ExtremeWireless™ Getting Started Guide

Release V10.31.01

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: http://www.extremenetworks.com/support/contact/

For product documentation online, visit: https://www.extremenetworks.com/documentation/

For information, contact:
Extreme Networks, Inc.
6480 Via Del Oro
San Jose, California 95119
USA

Table of Contents

Preface

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
	New	This command or section is new for this release.

Table 2: Text Conventions

Convention	Description
Screen displays	This typeface indicates command syntax, or represents information as it appears on the screen.
The words **enter** and **type**	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
[Key] names	Key names are written with brackets, such as **[Return]** or **[Esc]**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **[Ctrl]**+**[Alt]**+**[Del]**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at internalinfodev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- **GTAC (Global Technical Assistance Center) for Immediate Support**
  - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **GTAC Knowledge** — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- **The Hub** — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- **Support Portal** — Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Related Publications

ExtremeWireless and ExtremeWireless AP documentation can be found on Extreme Documentation page at: http://documentation.extremenetworks.com

Extreme recommends the following guides for users of ExtremeWireless products:

- *ExtremeWireless AP3916ic Installation Guide*
- *ExtremeWireless AP3912i Installation Guide*
- *ExtremeWireless AP3965i & AP3965e Installation Guide*
- *ExtremeWireless AP3935i & AP3935e Installation Guide*
- *ExtremeWireless AP3825i & AP3825e Installation Guide*
- *ExtremeWireless AP3805i FCC/ROW Installation Guide*
- *ExtremeWireless AP3801i Quick Reference Guide*

- *ExtremeWireless Appliance C5210 Quick Reference*
- *ExtremeWireless Appliance C5110 Quick Reference*
- *ExtremeWireless Appliance C4110 Quick Reference*
- *ExtremeWireless Appliance C25 Quick Reference*
- *ExtremeWireless Appliance C35 Quick Reference*
- *ExtremeWireless CLI Reference Guide*
- *ExtremeWireless End User License Agreements*
- *ExtremeWireless External Antenna Site Preparation and Installation Guide*
- *ExtremeWireless External Antenna with Wave 2 Site Preparation and Installation Guide*
- *ExtremeWireless Getting Started Guide*
- *ExtremeWireless Integration Guide*
- *ExtremeWireless Maintenance Guide*
- *ExtremeWireless Open Source Declaration*
- *ExtremeWireless User Guide*
- *IdentiFi Wireless WS-AP3865e Installation Guide*
- *IdentiFi Wireless WS-AP3825i & WS-AP3825e Installation Guide*
- *IdentiFi Wireless WS-AP3805i & WS-AP3805e Installation Guide*

1 Extreme Networks ExtremeWireless Software Solution

Wireless APs
Extreme Networks Wireless LAN (WLAN) Solution Optional Modules
WLAN Solution Topology and Network Elements
Discovery Mechanisms in the ExtremeWireless Software Solution
DHCP and the Extreme Networks ExtremeWireless Software Solution
ExtremeWireless Appliance Physical Description
Collecting Information for the Installation

The Extreme Networks ExtremeWireless Software solution is an enterprise solution that consists of the following components:

- ExtremeWireless Appliance
- Extreme Networks ExtremeWireless Software
- ExtremeWireless AP
- Extreme Management Center and Wireless Advanced Services

Extreme Management Center and Wireless Advanced Services

The ExtremeWireless Appliance provides several network functions, including centralized management and configuration of Wireless APs, user authentication, and advanced radio frequency management.

The ExtremeWireless Appliance is driven by the ExtremeWireless Software. The software resides on the ExtremeWireless Appliance and provides an intuitive web-based interface — the ExtremeWireless Assistant — to enable you to manage the entire wireless network from a laptop or a PC connected to the network. A command line interface (CLI) is also available to manage the wireless network.

The ExtremeWireless Appliance is a fully functioning dynamic router/switch that aggregates and coordinates all Wireless APs and manages client devices. Some key features of the ExtremeWireless Appliance are described in the following sections.

> **Note**
> The word *appliance* is synonymous with *controller.* It refers to both controller devices and virtual gateways.

Web-based Centralized Management of Wireless APs

The ExtremeWireless Appliance enables you to monitor and manage Wireless APs from a centralized web-based user interface — the ExtremeWireless Assistant. You can separately configure, enable, or disable each Wireless AP from the ExtremeWireless Appliance using the ExtremeWireless Assistant.

Virtualized User Segmentation

The ExtremeWireless Appliance allows you to create and manage unique that enable you to group specific mobile users, devices, and applications on the basis of policy class (role), in order to provide unique levels of service, access permission, encryption, and device authorization.

Role (also known as policy) defines the station's topology (network segment), filtering (access restrictions) and Class of Service definitions. A VNS definition consists of a WLAN Service bound to one or two roles that are applied to stations by default. Until associated with a role definition, a WLAN Service remains inactive.

When a user associates with a particular SSID (WLAN Service), the user's experience is shaped by the corresponding role that the VNS defines as its default. The user is mapped to a specific segment, its traffic access restricted by the role filters, and its network access rate correspondingly restricted as defined in the role.

However, user authentication responses (such as) or an explicit external API call may remap the user to a different policy. The role reassignment may move the user to a completely different segment (), access state (filters), and rate restriction setting.

Role assignment for a particular user session remains as the user roams across the mobility domain. Role assignment is independent of the underlying characteristics of the transport network and the point of presence of network devices, as well as access points.

In a properly coordinated mobility domain, the user's point of presence is retained, so as to provide an ubiquitous coverage area to the user, wherever the intended SSID is available.

ExtremeWireless Appliances can support the following number of VNSs, topologies, roles, and rate control profiles:

Table 3: ExtremeWireless Appliance VNS Support

Controller	Maximum Number of				
	Active VNSs	VNSs	Topologies	Roles	Rate Control Profiles
C5210	128	256	256	1024	128
C5110	128	256	256	1024	128
C4110	64	128	128	512	128
C25	16	32	32	128	128
C35	16	32	32	128	128
V2110	64	128	128	512	128

Authentication and Encryption

The ExtremeWireless Appliance and ExtremeWireless AP work together to support comprehensive authentication, encryption, and intrusion detection capabilities. A range of security features based upon the 802.11 and WPA2 standards protect your network from intrusion and attack.

An 802.1x mechanism in conjunction with RADIUS and pre-shared key authentication allow only authorized users to access the network. Other features include Captive Portal for redirected web-based authentication.

Radar WIDS-WIPS

ExtremeWireless Radar is a set of advanced, intelligent, Wireless-Intrusion-Detection-Service and Wireless-Intrusion-Prevention-Service (WIDS-WIPS) features that are integrated into the Wireless Controller, its APs, and the Convergence Software. 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: dynamic channel and frequency selection support, location visualization (requires Extreme Management Center), interference classification and adaptation, and wireless intrusion detection and protection.

When Radar is enabled:

- All APs simultaneously provide WIDS-WIPS and wireless bridging functions. The 3825, 3801, 3705, 3710, and 3715 type APs monitor and protect the channels for which they are bridging.
- All APs, except the 3705i, can be configured as Guardian APs, which are APs dedicated to full-time intrusion detection scans and threat prevention countermeasures on all active channels. APs in Guardian mode cannot serve to bridge traffic, but can be switched to Traffic Bridging mode when necessary.
- The APs can be configured to take active countermeasures against specific types of threat that they have detected. Available countermeasures include: sending de-authentication frames to devices and threatening APs, automatically blacklisting devices performing WIDS-WIPS attacks (when that action mitigates the attack), and rate limiting wireless frames detected as part of a Denial of Service (DoS) attack.

The full Radar feature requires a license, but a non-licensed subset of Radar functions is provided in the base Convergence Software package.

For detailed information about Radar WIDS-WIPS features and how to configure them, see the *ExtremeWireless User Guide*.

Automatic Assignment of IP Addresses to the Client Devices

The ExtremeWireless Appliance has a built-in server that may be used to assign IP addresses to the client devices on specific topologies. The ExtremeWireless Appliance is also capable of working with an external DHCP server, by relaying segment DHCP requests to the configured server.

Web Authentication

The ExtremeWireless Appliance has a built-in Captive Portal capability that allows web authentication (web redirection) to take place. The ExtremeWireless Appliance is also capable of working with an external captive portal.

Wireless APs

The ExtremeWireless APs are enterprise-class access points that deliver secure wireless access via the Layer 3 tunnel for enterprise deployments. They provide advanced RF capabilities, security, reliability, and scalability. Individual services may also be configured to be handled locally.

The Wireless provide an unmatched level of flexibility and performance for complex, time-sensitive functions including , encryption, and network intrusion and detection.

The Wireless AP physically connects to a LAN infrastructure and establishes an IP connection with the ExtremeWireless Appliance. You configure and manage global or individual functions on Wireless APs using the Extreme Networks ExtremeWireless Software, which runs on the ExtremeWireless Appliance.

All communication between the ExtremeWireless Appliance and the Wireless AP is carried out using a UDP-based protocol. The IP traffic coming from the Wireless AP is encapsulated and directed to the ExtremeWireless Appliance. The ExtremeWireless Appliance exposes the packets and forwards or bridges them to the appropriate destinations, while managing sessions and applying roles (policies).

Extreme Networks offers cloud-enabled ExtremeWireless APs . ExtremeCloud supports a variety of deployment models, from the simple deployment of one or more cloud-enabled APs to deployments of cloud-enabled APs with cloud-enabled switches, both of which can be deployed with existing on-premise equipment. For more information about ExtremeCloud™, see *ExtremeCloud™Information Center*.

For more information about ExtremeWireless APs, and the firmware supported, see ExtremeWireless Hardware Firmware Support Matrix.

> **Note**
> The configuration process for all Wireless APs is identical, unless otherwise specified.

For detailed information on a specific AP, see the *User Guide* and appropriate AP *Installation Guide*.

Mesh and WDS

A Mesh network or Wireless Distribution System (WDS) enables you to expand the network by wirelessly interconnecting Wireless APs rather than physical connections via a wired network. A mesh network is a self-healing, dynamic network; a WDS deployment is also known as a static form of a mesh network. Mesh and WDS deployments are ideally suited for locations where installing Ethernet cabling is costly or difficult.

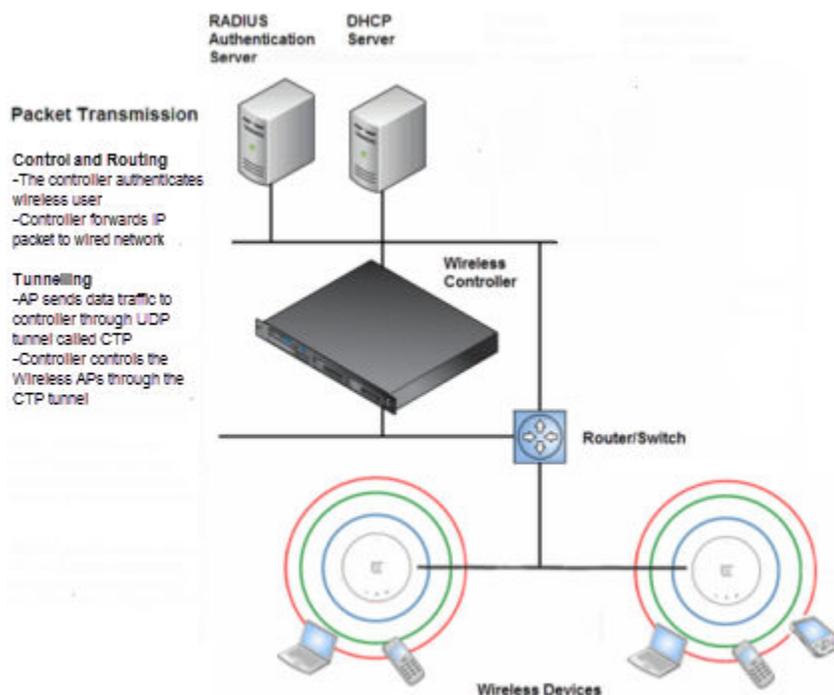## Extreme Networks Wireless LAN (WLAN) Solution Optional Modules

The Extreme Networks Wireless LAN () Solution has two optional modules:

- **Extreme Management Center:** Extreme Management Center simplifies network configuration by enabling you to configure and manage multiple wireless controllers and their associated wireless APs. Using the Wireless Manager wizards and configuration tools, you can create a new network configuration or clone an existing one an apply that same configuration to multiple controllers and APs. Wireless Manager is a component of Extreme Management Center. For more information, see the *User Guide* or the Extreme Management Center Online Help.

- **Wireless Advanced Services:** Wireless Advanced Services is a separately licensed application that enables you to monitor the wireless network, locate wireless devices on maps, configure sensors, generate security compliance reports, and use wireless forensic analysis tools.
  - Monitoring – 2.4 GHz and 5 GHz, all channel association activity
  - Identification – Detects all Wi-Fi activity and correlates information from multiple sensors
  - Auto-Classification – Limits user intervention to maximize the protection of all devices from all threats
  - Visualization – Visualizes measured coverage for service, detection, and prevention
  - Location – Identifies rogue APs and clients on the floor-plan for permanent removal

WLAN Solution Topology and Network Elements

The following figure illustrates a typical configuration with a single ExtremeWireless Appliance and two ExtremeWireless APs, each supporting a wireless device. A server on the network provides user authentication, and a server assigns IP addresses to the Wireless APs. Network inter-connectivity is provided by the infrastructure routing and switching devices.

Figure 1: Extreme Networks Wireless LAN Topology

- RADIUS server (Remote Access Dial-in User Service)

  An authentication server that assigns and manages ID and password protection throughout the network. The RADIUS server system can be set up for certain standard attributes such as Filter ID, which can be used to provide policy assignment indications for a specific user, and for the vendor specific attributes (VSAs). The appliance does not implement its own RADIUS server but rather

depends on the interaction with infrastructure (customer) available servers. This facilitates the centralization of user policy for wireless and other access methods.

* **DHCP server (Dynamic Host Configuration Protocol)**

  A server that assigns the IP addresses, gateways, and subnet masks dynamically. The external DHCP server, depicted in Figure 1-1, is used to provide addresses to infrastructure equipment such as APs. If you do not have a DHCP server, you can configure the appliance's built-in DHCP server to provide the IP addresses to infrastructure equipment, including the APs (if the APs are connected on the same segment as the corresponding controller port on which the service is enabled). In addition, the IP addresses to the mobile devices are provided by the built-in DHCP server of the appliance. You can also configure the appliance to relay DHCP requests to the external DHCP server.

* **SLP (Service Location Protocol)**

  A service discovery protocol that allows computers and other devices to find services in a local area network without prior configuration. The client applications are user agents and services that are advertised by a service agent. In larger installations, a directory agent collects information from service agents and creates a central repository. SLP is one of several modes that the Wireless APs use to discover the appliance.

* **Domain Name Server (DNS)**

  A server that translates the domain names into IP addresses. The DNS is used as an alternative mechanism for the automatic discovery process. In addition to an end-user's usage of DNS to obtain IP references to common internet resources (web-sites), it may also be used as an alternative method for AP-Controller discovery. The ExtremeWireless Appliance, its software, and the APs rely on the DNS for Layer 3 deployments. In addition, appliances use DNS to discover their controller. The appliance can be registered in DNS as controller.<domain> to provide DNS-assisted discovery by APs

Discovery Mechanisms in the ExtremeWireless Software Solution

The Extreme Networks ExtremeWireless Software solution provides auto-discovery capabilities between Wireless APs and ExtremeWireless Appliance Mobility manager and mobility agents. For more information, see the *User Guide*.

