
2. Refer to the Overview table to view rectangles representing subnet associations. The three possible colors indicate the current access level, as defined, for each subnet association.

Color	Access Type	Description
Green	Full Access	No protocol exceptions (rules) are specified. All traffic may pass between these two areas.
Yellow	Limited Access	One or more protocol rules are specified. Specific protocols are either enabled or disabled between these two areas. Click the table cell of interest and look at the exceptions area in the lower half of the screen to determine the protocols that are either allowed or denied.
Red	No Access	All protocols are denied, without exception. No traffic will pass between these two areas.



----To----

From	WAN	LAN1	LAN2
LAN1	🟩		🟩
LAN2	🟩	🟨 *	

🟩 Full Access
🟨 Limited Access
🟥 No Access

Allow ▾ all protocols, except:

☐ HTTP (TCP, 80)
☑ TELNET (TCP, 23)
☐ FTP (TCP, 21)
☑ SMTP (TCP, 25)
☑ POP (TCP, 109:110)
☐ DNS (TCP+UDP, 53)

Name	Transport	Start Port	End Port
TELNET	TCP	23	23
SMTP	TCP	25	25
POP	TCP	109	110

3. Configure the **Rules** field as required to allow or deny access to selected (enabled) protocols.

Allow or Deny all protocols, except

Use the drop-down menu to select either **Allow** or **Deny.** The selected setting applies to all protocols except those with enabled checkboxes and any traffic that is added to the table. For example, if the adoption rule is to Deny access to all protocols except those listed, access is allowed only to those selected protocols.

Pre configured Rules

The following protocols are preconfigured with the access point. To enable a protocol, check the box next to the protocol name.

- **HTTP** - *Hypertext Transfer Protocol* is the protocol for transferring files on the Web. HTTP is an application protocol running on top of the TCP/IP suite of protocols, the foundation protocols for the Internet. The HTTP protocol uses TCP port 80.
- **TELNET** - TELNET is the terminal emulation protocol of TCP/IP. TELNET uses TCP to achieve a virtual connection between server and client, then negotiates options on both sides of the connection. TELNET uses TCP port 23.
- **FTP** - *File Transfer Protocol (FTP)* is an application protocol using the Internet's TCP/IP protocols. FTP provides an efficient way to exchange files between computers on the Internet. FTP uses TCP port 21.
- **SMTP** - *Simple Mail Transfer Protocol* is a TCP/IP protocol for sending and receiving email. Due to its limited ability to queue messages at the receiving end, SMTP is often used with POP3 or IMAP. SMTP sends the email, and POP3 or IMAP receives the email. SMTP uses TCP port 25.
- **POP** - *Post Office Protocol* is a TCP/IP protocol intended to permit a workstation to dynamically access a maildrop on a server host. A workstation uses POP3 to retrieve email that the server is holding for it.
- **DNS** - *Domain Name Service* protocol searches for resources using a database distributed among different name servers.

Add

Click **Add** to create a new table entry.

Del (Delete)

Click **Del** *(Delete)* to remove a selected list entry.

Name

Specify a name for a newly configured protocol.

Transport — Select a protocol from the drop-down menu. For a detailed description of the protocols available, see *Available Protocols on page 6-30*.

Start Port — Enter the starting port number for a range of ports. If the protocol uses a single port, enter that port in this field.

End Port — Enter the ending port number for a port range. If the protocol uses a single port, leave the field blank. A new entry might use *Web Traffic* for its name, *TCP* for its protocol, and *80* for its port number.

4. Click **Apply** to save any changes to the Subnet Access screen. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.
5. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Subnet Access screen to the last saved configuration.
6. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

6.10.1.1 Available Protocols

Protocols that are not pre-configured can be specified using the drop down list within the **Transport** column within the Subnet Access and Advanced Subnet Access screens. They include:

- **ALL** - Enables all of the protocol options displayed in the drop-down menu (as described below).
- **TCP** - *Transmission Control Protocol* is a set of rules for sending data as message units over the Internet. TCP manages individual data packets. Messages are divided into packets for efficient routing through the Internet.
- **UDP** - *User Datagram Protocol* is used for broadcasting data over the Internet. Like TCP, UDP runs on top of Internet Protocol (IP) networks. Unlike TCP/IP, UDP/IP provides few error recovery services. UDP offers a way to directly connect, and then send and receive datagrams over an IP network.
- **ICMP** - *Internet Control Message Protocol* is tightly integrated with IP. ICMP messages are used for out-of-band messages related to network operation. ICMP packet delivery is unreliable. Hosts cannot count on receiving ICMP packets for a network problem.
- **AH** - Authentication Header is one of the two key components of IP Security Protocol (IPsec). The other key component is *Encapsulating Security Protocol (ESP).*

  AH provides authentication, proving the packet sender really is the sender, and the data really is the data sent. AH can be used in transport mode, providing security between two end points. Also, AH can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).

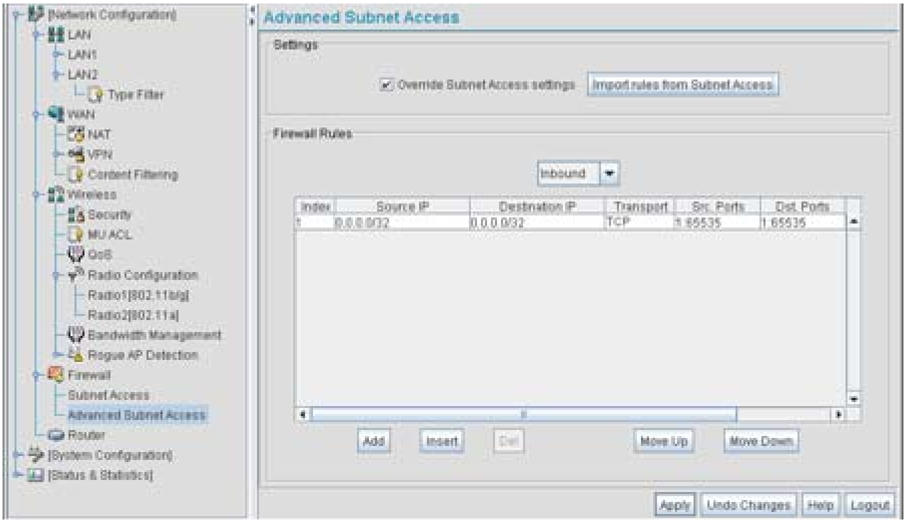
- **ESP** - *Encapsulating Security Protocol* is one of two key components of IP Security Protocol (IPsec). The other key component is Authentication Header (AH). ESP encrypts the packets and provides authentication services. ESP can be used in transport mode, providing security between two end points. ESP can also be used in tunnel mode, providing security like that of a *Virtual Private Network (VPN).*
- **GRE -** *General Routing Encapsulation* supports VPNs across the Internet. GRE is a mechanism for encapsulating network layer protocols over any other network layer protocol. Such encapsulation allows routing of IP packets between private IP networks across an Internet using globally assigned IP addresses.

6.10.2 Configuring Advanced Subnet Access

Use the **Advanced Subnet Access** screen to configure complex access rules and filtering based on source port, destination port, and transport protocol. To enable advanced subnet access, the subnet access rules must be overridden. However, the Advanced Subnet Access screen allows you to import existing subnet access rules into the advanced subnet access rules.

To configure access point Advanced Subnet Access:

1. Select **Network Configuration** -> **Firewall** -> **Advanced Subnet Access** from the access point menu tree.



Advanced Subnet Access

Settings

☑ Override Subnet Access settings

Firewall Rules

Inbound

Index	Source IP	Destination IP	Transport	Src. Ports	Dst. Ports
1	0.0.0.0/32	0.0.0.0/32	TCP	1:65535	1:65535

2. Configure the **Settings** field as needed to override the settings in the Subnet Access screen and import firewall rules into the Advanced Subnet Access screen.

    Override Subnet Access settings — Select this checkbox to enable advanced subnet access rules and disable existing subnet access rules, port forwarding, and 1 to many mappings from the system. Only enable advanced subnet access rules if your configuration requires rules that cannot be configured within the **Subnet Access** screen.

    Import rules from Subnet Access — Select this checkbox to import existing access rules (NAT, packet forwarding, VPN rules etc.) into the **Firewall Rules** field. This rule import overrides any existing rules configured in the Advanced Subnet Access screen. A warning box displays stating the operation cannot be undone.

3. Configure the **Firewall Rules** field as required add, insert or delete firewall rules into the list of advanced rules.

    Inbound or Outbound — Select **Inbound** or **Outbound** from the drop-down menu to specify if a firewall rule is intended for inbound traffic to an interface or outbound traffic from that interface.

    Add — Click the **Add** button to insert a new rule at the bottom of the table. Click on a row to display a new window with configuration options for that field.

    Insert — Click the **Insert** button to insert a new rule directly above a selected rule in the table. Clicking on a field in the row displays a new window with configuration options.

    Del (Delete) — Click **Del** to remove the selected rule from the table. The index numbers for all the rows below the deleted row decrease by 1.

    Move Up — Clicking the **Move Up** button moves the selected rule up by one row in the table. The index numbers for the affected rows adjust to reflect the new order.

    Move Down — Clicking the **Move Down** button moves the selected rule down by one row in the table. The index numbers for the affected rows adjust to reflect the new order.

    Index — The index number determines the order firewall rules are executed. Rules are executed from the lowest number to the highest number.

Source IP The **Source IP** range defines the origin address or address range for the firewall rule. To configure the Source IP range, click on the field. A new window displays for entering the IP address and range.

Destination IP The **Destination IP** range determines the target address or address range for the firewall rule. To configure the Destination IP range, click on the field. A new window displays for entering the IP address and range.

Transport Select a protocol from the drop-down list. For a detailed description of the protocols available, see *Available Protocols on page 6-30*.

Src. Ports (Source Ports) The source port range determines which ports the firewall rule applies to on the source IP address. Click on the field to configure the source port range. A new window displays to enter the starting and ending port ranges. For rules where only a single port is necessary, enter the same port in the start and end port fields.

Dst. Ports (Destination Ports The destination port range determines which ports the firewall rule applies to on the destination IP address. Click on the field to configure the destination port range. A new window displays to enter the starting and ending ports in the range. For rules where only a single port is necessary, enter the same port in the start and end port fields.

4. Click **Apply** to save any changes to the Advanced Subnet Access screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.
5. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Advanced Subnet Access screen to the last saved configuration.
6. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

6.11 Configuring VPN Tunnels

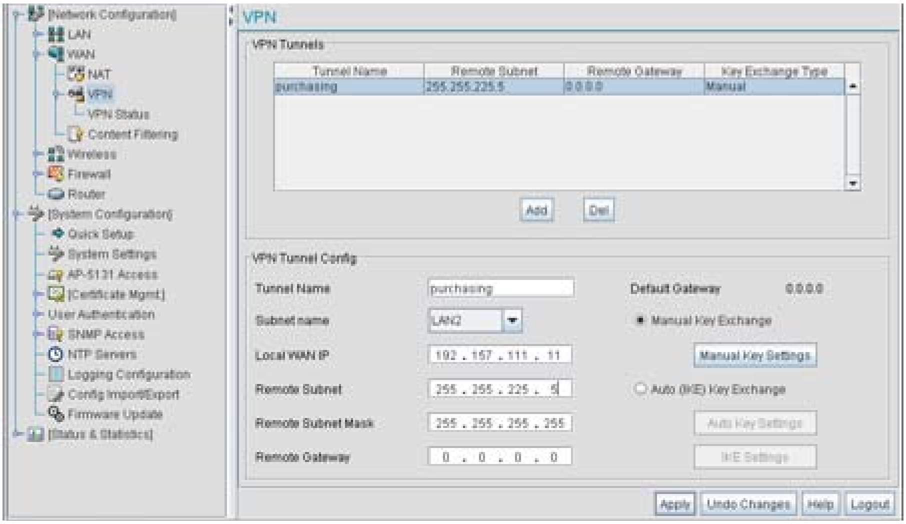
The access point allows up to 25 VPN tunnels to either a VPN endpoint or to another access point. VPN tunnels allow all traffic on a local subnet to route securely through a IPSEC tunnel to a private network. A VPN port is a virtual port which handles tunneled traffic.

When connecting to another site using a VPN, the traffic is encrypted so if anyone intercepts the traffic, they cannot see what it is unless they can break the encryption. The traffic is encrypted from your computer through the network to the VPN. At that point the traffic is decrypted.

Use the **VPN** screen to add and remove VPN tunnels. To configure an existing VPN tunnel, select it from the list in the **VPN Tunnels** field. The selected tunnel's configuration displays in a **VPN Tunnel Config** field.

To configure a VPN tunnel on the access point:

1. Select **Network Configuration** -> **WAN** -> **VPN** from the access point menu tree.



VPN Tunnels

Tunnel Name	Remote Subnet	Remote Gateway	Key Exchange Type
purchasing	255.255.225.5	0.0.0.0	Manual

VPN Tunnel Config

Tunnel Name: purchasing

Subnet name: LAN2

Local WAN IP: 192 . 157 . 111 . 11

Remote Subnet: 255 . 255 . 225 . 5

Remote Subnet Mask: 255 . 255 . 255 . 255

Remote Gateway: 0 . 0 . 0 . 0

Default Gateway: 0.0.0.0

● Manual Key Exchange

○ Auto (IKE) Key Exchange

2. Use the **VPN Tunnels** field to add or delete a tunnel to the list of available tunnels, list tunnel network address information and display key exchange information for each tunnel.

Add	Click **Add** to add a VPN tunnel to the list. To configure a specific tunnel, select it from the list and use the parameters within the **VPN Tunnel Config** field to set its properties.
Del	Click **Del** to delete a highlighted VPN tunnel. There is no confirmation before deleting the tunnel.
Tunnel Name	The **Tunnel Name** column lists the name of each VPN tunnel on the access point.
Remote Subnet	The **Remote Subnet** column lists the remote subnet for each tunnel. The remote subnet is the subnet the remote network uses for connection.

Remote Gateway The **Remote Gateway** column lists a remote gateway IP address for each tunnel. The numeric remote gateway is the gateway IP address on the remote network the VPN tunnel connects to. Ensure the address is the same as the WAN port address of the target gateway AP or switch.

Key Exchange Type The **Key Exchange Type** column lists the key exchange type for passing keys between both ends of a VPN tunnel. If *Manual Key Exchange* is selected, this column displays Manual. If *Auto (IKE) Key Exchange* is selected, the field displays **Automatic**.

✓ **NOTE** When creating a tunnel, the remote subnet and remote subnet mask must be that of the target device's LAN settings. The remote gateway must be that of the target device's WAN IP address.

If access point #1 has the following values:

- WAN IP address: 20.1.1.2
- LAN IP address: 10.1.1.1
- Subnet Mask: 255.0.0.0

Then, the VPN values for access point #2 should be:

- Remote subnet: 10.1.1.0 or 10.0.0.0
- Remote subnet mask: 255.0.0.0
- Remote gateway: 20.1.1.2

3. If a VPN tunnel has been added to the list of available access point tunnels, use the **VPN Tunnel Config** field to optionally modify the tunnel's properties.

Tunnel Name Enter a name to define the VPN tunnel. The tunnel name is used to uniquely identify each tunnel. Select a name best suited to that tunnel's function so it can be selected again in the future if required in a similar application.

Subnet name Use the drop-down menu to specify the LAN1 or LAN2 connection used for routing VPN traffic. Remember, only one LAN connection can be active on the access point Ethernet port at a time. The LAN connection specified from the LAN screen to receive priority for Ethernet port connectivity may be the better subnet to select for VPN traffic.

Local WAN IP Enter the WAN’s numerical (non-DNS) IP address in order for the tunnel to pass traffic to a remote network.

Remote Subnet Specify the numerical (non-DNS) IP address for the Remote Subnet.

Remote Subnet Mask Enter the subnet mask for the tunnel’s remote network for the tunnel. The remote subnet mask is the subnet setting for the remote network the tunnel connects to.

Remote Gateway Enter a numerical (non-DNS) remote gateway IP address for the tunnel. The remote gateway IP address is the gateway address on the remote network the VPN tunnel connects to.

Default Gateway Displays the WAN interface's default gateway IP address.

Manual Key Exchange Selecting **Manual Key Exchange** requires you to manually enter keys for AH and/or ESP encryption and authentication. Click the **Manual Key Settings** button to configure the settings.

Manual Key Settings Select **Manual Key Exchange** and click the **Manual Key Settings** button to open a screen where AH authentication and ESP encryption/authentication can be configured and keys entered. For more information, see *Configuring Manual Key Settings on page 6-37*.

Auto (IKE) Key Exchange Select the Auto (IKE) Key Exchange checkbox to configure AH and/or ESP without having to manually enter keys. The keys automatically generate and rotate for the authentication and encryption type selected.

Auto Key Settings Select the Auto (IKE) Key Exchange checkbox, and click the **Auto Key Settings** button to open a screen where AH authentication and ESP encryption/authentication can be configured. For more information, see *Configuring Auto Key Settings on page 6-41*.

IKE Settings After selecting Auto (IKE) Key Exchange, click the **IKE Settings** button to open a screen where IKE specific settings can be configured. For more information, see *Configuring IKE Key Settings on page 6-43*.

4. Click **Apply** to save any changes to the **VPN** screen as well as changes made to the Auto Key Settings, IKE Settings and Manual Key Settings screens. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.

5. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the VPN, Auto Key Settings, IKE Settings and Manual Key Settings screens to the last saved configuration.
6. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

6.11.1 Configuring Manual Key Settings

A transform set is a combination of security protocols and algorithms applied to IPSec protected traffic. During *security association (SA)* negotiation, both gateways agree to use a particular transform set to protect data flow.

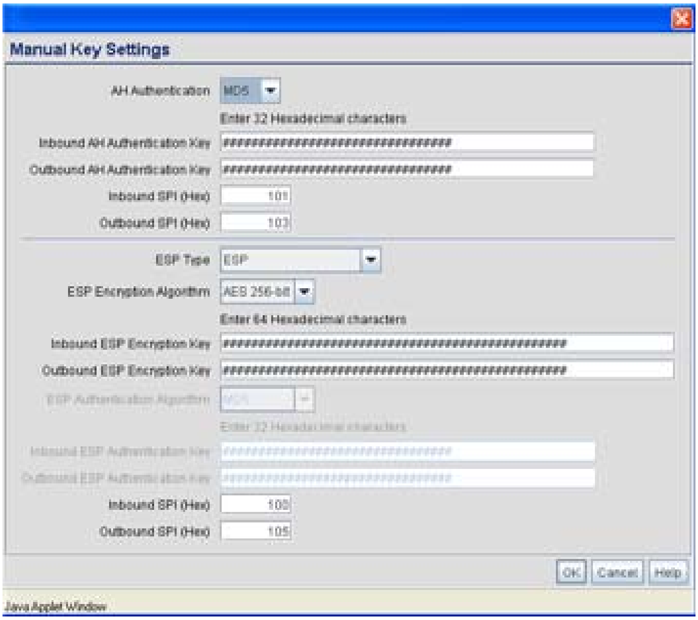
A transform set specifies one or two IPSec security protocols (either AH, ESP, or both) and specifies the algorithms to use for the selected security protocol. If you specify an ESP protocol in a transform set, specify just an ESP encryption transform or both an ESP encryption transform and an ESP authentication transform.

