

- 1 Configure the VNS filtering settings:
 - a In the **Filter ID** drop-down list, click one of the following:
 - **Authenticated** — Controls network access after the user has been authenticated.
 - **Non-authenticated** — Controls network access and to direct users to a Captive Portal Web page for login.
- 2 In the **Filter** table, select the **Enable** check box for the desired filters, then select the **Allow** or **Deny** option buttons for each filter as needed.
- 3 At the bottom of the Filter list, select **Allow** or **Deny** for **All Other Traffic**.
- 4 Click **Next**. The **Privacy** screen displays.

Creating a New GuestPortal VNS Using the VNS Wizard - Radio Assignment Screen

The **Radio Assignment** screen displays:

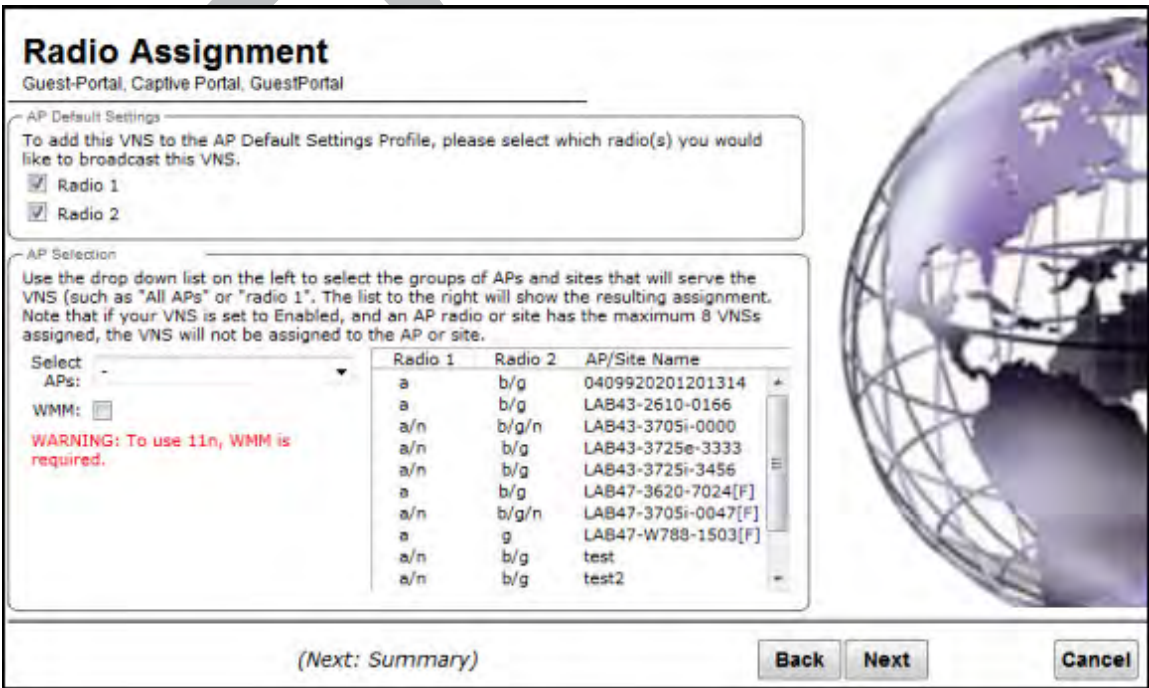


Table 101: Guest Portal Radio Assignment Page - Fields and Buttons

Field/Button	Description
AP Default Settings	
Radio 1 / Radio 2	Select the radios of the AP default settings profile that you want to broadcast the Captive Portal VNS.
AP Selection	

Table 101: Guest Portal Radio Assignment Page - Fields and Buttons (continued)

Field/Button	Description
Select APs	<p>Select the group of APs that will broadcast the Captive Portal VNS:</p> <ul style="list-style-type: none"> • all radios — Click to assign all of the APs' radios. • radio 1 — Click to assign only the APs' Radio 1. • radio 2 — Click to assign only the APs' Radio 2. • local APs - all radios — Click to assign only the local APs. • local APs - radio 1 — Click to assign only the local APs' Radio 1. • local APs - radio 2 — Click to assign only the local APs' Radio 2. • foreign APs - all radios — Click to assign only the foreign APs. • foreign APs - radio 1 — Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 — Click to assign only the foreign APs' Radio 2.
WMM	<p>(Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the outbound traffic for all WMM clients. WMM clients will also classify and prioritize the inbound traffic.</p>

Click **Next**. The **Summary** screen displays.

Creating a New GuestPortal VNS Using the VNS Wizard - Privacy Screen

The **Privacy** screen displays:

Privacy
Guest Portal, Captive Portal, GuestPortal

WARNING: To use 11n, Privacy can only be "None" or WPA v.2 with AES only Encryption

☐ None
 ☐ Static Keys (WEP)
 ☒ WPA - PSK

☐ WPA v.1
 Encryption: Auto

☐ WPA v.2
 Encryption: Auto

☒ Broadcast re-key interval: 3600 seconds (30 - 86400 seconds)

Input Method: ☒ Input String ☐ Input Hex
 Pre-shared key String:
 (min 8 characters; max 63)

(Next: RF)

Table 102: Guest Portal Privacy Page - Fields and Buttons

Field/Button	Description
None	Select if you do not want to assign any privacy mechanism.
Static Keys (WEP)	<p>Select to configure static keys. Then enter:</p> <ul style="list-style-type: none"> • WEP Key Index — Click the WEP encryption key index: 1, 2, 3, or 4. <p>Specifying the WEP key index is supported only for AP37XX wireless APs.</p> <ul style="list-style-type: none"> • WEP Key Length — Click the WEP encryption key length: 64 bit, 128 bit, or 152 bit. <p>Select an Input Method:</p> <ul style="list-style-type: none"> • Input Hex — type the WEP key input in the WEP Key box. The key is generated automatically based on the input. • Input String — type the secret WEP key string used for encrypting and decrypting in the WEP Key String box. The WEP Key box is automatically filled by the corresponding Hex code.
WPA-PSK	<p>Select to use a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK (Wi-Fi Protected Access Pre-Shared key) is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office.</p> <p>To enable WPA v1 encryption, select WPA v.1. In the Encryption drop-down list, select one of the following encryption types:</p> <ul style="list-style-type: none"> • Auto — The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • TKIP only — The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP. <p>To enable WPA v2 encryption, select WPA v.2. In the Encryption drop-down list, click one of the following encryption types:</p> <ul style="list-style-type: none"> • Auto — The AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • AES only — The AP advertises CCMP as an available encryption protocol. It will not advertise TKIP. <p>To enable re-keying after a time interval, select Broadcast re-key interval. If this check box is not selected, the Broadcast encryption key is never changed and the AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications.</p> <p>In the Broadcast re-key interval box, type the time interval after which the broadcast encryption key is changed automatically.</p> <p>To enable the group key power save retry, select Group Key Power Save Retry.</p> <p>The group key power save retry is supported only for AP37XX wireless APs.</p>

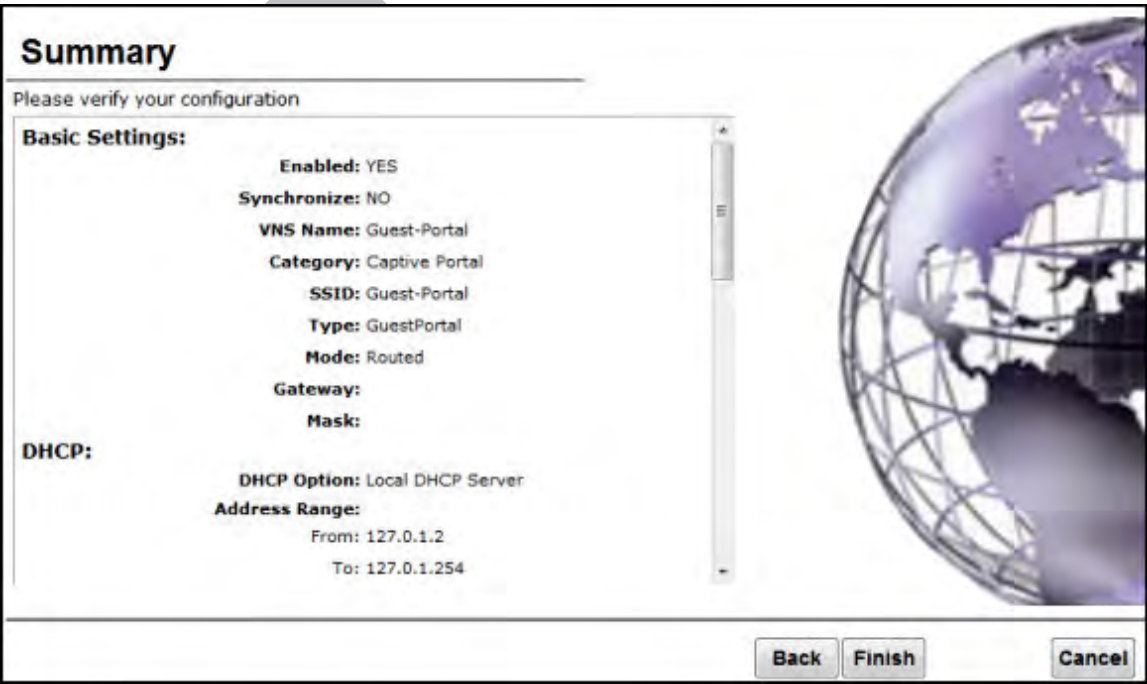
Table 102: Guest Portal Privacy Page - Fields and Buttons (continued)

Field/Button	Description
	In the Pre-shared key box, type the shared secret key to be used between the wireless device and AP. The shared secret key is used to generate the 256-bit key. Mask/Unmask — Click to display or hide your shared secret key.

Click **Next**. The **Radio Assignment** screen displays.

Creating a New GuestPortal VNS Using the VNS Wizard - Summary Screen

The **Summary** screen displays:



- 1 Confirm your VNS configuration. To revise your configuration, click **Back**.
- 2 To create your VNS, click **Finish**, and then click **Close**.
If the controller is configured to be part of an availability pair, you can chose to synchronize the VNS on the secondary controller.
- 3 If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Enabling and Disabling a VNS

By default, when a new VNS is created, the VNS is added to the system as an enabled VNS. A VNS can be enabled or disabled. Disabling a VNS provides the ability to temporarily stop wireless service on a VNS. The disabled VNS configuration remains in the database for future use.

The controller can support the following VNSs:

Table 103: ExtremeWireless Appliance Active and Defined VNS Support

Platform	Active VNSs	Defined VNSs
C5110	128	256
C5210	128	256
C5215	128	256
C4110	64	128
C25	16	32
C35	16	32
V2110 (Small)	16	32
V2110 (Medium)	64	128
V2110 (Large)	128	256

To enable or disable a VNS:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, expand the **Virtual Networks** pane and select the VNS to enable or disable.
- 3 On the **Core** tab, in the Status box, select or de-select the **Enable** check box.
- 4 Click **Save**. The VNS is enabled or disabled accordingly.

Renaming a VNS

To rename a VNS:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **Virtual Networks** pane, then select the VNS you want to rename.
- 3 On the **Core** tab, in the **VNS Name** field, enter the new name.
- 4 Click **Save**. The VNS is renamed.

Deleting a VNS

You can delete a VNS that is no longer necessary.

To delete a VNS:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **Virtual Networks** pane, then select the VNS you want to rename.
- 3 On the **Core** tab, click the **Delete** button. A pop-up window prompts you to confirm you want to delete the VNS. Click **OK**.
- 4 Click **Save**. The VNS is deleted.

9 Configuring Classes of Service

Classes of Service Overview
Configuring Classes of Service
CoS Rule Classification
Priority and ToS/DSCP Marking
Rate Limiting

Classes of Service Overview

In general, *CoS (Class of Service)* refers to a set of attributes that define the importance of a frame while it is forwarded through the network relative to other packets, and to the maximum throughput per time unit that a station or port assigned to a specific role is permitted. For more information on configuring roles, see [Configuring Default VLAN and Class of Service for a Role](#) on page 284.

The CoS defines actions to be taken when rate limits are exceeded.

All incoming packets may follow these steps to determine a CoS:

- Classification - identifies the first matching rule that defines a CoS.
- Marking - modifies the L2 802.1p and/or L3 ToS based on CoS definition.
- Rate limiting (drop) is set.
- Transmit queue assignment.

Configuring Classes of Service

The *CoS* feature is a configuration entity containing QoS Marking (802.1p and ToS/DSCP), Inbound/Outbound Rate Limiting and Transmit Queue Assignments. The CoS ToS marking capability allows for NAC-based redirection to different captive portals on the same *WLAN (Wireless Local Area Network)* Service.

The supported CoS attributes are enforced on the controller (data plane) and on the APs.

To configure Classes of Service:

- 1 From the top menu, click **VNS**.

- 2 In the left pane click **Classes of Service**.

Logs

Reports

Controller

AP

VNS

WIPS

Classes of Service

	Name	802.1p	ToS/DSCP	Inbound Rate Profile	Outbound Rate Profile	TXQ
<input type="checkbox"/>	No CoS	-	-	-	-	-
<input type="checkbox"/>	Scavenger	0	-	-	-	-
<input type="checkbox"/>	Best Effort	1	-	-	-	1
<input type="checkbox"/>	Bulk Data	2	-	-	-	2
<input type="checkbox"/>	Critical Data	3	-	-	-	3
<input type="checkbox"/>	Network Control	4	-	-	-	4
<input type="checkbox"/>	Network Management	5	-	-	-	5
<input type="checkbox"/>	RTP/Voice/Video	6	-	-	-	6
<input type="checkbox"/>	High Priority	7	-	-	-	7

New

Delete Selected

Note



"No CoS" means that the traffic to which it is assigned will not be remarked, the controller software will decide the appropriate transmit queue and no rate limits will be applied on traffic traveling to or from the station to which the CoS is applied. The "No CoS" CoS is predefined and cannot be removed.

- 3 In the left pane, click the name of the Classes of Service that you want to edit.

The **Class of Service** configuration page displays. By default, the **General** tab displays. [Table 104](#) describes the fields and buttons on the **General** tab.

Alternately, click the **New** button to create a new CoS.

Logs	Reports	Controller	AP	VNS	WIPS
------	---------	------------	----	-----	------

Class of Service:

General

Core

Name:

Marking

☐ Use Legacy Priority Override defined in the WLAN Service

☐ **802.1p Priority:**

☐ **ToS/DSCP:** 0x (DSCP:) **Mask:** 0x

Rate Limiting

☐ **Inbound Rate Limit:**

☐ **Outbound Rate Limit:**

Transmit Queue Assignment

☐ **Transmit Queue:**

Table 104: General Tab - Fields and Buttons

Field/Button	Description
Core	
Name	Enter a name to assign to this class of service.
Marking	
Use Legacy Priority Override defined in the WLAN Service	Priority override allows you to define and force the traffic to a desired priority level. Priority override can be used with any combination. You can configure the service class and the DSCP values. Select this check box to use Priority Override defined in the WLAN as in previous releases. For more information, see Configuring the Priority Override on page 370.
802.1p Priority	<p>Select this check box to define how the Layer 2 priority of the packet will be marked. From the drop-down list, select Priority 0 to Priority 7. For more information, see Priority and ToS/DSCP Marking on page 491.</p> <p>Note: This selection is not available if Legacy Priority Override is checked.</p>

Table 104: General Tab - Fields and Buttons (continued)

Field/Button	Description
ToS/DSCP Marking	<p>Select this check box to define how the Layer 3 ToS/DSCP will be marked.</p> <p>Enter a hexadecimal value in the 0x (DSCP:) field, or</p> <p>Click the Select button to open the ToS/DSCP Configuration dialog. For more information, see Configuring ToS/DSCP Marking on page 491.</p> <p>Note: This selection is not available if Legacy Priority Override is checked.</p>
Mask: 0x	<p>Displays the hexadecimal value to use for the ToS/DSCP value. For example, if the mask is 0xF0, then only the four most significant bits of the ToS of the received packets are marked. So, if the received ToS is 0x33 and the ToS marking is set to 0x2A, then the resulting ToS is 0x22.</p>
Rate Limiting	
Inbound Rate Limit	<p>Select this check box, and then select an inbound rate limit from the drop-down list or click the New button to create a new inbound rate limit profile.</p> <p>To edit an existing inbound rate limit profile, select the profile from the drop-down list and then click the Edit button.</p> <p>For more information, see Rate Limiting on page 492.</p>
Outbound Rate Limit	<p>Select this check box, and then select an outbound rate limit from the drop-down list or click the New button to create a new outbound rate limit profile.</p> <p>To edit an existing outbound rate limit profile, select the profile from the drop-down list and then click the Edit button.</p> <p>For more information, see Rate Limiting on page 492.</p>
Transmit Queue Assignment	
Transmit Queue	<p>Select this check box, and select a Transmit Queue from the drop-down list.</p> <p>The Transmit Queue assignment is an override to the default TXQ assignment specified in the 802.1p priority, but without remarking the actual 802.1p field.</p>

CoS Rule Classification

Classification is the process of finding the first matching rule that defines a CoS for an incoming packet. The order of classification is as follows:

- 1 Use the CoS assigned by the first role rule matched by the packet that explicitly assigns a CoS.
- 2 If no CoS found, use the default CoS of the Role.
- 3 If still no CoS found, use the default CoS of the WLAN (for non-auth role).

For inbound traffic, classification is done at the AP (if AP Filtering is enabled), otherwise it is done at the controller. For outbound traffic, classification is always done at the controller.

The Rule that assigns authorization (Access Control) may not be the same rule that assigns CoS. Therefore, up to two passes are made through the policy rules for each packet. If the first pass results in the packet being allowed a second pass will take place to classify the packet for CoS.

- The first pass looks for authorization (allow, deny).
- The second pass classifies and assigns the CoS.

The number of rules reported to Policy Manager are limited to the number of rules allowed on the controller. On the controller, a single rule can contain different classification types whereas for Policy Manager this rule may be split into several rules. For example, if a rule defines an IP source address and also a ToS value, then this rule would be split into an IP type and a ToS type. Rules exceeding the limit after splitting will be dropped.

Priority and ToS/DSCP Marking

After packets are classified, they are assigned a final User Priority (UP) value. The Priority and ToS/DSCP Marking bits to be applied to the packet is taken from the CoS and if not set, the received value (ToS/DSCP) is used. ToS/DSCP Marking rewrites the Layer 3 Type of Service (ToS) byte.

Configuring ToS/DSCP Marking

To configure ToS/DSCP marking:

- 1 From the **Class of Service General** tab, click **ToS/DSCP Marking**.
- 2 Click the **Select** button.

The **ToS/DSCP Configuration** dialog displays:



Note

Select either **Type of Service (ToS)** or **Diffserv Codepoint (DSCP)** from this dialog. You cannot configure both types.

- 3 If you select **Type of Service (ToS)**:
 - a Select a Precedence value from the drop-down list.
 - b Select a specific ToS from the following list:
 - Delay Sensitive
 - High Throughput
 - High Reliability
 - Explicit Congestion Notification
- 4 If you select **Diffserv Codepoint (DSCP)**:
 - Choose a Well-known Value, or
 - Enter a Raw Binary Value

5 Close the **Configuration** dialog.

The logic used to find the final User Priority (UP) depends on the CoS, the received UP, or the final ToS/DSCP value. Here are the steps followed to determine the final UP:

- 6 Use UP markings defined in CoS (directly or via Legacy UP override).
- 7 If still no UP, use UP from the received packet.
- 8 If still no UP, use DSCP marking defined in CoS and map to UP with WLANs DSCP-to-UP mapping table.
- 9 If still no UP, use received DSCP value and map to UP with WLANs DSCP-to-UP mapping table.

Rate Limiting

The Inbound and Outbound Rate Limit is enforced on a per-station basis whether the rate limit is assigned to a rule, role or WLAN. Each station has its own set of counters that are used to monitor its wireless network utilization. Traffic from other stations never count against a station's rate limits.

- Controllers support up to 128 system wide rate profiles when managed from the controller.
- Each role can use a maximum of 9 inbound rate profiles and 9 outbound rate profiles. For each direction there can be one rate profile assigned by the role's default CoS and 8 other rate profiles assigned by the role's rules.
- There is no limit to how many rules allow CoS assignments as long as there are never more than 8 + 8 rate profiles assigned by Classes of Service.

If two or more rules in the same role assign the same named rate profile to a station's packets, then those rules "share" the rate profile. In [Figure 147](#), a role's rules assign both HTTP and FTP traffic to the same rate limiter. The sum of the amounts of HTTP and FTP traffic determine whether the rate limit is being exceeded. Each station gets its own set of rate limiters. So the HTTP and FTP traffic of other stations never gets counted against a station's own rate profile limits.

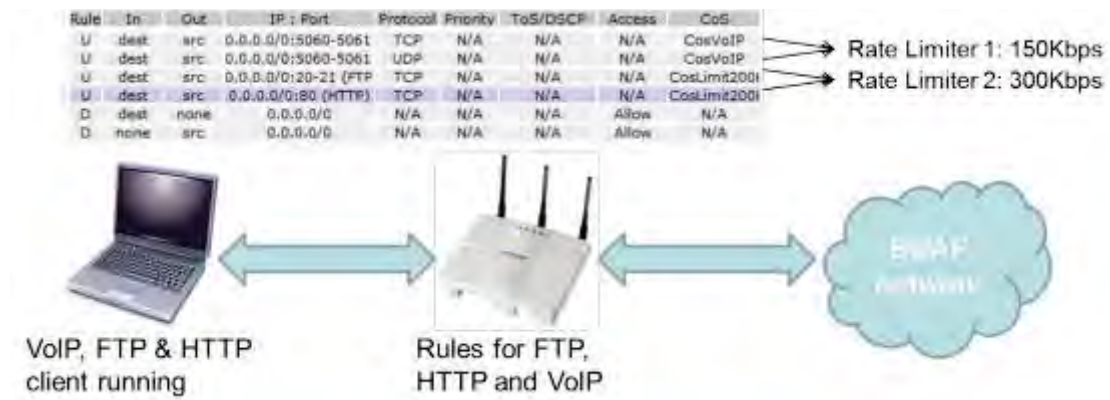


Figure 147: Rate Limiter Example

10 Configuring Sites

VNS Sites Overview
Configuring Sites
Recommended Deployment Guidelines
Radius Configuration
Selecting AP Assignments
Selecting WLAN Assignments

VNS Sites Overview

A Site is a mechanism for grouping APs and refers to specific Roles, *CoS (Class of Service)* and RADIUS servers that are grouped to form a single configuration. Sites allow for deployment where the authentication server is local and provides the ability to associate a new 802.1x client and to allow 802.1x clients to roam with Fast Roaming when the AP's home controller is unreachable.

When configuring a Site profile, two additional tabs are included:

- An AP Assignments tab provides a list of APs that can be assigned to a specific Site. Once an AP is assigned, the controller preloads the APs with the server configuration used by the Site.
- A *WLAN (Wireless Local Area Network)* Assignments tab lists available WLAN Services and specific radio assignments. WLAN Services can be assigned in the same way as AP Load Groups (see [Configuring Co-Located APs in Load Balance Groups](#) on page 213).

The number of sites supported on each controller model is equal to the number of APs supported. For more information, see [Table 4](#) on page 30.

Configuring Sites

Topology groups for sites is not supported. You can add a *WLAN* or Role to a site if it does not use a topology group. You can change the configuration of a WLAN, Role, and VNS to use a topology group, but if the WLAN, Role, or VNS is part of the Site configuration, the Site configuration will become invalid. At that point, you must remove the topology group related configuration from the site configuration.

A site can also use any Bridged at AP, Bridged at Controller, or Routed Topology defined in the controller. Once an AP is assigned to a site, the controller will preload the AP with Topologies, Roles, *CoS* and RADIUS server configuration used by the site. The AP will then be able to use these configuration items even when the controller is unreachable.

An AP that is part of a site that has local RADIUS client services enabled will use its own RADIUS client to do the following:

- Perform all MAC-based authentication for all stations associated with it on any of the WLAN Services assigned to it.

- Perform all RADIUS server interactions for 802.1x authentications for all stations associated with it on any 802.1x WLAN Service assigned to it.
- Perform all user authentication for all stations associated with it on any of the FF-ECP WLAN Services required user authentication.

Recommended Deployment Guidelines

The Sites feature introduces new and complex interactions between hardware and software components. Sites are recommended for customers who have an AP-to-controller link (in a normal deployment) which they expect will be disconnected for long periods of time, but still expect to give service to users.



Note

For best performance and maintainability, do not use the Sites feature if the AP-to-controller link is normally connected.

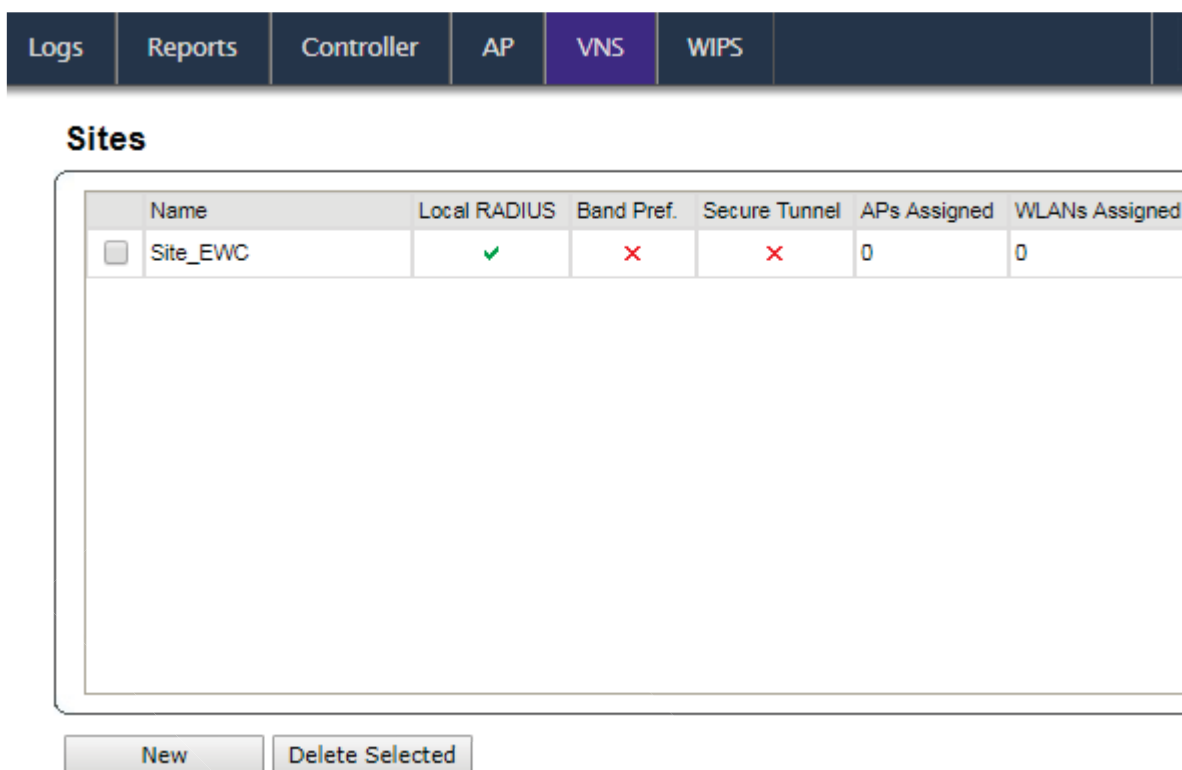
The following guidelines are recommended to configure a secure and easy-to-maintain Site:

- Use 802.1x and WPA2 Enterprise authentication and privacy.
- Do not use MAC-based authentication (MBA) unless absolutely required.
- Do not use more than 32 policy rules within a single AP filter.
- Do not configure a Sites AP Session Availability function without an AP-to-controller link.
- Do not configure the following features in a Sites configuration since they rely on a consistent AP-to-controller link:
 - Tunneled/Routed topologies
 - RADIUS accounting
 - Captive Portal

Defining Roles, CoS, and RADIUS Servers for Local RADIUS Authentication

- 1 From the top menu, click **VNS**.

- 2 In the left pane, click **Sites**. The **Sites** screen displays.



The screenshot shows the 'Sites' configuration screen. At the top is a navigation bar with tabs: Logs, Reports, Controller, AP, VNS (selected), and WIPS. Below the navigation bar is the 'Sites' section header. Underneath is a table with the following columns: Name, Local RADIUS, Band Pref., Secure Tunnel, APs Assigned, and WLANs Assigned. The table contains one entry: Site_EWC, with a green checkmark for Local RADIUS, red X's for Band Pref. and Secure Tunnel, and 0 for APs Assigned and WLANs Assigned. Below the table are two buttons: 'New' and 'Delete Selected'.

	Name	Local RADIUS	Band Pref.	Secure Tunnel	APs Assigned	WLANs Assigned
<input type="checkbox"/>	Site_EWC	✓	✗	✗	0	0

New Delete Selected

- 3 In the left pane, click the name of the Site that you want to edit, or click the **New** button to create a new Site. The **Site** configuration page displays. By default, the **Configuration** tab displays. Table 105 describes the fields and buttons on the Configuration tab.

Table 105: Configuration Tab - Fields and Buttons

Field/Button	Description
Site Name	Enter a name to assign to this Site. The name is unique among Sites on the controller. AP load group names and Site names are part of the same space so a load group and a Site cannot have the same name.
Local Radius Authentication	Select this check box to choose a local RADIUS Server for login credentials and authentication.
Default DNS Server	This field is used to resolve RADIUS server names to IP addresses if necessary.

Table 105: Configuration Tab - Fields and Buttons (continued)

Field/Button	Description
Roles to download to member APs	Select roles that will be applied to APs with this specific Site configuration. Physical topologies and third party AP enabled topologies cannot be assigned to a Site.
CoS to download to member APs	Displays the Class of Service that will be applied to APs with this specific Site configuration.
RADIUS Server used	Displays the list of available RADIUS servers used for this Site (for more information, see Radius Configuration on page 499). The RADIUS servers assigned to a Site override the list of RADIUS servers in the WLAN Service definition for APs that are part of the Site.
Status: Synchronize: (unknown)	Select this check box to enable automatic synchronization with an availability peer. Refer to Using the Sync Summary on page 414 for information about viewing synchronization status. If this Site is part of an availability pair, Extreme Networks recommends that you enable this feature.
Advanced Button	
Secure Tunnel	<p>This feature, when enabled, provides encryption, authentication, and key management between the AP and/or controllers.</p> <p>Select the desired Secure Tunnel mode from the drop-down list:</p> <p>Disabled — Secure Tunnel is turned off and no traffic is encrypted. All SFTP/SSH/TFTP traffic works normally.</p> <p>Encrypt control traffic between AP & Controller — An IPSEC tunnel is established from the AP to the controller and all SFTP/SSH/TFTP/WASSP control traffic is encrypted. The AP skips the registration and authentication phases and when selected, the Secure Tunnel Lifetime feature can be configured.</p> <p>Encrypt control and data traffic between AP & Controller — This mode only benefits routed/bridged@AP Controller Topologies. An IPSEC tunnel is established from the AP to the controller and all SFTP/SSH/TFTP/WASSP control and data traffic is encrypted. The AP skips the registration and authentication phases, and when selected, the Secure Tunnel Lifetime feature can be configured.</p> <p>Note: This option is not available for AP3805 models.</p> <p>Debug mode — An IPSEC tunnel is established from the AP to the controller, no traffic is encrypted, and all SFTP/SSH/TFTP traffic works normally. The AP skips the registration and authentication phases and when selected, the Secure Tunnel Lifetime feature can be configured.</p> <p>Note: Changing a Secure Tunnel mode will automatically disconnect and reconnect the AP.</p>
Secure Tunnel Lifetime	<p>When Secure Tunnel is enabled, enter an interval (in hours) at which time the keys of the IPSEC tunnel are renegotiated. Only applies if both the AP and controller are running V8.31 or newer.</p> <p>Note: Changing the Secure Tunnel Lifetime setting will not cause any AP disruption.</p>

Table 105: Configuration Tab - Fields and Buttons (continued)

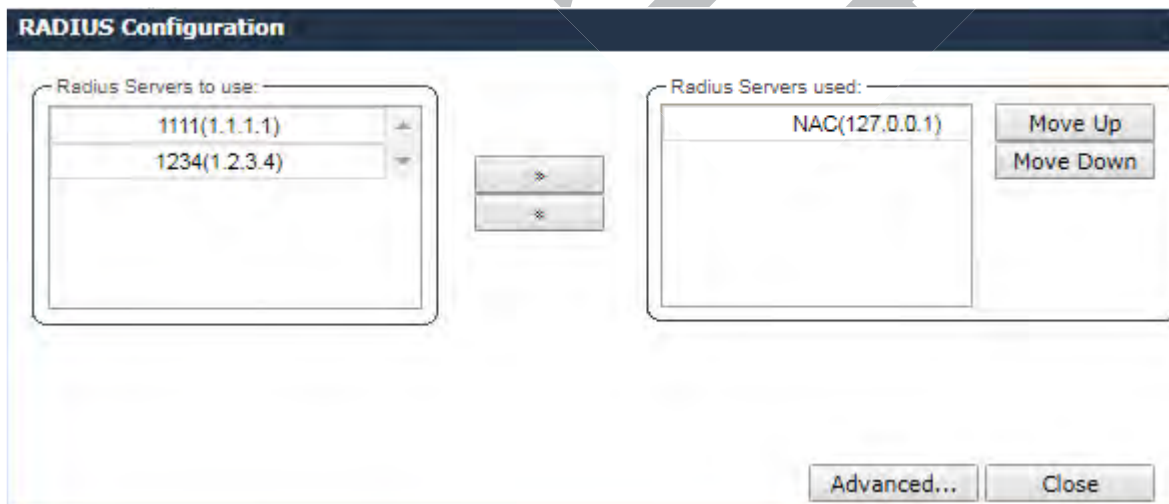
Field/Button	Description
Encrypt control traffic between APs	Select check box to provide encryption, authentication, and key management between APs and/or controllers.
Band Preference	Select this check box to enable APs to become members of both this Site and a load group at the same time.
Load Control	Select the following parameters for each radio assigned to this Site: <ul style="list-style-type: none"> • Enable: Select this check box to enable Radio Load Control (RLC) for individual radios (Radio1 and Radio2) associated with this Site. • Max. # of Clients: Enter the maximum number of clients for Radio 1 and Radio 2. The default limit is 60. The valid range is: 5 to 60. • Strict Limit: Select this check box to enable a strict limit on the number of clients allowed on a specific radio, based on the max # of clients allowed. Limits can be enforced separately for radio1 and radio 2.
RADIUS Authentication: Replace Called Station ID with Zone	Select this check box to allow the RADIUS client to send the AP Zone as the Called-Station ID instead of the radio MAC address. This feature can be enabled regardless of whether the Site is using centrally located or local RADIUS servers.

Radius Configuration

A single Site definition can be configured with one or two RADIUS servers. The RADIUS servers assigned to a Site can only be selected from the list of servers displayed on the **RADIUS Configuration** dialog.

To select site RADIUS servers:

- 1 From the **Configuration** tab, under RADIUS Server used, click **Configure**. The RADIUS Configuration dialog displays.



- 2 Select a RADIUS server from the list of available servers and click the right-arrow button.

The server will be moved under the RADIUS Servers used list.

- 3 Click the **Move Up** or **Move Down** buttons to change the order of the RADIUS Servers used.
- 4 Click the **Advanced** button. The **RADIUS Advanced Configuration** dialog appears.

RADIUS Advanced Configuration [?] [X]

NAS IP Address: ☒ Use VNS IP address or use:

NAS identifier: ☒ Use VNS name or use:

Auth. type:

Password:

Note: RADIUS Password override is for MBA only

- 5 The following values can be edited:
 - NAS IP Address — Click the check box to use the existing IP address of the VNS server, or enter an alternate IP Address in the box provided.
 - NAS Identifier — Click the check box to use the name of the existing VNS server, or enter an alternate name in the box provided.
 - Auth. type — Select an authorization protocol from the drop-down list (PAP, CHAP, MS-CHAP, or MS-CHAP2).
 - Password — To override the default password (see [VNS Global Settings](#) on page 392) for MBA - MAC Based authorization only. Select Mask to display the password, and select Unmask to hide the entry.
- 6 Click **Close**.

Selecting AP Assignments

To select AP assignments:

- 1 Go to **VNS > Sites**.
- 2 Select a site and click the **AP Assignments** tab.

- 3 Select the APs to apply to the Site configuration.

Logs	Reports	Controller	AP	VNS	WIPS
------	---------	------------	----	-----	------

Site: Site_EWC

Configuration	AP Assignments	WLAN Assignments
---------------	----------------	------------------

AP Name	
14300167085D0000[F]	<input type="checkbox"/>
1548Y-1007900000	<input type="checkbox"/>

Selecting WLAN Assignments

To select WLAN Assignments:

- 1 Go to **VNS > Sites**.
- 2 Select a site and click the **WLAN Assignments** tab.
- 3 Select Radio assignments (Radio 1 and Radio 2) for specific WLANs that will be applied to this Site configuration.
- 4 Click **Save**.

Reports	Controller	AP	VNS	WIPS	Help
---------	------------	----	-----	------	------

[Logout](#)

Site: Site_EWC

Configuration	AP Assignments	WLAN Assignments
---------------	----------------	------------------

WLAN Name	Airtime (%)	Radio 1	Radio 2	Ports
Lab46-WPA	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> P1/CAM <input type="checkbox"/> P2 <input type="checkbox"/> P3

11 Working with a Mesh Network

About Mesh

Simple Mesh Configuration

Wireless Repeater Configuration

Wireless Bridge Configuration

Examples of Deployment

Mesh WLAN Services

Key Features of Mesh

Deploying the Mesh System

Changing the Pre-shared Key in a Mesh WLAN Service

About Mesh

Mesh networks enable you to expand the wireless network by interconnecting the wireless APs through wireless links in addition to the traditional method of interconnecting wireless APs via a wired network. In a Mesh deployment, each node not only captures and disseminates its own data, but it also serves as a relay for other nodes, that is, it collaborates to propagate the data in the network.

A Mesh deployment is ideally suited for locations where installing Ethernet cabling is too expensive, or physically impossible.

The Mesh network can be deployed in three configurations:

- Simple Mesh Configuration
- Wireless Repeater Configuration
- Wireless Bridge Configuration

Simple Mesh Configuration

In a typical Mesh configuration, the APs are connected to the distribution system via an Ethernet network, which provides connectivity to the ExtremeWireless Appliance.

However, when an AP is installed in a remote location and can't be wired to the distribution system, an intermediate AP is connected to the distribution system via the Ethernet link. This intermediate AP forwards and receives the user traffic from the remote AP over a radio link.

The intermediate AP that is connected to the distribution system via the Ethernet network is called Mesh portal, and the AP that is remotely located is called the Mesh AP.

Figure 148 illustrates the Simple Mesh configuration:

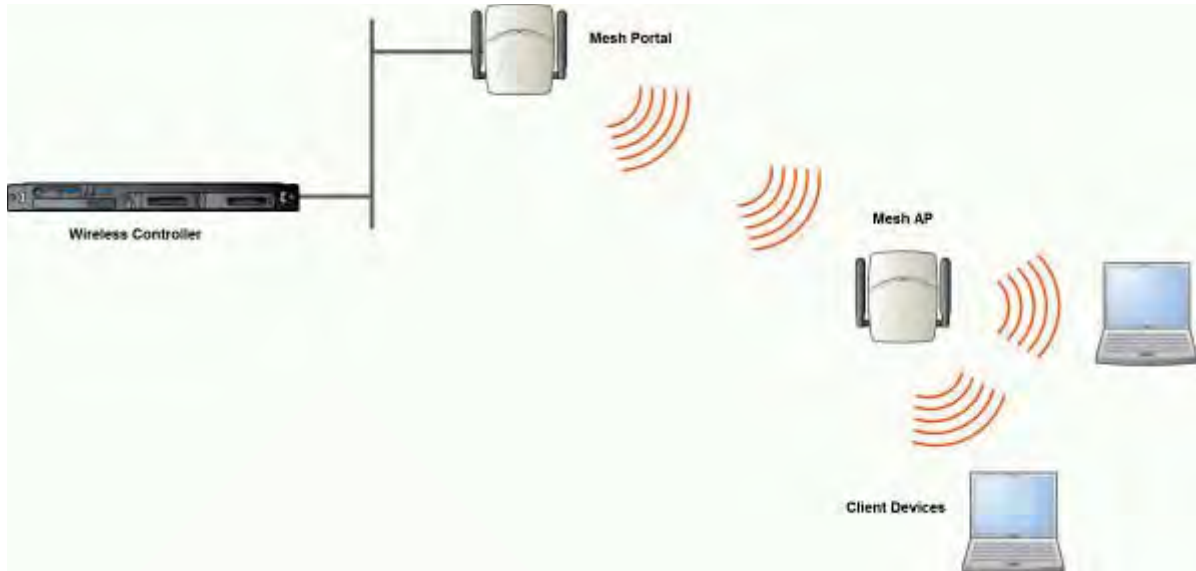


Figure 148: Simple Mesh Configuration

Wireless Repeater Configuration

In Wireless Repeater configuration, a Mesh AP is installed between the Mesh Portal and the destination Mesh AP. The Mesh AP relays the user traffic between the Mesh Portal and the destination Mesh AP. This increases the *WLAN (Wireless Local Area Network)* range.

Figure 149 illustrates the Wireless Repeater configuration:

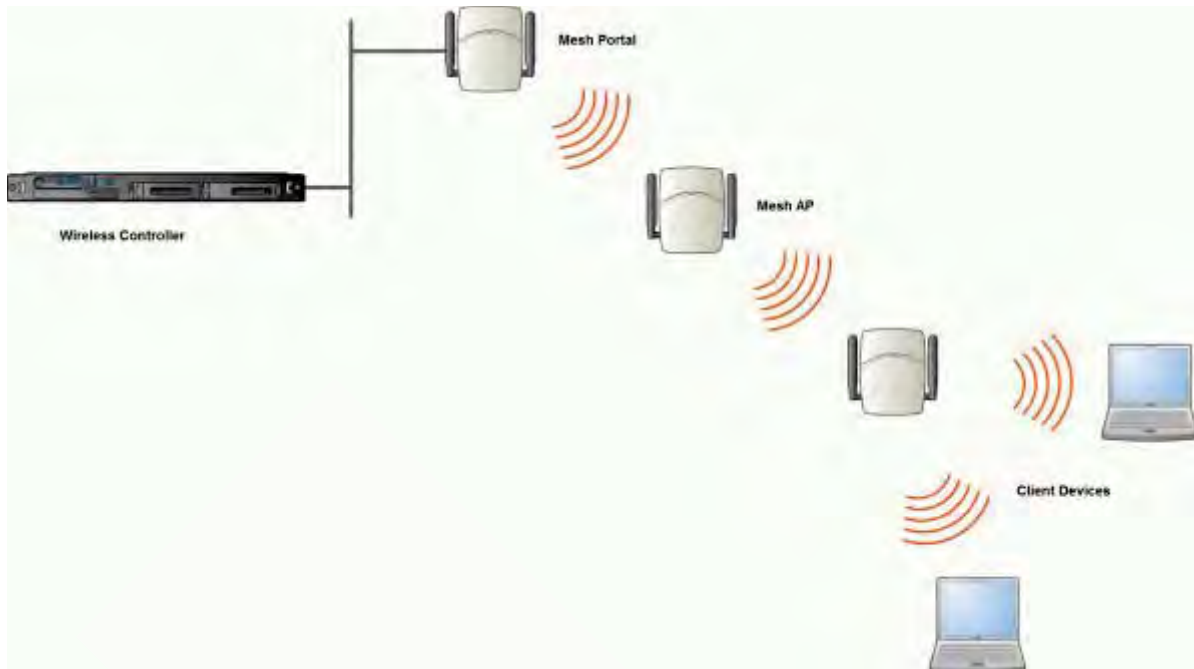


Figure 149: Wireless Repeater Configuration



Note

You should restrict the number of repeater hops in a Wireless Repeater configuration to three for optimum performance.

Wireless Bridge Configuration

In Wireless Bridge configuration, the traffic between two APs that are connected to two separate wired LAN segments is bridged via Mesh link. You may also install a Mesh AP between the two Wireless APs connected to two separate LAN segments.



Figure 150: Wireless Bridge Configuration

When you are configuring the Wireless Bridge configuration, you must specify on the user interface that the Mesh AP is connected to the wired LAN.

Examples of Deployment

The following illustration depicts a few examples of Mesh deployment.

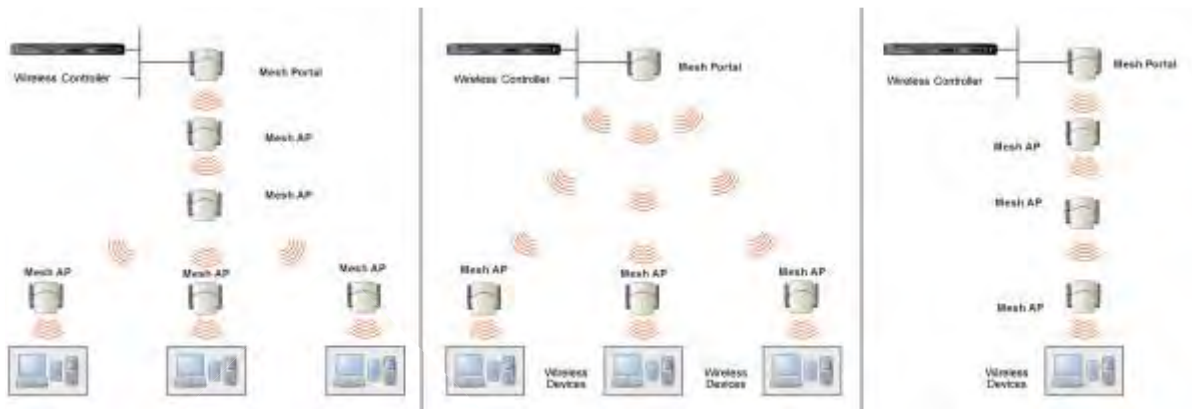


Figure 151: Examples of Mesh Deployment

Mesh WLAN Services

In a traditional WLAN deployment, each radio of the AP can interact with the client devices on a maximum of eight networks.

In Mesh deployment, one of the radios of every Mesh AP establishes a Mesh link on an exclusive WLAN Service. The Mesh AP is therefore limited to seven network WLAN Services on the Mesh radio. The other radio can interact with the client devices on a maximum of eight WLAN Services.

The WLAN Service on which the APs establish the Mesh link is called the Mesh WLAN Service.

A Mesh can be setup either by using either a single Mesh WLAN Service or multiple Mesh WLAN Services. The following figures illustrate the point.

In [Figure 152](#) on page 506:

- The rectangular enclosure denotes an office building.
- The four wireless APs — Minoru, Yosemite, Bjorn and Lancaster — are within the confines of the building and are connected to the wired network.
- The space around the office building is a warehouse.
- The solid arrows point towards Current Parents.
- The dotted arrows point towards Alternative Parents.

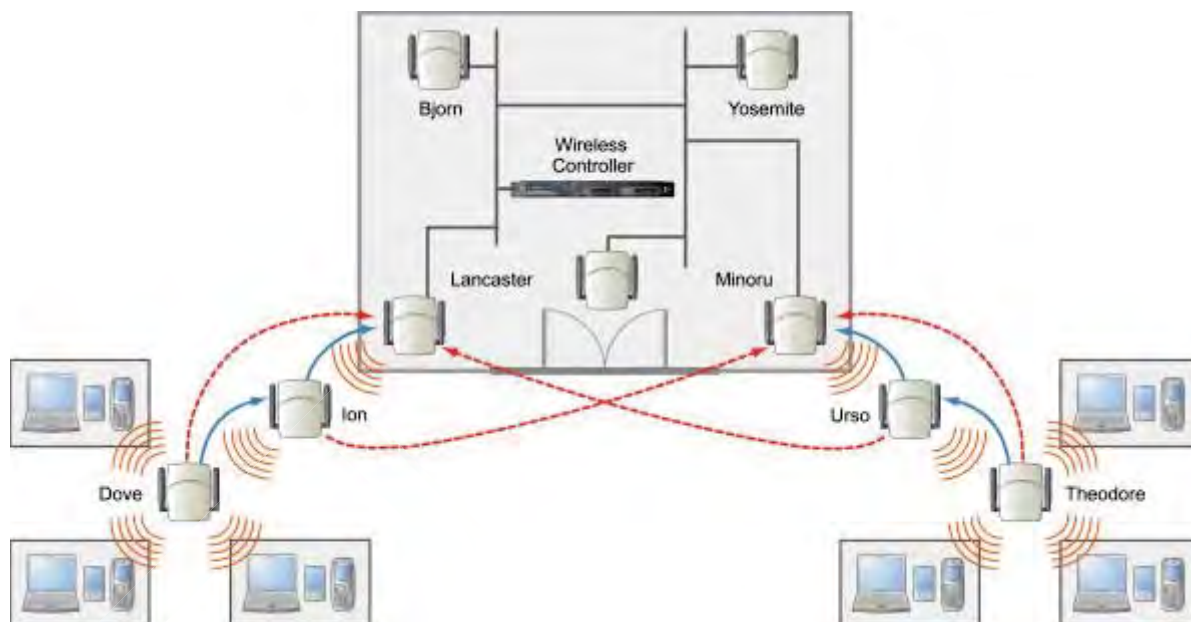


Figure 152: Deployment Example

Mesh Setup with a Single Mesh WLAN Service

Deploying the Mesh for the above example using a single Mesh *WLAN* Service results in the following structure shown in [Figure 153](#).

The tree will operate as a single Mesh entity. It will have a single Mesh SSID and a single pre-shared key for Mesh links. This tree will have multiple roots. For more information, see [Multi-Root Mesh Topology](#) on page 511.