Discovery Mechanism Between a Wireless AP and ExtremeWireless Appliance

The Wireless APs discover the ExtremeWireless Appliance by one of the following modes:

* SLP (Multicast and Unicast) – For more information, see SLP's description in WLAN Solution Topology and Network Elements on page 11.
* DNS – For more information, see Domain Name Server's description in WLAN Solution Topology and Network Elements on page 11
* Static IP address configuration – ExtremeWireless Appliance's IP address is defined in the Wireless AP configuration. For more information, see the "Setting up static routes" section of the *User Guide*.

Discovery Mechanism Between Mobility Manager and Mobility Agents

The mobility agents discover the mobility manager by one of the following modes:

- SLP-DA with Option 78 – The mobility agent on each ExtremeWireless Appliance discovers the address of the mobility manager. SLP-DA is a normal network function. If your network already deploys such a device, the controllers will promptly register their services with it (assuming that the controllers can identify the device via DHCP Option78 query on its locally attached segments). If your deployment does not have an existing SLP-DA, each controller has that function enabled by default (and will correspondingly register with itself). In order for other controllers or APs to find the preferred SLP-DA for the network, simply provision DHCP Option 78 on each of the required networks to refer to the IP address of the selected controller.
- Direct IP address option – Defined while configuring the mobility agent. By explicitly defining the manager's IP address while configuring the agents, this enables the manager and agents to find each other directly without using the SLP discovery mechanism.

DHCP and the Extreme Networks ExtremeWireless Software Solution

The Extreme Networks ExtremeWireless supports the following configurations per topology:

- Controller is the DHCP server and available for routed topologies. For more information, see "DHCP Service Configuration" on page 3-1.
- Controller is a DHCP relay agent and available for routed topologies.
- Controller is neither a DHCP server or relay agent and available for Bridged@AP topologies. DHCP for traffic bridged locally at the Wireless AP is performed by a local DHCP server on the network and does not go through a controller at all.

For more information, see the *User Guide*.

Note

All three DHCP configurations are available for Bridged@Controller topologies. For Bridged@Controller topologies, the controller may be configured as the DHCP server for the corresponding . In this configuration, the controller bridges all the received traffic from a connected mobile user to the corresponding VLAN. The VLAN IP assignment must already have been configured for DHCP service. The wireless user joins that VLAN as a normal wired user. The address for the user is provided by the corresponding server. The controller learns the assigned IP address from a user based on IP inspection.

ExtremeWireless Appliance Physical Description

ExtremeWireless Appliances are described in detail in the *Maintenance Guide* and in the *Quick Reference Guide* for each controller.

Collecting Information for the Installation

Before installing and configuring your wireless network, consider the following and write down key information that you will need for the process:

- Will the controller be managed remotely via a management, data, or wireless interface? By default, the controller cannot be managed over its data plane or wireless interface. These capabilities must be enabled explicitly using the controller's user interface.
- If the controller will be managed over the management port, will IPv4 or IPv6 be used?

- For availability services determine the following:
  - services. Which wireless LAN services will be offered by the controller?
  - Privacy settings. Do the WLAN Services require WEP, WPA-PSK, or WPA2 privacy settings?
  - Authorization. Will MAC or MAC-based authorization be required prior to gaining access to the network?
  - Authentication. Determine the mechanism that is required for users to access each WLAN Service: None, Captive Portal (internal, external, Guest Portal), AAA//Certificate? RADIUS requires connectivity to an infrastructure RADIUS server.
  - The controller's location on the network.
  - The segments that the controllers need to connect to.
  - The routed or bridged segments that will deliver user traffic.
  - The VLANs that the controllers need to connect to.
  - The switch ports that provide the VLANs that controllers need to connect to?
  - How wireless services map or make use of the available network segments.
  - The restrictions that the users will be subject to when accessing the network?
- Controller deployment.
  - Is more than a single controller going to be deployed? If multiple controllers are deployed, are the controllers deployed in availability pairs?
  - Are controllers going to be deployed as part of a mobility domain? A mobility domain is a collection of controllers that collaborate to allow stations to roam seamlessly between the APs of different member controllers.
- Time synchronization. If controllers will be time synchronized, to what source will they be synchronized?
- Controller logs. Will controller logs be remotely aggregated using syslog? If syslog is used, determine the syslog server.
- AP deployment. Will APs be deployed on the same segment or several segments away from the controller's network point?
- AP discovery. Which discovery mechanism will be used to register an AP to the controller: SLP, DNS, multicast, or static listing?
- Controller interfaces. Which controller interfaces will be defined to allow AP registration?

Use the following table to document all the pertinent information about the ExtremeWireless Appliance before starting the installation process.

Some of the information listed in the table may not be relevant to your network configuration. Only record the information that is pertinent to your network configuration.

Table 4: Information Gathering Table

Configuration Data	Description	Your Entry
/WLAN Service and Role (Policy) creation and dependencies	• Service types the system is expected to provide • Controller services • Topologies made up of VLANs and port assignments with the corresponding switch ports • Policies that will be bound to topologies • Classes of Service • WLAN Service and wireless user credentials authentication • Creation of VNS that binds WLAN service to roles (policies) • A tagged for each bridge in the controller, along with a network port on which the VLAN is assigned • A virtual subnet on the controller for each VNS: Topology type of bridged@controller, routed, or bridged@AP Policy for network point of attachment: user network access policy, filtering at the controller or also at the AP Whether bandwidth restrictions are imposed on users WLAN Service: type of SSID, advertised SSID by APs representing the service, AP radios corresponding to band that will advertise the service, method of authentication, wireless security method, and VNS: WLAN service the VNS represents, Default Non-Auth Policy, Default Auth Policy, VNS mapping between the WLAN service and default policies, method of AP controller discovery	
Accessing the ExtremeWireless Appliance for the first time	• **Factory default IP address of the ExtremeWireless Appliance** – The factory default IP address is https://192.168.10.1:5825. You must type this IP address in the address bar of your web browser when you access the ExtremeWireless Appliance for the first time. • **Unused IP address in the 192.168.10.0/24 subnet** – This IP address must be assigned to the Ethernet port of your laptop computer, for the initial provisioning only. You can use any IP address from 192.168.10.2 to 192.168.10.254. • **Login Information** – The login information is as follows: • User Name: admin • Password: abc123 After you have logged in, change the default user name and password.	

Table 4: Information Gathering Table (continued)

Configuration Data	Description	Your Entry
System Settings	• **Hostname** – Specifies the name of the ExtremeWireless Appliance. • **Domain** – Specifies the IP domain name of the enterprise network. • **Primary** DNS – The primary DNS server used by the network. • **Secondary DNS** – The secondary DNS server used by the network.	
Hardware information	**MAC Address** – MAC address of the ExtremeWireless Appliance's management port.	
License Key	A license key is provided by redeeming an entitlement voucher on the Extreme Networks website by selecting the Extreme Networks Activation Key link at page: www.extremenetworks.com/support/. Enter the license key for system activation, capacity upgrades, or feature enablement. For more information about ExtremeWireless licensing, see Step 6. Apply the Activation License Key on page 30.	
Data Ports Physical Topology	• **IP address** – IP address of the physical Ethernet port. • **Subnet mask** – Subnet mask for the IP address, which separates the network portion from the host portion of the address (typically 255.255.255.0). • **MTU** – The maximum transmission unit or maximum packet size for this port. The default setting is 1500. If you change this setting, and are using OSPF, you must make sure that the MTU of each port in the OSPF link matches. • **Function** – The port's function. • **Third-party AP Port** – A port to which the third-party AP is connected. • **Router Port** – A port that connects to an upstream, next-hop router in the network. • **VLAN ID** – The ID of the VLAN to which the AP is connected.	
Static Routing	**Static IP address** – The static IP address that is assigned to the ExtremeWireless Appliance when it is configured for static routing. Configurable physical properties: • **Allow Management** – Determines whether or not this particular interface will allow management operations (, HTTPS, SSH). • **AP Registration** – Determines whether this interface is advertised as allowing AP registration. • **Server** – Determines whether the controller should operate as DHCP server for the corresponding segment.	

Table 4: Information Gathering Table (continued)

Configuration Data	Description	Your Entry
OSPF Routing	**Routed VNS** – if you are planning to deploy a routed VNS, you may need to enable OSPF on the controller. The OSPF option applies only to routed VNS. • **Router ID** – The router ID is its own IP address. • **Area ID of OSPF** – ID of OSPF's area. 0.0.0.0. is the main area in OSPF. • **OSPF Authentication Password** – If you select Authentication type as Password, you will need to provide a password.	

Table 4: Information Gathering Table (continued)

Configuration Data	Description	Your Entry

DHCP service not hosted by controller	**Bridge traffic locally at AP** – IP assignment is not applicable; all traffic for users in that VNS will be directly bridged by the AP at the local network point of attachment; disabled by default.
	Local server – The ExtremeWireless Appliance's local DHCP server is used for managing IP address allocation:
	• **Domain Name** – The external enterprise domain name server to be used
	• **Lease default** – The default time limit which dictates how long a wireless device can keep the DHCP server assigned IP address
	• **DNS servers** – The IP Address of the Domain Name servers to be used
	• **WINS** – The IP address if the DHCP server uses Windows Internet Naming Service (WINS)
	• **Enable DLS DHCP Option** – An application that provides configuration management and software deployment and licensing for optiPoint WL2 phones, if you expect optiPoint WL2 wireless phone traffic on the VNS.
	• **Gateway** – The ExtremeWireless Appliance's own IP address in the topology, which is the default gateway for the topology
	• **Address Range** – The range from which the IP address is distributed across the network.
	
	    Address range from – The start IP address of the range.
	
	    Address range to – The end IP address of the range.
	
	    DHCP Address exclusion – IP addresses to be excluded from this range
	• **Broadcast Address** – Automatically populates automatically based on the Gateway IP address and subnet mask of the VNS
	
	Use Relay – The ExtremeWireless Appliance forwards DHCP requests to an external DHCP server on the enterprise network:
	• **DHCP servers** – IP address of the DHCP server to which DHCP discover and request messages are forwarded for clients on this VNS	

Table 4: Information Gathering Table (continued)

Configuration Data	Description	Your Entry
Gateway for installing DHCP service	**Gateway** – Determine the gateway device for the DHCP service. • For a physical topology or bridged@AC, the specified gateway must be a connecting device on the same segment. • For a routed topology, the segment is owned by the controller. The controller's interface on the segment is defined as the default gateway (option3) for the segment.	
Domain name for devices on this network segment	**Domain name** – Your organization's domain name.	
RADIUS Server's IP address	**IP address** – The IP address of the RADIUS server.	
SLP DA's IP address	**Hexadecimal values of SLP DA's IP address** – The Wireless APs use the SLP DA to discover the ExtremeWireless Appliance. The mobility agents use the SLP DA to discover the mobility manager. SLP-DA is configured in hexadecimal on the target DHCP server (this element is not provisioned on the controller). The value is configured in relation to option 78 on the segment definitions of the DHCP server that provides the IP addresses of the APs or that the controller can query to determine the selected SLP-DA service in the network. This provisioning is done per such segment.	
Internet Protocol configuration for DNS service server	• **Static IP address** – The DNS server's static IP address. • **Subnet Mask** – Subnet mask of the DNS server's static IP address. • **Gateway** – The DNS server's gateway. • **ISP's IP address** – Your ISP's (Internet Service Provider) IP address. • **IP address** – ExtremeWireless Appliance's IP address.	
Port information for installing IAS on the server	• **Authentication Port** – ExtremeWireless Appliance's port number used to access the IAS service. • **Accounting Port** – Type the ExtremeWireless Appliance's port number that is used to access the accounting service. The values must match what you define in the **Acc & Acct** tab.	

Table 4: Information Gathering Table (continued)

Configuration Data	Description	Your Entry
Wireless AP properties	• **ExtremeWireless Appliance's Port #** – ExtremeWireless Appliance's Ethernet port to which the Wireless AP is connected. • **Country** – The country where the Wireless AP operates. • **Serial #** – A unique identifier that is assigned during the manufacturing process of the Wireless APs. When an AP discovers and registers with a controller, its name defaults to its serial number, therefore tracking the serial number for an AP helps identify the specific device, so as to ensure proper configuration of location dependent settings. • **Hardware version** – The current version of the Wireless AP hardware. • **Application version** – The current version of the Wireless AP software. • **VLAN ID** – The ID of the VLAN on which the Wireless AP operates.	
Next Hop Routing for Routed VNS	An optional configuration element that allows the customer to define an explicit next hop router via which all the segment's traffic should be forwarded. If left unspecified, the traffic is forwarded in accordance to the system's routing table. • **Next hop IP address** – The next-hop IP identifies the target device to which all VNS (user traffic) is forwarded. Next-hop definition supersedes any other possible definition in the routing table. • **OSPF routing cost** – The OSPF cost value provides a relative cost indication to allow upstream routers to calculate whether or not to use the ExtremeWireless Appliance as a better fit, or lowest cost path to reach the devices in a particular network. The higher the cost, the less likely that the ExtremeWireless Appliance is chosen as a route for traffic, unless that ExtremeWireless Appliance is the only possible route for that traffic.	

Table 4: Information Gathering Table (continued)

Configuration Data	Description	Your Entry
VLAN Information for Bridge Traffic Locally at EWC topology	**VLAN ID** – The VLAN ID to which traffic on the topology is bridged. Wireless users referring to this topology become a natural extension of the VLAN/segment. Traffic from the wireless is tagged with the corresponding ID when bridging to the core. **Port** – The name of the L2 port to which the VLAN is mapped. **Interface IP address** – The interface's IP address. **Mask** – The subnet mask of the topology. The interface IP address and mask are not required if the controller and AP do not provide L3 services (such as a Captive Portal web page) on the topology/VLAN and are not managed on the VLAN. L3 interface presence is required for several operations such as: • If topology is to be used to support internal captive portal or guest portal authentication for wireless users. The configuration is optional for external captive topology is to provide DHCP service (local or relay) to the VLAN (includes wireless and wired users) • If the topology is to offer access to management functions (SSH, SNMP, HTTPS) via wired or wireless users. • If the topology is to offer AP registration. L3 interface presence is not required if the topology is: • Only expected to provide straight bridging of wireless traffic • The topology is serviced by WLAN services that don't require authentication (NONE) or that use EAP (AAA) authentication • The DHCP server is provided by the infrastructure (VLAN).	
VLAN ID for Bridge traffic locally at AP topology	**VLAN ID** – The VLAN ID to which traffic is bridged directly at AP. The AP tags traffic for users associated with this topology to the specified VLAN ID. The VLAN must be configured/trunked on the switch port to which the AP is connected.	

Table 4: Information Gathering Table (continued)

Configuration Data	Description	Your Entry
Captive Portal	Will this network segment have a captive portal service? If so, which type of captive portal will be deployed: • An external captive portal which is a web server provided by another host in the network that authenticates stations and tells the controller whether the station is authenticated and which policy to apply to it. • A Guest Portal captive portal. The controller serves the Guest Portal login page to unauthenticated stations. Station accounts are defined directly on the controller through an interface designed for non-technical users. • A Guest-Splash Screen Portal. The controller serves a splash screen web page to unauthenticated users. Users are not considered authenticated until they click a button on the page to acknowledge terms and conditions on the splash screen page. Users are not required to provide a user ID and password to login. • Internal Captive Portal. The controller serves the login page on an internal captive portal to unauthenticated stations. The controller collects user IDs and passwords from stations attempting to access the network and forwards them to a configured RADIUS server for authentication.	
Authentication and Accounting information for captive portal configuration	• **Port** – Used to access the RADIUS server. The default for authentication is 1812 and for accounting is 1813. • **# of Retries** – The number of times the ExtremeWireless Appliance attempts to access the RADIUS server. • **Timeout** – The maximum time for which ExtremeWireless Appliancereless Appliance waits for a response from the RADIUS server before making a re-attempt. • **NAS Identifier** – A RADIUS attribute that identifies the controller to the RADIUS server for purposes of a specific WLAN service. This is optional.	