When the particular transform set is used during negotiations for IPSec SAs, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote end of the gateway.

Use the **Manual Key Settings** screen to specify the transform sets used for VPN access.

To configure manual key settings for the access point:

1. Select **Network Configuration** -> **WAN** -> **VPN** from the access point menu tree.
2. Refer to the **VPN Tunnel Config** field, select the **Manual Key Exchange** radio button and click the **Manual Key Settings** button.



Manual Key Settings

AH Authentication: MD5

Enter 32 Hexadecimal characters

Inbound AH Authentication Key: ################################

Outbound AH Authentication Key: ################################

Inbound SPI (Hex): 101

Outbound SPI (Hex): 103

ESP Type: ESP

ESP Encryption Algorithm: AES 256-bit

Enter 64 Hexadecimal characters

Inbound ESP Encryption Key: ##

Outbound ESP Encryption Key: ##

ESP Authentication Algorithm: MD5

Enter 32 Hexadecimal characters

Inbound ESP Authentication Key: ################################

Outbound ESP Authentication Key: ################################

Inbound SPI (Hex): 100

Outbound SPI (Hex): 105

3. Configure the **Manual Key Settings** screen to modify the following:

☑ **NOTE** When entering Inbound or Outbound encryption or authentication keys, an error message could display stating the keys provided are "weak". Some WEP attack tools invoke a dictionary to hack WEP keys based on commonly used words. To avoid entering a weak key, try to not to produce a WEP key using commonly used terms and attempt to mix alphabetic and numerical key attributes when possible.

AH Authentication AH provides data authentication and anti-replay services for the VPN tunnel. Select the required authentication method from the drop-down menu:

- None - Disables AH authentication. The rest of the fields are not active.
- MD5 - Enables the Message Digest 5 algorithm requiring 128-bit (32-character hexadecimal) keys.
- SHA1 - Enables Secure Hash Algorithm 1, requiring 160-bit (40-character hexadecimal) keys.

Inbound AH Authentication Key

Configure a key for computing the integrity check on inbound traffic with the selected authentication algorithm. The key must be 32/40 (for MD5/SHA1) hexadecimal (0-9, A-F) characters in length. The key value must match the corresponding outbound key on the remote security gateway.

Outbound AH Authentication Key

Configure a key for computing the integrity check on outbound traffic with the selected authentication algorithm. The key must be 32/40 (for MD5/SHA1) hexadecimal (0-9, A-F) characters in length. The key value must match the corresponding inbound key on the remote security gateway.

Inbound SPI (Hex)

Enter an up to six-character hexadecimal value to identify the inbound security association created by the AH algorithm. The value must match the corresponding outbound SPI value configured on the remote security gateway.

Outbound SPI (Hex)

Provide an up to six-character hexadecimal value to identify the outbound security association created by the AH algorithm. The value must match the corresponding inbound SPI value configured on the remote security gateway.

ESP Type

ESP provides packet encryption, optional data authentication and anti-replay services for the VPN tunnel. Use the drop-down menu to select the ESP type. Options include:

- None - Disables ESP. The rest of the fields are not be active.
- ESP - Enables ESP for the tunnel.
- ESP with Authentication - Enables ESP with authentication.

ESP Encryption Algorithm

Select the encryption and authentication algorithms for the VPN tunnel using the drop-down menu.

- DES - Uses the DES encryption algorithm requiring 64-bit (16-character hexadecimal) keys.
- 3DES - Uses the 3DES encryption algorithm requiring 192-bit (48-character hexadecimal) keys.
- AES 128-bit: - Uses the Advanced Encryption Standard algorithm with 128-bit (32-character hexadecimal) keys.
- AES 192-bit: - Uses the Advanced Encryption Standard algorithm with 192-bit (48-character hexadecimal) keys.
- AES 256-bit: - Uses the Advanced Encryption Standard algorithm with 256-bit (64-character hexadecimal) keys.

Inbound ESP Encryption Key
Enter a key for inbound traffic. The length of the key is determined by the selected encryption algorithm. The key must match the outbound key at the remote gateway.

Outbound ESP Encryption Key
Define a key for outbound traffic. The length of the key is determined by the selected encryption algorithm. The key must match the inbound key at the remote gateway.

ESP Authentication Algorithm
Select the authentication algorithm to use with ESP. This option is available only when **ESP with Authentication** was selected for the ESP type. Options include:

- MD5 - Enables the Message Digest 5 algorithm, which requires 128-bit (32-character hexadecimal) keys.
- SHA1 - Enables Secure Hash Algorithm 1, which requires 160-bit (40-character hexadecimal) keys.

Inbound ESP Authentication Key
Define a key for computing the integrity check on the inbound traffic with the selected authentication algorithm. The key must be 32/40 (for MD5/SHA1) hexadecimal (0-9, A-F) characters in length. The key must match the corresponding outbound key on the remote security gateway.

Outbound ESP Authentication Key
Enter a key for computing the integrity check on outbound traffic with the selected authentication algorithm. The key must be 32/40 (for MD5/SHA1) hexadecimal (0-9, A-F) characters in length. The key must match the corresponding inbound key on the remote security gateway.

Inbound SPI (Hex)
Define an up to six-character (maximum) hexadecimal value to identify the inbound security association created by the encryption algorithm. The value must match the corresponding outbound SPI value configured on the remote security gateway.

Outbound SPI (Hex)
Enter an up to six (maximum) hexadecimal value to identify the outbound security association created by the encryption algorithm. The value must match the corresponding inbound SPI value configured on the remote security gateway.

The Inbound and Outbound SPI settings are required to be interpolated to function correctly. For example:

AP1 Inbound SPI = 800

AP1 Outbound SPI = 801

AP2 Inbound SPI = 801

AP2 Outbound SPI = 800

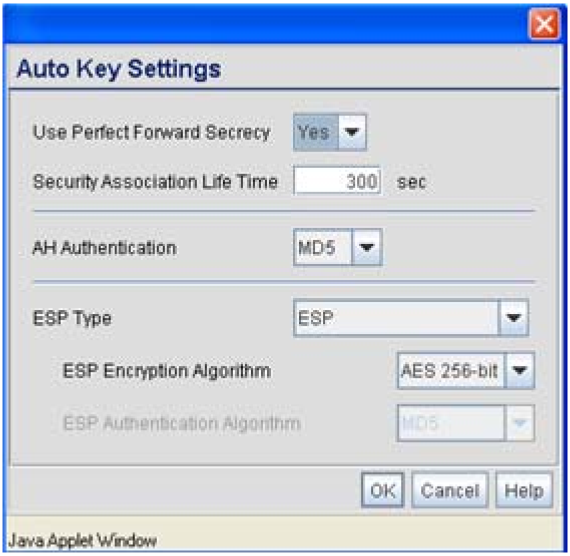
4. Click **Ok** to return to the VPN screen. Click Apply to retain the settings made on the **Manual Key Settings** screen.
5. Click **Cancel** to return to the VPN screen without retaining the changes made to the **Manual Key Settings** screen.

6.11.2 Configuring Auto Key Settings

The access point’s Network Management System can automatically set encryption and authentication keys for VPN access. Use the **Auto Key Settings** screen to specify the type of encryption and authentication, without specifying the keys. To manually specify keys, cancel out of the **Auto Key Settings** screen, select the **Manual Key Exchange** radio button, and set the keys within the **Manual Key Setting** screen.

To configure auto key settings for the access point:

1. Select **Network Configuration** -> **WAN** -> **VPN** from the access point menu tree.
2. Refer to the **VPN Tunnel Config** field, select the **Auto (IKE) Key Exchange** radio button and click the **Auto Key Settings** button.



Auto Key Settings

Use Perfect Forward Secrecy: Yes

Security Association Life Time: 300 sec

AH Authentication: MD5

ESP Type: ESP

ESP Encryption Algorithm: AES 256-bit

ESP Authentication Algorithm: MD5

3. Configure the **Auto Key Settings** screen to modify the following:

Use Perfect Forward Secrecy — Forward secrecy is a key-establishment protocol guaranteeing the discovery of a session key or long-term private key does not compromise the keys of other sessions. Select **Yes** to enable Perfect Forward Secrecy. Select **No** to disable Perfect Forward Secrecy.

Security Association Life Time — The Security Association Life Time is the configurable interval used to timeout association requests that exceed the defined interval. The available range is from 300 to 65535 seconds. The default is 300 seconds.

AH Authentication — AH provides data authentication and anti-replay services for the VPN tunnel. Select the desired authentication method from the drop-down menu.

- None - Disables AH authentication. No keys are required to be manually provided.
- MD5 - Enables the Message Digest 5 algorithm. No keys are required to be manually provided.
- SHA1 - Enables Secure Hash Algorithm 1. No keys are required to be manually provided.

ESP Type — ESP provides packet encryption, optional data authentication and anti-replay services for the VPN tunnel. Use the drop-down menu to select the ESP type.

- None - Disables ESP. The rest of the fields are not active.
- ESP - Enables ESP for this tunnel.
- ESP with Authentication - Enables ESP with authentication.

ESP Encryption Algorithm

Use this menu to select the encryption and authentication algorithms for this VPN tunnel.

- DES - Selects the DES algorithm.No keys are required to be manually provided.
- 3DES - Selects the 3DES algorithm. No keys are required to be manually provided.
- AES 128-bit: - Selects the Advanced Encryption Standard algorithm with 128-bit. No keys are required to be manually provided.
- AES 192-bit: - Selects the Advanced Encryption Standard algorithm with 192-bit. No keys are required to be manually provided.
- AES 256-bit: - Selects the Advanced Encryption Standard algorithm with 256-bit. No keys are required to be manually provided.

ESP Authentication Algorithm

Use this menu to select the authentication algorithm to be used with ESP. This menu is only active when ESP with Authentication was selected for the ESP type.

- MD5 - Enables the Message Digest 5 algorithm requiring 128-bit. No keys are required to be manually provided.
- SHA1 - Enables Secure Hash Algorithm. No keys are required to be manually provided.

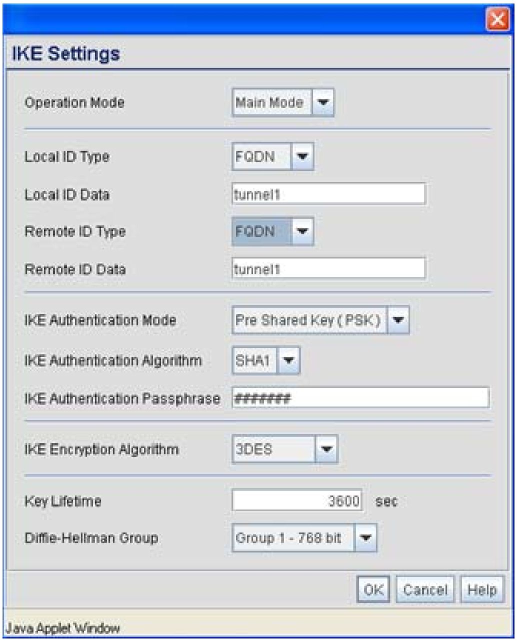
4. Click **Ok** to return to the VPN screen. Click Apply to retain the settings made on the **Auto Key Settings** screen.
5. Click **Cancel** to return to the VPN screen without retaining the changes made to this screen.

6.11.3 Configuring IKE Key Settings

The *Internet Key Exchange (IKE)* is an IPsec standard protocol used to ensure security for VPN negotiation and remote host or network access. IKE provides an automatic means of negotiation and authentication for communication between two or more parties. In essence, IKE manages IPSec keys automatically for the parties.

To configure IKE key settings for the access point:

1. Select **Network Configuration** -> **WAN** -> **VPN** from the access point menu tree.
2. Refer to the **VPN Tunnel Config** field, select the **Auto (IKE) Key Exchange** radio button and click the **IKE Settings** button.



IKE Settings

Operation Mode: Main Mode

Local ID Type: FQDN

Local ID Data: tunnel1

Remote ID Type: FQDN

Remote ID Data: tunnel1

IKE Authentication Mode: Pre Shared Key (PSK)

IKE Authentication Algorithm: SHA1

IKE Authentication Passphrase: #######

IKE Encryption Algorithm: 3DES

Key Lifetime: 3600 sec

Diffie-Hellman Group: Group 1 - 768 bit

3. Configure the **IKE Key Settings** screen to modify the following:

Operation Mode	The Phase I protocols of IKE are based on the ISAKMP identity-protection and aggressive exchanges. IKE main mode refers to the identity-protection exchange, and IKE aggressive mode refers to the aggressive exchange. • Main - Standard IKE mode for communication and key exchange. • Aggressive - Aggressive mode is faster, but less secure than Main mode. Identities are not encrypted unless public key encryption is used. The authentication method cannot be negotiated if the initiator chooses public key encryption

Local ID Type

Select the type of ID to be used for the access point end of the SA.

- IP - Select IP if the local ID type is the IP address specified as part of the tunnel.
- FQDN - Use FQDN if the local ID is a fully qualified domain name (such as sj.symbol.com).
- UFQDN - Select UFQDN if the local ID is a user fully-qualified email (such as johndoe@symbol.com).

Local ID Data

Specify the FQDN or UFQDN based on the Local ID type assigned.

Remote ID Type

Select the type of ID to be used for the access point end of the tunnel from the **Remote ID Type** drop-down menu.

- IP - Select the IP option if the remote ID type is the IP address specified as part of the tunnel.
- FQDN - Select FQDN if the remote ID type is a fully qualified domain name (such as sj.symbol.com). The setting for this field does not have to be fully qualified, however it must match the setting for the Certificate Authority.
- UFQDN - Select this item if the remote ID type is a user unqualified email address (such as johndoe@symbol.com). The setting for this field does not have to be unqualified, it just must match the setting of the field of the Certificate Authority.

Remote ID Data

If FQDN or UFQDN is selected, specify the data (either the qualified domain name or the user name) in the **Remote ID Data** field.

IKE Authentication Mode

Select the appropriate IKE authentication mode:

- Pre-Shared Key (PSK) - Specify an authenticating algorithm and passcode used during authentication.
- RSA Certificates - Select this option to use RSA certificates for authentication purposes. See the CA Certificates and Self certificates screens to create and import certificates into the system.

IKE Authentication Algorithm

IKE provides data authentication and anti-replay services for the VPN tunnel. Select an authentication methods from the drop-down menu.

- MD5 - Enables the Message Digest 5 algorithm. No keys are required to be manually provided.
- SHA1 - Enables Secure Hash Algorithm. No keys are required to be manually provided.

IKE Authentication Passphrase

If you selected **Pre-Shared Key** as the authentication mode, you must provide a passphrase.

IKE Encryption Algorithm

Select the encryption and authentication algorithms for the VPN tunnel from the drop-down menu.

- DES - Uses the DES encryption algorithm. No keys are required to be manually provided.
- 3DES - Enables the 3DES encryption algorithm. No keys are required to be manually provided.
- AES 128-bit - Uses the Advanced Encryption Standard algorithm with 128-bit. No keys are required to be manually provided.
- AES 192-bit - Enables the Advanced Encryption Standard algorithm with 192-bit. No keys are required to be manually provided.
- AES 256-bit - Uses the Advanced Encryption Standard algorithm with 256-bit. No keys are required to be manually provided.

Key Lifetime

The number of seconds the key is valid. At the end of the lifetime, the key is renegotiated.

The access point forces renegotiation every 3600 seconds. There is no way to change the renegotiation value. If the IKE Lifetime is greater than 3600, the keys still get renegotiated every 3600 seconds.

Diffie Hellman Group Select a **Diffie-Hellman Group** to use. The Diffie-Hellman key agreement protocol allows two users to exchange a secret key over an insecure medium without any prior secrets. Two algorithms exist, 768-bit and 1024-bit. Select one of the following options:

- Group 1 - 768 bit - Somewhat faster than the 1024-bit algorithm, but secure enough in most situations.
- Group 2 - 1024 bit - Somewhat slower than the 768-bit algorithm, but much more secure and a better choice for extremely sensitive situations.

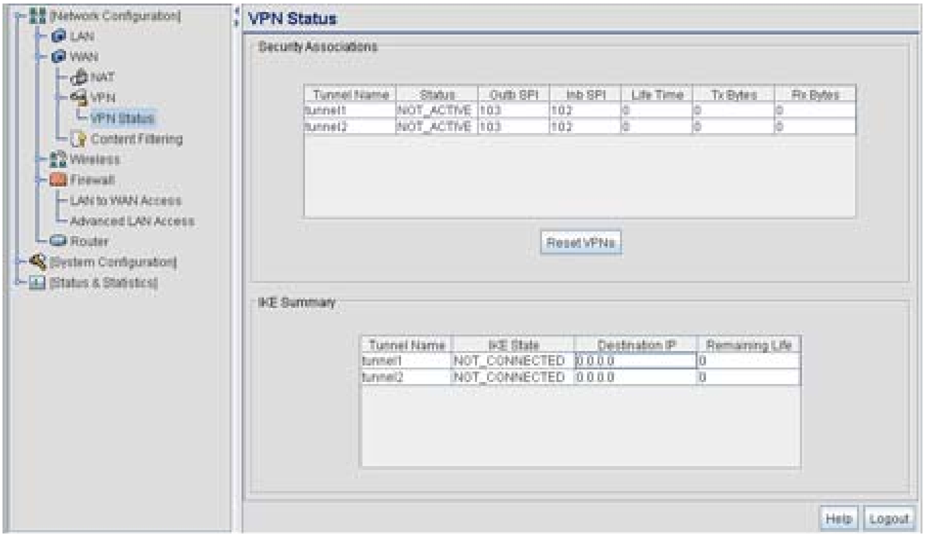
4. Click **Ok** to return to the VPN screen. Click Apply to retain the settings made on the **IKE Settings** screen.
5. Click **Cancel** to return to the VPN screen without retaining the changes made to the **IKE Settings** screen.

6.11.4 Viewing VPN Status

Use the **VPN Status** screen to display the status of the tunnels configured on the access point as well as their lifetime, transmit and receive statistics. The VPN Status screen is read-only with no configurable parameters. To configure a VPN tunnel, use the *VPN* configuration screen in the WAN section of the access point menu tree.

To view VPN status on the access point:

1. Select **Network Configuration** -> **WAN** -> **VPN** -> **VPN Status** from the access point menu tree.



VPN Status

Security Associations

Tunnel Name	Status	Outb SPI	Inb SPI	Life Time	Tx Bytes	Rx Bytes
tunnel1	NOT_ACTIVE	103	102	0	0	0
tunnel2	NOT_ACTIVE	103	102	0	0	0

IKE Summary

Tunnel Name	IKE State	Destination IP	Remaining Life
tunnel1	NOT_CONNECTED	0.0.0.0	0
tunnel2	NOT_CONNECTED	0.0.0.0	0

2. Reference the **Security Associations** field to view the following:

Tunnel Name The **Tunnel Name** column lists the names of all the tunnels configured on the access point. For information on configuring a tunnel, see *Configuring VPN Tunnels on page 6-33*.

