

Aerohive Deployment Guide



Aerohive Deployment Guide

For HiveAP and HiveManager Devices



Aerohive Technical Publications

Copyright Notice

Copyright © 2010 Aerohive Networks, Inc. All rights reserved.

Aerohive Networks, the Aerohive Networks logo, HiveOS, HiveAP, 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.
3150-C Coronado Drive
Santa Clara, CA 95054

P/N 330002-14, Rev. A

HiveAP Compliance Information

Federal Communication Commission Interference Statement

Aerohive products that show an FCC identifier on the product label (FCC ID: WBV-`<model_name>`) comply with part 15 of the FCC Rules when operating under the following restrictions: (1) they do not cause harmful interference, and (2) they must accept any RF interference received, including interference that might cause an unwanted impact on their operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

In compliance with FCC Part 15 regulations, the HiveAP automatically discontinues transmission if there is no valid information to transmit or if there is an operational failure.

Important: FCC Regulatory Warnings Notice

This equipment is restricted to indoor use due to its operation in 5 GHz frequencies, which are shared by mobile satellite systems and government radar systems. The FCC requires that this product only be used indoors to reduce the potential for harmful interference with co-channel radar that might be operating in the 5.25-5.35 or 5.47-5.725 GHz frequency ranges in the same area. The conflicting activity of radar stations and this device can cause interference or damage to each other. In addition, this device has a radar detection function that might interrupt normal operations when it detects a radar signal.

To reduce the risk of interference even further, installing this device away from windows is recommended.

Only attach antennas that are certified for use with this device. Replacing antennas with unauthorized, high-gain antennas greatly increases the risk of interference and invalidates the FCC certification.

Wireless 5 GHz Band Statements

To comply with FCC regulations when deploying a HiveAP outdoors in the FCC region, set the 5 GHz radio to use a channel from 149 to 161 (5.725 GHz to 5.825 GHz). When deploying it indoors, then the 5 GHz radio can also use channels 36 to 48 (5.180 GHz to 5.240 GHz). The maximum transmit power for channels from 36 to 48 is 15 dBm in the FCC region. Because this maximum is enforced by HiveOS, the HiveAP automatically limits the power to 15 dBm even if the setting is greater than that.

Because radar systems use some bands in the 5 GHz spectrum, WLAN devices operating in these bands must use DFS (Dynamic Frequency Selection) to detect radar activity and switch channels automatically to avoid interfering with radar operations. For the ETSI region, the HiveAP 300 series is certified for the latest ETSI EN 301 893 v1.5.1 DFS requirements and can use DFS channels 52 to 140 (5.26 GHz to 5.32 GHz, and 5.5 GHz to 5.7 GHz). To comply with ETSI regulations when deploying a HiveAP 300 series device outdoors, set the 5 GHz radio to operate on the DFS channels and enable DFS. When deploying it indoors, then the 5 GHz radio can also use channels 36 to 48 as well as the DFS channels. The maximum transmit power for channels from 36 to 48 is 17 dBm in the ETSI region. Because this maximum is enforced by HiveOS, the HiveAP automatically limits the power to 17 dBm even if the setting is greater than that.

Note: The term "IC" before the radio certification number signifies that Industry Canada technical specifications were met.

Industry Canada

Products that show an Industry Canada identifier on the product label (IC: 7774A-`<model_name>`) can be operated in Canada under the following restrictions:

- The device must not cause interference and must accept any interference, including that which might cause an unwanted impact on the operation of the device.
- To reduce potential radio interference to other users, the antenna type and its gain must be chosen so that the EIRP (equivalent isotropically radiated power) is not more than that permitted for successful communication.
- The use of the Unlicensed National Informational Infrastructure (UNII) band UNII-1 (5.15-5.25 GHz; channels 36-48) must be limited to indoor deployments to reduce the potential for harmful interference with co-channel mobile satellite systems.
- The maximum permitted antenna gain for operation in the UNII-2 band (5.25-5.35 GHz; channels 52-64) and UNII-2 Extended band (5.47-5.725 GHz; channels 100-116, 132-140) must comply with the EIRP limit.
- The maximum permitted antenna gain for operation in the UNII-3 band (5.725-5.825 GHz; channels 149-165) must comply with EIRP limits specified for point-to-point and non point-to-point operation as stated in the Industry Canada Radio Standards Specification RSS-210, section A9.2(3).
- High-power radar systems are allocated as primary users for the 5.25-5.35 GHz bands (channels 52-64) and 5.65-5.85 GHz bands (channels 132-165) with priority to use them. These systems can cause interference to and possibly damage HiveAP devices.

Class B

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of Industry Canada.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par l'Industrie.

Important: Radiation Exposure Statement

This equipment complies with radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters (8 inches) between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. For more information about RF exposure limits, visit (Canada) www.ic.gc.ca and (US) www.fcc.gov

Wi-Fi Certification



The Wi-Fi CERTIFIED™ Logo is a certification mark of the Wi-Fi Alliance®. The HiveAP 20, 100, 300 series have been certified for WPA™, WPA2™, WMM® (Wi-Fi Multimedia™), WMM Power Save, IEEE 802.11d, IEEE 802.11h, and the following types of EAP (Extensible Authentication Protocol):

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM
- EAP-AKA
- EAP-FAST

The HiveAP 100 and 300 series have also been certified for short guard interval and 40-MHz operation in the 5-GHz band.

EC Conformance Declaration $\text{CE0560} \text{D}$ $\text{CE0700} \text{D}$

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

- EN 60950-1 (IEC 60950-1) - Product Safety
- EN 301 893 - Technical requirements for 5 GHz radio equipment
- EN 300 328 - Technical requirements for 2.4 GHz radio equipment
- EN 301 489-1 / EN 301 489-17 - EMC requirements for radio equipment

Declarations of conformity, compliance statements, and other regulatory documentation are available at www.aerohive.com/support.

WEEE and RoHS Compliance



Aerohive Networks products have been reviewed, analyzed and found to be in compliance with the European Union (EU) directive for Waste Electrical and Electronic Equipment (WEEE) and with the EU directive for the Restriction of Hazardous Substances (RoHS).

WEEE Collection Programs in the U.S. and EU

At end of life, customers are requested to contact Aerohive to make arrangements for WEEE collection of their products. The Aerohive collection center in the U.S. is at the following address:

Aerohive Inc.
650 Kaiser Drive
Fremont, CA 94555
Telephone: 510-608-7790
Contact: Technical Support, weee@aerohive.com

Aerohive, in association with M-Cubed LLC, also has a collection center at the following address in Germany, a member state of the European Union:

EXTRABYTE - M Cubed LLC
Klopstock Strasse #8
33613 BIELEFELD
Telephone: 49-521-882245
Contact: Mr. Andreas Budde

Countries of Operation and Conditions of Use in the European Community

HiveAPs are intended to be operated in all countries of the European Community. Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below.

- Before operating a HiveAP, the admin or installer must properly enter the current country code as described in Aerohive product documentation.
Note to U.S. model owners: To comply with U.S. FCC regulations, the country selection function has been completely removed from all U.S. models. The above function is for non-U.S. models only.

- HiveAPs automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation might result in illegal operation and cause harmful interference to other systems. The admin is obligated to ensure HiveAPs are operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this section.
- HiveAPs can be operated indoors or outdoors in all countries of the European Community using the 2.4 GHz band: Channels 1-13, except where noted below:
 - In Italy and Luxembourg, you must apply for a license from the national spectrum authority to operate a HiveAP outside your own premises and for public use or service.
 - In Belgium outdoor operation is only permitted using the 2.46 to 2.4835 GHz band: Channel 13.
 - In France outdoor operation is limited to the 2.454 to 2.4835 GHz band (channels 8 to 13) at a maximum of 10 mW EIRP (effective isotropic radiated power).
 - In Norway, the 2.4 GHz band cannot be used outdoors within a 20-km radius of the center of Ny-Ålesund.
 - In Russia, the 2.4 GHz band is for indoor use only.
- HiveAPs using the 5.15 to 5.35 GHz band (Channels 36 to 64) are restricted to indoor use when operated in the European Community. Because the frequency ranges 5.25 to 5.35 and 5.47 to 5.725 are affected by DFS (Dynamic Frequency Selection), HiveAP 20 and 28 models block channels 52 to 64 and 100 to 140.
- The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at installation to match the intended destination. The firmware setting is accessible by the end user. Some national restrictions are noted below:
 - In Italy and Luxembourg, you must apply for a license from the national spectrum authority to operate a HiveAP outside your own premises and for public use or service in the 5.15 to 5.35 GHz band (channels 36 to 64) and 5.47 to 5.725 GHz band (channels 100 to 140).
 - In Russia, you can only use the 5.15 to 5.35 GHz band at 100 mW (20 dBm) indoors, in closed industrial and warehouse areas, and on board aircraft for local network and crew communications during all stages of a flight and for public WLAN access only at an altitude of 3000 meters or higher. You can only use the 5.65 to 5.825 GHz band with 100 mW EIRP on board aircraft at an altitude of 3000 meters or higher.
- The 5 GHz Turbo Mode feature is not allowed for operation in any European Community country. You can find the current setting for this feature in two places. In the HiveManager GUI, click **Configuration > Advanced Configuration > Network Objects > Radio Profiles**. In the HiveAP CLI, enter this command: `show radio profile profile`. By default, Turbo Mode is disabled.

Declaration of Conformity in Languages of the European Community

English	Hereby, Aerohive, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	Valmistaja Aerohive vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Dutch	Hierbij verklaart Aerohive dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. Bij deze Aerohive dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.