Table 4: Information Gathering Table (continued)

Configuration Data	Description	Your Entry
Internal Captive Portal, Guest Portal, and Guest splash screen portal settings information	• **Login Page layout** – The controller provides a default login page for each internal captive portal, guest portal and guest splash screen portal it serves. The controller contains a web page layout editor that allows the administrator to fully customize the login page with custom layouts, graphics and styles. • **Replace Gateway IP with FQDN** – By default the controller explicitly encodes the IP address of the corresponding topology (From Non-auth Policy defined by the WLAN service). However, in some cases it is preferable to provide the user with a Fully Qualified Domain Name (FQDN). Ensure that the DNS server is configured to map the corresponding name to the topology's IP address. • **Default Redirection URL** – By default, once the authentication completes, the user is redirected back to the initial web site that was intercepted for redirection to authentication. The customer can provide an explicit override URL to which the user is redirected upon successful authentication.	
External Captive Portal (ECP) Type	Select the type of captive portal configuration to provide authentication services for the WLAN Service: • No captive portal • Internal captive portal – Controller provides the web server that operates as the authentication portal. The controller is also responsible for the credential's verification with a specified RADIUS server. • External captive portal – You provide the web server that hosts the authentication website. This option provides the most flexible approach in terms of customization of the authentication service. Web server interfaces provide alternate methods of user authentication, such as payment systems. Or, provide the web service but rely on the controller to perform the credential authentication via RADIUS. • Internal Guest Portal Splash Screen • Internal Guest Portal	
Shared Secret Password for external captive portal configuration	**ECP privacy** – Whether to require traffic sent between the controller and the external captive portal host to be encrypted and if so with or AES. **Password** – When using ECP, define a Shared Secret (password) that can be used to perform MD5 encryption of sensitive information on the exchange between the authentication server and the controller (such as during credentials exchange for authentication). This password encrypts the information exchanged between the ExtremeWireless Appliancereless Appliance and the external captive portal server.	

Table 4: Information Gathering Table (continued)

Configuration Data	Description	Your Entry
MAC-based authentication information	See authentication and accounting information.	
Exception Filter Rules information	IP/Port - By default, all controller interfaces, including those represented by physical topologies and virtual topologies with L3 presence, are protected by a set of rules that restrict the type of traffic allowed access to management plane functions. The default set of rules allows only services that are explicitly of use to the controller's operations. This set of rules protects the controllers management plane from inadvertent access to lower level functions and provides an effective DoS protection layer. This set of rules however can be augmented or altogether overridden (not recommended) so that additional services may be exposed or restricted. For example, the default method to allow access to management services is to explicitly enable the "Allow Management" property for the topology. Doing so however automatically augments the exception filter rule set to allow administration HTTPS (5825), SSH (22) or SNMP services. An alternate method to enabling such a checkbox would be to manually add the corresponding set of rules for each interested service to the exception rule set. That way you may elect to enable only a subset of the services or to disable access to one of the services the checkbox enabled.	

WLAN Service Wireless Privacy Information

For service wireless privacy information you need to:

- Determine the level of protection (privacy) the Wireless LAN service is to offer (None, WEP, WPA-PSK, DynWEP, WPA).
- Ensure that clients of the WLAN Service/SSID are adequately configured to match the required settings RF settings.

Use the following table to document pertinent WLAN service wireless privacy information about the ExtremeWireless Appliance before starting the installation process.

Table 5: WLAN Service Wireless Privacy Information

Configuration Data	Description	Your Entry

Static WEP privacy information	Keys for a selected , so that it matches the WEP mechanism used on the rest of the network.
	• **WEP Key Length** – Size of a WEP key.
	
	Select an input method:
	  • **Strings** – This is the secret WEP key string.
	  • **Hex** – The WEP key input in the WEP Key box. The key is generated automatically based on the input.	

WPA-PSK privacy information	• **WPA v2 or mixed v1 and v2** – The WPA encryption type further specifying Auto or TKIP only. • **Broadcast re-key interval** – The time interval (in seconds) after which you want the broadcast encryption key to be changed automatically. The default is 3600. • **Pre-shared Key** – The shared secret key that is to be used between the wireless device and the Wireless AP. The shared secret key is used to generate the 256 bit key.	
Dynamic WEP privacy information	**Broadcast re-key interval** – The time interval (in seconds) after which you want the broadcast encryption key to be changed automatically. The default is 3600.	

Availability Pairs Information

If deploying controllers in availability pairs, determine the interface over which the availability link is established. Manually enable the service on both controllers, or run the Availability Wizard to be guided through the steps necessary to enable paired availability between two controllers. Both controllers are automatically configured.

Optionally, you can select whether the availability configuration is to be set to use standard or fast failover operations. If fast-failover is enabled, session-availability is automatically enabled.

You are given the choice to enable automatic configuration synchronization. Once enabled, a modification to service configuration on one controller (such as services, topologies, and policies) is automatically coordinated and synchronized with the peer. You may be requested to provide information details pertaining to the representation of the entity on the other controller, such as the IP address (layer 3 configuration) of the interface on the other controller.

Note
Automatic synchronization is strongly recommended when either fast-failover or session-availability is enabled.

Table 6: Availability Pair Information

Configuration Data	Description	Your Entry
Availability information	• Primary ExtremeWireless Appliance's IP address • Secondary ExtremeWireless Appliance's IP address • IP address of primary ExtremeWireless Appliance's physical port • IP address of secondary ExtremeWireless Appliance's physical port.	

Mobility Domains Information

Plan out the topology relationship between controllers so as to define the corresponding mobility domain.

Table 7: Mobility Settings Information

Configuration Data	Description	Your Entry
Mobility manager information	If more than one controller is being deployed, it is typically recommended that the inter-controller domain service be set up so as to facilitate ubiquitous roaming across the various APs on the infrastructure. Even when the domain is restricted to two controllers in an availability pair, inter-controller mobility between the two controllers should correspondingly be enabled, especially when deploying services that rely on routed topologies. A mobility domain is characterized by one of the controllers defined as the domain's manager and a set of mobility agents. The manager's role is to aggregate, consolidate and distribute the complete list of user-to-controller mapping so that any domain participant knows which controller may already own the session for a roaming user. The manager may be configured to automatically accept any membership domain requests from agents or may be configured in restricted mode so that the administrator must explicitly approve the registration of a new controller into the mobility domain. • **Port** – The interface of the ExtremeWireless Appliance that is to be used as the mobility manager. Verify that the selected interface is routable on the network. • **Heartbeat** – The time interval (in seconds) at which the mobility manager sends a heartbeat message to the agent. The default is 5.	

Mobility agent information	• **Port** – The interface of the ExtremeWireless Appliance that is to be used as the mobility agent. Verify that the selected interface is routable on the network.
	• **Heartbeat** – The time interval (in seconds) for which the mobility agent waits for the connection establishment response before trying again. The default is 60.
	• **Discovery Method** – The method by which the mobility agent will discover the mobility manager. You have two options:
	  • **SLPD (Service Location Protocol Daemon)** – Enables the discovery of the mobility manager ExtremeWireless Appliance, using SLP. The mobility manager's address must be configured on the network using SLP when selecting this option.
	  • **Static Configuration** – Allows the mobility agent to discover the mobility manager without the SLP support. If you select Static Configuration, use the IP address of the	

Table 7: Mobility Settings Information (continued)

Configuration Data	Description	Your Entry
	ExtremeWireless Appliance that serves as the mobility manager.	

2 Wireless Appliance Configuration

This section provides a high-level overview of the steps involved in the initial configuration of your system:

Step 1. Before You Begin Configuration

Research the type of deployment that is required. For example, SSIDs, security requirements, and filter policies.

Step 2. Prepare the Network

Ensure that the external servers, such as and servers (if applicable) are available and appropriately configured.

Step 3. Install the Controller

Install the ExtremeWireless Appliance. For more information, see the appropriate guide from Related Publications on page 5.

Step 4. Perform the First Time Setup

> **Note**
> Verify that the latest firmware is running on your system by going to the firmware and software link of the Extreme Networks support page at:
> `https://extranet.extremenetworks.com/downloads`
> . If the latest firmware is not running on your system, invoke the upgrade procedures as defined in the *User Guide*.

Perform the first time setup of the ExtremeWireless Appliance on the physical network, which includes configuring the IP addresses of the interfaces on the ExtremeWireless Appliance. For more information on the following topics, see the "System Configuration Overview" section in the *User Guide*.

1   Begin by determining the type of connectivity required between the controller and the switch infrastructure.

    a   Determine which physical interfaces (L2 Port) are going to be connected.

    b   Determine which s are associated with the physical interfaces.

    c   Determine which Service (Virtual) Topologies are going to be offered by the service and which physical interface(s) will carry those VLANs into the switch infrastructure. Ensure that the corresponding switch ports are provisioned to trunk the same set of VLANs. The L2 Port Summary view provides a listing of which VLAN IDs are configured on which port.

2   The topologies corresponding directly to physical (L2) port connectivity are explicitly identified via the "Physical" tag as their mode.

> **Note**
>
> If defining tagged VLANs for topologies, please verify that the same tagged VLAN reference is defined on the connecting switch port.

3   To manage the ExtremeWireless Appliance through the interface, select the Mgmt checkbox on the corresponding Topology profile.

4   Configure the data port interfaces to be on separate VLANs. Ensure also that the tagged versus untagged state is consistent with the switch port configuration.

5   Configure the ExtremeWireless Appliance for remote access, which includes:

    a   Setting up an administration station (laptop) on subnet 192.168.10.0/24. By default, the ExtremeWireless Appliance's Management interface is configured with the static IP address 192.168.10.1.

    b   If you intend to connect the controller to a dedicated management segment, then the default shipping settings of the Admin port (192.168.10.1/24) need to be modified with the correct address. A default gateway to which management traffic associated with the Admin port is forwarded may be specified. See Accessing the Wireless Appliance for the First Time on page 36.

6   Configure the ExtremeWireless Virtual Gateway V2110, which includes:

    a   Determining the IP address range of the virtual switch to which the V2110 management port is connected.

    b   Using the vSphere Client Console window to assign the controller's management port an available IP address on the subnet

    c   Logging onto the V2110 through its web GUI and use the installation wizard to complete the initial setup. See Accessing the Wireless Appliance for the First Time on page 36.

Step 5. Setting System Time

You have the option to manually set the controller's time or use an NTP server to provide a time stamp consistent with a central reference. Controllers that are part of a mobility zone must be configured to use the NTP time stamp. For more information, see "Configure the Network Time Using System Time" section in the Extreme Networks ExtremeWireless Software.

Step 6. Apply the Activation License Key

The activation key:

- Provides the controller with information as to the regulatory domain on which the controller provides service. The regulatory domain restricts the set of operational countries that are available for AP configurations.
- Is registered to the management MAC address of the controller.
- Provides a basic set of operational capacities (dependent on platform). The customer can upgrade the system's base capacity by purchasing additional Capacity Upgrade licenses.

With ExtremeWireless v10.01 and later each controller is licensed in a specific domain. The domain licenses include:

- FCC
- ROW
- MNT
- EGY

The user interface reflects the domain of the controller. The following are use cases for each domain:

- A wireless controller with an FCC license can manage Access Points deployed in the United States, Puerto Rico, or Colombia.
- A wireless controller with a ROW license can manage Access Points deployed in any country *except* the United States, Puerto Rico, Egypt, or Colombia.
- A wireless controller with a EGY license will continue to require ROW hardware, but the license will restrict country selection to Egypt only.
- A wireless controller with a EGY license can manage Access Points deployed in Egypt.

> **Note**
>
> If upgrading from v10.21 with an EGY license, call customer support for assistance.

- A wireless controller with a MNT license can manage only domain-locked Access Points, which are the AP39xx-FCC and the AP39xx-ROW only. The AP39xx-FCC must be deployed in the United States, Puerto Rico, or Colombia. The AP39xx-ROW must be deployed in any country *except* the United States, Puerto Rico, or Colombia.

> **Note**
>
> The AP37xx and AP38xx will NOT be able to connect to a controller licensed in the MNT domain.

> **Caution**
>
> Whenever the licensed region changes on the ExtremeWireless Appliance, all Wireless APs are changed to Auto Channel Select to prevent possible infractions to local RF regulatory requirements. If this occurs, all manually configured radio channel settings are lost.
>
> Installing the new license key (other than EGY) before upgrading prevents the ExtremeWireless Appliance from changing the licensed region, and in addition, manually configured channel settings are maintained. For more information, see the *Maintenance Guide*.
>
> **EGY License exception:** If an appliance that is licensed with ROW or MNT Regulatory Keys is hosting APs inside Egypt or APs outside Egypt, upon upgrade to v10.31.01, the AP radios are disabled. If upgrading from v10.21 with an EGY license, call customer support for assistance.

Step 7. Configure for AP Controller Discovery

Determine the method of AP controller discovery used by the APs to find the controller(s) to which the AP registers to provide network service. The AP supports:

- SLP-DA Discovery: Configure the segment settings for the server that provides IP assignment to the APs to include a reference to the SLP-DA to which controllers are registered. This allows the AP to obtain a list of eligible controllers.
- DNS: Configure the `controller.<network domain>` entry to resolve to the IP address of a specific controller.
- Multicast: Verify that the switching gear and interconnecting VLANs are provisioned so as to allow multicast traffic, and snooping allows for the establishment of multicast trees, allowing the APs to subscribe to SLP-DA server advertisements. The SLP-DA server sends queries to determine the list of registered controllers.

Step 8. Configure Routing

Even if you are using only bridged topologies on your , chances are you will need to access servers, NTP servers, Syslog servers, DNS servers, server for Relay, FTP servers for file and configuration backup management, and admin stations which may be several hops away from the controller. Also, the controller may need to be accessed by stations several hops from the network point of presence.

Routing configuration for the system is therefore strongly recommended and in most cases necessary. At a minimum the next hop default gateway that the controller interacts with to access these services should be defined.

Step 9. Configure the VNS

A is created by binding a particular Service to one or more policies that are applied to wireless stations by default. This mapping can be overridden by authentication or an external interface. The configuration consists of configuring the topologies that represent the method by which user's traffic will be connected to the network.

Policies define the level of access that users are granted, whether users are restricted in the amount of bandwidth available to the user and the specification on which topology represents the user's point and method of network interface. Policies are implicitly assigned by a VNS by way of authentication and default states, or may be explicitly assigned by way of responses to user's authentication (ACCESS-ACCEPT message).

The VNS Creation Wizard on the controller steps you through the service creation and its necessary subcomponents, resulting in a fully resolved set of elements and an active service.

1. Research the service types the system is expected to provide, such as wireless services, encryption types, infrastructure mapping (s), and connectivity points such as switch ports (switch port VLAN configuration and trunks must match the controller's configuration. Then configure the traffic topologies your network must support in order to provide wireless user connectivity to infrastructure resources.

2   You can run the Basic Configuration Wizard to setup controller services such as NTP, Routing, DNS, and RADIUS servers, or you can define necessary infrastructure components such as the RADIUS servers, if CP or AAA services are to be used for user authentication. RADIUS servers are defined via the "VNS Configuration/Global/Authentication" tab.

3   Define the Topologies: Topologies represent the controller point of network attachment, therefore VLANS and port assignments must be coordinated with the corresponding switch ports.