Status The **Status** column lists the status of each configured tunnel. When the tunnel is not in use, the status reads **NOT_ACTIVE**. When the tunnel is connected, the status reads **ACTIVE**.

Outb SPI The **Outb SPI** column displays the outbound Security Parameter Index (SPI) for each tunnel. The SPI is used locally by the access point to identify a security association. There are unique outbound and inbound SPIs.

Inb SPI The **Inb SPI** column displays the inbound SPI Security Parameter Index (SPI) for each of the tunnels. The SPI is used locally by the access point to identify a security association. There are unique outbound and inbound SPIs.

Life Time Use the **Life Time** column to view the lifetime associated with a particular Security Association (SA). Each SA has a finite lifetime defined. When the lifetime expires, the SA can no longer be used to protect data traffic. The maximum SA lifetime is 65535 seconds.

Tx Bytes — The **Tx Bytes** column lists the amount of data (in bytes) transmitted through each configured tunnel.

Rx Bytes — The **Rx Bytes** column lists the amount of data (in bytes) received through each configured tunnel.

3. Click the **Reset VPNs** button to reset active VPNs. Selecting **Reset VPNs** forces renegotiation of all the Security Associations and keys. Users could notice a slight pause in network performance.
4. Reference the **IKE Summary** field to view the following:

Tunnel Name — Displays the name of each of the tunnels configured to use IKE for automatic key exchange.

IKE State — Lists the state for each of the tunnels configured to use IKE for automatic key exchange. When the tunnel is not active, the **IKE State** field displays **NOT_CONNECTED.** When the tunnel is active, the **IKE State** field displays **CONNECTED**.

Destination IP — Displays the destination IP address for each tunnel configured to use IKE for automatic key exchange.

Remaining Life — Lists the remaining life of the current IKE key for each tunnel. When the remaining life on the IKE key reaches 0, IKE initiates a negotiation for a new key. IKE keys associated with a renegotiated tunnel.

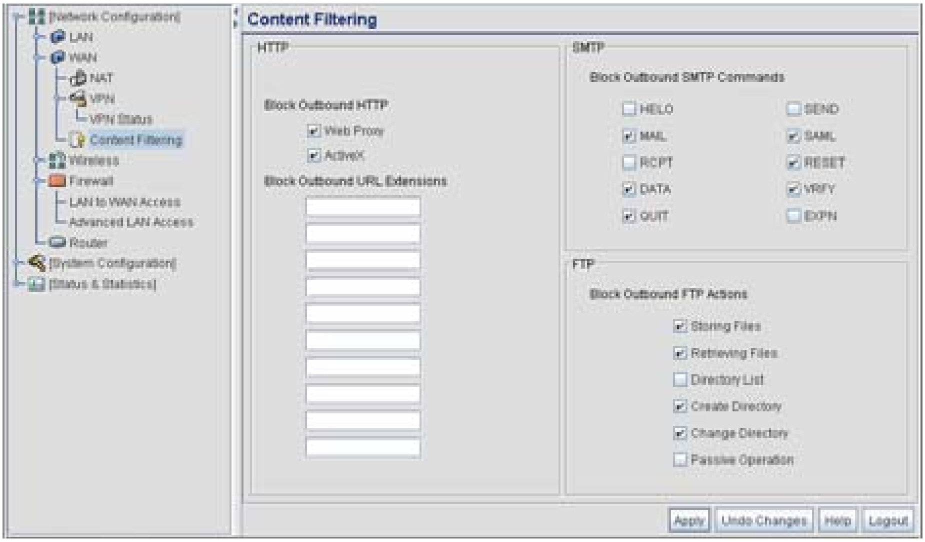
5. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

6.12 Configuring Content Filtering Settings

Content filtering allows system administrators to block specific commands and URL extensions from going out through the access point WAN port. Therefore, content filtering affords system administrators selective control on the content proliferating the network and is a powerful data and network screening tool. Content filtering allows the blocking of up to 10 files or URL extensions and allows blocking of specific outbound HTTP, SMTP, and FTP requests.

To configure content filtering for the access point:

1. Select **Network Configuration** -> **WAN** -> **Content Filtering** from the access point menu tree.



Content Filtering

HTTP

Block Outbound HTTP

☑ Web Proxy

☑ ActiveX

Block Outbound URL Extensions

SMTP

Block Outbound SMTP Commands

□ HELO	□ SEND
☑ MAIL	☑ SAML
□ RCPT	☑ RESET
☑ DATA	☑ VRFY
☑ QUIT	□ EXPN

FTP

Block Outbound FTP Actions

☑ Storing Files

☑ Retrieving Files

□ Directory List

☑ Create Directory

☑ Change Directory

□ Passive Operation

2. Configure the **HTTP** field to configure block Web proxies and URL extensions.

Block Outbound HTTP

HyperText Transport Protocol (HTTP) is the protocol used to transfer information to and from Web sites. HTTP Blocking allows for blocking of specific HTTP commands going outbound on the access point WAN port. HTTP blocks commands on port 80 only.

The Block Outbound HTTP option allows blocking of the following (user selectable) outgoing HTTP requests:

- Web Proxy: Blocks the use of Web proxies by clients
- ActiveX: Blocks all outgoing ActiveX requests by clients. Selecting ActiveX only blocks traffic (scripting language) with an .ocx extension.

Block Outbound URL Extensions

Enter a URL extension or file name per line in the format of *filename.ext*. An asterisk (*) can be used as a wildcard in place of the filename to block all files with a specific extension.

3. Configure the **SMTP** field to disable or restrict specific kinds of network mail traffic.

Block Outbound SMTP Commands

Simple Mail Transport Protocol (SMTP) is the Internet standard for host-to-host mail transport. SMTP generally operates over TCP on port 25. SMTP filtering allows the blocking of any or all outgoing SMTP commands. Check the box next to the command to disable that command when using SMTP across the access point's WAN port.

- HELO - (Hello) Identifies the SMTP sender to the SMTP receiver.
- MAIL- Initiates a mail transaction where data is delivered to one or more mailboxes on the local server.
- RCPT: (Recipient) Identifies a recipient of mail data.
- DATA - Tells the SMTP receiver to treat the following information as mail data from the sender.
- QUIT - Tells the receiver to respond with an **OK** reply and terminate communication with the sender.
- SEND - Initiates a mail transaction where mail is sent to one or more remote terminals.
- SAML - (Send and Mail) Initiates a transaction where mail data is sent to one or more local mailboxes and remote terminals.
- RESET - Cancels mail transaction and informs the recipient to discard data sent during transaction.
- VRFY - Asks receiver to confirm the specified argument identifies a user. If argument does identify a user, the full name and qualified mailbox is returned.
- EXPN - (Expand) Asks receiver to confirm a specified argument identifies a mailing list. If the argument identifies a list, the membership list of the mailing list is returned.

4. Configure the **FTP** field to block or restrict various FTP traffic on the network.

Block Outbound FTP Actions

File Transfer Protocol (FTP) is the Internet standard for host-to-host mail transport. FTP generally operates over TCP port 20 and 21. FTP filtering allows the blocking of any or all outgoing FTP functions.

Check the box next to the command to disable the command when using FTP across the access point’s WAN port.

- Storing Files - Blocks the request to transfer files sent from the client across the AP’s WAN port to the FTP server.
- Retrieving Files: Blocks the request to retrieve files sent from the FTP server across the AP’s WAN port to the client.
- Directory List: Blocks requests to retrieve a directory listing sent from the client across the AP’s WAN port to the FTP server.
- Create Directory: Blocks requests to create directories sent from the client across the AP’s WAN port to the FTP server.
- Change Directory: Blocks requests to change directories sent from the client across the AP's WAN port to the FTP server.
- Passive Operation: Blocks passive mode FTP requests sent from the client across the AP's WAN port to the FTP server.

5. Click **Apply** to save any changes to the Content Filtering screen. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.
6. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Content Filtering screen to the last saved configuration.
7. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

6.13 Configuring Rogue AP Detection

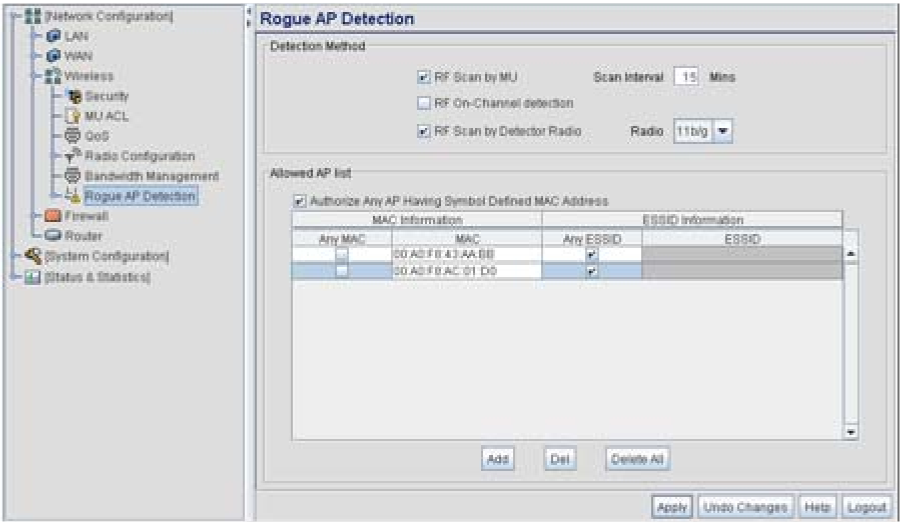
It is possible that not all of the devices identified by the access point are operating legitimately within the access point’s radio coverage area. A rogue AP is a device located nearby an authorized Symbol access point but recognized as having properties rendering its operation illegal and threatening to the access point and the LAN. Rogue AP detection can be configured independently for both access point 802.11a and 802.11b/g radios (if using a dual radio sku access point). A rogue detection interval is the user-defined interval the access point waits to search for rogue APs. Additionally, the access point does not detect rogue APs on illegal channels (channels not allowed by the regulatory requirements of the country the access point is operating in).

The rogue detection interval is used in conjunction with Symbol MUs that identify themselves as rogue detection capable to the access point. The detection interval defines how often the access point requests these MUs to scan for a rogue AP. A shorter interval can effect the performance of the MU, but it will also decrease the time it takes for the access point to scan for a rogue AP. A longer interval will have less of an impact to the MU's, but it will increase the amount of time used to detect rogue APs. Therefore, the interval should be set according to the perceived risk of rogue devices and the criticality of MU performance.

CAUTION Using an antenna other than the Dual-Band Antenna (Part No. ML-2452-APA2-01) could render the access point's Rogue AP Detector Mode feature inoperable. Contact your Symbol sales associate for specific information.

To configure Rogue AP detection for the access point:

1. Select **Network Configuration** -> **Wireless** -> **Rogue AP Detection** from the access point menu tree.



Rogue AP Detection

Detection Method

☑ RF Scan by MU   Scan Interval 15 Mins

□ RF On-Channel detection

☑ RF Scan by Detector Radio   Radio 11b/g

Allowed AP list

☑ Authorize Any AP Having Symbol Defined MAC Address

MAC Information		ESSID Information	
Any MAC	MAC	Any ESSID	ESSID
□	00 A0 F8 43 AA BB	☑	
□	00 A0 F8 AC 01 D0	☑	

2. Configure the **Detection Method** field to set the detection method (MU or access point) and define the 802.11a or 802.11b/g radio to conduct the rogue AP search.

RF Scan by MU
Select the **RF Scan by MU** checkbox to enable MUs to scan for potential rogue APs within the network. Define an interval in the **Scan Interval** field for associated MUs to beacon in an attempt to locate a rogue AP. Set the interval to a value sooner than the default if a large volume of device network traffic is anticipated within the coverage area of the target access point access point. The **Scan Interval** field is not available unless the RF Scan by MU checkbox is selected. Symbol clients must be associated and have rogue AP detection enabled.

RF On-Channel Detection
Select the **RF On-Channel Detection** checkbox to enable the access point to detect rogue APs on its current (legal) channel setting.

RF Scan by Detector Radio
If the access point supports a dual-radio SKU, select the **RF Scan by Detector Radio** checkbox to enable the selected **11a** or **11b/g** radio to scan for rogue APs.

3. Use the **Allowed AP List** field to restrict Symbol AP's from Rogue AP detection and create a list of device MAC addresses and ESSID's approved for interoperability with the access point.

Authorize Any AP Having Symbol Defined MAC Address
Select this checkbox to enable all access points with a Symbol MAC address to interoperate with the access point conducting a scan for rogue devices.

Add
Click **Add** to display a single set of editable MAC address and ESS address values.

Del (Delete)
Click the **Delete** button to remove the highlighted line from the Rule Management field. The MAC and ESS address information previously defined is no longer applicable unless the previous configuration is restored.

Delete All
Click the **Delete All** button to remove all entries from the Rule Management field. All MAC and ESS address information previously defined is no longer applicable unless the previous configuration is restored.

Any MAC
Select the **Any MAC** checkbox to prevent a device's MAC address (whether it is a known device MAC address or not) from being considered a rogue device.

MAC Address — Click **Add,** and enter the device MAC address to be excluded from classification as a rogue device.

Any ESSID — Select the **Any ESSid** checkbox to prevent a device's ESSID (whether it is a known device ESSID or not) from being considered a rogue device

ESSID — Click **Add,** and enter the name of a device ESSid to be excluded from classification as a rogue device.

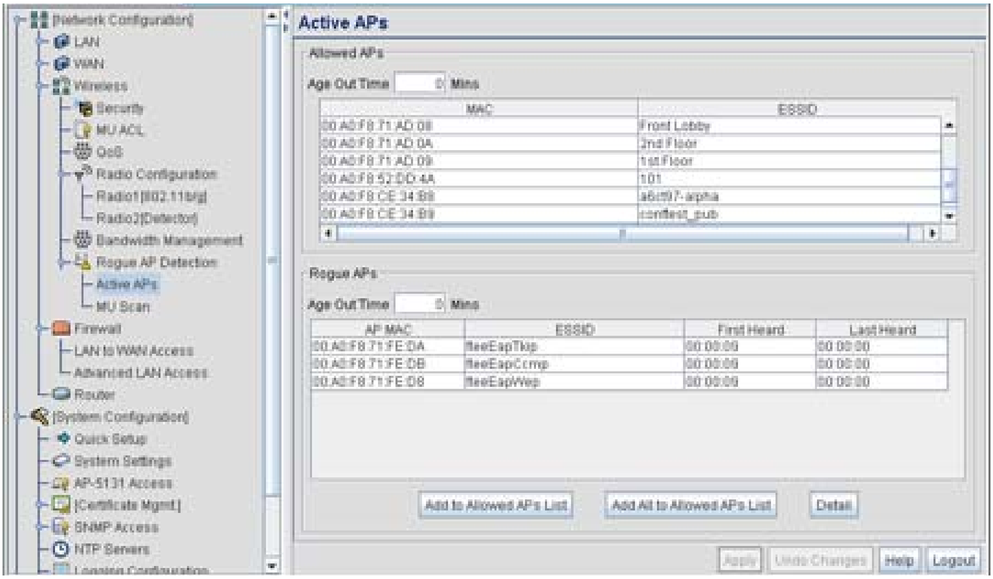
4. Click **Apply** to save any changes to the Rogue AP Detection screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.
5. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Rogue AP Detection screen to the last saved configuration.
6. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

6.13.1 Moving Rogue APs to the Allowed AP List

The **Active APs** screen enables the user to view the list of detected rogue APs and, if necessary, select and move an AP into a list of allowed devices. This is helpful when the settings defined within the **Rogue AP Detection** screen inadvertently detect and define a device as a rogue AP.

To move detected rogue APs into a list of allowed APs:

1. Select **Network Configuration** -> **Wireless** -> **Rogue AP Detection** -> **Active APs** from the access point menu tree.



Active APs

Allowed APs

Age Out Time 0 Mins

MAC	ESSID
00:A0:F8:71:AD:08	Front Lobby
00:A0:F8:71:AD:0A	2nd Floor
00:A0:F8:71:AD:09	1stFloor
00:A0:F8:52:DD:4A	101
00:A0:F8:CE:34:B9	a6cf97-alpha
00:A0:F8:CE:34:B9	conftest_pub

Rogue APs

Age Out Time 0 Mins

AP MAC	ESSID	First Heard	Last Heard
00:A0:F8:71:FE:DA	fleeEapTkip	00:00:00	00:00:00
00:A0:F8:71:FE:DB	fleeEapCcmp	00:00:00	00:00:00
00:A0:F8:71:FE:D8	fleeEapWep	00:00:00	00:00:00

The Active APs screen displays with detected rogue devices displayed within the **Rogue APs** table.

2. Enter a value (in minutes) in the Allowed APs **Age Out Time** field to indicate the number of elapsed minutes before an AP will be removed from the approved list and reevaluated. A zero (0) for this value (default value) indicates an AP can remain on the approved AP list permanently.
3. Enter a value (in minutes) in the Rogue APs **Age Out Time** field to indicate the number of elapsed minutes before an AP will be removed from the rogue AP list and reevaluated. A zero (0) for this value (default value) indicates an AP can remain on the rogue AP list permanently.
4. Highlight an AP from within the Rogue APs table and click the **Add to Allowed APs List** button to move the device into the list of Allowed APs.
5. Click the **Add All to Allowed APs List** button to move each of the APs displayed within the Rogue APs table to the list of allowed APs.
6. Highlight a rogue AP and click the **Details** button to display a screen with device and detection information specific to that rogue device. This information is helpful in determining if a rogue AP should be moved to the Allowed APs table.

   For more information on the displaying information on detected rogue APs, see *Displaying Rogue AP Details on page 6-57*.

7. To remove the Rogue AP entries displayed within the e Rogue APs field, click the **Clear Rogue AP List** button.

   Symbol only recommends clearing the list of Rogue APs when the devices displaying within the list do not represent a threat to the access point managed network.

8. Click **Apply** to save any changes to the Active APs screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.
9. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Active APs screen to the last saved configuration.
10. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

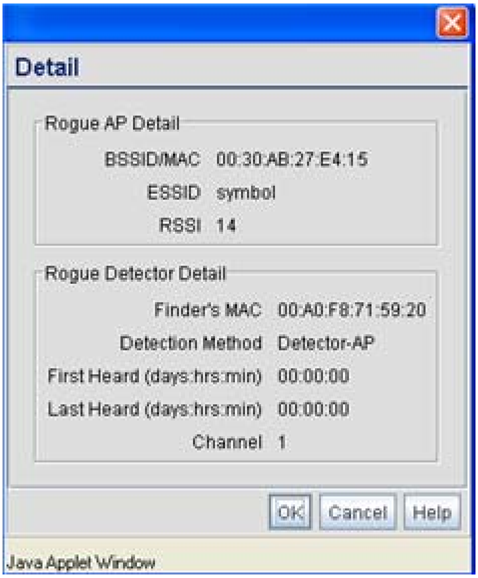
6.13.1.1 Displaying Rogue AP Details

Before moving a rogue AP into the list of allowed APs within the Active APs screen, the device address and rogue detection information for that AP should be evaluated.