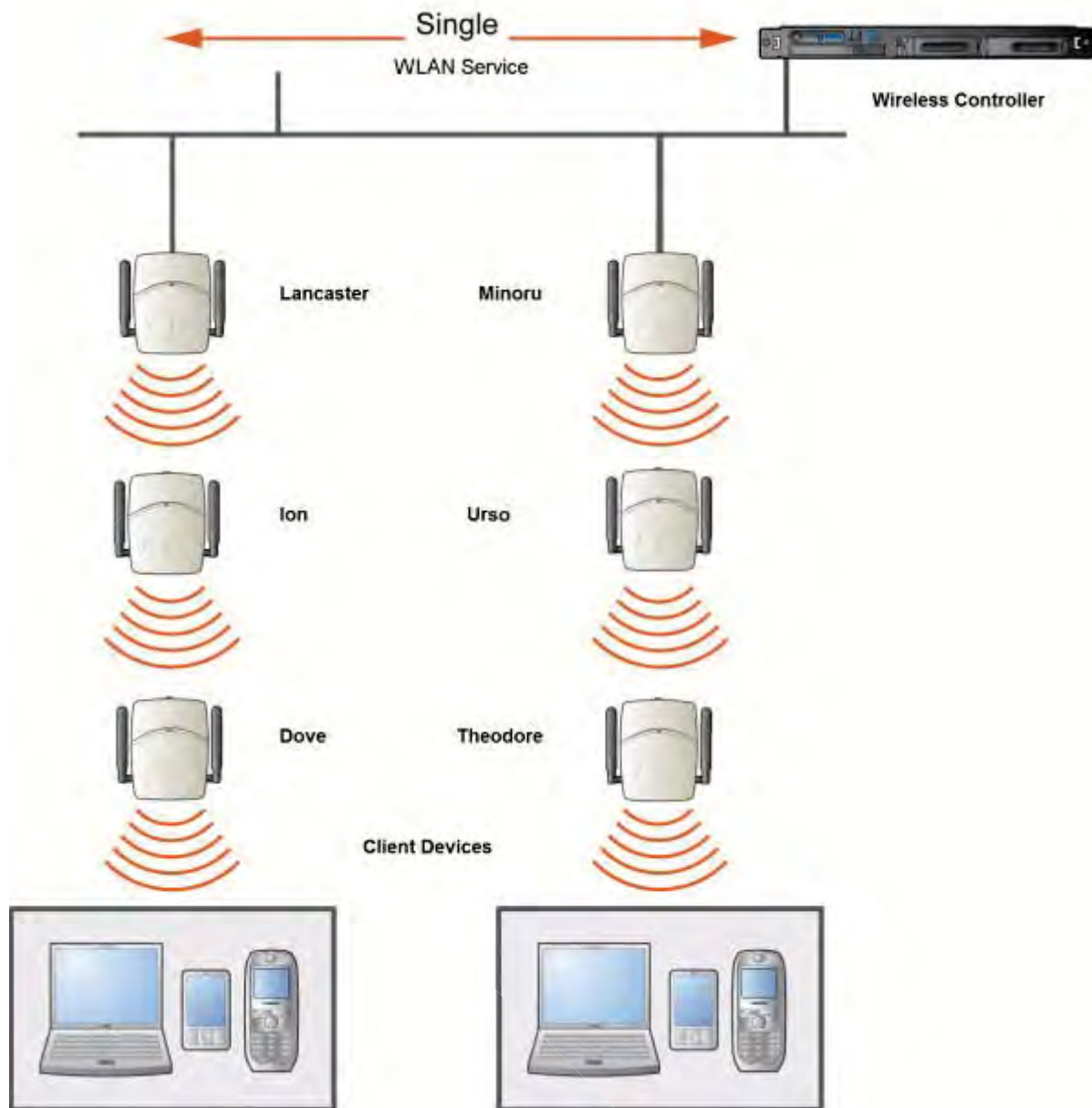


Figure 153: Mesh Setup with a Single Mesh WLAN Service

Mesh Setup with Multiple Mesh WLAN Services

You can also deploy the same Mesh in [Figure 152](#) on page 506 using two Mesh *WLAN* Services. The Two Mesh WLAN Services will create two independent Mesh trees. Both the trees will operate on separate SSIDs and use separate pre-shared keys.

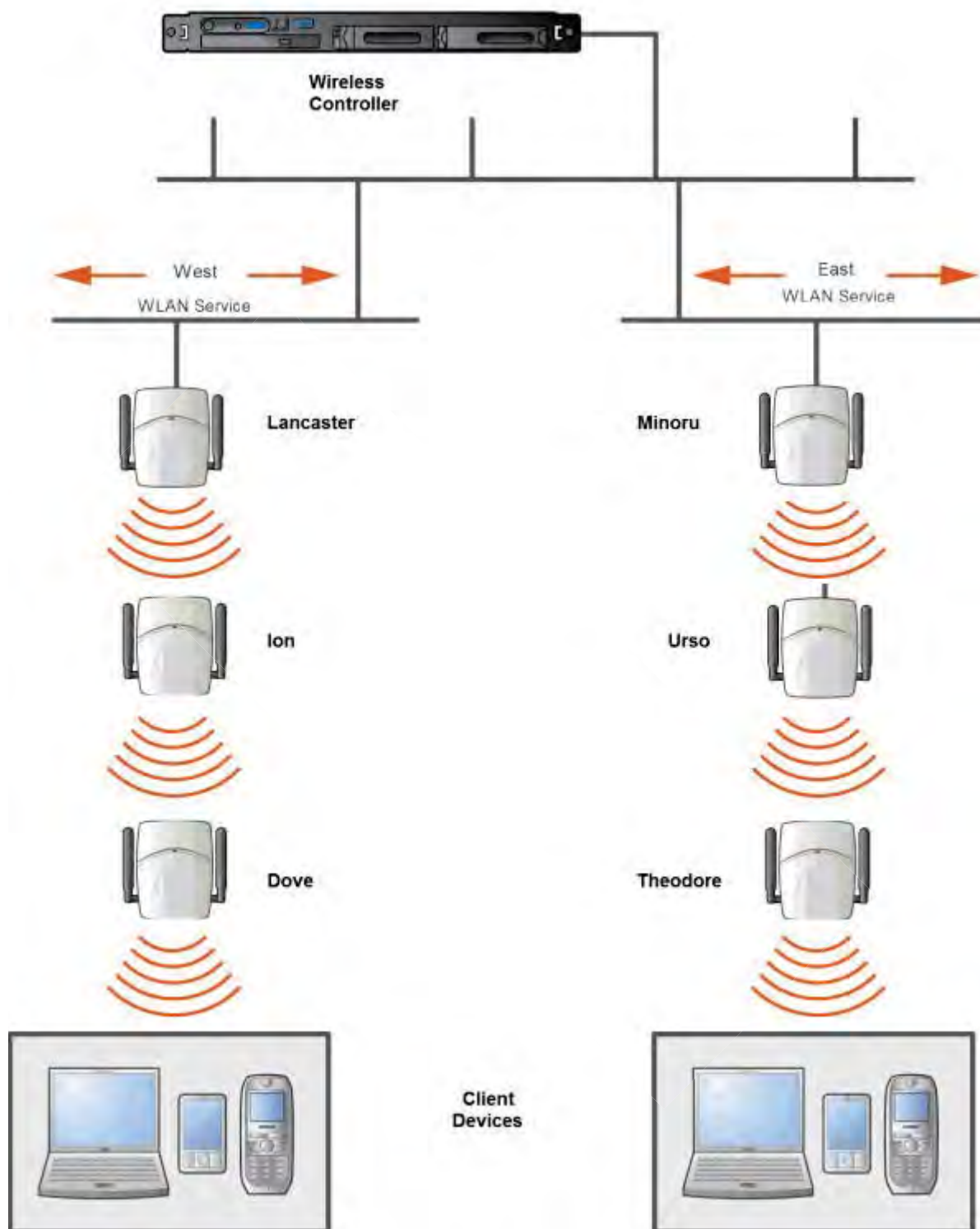


Figure 154: Mesh Setup with Multiple Mesh WLAN Services

Key Features of Mesh

Some key features of Mesh are:

- [Self-Healing Network](#) on page 509
- [Tree-like Topology](#) on page 509
- [Radio Channels](#) on page 510
- [Multi-Root Mesh Topology](#) on page 511
- [Figure 156](#) on page 511

Self-Healing Network

Data in a Mesh network propagates along a path, by hopping from node to node until the destination is reached. To ensure that all its paths' availability, the Mesh network allows for continuous connections and reconfiguration around broken or blocked paths, referred to as self-healing. The self-healing capability enables a routing based network to operate when one node breaks down or a connection goes bad.

Tree-like Topology

The APs in Mesh configuration can be regarded as nodes, and these nodes form a tree-like structure. The tree builds in a top down manner with the Mesh Portal being the tree root, and the Mesh AP being the tree leaves.

The nodes in the tree-structure have a parent-child relationship. The Mesh AP dynamically selects the best parent for connecting to the Mesh portal. A Mesh AP can have the role of both parent and child at the same time and the AP's role can change dynamically.

[Figure 155](#) on page 510 illustrates the parent-child relationship between the nodes in a Mesh topology.

- Mesh Portal is the parent of Mesh AP 1.
- Mesh AP 1 is the child of Mesh Portal.
- Mesh AP 1 is the parent of Mesh AP 2.
- Mesh AP 2 is the child of Mesh AP 1.
- Mesh AP 2 is the parent of the following Wireless APs:
 - Mesh AP 5
 - Mesh AP 4
 - Mesh AP 3
- All the three Mesh APs are the children of Mesh AP 2.

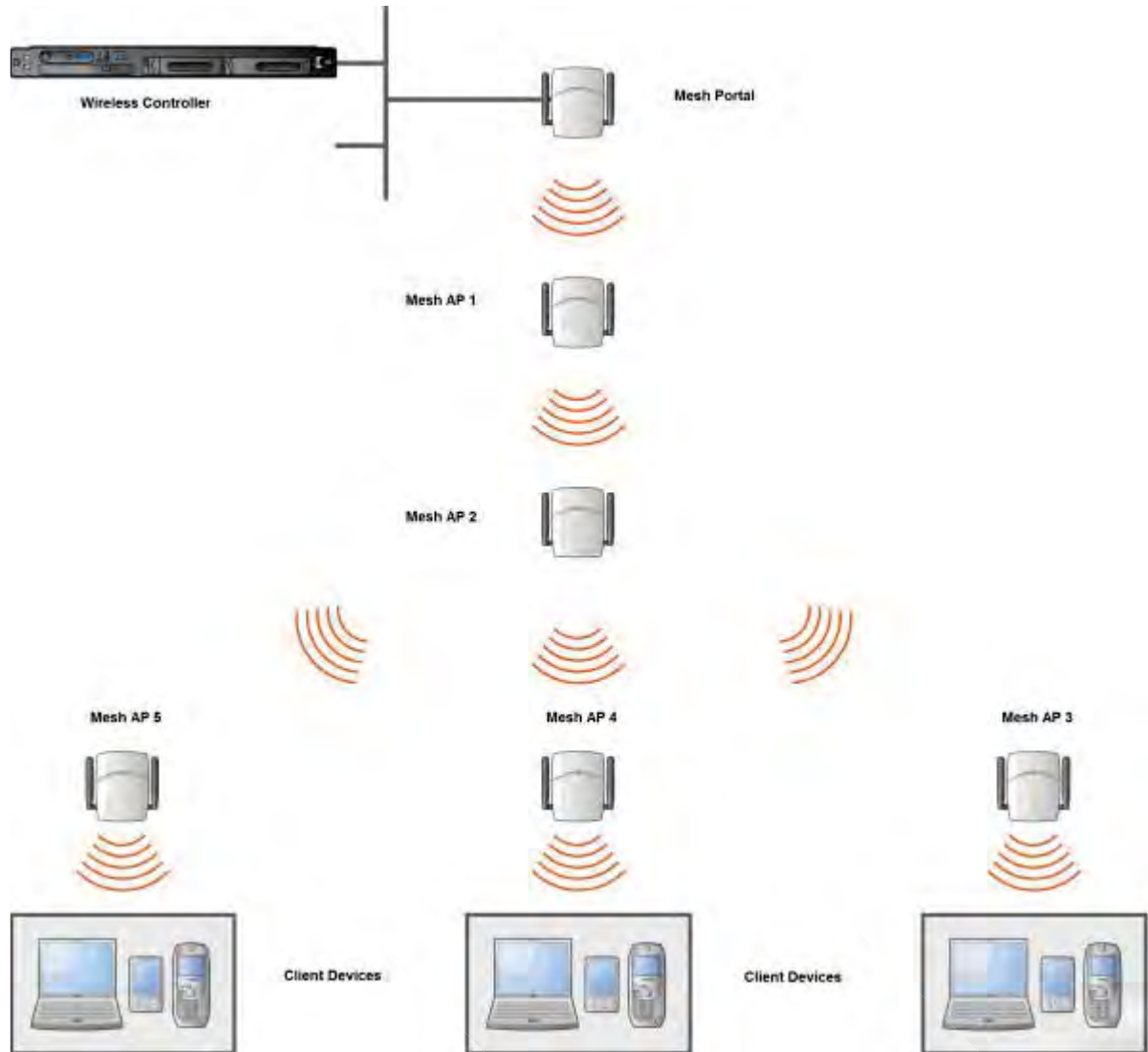


Figure 155: Parent-Child Relationship Between Wireless APs in Mesh Configuration



Note

If an AP is configured to serve as a scanner in Radar, it cannot be used in a Mesh tree. For more information, see [Working with ExtremeWireless Radar](#) on page 563.



Note

It is recommended that you limit the number of APs participating in a Mesh tree to 50. This limit guarantees decent performance in most typical situations.

Radio Channels

All APs in a mesh deployment must have Mesh configured on the same radio. On the backhaul radio, the following settings must be set the same way for all APs in the Mesh:

- Radio mode

- Minimum Basic Rate

Multi-Root Mesh Topology

A Mesh topology can have multiple Mesh Portals. Figure 156 illustrates the multiple-root Mesh topology.

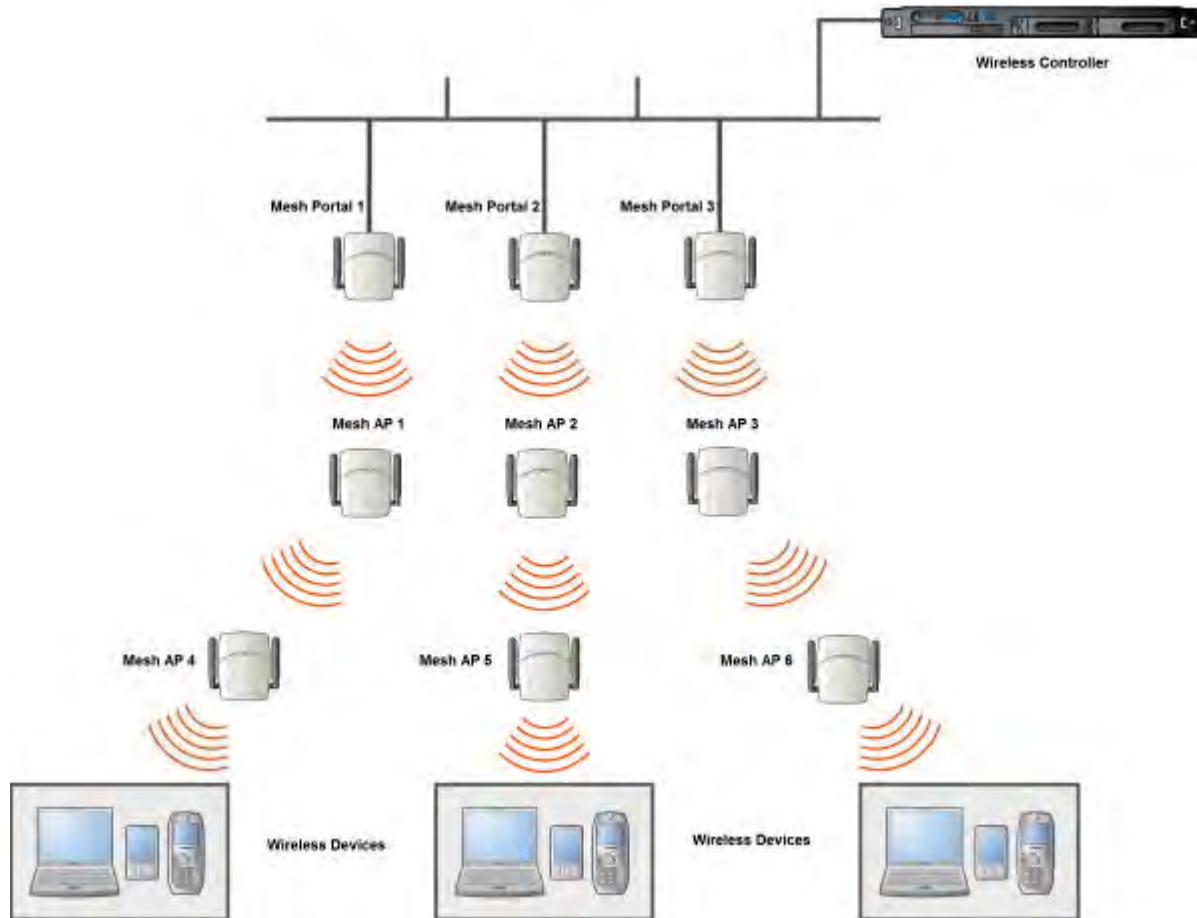


Figure 156: Multiple-Root Mesh Topology

Link Security

The Mesh link is encrypted using Advance Encryption Standard (AES).



Note

The keys for AES are configured prior to deploying the Repeater or Mesh APs.

Deploying the Mesh System

Before you start configuring the Mesh APs, you must ensure the following:

- The APs that are part of the wired WLAN are connected to the wired network.

- The wired APs that will serve as the Mesh Portal of the proposed Mesh topology are operating normally.
- The WLAN is operating normally.

Planning the Mesh Topology

You may sketch the proposed *WLAN* topology on paper before you start the Mesh deployment process. You should clearly identify the following in the sketch:

- Mesh APs with their names
- Radios that you will choose to link the APs

Provisioning the Mesh Wireless AP

This step is of crucial importance and involves connecting the Mesh APs to the enterprise network via the Ethernet link. This is done to enable the Mesh APs to connect to the wireless controller so that they can derive their Mesh configuration.

The Mesh AP's configuration includes pre-shared key and its role, preferred parent name and the backup parent name.



Note

The provisioning of Mesh APs must be done before they are deployed at the target location. If the APs are not provisioned, they will not work at their target location.

Mesh Deployment Overview

The following is the high-level overview of the Mesh deployment process:

- 1 Connecting the Mesh APs to the enterprise network via the Ethernet network to enable them to discover and register themselves with the wireless controller. For more information, see [Discovery and Registration](#) on page 120.
- 2 Disconnecting the Mesh APs from the enterprise network after they have discovered and registered with the wireless controller.
- 3 Creating a Mesh VNS.
- 4 Assigning roles, parents and backup parents to the Mesh wireless APs.
- 5 Assigning the Mesh APs' radios to the network VNSs.
- 6 Connecting the Mesh APs to the enterprise network via the Ethernet link for provisioning. For more information, see [Provisioning the Mesh Wireless AP](#) on page 512.
- 7 Disconnecting the Mesh APs from the enterprise network and moving them to the target location.



Note

During the Mesh deployment process, the Mesh APs are connected to the enterprise network on two occasions — first to enable them to discover and register with the wireless controller, and then the second time to enable them to obtain the provisioning from the wireless controller.

Connecting the Mesh APs to the Network for Discovery and Registration

Connect each Mesh wireless AP to the enterprise network to enable it to discover and register itself with the wireless controller.

Note



Before you connect the Mesh APs to the enterprise network for discovery and registration, you must ensure that the **Security mode** property of the wireless controller is defined according to your security needs. The **Security mode** property dictates how the wireless controller behaves when registering new and unknown devices. For more information, see [Wireless AP Registration](#) on page 123. If the **Security mode** is set to **Allow only approved Wireless APs to connect** (this is also known as secure mode), you must manually approve the Mesh APs after they are connected to the network for the discovery and registration. For more information, see [New Button -- Adding and Registering a Wireless AP](#) on page 131.

Depending upon the number of Ethernet ports available, you may connect one or more Mesh wireless APs at a time, or you may connect all of them together.

Once a Mesh wireless AP has discovered and registered itself with the wireless controller, disconnect it from the enterprise network.

Configuring the Mesh Wireless APs Through the Controller

Configuring the Mesh wireless APs involves the following steps:

- 1 Creating a Mesh WLAN Service.
- 2 Defining the SSID name and the pre-shared key.

For ease of understanding, the Mesh configuration process is explained with an example. [Figure 157](#) on page 514 depicts a site with the following features:

- An office building, denoted by a rectangular enclosure.
- Four APs — Ardal, Arthur, Athens and Auberon — are within the confines of the building, and are connected to the wired network.
- The space around the building is the warehouse.
- The solid arrows point toward Current Parents.
- The dotted arrows point toward Alternative Parents.

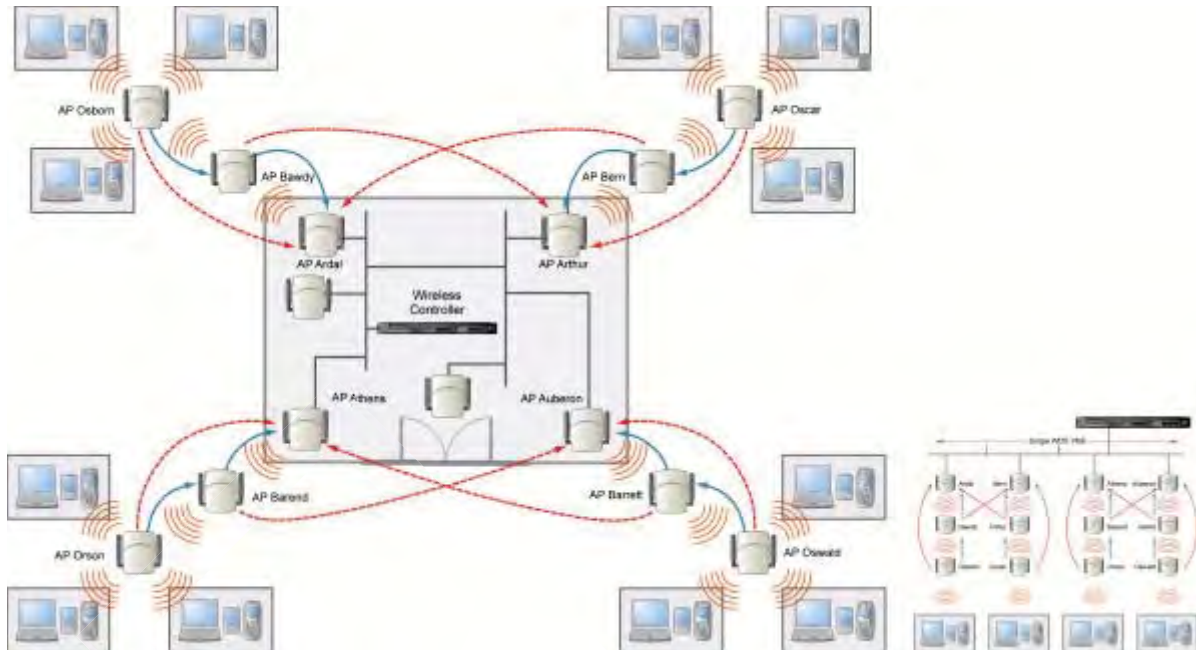


Figure 157: Mesh Deployment

Note



With the single Mesh VNS, the tree structure for the Mesh deployment will be as depicted on the bottom right of [Figure 157](#). You can also implement the same deployment using four Mesh VNSs, each for a set of APs in the four corners of the building. Each set of APs will form an isolated topology and will operate using a separate SSID and a separate Pre-shared key. For more information, see [Figure 151](#) on page 505.

To configure the Mesh wireless APs through the controller:

Before configuring Mesh, be sure that the following conditions are met:

- Energy Save is set to Off
- Beacon Interval is set to 100 msec
- AP names are 32 characters or less for statistics display purposes
- ATPC and DCS are both disabled.

If possible, follow these guidelines for the backhaul radio to achieve a balance of stability, throughput, and latency:

- Use a 5.2 GHz band for backhaul
- Select a non-DFS channel for the Mesh Portal
- Use a 40 MHz Channel Width and Short guard interval
- Disable Aggregate MSDUs
- Enable Aggregate MPDUs
- Enable ADDBA support
- Configure the settings on the Radio configuration page the same for all APs in the Mesh.
- Set the Poll Timeout to be at least 60 seconds.

- 1 From the top menu, click **VNS**.
- 2 In the left pane, expand the **WLAN Services** pane and select a Mesh service to edit or click the **New** button.
- 3 Enter a name for the service in the **Name** field.
- 4 The **SSID** field is automatically filled in with the name, but you can change it if desired.
- 5 For **Service Type**, select **Mesh**.

The screenshot shows a web interface with a top navigation bar containing tabs: Logs, Reports, Controller, AP, VNS (selected), and WIPS. Below the navigation bar, the page is titled "WLAN:". Underneath, there is a section titled "WLAN Services". This section contains two main panels. The first panel, labeled "Core", contains the following fields: "Name:" with a text input field containing "Mesh_Network"; "Service Type:" with a group of radio buttons where "Mesh" is selected (others are Standard, WDS, Third Party AP, and Remote); and "SSID:" with a text input field. The second panel, labeled "Status", contains an "Enable:" checkbox which is checked.

- 6 To save your changes, click **Save**. The **WLAN configuration** window is re-displayed to show additional configuration fields.

Logs	Reports	Controller	AP	VNS	WIPS
------	---------	------------	----	-----	------

WLAN: Mesh_Network

Core

Name: Mesh_Network

Service Type: Mesh

SSID: Mesh_Network

☐ Suppress SSID

Mesh Settings

Pre-shared Key:

Backhaul Radio: a (5 GHz) ▼

Status

Enable: ☒

Wireless APs services

AP Name	Mesh Service	Bridge to LAN	Radio #
1548Y-1007900000	none ▼	<input type="checkbox"/>	1
14300167085D0000[F]	none ▼	<input type="checkbox"/>	1

- 7 In the **Mesh Pre-shared Key** box, type the key.



Note

The pre-shared key must be 8 to 63 characters long. The Mesh APs use this pre-shared key to establish a Mesh link between them.



Note

Changing the pre-shared key after the Mesh is deployed can be a lengthy process. For more information, see [Changing the Pre-shared Key in a Mesh WLAN Service](#) on page 517.

- 8 Assign a backhaul radio.



Note

After you save the configuration, you cannot change the backhaul radio. Please configure this setting wisely.

- 9 To save your changes, click **Save**.



Note

The **Mesh Bridge** feature on the user interface relates to Mesh Bridge configuration. When you are configuring the **Mesh Bridge** topology, you must select Mesh Bridge for Mesh AP that is connected to the wired network. For more information, see [Wireless Bridge Configuration](#) on page 504.

Connecting the Mesh Wireless APs to the Enterprise Network for Provisioning

You must connect the Mesh wireless APs to the enterprise network once more to enable them to obtain their configuration from the wireless controller. The configuration includes the pre-shared key, the AP's role, preferred parent and backup parent. For more information, see [Provisioning the Mesh Wireless AP](#) on page 512.



Warning

If you skip this step, the Mesh APs will not work at their target location.

Moving the Mesh Wireless APs to the Target Location



Note

If you change any of the following radio properties of a Mesh AP, the Mesh AP will reject the change: disabling the radio on which the Mesh link is established, lowering the radio's Tx Power of a radio on which the Mesh link is established, or changing the country.

- 1 Disconnect the Mesh APs from the enterprise network, and move them to the target location.
- 2 Install the Mesh APs at the target location.
- 3 Connect the APs to a power source. The discovery and registration processes are initiated.

Changing the Pre-shared Key in a Mesh WLAN Service

To Change the Pre-shared Key in a Mesh WLAN Service

- 1 Create a new Mesh WLAN Service with a new pre-shared key.
- 2 Assign the RF of the APs from the old Mesh to the new Mesh WLAN Service.
- 3 Wait at least 30 seconds to ensure that all APs got the configuration, then disable the old Mesh WLAN service.
- 4 Check the **Mesh Statistics** report page to ensure that all the Mesh APs have connected to the wireless controller via the new Mesh VNS. For more information, see [Viewing Statistics for APs](#) on page 627.
- 5 Delete the old Mesh WLAN Service. For more information, see [Deleting a VNS](#) on page 486.

12 Working with a Wireless Distribution System

About WDS

Simple WDS Configuration

Wireless Repeater Configuration

Wireless Bridge Configuration

Examples of Deployment

WDS WLAN Services

Key Features of WDS

Deploying the WDS System

Changing the Pre-shared Key in a WDS WLAN Service

About WDS

The Wireless Distribution System (WDS) enable you to expand the wireless network by interconnecting the wireless APs through wireless links in addition to the traditional method of interconnecting APs via a wired network.

A WDS deployment is ideally suited for locations, where installing Ethernet cabling is too expensive, or physically impossible.

The WDS can be deployed in three configurations:

- Simple WDS Configuration
- Wireless Repeater Configuration
- Wireless Bridge Configuration

Simple WDS Configuration

In a typical WDS configuration, the wireless APs are connected to the distribution system via an Ethernet network, which provides connectivity to the wireless controller.

However, when an AP is installed in a remote location and can't be wired to the distribution system, an intermediate AP is connected to the distribution system via the Ethernet link. This intermediate AP forwards and receives the user traffic from the remote AP over a radio link.

The intermediate AP that is connected to the distribution system via the Ethernet network is called Root AP, and the AP that is remotely located is called the Satellite AP.

Figure 158 illustrates the Simple WDS configuration:

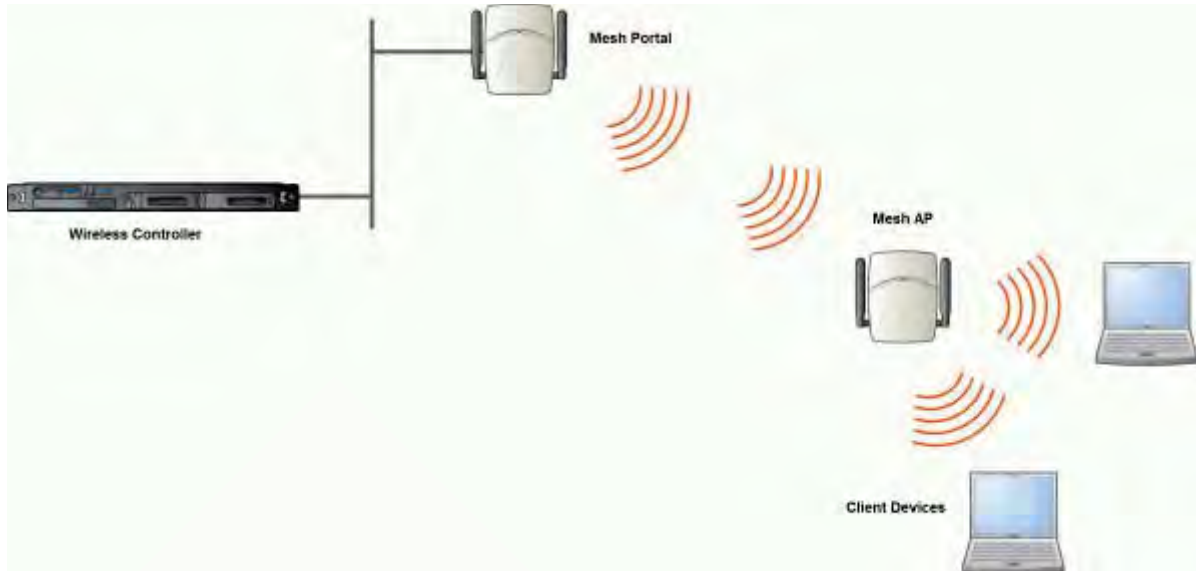


Figure 158: Simple WDS Configuration

Wireless Repeater Configuration

In Wireless Repeater configuration, a Repeater wireless AP is installed between the Root AP and the Satellite AP. The Repeater AP relays the user traffic between the Root AP and the Satellite AP. This increases the *WLAN (Wireless Local Area Network)* range.

Figure 159 illustrates the Wireless Repeater configuration:

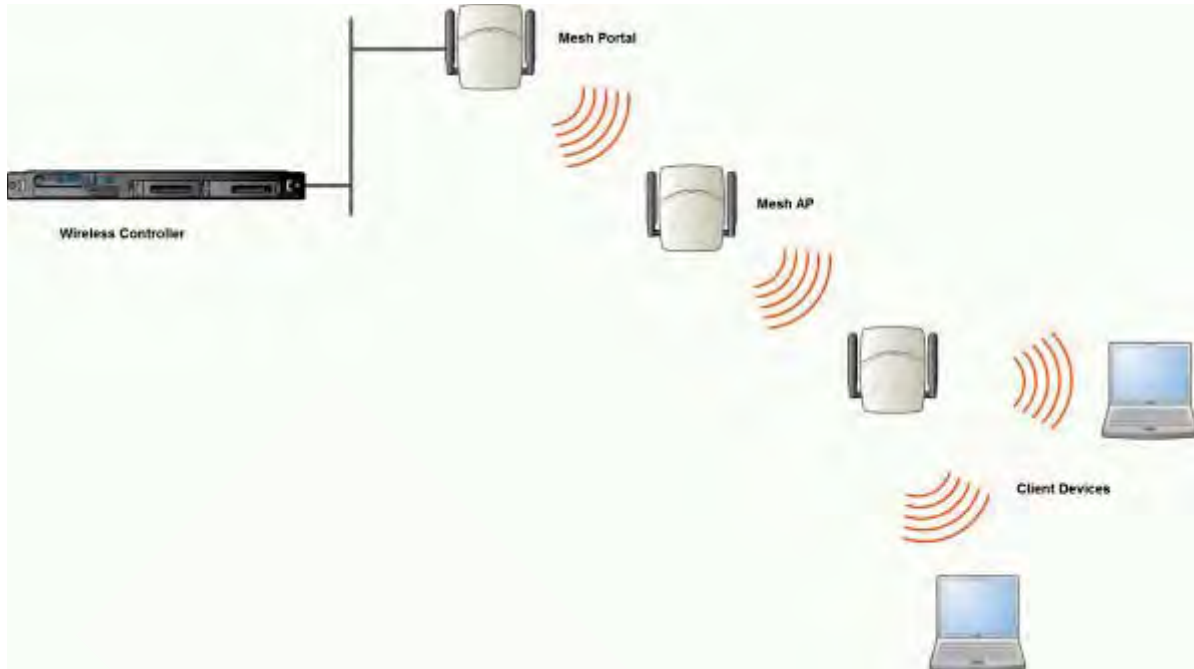


Figure 159: Wireless Repeater Configuration



Note

You should restrict the number of repeater hops in a Wireless Repeater configuration to three for optimum performance.

Wireless Bridge Configuration

In Wireless Bridge configuration, the traffic between two wireless APs that are connected to two separate wired LAN segments is bridged via WDS link. You may also install a Repeater AP between the two APs connected to two separate LAN segments.



Figure 160: Wireless Bridge Configuration

When you are configuring the Wireless Bridge configuration, you must specify on the user interface that the Satellite AP is connected to the wired LAN.

Examples of Deployment

Examples of Deployment on page 521 illustration depicts a few examples of WDS deployment.

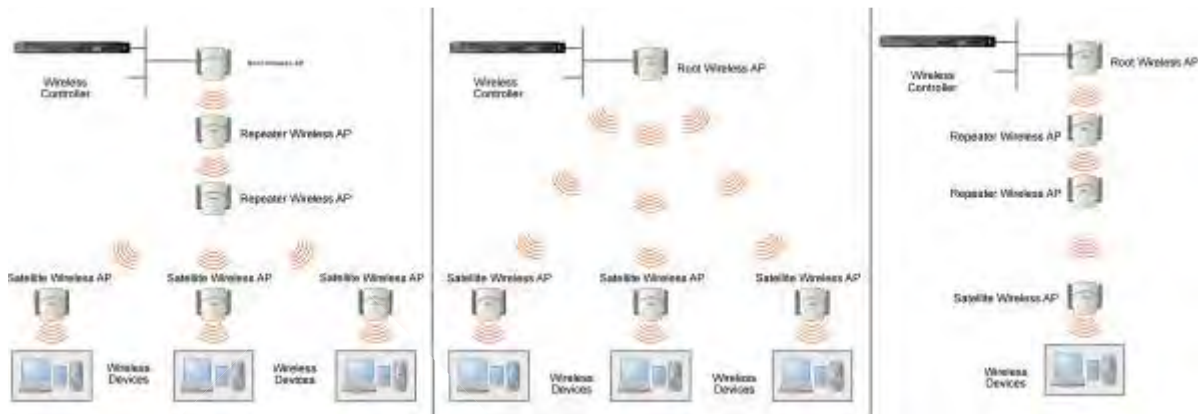


Figure 161: Examples of WDS Deployment

WDS WLAN Services

In a traditional *WLAN* deployment, each radio of the wireless AP can interact with the client devices on a maximum of eight networks.

In WDS deployment, one of the radios of every WDS AP establishes a WDS link on an exclusive WLAN Service. The WDS AP is therefore limited to seven network WLAN Services on the WDS radio. The other radio can interact with the client devices on a maximum of eight WLAN Services.



Note

The root wireless AP and the Repeater APs can also be configured to interact with the client-devices. For more information, see [Assigning the Satellite Wireless APs' Radios to the Network WLAN Services](#) on page 535.

The WLAN Service on which the APs establish the WDS link is called the WDS WLAN Service.

A WDS can be setup either by using either a single WDS WLAN Service or multiple WDS WLAN Services. The following figures illustrate the point.

Figure 162 on page 522 shows:

- The rectangular enclosure denotes an office building.
- The four wireless APs — Minoru, Yosemite, Bjorn and Lancaster — are within the confines of the building and are connected to the wired network.
- The space around the office building is a ware house.
- The solid arrows point towards Preferred Parents.
- The dotted arrows point towards Backup Parents.

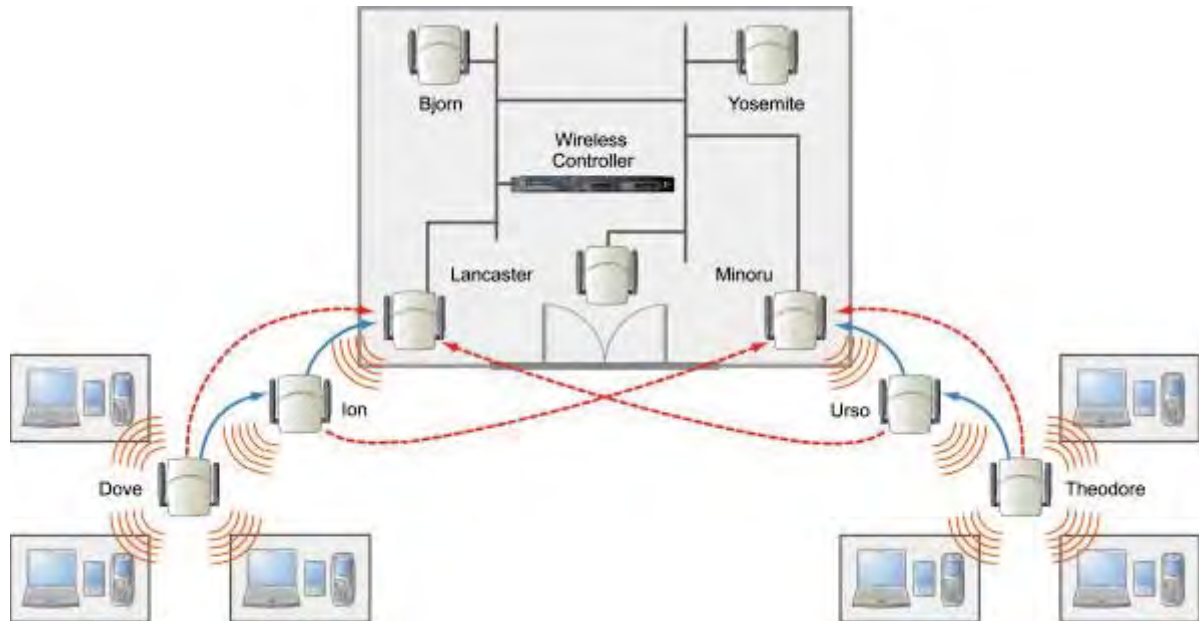


Figure 162: Deployment Example

WDS Setup with a Single WDS WLAN Service

Deploying the WDS for the above example using a single WDS WLAN Service results in the following structure.

The tree will operate as a single WDS entity. It will have a single WDS SSID and a single pre-shared key for WDS links. This tree will have multiple roots. For more information, see [Multi-Root WDS Topology](#) on page 527.

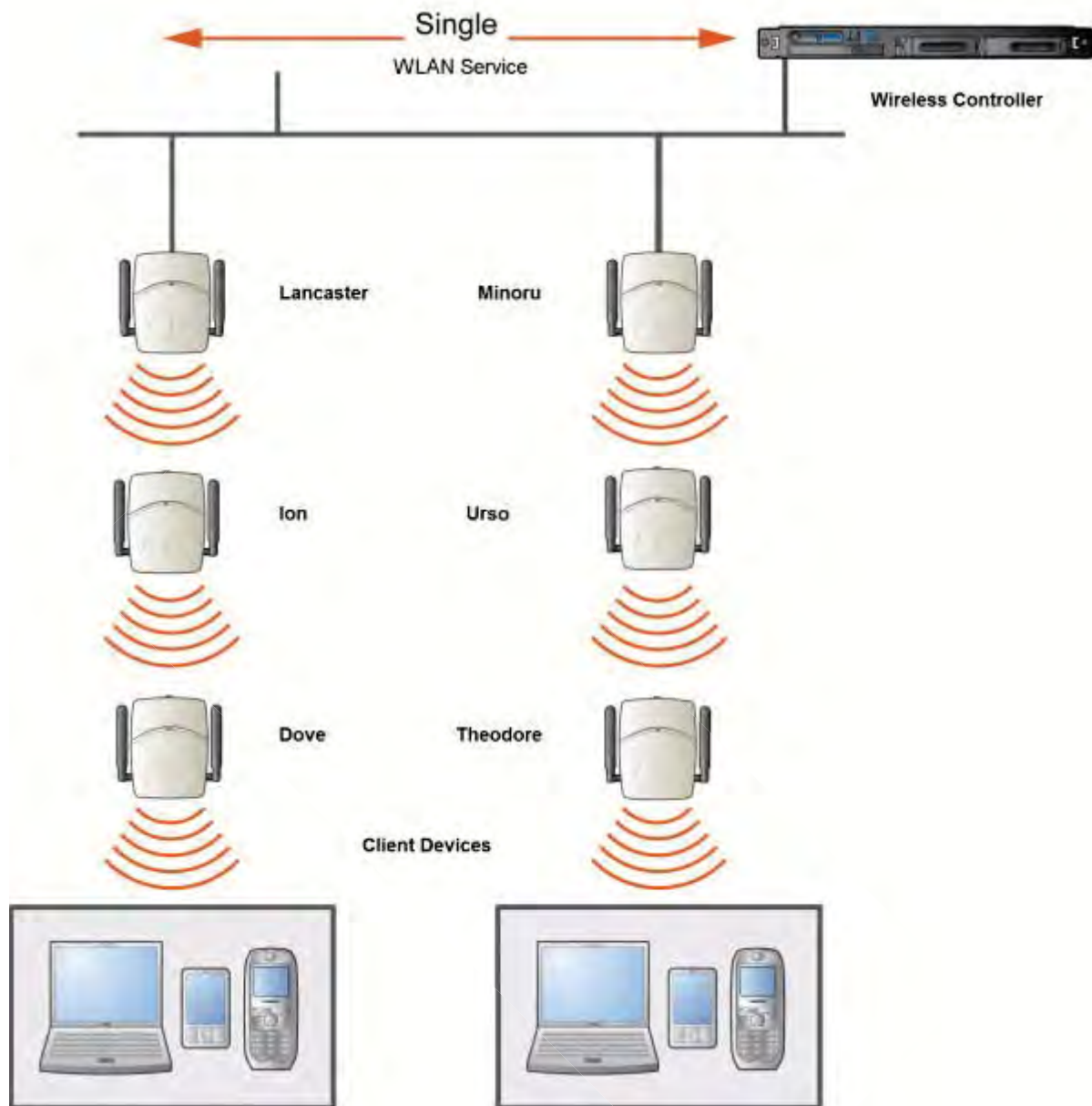


Figure 163: WDS Setup with a Single WDS WLAN Service

WDS Setup with Multiple WDS WLAN Services

You can also deploy the same WDS using two WDS WLAN Services. The Two WDS WLAN Services will create two independent WDS trees. Both the trees will operate on separate SSIDs and use separate pre-shared keys.

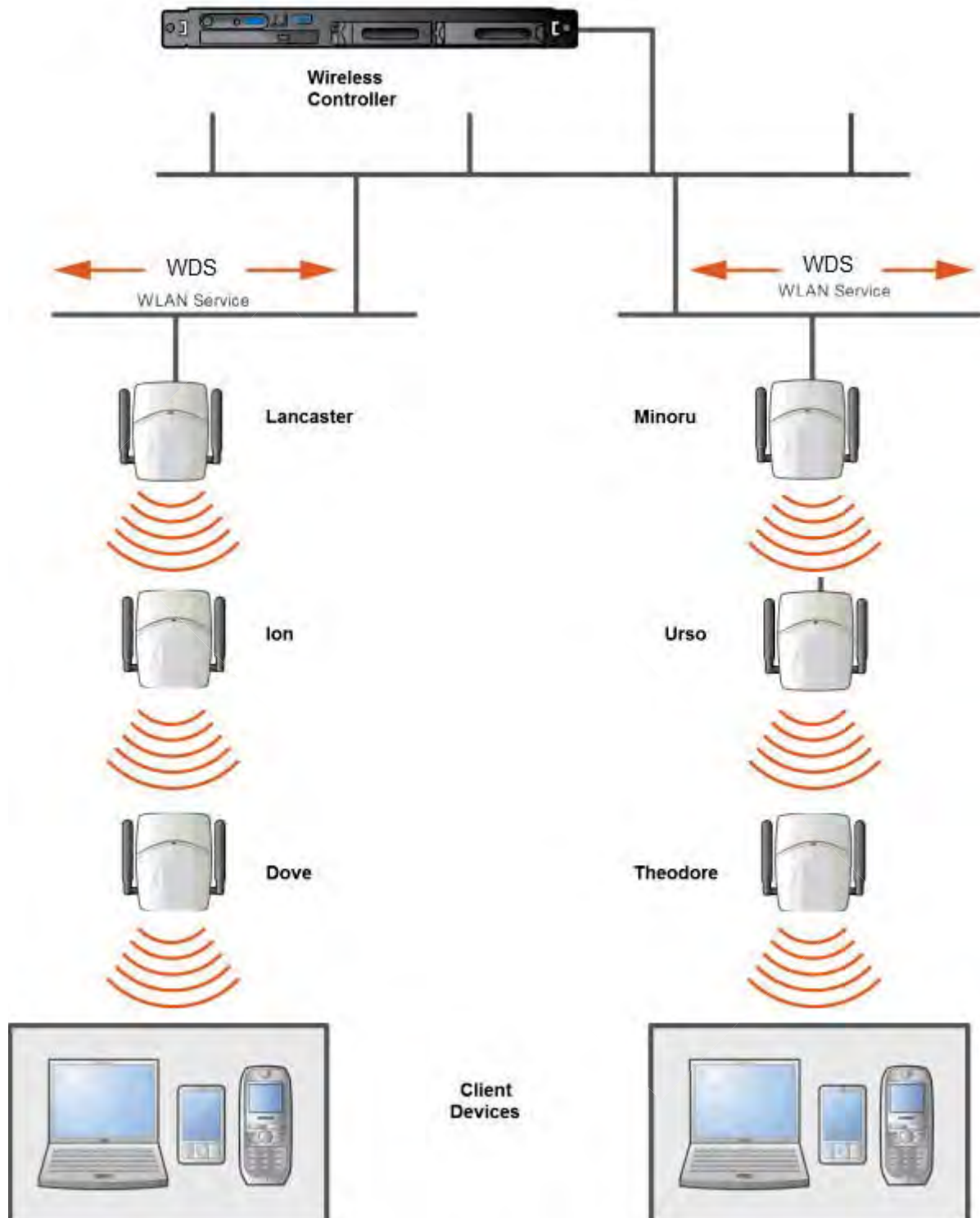


Figure 164: WDS Setup with Multiple WDS WLAN Services

Key Features of WDS

Some key features of WDS are:

- [Tree-like Topology](#) on page 525
- [Radio Channels](#) on page 527
- [Multi-Root WDS Topology](#) on page 527
- [Figure 166](#) on page 527
- [Link Security](#) on page 528

Tree-like Topology

The wireless APs in WDS configuration can be regarded as nodes, and these nodes form a tree-like structure. The tree builds in a top down manner with the Root AP being the tree root, and the Satellite AP being the tree leaves.

The nodes in the tree-structure have a parent-child relationship. The AP that provides the WDS service to the other APs in the downstream direction is a parent. The APs that establish a link with the AP in the upstream direction for WDS service are children.



Note

If a parent AP fails or stops to act a parent, the children APs will attempt to discover their backup parents. If the backup parents are not defined, the children APs will be left stranded.

The following figure illustrates the parent-child relationship between the nodes in a WDS topology. In [Figure 165](#) on page 526:

- Root Wireless AP is the parent of Repeater Wireless AP 1.
- Repeater Wireless AP 1 is the child of Root Wireless AP.
- Repeater Wireless AP 1 is the parent of Repeater Wireless AP 2.
- Repeater Wireless AP 2 is the child of Repeater Wireless AP 1.
- Repeater Wireless AP 2 is the parent of the following Wireless APs:
 - Satellite Wireless AP 1
 - Satellite Wireless AP 2
 - Satellite Wireless AP 3
- All the three Satellite APs are the children of Repeater Wireless AP 2.

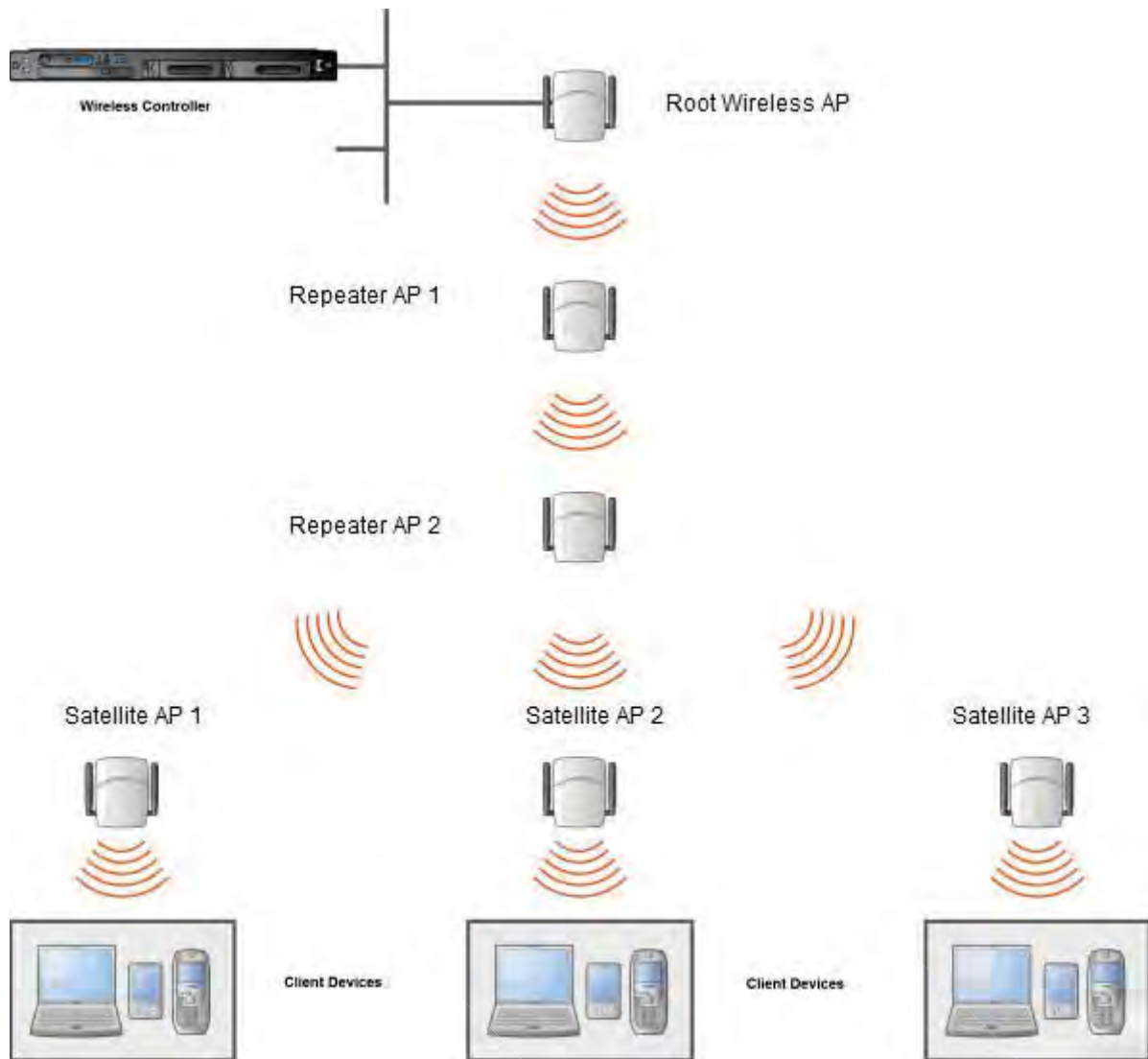


Figure 165: Parent-Child Relationship Between Wireless APs in WDS Configuration

The WDS system enables you to configure the AP's role — **parent**, **child** or **both** — from the wireless controller's interface. If the WDS AP will be serving as a parent and a child in a given topology, its role is configured as both.