4   Define Policies: Policies are typically bound to topologies. Policy application assigns user traffic to the corresponding network point. Policies define user access rights and reference a user's rate control profile. New definitions can be created in place.

5   Define the : CoS 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 the policy is permitted. The CoS defines actions to be taken when rate limits are exceeded.

6   Define the WLAN service:

   a   Select the set of APs/Radios on which the service is present

   b   Configure the method of wireless user credential authentication for this service (None, Internal, CP, External CP, Guest Portal, or 802.1x[EAP]

7   Create a VNS that binds the WLAN service to the policies that are used for default assignment upon user network attachment.

   For each Bridge Traffic Locally at EWC topology that is created, a tagged or untagged VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding ExtremeWireless Appliance interface must match the correct VLAN.

8   Set up one or more virtual subnetworks on the ExtremeWireless Appliance. For each VNS, configure the following:

   • **Topology** – Select the Topology type and perform the following steps:

Type	Steps
Bridged @ Controller	Specify the VLAN for the interface.
	Select physical port on which VLAN is trunked.
	If L3 presence is desired, specify the IP address and subnet mask.
	Determine whether the controller is the server for the segment; if so, configure DHCP range parameters.
	Determine if the controller provides the DHCP relay for the segment; if so, configure the IP address of DHCP server.
Routed	Specify the IP address and subnet mask.
	Specify the DHCP settings for segment; If this controller is the DHCP server for segment, configure DHCP range parameters. If the controller is providing the DHCP relay for segment, configure the IP address of the DHCP Server
Bridged	Configure as untagged, or specify a tag in the range 1-4094.
	Specify the VLAN ID for tagging at the AP.

   • **Policy** – Select the topology that represents the network point of attachment associated with the policy and configure filtering:

      • Define user network access policy.

- Determine if filtering is to be performed solely at the controller or whether it will also be performed at the AP (for Routed and Bridged @ controller (EWC) Topologies only).
- Determine whether bandwidth restrictions are imposed for users of this policy (default unlimited). Configure rate control if bandwidth restrictions are imposed.
- **Class of Service** – Class of Service (CoS) can be assigned to a packet by a filter rule that the packet matches or by the policy itself, and is used to control how a packet is handled when the network is busy. Class of Service specifies the following for affected traffic:
  - Maximum throughput rates (rate limits)
  - Transmit queue assignments, which determines how quickly the packet is forwarded, relative to other competing traffic.
  - Priority remarking behavior, which affects the priority downstream switches and routers give to the packet.
- The CoS defines actions to be taken when rate limits are exceeded. All incoming packets may follow these steps to determine a CoS:
  - Each incoming packet is matched against a set of administrator defined rules to find the first matching rule that assigns a CoS. If no matching rule that assigns a CoS is found a default CoS is assigned, based on the applied policy.
  - Apply new marking to the packet in accordance with the markings defined in the applied CoS.
  - Determine whether the packet will cause the station to exceed the rate limit assigned by the CoS. If so, the packet is dropped.
  - If the packet is not dropped, select the transmit queue that is used to forward the packet, based on the CoS.
- **WLAN Service**
  - Select the type of service to provide. Select Standard service to provide network access for wireless devices. Define the SSID that is advertised by APs representing this service (The SSID that clients see on RF scans).
  - Select the AP radios (radios correspond to Band [2.4 GHz, 5 GHz]) that advertise this service.
  - Select the method of authentication that users must successfully pass in order to gain network access:

Authentication Method	Steps
MBA (MAC address based authentication)	Device MAC address must be explicitly allowed to register by RADIUS server.
Captive Portal	
Internal	Configure presentation parameters for Captive Portal authentication page.
External	Configure connectivity parameters for interaction with external authentication server.
Guest Portal	Define the set of user credentials that will be granted access to the service.
RADIUS Accounting	Define the RADIUS accounting server to which interim usage accounting reports shall be sent.

- Privacy: Select and configure the wireless security method for the service (None, WEP, WPA-PSK, DynWep, WPA/EAP).
- : Configure QoS behavior definitions related to remapping of packet priority.
- VNS
  - Select the WLAN service that the VNS represents.
  - Configure the Default Non-Auth Policy by selecting the policy to which users are initially assigned upon association to the service.
  - Configure the Default Auth Policy by selecting the policy to which users are re-assigned upon successful completion of authentication steps (default behavior simply maps to Default Policy, so no specific transition occurs on straight authentication). The policy referenced by this setting is applied unless the RADIUS server provides a specific indication of a more specific policy via Login-Lat-Group and/or FilterID attributes.

Provisioning the VNS mapping between the WLAN service and the default policies enables the service to be advertised (unless WLAN service explicitly provisioned in disabled state).

Step 10. Install, Register, and Assign APs to the VNS

1. Deploy Wireless APs to their corresponding network locations.
2. If desired, change the default AP template for common radio and assignment, whereby APs automatically receive complete configuration. For typical deployments where all APs are to have the same configuration, this feature expedites deployment, as an AP automatically receives full configuration (including service assignment) upon initial registration with the ExtremeWireless Appliance. If applicable, modify the properties or settings of the Wireless APs.
3. Configure the "Registration mode" that governs how the APs become approved for service with the controllers:

Registration Mode	Description
Automatic approval	The AP discovery process automatically approves the AP so that it becomes eligible to provide service in connection with this controller's configuration.
Restricted Access	APs discovering the controller are not automatically approved but rather held in a state "pending" administrator explicit approval. This setting is highly recommended when several controllers may be available for connectivity, such as Mobility Domains or Availability pairs, as it allows the administrator to define which controller is the master point of configuration (Home) for the particular AP.

4. If a default AP configuration template is defined with WLAN service assignment, an approved AP is automatically assigned to such services.
5. Once the Wireless APs are powered on, they automatically begin the discovery process of the ExtremeWireless Appliance.

3 Accessing the Wireless Appliance for the First Time

**Wireless Controllers C5210, C5110, C4110, C25, C35 and V2110
Management Port Interface**

Configuring the Wireless Appliance's management port is an optional step. If you do not intend to connect your enterprise network to the controller management port, you can skip the following procedure and instead retain the default IP address of the controller's management port.

Wireless Controllers C5210, C5110, C4110, C25, C35 and V2110

The controller platforms have an admin port for dedicated administrative access. They create the IP address and Gateway address for the Admin topology on the controller/gateway. The Admin topology is a default physical topology that references the physical admin port.

Change the controller's management port and Gateway IP addresses using the Command Line Interface (CLI) so that the GUI can be accessed from a browser on the administrator's workstation. After that, the controller or V2110 can be accessed via CLI (ssh) or GUI (ssl) for configuration.

ExtremeWireless Appliance GUI via Ethernet

Use a laptop computer with a web browser. Connect the supplied cross-over Ethernet cable between the laptop and management Ethernet interface of the ExtremeWireless Appliance to perform configuration via the ExtremeWireless Assistant GUI.

CLI Commands via Null Modem

Use a console supporting VT100 emulation, attached to the DB9 serial port (COM1 port) of the ExtremeWireless Appliance via a cross-over (null modem) cable. Use the CLI commands to define IP addresses for the admin interface and gateway:

1 At the root level, enter the **topology** context:
   `EWC.extremenetworks.com# topology`
2 Enter the **Admin** context (Admin is a pre-defined topology-name):
   `EWC.extremenetworks.com:topology# Admin`
3 Enter the **Layer 3** context: (note that the first character of the command is an "l", as in "Layer"):
   `EWC.extremenetworks.com:topology:Admin# l3`
4 Enter the IP address for the admin interface with the `ip` command:
   `EWC.extremenetworks.com:topology:Admin:l3# ip <ipv4 address>/<CIDR>`
5 Enter the IP address for the gateway to the admin interface with the `gateway` command:
   `EWC.extremenetworks.com:topology:Admin:l3# gateway <ipv4 address of gateway>`
6 Apply the ip and gateway command inputs with the `apply` command:
   `EWC.extremenetworks.com:topology:Admin:l3# apply`

For more information about CLI commands and syntax, see the *CLI Guide*.

Virtual Gateway V2110

You cannot access the ExtremeWireless V2110 Virtual Gateway using a laptop and a back-to-back wired connection. The admin interface must be given an IP address for the virtual network inside the vSphere server. Use the vSphere console to log in to the controller CLI and use CLI commands to define IP addresses for the admin interface and gateway:

1 At the root level, enter the **topology** context:
   ```
   EWC.extremenetworks.com# topology
   ```
2 Enter the **Admin** context:
   ```
   EWC.extremenetworks.com:topology# Admin
   ```
3 Enter the **Layer 3** context (note that the first character of the command is a lowercase "L", as in "layer"):
   ```
   EWC.extremenetworks.com:topology:Admin# l3
   ```
4 Enter the IP address for the admin interface with the `ip` command:
   ```
   EWC.extremenetworks.com:topology:Admin:l3# ip <ipv4 address>/<CIDR>
   ```
5 Enter the IP address for the gateway to the admin interface with the `gateway` command:
   ```
   EWC.extremenetworks.com:topology:Admin:l3# gateway <ipv4 address of gateway>
   ```
6 Apply the ip and gateway command inputs with the `apply` command:
   ```
   EWC.extremenetworks.com:topology:Admin:l3# apply
   ```

For more information about CLI commands and syntax, see the *CLI Guide*.

Management Port Interface

The management port on the ExtremeWireless Appliance may be labeled differently depending on the ExtremeWireless Appliance.

Table 8: Management Port Label on the Wireless Appliance

Wireless Appliance	Management Port Label
C5210	Gb 1
C5110	Gb 1
C4110	Gb 1
C25	1 GbE
C35	1 GbE

Accessing the Wireless Appliance with a Web-enabled Laptop

1 Statically assign an unused IP address in the 192.168.10.0/24 subnet for the Ethernet port of the laptop computer.

   You can use any IP address from 192.168.10.2 to 192.168.10.254.

2   Connect the ExtremeWireless Appliance's management port to the web-enabled laptop computer with a cross-over RJ45 Ethernet cable.

> **Note**
> The IP address of the ExtremeWireless Appliance's management port is 192.168.10.1.

3   Launch your web browser and type `https://192.168.10.1:5825` in the address bar.

The Wireless Assistant login screen displays.
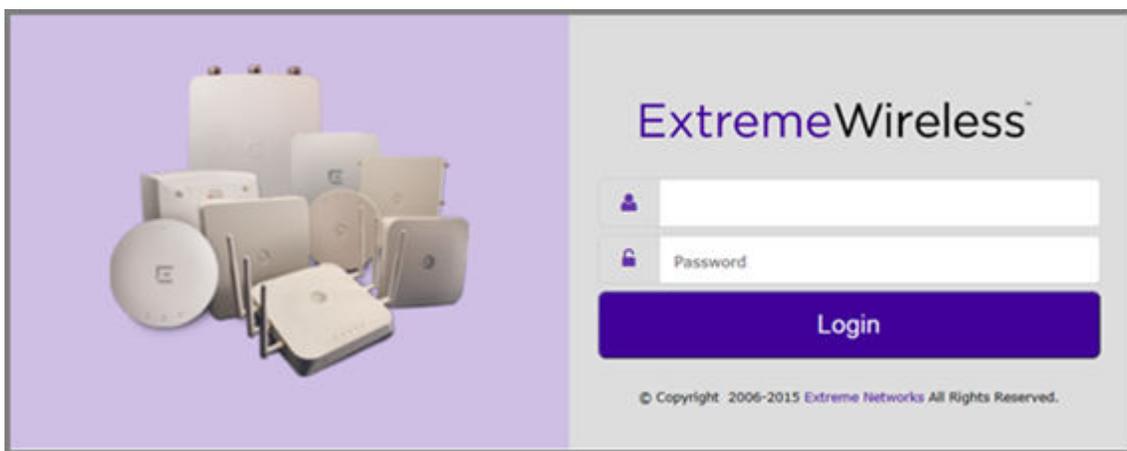
4   Enter the credentials:

User Name: `admin`

Password: `abc123`

5   Click **Login**.

The `Wireless Assistant Home` screen displays.

4 Working with the Basic Installation Wizard

The Extreme Networks ExtremeWireless Software system provides a basic installation wizard that can help administrators configure the minimum ExtremeWireless Appliance settings that are necessary to deploy a fully functioning ExtremeWireless Appliance on a network.

Administrators can use the basic installation wizard to quickly configure the ExtremeWireless Appliance for deployment, and then once the installation is complete, continue to revise the ExtremeWireless Appliance configuration accordingly.

The basic installation wizard is automatically launched when an administrator logs on to the ExtremeWireless Appliance for the first time, including if the system has been reset to the factory default settings. In addition, the basic installation wizard can also be launched at any time from the left pane of the ExtremeWireless Appliance Configuration screen.

To configure the ExtremeWireless Appliance with the Basic Installation Wizard:

1 Log on to the ExtremeWireless Appliance.

For more information, see

2 From the main menu, click **Controller**, and then click **Administration** > **Installation Wizard**.

The **Basic Installation Wizard** screen is displayed.

3   In the Time Settings section, configure the Wireless Appliance timezone:

- **Continent or Ocean** – Click the appropriate large-scale geographic grouping for the time zone.
- **Country** – Click the appropriate country for the time zone. The contents of the drop-down list change, based on the selection in the Continent or Ocean drop-down list.
- **Time Zone Region** – Select the appropriate time zone region for the selected country from the drop-down menu.

4   To configure the Wireless Appliance's time, do one of the following:

- To manually set the ExtremeWireless Appliance time, click **Set time** and specify values for the Year, Month, Day, HR, and Min.

  To use the ExtremeWireless Appliance as the NTP time server, select **Run local NTP Server**. In the Server field, enter the IP address or Domain Name for the NTP server.

- To use NTP to set the ExtremeWireless Appliance time, select **Use NTP**, and then type the IP address of an NTP time server that is accessible on the enterprise network.

  The Network Time Protocol is a protocol for synchronizing the clocks of computer systems over packet-switched data networks.

> **Note**
> The Server Address field supports both IPv4 and IPv6 addresses.

5   You can configure up to three DNS servers. The Server Address field supports both IPv4 and IPv6 addresses. In the Topology Configuration section, the physical interface of the Wireless Appliance data port, the IP Address and Netmask values for the data port, and the ID display as read-only values.

For information on how to obtain a temporary IP address from the network, click **How to obtain a temporary IP address**.

6 Click **Next**.

The **Management** screen displays.

7 In the AP Password section, enter a password for the AP. Click **Unmask** to display the password characters as you type. Access Points are shipped with default passwords. You must create a new SSH Access Password here.

> **Note**
>
> Passwords *can* include the following characters: A-Z a-z 0-9 ~!@#$%^&*()_+|-=\{}[];<>?,.
> Password *cannot* include the following characters: / ` ' " : or a space.

8 In the Management Port section, confirm the port configuration values that were defined when the Wireless Appliance was physically deployed on the network. If applicable, edit these values:

- **Static IP Address** — Displays the IPv4 address for the ExtremeWireless Appliance's management port. Revise this as appropriate for the enterprise network.
- **Netmask** — Displays the appropriate subnet mask for the IP address to separate the network portion from the host portion of the address.
- **Gateway** — Displays the default gateway of the network.
- **Static IPv6 Address** — Displays the IPv6 address for the ExtremeWireless Appliance's management port. Revise this as appropriate for the enterprise network.
- **Prefix Length** — Length of the IPv6 prefix. Maximum is 64 bits.
- **Gateway** — Displays the default gateway of the network.