HiveAP Compliance Information

French	Par la présente Aerohive déclare que cet appareil Radio LAN est conforme aux exigences essentielles et aux autres dispositions relatives à la directive 1999/5/CE.
Swedish	Härmed intygar Aerohive att denna Radio LAN device står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish	Undertegnede Aerohive erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
German	Hiermit erklärt Aerohive, dass sich dieser/diese/dieses Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMW) Hiermit erklärt Aerohive die Übereinstimmung des Gerätes Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek	με την παρούσα Aerohive δηλώνει ότι radio LAN device συμμορφώνεται προς τις ουσιαστικές απαιτήσεις και τις λυπτες σΧετικες διαταξεις της οδηγιας 1999/5/εκ
Italian	Con la presente Aerohive dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Spanish	Por medio de la presente Aerohive declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Portuguese	Aerohive declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

HiveAP 20 ag Safety Compliance

Power Cord Safety

Please read the following safety information carefully before installing a HiveAP.

Warning: Installation and removal of HiveAPs must be carried out by qualified personnel only.

- HiveAPs must be connected to an earthed (grounded) outlet to comply with international safety standards.
- Do not connect HiveAPs to an A.C. outlet (power supply) without an earth (ground) connection.
- The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN 60320/IEC 320 appliance inlet.
- The socket outlet must be near the HiveAP and easily accessible. You can only remove power from a HiveAP by disconnecting the power cord from the outlet.
- HiveAPs operate under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which they are connected also operates under SELV conditions.
- A HiveAP receiving power through its PoE (Power over Ethernet) interface must be in the same building as the equipment from which it receives power.

France and Peru only:

HiveAPs cannot be powered from IT* supplies. If your supplies are of IT type, then a HiveAP must be powered by 230 V (2P+T) via an isolation transformer ratio 1:1, with the secondary connection point labelled Neutral, connected directly to earth (ground). *Impédance à la terre

Important! Before making connections, make sure you have the correct cord set. Check it (read the label on the cable) against the description on the following page.

Power Cord Set	
U.S.A. and Canada	The cord set must be UL-approved and CSA certified.
	Minimum specifications for the flexible cord: - No. 18 AWG not longer than 2 meters, or 16 AWG - Type SV or SJ - 3-conductor
Denmark	The cord set must have a rated current capacity of at least 10 A.
	The attachment plug must be an earth-grounding type with NEMA 5-15P (15 A, 125 V) or NEMA 6-15 (15 A, 250 V) configuration.
Switzerland	The supply plug must comply with Section 107-2-D1, Standard DK2-1a or DK2-5a.
U.K.	The supply plug must comply with BS1363 (3-pin 13 A) and be fitted with a 5 A fuse that complies with BS1362.
Europe	The mains cord must be <HAR> or <BASEC> marked and be of type HO3VVF3GO.75 (minimum).
	The supply plug must comply with CEE7/7 ("SCHUKO"). The mains cord must be <HAR> or <BASEC> marked and be of type HO3VVF3GO.75 (minimum). IEC-320 receptacle.

Veuillez lire attentivement les informations de sécurité relatives à l'installation d'un point d'accès HiveAP.

Avvertimento: L'installazione e la deposizione di punti d'accesso HiveAP devono essere effettuate unicamente da personale qualificato.

- Les points d'accès HiveAP doivent être connectés sur le secteur par une prise électrique munie de terre (masse) afin de respecter les standards internationaux de sécurité.
- Ne jamais connecter des points d'accès HiveAP à une alimentation électrique non-pourvue de terre (masse).
- Le boîtier d'alimentation (connecté directement au point d'accès) doit être compatible avec une entrée électrique de type EN 60320/IEC 320.
- La prise secteur doit se trouver à proximité du point d'accès HiveAP et facilement accessible. Vous ne pouvez mettre hors tension un point d'accès HiveAP qu'en débranchant son alimentation électrique au niveau de cette prise.
- Pour des raisons de sécurité, le point d'accès HiveAP fonctionne à une tension extrêmement basse, conformément à la norme IEC 60950. Les conditions de sécurité sont valables uniquement si l'équipement auquel le point d'accès HiveAP est raccordé fonctionne également selon cette norme.
- Un point d'accès HiveAP alimenté par son interface réseau Ethernet en mode POE (Power over Ethernet) doit être physiquement dans le même bâtiment que l'équipement réseau qui lui fournit l'électricité.

France et Pérou uniquement:

Un point d'accès HiveAP ne peut pas être alimenté par un dispositif à impédance à la terre. Si vos alimentations sont du type impédance à la terre, alors le point d'accès HiveAP doit être alimenté par une tension de 230 V (2P+T) via un transformateur d'isolement à rapport 1:1, avec le neutre connecté directement à la terre (masse).

Cordon électrique - Il doit être agréé dans le pays d'utilisation	
Etats-Unis et Canada	Le cordon doit avoir reçu l'homologation des UL et un certificat de la CSA.
	Les spécifications minimales pour un câble flexible - AWG No. 18, ou AWG No. 16 pour un câble de longueur inférieure à 2 mètres. - Type SV ou SJ - 3 conducteurs
	Le cordon doit être en mesure d'acheminer un courant nominal d'au moins 10 A.
	La prise femelle de branchement doit être du type à mise à la terre (mise à la masse) et respecter la configuration NEMA 5-15P (15 A, 125 V) ou NEMA 6-15P (15 A, 250 V).
Danemark	La prise mâle d'alimentation doit respecter la section 107-2 D1 de la norme DK2 1a ou DK2 5a.
Suisse	La prise mâle d'alimentation doit respecter la norme SEV/ASE 1011.
Europe	La prise secteur doit être conforme aux normes CEE 7/7 ("SCHUKO"). LE cordon secteur doit porter la mention <HAR> ou <BASEC> et doit être de type HO3VVF3GO.75 (minimum).

Bitte unbedingt vor dem Einbauen des HiveAP die folgenden Sicherheitsanweisungen durchlesen.

Warnung: Die Installation und der Ausbau des Geräts darf nur durch Fachpersonal erfolgen.

- Das Gerät sollte nicht an eine ungeerdete Wechselstromsteckdose angeschlossen werden.
- Das Gerät muß an eine geerdete Steckdose angeschlossen werden, welche die internationalen Sicherheitsnormen erfüllt.
- Der Gerätestecker (der Anschluß an das Gerät, nicht der Wandsteckdosenstecker) muß einen gemäß EN 60320/IEC 320 konfigurierten Geräteeingang haben.
- Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkaabels aus der Netzsteckdose unterbrochen werden.

- Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 60950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.

Stromkabel. Dies muss von dem Land, in dem es benutzt wird geprüft werden:

U.S.A. und Kanada	Der Cord muß das UL geprüft und war das CSA beglaubigt.
Kanada	Das Minimum spezifikation für der Cord sind: - Nu. 18 AWG - nicht mehr als 2 meter, oder 16 AWG. - Der typ SV oder SJ - 3-Leiter Der Cord muß haben eine strombelastbarkeit aus wenigstens 10 A. Dieser Stromstecker muß hat einer erdschluss mit der typ NEMA 5-15P (15A, 125V) oder NEMA 6-15P (15A, 250V) konfiguration.
Danemark	Dieser Stromstecker muß die ebene 107-2-D1, der standard DK2-1a oder DK2-5a Bestimmungen einhalten.
Schweiz	Dieser Stromstecker muß die SEV/ASE 1011 Bestimmungen einhalten.
Europe	Europe Das Netzkabel muß vom Typ HO3VVF3GO.75 (Mindestanforderung) sein und die Aufschrift <HAR> oder <BASEC> tragen. Der Netzstecker muß die Norm CEE 7/7 erfüllen ("SCHUKO").

Liability Disclaimer

Installation of Aerohive equipment must comply with local and national electrical codes and with other regulations governing this type of installation. Aerohive Networks, its channel partners, resellers, and distributors assume no liability for personal injury, property damage, or violation of government regulations that might arise from failing to comply with the instructions provided and appropriate electrical codes.

Contents

Chapter 1 Preparing for a WLAN Deployment	13
Assessing Your Requirements	14
Planning	14
Upgrading from Existing Wi-Fi.....	14
New WLAN Deployment	15
Site Surveys	16
Budgeting Wi-Fi: The Chicken and Egg Problem.....	17
Planning Tools.....	17
Associated Access Point Costs	18
Bandwidth Assumptions for Wi-Fi.....	18
Overcoming Physical Impediments	19
Preparing the Wired Network for Wireless.....	21
Operational Considerations	22
Tuning.....	22
Troubleshooting	22
Management	22
Deploying with Confidence	22
Basic Wi-Fi Concepts	23
Chapter 2 The HiveAP 20 ag Platform.....	27
HiveAP 20 Product Overview.....	28
Ethernet and Console Ports.....	30
Status LEDs	31
Antennas.....	32
Mounting the HiveAP 20	33
Ceiling Mount	33
Surface Mount	34
Device, Power, and Environmental Specifications	35
Chapter 3 The HiveAP 28 Outdoor Platform	37
HiveAP 28 Product Overview.....	38
Ethernet Port	39
Power Connector	40
Antennas.....	41

Mounting the HiveAP 28 and Attaching Antennas.....	42
Pole Mount	43
Strand Mount	44
Surface Mount	45
Attaching Antennas	46
Connecting Antennas Directly to the HiveAP 28	46
Mounting Antennas Separately	46
Device, Power, and Environmental Specifications	48
Chapter 4 The HiveAP 340 Platform.....	49
HiveAP 340 Product Overview	50
Ethernet and Console Ports.....	52
Smart PoE	53
Aggregate and Redundant Interfaces	53
Console Port	55
Status LEDs	56
Antennas.....	56
MIMO	57
Using MIMO with Legacy Clients	59
Mounting the HiveAP 340	60
Ceiling Mount	61
Locking the HiveAP 340.....	62
Plenum Mount.....	63
Suspended Mount	66
Surface Mount	68
Device, Power, and Environmental Specifications	69
Chapter 5 The HiveAP 320 Platform.....	71
HiveAP 320 Product Overview	72
Ethernet and Console Ports.....	74
Status LEDs	74
Antennas.....	75
Mounting the HiveAP 320	76
Ceiling Mount	76
Locking the HiveAP 320.....	77
Surface Mount	78
Device, Power, and Environmental Specifications	79