Note

It is recommended that you limit the number of APs participating in a WDS tree to 8. This limit guarantees decent performance in most typical situations.



Note

If an AP is configured to serve as a scanner in Radar, it cannot be used in a WDS tree. For more information, see [Working with ExtremeWireless Radar](#) on page 563.

Radio Channels

The radio channel on which the child AP operates is determined by the parent AP.

An AP may connect to its parent AP and children APs on the same radio, or on different radios. Similarly, an AP can have two children operating on two different radios.



Note

When an AP is connecting to its parent AP and children APs on the same radio, it uses the same channel for both the connections.

Multi-Root WDS Topology

A WDS topology can have multiple Root wireless APs. Figure 166 illustrates the multiple-root WDS topology.

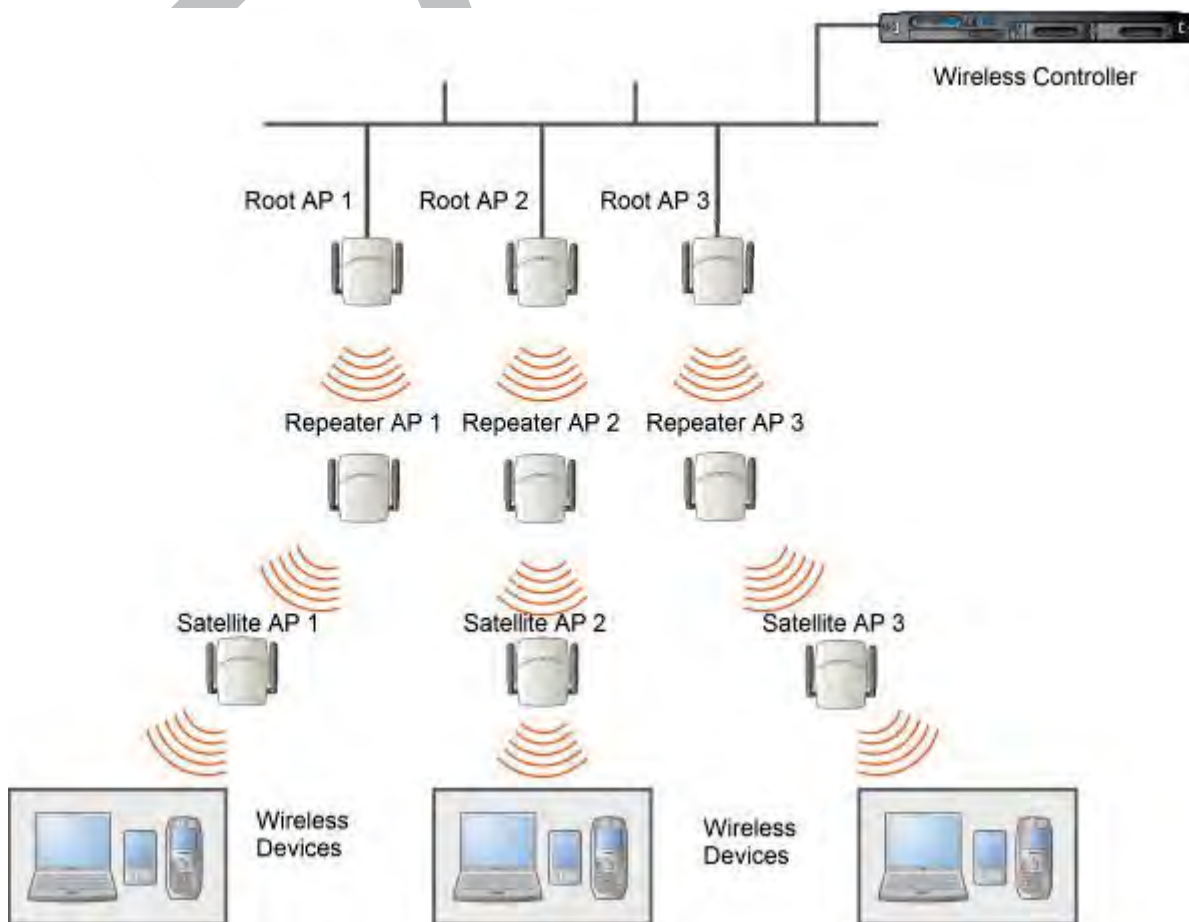


Figure 166: Multiple-root WDS Topology

Automatic Discovery of Parent and Backup Parent Wireless APs

The children wireless APs, including the Repeater wireless AP and the Satellite wireless APs, scan for their respective parents at a startup.

You can manually configure a parent and backup parent for the children APs or you can enable the children APs to automatically select the best parent out of all of the available APs. If you choose automatic parent AP selection, a child AP selects a parent AP based on its received signal strength and the number of hops to the root AP. After a parent AP and backup parent AP is selected, the wireless controller will first try to negotiate a WDS link with the parent wireless controller. If the WDS link negotiation is unsuccessful, the wireless controller will try to negotiate a link with the backup parent.

Link Security

The WDS link is encrypted using Advance Encryption Standard (AES).



Note

The keys for AES are configured prior to deploying the Repeater or Satellite APs.

Deploying the WDS System

Before you start configuring the WDS wireless APs, you must ensure the following:

- The wireless APs that are part of the wired WLAN are connected to the wired network.
- The wired wireless APs that will serve as the Root AP/Root APs of the proposed WDS topology are operating normally.
- The WLAN is operating normally.

Planning the WDS Topology

You may sketch the proposed WLAN topology on er before you start the WDS deployment process. You should clearly identify the following in the sketch:

- WDS wireless APs with their names
- Parent-child relationships between wireless APs
- Radios that you will choose to link the wireless APs' parents and children

Provisioning the WDS APs

This step is of crucial importance and involves connecting the WDS wireless APs to the enterprise network via the Ethernet link. This is done to enable the WDS APs to connect to the wireless AP controller so that they can derive their WDS configuration.

The WDS AP's configuration includes pre-shared key, its role, preferred parent name and the backup parent name.



Note

The provisioning of WDS APs must be done before they are deployed at the target location. If the APs are not provisioned, they will not work at their target location.

WDS Deployment Overview

The following is the high-level overview of the WDS deployment process:

- 1 Connecting the WDS wireless APs to the enterprise network via the Ethernet network to enable them to discover and register themselves with the wireless controller. For more information, see [Discovery and Registration](#) on page 120.
- 2 Disconnecting the WDS APs from the enterprise network after they have discovered and registered with the wireless controller.
- 3 Creating a WDS VNS.
- 4 Assigning roles, parents and backup parents to the WDS APs.
- 5 Assigning the Satellite APs' radios to the network VNSs.
- 6 Connecting the WDS APs to the enterprise network via the Ethernet link for provisioning. For more information, see [Provisioning the WDS APs](#) on page 528.
- 7 Disconnecting the WDS APs from the enterprise network and moving them to the target location.

Note



During the WDS deployment process, the WDS APs are connected to the enterprise network on two occasions — first to enable them to discover and register with the wireless controller, and then the second time to enable them to obtain the provisioning from the wireless controller.

Connecting the WDS Wireless APs to the Enterprise Network for Discovery and Registration

Connect each WDS wireless AP to the enterprise network to enable it to discover and register itself with the wireless controller.

Note



Before you connect the WDS APs to the enterprise network for discovery and registration, you must ensure that the **Security mode** property of the wireless controller is defined according to your security needs. The **Security mode** property dictates how the wireless controller behaves when registering new and unknown devices. For more information, see [Wireless AP Registration](#) on page 123. If the **Security mode** is set to **Allow only approved APs to connect** (this is also known as secure mode), you must manually approve the WDS APs after they are connected to the network for the discovery and registration. For more information, see [New Button -- Adding and Registering a Wireless AP](#) on page 131.

Depending upon the number of Ethernet ports available, you may connect one or more WDS APs at a time, or you may connect all of them together.

Once a WDS AP has discovered and registered itself with the wireless controller, disconnect it from the enterprise network.

Configuring the WDS Wireless APs Through the Wireless Controller



Note

You must identify and mark the Preferred Parents, Backup Parents and the Child APs in the proposed WDS topology before starting the configuration process.

Configuring the WDS wireless APs involves the following steps:

- Creating a WDS WLAN Service.
- Defining the SSID name and the pre-shared key.
- Assigning roles, parents and backup parents to the WDS APs.

For ease of understanding, the WDS configuration process is explained with an example. The following figure depicts a site with the following features:

- An office building, denoted by a rectangular enclosure.
- Four APs — Ardal, Arthur, Athens and Auberon — are within the confines of the building, and are connected to the wired network.
- The space around the building is the warehouse.
- The solid arrows point toward Preferred Parents.
- The dotted arrows point toward Backup Parents.

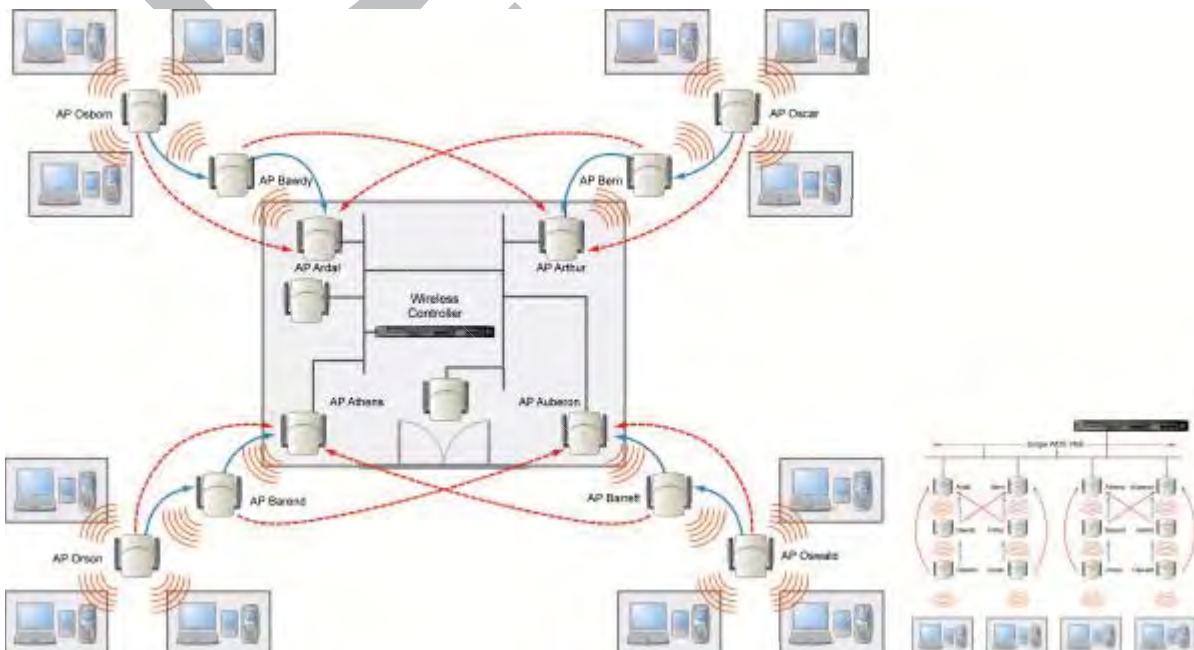


Figure 167: WDS Deployment



Note

With the single WDS VNS, the tree structure for the WDS deployment will be as depicted on the bottom right of the figure above. You can also implement the same deployment using four WDS VNSs, each for a set of APs in the four corners of the building. Each set of APs will form an isolated topology and will operate using a separate SSID and a separate Pre-shared key. For more information, see [Figure 161](#) on page 521.

To configure the WDS wireless APs through the wireless controller:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, expand the **WLAN Services** pane and select a WDS service to edit or click the **New** button.
- 3 Enter a name for the service in the **Name** field.
- 4 The **SSID** field is automatically filled in with the name, but you can change it if desired.
- 5 For **Service Type**, select **WDS**.

The screenshot displays the WLAN configuration interface. At the top, a navigation bar includes links for Home, Logs, Reports, Controller, AP, VNS, and WIPS. The left sidebar shows a tree view with categories: New..., Global, Sites, Virtual Networks, and WLAN Services. Under WLAN Services, 'Lab46-WPA' and 'WDS_network' are listed. The main content area is titled 'WLAN:' and contains a 'WLAN Services' section. Within this section, a 'Core' box contains the following fields: 'Name' (WDS_network2), 'Service Type' (with radio buttons for Standard, WDS, Mesh, Third Party AP, and Remote; WDS is selected), and 'SSID' (WDS_network2). Below the Core box, a 'Status' box contains an 'Enable' checkbox which is checked.

- 6 To save your changes, click **Save**.

The **WLAN configuration** window displays again to show additional configuration fields.

WLAN: WDS_network 2

WLAN Services

Core

Name: WDS_network2

Service Type: WDS

SSID: WDS_network2

☐ Suppress SSID

Status

Enable: ☒

WDS Pre-shared key

Wireless APs services

AP Name	Radio 1	Mode	Radio 2	Mode	WDS bridge
1548Y-1007900000	none	a/n/ac	none	g/n	<input type="checkbox"/>
14300167085D0000[F]	none	a/n/ac	none	g/n	<input type="checkbox"/>

Adding the first WDS/Mesh assignment or removing the last WDS/Mesh assignment will cause an AP to reboot.

New **Delete** **Save**

- 7 To improve security for WDS links and reduce inadvertent user associations to WDS SSID, check the **Suppress SSID** check box. (This option is available after you save the WDS type WLAN Service.)

When this option is checked:

- The SSID name is not included in the SSID IE field.
- The child AP inspects the beacon for proprietary information that identifies the service.

- 8 In the **WDS Pre-shared Key** box, type the key.



Note

The pre-shared key must be 8 to 63 characters long. The WDS APs use this pre-shared key to establish a WDS link between them.



Note

Changing the pre-shared key after the WDS is deployed can be a lengthy process. For more information, see [Changing the Pre-shared Key in a WDS WLAN Service](#) on page 536.

- 9 Assign the roles, preferred parents and backup parents to the AP Radios.



Note

The roles — parent, child, and both — are assigned to the Radios of the APs. An AP may connect to its parent wireless AP and children APs on the same Radio, or on a different Radio. Similarly, a AP can have two children operating on two different Radios. The Radio on which the child AP operates is determined by the parent AP. If the AP will be serving both as parent and child, you must select both as its role.

- 10 To configure the WDS with a single WDS VNS, you must assign the roles, preferred parents and backup parents to the APs according to [Table 106](#).

Table 106: Wireless APs and Their Roles

ExtremeWireless AP	Radio b/g	Radio a	Preferred Parent	Backup Parent
Ardal	Parent	Parent	See the note below.	See the note below.
Arthur	Parent	Parent	See the note below.	See the note below.
Athens	Parent	Parent	See the note below.	See the note below.
Auberon	Parent	Parent	See the note below.	See the note below.
Bawdy	Both	Child	Ardal	Arthur
Bern	Both	Child	Arthur	Ardal
Barend	Both	Child	Athens	Auberon
Barett	Both	Child	Auberon	Athens
Osborn	Child	Child	Bawdy	Ardal
Oscar	Child	Child	Bern	Arthur
Orson	Child	Child	Barend	Athens
Oswald	Child	Child	Barett	Auberon



Note

Since the Root APs — Ardal, Arthur, Athens and Auberon — are the highest entities in the tree structure, they do not have parents. Therefore, the Preferred Parent and Backup Parent drop-down lists of the Root APs do not display any AP. You must leave these two fields blank.

**Note**

You must first assign the 'parent' role to the APs that will serve as the parents. Unless this is done, the Parent APs will not be displayed in the Preferred Parent and Backup Parent drop-down lists of other APs.

**Note**

The WDS Bridge feature on the user interface relates to WDS Bridge configuration. When you are configuring the WDS Bridge topology, you must select WDS Bridge for Satellite AP that is connected to the wired network. For more information, see [Wireless Bridge Configuration](#) on page 520.

- 11 To assign the roles, preferred parent and backup parent:
 - a From the radio **b/g** drop-down list of the Root APs — Ardal, Arthur, Athens and Auberon, click **Parent**.
 - b From the radio **a** drop-down list of the Root APs — Ardal, Arthur, Athens and Auberon, click **Parent**.
 - c From the radio **a** and radio **b/g** drop-down list of other APs, click the roles according to [Table 106](#) on page 533.
 - d From the **Preferred Parent** drop-down list of other APs, click the parents according to [Table 106](#) on page 533.
 - e From the **Backup Parent** drop-down list of other APs, click the backup parents according to [Table 106](#) on page 533.

Wireless APs services						
AP Name	Radio 1	Mode	Radio 2	Mode	Preferred Parent	Backup Parent
Ardal	parent ▼	a	parent ▼	b/g		
Arthur	parent ▼	a	parent ▼	b/g		
Athens	parent ▼	a	parent ▼	b/g		
Auberon	parent ▼	a	parent ▼	b/g		
Bawdy	both ▼	a	child ▼	b/g		
Bern	both ▼	a	child ▼	b/g		
Barend	both ▼	a	child ▼	b/g		
Barett	both ▼	a	child ▼	b/g		
Osborn	child ▼	a	child ▼	b/g		
Oscar	child ▼	a	child ▼	b/g		
Orson	child ▼	a	child ▼	b/g		
Oswald	child ▼	a	child ▼	b/g		

Figure 168: Wireless AP Services

- 12 Click **Save** to save your changes.

Assigning the Satellite Wireless APs' Radios to the Network WLAN Services

You must assign the Satellite wireless APs' radios to the network *WLAN* Services.



Note

Network WLAN Services are the typical WLAN Services on which the APs service the client devices: Routed, Bridge Traffic Locally at EWC, and Bridge Traffic Locally at AP. For more information, see [VNS Global Settings](#) on page 392.

To assign the satellite wireless APs' radios to the Network WLAN Service:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, expand the **WLAN Services** pane and select a network WDS service to edit

Wireless APs services							
AP Name	Radio 1	Mode	Radio 2	Mode	WDS bridge	Preferred Parent	Backup Parent
1548Y-1007900000	none ▼	a/n/ac	none ▼	g/n	<input type="checkbox"/>	▼	▼
14300167085D0000[F]	none ▼	a/n/ac	none ▼	g/n	<input type="checkbox"/>	▼	▼

- 3 In the **Wireless APs** list, select the radios of the Satellite APs — Osborn, Oscar, Orson and Oswald.



Note

If you want the Root AP and the Repeater APs to service the client devices, you must select their radios in addition to the radios of the Satellite APs.

- 4 To save your changes, click **Save**.
- 5 Log out from the wireless controller.

Connecting the WDS Wireless APs to the Enterprise Network for Provisioning

You must connect the WDS wireless APs to the enterprise network once more to enable them to obtain their configuration from the wireless controller. The configuration includes the pre-shared key, the AP's role, preferred parent and backup parent. For more information, see [Provisioning the WDS APs](#) on page 528.



Warning

If you skip this step, the WDS wireless APs will not work at their target location.

Moving the WDS Wireless APs to the Target Location

Note



If you change any of the following configuration parameters of a WDS AP, the WDS AP will reject the change: Reassigning the WDS AP's role from **Child** to **None**, Reassigning the WDS AP's role from **Both** to **Parent**, and changing the **Preferred Parent** of the WDS AP. However, the wireless controller will display your changes, as these changes will be saved in the database. To enable the WDS AP to obtain your changes, you must remove it from the WDS location and then connect it to the wireless Controller via the wired network.

Note



If you change any of the following radio properties of a WDS AP, the WDS AP will reject the change: Disabling the radio on which the WDS link is established, lowering the radio's Tx Power of a radio on which the WDS link is established, or changing the country

- 1 Disconnect the WDS wireless APs from the enterprise network, and move them to the target location.
- 2 Install the WDS APs at the target location.
- 3 Connect the APs to a power source. The discovery and registration processes are initiated.

Changing the Pre-shared Key in a WDS WLAN Service

To change the Pre-shared Key in a WDS WLAN Service:

- 1 Create a new WDS WLAN Service with a new pre-shared key.
- 2 Assign the RF of the APs from the old WDS to the new WDS WLAN Service.
- 3 Check the **WDS AP Statistics** report page to ensure that all the WDS APs have connected to the wireless controller via the new WDS VNS. For more information, see [Viewing Statistics for APs](#) on page 627.
- 4 Delete the old WDS WLAN Service. For more information, see [Deleting a VNS](#) on page 486.

13 Availability and Session Availability

Availability
Session Availability
Viewing SLP Activity

Availability

The Extreme Networks ExtremeWireless Software system provides the availability feature to maintain service availability in the event of a controller outage.



Note

During the failover event, the maximum number of failover APs the secondary controller can accommodate is equal to the maximum number of APs supported by the hardware platform.

Wireless APs that attempt to connect to the secondary controller during a failover event are assigned to the *WLAN (Wireless Local Area Network)* Service that is defined in the system's default AP configuration, provided the administrator has not assigned the failover APs to one or more VNSs. If a system default AP configuration does not exist for the controller (and the administrator has not assigned the failover APs to any WLAN Service), the APs will not be assigned to any WLAN Service during the failover.

A controller will not accept a connection by a foreign AP if the controller believes its availability partner controller is in service. Also, the default AP configuration assignment is only applicable to new APs that failover to the backup controller. Any AP that has previously failed over and is already known to the backup system will receive the configuration already present on that system. For more information, see [Configuring the Default Wireless AP Settings](#) on page 134.

During the failover event when the AP connects to the secondary controller, the users are disassociated from the AP. Consequently, the users must log on again and be authenticated on the secondary controller before the wireless service is restored.



Note


If you want the mobile user's session to be maintained, you must use the 'session availability' feature that enables the primary controller's APs to failover to the secondary controller fast enough to maintain the session availability (user session). For more information, see [Session Availability](#) on page 545.

The availability feature provides APs with a list of local active interfaces for the active controller as well as the active interfaces for the backup controller. The list is sorted by top-down priority.

If the connection with an active controller link is lost (poll failure), the AP automatically scans (pings) all addresses in its availability interface list. The AP then connects to the highest priority interface that responds to its probe.

Events and Actions in Availability

If one of the controllers in a pair fails, the communication between the two controllers stops. This triggers a failover condition and a critical message is displayed in the information log of the secondary controller.

	Home	Logs	Reports	Controller	AP	VNS	WIPS
EWC: Events Station Events Restore/Import S/W Upgrade •AP: Logs Traces •Audit: UI •Services:							
Severity: Critical Major Minor Info All							
Timestamp ▾	Type	Component	Log Message				
11/01/17 11:37:52	Critical	RU Manager	Availability: Moving into failover mode				
10/03/17 12:07:46	Critical	RU Manager	Availability: Moving into failover mode				
09/28/17 10:46:58	Critical	RU Manager	Availability: Moving into failover mode				
09/27/17 14:24:07	Critical	RU Manager	Availability: Moving into failover mode				
09/27/17 13:23:01	Critical	RU Manager	Availability: Moving into failover mode				
09/27/17 09:19:43	Critical	RU Manager	Availability: Moving into failover mode				
09/26/17 13:25:18	Critical	RU Manager	Availability: Moving into failover mode				
08/15/17 09:50:14	Critical	RU Manager	Availability: Moving into failover mode				
07/28/17 20:19:39	Critical	RU Manager	Availability: Moving into failover mode				
07/21/17 11:39:45	Critical	RU Manager	Availability: Moving into failover mode				
06/06/17 16:26:57	Critical	RU Manager	Availability: Moving into failover mode				
06/06/17 14:29:50	Critical	RU Manager	Availability: Moving into failover mode				

After an AP on the failed controller loses its connection, it will try to connect to all enabled interfaces on both controllers without rebooting. If the AP is not successful, it will begin the discovery process. If the AP is not successful in connecting to the controller after five minutes of attempting, the AP will reboot if there is no **Bridge traffic locally at the AP** topology associated to it.

All mobile user's sessions using the failover AP will terminate except those associated to a **Bridge traffic locally at the AP** and if the **Maintain client sessions in event of poll failure** option is enabled on the **AP Properties** tab or **AP Default Settings** screen.

When the APs connect to the second controller, they are either assigned to the VNS that is defined in the system's default AP configuration or manually configured by the administrator. The mobile users log on again and are authenticated on the second controller.

When the failed controller recovers, each controller in the pair goes back to normal mode. They exchange information including the latest lists of registered APs. The administrator must release the APs manually on the second controller, so that they may re-register with their home controller. Foreign APs can now all be released at once by using the **Approve as Foreign** button on the **Access Approval** screen to select all foreign APs, and then clicking **Release**.

To support the availability feature during a failover event, you need to do the following:

- 1 Monitor the critical messages for the failover mode message, in the information log of the remaining controller (in the **Logs & Traces** section of the Wireless Assistant).
- 2 After recovery, on the controller that did not fail, select the foreign APs, and then click **Release** on the **Access Approval** screen.

Availability Prerequisites

Before you configure availability, you must do the following:

- Choose the primary and secondary controllers.
- Verify the network accessibility for the UDP connection between the two controllers. The availability link is established as a UDP session on port 13911.
- Set up a *DHCP (Dynamic Host Configuration Protocol)* server for AP subnets to support Option 78 for SLP, so that it points to the IP addresses of the physical interfaces on both the controllers.
- Ensure that the Poll Timeout value on the **AP Properties** tab **Advanced** dialog is set to 1.5 to 2 times of **Detect link failure** value on the **Controller > Availability** screen. For more information, see **AP Properties Tab - Advanced Settings** on page 164.

If the Poll Timeout value is more than 1.5 to 2 times of Detect link failure value, the APs failover will be unnecessarily delayed, because the APs will continue polling the primary controller even though the secondary controller is ready to accept them as the failover APs.

- To achieve ideal availability behavior, set the Poll Timeout value for all APs to 15 seconds, and the Detect link failure on the **Controller > Availability** screen to 10 seconds.

Configuring Availability Using the Availability Wizard

The availability wizard allows you to create an availability pair from one of the controllers that will be in the availability pair. When creating the availability pair, you also have the option to synchronize VNS definitions and GuestPortal user accounts between the paired controllers.

To configure availability using the availability wizard:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Administration > Availability**.

- 3 In the **Availability Wizard** section, click **Start**.

The **Availability Pair Wizard** screen displays.

- 4 In the **Connection Details** section, do the following:
- **Select Port** — Select the port and IP address of the primary controller that is to be used to establish the availability link.
 - **Peer Controller IP** — Type the IP address of the peer (secondary) controller.
 - **User** — Type the login user name credentials of an account that has full administrative privileges on the peer controller.
 - **Password** — Type the login password used with the user ID to login to the peer controller.
 - **Enable Fast Failover** — Select this check box to enable Fast Failover for the availability pair.
- 5 In the **Synchronize Options** section, do the following:

- **Synchronize System Configuration** — Select this check box to push the configured **Routed** and **Bridge Traffic Locally at Controller** VNS definitions from the primary controller to the peer controller. **WDS** and **3rd Party AP VNS** definitions are ignored and not synchronized.



Note

Synchronizing the VNS definitions will delete and replace existing VNS definitions on the peer controller.

- **Synchronize Guest Portal Accounts** — Select this check box to push GuestPortal user accounts to the peer controller.

- 6 Click **Next**.

- 7 If you are synchronizing topology definitions, the **Topology Definitions** screen displays. Do the following:
 - a In the Synchronization Settings section, complete the topology properties that are missing. Any topology that did not already exist on the peer controller will have missing properties on the **Topology Definitions** screen.
 The fields configured are actual parameter values that are configured at the remote Controller with respect to associated topologies chosen for synchronization. Some of these parameters are: Interface IP address, Netmask, L2 port, VLAN (Virtual LAN) ID, DHCP range, etc.
 - b Click **Finish**.
- 8 If you are not synchronizing topology definitions, the availability wizard completes the configuration.
- 9 Click **Close**.

This operation marks the desired topologies for synchronization. The two controllers exchange information and the configuration is applied to the remote controller.

On the local controller, the “Enable Synchronization of System Configuration” becomes selected. This can be double checked by navigating to **VNS > Global > Sync Summary**. This tab also lists all topologies, roles, WLAN Services and VNSes with their synchronization status (on or off).

The Sync status for any of these elements can also be changed from this tab.

All these configurable elements have a Synchronize check box (on their main/general configuration tab) that allows for individual control and selection of availability from the main element configuration page.

Configuring Availability Manually

When configuring availability manually, you configure each controller separately.

- 1 On the wireless controller **Availability** screen, set up the controller in **Paired Mode**.
- 2 On the **VNS configuration** window, define a VNS (through topology, WLAN service, role and VNS configuration) on each controller with the same SSID. The IP addresses must be unique. For more information, see **Manually Creating a VNS** on page 423. A controller VLAN Bridged topology can permit two controllers to share the same subnet. This setup provides support for mobility users in a VLAN Bridged VNS.
- 3 On both controllers, on the AP Registration screen, select the Security Mode **Allow only approved APs to connect** option so that no more APs can register unless they are approved by the administrator.
- 4 On each controller, on the AP configuration **Access Approval** screen, check the status of the APs and approve any APs that should be connected to that controller.

System AP defaults can be used to assign a group of VNSs to the foreign APs:

- If the APs are not yet known to the system, the AP will be initially configured according to AP default settings. To ensure better transition in availability, Extreme Networks recommends that the AP default settings match the desired assignment for failover APs.
- AP assignment to WLAN Services according to the AP default settings can be overwritten by manually modifying the AP assignment. (For example, select and assign each WLAN service that the AP should connect to.)
- If specific foreign APs have been assigned to a WLAN service, those specific foreign AP assignments are used.

Alternate Method to Setting Up a Wireless AP

An alternate method to setting up Wireless APs for Availability mode include:

- 1 Add each AP manually to each controller.
- 2 On the **AP Properties** screen, click **Add Wireless AP**.
- 3 Define the AP, and then click **Add Wireless AP**.

Manually defined APs will inherit the default AP configuration settings.



Caution

If two wireless controllers are paired and one has the Allow All option set for AP registration, all APs will register with that wireless controller.

Setting the Primary or Secondary Wireless Controllers for Availability

To set the primary or secondary controllers for availability:

- 1 From the top menu, click **Controller**. The **Wireless Controller Configuration** screen displays.
- 2 In the left pane, click **Administration** > **Availability**.

The screenshot shows the 'Wireless Controller Configuration' screen. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller' (selected), 'AP', 'VNS', and 'WIPS'. The left sidebar shows 'Administration' selected, with sub-items: 'Availability', 'Flash', 'Host Attributes', 'Installation Wizard', 'Login Management', 'Software Maintenance', 'System Maintenance', and 'Web Settings'. The main content area is titled 'Availability Wizard' and contains a 'Start' button. Below this is the 'Controller Availability Settings' section, which has two radio buttons: 'Stand-alone' (selected) and 'Paired'. Under the 'Paired' option, there is a 'Wireless Controller IP Address' field with the value '0.0.0.0'. There are also two checkboxes: 'Current Wireless Controller is primary connection point' and 'Fast Failover', both of which are unchecked. At the bottom, there is a 'Detect link failure in' field with the value '8' and a note '(2 - 30 seconds)'.

- 3 To enable availability, select the **Paired** option.
- 4 Do one of the following:
 - For a primary controller, in the **Wireless IP Address** box, type the IP address of the data interface of the secondary controller. This IP address must be on a routable subnet between the two controllers.
 - For a secondary controller, in the **Wireless IP Address** box, type the IP address of the Management port or data interface of the primary controller.

5 Set this controller as the primary or secondary connection point:

- To set this controller as the primary connection point, select the **Current Wireless is primary connect point** check box.
- To set this controller as the secondary connection point, clear the **Current Wireless is primary connect point** check box.

If the **Current Wireless is primary connect point** check box is selected, the specified controller sends a connection request. If the **Current Wireless is primary connect point** check box is cleared, the specified controller waits for a connection request. Confirm that one controller has this check box selected, and the second controller has this check box cleared, since improper configuration of this option will result in incorrect network configuration.

6 On both the primary and secondary controllers, type the **Detect link failure value**.



Note

Ensure that the Detect link failure value on both the controllers is identical.

7 On both the primary and secondary controllers, select the **Synchronize GuestPortal Guest Users** option to synchronize GuestPortal guest accounts between the controllers.

8 From the top menu, click **AP**.

9 In the left pane, click **Global Settings > AP Registration**. To set the **security mode** for the controller, select one of the following options:

- **Allow all wireless APs to connect** — If the controller does not recognize the serial number, it sends a default configuration to the AP. Or, if the controller recognizes the serial number, it sends the specific configuration (port and binding key) set for that AP.
- **Allow only approved wireless APs to connect** — If the controller does not recognize the serial number, the APs will be in pending mode and the administrator must manually approve them. Or, if the controller recognizes the serial number, it sends the configuration for that AP.



Note

During the initial setup of the network, it is recommended that you select the **Allow all Wireless APs to connect** option. This option is the most efficient way to get a large number of APs registered with the controller. Once the initial setup is complete, it is recommended that you reset the security mode to the **Allow only approved Wireless APs to connect** option. This option ensures that no unapproved APs are allowed to connect. For more information, see [Configuring Wireless AP Properties](#) on page 156.

10 To save your changes, click **Save**.



Note

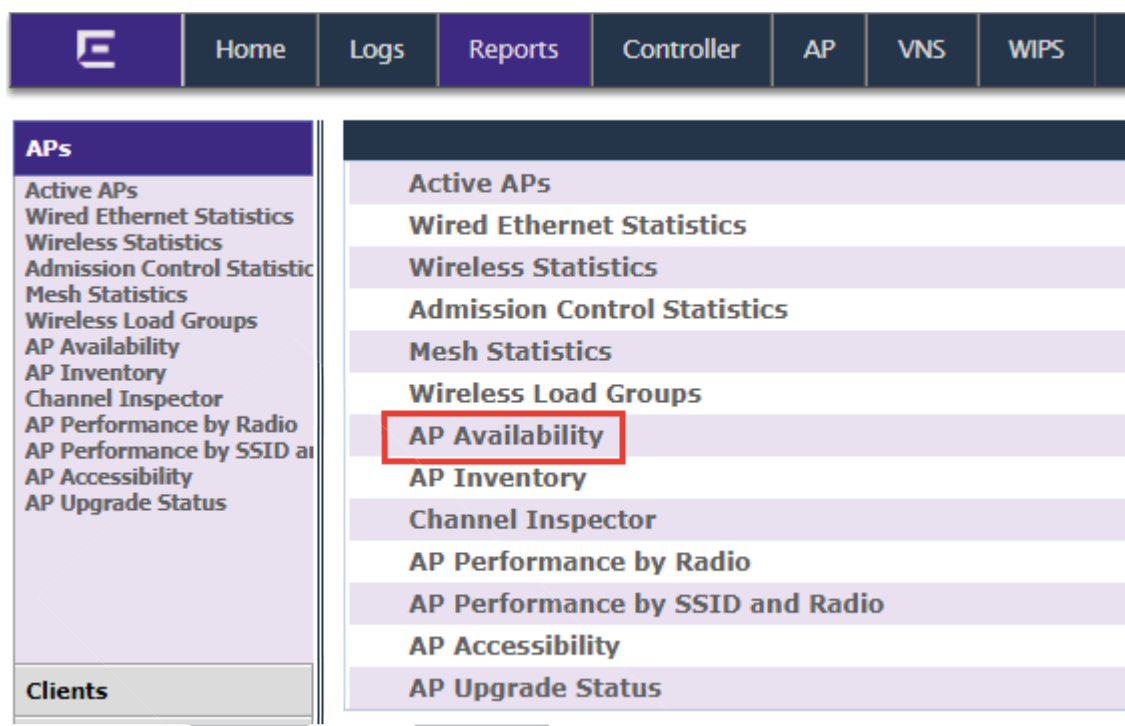
When two controllers have been paired as described above, each controller's registered APs will appear as foreign on the other controller in the list of available APs when configuring a VNS topology.

11 Verify that availability is configured correctly.

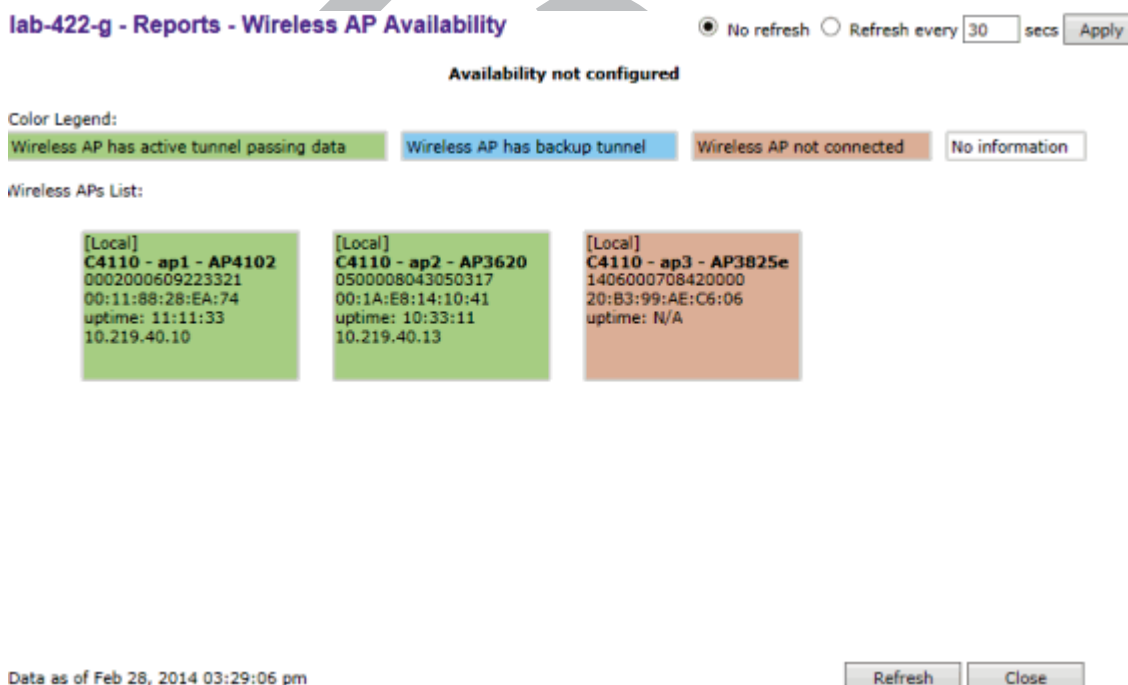
Verifying Availability

To verify that availability is configured correctly:

- 1 From the top menu of either of the two controllers, click **Reports**.



- 2 From the **Reports and Displays** menu, click **AP Availability**. The Wireless Availability Report is displayed.



- 3 Check the statement at the top of the screen.

If the statement reads **Availability link is up**, the availability feature is configured correctly. If the statement reads **Availability link is down**, check the configuration error logs. For more information on logs, see the Extreme Networks *ExtremeWireless Maintenance Guide*.

Session Availability

Session availability enables wireless APs to switch over to a standby (secondary) wireless controller fast enough to maintain the mobile user's session availability in the following scenarios:

- The primary wireless controller fails (see [Figure 169](#)).

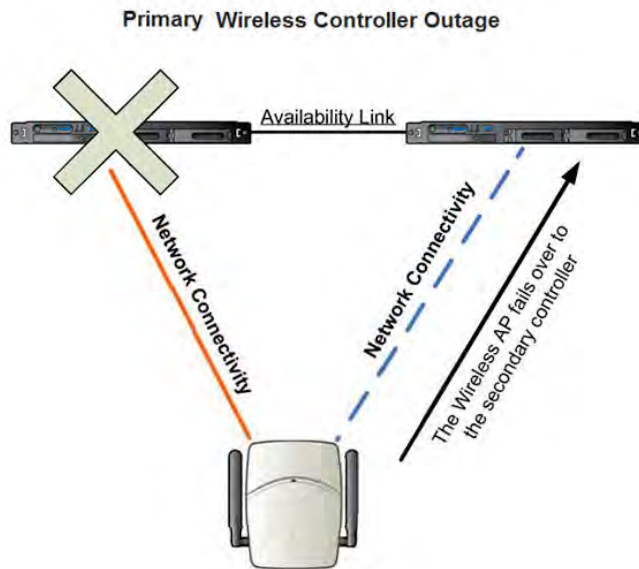


Figure 169: AP Fail Over When Primary Controller Fails

- The wireless AP's network connectivity to the primary controller fails (see [Figure 170](#)).

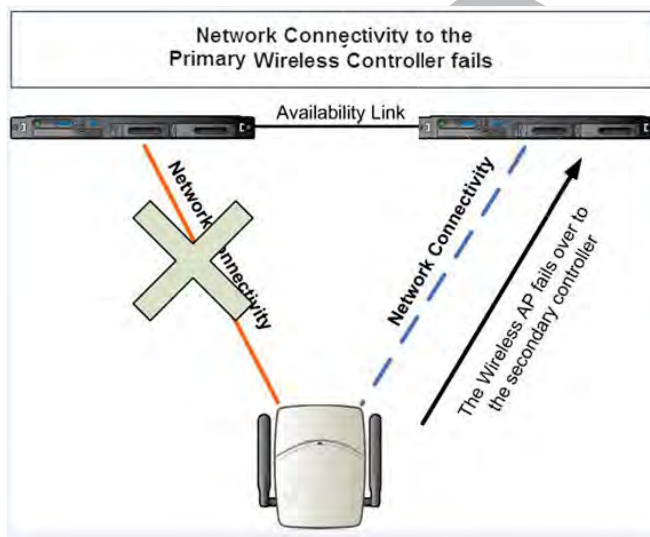


Figure 170: AP Fail Over When Connectivity to Primary Fails

The secondary controller does not have to detect its link failure with the primary controller for the session availability to kick in. If the AP loses five consecutive polls to the primary controller either due to the controller outage or connectivity failure, it fails over to the secondary controller fast enough to maintain the user session.

In session availability mode (Figure 171), the APs connect to both the primary and secondary controllers. While the connectivity to the primary controller is via the “active” tunnel, the connectivity to the secondary controller is via the “backup” tunnel.

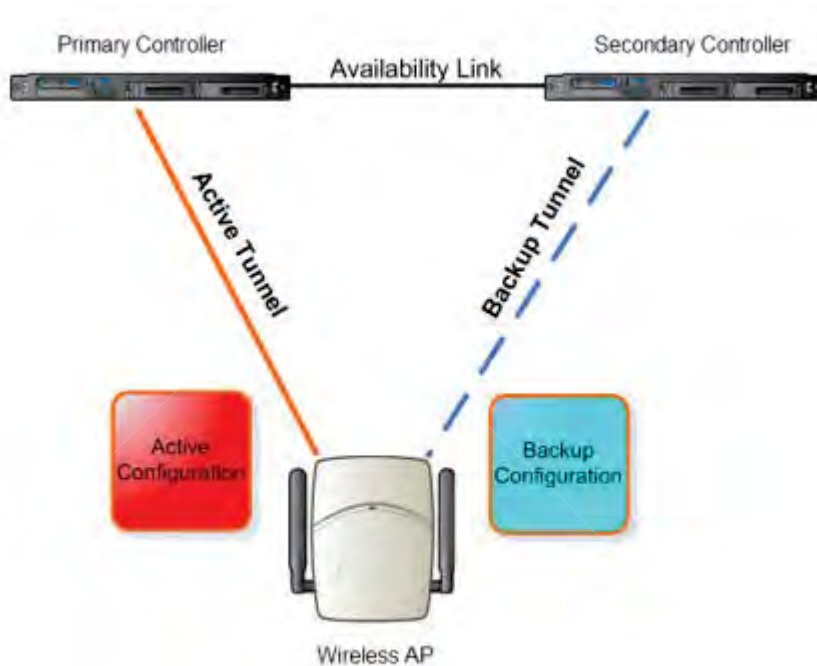


Figure 171: Session Availability Mode

The following is the traffic flow of the topology illustrated in Figure 171:

- The AP establishes the active tunnel to connect to the primary controller.
- The controller sends the configuration to the AP. This configuration also contains the port information of the secondary controller.
- On the basis of the secondary controller’s port information, the AP connects to the secondary controller via the backup tunnel.
- After the connection is established via the backup tunnel, the secondary controller sends the backup configuration to the wireless AP.
- The AP receives the backup configuration and stores it in its memory to use it for failing over to the secondary controller. All this while, the AP is connected to the primary controller via the ‘active’ tunnel.

Session availability applies only to the following topologies:

- Bridge Traffic Locally at Controller
- Bridge Traffic Locally at AP

Events and Actions in Session Availability

In the event of a primary controller outage, or the network connectivity failure to the primary controller, the wireless AP:

- Sends a 'tunnel-active-req' request message to the secondary controller.
- The secondary controller accepts the request by sending the 'tunnel-activate-response' message.
- The AP applies the backup configuration and starts sending the data. The client devices' authentication state is not preserved during failover.

When the fast failover takes place, a critical message is displayed in the information log of the secondary controller.



Note

In session availability, the maximum number of failover APs that the secondary controller can accommodate is equal to the maximum number of APs supported by the hardware platform.

When the failed controller recovers, each controller in the pair goes back to normal mode. They exchange information that includes the latest lists of registered APs. The administrator must release the APs manually on the second controller, so that they may re-register with their home controller. Foreign APs can now all be released at once by using the **Approve as Foreign** button on the **Access Approval** screen to select all foreign APs, and then clicking **Released**.

To support the availability feature during a failover event, administrators need to do the following:

- 1 Monitor the critical messages for the failover mode message, in the information log of the secondary controller (in the **Logs & Traces** section of the Wireless Assistant).
- 2 After recovery, on the secondary controller, select the foreign APs, and then click **Release** on the **Access Approval** screen.

After the APs are released, they establish the active tunnel to their home controller and backup tunnel to the secondary controller.

Enabling Session Availability

Session availability is supported when fast failover is enabled and when "Synchronize System Configuration" is selected. For more information, see [Configuring Fast Failover and Enabling Session Availability](#) on page 548.

In session availability, mobile user devices are able to retain their IP address. In addition, the mobile user device does not have to re-associate after the failover. These characteristics ensure that the failover is achieved within 5 seconds, which is fast enough to maintain the mobile user's session.



Note

In session availability, the fast failover is achieved within 5 seconds only if there is at least one client device (mobile unit) associated to the AP. In the absence of any client device, the AP takes more time to failover since there is no need to preserve the user session.

The authentication state is not preserved during fast failover. If a WLAN Service requires authentication, the client device must re-authenticate. However, in such a case, the session availability is not guaranteed because authentication may require additional time during which the user session may be disrupted.

Session availability is not supported in a WLAN Service that uses Captive Portal (CP) authentication.

Session availability does not support user-specific filters as these filters are not shared between the primary and secondary controller.

Configuring Fast Failover and Enabling Session Availability

Before you configure the fast failover feature, ensure the following:

- The primary and secondary controllers are properly configured in availability mode. For more information, see [Availability](#) on page 537.
- The pair of controllers in availability mode is formed by one of the following combinations:
 - C5110 and C5110
 - C5210 and C5210
 - C5215 and C5215
 - C4110 and C4110
 - C5110 and C4110
 - V2110 and V2110 (Using the same V2110 profile, two V2110 Small, or two V2110 Medium, or two V2110 Large.)
 - C25 and C25
 - C35 and C35
- Both the primary and secondary controllers are running the most recent Extreme Networks ExtremeWireless software.
- A network connection exists between the two controllers.
- The APs are operating in availability mode.
- The deployment is designed in such a way that the service provided by the APs is not dependent on which controller the APs associate with. For example, the fast failover feature will not support the deployment in which the two controllers in availability mode are connected via a WAN link.
- Both the primary and secondary controllers have equivalent upstream access to the servers on which they depend. For example, both the controllers must have access to the same RADIUS and DHCP servers.
- The users (client devices) that use DHCP must obtain their addresses from a DHCP Server that is external to the controller.
- Time on all the network elements (both the controllers in availability pair, APs, DHCP and RADIUS servers etc.) is synchronized. For more information, see [Configuring Network Time](#) on page 89.



Note

The fast failover feature works optimally in fast networks (preferably switched networks).

To configure Fast Failover and enable Session Availability:

- 1 Log on to both the primary and secondary controllers.
- 2 From the top menu of the primary controller, click **Controller**.

- 3 In the left pane, click **Administration** > **Availability**.

- 4 Under **Controller Availability Settings**, select **Paired**.
- 5 Select the **Fast Failover** check box.
- 6 Type the appropriate value in the **Detect link failure** box.

The **Detect link failure** field specifies the period within which the system detects link failure after the link has failed. For fast failover configuration, this parameter is tied closely to the **Poll Timeout** parameter on the **AP Properties** tab **Advanced** dialog. The **Poll Timeout** field specifies the period for which the wireless AP waits before re-attempting to establish a link when its polling to the primary controller fails.

For the fast failover feature to work within 5 seconds, the **Poll Timeout** value should be 1.5 to 2 times the **Detect link failure** value. For example, if you have set the **Detect link failure** value to 2 seconds, the **Poll Timeout** value should be set to 3 or 4 seconds.

- 7 In the **Synchronization Option** area, select **Synchronize System Configuration**.

This is a global parameter that enables synchronization of VNS configuration components (topology, role, *WLAN* Service, VNS) on both controllers paired for availability and/or fast failover.