9   In the section, click **V2c** or **V3** in the Mode drop-down list to enable SNMP, if applicable.

If you selected V2c, the Community options display:

- **Read Community** — Type the password used for read-only SNMP communication.
- **Write Community** — Type the password used for write SNMP communication.
- **Trap Destination** — Type the IP address of the server used as the network manager that receives SNMP messages.

If you selected V3, the Syslog Server options display:

- **Enable** — Click in the box to enable Syslog Server.
- **IP Address** — Enter the IP address for the Syslog Server.

10 In the OSPF section, select the **Enable** checkbox to enable OSPF, if applicable.

Use OSPF in a routed to allow the ExtremeWireless Appliance to participate in dynamic route selection. OSPF is a protocol designed for medium and large IP networks with the ability to segment routes into different areas by routing information summarization and propagation.

- **Area ID** — Type the area. 0.0.0.0 is the main area in OSPF.

11 In the Syslog Server section, select the **Enable** checkbox to enable the syslog protocol for the ExtremeWireless Appliance, if applicable. Syslog is a protocol used for the transmission of event notification messages across networks.

12 In the IP Address box, type the IP address of the syslog server and then click **Next**.

The **Services** screen displays.

13 In the section, select the **Enable** checkbox to enable RADIUS login authentication, if applicable.

RADIUS login authentication uses a RADIUS server to authenticate user login attempts. RADIUS is a client/server authentication and authorization access protocol used by a network access server (NAS) to authenticate users attempting to connect to a network device.

- **Server Alias** — Type a name that you want to assign to the RADIUS server.
- **IP Address** — Type the RADIUS server's IP address.
- **Shared Secret** — Type the password that is used to validate the connection between the Wireless Appliance and the RADIUS server.

14 In the Mobility section, select the **Enable** checkbox to enable the ExtremeWireless Appliance mobility feature, if applicable. Mobility allows a wireless device user to roam seamlessly between different Wireless APs on different appliances.

A dialog displays, informing you that NTP is required for the mobility feature and prompting you to confirm you want to enable mobility.

> **Note**
>
> If the Wireless Appliance is configured as a mobility agent, it acts as an NTP client and uses the mobility manager as the NTP server. If the Wireless Appliance is configured as a mobility manager, the Wireless Appliance's local NTP is enabled for the mobility domain.

15 Click **OK** to continue, and then do the following:

- **Role** — Select the role for the ExtremeWireless Appliance, Manager or Agent. One appliance on the network is designated as the mobility manager and all appliances are designated as mobility agents.
- **Port** — Click the interface on the ExtremeWireless Appliance to be used for communication between mobility manager and mobility agent. Verify that the selected interface is routable on the network.
- **Manager IP** — Type the IP address of the mobility manager port if the appliance is configured as the mobility agent.

16 In the Default VNS section, select the **Enable** checkbox to enable a default VNS for the appliance.

The default VNS parameters display.

17 Click **Next**.

The **Success** screen displays.

18 Change the factory default administrator password. Enter the new password and confirm it, and then click **Save**.

19 Click **OK**, and then **Close**.

The **ExtremeWireless Assistant** main menu screen displays.

Note

The appliance reboots after you click **Save** if the time zone is changed during the Basic Install Wizard. If the IP address of the management port is changed during the configuration with the Basic Install Wizard, the ExtremeWireless Assistant session is terminated and you will have to log back in with the new IP address.

---

5 Connecting the Wireless Appliance to the Enterprise Network

1 Disconnect your laptop computer from the Wireless Appliance management port.
2 Connect the Wireless Appliance management port to the enterprise Ethernet LAN. The Wireless Appliance resets automatically.
3 Log on to the Wireless Assistant from any computer on the enterprise network. Type the following URL in a browser to access the Wireless Assistant: `https://<IP Address>:5825`

6 Configuring the Wireless Appliance for the First Time

Some Wireless Appliance configuration is typically performed as soon as the Wireless Appliance is deployed.

Although the basic installation wizard has already configured some aspects of the Wireless Appliance deployment, you can continue to revise the ExtremeWireless Appliance configuration according to your network needs.

For more information on the following topics, see the *User Guide*.

- Changing the administrator passwords
- Configuring the network time
- Applying license keys
- Configuring physical topology
- Configuring Wireless APs
- Configuring the list of servers
- Configuring DNS settings/list of DNS servers (if necessary)
- Configuring Syslog server (if necessary to dynamically upload log messages/event occurrences on the controller)
- If required, configuring Agent access parameters
- Configuring controller network identification, including hostname and domain
- Configuring VNSs
- Configuring topologies the controller services represent
- Configuring policy parameters for user network access
- Configuring services and AP membership
- Configuring the set of VNSs mapping WLAN services to policies for default assignment
- Configuring availability
- Configuring mobility

7 Configuring DHCP, NPS, and DNS Services

This chapter describes how to configure and DNS (Domain Name System) services on a Windows Server 2012 R2 or Linux server for use by ExtremeWireless Appliance and APs. In addition, the chapter explains how to configure Network Policy Server (NPS) service on Windows Server 2012 R2. Use the configuration processes in this chapter as a reference when configuring services.

Note

Windows Server 2012 R2 or Linux server may have a different configuration process than what is described here. Refer to your manufacturer's documentation for the configuration process that is specific to your server.

This section includes the following procedures:
- DHCP Service Configuration on page 48
- NPS Service Configuration on page 65
- DNS Service Configuration on page 71

DHCP Service Configuration

Before you can configure the service, you must install it on the server. You can configure DHCP on Windows Server 2012 R2 or on a Red Hat Linux server.

This section includes the following procedures:
- Configuring DHCP on Windows Server 2012 R2 on page 48
- Configuring DHCP on a Red Hat Linux Server on page 62

Configuring DHCP on Windows Server 2012 R2

Install either during the initial installation of Windows Server 2012 R2 or after the initial installation is completed.

When you configure DHCP for ExtremeWireless LAN () solution, you can include 078 SLP DA Option.

You must enable 078 SLP DA Option for every scope you define. A scope is a collection of IP addresses meant to be distributed by the DHCP server to the client devices on a subnet. The SLP DA is used by:
- The Wireless APs to discover the ExtremeWireless Appliance.

- The mobility agents to discover the mobility manager.

> **Note**
>
> You may visit http://support.microsoft.com for instructions on how to install DHCP.

Configure DHCP option 43 for ExtremeWireless Appliance discovery when there is a need for a specific AP platform to connect to a specific controller.

For more information, see:

- Creating Option 78 on page 49
- Configuring Option 78 on page 49
- DHCP Option 43 on Windows Server 2012 R2 on page 53

Creating Option 78

To create option 78 as a byte array, perform the following steps:

1 Click **Start** > **Administrative Tool** > **DHCP**
2 Right-click the server node, and select **Set predefined options**.
3 Select **Add**, and type a name for the option, for example "SLP DA".
4 Set the data type to **Byte**, and select the **Array** checkbox.
5 In the Code field, type 78.
6 Type a description for the option, for example, "Extreme Networks SLP Discovery", and then select **OK**.

Figure 2: Option Type

Configuring Option 78

To configure on Windows Server 2012 R2:

1 Click **Start** > **Administrative Tool** > **DHCP**.
2 In the console tree, right-click the DHCP server, IPv4 on which you want to create the new DHCP scope, and then click **New Scope**.
3 Click **Next**.

4   In the Name and Description text boxes, type the scope name and description.

This can be any name that you want, but it should be descriptive enough so that you can identify the purpose of the scope on your network.

5   Click **Next**.

The `IP Address Range` window is displayed.

Figure 3: IP Address Range

6   In the Start IP address and the End IP address text boxes, type the start and end of the IP address range that you want to be distributed to the network.

You must use the range provided by your network administrator.

7   In the Length text box, type the numeric value of the subnet mask bits, or in the Subnet mask text box, type the subnet mask IP address.

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address. You must use the Length (or the Subnet mask) provided by your network administrator.

8   Click **Next**.

The `Add Exclusions` window displays.

9   In the Start IP address and the End IP address text boxes, type the start and end of the IP address range that you want to exclude from the distribution.

You must use the exclusion range provided by your network administrator.

10 Click **Next**.

The **Lease Duration** window displays.

The DHCP server assigns a client an IP address for a given amount of time. The amount of time for which the IP address can be leased is defined in the Lease Duration window.

11 In the Days, Hours and Minutes text box, type the lease duration.

You must use the Lease Duration as specified by your network administrator.

12 Click **Next**.

The **Configure DHCP Options** window displays.

13 Select **Yes, I want to configure these options now**, and then click **Next**.

The **Router (Default Gateway)** window displays.

14 In the IP address text box, type the network's default gateway and click **Add**.

You must use the default gateway provided by your network administrator.

Figure 4: Router Default Gateway

15 Click **Next**.

The `Domain Name and DNS Servers` window displays.

Figure 5: Domain Name and DNS Servers

16 In the Parent domain text box, type your company's domain name.

You must use the Parent Domain provided by your network administrator.

17 In the Server name text box, type your server name.

You must use the server name provided by your network administrator.

18 In the IP address text box, type your server's IP address, and then click **Add**.

19 Click **Next**.

The `WINS Servers` window displays.

20 Click **Next**.

The `Activate Scope` window displays.

21 Select **Yes, I want to activate this scope now**, and click **Next**.

The wizard displays the following message:
`You have successfully completed the New Scope wizard.`

22 Click **Finish**.

23 Click **Start** > **Administrative Tool** > **DHCP**.

The DHCP console tree displays.

24 Right-click **Server Options** in the tree and select **Configure Options**.
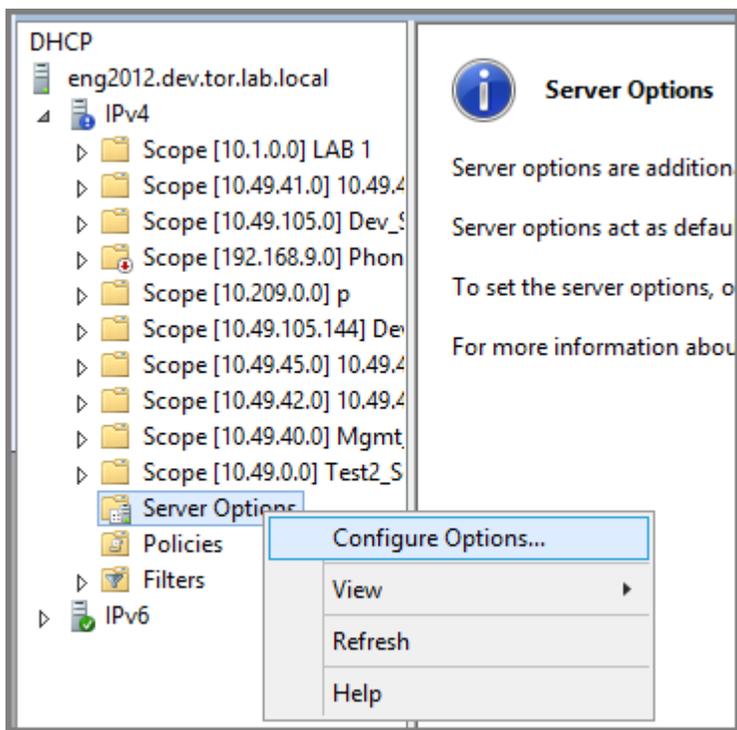
Figure 6: Configure Options

The **Server Options** dialog displays.

25 On the General tab, enable 078 SLP DA.

26 In the lower pane of the screen, type the dotted decimal values of the SLP DA's IP address.

The Wireless APs use the SLP DA to discover the ExtremeWireless Appliance.

The mobility agents use the SLP DA to discover the mobility manager.

> **Note**
>
> If there is no SLP deployment on the enterprise network, the ExtremeWireless Appliance is configured to act as a DA by default. If you put the appliance's IP address(es) in a DHCP server for Option 78, Wireless APs will interact with the appliance for discovery.
>
> Similarly, the mobility agents also interact with the ExtremeWireless Appliance to discover the mobility manager.

DHCP Option 43 on Windows Server 2012 R2

This section describes how to configure the Microsoft server to use DHCP option 43 for ExtremeWireless Appliance discovery. In the discovery process, the DHCP server returns vendor-specific information to the client as option 43. You must supply the following information to configure DHCP option 43:

- **Vendor Class Identifier (VCI)** — The VCI for an Extreme Networks AP is HiPath <AP model name>.

For example, the VCI for the Extreme Networks AP3965e is HiPath AP3965. The following table lists the Vendor Class Identifiers for each Extreme Networks AP model.

Table 9: AP Vendor Class Identifiers

AP Model	Vendor Class Identifier
AP3705i	HiPath AP3705
AP3710i	HiPath AP3710
AP3710e	HiPath AP3710
AP3715i	HiPath AP3715
AP3715e	HiPath AP3715
AP3765i	HiPath AP3765
AP3765e	HiPath AP3765
AP3767e	HiPath AP3767
AP3825i	HiPath AP3825
AP3801i	HiPath AP3801
AP3805i	HiPath AP3805
AP3805e	HiPath AP3805
AP3825e	HiPath AP3825
AP3865e	HiPath AP3865
AP3912i	HiPath AP3912
AP3916ic	HiPath AP3916
AP3935i	HiPath AP3935
AP3935e	HiPath AP3935
AP3965i	HiPathAP3965
AP3965e	HiPath AP3965

- **Option 43 sub-option code** — The option 43 sub-option code for the Extreme Networks APs is type 1 (0x1).
- IP addresses of ExtremeWireless Appliances

Configuring Option 43

To configure option 43 using the Windows Server 2012 R2 DHCP, IPv4 server utility:

1 In the DHCP server utility, right-click the DHCP server icon and choose **Define Vendor Classes**.

You will create a new vendor class to program the DHCP server to recognize the VCI **ExtremeWireless** *<AP model name>*.
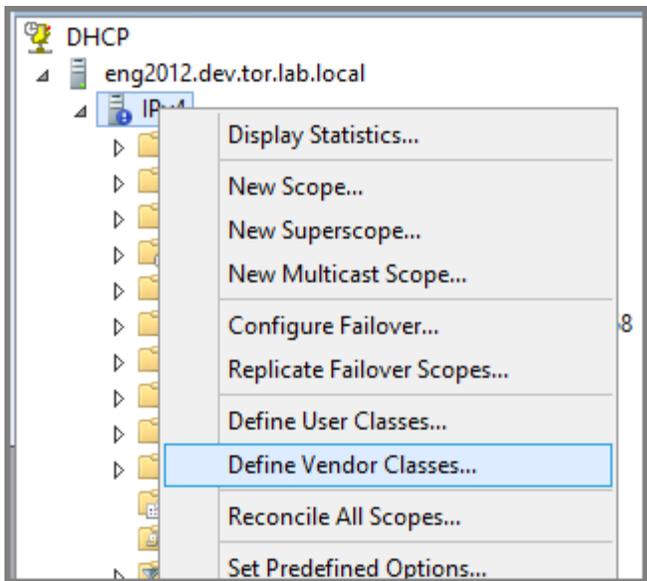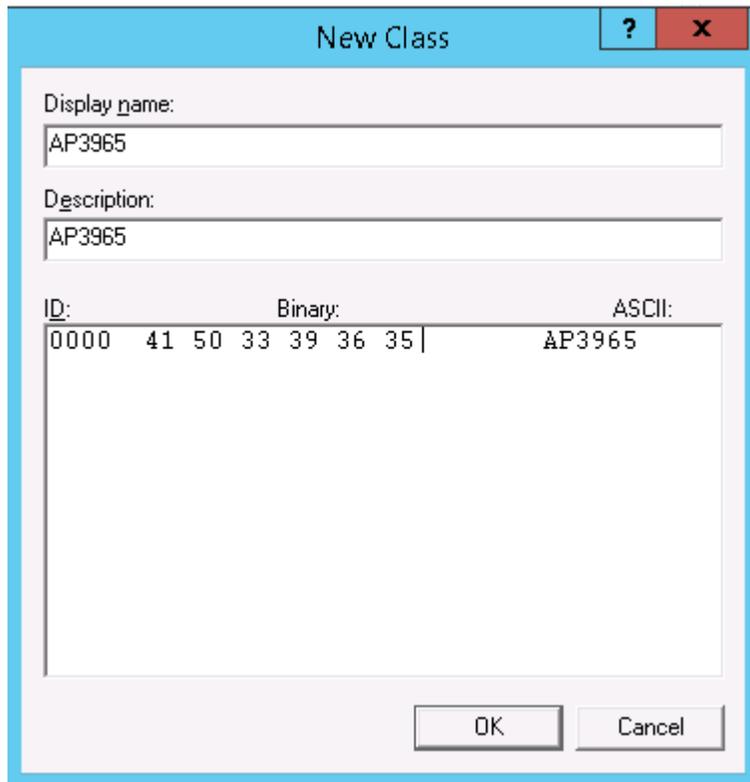
Figure 7: Define Vendor Classes