To evaluate the properties of a rogue AP:

1. Select **Network Configuration** -> **Wireless** -> **Rogue AP Detection** -> **Active APs** from the access point menu tree.
2. Highlight a target rogue AP from within Rogue APs table and click the **Details** button.

   The **Detail** screen displays for the rogue AP.



Detail

Rogue AP Detail

BSSID/MAC 00:30:AB:27:E4:15

ESSID symbol

RSSI 14

Rogue Detector Detail

Finder's MAC 00:A0:F8:71:59:20

Detection Method Detector-AP

First Heard (days:hrs:min) 00:00:00

Last Heard (days:hrs:min) 00:00:00

Channel 1

3. Refer to the **Rogue AP Detail** field for the following information:

BSSID/MAC Displays the MAC address of the rogue AP. This information could be useful if the MAC address is determined to be a Symbol MAC address and the device is interpreted as non-hostile and the device should be defined as an allowed AP.

ESSID Displays the ESSID of the rogue AP. This information could be useful if the ESSID is determined to be non-hostile and the device should be defined as an allowed AP.

RSSI Shows the *Relative Signal Strength* (RSSI) of the rogue AP. Use this information to assess how close the rogue AP is. The higher the RSSI, the closer the rogue AP. If multiple access point’s have detected the same rogue AP, RSSI can be useful in triangulating the location of the rogue AP.

4. Refer to the **Rogue Detector Detail** field for the following information:

Finder’s MAC The MAC address of the access point detecting the rogue AP.

Detection Method	Displays the **RF Scan by MU**, **RF On-Channel Detection** or **RF Scan by Detector Radio** method selected from the Rogue AP screen to detect rogue devices. For information on detection methods, see *Configuring Rogue AP Detection on page 6-52*.
First Heard (days:hrs:min)	Defines the time in (days:hrs:min) that the rogue AP was initially heard by the detecting AP.
Last Heard (days:hrs:min)	Defines the time in (days:hrs:min) that the rogue AP was last heard by the detecting AP.
Channel	Displays the channel the rogue AP is using.

5. Click **OK** to securely exit the Detail screen and return to the Active APs screen.
6. Click **Cancel** (if necessary) to undo any changes made and return to the Active APs screen.

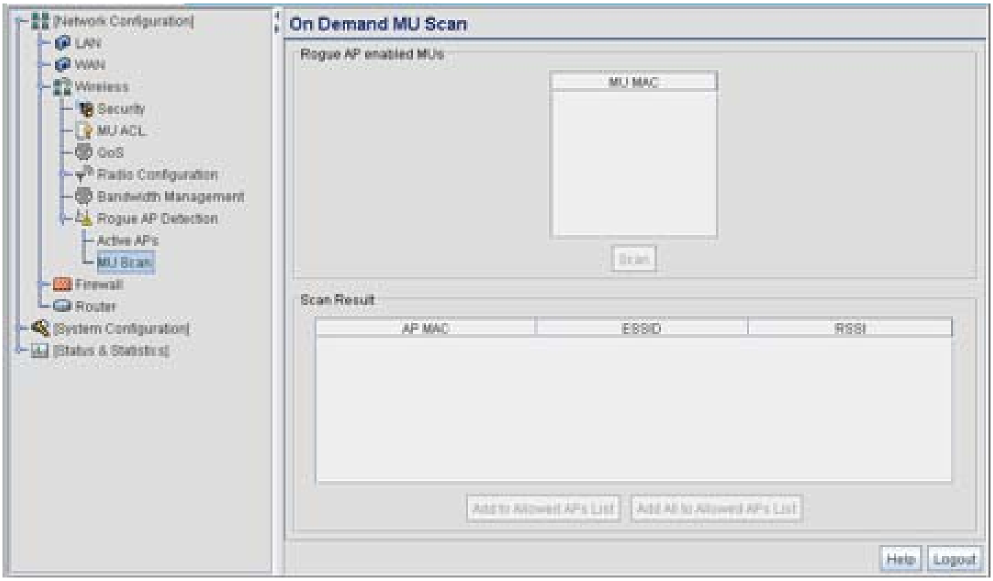
6.13.2 Using MUs to Detect Rogue Devices

The access point can use an associated MU that has its rogue AP detection feature enabled to scan for rogue APs. Once detected, the rogue AP(s) can be moved to the list of allowed devices (if appropriate) within the Active APs screen. When adding an MU's detection capabilities with the access point's own rogue AP detection functionality, the rogue detection area can be significantly extended.

To use associated rogue AP enabled MUs to scan for rogue APs:

1. Select **Network Configuration** -> **Wireless** -> **Rogue AP Detection** -> **MU Scan** from the access point menu tree.

   The **On Demand MU Scan** screen displays with associated MUs with rogue AP detection enabled



2. Highlight an MU from within the **Rogue AP enabled MUs** field and click the scan button.

   The target MU begins scanning for rogue devices using the detection parameters defined within the Rogue AP Detection screen. To modify the detection parameters, see *Configuring Rogue AP Detection on page 6-52*.

   Those devices detected as rogue APs display within the **Scan Result** table. Use the displayed AP MAC, ESSID and RSSI values to determine the device listed in the table is truly a rogue device or one inadvertently detected as a rogue AP.

3. If necessary, highlight an individual MU from within the Scan Result field and click the **Add to Allowed AP List** button to move the AP into the Allowed APs table within the **Active APs** screen.

4. Additionally, if necessary, click the **Add All to Allowed APs List** button to move every device within the Scan Result table into the Allowed APs table within the **Active APs** screen. Only use this option if you are sure all of the devices detected and displayed within the Scan Results table are non-hostile APs.

5. Highlight a different MU from the Rogue AP enabled MUs field as needed to scan for additional rogue APs.

6. Click **Logout** to return to the Rogue AP Detection screen.

6.14 Configuring User Authentication

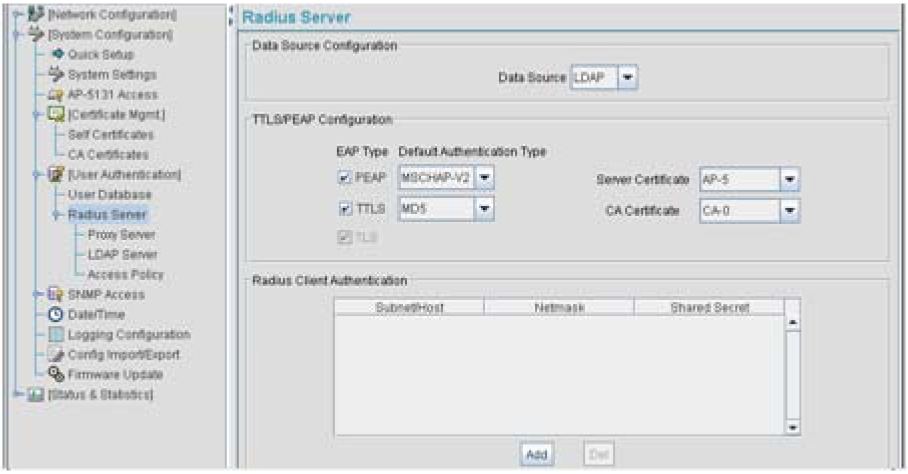
The access point can work with external Radius and LDAP Servers (AAA Servers) to provide user database information and user authentication.

6.14.1 Configuring the Radius Server

The **Radius Server** screen enables an administrator to define data sources and specify authentication information for the RADIUS Server.

To configure the Radius Server:

1. Select **System Configuration** -> **User Authentication** -> **RADIUS Server** from the menu tree.



Data Source Configuration

Data Source: LDAP

TTLS/PEAP Configuration

EAP Type	Default Authentication Type
☑ PEAP	MSCHAP-V2
☑ TTLS	MD5
☑ TLS	

Server Certificate: AP-5

CA Certificate: CA-0

Radius Client Authentication

Subnet/Host	Netmask	Shared Secret

2. From within the **Data Source Configuration** field, use the **Data Source** drop-down menu to select the data source for the Radius server.

Local An internal user database serves as the data source. Use the **User Database** screen to enter the user data. For more information, see *Managing the Local User Database on page 6-68*.

LDAP If LDAP is selected, the switch will use the data in an LDAP server. Configure the LDAP server settings on the LDAP screen under RADIUS Server on the menu tree. For more information, see *Configuring LDAP Authentication on page 6-64*.

3. Use the **TTLS/PEAP Configuration** field to specify the Radius Server default EAP type, EAP authentication type and a Server or CA certificate (if used).

EAP Type

Use the **EAP Type** checkboxes to enable the default EAP type(s) for the RADIUS server. Options include:

- PEAP - Select the PEAP checkbox to enable both PEAP types (GTC and MSCHAP-V2) available to the access point. PEAP uses a TLS layer on top of EAP as a carrier for other EAP modules. PEAP is an ideal choice for networks using legacy EAP authentication methods.
- TTLS - Select the TTLS checkbox to enable all three TTLS types (MD5, PAP and MSCHAP-V2) available to the access point.TTLS is similar to EAP-TLS, but the client authentication portion of the protocol is not performed until after a secure transport tunnel is established. This allows EAP-TTLS to protect legacy authentication methods used by some RADIUS servers.
- TLS - The TLS checkbox is selected but disabled by default and resides in the background as it does not contain user configurable parameters.

Default Authentication Type

Specify a PEAP and/or TTLS Authentication Type for EAP to use from the drop-down menu to the right of each checkbox item.

PEAP options include:

- GTC - *EAP Generic Token Card* (GTC) is a challenge handshake authentication protocol using a hardware token card to provide the response string.
- MSCHAP-V2 - *Microsoft CHAP*(MSCHAP-V2) is an encrypted authentication method based on Microsoft's challenge/ response authentication protocol.

TTLS options include:

- PAP - *Password Authentication Protocol* sends a username and password over a network to a server that compares the username and password to a table of authorized users. If the username and password are matched in the table, server access is authorized. WatchGuard products do not support the PAP protocol because the username and password are sent as clear text that a hacker can read.
- MD5 - This option enables the MD5 algorithm for data verification. MD5 takes as input a message of arbitrary length and produces a 128- bit fingerprint. The MD5 algorithm is intended for digital signature applications, in which a large file must be compressed in a secure manner before being encrypted with a private (secret) key under a public-key cryptographic system.
- MSCHAP-V2 - *Microsoft CHAP*(MSCHAP-V2) is an encrypted authentication method based on Microsoft's challenge/ response authentication protocol.

Server Certificate

If you have a server certificate from a CA and wish to use it on the Radius server, select it from the drop-down menu. Only certificates imported to the access point are available in the menu.For information on creating a certificate, see *Creating Self Certificates for Accessing the VPN on page 4-10*.

CA Certificate

You can also choose an imported CA Certificate to use on the Radius server. If using a server certificate signed by a CA, import that CA's root certificate using the CA certificates screen (for information, see *Importing a CA Certificate on page 4-8*). After a valid CA certificate has been imported, it is available from the CA Certificate drop-down menu.

4. Use the **Radius Client Authentication** table to configure multiple shared secrets based on the subnet or host attempting to authenticate with the Radius server. Use the **Add** button to add entries to the list. Modify the following information as needed within the table.

   Subnet/Host — Defines the IP address of the subnet or host that will be authenticating with the Radius server. If a WLAN has been created to support mesh networking, then enter the IP address of mesh client bridge in order for the MU to authenticate with a base bridge.

   Netmask — Defines the netmask (subnet mask) of the subnet or host authenticating with the Radius server.

   Shared Secret — Click the Passwords button and set a shared secret used for each host or subnet authenticating against the RADIUS server. The shared secret can be up to 7 characters in length.

5. Click **Apply** to save any changes to the Radius Server screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.
6. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Radius Server screen to the last saved configuration.
7. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

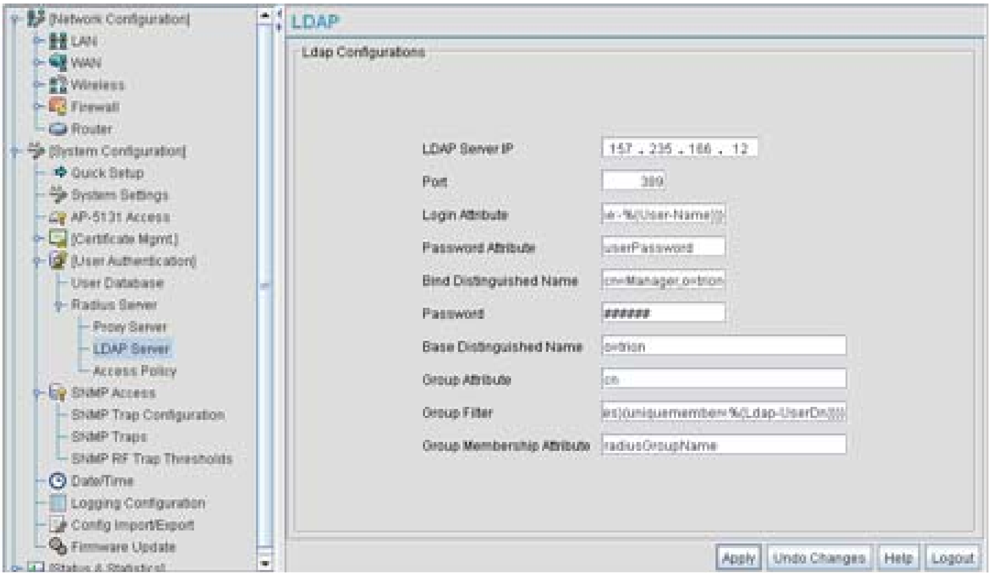
6.14.2 Configuring LDAP Authentication

When the Radius Data Source is set to use an external LDAP server (see *Configuring the Radius Server on page 6-61*), the **LDAP** screen is used to configure the properties of the external LDAP server.

To configure the LDAP server:

1. Select **System Configuration** -> **User Authentication** -> **RADIUS Server** -> **LDAP** from the menu tree.

NOTE The LDAP screen displays with unfamiliar alphanumeric characters (if new to LDAP configuration). Symbol recommends only qualified administrators change the default values displayed within the LDAP screen.



Ldap Configurations

LDAP Server IP 157 . 235 . 166 . 12

Port 389

Login Attribute e=%{User-Name}}

Password Attribute userPassword

Bind Distinguished Name cn=Manager,o=trion

Password ######

Base Distinguished Name o=trion

Group Attribute cn

Group Filter es)(uniquemember=%{Ldap-UserDn})))

Group Membership Attribute radiusGroupName

2. Enter the appropriate information within the LDAP Configuration field to allow the access point to interoperate with the LDAP server. Consult with your LDAP server administrator for details on how to define the values in this screen.

LDAP Server IP Enter the IP address of the external LDAP server acting as the data source for the Radius server. The LDAP server must be accessible from the WAN port or from the access point’s active subnet.

Port Enter the TCP/IP port number for the LDAP server acting as a data source for the Radius. The default port is 389.

Login Attribute Specify the login attribute used by the LDAP server for authentication. In most cases, the default value should work. Windows Active Directory users must use “sAMAccountName” as their login attribute to successfully login to the LDAP server.

Password Attribute Enter the password used by the LDAP server for authentication.

Bind Distinguished Name Specify the distinguished name used to bind with the LDAP server.

Password Enter a valid password for the LDAP server.

Base Distinguished Name Enter a name that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching.

Group Attribute Define the group attribute used by the LDAP server.

Group Filter Specify the group filters used by the LDAP server.

Group Member Attribute Enter the Group Member Attribute sent to the LDAP server when authenticating users.

CAUTION Windows Active Directory users must set their Login Attribute to "sAMAccountName" in order to successfully login to the LDAP server.

3. Click **Apply** to save any changes to the LDAP screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.
4. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the LDAP screen to the last saved configuration.
5. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

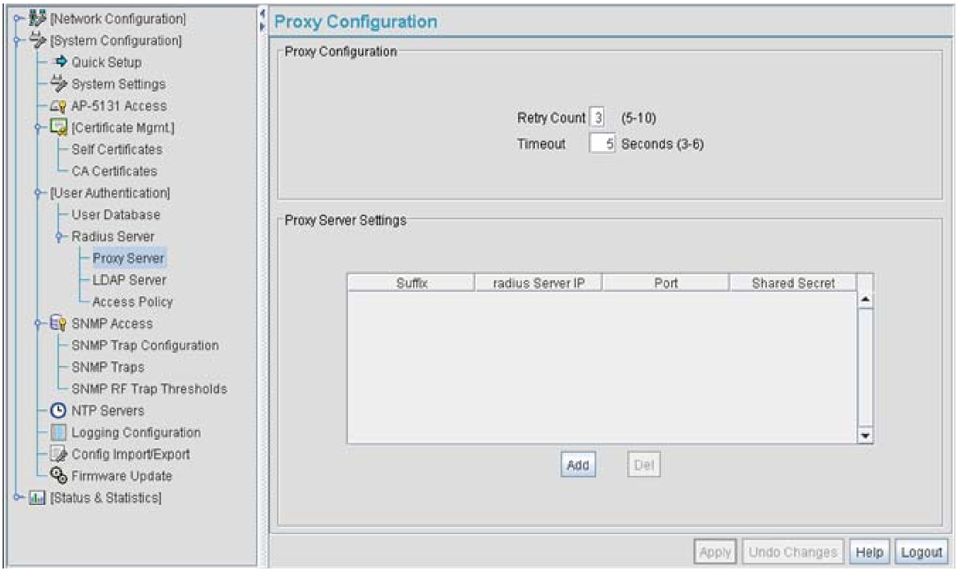
6.14.3 Configuring a Proxy Radius Server

The access point has the capability to proxy authentication requests to a remote Radius server based on the suffix of the user ID (such as myisp.com or company.com). The access point supports up to 10 proxy servers.

CAUTION If using a proxy server for Radius authentication, the **Data Source** field within the Radius server screen must be set to **Local**. If set to LDAP, the proxy server will not be successful when performing the authentication. To verify the existing settings, see *Configuring the Radius Server on page 6-61*.

To configure the proxy Radius server for the access point:

1. Select **System Configuration** -> **User Authentication** -> **RADIUS Server** -> **Proxy** from the menu tree.



Proxy Configuration

Proxy Configuration

Retry Count 3 (5-10)

Timeout 5 Seconds (3-6)

Proxy Server Settings

Suffix	radius Server IP	Port	Shared Secret

2. Refer to the **Proxy Configuration** field to define the proxy server's retry count and timeout values.

Retry Count Enter a value between 3 and 6 to indicate the number of times the access point attempts to reach a proxy server before giving up.