For more information about synchronization, see [Using the Sync Summary](#) on page 414.

- 8 Click **Save**.

- 9 Set the APs' **Poll Timeout** value for fast failover.
 - a From the top menu of the primary controller, click **AP**.
 - b Select the check box for one or more APs.
 - c Click **Actions > Multi Edit**.
The **Multi Edit** dialog displays.

The screenshot shows the **Multi Edit** dialog box. The **AP Properties** section is expanded, showing various configuration fields. The **Poll Timeout [Seconds]** field is highlighted with a red rectangle. Below it are fields for **Secure Tunnel**, **Secure Tunnel Lifetime [hours]**, **Remote Access**, **Location-based Service**, **Maintain client sessions in event of poll failure**, **Restart service without controller**, **Use broadcast for disassociation**, **LLDP**, **Multicast prioritized as voice**, **IP Multicast Assembly**, **Balanced Channel List Power**, **LED**, **Country**, and **Antennas**. The **Radio Settings** section is also expanded, showing fields for **Radio 1** and **Radio 2**, including **Admin Mode**, **Radio Mode**, and **Channel Width**. At the bottom are **Apply** and **Close** buttons.

- d In the **Poll Timeout** field, enter the poll timeout value in seconds.
- e Click **Apply**.

Note

ExtremeWireless® V10-411-06 User Guide
The failover configuration must be identical on both the primary and secondary controllers. Logs are generated if the configuration is not identical. For more information, see the ExtremeWireless *Maintenance Guide*.

After you have configured fast failover, you can verify session availability to preserve the user session during the failover.

Verifying Session Availability

To have session availability, you must ensure the following:

- The primary and secondary wireless controllers are properly configured in 'availability' mode. For more information, see [Availability](#) on page 537.
- The fast failover feature is properly configured. For more information, see [Configuring Fast Failover and Enabling Session Availability](#) on page 548.



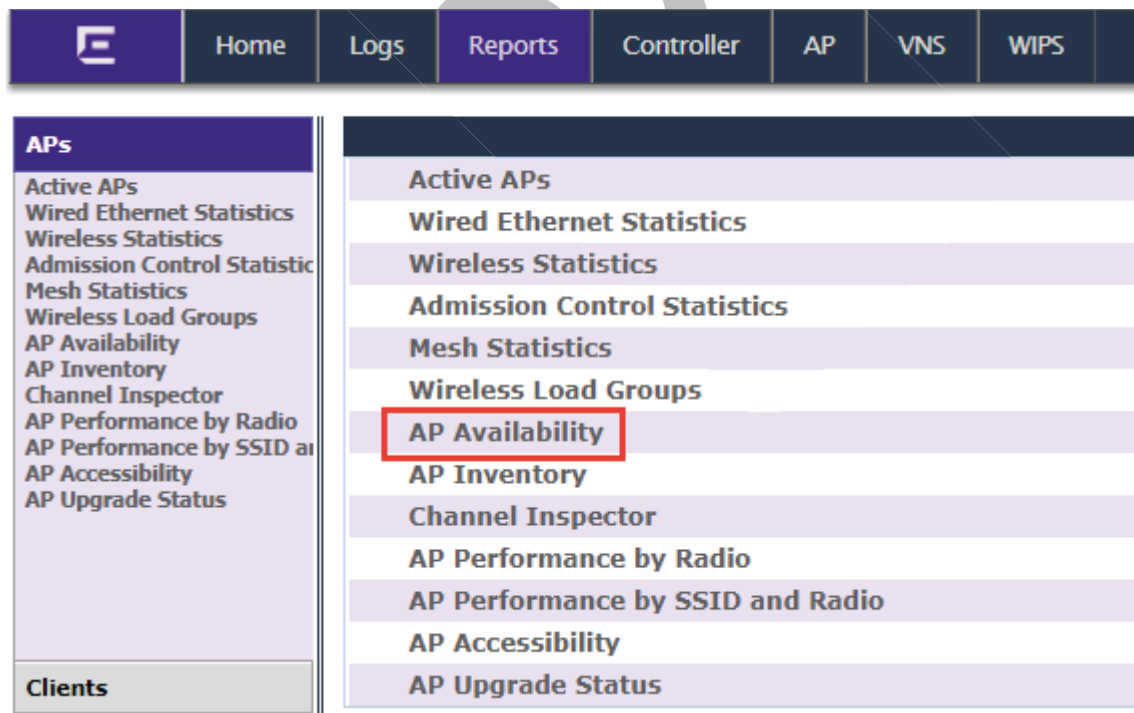
Note

If you haven't configured the fast failover feature, the **Enable Session Availability** check box is not displayed.

- Time on all the network elements — both the wireless controllers in availability pair, APs, [DHCP](#) and RADIUS servers etc. — is synchronized. For more information, see [Configuring Network Time](#) on page 89.
- Both the wireless controllers in fast failover mode must be running the most recent wireless controller software release.
- If you are using **Bridge Traffic Locally at Controller** topology, you must select **None** from the **DHCP Option** drop-down menu.
- The **Bridge Traffic Locally at Controller** must be mapped to the same [VLAN](#) on both the primary and secondary wireless controllers.

To Verify that the session availability feature is configured correctly:

- 1 From the top menu of either of the two controllers, click **Reports**.



- From the **Reports and Displays** menu, click **Wireless AP Availability**. The **Wireless Availability Report** is displayed.

Lab-110 - Reports - Wireless AP Availability ☒ No refresh ☐ Refresh every 30

Availability Link is UP

Color Legend:

- Wireless AP has active tunnel passing data
- Wireless AP has backup tunnel
- Wireless AP not connected

Wireless APs List:

AP ID	MAC Address	IP Address	Uptime	Status
[Foreign] 1637Y-1003100000	1637Y-1003100000	D8:84:66:74:FF:A7	uptime: N/A	Connected
[Local] AP3715i_12b269465000000	12b2694650000000	00:02:6F:EA:CF:44	uptime: 25 d, 23:57:10	Connected
[Local] AP3916_13c11223344550000	13c1122334455000	uptime: N/A		Not connected
[Local] AP3965i_1541D10030140001	1541D10030140001	00:1F:45:FF:F5:A0	uptime: 25 d, 23:55:13	Connected

- Check the statement at the top of the screen.
If the statement reads Availability link is up, the availability feature is configured correctly. If the statement reads Availability link is down, check the configuration error in logs. For more information on logs, see the Extreme Networks ExtremeWireless *Maintenance Guide*.

Verify Synchronization

To verify that all elements have been synchronized correctly, navigate to the VNS tab on both the primary and secondary controllers, and confirm that the topologies, WLAN services, roles and desired VNSs are displayed as **[synchronized]**.

You can verify this by selecting the appropriate tabs and then inspecting the Synchronized flags or by navigating to **VNS > Global > Sync Summary**.

Configuration synchronization:

- VNS configuration related synchronization will be supported with legacy or fast failover availability configuration as long as there is an availability link established.
- Synchronization for VNS, WLAN Services, Roles, Topologies, and Rate Limit Profiles can be enabled/disabled individually.

- VNS, WLAN Service, Role, Topology, and Rate Limit Profile configuration will be dynamically synchronized when synchronization is enabled individually between a pair of controllers.

MU session synchronization:

- MU session synchronization will be supported only when there is fast failover configured between two controllers.
- If mobility is disabled, MU session with Bridge Traffic Locally at AP, Bridge Traffic Locally at Controller, and Routed topologies will all be synchronized between a pair of controllers.
- If mobility is enabled, an MU session with Routed topologies will not be synchronized.

Viewing SLP Activity

In normal operations, the primary controller registers as an SLP service called ac_manager. The controller service directs the APs to the appropriate controller. During an outage, if the remaining controller is the secondary controller, it registers as the SLP service ru_manager.

To view SLP activity:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global Settings > AP Registration**.

Wireless AP Registration

Security Mode:

- ☒ Allow all Wireless APs to connect
- ☐ Allow only approved Wireless APs to connect

Discovery Timers:

Number of retries: (1 - 255)

Delay between retries: (1 - 10 seconds)

SSH Access:

Password:

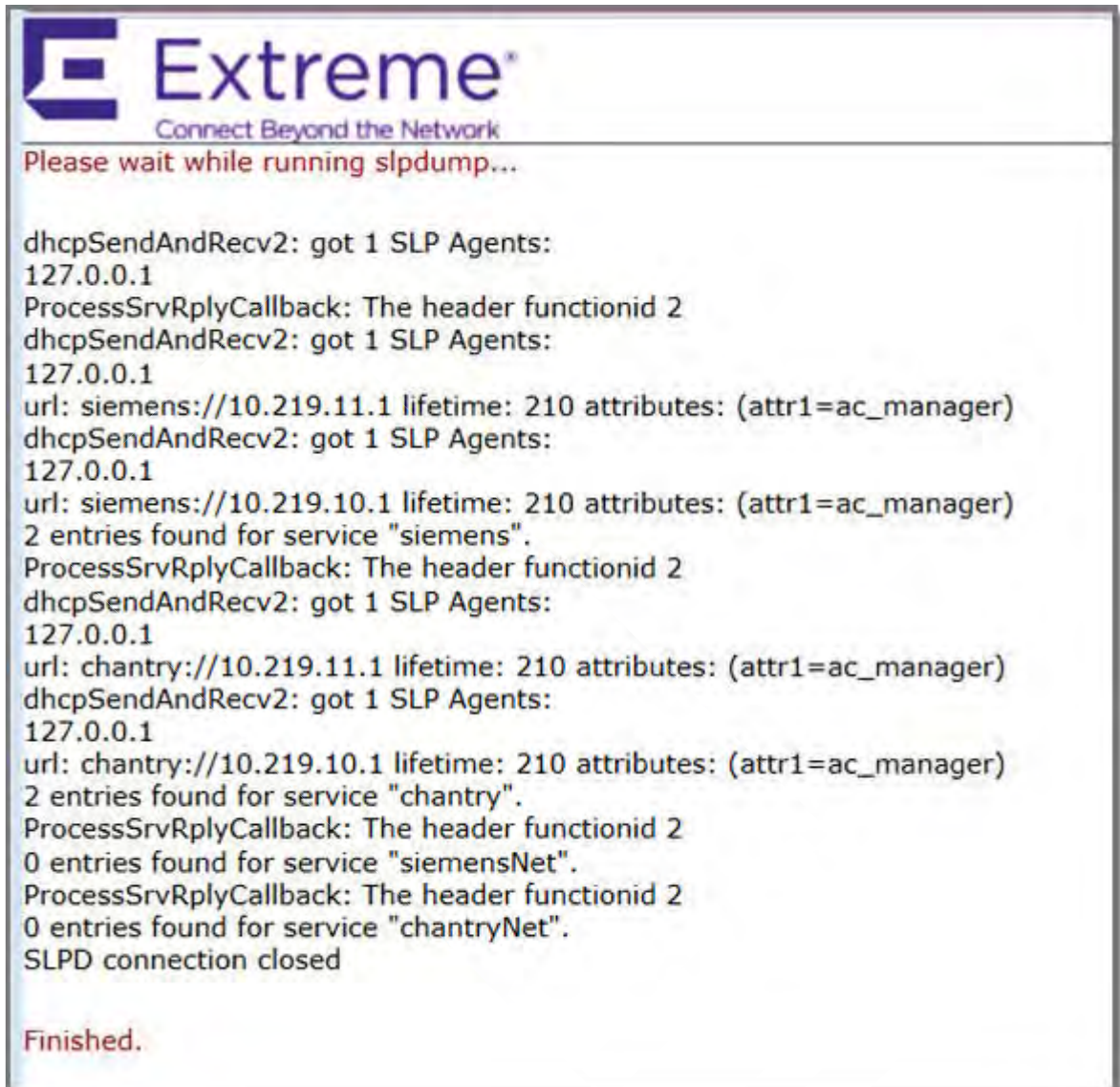
Confirm password:

Secure Cluster:

Cluster Shared Secret:

☐ Use Cluster Encryption

- 3 To confirm SLP registration, click **View SLP Registration**. A screen displays the results of the diagnostic slpdump tool, to confirm SLP registration.

The screenshot shows a web interface for Extreme Networks. At the top left is the Extreme logo with the tagline "Connect Beyond the Network". Below the logo, a red message says "Please wait while running slpdump...". The main area displays the output of the slpdump tool, showing SLP agent information for "siemens" and "chantry" services. The output includes IP addresses (127.0.0.1), URIs, lifetimes, and attributes. It also shows the results of service discovery for "siemensNet" and "chantryNet", indicating 0 entries found for each. The session ends with "SLPD connection closed" and a red "Finished." message at the bottom.

```
dhcpcSendAndRecv2: got 1 SLP Agents:
127.0.0.1
ProcessSrvRplyCallback: The header functionid 2
dhcpcSendAndRecv2: got 1 SLP Agents:
127.0.0.1
url: siemens://10.219.11.1 lifetime: 210 attributes: (attr1=ac_manager)
dhcpcSendAndRecv2: got 1 SLP Agents:
127.0.0.1
url: siemens://10.219.10.1 lifetime: 210 attributes: (attr1=ac_manager)
2 entries found for service "siemens".
ProcessSrvRplyCallback: The header functionid 2
dhcpcSendAndRecv2: got 1 SLP Agents:
127.0.0.1
url: chantry://10.219.11.1 lifetime: 210 attributes: (attr1=ac_manager)
dhcpcSendAndRecv2: got 1 SLP Agents:
127.0.0.1
url: chantry://10.219.10.1 lifetime: 210 attributes: (attr1=ac_manager)
2 entries found for service "chantry".
ProcessSrvRplyCallback: The header functionid 2
0 entries found for service "siemensNet".
ProcessSrvRplyCallback: The header functionid 2
0 entries found for service "chantryNet".
SLPD connection closed

Finished.
```

14 Configuring Mobility

Mobility Overview

Mobility Domain Topologies

Configuring a Mobility Domain

Mobility Overview

The ExtremeWireless system allows up to 12 controllers on a network to discover each other and exchange information about a client session. This technique enables a wireless device user to roam seamlessly between different APs on different controllers.

The solution introduces the concept of a mobility manager; one controller on the network is designated as the mobility manager and all others are designated as mobility agents.

The wireless device keeps the IP address, and the service assignments it received from its home controller—the controller that it first connected to. The WLAN (Wireless Local Area Network) Service on each controller must have the same SSID and RF privacy parameter settings.

You have two options for choosing the mobility manager:

- Rely on SLP with DHCP (Dynamic Host Configuration Protocol) Option 78
- Define at the agent, the IP address of the mobility manager. By explicitly defining the IP address, the agent and the mobility manager are able to find each other directly without using the SLP discovery mechanisms. Direct IP definition is recommended to provide tighter control of the registration steps for multi-domain installations.

The controller designated as the mobility manager:

- Is explicitly identified as the manager for a specific mobility domain. Agents connect to this manager to establish a mobility domain.
- Defines, at the agent, the IP address of the mobility manager, which allows for the bypass of SLP. Agents directly find and attempt to register with the mobility manager.
- Uses SLP, if this method is preferred, to register itself with the SLP Directory Agent as Extreme NetworksNet.
- Defines the registration behavior for a multi-controller mobility domain set:
 - **Open mode** — A new agent is automatically able to register itself with the mobility manager and immediately becomes part of the mobility domain.
 - **Secure mode** — The mobility manager does not allow a new agent to automatically register. Instead, the connection with the new agent is placed in a pending state until the administrator approves the new device.
- Listens for connection attempts from mobility agents.
- Establishes connections and sends a message to the mobility agent specifying the heartbeat interval, and the mobility manager's IP address if it receives a connection attempt from the agent.

- Sends regular heartbeat messages containing wireless device session changes and agent changes to the mobility agents and waits for a returned update message.
- Establishes a connection to an optional backup mobility manager that can be configured to back up the primary mobility manager.

The controller designated as a mobility agent does the following:

- Uses SLP or a statically configured IP address to locate the mobility manager.
- Defines at the agent the IP address of the mobility manager, which allows for the bypass of SLP. Agents directly find and attempt to register with the mobility manager.
- Attempts to establish a TCP/IP connection with the mobility manager.
- Connects to an optional backup mobility manager that can be configured to back up the primary mobility manager.
- Sends updates, in response to the heartbeat message, on the wireless device users and the data tunnels to the mobility manager.

If a controller configured as the mobility manager is lost, with a backup mobility manager configured, the following occurs:

- If enabled, the controller establishes a connection to the optional backup mobility manager. When a failure occurs, the backup manager becomes the primary manager and control tunnels are re-negotiated. The data tunnels are not affected. When the primary manager comes back online, the backup manager detects the higher priority manager and switches back to agent (passive) mode.

If a controller configured as the mobility manager is lost, without a backup mobility manager, the following occurs:

- Agent to agent connections remain active.
- The mobility agents continue to operate based on the mobility information last coordinated before the manager link was lost. The mobility location list remains relatively unaffected by the controller failure. Only entries associated with the failed controller are cleared from the registration list, and users that have roamed from the manager controller to other agents are terminated and required to re-register as local users with the agent where they are currently located.
- The data link between active controllers remains active after the loss of a mobility manager.
- Mobility agents continue to use the last set of mobility location lists to service known users.
- Existing users remain in the mobility scenario, and if the users are known to the mobility domain, they continue to be able to roam between connected controllers.
- New users become local at attaching controller.
- Roaming to another controller resets session.

The mobility network that includes all the wireless controllers and the APs is called the Mobility Domain.



Note

The mobility feature is not backward compatible. This means that all the controllers in the mobility domain must be running the most recent controller software release.

Mobility Domain Topologies

You can configure a mobility domain in the following scenarios:

- Mobility domain without availability
- Mobility domain with availability
- Mobility domain with session availability



Note

When configuring a mobility domain with availability or session availability, synchronize time on all the wireless controllers that are part of your mobility domain. For more information, see [Configuring Network Time](#) on page 89.

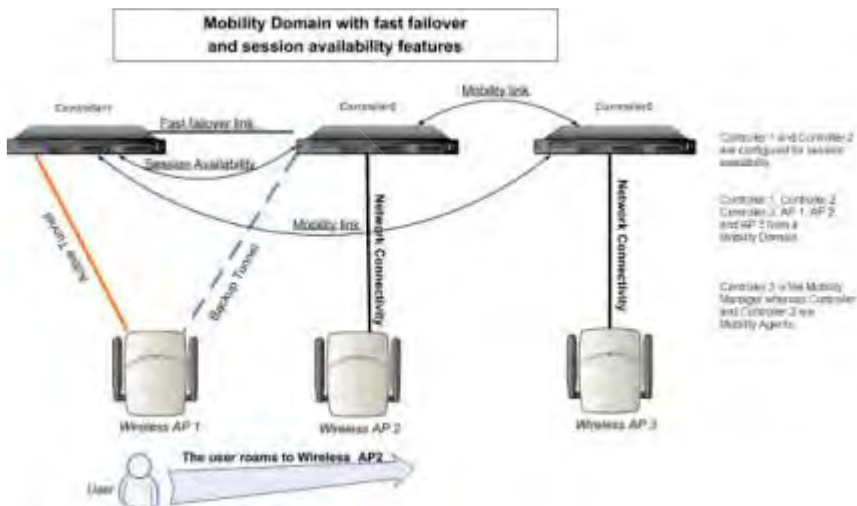


Figure 172: Mobility Domain with Fast Failover and Session Availability Features

- The user's home session is with Controller1.
- When the user roams from wireless AP 1 to wireless AP 2, he establishes his home session with Controller2.
- When the user roams, AP 1 receives a notification that the user has roamed away following which it marks the user session as "inactive". Consequently, no statistics are sent to the Controller 1 for that user.
- In response to the heart beat message from the mobility manager (Controller 3), the Controller 2 sends updates that the user has a new home on Controller 2. Upon receiving the updates, the mobility manager updates its own tables.



Note

The mobility manager's heart beat time is configurable. If you are configuring a mobility domain with session availability, you should configure the heart beat time as one second to enable the mobility manager to update its tables quickly.

- If a failover takes place, and the user is still associated with AP 1:
 - AP1 fails over, and establishes an active session with Controller 2.
 - In response to the heart beat message from the mobility manager (Controller 3), the Controller 2 sends updates to the mobility manager on the failover AP and its user.
- If a failover takes place, and the user has roamed to wireless AP 2:
 - As part of roaming, the user's home session moves from Controller 1 to Controller 2.
 - AP1 establishes active session with Controller 2. AP 2 is not impacted by the failover.

Configuring a Mobility Domain

When configuring a mobility domain with availability or session availability, synchronize time on all the wireless controllers that are part of your mobility domain. For more information, see [Configuring Network Time](#) on page 89.

Designating a Mobility Manager

To designate a mobility manager:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Services > Mobility Manager**.
- 3 To enable mobility for this controller, select the **Mobility** check box. The controller mobility options are displayed.

Mobility Manager Settings

☒ **Mobility**

☐ **This Wireless Controller is a Mobility Manager**

Port:

Heartbeat: seconds

SLP Registration:

Permission List: **Agent IP Address (State)**

192.168.0.133 (approved)	Approve
	Backup mgr
	Delete
	Add

Security Mode: ☐ Allow all mobility agents to connect
☒ Allow only approved mobility agents to connect

☐ **This Wireless Controller is a Mobility Agent**

- 4 Select the **This Wireless Controller is a Mobility Manager** option. The mobility manager options are displayed.
- 5 In the **Port** drop-down list, select the interface on the controller to be used for the mobility manager process. Ensure that the selected interface's IP address is routable on the network.

- 6 In the **Heartbeat** field, type the time interval (in seconds) at which the mobility manager sends a Heartbeat message to a mobility agent.

**Note**

When the mobility domain is configured for fast failover and session availability, configure the mobility manager's heart beat time as one second.

- 7 In the **SLP Registration** drop-down list, select whether to enable or disable SLP registration.
- 8 In the **Permission** list, select the agent IP addresses you want to approve that are in pending state, by selecting the agent and clicking **Approve**. New agents are only added to the domain if they are approved.
 - To add a controller to the mobility domain, type the agent IP address in the box, and then click **Add**. This can only be done from the primary manager.
 - To assign a backup manager, select a controller from the Permission List, and click **Backup mgr**.
 - To delete a controller, click the controller in the list, and then click **Delete**. This can only be done from the primary manager.
- 9 Select the **Security Mode** option:
 - **Allow all mobility agents to connect** — All mobility agents can connect to the mobility manager.
 - **Allow only approved mobility agents to connect** — Only approved mobility agents can connect to the mobility manager.
- 10 Click **Save**.

**Note**

If you set up one wireless controller on the network as a mobility manager, all other controllers must be set up as mobility agents.

Designating a Mobility Agent

To designate a mobility agent:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Services > Mobility Manager**.
- 3 Select the **Mobility** check box. The controller mobility options are displayed.

- 4 Select the **This Wireless Controller is a Mobility Agent** option. The mobility agent options are displayed.

The screenshot shows the 'Mobility Manager Settings' page. On the left is a navigation menu with the following items: Administration, Logs, Network, Services (highlighted), Location-based Service, and Mobility Manager. The main content area is titled 'Mobility Manager Settings'. Under the 'Mobility' section, there are two radio button options: 'This Wireless Controller is a Mobility Manager' (unselected) and 'This Wireless Controller is a Mobility Agent' (selected). Below these options, there are two dropdown menus: 'Port' set to 'physical 1 (10.0.0.1)' and 'Discovery Method' set to 'SLPD'.

- 5 From the **Port** drop-down list, select the port on the controller to be used for the mobility agent process. Ensure that the port selected is routable on the network.
- 6 From the **Discovery Method** drop-down list, select one of the following:
- **SLPD** — Service Location Protocol Daemon, a background process acting as an SLP server, provides the functionality of the Directory Agent and Service Agent for SLP. Use SLP to locate the area mobility manager controller.
 - **Static Configuration** — You must provide the IP address of the mobility manager manually. Defining a static configuration for a mobility manager IP address bypasses SLP discovery.
- 7 In the **Mobility Manager Address** box, type the IP address for the designated mobility manager. The **Backup Manager Address** box displays the IP address of the backup controller.
- 8 Click **Save**.

For information about viewing mobility manager displays, see [Viewing Mobility Reports](#) on page 650.

15 Working with Third-party APs

Defining Authentication by Captive Portal for the Third-party AP WLAN Service
Defining the Third-party APs List
Defining Policy Rules for the Third-party APs

Defining Authentication by Captive Portal for the Third-party AP WLAN Service

802.1x Authentication is not supported directly by the wireless controller. However, this type of authentication can be supported by the actual third-party AP. All other options for authentication are supported at the controller.

- 1 On the **WLAN configuration** window for the third-party *WLAN (Wireless Local Area Network)* Service, click the **Auth & Acct** tab.
- 2 In the **Authentication Mode** drop-down list, click **Internal** or **External**, and then click **Configure**.
- 3 Define the Captive Portal configuration as described in [Configuring Captive Portal for Internal or External Authentication](#) on page 349.

Defining the Third-party APs List

- 1 In the **WLAN Services** panel, select the third-party *WLAN* Service.
- 2 In the **IP Address** field, type the IP address of a third-party AP.
- 3 In the **Wired MAC Address** field, type the MAC address of the AP.
- 4 Click **Add** to add the AP to the list.
- 5 Repeat for all third-party APs to be assigned to this WLAN Service.

Defining Policy Rules for the Third-party APs

- 1 Because the third-party APs are mapped to a physical topology, you must define the Exception filters on the physical topology, using the **Exception Filters** tab. For more information, see [Exception Filtering](#) on page 278.
- 2 Define policy rules that allow access to other services and protocols on the network such as HTTP, FTP, and *SNMP (Simple Network Management Protocol)*.
- 3 On the **Multicast Filters** tab, select **Enable Multicast Support** and configure the multicast groups whose traffic is allowed to be forwarded to and from the VNS using this topology. For more information, see [Multicast Filtering](#) on page 281.

In addition, modify the following functions on the third-party AP:

- Disable the AP's *DHCP (Dynamic Host Configuration Protocol)* server, so that the IP address assignment for any wireless device on the AP is from the DHCP server at the controller with VNS information.
- Disable the third-party AP's layer-3 IP routing capability and set the access point to work as a layer-2 bridge.

The following are the differences between third-party APs and APs on the Extreme Networks ExtremeWireless system:

- A third-party AP exchanges data with the controller's data port using standard IP over Ethernet protocol. The third-party access points do not support the tunnelling protocol for encapsulation.
- For third-party APs, the VNS is mapped to the physical data port and this is the default gateway for mobile units supported by the third-party access points.
- A controller cannot directly control or manage the configuration of a third-party access point.
- Third-party APs are required to broadcast an SSID unique to their segment. This SSID cannot be used by any other VNS.
- Roaming from third-party APs to wireless APs and vice versa is not supported.

16 Working with ExtremeWireless Radar

Radar Overview
Radar Components
Radar License Requirements
Enabling the Analysis Engine
Radar Scan Profiles
AirDefense Profile
Viewing Existing Radar Profiles
Adding a New Radar Profile
Configuring an In-Service Scan Profile
Configuring a Guardian Scan Profile
Assigning an AP to a Profile
Viewing the List of Assigned APs
Maintaining the Radar List of APs
Working with Radar Reports

Radar Overview

Radar is a set of advanced, intelligent features for managing the wireless environment. Radar includes advanced features for:

- Device location tracking
- Wireless-Intrusion-Detection and Wireless-Intrusion-Prevention (WIDS-WIPS)
- Advanced load balancing capability

Radar provides a basic solution for discovering unauthorized devices within the wireless coverage area. Radar performs basic RF network analysis to identify unmanaged APs and personal ad-hoc networks. The Radar feature set includes: intrusion detection, prevention and interference detection.

All APs can provide WIDS and traffic forwarding functionality, simultaneously and, if configured to do so, will apply countermeasures to detected wireless intrusions.

All APs (except 3705) can be placed in Guardian mode. In this mode, the AP dedicates both radios for intrusion detection and prevention functions. Guardians are capable of detecting and mitigating attacks on wireless channels that are not being used for traffic forwarding by the authorized network.

When controllers are configured in an availability pair, the Radar feature operates in High Availability mode, allowing Radar to retain its configuration, historical, and runtime data in the case of an availability pair controller failure. In High Availability mode, the configuration and runtime on both controllers is synchronized.

Radar Components

Figure 173 illustrates the major components of Radar.

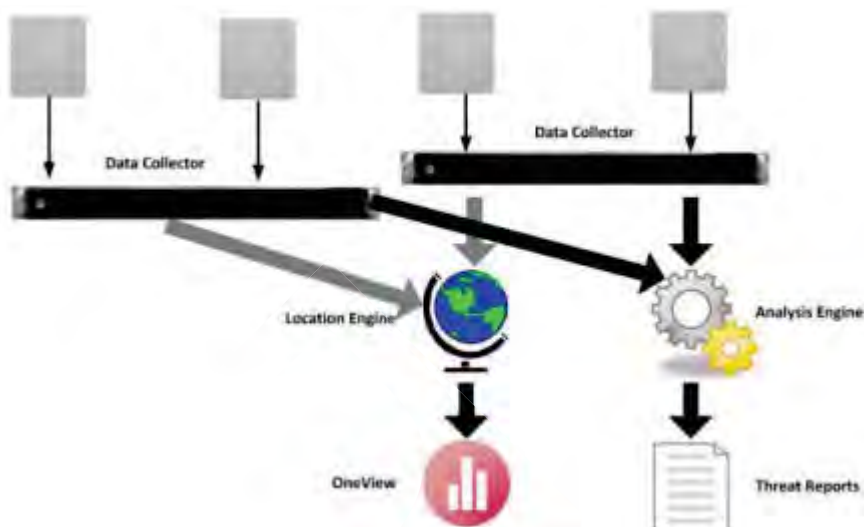


Figure 173: Radar System Components

Analysis Engine Overview

Radar requires that one controller host the Analysis Engine, and a data collector application, is installed on each controller. The data collector receives and manages the RF scan messages sent by each AP. The data collector forwards to the Analysis Engine lists of all connected wireless APs, third-party APs and RF scan information collected from participating APs.

The Analysis Engine processes the scan data from the data collectors through algorithms that make decisions about whether any of the detected APs or clients are threats or are running in an unsecure environment (for example, in ad-hoc mode).

APs must be part of a Radar scan profile to participate in WIDS-WIPS activity. A scan profile is a collection of WIDS-WIPS configuration options that can be assigned to appropriate APs. The actual configuration options depend on whether the profile is an In-Service or Guardian scan profile.

The Analysis Engine relies on a database of connected devices on the Extreme Networks ExtremeWireless system. The database is basically a compiled list of all APs and clients connected to the controller. The Analysis Engine compares the data from the data collector with the database of known devices. For more information on enabling the Analysis Engine, see [Enabling the Analysis Engine](#) on page 565.

Radar Functionality on the Controller

The Analysis Engine can run on a standalone controller or on a High Availability pair. The controller's Analysis Engine works only with local data collectors and with data collectors of the controller's availability partner.

Radar Functionality on the Wireless AP

An AP can be assigned to only one scan profile and only needs to be added to a profile if it is to be used for scanning.

APs run a radio frequency (RF) scanning task.

The APs scan for threats and perform countermeasures while simultaneously providing full traffic forwarding services including the application of role.



Note

When you enable countermeasures, the countermeasures apply to threats on channels that receive forwarded traffic.

All APs, except 3705, support Guardian mode profile. In Guardian mode, the APs rapidly sweep across multiple channels. This allows for threat detection on channels that are being used by APs that are not authorized to provide service. However, the more channels the AP has to defend concurrently, the less thoroughly it can defend any one channel. The AP will only defend a channel if an actual threat is detected on that channel, and if the Analysis Engine on the controller is able to distribute responsibility for dealing with concurrent active threats among multiple APs.



Note

If an AP is part of a WDS/Mesh link, you cannot configure it to act as a Guardian AP or In Service profile AP in Radar.

Radar License Requirements

Radar functionality is controlled by capacity licenses installed on the controller and activated as an option key. For more information on the Option Key, see [Applying Product License Keys](#) on page 47. Any AP assigned to an In-Service scan profile counts as 1 against the licensed Radar capacity. The base capacity for all controllers is 2, and any capacity increment can be installed on any controller.

The radar capacity is twice the platform system AP limit for Cloud Provider and Subscription license types.

AP Limitations

The maximum number of APs that can be licensed for Radar is twice the platform limit for local APs. Once the maximum number of APs is reached, no new licenses can be installed.

Enabling the Analysis Engine

Before using WIPS (Wireless Intrusion Prevention System), you must enable and define the Analysis and Data Collector Engines.

If using In-Service scan profiles, only the controller itself and its availability pair report to the Analysis Engine. For more information, see [Configuring an In-Service Scan Profile](#) on page 574.

To enable the Analysis Engine:

- 1 From the top menu, click **WIPS**.
The **Configuration > Engine Settings** screen displays.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.

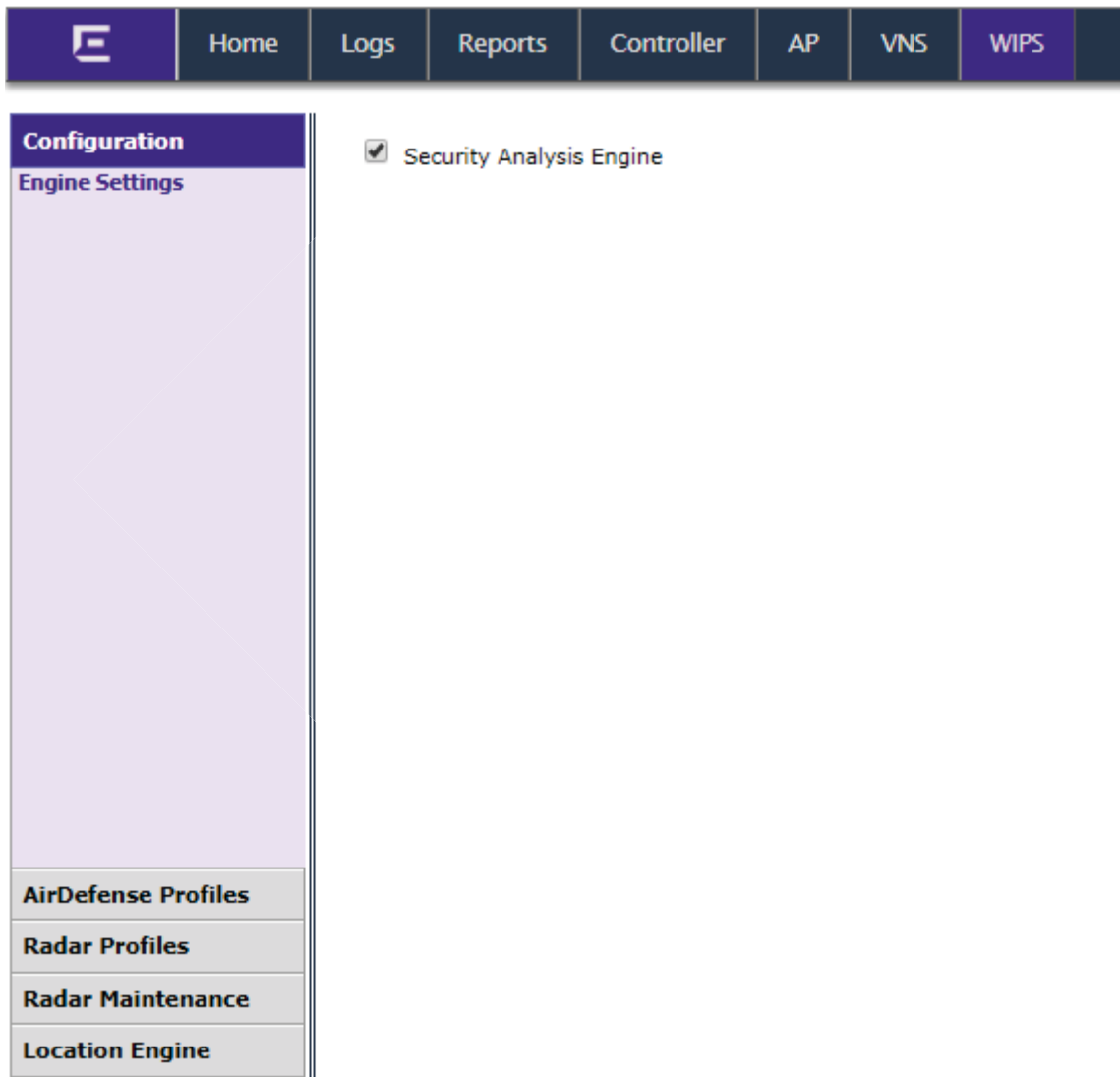


Figure 174: Radar Engine Settings

Radar Scan Profiles

Radar scan profiles provide the ability to organize scans for rogue activity based on a specific set of parameters such as radio assignments and desired channels. APs can be selected from a list of Assigned APs or a new AP can be added to the scan profile. An AP can only belong to one scan profile.

Radar provides In-Service and Guardian scan profiles.

- Any AP can use the In-Service scan profile.
- All APs, except 3705, can use the Guardian scan profile.

The AP39xx support the AirDefense profile. This profile integrates the AP39xx with the AirDefense Services Platform, offering an alternative to the Guardian Scan Profile.

Related Links

[Configuring an In-Service Scan Profile](#) on page 574

[Configuring a Guardian Scan Profile](#) on page 577

[Configuring an AirDefense Profile](#) on page 568

In-Service Scan Profiles

In-Service scan profiles work with any AP type and include the following:

- A set of countermeasure that lists possible prevention options to counter specific types of threats.
- Support for automatic blacklisting, which automatically removes network access from devices performing certain types of wireless attacks. The administrator can configure the length of time that a device remains on the blacklist.

Related Links

[In-Service Scan Profile Prevention Settings](#) on page 575

[Blacklisted Clients](#) on page 598

Guardian Scan Profiles

Guardian scan profiles work with all AP types (except AP3705) and include the following:

- An AP operating in Guardian mode does not bridge traffic and instead devotes all of the AP's resources to threat detection and countermeasures.
- An AP is added to a Guardian scan mode in its entirety. There is no option to dedicate one radio to scanning and the other to forwarding.
- An AP assigned to a Guardian scan profile stops providing any services (WLAN (Wireless Local Area Network) service, load groups, site) immediately.
- A list of all possible channels that the Guardian AP could scan. Each channel has a check box which when checked enables scanning by any AP in the group.
- A set of countermeasure that lists possible prevention options to counter specific types of threats. For more information, see [In-Service Scan Profile Prevention Settings](#) on page 575.
- Support for automatic blacklisting which allows the administrator to list which MAC addresses should be allowed or denied on the network. For more information, see [Blacklisted Clients](#) on page 598.
- Addresses added to the blacklist manually are there until they are manually removed. If blacklisting clients is enabled, you can set the maximum amount of time a device can be blacklisted.

Related Links

[AirDefense Profile](#) on page 567

AirDefense Profile

The AP integrates with the AirDefense Service Platform (ADSP), offering an additional profile option that allows the AP to function as an AirDefense sensor or to act as a sensor and retain the ability to

forward traffic. When the AP is configured with a AirDefense dedicated sensor profile, the functionality of the AP is controlled by the ADSP server. When the AP is configured as a AirDefense Radio Share profile, it continues to forward traffic while sending packets to an ADSP server.

In dedicated sensor mode, the AP operates independently from the controller while the controller continues to see the AP and display the AP Role as a dedicated AirDefense sensor. In its role as a dedicated sensor, the AP does not report statistics to the controller. However, the WASSP-tunnel is maintained to allow future reconfiguration.

In the Radio Share mode, both radios on the AP operate as both a sensor and a traffic forwarder. The controller configuration indicates whether the radios gather all packet traffic or packet traffic for only APs registered with ADSP. With Radio Share, you also have the option to scan neighboring channels in addition to the operating channel.

AP39xx supports AirDefense profiles.

Related Links

[Configuring an AirDefense Profile](#) on page 568

Configuring an AirDefense Profile

Configure an AirDefense profile that allows the AP to function as an AirDefense dedicated sensor or as a Radio Share profile.

- 1 From the top menu, click **WIPS**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 Select **AirDefense Profiles**.
- 4 From the **AirDefense Profiles** screen, click **New**.
- 5 Select the Profile type. Valid values are:

Dedicated	The radio is a dedicated ADSP sensor, controlled by the ADSP server.
Radio Share	The radios are both ADSP sensors and they forward traffic to the controller.

The screenshot shows the 'AirDefense Profile' configuration page. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', and 'WIPS'. The left sidebar has 'Configuration' and 'AirDefense Profiles' (selected), with 'Radar Profiles', 'Radar Maintenance', and 'Location Engine' below. The main content area is titled 'AirDefense Profile:' and contains a 'Configuration' tab. Under the 'Core' section, there is a 'Name' field with the value 'New_Profile'. Below this is the 'AirDefense Servers' section, which includes three input fields for 'Address 1:', 'Address 2:', and 'Address 3:'.

Configuration

Core

Name:

AirDefense Servers:

Address 1:

Address 2:

Address 3:

Figure 175: AirDefense Profile Dedicated Configuration

AirDefense Profile:

Configuration		Assigned APs
Core		
Name:	<input type="text"/>	
AirDefense Servers:	<div> Address 1: <input type="text"/> Address 2: <input type="text"/> Address 3: <input type="text"/> </div>	
Radio Share Configuration:	<div> <input type="checkbox"/> Off Channel Scanning RadioMode Off ▼ </div>	

Figure 176: AirDefense Profile Radio Share Configuration

- 6 On the **Configuration** tab configure the following parameters:

Table 107: AirDefense Profile Configuration Settings

Field	Description
Name	Scan profile name
AirDefense Servers	The IP address of the AirDefense servers. Provide the FQDN or IPv4 string, maximum 255 characters.
Radio Share	

Table 107: AirDefense Profile Configuration Settings (continued)

Field	Description
Off Channel Scanning	<p>Enable Off Channel Scanning. Allow the radio to perform periodic scanning on neighboring channels in addition to the operating channel.</p> <p>Note: Providing service on the operating channel has priority over scanning neighboring channels.</p>
Radio Mode	<p>Radio mode for packet transfer. Valid values are:</p> <ul style="list-style-type: none"> • Off. When the radio mode is set to Off, the Radio Share capability is disabled, regardless of the selected Profile type. • Inline. AP reports to the ADSP server only its own traffic and multicast / broadcast traffic such as beacons and probe requests. Inline mode has minimal impact on AP performance, because the AP reports to the ADSP server only traffic that it processes. • Promiscuous. AP receives all packets seen on its operating channel and forwards them to the ADSP server. Promiscuous mode loads the AP resources, because the AP processes traffic intended for all neighboring APs. In high-density, wireless deployments, use dedicated sensors instead of Radio Share in Promiscuous mode. <p>Note: Set AP to Promiscuous mode when AP is required to perform Termination.</p>

Related Links

[AirDefense Profile](#) on page 567

[Configuring an In-Service Scan Profile](#) on page 574

[Configuring a Guardian Scan Profile](#) on page 577

Viewing Existing Radar Profiles

- 1 From the top menu, click **WIPS**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 In the left pane, click **Radar Profiles**.

The **Radar Profiles** screen displays.

Logs Reports Controller AP VNS **WIPS**

Radar Profiles

	Name	Profile	Security Scan	Interference Scan	Status
<input type="checkbox"/>	V2110_InService	In-Service	✓	✓	Enabled

New Delete Selected

Figure 177: In-Service Profiles

Table 108: Scan Profiles - Fields and Buttons





Field/Button	Description
Name	The name of the scan profile.
Profile	In-Service or Guardian.
Security Scan	<p>Indicates whether the profile enables security scanning on APs assigned to the profile.</p> <div>  </div> <p>Indicates that the scan profile enables security scanning.</p> <div>  </div> <p>Indicates that the scan profile does not enable security scanning.</p>

Table 108: Scan Profiles - Fields and Buttons (continued)

Field/Button	Description
Interference Scan	<p>Interference classification compares patterns in RF interference to known interference patterns to help identify the source of the interference.</p> <p></p> <p>Indicates that the interference scan classification is enabled on specific APs assigned to the profile.</p> <p></p> <p>Indicates that the interference scan classification is not enabled on specific APs assigned to the profile.</p>
Status	<p>Enabled: Indicates that the scan profile is enabled (for example, whether the APs assigned to the profile are scanning in accordance with the profile). Scan profiles are Enabled if either security scanning or interference scanning is enabled.</p> <p>Disabled: Indicates that the scan profile is disabled. A disabled profile means the profile is defined but any APs assigned to the profile are not performing scans.</p>
New	Click to create a new scan profile (see Adding a New Radar Profile on page 573).
Delete Selected	Click to delete the selected scan profile.

Adding a New Radar Profile

- 1 From the top menu, click **WIPS**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 Select **Radar Profiles**.
- 4 From the **Radar Profiles** screen, click **New**.

- 5 In the **Add Radar Profile** dialog, select the profile type:
- Guardian
 - In-Service

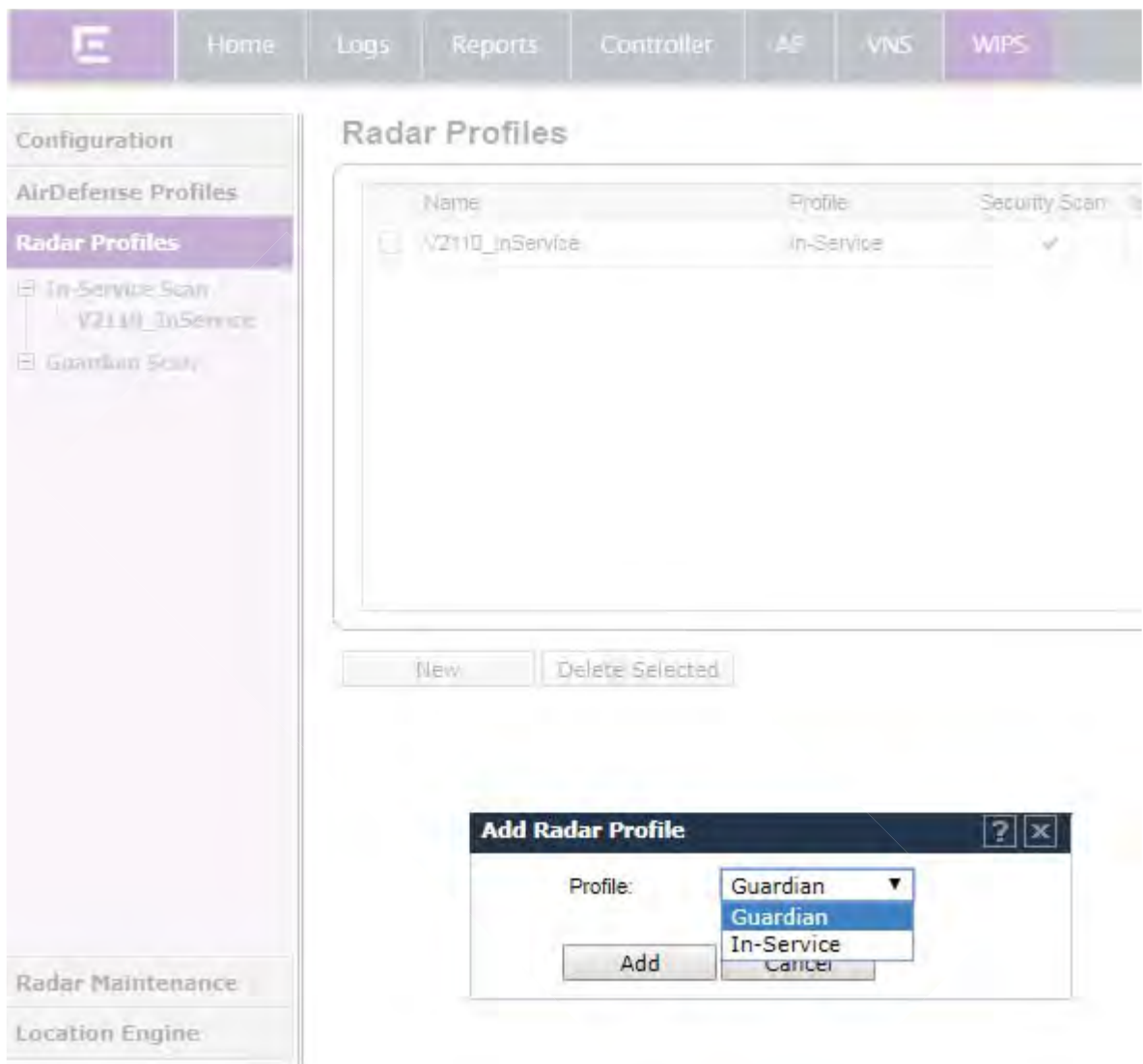


Figure 178: Add Radar Profile

For information about configuring the profile:

- [Configuring an AirDefense Profile](#) on page 568
- [Configuring a Guardian Scan Profile](#) on page 577.
- [Configuring an In-Service Scan Profile](#) on page 574.

Configuring an In-Service Scan Profile

Configure the following for an In-Service scan profile:

- Detection Settings
- Prevention Settings

- List of Assigned APs

Related Links

[Assigning an AP to a Profile](#) on page 581

[Viewing the List of Assigned APs](#) on page 581

In-Service Scan Profile Detection Settings



Note

Once an In-Service scan profile is created, the **Detection** tab appears.

Select the **Detection** tab.

Scan Profile: inservice

Detection	Prevention	Assigned APs
<p>Core</p> <p>Name: <input type="text" value="inservice"/></p> <p><input checked="" type="checkbox"/> Scan for security threats</p> <p><input checked="" type="checkbox"/> Rogue AP detection Listener port: <input type="text" value="348"/> (1-32768)</p> <p><input checked="" type="checkbox"/> Classify sources of interference</p>		

Figure 179: Detection Settings

From the Core pane, type a unique name for the scan profile and configure the following detection options:

- Scan for security threats. For more information, see [Security Threats](#) on page 594.
- Rogue AP detection. Select this option to detect rogue APs serving open SSIDs (for example an AP attached to an Ethernet wall jack and the AP is running an open SSID). If a rogue AP is detected, countermeasures can be optionally applied to prevent any station from using this rogue AP.
- Listener port: Enter the UDP port for rogue AP detection.
- Classify sources of interference. Interference classification compares patterns in RF interference to known interference patterns to help identify the source of the interference. All APs based on the AP371x, AP38xx, and AP39xx architecture are capable of performing interference classification.
- Click **Save**.

In-Service Scan Profile Prevention Settings

Radar provides multiple countermeasures which can be enabled in an In-Service scan profile. The level of prevention for the profile is dependent on the countermeasures selected. For more information on the Radar threat categories for which countermeasures can be applied, see [Radar Scan Profiles](#) on page 566.

When Radar WIDS-WIPS is enabled, all detected threats are reported when they start and when they stop. The reports are available in the controller's event logs and can be streamed off the controller using [SNMP \(Simple Network Management Protocol\)](#) and syslog. These event reports are always generated regardless of which other countermeasures are enabled. For more information on these reports, see [Working with Radar Reports](#) on page 593.