The **DHCP Vendor Classes** window displays.
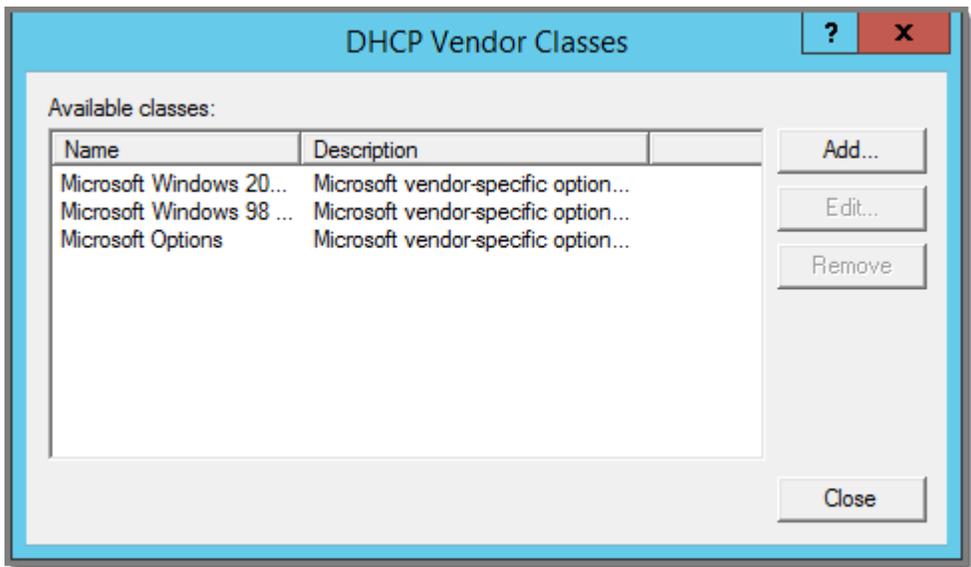
Figure 8: DHCP Vendor Classes

2   Click **Add** to create the new class.

The **New Class** window displays.

Figure 9: New Class

3   In the Display name field, enter a name. In this example, AP3965 is used as the display name.

4   In the Description field, enter a short description of the vendor class: AP3965.

5   Add the Vendor Class Identifier string. Click the ASCII field, and enter the appropriate value (for example, AP3965).

6   Click **OK**.

The new class is created.
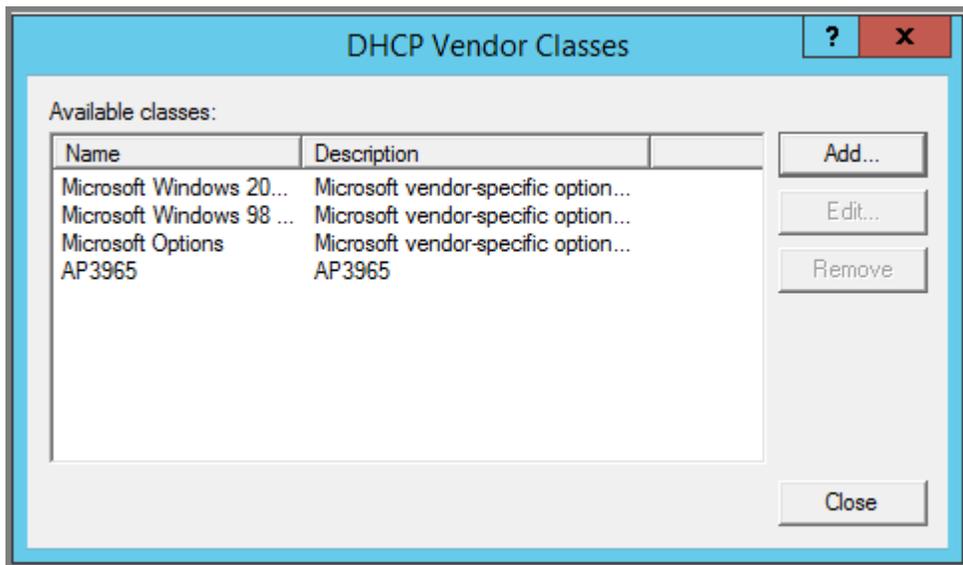
Figure 10: DHCP Vendor Classes

7   Click **Close**.

8   In the DHCP server, IPv4 utility, right-click the server icon and select **Set Predefined Options** to add an entry for the controller sub-option for the newly created vendor class.

The sub-option code type and the data format is used to deliver the vendor specific information to the APs.
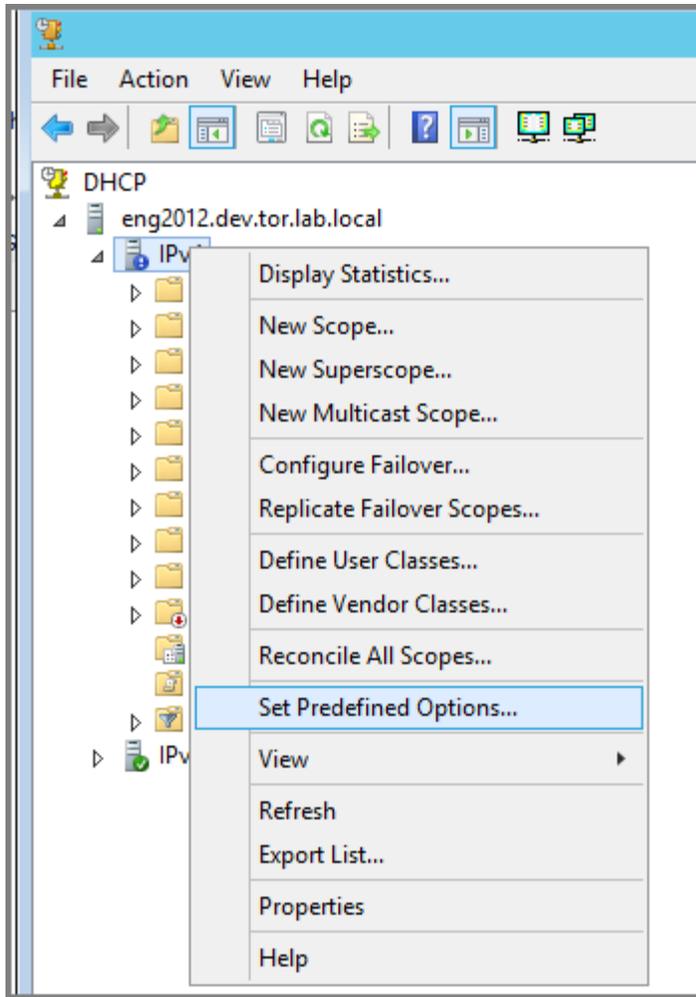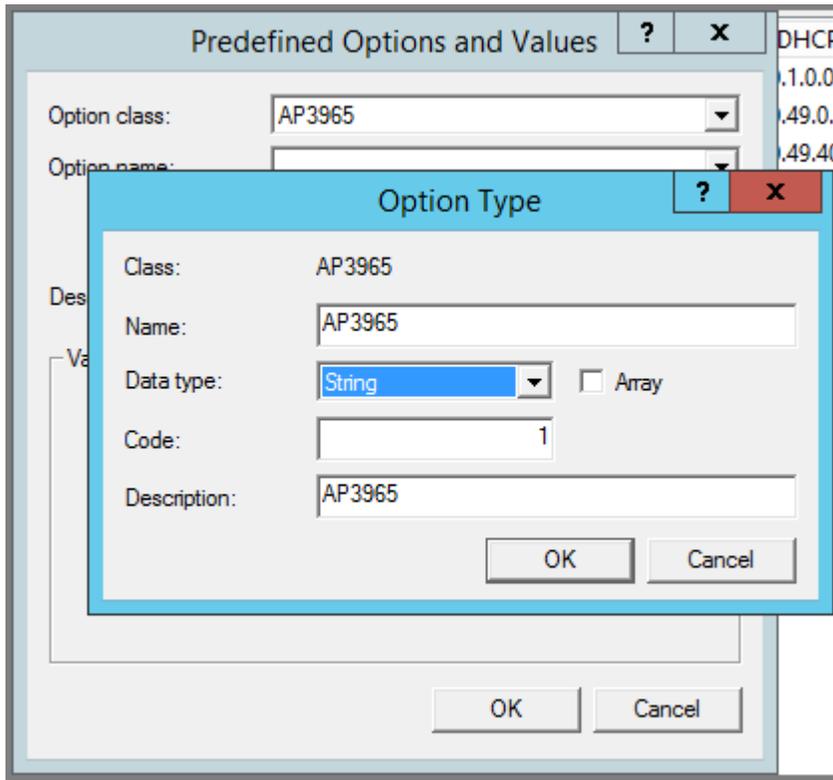
Figure 11: Set Predefined Options
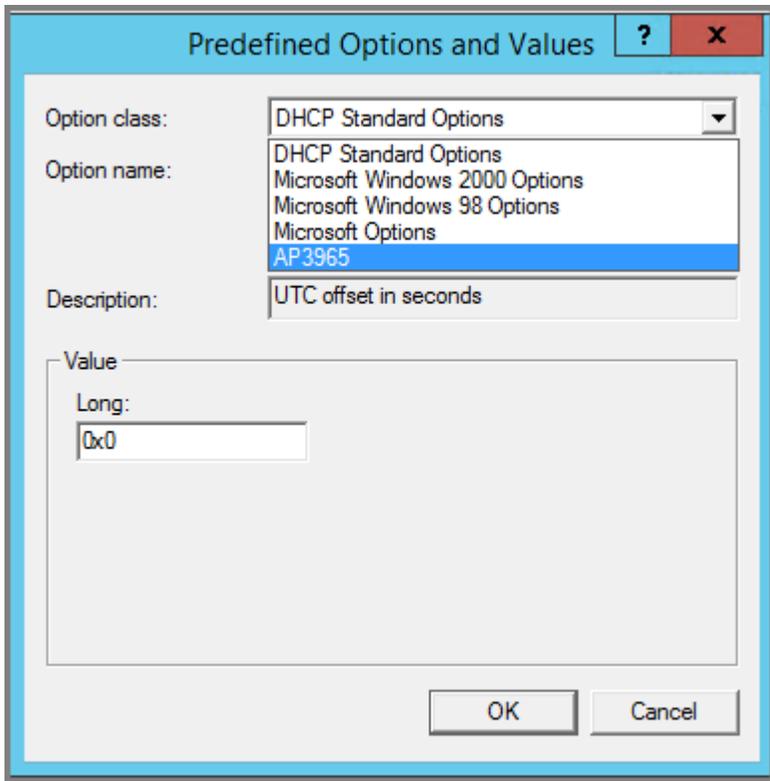
Figure 12: Predefined Options and Values

9 In the Option class field, select the value you configured for the vendor class and click **Add**.

The **Option Type** window displays.

Figure 13: Option Type

10 Enter a value in the Name field.

11 In the Data type field, select **String**.

12 In the Code field, enter the sub-option value 1.

13 Enter a description in the Description field (Optional).

14 Click **OK**.

The new predefined option is displayed in the **Predefined Options and Values** window.

15 Click **OK**.

You have created the vendor class and sub-option type needed in order to support controller discovery.

Configuring Server Options

1   In the server utility, right-click the **Server Options** folder under the DHCP scope, and select **Configure Options**.
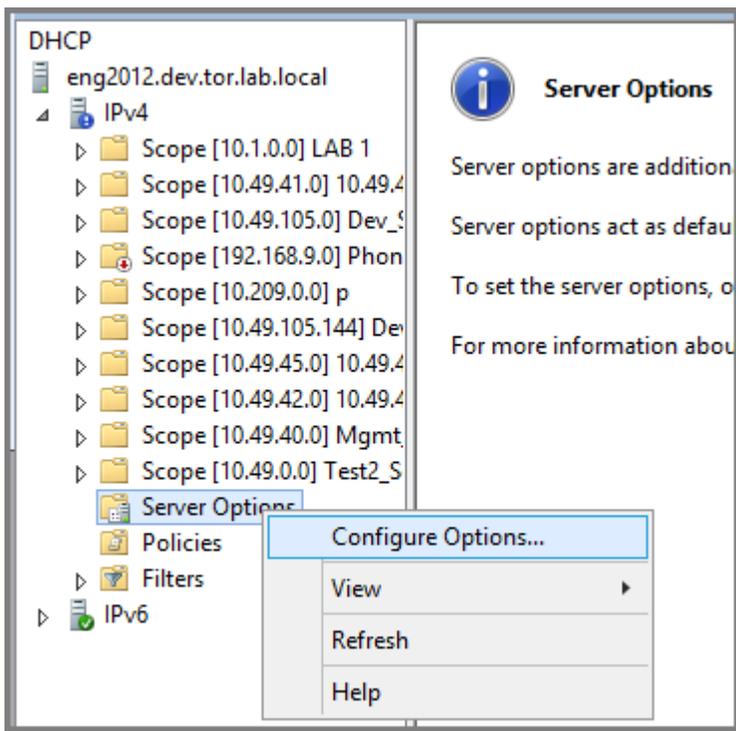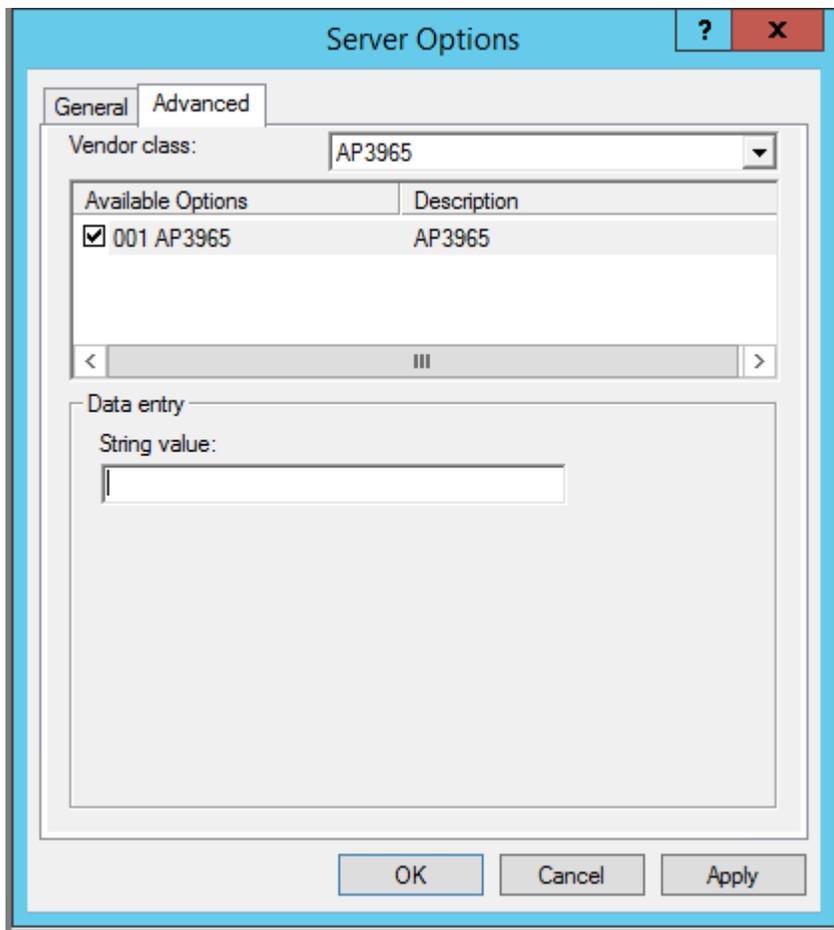

Figure 14: Configure Options

The Server Options window displays.

