

Aerohive Deployment Guide



Aerohive Deployment Guide

For Aerohive APs, Routers, HiveOS
Virtual Appliances, and HiveManager



Aerohive Technical Publications

To register, get the latest product documentation, see compliance information, and download software updates, visit www.aerohive.com/support.

Copyright Notice

Copyright © 2013 Aerohive Networks, Inc. All rights reserved.

Aerohive Networks, the Aerohive Networks logo, HiveOS, and HiveManager are trademarks of Aerohive Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

Aerohive Networks, Inc.

330 Gibraltar Drive

Sunnyvale, CA 94089

P/N 330002-22, Rev. A

About This Guide

This guide summarizes the different HiveManager systems—physical HiveManager appliance, HiveManager Virtual Appliance, and HiveManager Online—and presents the basics of using the HiveManager GUI. It explains how to deploy and configure Aerohive APs in wireless-only environments and how to deploy and configure Aerohive routers and HiveOS Virtual Appliances as Layer 3 VPN gateways in wireless and routing environments. The guide also introduces HiveOS, the operating system that runs on Aerohive APs, routers, and HiveOS Virtual Appliances, and includes some example configurations using the CLI. Finally, it contains several tables listing the various traffic types that must traverse the network to support Aerohive device functionality. This guide is intended as a resource for all Aerohive administrators to aid in the deployment of their Aerohive products.

Contents

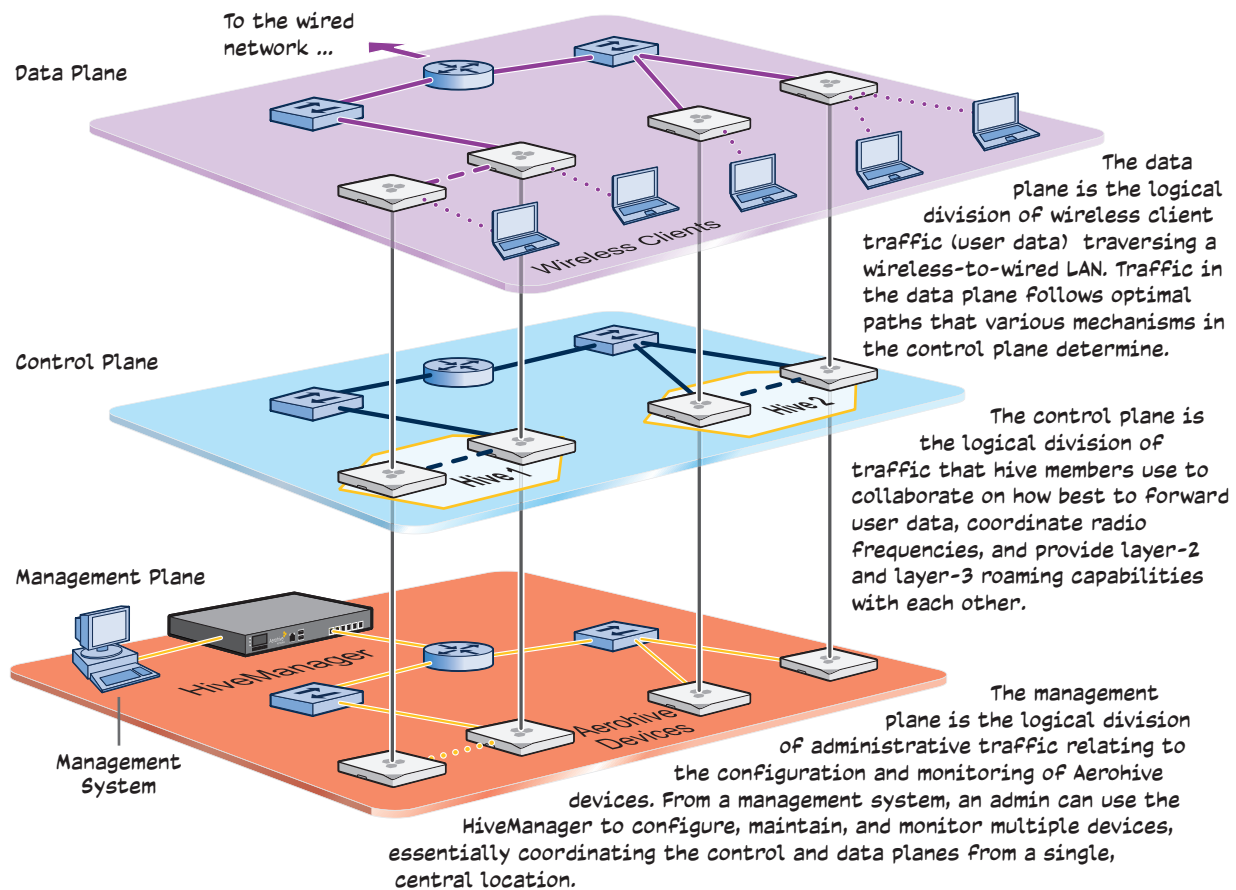
Chapter 1 Using HiveManager	5
HiveManager Management Systems	6
HiveManager Online.....	8
HiveManager Virtual Appliance.....	8
Installing and Connecting to the HiveManager GUI	9
Introduction to the HiveManager GUI	14
Viewing Reports.....	15
Searching	16
Dragging Firewall Policy Rules	17
Multiselecting.....	18
Cloning Configurations.....	18
Sorting Displayed Data.....	19
HiveManager Configuration Workflow (Enterprise Mode)	20
Updating Software on HiveManager.....	22
Updating HiveOS Firmware	23
Updating Devices in a Mesh Environment	24
Chapter 2 Wireless-Only Configuration	27
Example 1: Connecting APs to HiveManager	28
Example 2: Creating a Network Policy with a Hive	35
Example 3: Defining an SSID.....	37
Example 4: Assigning a User Profile and VLAN to the SSID	39
Example 5: Assigning the Configuration to APs	42
Chapter 3 Wireless and Routing Configuration	47
Example 1: Deploying a HiveOS Virtual Appliance	48
Installing an ESXi Hypervisor on a Server.....	48
Creating and Activating Virtual Networks and Mapping Network Settings	49
Promiscuous Mode	51
Deploying a HiveOS Virtual Appliance as a Layer 3 VPN Gateway	52
Example 2: Configuring the VPN Gateway and Routers.....	60
Example 3: Auto Provisioning the Routers.....	66
Example 4: Deploying Routers on the Network	67

Chapter 4 HiveOS.....	71
Common Default Settings and Commands	72
Configuration Overview	73
Device-Level Configurations.....	73
Policy-Level Configurations.....	74
HiveOS Configuration File Types	75
Chapter 5 Deployment Examples (CLI).....	79
Example 1: Deploying a Single AP.....	80
Example 2: Deploying a Hive	83
Example 3: Using IEEE 802.1X Authentication	89
Example 4: Applying QoS	92
Example 5: Loading a Bootstrap Configuration	99
CLI Commands for Examples	102
Commands for Example 1.....	102
Commands for Example 2.....	102
Commands for Example 3.....	103
Commands for Example 4.....	104
Commands for Example 5.....	106
Chapter 6 Traffic Types	107
Index	115

Chapter 1 Using HiveManager

You can conceptualize the Aerohive cooperative control architecture as consisting of three broad planes of communication. On the data plane, wireless clients gain network access by forming associations with Aerohive APs and routers. On the control plane, Aerohive devices communicate with each other to coordinate functions such as best-path forwarding, fast roaming, and automatic RF (radio frequency) management. On the management plane, HiveManager provides centralized configuration, monitoring, and reporting of multiple devices. These three planes are shown in [Figure 1](#).

Figure 1 Three communication planes in the Aerohive cooperative control architecture



As you can see in [Figure 1](#), HiveManager operates solely on the management plane. Any loss of connectivity between HiveManager and the devices it manages only affects device manageability; such a loss has no impact on communications occurring on the control and data planes.

This chapter explains how to do the following basic tasks:

- Use the console port to change the network settings for the MGT interface
- Power on HiveManager and connect it to a network
- Make an HTTPS connection from your management system to HiveManager and log in to the GUI

It then introduces the HiveManager GUI and includes a summary of the configuration workflow. Finally, the chapter concludes with procedures for updating HiveManager software and device firmware. The sections are as follows:

- ["HiveManager Management Systems" on page 6](#)
 - ["HiveManager Online" on page 8](#)
 - ["HiveManager Virtual Appliance" on page 8](#)
- ["Installing and Connecting to the HiveManager GUI" on page 9](#)
- ["Introduction to the HiveManager GUI" on page 14](#)
 - ["Viewing Reports" on page 15](#)
 - ["Searching" on page 16](#)
 - ["Dragging Firewall Policy Rules" on page 17](#)
 - ["Multiselecting" on page 18](#)
 - ["Cloning Configurations" on page 18](#)
 - ["Sorting Displayed Data" on page 19](#)
- ["HiveManager Configuration Workflow \(Enterprise Mode\)" on page 20](#)
- ["Updating Software on HiveManager" on page 22](#)
- ["Updating HiveOS Firmware" on page 23](#)
 - ["Updating Devices in a Mesh Environment" on page 24](#)

HIVEMANAGER MANAGEMENT SYSTEMS

The Aerohive HiveManager Network Management System provides centralized configuration, monitoring, and reporting for all types of Aerohive devices: APs, routers, and Cloud VPN Gateways. Aerohive offers two main types of HiveManager systems:

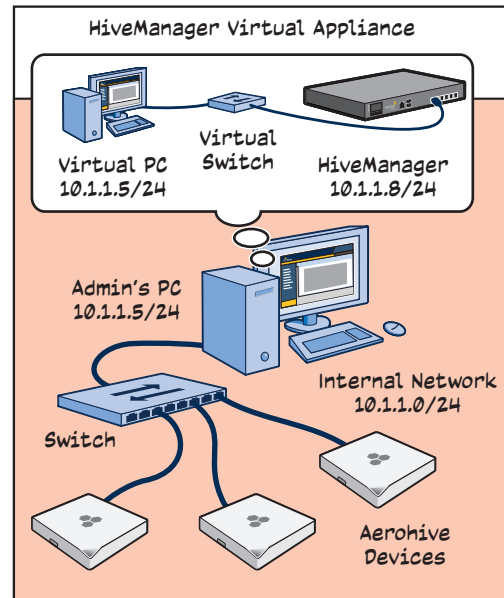
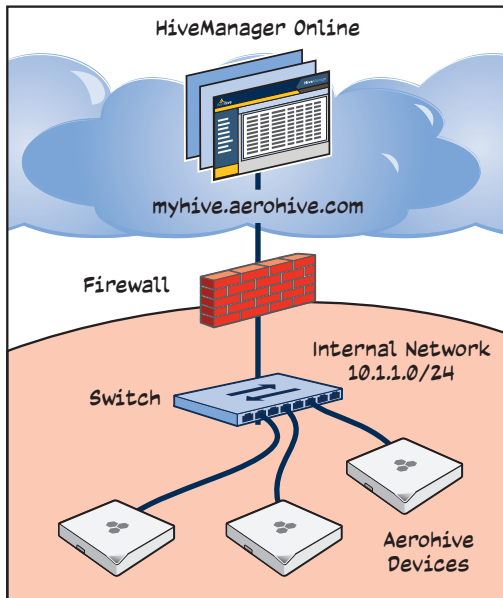
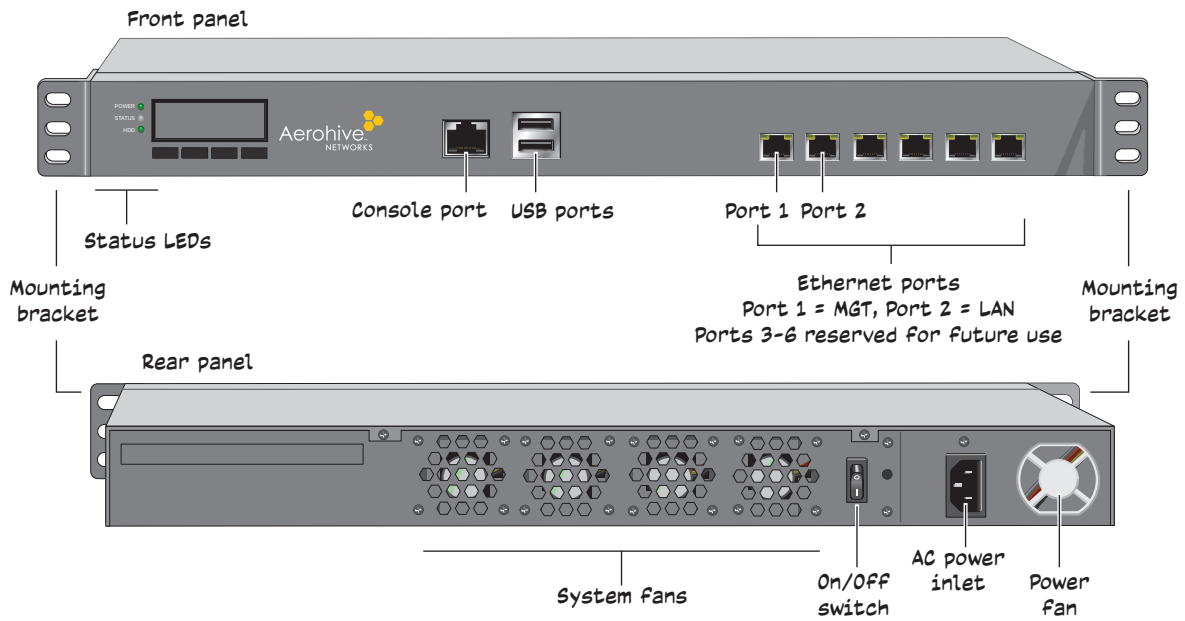
- HiveManager Online, which is a cloud-based management system hosted by Aerohive
- Standalone HiveManager appliances, which can be physical or virtual appliances (VMware) that you own and operate on your premises

HiveManager Online is a cloud-based service running on hardware hosted and maintained by Aerohive.

The HiveManager appliance can be either a physical high-capacity 1U appliance or a HiveManager Virtual Appliance, which is a virtual machine for VMware hypervisors that you can install and run on a computer on your network (see [Figure 2 on page 7](#)).

Figure 2 Physical HiveManager appliance, HiveManager Online, and HiveManager Virtual Appliance

HiveManager 1U High Capacity Appliance



For details about the physical HiveManager appliances, see the Aerohive Hardware Reference Guide.

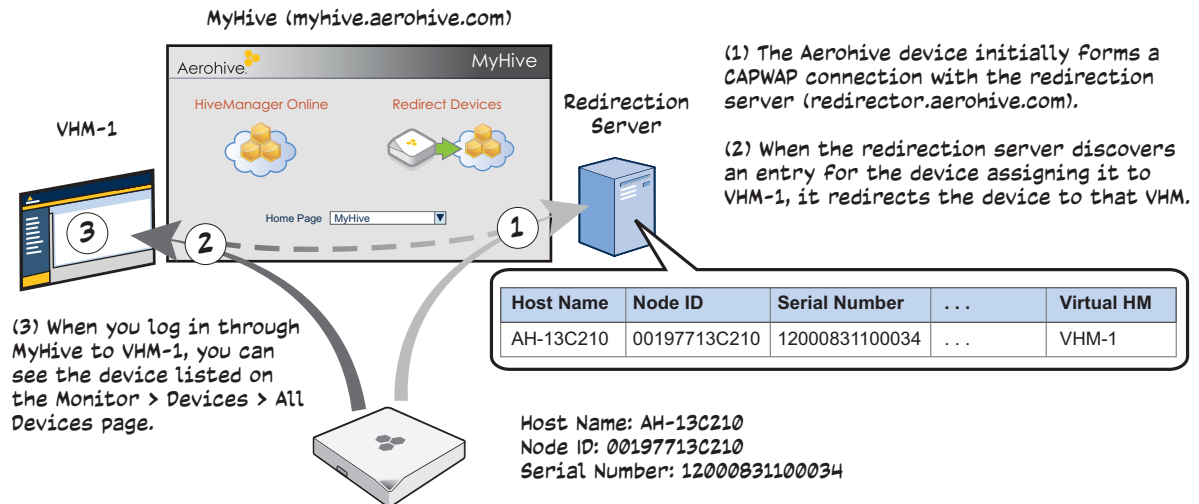
HiveManager Online

Aerohive hosts HiveManager Online at myhive.aerohive.com, maintaining the HiveManager hardware and updating the HiveManager software as new releases become available. You receive access to a VHM (virtual HiveManager) running on the HiveManager hardware. Each VHM is an independent management system with its own administrators managing their own set of Aerohive devices. Without the expense of buying a physical appliance or HiveManager Virtual Appliance, HiveManager Online can be the most cost-efficient choice for managing a small number of devices.

After purchasing a HiveManager Online account, you receive your login URL and credentials in an email message. After logging in, you enter the MyHive landing space. From there, you can access the HiveManager Online redirection server (or redirector) and your VHM.

Through your VHM, you can manage Aerohive devices deployed remotely. By default, devices first try to connect to a local HiveManager. If they cannot find one locally, they then automatically try to reach the redirector, and if the serial number of the device is already assigned to a VHM, the server redirects the device to it (see [Figure 3](#)).

Figure 3 MyHive



If a device serial number is not in the redirection server, then the server does not respond to the CAPWAP connection attempts from that device. For details about the initial CAPWAP connection process, see ["How Aerohive Devices Connect to HiveManager"](#) on page 32.

HiveManager Virtual Appliance

HiveManager Virtual Appliance is similar to a physical HiveManager appliance except that it is available as a virtual machine that you load onto a computer of your choice. It ships on a USB flash drive.

Figure 4 HiveManager Virtual Appliance ships as a virtual machine on a USB Flash drive



You must first install a VMware product such as VMware Workstation or VMware Player on your computer. Then install HiveManager Virtual Appliance on the VMware workstation or player, where it runs like a virtual server inside your computer. HiveManager Virtual Appliance forms a virtual layer 2 connection to your computer—much as if the two were connected by a layer 2 switch internally—and shares the Ethernet connection with your computer.



You can find full installation instructions on Aerohive Networks HiveManager Virtual Appliance QuickStart, which is also included on the USB flash drive.

INSTALLING AND CONNECTING TO THE HIVEMANAGER GUI

To begin using the HiveManager GUI, you must first configure the MGT interface to be accessible on the network, cable HiveManager and your management system (that is, your computer) to the network, and then make an HTTP connection from your system to the MGT interface.



HiveManager has two Ethernet interfaces—MGT and LAN. You can put just the MGT interface on the network and use it for all types of traffic, or you can use both interfaces—which must be in different subnets—and separate HiveManager management traffic (MGT) from device management traffic (LAN).

Besides HiveManager and your management system, you need two or three Ethernet cables and a serial cable (or "null modem"). The Ethernet cables can be standard cat3, cat5, cat5e, or cat6 cables with T568A or T568B terminations and RJ-45 connectors. The serial cable must comply with the RS-232 standard and terminate on the HiveManager end with a female DB-9 connector.

The GUI requirements for the management system are as follows:

- Minimum screen resolution of 1280 x 1024 pixels
- Standard browser—Aerohive recommends Internet Explorer v7.0 or Mozilla Firefox v2.0.0 or later—with Flash v9.0 or later, which is required for viewing charts with dynamically updated device alarms and wireless client data

Your management system also needs a VT100 terminal emulation program, such as Tera Term Pro[®] (a free terminal emulator) or Hilgraeve Hyperterminal[®] (provided with Windows[®] 95 to Windows XP operating systems).

Finally, you need an entitlement key or, for a physical HiveManager appliance that does not have Internet access to the entitlement server, a license key. You can obtain these by sending an email request to Aerohive at orderentry@aerohive.com. Include your sales order number and customer ID. Aerohive will send you an entitlement or license key, as requested.

Changing Network Settings

To connect HiveManager to the network, you must first set the IP address/netmask of its MGT interface so that it is in the subnet to which you plan to cable it. To do this, you can use the HiveManager console port.

1. Connect the power cable to a 100 – 240-volt power source, and turn on HiveManager. The power switch is on the back panel of the device.
2. Connect one end of an RS-232 serial cable to the serial port (or COM port) on your management system.
3. Connect the other end of the cable to the male DB-9 console port on HiveManager.

4. On your management system, run a VT100 emulation program using the following settings:
 - Bits per second (baud rate): 9600
 - Data bits: 8
 - Parity: none
 - Stop bits: 1
 - Flow control: none
5. Log in by entering the default user name (admin) and password (aerohive).
6. The HiveManager CLI shell launches. To change network settings, enter **1** (1 Network Settings and Tools), and then enter **1** again (1 View/Set IP/Netmask /Gateway/DNS Settings).
7. Follow the instructions to configure the IP address and netmask for the MGT interface, its default gateway, the HiveManager host name and domain name, and its primary DNS server.

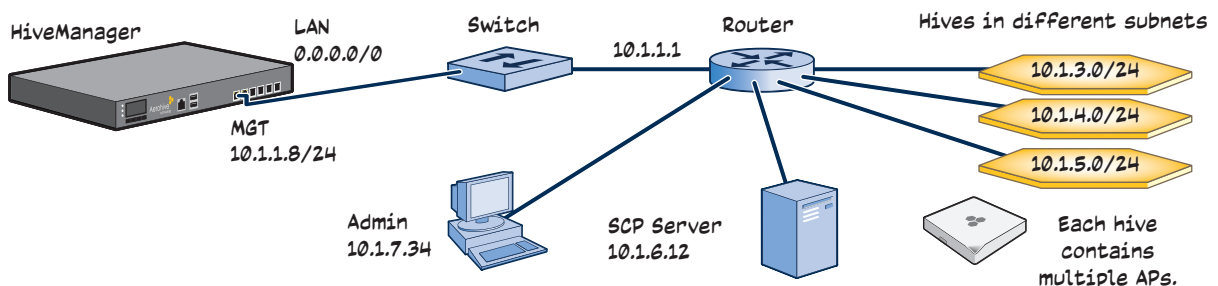
((1)) The default IP address/netmask for the MGT interface is 192.168.2.10/24. The default gateway IP address is 192.168.2.1. The LAN interface is disabled by default and does not have a default IP address. You can define network settings for the LAN interface through the HiveManager GUI after you log in.

When deciding to use one interface (MGT) or both (MGT and LAN), keep in mind that there are two main types of traffic to and from HiveManager:

- HiveManager management traffic for admin access and file uploads
- Device management traffic and configuration, file, and HiveOS image downloads to managed devices

When only the MGT interface is enabled, both types of management traffic use it. A possible drawback to this approach is that you cannot separate the two types of management traffic into two different networks. For example, if you have an existing management network, you would not be able to use it for HiveManager management traffic. Both HiveManager and Aerohive device management traffic would need to flow on the operational network because HiveManager would need to communicate with the devices from its MGT interface (see [Figure 5](#)). However, if the separation of both types of traffic is not an issue, then using just the MGT interface is a simple approach to consider.

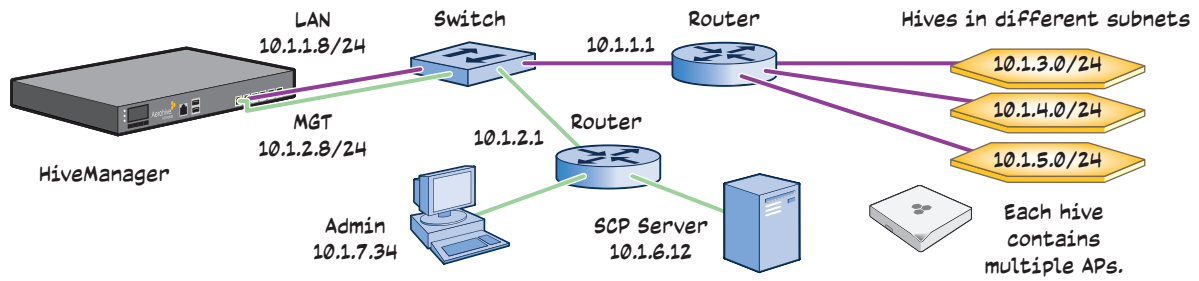
Figure 5 Using just the MGT interface



Default Gateway: 10.1.1.1 (HiveManager sends all traffic to the default gateway.)

When you enable both interfaces, HiveManager management traffic uses the MGT interface while device management traffic uses the LAN interface, as shown in [Figure 6 on page 11](#).

Figure 6 Using both MGT and LAN interfaces



Static Routes: HiveManager sends traffic destined for 10.1.6.0/24 to 10.1.2.1.

HiveManager sends traffic destined for 10.1.7.0/24 to 10.1.2.1.

Default Gateway: 10.1.1.1 (HiveManager sends traffic here when there are no specific routes to a destination.)

1 To set static routes after you log in to the GUI, click Home > Administration > HiveManager Settings > Routing > Add, set the destination IP address, netmask, and gateway, and then click **Apply**.

8. After you finish configuring the network settings, restart network services by entering `6` (6 Restart Network Services) and then enter **yes** to confirm the action.

You can now disconnect the serial cable.

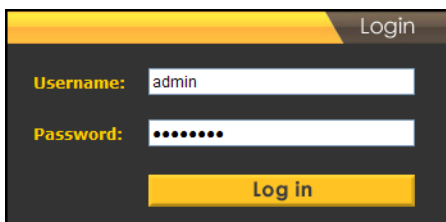
Connecting to the GUI through the MGT Interface

1. Connect Ethernet cables from the MGT interface and LAN interface—if you are using it—to the network.
2. Connect an Ethernet cable from your management system to the network so that you can make an HTTPS connection to the IP address that you set for the MGT interface.
3. Open a web browser and enter the IP address of the MGT interface in the address field. For example, if you changed the IP address to 10.1.1.8, enter this in the address field: **https://10.1.1.8** If you later add a GuestManager license, log in to HiveManager by entering **https://10.1.1.8/hm** and log in to GuestManager by entering **https://10.1.1.8/gm**

1 If you ever forget the IP address of the MGT interface and cannot make an HTTPS connection to HiveManager, make a serial connection to its console port and enter 1 for "Network Settings and Tools" and then 1 again for "View/Set IP/Netmask/Gateway/DNS Settings". The serial connection settings are explained in "Changing Network Settings" on page 9.

A certificate warning appears, which is normal because HiveManager uses a self-signed certificate. After you accept the certificate, a login prompt appears.

4. Type the default name (*admin*) and password (*aerohive*) in the login fields, and then click **Log in**.



- After logging in to HiveManager or HiveManager Virtual Appliance, or after logging in to myhive.aerohive.com and clicking **HiveManager Online**, the Aerohive Networks, Inc. End User License Agreement appears. Read it over, and if you agree with its content, click **Agree**.

An initial "Welcome to Aerohive HiveManager" dialog box appears.

- HiveManager can operate in one of two administrative modes: Express and Enterprise. Express mode (the default) provides a simple set of configuration components designed for managing a single set of wireless-only configuration policies. Enterprise mode provides configuration components for managing multiple networks and supports APs, routers, and Cloud VPN Gateways in wireless-and-routing network policies as well as just APs in wireless-only network policies. Because the examples throughout this guide are based on Enterprise mode, switch to that mode by selecting **Enterprise**.¹

Several new options appear in the dialog box as shown below.

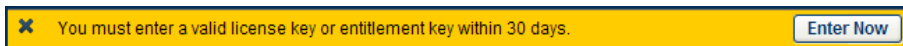
- Change the hive name for your devices (default: *Aerohive*) and your HiveManager login password (default: *aerohive*). Set a QuickStart SSID password, which will be the preshared key for an automatically created SSID called *QS-SSID* that is used in an automatically created network policy called *QuickStart-Wireless-Routing*. Set the time zone where you are located, which might be the same time zone as that for HiveManager or a different one. Finally, if you have an entitlement key or license key, click **Enter Key**. One of the following dialog boxes appears.

1. If you choose **Express**, you can later switch to Enterprise mode, and HiveManager will automatically convert your settings from the structure used in Express mode to that used in Enterprise mode. However, after choosing **Enterprise**, you cannot later switch to Express mode and preserve your settings. To change from Enterprise to Express mode, you must erase the database, reboot HiveManager, and then choose **Express** after you log back in.

For a physical HiveManager appliance with Internet access, select **Enter Entitlement Key**. Copy the entitlement key text string that Aerohive sent you in an email message, paste it in the Entitlement Key field, and then click **Enter**. You also have the option of installing a HiveManager license key, which is useful if you are working with the appliance in a location that does not have Internet access, such as a test lab. If you already have a license, select **Install License Key**, copy the license key text string previously supplied by Aerohive in an email message, paste it in the License Key field, and then click **Enter**.

For HiveManager Online and HiveManager Virtual Appliance, copy the entitlement key text string, paste it in the Entitlement Key field, and then click **Enter**. HiveManager transmits the entitlement key to the online Aerohive entitlement server, which replies with all licenses associated with that key.

8. If you do not have an entitlement key or license key yet, click **Continue**. You can access the GUI for a 30-day period without a key. To request an entitlement key or license key, you can send an email to orderentry@aerohive.com. Make sure to include your sales order number, customer ID, the email address where you would like the key to be sent, and the phrase "entitlement key request" or "license key request" in the subject or body of the email. Aerohive will send an entitlement or license key, as requested, to the specified address. When you receive the key, click **Enter Now** in the prompt displayed at the top of the GUI (shown below) or click **Home > Administration > License Management**. Copy the key from the email and paste it in the appropriate field.



HiveManager displays the Network Configuration page to assist you with the main configuration steps:

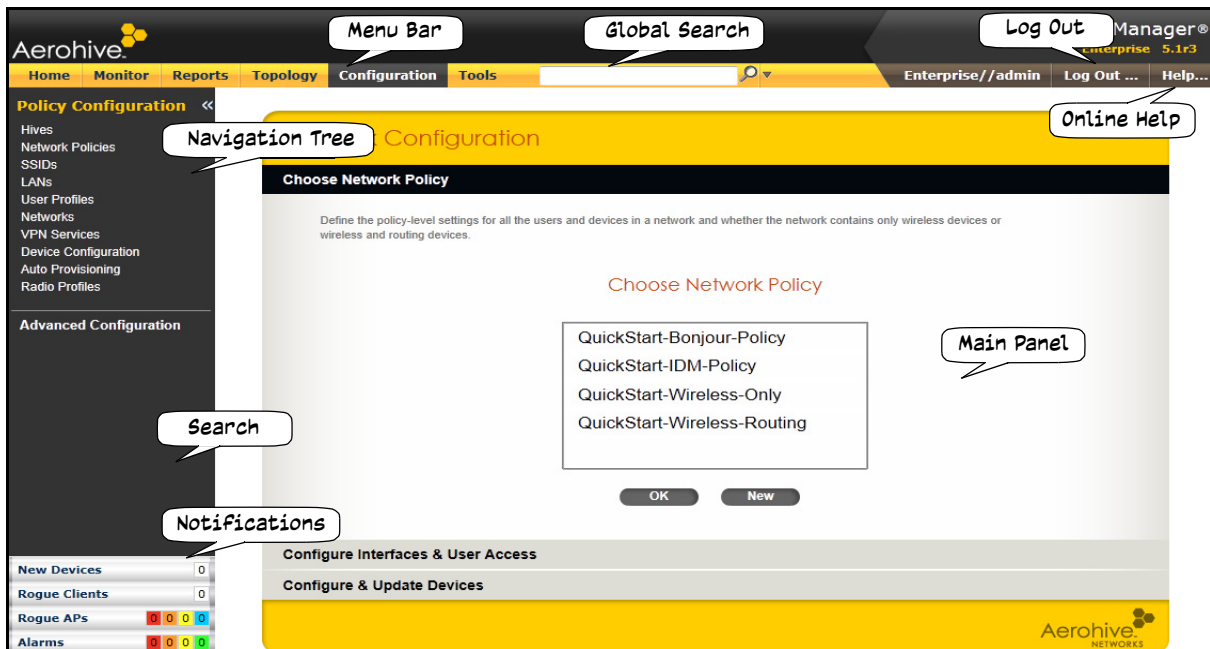
- Network policy-level configuration objects
- Device-level settings
- The transfer of the policy- and device-level settings from HiveManager to Aerohive devices

Through the settings on the Network Configuration page, you can define network policies for wireless-only deployments and deployments involving wireless and routing. You can see configuration examples for each of these in "[Wireless-Only Configuration](#)" on page 27 and "[Wireless and Routing Configuration](#)" on page 47.

INTRODUCTION TO THE HIVEMANAGER GUI

Using the HiveManager GUI, you can set up the configurations needed to deploy, manage, and monitor large numbers of devices. The configuration workflow is described in "[HiveManager Configuration Workflow \(Enterprise Mode\)](#)" on page 20. The GUI consists of several important sections, which are shown in [Figure 7](#).

Figure 7 Important sections of the HiveManager GUI



Menu Bar: The items in the menu bar open the major sections of the GUI. You can then use the navigation tree to navigate to specific topics within the selected section.

Global Search and **Search:** The Global Search tool in the menu bar is only available on HiveManager appliances and can be used to perform a search throughout the GUI. When logged in to HiveManager Online or a HiveManager appliance, you can use the Search tool below the navigation tree to find a text string within the Configuration section of the GUI.

Log Out: Click to log out of your administrative session. If you are logged in as an admin with super user privileges and there are virtual systems, you can exit the home system and enter a different virtual system from here.

Help: Access a comprehensive online context-sensitive Help system. Internet access is required to view the Help files at their default location. You can also download the Help files from Aerohive Support and post them on a local HTTP server if you like. In addition to Help files, you can also access product documentation and online training videos by clicking the down arrow to the right of the Help button.

Navigation Tree: The navigation tree contains all the topics within the GUI section that you chose in the menu bar. Items you select in the navigation tree appear in the main panel. You can hide the navigation tree by clicking the double-left arrows (<<) at the upper right of the navigation tree panel. To expand it again, click the double-right arrows (>>) on the *Show Nav* tab.

Main Panel: The main panel contains the windows in which you set and view various parameters.

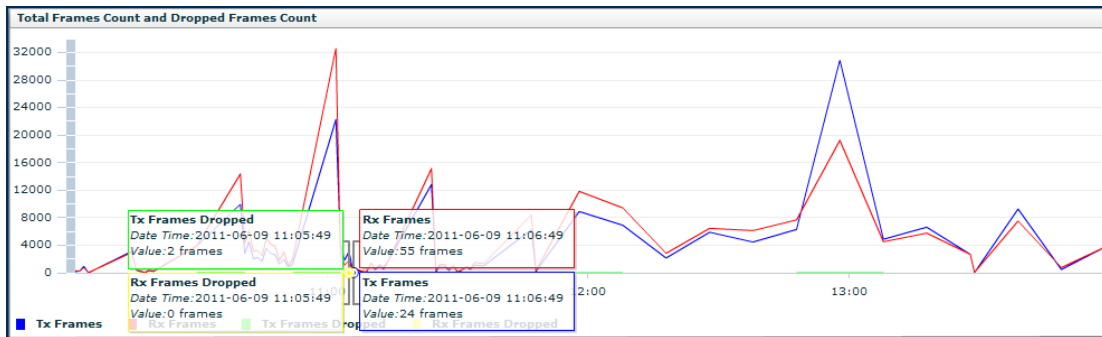
Notifications: HiveManager displays a summary of new Aerohive devices, rogue clients, rogue APs, and alarms detected on managed devices here. Clicking a displayed number opens the relevant page with more details.

Some convenient aspects that the HiveManager GUI offers are the ability to clone configurations, apply configurations to multiple devices at once, and sort displayed information. Brief overviews of these functions are presented in the following sections.

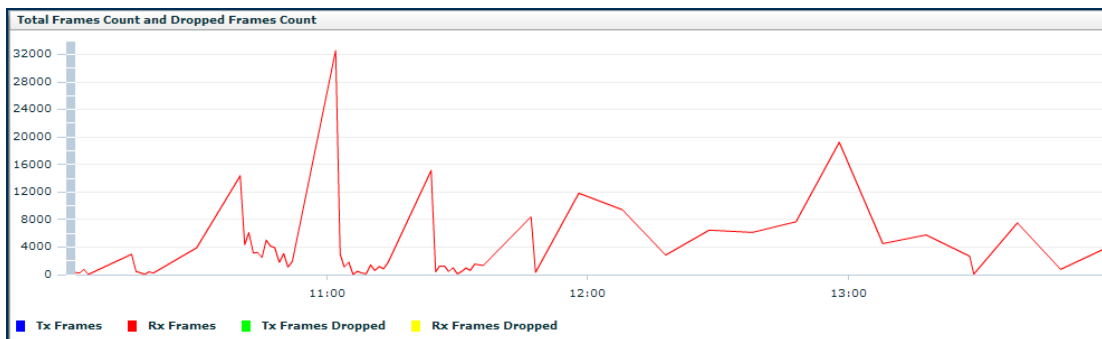
Viewing Reports

When viewing reports that contain graphs (Monitor > Reports ...), you can use your mouse to control what information HiveManager displays. Moving your mouse over a measurement point on any line in a graph displays the type of data being reported and the date, time, and value of the measurement. In the graph for active client details (Monitor > Clients > Active Clients > *client_mac_addr*), moving your mouse over a color box in the legend hides all other lines except the one matching that color (see [Figure 8](#)).

Figure 8 Working with graphs in reports



Moving the mouse over a measurement point in a graph displays data about that measurement. If measurement points on multiple lines happen to converge at the same point, HiveManager displays data for all of them. Here you can see information about the total number of transmitted (Tx) and received (Rx) frames and dropped frames.