Chapter 6 HiveAP 100 Series Platforms	81
HiveAP 110 and 120 Product Overview	82
Ethernet Port	83
Status Indicator.....	84
Antennas.....	84
Mounting a HiveAP 100 Series Device.....	85
Ceiling Mount	85
Locking the HiveAP	87
Surface Mount	87
Device, Power, and Environmental Specifications	88
Chapter 7 The HiveManager Platform	89
Product Overview.....	90
Ethernet and Console Ports.....	91
Status LEDs	92
Rack Mounting the HiveManager	93
Device, Power, and Environmental Specifications	94
Chapter 8 The High Capacity HiveManager Platform	95
Product Overview.....	96
Rack Mounting the High Capacity HiveManager	98
Replacing Power Supplies	101
Replacing Hard Disk Drives	102
Device, Power, and Environmental Specifications	103
Chapter 9 HiveManager Online and HiveManager Virtual Appliance	105
HiveManager Online	105
HiveManager Virtual Appliance	106

Chapter 10 Using HiveManager	107
Installing and Connecting to the HiveManager GUI	109
Introduction to the HiveManager GUI.....	113
Viewing Reports	114
Searching	115
Multiselecting.....	116
Cloning Configurations	116
Sorting Displayed Data	117
HiveManager Configuration Workflow (Enterprise Mode).....	118
Updating Software on HiveManager	119
Updating HiveOS Firmware.....	120
Updating HiveAPs in a Mesh Environment	121
Chapter 11 Basic Configuration Examples	123
Example 1: Defining an SSID	124
Example 2: Creating a Hive	127
Example 3: Creating a WLAN Policy	128
Example 4: Connecting HiveAPs to HiveManager	129
Example 5: Assigning the Configuration to HiveAPs.....	135
Chapter 12 Common Configuration Examples	139
Example 1: Mapping Locations and Installing HiveAPs	140
Setting Up Topology Maps.....	140
Preparing the HiveAPs.....	144
Using MAC Addresses	144
Using SNMP	144
Example 2: IEEE 802.1X with an External RADIUS Server.....	145
Example 3: Providing Guest Access through a Captive Web Portal	151
Registration Types	151
Providing Network Settings.....	152
Captive Web Portal with External DHCP and DNS Servers.....	152
Captive Web Portal with Internal DHCP and DNS Servers	154
Modifying Captive Web Portal Pages	155
Configuring a Captive Web Portal	158
Example 4: Private PSKs.....	165
Example 5: Using HiveAP Classifiers	170

Chapter 13 HiveOS	173
Common Default Settings and Commands	174
Configuration Overview.....	175
Device-Level Configurations.....	175
Policy-Level Configurations.....	176
HiveOS Configuration File Types	177
Chapter 14 Deployment Examples (CLI)	181
Example 1: Deploying a Single HiveAP	182
Example 2: Deploying a Hive.....	185
Example 3: Using IEEE 802.1X Authentication.....	190
Example 4: Applying QoS	194
Example 5: Loading a Bootstrap Configuration	200
CLI Commands for Examples	203
Commands for Example 1	203
Commands for Example 2	203
Commands for Example 3	204
Commands for Example 4	205
Commands for Example 5	207
Chapter 15 Traffic Types	209
Appendix A Country Codes	213
Index	217

Chapter 1 Preparing for a WLAN Deployment

To ensure a smooth WLAN deployment, you need to begin with a bit of planning. A straightforward review of your deployment plan before you begin will result in optimal results more quickly. The goals of this chapter are to assist you in assessing your readiness for WLAN implementation and to provide tips and tricks to resolve any issues that might arise in your environment. The chapter covers the following topics:

- ["Assessing Your Requirements" on page 14](#)
- ["Planning" on page 14](#)
 - ["Upgrading from Existing Wi-Fi" on page 14](#)
 - ["New WLAN Deployment" on page 15](#)
 - ["Site Surveys" on page 16](#)
 - ["Budgeting Wi-Fi: The Chicken and Egg Problem" on page 17](#)
 - ["Bandwidth Assumptions for Wi-Fi" on page 18](#)
 - ["Overcoming Physical Impediments" on page 19](#)
- ["Operational Considerations" on page 22](#)
 - ["Preparing the Wired Network for Wireless" on page 21](#)
 - ["Deploying with Confidence" on page 22](#)

Although this guide assumes an understanding of corporate data networking, previous experience with LAN configuration and deployment, and some basic Wi-Fi understanding, the chapter concludes with a section that provides additional support for the preceding sections: ["Basic Wi-Fi Concepts" on page 23](#).

Note: This guide assumes an understanding of corporate data networking and past experience with LAN configuration and deployment. It also assumes some basic Wi-Fi understanding.

ASSESSING YOUR REQUIREMENTS

To get started with your Aerohive WLAN installation, examine the basic requirements of your implementation. First, consider who your stakeholders are and take the time to fully understand their access requirements. Talk to department managers within your organization and make sure everyone has documented the full complement of potential users of your network. Check if the applications are standard employee applications or if there are other requirements, such as access for guests or consultants.

Next, make a complete list of the application types that your Aerohive network will need to support. Begin your list with mission-critical applications, paying special attention to those that generate high levels of traffic and those requiring deterministic behavior. Identify applications with heavy data requirements and expected service levels.

Demanding applications such as voice and video will require a higher density of access points. Many enterprises are investigating the potential of VoWLAN (Voice over WLAN) in the hopes of integrating mobile phones and IP-PBX systems. Doing so requires an evaluation of other data transmission types that can disrupt the quality of voice conversations. Because voice traffic is sensitive to network jitter and latency, an inadequate number of access points can degrade quality. To the user, excessive jitter and delay can cause clipped conversations or dropped calls. Additional quality and reliability issues might arise when transmitting video, such as for training video or surveillance operations, because of the sheer size of the data stream.

Other applications such as network backup and file transfers can also have an impact on the network. Therefore, take into account any bandwidth-intensive applications if you expect your mobile workforce to be accessing the WLAN while these applications or services are occurring.

Considering the above issues will result in a more informed—and therefore more successful—deployment plan.

PLANNING

This section reviews the fundamental elements for planning your WLAN deployment. This includes conducting a site survey, both for an upgrade from an existing WLAN and for a completely fresh—or greenfield—deployment.

Upgrading from Existing Wi-Fi

If you are upgrading to Aerohive from an existing WLAN, you already have plenty of data about how your current network is performing. This information can lead to more informed decisions about your new implementation.

To begin, perform a quick site survey with the existing access points in place. If they are less than three years old and support 802.11g, their coverage and capacity will be lower than the Aerohive 802.11n radio. If the coverage is good and has the appropriate density for your deployment, the simplest approach is to replace one set of access points with a new set of HiveAPs. However, this scenario is rare because network upgrades are usually done to improve capacity and to augment the existing layout with a denser deployment of access points.

Be sure to take note whether your existing network uses "fat" or "thin" APs (access points). A "fat" AP is an autonomous or standalone access point, which contains the capability to connect to any Ethernet switch. With a "thin" AP, most of the intelligence has been removed and replaced in a centralized WAN controller. An upgrade from fat APs to Aerohive HiveAPs is very natural. Generally, with fat APs you simply need to unplug the existing ones and plug in the new HiveAPs and provision them. With this approach, you can maintain or enhance all existing VLANs and security policies. This is a huge advantage over migrating from fat AP to controller-based solutions because you typically need to re-architect the network.

Upgrading from a thin AP solution is also easy. However, because a thin AP makes use of an overlay tunneled network, you sometimes have to add a local VLAN for access or use tunnels to replicate the overlay network. However, because using VLANs rather than tunnels provides significant performance and scalability advantages, which is clearly the recommended path.

New WLAN Deployment

In a new—or greenfield—WLAN deployment, you do not have the benefit of an existing network for testing and analysis, which makes your job a bit more difficult. In this case, the following key questions are critical to the proper design of your WLAN:

- How many users will need wireless service and what applications will they use?

Determining the scope of your WLAN deployment will have a major impact on capacity and coverage. Will only certain groups within the organization have WLAN access, or will it be rolled out across the enterprise? Will you provide guest access to visitors, consultants, and contractors? Most WLANs support just data applications, but many organizations are considering adding voice services. Voice support raises other design considerations that drive the need for denser deployments of access points and different QoS (Quality of Service) settings.

- Are there any known major sources of interference?

For example, is there a nearby cafeteria with microwave ovens? Commercial-grade microwaves are a particularly bad source of interference. Is there a wireless telephone or video surveillance system not using Wi-Fi? Is there a radar installation nearby? If you cannot find the answer to these questions easily, consider employing a spectrum analysis product, such as the AirMagnet Spectrum Analyzer.

- Are building blueprints available?

With blueprints, you can see the location of elevators, load-bearing walls, and other building characteristics that can impact signal quality. Different materials, such as concrete walls, brick walls, cubicle walls, glass, and elevator shafts impact signal quality differently. You can often load these blueprints into a planning or site survey tool to make the process easier.

- What devices need to access the WLAN?

Determine and document the full complement of devices that people will use to access the WLAN. The performance requirements of the WLAN will depend on both the applications and the capabilities of the client devices. For example, design engineers, architects, and doctors tend to work with bandwidth-hungry applications, so you might need to provide greater capacity. Conversely, if it is a warehouse with a low client density of mostly barcode scanners, a lower access point density might be suitable. Finally it is important to consider voice, or the future use of voice. If some or all people will use VoWLAN (Voice over WLAN) devices, that can affect how many users each access point can accommodate.

Note: For some access point deployment guidelines, see "Bandwidth Assumptions for Wi-Fi" on page 18.

Site Surveys

One of the first questions IT managers ask when they are preparing for a WLAN deployment is whether or not a site survey should be performed. In a site survey, the administrator walks around the facility with a site survey tool to measure the RF (radio frequency) coverage of a test access point or the existing WLAN infrastructure.