2 Click the **Advanced** tab and configure the following parameters:

- Vendor Class. Select the vendor class that you plan to use. For example, AP3965.
- Available Options. Select the predefined 001 sub-option to assign to this scope.
- Data Entry. Enter the controller IP addresses to return to the APs. This is a comma-delimited list.

Figure 15: Server Options

3 Click **OK**.

DHCP Option 43 is now configured. This DHCP option is available for all the DHCP scopes that are configured in the DHCP server. When an AP requests vendor specific information, the DHCP server sends the ExtremeWireless Appliance IP addresses in Option 43 to the AP.

Configuring DHCP on a Red Hat Linux Server

You can configure a server using the configuration file `/etc/dhcpd.conf`.

DHCP also uses the file /var/lib/dhcp/dhcpd.leases to store the client lease database.

The first step in configuring a DHCP server is to create the configuration file that stores the network information for the clients. Global options can be declared for all clients, or options can be declared for each client system.

The configuration file can contain any extra tabs or blank lines for easier formatting. The keywords are not case-sensitive and lines beginning with a hash mark (#) are considered comments.

To use the recommended mode, add the following line to the top of the configuration file:

```
ddns-update-style interim;
```

Read the dhcpd.conf man page for details about the different modes.

There are two types of statements in the configuration file:
- Parameters – State how to perform a task, whether to perform a task or what networking configuration options to use to send to the client.
- Declarations – Describe the Topology of the network, describe the clients, provide addresses for the clients, or apply a group of parameters to a group of declarations.

Some parameters must start with the option keyword and are referred to as options. Options configure DHCP options; whereas, parameters configure values that are not optional or control how the DHCP server behaves.

Parameters (including options) declared before a section enclosed in curly brackets {} are considered global parameters. Global parameters apply to all the sections below it.

> **Note**
> If you change the configuration file, the changes will not take effect until you restart the DHCP daemon with the command service dhcpd restart.

The following is an example of a DHCP configuration on a Red Hat Linux server.

For Wireless AP Subnet

```
subnet 10.209.0.0 netmask 255.255.255.0 {
option routers 10.209.0.2; ### This is the network's default gateway address.
option subnet-mask 255.255.255.0
option domain-name xyznetworks.ca
option domain-name servers 192.168.1.3, 207.236, 176.11
range 10.209.0.3 10.209.0.40;
default-lease-time 7200000 ###The figures are in seconds.
option slp-directory-agent true 10.209.0.1, 10.209.0.3; ####The Wireless APs
use the SLP DA to discover the ExtremeWireless Appliance, and the mobility
agents use it to discover the mobility manager.
authoritative;
```

Configuring DHCP Option 43 on a Linux Server

This section describes the configurations necessary on the Linux server to use DHCP option 43 for ExtremeWireless Appliance discovery. Option 43 requires the following information:
- Vendor Class Identifier (VCI) — The VCI for an ExtremeWireless AP is HiPath <AP model name>. Table 9 on page 54 lists the Vendor Class Identifiers for Extreme Networks APs.
- Option 43 sub-option code — The option 43 sub-option code for the ExtremeWireless APs is type 1 (0x1).
- IP addresses of ExtremeWireless Appliances

To configure the vendor encapsulated option on a Linux server, you must do the following:
- Define an option space.
- Define some options in that option space.

- Provide values for the options.
- Specify that this option space should be used to generate the vendor-encapsulated-options option.

To configure DHCP option 43:

1   Modify the dhcp.conf file (modifications are in bold).
```
[root@localhost ~]# vim /etc/dhcpd.conf
authoritative;
ddns-update-style interim;
ignore client-updates;
option space HAP;
option HAP.HWC code 1 = text;

subnet 10.100.1.0 netmask 255.255.255.0 {
range 10.100.1.10 10.100.1.254;
option subnet-mask 255.255.255.0;
option slp-directory-agent false 10.1.100.11;
option domain-name-servers 10.100.1.2;
option domain-name "bpmgmt.com";
option routers 10.100.1.1;
default-lease-time 40000;
}
…
subnet 10.100.4.0 netmask 255.255.255.0 {
range 10.100.4.100 10.100.4.254;
option subnet-mask 255.255.255.0;
option slp-directory-agent false 10.100.4.46, 10.100.4.47;
option domain-name-servers 10.100.1.2;
option domain-name "bpmgmt.com";
option routers 10.100.4.1;
default-lease-time 40000;
class "HAP" {
match option vendor-class-identifier;
}
subclass "HAP" "AP3935" {
vendor-option-space HAP;
option HAP.HWC "10.100.2.36, 10.100.2.22";
}
```
2   Restart the DHCP server.
```
[root@localhost ~]# /etc/init.d/dhcpd restart
```

Configuring the ExtremeWireless Appliance as an NPS Client

1   Click **Start** > **Administrative Tools** > **Network Protocol Server**.

2   Expand **RADIUS Clients and Servers**, right-click **RADIUS Clients**, and then click **New**.

The dialog apprears.

3 Configure the following parameters:

- Friendly name. Type the name that you want to assign to the ExtremeWireless Appliance
- Client address (IP or DNS). Type the IP address of the ExtremeWireless Appliance, and then click **Verify**.
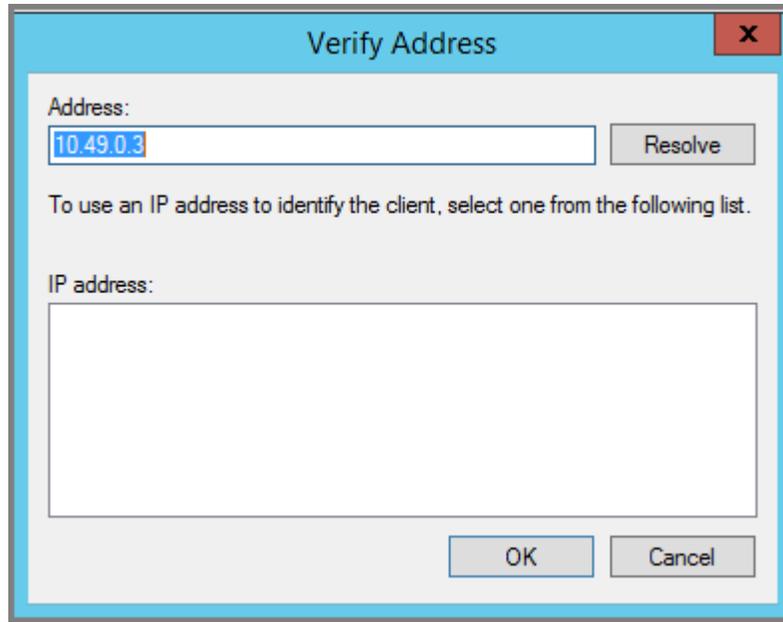
Figure 16: Verify Address

1 Click **Resolve**.

   If the IP address is correct, it appears in the Search results text box.

2 Click **OK**.

- Shared Secret. Select a Shared Secret Template (Optional).

   You can opt to enter a Shared Secret manually or have NPS generate the Shared Secret.

   - Manual. Type a password that both the NPS server and the ExtremeWireless Appliance will use to mutually authenticate. This password is case-sensitive. You can use alpha-numeric characters. You must configure the same shared secret password for Global Settings. For more information, see the *User Guide*.
   - Generate. Click **Generate** to have NPS generate the password. Not all servers support long generated secrets.

4 Click **OK**.

NPS Service Configuration

Microsoft Network Policy Server (NPS) can run as a server. You can use NPS for centralized authentication and accounting of multiple client devices. To install NPS on Windows Server 2012 R2, see http://support.microsoft.com. This section outlines the following configuration procedures:

- Adding a New Network Policy on page 66
- Configuring the ExtremeWireless Appliance as an NPS Client on page 64

Adding a New Network Policy

Create one or more network policies. In this section, we outline how to create two specific policy conditions. Adding policy conditions is optional.

- Create a condition to limit the policy to specific IP addresses.
- Create a condition to limit the policy to a specific group that corresponds to an ExtremeWireless Role.

To create a new network policy:

1 Click **Start** > **Administrative Tool** > **Network Policy Server**.
2 In the tree view, expand **NPS (Local)**, expand **Policies**, and right-click **Network Policies**.
3 Click **New**
4 Provide a **Policy name**.

- Type of network access server is **Unspecified**.
- Do not select **Vendor Specific**

5 Click **Next** to configure a condition if applicable.

Related Links

Create Condition: Client IPv4 Addresses on page 66

Create Condition: Windows Groups on page 68

Create Condition: Client IPv4 Addresses

1 Click **Add** to add a condition.
2 Scroll down to Radius Client Properties and select **Client IPv4 Addresses**.

3   Enter the IP Address of the ExtremeWireless controller and click **OK**.
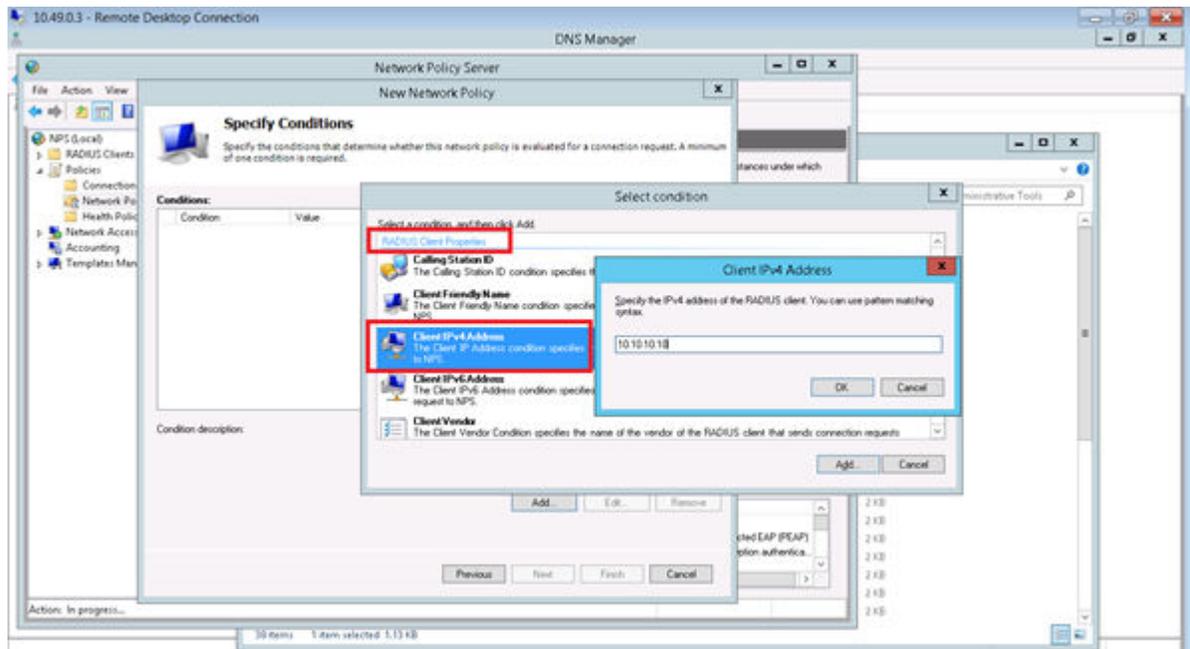
Figure 17: Condition: Client IPv4 Address

4   Click **Next**.

5   On the `Specify Access Permission` screen, select **Access granted** and click **Next**.

6   On the `Configure Authentication Methods` screen, click **Add** and select **Microsoft: Smart Card or other certificate**. Then, click **OK**.
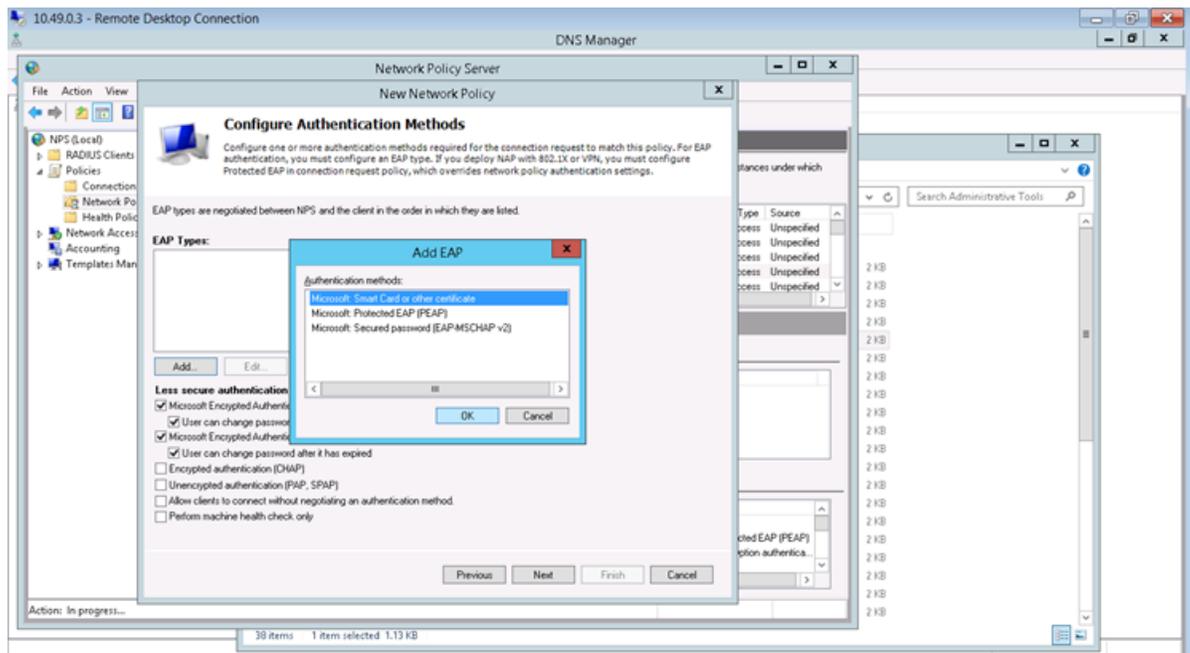

Figure 18: Add EAP

7   Click **Next**.

8   Configure the Idle Timeout and click **Next**.

9   Configure the Radius Attributes and click **Next**.

10 Click **Finish**.

Create Condition: Windows Groups

Create a condition specifying a Windows group to add flexibility to policy management.