In the graph showing details for a selected active client, moving the mouse over a colored box in the legend hides all other lines except the one that is the same color as the box under the mouse. Here HiveManager only shows the red line for transmitted frames because the mouse is over the red box next to Rx Frames in the legend.

Searching

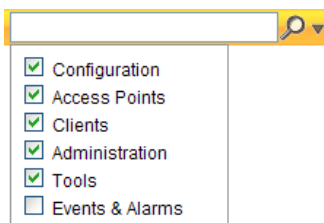
HiveManager appliances (physical HiveManager appliances and HiveManager Virtual Appliance) contain two types of search tools, differentiated by their scopes:

- The global search tool, which is located in the menu bar and can find text strings throughout the GUI
- The search tool, which is located below the navigation tree in the Configuration section and only searches within the Configuration section

HiveManager Online provides just the search tool that focusses on the Configuration section of the GUI.

The global search feature on HiveManager appliances finds text strings throughout the HiveManager database and the entire GUI (except in Reports and Topology) or within one or more specified sections of the GUI. By default, HiveManager searches through the following sections of the GUI: Configuration, Access Points, Clients, Administration, and Tools. You can also include Events and Alarms in your search, but not Topology. To restrict the scope of your search, click the down arrow to the right of the search icon and select the areas of the GUI that you want to include and clear those that you want to exclude (see [Figure 9](#)).

Figure 9 Global search tool

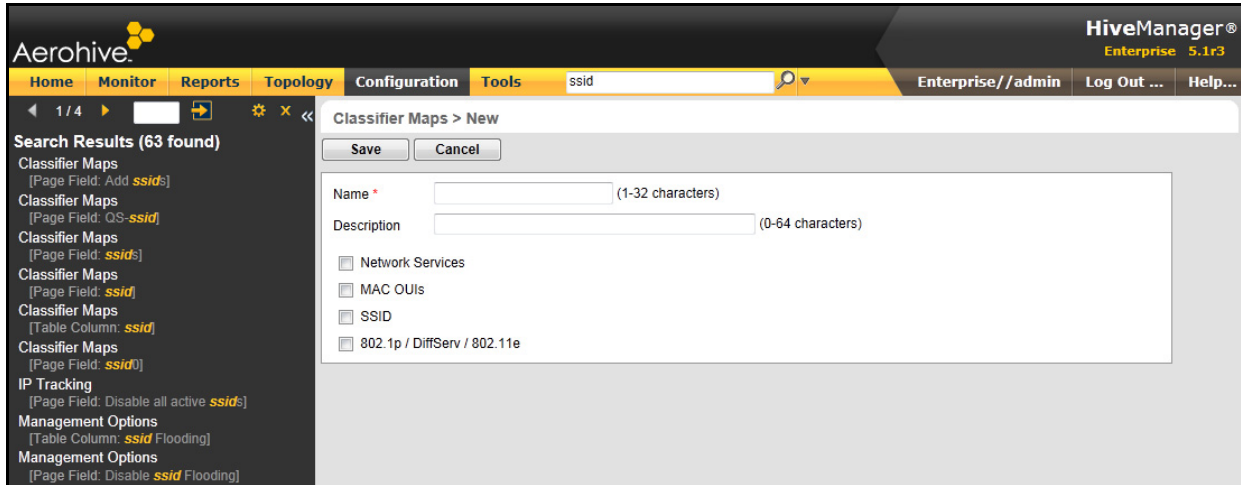


The following items are ignored when using the global search tool:

- The names of fields in dialog boxes
- The settings on the following Home > Administration pages: HiveManager Settings, HiveManager Services, and HM Notification Mail List
- Certificates, captive web portal web page files, and image files
- Reports

When you enter a word or phrase in the search field and then click the **Search** icon—or press the **Enter** key on your keyboard—HiveManager displays the search results in the left panel that usually contains the navigation tree. The first item in the list is displayed in the main window. To view a different page, click the page name (see [Figure 10 on page 17](#)).

Figure 10 Search results

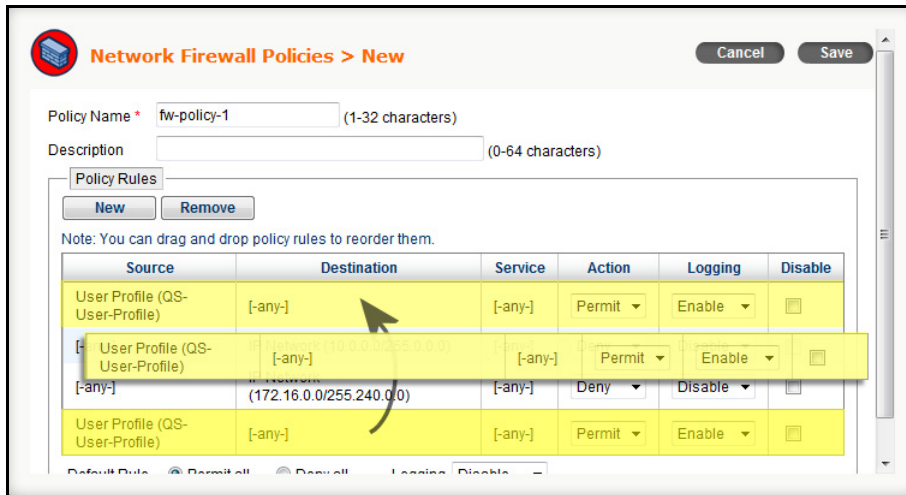


(1) Do not use quotation marks to enclose a phrase of two or more words. Simply enter the phrase that you want to find with spaces. See the HiveManager online Help for more information on the Search tool.

Dragging Firewall Policy Rules

Because a firewall policy applies its rules in order from the top, the position of a rule within a policy determines whether the firewall applies it before or after another rule. To reposition a rule within a firewall policy, simply click-drag it to a new location (see Figure 11).

Figure 11 Dragging firewall policy rules



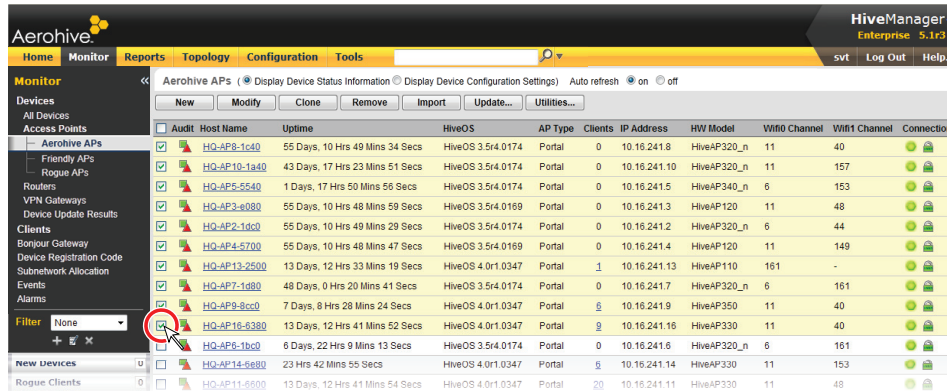
Click and drag a rule from one location in the firewall policy list to another.

Multiselecting

You can select multiple objects to make the same modifications or perform the same operation to all of them at once (see [Figure 12](#)).

Figure 12 Selecting multiple new APs

Select the check boxes to select multiple noncontiguous objects, or shift-click to select check boxes for multiple contiguous objects. Then click the **Modify** button to configure them with the same settings.



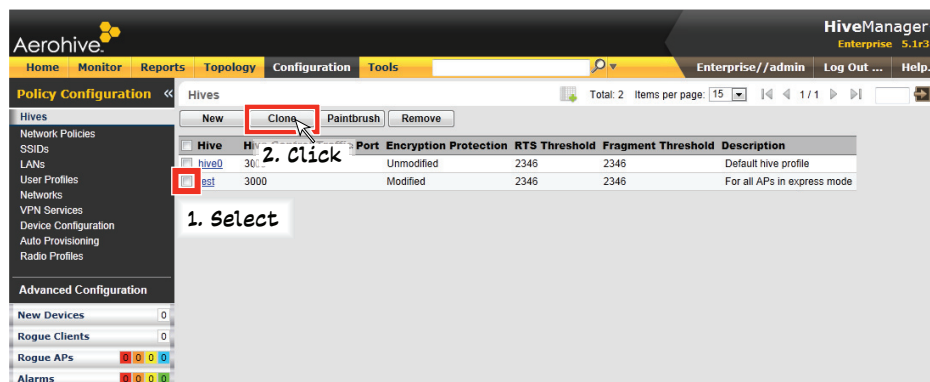
Here, you use the shift-click multiselection method to select a set of the topmost ten devices in the list; that is, you select the check box for the top device and hold down the SHIFT key while selecting the check box for the tenth device from the top.

Cloning Configurations

When you need to configure multiple similar objects, you can save time by configuring just the first object, cloning it, and then making slight modifications to the subsequent objects. With this approach, you can avoid re-entering repeated data (see [Figure 13](#)).

Figure 13 Cloning a hive

To clone an object, select it in an open window, and then click the **Clone** button. Retain the settings you want to keep, and modify those you want to change.

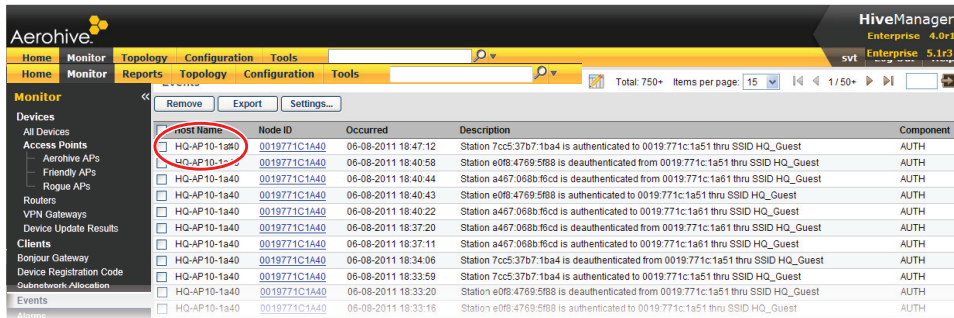


Sorting Displayed Data

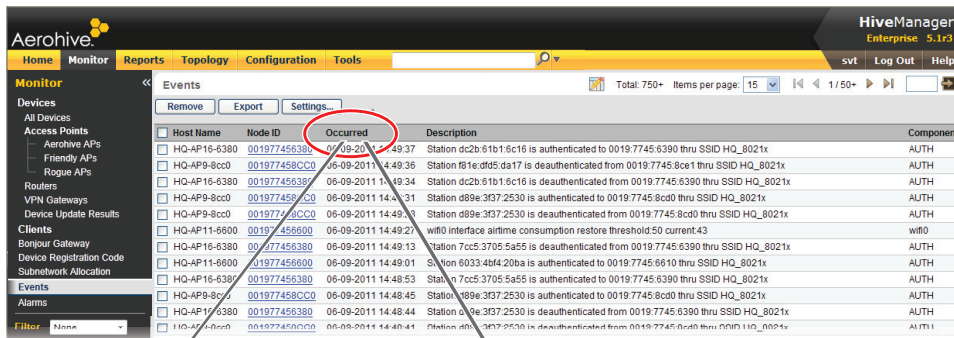
You can control how the GUI displays data in the main panel by clicking a column header. This causes the displayed content to reorder itself alphanumerically or chronologically in either ascending or descending order. Clicking the header a second time reverses the order in which the data is displayed (see Figure 14).

Figure 14 Sorting event log entries by device host name and then chronologically

By default, displayed objects are sorted alphanumerically from the top by name. If you click the name again, the order is reversed; that is, the objects are ordered alphanumerically from the bottom.



By clicking the heading of a column, you can reorder the display of objects either alphanumerically or chronologically, depending on the content of the selected column. Here you reorder the data chronologically.



Indicates that the list appears in descending order



Indicates that the list appears in ascending order

HIVEMANAGER CONFIGURATION WORKFLOW (ENTERPRISE MODE)

Assuming that you have already set HiveManager in Enterprise mode and configured its basic settings, and that you have deployed devices that are now connected to HiveManager, you can start configuring the devices through HiveManager.² A simple configuration strategy is to create a network policy and add objects by clicking the **New** icon to define objects as necessary.



An important initial configuration task to perform is to synchronize the internal clocks of all the managed devices either with the clock on HiveManager or with the time on an NTP server. If you plan on having devices validate RADIUS, VPN, and HTTPS (captive web portal) certificates, synchronizing all the devices with the same NTP server helps ensure synchronization

HiveManager in Enterprise mode supports the configuration, monitoring, and management of two main types of networks: those containing wireless devices and networks containing wireless and routing devices. HiveManager in Express mode supports only wireless networks.

For a deployment consisting of only wireless devices, the typical workflow proceeds like this:

1. Use default settings or configure new settings for various features that, when combined, constitute a network policy that determines how users access the wireless network. The main configuration objects (although not all the individual settings) used in a wireless-only network policy are shown below.

Network Policy - Wireless Only	
Hive	MAC filters and MAC DoS protection settings
SSIDs	User and client authentication: captive web portal (possibly including RADIUS and certificates) and MAC authentication
	MAC filters, traffic filter, MAC and IP DoS protection settings
	User profiles
VLAN settings	MGT interface VLAN, native (untagged) VLAN
Layer 2 IPsec VPN	Certificates
Traffic filter settings	
Service settings	WIPS, access console, ALG services, Mgt IP filter, management options, LLDP/CDP link discovery protocols, and IP tracking
Management services	SNMP, syslog, DNS, NTP, and location services
QoS settings	QoS classifier and marker maps, and dynamic airtime scheduling

2. Define various device-level settings to apply to individual Aerohive devices. These include a map assignment, device type, radio profiles, captive web portal for its Ethernet ports, scheduled configuration audits, RADIUS authentication server settings, DHCP server or DHCP relay agent settings, and CAPWAP server configuration settings.

2. When Aerohive devices are in the same subnet as HiveManager, they can use CAPWAP (Control and Provisioning of Wireless Access Points) to discover HiveManager on the network. CAPWAP works within a layer-2 broadcast domain and is enabled by default on all Aerohive devices. If the devices and HiveManager are in different subnets, then you can use one of several approaches to enable devices to connect to HiveManager. For information about these options, see ["How Aerohive Devices Connect to HiveManager" on page 32](#).

3. Apply the policy-level settings (contained within the network policy) to one or more devices, and then push the configurations to Aerohive devices across the network.

For a deployment consisting of wireless and routing devices, the typical workflow proceeds like this:

1. Use default settings or configure new settings for various features that, when combined, constitute a network policy that determines how users access the wired and wireless network. The main configuration objects of a wireless-and-routing network policy are shown below.

Network Policy - Wireless and Routing				
Hive	MAC filters and MAC DoS protection settings			
SSIDs	User and client authentication: captive web portal (possibly including RADIUS and certificates) and MAC authentication			
	MAC filters, traffic filter, MAC and IP DoS protection settings			
	User profiles	Network and VLAN	Subnetworks	
		GRE tunnels, MAC and IP firewall policies for users, QoS rate control and queuing, schedules, SLA settings, and client classification policy		
Router LAN Ports	LAN port assignments			
	User and client authentication: captive web portal (possibly including RADIUS and certificates) and MAC authentication			
	Management traffic filter			
	User profiles (if ports are in access mode)	Network object	VLAN	
			Subnetworks	
		GRE tunnels, MAC and IP firewall policies for users, QoS rate control and queuing, schedules, SLA settings, and client classification policy		
Network objects (if ports are in trunk mode)		VLAN		
One = untagged/native; One or more = tagged		Subnetworks		
VLAN settings	MGT interface VLAN, native (untagged) VLAN			
Router Firewall				
Layer 3 IPsec VPN	Certificates, user profiles (for routing exceptions)			
Traffic filter settings				
Service settings	WIPS, access console, ALG services, Mgt IP filter, management options, LLDP/CDP link discovery protocols, and IP tracking			
Management services	SNMP, syslog, DNS, NTP, and location services			
QoS settings	QoS classifier and marker maps, and dynamic airtime scheduling			

2. Define various device-level settings to apply to individual Aerohive devices. Depending on the device type (access point, router, Cloud VPN Gateway), these can include a map assignment, device type, radio profiles, captive web portal for its Ethernet ports, scheduled configuration audits, RADIUS authentication server settings, DHCP server or DHCP relay agent settings, and CAPWAP server configuration settings.
3. Apply the policy-level settings (contained within the network policy) to one or more devices, and then push the configurations to Aerohive devices across the network.

UPDATING SOFTWARE ON HIVEMANAGER

You can update the software running on HiveManager from either a local directory on your management system or an SCP (Secure Copy) server. If you download an image and save it to a local directory, you can load it from there. If you save the image to an SCP server, you can direct HiveManager to log in and load it from a directory there.

1. If you do not yet have an account on the Aerohive Support portal, visit www.aerohive.com/support/login.html and complete the Support Portal Account Registration form to set one up.
2. When you have login credentials, return to www.aerohive.com/support/login, and log in.
3. Navigate to the software image that you want to load onto HiveManager (Customer Support > Software Downloads > HiveManager software images) and download the file.
4. Save the HiveManager image file to a local directory or an SCP server.
5. Log in to HiveManager and navigate to **Home > Administration > HiveManager Operations > Update Software**.
6. To load files from a directory on your local management system, choose either **Update and clear alarm and event logs** or **Full update** (to keep existing log entries after the upgrade), and then enter the following:

File from local host: (select); type the directory path and a file name; or click **Browse**, navigate to the software file, and select it.

or

To load a file from an SCP server:

File from remote server: (select)

IP Address: Enter the IP address of the SCP server.

SCP Port: Enter the port number of the SCP server (the default port number for SCP is 22).

File Path: Enter the directory path and HiveManager software file name. If the file is in the root directory of the SCP server, you can simply enter the file name.

User Name: Type a user name with which HiveManager can access the SCP server.

Password: Type a password with which HiveManager can use to log in securely to the SCP server.

or

To load a file from the Aerohive update server:

File from Aerohive update server: (select)

A pop-up window appears with a list of newer HiveManager image files. If you have the latest available version, the list will be empty. If there are newer images, select the one you want, and upgrade HiveManager to that image by transferring the file over an HTTPS connection from the server to HiveManager.

7. To save the new software and reboot HiveManager, click **OK**.

UPDATING HIVEOS FIRMWARE

HiveManager makes it easy to update HiveOS firmware running on managed devices. First, you obtain new HiveOS firmware from Aerohive Support and upload it onto HiveManager. Then you push the firmware to the devices and activate it by rebooting them.

((1))	<p>When upgrading both HiveManager software and HiveOS firmware, do so in this order:</p> <ul style="list-style-type: none"> • Upgrade HiveManager (HiveManager can manage devices running the current version of HiveOS and also previous versions going back two major releases). • Upload the new HiveOS firmware to the managed devices, and reboot them to activate it. • Reload the HiveOS configurations to the managed devices—even if nothing in the configurations has changed—and reboot them to activate the configuration that is compatible with the new HiveOS image.
-------	---

1. Log in to the Aerohive Support portal to obtain a new HiveOS image.
2. Save the HiveOS image file to a directory on your local management system or network.
3. Log in to HiveManager and navigate to **Monitor > Devices > All Devices**.
4. In the All Devices window, select one or more Aerohive devices, and then click **Update > Upload and Activate HiveOS Software**.

The *Upload and Activate HiveOS Software* dialog box appears.

5. To the right of the HiveOS Image field, click **Add/Remove**.
6. In the *Add/Remove HiveOS Image* dialog box that appears, enter one of the following—depending on how you intend to upload the HiveOS image file to HiveManager—and then click **Upload**:

To load a HiveOS image file from the Aerohive update server:

HiveOS <version> images from Aerohive update server: (select)

To load a HiveOS image file from a directory on your local management system:

Local File: (select); type the directory path and image file name, or click **Browse**, navigate to the image file, and select it.

To load a HiveOS image file from an SCP server:

SCP Server: (select)

IP Address : Enter the IP address of the SCP server.

SCP Port: Enter the port number of the SCP server (the default port number for SCP is 22).

File Path: Enter the path to the HiveOS image file and the file name. If the file is in the root directory of the SCP server, you can simply enter the file name.

User Name: Type a user name with which HiveManager can access the SCP server.

Password: Type a password that HiveManager can use to log in securely to the SCP server.

((2))	To delete an old HiveOS file, select the file in the "Available Images" list, and then click Remove.
-------	--

7. Click **Upload**.
8. Close the dialog box by clicking the **Close** icon (X) in the upper right corner.
9. By default, the HiveManager uses SCP to transfer the file to the selected devices and requires a manual reboot of the devices to activate it. If you want to change these settings, click **Settings** in the upper right corner of the *Upload and Activate HiveOS Software* page.

A section expands allowing you to change how HiveOS images are displayed (by software version or by file name), how the software is activated (these options are explained below), which transfer protocol to use (SCP or TFTP), the type of connection between HiveManager and the devices, and how long to wait before timing out an incomplete update attempt.

In the Activation Time section, select one of the following options, depending on when you want to activate the firmware—by rebooting the devices—after HiveManager finishes loading it:

- **Activate at:** Select and set the time at which you want the devices to activate the firmware. To use this option accurately, make sure that both HiveManager and managed device clocks are synchronized.
- **Activate after:** Select to load the firmware on the selected devices and activate it after a specified interval. The range is 0 – 3600 seconds; that is, immediately to one hour. The default is 5 seconds. This option is useful if you are updating devices in a mesh environment. Setting a longer activation interval ensures that mesh points receive their firmware well before Ethernet-connected portals get theirs and then reboot to activate it, which—if they rebooted too soon—could disrupt the firmware upload to the mesh points and potentially leave them stranded.
- **Activate at next reboot:** Select to load the firmware and not activate it. The loaded firmware gets activated the next time the device reboots.



When choosing which option to use, consider how HiveManager connects to the devices it is updating. See "[Updating Devices in a Mesh Environment](#)".

- To save your settings, click the **Save** icon in the upper right corner. Otherwise, click the **Close** icon to use these settings just this time. If you do not save your modified settings, the next time you upload a HiveOS image to devices, HiveManager will again apply the default settings.
- Select the file you just loaded from the HiveOS Image drop-down list, select one or more devices at the bottom of the dialog box, and then click **Upload**.

HiveManager displays the progress of the HiveOS image upload—and its eventual success or failure—on the Monitor > Devices > Device Update Results page.

Updating Devices in a Mesh Environment

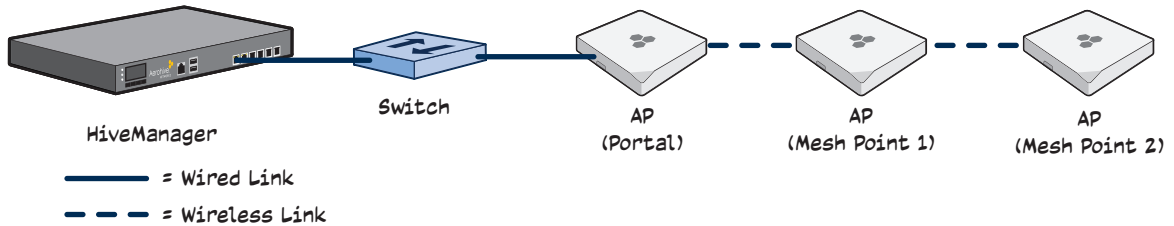
When updating hive members in a mesh environment, be careful of the order in which the devices reboot. If a portal completes the upload and reboots before a mesh point beyond it completes its upload—which most likely would happen because portals receive the uploaded content first and then forward it to mesh points—the reboot will interrupt the data transfer to the mesh point. This can also happen if a mesh point linking HiveManager to another mesh point reboots before the more distant mesh point completes its upload. As a result of such an interruption, the affected mesh point receives an incomplete firmware or configuration file and aborts the update.



A mesh point is a hive member that uses a wireless backhaul connection to communicate with the rest of the hive. HiveManager manages mesh points through another hive member that acts as a portal, which links mesh points to the wired LAN.

Figure 15 Aerohive devices in a mesh environment

When updating devices in a mesh environment, the HiveManager communicates with mesh points through their portal and, if there are any intervening mesh points, through them as well. While updating devices in such an environment, it is important to keep the path from the HiveManager to all devices clear so that the data transfer along that path is not disrupted. Therefore, when updating a firmware image or configuration on devices in a mesh environment, make sure that the portal or a mesh point closer to the portal does not reboot before the upload to a mesh point farther away completes.



To avoid the reboot of an intervening device from interfering with an ongoing upload to a mesh point beyond it, allow enough time for the firmware to reach the farthest mesh points before activating the firmware. After all the devices have the firmware, rebooting any devices between them and HiveManager becomes inconsequential.

Chapter 2 Wireless-Only Configuration

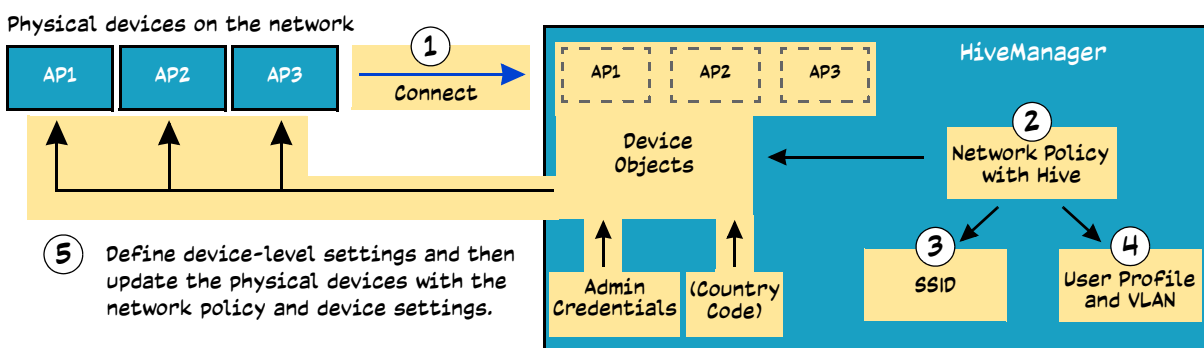
This chapter introduces the HiveManager GUI in Enterprise mode through a series of examples showing how to create a basic wireless-only network policy with a hive and an SSID. It then explains how to connect several APs to HiveManager, accept them for management, and push the configuration to them over the network.

(i) Although maps provide a convenient method for organizing and managing your AP deployment, they are not strictly required and are not covered in this chapter. For information about using maps, see the HiveManager online Help.

You can look at any of the following examples individually to study how to configure a specific feature or view all of them sequentially to understand the basic workflow for configuring and managing APs through HiveManager. The examples are as follows:

- "Example 1: Connecting APs to HiveManager" on page 28
Cable two APs to the network to act as portals and set up a third as a mesh point. Put the APs on the same subnet as HiveManager and allow them to make a CAPWAP connection to HiveManager.
- "Example 2: Creating a Network Policy with a Hive" on page 35
Define a wireless-only network policy to contain a hive and an SSID.
- "Example 3: Defining an SSID" on page 37
Define the security and network settings that wireless clients and APs use to communicate.
- "Example 4: Assigning a User Profile and VLAN to the SSID" on page 39
Define a user profile and specify the VLAN to assign to traffic from wireless clients.
- "Example 5: Assigning the Configuration to APs" on page 42
Assign the network policy to the APs, make some device-level settings, and push the configurations to the APs. Also, if necessary, set country codes.

The conceptual relationships among the configuration examples in this chapter

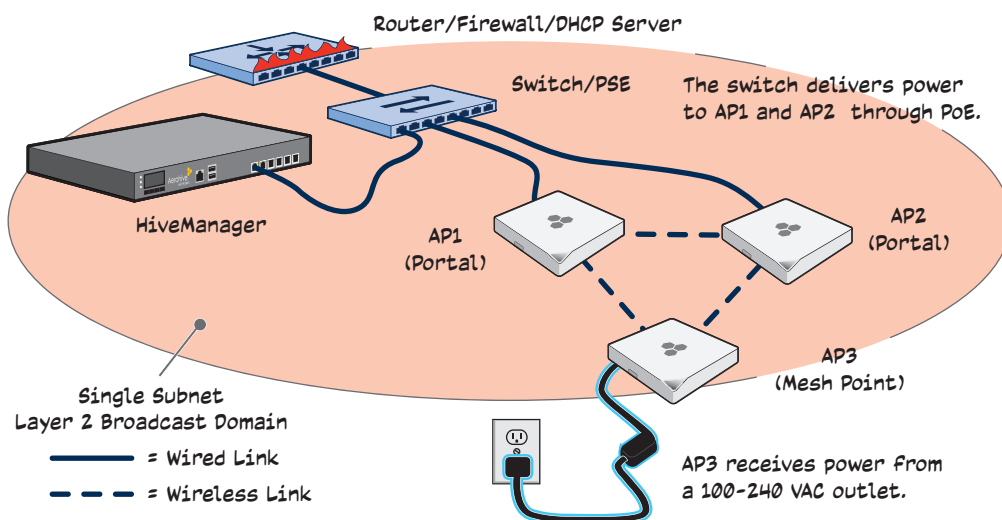


After connecting some APs to the network, you enable them to make a CAPWAP connection to HiveManager. You then create a network policy that includes a hive and an SSID and apply it plus some device-level settings to the APs. Finally, you push the configurations to them.

EXAMPLE 1: CONNECTING APs TO HIVEMANAGER

In this first example, you set up three APs for management through HiveManager. Cable two of the APs—AP1 and AP2—to the network. Run an Ethernet cable from the eth0 port on each AP to a switch so that they are in the same subnet as the IP address of the MGT interface on HiveManager. (Neither the AP300 eth1 port nor the HiveManager LAN port are used in this example.) You can use AC/DC power adapters to connect them to a 100-240 VAC power source or allow them to obtain power through PoE (Power over Ethernet) from PSE (power sourcing equipment) on the network. (Both power adapters and PoE injectors are available from Aerohive as options.) Place the third AP—AP3—within range of the other two, and use a power adapter to connect it to an AC power source. See [Figure 1](#), in which the switch uses PoE to provide power to APs 1 and 2.

Figure 1 Connecting APs to the network



By default, the APs obtain their network settings dynamically from a DHCP server. AP3 reaches the DHCP server after first forming a wireless link with the other two APs. (An AP in the position of AP3 is referred to as a mesh point, and APs such as AP1 and 2 are called portals.)

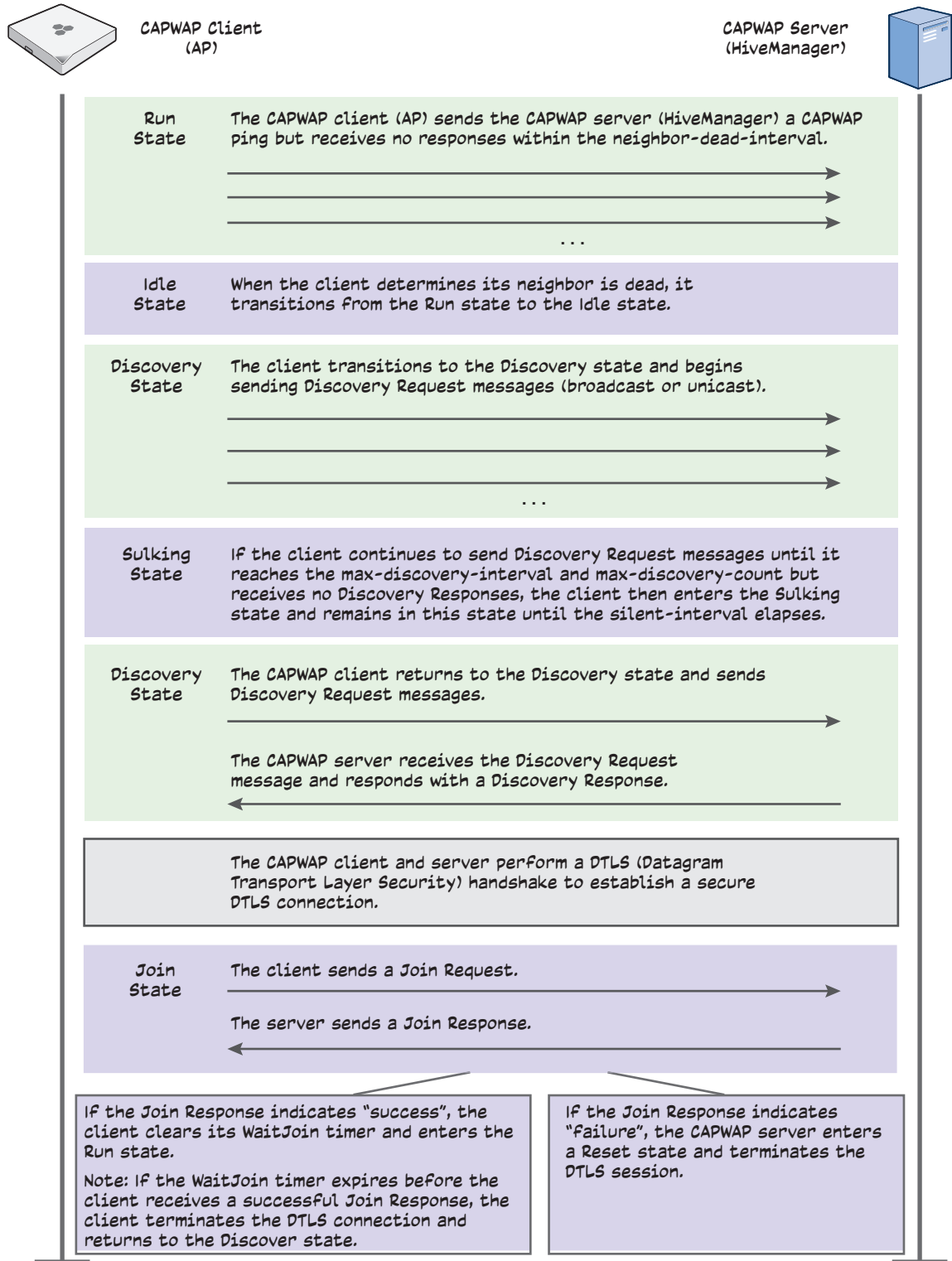
Within the framework of the CAPWAP (Control and Provisioning of Wireless Access Points) protocol, APs act like CAPWAP clients and HiveManager like a CAPWAP server. Because all devices are in the same subnet in this example, the clients can broadcast CAPWAP Discovery Request messages to discover and establish a secure connection with the server automatically. During the connection process, each client proceeds through a series of CAPWAP states, resulting in the establishment of a secure DTLS (Datagram Transport Layer Security) connection. These states and the basic events that trigger the client to transition from one state to another are shown in [Figure 2 on page 29](#).



To illustrate all possible CAPWAP states, [Figure 2 on page 29](#) begins by showing an Aerohive AP and HiveManager already in the Run state. When an AP first attempts to discover a HiveManager—after the AP has an IP address for its mgt0 interface and has discovered or has been configured with the HiveManager IP address—it begins in the Discovery state.

For information about various ways that APs can form a secure CAPWAP connection with a physical HiveManager appliance or a HiveManager Virtual Appliance in the same or different subnets, and with HiveManager Online, see ["How Aerohive Devices Connect to HiveManager" on page 32](#).

Figure 2 CAPWAP Connection process—beginning from the run state



Check that the APs have made a CAPWAP connection with HiveManager:

Click **Monitor > Devices > Access Points > APs**.

The page displays the three APs that you put on the network. If you see the three APs, refer to [Figure 3 on page 32](#). If you do not see them, check the following:

- Do the APs have power?
Check the PWR (Power) status LED on the top of the devices. If it is glowing steady green, it has power and has finished booting up. If the PWR status LED on an AP300 series device is pulsing green, it is still loading HiveOS firmware. The Power LED on the AP100 series device indicates that it is loading firmware by glowing steady amber. If the PWR status LED is dark, the device does not have power. If an AP is getting power through PoE from the switch or from a power injector, make sure that the PSE is configured and cabled correctly. If an AP is powered from an AC outlet, make sure that the power cable is firmly attached to the power connector, the AC/DC power adapter, and the outlet.
- Are the two portals—AP1 and AP2—connected to the Ethernet network?
When the devices are properly connected, the ETH0 status LED on the AP 300 series device pulses green to indicate a 1000 Mbps link or amber for a 10/100 Mbps link. On the AP 20, the LAN status LED blinks green to indicate that the link is up and active. If the ETH0 or LAN LED is dark, make sure that both ends of the Ethernet cable are fully seated in the AP and switch ports. If the ETH0 or LAN status LED is still dark, try a different cable.
- Did the APs receive network settings from a DHCP server? At a minimum, each AP needs to receive an IP address, netmask, and default gateway in the same subnet as HiveManager. To check their settings, make a physical or virtual console connection to the APs,¹ and do the following:

To check the IP address, netmask, and default gateway of the mgt0 interface on an AP, enter **show interface mgt0**, and look at the settings displayed in the output.

A mesh point must first establish a wireless link to a portal over their backhaul interfaces before it can contact a DHCP server. To see that the mesh point (AP3) has successfully formed a link with a portal using the default hive "hive0", enter **show hive hive0 neighbor** and check the Hstate column. If at least one other AP is listed as a neighbor and its hive state is Auth, the mesh point has successfully formed a link and can access the network. If the hive state is anything else, it might still be in the process of forming a link. The following are the various hive states:

Disv (Discover) - Another AP has been discovered, but there is a mismatch with its hive ID.