Whether or not you decide to do a site survey for your enterprise depends on the cost of the survey and the complexity of the environment. The three ways to deploy a wireless network—with and without a site survey—are explained below:

- **Predeployment Survey**

The safest approach is to perform a site survey before deployment to determine the best locations for the access points. Typically, site survey professionals temporarily place access points in different locations, take measurements, and adjust their settings and locations as necessary. After they complete the survey, they install the access points, and then perform another site survey to confirm that the goals have been achieved. This method is clearly the most reliable way to deploy a wireless network; however, it can be expensive, time consuming, and impractical if an enterprise has many sites.

- **Deploy and Check**

In this scenario, an initial site survey is not performed. Instead, wireless administrators make educated guesses on the best locations for the access points or they use a planning tool to determine the locations more reliably. After deploying the access points, the administrators do a quick site survey. If they need to provide greater coverage, they deploy additional access points. If there are areas where access points are interfering with each other, they then relocate one or more of them. With the Aerohive cooperative RF control, HiveAPs automatically adjust their channel and power to compensate for coverage gaps and areas of interference.

The deploy-and-check approach is often much cheaper and faster than doing a predeployment site survey. The risk is that you might have to move some access points and CAT5 (Category 5) Ethernet cables if you do not plan properly. Aerohive provides a huge competitive advantage in the deploy-and-check approach, thanks to its flexible mesh networking capability. An administrator can deploy with mesh (before running wires) and check the performance in several layouts, determine the best layout, and then run the wires to their final location.

- **Deploy without Survey**

While it is usually advisable to do a site survey, there are many situations in which it is not feasible or even necessary. If the location is sufficiently small—for example, a deployment of only three or fewer access points—site surveys have limited value because there is virtually no opportunity for interference. If there are numerous remote locations, a site survey might be impractical because of the cost of traveling to each site. In these locations, you can use a slightly denser deployment to ensure appropriate coverage and capacity. With Aerohive Cooperative RF control, HiveAPs automatically adjust their radio power levels to ensure that there is minimal overlap from interfering channels. Usually the cost of extra access points is offset by the cost saved by not doing a site survey in a remote location.

Budgeting Wi-Fi: The Chicken and Egg Problem

The hardware cost of a Wi-Fi solution is generally driven by the number of access points needed, and an Aerohive network is no exception. Unfortunately, a traditional challenge of budgeting for Wi-Fi is that it is difficult to know how many access points to plan for until you have deployed and measured them. There are methods of doing site surveys before a deployment to answer these questions. While doing so is often worthwhile, you might just need a general idea of what you would need to budget. Fortunately there are some simple guidelines that you can use to figure out how many access points you need, including the number of access points per square foot, the number of clients per access point, and the distance between access points.

- **Access Points per Square Foot**

The simplest and most common way of budgeting access points is per square foot. You simply take the square footage of a building and divide it by some number. The most common metric used today is one access point for every 4,000 to 5,000 square feet for standard offices with cubicles. However, if you need to support voice applications, you need a higher concentration of access points. In this case, the recommended formula is one access point for every 3,000 square feet, or even as low as one access point for every 2,000 square feet. In the lightest weight convenience networks, it is possible to use fewer access points, and densities as low as one access point for every 10,000 to 15,000 square feet can be successful. Keep in mind that such a deployment often has dead spots and can only support very low client densities.

- **Number of Clients for Each Access Point**

Another way to determine the number of access points needed is to consider the number of clients you want each access point to support. In a standard office environment, most enterprises plan to support an average of 5 to 15 clients per access point. While the specifications of most access points state that they can support up to about 120 clients, a significantly lower density is recommended to get an acceptable throughput for standard office applications. If you expect to support voice over Wi-Fi in the enterprise, account for those phones as well. With the addition of voice, the client density substantially increases, requiring you to plan for an average of 5 to 10 data clients and 5 to 10 voice clients for each access point. Remember that voice clients consume virtually zero bandwidth when they are not on a call. However, when they are on a call, it is imperative that the traffic goes through.

- **Distance Between Access Points**

In a standard office environment, it is a good idea to ensure that access points are between 30 and 100 feet from one another. A distance of 30 feet is needed in high-density environments and those with many walls separating access points. A distance of 100 feet is sufficient in low-density areas with plenty of open space.

The three tips above can help determine how many access points to deploy in a given area. In general, the square footage estimate provides the best budgeting estimate, with client estimations and the distance between access points confirming the square footage calculations.

As with all rules, there are exceptions. If certain locations in the network have a higher density of clients, such as conference rooms or lecture halls, a higher density of access points is required. Conversely if there are large open areas with few active clients, fewer access points are sufficient.

Planning Tools

If following general guidelines does not provide enough confidence or if the deployment environment is particularly challenging, you might consider using software planning tools like AirMagnet's Planner or Ekahau's Site Survey (ESS). Aerohive also includes a free planning tool with its HiveManager platform and online at www.aerohive.com. Such tools are useful in determining the placement of access points without performing a site survey.

Associated Access Point Costs

After you determine how many access points you need, it becomes simpler to determine the other costs involved with deploying Wi-Fi because most are driven by the quantity of access points. These costs include the following:

- **Installation and Wiring**
 - CAT5 - CAT5 wiring is required for all HiveAPs acting as portals.¹ One advantage of Aerohive Networks is that you can deploy HiveAPs in a mesh to avoid some of the wiring costs.
 - Power - Power lines are required for all HiveAPs acting as mesh points.² Portals receive power through power lines or through Ethernet cables by using the Power-over-Ethernet (PoE) option.
 - Installation - HiveAPs can simply snap into standard dropped-ceiling environments. However, if the installation is in a warehouse or any environment without dropped ceilings, consider the installation costs.
- **Infrastructure: PoE Switches**

You must cable every HiveAP acting as a portal to a switch port. For PoE, there are several considerations:

 - 802.3af - The current PoE specification provides enough power for all 802.11a/b/g access points.
 - 802.3at - The emerging PoE specification supports higher power devices like 802.11n access points. This standard is expected to be ratified at the end of 2008, so products are not yet available.
 - PoE injectors and midspans - These save money on switch upgrades by injecting power into standard Ethernet connections.
- **Site Survey and Debugging Software**
 - For a sizable deployment, you probably will use site survey and debugging software. Deployment and troubleshooting tools from Ekahau and AirMagnet pay for themselves very quickly. These products enable the validation of a deployment and allow you to troubleshoot client and access point issues. (For more information, see the section on "[Operational Considerations](#)" on page 22.)
- **Professional Services**
 - When deploying wireless LANs, professional services are often required perform site surveys.
- **Client Software**
 - Depending on the deployment, users can use built-in Microsoft Windows, Linux and/or Macintosh client software (suplicants).
 - For better services and troubleshooting, consider a third-party supplicant such as Juniper Networks Odyssey Client.

Bandwidth Assumptions for Wi-Fi

People frequently talk about how much coverage an access point provides; however, it is capacity—not coverage—that typically constrains an access point in an enterprise environment. The challenge is not how far the RF signal can travel (coverage), but how to deliver enough bandwidth to meet the demands of business applications (capacity). In other words, you might be able to cover an office of 50 people with one access point, but if all 50 people choose to access it at the same time, it might become overloaded. Indeed, if you use the formulas provided in this paper, you should find the saturation of access points on your campus to be more than sufficient. Enterprise users are accustomed to speedy switched networks and expect similar performance from their wireless LAN connections. This is why documenting the size and type of applications that will rely on your WLAN is so critical to your planning. In short, if you plan for optimal capacity, complete coverage will follow automatically.

1. A portal is a hive member that links one or more mesh points to the wired LAN.

2. Mesh points are hive members that use a wireless backhaul connection to link through a portal to the wired LAN.

In general, the way to increase capacity is to add more access points (within reason) and tune down the radio power to avoid interference. One reason for deploying a high capacity network is to create a WLAN for voice and data applications. In such a WLAN, everyone has a VoIP handset running wirelessly all the time.

In general, the following table shows the standard densities for office deployments.

Office Requirements	Expected Data Rate with 802.11g Clients	Expected Data Rate with 802.11n Clients		Access Point Density
		20 MHz	40 MHz	
Coverage (low capacity)	12 Mbps to 24 Mbps	~39 Mbps	~81 Mbps	1 access point per 8000 square feet
Standard office deployment	36 Mbps	~104 Mbps	~216 Mbps	1 access point per 5000 square feet
Standard office deployment with voice	54 Mbps	~130 - 144 Mbps	~270 - 300 Mbps	1 access point per 2000 - 3000 square feet

Note: Data rate is not the same as TCP throughput. Because of various headers, inter-frame gaps, and session creation, real TCP throughput usually does not exceed 22 Mbps at data rates of 54 Mbps.

Overcoming Physical Impediments

Not every potential deployment is a standard business campus. The following scenarios are a few that merit special consideration.

- **Open Space**

Open spaces, such as a large foyer or an outdoor area, are very easy to cover with Wi-Fi because there are few impediments to propagation and fewer opportunities for multipath interference. In such spaces, Wi-Fi signals can propagate many hundreds of feet. This is good if you want to provide coverage for just a few users.

You will run into challenges if there are many users and high capacity service goals. In these situations, it is important to tune down the RF to a minimal level. If you are using Aerohive cooperative RF control, the HiveAPs do this on their own automatically. Another trick is to take advantage of obstacles that block Wi-Fi. Look for trees or walls and put neighboring access points on either side of them. Doing so limits the interference of the two access points and allows for the installation of more access points with less interference.