Related Links

[Selecting Countermeasures](#) on page 576

Selecting Countermeasures

Countermeasures mitigate the impact of a security threat:

- Sending standard 802.11 deauthentication frames to prevent stations from associating to threat devices.
- Rate limiting flooded frames. This can prevent floods from propagating through the AP to the wired network.
- Blacklisting attacking devices to prevent them from gaining access to the network.

Countermeasures are enabled on a per-scan-profile basis. Some scan profiles can have countermeasures enabled while others cannot.

To select a specific countermeasure:

- 1 From the top menu, click **WIPS**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 In the left pane, click **Radar Profiles**.
- 4 Select an In-Service scan profile and click the **Prevention** tab.

Scan Profile: inservice

Detection	Prevention	Assigned APs
<p>Countermeasures</p> <ul style="list-style-type: none"> <input type="checkbox"/> Prevent authorized stations from roaming to external honeypot APs <input type="checkbox"/> Prevent authorized stations from roaming to friendly APs <input type="checkbox"/> Prevent any station from using an internal honeypot AP <input type="checkbox"/> Prevent any station from using a rogue AP <input type="checkbox"/> Prevent any station from using a spoofed AP <input type="checkbox"/> Drop frames in a controlled fashion during a flood attack <input type="checkbox"/> Prevent any station from using an ad hoc mode device <input type="checkbox"/> Remove network access from clients originating DoS and password-cracking attacks Remove network access from violating clients for <input type="text" value="900"/> seconds 		

Figure 180: Prevention Settings

Table 109: Prevention Tab - Fields and Buttons

Field/Button	Description
Countermeasures	
Prevent authorized stations from roaming to external honeypot APs	An external honeypot is an AP that is attempting to make itself a man-in-the-middle by advertising a popular SSID, such as an SSID advertised by a coffee shop or an airport
Prevent authorized stations from roaming to friendly APs	Friendly APs are APs that are not part of the authorized wireless network, but they operate in the vicinity of the authorized wireless network.
Prevent any station from using an internal honeypot AP	An internal honeypot is an AP that is attempting to make itself a man-in-the-middle by advertising an SSID belonging to the authorized network.
Prevent any station from using a rogue AP	A rogue AP is an unauthorized AP connected to the authorized wired network.
Prevent any station from using a spoofed AP	A spoofed AP is an AP that is not part of the authorized network is advertising a BSSID (MAC address) that belongs to an authorized AP on the authorized network.
Drop frames in a controlled fashion during a flood attack	Prevents some types of Denial of Service (DoS) attack from affecting the authorized network instead of just the target AP. For example, rate limiting the flooded frames.
Prevent any station from using an ad hoc mode device	Deauthentication messages are used to prevent devices from using an ad hoc mode device.
Remove network access from clients originating DoS and password-cracking attacks	Prevents propagation of the DoS attack from the AP to the authorized network. Many types of DoS attack involve deluging an AP with a large volume of messages of one or two specific types. When this option is enabled, the AP will apply rate limits to the specific type of frame that is being deluged. The selected clients for this countermeasure are denied access to the network for the amount of time that is specified in "Remove network access from violating clients for a period of time."
Remove network access from violating clients for a period of time	Enter a numeric value in seconds.
New	Click to create a new scan profile. For more information, see Adding a New Radar Profile on page 573.
Delete	Click to delete the selected scan profile.
Save	Click to save changes.

Configuring a Guardian Scan Profile

Configure the following for a Guardian scan profile:

- Detection Settings
- Prevention Settings
- List of Assigned APs

Related Links

Guardian Scan Profile Detection Settings on page 578
 Guardian Scan Profile Prevention Settings on page 579
 Selecting Countermeasures on page 579
 Assigning an AP to a Profile on page 581
 Viewing the List of Assigned APs on page 581

Guardian Scan Profile Detection Settings



Note

Once a new Guardian Scan Profile is created, the Detection tab appears.

Scan Profile: Guardian-1

Detection | Prevention | Assigned APs

Core

Name:

☒ Scan for security threats

☒ Rogue AP detection Listener port: (1-32768)

☒ Classify sources of interference

Channels to Monitor

2.4 GHz | 5 GHz

<input checked="" type="checkbox"/> 1: 2412 MHz	<input checked="" type="checkbox"/> 2: 2417 MHz	<input checked="" type="checkbox"/> 3: 2422 MHz	<input checked="" type="checkbox"/> 4: 2427 MHz
<input checked="" type="checkbox"/> 5: 2432 MHz	<input checked="" type="checkbox"/> 6: 2437 MHz	<input checked="" type="checkbox"/> 7: 2442 MHz	<input checked="" type="checkbox"/> 8: 2447 MHz
<input checked="" type="checkbox"/> 9: 2452 MHz	<input checked="" type="checkbox"/> 10: 2457 MHz	<input checked="" type="checkbox"/> 11: 2462 MHz	<input checked="" type="checkbox"/> 12: 2467 MHz
<input checked="" type="checkbox"/> 13: 2472 MHz	<input checked="" type="checkbox"/> 14: 2484 MHz		

Figure 181: Detection Settings

- 1 In the **Name** box, type a unique name for this scan profile.

Select from the following detection options:

- Scan for security threats. For more information, see [Security Threats](#) on page 594.
- Classify sources of interference. Interference classification compares patterns in RF interference to known interference patterns to help identify the source of the interference. All APs based on the AP371x, AP38xx, and AP39xx architecture are capable of performing interference classification.

- 2 Under Channels to Monitor:

- Click the **2.4 GHz** tab and select channels to be monitored within this band for the scan profile.

- Click the **5 GHz** tab and select channels to be monitored within this band for the scan profile.

Guardian Scan Profile Prevention Settings

Radar provides multiple countermeasures which can be enabled in a Guardian scan profile. The level of prevention for the profile is dependent on the countermeasures selected. For more information on the Radar threat categories for which countermeasures can be applied, see [Radar Scan Profiles](#) on page 566.

When Radar WIDS-WIPS is enabled, all detected threats are reported when they start and when they stop. The reports are available in the controller's event logs and can be streamed off the controller using [SNMP](#) and syslog. These event reports are always generated regardless of which other countermeasures are enabled. For more information on these reports, see [Working with Radar Reports](#) on page 593.

Selecting Countermeasures

Countermeasures mitigate the impact of a security threat. Three main countermeasures are used by the Guardian APs:

- Sending standard 802.11 deauthentication frames to prevent stations from associating to threat devices.
- Rate limiting flooded frames. This can prevent floods from propagating through the AP to the wired network.
- Blacklisting attacking devices to prevent them from gaining access to the wireless network.

To select a specific countermeasure:

Countermeasures are enabled on a per-scan-profile basis. Some scan profiles can have countermeasures enabled while others cannot.

- 1 From the top menu, click **WIPS**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 In the left pane, click **Radar Profiles**.

- 4 Select a Guardian scan profile and click the **Prevention** tab.

Scan Profile:

Detection	Prevention	Assigned APs
<p>Countermeasures</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Prevent authorized stations from roaming to external honeypot APs <input checked="" type="checkbox"/> Prevent authorized stations from roaming to friendly APs <input checked="" type="checkbox"/> Prevent any station from using an internal honeypot AP <input checked="" type="checkbox"/> Prevent any station from using a rogue AP <input checked="" type="checkbox"/> Prevent any station from using a spoofed AP <input checked="" type="checkbox"/> Drop frames in a controlled fashion during a flood attack <input checked="" type="checkbox"/> Prevent any station from using an ad hoc mode device <input checked="" type="checkbox"/> Remove network access from clients originating DoS and password-cracking attacks <p>Remove network access from violating clients for <input type="text" value="900"/> seconds</p>		
<p>Defense Options</p> <p>Maximum number of channels per radio to defend concurrently</p> <p><input type="range" value="1"/> 1 2 3 4</p>		

Figure 182: Prevention Settings

- 5 Select desired prevention method.
- 6 Select number of channels per radio to defend concurrently. Number of defended channels can be between 1 and 4.

Table 110: Prevention Tab - Fields and Buttons

Field/Button	Description
Countermeasures	
Prevent authorized stations from roaming to external honeypot APs	An external honeypot is an AP that is attempting to make itself a man-in-the-middle by advertising a popular SSID, such as an SSID advertised by a coffee shop or an airport
Prevent authorized stations from roaming to friendly APs	Friendly APs are APs that are not part of the authorized wireless network, but they operate in the vicinity of the authorized wireless network.
Prevent any station from using an internal honeypot AP	An internal honeypot is an AP that is attempting to make itself a man-in-the-middle by advertising an SSID belonging to the authorized wireless network.
Prevent any station from using a rogue AP	A rogue AP is an unauthorized AP connected to the authorized wired or wireless network.
Prevent any station from using a spoofed AP	A spoofed AP is an AP that is not part of the authorized network is advertising a BSSID (MAC address) that belongs to an authorized AP on the authorized network.

Table 110: Prevention Tab - Fields and Buttons (continued)

Field/Button	Description
Drop frames in a controlled fashion during a flood attack	Prevents some types of Denial of Service (DoS) attack from affecting the authorized network instead of just the target AP. For example, rate limiting the flooded frames.
Prevent any station from using an ad hoc mode device	Deauthentication messages are used to prevent devices from using an ad hoc mode device.
Remove network access from clients originating DoS and password-cracking attacks	Prevents propagation of the DoS attack from the AP to the authorized network. Many types of DoS attack involve deluging an AP with a large volume of messages of one or two specific types. When this option is enabled, the AP will apply rate limits to the specific type of frame that is being deluged. The selected clients for this countermeasure are denied access to the network for the amount of time that is specified in "Remove network access from violating clients for a period of time."
Remove network access from violating clients for a period of time	Enter a numeric value in seconds.
Defense Options	
Maximum number of channels per radio to defend concurrently	Click the slider to select the number of channels desired.
New	Click to create a new Guardian scan profile. For more information, click Adding a New Radar Profile on page 573.
Delete	Click to delete the selected Guardian scan profile.
Save	Click to save changes.

Assigning an AP to a Profile

To assign an AP to a scan profile:

- 1 From the top menu, click **WIPS**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 In the left pane, click **Radar Profiles** or **AirDefense Profiles**.
- 4 Select a profile, and click the **Assigned APs** tab.
- 5 Select an AP from the list of Assigned APs and click **Save**.

Related Links

[Viewing the List of Assigned APs](#) on page 581

Viewing the List of Assigned APs

The list of Assigned APs is a list of all APs reported by the data collectors. Assigned APs automatically appear once a profile is created. To view the list of APs assigned to a profile, click the **Assigned APs** tab.

Table 111: Assigned APs Tab - Fields and Buttons

Field/Button	Description
Wireless APs	Identifies the wireless APs assigned to the profile. May include the AP name or serial number.
Controller (Radar Profiles)	Identifies the controller associated with the wireless AP. An IP address indicates a remote data collector. Local Controller indicates a controller local to the AP. Applies to Radar Profiles only.
Assignment (Guardian AP)	Indicates if the Guardian AP is assigned to a Site, Load Group, or WLAN Service.
Search	To search for a profile in the list, enter the full name of a scan profile and press Enter.
Select All	Select all APs in the list.
Deselect All	Clear the selection of all APs in the list.
Save	Click to save changes.

The list of Assigned APs are APs that are available to any profile. However, an AP can only be assigned to one profile.

Related Links

[Assigning an AP to a Profile](#) on page 581

[Configuring an AirDefense Profile](#) on page 568

[Configuring an In-Service Scan Profile](#) on page 574

[Configuring a Guardian Scan Profile](#) on page 577

Maintaining the Radar List of APs

Wireless Intrusion Prevention System (WIPS) provides a list of APs organized in categories based on the scan results of the Analysis Engine. WIPS will try to assign each discovered AP to one of these categories. If it can't find a specific category for the AP, it will assign it to the Uncategorized APs category. Uncategorized APs require manual classification. To get the best protection from WIPS, classify uncategorized APs as soon as possible.

You can manually assign APs from one category to another using WIPS. For more information, see [Reclassifying APs](#) on page 592.

AP Categories

APs belong to one of the following categories when they are added to the Analysis Engine database:

- **Scanning APs** - This is the subset of authorized APs configured to provide WIDS-WIPS services.
- **Friendly APs** - These are APs that are not part of the authorized network, but they operate in the vicinity of the authorized network. Friendly APs are operated by a neighboring enterprise for their own use. Authorized APs can prevent authorized devices from using friendly APs.
- **Uncategorized APs** - APs discovered by scanning APs and which do not fall into any other category. Uncategorized APs require manual classification. To get the best protection from WIPS, classify uncategorized APs as soon as possible.

- **Authorized APs** - APs that can be used by devices authorized to use the network. APs can be added to the list automatically (for example, if the APs are active on the current host or the host's availability partner) or manually.
- **Prohibited APs** - These are APs that have been manually added to the Radar database so that the Radar WIDS-WIPS system will detect them and, if so configured, protect against them. An example of manually prohibited APs might be APs that were stolen from the authorized network and now could be used to generate a security breach.

Viewing the List of Scanning APs

- 1 From the top menu, click **WIPS**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 In the left pane, click **Radar Maintenance**.

The **Scanning APs** screen displays.

Scanning APs (16)				
Wireless Controllers		Wireless APs		
	Name	Serial	Profile Name	Licensed
Local Controller	12B2694430000000	12B2694430000000	inservice »	✓
	12B2694680000000	12B2694680000000	inservice »	✓
	3705-1234	12341753905A0000	inservice »	✓
	3715i-mm1344	13440720085E0000	inservice »	✓
	3801i-145045	1450451708410000	inservice »	✓
	3935-ext-1549Y	1549Y-1191100000	inservice »	✓
	3935-IPv6	1544Y-1001800000	inservice »	✓
	AP-3710-1313	1313275359510000	inservice »	✓
	C51-3801i-2345	23456789eAP3801e	inservice »	✓
	C51-3825ext-1344	1344000A01410000	inservice »	✓
	C51-3825i-1404	1404014208410000	inservice »	✓
	C51-3865e-1416	0000141600060802	inservice »	✓
	C51-AP3916ic1652D	1652D10000240000	inservice »	✓
	C51-AP3917-1737Y	1737Y-1000400000	inservice »	✓
	C51-AP3965-1602Y	1602Y-1211600000	inservice »	✓
	C5110-3825i-1404	1404013908410000	inservice »	✓

» In-service Scan Profile Guardian Scan Profile

Figure 183: Scanning APs

Table 112: Scanning APs - Fields and Buttons

Field/Button	Description
Wireless Controllers	Displays the name of wireless controllers reporting to the Analysis Engine on this host. Can be the IP address of another controller or "Local Controller" which represents the controller hosting this instance of the Analysis Engine.
Wireless APs	Name - Name of the Access Point
	Serial - Serial number of the Access Point
	Profile Name - Describes the scan profile. The shield icon indicates a Guardian scan profile.
	Licensed - A check mark indicates that the AP is licensed.

Viewing the List of Friendly APs

The Friendly APs page allows you to manage the list of APs that are considered to be operating in the vicinity legitimately but to which authorized devices should not roam. A Friendly AP has to be added manually to the list, or manually reclassify an Uncategorized AP as Friendly.

To view a list of Friendly APs:

- 1 From the top menu, click **WIPS**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.

- 3 In the left pane, click **Radar Maintenance > Friendly APs**

Friendly APs (1)

	MAC Address	SSID	Description	Manufacturer
<input type="checkbox"/>	00:1D:D7:59:4A:AA	Test-1	Friendly AP	Algoith

Categorize Selected APs as

Table 113: Friendly APs Screen - Fields and Buttons

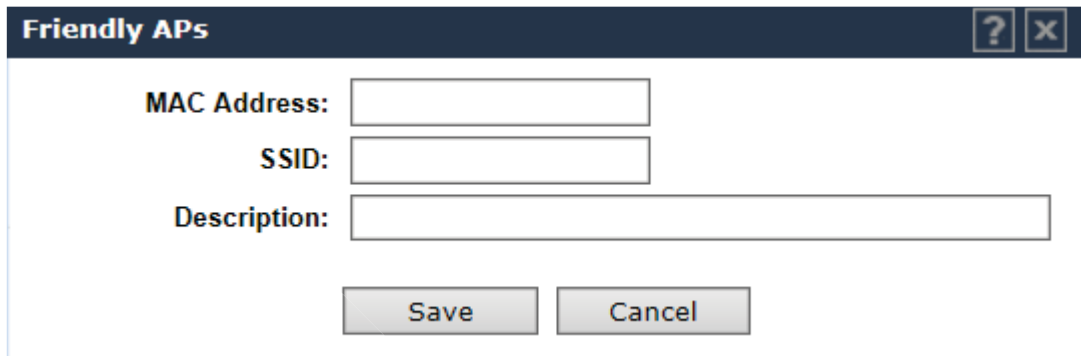
Field/Button	Description
MAC Address	Specifies the MAC address for the Friendly AP
SSID	Unique identifier attached to the header of packets sent over a wireless local-area network (<i>WLAN</i>) from the Friendly AP
Description	Specifies a brief description for the Friendly AP
Manufacturer	Lists the AP manufacturer
Categorize Selected APs as	APs categorized as Friendly APs can be reclassified as authorized or threats. For more information, see Reclassifying APs on page 592.
New	Click to create a new Friendly AP. For more information, see Adding Friendly APs on page 585.
Delete Selected	Select an AP from the list of Friendly APs, and click to delete them from the list.

Adding Friendly APs

To add a Friendly AP:

- 1 From the top menu, click **WIPS**.

- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 Click **Maintenance > Friendly APs**.
- 4 Click **New**.



Friendly APs [?] [X]

MAC Address:

SSID:

Description:

Save **Cancel**

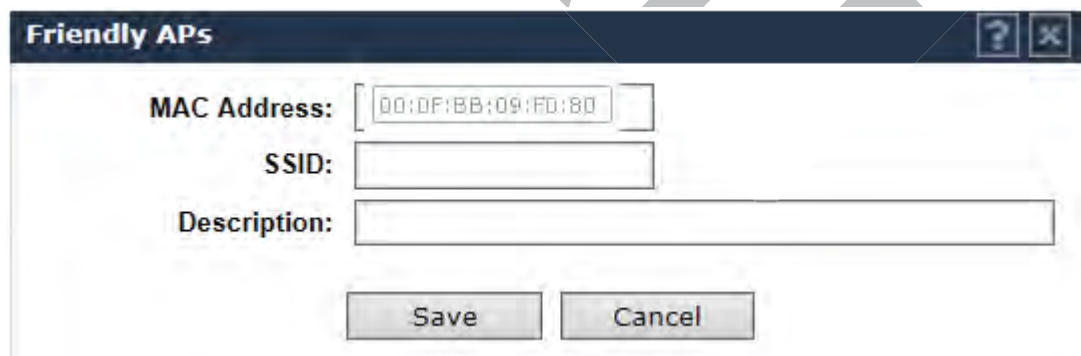
Figure 184: New Friendly AP

- 5 Configure the following parameters:
 - **MAC Address** — Specifies the MAC address of the Friendly AP
 - **SSID** — Specifies the SSID of the Friendly AP
 - **Description** — Specifies a brief description of the Friendly AP
- 6 Click **Save**. The new access point is displayed in the Friendly APs list.

Modifying Friendly APs

To modify a Friendly AP:

- 1 From the top menu, click **WIPS**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 Click **Maintenance > Friendly APs**.
- 4 In the **Friendly APs** list, double-click the access point you want to modify.
- 5 Modify the access point fields as required and click **Save**.



Friendly APs [?] [X]

MAC Address:

SSID:

Description:

Save **Cancel**



Note

The MAC Address field cannot be modified

Figure 185: Modify Friendly AP

Viewing the List of Uncategorized APs

Uncategorized APs are discovered but do not fall into any other category.

To view a list of Uncategorized APs:

- 1 From the top menu, click **WIPS**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 In the left pane, click **Radar Maintenance > Uncategorized APs**.

Uncategorized APs (352)

	MAC Address	SSID	Manufacturer
<input type="checkbox"/>	20:B3:99:43:C1:58	cnl106C5110bap	Enterasys
<input type="checkbox"/>	D8:84:66:94:C4:F0	nslab	Extreme Networks
<input type="checkbox"/>	D8:84:66:C2:14:60	H_6	Extreme Networks
<input type="checkbox"/>	D8:84:66:C2:1C:20	SG01	Extreme Networks
<input type="checkbox"/>	D8:84:66:81:EA:78	L103-C5210-CPn	Extreme Networks
<input type="checkbox"/>	D8:84:66:C2:15:D0	Test_Wlan_AAA	Extreme Networks
<input type="checkbox"/>	D8:84:66:71:63:BA	nslabAaa	Extreme Networks
<input type="checkbox"/>	20:B3:99:AE:C7:78	WLAN-CNL-V2110-1	Enterasys
<input type="checkbox"/>	20:B3:99:9C:DB:C3	L103-V2110-bac-ECP	Enterasys
<input type="checkbox"/>	D8:84:66:94:C7:A0	testRBR	Extreme Networks
<input type="checkbox"/>	D8:84:66:81:EA:C9	IPv6P	Extreme Networks

Export

Categorize Selected APs as

Authorized

Friendly

Prohibited

Figure 186: Uncategorized APs

Table 114: Uncategorized APs Screen - Fields and Buttons

Field/Button	Description
MAC Address	Specifies the MAC address of the uncategorized AP
SSID	Unique identifier attached to the header of packets sent over a wireless local-area network (<i>WLAN</i>) from the uncategorized AP.

Table 114: Uncategorized APs Screen - Fields and Buttons (continued)

Field/Button	Description
Manufacturer	Lists the AP manufacturer
Categorize Selected APs as	APs categorized as uncategorized APs can be reclassified as authorized, friendly, or prohibited. For more information, see Reclassifying APs on page 592.

- Click **Export** to download the list of Uncategorized APs in .xml format.

Viewing the List of Authorized APs

The list of Authorized APs includes the APs that an authorized device is permitted to associate with. APs can be added to the list automatically (for example if the AP is active on the current host or its availability partner) or manually.

Re-categorize an AP as Authorized, to protect it from an unwanted countermeasure when there is a non-authorized AP with a problematic SSID (an External Honeypot) in the vicinity of the authorized network and you want to exclude the AP from an undesired counter attack.

To view a list of Authorized APs:

- From the top menu, click **WIPS**.
- If not already selected, select **Security Analysis Engine** and click **Save**.

- 3 In the left pane, click **Radar Maintenance > Authorized APs**.

Authorized APs (2)

	MAC Address	Description	Manufacturer
<input type="checkbox"/>	11:22:11:22:11:22	Authorized	Unknown Manufacturer
<input type="checkbox"/>	22:22:22:33:33:33		Unknown Manufacturer

Categorize Selected APs as

Figure 187: Authorized APs

Table 115: Authorized APs Screen - Fields and Buttons

Field/Button	Description
MAC Address	Specifies the MAC address of the authorized AP
Description	Specifies a brief description of the authorized AP
Manufacturer	Lists the AP manufacturer
Categorize Selected APs as	APs categorized as authorized APs can be reclassified as friendly APs. For more information, see Reclassifying APs on page 592.
New	Click to create a new authorized AP. For more information, see Adding Authorized APs on page 589.
Delete Selected	Select an AP from the list of authorized APs, and click to delete them from the list.

Adding Authorized APs

You do not have to manually add APs to the authorized AP list. The controllers create the list automatically. However, sometimes you may need to do this manually:

- An AP of a controller that is not sending information to the Analysis Engine is included on the Scanning APs screen. Devices should be able to roam between that AP and the APs of the controllers managed by the Analysis Engine.
- When adding a foreign AP (External or Internal Honeypot, or Rogue AP) to the list of Authorized APs, accidental countermeasures applied to that AP can be prevented.
- You have a third-party AP that its authorized devices should be allowed to use even though the AP is not managed by a controller.

To add an Authorized AP

- 1 To add Friendly access points manually to the **Authorized APs** list, from the Authorized APs screen, click **New**. The **Authorized APs** dialog displays.

- 2 In the **Authorized APs** dialog, type the following:
 - **MAC Address** — Specifies the MAC address for the AP
 - **Description**— Specifies a brief description for the AP
- 3 Click **Save**. The new access point is displayed in the authorized APs list.

Viewing the List of Prohibited APs

The list of Prohibited APs are APs that you have manually added to the Radar database so that the Radar WIDS-WIPS system will detect them and, if so configured, protect against them.

Manually add an AP to the list of Prohibited APs, when a non-authorized AP is a threat, but it cannot be detected by existing threat criteria.

To view a list of Prohibited APs:

- 1 From the top menu, click **WIPS**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.

- 3 In the left pane, click **Radar Maintenance > Prohibited APs**.

Prohibited APs (1)

	MAC Address	Category	Description	Manufacturer
<input type="checkbox"/>	22:22:33:33:22:22	Report presence only	Prohibited	Unknown Manufacturer

Categorize Selected APs as Friendly
New
Delete Selected

Figure 188: Prohibited APs

Table 116: Prohibited APs Screen - Fields and Buttons

Field/Button	Description
MAC Address	Specifies the MAC address of the prohibited APs
Category	Threat category
Description	Specifies a brief description of the prohibited AP
Manufacturer	Lists the AP manufacturer
Categorize Selected APs as	APs categorized as prohibited APs can be reclassified as friendly APs. For more information, see Reclassifying APs on page 592.
New	Click to create a new prohibited AP. For more information, see Adding Prohibited APs on page 591.
Delete Selected	Select APs from the list of prohibited APs, and click to delete them from the list.

Adding Prohibited APs

To add a Prohibited AP:

- 1 To add access points manually to the **Prohibited APs** list, from the **Prohibited APs** screen, click **New**. The **Prohibited APs** dialog displays.

- 2 For **MAC Address**, specify the MAC address for the Prohibited AP.
- 3 For **Description**, enter a brief description of the AP.
- 4 For **Action**, select from the following options:
 - **Report presence only** - When the MAC address of the prohibited AP is detected by an authorized scanning AP, the prohibited AP's presence will be reported in an event message. This in turn will result in the presence of the MAC being included in the Radar threat reports. No countermeasures will be taken against the device with the MAC address by Radar.
 - **Treat like an internal honeypot AP** - The device with the MAC address is considered to be as harmful as an AP that is 'impersonating' one of the authorized APs. If countermeasures are enabled, no devices will be allowed to associate to this MAC address, including devices of other neighboring enterprises.
 - **Treat like an external honeypot** - The device with the entered MAC address is considered to be as harmful as an AP that is advertising a popular SSID. Authorized devices will be prohibited from roaming to the device with this MAC address. Unauthorized devices and unrecognized devices will be allowed to roam to the device with the MAC address.
- 5 Click **Save**. The new access point is displayed in the Prohibited APs list.
For information about reclassifying an existing AP to Prohibited, see .

Reclassifying APs

You can manually assign APs from one category to another depending on the APs current classification. Categorize selected APs directly from its current category list. For example, APs on the Friendly and Uncategorized lists can be reclassified as Authorized.

To reclassify an AP:

- 1 From the top menu, click **WIPS**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.

- 3 In the left pane, click **Radar Maintenance** and select one of the AP lists. An AP can be reclassified depending on its current classification. See [Table 117](#).

Table 117: AP Classifications

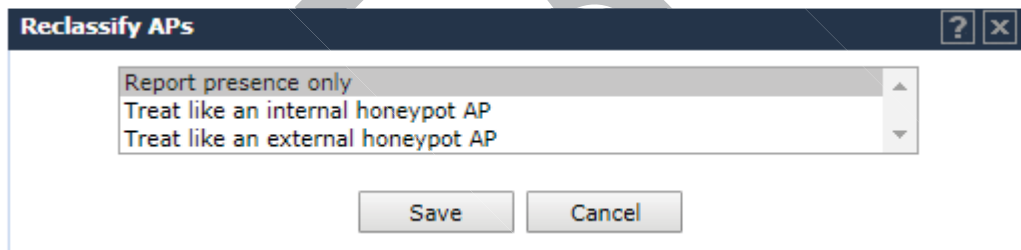
Current AP Category	Possible Reclassification
Friendly	<ul style="list-style-type: none"> • Authorized • Prohibited
Uncategorized	<ul style="list-style-type: none"> • Authorized • Friendly • Prohibited
Authorized	<ul style="list-style-type: none"> • Friendly
Prohibited	<ul style="list-style-type: none"> • Friendly

- 4 Select one or more APs from the list and choose an available classification from **Categorize Selected APs as**.
- 5 Click **OK** to reclassify the selected APs.

Reclassifying an AP as a Threat

Friendly and Uncategorized APs can be reclassified as a threat.

- 1 From the **Friendly** or **Uncategorized** AP List, select one or more APs and click **Prohibited**. The **Reclassify APs** dialog displays.

**Figure 189: Reclassify an AP as a Threat**

- 2 Select a threat classification from the list displayed.
- 3 Click **Save**.

Related Links

[Viewing the List of Friendly APs](#) on page 584

[Viewing the List of Uncategorized APs](#) on page 587

Working with Radar Reports

The Analysis Engine receives reports of threats from multiple APs. Different APs can be reporting the same threat incident at the same time. The Analysis Engine needs a way to decide which reports are actually reports of the same threat. It takes a number of factors into account when making this decision. Location is an important attribute used to decide whether two different reports are actually for the same threat.

To view Radar AP reports and statistics:

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**.

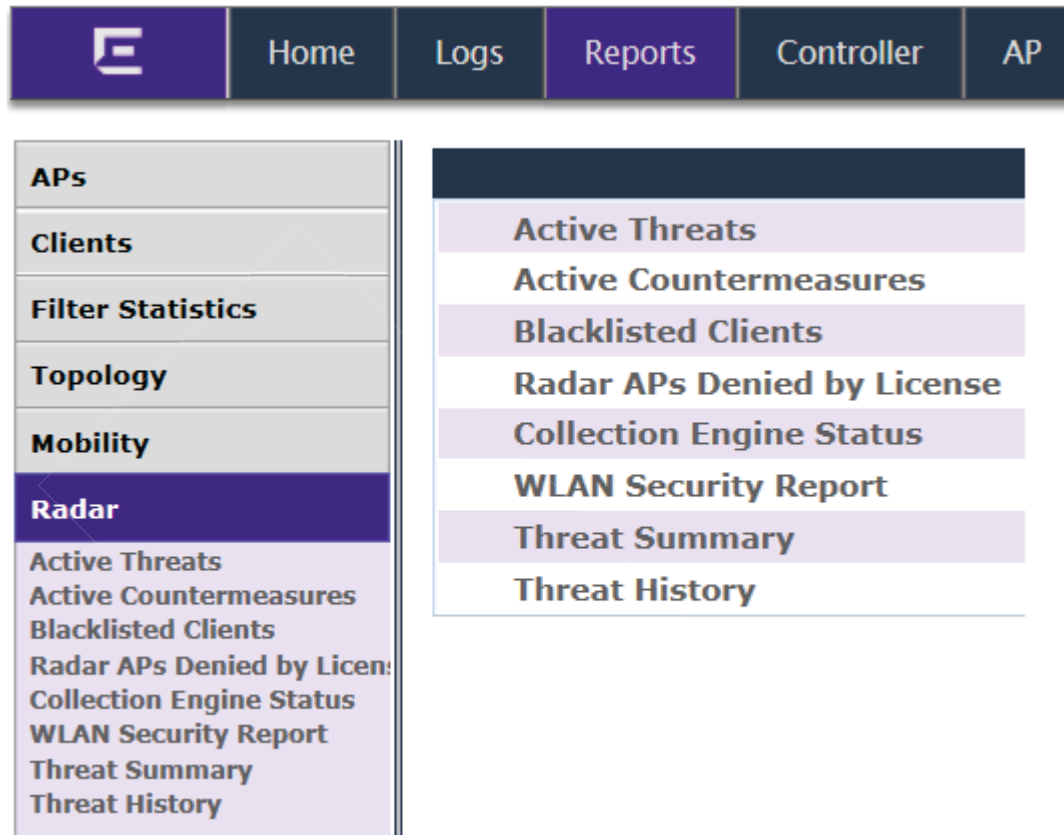


Figure 190: Radar Reports

- 3 Click on the desired report:
 - [Active Threats](#) on page 595
 - [Active Countermeasures](#) on page 597
 - [Blacklisted Clients](#) on page 598
 - [Radar APs Denied by License](#) on page 599
 - [Collection Engine Status](#) on page 599
 - [WLAN Security Report](#) on page 600
 - [Threat Summary](#) on page 601
 - [Threat History](#) on page 603

Security Threats

The Radar reports provide information about security threats. Threat APs are APs that have been detected performing one or more types of attack on the authorized network.

Each AP defined on the controller has a text location attribute that can be set using the controller's GUI, CLI, and *SNMP* agent. By default the location attribute is empty for all APs. It is strongly recommended

that you set the location attribute of each AP. The attribute should be set so that APs at the same location have exactly the same location attribute. For example all the APs on the 3rd floor of a building could have the same location, such as "Boston/123 4th street/3rd floor". The controller's multi-edit page provides a convenient way to assign groups of APs to the same location.

The types of threat recognized by the Radar WIDS-WIPS system include:

- **Ad Hoc Device** - A device in ad hoc mode can participate in direct device-to-device wireless networks. Devices in ad hoc mode are a security threat because they are prone to leaking information stored on file system shares and bridging to the authorized network.
- **Cracking** - This refers to attempts to crack a password or network passphrase (such as a WPA-PSK). The Chop-Chop attack on WPA-PSK and WEP is an example of an active password cracking attack.
- **Denial of Service (DoS) attacks** - DoS attacks
- **External Honeypot** - An AP that is attempting to make itself a man-in-the-middle by advertising a popular SSID, such as an SSID advertised by a coffee shop or an airport.
- **Interference Source** - A device that is generating a radio signal that is interfering with the operation of the wireless network. An example of an interference source is a microwave oven which can interfere with 2.4GHz transmissions.
- **Internal Honeypot** - An AP that is attempting to make itself a man-in-the-middle by advertising an SSID belonging to the authorized network.
- **Roque AP** - A rogue AP is an unauthorized AP connected to the authorized wired or wireless network.
- **Performance** - Performance issues pertain to overload conditions that cause a service impact. Performance issues aren't necessarily security issues but many types of attack do generate performance issues.
- **Prohibited Device** - A MAC address or BSSID is detected that matches an address entered manually into the Radar database.
- **Spoofed AP** - An AP that is not part of the authorized network is advertising a BSSID (MAC address) that belongs to an authorized AP on the authorized network.
- **Surveillance** - A device or application that is probing for information about the presence and services offered by a network.



Note

Surveillance can be passive (purely listening) or active (surveyor sends messages to speed up the process of surveillance). It is only possible to detect active surveillance. Netstumbler and Wellenreiter are examples of active surveillance tools.

Active Threats

The Active Threats report lists all currently detected threats. Active threats are devices that are being detected performing attacks on the authorized network. Threat APs are identified as APs that have been detected to be performing one or more types of attacks on the authorized network. The report only lists currently active threats, not historic threats. For more information, see [Threat History](#) on page 603.

Viewing Active Threats Scan Results

- 1 From the top menu, click **Reports**.

- 2 In the left pane, click **Radar**.
- 3 Click **Active Threats**.

The screenshot shows a web interface for 'Active Threats Report'. At the top, it says 'Showing 1 to 1 of 1 entries'. Below this is a table with the following columns: Detected Active At, Threat MAC Address, Threat, Threat Category, Countermeasures Applied, Location - AP Name, Location - RSS, and Additional Details. The table contains one row with the following data: 09/13/2016 06:28:17, FF:FE:FF:FE:FF:FF, Possible attack on WEP or WPA - Extensive frame receive errors, Cracking, No, C5110 - ap3 - AP2825e, N/A, and frequency=N/A. At the bottom, it says 'Showing 1 to 1 of 1 entries' again.

Figure 191: Active Threats Report

Table 118: Active Threats Report - Fields and Buttons

Field/Button	Description
Detected Active At	Date and time that the threat was identified.
Threat MAC Address	MAC address of the device.
Threat	Type of threat.
Threat Category	For more information, see Security Threats on page 594.
Countermeasures Applied	Indicates if a countermeasure has been applied.
Location - AP Name	Name of the threat AP.
Location - RSS	Threat AP Received Signal Strength (displayed in dBm).
Additional Details	<p>Details of the threat including frequency, SSID, and Rogue Threats.</p> <ul style="list-style-type: none"> Rogue threats details are accessed by clicking 3 dots “...” that display in the column. The following parameters display in the Rogue Details dialog: Sent MAC address: Sent wireless test packet source MAC address. Received MAC address: Received wired test packet source MAC address. <p>When the Threat Report is based on MAC address, we can determine the SSID and encryption type associated with the threat. This information is not preserved after upgrade, and historical data is aged every 30 days regardless of upgrade.</p> <ul style="list-style-type: none"> Sent IP address: Wireless test packet source IP address. This IP address is automatically assigned via <i>DHCP (Dynamic Host Configuration Protocol)</i> (DHCP is through the Rogue AP). Received IP address: Wired test packet source IP address. TTL difference: TTL (Time-To-Live or hop limit) difference between sent wireless test packet TTL and received wireless test packet TTL. For example, if the TTL of the sent wireless test packet is 64 and the TTL of the received wireless test packet is 62, then the TTL difference is 2 indicating the packet went through 2 hops. Learned gateway: Wireless gateway IP address as specified from the DHCP server (DHCP is through the Rogue AP).

Modifying the Page's Refresh Rate:

- 1 Type a time (in seconds) in the **Refresh every ___ seconds** box at the top of the screen and click **Apply**. The new refresh rate is applied.
- 2 To add a specific threat to the list of Friendly APs, select the threat and click **Add to Friendly List**.
- 3 To refresh the page, click **Refresh**.
- 4 To export a copy of the report in XML format, click **Export**.
- 5 To close the report window, click **Close**.

Active Countermeasures

The Active Countermeasures report lists each AP currently taking countermeasures. The list also contains the type of attack being countered, when the counter attack started, which channel is being defended, the type of countermeasure in use and when appropriate, the identifiers for the target of the attack.

Viewing Active Countermeasures Scan Results

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**. The **Available Radar Reports** screen displays.
- 3 Click **Active Countermeasures**. The **Active Countermeasures Report** screen displays.

Table 119: Active Countermeasures Report - Fields and Buttons

Field/Button	Description
AP Name	Name of the AP taking countermeasures.
AP Serial Number	Serial number of the AP
Threat Category	For more information, see Active Threats on page 595.
Countermeasure	Indicates type of countermeasure applied.
Threat MAC Address	MAC address of the device being countered.
Started At	Date and time that the threat was identified.

Modifying the Page's Refresh Rate:

- 1 Type a time (in seconds) in the **Refresh every __ seconds** box at the top of the screen and click **Apply**. The new refresh rate is applied.
- 2 To refresh the page, click **Refresh**.
- 3 To export a copy of the report in XML format, click **Export**.
- 4 To close the report window, click **Close**.

Blacklisted Clients

The Blacklisted Clients report lists all devices that are currently on the blacklist (or removed from the whitelist if the list is in whitelist mode) because of the application of countermeasures to an attack. Clients automatically added to the Blacklist will be removed automatically after the interval configured passes. Station addresses manually added to the Blacklist (or manually removed from the Whitelist) do not appear in this report.

Viewing Blacklisted Clients Scan Results

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**.
- 3 Click **Blacklisted Clients**. The **Blacklisted Clients Report** screen displays.

Table 120: Blacklisted Clients Report - Fields and Buttons

Field/Button	Description
Blacklisted Address	MAC address of the blacklisted device.
Blacklisting Started at	Date and time when the device was added to the blacklist.
Blacklisting Ends at	Date and time when the device was removed from the blacklist.
Reason	Reason for blacklisting the device.

To modify the page's refresh rate:

- 1 Type a time (in seconds) in the **Refresh every __ seconds** box at the top of the screen and click **Apply**. The new refresh rate is applied.
- 2 To refresh the page, click **Refresh**.

- 3 To export a copy of the report in XML format, click **Export**.
- 4 To close the report window, click **Close**.

Radar APs Denied by License

The Radar APs Denied by License report lists all currently unlicensed APs.

Viewing Radar APs Denied by License Results

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**.
- 3 Click **Radar APs Denied by License**. The Radar APs Denied by License screen displays.



Table 121: Radar APs Denied by License Report - Fields and Buttons

Field/Button	Description
Assigned APs	Identifies the name of the assigned Radar APs denied by license.
Scan Profile	Identifies the associated scan profile for the assigned AP.

Collection Engine Status

You can view a report on the connection status between the Analysis Engine and the remote data collector engine on each controller.

To view the collection engine status:

- 1 From the top menu, click **Reports**.
- 2 In the left pane, under **Radar**, click **Collection Engine Status**.



The boxes display the IP address of the Data Collector engine. The status of the Data Collector engine is indicated by one of the following colors:

- **Green** — The Analysis Engine has connection with the Data Collector on that controller.
- **Yellow** — The Analysis Engine has connected to the Data Collector but has not synchronized with it. Ensure that the Data Collector is running on the remote controller.
- **Red** — The Analysis Engine is aware of the Data Collector and attempting to connect.

If no box is displayed, the Analysis Engine is not attempting to connect with that Data Collector Engine.



Note

If the box is displayed red and remains red, ensure your IP address is correctly set up to point to an active controller. If the box remains yellow, ensure the Data Collector is running on the remote controller.

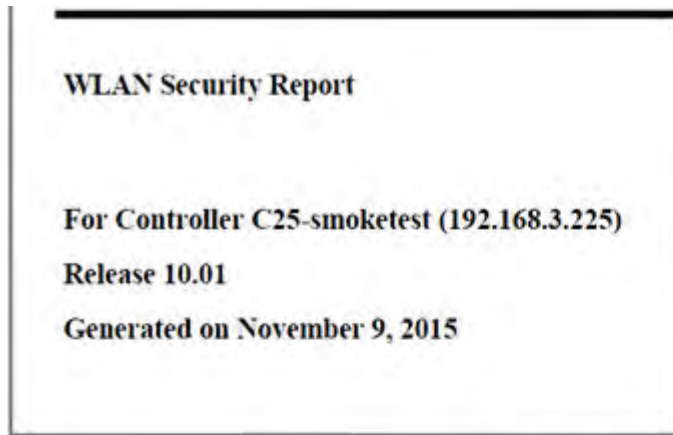
- 1 To modify the page's refresh rate, type a time (in seconds) in the **Refresh every __ seconds** box at the top of the screen and click **Apply**. The new refresh rate is applied.
- 2 To refresh the page, click **Refresh**.
- 3 To close the report window, click **Close**.

WLAN Security Report

The WLAN Security Report creates a PDF identifying security-related problems in the configuration of the wireless controller WLAN Services. The report identifies issues and provides guidance for their resolution. The report can be printed or saved locally.

Viewing WLAN Security Report Scan Results

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**.
- 3 Click **WLAN Security Report**.



Introduction

This report identifies security-related problems in the configuration of the controller EWC's WLAN services. The report identifies issues and provides guidance for their resolution.

Report Summary

Issue Summary

Table 1: Counts of WLAN Services and WLAN Services with Issues

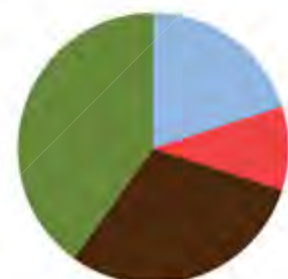
	Enabled Services	Disabled Services
WLAN Service	16	3
WLAN Service with Issues	8	1

Distribution of Issues

Enabled WLANs



All WLANs



- WLANs with Open Security
- WLANs using WEP
- WLANs using TKIP
- WLANs using WEAK passphrases
- WLANs using vulnerable SSIDs
- WLANs using Hotspot or Default SSIDs

Figure 192: WLAN Security Report

Threat Summary

The Threat Summary report includes both Active and Historical Threats displayed in the form of pie chart graphs. A device can be counted more than once if it is the source of more than one threat. Each threat category is highlighted using a different color to quickly identify specific threats.

Viewing the Threat Summary

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**.
- 3 Click **Threat Summary**. The Threat Summary screen is displayed.

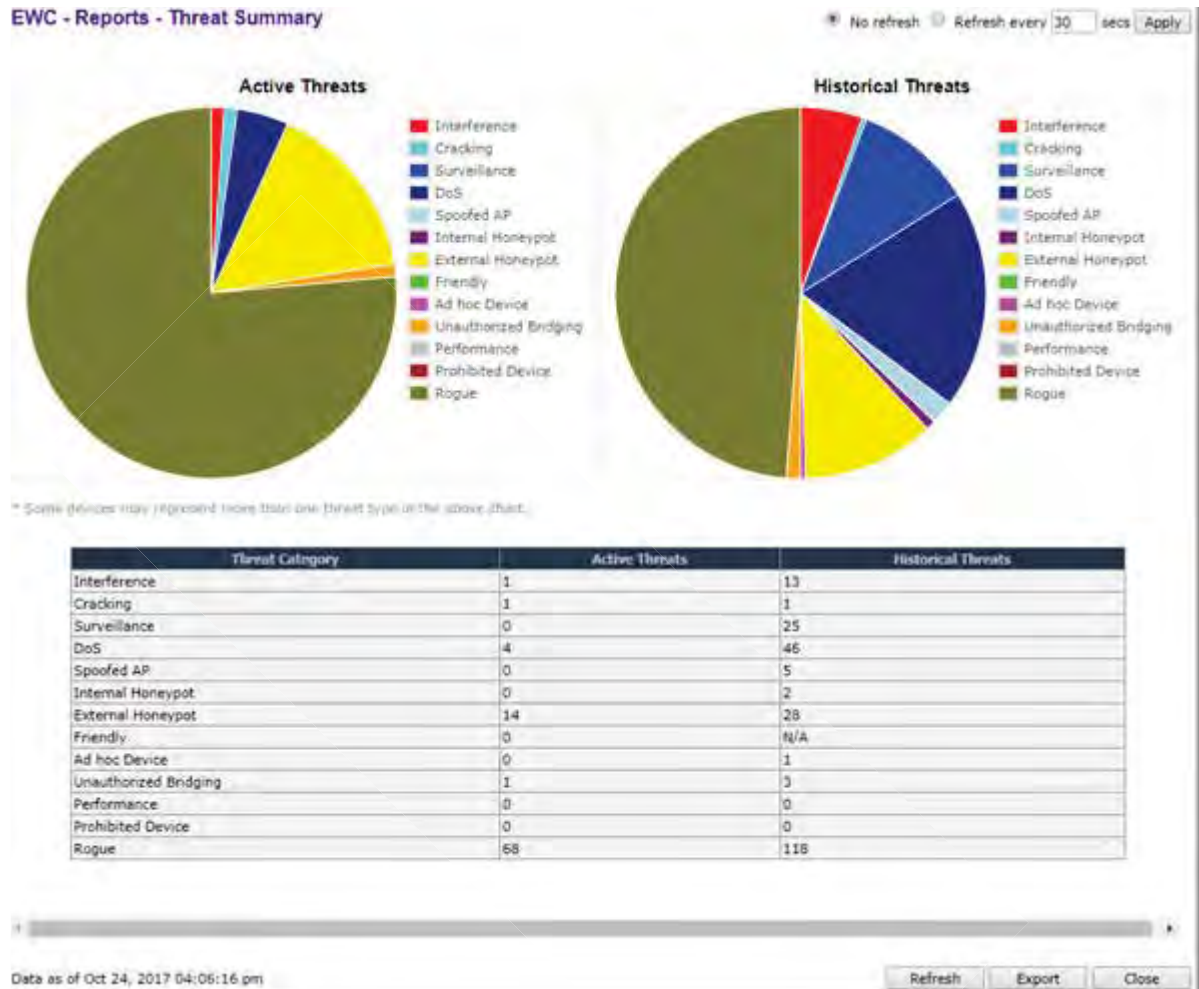


Table 122: Threat Summary Report - Fields and Buttons

Field/Button	Description
Threat Category	List of possible threat categories that are displayed on the summary report. For more information, see Security Threats on page 594.
Active Threats	Total number of active threats identified for each threat category.
Historical Threats	Total number of threats that are no longer active but have been retained on the list for historical tracking purposes. Threats are identified for each threat category.

Modifying the Page's Refresh Rate

- 1 Type a time (in seconds) in the **Refresh every __ seconds** box at the top of the screen and click **Apply**.
- 2 To refresh the page, click **Refresh**.
- 3 To export a copy of the report in XML format, click **Export**.
- 4 To close the report window, click **Close**.

Threat History

Viewing the Threat History

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**.
- 3 Click **Threat History**. The **Threat History** screen displays.

C5110-smoketest - Reports - Historical threat report

Showing 1 to 27 of 27 entries

First Previous 1 Next Last Search:

Last Reported	First Detected	Threat MAC Address	Threat	Threat Category	Currently Active	Location	Additional Details
09/13/2016 13:58:59	09/13/2016 08:25:41	FF:FF:FF:FF:FF:FF	Null probe response attack	DoS	Inactive	C5110 - ap3 - AP3825e	N/A frequency=2427
09/13/2016 13:58:17	09/13/2016 04:27:56	FF:FF:FF:FF:FF:FF	Possible attack on WEP or WPA - Excessive frame receive errors	Cracking	Active	C5110 - ap3 - AP3825e	N/A frequency=N/A
09/13/2016 13:13:08	09/13/2016 12:51:11	FF:FF:FF:FF:FF:FF	Authentication frame flood attack	DoS	Inactive	C5110 - ap3 - AP3825e	N/A frequency=5785
09/13/2016 12:44:05	09/13/2016 12:36:05	FF:FF:FF:FF:FF:FF	Invalid disconnect code attack	DoS	Inactive	C5110 - ap3 - AP3825e	N/A frequency=5785
09/13/2016 09:45:10	09/13/2016 05:46:44	N/A	Microwave	Interference	Inactive	C5110 - ap3 - AP3825e	N/A frequency=2422
09/13/2016 09:44:08	09/13/2016 05:42:01	N/A	Microwave	Interference	Inactive	C5110 - ap3 - AP3825e	N/A frequency=2417
09/13/2016 09:41:06	09/13/2016 09:40:39	N/A	Video Bridge	Interference	Inactive	C5110 - ap3 - AP3825e	N/A frequency=2432
09/13/2016 09:41:06	09/13/2016 09:40:50	N/A	Photo	Interference	Inactive	C5110 - ap3 - AP3825e	N/A frequency=2432
09/13/2016 09:40:46	09/13/2016 09:40:40	N/A	Video Bridge	Interference	Inactive	C5110 - ap3 - AP3825e	N/A frequency=2427

Table 123: Historical Threat Report - Fields and Buttons

Field/Button	Description
Last Reported	Date and time when the threat was most recently reported.
First Detected	Date and time that the threat was identified.
Threat MAC Address	MAC address of the device.
Threat	Type of threat.
Threat Category	For more information, see Active Threats on page 595.
Currently Active	Current status of the threat.
Location - AP Name	Name of the threat AP.
Location - RSS	Threat AP Received Signal Strength (displayed in dBm).
Additional Details	Detail information on the specific threat. When the Threat Report is based on MAC address, we can determine the SSID and encryption type associated with the threat. This information is not preserved after upgrade, and historical data is aged every 30 days regardless of upgrade.