Neibor (Neighbor) - Another AP has been discovered whose hive ID matches, but it has not yet been authenticated.

CandPr (Candidate Peer) - The hive ID on a discovered AP matches, and it can accept more neighbors.

1. To make a physical console connection, connect a console cable to the AP as explained in the *Aerohive Hardware Reference Guide*. A virtual access console is an SSID that the AP automatically makes available for administrative access when it does not yet have a configuration and cannot reach its default gateway. By default, the SSID name is "<hostname>_ac". Form a wireless association with the AP through this SSID, check the IP address of the default gateway that the AP assigns to your wireless client, and then make an SSH or Telnet connection to the AP at that IP address. When you first connect, the Initial CLI Configuration Wizard appears. Because you do need to configure all the settings presented in the wizard, enter **N** to cancel it. When prompted to log in, enter the default admin name and password: admin, aerohive. For APs set with "world" as the region code, enter the **boot-param country-code number** command. For number, enter the country code for the location where you intend to deploy the AP. For a list of country codes, see the list in the HiveManager GUI.

AssocPd (Association Pending) - A AP is on the same backhaul channel, and an association process in progress.

Assocd (Associated) - A AP has associated with the local AP and can now start the authentication process.

Auth (Authenticated) - The AP has been authenticated and can now exchange data traffic.

You can also check the presence of hive neighbors by viewing the entries listed in the Supplicant column for the wifi1.1 interface in the output of the **show auth** command.

If the AP does not have any network settings, check that it can reach the DHCP server. To check if a DHCP server is accessible, enter **interface mgt0 dhcp-probe vlan-range <number1> <number2>**, in which <number1> and <number2> indicate the range of VLAN IDs on which you want the AP to probe for DHCP servers. The results of this probe indicate if a DHCP server is present and has responded. If the probe succeeds, check the DHCP server for MAC address filters or any other settings that might interfere with delivery of network settings to the AP.

- Are the APs in the same subnet as HiveManager?
APs must be in the same subnet and the same VLAN as HiveManager for their broadcast CAPWAP Discovery messages to reach it. If you can move the APs or HiveManager so that they are all in the same subnet, do so. If they must be in different subnets from each other, it is still possible for the APs to contact HiveManager, but not by broadcasting CAPWAP messages. For a list of other connection options, see ["How Aerohive Devices Connect to HiveManager" on page 32](#).
- Can the APs ping the IP address of the HiveManager MGT interface?
Enter the **ping <ip_addr>** command on the AP, where the variable <ip_addr> is the IP address of the HiveManager MGT interface. If it does not elicit any ICMP echo replies from HiveManager, make sure that HiveManager is connected to the network through its MGT interface, not its LAN interface, and that the IP address settings for the MGT interface are accurate (see Home > Administration > HiveManager Settings > Interface Settings in the HiveManager GUI).
- What is the status of the CAPWAP client running on the AP?
To check the CAPWAP status of an AP, enter the **show capwap client** command. Compare the "RUN state" with the CAPWAP states explained in [Figure 2 on page 29](#). Check that the AP has an IP address for itself and the correct address for HiveManager. If for some reason, the AP does not have the correct address for HiveManager, you can set it manually by entering the **capwap client server name <ip_addr>** command, in which <ip_addr> is the HiveManager MGT interface IP address.

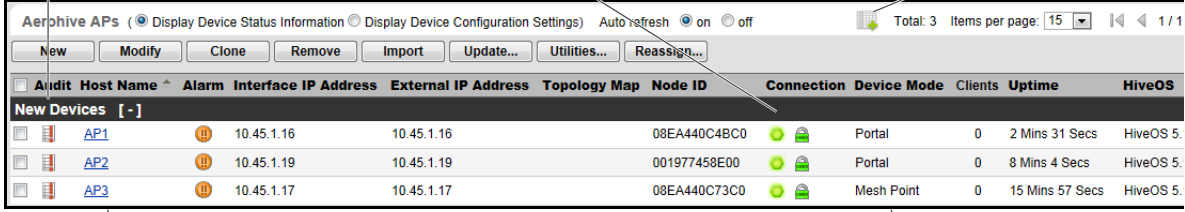
When APs have contacted HiveManager, they appear on the Monitor > Devices > Access Points > APs page, as shown in [Figure 3 on page 32](#).

Figure 3 Monitor > Devices > Access Points > Aerohive APs (view mode: Display Device Status Information)

Audit icon
File with red exclamation point: The configuration on an AP does not match that on HiveManager. Green exclamation point: Match!

CAPWAP connection and security icons
Green or gray hexagon: The AP is connected (green) or disconnected (gray). Green locked/red unlocked padlock: Connection is secured with DTLS or not.

You can customize the table contents by clicking the Edit Table icon. You can add more columns (radio channels and power for example), remove columns, and reorder them.



Audit	Host Name	Alarm	Interface	IP Address	External IP Address	Topology Map	Node ID	Connection	Device Mode	Clients	Uptime	HiveOS
	AP1	🟡		10.45.1.16	10.45.1.16		08EA440C4BC0	🟢🔒	Portal	0	2 Mins 31 Secs	HiveOS 5.
	AP2	🟡		10.45.1.19	10.45.1.19		001977458E00	🟢🔒	Portal	0	8 Mins 4 Secs	HiveOS 5.
	AP3	🟡		10.45.1.17	10.45.1.17		08EA440C73C0	🟢🔒	Mesh Point	0	15 Mins 57 Secs	HiveOS 5.

The host names have been changed to match those in the example. By default, the host name is AH- + the last six bytes of its MAC address. (Example: AH-0E55B0)

The AP type for AP1 and AP2 is "Portal"; they have Ethernet connections to the network. AP3 is "Mesh Point"; it connects to the network through a portal.



If you see a different group of AP settings, make sure that Display Device Status Information is selected at the top of the APs page. The GUI provides two view modes for APs, one that focuses on monitoring APs and another that focuses on configuring them.

How Aerohive Devices Connect to HiveManager

Aerohive devices—APs, routers, and HiveOS Virtual Appliances—and HiveManager communicate with one another through CAPWAP (Control and Provisioning of Wireless Access Points). The devices act as CAPWAP clients and HiveManager acts as a CAPWAP server. The Aerohive devices can form a CAPWAP connection with HiveManager in any of the following ways:

- When the devices are in the same layer 2 broadcast domain as a HiveManager appliance, they broadcast CAPWAP Discovery Request messages to discover HiveManager and establish a secure connection with it automatically.
- If there is no HiveManager in the same broadcast domain but they can reach the MyHive redirector—and serial number entries for them have already been added to your MyHive ACL (access control list)—then they can form secure CAPWAP connections with the redirector (redirection server). The connected devices are redirected to a VHM (virtual HiveManager) at the MyHive site if you have a HiveManager Online account or to a HiveManager appliance—physical or virtual—at another site if you have a Standalone account (available for free upon request).
- Finally, Aerohive devices and a local HiveManager might be in different subnets and the devices either cannot reach the redirector or they can but they are not listed in the ACL. In this case, they cannot discover HiveManager by broadcasting CAPWAP Discovery Request messages, nor can they reach the redirector. So that the devices can form a CAPWAP connection to HiveManager, you can use one of the following methods to configure them with the HiveManager domain name or IP address or configure them so that they can learn it through DHCP or DNS settings. When they have the IP address of the CAPWAP server, they then send unicast CAPWAP Discovery Request messages to that address.

Log in to the CLI on each Aerohive device and enter the IP address of the CAPWAP server with the following command:

```
capwap client server name <string>
```

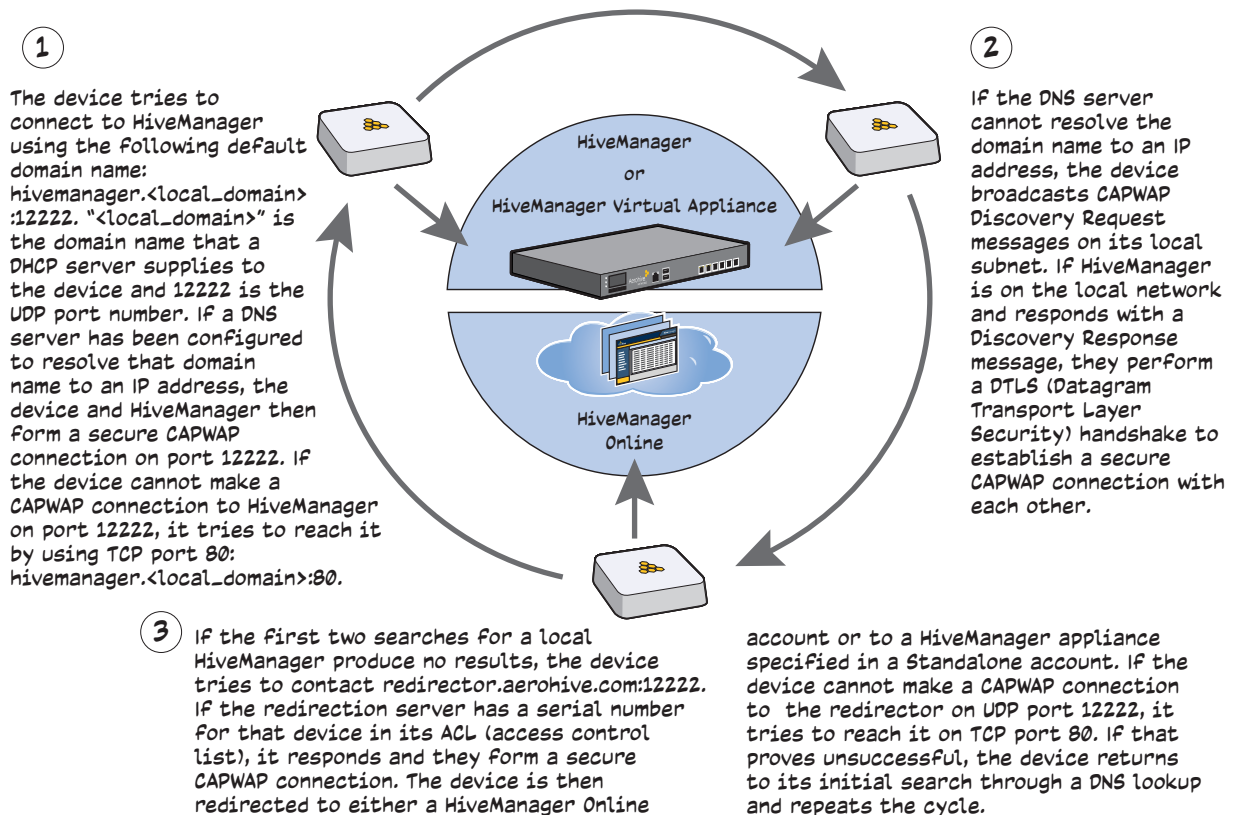
Configure the DHCP server to supply the domain name of the CAPWAP server as DHCP option 225 or its IP address as option 226 in its DHCP OFFER. (If you use a domain name, the authoritative DNS server for that domain must also be configured with an A record that maps the domain name to an IP address for the CAPWAP server.) Aerohive devices request DHCP option 225 and 226 by default when they broadcast DHCPDISCOVER and DHCPREQUEST messages.

(1) If you must change the DHCP option number (perhaps because another custom option with that number is already in use on the DHCP server), enter this command with a different option number: `interface mgt0 dhcp client option custom hivemanager <number> { ip | string }`

If HiveManager continues to use its default domain name ("hivemanager") plus the name of the local domain to which it and the Aerohive devices belong, configure an authoritative DNS server with an A record that resolves "hivemanager.<local_domain>" to an IP address. If the devices do not have an IP address or domain name configured for the CAPWAP server and do not receive an address or domain name returned in a DHCP option, then they try to resolve the domain name to an IP address.

When the devices go online for the first time without any specific CAPWAP server configuration entered manually or received as a DHCP option, they progress through the cycle of CAPWAP connection attempts shown in [Figure 4 on page 33](#).

Figure 4 Discovering the CAPWAP server



If the devices form a CAPWAP connection with the Aerohive redirection server and their serial numbers have been entered in an ACL, the redirection server automatically redirects their CAPWAP connections to a corresponding HiveManager Online account or—when using a Standalone MyHive account—to a HiveManager appliance. The redirection server does this by sending the devices the HiveManager domain name or IP address as their new CAPWAP server and the name of the appropriate VHM or IP address or domain name of the HiveManager appliance. If the devices are currently using HTTP, the redirection server includes the configuration needed for them to continue using it. Similarly, if they are configured to access the public network through an HTTP proxy server, the redirection server saves the relevant settings on the devices so they will continue using the HTTP proxy server when connecting to HiveManager.

If the redirector does not have the device serial numbers, then the ACL on the redirector ignores the CAPWAP connection attempts, and they repeat the connection cycle shown above.

Troubleshooting the Initial CAPWAP Connection to HiveManager Online

As explained in the previous section, when you connect an Aerohive device to the network and power it on, it first tries to connect to a local HiveManager. If it cannot do that, it automatically tries to connect to the redirector. The redirector checks if the serial number of the device is listed in its ACL—which should be the case as Aerohive enters the serial numbers of newly purchased devices in the appropriate ACL as part of the sales process. If the ACL contains the device serial number, the redirector then redirects it to the correct HiveManager Online account, where the device appears at Monitor > Devices > All Devices. Log in to MyHive, click **HiveManager Online**, and then navigate to the *All Devices* page. If you do not see the device listed there, take the following steps to resolve the situation:

((1))	<i>Depending on network conditions and firewall policies, it can sometimes take up to ten minutes for a device to connect to the redirection server and be redirected to the HiveManager Online VHM to which it belongs. Be sure to give it enough time to complete the connection process before proceeding.</i>
-------	---

1. Click **Redirector > Monitor > AP Access Control List**, and check if the device serial number is listed there.
2. If the serial number is absent from the ACL, do the following:
 - 2.1 Click **Enter**, type the serial number, and then click **Save**.

((1))	<i>If an error message appears stating that the serial number already exists in the system, contact Aerohive Technical Support for further assistance: support@aerohive.com.</i>
-------	--

- 2.2 Check if the device appears at Monitor > Devices > All Devices in the HiveManager Online GUI. Note that it can take up to ten minutes to complete the connection process.
- 2.3 If the device still does not appear on the *All Devices* page, power the AP off, wait five seconds, power it back on, and then check the *All Devices* page again.
- 2.4 If the device still does not appear on the *All Devices* page, check that it can access the Internet and that any firewall between it and the redirector allows outbound traffic on UDP 12222 or TCP 80.

If the device connects and appears on the *All Devices* page in your HiveManager Online VHM, you have successfully resolved the issue and can stop troubleshooting. If not, continue to the next step.

3. If the serial number of the device is listed in the ACL on the redirector but it does not appear on the *All Devices* page in HiveManager Online, first follow steps 2.3 and 2.4 (if you have not already done so). If it still does not appear, the device might be redirected to the HiveManager Online home system, which can occur if the CAPWAP server name on the device was accidentally misconfigured. To reassign it your VHM, do the following:
 - 3.1 In HiveManager Online, click **Configuration > Show Nav > Auto Provisioning > SN Management > Scan SN**, type the 14-digit serial number for the Aerohive device, and then click **Save**. After that, click **Cancel** to close the *Imported AP Serial Numbers* dialog box.
 - 3.2 On the *AP Auto Provisioning* page, click **New**, enter the following, and then click **Save**:
 - Enable AP Auto Provisioning**: (select)
 - Name**: Enter a name for the auto provisioning profile.
 - Description**: Enter a useful note or comment about the profile.
 - Device Model**: Choose the appropriate device model from the drop-down list.
 - Device Type**: Choose the type of device for which you are configuring automatic provisioning.
 - Apply to devices with the following identification**: (select)
 Select the serial number that you just entered in the previous step and click the right arrow (>) to move it from the Available Serial Numbers column to the Selected Serial Numbers column.
 - 3.3 Reboot the device to reset its CAPWAP state to Discovery. When it contacts the redirection server this time, HiveManager Online will apply the access control defined in the automatic provisioning configuration and redirect the device to your VHM.

EXAMPLE 2: CREATING A NETWORK POLICY WITH A HIVE

Using HiveManager, you can configure two broad types of features:

- Policy-level features – In combination, these features form policies that control how users access the network: SSIDs, user profiles, QoS forwarding mechanisms and rates, hives, AAA (authentication, authorization, accounting) services, management services (DNS, NTP, SNMP, and syslog), tunnel policies, IP and MAC firewall policies, and VLAN assignments.
- Device-level features – These features control how hive members communicate with the network and how radios operate in different modes, frequencies, and signal strengths.

A network policy is an assembly of policy-level feature configurations that HiveManager pushes to all Aerohive devices that you assign to the policy. Because these configurations are policy-based, they can apply across multiple physical devices. In contrast, device-level configurations are more appropriately applied to smaller sets of devices or to individual devices themselves.

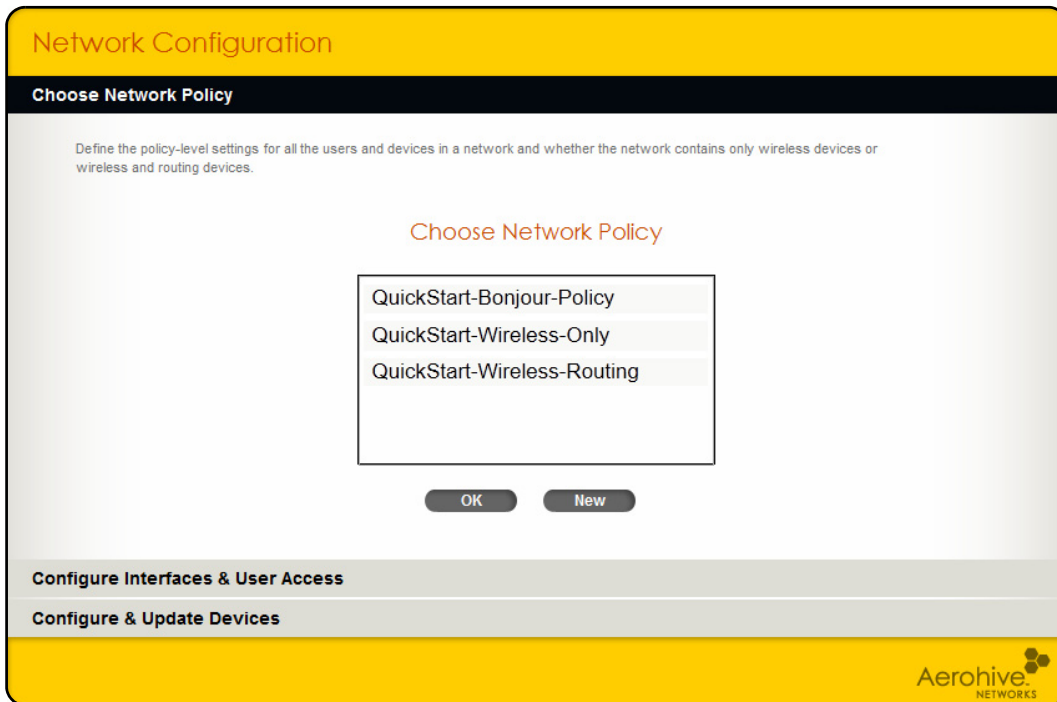
In this example, you create a network policy for wireless devices with a hive and SSID.


1. Click **Configuration**.

The Network Configuration page appears. It is a type of wizard consisting of three main panels:

- *Choose Network Policy*
- *Configure Interfaces & User Access*
- *Configure & Update Devices*

By following this guided configuration sequence, you can easily and efficiently set up a simple wireless network.



2. Click **Configuration**, choose **QuickStart-Wireless-Only** from the network policy list, click the tool icon on its right (), and then click **Clone**. Keep all the cloned settings to preserve the preconfigured settings, rename it, and then click **Clone**. In this example, it is simply called "QuickStart-Wireless-Only2".

Because hives are a fundamental concept in Aerohive architecture, the following description is provided in case you unfamiliar with them. A hive is a group of devices that exchange information with each other to coordinate client access, provide best-path forwarding, and enforce QoS policy. Through these coordinated actions based on shared information, hive members can provide the following services:

- Consistent QoS (Quality of Service) policy enforcement across all hive members
- Coordinated and predictive wireless access control that provides seamless layer 2 and layer 3 roaming to clients moving from one hive member to another (The members of a hive can be in the same subnet or different subnets, allowing clients to roam across subnet boundaries.)
- Dynamic best-path routing for optimized data forwarding and network path redundancy
- Automatic radio frequency and power selection for wireless mesh and access radios
- Tunneling of client traffic from one hive member to another, such as the tunneling of guest traffic from a device in the internal network to another device in the corporate DMZ

Hive members use WPA-PSK (Wi-Fi Protected Access with a preshared key) to exchange keys and secure wireless hive communications. To authenticate and encrypt wireless hive communications, hive members use WPA with a preshared key and CCMP (AES) encryption. CCMP is a rough acronym for "Counter Mode with Cipher Block Chaining Message Authentication Code Protocol" and makes use of AES (Advanced Encryption Standard).

After you click **Clone**, the network configuration wizard advances to *Configure Interfaces & User Access*.

EXAMPLE 3: DEFINING AN SSID

An SSID (service set identifier) is an alphanumeric string that identifies a group of security and network settings that wireless clients and access points use when establishing wireless communications with each other. In this example, you create a new SSID that uses a PSK (preshared key) for client authentication and data encryption.

A PSK is the simplest way to provide client authentication and data encryption. A PSK authenticates clients by the simple fact that the clients and access point have the same key. For data encryption, both the AP and clients use the PSK as a PMK (pairwise master key) from which they generate a PTK (pairwise transient key), which they use to encrypt unicast traffic. Although the PSK/PMK is the same on all clients, the generated PTKs are different not only for each client but for each session.

Because of its simplicity, a PSK is suitable for testing and small deployments; however, there is a drawback with using PSKs on a larger scale. All clients connecting through the same SSID use the same PSK, so if the key is compromised or a user leaves the company, you must change the PSK on the APs and all their clients. With a large number of APs and clients, this can be very time-consuming. For key management solutions that are more suitable for large-scale deployments, consider the WPA/WPA2 802.1X (Enterprise) and private PSK options. For the present goal of showing how to use HiveManager to configure an SSID, the PSK method works well.

1. To create an SSID, click **Choose** next to SSIDs, click **New** in the Choose SSIDs dialog box, enter the following in the New SSID sub-panel that appears, and then click **Save**:

Profile Name: `test1-psk` (A profile name does not support spaces, although an SSID name does.)

The profile name is the name for the entire group of settings for an SSID. It can include default or modified data rate settings, apply DoS (denial of service) policies and MAC filters, and specify the SSID name that the AP advertises in beacons and probe responses. The profile name—not the SSID name (although they can both be the same)—is the one that appears in the *Choose SSIDs* dialog box.

When you enter a profile name, HiveManager automatically fills in the SSID field with the same text string. By default, the profile and SSID names are the same, yet they can also be different. You can create many different SSID profiles, each with a different group of settings, but each with the same SSID name. For users, their clients connect to the same SSID at different locations. From the AP perspective, each SSID profile applies a different group of settings.

SSID: `test1-psk`

This is the SSID name that clients discover from beacons and probe responses.

SSID Broadcast Band: `2.4 GHz & 5 GHz (11n/a + 11n/b/g)`

Most Aerohive APs have two radios: a 2.4 GHz radio, which supports 802.11n/b/g, and a 5 GHz radio, which supports 802.11n/a. On all AP models except the AP110, both radios can function concurrently. This setting broadcasts the SSID on the `wifi0` interface, which is bound to the 2.4 GHz radio, and the `wifi1` interface, which is bound to the 5 GHz radio.

As seen earlier in this chapter, one Aerohive AP is deployed as a mesh point; that is, it does not have an Ethernet connection but connects to the wired network over a wireless backhaul link through another AP that does have an Ethernet connection (see ["Example 5: Assigning the Configuration to APs" on page 42](#)). Because of this, the APs must have at least one radio in dual mode for both wireless backhaul communications and client access.

Description: Test SSID for learning how to use the GUI; remove later

This note and the very name "test1-psk" are deliberately being used as reminders to replace this configuration later with an SSID profile and SSID name that you really intend to use in your WLAN.

SSID Access Security: WPA/WPA2 PSK (Personal)

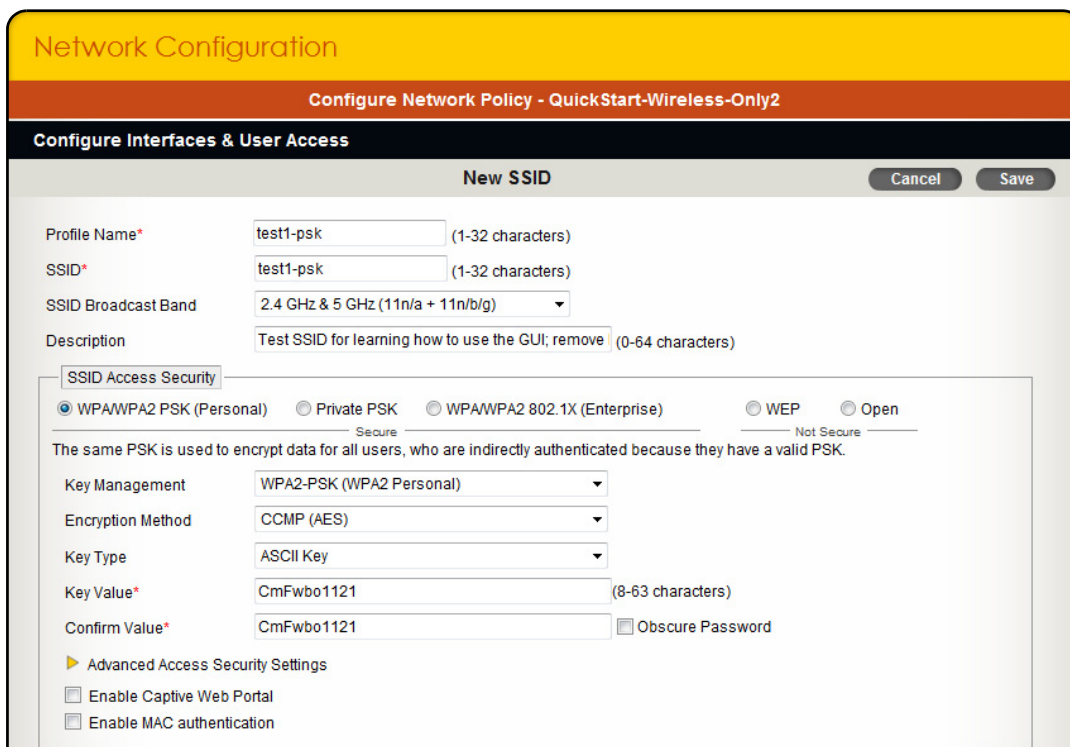
(((1))) By default, when an Aerohive AP hosts a WPA/WPA2 PSK (Personal) SSID, it uses WPA2 for key management and CCMP (AES) for encryption. Also, the PSK text string is in ASCII format by default. If you want to change these settings and others, choose different options from the drop-down lists and expand the Advanced Access Security Settings **section**.

Key Value and Confirm Value: CmFwbo1121 (To see the text strings that you enter, clear the **Obscure Password** check box.)

With these settings, the AP and its clients can use either WPA or WPA2 for key management, CCMP (AES) or TKIP for data encryption, and the preshared key "CmFwbo1121" as the pairwise master key from which they each generate pairwise transient keys.

Enable Captive Web Portal: (clear)

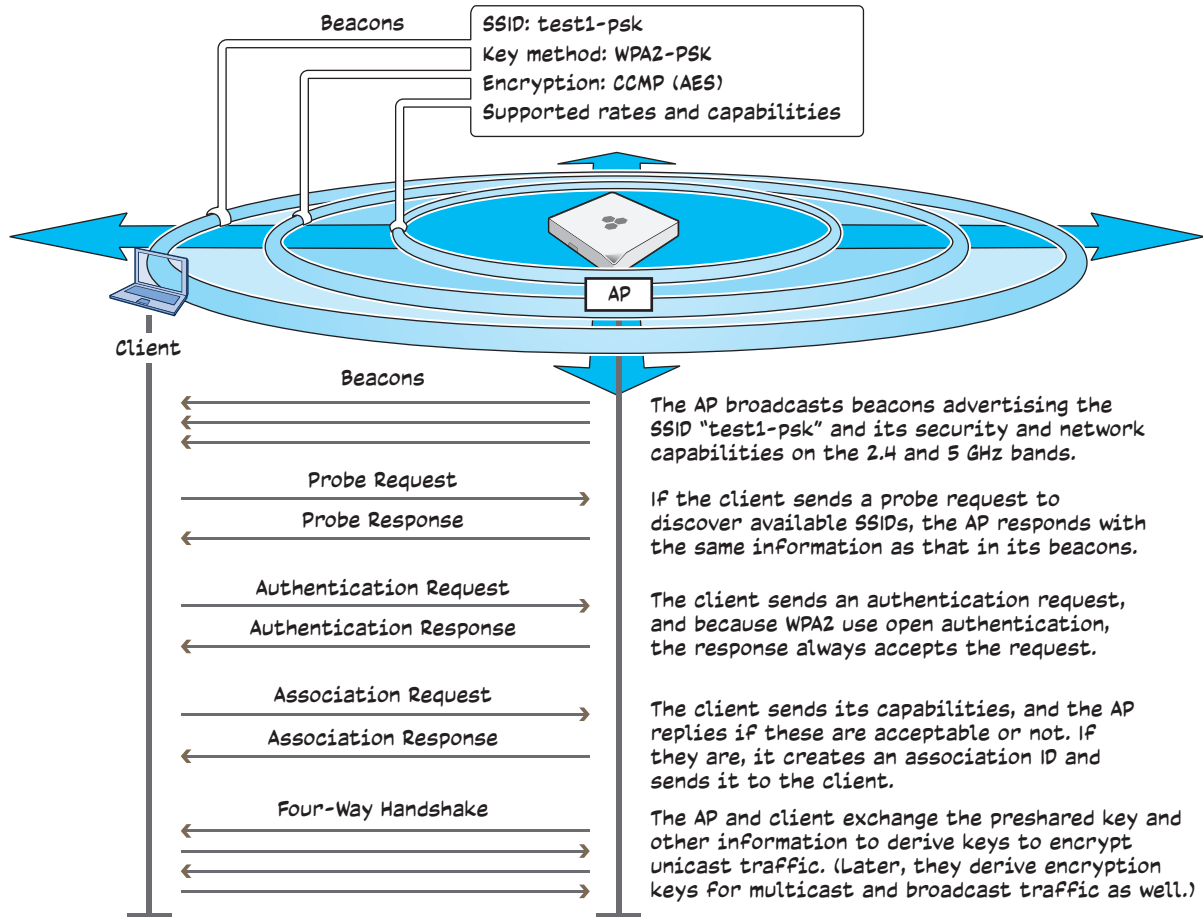
Enable MAC Authentication: (clear)



2. Highlight **test1-psk** in the *Choose SSIDs* dialog box, and then click **OK**.

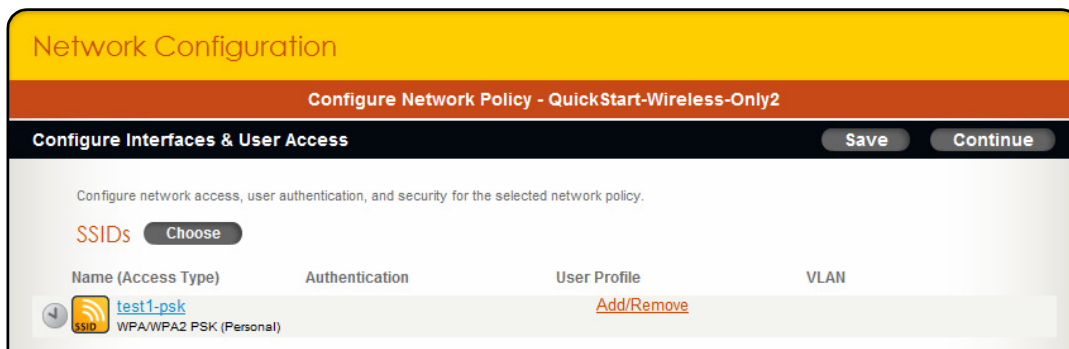
To see how the AP advertises the SSID and how clients form associations with it, see [Figure 5 on page 39](#).

Figure 5 How a client discovers the SSID and forms a secure association



EXAMPLE 4: ASSIGNING A USER PROFILE AND VLAN TO THE SSID

Because the SSID that you created in "Example 3: Defining an SSID" on page 37 does not require a captive web portal or RADIUS authentication, the Authentication section to the right of the SSID profile name is empty. However, there is now an Add/Remove link in the User Profile section. You must define a user profile and apply it to the traffic of users accessing the network through this SSID.



1. To create and assign a user profile to the SSID, click **Add/Remove** in the User Profile section, click **New** in the *Choose User Profiles* dialog box that appears, and then enter the following:

Name: test1-user

Attribute Number: 2

When an SSID uses WPA/WPA2 PSK (Personal), WEP, or Open for access security, an AP can assign only one user profile to all traffic on that SSID.² In these cases, APs use the user profile attribute to associate that user profile with the SSID. When the access security method is WPA/WPA2 802.1X (Enterprise), WEP-802.1X, or when the SSID has MAC authentication or a captive web portal with user authentication enabled, the AP can use returned RADIUS attributes for authenticated users to assign multiple user profiles to traffic on the same SSID. Similarly, when the access security method is Private PSK, the SSID can also support the application of multiple user profiles. A AP learns the attributes of user groups to which different valid private PSK users belong and maps them to different user profiles with matching attributes. In this example, any unused attribute value will suffice.

Network or VLAN-only Assignment: 1

This assigns user traffic to VLAN 1, which is the native VLAN.

Description: Test user profile for learning how to use the GUI; remove later

This note and the user profile name "test1-user" are being used as reminders to replace this later with one that you really intend to use in your WLAN.

Manage users for this profile via User Manager: (clear)

This option is only relevant when you want User Manager administrators and operators to assign private PSK user keys to users. For more information about User Manager, see the online HiveManager and User Manager Help.

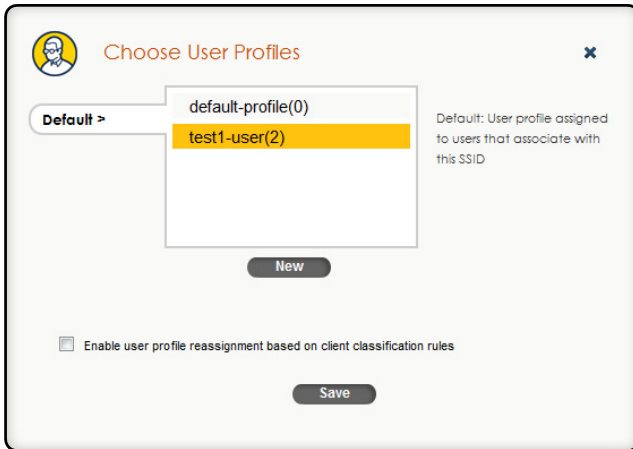
The screenshot shows a web-based configuration interface. At the top, there's a yellow banner with the text 'Network Configuration'. Below it is a red banner with 'Configure Network Policy - QuickStart-Wireless-Only2'. Underneath is a black banner with 'Configure Interfaces & User Access'. The main content area is a white dialog box titled 'New User Profile' with 'Cancel' and 'Save' buttons in the top right. The dialog contains the following fields:

- Name ***: A text input field containing 'test1-user' with a character count '(1-32 characters)'.
- Attribute Number ***: A text input field containing '2' with a character count '(1-4095)'.
- Network or VLAN-only Assignment ***: A dropdown menu showing '1' with a '+' icon and a document icon.
- Description**: A text input field containing 'Test user profile for learning how to use the GUI;' with a character count '(0-64 characters)'.
- Manage users for this profile via User Manager**

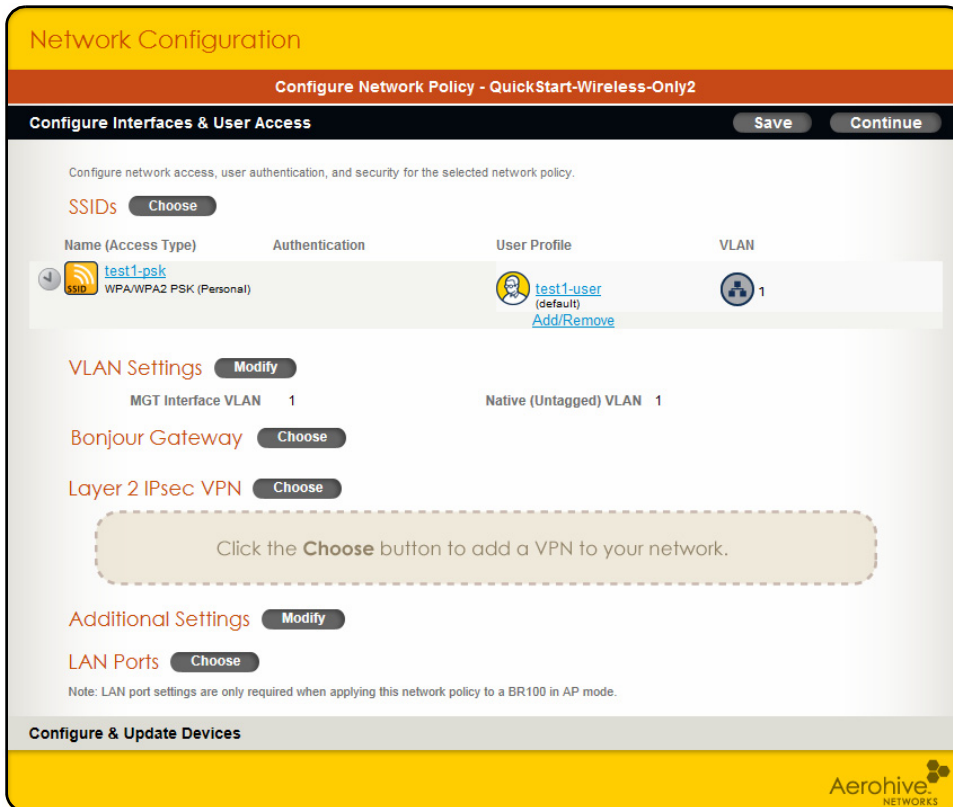
2. Leave the various settings in the *Optional Settings* section as they are, and then click **Save**.