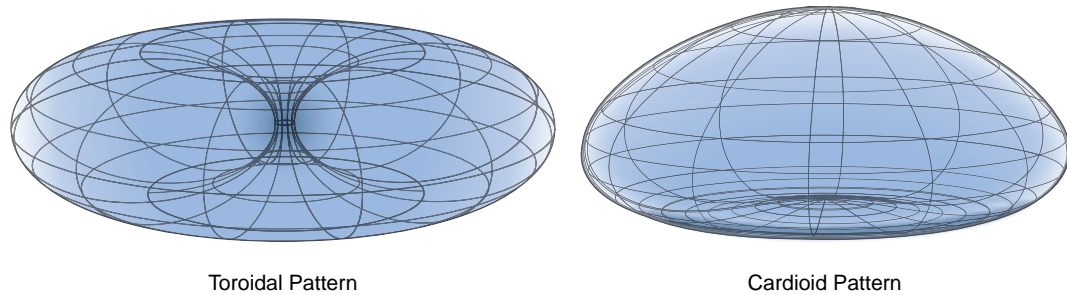
- **Warehouse and Retail**

Warehouse and retail environments present many challenges. One of the largest challenges is that RF characteristics often change because of varying inventory levels and, in the case of retail, seasonal displays (such as tinsel or a stack of soda cans on an end cap). Additionally, metal shelves and high ceilings can be challenges to propagation. To resolve with these issues, it is wise to put at least one access point per aisle to ensure coverage for that aisle. This usually requires a higher density of access points than would otherwise be required.

- **Configuring Antennas**

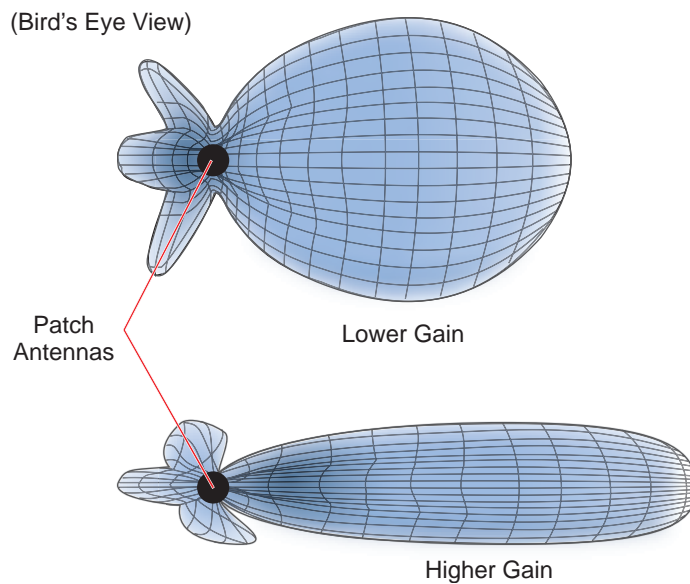
As anyone who has administered a WLAN system in the past knows, proper configuration of the access point antennas at the outset can save you lots of trouble. The HiveAP 100 series and HiveAP 320 have internal antennas that cannot be adjusted. However, the antennas for both the HiveAP 20 and HiveAP 340 are adjustable. The HiveAP 20 has a pair of fixed, dual-band omnidirectional antennas; and the HiveAP 340 can support up to six single-band omnidirectional antennas (three for the 2.4 GHz radio and three for the 5 GHz radio). You typically orient these antennas vertically, positioning the antennas on all HiveAPs in the same direction. Omnidirectional antennas create a coverage areas that can be toroidal (doughnut-shaped) or cardioid (heart- or plum-shaped), broadcasting to the sides much more effectively than up or down (see [Figure 1 on page 20](#)). In general, this is good for most office environments because you have large flat floors. However, it can be a problem in environments with high ceilings.

Figure 1 Omnidirectional antenna radiation patterns



The HiveAP can accommodate external antennas via coaxial jacks on its chassis (see "Antennas" on page 32). The jack is a standard male RP-SMA connector. Various patch, directional, and omnidirectional antennas can be used to change the coverage pattern. The most common external antennas are patch antennas. These are directional antennas that provide coverage in a single direction. Most commonly they have a transmission pattern as shown in Figure 2. Based on the gain, the signal will be wide (like the low gain antenna shown on top) or narrow and long (like the high gain antenna shown on the bottom). Note that the coverage patterns are not perfect for these antennas and that they often broadcast slightly in other directions than the primary one. These extra "lobes" can be seen in both of the patterns shown below.

Figure 2 Directional antenna patterns



The following are some quick hints for deploying access points:

- Standard sheetrock walls and dropped ceilings are the best locations for mounting access points.
- When deploying WLANs in retail stores, doing a site survey at each store is likely to be impractical. It is more common to run detailed site surveys at a few locations and use the results to set up deployment guidelines for the remaining sites.
- Be aware of metal-lined firewalls, steel pillars, and other metallic surfaces. RF signals can reflect off metal surfaces, which can cause unexpected coverage patterns. Also watch out for objects that can block or reflect signals, such as mirrors, plants, walls, steel doors, elevator shafts, and bathroom stalls.

- The quality and performance of a Wi-Fi network is a function of the signal-to-noise ratio. To avoid noise issues, check the area for common noise generators such as industrial microwave ovens, wireless video cameras, cordless phones and headsets, and Bluetooth devices. Such devices especially cause interference in the 2.4 GHz spectrum.
- Plan appropriately for high ceilings. With an omnidirectional antenna, the downward coverage is not great. In normal office space, the ceilings rarely exceed 15 feet, so this issue does not come up very often. In environments such as warehouses, where ceilings can be up to 50 feet high, ceiling-mounted access points are not optimal. It is best to deploy them on non-metallic walls about 10 feet to 15 feet above the floor. If this is not feasible, using patch antennas can help direct the RF energy downward.
- In high-density or high-capacity environments, placing access points on exterior walls allows for a greater number of cells inside the building and more capacity. In other deployments, it is recommended that the outer access points be no farther than 30 feet from the exterior walls to ensure coverage.

Preparing the Wired Network for Wireless

One of the advantages of moving to an Aerohive WLAN is that you do not have to make changes to the underlying network, such as putting controllers into wiring closets. This can save you considerable time and effort during installation. However, some network changes might make sense for some deployments. For example, you might want to add additional VLANs or security settings. This section covers a few of the more common considerations that IT departments are handling.

- **802.1Q VLANs**

HiveAPs can segment users into VLANs if an administrator wants. This decision can be made by a returned RADIUS attribute or it can be configured as part of a user profile or SSID. Enterprises often set up separate VLANs for wireless and guest access, so that this traffic is segmented from the rest of the network; however, it is possible to set up any number of other VLANs for further segmentation.

- **Firewalls**

Depending on the environment, enterprises might use firewalls to segment wired and wireless data. This can be implemented as a discrete firewall enforcing traffic between VLANs or between ports, or you might use the stateful firewall that is integrated in HiveOS (the HiveAP operating system).

- **RADIUS Authentication**

If RADIUS authentication is required, then a RADIUS server must be in place and be able to support the necessary protocols for wireless—often called 802.1X EAP types: PEAP, EAP-TLS, EAP-TTLS, WEP 8021.x (dynamic WEP), LEAP, EAP-FAST, and captive web portal authentication using CHAP.

- **DNS and DHCP Configuration**

If you use the Aerohive HiveManager (see the section on ["Operational Considerations" on page 22](#)), it is possible to install HiveAPs without any extra configuration and they will be able to contact HiveManager for management. If the HiveAPs are linked to a different subnet than the one to which HiveManager is connected, then you can set either a DHCP option or DNS entry to give the location of HiveManager (see ["How HiveAPs Connect to HiveManager" on page 133](#)).

OPERATIONAL CONSIDERATIONS

To make your WLAN deployment process as smooth as possible, you should consider more than just the distribution and installation of access points. You should also consider how you will manage, optimize, and troubleshoot your WLAN after deployment.

Tuning

Approach building an enterprise WLAN with the same life-cycle approach you would apply to a wired network. After you deploy the WLAN, revisit key network engineering processes to account for changes in the environment. Watch for access points that are overloaded or are under utilized, and check for potential dead spots. Furthermore, be aware that the likely points of failure can change as the environment changes. For example, a neighboring business might install access points that cause RF interference on your network. You should schedule and perform periodic walkthroughs to ensure that the design goals of the wireless network continue to be met. The Aerohive HiveManager provides quick views into how the network is behaving, which HiveAPs are the most heavily loaded, and which have the most clients.

Troubleshooting

Some of the most common issues that arise after deploying a new wireless network are RF interference, RADIUS issues, and desktop client issues. The first step in troubleshooting is to look at logs and use debug commands. Aerohive offers an extensive set of event monitoring and debug tools that you can use through HiveManager, the Aerohive network management system. For additional troubleshooting, particularly of clients or neighboring networks, Aerohive recommends two tools: Ethereal Warehouser (<http://www.wireshark.org/>) and AirMagnet Laptop Analyzer (<http://www.airmagnet.com/products/laptop.htm>).

Management

Current Wi-Fi networks typically span an entire company and have complex security policies. Fortunately, the HiveManager Network Management System makes it simple to manage large networks from a central location. It provides a single centralized management instance for the entire wireless network. While managed HiveAPs can operate without HiveManager, it simplifies the provisioning of global policy management and centralized configuration and monitoring. HiveManager lowers operating costs by speeding deployment, configuration, and monitoring of the wireless network.

Managing faults and alarms is critical to maintaining uptime. You can view and manage events through HiveManager logging. Optionally, you can use a third-party tool such as HP OpenView.

HiveManager makes it easy to monitor and troubleshoot HiveAPs within a WLAN infrastructure. HiveManager can import hierarchical map views that represent the physical location of the network, from the perspective of the entire world down to the floor level.

Deploying with Confidence

Moving a large enterprise—or even a small one—to a WLAN for the very first time need not be daunting. If you have moderate experience with LAN deployments of other types and you have taken time to get answers to the important questions that will affect the network data load, you have every prerequisite for success. The bottom line is to remember to take stock of your project before you begin to ward against unforeseen costs and performance bottlenecks. If you have considered the issues and guidelines presented here, you are not far away from a successful Aerohive WLAN deployment.

BASIC WI-FI CONCEPTS

The goal of this section is to provide some background on Wi-Fi propagation and how to lay out a wireless network. While RF (radio frequency) engineering is a rather complicated science, this section provides a simple overview on the basics of Wi-Fi propagation and channel layout that you need to be able to install an enterprise WLAN.