Timeout Enter a value between 5 and 10 to indicate the number of elapsed seconds causing the access point to time out on a request to a proxy server.

3. Use the **Add** button to add a new proxy server. Define the following information for each entry:

Suffix Enter the domain suffix (such as myisp.com or mycompany.com) of the users sent to the specified proxy server.

RADIUS Server IP Specify the IP address of the Radius server acting as a proxy server.

Port Enter the TCP/IP port number for the Radius server acting as a proxy server. The default port is 1812.

Shared Secret Set a shared secret used for each suffix used for authentication with the RADIUS proxy server.

4. To remove a row, select the row and click the **Del** (Delete) button.
5. Click **Apply** to save any changes to the Proxy screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.
6. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Proxy screen to the last saved configuration.
7. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

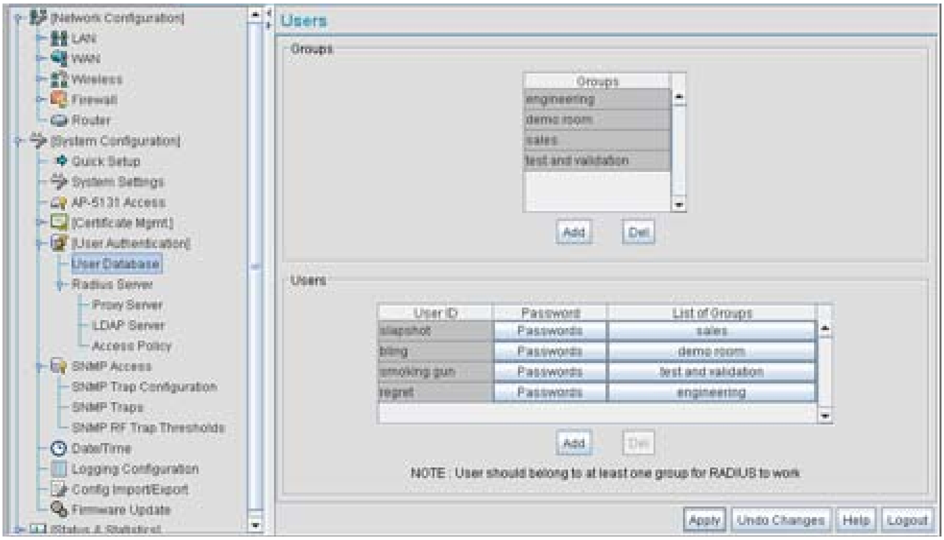
6.14.4 Managing the Local User Database

Use the **User Database** screen to create groups for use with the Radius server. The database of groups is employed if **Local** is selected as the Data Source from the Radius Server screen. For information on selecting Local as the Data Source, see *Configuring the Radius Server on page 6-61*.

To add groups to the User database:

NOTE Each group can be configured to have its own access policy using the Access Policy screen. For more information, see *Defining the User Access Policy on page 6-70*.

1. Select **System Configuration** -> **User Authentication** -> **User Database** from the menu tree.



Groups
engineering
demo room
sales
test and validation

User ID	Password	List of Groups
slapshot	Passwords	sales
bling	Passwords	demo room
smoking gun	Passwords	test and validation
regret	Passwords	engineering

NOTE : User should belong to at least one group for RADIUS to work

Refer to the **Groups** field for a list of all groups in the local Radius database. The groups are listed in the order added. Although groups can be added and deleted, there is no capability to edit a group name.

2. Click the **Add** button and enter the name of the group in the new blank field in the Groups table.
3. To remove a group, select the group from the table and click the **Del** (Delete) key.

   The **Users** table displays the entire list of users. Up to 100 users can be entered here. The users are listed in the order added. Users can be added and deleted, but there is no capability to edit the name of a group.
4. To add a new user, click the **Add** button at the bottom of the Users area.
5. In the new line, type a **User ID** (username).
6. Click the **Password** cell. A small window displays. Enter a password for the user and click **OK** to return to the Users screen.
7. Click the **List of Groups** cell. A new screen displays enabling you to associate groups with the user. For more information on mapping groups with a user, see *Mapping Users to Groups on page 6-69*.
8. Click **Apply** to save any changes to the Users screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.
9. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Users screen to the last saved configuration.
10. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

6.14.4.1 Mapping Users to Groups

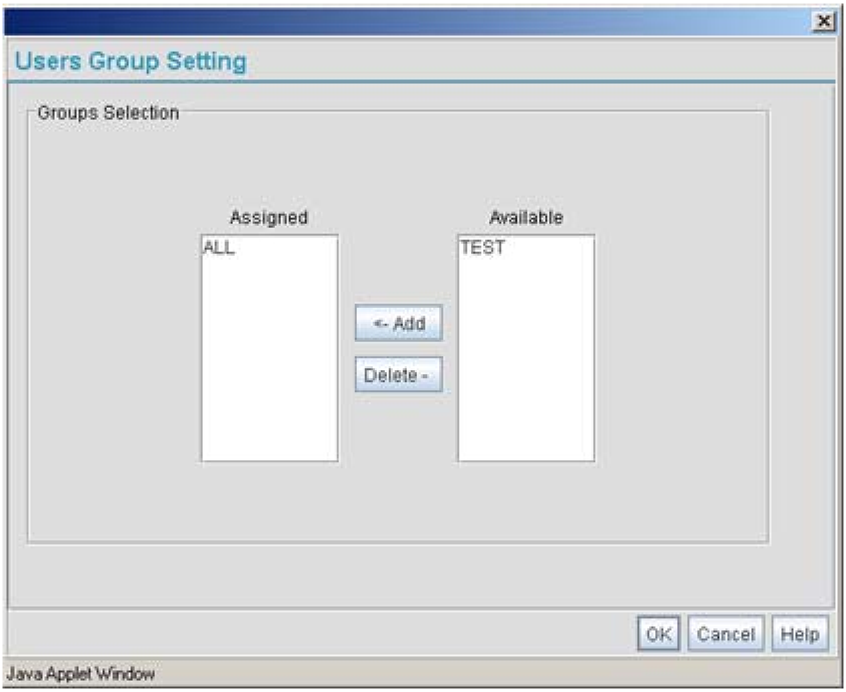
Once users have been created within the **Users** screen, their access privileges need to be configured for inclusion to one, some or all of the groups also created within the Users screen.

To map users to groups for group authentication privileges:

1. If you are not already in the Users screen, select **System Configuration** -> **User Authentication** -> **User Database** from the menu tree.

   Existing users and groups display within their respective fields. If user or group requires creation or modification, make your changes before you begin to map them.
2. Refer to the Users field and select the **List of Groups** column for the particular user you wish to map to one or more groups.

The **Users Group Setting** screen displays with the groups available for user inclusion displayed within the **Available** column.



3. To add the user to a group, select the group in the **Available** list (on the right) and click the **<-Add** button.

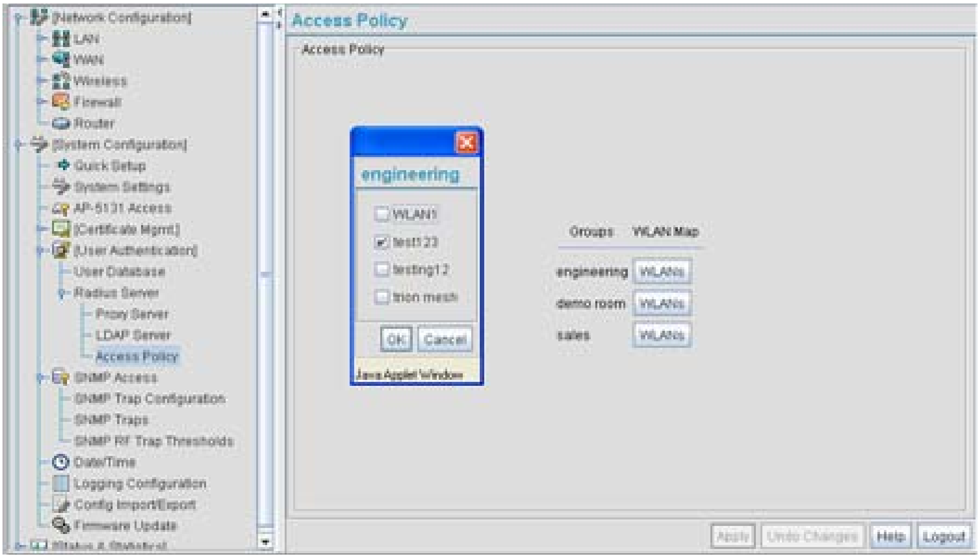
   Assigned users will display within the **Assigned** table. Map one or more groups as needed for group authentication access for this particular user.

4. To remove the user from a group, select the group in the Assigned list (on the left) and click the **Delete->** button.
5. Click the **OK** button to save your user and group mapping assignments and return to the Users screen.

6.14.5 Defining the User Access Policy

Refer to the **Access Policy** screen to define WLAN access for the user group(s) defined within the Users screen. Each group created within the Users screen displays within the Access Policy screen under the group column. Similarly, existing WLANs can be individually mapped to user groups by clicking the WLANs button to the right of each group name. For more information on creating groups and users, see *Managing the Local User Database on page 6-68*. For information on creating a new WLAN or editing the properties of an existing WLAN, see *Creating/Editing Individual WLANs on page 5-24*

1. Select **User Authentication** -> **Radius Server** -> **Access Policy** from the menu tree.



☐ WLAN1
☑ test123
☐ testing12
☐ trion mesh

Groups	WLAN Map
engineering	WLANs
demo room	WLANs
sales	WLANs

2. Click the **WLANs** button to the right of a specific group name.

   A pop-up window displays with the name of the user group appearing on the top of the screen and the names of existing WLANs displaying within the screen. Each WLAN has a checkbox to the left of it for mapping the WLAN to this group.

3. Select the WLAN checkboxes for those specific WLANs you would like to assign access for this particular user group.

4. Click **OK** within the pop-up group screen to save the WLAN mapping configuration for that specific group.

5. Click **Apply** to save any changes to the Access Policy screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.

6. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Access Policy screen to the last saved configuration.

7. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

7

Monitoring Statistics

The access point has functionality to display robust transmit and receive statistics for its WAN and LAN port. *Wireless Local Area Network (WLAN)* stats can also be displayed collectively for each enabled WLAN as well as individually for up to 16 specific WLANs.

Transmit and receive statistics can also be displayed for the access point's 802.11a and 802.11b/g radios. An advanced radio statistics page is also available to display retry histograms for specific data packet retry information.

Associated MU stats can be displayed collectively for associated MUs and individually for specific MUs. An echo (ping) test is also available to ping specific MUs to assess the strength of the AP association.

Finally, the access point can detect and display the properties of other APs detected within the access point radio coverage area. The type of AP detected can be displayed as well as the properties of individual APs.

See the following sections for more details on viewing statistics for the access point:

- *Viewing WAN Statistics*
- *Viewing LAN Statistics*
- *Viewing Wireless Statistics*
- *Viewing Radio Statistics Summary*
- *Viewing MU Statistics Summary*
- *Viewing the Mesh Statistics Summary*
- *Viewing Known Access Point Statistics*

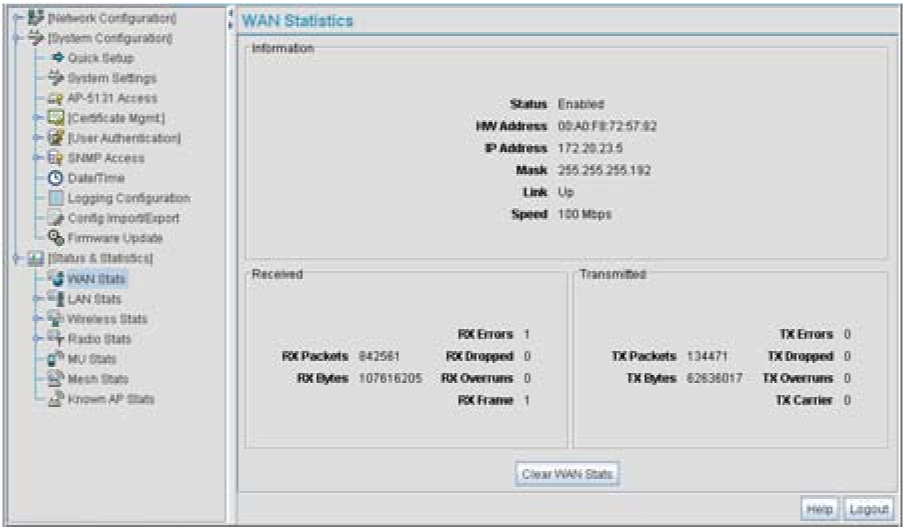
7.1 Viewing WAN Statistics

Use the access point **WAN Stats** screen to view real-time statistics for monitoring the access point activity through its *Wide Area Network (WAN)* port.

The **Information** field of the WAN Stats screen displays basic WAN information, generated from settings on the WAN screen. The **Received** and **Transmitted** fields display statistics for the cumulative packets, bytes, and errors received and transmitted through the WAN interface since it was last enabled or the AP was last rebooted. The access point **WAN Stats** screen is view-only with no configurable data fields.

To view access point WAN Statistics:

1. Select **Status and Statistics** -> **WAN Stats** from the access point menu tree.



WAN Statistics

Information

Status Enabled
HW Address 00:A0:F8:72:57:82
IP Address 172.20.23.5
Mask 255.255.255.192
Link Up
Speed 100 Mbps

Received

RX Errors 1
RX Packets 842561 RX Dropped 0
RX Bytes 107616205 RX Overruns 0
RX Frame 1

Transmitted

TX Errors 0
TX Packets 134471 TX Dropped 0
TX Bytes 62636017 TX Overruns 0
TX Carrier 0

2. Refer to the **Information** field to reference the following access point WAN data:

Status The **Status** field displays **Enabled** if the WAN interface is enabled on the **WAN** screen. If the WAN interface is disabled on the WAN screen, the WAN Stats screen displays no connection information and statistics. To enable the WAN connection, see *Configuring WAN Settings on page 5-14*

HW Address The *Media Access Control (MAC)* address of the access point WAN port. The WAN port MAC address is hard coded at the factory and cannot be changed.

IP Addresses The displayed *Internet Protocol (IP)* addresses for the access point WAN port.

Mask The **Mask** field displays the subnet mask number for the access point's WAN connection. This value is set on the **WAN** screen. Refer to *Configuring WAN Settings on page 5-14* to change the subnet mask.

Link The **Link** field displays **Up** if the WAN connection is active between the access point and network, and **Down** if the WAN connection is interrupted or lost. Use this information to assess the current connection status of the WAN port.

Speed The WAN connection speed is displayed in Megabits per second (Mbps), for example, 54Mbps. If the throughput speed is not achieved, examine the number of transmit and receive errors, or consider increasing the supported data rate. To change the data rate of the 802.11a or 802.11b/g radio, see *Configuring the 802.11a or 802.11b/g Radio on page 5-47*.

3. Refer to the **Received** field to reference data received over the access point WAN port.

RX Packets RX packets are data packets received over the WAN port. The displayed number is a cumulative total since the WAN interface was last enabled or the access point was last restarted.

RX Bytes RX bytes are bytes of information received over the WAN port. The displayed number is a cumulative total since the WAN interface was last enabled or the AP -5131 was last restarted. To restart the access point to begin a new data collection, see *Configuring System Settings on page 4-2*.

RX Errors RX errors include dropped data packets, buffer overruns, and frame errors on inbound traffic. The number of RX errors is a total of *RX Dropped*, *RX Overruns* and *RX Carrier* errors. Use this information to determine performance quality of the current WAN connection.

RX Dropped The **RX Dropped** field displays the number of data packets that fail to reach the WAN interface. If this number appears excessive, consider a new connection to the device.

RX Overruns RX overruns are buffer overruns on the WAN connection. RX overruns occur when packets are received faster than the WAN port can handle them. If RX overruns are excessive, consider reducing the data rate, for more information, see *Configuring the 802.11a or 802.11b/g Radio on page 5-47*.

RX Frame The **RX Frame** field displays the number of TCP/IP data frame errors received.

4. Refer to the **Transmitted** field to reference data received over the access point WAN port.

TX Packets TX packets are data packets sent over the WAN connection. The displayed number is a cumulative total since the WAN interface was last enabled or the access point was last restarted. To begin a new data collection, see *Configuring System Settings on page 4-2*.

TX Bytes TX bytes are bytes of information sent over the WAN connection. The displayed number is a cumulative total since the WAN interface was last enabled or the access point was last restarted. To begin a new data collection, see *Configuring System Settings on page 4-2*.

TX Errors TX errors include dropped data packets, buffer overruns, and carrier errors on outbound traffic. The displayed number of TX errors is the total of *TX Dropped*, T*X Overruns* and *TX Carrier* errors. Use this information to re-assess access point location and transmit speed.

TX Dropped The **TX Dropped** field displays the number of data packets that fail to get sent from the WAN interface.

TX Overruns TX overruns are buffer overruns on the WAN connection. TX overruns occur when packets are sent faster than the WAN interface can handle. If TX overruns are excessive, consider reducing the data rate, for more information, see *Configuring the 802.11a or 802.11b/g Radio on page 5-47*.

TX Carrier The **TX Carrier** field displays the number of TCP/IP data carrier errors.

5. Click the **Clear WAN Stats** button to reset each of the data collection counters to zero in order to begin new data collections. The RX/TX Packets and RX/TX Bytes totals remain at their present values and are not cleared.

   Do not clear the WAN stats if currently in an important data gathering activity or risk losing all data calculations to that point.

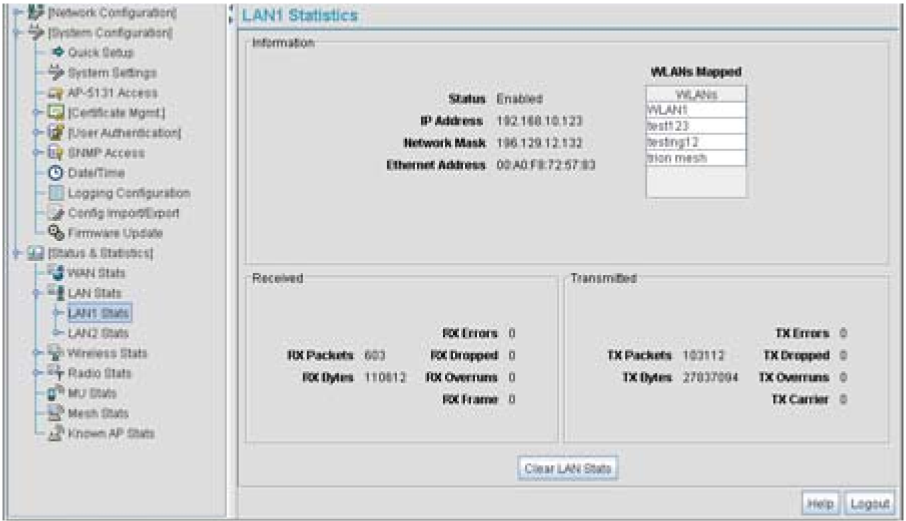
6. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

7.2 Viewing LAN Statistics

Use the **LAN Stats** screen to monitor the activity of the access point LAN1 or LAN2 connection. The **Information** field of the LAN Stats screen displays network traffic information as monitored over the access point LAN1 or LAN2 port. The **Received** and **Transmitted** fields of the screen display statistics for the cumulative packets, bytes, and errors received and transmitted over the LAN1 or LAN2 port since it was last enabled or the access point was last restarted. The **LAN Stats** screen is view-only with no user configurable data fields.