- 4 To export a copy of the report in XML format, click **Export**.
- 5 To close the report window, click **Close**.

Draft

17 Working with Location Engine

Location Engine Overview

Location Engine on the Controller

Deploying APs for Location Aware Services

Configuring the Location Engine

ExtremeLocation Support

Location Engine Overview

Station location tracking is one of the advanced ExtremeWireless Radar features designed for managing a wireless environment and its resources. The Location Engine works in conjunction with Extreme Management Center maps to define specific floor plan areas for Location Aware Services.

The Location Engine determines location based on measured Received Signal Strength (RSS) of the client stations at the AP. The location algorithm uses RF finger printing based on a Path Loss model and determines location by triangulating RSS reported from one or more APs.

Estimating location using readings from multiple APs provides a more accurate location estimate. Estimating location using RSS from a single AP is sufficient to determine the location of client in terms of proximity to the associated AP. The client location is indicated on the map as a circle around the AP. Estimation using multiple RSS offers a pinpoint location estimate of the client. The client location is indicated as a pin, in the most probable position, on the map. The colors displayed around the pin indicate the level of confidence that the client is physically located there.

The Location Engine tracks location of multiple clients simultaneously and returns position relative to the floor plan.

The Location Engine can be configured to track on-demand users, associated users, and unassociated users:

- An on-demand user is a client that is manually added to a preferred list of clients. Space is guaranteed for on-demand users in the Location Engine table. An on-demand user can be either an associated user, such as an employee, or an unassociated user, such as a rogue client that can be tracked as a possible network threat.
- An associated user is an authenticated client. An associated user joins the SSID provided by the AP by simply associating to the open or protected SSID. Location Engine can track location for every associated client up to the controller limit of associated clients.
- An unassociated user is a client that is not authenticated but is in the designated area. Location Engine can track these clients.

No additional license is required to use the Location Engine functionality in the controller. However, to draw maps and to visualize location tracking, Extreme Management Center is required, which comes with its own licensing requirements.

Location Solution Architecture

The ExtremeWireless controller is at the center of the Location Aware Services solution. Location Engine collects RSS reading from APs and displays location data using Extreme Management Center maps or other third-party applications. The following diagram illustrates the solution architecture.

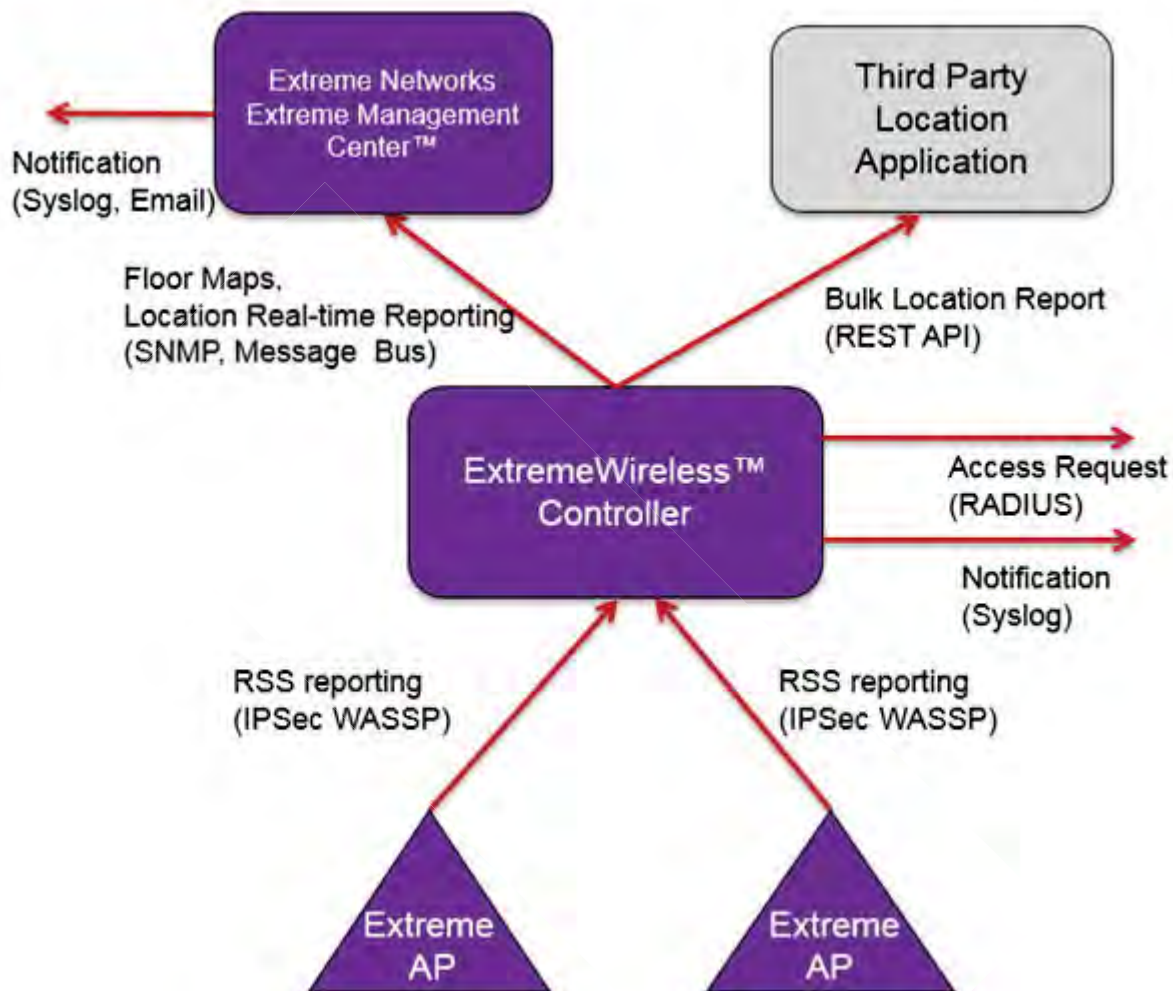


Figure 193: Components of Location Aware Services Solution

Dynamic Filtering

Dynamic filtering is a primary use case for Location Aware Services. This feature controls client access based on location. Customers can use Location Aware Services in schools and hospitals to define access parameters within a designated area. This functionality combined with the role assignment from Network Access Control (NAC), makes it possible to implement dynamic filtering on the client location. Network access rights (access to servers or applications) can depend on the client location -- inside or outside the defined area. Role assignment is accomplished dynamically by the controller and NAC as client moves within the floor plan.

Bulk Reporting

Location Engine can export bulk reporting data for use in third-party applications. For example, use Location Engine data to determine traffic flow in large venues and time-of-use analytics. The controller's bulk reporting data includes location of the client, the serial number of the associated AP, the name of the floor plan, and more. Third-party location client applications can synchronize their floor maps directly from the controller (either on-demand or on a scheduled basis using the controller CLI).

Although it is possible to access the Location Engine data directly using a CLI session, most users will choose to access location data using Extreme Management Center maps or a third-party location client application.

Location Engine on the Controller

Location Engine tracks location of multiple clients simultaneously and returns position relative to the floor plan. The following are components of the Location Engine:

- **Heat Map.** The Location Engine generates a heat map of each AP on a user-provided floor plan. The Location Engine analyzes the floor plan and considers the presence and material of structures or obstacles, such as walls, when calculating the predictive coverage map.

Extreme Management Center™ is required to define the floor plan. Be sure to include the presence of walls and obstacles when defining the floor plan. For information about defining a floor plan, see the *Extreme Management Center™ User Guide*.

- **Localization algorithms.** Location Engine algorithms scan all APs that report the client and select RSS readings from three or more APs that are most likely to provide the best location estimates. Using the selected RSS readings, location is triangulated and returned as the Cartesian coordinates relative to the floor plan.
- **Notification.** Location is reported immediately on a real-time stream and as a notification on the event stream (syslog). The controller tracks the client location and can determine when a client is inside a predefined area. You can define up to 16 areas of interest per floor map using Extreme Management Center. The Location Engine offers a Track Area Change feature, that, when enabled, triggers a notification each time a client moves from one area to another. The notification events can be used for improved radio resource management such as Network Access Control (NAC). For information about how to enable Track Area Change, see [Configuring the Location Engine](#) on page 609.
- **Simultaneous updates.** Location Engine simultaneously updates the location of tracked clients. It can track the number of clients that can be supported by the controller. If the controller is part of an availability pair, it can also track the clients supported by the availability partner, and Location Engine is not restricted by floor size.

Client location is presented in Extreme Management Center. [Figure 194](#) illustrates a blue pin placed on the most probable position of the client. The map is colored according to the expected probability of the client position. Black is the most likely and yellow is the least likely position.

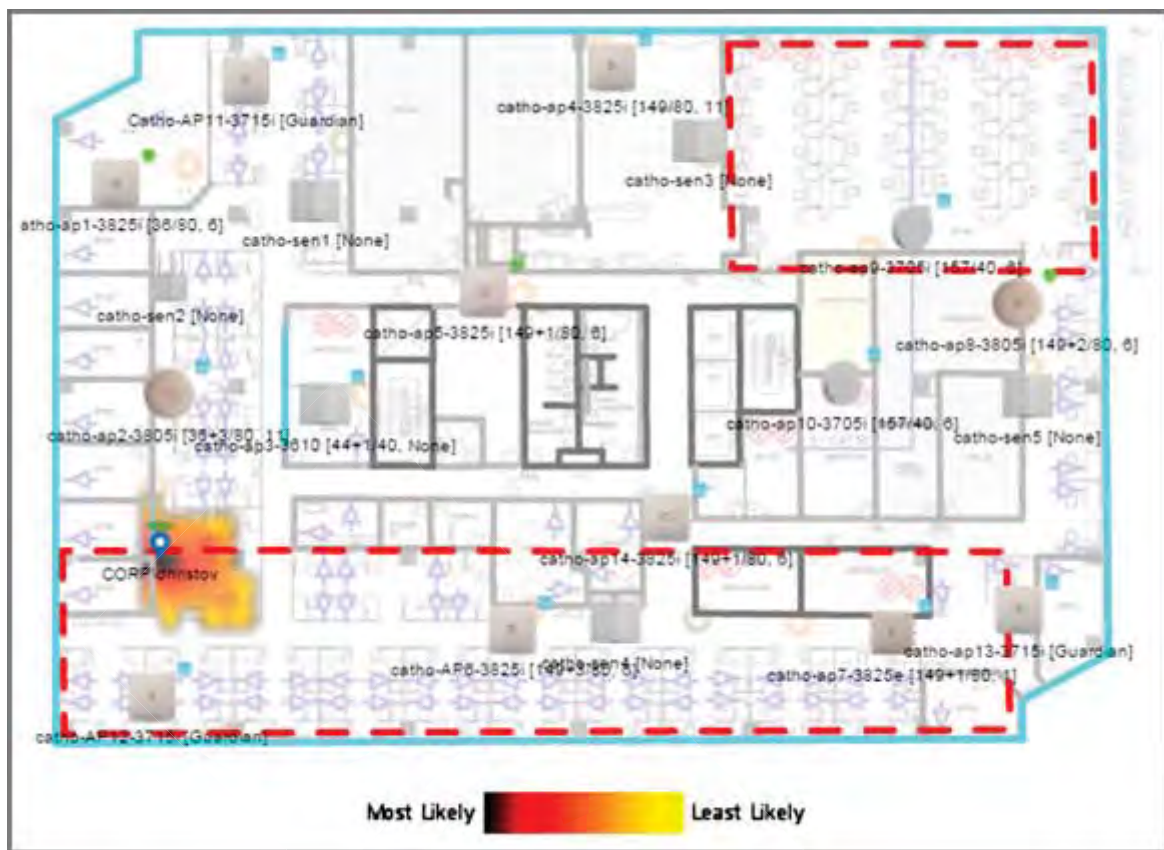


Figure 194: Extreme Management Center Floor Plan

Deploying APs for Location Aware Services

Deploying APs for location tracking requires additional consideration above the standard AP deployment guidelines for coverage and capacity. The following are best practices for AP deployment:

- Minimum Received RSS. No less than three APs should be detecting and reporting the RSS of any client station. Only RSS reading stronger than -75 dBm are used by the Location Engine.
- Use the same AP model for the entire floor plan, so that the RSS readings in that area will have less variation.
- Design your floor plan with the APs installed at the corners of the floor plan, along the perimeter of the location area. (An area is considered a closed polygon.) Do not cluster APs in the center of the location area. The following illustration shows a recommended AP placement.

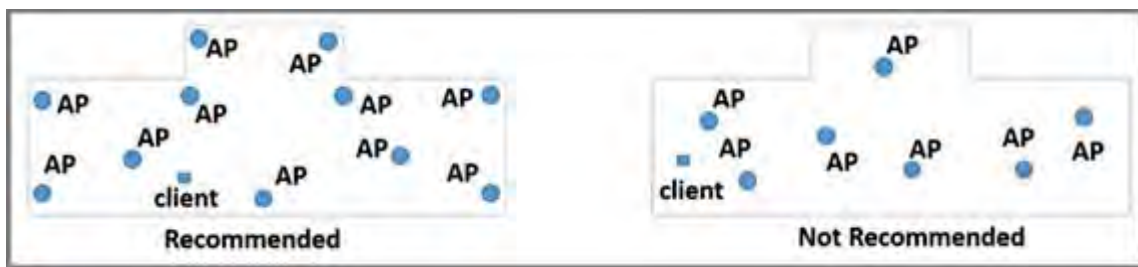


Figure 195: Recommended AP Placement

- The maximum distance between APs depends on environmental factors such as the presence of walls and structures, but as rule of thumb, in a location aware deployment, place the APs 10 to 20 meters apart.
- Install APs at the same height on the wall, and do not install APs behind walls or ceilings.
- Install APs away from metal structures like poles or racks, because metal can affect the radiated pattern.

When location accuracy is paramount, augment your in-service deployment with Guardian APs. Guardian APs scan multiple channels where in-service APs operate on a single channel. Therefore, Guardian APs are capable of registering readings from more clients than in-service APs. Guardian APs also increase the number of triangulation points. The Guardian mitigates the problem of non-probing clients and is capable of sensing a client based on the data packets. For more information, see [Configuring an AP as a Guardian](#) on page 221.

Configuring the Location Engine

Location Engine configuration involves defining environmental factors in the floor plan, location targets, area change notification, and client targets. The following information is provided to help you configure the Location Engine:

- [Enabling the Location Engine](#) on page 609
- [Location Batch Reporting](#) on page 611
- [Creating a New Destination URL](#) on page 613
- [Creating a New On-Demand User](#) on page 613
- [Downloading a Floor File](#) on page 614
- [Uploading a Floor File](#) on page 616
- [Deleting a Floor File](#) on page 618

Enabling the Location Engine

- 1 From the top menu, click **WIPS**.
- 2 In the left pane, click **Location Engine**. The **Location Engine Settings** screen displays.

- 3 To Enable/Disable the Location Engine, select or clear the **Location Engine** check box.

The screenshot shows the 'Location Engine' configuration interface. The sidebar on the left lists various configuration categories, with 'Location Engine' currently selected. The main panel displays the 'Location Engine' settings, which are currently enabled (checked). Under 'Environment Settings', the 'Default AP Height (cm)' is set to 300, and the 'Default Environment Model' is set to 'Office Environment with dry walls divisions'. The 'Location Targets' section shows 'Locate' set to 'All', 'Track Area Change' is checked, and there is an 'On-Demand Users' list with 'Add' and 'Delete Selected' buttons. At the bottom right, there are 'Advanced...' and 'Save' buttons.

Table 124: Location Engine Settings Dialog - Fields and Buttons

Field/Button	Description
Environment Settings	
Default AP Height (cm)	Enter the height of the AP based on its location on the wall.
Default Environmental Model	<p>Select a mode that best matches the environment identified by the floor plan. Choose from one of the following modes from the drop-down list:</p> <ul style="list-style-type: none"> Indoor open space (halls, auditoriums) Office Environment with light divisions (cubicles) Office Environment with dry wall divisions Office Environment with hard divisions (brick) Interior Walls (need be defined in the floor plan)
None	Locator does not collect or triangulate RSS readings.
Clients	Locator tracks active sessions only.

Table 124: Location Engine Settings Dialog - Fields and Buttons (continued)

Field/Button	Description
All	Locates all active users and all non-associated users (MAC) around deployed APs located within the signal range. RSS readings from non-associated users are included in the Location Engine table. Note: The Location Engine table is shared between all tracked users. This table does not increase in size and does not reserve space for associated users. Once the number of tracked users exceeds the limit, additional users will not be added to the table. Users remain in the table until they time out. Users designated as On-Demand are guaranteed space in the Location Engine table.
Track Area Change	The controller tracks the client location and can determine when a client is inside a predefined area. Select Track Area Change to trigger a notification when a client moves from one area to another. Use the notification events to improve radio resource management such as Network Access Control (NAC).
On-Demand Users	Displays a list of known MAC addresses present in the area, for example, a list of employees. On-demand users are guaranteed space in the Location Engine table.
Add	Click to create a new on-demand user. For more information, see Creating a New On-Demand User on page 613
Delete Selected	Click to delete the selected on-demand user.
Advanced	Click to open the Advanced dialog, which lists available floor plans. From the Advanced dialog, you can upload and download floor plans. For more information, see Downloading a Floor File on page 614
Save	Click to save changes.

Location Batch Reporting

When the Location Engine is enabled and configured to publish locations, it posts location data in XML format to a given location. The location data is pushed to up to five given destinations periodically within the given time interval. Batch reporting continues until Location Batch Reporting is disabled, the Location Engine is disabled, or the controller is powered off.

In location-based applications and user traffic analytics, integrating partners often require more detail than simply the location of a MAC address. The client reporting option allows users to generate a report with details from the MU-Table.

The AP reporting option provides AP details that give a third-party App server context for the AP location.

To generate a report:

- 1 From the top menu, click **WIPS**.
- 2 In the left pane, click **Location Engine**.
- 3 To enable/disable the Location Batch Reporting, in the left pane, select **Location Batch Reporting** then select the **Location Batch Reporting** check box.

- 4 To enable/disable the Client Reporting, in the left pane, select **Location Batch Reporting** then select the **Clients Detail Reporting** check box.
- 5 To enable/disable the AP Detail Reporting, in the left pane, select **Location Batch Reporting** then select the **AP Detail Reporting** check box.

Configuration

AirDefense Profiles

Radar Profiles

Radar Maintenance

Location Engine

Location Engine Settings

Location Batch Reporting

ExtremeLocation™

☐ Location Batch Reporting

☐ Clients Detail Reporting

☒ AP Detail Reporting

Report every minute(s)

Dimension Unit

Post all location destinations to the following URLs:

Login	Password	Destination URL

Figure 196: Reporting Options

The following details are provided with the AP Detail Reporting option:

- name
- serial
- hostname
- ipAddress
- macAddress
- iotMacAddress
- iotRadioMode
- iotProtocol
- iBeaconProperties
 - iBeaconUUID
 - iBeaconMajor
 - iBeaconMinor



Note

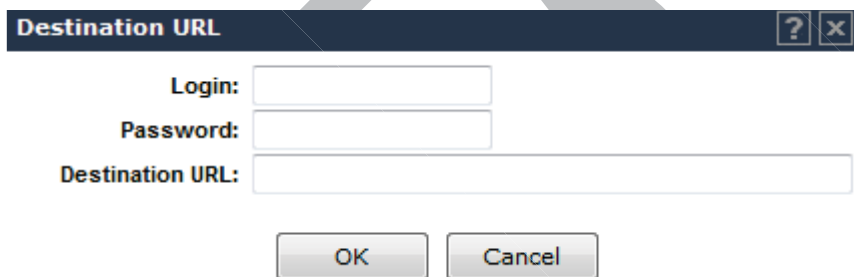
The IoT data is provided when the IoT port is enabled and provisioned. IoT is enabled by default for supported APs.

Table 125: Reporting Fields and Buttons

Field/Button	Description
Report all station locations every (X) minutes	Select a time (in minutes) for station reporting from the drop-down list.
Dimension Unit	Select a dimension unit, from the drop-down list, for measuring location destinations. (Displayed for Location Batch Reporting only.)
Login	Login ID of the destination URL.
Password	Password of the destination URL.
Destination URL	List of destination URLs.
Add	Click to create a new Destination URL. For more information, see Creating a New Destination URL on page 613.
Delete Selected	Click to delete the selected Destination.
Save	Click to save changes.

Creating a New Destination URL

- 1 From the top menu, click **WIPS**.
- 2 In the left pane, click **Location Engine > Location Batch Reporting** and select either **Location Batch Reporting** or **Client Detail Reporting**.
- 3 Click **Add**. The Destination URL dialog displays.



Destination URL [?] [X]

Login:

Password:

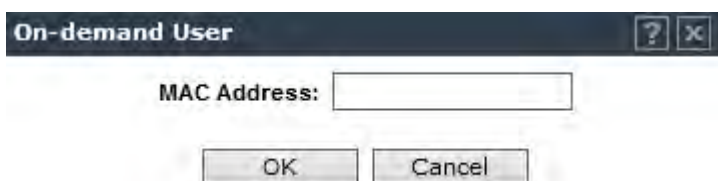
Destination URL:

- 4 Enter a user ID and password for the destination URL.
- 5 Enter a URL for the new destination.
- 6 Click **OK**.

Creating a New On-Demand User

- 1 From the top menu, click **WIPS**.
- 2 In the left pane, click **Location Engine**. The Location Engine Settings screen displays.

- 3 Click **Add**. The **On-demand User** dialog displays.



- 4 Enter a MAC Address for the new on-demand user.
- 5 Click **OK**.

Extreme Management Center Floor Files

Generate floor files using Extreme Management Center™. Floor files have the file type .fxml. Once .fxml files are generated locally, they automatically display on the Location Engine Settings **Advanced** dialog.

It is possible to download .fxml files from a server, but it is most common to generate the file locally using Extreme Management Center.

Related Links

[Downloading a Floor File](#) on page 614

[Uploading a Floor File](#) on page 616

[Deleting a Floor File](#) on page 618

Downloading a Floor File

The **Download** button is always enabled. All information about the floor plan is contained in the file being downloaded including unique identifiers for the floor plan.

- 1 From the top menu, click **WIPS**.
- 2 In the left pane, click **Location Engine**. The **Location Engine Settings** screen displays.

- 3 Click **Advanced**. The **Advanced** dialog displays.



The **Advanced** dialog box displays a table with the following data:

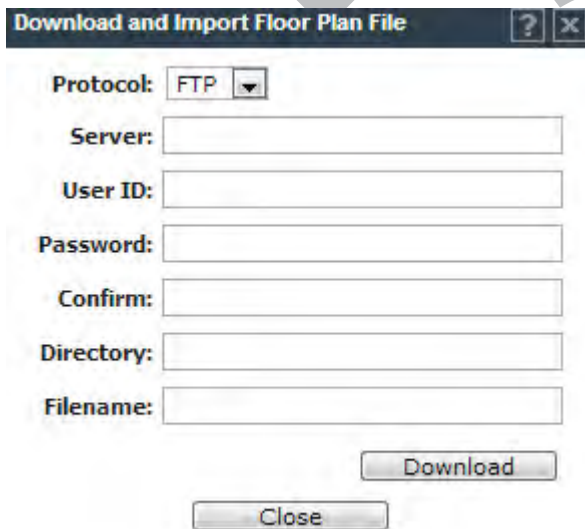
Floor ID	Floor Name	Number of APs	Cell Size	Floor Size			Type of Environment
				Number of Cells	Width	Length	
1	Thornhill	9	100X100	2035	3700	5500	Model 4

Showing 1 to 1 of 1 entries

Buttons: Download..., Upload Selected..., Delete Selected..., Close

¹ To sort by multiple columns, click the first column, hold down the SHIFT key, and then click the next column. As many columns as you wish can be added to the sort.

- 4 Click **Download**. The **Download and Import Floor Plan File** dialog displays.



The **Download and Import Floor Plan File** dialog box contains the following fields and buttons:

Protocol: **FTP**

Server:

User ID:

Password:

Confirm:

Directory:

Filename:

Buttons: Download, Close

Table 126: Download and Import Floor File Dialog - Fields and Buttons

Field/Button	Description
Protocol	Select the transfer protocol from one of the following: <ul style="list-style-type: none"> • FTP • SCP
Server	IP address of the server containing the floor file.
User ID	Required ID to access the server.
Password	Password required for access to the server.
Confirm	Enter the password for confirmation
Directory	Location of the floor file on the selected server
Filename	File name of the floor plan file on the selected server.

- 5 Click **Download** to import the floor plan, or click **Close** to cancel the import.

Related Links

[Extreme Management Center Floor Files](#) on page 614

[Uploading a Floor File](#) on page 616

[Deleting a Floor File](#) on page 618

Uploading a Floor File

The **Upload Selected** button is enabled when a row within the list of floor plans is highlighted.

- 1 From the top menu, click **WIPS**.
- 2 In the left pane, click **Location Engine**. The **Location Engine Settings** screen displays.
- 3 Click **Advanced**. The **Advanced** dialog displays.

Advanced [?] [X]

Show entries Search:

Floor ID	Floor Name	Number of APs	Cell Size	Floor Size			Type of Environment
				Number of Cells	Width	Length	
1	Thornhill	9	100X100	2035	3700	5500	Model 4

Showing 1 to 1 of 1 entries

Download... Upload Selected... Delete Selected...

¹ To sort by multiple columns, click the first column, hold down the SHIFT key, and then click the next column. As many columns as you wish can be added to the sort.

Close

- 4 Select a floor file from the list of floor files.
- 5 Click **Upload Selected**. The Upload Floor Plan File dialog displays.

Upload Floor Plan File [?] [X]

Protocol:

Server:

User ID:

Password:

Confirm:

Directory:

Filename:

Upload

Table 127: Upload Floor Plan File Dialog - Fields and Buttons

Field/Button	Description
Protocol	Select the transfer protocol from one of the following: <ul style="list-style-type: none"> FTP SCP
Server	IP address of the server where the file will be exported.

Table 127: Upload Floor Plan File Dialog - Fields and Buttons (continued)

Field/Button	Description
User ID	Required ID to access the server.
Password	Password required for access to the server.
Confirm	Enter the password for confirmation
Directory	Location of the floor file directory on the destination server.
Filename	File name of the floor plan file on the destination server.

- Click **Upload** to export the floor plan, or click **Close** to cancel the export.

Related Links

[Extreme Management Center Floor Files](#) on page 614

[Downloading a Floor File](#) on page 614

[Deleting a Floor File](#) on page 618

Deleting a Floor File

- From the top menu, click **WIPS**.
- In the left pane, click **Location Engine**. The **Location Engine Settings** screen displays.
- Click **Advanced**. The **Advanced** dialog displays.



- Select a floor file from the list of floor files. Only one floor file can be deleted at a time.
- Click **Delete Selected** to delete the floor file from the list. Click **OK** to confirm the delete operation.
- Click **Close**.

Related Links

[Extreme Management Center Floor Files](#) on page 614

[Downloading a Floor File](#) on page 614

[Uploading a Floor File](#) on page 616

ExtremeLocation Support

ExtremeWireless supports integration with ExtremeLocation™ for on-premise controller and ExtremeCloud™ deployments using AP39xx.

ExtremeLocation is a premier location tracking and analytics solution by Extreme Networks. Using HTTPS with self-signed certificates, an AP opens WebSocket connections to the ExtremeLocation Server and reports RSS signal strength readings based on the ExtremeLocation configuration. An ExtremeLocation user associates the Tenant ID and Site information with the AP MAC address over AP WebSocket.

The AP can be the RSS source for both Location Engine (integrated with Extreme Management Center) and ExtremeLocation at the same time. RSS information travels both through the WASSP tunnel to the controller and through WebSocket to ExtremeLocation. The AP operates as the ExtremeLocation client in both modes: as an in-service AP (while providing service to the associate users, collects RSS on the same channel) and as a Guardian AP (scan multiple channels and provide RSS on the channels scanned). Channels and dwell time are defined in the Guardian Group configuration.

Related Links

[Configuring ExtremeLocation](#) on page 619

Configuring ExtremeLocation

To configure ExtremeLocation support for ExtremeWireless, do the following:

- 1 Go to **WIPS > Location Engine > ExtremeLocation™**.

- 2 Check **Report to ExtremeLocation™**.

Configuration

AirDefense Profiles

Radar Profiles

Radar Maintenance

Location Engine

Location Engine Settings

Location Batch Reporting

ExtremeLocation™

☒ **Report to ExtremeLocation™**

Server Address

Minimum RSS reporting: dBm

Report every second(s)

APs

Search for AP name

<input type="checkbox"/>	Name
<input checked="" type="checkbox"/>	1548Y-1007900000
<input type="checkbox"/>	3916[F]
<input type="checkbox"/>	AP3912i-ROW-1[F]
<input type="checkbox"/>	AP3915

Figure 197: ExtremeLocation Configuration

- 3 Configure the following parameters:

Table 128: ExtremeLocation™ Configuration Parameters

Field	Description
Server Address	The IP address or FQDN (fully-qualified domain name) of the LocationEngine Server.
Minimum RSS Reporting	RSS threshold for reporting location data. Valid values are -90 to -70 dBm.
Report every number of seconds	Reporting interval in seconds.

- 4 Select one or more APs to assign for ExtremeLocation™ support. Use the search field to find a specific AP in the list. AP39xx models are supported.
- 5 Click **Save**.

Related Links

[ExtremeLocation Support](#) on page 619

18 Working with Reports and Statistics

Application Visibility and Device ID
Viewing AP Reports and Statistics
Available Client Reports
Viewing Role Filter Statistics
Viewing Topology Reports
Viewing Mobility Reports
Viewing Controller Status Information
Viewing Routing Protocol Reports
Viewing RADIUS Reports
Call Detail Records (CDRs)

This chapter describes the various reports and statistics available in the Wireless system including:

- Viewing AP Reports and Statistics
- Viewing Active Clients
- Viewing Role Filter Statistics
- Viewing Topology Reports
- Viewing Mobility Reports
- Viewing Controller Status Information
- Viewing Routing Protocol Reports
- Call Detail Records (CDRs)
- Application Visibility and Device Identification

Application Visibility and Device ID

With ExtremeWireless, you can identify devices and applications on the wireless network. From the dashboard and the Active Client report, you can view:

- IPv4 and IPv6 Addresses
- Host Name
- Operating System
- Device Type
- Top 5 Application Groups by Throughput (2-minute interval)
- Top 5 current Application Groups by Bytes, from session start.
- Throughput chart for an application group.
- Average TCP Round Trip Time.
- Average DNS Round Trip Time.

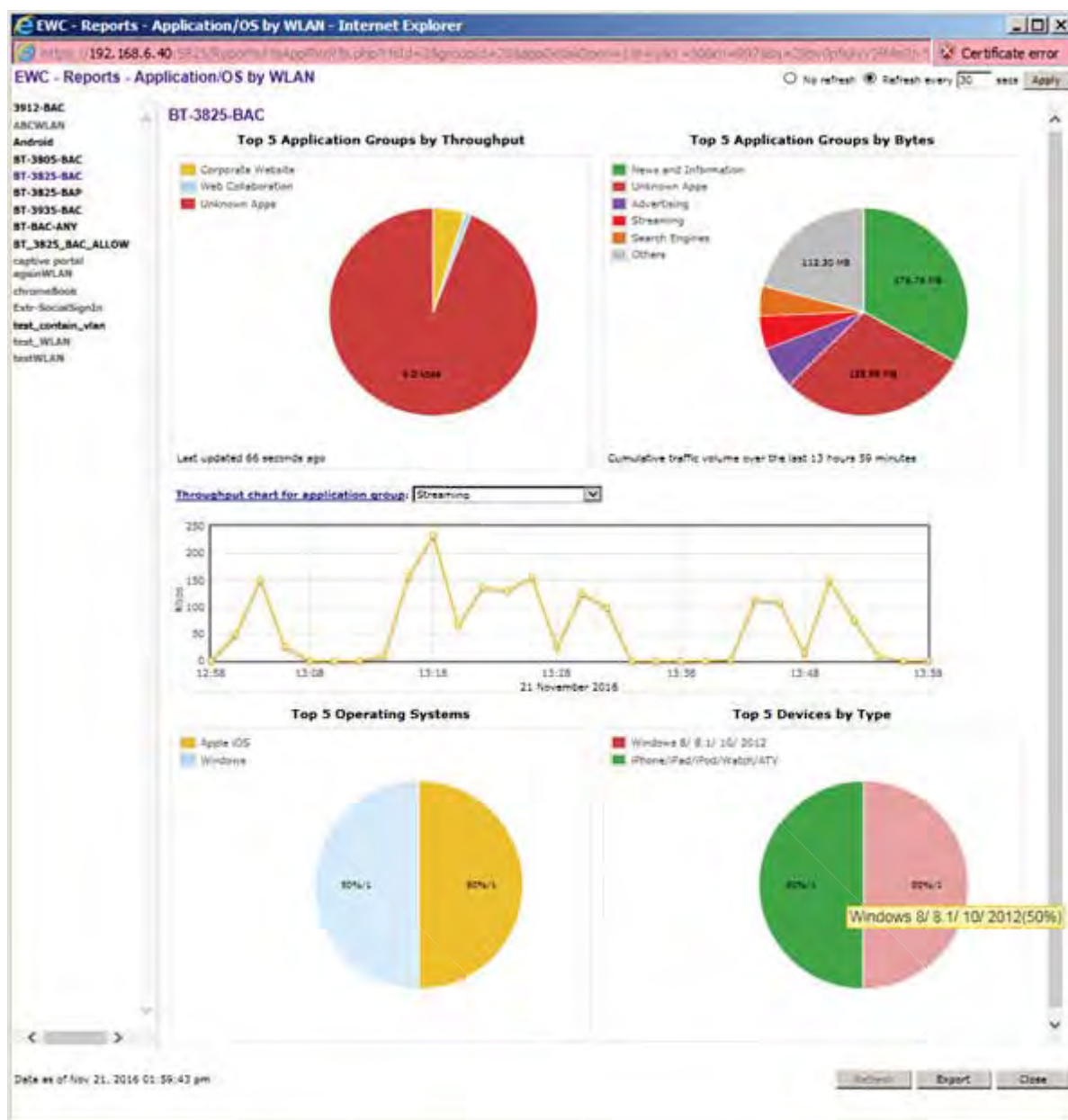


Figure 198: Application Visibility by WLAN

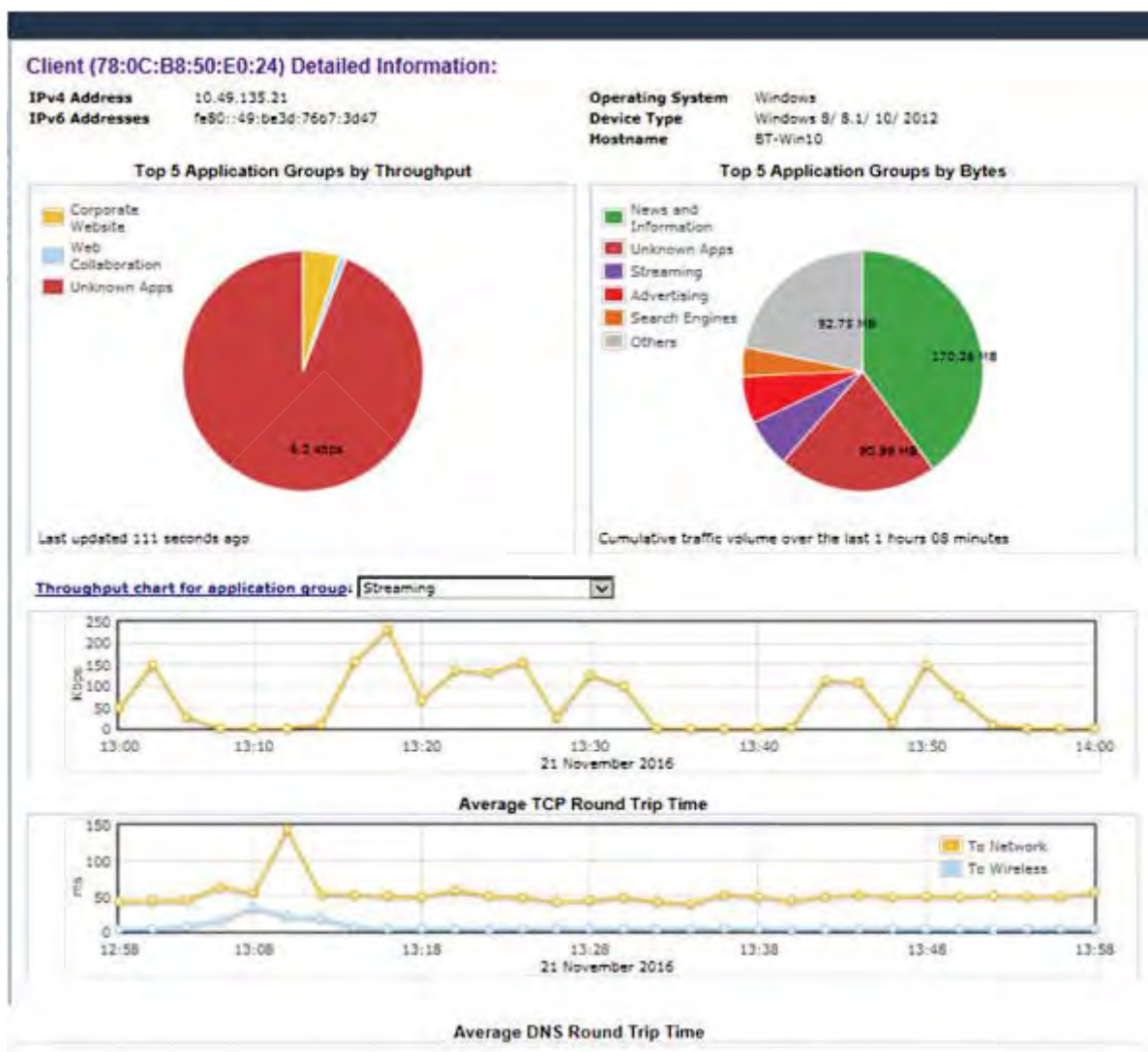


Figure 199: Application Visibility by Client

Related Links

- [Application Visibility](#) on page 623
- [Device Identification](#) on page 625
- [Enabling Application Visibility with Device Identification](#) on page 626
- [Displaying Client Details](#) on page 643
- [Wireless Assistant Home Screen](#) on page 34

Application Visibility

With the ability to gather application analytics, you can engineer wireless traffic to support company policies, preserve bandwidth, identify critical applications, assign higher priority and QoS values, and enhance network security. Application Visibility and Application Enforcement makes it possible to block restricted web content and block or limit peer-to-peer protocols to preserve network bandwidth.

With ExtremeWireless, you can view the top 5 application groups by *WLAN (Wireless Local Area Network)* from the controller Home dashboard and the top 5 application groups for each client from the [Client Details report](#).

The **Applications by WLAN** pie chart displays the top 5 application groups running on that WLAN. ExtremeWireless cycles through the active WLAN Services displaying statistics. To view detailed statistics, enable Application Visibility during the WLAN configuration; then, on the Home dashboard, click the displayed pie chart under **Applications by WLAN**. Or, click **Enable Application Visibility** from the Home dashboard.

The controller and AP capture statistics for 31 pre-selected application groups. The top 5 application groups are displayed based on bytes and throughput over the last two-minute measuring period. The stats for each WLAN display for 30 seconds on a continuous cycle. Historical statistical data is available from ExtremeCloud™ and Extreme Application Analytics™.

To manage wireless traffic in support of company policies, define Layer 7 filter rules from the **Filter Rule Definition** dialog. Layer 7 represents the application layer of the OSI communication module. Define policy rules with access control actions for specific applications or groups of applications. Application visibility supports standard Extreme Application Analytics™ signatures. You can also configure up to 64 extended web application signatures.



Note

For application enforcement, you must enable Application Visibility in WLAN configuration.

Related Links

[L7 Configuration](#) on page 307

[Application Visibility and Device ID](#) on page 621

[Device Identification](#) on page 625

[Wireless Assistant Home Screen](#) on page 34

[Enabling Application Visibility with Device Identification](#) on page 626

Application Control for Tunneled Traffic

To classify a flow, the DPI engine must examine both client and server packets. The controller enforces policy for downstream traffic and the AP enforces policy for upstream traffic. For tunnel traffic, the DPI engine must examine the packets at the controller. Enforce this by clearing the **AP Filtering** check box on the **Policy Rules** tab.

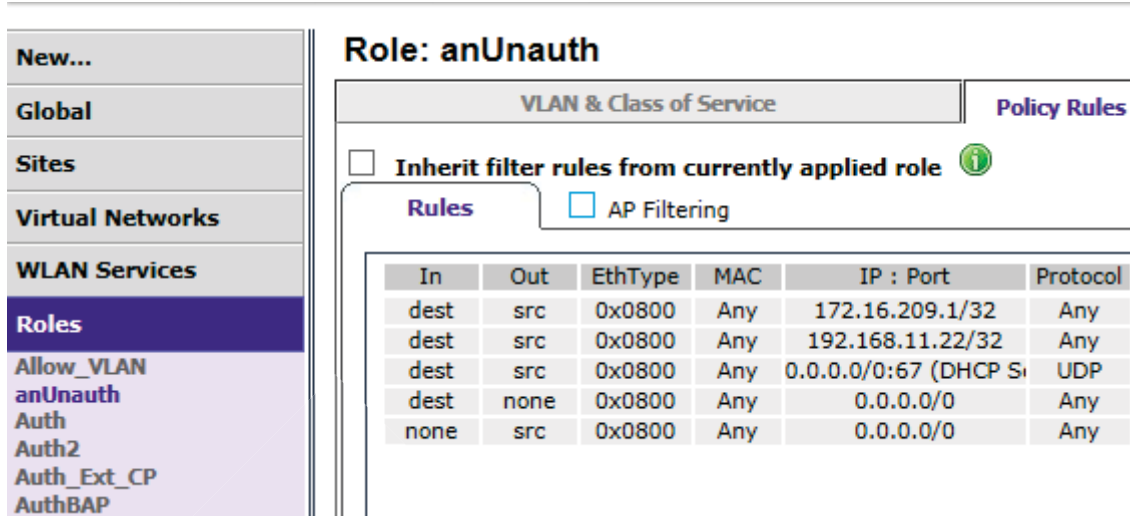


Figure 200: Configuring Policy Rules for Downstream Traffic at the Controller

Device Identification

ExtremeWireless can identify the device type and operating system used by clients associated with an ExtremeWireless AP. Gathering this information in a site deployment furthers mobile user statistical reporting on the controller or Cloud. This feature is supported on the ExtremeWireless AP38xx or AP39xx series APs. This discovery is implemented on the AP through deep packet inspection of the *DHCP (Dynamic Host Configuration Protocol)* and HTTP packets. Regardless of how the traffic is bridged -- at the controller or routed -- fingerprinting is handled on the AP. This approach offers a consistent implementation that does not require a large processing load. The AP fingerprints the same messages as Extreme Access Control.

Device ID is based on a DHCP database. The database is defined by an XML file that is built into both the AP and controller image. The XML file can be updated each time the image file is updated.

The precision of the client's identity improves overtime. Each DHCP fingerprint has an assigned weight in the XML file. HTTP fingerprints are assigned a greater weight than DHCP fingerprints. The AP tracks the weight of a client's fingerprint. If a client is identified with a fingerprint that has a greater weight than what was previously stored in the database, the new device identity and weight value are updated in the database.

The AP reports device identity changes to the controller and to the Cloud. This information is available to the user through the ExtremeWireless dashboard and through the controller reporting system. The client device type is included in all data streams where client parameters are included. For instance, this information is available to the ExtremeWireless Location Engine and to Extreme Management Center™.

Related Links

[Application Visibility and Device ID](#) on page 621

[Wireless Assistant Home Screen](#) on page 34

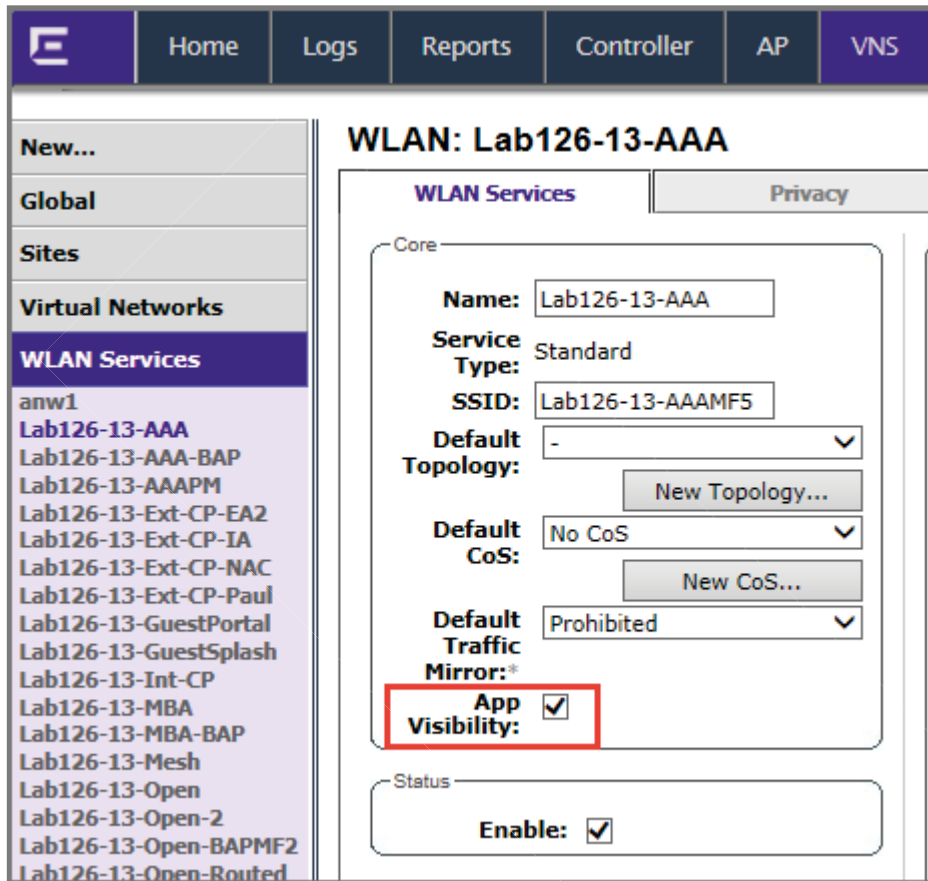
[Displaying Client Details](#) on page 643

Enabling Application Visibility with Device Identification

To view statistics on the applications and devices associated with a specific *WLAN* Service, configure the WLAN Service with Application Visibility enabled. You can enable visibility from the **WLAN Services** configuration screen or temporarily enable visibility from the **Home** screen dashboard.

To enable Application Visibility from the WLAN Service:

- 1 Go to **VNS > WLAN Services** and select a WLAN Service or click **New**.



The screenshot shows the 'WLAN Services' configuration page for 'Lab126-13-AAA'. The left sidebar lists various WLAN services, with 'Lab126-13-AAA' selected. The main panel has two tabs: 'WLAN Services' (active) and 'Privacy'. Under the 'WLAN Services' tab, there are two sections: 'Core' and 'Status'. In the 'Core' section, several fields are visible: 'Name' (Lab126-13-AAA), 'Service Type' (Standard), 'SSID' (Lab126-13-AAAMF5), 'Default Topology' (a dropdown menu), 'Default CoS' (No CoS), and 'Default Traffic Mirror' (Prohibited). The 'App Visibility' checkbox is checked and highlighted with a red box. In the 'Status' section, the 'Enable' checkbox is also checked.

Figure 201: Application Visibility Check box Option

- 2 Check the **App Visibility** option and click **Save**.



Note

You can enable Application Visibility from the Home dashboard for WLAN Services that do not have this configuration option enabled.

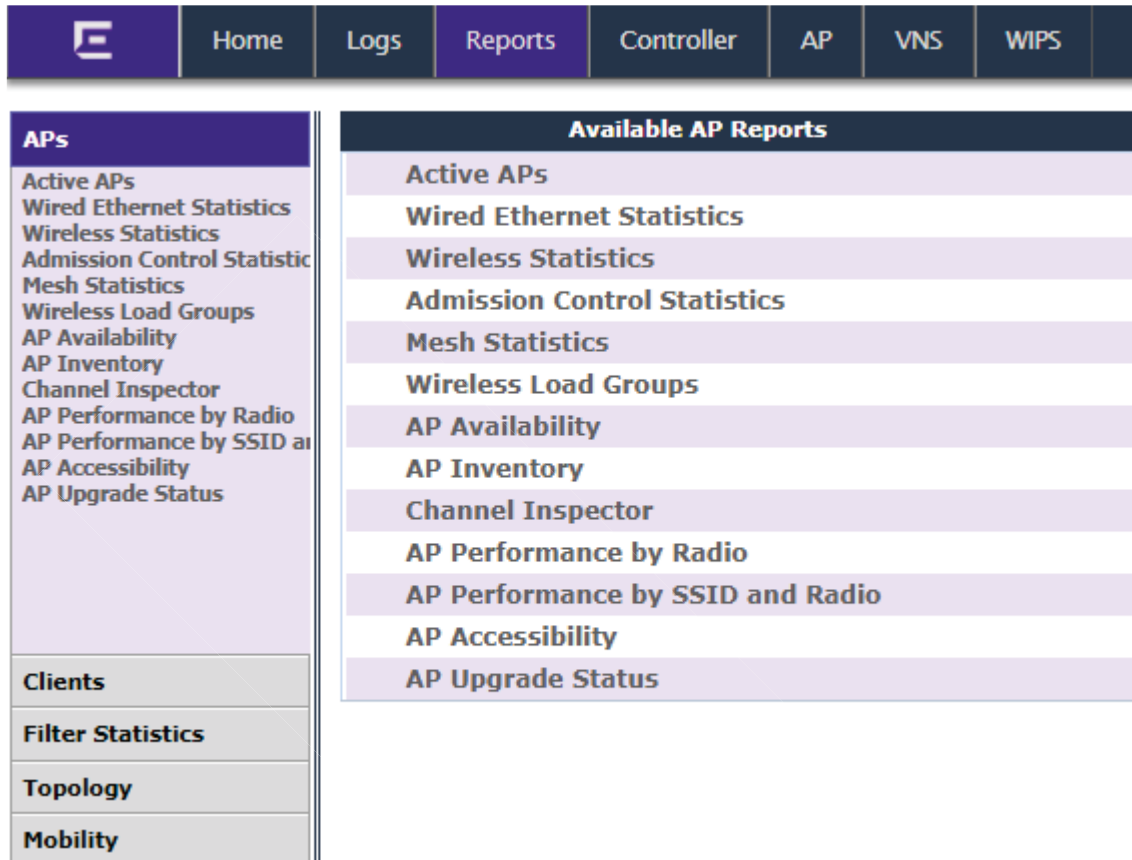
Related Links

- [Application Visibility](#) on page 623
- [Device Identification](#) on page 625
- [Wireless Assistant Home Screen](#) on page 34

Viewing AP Reports and Statistics

To view AP reports:

From the top menu, click **Reports**.