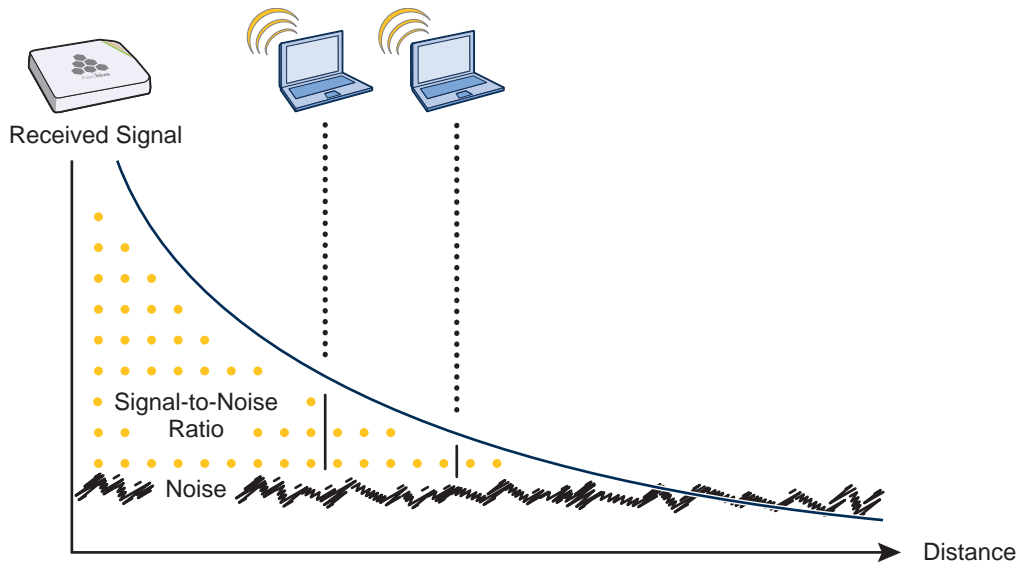
The first thing to know is that Wi-Fi is forgiving. Wi-Fi tends to transmit a bit farther than you expect, and even in cases of interference, it tends to just work. This can be both a blessing and a curse. It is a blessing because people will likely have access to the network, and it is a curse because your overall performance might be suboptimal without obvious symptoms, like lack of connectivity. Understanding the basics presented in this section will help ensure a high performance layout.

The first concept to understand is signal strength and how it relates to throughput. Radio power is measured in dBm (decibels relative to one milliwatt) where 0 dBm = 1 milliwatt, but decibels increase using a \log_{10} math function. Rather than dusting off your old math books and pulling out your calculator, look at the dBm-to-milliwatt converter that appears below. Often in Wi-Fi, dBm and milliwatts (mW)—and microwatts (μ W)—are used interchangeably. The following table converts between the two units of measurement.

dBm-to-milliwatt	
20 dBm = 100 mW	2 dBm = 1.6 mW
15 dBm = 32 mW	1 dBm = 1.3 mW
10 dBm = 10 mW	0 dBm = 1.0 mW
5 dBm = 3.2 mW	-1 dBm = 794 μ W
4 dBm = 2.5 mW	-5 dBm = 316 μ W
3 dBm = 2.0 mW	-10 dBm = 100 μ W

In RF, there is also a relative measurement that you can use to compare two numbers. This measurement is simply dB (without the "m"). To see how this concept is applied, consider how radio signal propagation changes over a distance and how it can be affected. [Figure 3 on page 24](#) shows signal strength over distance as a curve that has the best signal strength closer to the access point. It also shows noise. In general, noise is considered to be low-level background RF signals that can interfere with a WLAN. This noise tends to be the garbled background RF that comes from everything from the sun and stars to man-made interfering devices like Bluetooth headsets. It is impossible to block out noise and it should not be attempted. This low level of background noise is called the "noise floor".

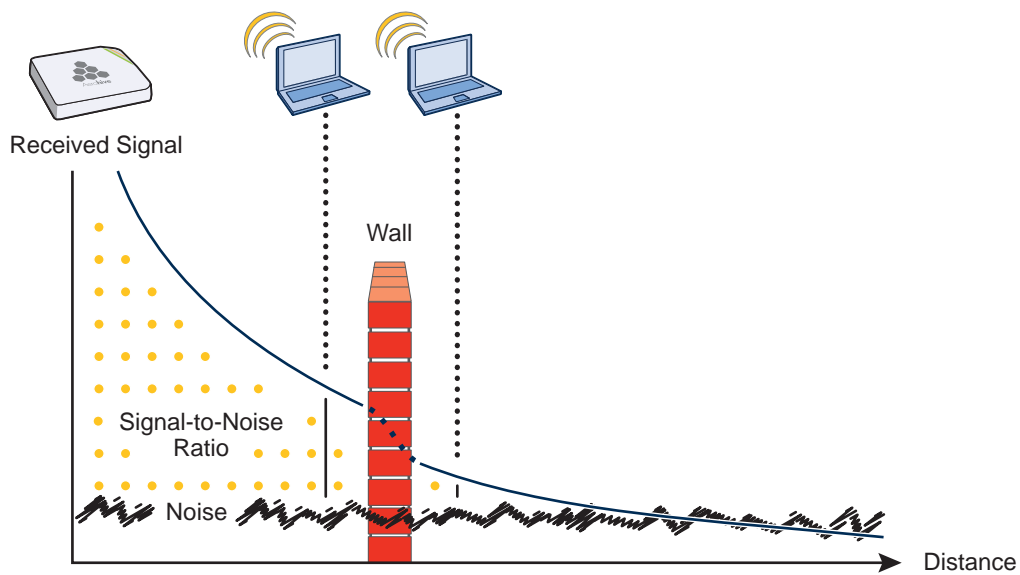
Figure 3 Path loss in an open space



When clients send a packet, the ratio of the signal-to-noise (SNR) level defines the quality of the link, which is directly related to the performance of the network. Based on the SNR, the client and AP negotiate a data rate in which to send the packet, so the higher the SNR the better. For good performance, the SNR should be greater than 20 dB, and for optimal performance it should be at least 25 dB.

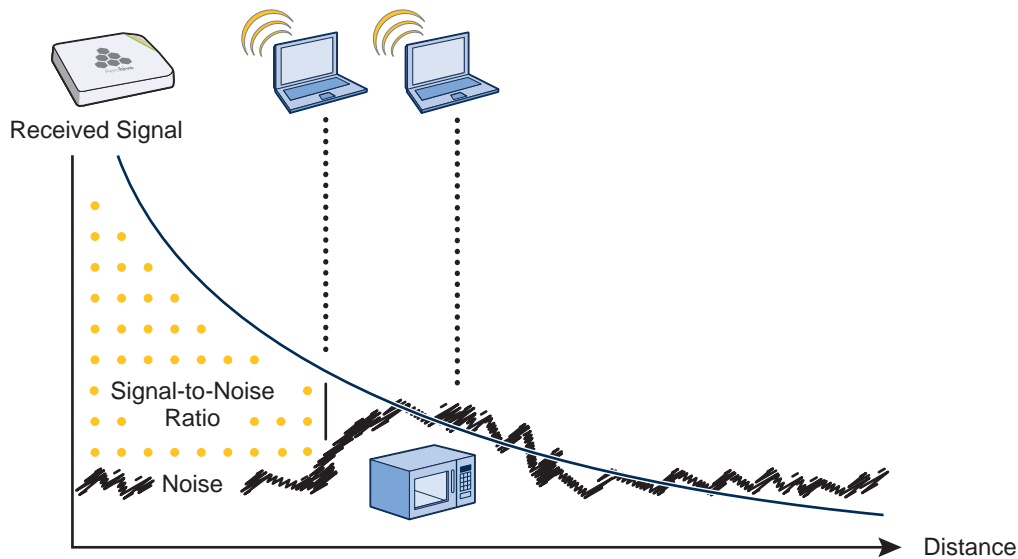
Signal strength not only diminishes over distance but it can also be affected by objects in the way (see Figure 4). This can be a wall, a tree, or even a person. There is a fairly predictable dB drop through most objects that also decreases the SNR, thus decreasing the data rate. While this appears to be a bad thing, clever Wi-Fi installers use it to their advantage. It allows them to place more access points in a tighter spot by using pre-existing walls and other impediments to Wi-Fi propagation to keep them from interfering with each other.

Figure 4 Path loss through a wall



Microwave ovens, wireless video cameras, Bluetooth headsets, and cordless phones can all interfere with Wi-Fi signals (see Figure 5). Excess noise in an environment is often difficult to diagnose and can have a major negative impact on network performance. To discover noise sources, a spectrum analysis system is needed. AirMagnet provides an affordable spectrum analysis tool that operates in the 2.4 GHz and 5 GHz spectra.

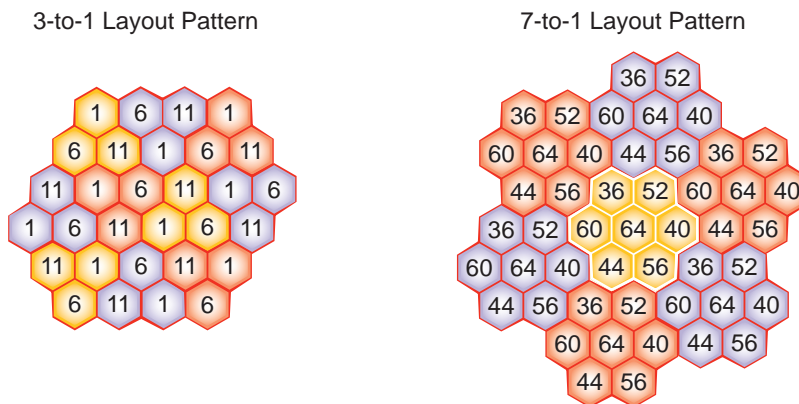
Figure 5 Path loss with noise (from a microwave)



Now that you have a sense of how Wi-Fi performance changes over distance and with noise, look at some ways to perform channel assignment. If two access points are on the same channel right next to each other, they are forced to share the same spectrum. This means that they share the 54-Mbps speeds available in 802.11a/g or the 300-Mbps speeds in 802.11n rather than each being capable of 54- or 300-Mbps speeds independently. This essentially halves the bandwidth for each access point. To manage this situation, make sure that neighboring APs are on different channels and that their power is adjusted so that it does not overlap that of other APs with the same channel.