To view access point LAN connection stats:

1. Select **Status and Statistics** -> **LAN Stats** -> **LAN1 Stats** (or LAN2 Stats) from the access point menu tree.



LAN1 Statistics

Information

Status Enabled
IP Address 192.168.10.123
Network Mask 196.129.12.132
Ethernet Address 00:A0:F8:72:57:83

WLANs Mapped

WLANs
WLAN1
test123
testing12
tion mesh

Received

RX Packets 603
RX Bytes 110812
RX Errors 0
RX Dropped 0
RX Overruns 0
RX Frame 0

Transmitted

TX Packets 103112
TX Bytes 27037094
TX Errors 0
TX Dropped 0
TX Overruns 0
TX Carrier 0

2. Refer to the **Information** field to view the following access point device address information:

LAN Interface	Displays whether this particular LAN has been enabled as viable subnet from within the LAN Configuration screen.
IP Address	The *Internet Protocol (IP)* addresses for the access point LAN port.

Network Mask
The first two sets of numbers specify the network domain, the next set specifies the subset of hosts within a larger network. These values help divide a network into subnetworks and simplify routing and data transmission.

Ethernet Address
The *Media Access Control (MAC)* address of the access point. The MAC address is hard coded at the factory and cannot be changed.

WLANs Connected
The **WLANs Connected** table lists the WLANs using this LAN (Either LAN1 or LAN2) as their LAN interface.

3. Refer to the **Received** field to view data received over the access point LAN port.

RX Packets
RX packets are data packets received over the access point LAN port. The number is a cumulative total since the LAN connection was last enabled or the access point was last restarted. To begin a new data collection, see *Configuring System Settings on page 4-2*.

RX Bytes
RX bytes are bytes of information received over the LAN port. The value is a cumulative total since the LAN connection was last enabled or the access point was last restarted. To begin a new data collection, see *Configuring System Settings on page 4-2*.

RX Errors
RX errors include dropped data packets, buffer overruns, and frame errors on inbound traffic. The number of RX errors is a total of *RX Dropped*, *RX Overruns* and *RX Carrier* errors. Use this information to determine performance quality of the current LAN connection.

RX Dropped
The **RX Dropped** field displays the number of data packets failing to reach the LAN port. If this number appears excessive, consider a new connection to the device.

RX Overruns
RX overruns are buffer overruns on the access point LAN port. RX overruns occur when packets are received faster than the LAN connection can handle them. If RX overruns are excessive, consider reducing the data rate, for more information, see *Configuring the 802.11a or 802.11b/g Radio on page 5-47*.

RX Frame
The **RX Frame** field displays the number of TCP/IP data frame errors received.

4. Refer to the **Transmitted** field to view statistics transmitted over the access point LAN port.

TX Packets — TX packets are data packets sent over the access point LAN port. The displayed number is a cumulative total since the LAN connection was last enabled or the access point was last restarted. To begin a new data collection, see *Configuring System Settings on page 4-2*.

TX Bytes — TX bytes are bytes of information sent over the LAN port. The displayed number is a cumulative total since the LAN Connection was last enabled or the access point was last restarted. To begin a new data collection, see *Configuring System Settings on page 4-2*.

TX Errors — TX errors include dropped data packets, buffer overruns, and carrier errors on outbound traffic. The displayed number of TX errors is a total of *TX Dropped, TX Overruns* and *TX Carrier* errors. Use this information to re-assess AP location and transmit speed.

TX Dropped — The **TX Dropped** field displays the number of data packets that fail to get sent from the access point LAN port.

TX Overruns — TX overruns are buffer overruns on the LAN port. TX overruns occur when packets are sent faster than the LAN connection can handle. If TX overruns are excessive, consider reducing the data rate, for more information, see *Configuring the 802.11a or 802.11b/g Radio on page 5-47*.

TX Carrier — The **TX Carrier** field displays the number of TCP/IP data carrier errors.

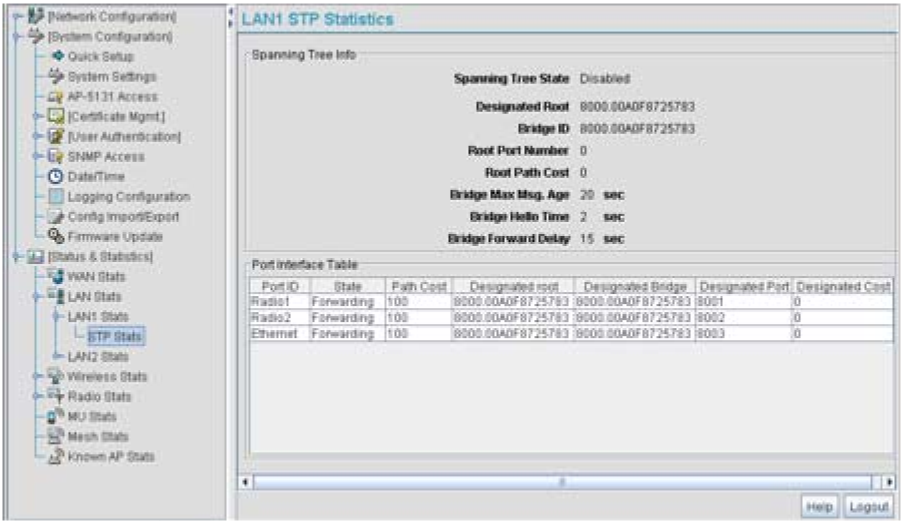
5. Click the **Clear LAN Stats** button to reset each of the data collection counters to zero in order to begin new data collections. The RX/TX Packets and RX/TX Bytes totals remain at their present values and are not cleared.
6. Click the **Logout** button to securely exit the access point Symbol Access Point applet. There will be a prompt confirming logout before the applet is closed.

7.2.1 Viewing a LAN's STP Statistics

Each access point LAN has the ability to track its own unique STP statistics. Refer to the LAN STP Stats page when assessing mesh networking functionality for each of the two access point LANs. Access points in bridge mode exchange configuration messages at regular intervals (typically 1 to 4 seconds). If a bridge fails, neighboring bridges detect a lack of configuration messaging and initiate a spanning-tree recalculation (when spanning tree is enabled).

To view access point LAN's STP statistics:

1. Select **Status and Statistics** -> **LAN Stats** -> **LAN1 Stats** (or LAN2 Stats) > **STP Stats** from the access point menu tree.



LAN1 STP Statistics

Spanning Tree Info

Spanning Tree State Disabled

Designated Root 8000.00A0F8725783

Bridge ID 8000.00A0F8725783

Root Port Number 0

Root Path Cost 0

Bridge Max Msg. Age 20 **sec**

Bridge Hello Time 2 **sec**

Bridge Forward Delay 15 **sec**

Port Interface Table

Port ID	State	Path Cost	Designated root	Designated Bridge	Designated Port	Designated Cost
Radio1	Forwarding	100	8000.00A0F8725783	8000.00A0F8725783	8001	0
Radio2	Forwarding	100	8000.00A0F8725783	8000.00A0F8725783	8002	0
Ethernet	Forwarding	100	8000.00A0F8725783	8000.00A0F8725783	8003	0

2. Refer to the **Spanning Tree Info** field to for details on spanning tree state, and root access point designation.

Spanning Tree State Displays whether the spanning tree state is currently enabled or disabled. The spanning tree state must be enabled for a unique spanning-tree calculation to occur when the bridge is powered up or when a topology change is detected.

Designated Root Displays the access point MAC address of the bridge defined as the root bridge in the Bridge STP Configuration screen. For information on defining an access point as a root bridge, see *Setting the LAN Configuration for Mesh Networking Support on page 9-5*.

Bridge ID The Bridge ID identifies the priority and ID of the bridge sending the message

Root Port Number Identifies the root bridge by listing its 2-byte priority followed by its 6-byte ID.

Root Path Cost Bridge message traffic contains information identifying the root bridge and the sending bridge. The root path cost represents the distance (cost) from the sending bridge to the root bridge.

Bridge Max Msg. Age The Max Msg Age measures the age of received protocol information recorded for a port, and to ensure the information is discarded when it exceeds the value set for the Maximum Message age timer. For information on setting the Maximum Message Age. For information on setting the Bridge Max Msg. Age, see *Setting the LAN Configuration for Mesh Networking Support on page 9-5*.

Bridge Hello Time The Bridge Hello Time is the time between each bridge protocol data unit sent. This time is equal to 2 seconds (sec) by default, but can tuned between 1 and 10 sec. For information on setting the Bridge Hello Time, see *Setting the LAN Configuration for Mesh Networking Support on page 9-5*. The 802.1d specification recommends the Hello Time be set to a value less than half of the Max Message age value.

Bridge Forward Delay The Bridge Forward Delay value is the time spent in a listening and learning state. This time is equal to 15 sec by default, but you can tune the time to be between 4 and 30 sec. For information on setting the Bridge Forward Delay, see *Setting the LAN Configuration for Mesh Networking Support on page 9-5*.

3. Refer to the **Port Interface Table** to assess the state of the traffic over the ports listed within the table for the root and bridge and designated bridges.

Port ID Identifies the port from which the configuration message was sent.

State Displays whether a bridge is forwarding traffic to other members of the mesh network (over this port) or blocking traffic. Each viable member of the mesh network must forward traffic to extent the coverage area of the mesh network.

Path Cost The root path cost is the distance (cost) from the sending bridge to the root bridge.

Designated Root Displays the MAC address of the access point defined with the lowest priority within the Mesh STP Configuration screen.

Designated Bridge There is only one root bridge within each mesh network. All other bridges are designated bridges that look to the root bridge for several mesh network timeout values. For information on root and bridge designations, see *Setting the LAN Configuration for Mesh Networking Support on page 9-5*.

Designated Port Each designated bridge must use a unique port. The value listed represents the port used by each bridge listed within the table to route traffic to other members of the mesh network.

Designated Cost Displays the unique distance between each access point MAC address listed in the Designated Bridge column and the access point MAC address listed in the Designated Root column.

4. Click the **Logout** button to securely exit the access point Symbol Access Point applet. There will be a prompt confirming logout before the applet is closed.

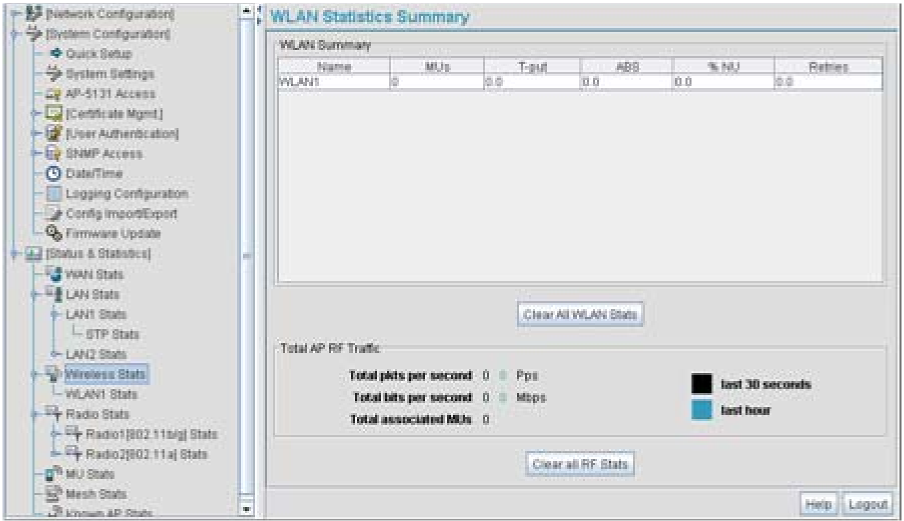
7.3 Viewing Wireless Statistics

Use the **WLAN Statistics Summary** screen to view overview statistics for active (enabled) WLANs on the access point. The **WLAN Summary** field displays basic information such as number of Mobile Units (MUs) and total throughput for each of the active WLANs. The **Total RF Traffic** section displays basic throughput information for all RF activity on the access point. The WLAN Statistics Summary screen is view-only with no user configurable data fields.

If a WLAN is not displayed within the **Wireless Statistics Summary** screen, see *Enabling Wireless LANs (WLANs) on page 5-22* to enable the WLAN. For information on configuring the properties of individual WLANs, see *Creating/Editing Individual WLANs on page 5-24*.

To view access point WLAN Statistics:

1. Select **Status and Statistics** -> **Wireless Stats** from the access point menu tree.



WLAN Statistics Summary

WLAN Summary

Name	MUs	T-put	ABS	% NU	Retries
WLAN1	0	0.0	0.0	0.0	0.0

Total AP RF Traffic

Total pkts per second 0 Pps
Total bits per second 0 Mbps
Total associated MUs 0

■ **last 30 seconds**
🟦 **last hour**

2. Refer to the **WLAN Summary** field to reference high-level data for each enabled WLAN.

Name Displays the names of all the enabled WLANs on the access point. For information on enabling a WLAN, see *Enabling Wireless LANs (WLANs) on page 5-22*.

MUs Displays the total number of MUs currently associated with each enabled WLAN. Use this information to assess if the MUs are properly grouped by function within each enabled WLAN. To adjust the maximum number of MUs permissible per WLAN, see *Creating/Editing Individual WLANs on page 5-24*.

T-put Displays the total throughput in Megabits per second (Mbps) for each active WLAN.

ABS Displays the *Average Bit Speed (ABS)* in Megabits per second (Mbps) for each active WLAN displayed.

% NU Displays a percentage of the total packets for each active WLAN that are non-unicast. Non-unicast packets include broadcast and multicast packets.

Retries Displays the average number of retries per packet. An excessive number could indicate possible network or hardware problems.

Clear All WLAN Stats Click this button to reset each of the data collection counters to zero in order to begin new data collections.

Do not clear the WLAN stats if currently in an important data gathering activity or risk losing all data calculations to that point.

3. Refer to the **Total AP RF Traffic** field to view throughput information for the access point and WLAN.

Total pkts per second Displays the average number of RF packets sent per second across all active WLANs on the access point. The number in black represents packets for the last 30 seconds and the number in blue represents total pkts per second for the last hour.

Total bits per second Displays the average bits sent per second across all active WLANs on the AP.-5131 The number in black displays this statistic for the last 30 seconds and the number in blue displays this statistic for the last hour.

Total associated MUs Displays the current number of MUs associated with the active WLANs on the access point. If the number is excessive, reduce the maximum number of MUs that can associate with the access point, for more information, see *Creating/Editing Individual WLANs on page 5-24*.

Clear all RF Stats Click the **Clear all RF Stats** button to reset statistic counters for each WLAN, and the Total AP RF totals to 0. Do not clear RF stats if currently in an important data gathering activity or risk losing all data calculations to that point.

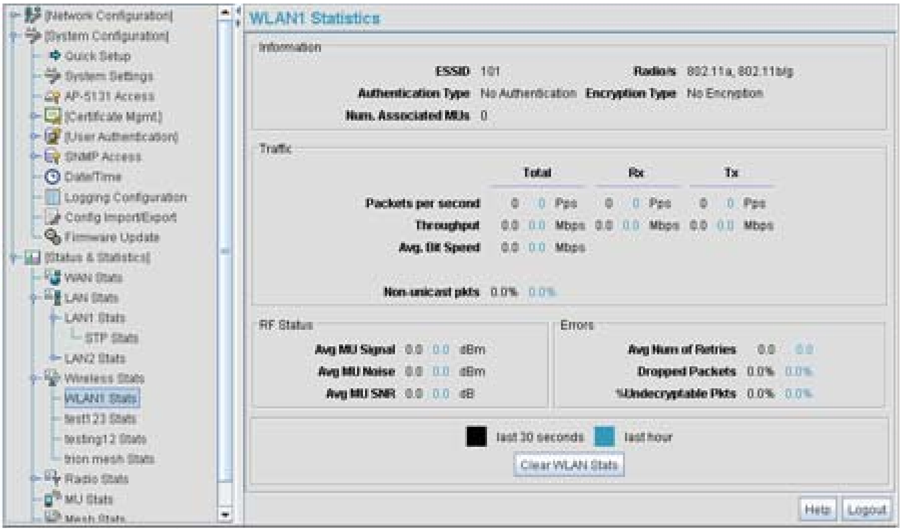
4. Click the **Clear RF Stats** button to reset each of the data collection counters to zero in order to begin new data collections.
5. Click the **Logout** button to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

7.3.1 Viewing WLAN Statistics

Use the **WLAN Stats** screen to view detailed statistics for individual WLANs.The WLAN Stats screen is separated into four fields; *Information, Traffic*, *RF Status*, and *Errors*. The **Information** field displays basic information such as number of associated Mobile Units, ESSID and security information. The **Traffic** field displays statistics on RF traffic and throughput. The **RF Status** field displays information on RF signal averages from the associated MUs. The **Error** field displays RF traffic errors based on retries, dropped packets, and undecryptable packets. The **WLAN Stats** screen is view-only with no user configurable data fields.

To view statistics for an individual WLAN:

1. Select **Status and Statistics** -> **Wireless Stats** -> **WLAN*x* Stats** (*x* = target WLAN) from the access point menu tree.



WLAN1 Statistics

Information

ESSID 101 Radio/s 802.11a, 802.11b/g
Authentication Type No Authentication Encryption Type No Encryption
Num. Associated MUs 0

Traffic

	Total			Rx			Tx		
Packets per second	0	0	Pps	0	0	Pps	0	0	Pps
Throughput	0.0	0.0	Mbps	0.0	0.0	Mbps	0.0	0.0	Mbps
Avg. Bit Speed	0.0	0.0	Mbps						
Non-unicast pkts	0.0%	0.0%							

RF Status

Avg MU Signal 0.0 0.0 dBm
Avg MU Noise 0.0 0.0 dBm
Avg MU SNR 0.0 0.0 dB

Errors

Avg Num of Retries 0.0 0.0
Dropped Packets 0.0% 0.0%
%Undecryptable Pkts 0.0% 0.0%

■ last 30 seconds 🟦 last hour

2. Refer to the **Information** field to view specific WLAN address, MU and security scheme information for the WLAN selected from the access point menu tree.

ESSID Displays the *Extended Service Set ID (ESSID)* for the target WLAN.

Radio/s Displays the name of the 802.11a or 802.11b/g radio the target WLAN is using for access point transmissions.

Authentication Type Displays the authentication type (802.1x EAP or Kerberos) defined for the WLAN. If the authentication type does not match the desired scheme for the WLAN or needs to be enabled, see *Enabling Authentication and Encryption Schemes on page 6-5*.