2. Although an AP can only assign one user profile to all clients connecting through an SSID that uses WPA/WPA2 PSK (Personal), WEP, or Open, it can reassign user profiles based on the MAC OUI, device domain name, or OS of the client. See the HiveManager Help for more information about user profile reassignment.

- Highlight **test1-user(2)** in the *Choose User Profiles* dialog box, clear **Enable user profile reassignment based on client classification rules**,³ and then click **Save**.

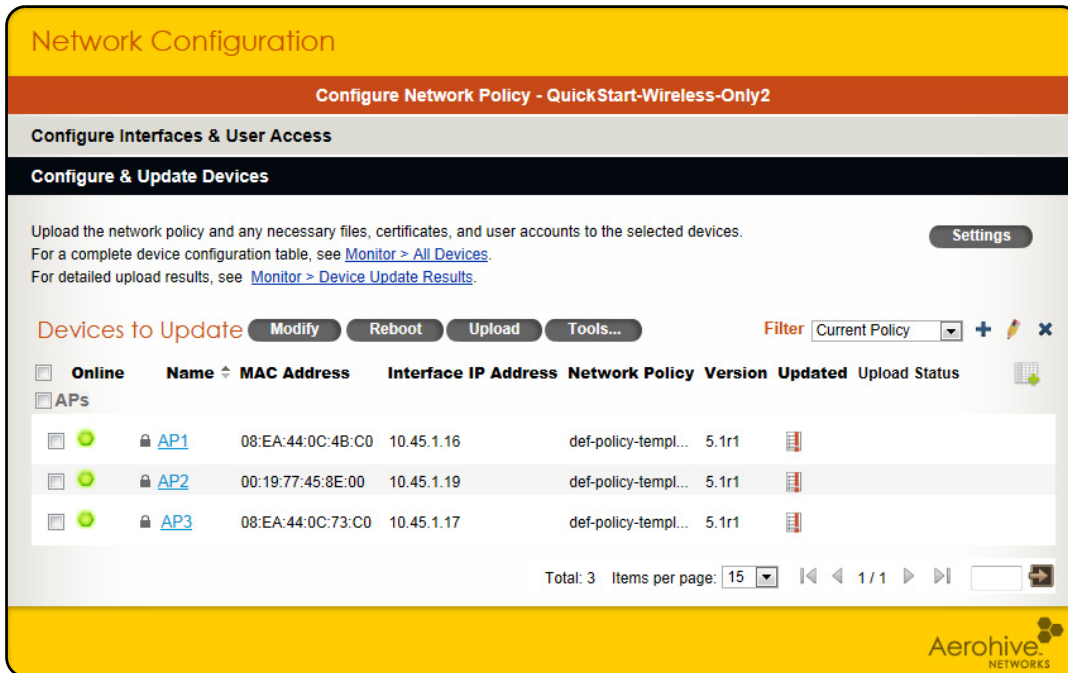


- Leave the VLAN Settings at their default values—MGT interface VLAN = 1, native (untagged) VLAN = 1—and do not add a Layer 2 IPsec VPN to the network policy. Additionally, for this example, you do not have to configure or modify any of the additional settings, so leave those as they are as well.



- When you enable this option, an AP might reassign traffic from the selected user profile to another profile based on client classification rules regarding client MAC address or OUI, operating system, and device domain if such rules are defined in the selected user profile and if a client matches one of them.

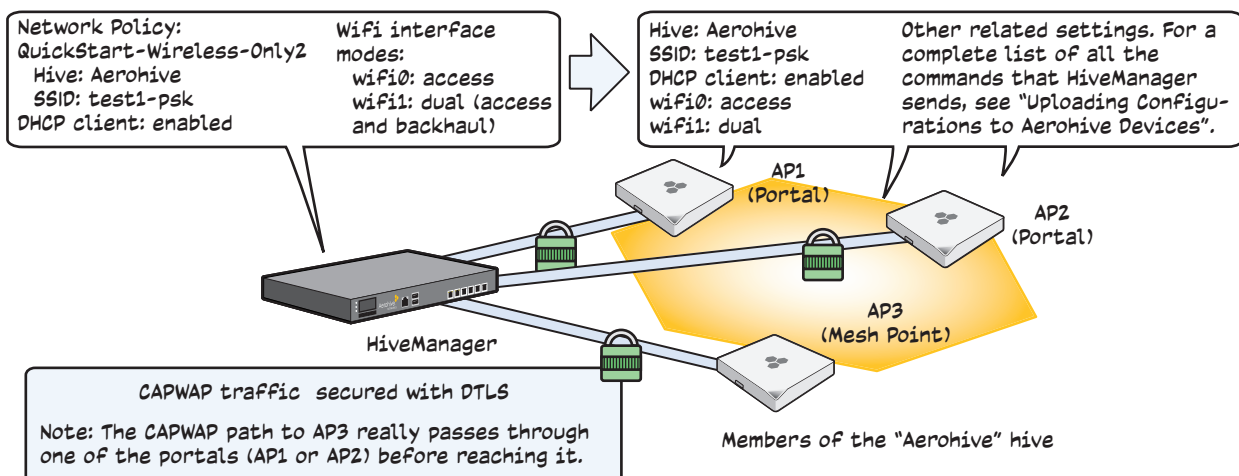
- Click **Continue** or **Configure & Update Devices** to save all the settings and advance the network configuration wizard to *Configure & Update Devices*. You can see the three APs that you connected to HiveManager in "Example 1: Connecting APs to HiveManager" on page 28.



EXAMPLE 5: ASSIGNING THE CONFIGURATION TO APs

After completing the steps in the previous examples, assign the network policy and some device-level settings to the APs and then push the configuration to them. The transfer of AP configuration assignments is presented conceptually in Figure 6. Finally, if you need to change the country code for the APs, see the instructions at the end of this chapter.

Figure 6 AP configuration assignments



Assigning Configurations

1. Click **AP1** to open the *Edit Device* dialog box.
2. Enter the following, leave the other settings as they are, and then click **Save**:

Network Policy: QuickStart-Wireless-Only2

This is the network policy that you created in ["Example 2: Creating a Network Policy with a Hive"](#) on page 35.

Use one radio (2.4 GHz) for client access and one radio (5 GHz) for client access and a mesh link:
(select)

This is the default radio mode setting, so you do not need to change it. However, it is mentioned here to emphasize the importance of having at least one radio in backhaul mode so that AP3, which is functioning as a mesh point, can form a wireless backhaul link with one of the other devices functioning as portals.

Credentials: (click to expand the section)

New Admin Name: It is a good security practice to change the default name of the root AP admin (Default: *admin*). Enter an alphanumeric string from 3 to 20 characters long.

New Password: Change the password for the root AP admin. (Default: *aerohive*) It can be an alphanumeric string from 5 to 32 characters long.

Confirm New Password: Enter the password again to confirm its accuracy. To see the text strings you entered in the two password fields, clear the **Obscure Password** check box.

3. Repeat the previous steps for AP2 and AP3.

Uploading Configurations to Aerohive Devices

At this point, you have finished assigning configurations to the AP objects on HiveManager, and it is time to push these configurations from HiveManager to the physical AP devices. Because this is the first time to use HiveManager to update the configuration on these APs, you must perform a full upload, which requires rebooting the APs to activate their new configurations.

Because AP3 is a mesh point and the update involves changing its hive—from *hive0* to *Aerohive*—you must make sure to update its configuration before updating the configurations on AP1 and AP2. If you upload the configuration on all of them at the same time and schedule them to reboot too quickly (say, 1 second after the upload process completes), there is a chance that the portal through which the configuration for the mesh point is passing will reboot before the mesh point finishes receiving its configuration. If that happens, only the configuration on the portals will be updated. As a result, the portals will become members of a different hive (*Aerohive*) from the mesh point (*hive0*). The mesh point will no longer be able to connect to the network through a portal using *hive0* and will become disconnected from the network and from HiveManager.

To avoid the preceding scenario, you must first change the hive on mesh points while they can still connect to the network. After you change the hive to which the mesh points belong, they will lose network and HiveManager connectivity temporarily until you update the configuration on the portals. After they also join the new hive, the mesh points will once again be able to connect through their portals to the network and to HiveManager. For more information on this topic, see ["Updating Devices in a Mesh Environment"](#) on page 24.

1. In *Configure & Update Devices*, click **Settings**.
The *Device Upload Options* dialog box appears.
2. Enter the following, and then click **Save**:

Auto (First time with complete upload; subsequent uploads compare with running AP config): (select)

When initially sending the configuration to APs, HiveManager must perform a complete upload, which it does automatically. After that, it automatically performs a delta upload by comparing the current configuration for the AP stored on HiveManager with that running on the AP and then uploading only the parts that are different. The other three options for uploading configurations are as follows:

Complete Upload: This option uploads the complete configuration to the selected APs and reboots them to activate their new configuration.

Delta Upload (Compare with last HiveManager config): This option uploads only the parts of the configuration that were not previously pushed to the APs from HiveManager.

Delta Upload (Compare with running Aerohive device config): This option uploads only the changes to the configuration based on a comparison of the current configuration for the selected APs on HiveManager with the current configuration running on the APs.

Uploading a delta configuration does not require activation by rebooting the AP and is, therefore, less disruptive. However, before HiveManager can upload a delta configuration to a managed AP, it must first upload the full configuration and activate it by rebooting the AP. After that, you can use the delta options.

	<i>If there is any failure when performing a delta upload, use a complete upload the next time.</i>
--	---

Activate after: (select) Leave the default interval of 5 seconds.

The three options for controlling the activation of an uploaded configuration are as follows:

Activate at: Select this option and set the time when you want the updated APs to activate their new configuration. This is a good choice if you want to stagger the activation, or if you want to load a configuration now but activate it when the network is less busy. To use this option accurately, both HiveManager and the managed APs need to have NTP enabled.

Activate after: Select this option to load a configuration on the selected APs and activate it after a specified interval. The range is 0 – 3600 seconds; that is, immediately to one hour. The default is 5 seconds.

Activate at next reboot: Select this option to load the configuration and not activate it. The loaded configuration is activated the next time the AP reboots.

Upload and activate configuration: (select)

Upload and active captive web portal pages and server key: (clear)

Upload and activate certificates for RADIUS and VPN services: (clear)

Upload and activate employee, guest, and contractor credentials: (clear)

It is only necessary to push the configuration itself to the APs. No captive web portal files, digital certificates, or user accounts need to be transferred at this time.

3. Select the check box for AP3, and then click **Upload**.

HiveManager begins transferring the configuration to AP3 and displays the progress in the Upload Status column.

After AP3 reboots to activate its new configuration, it tries to reconnect with HiveManager. However, it cannot do so because it is a mesh point that now belongs to the Aerohive hive while its portals—AP1 and AP2—are still using their original configurations in which they are members of hive0. This loss of connectivity will continue until you update the portals, which you do next.

4. Select the check boxes for AP1 and AP2, and then click **Upload**.

After they reboot and activate their new configurations, check the status of their CAPWAP connections by looking at the CAPWAP column on the Monitor > Devices > Access Points > APs page with the View mode set as Display Device Status Information. After a few minutes, all three APs will reestablish their connections.

Updating the Country Code

For APs intended for use in the United States, the region code is preset as "FCC"—for "Federal Communications Commission"—and the country code is preset as "United States". If this is the case, you can skip this section.

If the preset region code for the managed APs is "World", you must set the appropriate country code to control the radio channel and power selections that APs can use. If this is the case, set the country code as follows:

1. On the Monitor > Devices > Access Points > Aerohive APs page, select the check box for AP3, and then click **Update > Update Country Code**.⁴
2. In the *Update Country Code* dialog box, enter the following, and then click **Upload**:

Choose the country where the device is deployed from the New Country Code drop-down list.

	<i>Be sure to choose the correct country. An incorrect choice might result in illegal radio operation and cause harmful interference to other systems.</i>
--	--

In the Activate after field, set an interval in seconds after which the AP reboots to activate the updated country code settings.

Make sure that the check box for AP3 is selected.

HiveManager updates the country code on AP3 and then reboots it after the activation interval that you set elapses. After AP3 reboots, it puts the appropriate radio settings for the updated country code into effect.

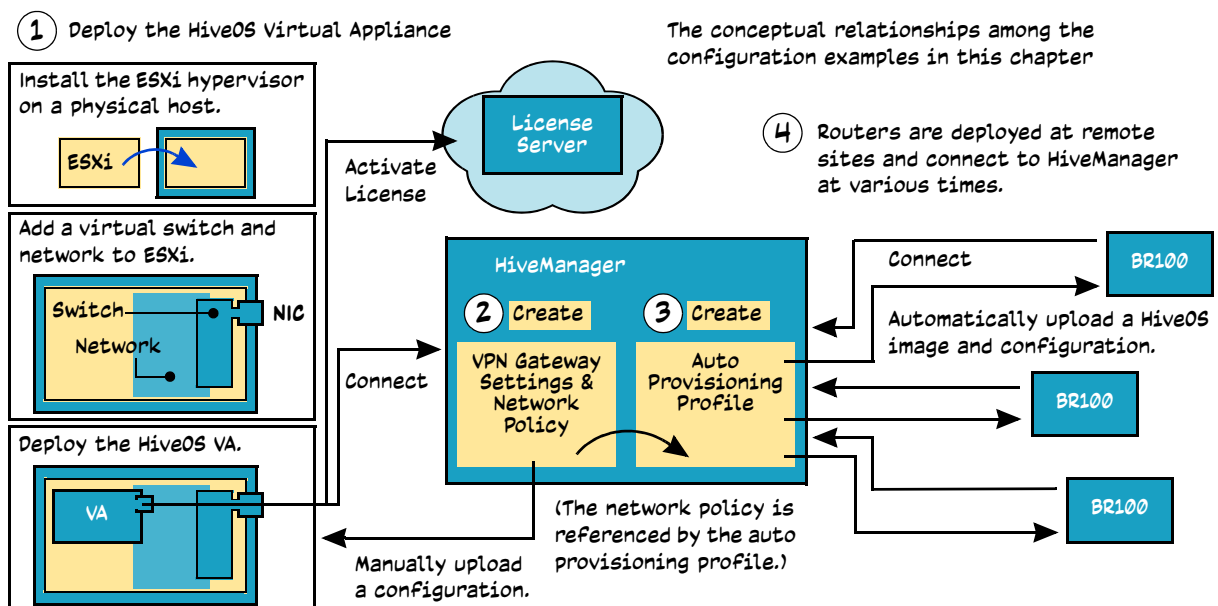
3. Select the check boxes for the two portals AP1 and AP2, and then repeat the previous steps to update their country codes.
After they reboot, all the APs will have the correct country code, will reform into a hive, and reconnect to HiveManager.

4. When updating the country code on APs in a mesh environment, you do not want the rebooting of portals to interrupt the data path between the HiveManager and mesh points before they can complete their update process. Therefore, try to update and reboot mesh points first. Then, update and reboot the portals. See ["Updating Devices in a Mesh Environment" on page 24](#).

Chapter 3 Wireless and Routing Configuration

This chapter includes a series of configuration examples showing how to create networks at various sites connected by IPsec VPN tunnels between routers and a Layer 3 VPN Gateway. The following examples present the main configuration steps:

- ["Example 1: Deploying a HiveOS Virtual Appliance" on page 48](#)
Load a VMware ESXi hypervisor on a server connected to the network and then deploy VMware for the HiveOS Virtual Appliance on the hypervisor. This example includes the following subsections:
 - ["Installing an ESXi Hypervisor on a Server" on page 48](#)
 - ["Creating and Activating Virtual Networks and Mapping Network Settings" on page 49](#)
 - ["Deploying a HiveOS Virtual Appliance as a Layer 3 VPN Gateway" on page 52](#)
- ["Example 2: Configuring the VPN Gateway and Routers" on page 60](#)
Use HiveManager to configure device settings for the VPN gateway and a network policy for the routers.
- ["Example 3: Auto Provisioning the Routers" on page 66](#)
Define an auto provisioning profile so that HiveManager automatically pushes the configuration to the routers whenever they come online and contact HiveManager.
- ["Example 4: Deploying Routers on the Network" on page 67](#)
Connect routers to the network so that they can form a CAPWAP connection to HiveManager and then download the latest HiveOS firmware image and configuration settings.



EXAMPLE 1: DEPLOYING A HIVEOS VIRTUAL APPLIANCE

The HiveOS Virtual Appliance is a virtual machine that you can download in an .ova (Open Virtual Appliance) file and deploy on a VMware ESXi hypervisor running on a physical device on your corporate network. The ESXi hypervisor is a server dedicated to running VMs (virtual machines), and VMs are containers that can run their own operating systems and execute applications. If you do not already have VMware ESXi deployed, you can obtain free ESXi software from the following location:

www.vmware.com/products/vsphere/esxi-and-esx/overview.html. You can download the AH_HiveOS_VA .ova file from HiveManager: Monitor > All Devices > Update > Download HiveOS Virtual Appliance.

Although a HiveOS Virtual Appliance is 32-bit Linux, ESXi requires hardware that is 64-bit capable (Core 2 family). Remember to enable the virtualization feature in the BIOS of the host device. Consult your hardware documentation for instructions. Your virtualization host must have one or two physical network adapters and a minimum of 512 MB of RAM and 256 MB of disk space.



512 MB is the initial RAM setting for the HiveOS Virtual Appliance, but you can increase it. A single HiveOS Virtual Appliance uses 256 MB of disk space.

Before beginning the deployment, connect Ethernet cables to the physical network adapters that you intend to use. The HiveOS Virtual Appliance has two interfaces: WAN (eth0) and LAN (eth1). You can use the WAN interface only or both interfaces (see "Creating and Activating Virtual Networks and Mapping Network Settings" on page 49). To install VMware ESXi from a bootable CD, make sure the BIOS is able to boot from the CD/DVD drive. See the hardware vendor documentation for information on changing the boot order.

You also need to install VMware vSphere Client on your management system and use it to access the ESXi hypervisor and HiveOS Virtual Appliance. Computers running Windows support vSphere Client.¹

Installing an ESXi Hypervisor on a Server

Follow these steps to install an ESXi hypervisor on a server or dedicated PC that meets the minimum requirements noted above.



The following procedure assumes that you have a keyboard and monitor attached to the device you intend to make the ESXi host.

1. From the VMware website (see link above), register for a free account, and download ESXi 4x or later. ESXi 3 does not support the HiveOS Virtual Appliance.
2. Burn the ESXi image to a CD or DVD. You will use this disc to install the image on the virtualization host.
3. Load the disc with the ESXi image on the host and boot it up from the disc.
4. After accepting the end user license agreement, follow the onscreen VMware ESXi installer instructions to select a hard disk on which to install ESXi, set a keyboard layout preference, and define an ESXi hypervisor root admin password. When the installation is complete, remove the disc and reboot the system.
5. After the system reboots, press the **F2** key to log in to the ESXi Direct Control User Interface using the root admin password that you just set. Check if the host received its network settings through DHCP. If so, note its IP address. If not, configure static network settings through the onscreen interface.
6. On your management system, open a browser and make an HTTP connection to the ESXi hypervisor IP address. Click **Download vSphere Client**, and download and install VMware vSphere Client on your system.

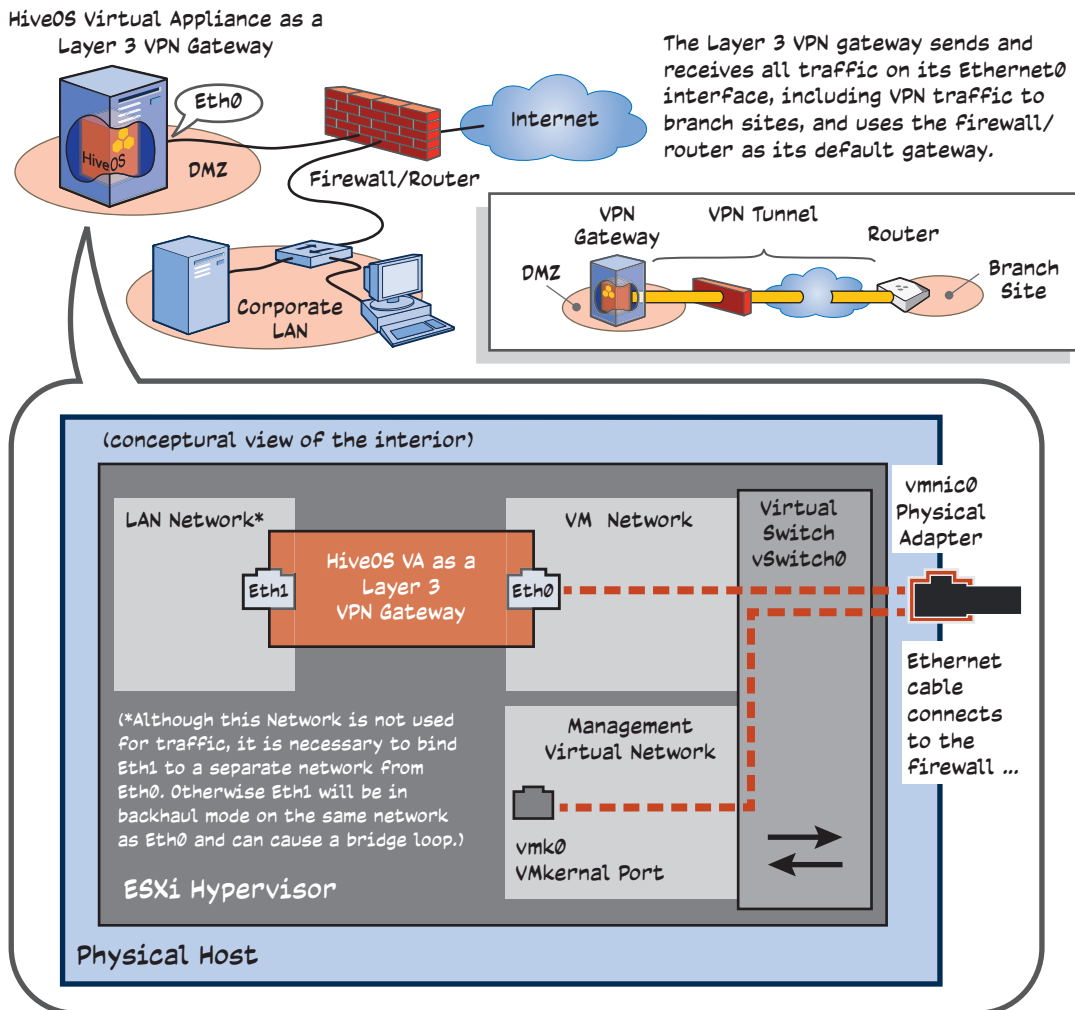
1. VMware provides release notes for each version of vSphere. For example, the release notes for vSphere 5.0 are available at www.vmware.com/support/vsphere5/doc/vsphere-esx-vcenter-server-50-release-notes.html

Creating and Activating Virtual Networks and Mapping Network Settings

By default, ESXi has two virtual networks: Management Network and VM Network. Both networks are bound to the vSwitch0 virtual switch, which in turn connects to the vmnic0 physical adapter. The interface for the ESXi hypervisor is bound to the management network. The interfaces of the virtual machines that you deploy—such as the HiveOS Virtual Appliance—are bound to the VM network and to another network that you define. If the physical host on which you are running the ESXi hypervisor has another physical adapter (vmnic1), you can create another virtual network and virtual switch and connect them to the vmnic1 adapter. You can then bind VM interfaces to the new network. For the HiveOS Virtual Appliance, you have two options for connecting it to the network, depending on whether you use one or two physical adapters on the physical host:

HiveOS VA with one interface: You can use the Eth0 interface only. Connect it to the VM network, which links to the vmnic0 physical adapter, which in turn is cabled to the firewall interface in the DMZ. Create a second virtual network for the Eth1 interface but, because it is unused, do not bind it to anything. In this case, the device hosting the HiveOS Virtual Appliance needs only one physical network adapter as shown in [Figure 1](#).

Figure 1 HiveOS Virtual Appliance using only its Ethernet0 interface

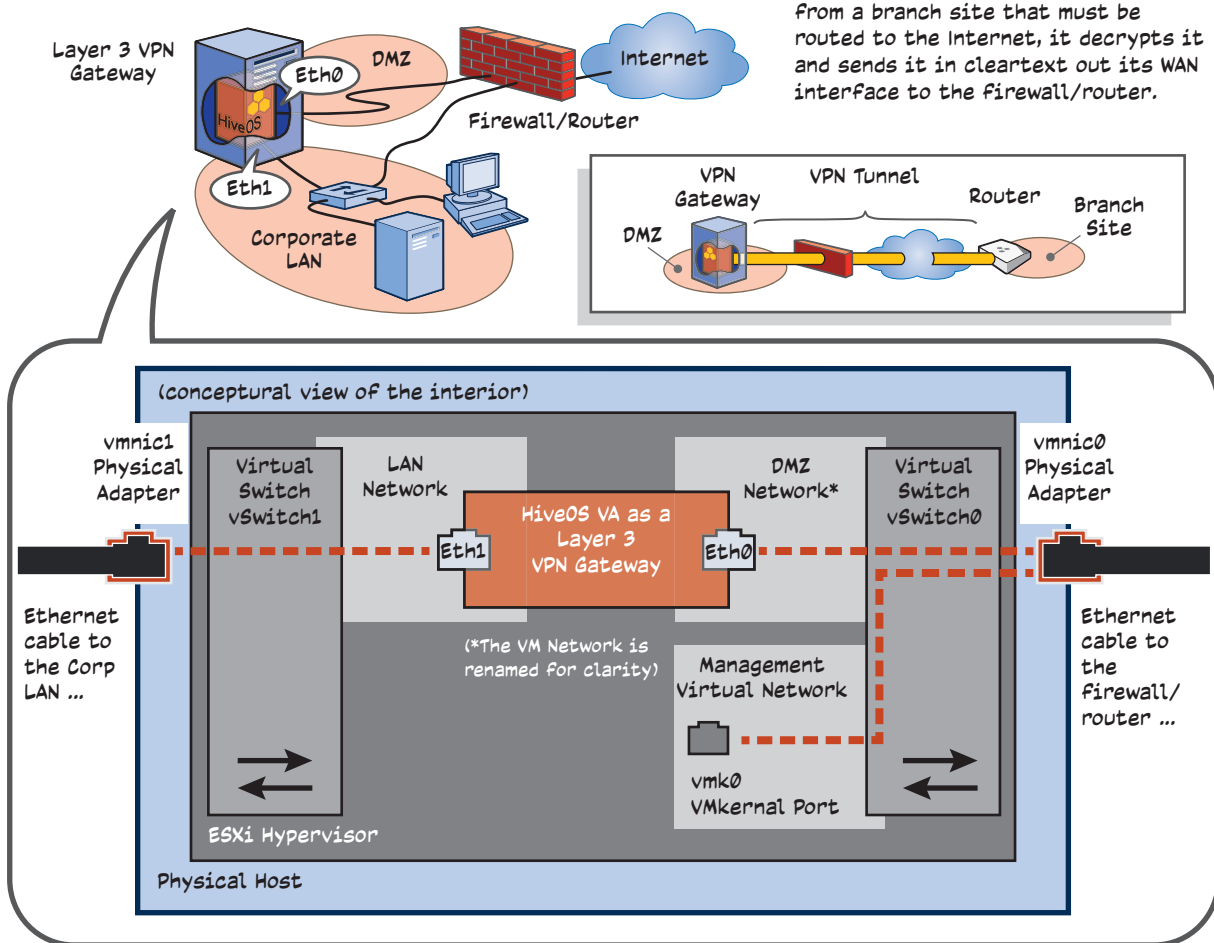


HiveOS VA with two interfaces: You can bind Eth0 and Eth1 to different virtual networks, which link to separate physical adapters—Eth0 to vmnic0 and Eth1 to vmnic1. In this case, the physical host must have at least two adapters as shown in Figure 2.

Figure 2 HiveOS Virtual Appliance using its Eth0 and Eth1 interfaces

The Layer 3 VPN gateway sends and receives tunneled traffic on its Eth0 interface in the DMZ. It sends and receives traffic to and from the corporate LAN on its Eth1 interface.

The VPN gateway uses the firewall/router as its default gateway. If it receives traffic through a tunnel from a branch site that must be routed to the Internet, it decrypts it and sends it in cleartext out its WAN interface to the firewall/router.



Configuration instructions for the first option—the method using just the Eth0 interface—are provided below. For complete configuration steps for setting up a HiveOS Virtual Appliance using both its Eth0 and Eth1 interfaces, see *The New Features Guide for HiveOS and HiveManager 5.0r1*. The main difference between the configuration in 5.0r1 and 5.0r3 and later releases is that a network policy is no longer applied to Layer 3 VPN gateways. After 5.0r3, all VPN gateway settings are device-based rather than policy-based.

Promiscuous Mode

When a Layer 3 VPN gateway exchanges dynamic routing information with routers on the corporate LAN or receives multicast traffic, you might have to enable promiscuous mode on the port group for the interface through which the gateway communicates with its dynamic routing peers or multicast routers. When using two vSwitches and two physical NICs, the VPN gateway terminates tunnels on Eth0 and communicates with dynamic routing peers and multicast routers through Eth1. When using just one vSwitch and one NIC, then all traffic—including dynamic routing communications and multicast traffic—traverses Eth0.

Read the following descriptions to learn when you must enable promiscuous mode and on which port group, and when not to enable it:

- For a new deployment of a HiveOS Virtual Appliance, promiscuous mode is not required.
- For any deployment that does not support dynamic routing and multicasting, promiscuous mode is not required.
- When upgrading a Layer 3 VPN gateway from HiveOS 5.0 to HiveOS 5.1r2 or 5.1r3, or from 5.0 to 5.1r1 and then to 5.1r2 or 5.1r3, and both the Eth0 and Eth1 interfaces are used, you must enable promiscuous mode on the port group to which the Ethernet1 interface belongs. If only the Ethernet0 interface is used, enable promiscuous mode on its port group.



Other port groups on the vSwitches do not need to be in promiscuous mode.

To create a port group, also referred to as a "destination network" in hypervisor, do the following:

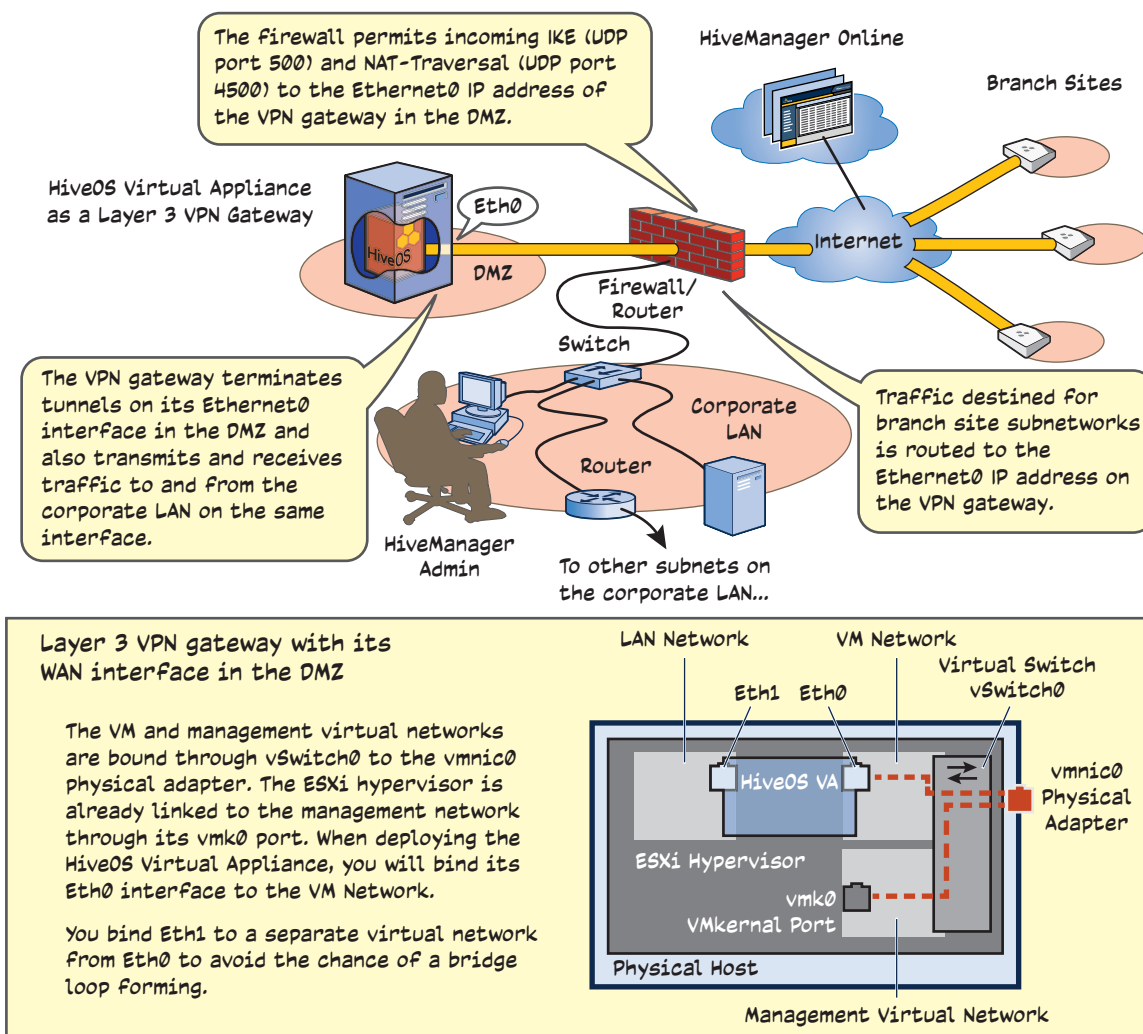
1. Use your vSphere Client to log in your ESX or ESXi hypervisor, select the host on which you intend to install the HiveOS Virtual Appliance, and then click **Configuration > Networking**.
2. Click **Properties** for the vSwitch on which you want to create the port group. When you are going to use just one interface on the HiveOS Virtual Appliance, click **Properties** for vSwitch0. When you are going to use two interfaces, click **Properties** for vSwitch1.
3. In the *vSwitch0 Properties* or *vSwitch1 Properties* dialog box that appears, click **Add**.
4. In the *Add Network Wizard* dialog box, select **Virtual Machine** for the connection type, and then click **Next**.
5. In the *Port Group Properties* section, type a name in the Network Label field and choose **None (0)** from the VLAN ID drop-down list, and then click **Next**.
6. Check your settings in the *Preview* pane, and then click **Finish**.
7. Highlight the port group that you just created, click **Edit**, and then click the **Security** tab.
8. Select **Promiscuous Mode**, choose **Accept**, click **OK**, and then click Close.

When deploying the HiveOS Virtual Appliance, be sure to choose the port group that you just defined with promiscuous mode enabled.

Deploying a HiveOS Virtual Appliance as a Layer 3 VPN Gateway

The following procedure explains how to deploy a HiveOS Virtual Appliance as a Layer 3 VPN gateway so that its Eth0 interface connects to the DMZ network. The firewall must allow inbound IKE and NAT-Traversal traffic (UDP ports 500 and 4500 respectively) to the IP address of the Eth0 interface. Finally, you must either manually set static routes on the corporate LAN to send traffic destined for the branch site subnetworks to the Eth0 interface or employ a dynamic routing protocol—OSPF or RIPv2—on the corporate LAN to exchange routes with the Layer 3 VPN gateway and manage the routing automatically as shown in [Figure 3](#).