1   Click **Add** to add a condition.

2   Select **Windows Groups** and click **Add**.

3   Click **Add Groups**.

The `Select Groups` dialog appears.
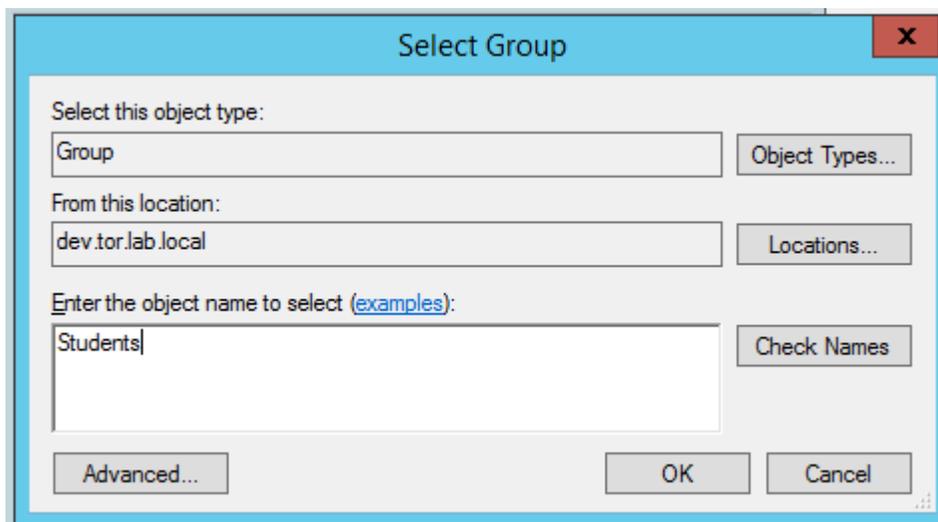
Figure 19: Select Group

4   Type `Group` as the object type.

5   Specify the location.

6   Enter the name of the group. This name must match a configured Active Directory group. You may be prompted to specify the Active Directory Windows group that the group corresponds to.

7   Click **OK**.

8   On the `Specify Access Permission` screen, specify the level of access permission and click **Next**.

9 On the **Configure Authentication Methods** screen, click **Add** and select one or more EAP methods. Then, click **OK**.
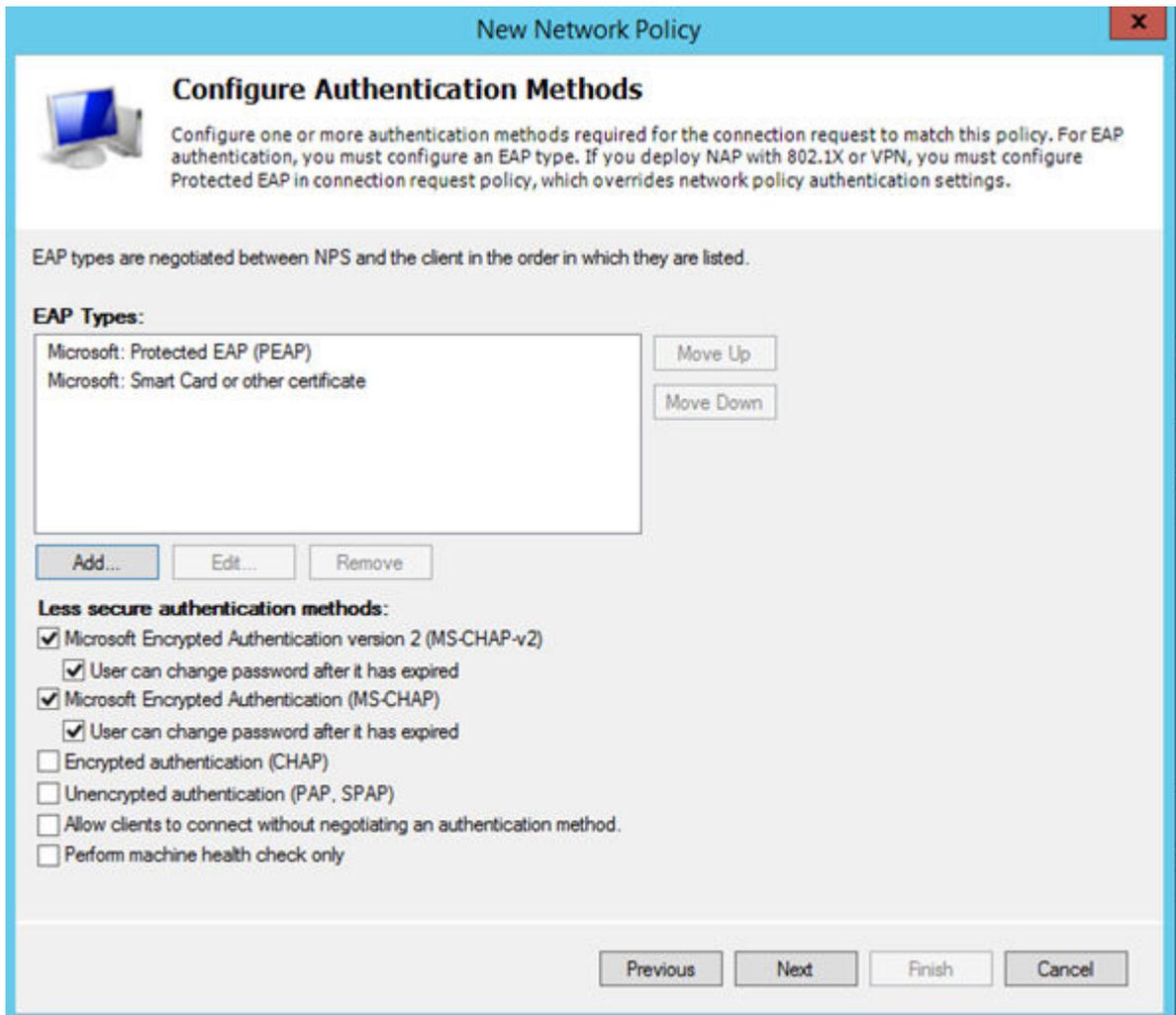
Figure 20: Configure Authentication Methods

10 Click **Next**.

11 Configure the Idle Timeout and click **Next**.

12 Configure the Radius Attributes. As an example, you can set the Filter-Id attribute to a wireless controller role. This will override the default role. The following procedure illustrates how to set the Filter-Id:

13 Click **Add**, select the **Filter-Id** attribute.

14 Click **Add**.

15 Click **Add** again and type the attribute name. The Attribute name is case sensitive and must match the Role on the wireless controller.
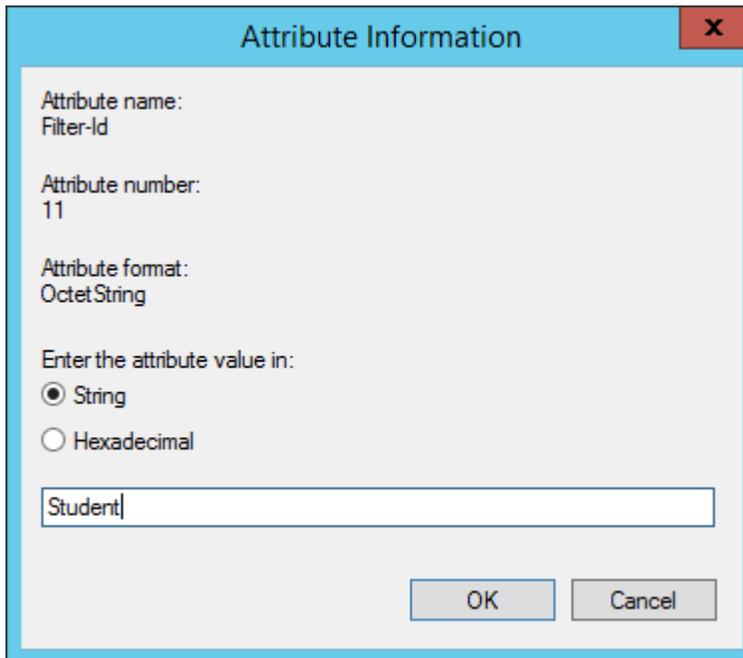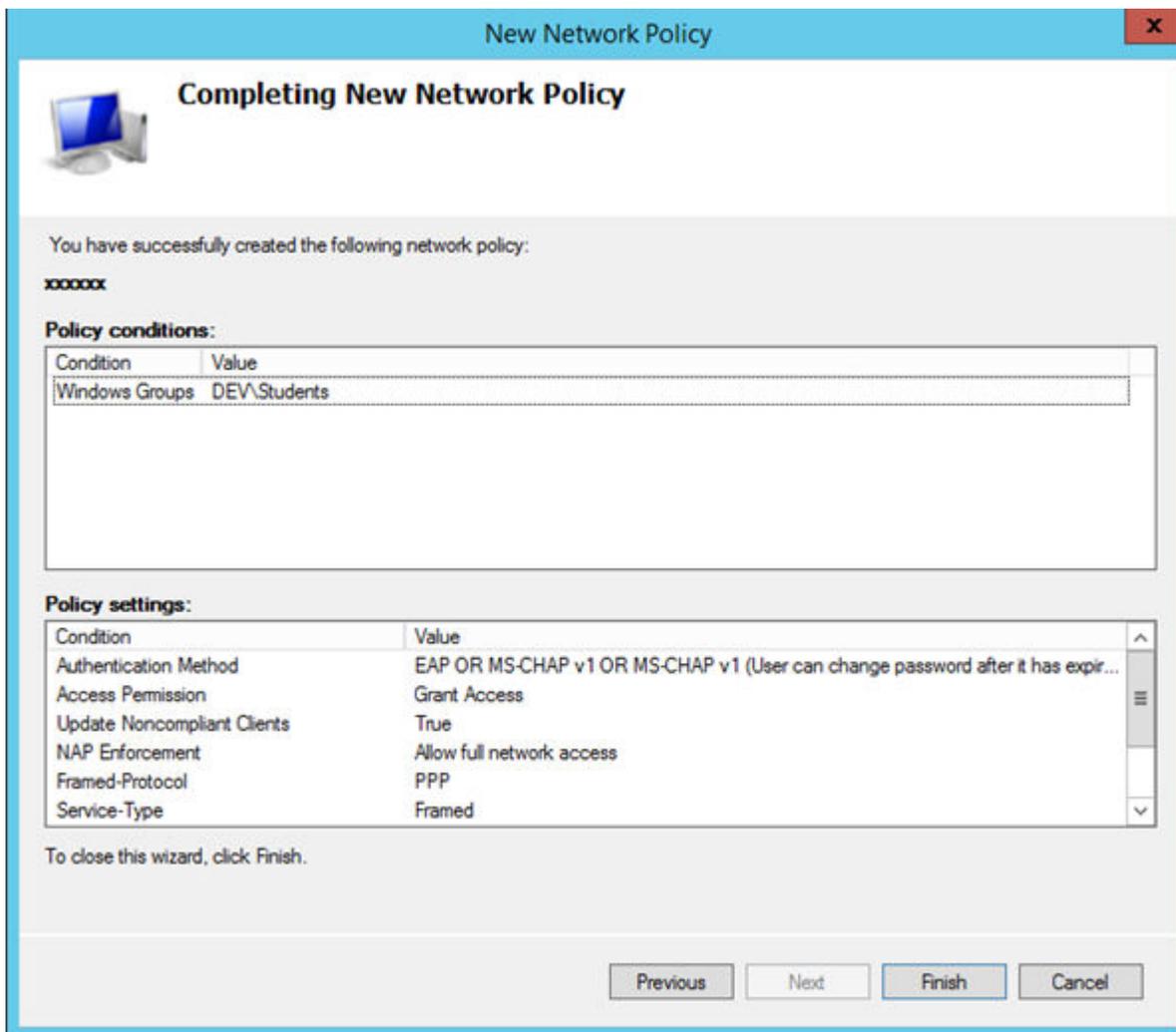

Figure 21: Attribute Information

16 Click **OK**.

17 Click **Close** to close the **RADIUS Attribute** dialog.

18 Click **Next**.

Figure 22: Completing New Network Policy

19 Click **Finish**.

DNS Service Configuration

The domain name system (DNS) stores and associates many types of information with domain names, but most importantly, it translates domain names (computer hostnames) to IP addresses.

You must install DNS on Windows Server 2012 R2 according to the server documentation. Visit http://support.microsoft.com to learn how to install and configure DNS on Windows Server 2012 R2.

The instructions here are limited to Configuring DNS for Wireless APs Discovery.

For configuration on Linux, see Configuring DNS on a Linux Server on page 72.

Configuring DNS for Wireless APs Discovery

1 Click **Start** > **Administrative Tools** > **DNS** .

2 Expand the tree and right-click on a domain.

3 Select **New Host (A or AAA)**.

The `New Host` window displays.

Figure 23: New Host

4 In the Name text box, type `controller`

5 In the IP address text box, type the ExtremeWireless Appliance's IP address.

If configuring multiple controllers, create all records with the same name `controller`, and provide unique IP addresses.

6 Select **Create associated pointer (PTR) record** checkbox.

This option creates a record for reverse lookup.

7 Click **Add Host**.

The new host is displayed in the right pane of the screen.

8 Click **Done**.

You must now configure the Wireless APs via the ExtremeWireless Assistant.

Configuring DNS on a Linux Server

This section describes the procedure to configure Linux DNS server for ExtremeWireless Appliance IP addresses discovery.

1. Configure the Linux server to include DNS information. In the `/etc/dhcp.conf` file, add domain-name-servers and domain-name DHCP options.

```
subnet 10.2.221.0 netmask 255.255.255.0 {
range 10.2.221.30 10.2.221.130;

option slp-directory-agent true 10.2.221.2;
option subnet-mask 255.255.255.0;
option domain-name-servers 192.168.6.2;
option domain-name "Availability-221.com";
option routers 10.2.221.1;
default-lease-time 40000;
}
```

2. Configure the Linux DNS server to include ExtremeWireless Appliance IP addresses.

   Create a file for the domain name configured in dhcp.conf (in this example, "Availability-221.com") as follows at `/var/named/chroot/var/named`.

   The name of the file should be the following: `/var/named/chroot/var/named/named.Availability-221.com`

```
/var/named/chroot/var/named/named.Availability-221.com
$TTL 86400
@    IN    SOA   ns1.availability-221.com.    hostmaster.availability-221.com.   (
                          2       ; serial #
                          28800   ; refresh
                          14400   ; retry
                          3600000 ; expire
                          86400   ; ttl
                          )
              IN    NS    ns1.availability-221.com.
Controller    IN    A     10.2.221.2
```

3. Add the domain name to the DNS configuration file (`/var/named/chroot/etc/named.conf`).

```
$//
// a caching only nameserver config
//
options {
/*
 * If there is a firewall between you and nameservers you want
 * to talk to, you might need to uncomment the query-source
 * directive below.  Previous versions of BIND always asked
 * questions using port 53, but BIND 8.1 uses an unprivileged
 * port by default.
 */
// query-source address * port 53;
version "Bind";
recursion no;
directory "/var/named";
};
zone "Availability-221.com" {
      type master;
      file "named.Availability-221.com";
};
zone "0.0.127.in-addr.arpa" {
type master;
file "named.local";
allow-update { none; };
```

4. Confirm that DNS service is running.

```
ps -ef | grep named
named 10023 1 0 Feb18 ? 00:00:00 /usr/sbin/named -u named -t /var/named/chroot
root 7687 7531 0 22:14 pts/982 00:00:00 grep named
```

5   Verify that the domain name is configured properly.

```
nslookup Controller.Availability-221.com
Server:            127.0.0.1
Address:           127.0.0.1#53

Name:  Controller.Availability-221.com
Address: 10.2.221.2
```