Encryption Type Displays the encryption method defined for the WLAN. If the encryption type does not match the desired scheme for the WLAN or needs to be enabled, see *Enabling Authentication and Encryption Schemes on page 6-5*.

Num. Associated MUs Displays the total number of MUs currently associated with the WLAN. If this number seems excessive, consider segregating MU's to other WLANs if appropriate.

3. Refer to the **Traffic** field to view performance and throughput information for the WLAN selected from the access point menu tree.

Pkts per second The **Total** column displays the average total packets per second crossing the selected WLAN. The **Rx** column displays the average total packets per second received on the selected WLAN. The **Tx** column displays the average total packets per second sent on the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

Throughput The **Total** column displays average throughput in Mbps for a given time period on the selected WLAN. The **Rx** column displays average throughput in Mbps for packets received on the selected WLAN. The **Tx** column displays average throughput for packets sent on the selected WLAN. The number in black represents statistics for the last 30 seconds and the number in blue represents statistics for the last hour. Use this information to assess whether the current access point data rate is sufficient to support required network traffic.

Avg. Bit Speed The **Total** column displays the average bit speed in Mbps for a given time period on the selected WLAN.This includes all packets that are sent and received. The number in black represents statistics for the last 30 seconds and the number in blue represents statistics for the last hour. If the bit speed is significantly slower than the selected data rate, refer to the **RF Statistics** and **Errors** fields to troubleshoot.

% Non-unicast pkts Displays the percentage of the total packets that are non-unicast. Non-unicast packets include broadcast and multicast packets.The number in black represents packets for the last 30 seconds and the number in blue represents packets for the last hour.

4. Refer to the **RF Status** field to view the following MU signal, noise and performance information for the WLAN selected from the access point menu tree.

Avg MU Signal

Displays the average RF signal strength in dBm for all MUs associated with the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour. If the signal is low, consider mapping the MU to a different WLAN if a better functional grouping of MUs can be determined.

Avg MU Noise

Displays the average RF noise for all MUs associated with the selected WLAN. The number in black represents MU noise for the last 30 seconds and the number in blue represents MU noise for the last hour. If MU noise is excessive, consider moving the MU closer to the access point, or in area with less conflicting network traffic.

Avg MU SNR

Displays the average *Signal to Noise Ratio (SNR)* for all MUs associated with the selected WLAN. The Signal to Noise Ratio is an indication of overall RF performance on your wireless networks.

5. Refer to the **Errors** field to view MU association error statistics for the WLAN selected from the access point menu tree.

Avg Num of Retries

Displays the average number of retries for all MUs associated with the selected WLAN. The number in black represents average retries for the last 30 seconds and the number in blue represents average retries for the last hour.

Dropped Packets

Displays the percentage of packets which the AP gave up on for all MUs associated with the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

% of Undecryptable Pkts

Displays the percentage of undecryptable packets for all MUs associated with the selected WLAN. The number in black represents undecryptable pkts for the last 30 seconds and the number in blue represents undecryptable pkts for the last hour.

NOTE The **Apply** and **Undo Changes** buttons are not available on the **WLAN Statistics** screen as this screen is view only with no configurable data fields.

6. Click the **Clear WLAN Stats** button to reset each of the data collection counters to zero in order to begin new data collections.

Do not clear the WLAN stats if currently in an important data gathering activity or risk losing all data calculations to that point.

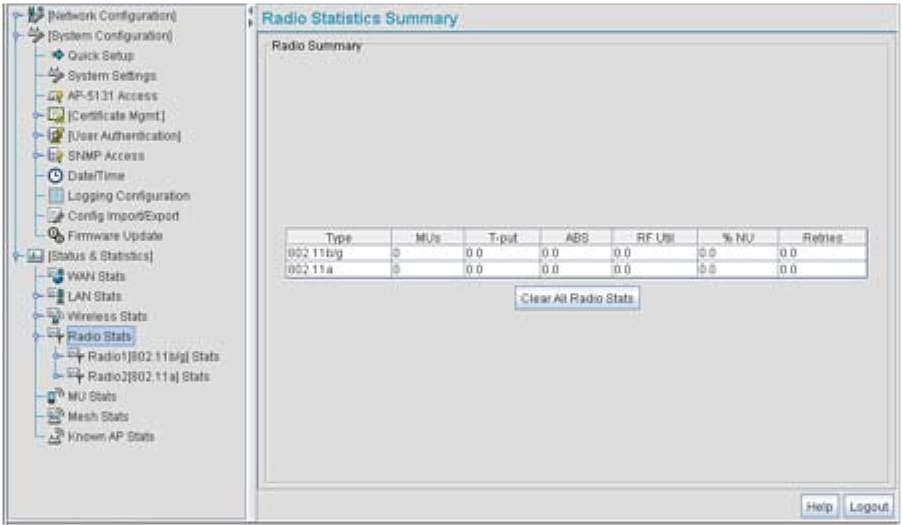
7. Click the **Logout** button to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

7.4 Viewing Radio Statistics Summary

Select the **Radio Stats Summary** screen to view high-level information (radio name, type, number of associated MUs, etc.) for the radio(s) enabled on an access point. Individual radio statistics can be displayed as well by selecting a specific radio from within the access point menu tree.

To view high-level access point radio statistics:

1. Select **Status and Statistics** -> **Radio Stats** from the access point menu tree.



Type	MUs	T-put	ABS	RF Util	% NU	Retries
802.11b/g	0	0.0	0.0	0.0	0.0	0.0
802.11a	0	0.0	0.0	0.0	0.0	0.0

2. Refer to the **Radio Summary** field to reference access point radio information.

Type Displays the type of radio (either 802.11a or 802.11b/g) currently deployed by the access point. To configure the radio type, see *Setting the WLAN's Radio Configuration on page 5-44*.

MUs Displays the total number of MUs currently associated with each access point radio.

T-put Displays the total throughput in Megabits per second (Mbps) for each access point radio listed. To adjust the data rate for a specific radio, see *Configuring the 802.11a or 802.11b/g Radio on page 5-47*.

ABS Displays the *Average Bit Speed (ABS)* in Megabits per second (Mbps) for each access point radio.

RF Util Displays the approximate RF Utilization for each access point radio

% NU Displays the percentage of the total packets that are non-unicast. Non-unicast packets include broadcast and multicast packets.

Retries Displays the average number of retries per packet on each radio. A high number could indicate network or hardware problems.

3. Click the **Clear All Radio Stats** button to reset each of the data collection counters to zero in order to begin new data collections.

   Do not clear the radio stats if currently in an important data gathering activity or risk losing all data calculations to that point.

   For information on viewing radio statistics particular to the access point radio type displayed within the AP Stats Summary screen, see *Viewing Radio Statistics on page 7-18*.

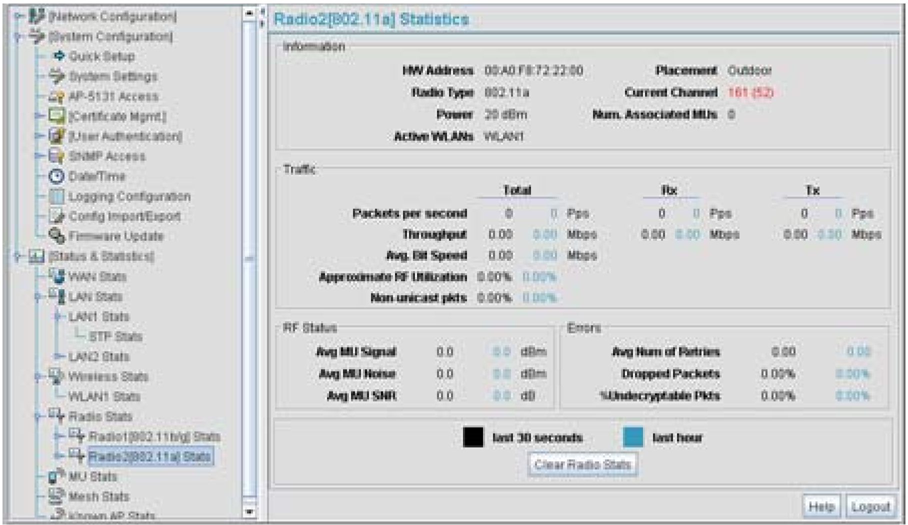
4. Click the **Logout** button to securely exit the access point Symbol Access Point applet.

7.4.1 Viewing Radio Statistics

Refer to the **Radio Stats** screen to view detailed information for the access point radio (either 802.11a or 802.11b/g) displayed within the Radio Summary screen. There are four fields within the screen. The **Information** field displays device address and location information, as well as channel and power information. The **Traffic** field displays statistics for cumulative packets, bytes, and errors received and transmitted. The Traffic field does not add retry information to the stats displayed. Refer to the **RF Status** field for an average MU signal, noise and signal to noise ratio information. Finally, the **Errors** field displays retry information as well as data transmissions the access point radio either dropped or could not decrypt. The information within the 802.11a Radio Statistics screen is view-only with no configurable data fields.

To view detailed radio statistics:

1. Select **Status and Statistics** -> **Radio Stats** -> **Radio1(802.11b/g) Stats** from the access point menu tree.



Radio2[802.11a] Statistics

Information

HW Address	00:A0:F8:72:22:00	Placement	Outdoor
Radio Type	802.11a	Current Channel	161 (52)
Power	20 dBm	Num. Associated MUs	0
Active WLANs	WLAN1		

Traffic

	Total			Rx			Tx		
Packets per second	0	0	Pps	0	0	Pps	0	0	Pps
Throughput	0.00	0.00	Mbps	0.00	0.00	Mbps	0.00	0.00	Mbps
Avg. Bit Speed	0.00	0.00	Mbps						
Approximate RF Utilization	0.00%	0.00%							
Non-unicast pkts	0.00%	0.00%							

RF Status

Avg MU Signal	0.0	0.0	dBm
Avg MU Noise	0.0	0.0	dBm
Avg MU SNR	0.0	0.0	dB

Errors

Avg Num of Retries	0.00	0.00
Dropped Packets	0.00%	0.00%
%Undecryptable Pkts	0.00%	0.00%

■ last 30 seconds 🟦 last hour

2. Refer to the **Information** field to view the access point 802.11a or 802.11b/g radio's MAC address, placement and transmission information.

HW Address	The *Media Access Control (MAC)* address of the access point housing the 802.11a radio. The MAC address is set at the factory and can be found on the bottom of the AP.
Radio Type	Displays the radio type (either 802.11a or 802.11b/g).
Power	The power level in milliwatts (mW) for RF signal strength. To change the power setting for the radio, see *Configuring the 802.11a or 802.11b/g Radio on page 5-47*.
Active WLANs	Lists the access point WLANs adopted by the 802.11a or 802.11b/g radio.
Placement	Lists whether the access point radio is indoors or outdoors. To change the placement setting, see *Configuring the 802.11a or 802.11b/g Radio on page 5-47*.
Current Channel	Indicates the channel for communications between the access point radio and its associated MUs. To change the channel setting, see *Configuring the 802.11a or 802.11b/g Radio on page 5-47*.
Num Associated MUs	Lists the number of mobile units (MUs) currently associated with the access point 802.11a or 802.11b/g radio.

3. Refer to the **Traffic** field to view performance and throughput information for the target access point 802.11a or 802.11b/g radio.

   Pkts per second — The **Total** column displays the average total packets per second crossing the radio. The **Rx** column displays the average total packets per second received. The **Tx** column displays the average total packets per second transmitted. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

   Throughput — The **Total** column displays average throughput on the radio. The **Rx** column displays average throughput in Mbps for packets received. The **Tx** column displays average throughput for packets transmitted. The number in black represents statistics for the last 30 seconds and the number in blue represents statistics for the last hour. Use this information to assess whether the current throughput is sufficient to support required network traffic.

   Avg. Bit Speed — The **Total** column displays the average bit speed in Mbps for the radio This includes all packets transmitted and received. The number in black represents statistics for the last 30 seconds and the number in blue represents statistics for the last hour.

   Approximate RF Utilization — The approximate RF utilization of the access point radio. This value is calculated as throughput divided by average bit speed. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

   % Non-unicast pkts — Displays the percentage of total radio packets that are non-unicast. Non-unicast packets include broadcast and multicast packets.The number in black represents packets for the last 30 seconds and the number in blue represents packets for the last hour.

4. Refer to the **RF Status** field to view the following MU signal, noise and performance information for the target access point 802.11a or 802.11b/g radio.

   Avg MU Signal — Displays the average RF signal strength in dBm for all MUs associated with the radio. The number in black represents the average signal for the last 30 seconds and the number in blue represents the average signal for the last hour. If the signal is low, consider mapping the MU to a different WLAN, if a better functional grouping of MUs can be determined.

Avg MU Noise Displays the average RF noise for all MUs associated with the access point radio. The number in black represents MU noise for the last 30 seconds and the number in blue represents MU noise for the last hour. If MU noise is excessive, consider moving the MU closer to the access point, or in area with less conflicting network traffic.

Avg MU SNR Displays the average *Signal to Noise Ratio (SNR)* for all MUs associated with the access point radio. The Signal to Noise Ratio is an indication of overall RF performance on your wireless network.

5. Refer to the **Errors** field to reference retry information as well as data transmissions the target access point 802.11a or 802.11 b/g radio either gave up on could not decrypt.

Avg Num. of Retries Displays the average number of retries for all MUs associated with the access point 802.11a or 802.11b/g radio. The number in black represents retries for the last 30 seconds and the number in blue represents retries for the last hour.

Dropped Packets Displays the percentage of packets the AP gave up on for all MUs associated with the access point 802.11a or 802.11b/g radio. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

% of Undecryptable Pkts Displays the percentage of undecryptable packets for all MUs associated with the 802.11a or 802.11b/g radio. The number in black represents packets for the last 30 seconds and the number in blue represents packets for the last hour.

6. Click the **Clear Radio Stats** button to reset each of the data collection counters to zero in order to begin new data collections.
7. Click the **Logout** button to securely exit the access point Symbol Access Point applet.

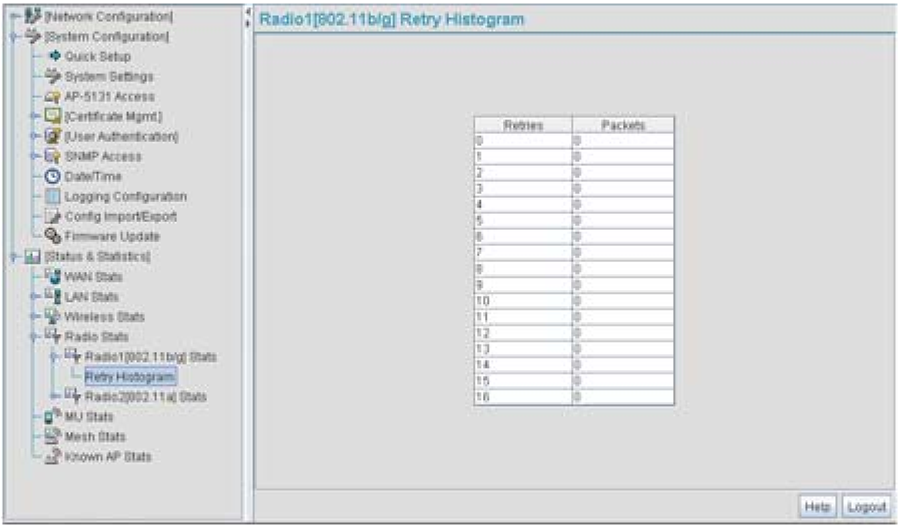
7.4.1.1 Retry Histogram

Refer to the **Retry Histrogram** screen for an overview of the retries transmitted by an access point radio and whether those retries contained any data packets. Use this information in combination with the error fields within a Radio Stats screen to assess overall radio performance.

To display a Retry Histogram screen for an access point radio:

1. Select **Status and Statistics** -> **Radio Stats** -> **Radio1(802.11b/g) Stats** -> **Retry Histogram** from the access point menu tree.

   A Radio Histogram screen is available for each access point radio (regardless of single or dual-radio model).



Radio1[802.11b/g] Retry Histogram

Retries	Packets
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0

   The table's first column shows 0 under **Retries**. The value under the **Packets** column directly to the right shows the number of packets transmitted by this access point radio that required 0 retries (delivered on the first attempt). As you go down the table you can see the number of packets requiring 1 retry, 2 retries etc. Use this information to assess whether an abundance of retries warrants reconfiguring the access point radio to achieve better performance.

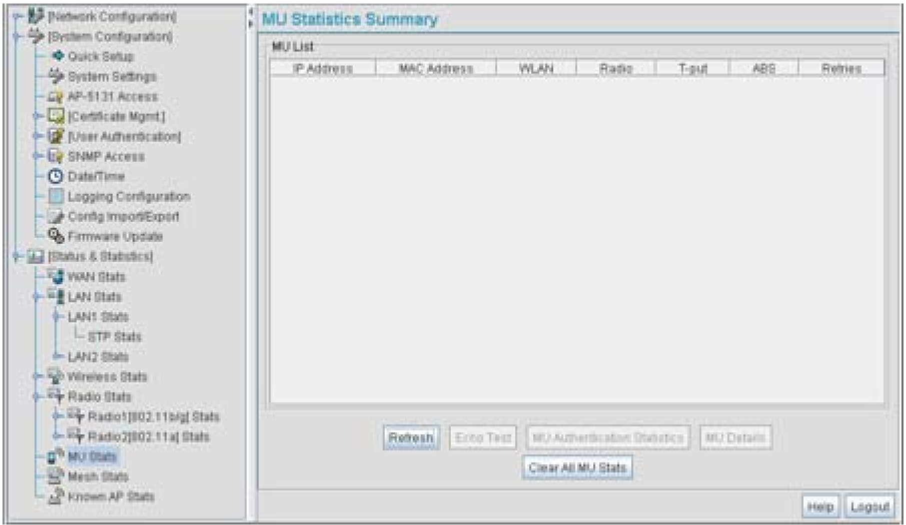
2. Click **Apply** to save any changes to the Radio Histogram screen. Navigating away from the screen without clicking Apply results in changes to the screens being lost.
3. Click **Undo Changes** (if necessary) to undo any changes made to the screen. Undo Changes reverts the settings to the last saved configuration.
4. Click **Logout** to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

7.5 Viewing MU Statistics Summary

Use the **MU Stats Summary** screen to display overview statistics for mobile units (MUs) associated with the access point. The **MU List** field displays basic information such as IP Address and total throughput for each associated MU. The MU Stats screen is view-only with no user configurable data fields. However, individual MUs can be selected from within the MU Stats Summary screen to either ping to assess interoperability or display authentication statistics.

To view access point overview statistics for all of the MUs associated to the access point:

1. Select **Status and Statistics** - > **MU Stats** from the access point menu tree.



MU Statistics Summary

MU List

IP Address	MAC Address	WLAN	Radio	T-put	ABS	Retries

2. Refer to the **MU List** field to reference associated MU address, throughput and retry information.

IP Address Displays the IP address of each of the associated MU.