In the 2.4 GHz spectrum, there are 11 channels in the United States. However, a Wi-Fi signal consumes more than one channel. Consequently, there are only 3 non-overlapping channels: 1, 6, and 11. To achieve optimal performance, you need to design a channel layout pattern such as the one on the left in Figure 6.

Figure 6 Channel layout patterns

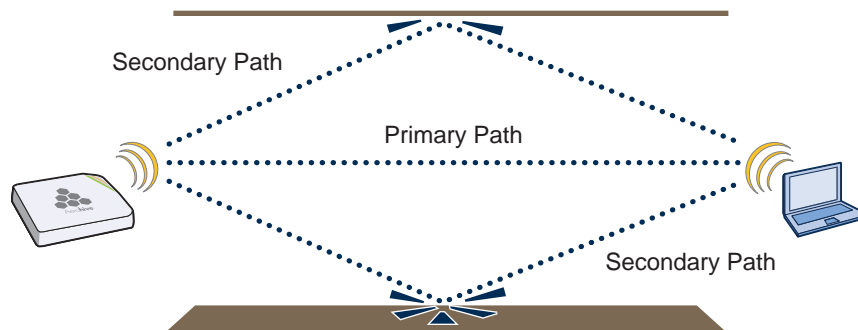


Note: There are alternative 2.4 GHz channel layouts, such as one for four channels using 1, 4, 8 and 11 and another using channels 1, 5, 9 to counter interference from microwaves, which tend to cause interference in the high end of the spectrum. Aerohive recommends alternative channel layouts only for the most challenging radio environments.

Designing a channel pattern is easier for the 5 GHz spectrum. Depending on the country and the device being used, there are between 4 and 24 channels available for Wi-Fi use. However, in most countries there are at least 8 40-MHz-wide channels with which to work. To simplify the layout of more than 3 channels most use a 7-to-1 pattern, as is shown on the right in [Figure 6 on page 25](#). This channel layout is much more flexible than the 3-channel system and allows for much better capacity over all channels.

The last topic to cover is the concept of multipath. When a client receives a transmission from an access point (or vice versa), the RF signal reaches the client first through a "direct path", but then shortly thereafter by the "indirect paths" reflected off other objects. The direct path combined with the indirect paths make up multipaths (see [Figure 7](#)). RF signals can bounce off of almost anything—walls, people, plants, and so on—but they bounce the greatest off of metal. As the RF signals bounce about while propagating, one or more of the secondary paths can interfere with the primary path, causing the signal strength of the direct path to diminish. In doing so, multipath can greatly decrease signal to noise ratio with legacy 802.11a/g radios. With 802.11n, a certain amount of multipath is desirable and increases performance.

Figure 7 Multipath radio waves



Note: If you would like to learn more about how radio frequency propagation works or the details of 802.11, Wikipedia provides excellent background information under the entries "IEEE 802.11", "radio propagation", and "multipath". Additionally, spending a few hours with a site survey tool such as AirMagnet Surveyor or Ekahau's Site Survey (ESS) and a few test APs can increase both your familiarity with Wi-Fi propagation and your confidence about how it behaves.

Chapter 2 The HiveAP 20 ag Platform

The Aerohive HiveAP 20 ag is a new generation wireless access point. HiveAPs have the unique ability to self-organize and coordinate with each other, creating a distributed-control WLAN solution that offers greater mobility, security, quality of service, and radio control.

This guide combines product information, installation instructions, and configuration examples for both the HiveAP and HiveManager platforms. This chapter covers the following topics relating to the HiveAP:

- ["HiveAP 20 Product Overview" on page 28](#)
 - ["Ethernet and Console Ports" on page 30](#)
 - ["Status LEDs" on page 31](#)
 - ["Antennas" on page 32](#)
- ["Mounting the HiveAP 20" on page 33](#)
- ["Device, Power, and Environmental Specifications" on page 35](#)

HIVEAP 20 PRODUCT OVERVIEW

The HiveAP 20 ag is a multi-channel wireless AP (access point). It is compatible with IEEE 802.11b/g (2.4 GHz) and IEEE 802.11a (5 GHz) standards and supports a variety of Wi-Fi (wireless fidelity) security protocols, including WPA (Wi-Fi Protected Access) and WPA2.

You can see the hardware components on the HiveAP in [Figure 1](#). Each component is described in [Table 1](#).

Figure 1 HiveAP 20 hardware components

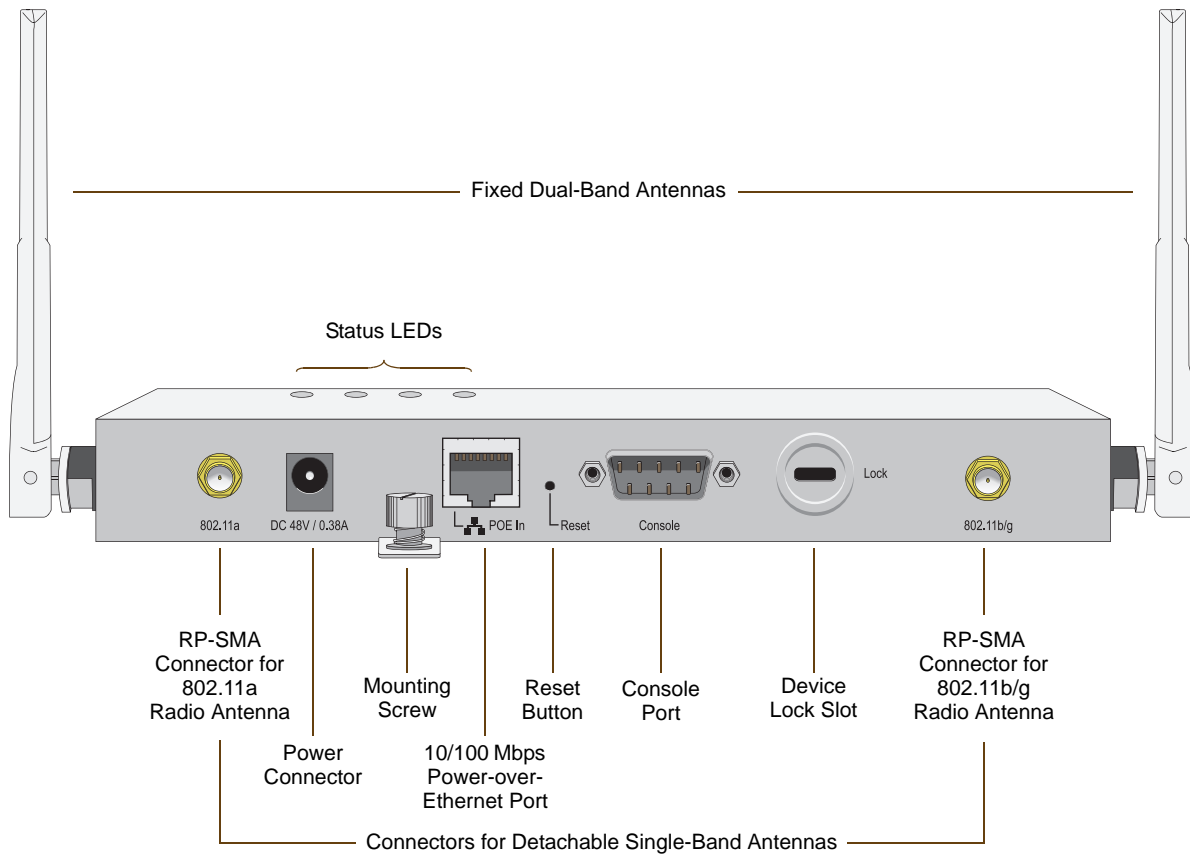


Table 1 HiveAP 20 component descriptions

Component	Description
Fixed Dual-Band Antennas	The two fixed omnidirectional dipole antennas can operate at two radio frequencies: 2.4 GHz (for IEEE 802.11b/g) and 5 GHz (for IEEE 802.11a). For details, see "Antennas" on page 32 .
Status LEDs	The status LEDs convey operational states for system power, and the LAN, Access, and Mesh interfaces. For details, see "Status LEDs" on page 31 .
802.11a RP-SMA Connector	You can connect a detachable single-band antenna, such as the Pulse W1028 dipole antenna for the 5 GHz band, to the male 802.11a RP-SMA (reverse polarity-subminiature version A) connector. Note that doing so disables the adjacent fixed antenna.