Viewing Statistics for APs

Several displays are snapshots of activity at that point in time on available APs:

- Active APs
- Wired Ethernet Statistics
- Wireless Statistics
- Admission Control Statistics
- Mesh Statistics
- Wireless Load Groups
- AP Availability
- AP Inventory
- Channel Inspector
- AP Performance by Radio
- AP Performance by SSID and Radio
- AP Accessibility
- AP Dashboard. See [AP Dashboard](#) on page 157



The statistics displayed are those defined in the 802.11 MIB, in the IEEE 802.11 standard.

Viewing Active Wireless APs

Statistics in the **Active Wireless APs** report are expressed in respect to the AP. For example, Packets Sent indicates the packets the AP has sent to a client and Packets Rec'd indicates the packets the AP has received from a client.

- 1 From the top menu, click **Reports**.
- 2 Click the **Active APs** display option. The **Active Wireless APs** display opens in a new browser window.

Lab-110 - Reports - Active Wireless APs

Wireless AP ▾	Serial ▾	AP IP ▾	Clients ▾	Home ▾	Role ▾	Mesh/WDS Children ³ ▾
AP3965i_1541D10030140001	1541D10030140001	10.47.13.102	0	Local	Guardian	0
AP3715i_12b2694650000000	12b2694650000000	10.47.13.103	0	Local	Traffic forwarder (AP)	0
Summary		2 active APs		0		

Sec. Tunnel ¹ ▾	Tunnel Duration ▾	Packets Sent ▾	Packets Rec'd ▾	Bytes Sent ▾	Bytes Rec'd ▾	Uptime ▾
N/A	7:15:24	11911	13891	2823438	2402789	7:15:54
N/A	7:17:09	9522	13520	1035947	2395276	7:17:54

Capture Timeout ▾	Invalid Role ▾	Radio 1			Radio 2			IoT ▾
		Mode ▾	Ch/Tx ▾	g PM ▾	Mode ▾	Ch/Tx ▾	g PM ▾	
off	0	a/n/ac	N/A/N/A	-	b/g/n	N/A/N/A	off	N/A
off	0	off	off	-	off	off	-	N/A

Figure 202: Active Wireless APs Report

Note

IoT column indicates the IoT status for an AP. Valid values are:



- Off. The iBeacon application is not running.
- iBeacon. The iBeacon application is running.
- N/A. IoT is not supported on this AP. Only AP models AP39xx support IoT.

Viewing Wired Ethernet Statistics:

- 1 From the top menu, click **Reports**. The **Available AP Reports** screen displays.
- 2 Click the **Wired Ethernet Statistics** display option. The **Wired Ethernet Statistics by Wireless APs** display opens in a new browser window.

cathohwc2 - Reports - Wired Ethernet Statistics by Wireless APs

APs refresh Refresh every 30 secs Apply

Status	Approved	IP Address	MAC Address	MTU Interface	MTU Tunnel
catho-ap16-3805e		194.141.121.226	D8:64:68:74:FF:7B	1500	1500
catho-ap20-3805e					
catho-ap21-3805e					
catho-ap22-3805e					
catho-ap23-3915e					
catho-ap24-3915e					
catho-ap25-3915e					
catho-ap26-3912e					
catho-ap27-3912e					
catho-ap28-3912e					
catho-ap29-3912e					

Up Link

Statistics	Sent	Received
Discarded Packets	0	2
Total Errors	0	0
Unicast Packets	8188150	12249776
Multicast Packets	363526	8189636
Broadcast Packets	38923	984902
Total Packets	8450899	21343908
Total Bytes	2657349764	12888645861

Client Ports

Statistics	p1		p2		p3	
	Sent	Received	Sent	Received	Sent	Received
Discarded Packets	0	0	0	0	0	0
Total Errors	0	0	0	0	0	0
Unicast Packets	0	0	0	0	0	0
Multicast Packets	0	0	0	0	0	0
Broadcast Packets	0	0	0	0	0	0
Total Packets	0	0	0	0	0	0
Total Bytes	0	0	0	0	0	0

Data as of Jan 25, 2017 03:02:08 pm

Refresh Export Close

- 3 In the left pane, click a registered AP to display its information.

Viewing Wireless Statistics:

- 1 From the top menu, click **Reports**.
- 2 Click the **Wireless Statistics** display option. The **Wireless Statistics by Wireless APs** display opens in a new browser window.

lab-422-g - Reports - Wireless Statistics by Wireless APs

No refresh Refresh every 30 secs Apply

AP Status	Approved	AP IP Address
C4110 - ap1 - AP4102		10.219.40.10
C4110 - ap2 - AP3620		

Radio1

MAC Address	00:11:88:38:47:80 00:11:88:38:47:81 00:11:88:38:47:82 00:11:88:38:47:83 00:11:88:38:47:84 00:11:88:38:47:85 00:11:88:38:47:86 00:11:88:38:47:87	Mode Channel Current Power Level Operational Max Rate	a 157 10 dBm 54 Mbps
SSID	CNL-422-1-7-ssid CNL-422-1-6-ssid CNL-422-1-5-ssid CNL-422-0-3-ssid CNL-422-0-2-ssid CNL-422-0-1-ssid CNL-422-0-0-ssid CNL-422-WDS-ssid		

Associated Clients There are no active clients on this radio.

Active Immediate WDS child APs 1

Statistics	Sent	Received
Discarded Packets	49	286
Errors	49	221413
Unicast Packets	1251293	290501
Multicast Packets	0	2038

Data as of Mar 03, 2014 10:55:24 am

Refresh Export Close

- 3 In the **Wireless Statistics by Wireless APs** display, click a registered AP to display its information.
- 4 Click the appropriate tab to display information for each Radio on the AP.

Viewing Admission Control Statistics by Wireless AP:

- 1 From the top menu, click **Reports**.
- 2 Click the **Admission Control Statistics** display option. The **Admission Control Statistics by Wireless AP** display opens in a new browser window.



- 3 In the **Admission Control Statistics by Wireless AP** display, click a registered AP to display its information:
- 4 The **Admission Control Statistics by Wireless AP** lists the TSPEC statistics associated with this AP:
 - **AC** — Access class where TSPEC is applied,
 - **Direction** — Inbound, Outbound or Bidirectional,
 - **MDR** — Mean Data Rate
 - **NMS** — Nominal Packet Size
 - **SBA** — Surplus Bandwidth (ratio)

The following statistics are of measured traffic:

- **Rate** — Rate in 30 second intervals (inbound and outbound)
- **Violation** — Number of bits in excess in the last 30 seconds (inbound and outbound)

Viewing Mesh VNS Wireless AP Statistics:

- 1 From the top menu, click **Reports**.

- From the Available AP Reports screen, click **Mesh Statistics**.

The **Mesh Statistics** display opens in a new browser window.

lab-422-g - Reports - Mesh Statistics ☒ No refresh ☐ Refresh every 30 secs

AP Name	SSID	Rx RSS	Hops	Rx/Tx Rate	Backhaul Channel	Parent Change	Rx Frames	Tx Frames	Rx/Tx Errors	Retry Percent
C4110 - ap1 - AP4102[MP]	N/A	N/A	0	N/A	N/A	N/A	N/A	N/A	N/A	N/A
C4110 - ap2 - AP3620	CNL-422-WDS-ssid	-52	1	54/54	157: (5785)	2	393988	223782	0/2	5

Data as of Mar 03, 2014 10:59:02 am

The Rx RSS value on the Mesh Statistics display represents the received signal strength (in dBm).

Viewing Load Balance Group Statistics

The **Active Wireless Load Groups** report lists all load groups, and for the selected load group, all active AP radios.

To view the active wireless load groups report:

- From the top menu, click **Reports**.
- Click the **Wireless Load Groups** report.

The **Active Wireless Load Groups** report opens in a new browser window. Reports display differently when reporting on client balance load groups and radio preference load groups.

CNL-208-C20-1

Members	4
Clients	0
Average Load	0.0

AP	Radio	Load	State	Probes Declined	Auth/Assoc Declined	Rebalance Event
0500008043050356	1	0	Under-Loaded	0	0	0
0500008043050356	2	0	Under-Loaded	0	0	0
10490056235A0000	1	0	Under-Loaded	0	0	0
10490056235A0000	2	0	Under-Loaded	0	0	0

Members: 4 Clients: 0 Average Load: 0.0

About Radio Preference/Load Control Statistics

The statistics reported for each radio preference load balance group are:

- Members** — The number of AP members

The statistics reported for each member of the load balance group are:

- **AP** — AP name
- **Band Preference**
 - **Status** —The operational status: enabled or disabled
 - **Probes Declined** —The number of probes declined
 - **Auth/Assoc Requests Declined** —The number of authentications or associations declined
- **Load Control**
 - **Radio 1**
 - Status** —The operational status: enabled or disable
 - Rejected** —The number of clients declined at the first association attempt
 - **Radio 2**
 - Status** —The operational status: enabled or disabled
 - Rejected** —The number of clients declined at the first association attempt
 - Returned** —The number of clients declined at the second association attempt

Load balance group statistics are reported on the foreign controller when APs fail over with load groups from a different controller indicated with an "(F)" following the load group name.

About Client Balancing Statistics Reports

lab-422-g - Reports - Active Wireless Load Groups

☒ No refresh
 ☐ Refresh every secs

CNL-208-C20-1

Members 4

Clients 0

Average Load 0.0

AP	Radio	Load	State	Probes Declined	Auth/Assoc Declined	Rebalance Event
0500008043050356	1	0	Under-Loaded	0	0	0
0500008043050356	2	0	Under-Loaded	0	0	0
10490056235A0000	1	0	Under-Loaded	0	0	0
10490056235A0000	2	0	Under-Loaded	0	0	0

Members: 4 Clients: 0 Average Load: 0.0

In a client balancing/load control statistics report, the statistics reported for each client balancing load balance group are:

- **Members** — Number of radio members
- **Clients** — Total number of clients for all radio members
- **Average Load** — Average load for the group

The reported average load may not be correct in a failover situation. If some APs in the load balance group fail over the foreign controller, those APs will report to the foreign controller. The member APs will continue to use the member count for the whole group, but the member count displayed on the controller will be for only those APs that are reporting. Since the member count reported on the

controller is not the complete set, the average will not be consistent with what the APs are using for the state determination.

The statistics reported for each member of the load balance group are:

- **AP** — AP name
- **Radio** — Radio number
- **Load** — Load value (number of clients currently associated with the AP)
- **State** — Load state
- **Probes Declined**
- **Auth/Assoc Requests Declined**
- **Rebalance Event** — Clients removed because of an over-loaded state

The report identifies SIAPP sub-groupings and provide separate group statistics for each sub-group.

When the load group includes sub-groups, **Average Load**, in red, is the average of the entire group. The average for each sub-group is also reported. The sub-group average is reported in red when group membership changes and not all members have been updated with the new member count.

Load balance group statistics are reported on the foreign controller when APs fail over with load groups from a different controller indicated with an "(F)" following the load group name.

Viewing Wireless AP Availability

In session availability, the **Wireless Availability** report displays the state of both the tunnels — active tunnel and backup tunnel — on both the primary and secondary wireless controllers.

The report uses a **Color Legend** to indicate the tunnel state:

- **Green** — AP has established an active tunnel.
- **Blue** — AP has established a backup tunnel.
- **Red** — AP is not connected.

In the report, each AP is represented by a box.

- The label, **Foreign** or **Local**, indicates whether the AP is local or foreign on the controller.
- The color in the upper pane of the box represents the state of the tunnel that is established to the current controller.



Note

The current controller is the one on which the AP Availability report is viewed.

- The color in the lower pane of the box represents the state of the tunnel that is established with the other controller.

For the ease of understanding, take the example of the following scenario:

- Controller1 and Controller2 are paired in session availability
- A Wireless AP has established an active tunnel to Controller1.
- The same AP has established a backup tunnel to Controller2.

If you open the Wireless AP Availability report on Controller2, the report will appear as follows:



In the above example, the circled AP has established a backup tunnel to the foreign (secondary) controller, and an active tunnel to the local (Primary) controller.

AP Inventory Reports

To view reports:

- 1 From the top menu, click **Reports**.
- 2 In the **Available AP Reports** list, click the report you want to view.



Note

All AP Inventory reports open in a new browser window.



Note

If you open only automatically refreshed reports, the Web management session timer will not be updated or reset. Your session will eventually time out.

The following is an example of the Wireless AP Inventory report:

Lab-110 - Reports - Wireless AP Inventory																																																																																																																																																																																				
Wireless AP (Serial)	Topology										SW		Country	Antenna	Power/LAN	Sec. Tunnel	Cert.	SW	LBS	Host Assembly	RD	Po																																																																																																																																																														
	Side	Address	Ra	Rb	Rg	Rn	DP	BP	BT	FT	Req Ch	Ch / Tx	Ai	TaPn	TaTrn	A/T	Zone	Model	Power																																																																																																																																																																	
	11n Channel Width										11n Guard Interval										11n Protection Mode																																																																																																																																																															
	Failure Maintn.										Assoc										IP Address																																																																																																																																																															
	IoT MAC										Mode										Network																																																																																																																																																															
										Gateway										MTU Interface																																																																																																																																																																
										Interval										MTU Tunnel																																																																																																																																																																
AP17131-1282694650000000 (1282694650000000) Role:Traffic Forwarder (AP)	Pwr_VLA0_110										Wireless AP3715 Internal										10.11.01.0030										Australia										LAN1:150Mbps LAN2:10Mbps										Power										50m										enabled										disabled										disabled																																																																																									
	40MHz										Short										None																																																																																																																																																															
	2										on																																																																																																																																																																									
	disabled										DHCP										10.47.13.103										255.255.255.0																				10.47.13.1										1500										1500																																																																																																													
AP19123-16371-1001100000 (16371-1001100000) Role:Traffic Forwarder (AP)											Wireless AP1913-40MHz Internal										10.11.01.0030										Australia										N/A																				Edu										enabled										disabled										disabled																																																																																									
	1										on																																																																																																																																																																									
	40MHz										Short										Auto																																																																																																																																																															
	2										on																																																																																																																																																																									
	disabled										DHCP										10.0.0.0										0.0.0.0										2.0.0.0										100																																																																																																																																	
10.10.10.1-4-FF-A8										off																																																																																																																																																																										
AP19123-16371-1001100000 (16371-1001100000) Role:Guardian	Pwr_VLA0_110										Wireless AP1913-40MHz Internal										10.11.01.0030										Australia										Low Pwr:5W Port1:1AP Port2:1N/A LAN1:1G/10A LAN2:N/A																				60m										enabled										disabled										disabled																																																																																									
	1										on										on										on										3										120										2348										2348										wds										N/A										6.00										18.00																				Hydrex										6 Mbps																																							
	40MHz										Short										Auto																																																																																																																																																															
	2										on										on										on										3										120										2348										2348										1+										N/A										6.00										18.00																				Hydrex										7 Mbps										Larg																													
	disabled										DHCP										10.47.13.101										255.255.255.0																				10.47.13.1										1500										1500																																																																																																													
Export																																																																																																																																																																																				

Table 129 lists the column names and abbreviations found in the AP Inventory report:

Table 129: AP Inventory Report Columns

Column Name	Description
Wireless AP (Serial)	Includes AP type, AP name, serial number, and role (including role type)
Topology	Ethernet port and associated IP address of the interface on the controller through which the AP communicates.
HW	Hardware version of the AP.
SW	Software version executing on the AP.
Country	Country in which the AP is deployed
Antennas	Antennas used
Power Status	Indicates ports on the AP39xx with low power status. Feature available for AP39xx only.
Sec. Tunnel	Secure tunnel mode
Cert.	AP certification (enabled or disabled)
SSH	SSH access (enabled or disabled)
LBS	Location-based service (enabled or disabled)
Mcast Assembly	Multicast Assembly (enabled or disabled)
BD	Broadcast disassociation (enabled or disabled).
Persistence	Enabled or disabled
P/To	Poll timeout. If polling is enabled, a numeric value.
P/I	Poll interval. If polling is enabled, a numeric value.
Wired MAC	The physical address of the AP's wired Ethernet interface.
Description	As defined on the AP Properties screen.
Rdo	Radios: 1 or 2.
Ra	802.11a radio. The data entry for an AP indicates whether the a radio is on or off.
Rb	802.11b protocol enabled. Possible values are on or off.
Rg	802.11g protocol enabled. Possible values are on or off.
Rn	802.11n protocol enabled. Possible values are on or off.
DP	DTIM period
BP	Beacon Period
RT	RTS Threshold
FT	Fragmentation Threshold
Req Ch	Last requested channel
Ch / Tx	Current channel Tx power level
Aj	Auto Tx Power Ctrl Adjust when ATPC is enabled
TxMn	Minimum Tx power, in decibels

Table 129: AP Inventory Report Columns (continued)

Column Name	Description
TxMx	Maximum Tx power, in decibels
ATT	Attenuation for APs that support professional antenna installation.
Dom	RF domain
MnBR	Minimum Basic Rate (For more information, see the Wireless AP radio configuration tabs.)
Pmb	Preamble (long, short)
PM	Protection Mode
PR	Protection Rate
PT	Protection Type
VNS Name: MAC	Also called BSSID, this is the MAC address of a (virtual) wireless interface on which the AP serves a BSS/VNS. There could be 8 per radio.
11n Channel Width	20MHz, 40MHz, or auto
11n Guard Interval	If 11n Channel Width is 40MHz, long or short
11n Channel Bonding	Enabled only if 11n Channel Width is 40MHz
11n Protection Mode	Protects high throughput transmissions on primary channels from non-11n APs and clients. Enabled or disabled.
Failure Maintn.	Maintain MU sessions on the Wireless AP when the AP loses the connection to the controller.
Assn	Assignment (address assignment method)
IP Address	Wireless AP's IP address if statically configured (same as the Static Values button on the AP Static Configuration screen).
Netmask	If the AP's IP address is configured statically, the net mask that is statically configured for the AP.
Gateway	If the AP's IP address is configured statically, the IP address of the gateway router that the AP will use.
MTU Interface	MTU Interface (enabled or disabled)
MTU Tunnel	MTU Tunnel value
TLS	802.1x EAP-TLS authentication configuration
PEAP	802.1x PEAP authentication configuration
EWC Search List	The list of IP addresses that the AP is configured to try to connect to in the event that the current connection to the controller is lost.
IoT MAC	MAC address of the IoT hardware.
Mode	Indicates the image type for the IoT hardware. Valid values are: Bluetooth or Thread. Bluetooth is the default.
Power	Indicates the received RSSI for the beacon application. Currently fixed. Valid values are: Min.-127dBm, Max. 127dBm, Default. -45dBm.
Interval	The advertising interval for the beacon application. Valid values are: Min (100ms) and Max (10240ms). The default value is Min (100ms).

Table 129: AP Inventory Report Columns (continued)

Column Name	Description
Major	Identifies <i>a subset of beacons</i> within the larger set. This value could represent a venue specific attribute, such as a specific store or wing in a building. Valid values are 0 to 65635.
Minor	Identifies <i>an individual beacon</i> . Used to more precisely pinpoint beacon location. This value complements the UUID and Major values to provide more granular identification of a specific location, such as a particular shelf, doorway, or item. Valid values are 0 to 65635.
Available for Export Only:	
UUID Beacon	Identifier used to differentiate a large group of related beacons. A company can have a network of beacons with the same UUID.
Location of AP XY	Map coordinates. Used in conjunction with a site map. (Top left corner of the map is considered 0,0.)

Channel Inspector Report

The Channel Inspector Report enhances Automatic Channel Selection (ACS) on the controller by providing an audit trail of selected channels and presenting a history of channel selection. The channel data generated from ACS populates the report, or you can initiate a channel scan on-demand from the user interface. The report is generated from the last channel scan. The date and time of the last channel scan appear on the report.

Related Links

[Viewing the Channel Inspector Report](#) on page 637

[Running Auto Channel Select \(ACS\)](#) on page 638

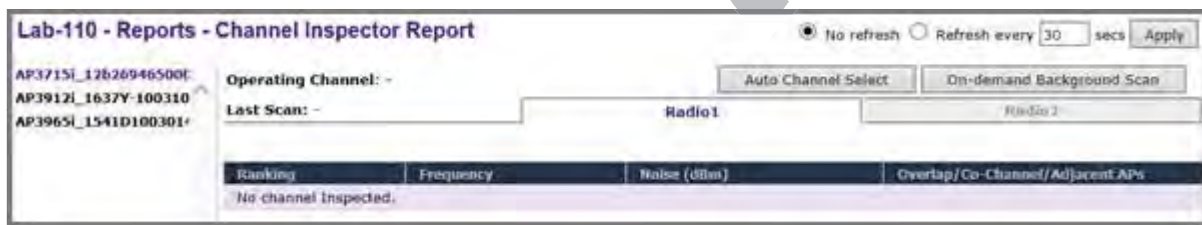
[Running a Background Scan](#) on page 638

[Channel Inspector Report Fields](#) on page 638

Viewing the Channel Inspector Report

To view the Channel Inspector Report:

- 1 From the top menu, click **Reports**.
- 2 Select **Channel Inspector**.



- 3 Select **Radio 1** tab or **Radio 2** tab to see details for the different radios.

Running Auto Channel Select (ACS)

ACS provides an easy way to optimize channel arrangement based on the current situation in the field. An optimal solution is provided only if ACS is triggered on all APs in a deployment, or all APs placed in a distinct area like a floor. ACS forces the channel width selection of the involved APs to Auto width. The ACS algorithm selects the optimal channel width for all the selected APs and places each AP on the best channel available in its area. Use the Channel Inspector Report to visualize why the AP was placed on the selected channel.

To initiate ACS from the Channel Inspector Report, click **Auto Channel Select**.

To verify channel assignment without making changes, see [Running a Background Scan](#) on page 638.

Related Links

[Channel Inspector Report Fields](#) on page 638

[Dynamic Radio Management \(DRM\)](#) on page 174

Running a Background Scan

Background scan extends the usefulness of the Automatic Channel Scan (ACS) feature. It is a reporting tool that helps you verify and understand channel assignments. Where ACS will disrupt service and result in a persistent channel assignment, the on-demand background scan runs without disrupting service. To verify channel assignments and review channel details without having to run a full ACS, run an on-demand background scan.

The background scan does not change channel assignments, it simply provides details about the current assignments. Run background scan on each radio separately. To change channel assignments, you must run ACS.

From the Channel Inspector Report, click **On-Demand Background Scan**.

Related Links

[Channel Inspector Report Fields](#) on page 638

Channel Inspector Report Fields

Table 130: Channel Inspector Report

Field	Description
Operating Channel	Indicates the operating channel of the AP. This is not necessarily the highest ranked channel. For best performance, you want the highest ranked channel to be the operating channel.
Last Scan	Date and time of the last background scan.
Refresh	Auto refresh ensures that the most recent scan data is presented. Enable or disable auto refresh at the top of the report. 30 seconds is the default auto refresh value. If auto refresh is disabled, click the Refresh button to manually refresh the display.
Auto Channel Select	Initiates Auto Channel Selection (ACS). ACS will disrupt service and result in a persistent channel assignment. Use this option to reassign the channels. The ACS scan will disrupt network activity.

Table 130: Channel Inspector Report (continued)

Field	Description
On-Demand Background Scan	The background scan does not change channel assignments, it simply provides details about the current assignments. Run background scan on each radio separately. To change channel assignments, you must run ACS.
Ranking	Indicates the best operating channel based on a 5-star ranking. This ranking is relative to the channels that are available.
Frequency	Radio Frequency channels with the beacon channel (primary) denoted with brackets. The following is an 80MHz channel example showing [5220] as the beacon channel. 44: (5180 5200 [5220] 5240).
Noise	Channel noise measured in Decibel-milliwatts (dBm).
Channel Details Interference Type	<p>Click the details link to display the following channel details: Describes the channel interference in relation to the operating channel. Possible values are:</p> <ul style="list-style-type: none"> • Co-Channel. All the APs on the same channel as the target AP are competing. Using Distributed Control Function (DCF) collisions are avoided because the APs know to avoid each other; however, the more traffic on the channel the greater the chance of collisions. Throughput slows but all packets get through. • Adjacent. APs on adjacent channels are close enough to interfere, but not close enough to know they are interfering. They do not have the benefit of DCF. • Overlapping. Applicable for 40MGz and 80MGz channels only. The 20MGz channel is designated as the primary and the other channels are designated as extension channels (secondary). If the primary channel of one AP is the same as the extension channel of another AP it is considered overlapping. Overlapping is the worst type of interference. <p>Example Notation, Co-Channel 20 44: (5220) indicates that there is co-channel interference on the beacon channel 5220.</p>
Frequency	Radio Frequency channels with the beacon channel (primary) denoted with brackets. The following is an 80MHz channel example showing [5220] as the beacon channel. 44: (5180 5200 [5220] 5240).
RSS	Received signal strength value.
BSSID	Basic Service Set Identifier. Identifies the AP.
SSID	Service Set Identifier. Identifies the network.
AP Name	Name of the AP provided at network setup.

AP Performance by Radio Report

- 1 From the top menu, click **Reports**.

- Click the **AP Performance by Radio** display option.

The AP Performance by Radio display opens in a new browser window.

lab13 - Reports - AP Performance Report by Radio to refresh Refresh every 30 sec Apply

Wireless AP	Radio Radio	Client Load (%)				RSSI (dBm)				SNR (dB)				Packet Retransmission (ppt)			
		Peak	Avg	Min	Max	Peak	Avg	Min	Max	Peak	Avg	Min	Max	Peak	Avg	Min	Max
AP3718_1230694650000003	w/n	0	0	0	0	0	0	-18	-3	0	94	78	92	0	0	0	0
AP3718_1230694650000002	w/g	0	0	0	0	0	0	-66	N/A	0	95	10	-5	0	0	0	0

Data as of Mar 16, 2015 16:08:32 am Refresh Export Close

AP Performance by SSID and Radio Report

- From the top menu, click **Reports**.

- 2 Click the **AP Performance by SSID and Radio** display option.

The AP Performance by SSID and Radio display opens in a new browser window.

LAB62 - Reports - AP Performance Report by SSID and Radio

No refresh Refresh every: 30 sec Apply

Wireless AP	Radio	SSID	# of Clients			Uplink Throughput						Download Throughput					
						Bytes Per Second			Packets Per Second			Bytes Per Second			Packets Per Second		
			Peak	Avg	Cur	Peak	Avg	Cur	Peak	Avg	Cur	Peak	Avg	Cur	Peak	Avg	Cur
Wireless AP	Radio	SSID	Peak	Avg	Cur	Peak	Avg	Cur	Peak	Avg	Cur	Peak	Avg	Cur	Peak	Avg	Cur
13210613085D0000	a	LAD6162	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13210613085D0000	a	ACTY	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13210613085D0000	b/g	LAD6162	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Data as of Mar 16, 2015 10:25:21 am

Refresh Export Close

AP Accessibility Report

- 1 From the top menu, click **Reports**. The Available AP Reports screen displays.

- Click the **AP Accessibility Report** display option.

The **AP Accessibility Report** display opens in a new browser window.

Wireless AP	Radio Type	Access Ring Rx				Non-access Ring Rx				Downstream/Upstream Ring Rx				Downstream/Upstream Ring Rx			
		Peak	Avg	Cur	Cur	Peak	Avg	Cur	Cur	Peak	Avg	Cur	Cur	Peak	Avg	Cur	Cur
AP3719_11b1b4485000000	802.11n	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3719_12b1b4485000000	802.11n	0	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Available Client Reports

ExtremeWireless offers reports to view data related to the network clients. View reports in any of the following ways:

- By AP — Displays a list of available APs in the left pane. Select an AP to view a list of connected clients.
- By VNS — Displays a list of configured VNS. Select a VNS to view a list of connected clients.

Each report displays the number of connected users, broken down into a count of active users, authenticated users, and non-authenticated users.

- All Active Clients — Displays a list of all active clients.

Related Links

[Viewing All Clients](#) on page 642

[Displaying Client Details](#) on page 643

[Client Search Facility](#) on page 645

[Viewing Client MAC and OUI](#) on page 646

Viewing All Clients

View a list of all clients and take action on one or more clients in the list. You can also export the list of clients to an XML file.

- 1 From the top menu, click **Reports > Clients > All Active Clients**.

C25-smoketest - Reports - Active Clients Report

Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Client IP	Device Type	AP	WLAN
<input type="checkbox"/>	10.219.110.26	Windows 8/ 8.1/ 10/ 2012	C25 - ap3 - AP3865e	CNL-220-0-3-ssid

Figure 203: All Active Client Report

- 2 Use the Search facility to find a specific client. For more information, see [Client Search Facility](#) on page 645.



Note

Clients supporting 802.11W Protected Management Frame (PMF) display a W in the client Protocol field.

- 3 To take action on one or more clients, select the check box for the client and click one of the action buttons:
 - **Add to Blacklist.** Add the selected wireless device's MAC address to a blacklist of wireless clients that will not be allowed to associate with the AP.
 - **Disassociate.** Cut the connection with a particular wireless device.
 - **Show OUI.** The Organizationally Unique Identifier (OUI) is a 24-bit number that uniquely identifies the client vendor or manufacturer.
 - **Export.** Export selected clients to an XML file. System prompts you to open or save the XML file.
- 4 To view client details, click the client row (not the check box). For more information, see [Displaying Client Details](#) on page 643.

Displaying Client Details

Display client details to determine client activity and usage of network resources. From the All Client report, you can display the following information for each client:

- IPv4 and IPv6 Addresses
- Host Name
- Operating System
- Device Type
- Top 5 Application Groups by Throughput (2-minute interval)
- Top 5 current Application Groups by Bytes, from session start.
- Throughput chart for an application group.
- Average TCP Round Trip Time.
- Average DNS Round Trip Time.

1 Go to **Reports > Clients**.

The All Clients report appears.

2 Click on a client row (not the check box).

The **Detailed Information** dialog for the client appears.

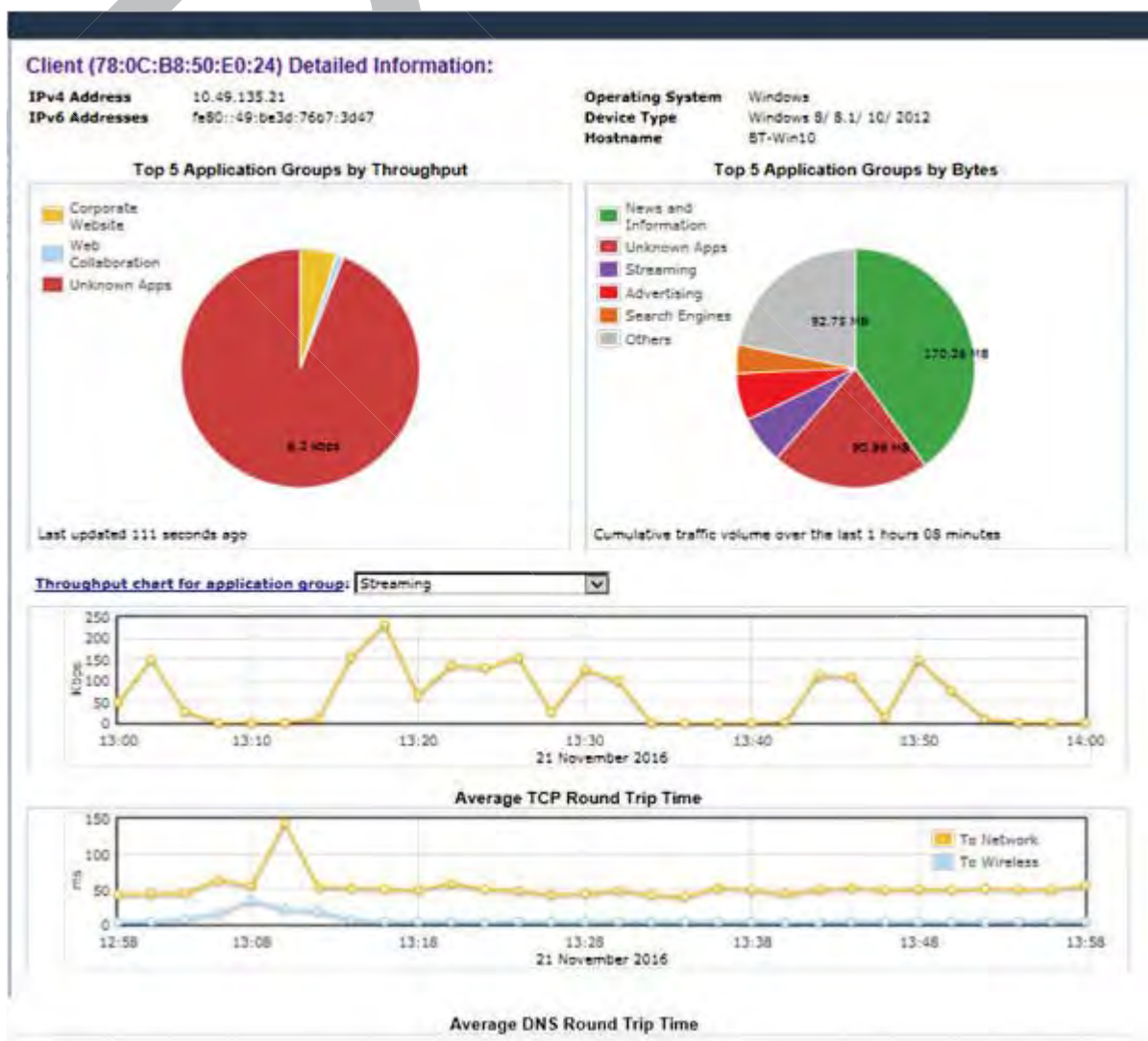


Figure 204: Client Detailed Information

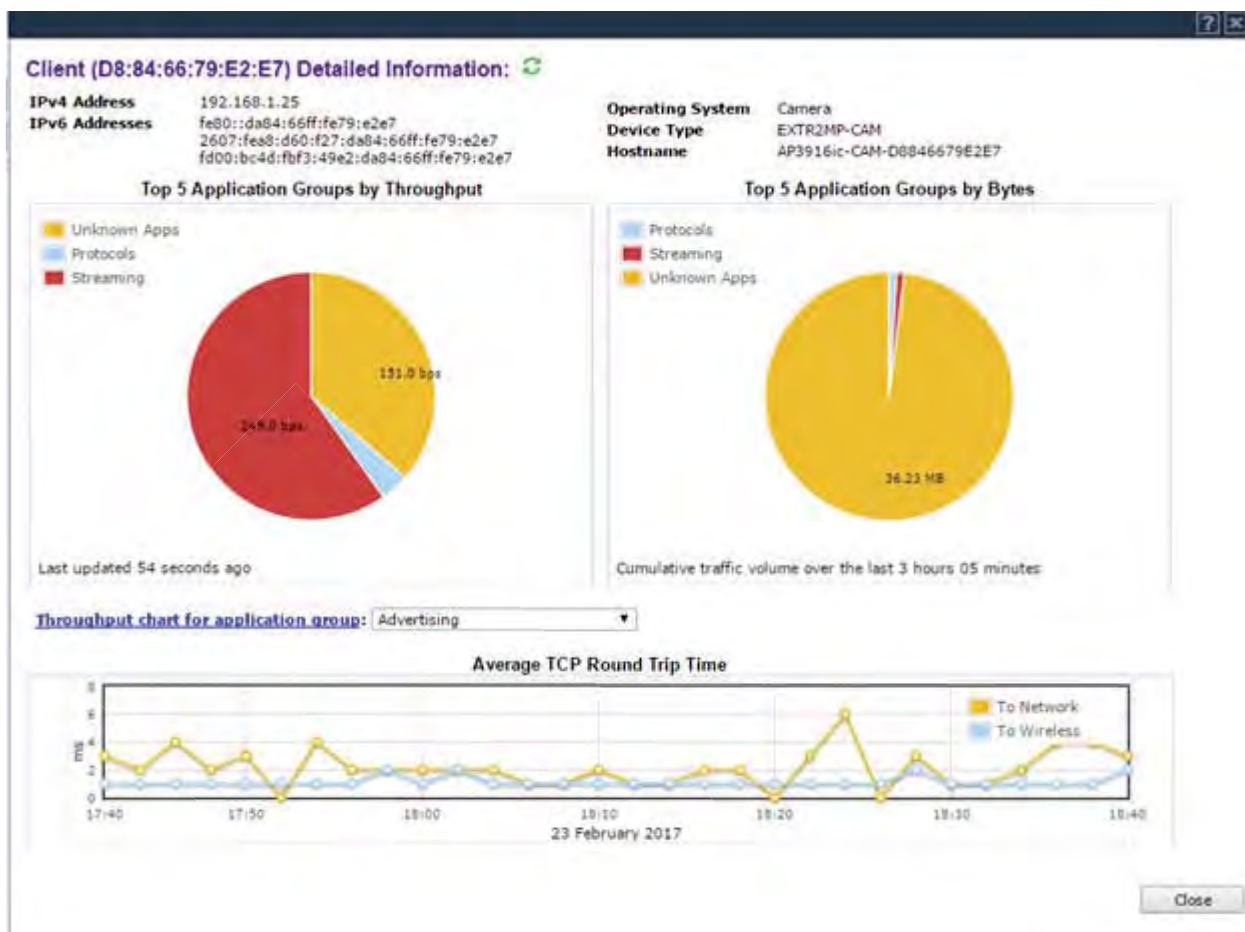


Figure 205: Camera as a Client

Related Links

[Application Visibility and Device ID](#) on page 621

[AP3916ic \(Integrated Camera\)](#) on page 104

Client Search Facility

On the **All Active Clients** report, search for any part of the client string.

When viewing the **Clients by AP** report or the **Clients by VNS** report, search the client report for a specific client by one of the following criteria:

- user name
- MAC Address
- IP Address
- OUI (Organizationally Unique Identifier)

Results:

- Clients that match the search criteria appear.
- Select one or more clients and apply actions to selected clients.

Viewing Client MAC and OUI

Take the following steps to view the MAC address and OUI for selected clients. The Organizationally Unique Identifier (OUI) is a 24-bit number that uniquely identifies the client vendor or manufacturer.

- 1 From the top menu, click **Reports > Clients**.
- 2 Select the check box next to a client row and click **Show OUI**.

The **Client MAC** and **OUI Full Name** for the selected client display.

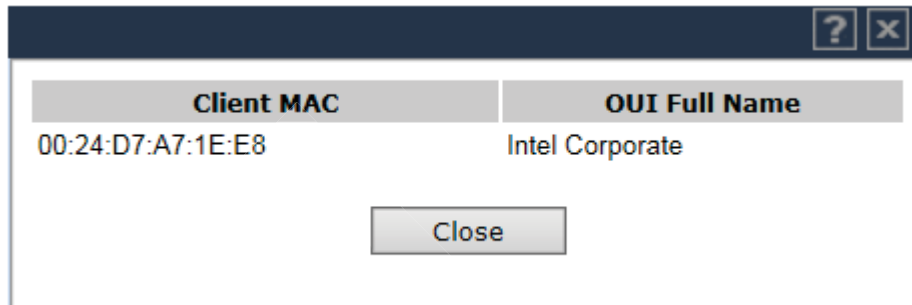
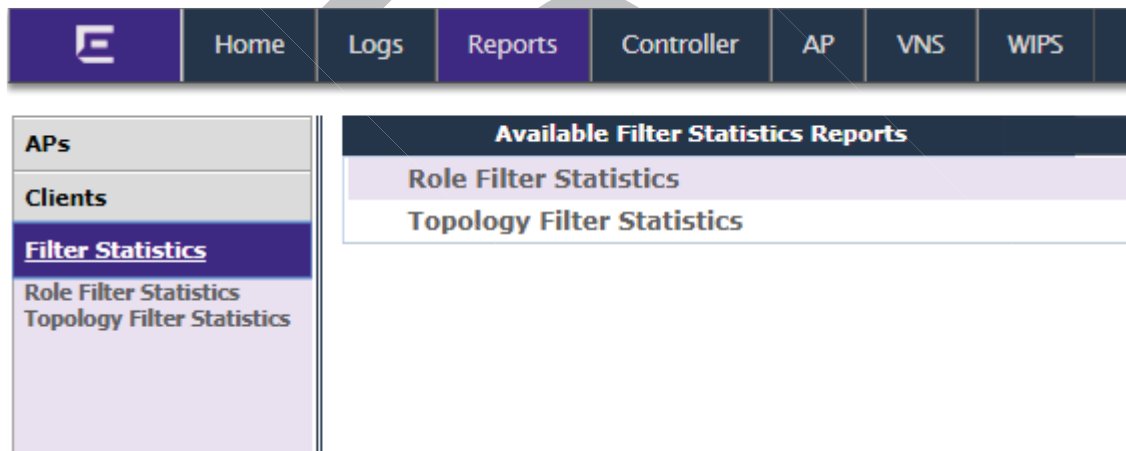


Figure 206: Show OUI dialog

Viewing Role Filter Statistics

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Filter Statistics**. The Available Filter Statistics Reports screen displays.



- 3 Under Available Filter Statistics Reports, click **Role Filter Statistics**. The **Role Filter Statistics** display opens in a new browser window.

lab-422-g - Reports - Role Filter Statistics ☒ No refresh ☐ Refresh every 30 secs

Role	Packets Allowed	Packets Denied
CNL-422-0-0-default	0	0
CNL-422-0-0-non-authenticated	0	0
CNL-422-0-1-default	0	0
CNL-422-0-1-non-authenticated	0	0
CNL-422-0-2-default	0	0
CNL-422-0-2-non-authenticated	0	0
CNL-422-0-3-default	0	0
CNL-422-1-2-wds-default	0	0
CNL-422-1-2-wds-non-authenticated	0	0
CNL-422-1-4-wds-default	0	0
CNL-422-1-5-default	0	0
CNL-422-1-5-non-authenticated	0	0
CNL-422-1-6-default	0	0
CNL-422-1-7-default	0	0
CNL-422-1-7-non-authenticated	0	0
CNL-422-2-10-default	0	0
CNL-422-2-11-default	0	0
CNL-422-2-11-non-authenticated	0	0
CNL-422-2-12-wds-default	17867	0
CNL-422-2-8-default	0	0
CNL-422-2-9-default	0	0
CNL-422-3-12-default	0	0
CNL-422-3-13-default	0	0
CNL-422-3-14-default	0	0
CNL-422-3-15-wds-default	0	0

Total Invalid Role Count: 3011515936

Data as of Mar 03, 2014 11:29:56 am

- Statistics are expressed in respect to the AP. Therefore, Packets Allowed indicates the packets the AP has received from a client and Packets Denied indicates the packets the AP has rejected.
- A client is displayed as soon as the client connects (or after a refresh of the screen). The client disappears as soon as it times out.

- 4 Under Available Filter Statistics Reports, click **Topology Filter Statistics**. The **Topology Filter Statistics** display opens in a new browser window.

lab-422-g - Reports - Topology Filter Statistics ☒ No refresh ☐ Refresh every 30 secs

Topology	Packets Allowed	Packets Denied
Port1	17831	0
Port2	3060	0
Port3	0	0
Port4	0	0
CNL-422-0-0	0	0
CNL-422-0-1	0	0
CNL-422-0-2	0	0
CNL-422-0-3	0	0
CNL-422-1-5	0	0
CNL-422-1-6	0	0
CNL-422-1-7	0	0
CNL-422-2-10	0	0
CNL-422-2-11	0	0
CNL-422-2-12-wds	2	2146
CNL-422-2-9	0	0
CNL-422-3-12	0	0
CNL-422-3-13	0	0
CNL-422-3-14	0	0
CNL-422-3-15-wds	0	0

Data as of Mar 03, 2014 11:31:36 am

- Statistics are expressed in respect to the AP. Therefore, Packets Allowed indicates the packets the AP has received from a client and Packets Denied indicates the packets the AP has rejected.
- A client is displayed as soon as the client connects (or after a refresh of the screen). The client disappears as soon as it times out.

Viewing Topology Reports

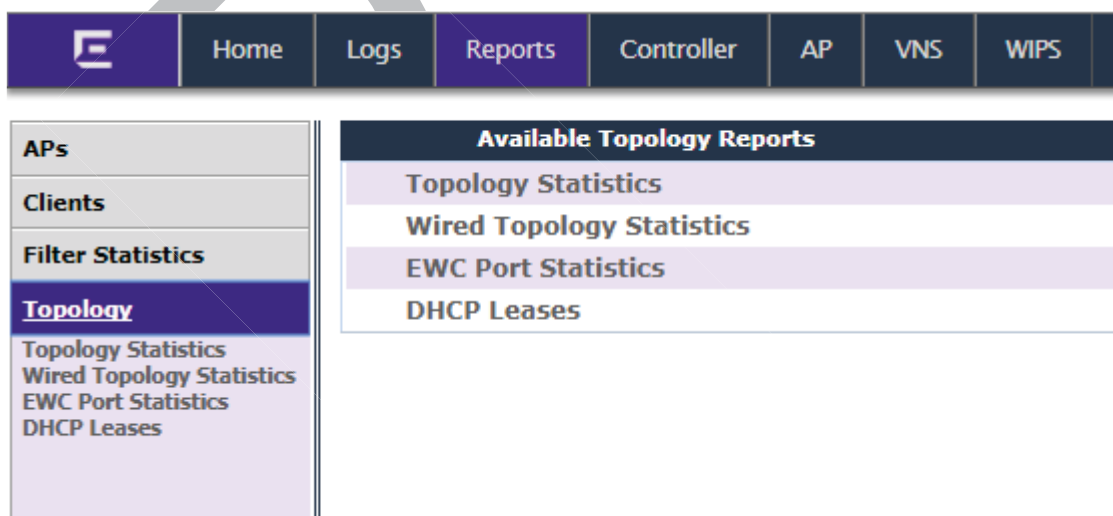
Topology Statistics — Displays statistics for total sent and received packets, octets, multicast packets, and broadcast packets.

Wired Topology Statistics — Displays statistics for each topology including total packets sent and received.

EWC Port Statistics — Displays port statistics for active Topologies including current status and totals for frames, octets, multicast frames and broadcast frames sent and received.

DHCP Leases — Displays statistics to help determine if you have sufficient *DHCP* addresses for your needs and whether the lease times are too long.

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Topology**. The **Available Topology Reports** screen displays.



- 3 Under Available Topology Reports, click **Topology Statistics**. The **Topology Statistics** display opens in a new browser window.

lab-422-g - Reports - Topology Statistics

☒ No refresh ☐ Refresh every 30 secs

Topology	Packets		Octets		Multicast Packets		Broadcast Packets	
	Sent	Received	Sent	Received	Sent	Received	Sent	Received
Port1	71684	77969	13818710	14510451	2787	9014	3104	3104
Port2	6447	8542	2901376	3062392	158	2276	3096	3096
Port3	1	0	60	0	0	0	0	0
Port4	0	0	0	0	0	0	0	0
CHL-422-0-0	0	0	0	0	0	0	0	0
CHL-422-0-1	0	0	0	0	0	0	0	0
CHL-422-0-2	202	2298	9924	171000	158	2276	0	0
CHL-422-0-3	0	0	0	0	0	0	0	0
CHL-422-1-5	0	0	0	0	0	0	0	0
CHL-422-1-6	0	0	0	0	0	0	0	0
CHL-422-1-7	0	0	0	0	0	0	0	0
CHL-422-2-9	0	0	0	0	0	0	0	0
CHL-422-2-10	200	2297	9804	170940	158	2276	0	0
CHL-422-2-11	0	0	0	0	0	0	0	0
CHL-422-2-12-rds	14179	21550	1211132	2620320	0	6116	4337	2169
CHL-422-3-12	0	0	0	0	0	0	0	0
CHL-422-3-13	0	0	0	0	0	0	0	0
CHL-422-3-14	0	0	0	0	0	0	0	0
CHL-422-3-15-rds	0	0	0	0	0	0	0	0

Data as of Mar 03, 2014 11:35:17 am

- 4 Under Available Topology Reports, click **Wired Topology Statistics**. The **Wired Topology Statistics** display opens in a new browser window.

EWC - Reports - Wired Topology Statistics No refresh Refresh every 30 secs Apply

Topology	Group	Total Packets		Octets		Multicast Packets		Broadcast Packets	
		Sent	Received	Sent	Received	Sent	Received	Sent	Received
physical 1	Ro	6854	6856	4042708	4042908	2	2	6852	6852

Data as of May 22, 2015 09:13:18 am Refresh Export Close

- 5 Under Available Topology Reports, click **EWC Port Statistics**. The **Port Statistics** display opens in a new browser window.

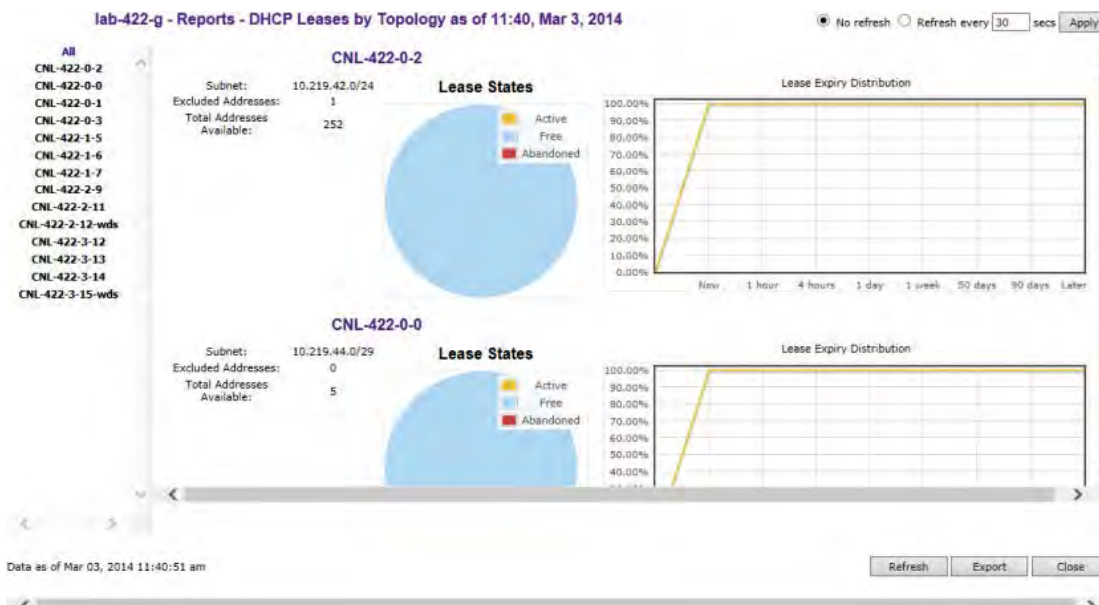
lab-422-g - Reports - Wireless Controller Port Statistics No refresh Refresh every 30 secs Apply

Port Statistic	Port1	Port2	Port3	Port4	lag1	lag2
Current Status	UP	UP	DOWN	DOWN	DOWN	DOWN
Frames Sent	32404	3666	0	0	0	0
Frames Received	57525	111983	0	0	0	0
Octets Sent	5162655	1881552	0	0	0	0
Octets Received	11167393	15755957	0	0	0	0
Multicast Frames Sent	2814	480	0	0	0	0
Multicast Frames Received	17663	48625	0	0	0	0
Broadcast Frames Sent	3123	3120	0	0	0	0
Broadcast Frames Received	99	59736	0	0	0	0

Data as of Mar 03, 2014 11:38:06 am Refresh Export Close

- Statistics are expressed in respect to the AP. Therefore, **Frames Sent** indicates packets sent to the AP from a client and **Frames Received** indicates the packets received from the AP.