MAC Address Displays the MAC address of each of the associated MU.

WLAN Displays the WLAN name each MU is interoperating with.

Radio Displays the name of the 802.11a or 802.11b/g radio each MU is associated with.

T-put Displays the total throughput in Megabits per second (Mbps) for each associated MU.

ABS Displays the *Average Bit Speed (ABS)* in Megabits per second (Mbps) for each associated MU.

Retries Displays the average number of retries per packet. A high number retries could indicate possible network or hardware problems.

3. Click the **Refresh** button to update the data collections displayed without resetting the data collections to zero.
4. Click the **Echo Test** button to display a screen for verifying the link with an associated MU.

   For detailed information on conducting a ping test for an MUs, see *Pinging Individual MUs on page 7-27.*

NOTE An echo test initiated from the access point **MU Stats Summary** screen uses WNMP pings. Therefore, target clients that are not Symbol MUs are unable to respond to the echo test.

5. Click the **MU Authentication Statistics** button to display a screen with detailed authentication statistics for the an MU.

   For information on individual MU authentication statistics, see *MU Authentication Statistics on page 7-28*.
6. Click the **MU Details** button to display a screen with detailed statistics for a selected MU.

   For detailed information on individual MU authentication statistics, see *Viewing MU Details on page 7-24.*
7. Click the **Clear All MU Stats** button to reset each of the data collection counters to zero in order to begin new data collections.
8. Click the **Logout** button to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

7.5.1 Viewing MU Details

Use the **MU Details** screen to display throughput, signal strength and transmit error information for a specific MU associated with the access point.

The MU Details screen is separated into four fields; *MU Properties*, *MU Traffic*, *MU Signal*, and *MU Errors*. The **MU Properties** field displays basic information such as hardware address, IP address, and associated WLAN and AP. Reference the **MU Traffic** field for MU RF traffic and throughput data. Use the **RF Status** field to reference information on RF signal averages from the target MU. The **Error** field displays RF traffic errors based on retries, dropped packets and undecryptable packets. The MU Details screen is view-only with no user configurable data fields.

To view details specific to an individual MU:

1. Select **Status and Statistics** -> **MU Stats** from the access point menu tree.
2. Highlight a specific MU.
3. Select the **MU Details** button.
4. Refer to the **MU Properties** field to view MU address information.

IP Address	Displays the IP address of the MU.
WLAN Association	Displays the name of the WLAN the MU is associated with. Use this information to assess whether the MU is properly grouped within that specific WLAN.
PSP State	Displays the current PSP state of the MU. The **PSP Mode** field has two potential settings. PSP indicates the MU is operating in Power Save Protocol mode. In PSP, the MU runs enough power to check for beacons and is otherwise inactive. CAM indicates the MU is continuously aware of all radio traffic. Symbol recommends CAM for those MUs transmitting with the AP frequently and for periods of time of two hours.
HW Address	Displays the *Media Access Control (MAC)* address for the MU.
Radio Association	Displays the name of the AP MU is currently associated with. If the name of the access point requires modification, see *Configuring System Settings on page 4-2*.
QoS Client Type	Displays the data type transmitted by the mobile unit. Possible types include **Legacy**, **Voice**, **WMM Baseline** and **Power Save**. For more information, see *Setting the WLAN Quality of Service (QoS) Policy on page 5-33*.
Encryption	Displays the encryption scheme deployed by the associated MU.

5. Refer to the **Traffic** field to view individual MU RF throughput information.

Packets per second

The **Total** column displays average total packets per second crossing the MU. The **Rx** column displays the average total packets per second received on the MU. The **Tx** column displays the average total packets per second sent on the MU. The number in black represents Pkts per second for the last 30 seconds and the number in blue represents Pkts per second for the last hour.

Throughput

The **Total** column displays the average total packets per second crossing the selected MU. The **Rx** column displays the average total packets per second received on the MU. The **Tx** column displays the average total packets per second sent on the MU. The number in black represents throughput for the last 30 seconds, the number in blue represents throughput for the last hour.

Avg. Bit Speed

The **Total** column displays the average bit speed in Mbps for a given time period on the MU. This includes all packets sent and received. The number in black represents average bit speed for the last 30 seconds and the number in blue represents average bit speed for the last hour. Consider increasing the data rate of the AP if the current bit speed does not meet network requirements. For more information, see *Configuring the 802.11a or 802.11b/g Radio on page 5-47*. The associated MU must also be set to the higher rate to interoperate with the access point at that data rate.

% of Non-unicast pkts

Displays the percentage of the total packets for the selected mobile unit that are non-unicast. Non-unicast packets include broadcast and multicast packets. The number in black represents packets for the last 30 seconds and the number in blue represents packets for the last hour.

6. Refer to the **RF Status** field to view MU signal and signal disturbance information.

Avg MU Signal

Displays RF signal strength in dBm for the target MU. The number in black represents signal information for the last 30 seconds and the number in blue represents signal information for the last hour.

Avg MU Noise

Displays RF noise for the target MU. The number in black represents noise for the last 30 seconds, the number in blue represents noise for the last hour.

Avg MU SNR Displays the *Signal to Noise Ratio (SNR)* for the target MU. The Signal to Noise Ratio is an indication of overall RF performance on your wireless network.

7. Refer to the **Errors** field to view MU retry information and statistics on packets not transmitted.

Avg Num of Retries Displays the average number of retries for the MU. The number in black represents average retries for the last 30 seconds and the number in blue represents average retries for the last hour.

Dropped Packets Displays the percentage of packets the AP gave up as not received on for the selected MU. The number in black represents the percentage of packets for the last 30 seconds and the number in blue represents the percentage of packets for the last hour.

% of Undecryptable Pkts Displays the percentage of undecryptable packets for the MU. The number in black represents the percentage of undecryptable packets for the last 30 seconds and the number in blue represents the percentage of undecryptable packets for the last hour.

8. Click **OK** to exit the screen.

7.5.2 Pinging Individual MUs

The access point can verify its link with an MU by sending WNMP ping packets to the associated MU. Use the **Echo Test** screen to specify a target MU and configure the parameters of the ping test.

NOTE An echo test initiated from the access point **MU Stats Summary** screen uses WNMP pings. Therefore, target clients that are not Symbol MUs are unable to respond to the echo test.

To ping a specific MU to assess its connection with an access point:

1. Select **Status and Statistics** - > **MU Stats** from the access point menu tree.
2. Select the **Echo Test** button from within the **MU Stats Summary** screen
3. Specify the following ping test parameters.

Station Address The IP address of the target MU. Refer to the **MU Stats Summary** screen for associated MU IP address information.

Number of ping — Specify the number of ping packets to transmit to the target MU. The default is 100.

Packet Length — Specify the length of each data packet transmitted to the target MU during the ping test. The default is 100 bytes.

Packet Data — Defines the data to be transmitted as part of the test.

4. Click the **Ping** button to begin transmitting ping packets to the station address specified.

   Refer to the **Number of Responses** parameter to assess the number of responses from the target MU versus the number of pings transmitted by the access point. Use the ratio of packets sent versus packets received to assess the link quality between MU and the access point

   Click the **Ok** button to exit the Echo Test screen and return to the MU Stats Summary screen.

7.5.3 MU Authentication Statistics

The access point can access and display authentication statistics for individual MUs.

To view access point authentication statistics for a specific MU:

1. Select **Status and Statistics** - > **MU Stats** from the access point menu tree.
2. Highlight a target MU from within the **MU List** field.
3. Click the **MU Authentication Statistics** button

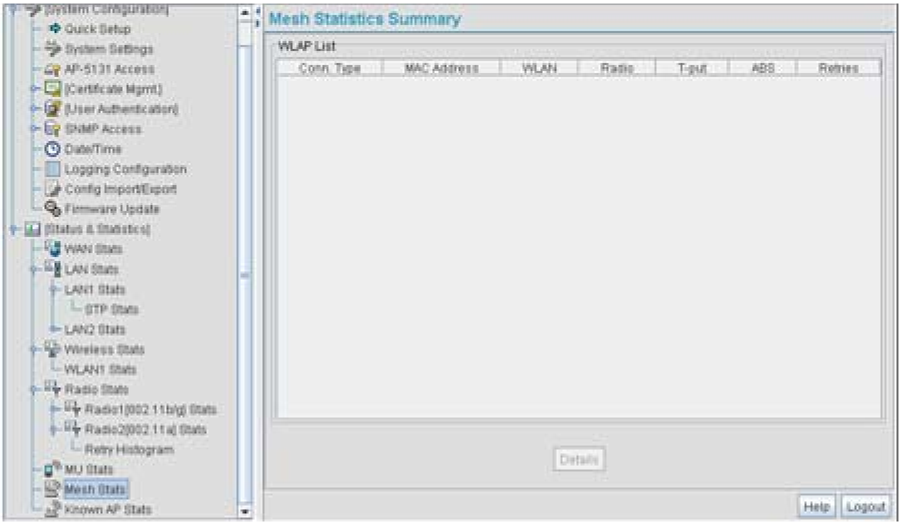
   Use the displayed statistics to determine if the target MU would be better served with a different access point WLAN or access point radio.
4. Click **Ok** to return to the MU Stats Summary screen.

7.6 Viewing the Mesh Statistics Summary

The access point has the capability of detecting and displaying the properties of other access points in mesh network (either base bridges or client bridges) mode. This information is used to create a list of known wireless bridges.

To view detected mesh network statistics:

1. Select **Status and Statistics** -> **Mesh Stats** from the access point menu tree.



Conn. Type	MAC Address	WLAN	Radio	T-put	ABS	Retries

The **Mesh Statistics Summary** screen displays the following information:

Conn Type Displays whether the bridge has been defined as a base bridge or a client bridge. For information on defining configuring the access point as either a base or client bridge, see *Configuring the AP-5131 Radio for Mesh Networking Support on page 9-10*.

MAC Address The unique 48-bit, hard-coded Media Access Control address, known as the devices station identifier. This value is hard coded at the factory by the manufacturer and cannot be changed.

WLAN Displays the WLAN name each wireless bridge is interoperating with.

Radio Displays the name of the 802.11a or 802.11b/g radio each bridge is associated with.

T-put	Displays the total throughput in Megabits per second (Mbps) for each associated bridge.
ABS	Displays the *Average Bit Speed (ABS)* in Megabits per second (Mbps) for each associated bridge.
Retries	Displays the average number of retries per packet. A high number retries could indicate possible network or hardware problems.

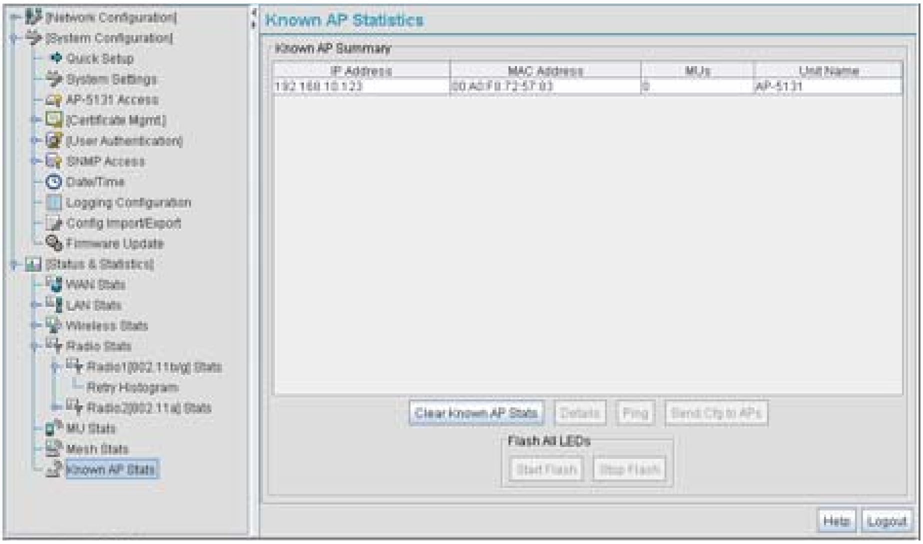
2. Click the **Refresh** button to update the display of the Mesh Statistics Summary screen to the latest values.
3. Click the **Details** button to display address and radio information for those access points in a client bridge configuration with this detecting access point.
4. Click the **Logout** button to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

7.7 Viewing Known Access Point Statistics

The access point has the capability of detecting and displaying the properties of other Symbol access points located within its coverage area. Detected access point's transmit a WNMP message indicating their channel, IP address, firmware version, etc. This information is used to create a known AP list. The list has field indicating the properties of the access point discovered.

To view detected access point statistics:

1. Select **Status and Statistics** -> **Known AP Stats** from the access point menu tree.



IP Address	MAC Address	MUs	Unit Name
192.168.10.123	00:A0:F8:72:57:03	0	AP-5131

The **Known AP Statistics** screen displays the following information:

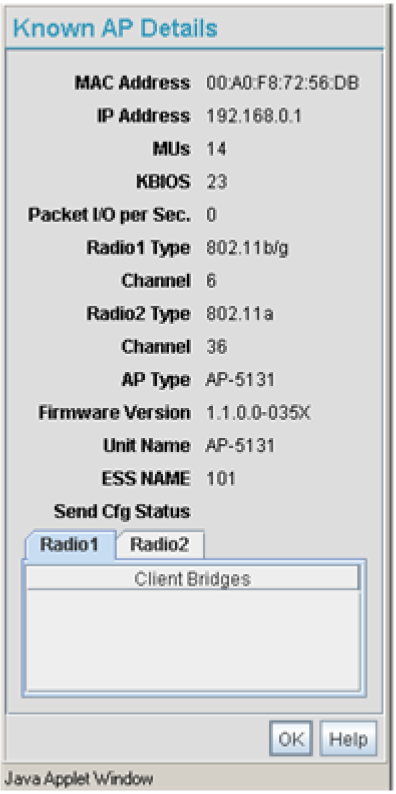
IP Address The network-assigned Internet Protocol address of the located AP.

MAC Address The unique 48-bit, hard-coded Media Access Control address, known as the devices station identifier. This value is hard coded at the factory by the manufacturer and cannot be changed.

MUs The number MUs associated with the located access point.

Unit Name Displays the name assigned to the access point using the System Settings screen. For information on changing the unit name, see *Configuring System Settings on page 4-2*.

2. Click the **Clear Known AP Stats** button to reset each of the data collection counters to zero in order to begin new data collections.
3. Click the **Details** button to display access point address and radio information.



Known AP Details

MAC Address	00:A0:F8:72:56:DB
IP Address	192.168.0.1
MUs	14
KBIOS	23
Packet I/O per Sec.	0
Radio1 Type	802.11b/g
Channel	6
Radio2 Type	802.11a
Channel	36
AP Type	AP-5131
Firmware Version	1.1.0.0-035X
Unit Name	AP-5131
ESS NAME	101
Send Cfg Status	

The Known AP Details screen displays the target AP's MAC address, IP address, radio channel, number of associated MUs, packet throughput per second, radio type(s), model, firmware version, ESS and client bridges currently connected to the AP radio. Use this informatiaccess point on to determine whether this AP provides better MU association support than the locating access point or warrants consideration as a member of a different mesh network.

4. Click the **Ping** button to display a screen for verifying the link with a highlighted Symbol access point.

✓ **NOTE** A ping test initiated from the access point **Known AP Statistics** screen uses WNMP pings. Therefore, target devices that are not Symbol access points are unable to respond to the ping test.

5. Click the **Send Cfg to APs** button to send the your access point's configuration to other access point's. The recipient access point must be the same single or dual-radio model as the access point sending the configuration. The sending and recipient access point's must also be running the same major firmware version (i.e., 1.1 to 1.1).

⚠ **CAUTION** When using the Send Cfg to APs function to migrate an access point's configuration to other access points, it is important to keep in mind mesh network configuration parameters do not get completely sent to other access points. The Send Cfg to APs function will not send the "auto-select" and "preferred list" settings. Additionally, LAN1 and LAN2 IP mode settings will only be sent if the sender's AP mode is DHCP or BOOTP. The WAN's IP mode will only be sent if the sender's IP mode is DHCP.

6. Click the **Start Flash** button to flash the LEDs of other access points detected and displayed within the Known AP Statistics screen.

   Use the **Start Flash** button to determine the location of the devices displayed within the Known AP Statistics screen. When an access point is highlighted and the Start Flash button is selected, the LEDs on the selected access point flash. When the **Stop Flash** button is selected, the LEDs on the selected access point go back to normal operation.

7. Click the **Logout** button to securely exit the access point Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

8

Command Line Interface Reference

The access point *Command Line Interface (CLI)* is accessed through the serial port or a Telnet session. The access point CLI follows the same conventions as the Web-based user interface. The CLI does, however, provide an “escape sequence” to provide diagnostics for problem identification and resolution.

The CLI treats the following as invalid characters:

```
|   "   &   ,   \    '    <    >
```

In order to avoid problems when using the CLI, these characters should be avoided.

8.1 Connecting to the CLI

8.1.1 Accessing the CLI through the Serial Port

To connect to the access point CLI through the serial port:

1. Connect one end of a null modem serial cable to the access point’s serial connector.
2. Attach the other end of the null modem serial cable to the serial port of a PC running HyperTerminal or a similar emulation program.
3. Set the HyperTerminal program to use 19200 baud, 8 data bits, 1 stop bit, no parity, no flow control, and auto-detect for terminal emulation.
4. Press <ESC> or <Enter> to enter into the CLI.
5. Enter the default username of **admin** and the default password of **symbol**. If this is your first time logging into the access point, you are unable to access any of the access point’s commands until the country code is set. A new password will also need to be created.

8.1.2 Accessing the CLI via Telnet

To connect to the access point CLI through a Telnet connection:

1. Telnet into the access point using an IP address of 192.168.0.1
2. Enter the default username of **admin** and the default password of **symbol**. If this is your first time logging into the access point, you are unable to access any of the access point’s commands until the country code is set. A new password will also need to be created.

8.2 Admin and Common Commands

AP51xx>admin>

Description:

Displays admin configuration options. The items available under this command are shown below.

Syntax:

help	Displays general user interface help.
passwd	Changes the admin password.
summary	Shows a system summary.
network	Goes to the network submenu
system	Goes to the system submenu.
stats	Goes to the stats submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

AP51xx>admin>help

Description:

Displays general CLI user interface help.

Syntax:

help Displays command line help using combinations of function keys for navigation.

Example:

```
admin>help

  ?                          : display command help - Eg. ?, show ?, s?
* Restriction of “?”:        : “?” after a function argument is treated
                             : as an argument
                             : Eg. admin<network.lan> set lan enable?
                             : (Here “?” is an invalid extra argument,
                             : because it is after the argument
                             : “enable”)

  <ctrl-q>                   : go backwards in command history
  <ctrl-p>                   : go forwards in command history

  * Note                     : 1) commands can be incomplete
                             : - Eg. sh = sho = show
                             : 2) “//” introduces a comment and gets no
                             : resposne from CLI.

admin>
```