Figure 3 Layer 3 VPN gateway deployment

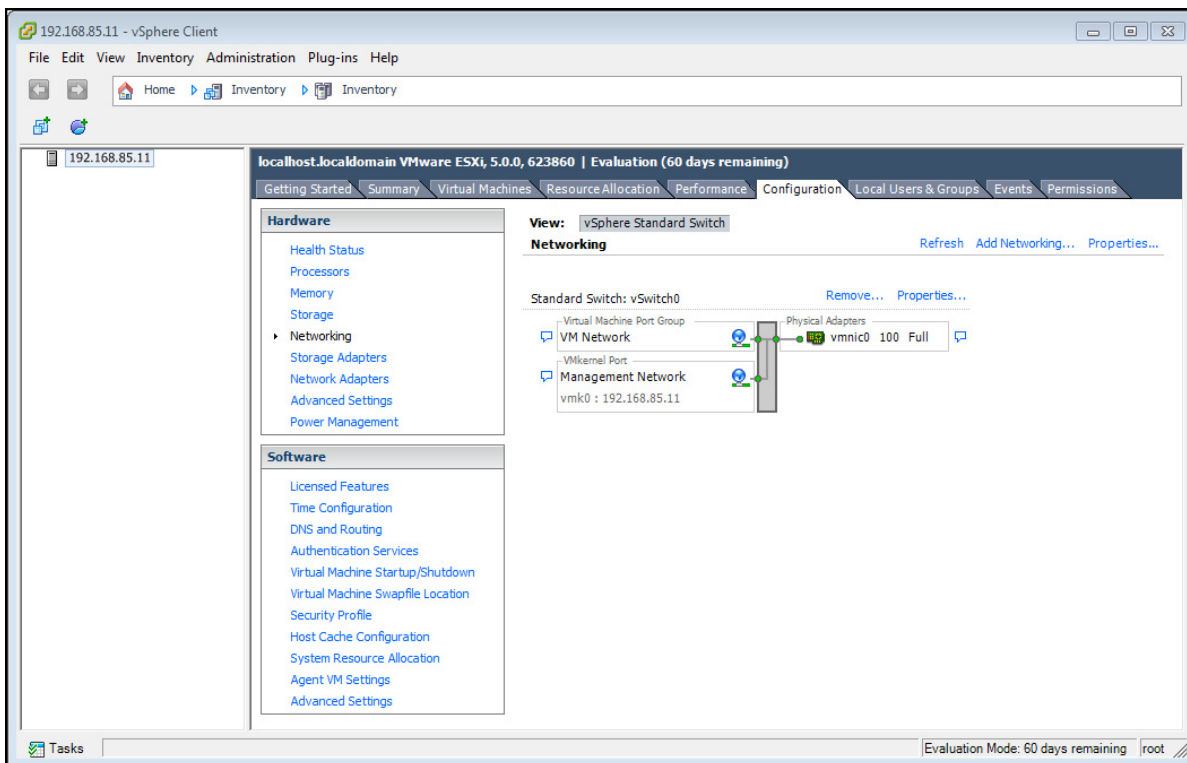


If you are upgrading a Layer 3 VPN gateway from a HiveOS release prior to 5.1r2 to HiveOS 5.1r2 or 5.1r3 and are using dynamic routing protocols, you must set the port group to which the Ethernet0 interface belongs in promiscuous mode. For new installations of the .ova file from HiveOS 5.1r2 and later, this is unnecessary. For more information, see ["Promiscuous Mode" on page 51](#).

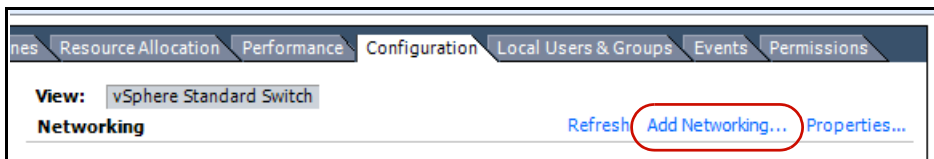
Creating a New Virtual Network and Switch

Use the following steps to log in to the ESXi hypervisor and create a new virtual network and switch.

1. Launch VMware vSphere Client, enter the IP address that you defined for the ESXi hypervisor, and then log in with the root admin credentials you set in the previous section. Select the hypervisor in the left panel, and then click **Configuration > Networking**.



2. To create a new virtual network and a virtual switch (vSwitch1) for this network, click **Add Networking**.



3. Select **Virtual Machine** for Connection Type, and then click **Next**.

Connection Type
Networking hardware can be partitioned to accommodate each service that requires connectivity.

Connection Type
Network Access
Connection Settings
Summary

Connection Types

- Virtual Machine**
Add a labeled network to handle virtual machine network traffic.
- VMkernel**
The VMkernel TCP/IP stack handles traffic for the following ESXi services: VMware vMotion, iSCSI, NFS, and host management.

4. Select **Create a vSphere standard switch**, select the **vmnic1** check box, and then click **Next**.

Virtual Machines - Network Access
Virtual machines reach networks through uplink adapters attached to vSphere standard switches.

Connection Type
Network Access
Connection Settings
Summary

Select which vSphere standard switch will handle the network traffic for this connection. You may also create a new vSphere standard switch using the unclaimed network adapters listed below.

- Create a vSphere standard switch**
Broadcom Corporation NetXtreme BCM5721 Gigabit Ethernet
 vmnic1
Speed: Down
Networks: None
- Use vSwitch0**
Broadcom Corporation NetXtreme BCM5721 Gigabit Ethernet
 vmnic0
Speed: 1000 Full
Networks: 10.16.131.104-10.16.131.107

5. In the Network Label field, enter **LAN Network**, leave the VLAN ID as **None (0)**, and then click **Next**.

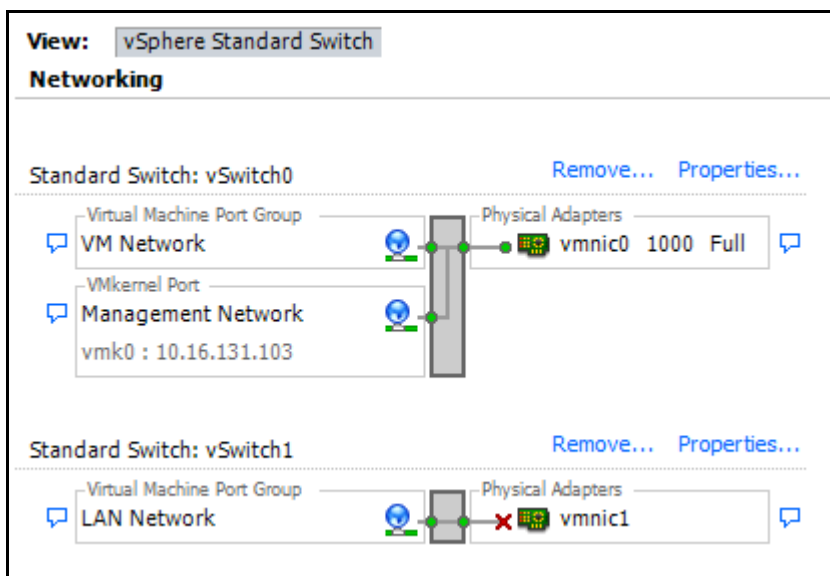
General | Security | Traffic Shaping | NIC Teaming

Port Group Properties

Network Label: LAN Network

VLAN ID (Optional): None (0)

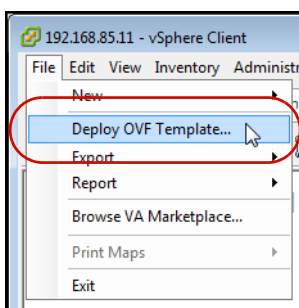
6. Confirm your settings, and then click **Finish**. In the *Configuration* tab, you can now see the LAN and VM virtual networks.



Deploying the HiveOS Virtual Appliance .ova Template

Use the following steps to download and deploy the .ova (Open Virtual Appliance) file on the ESXi hypervisor. An .ova file contains a virtual machine that is prepackaged and ready for deployment.

1. Log in to HiveManager, click **Monitor > Devices > All Devices > Update > Download HiveOS Virtual Appliance**, and then save the AH_HiveOS_VA.ova file to a directory on your management system. Its file size is about 30 MB.
2. Return to the ESXi hypervisor, and then click **File > Deploy OVF Template**.



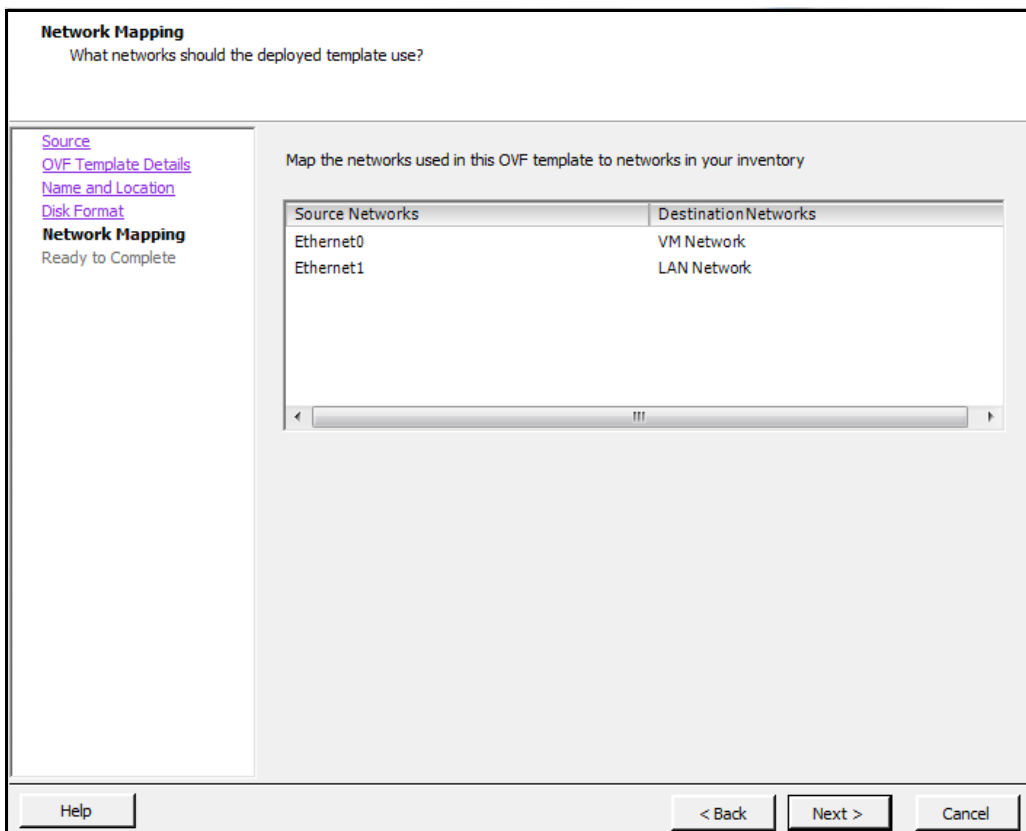
The *Deploy OVF Template* wizard launches.

3. Navigate to the location of the AH_HiveOS_VA.ova file that you downloaded, select the file, click **Open**, and then click **Next**.
4. Verify the template details, and then click **Next**.

5. Specify a name for the .ova template, and then click **Next**.
6. Select the disk format in which you want the virtual disks to be stored. You have three choices:
 - **Thick Provision Lazy Zeroed:** When you select this option, the HiveOS Virtual Appliance claims the entire amount of configured hard disk space from the virtualization host; however, the HiveOS VA does not immediately overwrite sectors with zeroes if it is not currently using them. As a result, any preexisting data occupying the claimed sectors might be recoverable from the host.
 - **Thick Provision Eager Zeroed:** When you select this option, the HiveOS Virtual Appliance claims the entire amount of configured hard disk space from the virtualization host and immediately overwrites all allocated—but as yet unused—sectors with zeroes. This option will take longer during the initial deployment.
 - **Thin Provision:** When you select this option, the ESXi hypervisor allocates only enough host disk space to the HiveOS Virtual Appliance for it to start, leaving the rest of the disk space for other virtual machines to use if needed. Note that one disadvantage to this approach is that the HiveOS VA might run more slowly as it reclaims disk space as needed.

Aerohive recommends selecting either of the thick provisioning options for better performance. Although thin provisioning is useful for space-demanding VMs, the HiveOS Virtual Appliance requires about 100 MB of storage, so space will not typically be an issue. After you make your selection, click **Next**.

7. Map the Ethernet0 and Ethernet1 source networks to the VM Network and LAN Network destination networks respectively. When the mapping is correct, click **Next**.



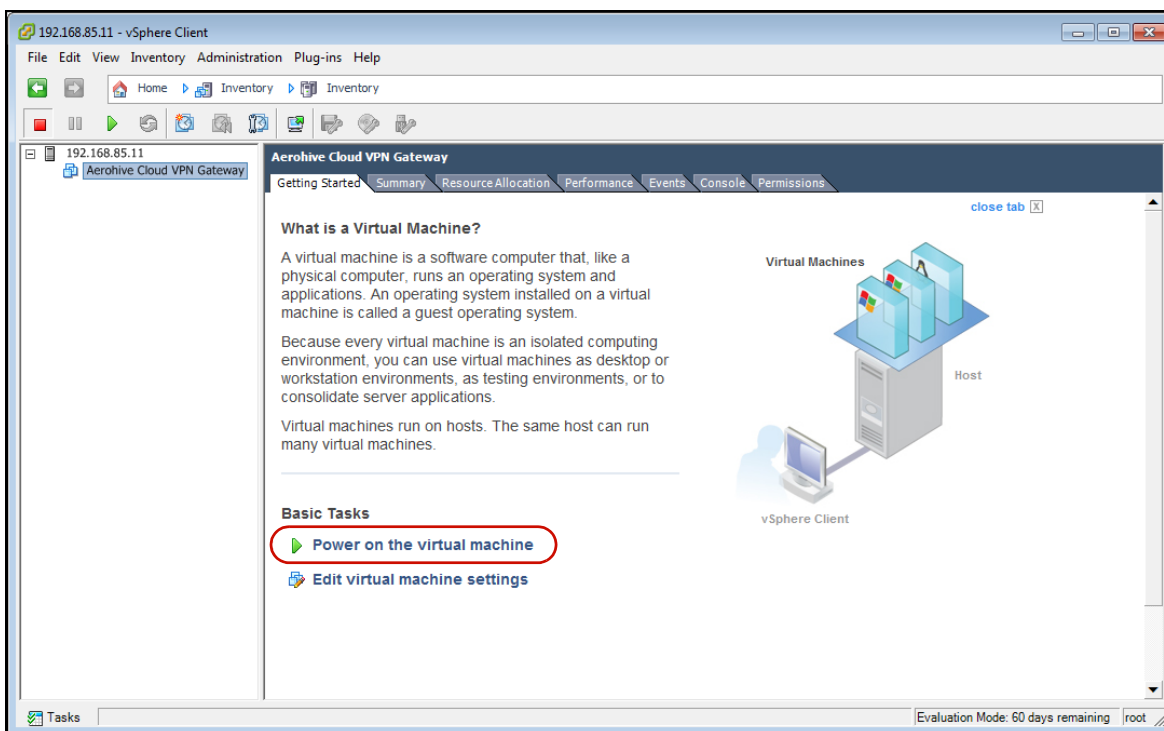
(((1))) If the destination network (or "port group") needs to support promiscuous mode and you have created a port group with promiscuous mode enabled, click **VM Network** for Ethernet0 and choose that port group from the drop-down list that appears. For information about whether you need to enable promiscuous mode, see "[Promiscuous Mode](#)" on page 51.

- Confirm your selected options, select **Power on after deployment** to start the HiveOS Virtual Appliance, and then click **Finish**.

Using the Setup Wizard to Configure VPN Gateway Network Settings

In this section, you configure network settings for the VPN gateway using the Setup Wizard.

- From the VMware vSphere Client, expand the ESXi icon in the left navigation panel, select the HiveOS Virtual Appliance icon under it, and then check in the *Getting Started* tab if it is powered on. If not, click **Power on the virtual machine**.



- Click the **Console** tab, and after the HiveOS Virtual Appliance finishes booting up, log in by entering **admin** for the login name and **aerohive** for the password.

3. When the initial setup wizard appears, type **1** and press the **ENTER** key to select **1. Configure network settings**.

```
Initial Setup Wizard

Help:
<ctrl-r> - Restart Initial HiveOS Virtual Appliance Wizard from the beginning

Values in brackets [ ] are default values
Type <enter> to accept the entered or default value

Select one of the following options:
  1. Configure network settings
  2. Enter the activation code
  3. Shut down
Enter option <[1] 2 or 3>:
```

4. In the *Network Settings* section, enter **2** to select **2. Manually configure the interface settings**. Define the network settings for Ethernet0, and then apply the settings by entering **yes**. (Substitute your actual IP address settings for those shown below.)

```
Network Settings
-----

The HiveOS Virtual Appliance must be able to communicate with hosts on the
Internet in order to process your activation code and be configured by
HiveManager.

Choose the method for configuring the eth0 interface settings:

1. Use DHCP to obtain the interface IP address, netmask, gateway, and DNS
   server IP address
2. Manually configure the interface settings

Enter option <[1] or 2>: 2

Manually Configure Interface Settings
-----

Enter the IP address for eth0: 192.168.85.250
Enter the netmask length [24]: 24
Enter the default gateway: 192.168.85.1
Enter the DNS server IP address: 1.1.1.220
Do you want to apply the change? <[yes] | no>: yes
```

5. When you enter **yes**, the HiveOS Virtual Appliance applies the network settings and then prompts you to test connectivity with the license server. Press **Enter** to begin. If all tests succeed, the following appears:

```

Testing the connection between the HiveOS Virtual Appliance and
license server. (Press Enter to start)

Checking the interface address:

    OK (eth0 address = 192.168.85.250)

Checking the default gateway:

    OK (IP 192.168.85.1 is alive)

Testing DNS:

    OK (The license server domain name can be resolved)

Pinging the license server:

    OK (License server is alive)

Do you want to reset the network settings? <yes | [no]>: no

```

(1) *If the HiveOS Virtual Appliance cannot reach the license server and you want to return to the beginning of the wizard, press CTRL-R. You can also return to the wizard later by entering the following command: **wizard startup***

6. Enter the activation code that you received in an email from Aerohive. A serial number is automatically assigned to your HiveOS Virtual Appliance so the redirector can point it to your instance of HiveManager Online.

```

Enter Activation Code
-----

Use an HTTP proxy to access the license server? <yes | [no]>: no

Enter the HiveOS Virtual Appliance activation code (4 to 5 chars): xxxxx

The HiveOS Virtual Appliance serial number 91012041790001 has been installed
successfully. To check it later, you can enter "show hw-info" command.

Do you want to reboot now to activate the changes? <[yes] | no>: yes

```

7. After the HiveOS Virtual Appliance reboots, log back in by accessing its console through the vSphere Client and entering **admin** and **aerohive**. If you are managing Aerohive devices through HiveManager Online or have a Standalone HiveManager account on myhive.aerohive.com that redirects devices to a HiveManager appliance, or if you have configured a DNS server to resolve hivemanager.<local_domain> to the IP address of a HiveManager appliance, the HiveOS Virtual Appliance will automatically form a secure CAPWAP connection with it. To see the CAPWAP status for the HiveOS Virtual Appliance, enter this command:

```
show capwap client
```


If you are using a HiveManager appliance without a Standalone account on myhive.aerohive.com and the DNS server is not configured to resolve hivemanager.<local_domain> to the HiveManager IP address, enter the following command so that the HiveOS Virtual Appliance can send unicast CAPWAP Discovery messages to it:

```
capwap client server name <ip_addr>
```

By default, a HiveOS Virtual Appliance functions as a Layer 3 VPN gateway, and that is what appears for it in the Device Function drop-down list when you click **Monitor > Devices > VPN Gateways > vpn_gateway > Modify**. (You can also configure it to function as a Layer 2 VPN gateway as explained in the online HiveManager Help.) From this point on, this document will refer to the HiveOS Virtual Appliance simply as a VPN gateway.

EXAMPLE 2: CONFIGURING THE VPN GATEWAY AND ROUTERS

The next step is to use HiveManager to configure a network policy for the routers and device settings for the VPN gateway so that they can build IPsec VPN tunnels between themselves. HiveManager contains a preconfigured network policy called QuickStart-Wireless-Routing that simplifies the configuration involved. If you clone this policy, you only need to configure firewall and Layer 3 IPsec settings, and then upload configurations to the routers and the device settings to the VPN gateway, as described in this section. You will use auto provisioning to have HiveManager upload the configuration to the routers as they come online and connect to HiveManager as explained in subsequent examples in this chapter.

1. Log in to HiveManager, click **Monitor > Devices > VPN Gateways** in the navigation tree, and confirm that the VPN gateway appears.
2. Click **Configuration**, choose **QuickStart-Wireless-Routing** from the network policy list, click the tool icon on its right (), and then click **Clone**. Keep all the cloned settings to preserve the working configuration, rename it, and then click **Clone**. In this example, it is simply called "QuickStart-Wireless-Routing2".

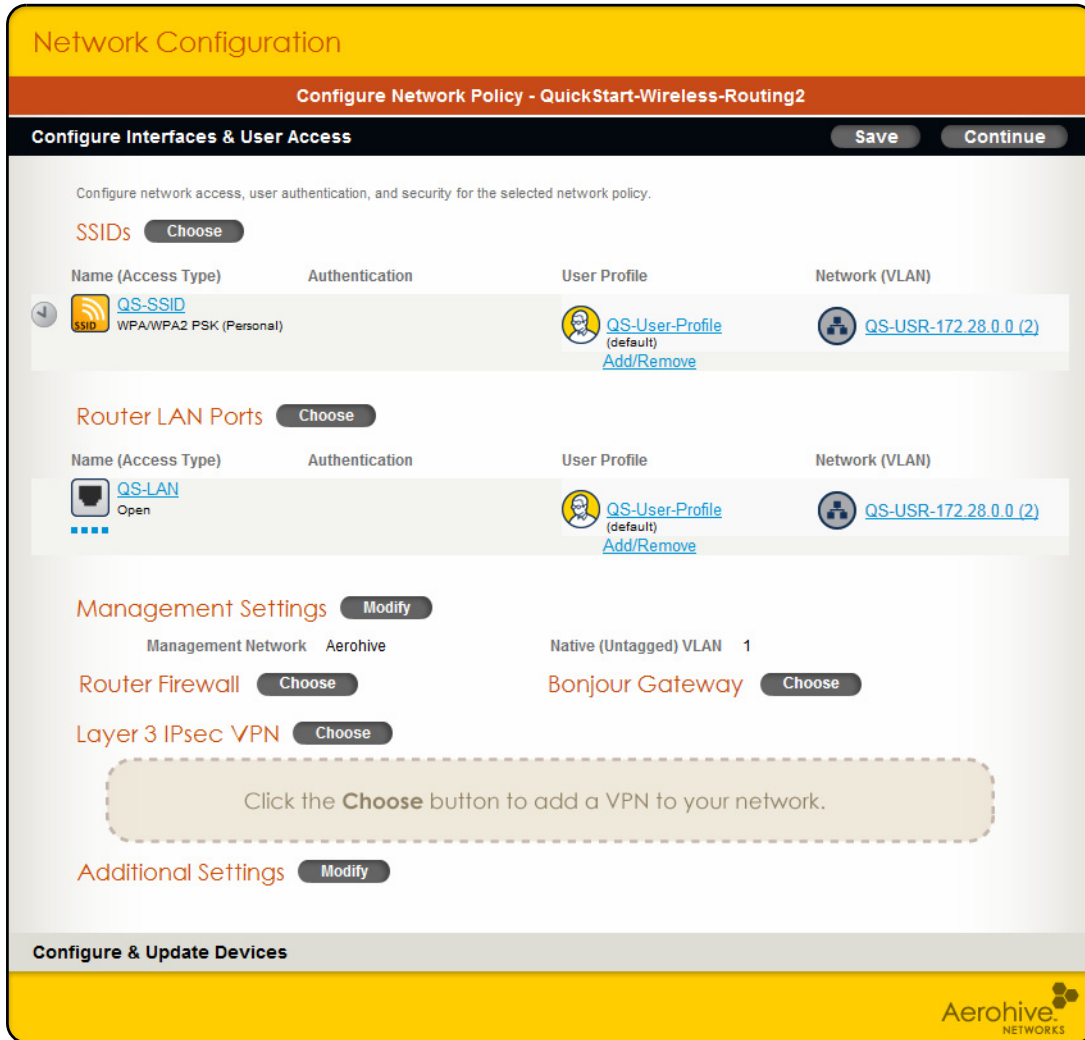
The QuickStart-Wireless-Routing policy is preconfigured for a wireless and routed network. It includes an SSID with an accompanying user profile, network (172.28.0.0/16), and VLAN (2). The PSK used in the SSID is the one that you set when you put HiveManager in Enterprise mode.

The policy also includes router LAN port assignments with the same accompanying user profile, network, and VLAN as those for the SSID. With these settings, the router will assign all users at the branch site to the same user profile and put them in the same subnet within the 172.28.0.0/16 network. HiveManager automatically allocates each site a subnet within the network based on the number of branches specified. For the QuickStart-Wireless-Routing policy, HiveManager divides the 172.28.0.0/16 network into 512 branches by default and allocates unique subnetworks to each branch from the pool.

By default, the network object QS-172.28.0.0/16 uses the DNS service profile that HiveManager created when you first enabled Enterprise mode. This DNS service profile directs clients to use their default gateway² for domain name lookups, and the router then proxies them to its name servers.

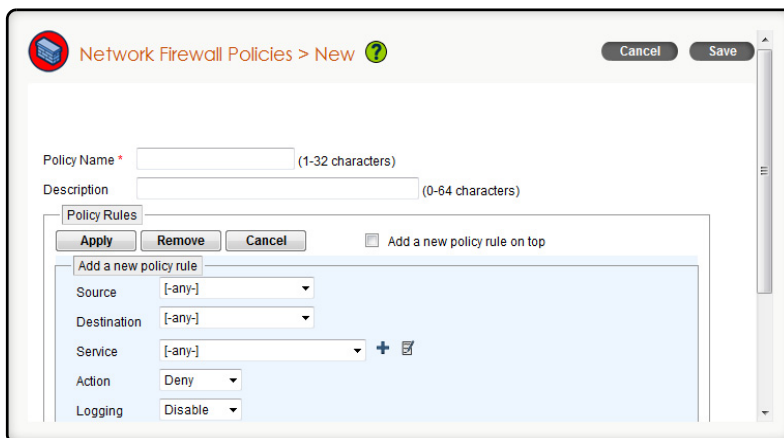
2. The default gateway for clients will be the IP address of the mgt0.x subinterface for both Ethernet and wireless connections.

If the other SSID and router LAN port settings do not suit your needs, you can modify them. However, if they are satisfactory, then you only need to configure the router firewall and Layer 3 IPsec VPN settings.



3. Click **Choose** for Router Firewall, and then click **New**. Name your firewall policy, add a description, and add the rules you want the router to apply. When finished, click **Save**.

(((1))) Because the router applies firewall rules in order from the top, their position in the list is important. To relocate a rule, click and drag it to different position in the policy.



- Click **Choose** for Layer 3 IPsec VPN, and then click **New**, enter the following, and then click **Save**:

Profile Name: Enter a name for the VPN profile.

Description: Enter a useful note about the VPN profile.

Layer 3 IPsec VPN: (select)

A Layer 3 IPsec VPN creates tunnels between routers and one or two VPN gateways. The routers do route lookups to determine whether to send traffic from hosts on their network to hosts on the networks behind the VPN gateways or to hosts at other sites similarly connected to the VPN gateways through tunnels. In contrast, a Layer 2 IPsec VPN creates tunnels between APs functioning as VPN clients and one or two HiveOS Virtual Appliances or other APs functioning as VPN servers and is applied to traffic based on user profiles. There is also a distinction between the IP address requirements at both ends of Layer 3 and Layer 2 VPN tunnels. The hosts at both ends of a Layer 3 VPN tunnel must be in different subnets whereas those at both ends of a Layer 2 VPN tunnel must be in the same subnet.

In the *VPN Gateway Settings* section, choose the name of your VPN gateway from the VPN Gateway drop-down list, click the **Modify** icon, enter the following, and then click **Save**:

General Settings

Host Name: Leave the host name as it is or modify it. The host name can be up to 32 alphanumeric characters long and cannot contain spaces.

Node ID: (read-only)

Management Network: Choose the name of the management network that you are using in the QuickStart-Wireless-Routing2 network policy from the drop-down list: **QS-172.18.0.0/16**. Although you assign a management network to routers and APs through a network policy, you must assign it to the VPN gateway through its device settings.

(((1))) *The VPN gateway does not have to be in the same management network as the routers. If you use a VPN profile in multiple network policies, each policy might apply a different management network to routers while the VPN gateway remains in the management network set for it here.*

Location: Enter the physical location of the VPN gateway for future reference.

Device Model: (read-only)

Device Function: Choose **L3 VPN Gateway**.

Topology Map: Choose the name of a map where the VPN gateway is located.

Interface Settings

Eth0 (WAN): Enter the IP address/netmask and default gateway for the Ethernet0 interface. To allow traffic through this interface, choose **Up** as the admin state.

Eth1 (LAN): Because the Ethernet1 interface is not used, leave the IP address/netmask empty.



If you ever want to block traffic through an Ethernet interface, set its admin state as Down. Note that doing so blocks all traffic on an interface, including management traffic. Therefore, be careful not to disable management access to the VPN gateway from HiveManager.

VPN Gateways

Cancel Save

Host Name * AH-347b8e Device Model HiveOS Virtual Appliance

Node ID * 000C29347B8E Device Function L3 VPN Gateway

Management Network * QS-MGT-172.18.0.0 VPN Service None

Location L1-R3-D5 Topology Map None available

Interface	IP Address	Default Gateway	Admin State
Eth0 (WAN)*	192.168.82.250/24 (Example: 10.1.1.1/24)	192.168.85.1	Up
Eth1 (LAN)			Up

Enable dynamic routing

OSPF

Route Advertisement Eth0 (WAN) Eth1 (LAN)

Use MD5 authentication

Area 0.0.0.0 Router ID

Internal Networks

Static Routes

Optional Settings

Management Server Settings

Enable dynamic routing: To enable the VPN gateway to learn routes from other routers on the corporate network dynamically, select the check box.

From the drop-down list, choose the dynamic routing protocol in use on the corporate network:

RIPv2 – A distance-vector routing protocol that uses hop count to determine the cost of a route. RIPv2 is suitable for small, stable networks because frequent changes in large networks can cause incorrect route information to propagate through the network.

OSPF – OSPF is a link-state routing protocol that uses link cost (an aggregate measure of availability, round-trip time of packets, throughput capacity, and so on) to determine the cost of a route. OSPF is suitable for larger networks because of faster convergence times and more accurate route advertisement.

Route Advertisement: Select the interface on which the VPN gateway will advertise routes about branch sites. When it is using its Ethernet1 interface, you can select **Eth1 (LAN)** to advertise routes about the branch sites on its Ethernet1 interface to the corporate routers. Select **Eth0 (WAN)** if you want it to advertise routes on its Ethernet0 interface. By default, a VPN gateway advertises routes only on its Ethernet1 interface. For the current example, choose **Eth0 (WAN)**.

((:)) 1	Aerohive routers at branch sites periodically poll the VPN gateway to learn routes at the corporate site. They can also send static route information to the VPN gateway, which can then distribute it to routers at the corporate site as well as through VPN tunnels to Aerohive routers at all other branch sites.
------------	---

Use MD5 authentication: Select the check box if the routers must authenticate one another before sharing routing information, and then enter the password used during the authentication process. You can use mutual authentication to restrict route updates among peers and prevent the malicious injection of false routes by attackers. Clear the check box if no authentication is required.

(OSPF Only) **Area:** Enter the OSPF area to which the VPN gateway belongs. Areas are logical groups of routers that share link state and route information. If you do not specify an area by leaving this blank, the VPN gateway uses area 0 (expressed in dotted decimal format as 0.0.0.0).

(OSPF Only) **Router ID:** Enter an explicit router ID in dotted decimal format (w.x.y.z). A router ID is used by a group of routers during the election of a DR (designated router) and a BDR (backup designated router), which take on central roles in maintaining peer information. If you do not specify a router ID, then the VPN gateway uses its highest IP address as its router ID.

Internal Networks: To ensure that the branch routers have all the relevant information regarding the corporate network, you can configure a list of internal networks that the VPN gateway advertises to the routers. This feature only controls the advertisement of routes to internal networks that you define here and does not affect the advertisement of connected routes or routes learned through dynamic routing protocols (RIPv2 and OSPF).

Static Routes: To add a static route, click **Static Routes** to expand the *Static Routes* section, click **New**, enter the following, and then click **Apply**:

Destination IP: Enter the destination host or subnet IP address.

Netmask: Enter the netmask to define the destination as either a host or a subnet.

Gateway: Enter the IP address of the gateway through which the router sends traffic for the specified destination.

Distribute to routers: Select the check box to enable the VPN gateway to distribute the static route to routers.

To add additional routes, click **New**, and repeat the above configuration steps.

In summary, a VPN gateway advertises routes to the following destinations:

- The network to which its Ethernet1 interface directly connects (if that interface is in use).
- The network to which its Ethernet0 interface directly connects if the IP address of the Ethernet0 interface is different from that of its external address, which is the address that routers use as the termination point of their VPN tunnels. If the addresses are different, it is assumed that there is an internal network on the Ethernet0 interface and that an external firewall or NAT device is mapping a public address to the internal address of the Ethernet0 interface. If the IP addresses of the Ethernet0 interface and external address are the same, then the Ethernet0 interface must be on the public network. In this case, the VPN gateway does not advertise that network to the routers. In addition, the VPN gateway automatically performs NAT on outbound traffic it sends to the Internet.
- Destinations learned through dynamic routing protocols.
- All entries listed in the *Internal Networks* table.
- All static routes that have the **Distribute to Routers** check box selected.

It is unnecessary to list the same destinations in both the *Internal Networks* and *Static Routes* tables. For a VPN gateway to advertise the destination in a static route to routers, simply select the **Distribute**

to Routers check box for that route. If you have an internal network that you want only the VPN gateway but not the routers to access, enter a static route but clear **Distribute to Routers**. Finally, if the VPN gateway uses its default route to reach an internal network (so there is no static route to it), make an entry for that destination in the *Internal Networks* table.

((1))	<i>The VPN gateway always advertises entries that you add to the Internal Networks table, regardless of whether the entry is also in the Static Routes table with the Distribute to Routers check box cleared.</i>
-------	--

Back in the VPN Services dialog box, enter the external IP address of the VPN gateway, and then click **Apply**. The external IP address is the public-facing address that the routers can contact. If the firewall performs NAT for devices in the DMZ, then enter the external IP address that the firewall maps to the internal IP address of the Ethernet0 interface. If the firewall does not perform NAT, then enter the Ethernet0 IP address, which must be a public one. When done, click **Save**.

- To control traffic through VPN tunnels from the branch sites to the corporate site, click **Modify** for *Additional Settings*, expand the *Router Settings* section, and then click the **New** icon for Routing Policy. Specify how you want the routers to process client traffic:
 - Split Tunnel:** Branch routers send all non-guest traffic for corporate resources through the VPN tunnel, route traffic for public sites through their WAN interface to the public network without tunneling, and drop all guest traffic for local branch site resources.
 - Tunnel All:** Branch routers send all non-guest traffic through the tunnel regardless of their destination being an internal resource at the corporate site or an external resource on the public network, and they drop all guest traffic.

When you select **Tunnel All**, you can apply a list of destinations that are excluded from the Tunnel All rule. Routers send traffic to these destinations on the public WAN instead of tunneling it. Click the **New** icon for Tunnel Exception Destination List, define one or more destinations, save the list, and then choose it.

- Custom:** Choose this option to create a set of routing rules based on user profiles. For each rule, you decide if it should use the specified Track IP group to fail over from the primary to the secondary WAN interface, and what the forwarding action is. (For more information about the routing policy settings, see the HiveManager Help.)

When finished, click **Save**.

((1))	<i>When you use VPN tunnels to connect branch sites to the corporate site—and from there to other branch sites—and you enable network access through router LAN ports, add 802.1X authentication or a captive web portal requiring user authentication on the LAN ports. Otherwise, it would be possible for anyone making an Ethernet connection to a LAN port to gain corporate access.</i>
-------	---

- In *Configure Network Policy*, click **Continue** to save your settings and advance to *Configure & Update Devices* where you can push the configuration to the VPN gateway. To push the configuration to devices automatically when they initially connect (and update the HiveOS image running on them as well), you will use the auto provisioning feature presented in ["Example 3: Auto Provisioning the Routers" on page 66.](#)
- In *Configure & Update Devices*, select the VPN gateway, click **Settings**, select **Complete Upload, Activate after 5 seconds**, and all the upload-and-activate options at the bottom of the dialog box. Then click **Upload**.



Although you are pushing a configuration to the VPN gateway from within the context of a network policy, HiveManager only pushes the device-level settings to it, not any of the policy-level settings. However, by creating the network policy in this step, you are now ready to reference this policy in the auto provisioning profile to be defined in the next step, "Auto Provisioning the Routers" on page 66

EXAMPLE 3: AUTO PROVISIONING THE ROUTERS

HiveManager can automatically update the configuration and HiveOS image on devices when they initially form a CAPWAP connection with HiveManager. This is a convenient way to update the configurations and images on routers distributed to users for installation on their home networks and branch sites because you cannot predict when their devices will come online. With auto provisioning, you do not have to monitor new connections to know when you can push configurations and update HiveOS software; HiveManager does this for you automatically.

1. Click **Configuration > Show Nav > Auto Provisioning**.
2. To identify which devices HiveManager will automatically provision by serial number, click **SN Management** and import a list of serial numbers for devices to be provisioned in a .csv (comma-separated values) file or enter them manually.