- 6 Under Available Topology Reports, click **DHCP Leases**. The DHCP Leases display opens in a new browser window.



The report applies only to the DHCP server hosted on the local controller. The report is empty if DHCP is not enabled on any of the controller's topologies. Otherwise, for each of the controller's topologies the report provides a summary table of the address range, number of excluded address and total addresses available, a pie chart showing the proportion of addresses that are free, in use or abandoned, and a graph that shows how many leases will become available at different times assuming that no more leases are handed out by the server from this instant.

Abandoned leases should rarely be seen. The presence of one or more abandoned leases indicates that another DHCP server may be operating on the same subnet, resulting in IP address conflicts. The server abandons the use of any address it thinks is being managed by another DHCP server.

The lease expiry graph indicates the proportion of available leases that will be available now, 1, 4 hours, 1 day, 1 week 50 and 90 days from now assuming that the server never hands out another lease. If the network serves a relatively small number of users, who are in fact the same users day in and day out, then you should use longer lease times, meaning that this graph should not show 100% address availability until farther to the right in the graph. If you have a high turn over of users (like in a university classroom that has a different set of people every 1 hour) then you should use shorter lease times (achieve 100% availability more towards the left in the graph). If you find that you are running out of addresses, you should use the line graph to decide if you can afford to shorten lease times to make leases available sooner as opposed to creating a new, bigger subnet to handle more users concurrently.

Viewing Mobility Reports

The Mobility Domain is a virtual combination of Wireless LAN Controllers (WLCs) grouped for the purpose of roaming. The controller group consists of a Mobility Manager, Mobility agents, and a Backup Mobility Manager. The Mobility Domain preserves information about user sessions, allowing users to roam through the use of identity-based networking. A Mobility Domain can also provide network flexibility and scalability.

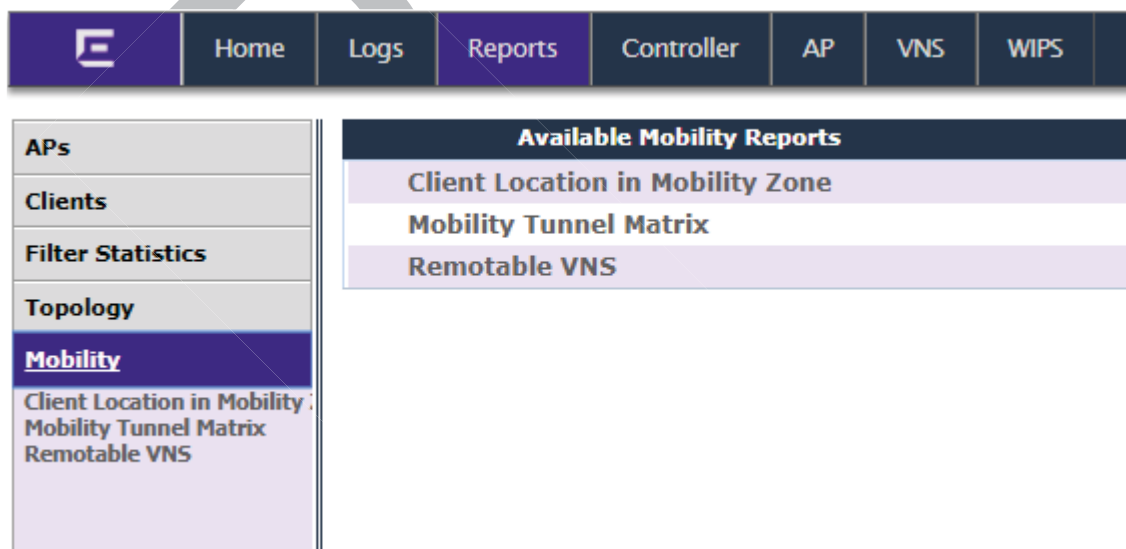
When a controller has been configured as a mobility manager, additional displays appear as options in the left pane:

- **Primary Manager Mobility Tunnel Matrix** — Displays a cross-connection view of the state of inter-controller tunnels, as well as relative loading for user distribution across the mobility domain.
- **Client Location in Mobility Zone** — Displays the active wireless clients and their status.
- **Backup Manager Mobility Tunnel Matrix** — Displays a cross-connection view of the state of inter-controller tunnels, as well as relative loading for user distribution across the mobility domain.
- **Remotable VNS** — Displays the active wireless clients and their status.



Note

There are four possible reports available from the **Available Mobility Reports** page depending on the configuration of the controller. If the controller does not have mobility enabled, it will just include the **Remotable VNS** report.



To view Mobility Manager reports:

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Mobility**.
- 3 Click the appropriate mobility manager report:
 - Client Location in Mobility Zone
 - Backup Manager Mobility Tunnel Matrix
 - Remotable VNS
 - Primary Manager Mobility Tunnel Matrix

The colored status indicates the following:

- **Green** — The mobility manager is in communication with an agent and the data tunnel has been successfully established.
- **Yellow** — The mobility manager is in communication with an agent but the data tunnel is not yet successfully established.
- **Red** — The mobility manager is not in communication with an agent and there is no data tunnel.

Client Location in Mobility Zone

This report displays the active wireless clients and their status.

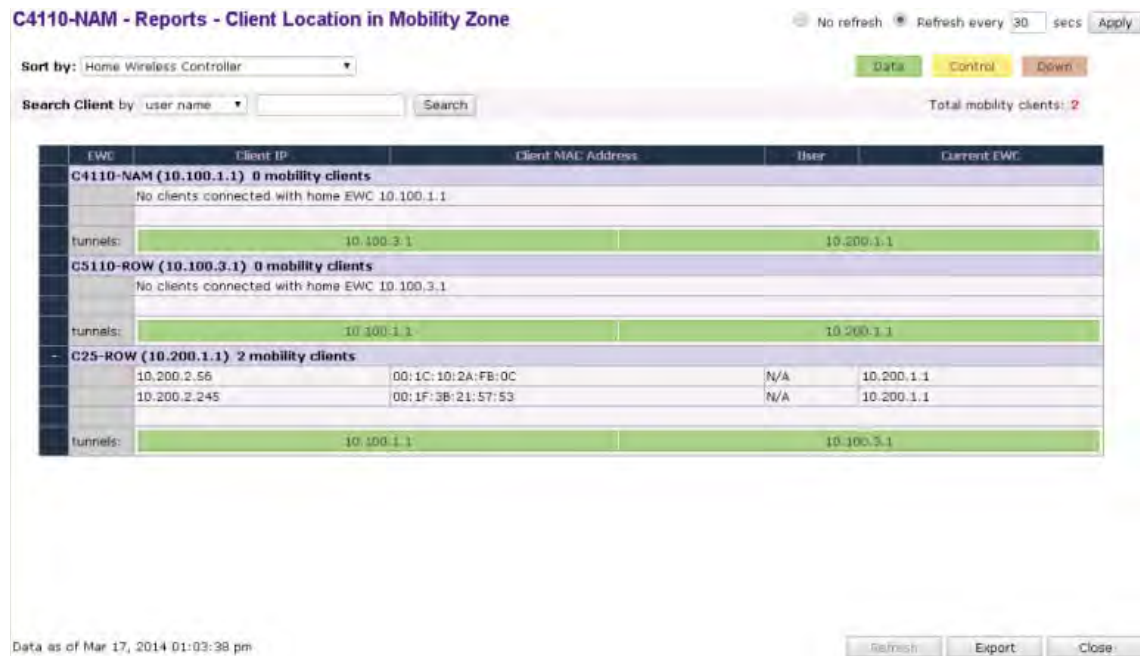


Figure 207: Client Location in Mobility Zone Report

You can do the following:

- Sort this display by home or foreign controller.
- Search for a client by MAC address, user name, or IP address, and typing the search criteria in the box.
- Define the refresh rates for this display.
- Export this information as a .xml file.

Primary/Backup Manager Mobility Tunnel Matrix

This report displays a cross-connection view of the state of inter-controller tunnels, as well as relative loading for user distribution across the mobility domain.

The following report illustrates a mobility setup with three controllers:

- Mobility Manager (M) (10.105.0.5)
- Mobility Agent/Backup Manager (BM) 10.105.0.9
- Mobility Agent (10.105.0.7)

In the following illustration, there is one client on the Primary Manager (M) and 0 clients on the other controllers. As the client moves through the Mobility group, the number of clients will change from 0 to 1 depending on which tunnel the client moves through. This report graphically displays the number of data tunnels, number of active mobility clients, and the number of clients on each controller.

Downed tunnels are represented in brown. **No tunnels: 0** indicates that all tunnels are up.



Figure 208: Primary/Backup Manager Mobility Tunnel Matrix

This report provides the following information:

- Provides connectivity matrix of mobility state.
- Provides a view of:
 - Tunnel state
 - If a tunnel between controllers is reported down, it is highlighted in red.
 - If only a control tunnel is present, it is highlighted in yellow.
 - If data and control tunnels are fully established, it is highlighted in green.
 - Tunnel Uptime
 - Number of clients roamed (Mobility loading)
 - Local controller loading
 - Mobility membership list

A controller is only removed from the mobility matrix if an administrator explicitly removes it from the by Mobility permission list. If there is a link between controllers, or the controller is down, the corresponding matrix connections are identified in red to identify the link.

The Active Clients by VNS report for the controller on which the user is home (home controller) will display the known user characteristics (IP, statistics, etc.). On the foreign controller, the Clients by VNS report does not show users that have roamed from other controllers, since the users remain associated with the home controller's VNS.

The Active Clients by AP report on each controller will show both the loading of local and foreign users (users roamed from other controllers) that are taking resources on the AP.



Note

Although you can set the screen refresh period less than 30 seconds, the screen will not be refreshed quicker than 30 seconds. The screen will be refreshed according to the value you set only if you set the value above 30 seconds.

Remotable VNS

This report displays the active wireless clients and their status.

SSID ▲	Privacy ▼	Home Controller ▼
CNL1050-1S-4wep	None	44
CNL1050-1S-4wep	None	4-C25

Data as of Oct 28, 2015 12:53:29 pm

Refresh Export Close

Figure 209: Remotable VNS Report

You can do the following:

- Sort this display by home or foreign controller.
- Search for a client by MAC address, user name, or IP address, and typing the search criteria in the box.
- Define the refresh rates for this display.
- Export this information as an xml file.

Viewing Controller Status Information

External Connection Statistics— Displays connection information including security level.

System Information — Displays system information including memory usage and CPU and board temperatures.

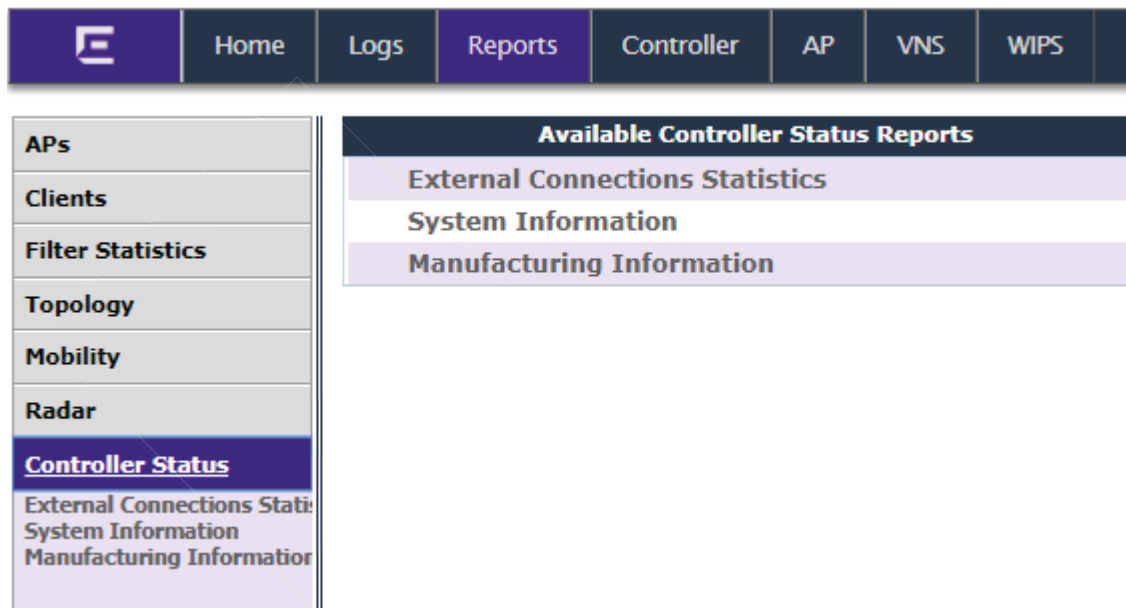
Manufacturing Information — Displays manufacturing information including the card serial number and CPU type and frequency.

Viewing External Connection Statistics

To view external connection statistics:

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Controller Status**.

The **Available Controller Status Reports** screen displays.



- 3 Click the **External Connection Statistics** option.

The **External Connection Statistics** display opens in a new browser window.



Viewing System Information

To view system information:

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Controller Status**.
The **Available Controller Status Reports** screen displays.
- 3 Click the **System Information** display option.

The **System Information** display opens in a new browser window.

lab-422-g - Reports - System Information ☒ No refresh ☐ Refresh every 30 secs

System Information

System Up Time: 5:45

- CPU Utilization: 7.60
- Memory Usage:
 - Free: 80 %
- Disk Usage (1 Kbyte blocks)

Partition	Total Space	Used	Available	Use %
root	27193624	430032	26944520	2%
tmp	131072	356	130716	1%
home	2040016	32840	1986636	2%
cdx	2032048	32824	1978744	2%
logs	1528032	32816	1479376	3%
reports	1522032	32812	1478880	3%
trace	1531008	32812	1492866	3%
- System Temperature
 - Processor 1 Temperature: -61 C degrees below meltdown
 - Power Supply 1 Temperature: 33 C
 - Power Supply 2 Temperature: 34 C
 - Memory Module 1 Temperature: 29 C
 - System Board 1 Ambient Temperature: 22 C
 - System Board 1 Planar Temperature: 31 C
- Fan Speed
 - 1A Fan: 5640 RPM
 - 1B Fan: 3960 RPM
 - 2A Fan: 5640 RPM
 - 2B Fan: 3960 RPM
 - 3A Fan: 4920 RPM
 - 3B Fan: 3480 RPM
 - 4A Fan: 4320 RPM
 - 4B Fan: 3480 RPM
 - 5A Fan: 5040 RPM
 - 5B Fan: 3480 RPM
- Port1 Interface:
 - Auto-negotiation: enabled
 - Auto-negotiation capability includes: any speed and any duplex
 - Interface State: up, 1000Mbps full duplex
- Port2 Interface:
 - Auto-negotiation: enabled
 - Auto-negotiation capability includes: any speed and any duplex
 - Interface State: up, 1000Mbps full duplex
- Port3 Interface:
 - Auto-negotiation: enabled
 - Auto-negotiation capability includes: any speed and any duplex
 - Interface State: down
- Port4 Interface:
 - Auto-negotiation: enabled
 - Auto-negotiation capability includes: any speed and any duplex
 - Interface State: down

Date as of Mar 03, 2014 11:51:10 am

Viewing Manufacturing Information

To view manufacturing information:

- 1 From the top menu, click **Reports**.

- 2 In the left pane, click **Controller Status**.
The **Available Controller Status Reports** screen displays.
- 3 Click the **Manufacturing Information** display option.
The **Manufacturing Information** display opens in a new browser window.

WLC - Reports - Manufacturing Information

Manufacturing Information

```

Manufacturing ID (Serial Number): B4858436
BIOS Version: V12.01.03
Hardware Revision: ES003
Software Version: 08.31.01.1022D
Model: WLC711
CPU Type: Intel(R) Core(TM)2 Duo CPU      U9300  @ 1.20GHz
CPU Frequency (MHz): 1197.129
HW Encryption Support: No
LAN    MAC address: 00:0E:8C:EB:CD:CD
ADMIN  MAC address: 00:0E:8C:EB:CD:BA

```

Viewing Routing Protocol Reports

The following reports are available in the Extreme Networks ExtremeWireless system:

- **Forwarding Table** — Displays the defined routes, whether static or *OSPF (Open Shortest Path First)*, and their current status.
- **OSPF Neighbor** — Displays the current neighbors for OSPF (routers that have interfaces to a common network).
- **OSPF Linkstate** — Displays the Link State Advertisements (LSAs) received by the currently running OSPF process. The LSAs describe the local state of a router or network, including the state of the router's interfaces and adjacencies.

Viewing Forwarding Table

To view the forwarding table:

- 1 From the top menu, click **Reports**.

- 2 In the left pane, click **Routing Protocols**.

The Available Routing Protocols Reports screen displays.

- 3 Click the **Forwarding Table** option.

The Forwarding Table displays in a new browser window.

lab-422-g - Reports - Forwarding Table

☒ No refresh ☐ Refresh every 30 secs

Route #	Destination	Netmask	Gateway	Interface	Type	Status
1	0.0.0.0	0.0.0.0	10.219.40.2	Port1	OSPF	Active
2	0.0.0.0	0.0.0.0	10.219.40.2	Port1	Static	Inactive
3	10.1.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
4	10.2.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
5	10.3.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
6	10.4.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
7	10.5.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
8	10.6.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
9	10.7.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
10	10.8.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
11	10.9.0.0	255.255.0.0	10.219.40.2	Port1	OSPF	Active
12	10.10.10.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
13	10.11.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
14	10.12.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
15	10.13.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
16	10.14.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
17	10.15.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
18	10.16.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
19	10.17.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
20	10.18.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
21	10.19.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active

Data as of Feb 26, 2014 10:56:12 am



Note

If you open only automatically refreshed reports, the Web management session timer will not be updated or reset. Your session will eventually time out.

Viewing OSPF Neighbor Table

To view the OSPF neighbor table:

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Routing Protocols**.
- 3 Click the **OSPF Neighbor** option.

The **OSPF Neighbor** displays in a new browser window.

lab-422-g - Reports - OSPF Neighbor ☒ No refresh ☐ Refresh every secs

Neighbor Router ID	Router Priority	State	IP Address	Interface Name
192.168.14.1	1	Full/DR	10.219.40.2	Port1:10.219.40.1

Data as of Mar 03, 2014 11:56:12 am

Viewing OSPF Linkstate Table

To view the OSPF Linkstate table:

- 1 From the top menu, click **Reports**.
The **Available AP Reports** screen displays.
- 2 In the left pane, click **Routing Protocols**.

- Click the **OSPF Linkstate** option.

The OSPF Linkstate displays in a new browser window.

lab-422-g - Reports - Forwarding Table

☒ No refresh ☐ Refresh every secs

Router LSA (Type 1)

Link ID	Advertising Router	Age	Sequence Number	checksum	Link Count
192.168.3.92	192.168.3.92	331	0x800010c7	0x6efc	2
192.168.3.110	192.168.3.110	5	0x80000016	0x8ec9	14
192.168.3.116	192.168.3.116	64	0x800019d1	0x7f4d	6
192.168.3.182	192.168.3.182	1570	0x80007cdd	0x29d9	4
192.168.3.200	192.168.3.200	405	0x80001e1d	0x16be	4
192.168.3.219	192.168.3.219	1192	0x800000b7	0x4ca2	6
192.168.3.225	192.168.3.225	6	0x80000094	0xb7f9	4
192.168.14.1	192.168.14.1	38	0x80008747	0xc868	176
192.168.14.4	192.168.14.4	1747	0x80000096	0xb890	4
192.168.14.11	192.168.14.11	119	0x80000016	0x2112	14
192.168.14.15	192.168.14.15	282	0x80000015	0x78f3	14
192.168.14.16	192.168.14.16	118	0x8000000c	0x8049	14
192.168.14.47	192.168.14.47	1462	0x8000039d	0x3770	2
192.168.14.48	192.168.14.48	570	0x8000021a	0xed2a	2
192.168.14.49	192.168.14.49	310	0x80000007	0xc960	3
192.168.14.50	192.168.14.50	61	0x800001e1	0x5b22	3
192.168.14.181	192.168.14.181	780	0x80000098	0x6184	4
192.168.14.182	192.168.14.182	1549	0x800000d0	0x1c10	3

Network LSA (Type 2)

Link ID	Advertising Router	Age	Sequence Number	checksum
10.11.0.2	192.168.14.1	351	0x80001dfe	0xf40c
10.12.0.2	192.168.14.1	351	0x80001dfe	0xe817
10.51.0.2	192.168.14.1	771	0x800001dc	0xfea3
10.52.0.2	192.168.14.1	291	0x80000004	0x99e2

Data as of Mar 03, 2014 12:07:22 pm

Saving Report In XML

To export and save a report in xml:

- On the report screen, click **Export**.
A Windows **File Download** dialog is displayed.
- Click **Save**. A Windows **Save As** dialog is displayed.



Note

If your default XML viewer is Internet Explorer or Netscape, clicking Open will open the exported data to your display screen. You must right-click to go back to the export display. The XML data file will not be saved to your local drive.

- Browse to the location where you want to save the exported XML data file, and in the **File name** box enter an appropriate name for the file.
- Click **Save**.
The XML data file is saved in the specified location.

Viewing RADIUS Reports

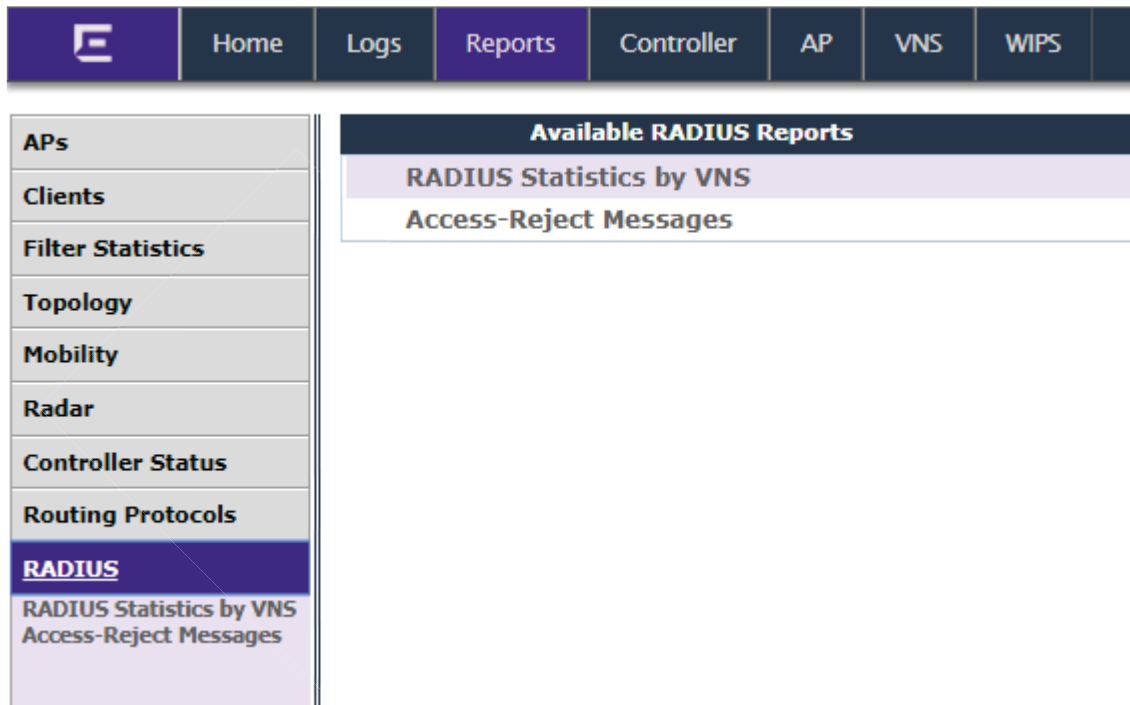
The following RADIUS reports are available in the Extreme Networks ExtremeWireless system:

- RADIUS Statistics by VNS** — Displays a list of VNS along with the number of Requests and their status (Failed or Rejected).

- **Access-Reject Reply-Message** — Displays the current list of messages along with an active count of all messages.

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **RADIUS**.

The Available RADIUS Reports screen displays.



- 3 Click **RADIUS Statistics by VNS** option.

The report displays in a new browser window.

lab-422-g - Reports - RADIUS Statistics by VNS ☒ No refresh ☐ Refresh every 30 secs

VNS	Requests	Failed	Rejected
CNL-422-0-0	0	0	0
CNL-422-0-1	0	0	0
CNL-422-0-2	0	0	0
CNL-422-0-3	0	0	0
CNL-422-1-2-wds	0	0	0
CNL-422-1-4-wds	0	0	0
CNL-422-1-5	0	0	0
CNL-422-1-6	0	0	0
CNL-422-1-7	0	0	0
CNL-422-2-10	0	0	0
CNL-422-2-11	0	0	0
CNL-422-2-12-wds	25	0	0
CNL-422-2-8	0	0	0
CNL-422-2-9	0	0	0
CNL-422-3-12	0	0	0
CNL-422-3-13	0	0	0
CNL-422-3-14	0	0	0
CNL-422-3-15-wds	0	0	0
CNL-422-WDS	0	0	0

Data as of Mar 03, 2014 11:36:58 am

- 4 To view the Access-Reject Messages, in the left pane, click **Access-Reject Messages** option.

lab13 - Reports - Access-Reject Messages ☒ No refresh ☐ Refresh every 30 secs

Access-Reject Reply-Message	Count
Controller - No Response from RADIUS Server.	4
Controller - No RADIUS Server Available.	1

Data as of Feb 27, 2015 03:28:05 pm

- 5 Click **Save**. A **Save As** dialog is displayed.

Call Detail Records (CDRs)

You can configure the wireless controller to generate Call Detail Records (CDRs), which contain usage information about each wireless session per VNS. For more information on how to configure the controller to generate CDRs, refer to [Defining Accounting Methods for a WLAN Service](#) on page 336.

CDRs are located in a CDR directory on the controller. To access the CDR file, you must first back up the file on the local drive, and then upload it to a remote server. After the CDR file is uploaded to a remote server, you can work with the file to view CDRs or import the records to a reporting tool.

You can back up and upload the file on the remote server either via the Wireless Assistant (GUI) or CLI.

CDR File Naming Convention

CDRs are written to a file on the controller. The filename is based on the creation time of the CDR file with the following format: YYYYMMDDhhmmss.<ext>

- **YYYY** — Four digit year
- **MM** — Two digit month, padded with a leading zero if the month number is less than 10
- **DD** — Two digit day of the month, padded with a leading zero if the day number is less than 10
- **hh** — Two digit hour, padded with a leading zero if the hour number is less than 10
- **mm** — Two digit minute, padded with a leading zero if the minute number is less than 10
- **ss** — Two digit second, padded with a leading zero if the second number is less than 10
- **<ext>** — File extension, either .work or .dat

CDR File Types

Two types of CDR files exist in the CDR directory on the controller:

- **.work** — The active file that is being updated by the accounting system. The file is closed and renamed with the **.dat** extension when it attains its maximum size (16 MB) or it has been open for the maximum allowed duration (12 hours). You can back up and copy the **.work** file from the controller to a remote server.
- **.dat** — The inactive file that contains the archived account records. You can back up and copy the **.dat** file from the controller to a remote server.

Note



The CDR directory on the controller only has two files — a **.work** file and a **.dat** file. When the **.work** file attains its maximum size of 16 MB, or it has been open for 12 hours, it is saved as a **.dat** file. This new **.dat** file overwrites the existing **.dat** file. If you want to copy the existing **.dat** file, you must do so before it is overwritten by the new **.dat** file.

CDR File Format

A CDR file contains a sequence of CDR records. The file is a standard ASCII text file. Records are separated by a sequence of dashes followed by a line break. The individual fields of a record are reported one per line, in "field=value" format.

The following table describes the records that are displayed in a CDR file.



Note

Most of the CDR records are typical RADIUS server attributes. For more information, refer to the user manual of your RADIUS server.

Table 131: CDR Records and Their Description

CDR Records	Description
Acct-Session-ID	A unique CDR ID
User-Name	The name of the user, who was authenticated.
Filter-ID	The name of the filter list for the user.
Acct-Interim-Interval	The number of seconds between interim accounting updates.
Session-Timeout	The maximum number of seconds of service to be provided to the user before termination of the session.
Class	This field is copied from the access-accept message sent by the RADIUS server during authentication.
Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop).
Acct-Delay-Time	Indicates how many seconds the client tried to authenticate send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request.
Acct-Authentic	Indicates how the user was authenticated, whether by RADIUS (AAA), Local (Internal CP) or Remote (External CP). The field displays one of the following values: <ul style="list-style-type: none"> 1 — AAA authentication 2 — Internal CP authentication 3 — External CP authentication
Framed-IP-Address	Indicates the address to be configured for the user
Connect-Info	This field is sent from the NAS to indicate the nature of the users' connection — 802.11b for Radio b/g or 802.11a for radio a.
NAS-Port-Type	Indicates RADIUS NAS Port Type is Wireless 802.11
Called-Station-ID	The Wireless AP's MAC address.
Calling-Station-ID	The client's MAC address.
Extreme Networks-AP-Serial	The AP's serial number.
Extreme Networks-AP-Name	The AP's name.
Extreme Networks-VNS-Name	The VNS name on which the session took place.
Extreme Networks-SSID	The SSID name on which the session took place.

Table 131: CDR Records and Their Description (continued)

CDR Records	Description
Acct-Session-Time	The number of seconds the user has received the service.
Acct-Output-Packets	The number of packets that were sent to the port in the course of delivering this service to a framed user.
Acct-Input-Packets	The number of packets that have been received from the port over the course of this service being provided to a Framed User.
Acct-Output-Octets	The number of octets that were sent to the port in the course of delivering the service.
Acct-Input-Octets	The number of octets that were received from the port over the course of the service.
Acct-Terminate-Cause	Indicates how the session was terminated. The field displays one of the following values: <ul style="list-style-type: none"> • 1 — User Request 4 — Idle Timeout • 5 — Session Timeout • 6 — Admin Reset • 11 — NAS Reboot • 16 — Callback • 17 — User Error
Authenticated_time	Indicates the time at which the client was authenticated. The time is in the following format: Date hh:mm:ss . For example, April 21 2008 14:50:24
Disassociation_time	Indicates the time at which the client was disassociated from the AP. The time is in the following format: Date hh:mm:ss . For example, April 21 2008 14:57:20 .

Viewing CDRs

The following is a high-level overview of how to view CDRs:

- 1 Back up the CDR files on the local drive of the controller.
- 2 Copy the CDR files from the controller to the remote server.
- 3 Unzip the file.
- 4 Download the CDR files from the remote server to view CDRs.



Note

You cannot access the CDR files directly from the CDR directory.

When you back up CDRs, both the **.work** and **.dat** files are zipped into a single .zip file. This .zip file is uploaded on the remote server. You can unzip this file from the remote server to extract the **.work** and **.dat** files.

You can back up and upload the files on the remote server either via the Wireless Assistant (GUI) or CLI.

This section describes how to back up and copy the CDR files to a remote server via the Wireless Assistant (GUI). For more information on how to copy the CDR file to the remote server via CLI, refer to the Extreme Networks ExtremeWireless *CLI Reference Guide*.

Backing Up and Copying CDR Files to a Remote Server

To back up and copy the CDR files to a remote server:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Administration** > **Software Maintenance**.
- 3 Click the **Backup** tab.

The screenshot displays the 'Backup' tab within the 'EWC Software' section. The interface includes a top navigation bar with 'Logs', 'Reports', 'Controller' (selected), 'AP', 'VNS', 'WIPS', and 'Help'. A 'Logout' link is located in the top right corner. The main content area is divided into several sections:

- Available Backups:** A list box containing two files: 'EWC7.01112017.174002.zip' and 'EWC7.31102017.174002.zip'. Below the list are 'Details' and 'Delete' buttons.
- Copy Selected Backup to:** A section with two radio buttons: 'Remote' (selected) and 'Flash'. Below them are input fields for 'Protocol' (set to 'FTP'), 'Server' (192.168.0.45), 'User ID' (extreme), 'Password' (masked with dots), 'Confirm' (empty), 'Directory' (./FTP/), and 'Filename' (EWC7.01112017.174002.zip). A 'Copy' button is at the bottom right of this section.
- Backup:** A section with a dropdown menu 'Select What to Back up:' set to 'Config's, CDRs, Logs and Audit', and another dropdown 'Backup to:' set to 'Local'. A 'Backup Now' button is to the right.
- Schedule Backups:** A section showing 'Next backup: Thursday, November 02, 2017 5:40pm', 'Schedule: Daily', 'Send To: Remote [192.168.0.45]', and 'Backup of: Config's, CDRs, Logs and Audit'. A 'Schedule Backups...' button is at the bottom right.
- Disk Space Left for Backup/Restore:** 12975 MB.

- 4 From the **Select what to backup** drop-down menu, click **CDRs only**, and then click **Backup Now**.
The following window displays the backup status.



- 5 To close the window, click **Close**. The backed up file is displayed in the **Available Backups** box.

**Note**

The **.work** and **.dat** files are zipped into a single file.

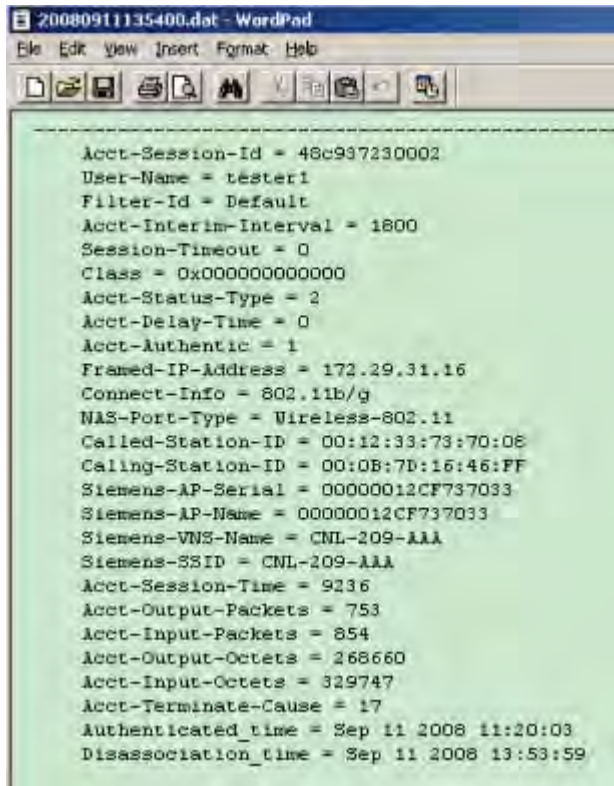
- 6 To upload a backup to a Remote, in the **Copy Selected Backup > to** section, select **Remote**, then do the following:
 - **Protocol** — Select the file transfer protocol you want to use to upload the backup file, SCP or FTP.
 - **Server** — Type the IP address of the server where the backup will be stored.

**Note**

The Server Address field supports both IPv4 and IPv6 addresses.

- **User ID** — Type the user ID to log in to the server.
 - **Password** — The password to log in to the server.
 - **Confirm** — The password to confirm the password.
 - **Directory** — The directory in which you want to upload the CDR file.
 - **Filename** — Select the zipped CDR file name.
- 7 To upload a backup to Flash, in the **Copy Selected Backup > to** section, select **Flash**, then do the following:
 - **Filename** — Select the zipped CDR file name.
 - 8 In the **Copy Selected Backup to** section, click **Copy**. The .zip file is uploaded on to the server.
 - 9 Unzip the file. The two CDR files — **.work** and **.dat** — are visible on the server.

- 10 To view CDRs, download the files.



```
Acct-Session-Id = 48c937230002
User-Name = tester1
Filter-Id = Default
Acct-Interim-Interval = 1800
Session-Timeout = 0
Class = 0x000000000000
Acct-Status-Type = 2
Acct-Delay-Time = 0
Acct-Authentic = 1
Framed-IP-Address = 172.29.31.16
Connect-Info = 802.11b/g
NAS-Port-Type = Wireless-802.11
Called-Station-ID = 00:12:33:73:70:08
Calling-Station-ID = 00:0B:7D:16:46:FF
Siemens-AP-Serial = 00000012CF737033
Siemens-AP-Name = 00000012CF737033
Siemens-VNS-Name = CNL-209-AAA
Siemens-SSID = CNL-209-AAA
Acct-Session-Time = 9236
Acct-Output-Packets = 753
Acct-Input-Packets = 854
Acct-Output-Octets = 268660
Acct-Input-Octets = 329747
Acct-Terminate-Cause = 17
Authenticated_time = Sep 11 2008 11:20:03
Disassociation_time = Sep 11 2008 13:53:59
```

Figure 210: Sample .dat File

19 Performing System Administration

Performing Wireless AP Client Management Defining Wireless Assistant Administrators and Login Groups

Performing Wireless AP Client Management

There are times when for business, service, or security reasons you want to cut the connection with a particular wireless device. You can view all the associated wireless devices, by MAC address, on a selected AP and do the following:

- Disassociate a selected wireless device from its AP. Take this action from the All Clients Report. See [Viewing All Clients](#) on page 642.
- Add a selected wireless device's MAC address to a blacklist of wireless clients that will not be allowed to associate with the AP. For more information, see [Adding Clients to a Blacklist](#) on page 669.
- Backup and restore the controller database. For more information, see the ExtremeWireless *Maintenance Guide*.

Related Links

[Viewing All Clients](#) on page 642

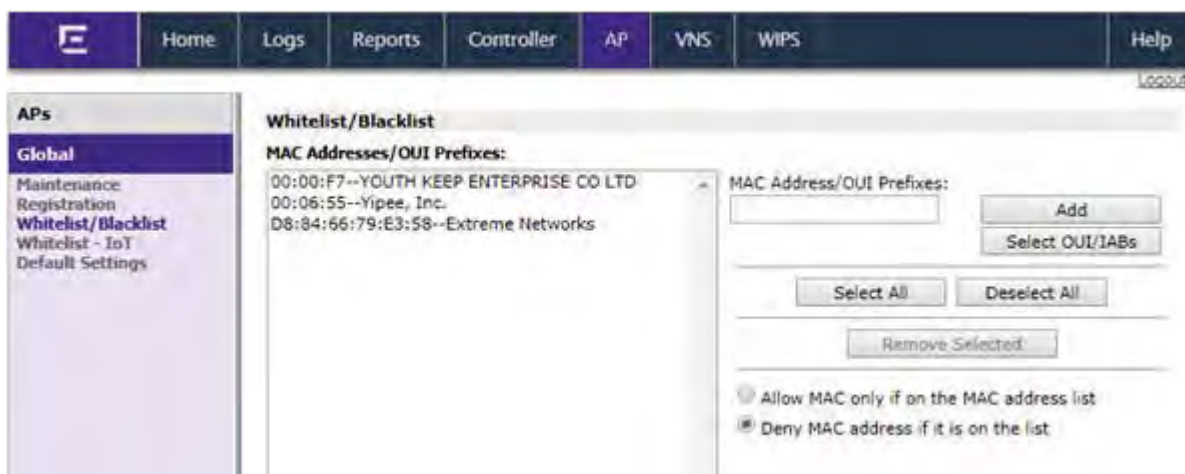
[Adding Clients to a Blacklist](#) on page 669

Adding Clients to a Blacklist

To create a client blacklist:

- 1 Go to **AP**.

- 2 In the left pane, click **Global > Whitelist/Blacklist**.



- 3 Do one of the following:
- Type the client MAC Address or OUI Prefix and click **Add**.
 - Click **Select OUI/IABs**, and search for a client OUI/IAB by company name.
 - The Organizationally Unique Identifier (OUI) is a 24-bit number that uniquely identifies the client vendor or manufacturer. (Search by company name.)
 - Individual Address Block (IAB) is a block of identifiers that uniquely identify the assignee of the IAB. The purpose of the IAB is to allow organizations to purchase smaller blocks of identifiers.

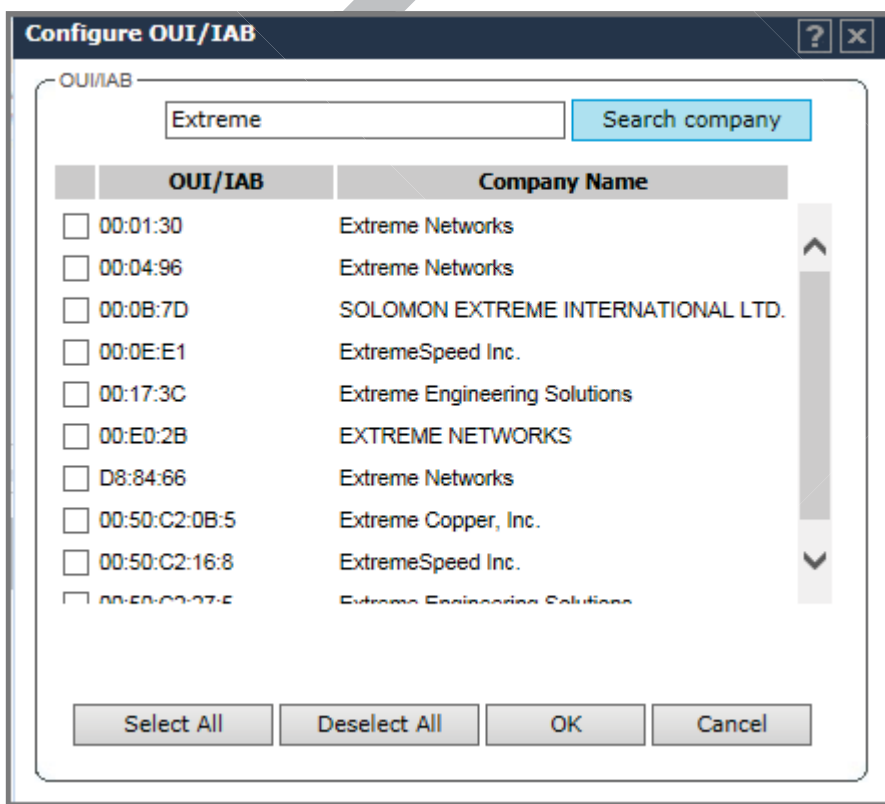


Figure 211: Searching OUI/IAB by Company Name

- 4 Select one or more items to add to the blacklist and click **OK**.

Whitelist/Blacklist

MAC Addresses/OUI Prefixes:

- 00:01:30--Extreme Networks
- 00:04:96--Extreme Networks
- 00:0B:7D--SOLOMON EXTREME INTERNATIONAL LT
- 00:0E:E1--ExtremeSpeed Inc.
- 00:17:3C--Extreme Engineering Solutions
- 00:E0:2B--Extreme Networks
- 5C:0E:8B--Extreme Networks
- 74:67:F7--Extreme Networks
- B4:C7:99--Extreme Networks
- B8:50:01--Extreme Networks
- D8:84:66--Extreme Networks
- FC:0A:81--Extreme Networks
- 00:50:C2:0B:5--EXTREME COPPER, INC.
- 00:50:C2:16:8--ExtremeSpeed Inc.
- 00:50:C2:27:5--Extreme Engineering Solutions

MAC Address/OUI Prefixes:

Add

Select OUI/IABs

Select All **Deselect All**

Remove Selected

☐ Allow MAC only if on the MAC address list

☒ Deny MAC address if it is on the list

Save **Cancel**

* Automatically added entry:

Figure 212: Example List

- 5 To remove clients from the list, select one or more clients on the list and click **Remove Selected**.

Related Links

[Viewing Client MAC and OUI](#) on page 646

[Viewing All Clients](#) on page 642

Managing an IoT Whitelist

Create a whitelist of approved nodes for the Thread Network. The IoT whitelist applies to all APs that are configured for Thread Gateway associated with the controller.

If your whitelist is empty, all sensors with the default password THREAD have access to the Thread Network. Once you configure at least one node on the whitelist, network access is limited to only nodes configured on the whitelist.



Note

Once a whitelist is configured, only nodes configured on the whitelist gain access to the Thread Network.

- 1 Go to **AP > Global > Whitelist - IoT**.
A list of approved nodes is displayed.
- 2 To add a node to the whitelist, click the plus sign and provide the EUI (Extended Unique Identifier) and shared-password for the node.
- 3 To delete a node from the whitelist, select a node and click the minus sign.

Whitelist - IoT	
Extended Unique Identifier (EUI) / Password (PSKd)	
	EUI
<input type="checkbox"/>	890763451234
<input type="checkbox"/>	9990-3458722345

+
-

Save

Figure 213: Whitelist - IoT

Related Links

[Whitelist Node Parameters](#) on page 672

Whitelist Node Parameters

Create a whitelist of approved nodes for the Thread Network. The IoT whitelist applies to all APs that are configured for Thread Gateway associated with the controller.

Use the long EUI for each sensor and the pre-shared password. The short EUI is not used. Currently, the whitelist can be comprised of a maximum 32 nodes.

Table 132: Node Parameters

Field	Description
EUI	Extended Unique Identifier for each sensor node, determined by the sensor manufacturer.
Password	Pre-shared password. Sensor passwords are created when the sensor is commissioned, outside of ExtremeWireless. The default password is THREAD.

Related Links

[Managing an IoT Whitelist](#) on page 671

[IoT Thread Gateway](#) on page 196

Defining Wireless Assistant Administrators and Login Groups

You can define the login user names and passwords for administrators that have access to the Wireless Assistant. You can also assign them to a login group — as full administrators, read-only administrators, or as GuestPortal managers. For each user added, you can define and modify a user ID and password.

- **Full administrators** — Users assigned to this login group have full administrator access rights on the controller. Full administrators can manage all aspects of the controller, including GuestPortal user accounts.
- **Read-only administrators** — Users assigned to this login group have read-only access rights on the controller, including the GuestPortal user accounts.
- **GuestPortal managers** — Users assigned to this login group can only manage GuestPortal user accounts. Any user who logs on to the controller and is assigned to this group can only access the **GuestPortal Guest Administration** page of the Wireless Assistant.

**Note**

Passwords can include the following characters: A-Z a-z 0-9 ~!@#\$%^&*()_+|=~\{}[];<>?., Password cannot include the following characters: / ` ' " : or a space.

To add a controller administrator to a login group:

- 1 From the top menu, click **Controller**.

- 2 From the left pane, click **Administration** > **Login Management**.

The following screen appears:

The screenshot shows the 'Local Authentication' tab selected. On the left, the 'Full Administrator' group is selected. The 'Add User' section is visible, with the 'Group' dropdown set to 'Full Administrator'. The 'Modify User' section shows the 'User ID' as 'admin'. At the bottom, the 'Authentication mode' is set to 'Local, RADIUS'.

- 3 In the **Group** drop-down list, click one of the following:

- **Full Administrator** — Users assigned to this login group have full administrator access rights on the controller.

Full administrators can manage GuestPortal user accounts.

- **Read-only Administrator** — Users assigned to this login group have read-only access rights on the controller.

Read-only administrators have read access to the GuestPortal user accounts.

- **GuestPortal Manager** — Users assigned to this login group can only manage GuestPortal user accounts. Any user who logs on to the controller and is assigned to this group can only access the **GuestPortal Guest Administration** page of the wireless assistant. For more information, see [Performing System Administration](#) on page 669.

- 4 In the **User ID** box, type the user ID for the new user. A user ID can only be used once, in only one category.
- 5 In the **Password** box, type the password for the new user.
- 6 In the **Confirm Password**, re-type the password.

- 7 Click **Add User**. The new user is added to the appropriate login group list.

Related Links

[Modifying Admin Password](#) on page 675

[Removing Administrator](#) on page 675

Modifying Admin Password

To modify a controller administrator password:

- 1 Go to **Controller**.
- 2 In the left pane, click **Administration** > **Login Management**.
- 3 Click the user whose password you want to modify.
- 4 In the **Password** box, type the new password for the user.
- 5 Under **Confirm Password** re-type the new password.
- 6 To change the password, click **Change Password**.

Removing Administrator

To remove a controller administrator:

- 1 Go to **Controller**.
- 2 In the left pane, click **Administration** > **Login Management**. The **Login Management** tab is displayed.
- 3 Click the user you want to remove.
- 4 Click **Remove user**. The user is removed from the list.

20 Logs, Traces, Audits and DHCP Messages

ExtremeWireless Appliance Messages

Working with Logs

Viewing Wireless AP Traces

Viewing Audit Messages

Viewing the DHCP Messages

Viewing the NTP Messages

Viewing Software Upgrade Messages

Viewing Configuration Restore/Import Messages

ExtremeWireless Appliance Messages

The ExtremeWireless Appliance generates four types of messages:

- **Logs (including alarms)** – Messages that are triggered by events
- **Traces** – Messages that display activity by component, for system debugging, troubleshooting, and internal monitoring of software

Caution



In order for the **Debug Info** option on the **Wireless AP Traces** screen to return trace messages, this option must be enabled while Wireless AP debug commands are running. To do so, you need to run a Wireless AP CLI command to turn on a specific Wireless AP debug. Once the CLI command is run, select the **Debug Info** option, and then click **Retrieve Traces**. For more information, see *Extreme Networks ExtremeWireless CLI Reference Guide*. Because Wireless AP debugging can affect the normal operation of Wireless AP service, enabling debugging is not recommended unless specific instructions are provided.

- **Audits** – Messages that record administrative changes made to the system
- **DHCP** – Messages that record *DHCP (Dynamic Host Configuration Protocol)* service events

Working with Logs

The log messages contain the time of event, severity, source component, and any details generated by the source component. Log messages are divided into three groups:

- Controller logs
- Wireless AP logs
- Login logs

Log Severity Levels

Log messages are classified at four levels of severity:

- Information (the activity of normal operation)
- Minor (alarm)
- Major (alarm)
- Critical (alarm)

The alarm messages (minor, major or critical log messages) are triggered by activities that meet certain conditions that should be known and dealt with. The following are examples of events on the wireless controller that generate an alarm message:

- Reboot due to failure
- Software upgrade failure on the wireless controller
- Software upgrade failure on the wireless AP
- Detection of rogue access point activity without valid ID
- Availability configuration not identical on the primary and secondary wireless controller

If *SNMP (Simple Network Management Protocol)* is enabled on the wireless controller, alarm conditions will trigger a trap in SNMP (Simple Network Management Protocol). An SNMP trap is an event notification sent by the managed agent (a network device) to the management system to identify the occurrence of conditions.

Note



The log statements **Low water mark level was reached** and **Incoming message dropped, because of the rate limiting mechanism** indicate that there is a burst of log messages coming to the event server and the processing speed is slower than the incoming rate of log messages. These messages do not indicate that the system is impaired in any way.

Viewing the Wireless Controller Logs

To view wireless controller logs:

- 1 From the top menu, click **Logs**.