You can filter AP330 and AP350 devices by either serial numbers or IP subnets. However, all BR100 devices initially go online with 192.168.85.0/24 as their mgt0 subnet, which is what they report to HiveManager to use for automatic provisioning. Therefore, you cannot initially distinguish routers by their subnets and must instead use their serial numbers.

3. On the Configuration > Auto Provisioning page, click **New**, enter the following, and then click **Save**:

Enable Auto Provisioning: (select)

Name: Enter a name for the auto provisioning settings.

Description: Enter a useful description for future reference.

Device Model: From the drop-down list, choose the model of the device that you are deploying as a router: **AP330**, **AP350**, **BR100**, **BR200**, or **BR200-WP**. If you have more than one type of device, you will have to create a different auto provisioning profile for each one.

Device Function: If you chose **BR200-WP**, **BR200**, or **BR100**, the device type must be **Router**. If you choose **AP330** or **AP350**, then change **AP** to **Router** so that when HiveManager will reconfigure it as a router when it connects.

Use serial numbers or IP subnetworks to identify devices for auto provisioning: If you imported or manually entered serial numbers or IP subnetworks, select the check box and then move items from the Available column to the Selected column.

Network Policy: Choose the network policy whose settings you want to push to the devices. For this example, choose **QuickStart-Wireless-Routing2**.

Country Code: Choose the country code for the location where the devices will be deployed.

Default Topology Map: Choose a default topology map to which you want icons for the devices to appear, or leave it as is.

Root Admin Configuration/Read-Only Admin Configuration: Enter new names and passwords for a root admin and read-only admin to use when logging in to the devices.

CAPWAP Configuration: In this section, you can change the bootstrap DTLS (Datagram Transport Layer Security) passphrase that the device and HiveManager use when deriving a shared key for authentication when forming a secure CAPWAP connection. You can also set the IP address of the primary CAPWAP server (most likely the current HiveManager) and that of a backup CAPWAP server (if you have two HiveManager devices configured in an HA pair).

Interface Settings: Set the Ethernet port settings and WLAN interface settings for the devices.

Advanced Settings: (expand)

Upload HiveOS upon device authentication: (select) Choose the HiveOS 5.1r1 image or later from the drop-down list. If it is absent, download it from Aerohive Support, and then use the Add/Remove button to import it to HiveManager.

Upload configuration automatically: (select)

Reboot after uploading: (select) This is necessary for devices to activate the configuration after loading it.

Device Classification: To apply tagged configuration objects to the devices, enter the same classification tags here.

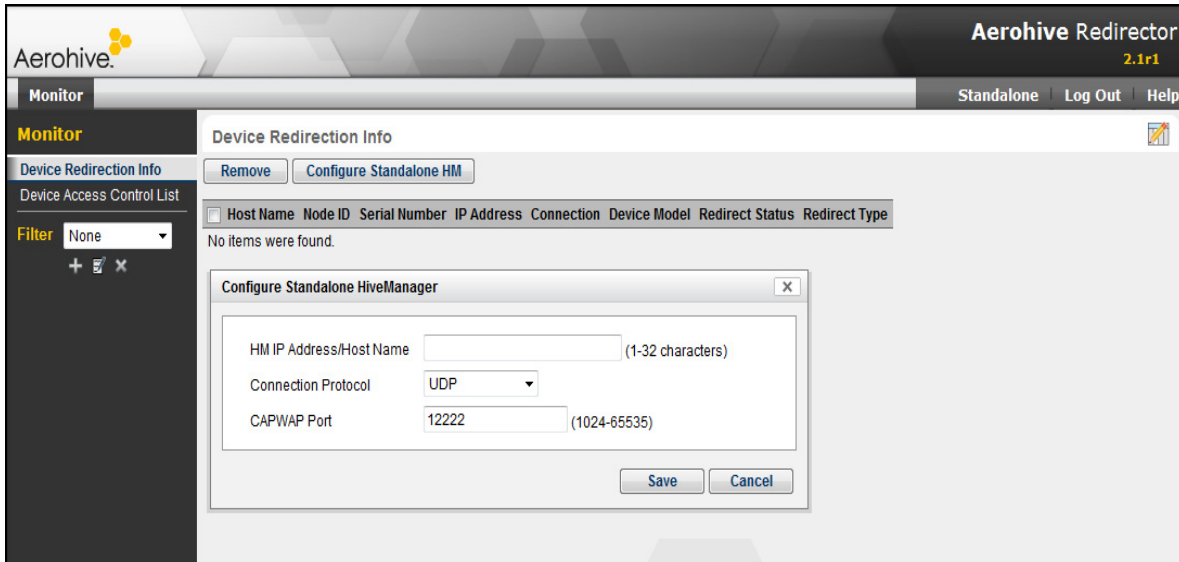
EXAMPLE 4: DEPLOYING ROUTERS ON THE NETWORK

You can use BR100, BR200, and BR200-WP devices as routers or configure AP330 and AP350 devices to function as routers. Note that when AP330 and AP350 devices initially come online, they function as Layer 2 devices with only a single IP address on their mgt0 interface. They change to Layer 3 devices after receiving a new configuration that enables routing functionality. At that point, they support IP addresses on their mgt0, mgt0.x, and eth0 interfaces.

If you have a HiveManager Online account, the routers will automatically discover it as long as they have an Internet connection. After checking for local HiveManager instances and not finding any, they then connect to redirector.aerohive.com, whose ACL (access control list) Aerohive has populated with the serial numbers of all purchased devices. The redirector checks its ACL, and if the router serial numbers match those in the list, they get redirected to the appropriate HiveManager Online management system (see "[How Aerohive Devices Connect to HiveManager](#)" on page 32).

If you are using a HiveManager appliance for device management, you have two options:

MyHive: You can request a Standalone account on the myhive.aerohive.com web site when placing an order with your Aerohive representative. As with HiveManager Online, Aerohive automatically adds the serial numbers of the devices you purchased to the ACL for your account. When you log in with the name and password that Aerohive provides, click **Configure Standalone HM**, enter the domain name or IP address of the HiveManager appliance, the connection protocol (UDP or HTTP), and the CAPWAP port on which your HiveManager appliance listens for CAPWAP connection requests (default: 12222), and then click **Save**.



When the routers come online and cannot discover a CAPWAP server through other means, they contact `redirector.aerohive.com`. When the redirector checks the ACL and finds the serial number of a device contacting it, the redirector pushes the Standalone HiveManager configuration to the device so that it can connect to your HiveManager appliance.

Manual Preprovisioning: Manually set the HiveManager IP address or domain name as the CAPWAP server on each Aerohive device before deploying it remotely. If HiveManager is in a network with a DHCP server, a simple approach is to connect the device to the same subnet as HiveManager so that it can get its network settings through DHCP and then broadcast CAPWAP Discovery messages to locate HiveManager. You can then configure the device with the IP address or domain name it can use to reach HiveManager when installed at a branch site. See the HiveManager Help system for information about where to configure the CAPWAP server settings for Aerohive devices.

The installation of routers at remote sites will most likely be performed by others at those sites such as branch office workers or home users. To install a router at a remote site, they must do the following:

1. Connect the device to a power source. An AP330 or AP350 can connect to either an AC power source or a PoE switch or injector; however, to use the USB modem for WAN connectivity, it must be connected to an AC power source. The BR100, BR200, and BR200-WP cannot receive power through PoE and can only connect to an AC power source.
2. Connect the WAN/ETH0 interface on a BR100, BR200, or BR200-WP or the ETH0 interface on an AP330 or AP350 to a modem, DSL router, or other Internet device. Note that BR200 and BR200-WP platforms can also bypass external modems and use PPPoE to communicate directly with a PPPoE concentrator at their ISP site (for information, see the *New Features Guide for HiveOS and HiveManager 5.0r3*).

By default, the device acts as a DHCP client and automatically obtains its network settings from a DHCP server for the mgt0 interface on an AP330 or AP350 and for the ETH0/WAN interface on a BR100, BR200, or BR200-WP.³ After that, the device automatically attempts to form a CAPWAP connection to a HiveManager appliance or HiveManager Online. In about five minutes, the device will form a CAPWAP connection with a HiveManager instance and appear in the HiveManager GUI on the Monitor > Devices > All Devices page.

An unconfigured AP330 or AP350 does not function as a router, so any devices connected to it will be unable to access the Internet until you upload a configuration to it from HiveManager. In contrast, an unconfigured BR100, BR200, or BR200-WP functions as a router, providing DHCP service and Internet access to devices connected to its LAN interfaces even before it is configured through HiveManager.

3. To provide Ethernet connections to devices on the LAN side of the device, connect the ETH1 – ETH4 interfaces on a BR100, BR200, or BR200-WP or the ETH1 interface on an AP330 or AP350 to one or more switches or directly to hosts. To provide only wireless connections, you can skip this step.

As each device goes online, it forms a secure CAPWAP connection with HiveManager because it has first contacted the redirector and been redirected to a HiveManager Online account or to a Standalone HiveManager appliance. Additionally, it might have been preprovisioned with the domain name or IP address of a HiveManager appliance. When it connects to HiveManager, the device performs the following tasks, depending upon the settings in the auto provisioning profile:

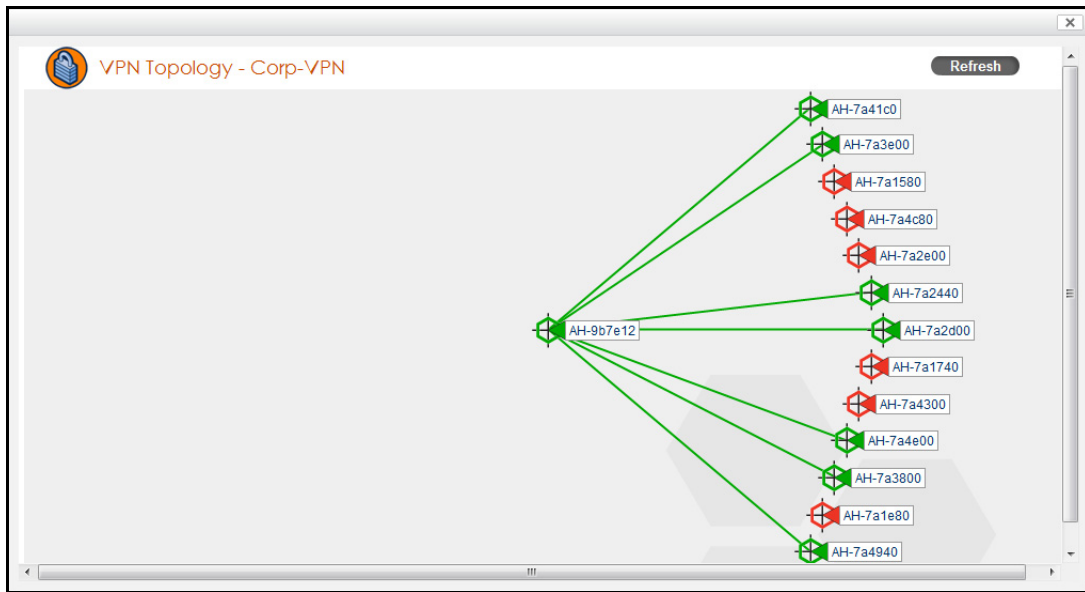
- The device downloads the latest HiveOS firmware and then activates it by rebooting.
- It downloads its configuration and then reboots to activate that.

Upon completing the auto provisioning process, the devices are connected to HiveManager for further management and monitoring, and they have the configurations they need to build IPsec VPN tunnels to the VPN gateway, provide firewall services, and function as access points and routers to provide network access to clients connecting through SSIDs and router LAN ports.

After the devices begin running their new configurations, people at the remote sites can check the network settings of clients connected to their router and test their network connectivity. They can do the following:

- Check that the client received network settings through DHCP from the router. The address will be in a subnet within the 172.28.0.0/16 network, and its default gateway and DNS server will be that of either the LAN interface (for an Ethernet connection) or the mgt0.n subinterface of the QS-SSID (for a wireless connection).
- To check routing functionality to the Internet, ping a public IP address, such as 206.80.44.205.
- To test DNS functionality, ping a domain name, such as ntp1.aerohive.com. If successful, open a web browser and visit an Internet address, such as www.aerohive.com.
- Finally, to test the VPN tunnel, ping the mgt0 interface on the VPN gateway. If successful, try to reach an internal address on the corporate network, such as the home page of a corporate intranet. You can also check the status of the VPN tunnels, on the VPN gateway details page that you can view by clicking **Monitor > Devices > VPN Gateways > Display Device Status Information > name**. HiveManager displays a diagram showing the VPN clients of the selected VPN gateway. Green icons and lines indicate that their tunnels are currently up. Red icons indicate that the tunnels are currently down. (If there are two VPN gateways, the router icons can be orange to indicate that they are configured with two VPN gateways but currently have an active tunnel to only one of them.)

3. The cable modems of some Internet service providers lock the physical MAC address of the device learned so that it can be the only device that connects to the Internet. If you replace your home router or firewall with a BR100, BR200, or BR200-WP and it does not work, put your router/firewall back in place and try to connect the Aerohive device to the router or firewall and see if that works. If it does, tell your ISP that you are switching your router and ask if they can reset the connection so that it will work.



COMMON DEFAULT SETTINGS AND COMMANDS

Many major components of HiveOS are automated and typically require no further configuration. For example, radio power and frequency selection occurs automatically, as does route learning. Also, after defining a hive and a password that hive members use to secure communications, all Aerohive devices belonging to that hive automatically initiate and maintain communications with each other.

Additionally, there are many default settings that simplify the setup of an AP because these are the typical settings for many of the most common deployments. The following are some important default settings and the commands necessary to change them if you need to do so. For a complete list of CLI commands, see one of the platform-dependent Aerohive CLI reference guides available online at

www.aerohive.com/techdocs.

	Default Settings	Commands
mgt0 interface	DHCP client = enabled	To disable the DHCP client: no interface mgt0 dhcp client To set an IP address: interface mgt0 ip ip_addr netmask
	VLAN ID = 1	To set the native (untagged) VLAN that the switch infrastructure in the surrounding wired and wireless backhaul network uses: interface mgt0 native-vlan number
	VLAN ID = 1	To set the VLAN for administrative access to the AP, management traffic between APs and HiveManager, and control traffic among hive members: interface mgt0 vlan number
wifi0 and wifi1 interfaces	wifi0 mode = access wifi1 mode = backhaul	To change the mode of the wifi0 or wifi1 interface: interface { wifi0 wifi1 } mode { access backhaul }
	wifi0 radio profile = radio_g0 wifi1 radio profile = radio_a0	To change the radio profile of the wifi0 or wifi1 interface to a different, previously defined profile: interface { wifi0 wifi1 } radio profile string
	antenna = internal	To have the wifi0 interface use an external antenna: interface { wifi0 wifi1 } radio antenna external
	channel = automatic selection	To set a specific radio channel: interface { wifi0 wifi1 } radio channel number
	power = automatic selection	To set a specific transmission power level (in dBms): interface { wifi0 wifi1 } radio power number
User profile	default-profile: group ID = 0 policy name = def-user-qos VLAN ID = 1	You cannot change the group ID or QoS policy name for the default user profile. To change its VLAN ID: user-profile default-profile vlan-id number

CONFIGURATION OVERVIEW

The amount of configuration depends on the complexity of your deployment. As you can see in ["Deployment Examples \(CLI\)" on page 79](#), you can enter a minimum of three commands to deploy a single AP, and just a few more to deploy a hive.

However, for cases when you need to fine tune access control for more complex environments, HiveOS offers a rich set of CLI commands. The configuration of Aerohive devices falls into two main areas: ["Device-Level Configurations"](#) and ["Policy-Level Configurations" on page 74](#). Consider your deployment plans and then refer to the following sections for guidance on the commands you need to configure them.

(🔍) To find all commands using a particular character or string of characters, you can do a search using the following command: `show cmds | { include | exclude } string`

Device-Level Configurations

Device-level configurations refer to the management of an Aerohive device and its connectivity to wired and wireless clients, the network, and other hive members. The following list contains some key areas of device-level configurations and relevant commands.

- Management
 - Administrators, admin authentication method, login parameters, and admin privileges


```
admin { auth | manager-ip | min-password-length | read-only | read-write |
        root-admin } ...
```
 - Logging settings


```
log { buffered | console | debug | facility | flash | server | trap } ...
```
- Connectivity settings
 - Interfaces


```
interface { eth0 | wifi0 | wifi1 } ...
```
 - Layer 2 and layer 3 forwarding routes


```
route mac_addr ...
ip route { default | host | net } ip_addr ...
```
- VLAN assignments

For users:

```
user-profile string qos-policy string vlan-id number attribute number
```

For the mgt0 interface (the native VLAN in the surrounding network, and the VLAN for administrative access, management traffic, and control traffic among hive members):

```
interface mgt0 native-vlan number
interface mgt0 vlan number
```
- Radio settings


```
radio profile string ...
```

Policy-Level Configurations

Policies control how wired and wireless clients access the network. The following list contains some key areas of policy-level configurations and relevant commands.

- QoS settings


```
qos { classifier-map | classifier-profile | marker-map | marker-profile |
      policy } ...
```
- User profiles

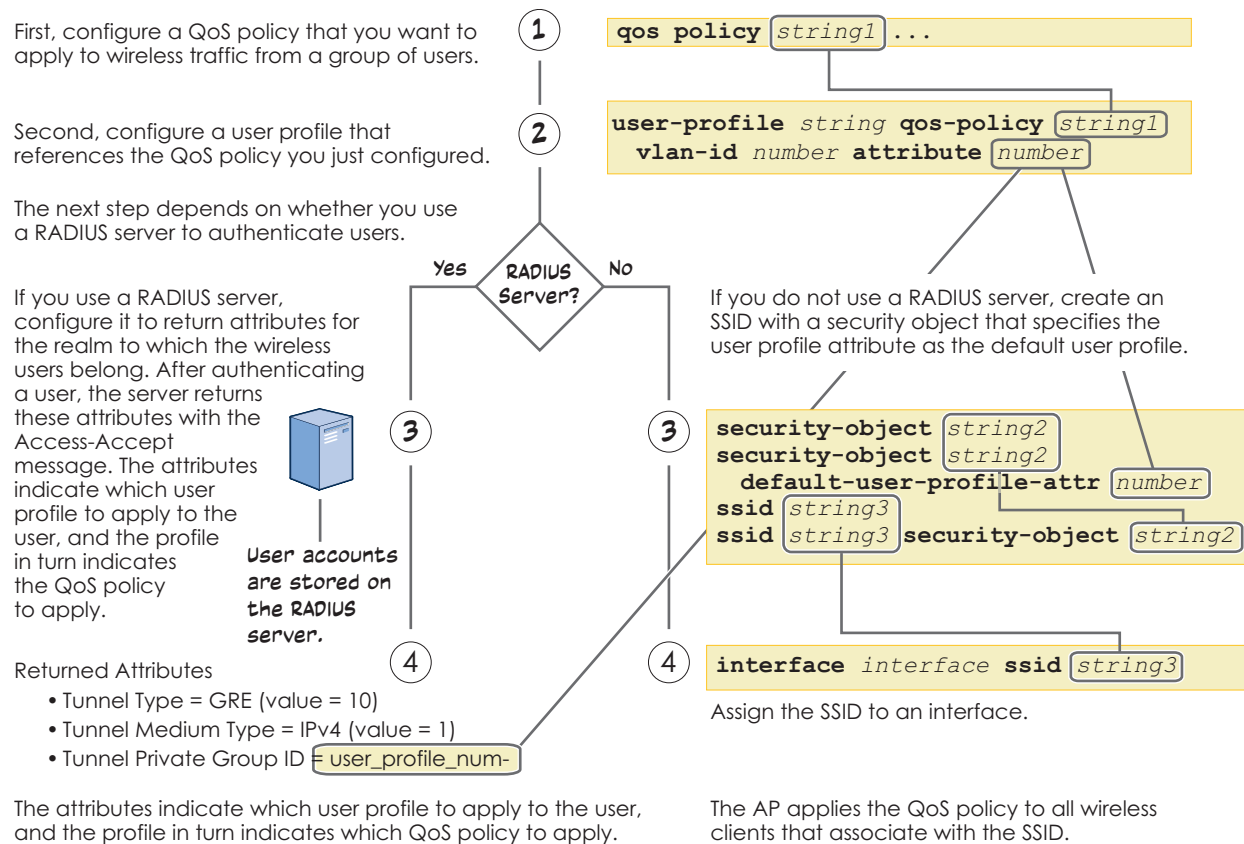

```
user-profile string ...
```
- SSIDs


```
security-object string
security-object string ...
ssid string
ssid string security-object string ...
```
- AAA (authentication, authorization, and accounting) settings for IEEE 802.1X authentication


```
aaa radius-server ...
```

While the configuration of most HiveOS features involves one or more related commands, to define and apply a QoS policy to a group of users, you must configure several different but related features: a QoS policy, a user profile, and—if you do not authenticate users with a RADIUS server—an SSID that references the user profile, and an interface to which you assign the SSID. The configuration steps are shown in [Figure 2](#).

Figure 2 Steps for configuring and applying QoS



HIVEOS CONFIGURATION FILE TYPES

HiveOS supports several types of configuration files: running, current, backup, bootstrap, default, and failed. The **running** configuration (config) is the configuration that is actively running in DRAM. During the bootup process, an Aerohive device loads the running config from one of up to four config files stored in flash memory:

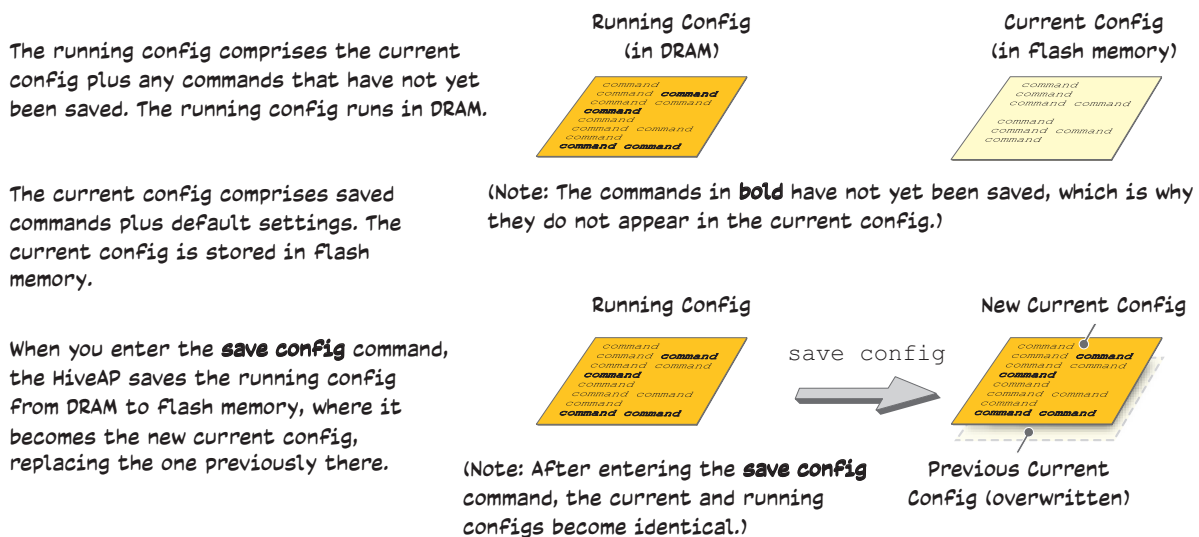
- **current**: a flash file containing a combination of default and admin-defined settings. During the bootup process, this is the first config that the device attempts to load as the running config. This is also the file to which you typically save commands from the running config (you can also save them to the bootstrap config). See [Figure 3](#).
- **backup**: a flash file that the device attempts to load during the reboot process if there is a newly uploaded current config file or if it cannot load the current config file. See [Figure 4 on page 76](#) and [Figure 5 on page 76](#).
- **bootstrap**: a flash file containing a second config composed of a combination of default and admin-defined settings. The device fails over to this config when you enter the **reset config** command or if both the current and backup config files fail to load. See [Figure 6 on page 77](#).
- **default**: a flash file containing only default settings. If there is no bootstrap config, the device reverts to this config when you enter the **reset config** command or if both the current and backup config files fail to load. See [Figure 6 on page 77](#).



There is also a failed config file, which holds any backup config that fails to load. See [Figure 5 on page 76](#).

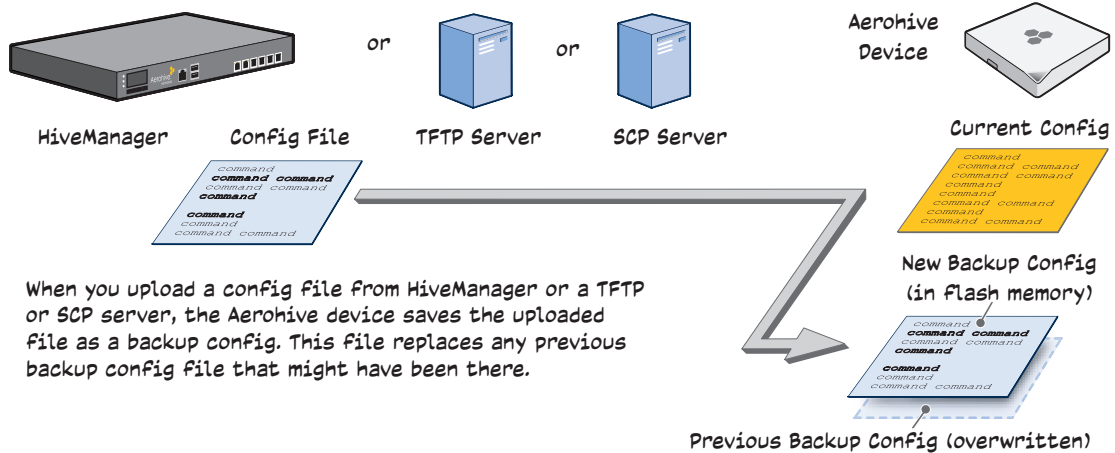
When using the CLI, the two most frequently accessed config types are the running config and current config. When you enter a command in the running config, the device performs it immediately. However, because the running config is stored in volatile memory (DRAM), the commands are not yet permanent and will be lost when the device next reboots. For your configuration settings to persist after rebooting, enter the **save config** command. This command saves the running config to the current config, which is a file stored in nonvolatile (flash) memory. See [Figure 3](#).

Figure 3 Relationship between running and current config files



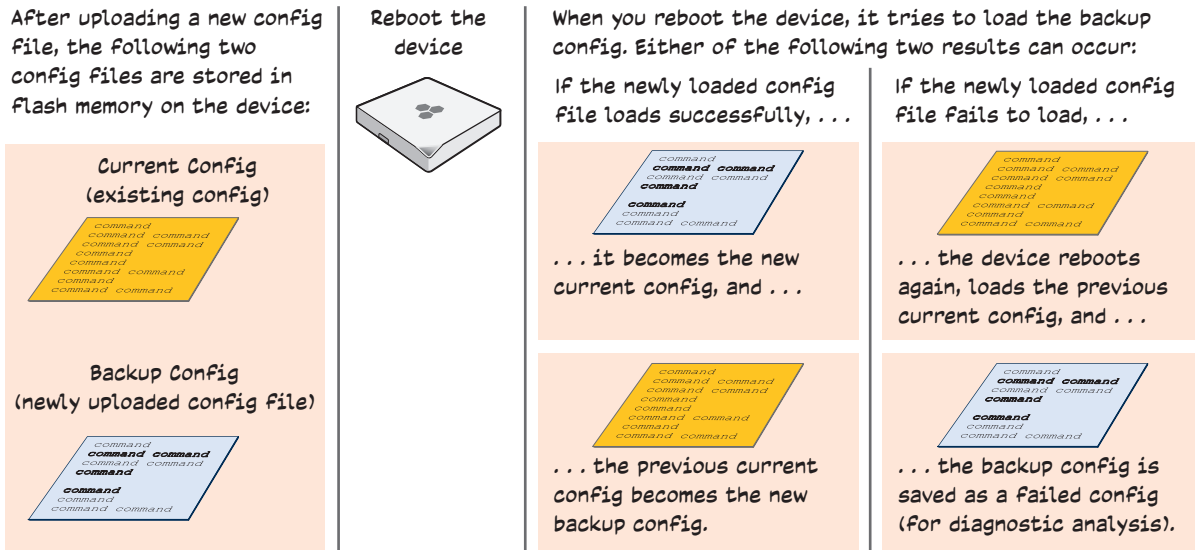
When you upload a configuration file from HiveManager or from a TFTP or SCP server, the device stores the uploaded file in the backup config partition in flash memory, where it remains until it reboots. If there is a backup config file already stored in flash, the newly uploaded file overwrites it. See [Figure 4](#).

Figure 4 Relationship between current and backup config files during a file upload



When the device reboots, it attempts to load the newly uploaded config file. If the file loads successfully, the device makes that file the new current config and makes the previous current config the new backup config. If the file does not load successfully, the device reboots again and loads the previous current config file. The device saves the file it was unable to load as a failed config for diagnostics. See [Figure 5](#).

Figure 5 Relationship between current and backup config files while rebooting an Aerohive device



(G) To upload and activate a config file from HiveManager, see ["Uploading Configurations to Aerohive Devices"](#) on page 43. To upload and activate a config file from a TFTP or SCP server using the CLI, use the following commands:

```

save config tftp://ip_addr:filename current { hh:mm:ss | now | offset hh:mm:ss }
save config scp://username@ip_addr:filename current { hh:mm:ss | now | offset hh:mm:ss }
    
```

When an Aerohive device ships from the factory, it is loaded with a default config file, which acts initially as the running and current configs. If you enter and save any commands, the device then stores a separate config file as the current config, combining the default settings with the commands you entered and saved. If you want to return to the default settings, you can press the reset button on the device or enter the **reset config** command. A device might also return to the default config if both the current and backup configs fail to load, which might happen if you update the HiveOS firmware to an image that cannot work with either config.

(i) You can disable the ability of the reset button to reset the configuration by entering this command:
no reset-button reset-config-enable

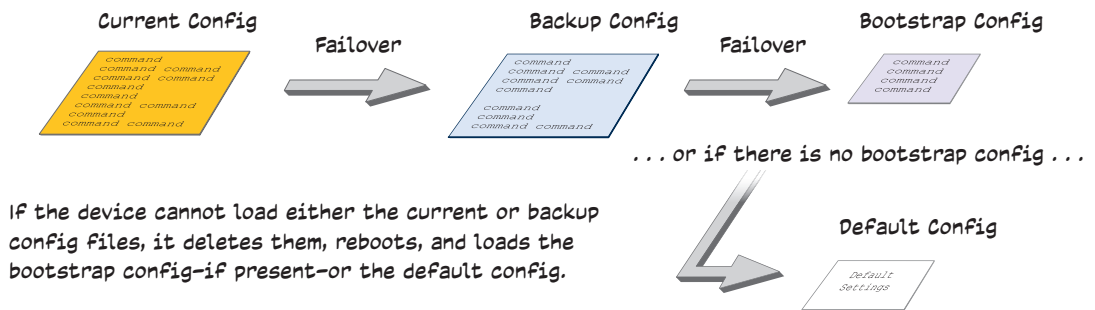
Reverting to the default config can be very useful, especially in the early stages when you are still learning about HiveOS and are likely to be experimenting with different settings. However, retaining the ability of an AP to revert to its default settings after its deployment can present a problem if it is a mesh point in a hive. If the AP reverts to the default config, it will not be able to rejoin its hive. Consequently, it will not be able to get an IP address through DHCP nor be able to communicate with HiveManager (assuming that you are managing it through HiveManager). In this case, you would have to make a serial connection to the console port on the AP and reconfigure its hive settings through the CLI.

To avoid the above situation, you can use a bootstrap config. A bootstrap config is typically a small config file that comes last in the boot order (current – backup – bootstrap) and that replaces the default config as the one an AP loads when you reset the configuration. See [Figure 6 on page 77](#).

(i) Be careful to remember the login name and password defined in the bootstrap config file. If they become lost or forgotten, you must obtain a one-time login key from Aerohive technical support. To get the key, you must already have had a support contract in place. The first one-time login key is free. After that, there is a small handling fee for each additional key.

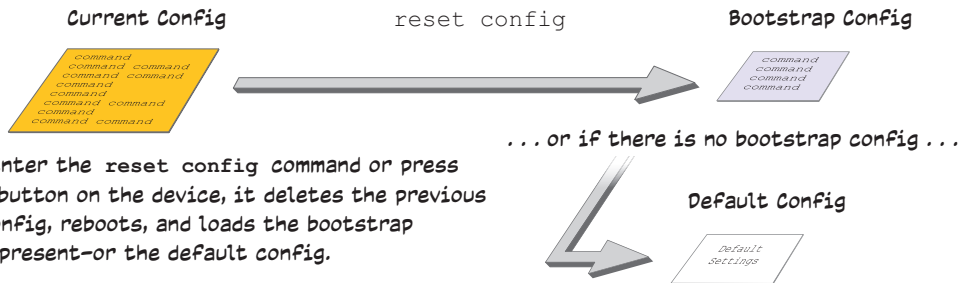
Figure 6 Relationship of current, backup, bootstrap, and default config files

Configuration Failover Behavior



If the device cannot load either the current or backup config files, it deletes them, reboots, and loads the bootstrap config-if present-or the default config.

Resetting the Configuration



When you enter the `reset config` command or press the reset button on the device, it deletes the previous current config, reboots, and loads the bootstrap config-if present-or the default config.

To create and load a bootstrap config, make a text file containing a set of commands that you want the device to load as its bootstrap configuration (for an example, see ["Loading a Bootstrap Configuration" on page 99](#)). Save the file locally and then load it with one of the following commands:

```
save config tftp://ip_addr:filename bootstrap
save config scp://username@ip_addr:filename bootstrap
```

((1))

Similar to the way that a current config consists of the commands you added on top of the default config, a bootstrap config consists of default definitions and settings plus whatever other settings you configure.

After it is loaded, you can enter the following command to view the bootstrap file: **show config bootstrap**

If you want to run the bootstrap config, enter the following commands:

```
load config bootstrap
reboot
```

When the bootstrap config loads, enter the login parameters you defined for that configuration. To return to your previous current config file, enter the following commands:

```
load config backup
reboot
```

Chapter 5 Deployment Examples (CLI)

This chapter presents several deployment examples to introduce AP configuration through the HiveOS CLI.

In ["Deploying a Single AP" on page 80](#), you deploy one AP as an autonomous access point. This is the simplest configuration: you only need to enter and save three commands.

In ["Deploying a Hive" on page 83](#), you add two more APs to the one deployed in the first example to form a hive with three members. The user authentication method in this and the previous example is very simple: a preshared key is defined and stored locally on each AP and on each wireless client.

In ["Using IEEE 802.1X Authentication" on page 89](#), you change the user authentication method. Taking advantage of existing Microsoft AD (Active Directory) user accounts, the APs use IEEE 802.1X EAP (Extensible Authentication Protocol) to forward authentication requests to a RADIUS server whose database is linked to that of the AD server.

In ["Applying QoS" on page 92](#), you apply QoS (Quality of Service) filters to user traffic so that delay-sensitive voice traffic receives higher priority than other more delay-resistant traffic.



To focus attention on the key concepts of an SSID (first example), hive (second example), and IEEE 802.1X authentication (third example), QoS was intentionally omitted from these examples. However, the QoS settings you define in the last example can apply equally well to the configurations in the others.

In ["Loading a Bootstrap Configuration" on page 99](#), you load a bootstrap config file on the APs. When a bootstrap config is present, it loads instead of the default config whenever HiveOS is reset or if the current and backup configs do not load. Using a bootstrap config can help minimize theft and increase convenience.

Because each example builds on the previous one, it is recommended to read them sequentially. Doing so will help build an understanding of the fundamentals involved in configuring APs.

If you want to view just the CLI commands used in the examples, see ["CLI Commands for Examples" on page 102](#). Having the commands in blocks by themselves makes it easy to copy-and-paste them at the command prompt. The following are the equipment and network requirements for these examples:

- Equipment
 - Management system (computer) capable of creating a serial connection to the AP
 - VT100 emulator on the management system
 - Serial cable ("null modem cable") that ships as an optional accessory (AH-ACC-Serial-DB9). You use this to connect your management system to the AP.



You can also access the CLI by using Telnet or SSH (Secure Shell). After connecting an AP to the network, make either a Telnet or SSH connection to the IP address that the DHCP server assigns the mgt0 interface. (Telnet is disabled by default.)

- Network
 - Layer 2 switch through which you connect the AP to the wired network
 - Ethernet cable—either straight-through or cross-over
 - Network access to a DHCP server
 - For the third and fourth examples, network access to Active Directory and RADIUS servers

EXAMPLE 1: DEPLOYING A SINGLE AP

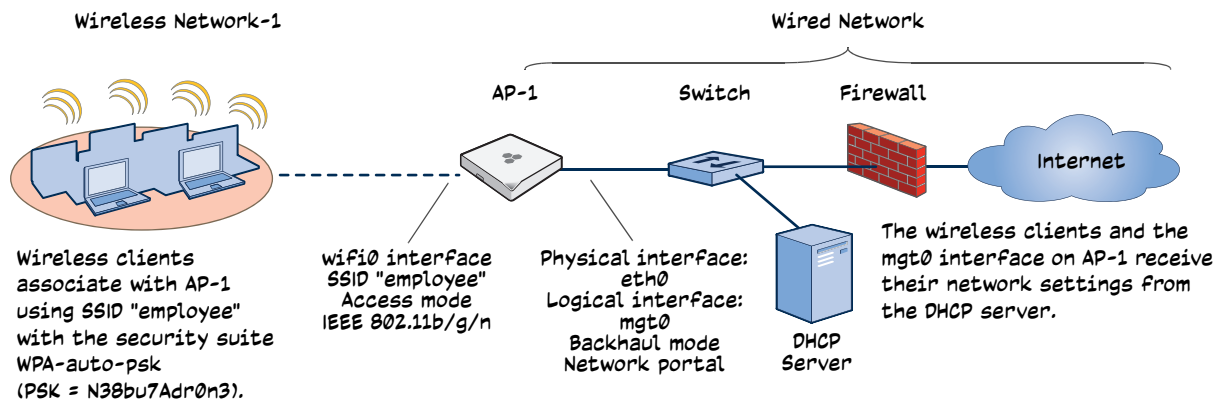
In this example, you deploy one AP (AP-1) to provide network access to a small office with 15 – 20 wireless clients. You only need to define the following SSID (service set identifier) parameters on the AP and clients:

- **SSID name:** employee
- **Security protocol suite:** WPA-auto-psk
 - WPA – Uses Wi-Fi Protected Access, which provides dynamic key encryption and mutual authentication of the client and AP
 - Auto – Automatically negotiates WPA or WPA2 and the encryption protocol: AES (Advanced Encryption Standard) or TKIP (Temporal Key Integrity Protocol)
 - PSK – Derives encryption keys from a preshared key that the client and AP both already have
- **Preshared key:** N38bu7Adr0n3

After defining SSID "employee" on AP-1, you then bind it to the wifi0 interface, which is in access mode by default. The wifi0 interface links to radio 1, which operates at 2.4 GHz (in accordance with the IEEE 802.11b, g, and n standards). This example assumes that the clients also support 802.11b, g, or n.


(1) By default, the wifi1 interface is in backhaul mode and links to the 5 GHz radio, supporting IEEE 802.11a and 802.11n. To put wifi1 in access mode so that both interfaces provide access—wifi0 at 2.4 GHz and wifi1 at 5 GHz—enter this command: `interface wifi1 mode access`. Then, in addition to binding SSID "employee" to wifi0 (as explained in step 2), also bind it to wifi1.

Figure 1 Single AP for a small wireless network



Step 1 Log in through the console port

1. Connect the power cable from the DC power connector on the AP to the AC/DC power adaptor that ships with the device as an option, and connect that to a 100 – 240-volt power source.

 *If the switch supports PoE (Power over Ethernet), the AP can receive its power that way instead.*

The Power LED glows steady amber during the bootup process. After the bootup process completes, it then glows steady green to indicate that the firmware is loaded and running.

2. Connect one end of an RS-232 serial (or "null modem") cable to the serial port (or Com port) on your management system.
3. Connect the other end of the cable to the male DB-9 or RJ-45 console port on the AP.
4. On your management system, run a VT100 terminal emulation program, such as Tera Term Pro® (a free terminal emulator) or Hilgraeve Hyperterminal® (provided with Windows® operating systems). Use the following settings:
 - Bits per second (baud rate): 9600
 - Data bits: 8
 - Parity: none
 - Stop bits: 1
 - Flow control: none

For APs set with "FCC" as the region code, the Initial CLI Configuration Wizard appears. For APs set with "world" as the region code, a prompt appears to set the country code for the location where you intend to deploy the AP. To set the country code, enter the **boot-param country-code number** command, in which *number* is the appropriate country code number. For a list of country codes, see the HiveManager GUI.

5. Because you do not need to configure all the settings presented in the wizard, press **N** to cancel it. The login prompt appears.
6. Log in using the default user name *admin* and password *aerohive*.

Step 2 Configure the AP

1. Create security parameters for an SSID, assign them to the SSID, and then assign the SSID to an interface.


```
security-object employee
```

```
security-object employee security protocol-suite wpa-auto-psk ascii-key N38bu7Adr0n3
```

You first create a security object named "employee" and define a protocol suite and preshared key (N38bu7Adr0n3) in standard ASCII (American Standard Code for Information Interchange) text for it.

```
ssid employee
```

```
ssid employee security-object employee
```

Then you create an SSID named "employee" and apply the security object to it.

```
interface wifi0 ssid employee
```

You assign the SSID to the wifi0 interface, which is in access mode by default. When you make this assignment, the AP automatically creates subinterface wifi0.1 and uses that for the SSID. (The HiveAP 20 series supports up to seven subinterfaces per Wi-Fi interface for a possible maximum total of 14 SSIDs when both wifi0 and wifi1 are in access mode. The AP100

and AP300 series support up to 16 per interface for a possible maximum total of 32.) An AP can use one or two Wi-Fi interfaces in access mode to communicate with wireless clients accessing the network, and a Wi-Fi interface in backhaul mode to communicate wirelessly with other APs when in a hive (see subsequent examples). Finally, if you enable the virtual access console, then you must subtract one from the maximum number of SSIDs for each radio on which you want the access console to be available.

- (Optional) Change the name and password of the root admin.

```
admin root-admin mwebster password 3fF8ha
```

As a safety precaution, you change the default root admin name and password to *mwebster* and *3fF8ha*. The next time you log in, use these instead of the default definitions.



By default, the minimum password length is 5 characters. You can change the minimum length by entering the following command: `admin min-password-length <number>` (The minimum password length can be between 5 and 32 characters.)

- (Optional) Change the host name of the AP.

```
hostname AP-1
```

- Save your changes to the currently running configuration, and then log out of the serial session.

```
save config
```

```
exit
```

The AP configuration is complete.

Step 3 Configure the wireless clients

Define the "employee" SSID on all the wireless clients. Specify WPA-PSK for network authentication, AES or TKIP for data encryption, and the preshared key *N38bu7Adr0n3*.

Step 4 Position and power on the AP

- Place the AP within range of the wireless clients and, optionally, mount it as explained in the mounting section in the chapter about the AP model that you are using.
- Connect an Ethernet cable from the PoE In port to the network switch.
- If you have powered off the AP, power it back on by reconnecting it to a power source.

When you power on the AP, the *mgt0* interface, which connects to the wired network through the *eth0* port, automatically receives its IP address through DHCP (Dynamic Host Configuration Protocol).

Step 5 Check that clients can form associations and access the network

- To check that a client can associate with the AP and access the network, open a wireless client application and connect to the "employee" SSID. Then contact a network resource, such as a web server.
- Log in to the AP CLI, and check that you can see the MAC address of the associated client and an indication that the correct SSID is in use by entering the following command:

```
show ssid employee station
```

```
Chan=channel number; Pow=Power in dbm;
```

```
A-Mode=Authentication mode; Cipher=Encryption mode;
```

```
A-Time=Associated time; Auth=Authenticated;
```

```
UPID=User profile Identifier; Phymode=Physical mode;
```

Mac Addr	IP Addr	Chan	Rate	Pow	A-Mode	Cipher	A-Time	VLAN	Auth	UPID	Phymode
0016:cf8c:57bc	10.1.1.35	11	54M	-38	wpa2-psk	aes ccm	00:00:56	1	Yes	0	11g

Check that the MAC address in the table matches that of the wireless client.

Check that the authentication and encryption modes match those in the SSID security protocol suite.

1 You can also enter the following commands to check the association status of a wireless client: `show auth`, `show roaming cache`, and `show roaming cache mac <mac_addr>`.

The setup of a single AP is complete. Wireless clients can now associate with the AP using SSID "employee" and access the network.

EXAMPLE 2: DEPLOYING A HIVE

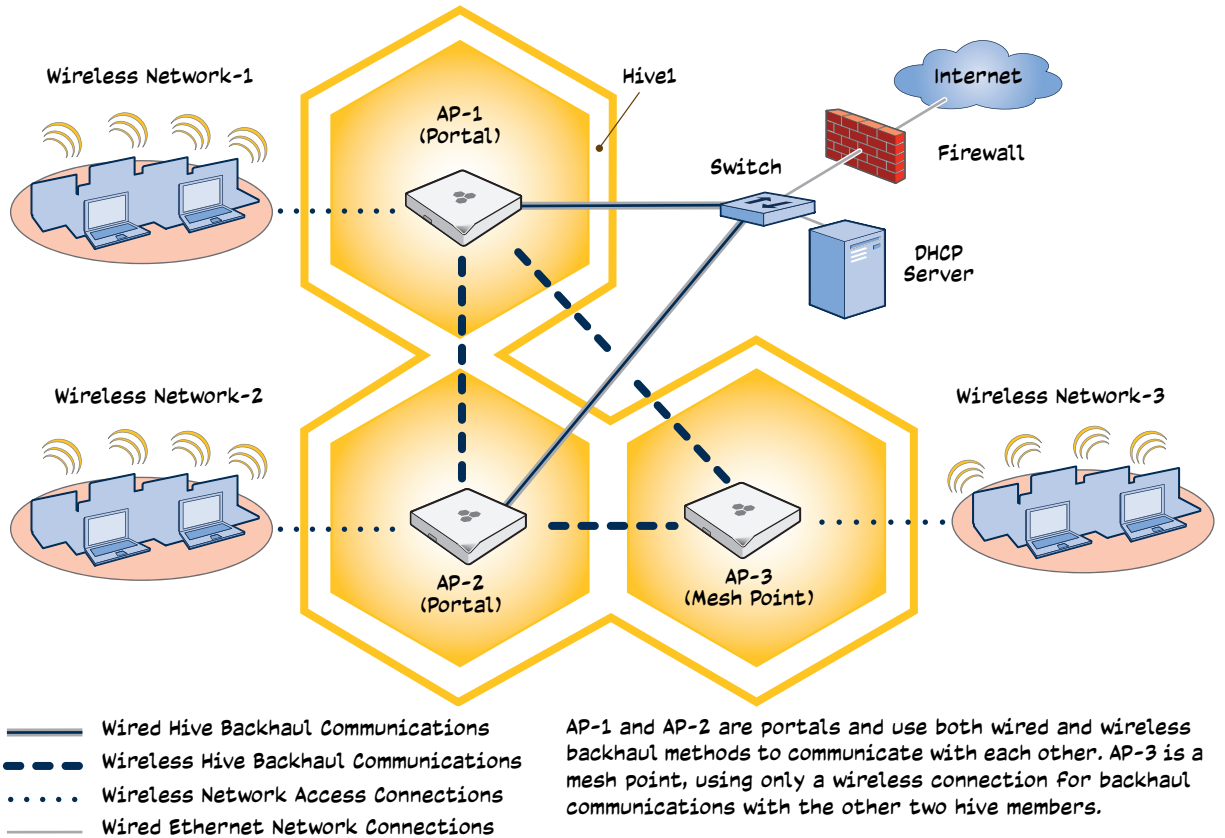
Building on "Deploying a Single AP" on page 80, the office network has expanded and requires more APs to provide greater coverage. In addition to the basic configuration covered in the previous example, you configure all three APs to form a hive within the same layer 2 switched network. The following are the configuration details for the hive:

- Hive name: hive1
- Preshared key for hive1 communications: s1r70ckH07m3s

1 The security protocol suite for hive communications is WPA-AES-PSK.

AP-1 and -2 are cabled to a switch and use the native (untagged) VLAN for wired backhaul communications. They communicate with each other over both wired and wireless backhaul links, the wired link taking precedence. However, AP-3 only communicates with AP-1 and -2 over a wireless link (see Figure 2). Because AP-1 and -2 connect to the wired network, they act as portals. In contrast, AP-3 is a mesh point.

Figure 2 Three APs in a hive



If all hive members can communicate over wired backhaul links, you can then use both radios for access. The `wifi0` interface is already in access mode by default. To put `wifi1` in access mode, enter this command: `interface wifi1 mode access`. In this example, however, a wireless backhaul link is required.

Step 1 Configure AP-1

- Using the connection settings described in the first example, log in to AP-1.
- Configure AP-1 as a member of "hive1" and set the security protocol suite.

```
hive hive1
```

You create a hive, which is a set of APs that collectively distribute data and coordinate activities among themselves, such as client association data for fast roaming, route data for making optimal data-path forwarding decisions, and policy enforcement for QoS (Quality of Service) and security.

```
hive hive1 password slr70ckH07m3s
```

You define the password that hive members use to derive the preshared key for securing backhaul communications with each other. The password must be the same on all hive members.

```
interface mgt0 hive hive1
```

By setting "hive1" on the mgt0 interface, you join AP-1 to the hive.

```
save config
```

- Before closing the console session, check the radio channel that AP-1 uses on its backhaul interface, which by default is wifi1:

```
show interface
```

```
State=Operational state; Chan=Channel;
```

```
Radio=Radio profile; U=up; D=down;
```

Name	MAC addr	Mode	State	Chan	VLAN	Radio	Hive	SSID
Mgt0	0019:7700:0020	-	U	-	1	-	hive1	-
Eth0	0019:7700:0020	backhaul	U	-	1	-	hive1	-
Wifi0	0019:7700:0024	access	U	11	-	radio_ng0	-	-
Wifi0.1	0019:7700:0024	access	U	11	-	radio_ng0	hive1	employee
Wifi1	0019:7700:0028	backhaul	U	149	-	radio_na0	-	-
Wifi1.1	0019:7700:0028	backhaul	U	149	1	radio_na0	hive1	-

The wifi1 interface and the wifi1.1 subinterface are in backhaul mode and are using channel 149. Both wifi1 and wifi1.1 use the default radio profile radio_na0. (Depending on the AP model, the default profile might be radio_a0.) This is a profile for radio2, which operates in the 5 GHz frequency range as specified in the IEEE 802.11a and n standards.

AP-1 is set to use wireless interface wifi1 and its subinterface wifi1.1 for backhaul communications.

Write down the radio channel for future reference (in this example, it is 149). When configuring AP-2 and -3, make sure that they also use this channel for backhaul communications.

```
exit
```

Step 2 Configure AP-2 and AP-3

1. Power on AP-2 and log in through its console port.
2. Configure AP-2 with the same commands that you used for AP-1:

```

security-object employee

security-object employee security protocol-suite wpa-auto-psk ascii-key N38bu7Adr0n3

ssid employee

ssid employee security-object employee

interface wifi0 ssid employee

hive hive1

hive hive1 password slr70ckH07m3s

interface mgt0 hive hive1

```
3. (Optional) Change the name and password of the superuser.

```

admin superuser mwebster password 3fF8ha

```
4. Check that the channel ID for wifi1 and wifi1.1 is now 149.

```

show interface

```

If the channel ID for wifi1 and wifi1.1 is not 149, set it to 149 so that AP-2 uses the same channel as AP-1 for backhaul communications.

```

interface wifi1 radio channel 149

```

Setting the channel for the parent interface (wifi1) sets it for all its subinterfaces. An interface in backhaul mode only needs one subinterface, which by default is wifi1.1.

```

save config

exit

```
5. Repeat the above steps for AP-3.

Step 3 Connect AP-2 and AP-3 to the network

1. Place AP-2 within range of its clients and within range of AP-1. This allows AP-1 and -2 to send backhaul communications to each other wirelessly as a backup path in case either member loses its wired connection to the network.
2. Connect an Ethernet cable from the PoE In port on AP-2 to the network switch.
3. Power on AP-2 by connecting it to a power source.

After AP-2 finishes booting up (indicated when the Power LED changes from steady amber to steady green), it automatically discovers another member of hive1 (AP-1). The two members use a preshared key based on their shared secret (*slr70ckH07m3s*) to authenticate each other and AES to encrypt wired backhaul communications and AES-CCMP to encrypt wireless backhaul communications between themselves. You can tell when they have formed a hive because the Mesh LED changes its blinking pattern from a fast to slow.
4. Place AP-3 within range of its wireless clients and one or both of the other hive members.

- Power on AP-3 by connecting it to a power source.

After AP-3 boots up, it discovers the two other members of hive1 over a wireless backhaul link. The members authenticate themselves and establish a security association for encrypting backhaul communications among themselves. AP-3 then learns its default route to the wired network from the other hive members. If the other members send routes with equal costs—which is what happens in this example—AP-3 uses the first route it receives. When it learns this route, it can communicate with the DHCP server to get an IP address for its mg10 interface.

- Check that AP-3 has associated with the other members at the wireless level.

Log in to AP-3 and enter this command to see its neighbors in hive1:

```

show hive hive1 neighbor
Chan=channel number; Pow=Power in dBm;
A-Mode=Authentication mode; Cipher=Encryption mode;
Conn-Time=Connected time; Hstate=Hive State;

Mac Addr          Chan  Tx Rate  Rx Rate  Pow  A-Mode  Cipher  Conn-Time  Hstate  Pymode  Hive
-----
0019:7700:0028    149   54M     54M     -16  psk     aes ccm  00:04:15  Auth    11a     hive1
0019:7700:0438    149   54M     54M     -16  psk     aes ccm  00:04:16  Auth    11a     hive1
    
```

Neighbors

AP-1



wifi1.1 MAC Address
0019:7700:0028

AP-2



wifi1.1 MAC Address
0019:7700:0438

In the output of the `show hive hive1 neighbor` command, you can see hive-level and member-level information. (On APs supporting 802.11n, the channel width for hive communications—20 or 40 MHz—is also shown.)

When you see the MAC addresses of the other hive members, you know that AP-3 learned them over a wireless backhaul link.

The following are the various hive states that can appear:

Disv (Discover) - Another AP has been discovered, but there is a mismatch with its hive ID.

Neibor (Neighbor) - Another AP has been discovered whose hive ID matches, but it has not yet been authenticated.

CandPr (Candidate Peer) - The hive ID on a discovered AP matches, and it can accept more neighbors.

AssocPd (Association Pending) - An AP is on the same backhaul channel, and an association process in progress.

Assocd (Associated) - An AP has associated with the local AP and can now start the authentication process.

Auth (Authenticated) - The AP has been authenticated and can now exchange data traffic.

- To check that the hive members have full data connectivity with each other, associate a client in wireless network-1 with AP-1 (the SSID "employee" is already defined on clients in wireless network-1; see "Deploying a Single AP"). Then check if AP-1 forwards the client's MAC address to the others to store in their roaming caches.

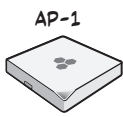
After associating a wireless client with AP-1, log in to AP-1 and enter this command:

```
show ssid employee station
```

Chan=channel number; Pow=Power in dBm;
A-Mode=Authentication mode; Cipher=Encryption mode;
A-Time=Associated time; Auth=Authenticated;
UPID=User profile Identifier; Phymode=Physical mode;

Mac Addr	IP Addr	Chan	Tx Rate	Rx Rate	Pow	A-Mode	Cipher	A-Time	VLAN	Auth	UPID	Phymode
0016:cf8c:57bc	10.1.1.73	1	54M	54M	-40	wpa2-psk	aes ccm	00:01:46	1	Yes	0	11b/g

Total station count: 1



AP-1

This MAC address is for the wireless adapter of the client (or "supplicant") associated with the SSID "employee".

Note: On APs supporting IEEE 802.11n, there are two additional columns for SM-PS (spatial multiplexing power save) and channel width (20 or 40 MHz). The SM-PS states can be "static" (use one data stream for 11a/b/g clients), "dynamic" (use multiple spatial streams for 11n clients when the AP sends an RTS frame), or "disabled" (always use spatial streams for 11n clients).

Then log in to AP-2 and enter this command:

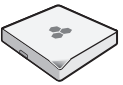
```
show roaming cache
```

Roaming Cache Table:
UID=User profile group ID; PMK=Pairwise Master Key;
TLC=PMK Time Left in Cache; Life=PMK Life; A=authenticated; L= CWP Logged In

Roaming for this AP: enabled
Maximum Caching Time: 3600 seconds
Caching update interval: 60 seconds
Caching update times: 60
Roaming hops: 1

SSID employee:
Maximum Caching Time: 3600 seconds
Caching update interval: 60 seconds
Caching update times: 60

No.	Supplicant	Authenticator	UID	PMK	PMKID	Life	Age	TLC	Hop	AL
0	0016:cf8c:57bc	0019:7700:0024	0	1349*	1615*	-1	46	195	1	YN



AP-2

MATCH!

This is the same MAC address for the client (station) that you saw listed on AP-1.

This MAC address is for the wifi0.1 subinterface of AP-1, the AP with which the wireless client associated.

When you see the MAC address of the wireless client that is associated with AP-1 in the roaming cache of AP-2, you know that AP-1 and -2 are successfully sending data over the backhaul link.

Repeat this to confirm that AP-3 also has a backhaul connection with the other members.

Step 4 Configure wireless clients

Define the "employee" SSID on all the wireless clients in wireless network-2 and -3. Specify WPA-PSK for network authentication, AES or TKIP for data encryption, and the preshared key *N38bu7Adr0n3*.

The setup of hive1 is complete. Wireless clients can now associate with the APs using SSID "employee" and access the network. The APs communicate with each other to share client associations (to support fast roaming) and routing data (to select optimal data paths).

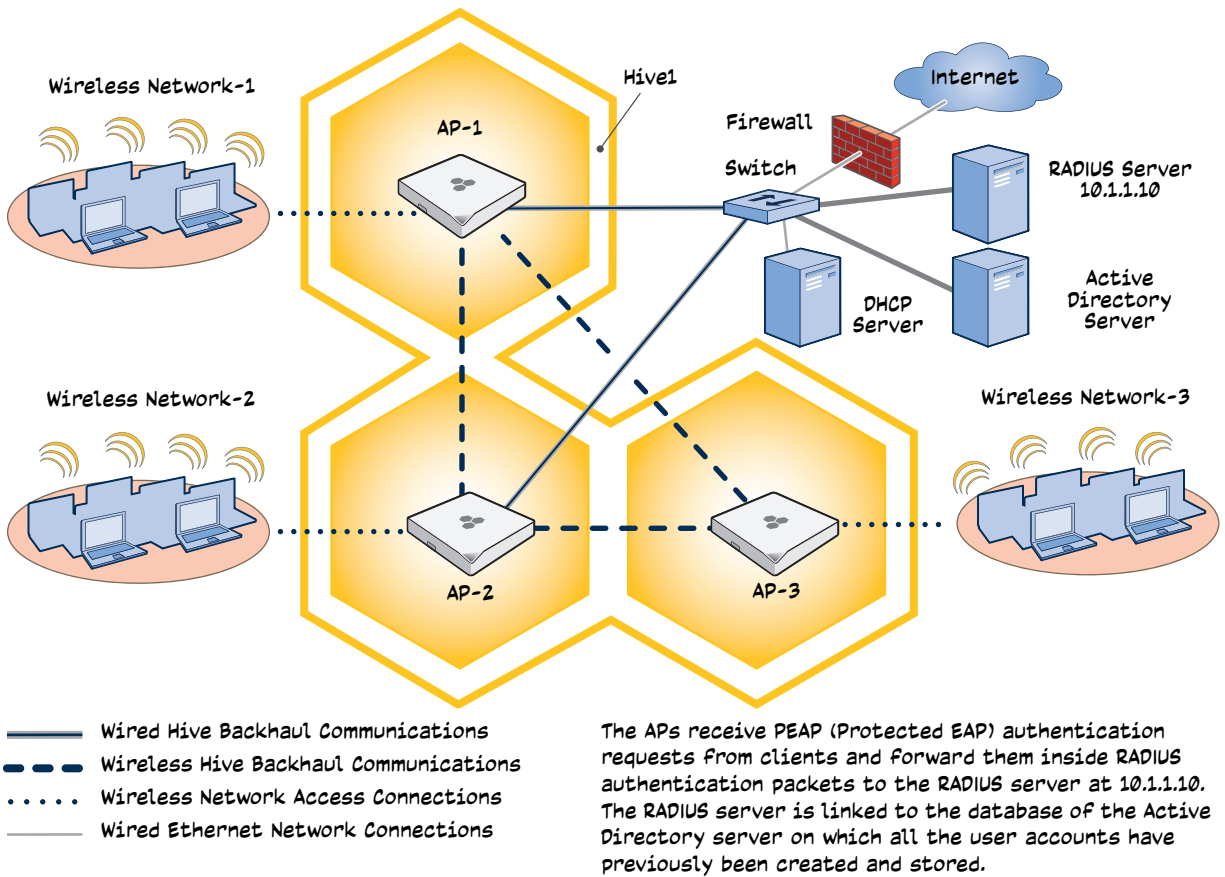
EXAMPLE 3: USING IEEE 802.1X AUTHENTICATION

In this example, you use a Microsoft AD (Active Directory) server and a RADIUS server to authenticate wireless network users. To accomplish this, you make the following modifications to the hive set up in "Deploying a Hive":

- Configure settings for the RADIUS server on the APs
- Change the SSID parameters on the APs and wireless clients to use IEEE 802.1X

The basic network design is shown in Figure 3.

Figure 3 Hive and 802.1X authentication



(1) This example assumes that the RADIUS and AD servers were previously configured and populated with user accounts that have been in use on a wired network (not shown). The only additional configuration on these servers is to enable the RADIUS server to accept authentication requests from the APs.

Step 1 Define the RADIUS server on the AP-1

Configure the settings for the RADIUS server (IP address and shared secret) on AP-1.

```
aaa radius-server primary 10.1.1.10 shared-secret s3cr3741n4b10X
```

The IP address of the RADIUS server is 10.1.1.10, and the shared secret that AP-1 and the RADIUS server use to authenticate each other is "s3cr3741n4b10X". You must also enter the same shared secret on the RADIUS server when you define the APs as access devices (see step 4).

Step 2 Change the SSID on AP-1

1. Change the authentication method in the security object referenced by SSID "employee".

```
security-object employee security protocol-suite wpa-auto-8021x
```

```
save config
```

The protocol suite requires WPA (Wi-Fi Protected Access) or WPA2 security protocol for authentication and key management, AES or TKIP encryption, and user authentication through IEEE 802.1X.

2. Enter the **show interface mgt0** command and note the dynamically assigned IP address of the mgt0 interface. You need to know this address to define AP-1 as an access device on the RADIUS server in step 4.

```
exit
```

Step 3 Configure AP-2 and AP-3

1. Log in to AP-2 through its console port.
2. Configure AP-2 with the same commands that you used for AP-1:

```
aaa radius-server primary 10.1.1.10 shared-secret s3cr3741n4b10X
```

```
security-object employee security protocol-suite wpa-auto-8021x
```

```
save config
```

(1) Although all APs in this example use the same shared secret, they can also use different secrets.

3. Enter the **show interface mgt0** command to learn its IP address. You need this address for step 4.
exit
4. Log in to AP-3 and enter the same commands.

Step 4 Configure the RADIUS Server to accept authentication requests from the APs

Log in to the RADIUS server and define the three APs as access devices. Enter their individual mgt0 IP addresses or the subnet containing the IP addresses of all their mgt0 interfaces and the shared secret: **s3cr3741n4b10x**

Step 5 Modify the SSID on the wireless clients

Modify the "employee" SSID on all the wireless clients in wireless network-2 and -3. Specify WPA or WPA2 for network authentication, AES or TKIP for data encryption, and PEAP (Protected EAP) for user authentication.

If the supplicant is on a PC running Windows Vista and is on a domain, and the RADIUS server is configured with domain authentication:

1. View the available SSIDs in the area, and select **employee**.
2. Click **Connect**.

Because most PC-based supplicants use their Windows login credentials to authenticate the client with the domain, the 802.1X authentication process happens automatically.

((c)) 1	<i>If the supplicant is on a PC running Windows XP, you must configure it to use PEAP for authentication. By default, a Windows XP wireless client uses Smart Card or other Certificate instead of PEAP.</i>
-------------------	--

If the supplicant is Windows-based and you are not on a domain

1. Configure the SSID on your client as follows:
 - Network name (SSID): **employee**
 - Network authentication: **WPA2**
 - Data encryption: **AES**
 - Enable IEEE 802.1X authentication for this network: (select)
 - EAP type: **Protected EAP (PEAP)**
 - Authenticate as computer when computer information is available: (clear)
 - Authenticate as guest when user or computer information is unavailable: (clear)
 - Validate server certificate: (clear)
 - Select Authentication Method: **Secured password (EAP-MSCHAP v2)**
 - Automatically use my Windows logon name and password (and domain if any): (clear)
2. View the available SSIDs in the area and select **employee**.
3. Click **Connect**.
4. When the prompt appears for you to select a certificate or enter other credentials to validate your identity, click the prompt, enter the user name and password that are stored on the RADIUS authentication server, and then click **OK**.

If the supplicant is on a Macintosh computer and is not on a domain:

1. View the available SSIDs in the area, and select **employee**.
2. Click **Join Network**.
3. Accept the certificate that the RADIUS server provides, assuming it is from a trustworthy source.

After the RADIUS authentication server validates your identity, the client connects to the WLAN.

Step 6 Check that clients can form associations and access the network

- To check that a client can associate with an AP and access the network, open a wireless client application and connect to the "employee" SSID. Then contact a network resource, such as a web server.
- Log in to the CLI, and check that you can see the MAC address or the associated client and an indication that the correct SSID is in use by entering the following command:

```
show ssid employee station
```

```
Chan=channel number; Pow=Power in dBm;
A-Mode=Authentication mode; Cipher=Encryption mode;
A-Time=Associated time; Auth=Authenticated;
UPID=User profile Identifier; Phymode=Physical mode;
```

Mac Addr	IP Addr	Chan	Tx Rate	Rx Rate	Pow	A-Mode	Cipher	A-Time	VLAN	Auth	UPID	Phymode
0016:cf8c:57bc	10.1.1.73	1	54M	54M	-40	8021x	aes ccm	00:02:34	1	Yes	0	11b/g

```
Total station count: 1
```

Check that the MAC and IP addresses in the table match those of the wireless client.

Check that the authentication and encryption modes match those in the SSID security protocol suite.

(C) You can also enter the following commands to check the association status of a wireless client:
show auth, **show roaming cache**, and **show roaming cache mac <mac_addr>**.

The setup for using IEEE 802.1X is complete. Wireless clients can now associate with the AP using SSID "employee", authenticate themselves through IEEE 802.1X to a RADIUS server, and access the network.

EXAMPLE 4: APPLYING QoS

In this example, you want the hive members to prioritize voice, streaming media, and e-mail traffic. First, you map distinguishing elements of these traffic types to three Aerohive QoS (Quality of Service) classes:

Class 6: voice traffic from VoIP phones with MAC OUI 00:12:3b (the OUI for all phones in the network)

Voice traffic is very sensitive to delay and cannot tolerate packet loss without loss of voice quality. When other traffic is competing with voice traffic for bandwidth, it becomes essential to prevent that traffic from interfering with voice traffic. Because voice traffic for a single call requires very little bandwidth—typically from 8 to 64 Kbps depending on the voice codec used—a good approach for setting its rate is to calculate the bandwidth necessary for a voice call plus related telephony traffic from a single user's computer, softphone, or handset and then multiply that by the potential number of concurrent VoIP users.

Class 5: streaming media using the MMS (Microsoft Media Server) protocol on TCP port 1755

Although streaming media is also time sensitive, streaming media software for both clients and servers offers limited buffering to prevent choppy sounds and pixelated video when network congestion occurs. Because congestion for more than a few seconds can adversely effect streaming media, it is important to assign this type of traffic a higher priority than other types, but its priority should be lower than that for voice, which is even more sensitive to delay.

Class 3: data traffic for e-mail using the following protocols:

SMTP (Simple Mail Transfer Protocol) on TCP port 25

POP3 (Post Office Protocol version 3) on TCP port 110

Then you create classifier profiles that reference these traffic-to-class mappings. You bind the profiles to the wifi0.1 and eth0 interfaces so that hive members map the traffic matching these profiles that arrives at these interfaces to the proper Aerohive classes.

You next define a QoS policy that defines how the hive members prioritize and process the traffic mapped to Aerohive classes 6, 5, and 3. The QoS policy (named "voice") is shown in [Figure 4 on page 94](#) and has these settings:

Class 6 (voice)

Forwarding: strict (Hive members forward traffic mapped to this class immediately without queuing it.)

Maximum rate for all class 6 traffic: 512 Kbps, which supports an 8- to 64-Kbps VoIP call (depending on the compression that the codec provides) plus other telephony traffic such as DHCP, DNS, HTTP, and TFTP.

Class 5 (streaming media)

Forwarding: WRR (weighted round robin) with a weight of 90

By assigning class 5 a higher weight (90) than class 3 and 2 weights (class 3 = 60, class 2 = 30), you give streaming media roughly a 3:2 priority over class 3 traffic and a 3:1 priority over class 2 traffic.

Maximum traffic rate for all class 5 traffic: 20,000 Kbps

You change the bandwidth available for streaming media when there is no competition for it (the default rate for class 5 is 10,000 Kbps on APs that do not support the IEEE 802.11n standard and 50,000 Kbps on APs that do. However, you do not set the maximum rate (54,000 or 1,000,000 Kbps, depending on the AP model that you are configuring) to ensure that streaming media does not consume all available bandwidth even if it is available.

Class 3 (e-mail)

Forwarding: WRR with a weight of 60

To help ensure that e-mail traffic remains flowing even when other types of data traffic compete with it for available bandwidth, you elevate its priority by mapping SMTP and POP3 traffic to class 3 and giving that class a higher weight (60) than the weight for class 2 traffic (30).


Maximum traffic rate for all class 3 traffic: 54,000 or 1,000,000 Kbps (the default, depending on the AP)

(1)	<i>The AP assigns all traffic that you do not specifically map to an Aerohive class to class 2, which by default uses WRR with a weight of 30 and a rate of 54,000 or 1,000,000 Kbps, depending on the AP.</i>
------------	--

Figure 4 QoS policy "voice" for voice, streaming media, and data


QoS Policy: "voice"

Voice `qos policy voice qos 6 strict 512 0`



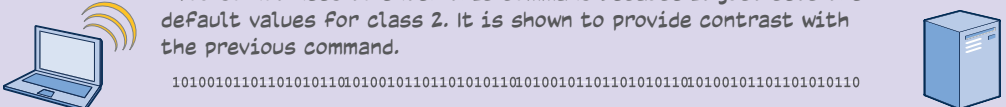
The policy assigns the highest priority to voice traffic (class 6). For each voice session up to 512 Kbps, hive members provide "strict" forwarding; that is, they forward traffic immediately without queuing it.

Streaming Media `qos policy voice qos 5 wrr 20000 90`



Because streaming media (class 5) needs more bandwidth than voice does, the policy defines a higher forwarding rate for it: 20,000 Kbps. It sorts streaming media into forwarding queues using the WRR (weighted round robin) mechanism. It also prioritizes streaming media by assigning a higher weight (90) than it assigns data traffic (class 3 = 60, class 2 = 30).

Data `qos policy voice qos 3 wrr { 54000 | 1000000 } 60`
`qos policy voice qos 2 wrr { 54000 | 1000000 } 30*`



* You do not need to enter this command because it just sets the default values for class 2. It is shown to provide contrast with the previous command.

1010010110110101011010101001011011010101101010010110110101010101001011011010110

The policy sorts class 3 and 2 traffic into forwarding queues using WRR and defines the highest forwarding rate: 54,000 Kbps or 1,000,000 Kbps, depending on the HiveAP model that you are configuring. It gives class 3 (for e-mail protocols SMTP and POP3) a higher WRR weight (60) so that the HiveAP queues more e-mail traffic in proportion to other types of traffic in class 2, which has a weight of 30 by default. As a result, e-mail traffic has a better chance of being forwarded than other types of traffic when bandwidth is scarce.

Class 2 is for all types of traffic not mapped to an Aerohive class—such as HTTP for example.

(i) This example assumes that the RADIUS and AD servers were previously configured and populated with user accounts and have been serving a wired network (not shown). The only additional configuration is to enable the RADIUS server to accept authentication requests from the APs.

Finally, you create a user profile "employee-net" and apply the QoS policy "voice" to the user profile on each hive member. You also configure the RADIUS server to return attributes in its authentication responses to indicate the user group to which the hive members then assign users.

Step 1 Map traffic types to Aerohive QoS classes on AP-1

1. Map the MAC OUI (organizational unit identifier) of network users' VoIP phones to Aerohive class 6.

```
qos classifier-map oui 00:12:3b qos 6
```

In this example, all network users use VoIP phones from the same vendor whose OUI (that is, the MAC address prefix) is 00:12:3b. When AP-1 receives traffic from a client whose source MAC address contains this OUI, it assigns it to Aerohive class 6.

2. Define the custom service that you need.

```
service mms protocol tcp port 1755
```

The MMS (Microsoft Media Server) protocol can use several transports (UDP, TCP, and HTTP). However, for an AP to be able to map a service to an Aerohive QoS class, it must be able to identify that service by a unique characteristic such as a static destination port number or a nonstandard protocol number. Unlike MMS/UDP and MMS/HTTP, both of which use a range of destination ports, MMS/TCP uses the static destination port 1755, which an AP can use to map the service to an Aerohive class. Therefore, you define a custom service for MMS using TCP port 1755.

3. Map services to Aerohive classes.

```
qos classifier-map service mms qos 5
```

```
qos classifier-map service smtp-tcp qos 3
```

```
qos classifier-map service pop3-tcp qos 3
```

By mapping these services to Aerohive class 5 and 3, you can prioritize e-mail traffic above other types of traffic that the AP assigns to class 2 by default. In this example, you prioritize voice, media, and e-mail traffic by assigning them to higher QoS classes than class 2, and then by defining the forwarding and weighting mechanisms for each class (see step 3).

Step 2 Create profiles to check traffic arriving at interfaces on AP-1

1. Define two classifier profiles for the traffic types "mac" and "service".

```
qos classifier-profile employee-voice mac
```

```
qos classifier-profile employee-voice service
```

```
qos classifier-profile eth0-voice mac
```

```
qos classifier-profile eth0-voice service
```

Classifier profiles define which components of incoming traffic AP-1 checks. Because you specify "mac" and "service", it checks the MAC address in the Ethernet frame header and the service type (by protocol number in the IP packet header and port number in the transport packet header). If it detects traffic matching a classifier-map, it maps it to the appropriate Aerohive class. However, before this can happen, you must first associate the profiles with the interfaces that will be receiving the traffic that you want checked. This you do with the next two commands.

2. Associate the classifier profiles with the employee SSID and the eth0 interface so that AP-1 can classify incoming traffic arriving at these two interfaces.

```
ssid employee qos-classifier employee-voice
```

```
interface eth0 qos-classifier eth0-voice
```

By creating two QoS classifiers and associating them with the employee SSID and eth0 interface, AP-1 can classify traffic flowing in both directions for subsequent QoS processing;

that is, it can classify traffic flowing from the wireless LAN to the wired LAN, and from the wired LAN to the wireless LAN.

(1) *If the surrounding network employs the IEEE 802.1p QoS classification system (for wired network traffic) or 802.11e (for wireless network traffic), you can ensure that AP-1 checks for them by entering these commands:*

```
qos classifier-profile eth0-voice 8021p
qos classifier-profile employee-voice 80211e
```

Step 3 Apply QoS on AP-1

1. Create a QoS policy.

For APs supporting IEEE 802.11a/b/g:

```
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 54000 60
```

For APs supporting IEEE 802.11a/b/g/n:

```
qos policy voice qos 6 strict 512 0
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 1000000 60
```

By default, a newly created QoS policy attempts to forward traffic mapped to classes 6 and 7 immediately upon receipt. This immediate forwarding of received traffic is called "strict" forwarding. To assign strict forwarding to VoIP traffic from phones whose MAC OUI is mapped to class 6, you simply retain the default settings for class 6 traffic on APs supporting 802.11a/b/g data rates. For APs supporting 802.11n data rates, the default user profile rate is 20,000 Kbps for class 6 traffic, so you change it to 512 Kbps.

For classes 5 and 3, you limit the rate of traffic and set WRR (weighted round robin) weights so that the AP can control how to put the rate-limited traffic into forwarding queues. You use the default settings for class 2 traffic.

When you enter any one of the above commands, the AP automatically sets the maximum bandwidth for all members of the user group to which you later apply this policy and the bandwidth for any individual group member. You leave the maximum traffic rate at the default 54,000 Kbps or 1,000,000 Kbps—depending on the AP model that you are configuring—for the user group. You also leave the maximum bandwidth for a single user at 54,000 or 1,000,000 Kbps, so that if a single user needs all the bandwidth and there is no competition for it, that user can use it all.

Also by default, the traffic rate for this policy has a weight of 10. At this point, because this is the only QoS policy, the weight is inconsequential. If there were other QoS policies, then their weights would help determine how the AP would allocate the available bandwidth.

The QoS policy that you define is shown in [Figure 5](#). Although you did not configure settings for Aerohive QoS classes 0, 1, 2, 4, and 7, the policy applies default settings to them. The AP assigns all traffic that you do not specifically map to an Aerohive class to class 2, which uses WRR with a weight of 30 and a default rate of 54,000 or 1,000,000 Kbps. Because nothing is mapped to classes 0, 1, 4, and 7, their settings are irrelevant.

Figure 5 QoS policy "voice"

The user profile rate defines the total amount of bandwidth for all users to which this policy applies. The user rate defines the maximum amount for any single user. The user rate can be equal to but not greater than the user profile rate. (Note: The maximums shown here are for APs that support 802.11n data rates. For other APs, the maximum rates are 54,000 Kbps.)

```
show qos policy voice
Policy name=voice; user rate limit=1000000kbps;
User profile rate=1000000kbps; user profile weight=10;
Class=0; mode=wrr; weight=10; limit=1000000kbps;
Class=1; mode=wrr; weight=20; limit=1000000kbps;
Class=2; mode=wrr; weight=30; limit=1000000kbps;
Class=3; mode=wrr; weight=60; limit=1000000kbps;
Class=4; mode=wrr; weight=50; limit=1000000kbps;
Class=5; mode=wrr; weight=90; limit=20000kbps;
Class=6; mode=strict; weight=0; limit=512kbps;
Class=7; mode=strict; weight=0; limit=20000kbps;
```

The forwarding mode for class 6 (voice) is strict. The AP forwards packets belonging to this class immediately without queuing them.

The forwarding mode for class 5 (streaming media) and 2 - 3 (data) is WRR (weighted round robin). The HiveAP forwards traffic belonging to these classes by putting them into forwarding queues. The weights determine how many bits per second go into each queue. For every 30 bits that the AP queues for class 2, it queues approximately 60 bits for class 3, and 90 bits for class 5. These amounts are approximations because the AP also has an internal set weights for traffic in different classes that skews forwarding in favor of traffic belonging to higher classes.

2. Create a user profile and apply the QoS policy to it.

```
user-profile employee-net qos-policy voice attribute 2
```

You apply the QoS policy "voice" to all users belonging to the user-profile "employee-net" with attribute 2. On the RADIUS server, you must configure attribute 2 as one of the RADIUS attributes that the RADIUS server returns when authenticating users (see step 5 on page 99).

((1))

When AP-1 does not use RADIUS for authentication, you must assign the user profile to an SSID. To do that, use the following command: `ssid employee default-user-profile-attr 2`

```
save config
```

```
exit
```

Step 4 Configure AP-2 and AP-3

1. Log in to AP-2 through its console port.
2. Configure AP-2 with the same commands that you used for AP-1:

```
qos classifier-map oui 00:12:3b qos 6
service mms protocol tcp port 1755
qos classifier-map service mms qos 5
qos classifier-map service smtp qos 3
qos classifier-map service pop3 qos 3
qos classifier-profile employee-voice mac
qos classifier-profile employee-voice service
qos classifier-profile eth0-voice mac
qos classifier-profile eth0-voice service
ssid employee qos-classifier employee-voice
interface eth0 qos-classifier eth0-voice
```

For APs supporting IEEE 802.11a/b/g:

```
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 54000 60
```

For APs supporting IEEE 802.11a/b/g/n:

```
qos policy voice qos 6 strict 512 0
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 1000000 60
```

```
user-profile employee-net qos-policy voice attribute 2
save config
exit
```

3. Log in to AP-3 and enter the same commands.

Step 5 Configure RADIUS server attributes

1. Log in to the RADIUS server and define the three APs as RADIUS clients.
2. Configure the following attributes for the realm to which the wireless user accounts in network-1, -2, and -3 belong:
 - Tunnel Type = GRE (value = 10)
 - Tunnel Medium Type = IP (value = 1)
 - Tunnel Private Group ID = 2

The RADIUS server returns the above attributes for all wireless users it authenticates from network-1, -2, and -3. The AP uses the combination of returned RADIUS attributes to assign users to the user group 2 ("employee-net"). It does not use them to create a GRE tunnel, which the tunnel type attribute might lead you to think.

When there is more traffic than available bandwidth, the AP applies the "voice" policy. It performs strict forwarding for voice and uses a WRR (weighted round robin) scheduling discipline for directing streaming media and data traffic to queues to await forwarding. The QoS configuration is complete.

EXAMPLE 5: LOADING A BOOTSTRAP CONFIGURATION

As explained in ["HiveOS Configuration File Types" on page 75](#), a bootstrap config file is typically a small set of commands to which an AP can revert when the configuration is reset or if the AP cannot load its current and backup configs. If you do not define and load a bootstrap config, the AP reverts to the default config in these situations, which can lead to two potential problems:

- If both the current and backup configs fail to load on an AP acting as a mesh point in a hard-to-reach location—such as a ceiling crawlspace—the AP would revert to the default config. Because a mesh point needs to join a hive before it can access the network and the default config does not contain the hive settings that the mesh point needs to join the hive, an administrator would need to crawl to the device to make a console connection to reconfigure the AP.
- If the location of an AP is publicly accessible, someone could press the reset button on the front panel of the device to return the configuration to its default settings, log in using the default login name and password (*admin, aerohive*), and thereby gain complete admin access. (Note that you can disable the ability of the reset button to reset the configuration by entering this command: **no reset-button reset-config-enable**)

A bootstrap configuration can help in both of these situations. For the first case, a bootstrap config with the necessary hive membership settings can allow the AP to connect to the network and thereby become accessible over the network for further configuring. For the second case, a bootstrap config with a number of obstacles such as a hard-to-guess login name and password and a disabled access subinterface can make the firmware inaccessible and the device unusable.

AP-1 and -2 are in locations that are not completely secure. AP-3 is a mesh point in a fairly inaccessible location. To counter theft of the first two APs and to avoid the nuisance of physically accessing the third AP, you define a bootstrap config file that addresses both concerns and load it on the APs.

Step 1 Define the bootstrap config on AP-1

1. Make a serial connection to the console port on AP-1, log in, and load the default config.

```
load config default
reboot
```

You do not want the bootstrap config to contain any of your previously defined settings from the current config. Therefore, you load the default config, which has only default settings. When you begin with the default config and enter the commands that define the bootstrap config, the bootstrap config will have just those commands and the default config settings.

2. Confirm the `reboot` command, and then, when you are asked if you want to use the Aerohive Initial Configuration Wizard, enter `no`.
3. Log in using the default user name `admin` and password `aerohive`.
4. Define admin login parameters for the bootstrap config that are difficult to guess.

```
admin root-admin Cwb12o11siNI8vhD2hs password 8wDamKC1Lo53Ku71
```

You use the maximum number of alphanumeric characters for the login name (20 characters) and password (32 characters). By mixing uppercase and lowercase letters with numbers in strings that do not spell words or phrases, you make the login much harder to guess.



Be careful to remember the login name and password defined in a bootstrap config file. If they become lost or forgotten, you must obtain a one-time login key from Aerohive technical support. To get the key, you must already have had a support contract in place. The first one-time login key is free. After that, there is a small handling fee for each additional key.

5. Leave the various interfaces in their default up or down states.

By default, the `wifi0` and `wifi0.1` interfaces are down, but the `mgt0`, `eth0`, `wifi1`, and `wifi1.1` subinterfaces are up. The hive members need to use `wifi1.1`, which is in backhaul mode, so that AP-3 can rejoin `hive1` and, through `hive1`, access DHCP and DNS servers to regain network connectivity. (By default, `mgt0` is a DHCP client.) You leave the `eth0` interface up so that `Hive-1` and `Hive-2` can retain an open path to the wired network. However, with the two interfaces in access mode—`wifi0` and `wifi0.1`—in the down state, none of the APs will be able provide network access to any wireless clients. Wireless clients cannot form associations through `wifi1.1` nor can a computer attach through the `eth0` interface—because it is also in backhaul mode—and obtain network access through the mesh.

6. Define the hive settings so that any of the three APs using the bootstrap config can rejoin the grid.

```
hive hive1
hive hive1 password s1r70ckH07m3s
interface mgt0 hive hive1
```

When an AP boots up using the bootstrap config, it can rejoin `hive1` because the configuration includes the hive name and password and binds the `mgt0` interface to the hive. This is particularly useful for AP-3 because it is a mesh point and can only access the wired network after it has joined the hive. It can then reach the wired network through either of the portals, AP-1 or AP-2.

7. Save the configuration as a bootstrap config.

```
save config running bootstrap
```

If anyone resets the current configuration, the AP will load this bootstrap config and thwart any thief from accessing the configuration and any wireless client from accessing the network.

Step 2 Save the bootstrap config to a TFTP server

1. Check the configurations to make sure the settings are accurate.

```
show config bootstrap
```

Check that the settings are those you entered in the previous step for the bootstrap config.

```
show config backup
```

Note that the backup config is the previous current config. This is the configuration that has all your previously defined settings.

2. Return to the previous current config.

```
load config backup
```

```
reboot
```

3. When AP-1 finishes rebooting, log back in using the login parameters you set in ["Example 1: Deploying a Single AP" on page 80](#) (*mwebster, 3fF8hq*).

4. Check that the current config is the same as your previous current config.

```
show config current
```

5. Save the file as bootstrap-hive1.txt to the root directory of your TFTP server running on your management system at 10.1.1.31, an address received by the same DHCP server and in the same subnet as the AP addresses.

```
save config bootstrap tftp://10.1.1.31:bootstrap-hive1.txt
```

Step 3 Load the bootstrap config file on AP-2 and AP-3

1. Make a serial connection to the console port on AP-2 and log in.
2. Upload the bootstrap-hive1.txt config file from the TFTP server to AP-2 as a bootstrap config.

```
save config tftp://10.1.1.31:bootstrap-hive1.txt bootstrap
```

3. Check that the uploaded config file is now the bootstrap config.

```
show config bootstrap
```

4. Repeat the procedure to load the bootstrap config on AP-3.

The bootstrap configs are now in place on all three APs.

CLI COMMANDS FOR EXAMPLES

This section includes all the CLI commands for configuring the APs in the previous examples. The CLI configurations are presented in their entirety (without explanations) as a convenient reference, and—if you are reading this guide as a PDF—as an easy way to copy and paste the commands. Simply copy the blocks of text for configuring the APs in each example and paste them at the command prompt.

((G))	<i>The following sections omit optional commands, such as changing the login name and password, and commands used to check a configuration.</i>
--------------	---

Commands for Example 1

Enter the following commands to configure the SSID “employee” on a single AP, change the login credentials for the root admin, and change the AP host name in ["Deploying a Single AP" on page 80](#):

```
security-object employee
security-object employee security protocol-suite wpa-auto-psk ascii-key N38bu7Adr0n3
ssid employee
ssid employee security-object employee
interface wifi0 ssid employee
admin root-admin mwebster password 3fF8ha
hostname AP-1
save config
```

Commands for Example 2

Enter the following commands to configure three APs as members of “hive1” in ["Deploying a Hive" on page 83](#):

AP-1

```
hive hive1
hive hive1 password slr70ckH07m3s
interface mgt0 hive hive1
save config
```

AP-2

```
security-object employee
security-object employee security protocol-suite wpa-auto-psk ascii-key N38bu7Adr0n3
ssid employee
ssid employee security-object employee
interface wifi0 ssid employee
hive hive1
hive hive1 password slr70ckH07m3s
```

```
interface mgt0 hive hive1
save config
```

AP-3

```
security-object employee
security-object employee security protocol-suite wpa-auto-psk ascii-key N38bu7Adr0n3
ssid employee
ssid employee security-object employee
interface wifi0 ssid employee
hive hive1
hive hive1 password slr70ckH07m3s
interface mgt0 hive hive1
save config
```

Commands for Example 3

Enter the following commands to configure the hive members to support IEEE 802.1X authentication in ["Using IEEE 802.1X Authentication" on page 89](#):

AP-1

```
aaa radius-server primary 10.1.1.10 shared-secret s3cr3741n4b10X
ssid employee security protocol-suite wpa-auto-8021x
save config
```

AP-2

```
aaa radius-server primary 10.1.1.10 shared-secret s3cr3741n4b10X
ssid employee security protocol-suite wpa-auto-8021x
save config
```

AP-3

```
aaa radius-server primary 10.1.1.10 shared-secret s3cr3741n4b10X
ssid employee security protocol-suite wpa-auto-8021x
save config
```


Commands for Example 4

Enter the following commands to configure the hive members to apply QoS (Quality of Service) to voice, streaming media, and data traffic in ["Applying QoS" on page 92](#):

AP-1

```
qos classifier-map oui 00:12:3b qos 6
service mms protocol tcp port 1755
qos classifier-map service mms qos 5
qos classifier-map service smtp qos 3
qos classifier-map service pop3 qos 3
qos classifier-profile employee-voice mac
qos classifier-profile employee-voice service
qos classifier-profile eth0-voice mac
qos classifier-profile eth0-voice service
ssid employee qos-classifier employee-voice
interface eth0 qos-classifier eth0-voice
```

For APs supporting IEEE 802.11a/b/g

```
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 54000 60
```

For APs supporting IEEE 802.11a/b/g/n

```
qos policy voice qos 6 strict 512 0
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 1000000 60
```

```
user-profile employee-net qos-policy voice attribute 2
save config
```

AP-2

```
qos classifier-map oui 00:12:3b qos 6
service mms protocol tcp port 1755
qos classifier-map service mms qos 5
qos classifier-map service smtp qos 3
qos classifier-map service pop3 qos 3
qos classifier-profile employee-voice mac
qos classifier-profile employee-voice service
qos classifier-profile eth0-voice mac
qos classifier-profile eth0-voice service
```

```
ssid employee qos-classifier employee-voice
interface eth0 qos-classifier eth0-voice
```

For APs supporting IEEE 802.11a/b/g

```
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 54000 60
```

For APs supporting IEEE 802.11a/b/g/n

```
qos policy voice qos 6 strict 512 0
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 1000000 60
```

```
user-profile employee-net qos-policy voice attribute 2
save config
```

AP-3

```
qos classifier-map oui 00:12:3b qos 6
service mms protocol tcp port 1755
qos classifier-map service mms qos 5
qos classifier-map service smtp qos 3
qos classifier-map service pop3 qos 3
qos classifier-profile employee-voice mac
qos classifier-profile employee-voice service
qos classifier-profile eth0-voice mac
qos classifier-profile eth0-voice service
ssid employee qos-classifier employee-voice
interface eth0 qos-classifier eth0-voice
```

For APs supporting IEEE 802.11a/b/g

```
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 54000 60
```

For APs supporting IEEE 802.11a/b/g/n

```
qos policy voice qos 6 strict 512 0
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 1000000 60
```

```
user-profile employee-net qos-policy voice attribute 2
save config
```

Commands for Example 5

Enter the following commands to create bootstrap config files and load them on the hive members in ["Loading a Bootstrap Configuration" on page 99](#):

bootstrap-security.txt

```
admin root-admin Cwb12o11siNIm8vhD2hs password 8wDamKC1Lo53Ku71
hive hive1
hive hive1 password s1r70ckH07m3s
interface mgt0 hive hive1
```

AP-1

```
save config tftp://10.1.1.31:bootstrap-security.txt bootstrap
show config bootstrap
```

AP-2

```
save config tftp://10.1.1.31:bootstrap-security.txt bootstrap
show config bootstrap
```

AP-3

```
save config tftp://10.1.1.31:bootstrap-meshpoint.txt bootstrap
show config bootstrap
```

Chapter 6 Traffic Types

This is a list of all the types of traffic that might be involved with an Aerohive deployment. If a firewall lies between any of the sources and destinations listed below, make sure that it allows these traffic types.

Traffic Supporting Network Access for Connected Clients

(()) When a router sends traffic from itself through a Layer 3 VPN tunnel, the source address is that of its tunnel interface, which is the same as that of its mgt0 interface. When an Aerohive VPN client sends traffic from itself through a Layer 2 VPN tunnel, the source address is also that of its tunnel interface, which the VPN server assigns it during the Xauth phase of the VPN tunnel setup.

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
Active Directory	AP RADIUS server mgt0 interface	Active Directory domain controller or global catalog server	6 TCP	1024-65535	139, and 445 or 3268	Required for an Aerohive RADIUS server to contact a domain controller on port 445 or a global catalog server on port 3268
			17 UDP	1024-65535	389	
APNs (Apple Push Notification service)	Apple devices	APNs server	6 TCP	1024-65535	5223	Required for mobile device management so Apple devices can conduct inventory and other management operations
APNs	JSS (JAMF Software Server)	APNs server	6 TCP	1024-65535	2195, 2196	Required for the JSS to send the APNs server messages (port 2195) and feedback queries (port 2196)
Bonjour	Bonjour-enabled devices	Multicast group at 224.0.0.251	17 UDP	1024-65535	5353	Required for devices to advertise services using Bonjour protocol
DHCP	unregistered captive web portal clients and DHCP clients	AP and router wifi or Ethernet access interface	17 UDP	68	67	Required for captive web portals and for assigning network settings to DHCP clients

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
DNS	unregistered captive web portal clients and DHCP clients	AP and router wifi or Ethernet access interface	17 UDP	53, or 1024 - 65535	53	Required for captive web portals and for proxying DNS requests
GRE	AP mgt0 interface	AP mgt0 interface	47 GRE	N.A.	N.A.	Required to support DNX (Dynamic Network Extensions) and Layer 3 roaming among hive members
HTTP	unregistered captive web portal clients	AP and router wifi or Ethernet access interface	6 TCP	1024 - 65535	80	Required for captive web portal functionality
HTTPS	unregistered captive web portal clients	AP and router wifi or Ethernet access interface	6 TCP	1024 - 65535	443	Required for captive web portal functionality using a server key
Proxied HTTP and HTTPS	router WAN interface	Barracuda or Websense server	6 TCP	1024-65535	8081 for Websense; 8080 for Barracuda*	Required to provide web security services
IKE	Layer 2 VPN: AP VPN client mgt0 interface Layer 3 VPN: router WAN interface	Layer 2 VPN: AP VPN server or HiveOS VA mgt0 interface Layer 3 VPN: HiveOS VA eth0 interface	17 UDP	500 and 4500 for NAT-Traversal	500 and 4500 for NAT-Traversal	Required for the initiation of Layer 2 and Layer 3 VPN tunnels
IPsec ESP	Layer 2: AP VPN client, HiveOS VA, or AP VPN server mgt0 interface Layer 3: router WAN interface or HiveOS VA eth0 interface	Layer 2: AP VPN server, HiveOS VA, or AP VPN client mgt0 interface Layer 3: router WAN interface or HiveOS VA eth0 interface	50 ESP	N.A.	N.A.	Required for IPsec VPN traffic to flow between VPN end points

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
IPsec ESP with NAT-Traversal enabled	Layer 2: AP VPN client, HiveOS VA, or AP VPN server mgt0 interface Layer 3: router WAN interface or HiveOS VA eth0 interface	Layer 2: AP VPN client, HiveOS VA, or AP VPN server mgt0 interface Layer 3: router WAN interface or HiveOS VA eth0 interface	17 UDP	4500	4500	Required for VPN traffic to flow when a NAT device is detected inline
LDAP	AP RADIUS server mgt0 interface	OpenLDAP server	6 TCP	1024-65535	389	Required for an Aerohive RADIUS server to contact an OpenLDAP server
LDAP	JSS (JAMF Software Server)	LDAP server	6 TCP	1024-65535	389	Required for the JSS to look up users on an LDAP server
LDAPS	AP RADIUS server mgt0 interface	OpenLDAP server	6 TCP	1024-65535	636	Required for an Aerohive RADIUS server to make an encrypted connection to an OpenLDAP server
Library SIP Patron Information Requests	Aerohive RADIUS authentication server	Library SIP server	6 TCP	1024-65535	6001*	Required to look up patron accounts on a Library SIP server
Open Directory	Aerohive RADIUS authentication server	Open Directory server	6 TCP	1024-65535	88, 389, 139, 445	Required to look up accounts on Open Directory
RADIUS accounting	AP mgt0 interface	RADIUS server	17 UDP	1024 - 65535	1813*	Required to support RADIUS accounting
RADIUS authentication	AP mgt0 interface	RADIUS server	17 UDP	1024 - 65535	1812*	Required for 802.1X authentication of users
SSL	AP or router mgt0 interface and Apple devices	JSS (JAMF Software Server)	6 TCP	1024-65535	8443 or 443	Required for Apple devices to enroll on a JSS
SSL	JSS	Apple Mac computers	6 TCP	1024-65535	443	Required for JSS to deploy packages and scripts to Macs

* This is the default destination port number. You can change it to a different port number from 1 to 65535.

Traffic Supporting Management of Aerohive Devices

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
CAPWAP (Control and Provisioning of Wireless Access Points)	Aerohive device mgt0 or WAN interface	HiveManager	17 UDP	12222	12222	Required for Aerohive devices to discover HiveManager and send it alarms, events, reports, traps, and SSH keys Used by HiveManager to upload delta configs to devices
Distributed HiveOS image download	AP mgt0 interface	AP mgt0 interface	6 TCP	1024-65535	3007	Required for distributing a HiveOS image downloaded to one AP from HiveManager and from there to all other hive members
HTTP	management system	HiveManager MGT port	6 TCP	1024-65535	80	Redirected to HTTPS when accessing the HiveManager and HiveManager Online GUI Used for uploading image files for maps to HiveManager Online
	management system	HiveManager MGT port	6 TCP	1024-65535	8080	Used for uploading image files for maps to HiveManager
	Aerohive device mgt0 or WAN interface	HiveManager MGT port	6 TCP	1024-65535	80	Used as CAPWAP transport by Aerohive devices connecting to HiveManager and HiveManager Online through HTTP proxy servers Used by HiveManager and HiveManager Online to monitor devices and push delta configs
HTTPS	management system	HiveManager MGT port	6 TCP	1024 - 65535	443	Required for accessing the HiveManager and HiveManager Online GUI Used for uploading HiveOS images, image files for captive web portals, and certificates to HiveManager and HiveManager Online
	Aerohive device mgt0 or WAN interface	HiveManager MGT port	6 TCP	1024-65535	443	Used to upload files—HiveOS images, full configs, captive web portal pages, certificates—from HiveManager and HiveManager Online to Aerohive devices
	HiveOS VA mgt0 interface	License server	6 TCP	1024-65535	443	Used by the HiveOS Virtual Appliance to register itself on the license server (hmupdates.aerohive.com)

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
Iperf	mgt0 interface on Iperf client	mgt0 interface on Iperf server	6 TCP	1024-65535	5001*	Required for performing diagnostic testing of network performance
Remote Sniffer	Admin workstation	Aerohive device mgt0 interface	6 TCP	1024 - 65535	2002*	Used when capturing packets on Aerohive device interfaces
SNMP	SNMP managers	AP and HiveOS VA mgt0 interface	17 UDP	1024 - 65535	161	Required for SNMP managers to contact Aerohive devices
SNMP traps	AP and HiveOS VA mgt0 interface	SNMP managers	17 UDP	1024 - 65535	162	Required for sending SNMP traps to configured SNMP managers
SSHv2	Aerohive device mgt0 or WAN interface	HiveManager	6 TCP	1024 - 65535	22	Required for the HiveManager to upload files—HiveOS images, full configs, captive web portals pages, certificates—to Aerohive devices
TFTP	Aerohive device mgt0 or WAN interface	HiveManager	17 UDP	1024 - 65535	69	Used for loading HiveOS image files from HiveManager to devices

* This is the default destination port number. You can change it to a different port number from 1 to 65535.

Traffic Supporting Device Operations

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
Aerohive Cooperative Control Messages	AP and router mgt0 interface	AP and router mgt0 interface	17 UDP	3000*	3000*	Required for hive communications and operates at layer 3
Aerohive Cooperative Control Messages	AP wifi and Ethernet backhaul interface Router wifi backhaul interface and LAN interface	AP wifi and Ethernet backhaul interface Router wifi backhaul interface and LAN interface	N.A.	N.A.	N.A.	Required for hive communications and operates at the LLC (Logical Link Control) sublayer of layer 2
Aerohive HA	HiveManager MGT or LAN ports	HiveManager MGT or LAN ports	6 TCP	12388 and 12389	12388 and 12389	Proprietary Aerohive services used for HA communications
AeroScout Reports	AeroScout engine	AP mgt0 interface	17 UDP	1024 - 65535	1144	Required to report tracked devices to an AeroScout engine

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
DHCP	Aerohive device mgt0 or WAN interface	DHCP server	17 UDP	68	67	By default, all Aerohive devices get their network settings through DHCP.
DNS	Aerohive device mgt0 or WAN interface	DNS server	17 UDP	53 or 1024-65535	53	Required for Aerohive devices to resolve domain names in their configurations; for example, the CAPWAP server and redirector Routers can proxy DNS lookups
Ekahau	Ekahau Positioning Engine (EPE)	AP mgt0 interface	17 UDP	1024-65535	8552, 8553, 8554	Required for APs to communicate with EPE
ICMP	Aerohive device mgt0 or WAN interface	tracked object	1 ICMP	N.A.	N.A.	Required for IP tracking
Linux-HA Heartbeat	HiveManager MGT port	HiveManager MGT port	17 UDP	694	694	Required for heartbeats between HA nodes
NTP	Aerohive device mgt0 or WAN interface HiveManager MGT port	NTP server	6 TCP	1024-65535	123	Required for time synchronization with an NTP server
OpenVPN	HiveManager MGT or LAN port	HiveManager MGT or LAN port	17 UDP	1024-65535	1194	Required to secure communications between HA nodes
OSPF	HiveOS VA eth0 or eth1 interface and peer routers	HiveOS VA eth0 or eth1 interface and peer routers	89 OSPF	N.A.	N.A.	Allows the HiveOS VA to engage in dynamic routing; OSPF uses IPv4 multicast addresses 224.0.0.5 and 224.0.0.6
PostgreSQL	HiveManager MGT or LAN port	HiveManager MGT or LAN port	6 TCP	1024-65535	5432	Required to synchronize data between nodes in an HA pair and to save data from a standalone HiveManager to an external database
RIPv2	HiveOS VA eth0 or eth1 interface and peer routers	HiveOS VA eth0 or eth1 interface and peer routers	17 UDP	520	520	Allows the HiveOS Virtual Appliance to engage in dynamic routing
SMTP	HiveManager MGT port	SMTP server	6 TCP	1024-65535	25*	Required for the HiveManager to send email alerts to administrators

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
SSHv2	management system	Aerohive device mgt0, mgt0.x, or WAN interface HiveManager MGT port	6 TCP	1024 - 65535	22	Used for secure network access to the Aerohive device or HiveManager CLI, and (SCP) for uploading files to and downloading files from Aerohive devices To connect through the WAN interface, WAN hardening must first be disabled [†]
syslog	Aerohive device mgt0 or WAN interface	syslog server	17 UDP	1024 - 65535	514	Required for remote logging to a syslog server
Telnet	management system	Aerohive device mgt0, mgt0.x, or WAN interface or HiveManager MGT port	6 TCP, 17 UDP	1024 - 65535	23	Used for unsecured network access to the CLI on the Aerohive device To connect through the WAN interface, WAN hardening must first be disabled [†]
TFTP	Aerohive device mgt0 or WAN interface	TFTP server	17 UDP	1024 - 65535	69	Used for uploading files to Aerohive devices and downloading files from them

* This is the default port number. You can change it to a different port number from 1024 to 65535.

† To disable WAN hardening on a HiveOS Virtual Appliance or router through the HiveManager GUI, navigate to the Monitor > Devices > All Devices page, select the device, click **Utilities > Device WAN Access**, select **Permit management traffic to the WAN interface**, and then click **Submit**.

Index

A

- admin
 - bootstrap login credentials 100
 - login credentials, changing 82
 - lost credentials, one-time login key 77
- AeroScout Reports 111

B

- bootstrap config 75, 77-78, 99-101
 - defining 100
 - login credentials, changing (CLI) 100
 - saving to a TFTP server 101
 - uploading from a TFTP server 101

C

- CAPWAP 20
 - CAPWAP traffic 110
 - checking status 31
 - DHCP options 33
 - server connection process 32
 - states 29

CLI

- admin system requirements 79
- administrators, creating 73
- common commands 72
- default user profile 72
- disabling the reset button 77
- layer 2 and 3 forwarding 73
- logging 73
- QoS settings 74
- radio profiles 72
- resetting the configuration 77
- updating AP country codes 81
- uploading a configuration file 76
- user profiles 74
- clock synchronization 20
- configuration file types
 - backup 75, 76
 - bootstrap 75, 77-78, 99-101
 - bootstrap config, defining 100
 - current 75, 76
 - default 75, 77
 - failed 75, 76
- cooperative control 5
 - messages 111

- country codes
 - updating through HiveManager 45
 - updating through the CLI 81

D

- default login credentials
 - devices 81
 - HiveManager 11
- DHCP 107, 112
- DNS 108

E

- Ekahau 112
- entitlement key 9
- ESXi hypervisor 48
 - vSphere Client 48, 53

F

- firewall
 - policy rules, moving 17
 - router firewall 61

G

- GRE 108

H

- hive 36
 - backhaul communications 86
 - checking member connectivity 88
 - defined 71
 - deploying 83-89
 - member communications 83
 - neighbor states 30, 87
 - password 85
 - secured communications 36
- HiveManager
 - CLI shell 10
 - cloning configuration objects 18
 - complete configuration uploads 44
 - configuration workflow 20
 - connecting APs to HiveManager 28
 - console 9
 - default IP addresses 10
 - default login credentials 11
 - delta configuration uploads 44
 - device-level configuration objects 20, 21
 - entitlement key 9

- Ethernet ports 9-11
 - GUI 14-19
 - GUI requirements 9
 - installing 9
 - LAN port 9-11
 - license key 9, 12
 - logging in to the GUI 11
 - MGT port 9-11
 - multiselecting configuration objects 18
 - policy-level configuration objects 20, 21
 - recovering the IP address 11
 - relationship of configuration objects 20
 - sales order number 9
 - search tool 16
 - software updates 22
 - sorting data 19
 - synchronize clocks 20
 - troubleshooting AP connectivity issues 34
 - troubleshooting device connectivity issues 29
 - updating AP country codes 45
 - uploading AP configurations 43
 - HiveManager Online 6-8
 - redirector 8, 34
 - troubleshooting AP connectivity issues 34
 - troubleshooting device connectivity issues 29
 - HiveManager Virtual Appliance 6-9
 - HiveOS
 - backup config 75, 76
 - bootstrap config 75, 77-78, 99-101
 - bootstrap config, defining 100
 - bootstrap login credentials 100
 - changing login credentials 82
 - common CLI commands 72
 - configuration file types 75-78
 - current config 75, 76
 - default config 75, 77
 - default login credentials 81
 - default settings 72
 - device-level configurations 73
 - failed config 75, 76
 - firmware updates 23
 - policy-level configurations 74
 - HiveOS Virtual Appliance
 - activation code 59
 - installation 48-60
 - Layer 3 VPN gateway 52
 - HTTP 108
 - HTTPS 108, 110
 - hypervisor 48
 - vSphere Client 48, 53
-
- I**
 - IEEE 802.1X
 - SSID (CLI) 89-92
 - supplicants 91
 - interfaces, default states 100
-
- L**
 - license key 9, 12
 - login credentials
 - changing (CLI) 82
 - default (devices) 81
 - default (HiveManager) 11
 - one-time login key 77
-
- M**
 - mesh points 24, 28, 43, 99
 - modem 69
-
- N**
 - network policy 20
 - QuickStart-Wireless-Only 36
 - QuickStart-Wireless-Routing 60
 - NTP 20, 112
-
- O**
 - order number 9
 - OSPF 63
 - area 64
 - router ID 64
-
- P**
 - PoE 28
 - portals 24, 28, 43
 - PSK 37
-
- Q**
 - QoS
 - applying QoS (CLI) 92-99
 - classifier maps 95
 - classifier profiles 95
 - data traffic 93
 - streaming media 92
 - strict forwarding 93
 - voice traffic 92
 - WRR (weighted round robin) 93
-
- R**
 - radio profiles 72
 - radios
 - access 37, 80
 - backhaul 37, 80
 - broadcasting SSIDs 37

RADIUS authentication

- accounting traffic 109
- authentication traffic 109
- RADIUS authenticators 91
- returned RADIUS attributes 99
- server connectivity settings (CLI) 90
- supplicants 91

redirection server. See redirector

redirector 8, 34, 67

reset button, disabling 77, 99

reset config 77

routers

- auto provisioning 66-67
- configuration overview 47
- deployment 67
- installation 68
- manual preprovisioning 68

routing

- dynamic routing protocols 63
- internal networks 64
- OSPF 63
- RIPv2 63
- route advertisement 63

S

sales order number 9

SMTP 112

SNMP 111

SNMP traps 111

SSHv2 111, 113

SSID 37

- 802.1X 89-92
- 802.1X, testing 92
- binding to an interface 81
- client configuration (PSK) 89
- creating with a PSK 81
- QS-SSID 60
- SSID names 37
- SSID profiles 37
- testing 82

syslog 113

T

Telnet 113

TFTP 111, 113

traffic types 107-113

troubleshooting, AP-HiveManager connectivity 34

troubleshooting, device-HiveManager connectivity 29

U

updates

- activation 24, 44, 76
- HiveManager software 22
- HiveOS firmware 23
- portals and mesh points 24
- recommended sequence 23

user profiles 40

- default user profile 72

V

VLAN

- default VLAN 72
- mgt0 interface (CLI) 73
- native VLAN 72
- user profiles (CLI) 73

VMware

- creating a virtual network 53
- deploying an .ova template 55
- ESXi hypervisor 48
- promiscuous mode 51
- vSphere Client 53

VPN gateway 52

- initial configuration 57-60
- Layer 3 IPsec VPN 62
- route advertisement 63

W

WLAN deployment

- connecting APs to HiveManager 28
- single AP 80-83