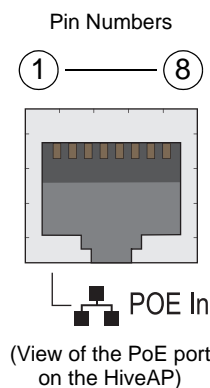
Component	Description
Power Connector	The 48-volt DC power connector (0.38 amps) is one of two methods through which you can power the HiveAP 20. To connect it to a 100 - 240-volt AC power source, use the AC/DC power adaptor that is available as an extra option. Because the HiveAP does not have an on/off switch, connecting it to a power source automatically powers on the device.
Mounting Screw	To mount the HiveAP 20 on a surface, attach the mounting plate that ships with the product to the HiveAP by inserting the two pins on the underside of the chassis into slots in the plate and tightening the mounting screw. For details, see "Mounting the HiveAP 20" on page 33 .
10/100 Mbps PoE Port	<p>The 10/100-Mbps Ethernet port supports IEEE 802.3af PoE (Power over Ethernet) and receives RJ-45 connectors. The HiveAP can receive its power through an Ethernet connection to PSE (power sourcing equipment) that is 802.3af-compatible, such as one of the PoE injectors available as an optional accessory from Aerohive. (If you connect the HiveAP to a power source through the power connector and PoE port simultaneously, the device draws power through the power connector and automatically disables PoE.)</p> <p>The HiveAP can also connect to the wired network or to a wired device (such as a security camera) through this port. It is compatible with 10/100Base-T/TX and automatically negotiates half- and full-duplex connections with the connecting device. It is autosensing and adjusts to straight-through and cross-over Ethernet cables automatically. It also automatically adjusts for 802.3af Alternative A and B methods of PoE. For details, see "Ethernet and Console Ports" on page 30.</p>
Reset Button	<p>The reset button allows you to reboot the device or reset the HiveAP to its factory default settings. Insert a paper clip, or something similar, into the Reset pinhole and press the reset button. To reboot the device, hold the button down between 1 and 5 seconds. To return the configuration to the factory default settings, hold it down for at least 5 seconds. After releasing the button, the Power LED goes dark, and then glows steady amber while the firmware loads and the system performs a self-test. After the software finishes loading, the Power LED glows steady green.</p> <p>To disable the reset button from resetting the configuration, enter this command: <code>no reset-button reset-config-enable</code> Pressing the button between 1 and 5 seconds will still reboot the HiveAP, but pressing it for more than 5 seconds will not reset its configuration.</p>
Console Port	A male DB-9 serial port to which you can make a console connection using an RS-232 (or "null modem") cable. The management station from which you make a serial connection to the HiveAP must have a VT100 emulation program, such as Tera Term Pro [®] (a free terminal emulator) or Hilgraeve Hyperterminal [®] (provided with Windows [®] operating systems). The following are the serial connection settings: bits per second: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none.
Device Lock Slot	You can physically secure the HiveAP by attaching a lock and cable (such as a Kensington [®] notebook lock) to the device lock slot. After looping the cable around a secure object, insert the T-bar component of the lock into the slot on the HiveAP and turn the key to engage the lock mechanism.
802.11b/g RP-SMA Connector	You can connect a detachable single-band antenna, such as the Pulse W1038 dipole antenna for the 2.4 GHz band, to the male 802.11b/g RP-SMA connector. Note that doing so disables the adjacent fixed antenna.

Ethernet and Console Ports

There are two ports on the HiveAP 20: a 10/100Base-T/TX Ethernet port and a male DB-9 console port. Both ports use standard pin assignments.

The pin assignments in the PoE (Power over Ethernet) Ethernet port follow the TIA/EIA-568-B standard (see [Figure 2](#)). The PoE port accepts standard types of Ethernet cable—cat3, cat5, cat5e, or cat6—and can receive power over this cable from power sourcing equipment (PSE) that is 802.3af-compatible. Such equipment can be embedded in a switch or router, or it can come from purpose-built devices that inject power into the Ethernet line en route to the HiveAP. Because the PoE port has autosensing capabilities, the wiring termination in the Ethernet cable can be either straight-through or cross-over.

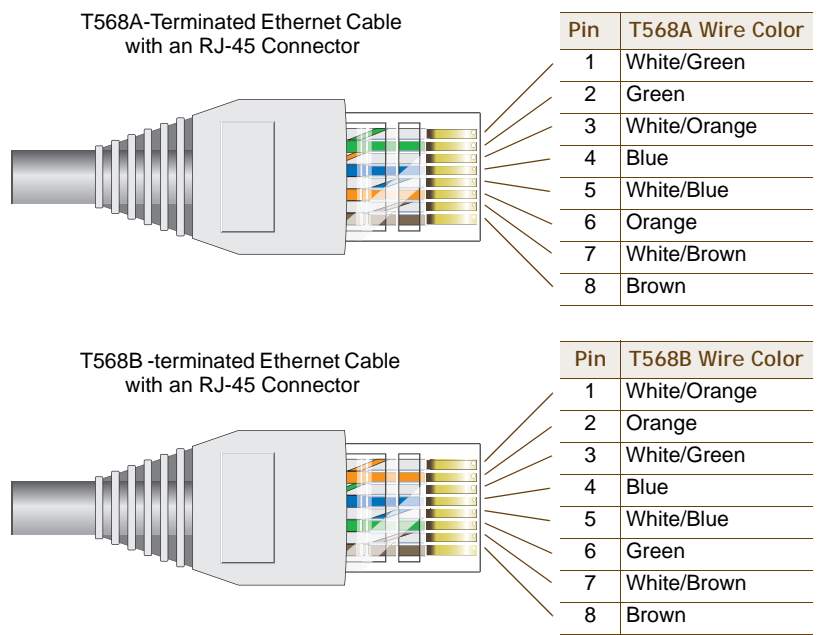
Figure 2 PoE wire usage and pin assignments



Pin	Data Signal	802.3af Alternative A (Data and Power on the Same Wires)		802.3af Alternative B (Data and Power on Separate Wires)
		MDI	MDI-X	MDI or MDI-X
1	Transmit +	DC+	DC-	---
2	Transmit -	DC+	DC-	---
3	Receive +	DC-	DC+	---
4	(unused)	---	---	DC+
5	(unused)	---	---	DC+
6	Receive -	DC-	DC+	---
7	(unused)	---	---	DC-
8	(unused)	---	---	DC-

MDI = Medium dependent interface for straight-through connections
 MDI-X = Medium dependent interface for cross-over (X) connections

The PoE port is auto-sensing and can automatically adjust to transmit and receive data over straight-through or cross-over Ethernet connections. Likewise, it can automatically adjust to 802.3af Alternative A and B power delivery methods. Furthermore, when the Alternative A method is used, the PoE port automatically allows for polarity reversals depending on its role as either MDI or MDI-X.



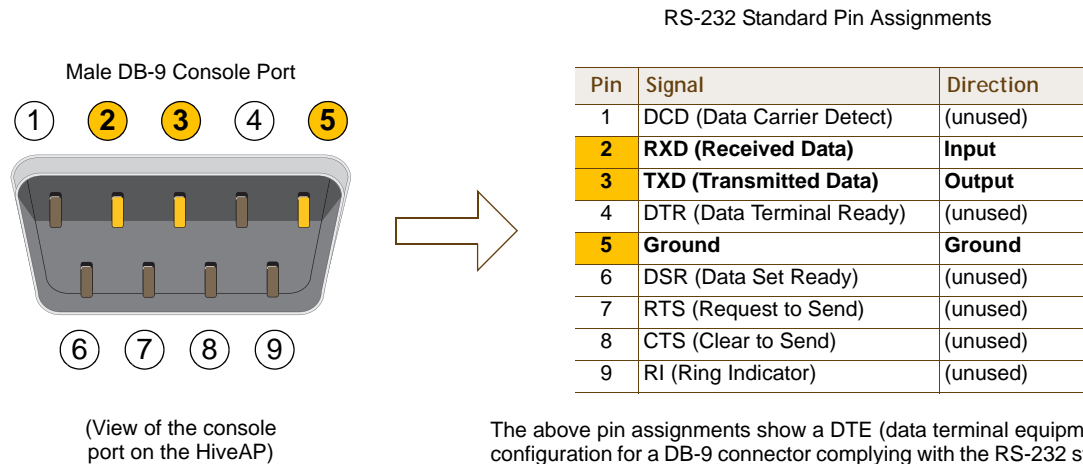
T568A and T568B are two standard wiring termination schemes. Note that the only difference between them is that the white/green + solid green pair of wires and the white/orange + solid orange pair are reversed.

For straight-through Ethernet cables—using either the T568A or T568B standard—the eight wires terminate at the same pins on each end.

For cross-over Ethernet cables, the wires terminate at one end according to the T568A standard and at the other according to T568B.

The pin assignments in the male DB-9 console port follow the EIA (Electronic Industries Alliance) RS-232 standard. To make a serial connection between your management system and the console port on the HiveAP, you can use a null modem serial cable, use another serial cable that complies with the RS-232 standard, or refer to the pin-to-signal mapping shown in [Figure 3](#) to make your own serial cable. Connect one end of the cable to the console port on the HiveAP and the other end to the serial (or COM) port on your management system. The management system must have a VT100 terminal emulation program, such as Tera Term Pro[®] (a free terminal emulator) or Hilgraeve Hyperterminal[®] (provided with Windows[®] operating systems).

Figure 3 Console port pin assignments



Status LEDs

The four status LEDs on the top of the HiveAP 20 indicate various states of activity through their color (dark, green, amber) and illumination patterns (steady glow or blinking). The meanings of the various color + illumination patterns for each LED are explained below.

Power

- Dark: No power
- Steady green: Powered on and the firmware is running normally
- Steady amber: Firmware is booting up or is being updated
- Blinking amber: Alarm indicating firmware failure

LAN

- Dark: Ethernet link is down or disabled
- Steady green: Ethernet link is up but inactive
- Blinking green: Ethernet link is up and active

Access

- Dark: Wireless link is disabled
- Steady green: Wireless link is up but inactive
- Blinking green: Wireless link is up and active

Mesh

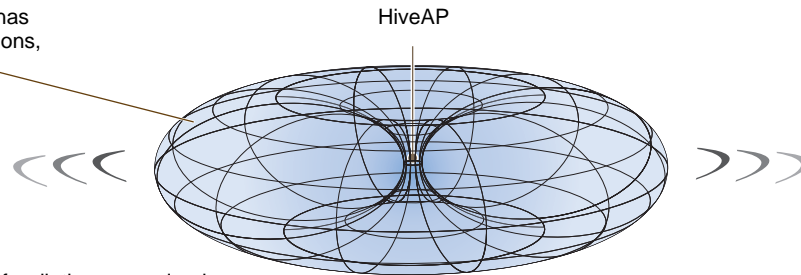
- Dark: Wireless link is disabled
- Steady green: Wireless link is up but inactive
- Blinking green (fast): Wireless link is up and the HiveAP is searching for other hive members
- Blinking green (slowly): Wireless link is up and active

Antennas

The HiveAP 20 includes two fixed dual-band antennas with 3-dBi gains. These antennas are omnidirectional, providing fairly equal coverage in all directions in a toroidal (donut-shaped) pattern around each antenna. When the antennas are vertically positioned, coverage expands primarily on the horizontal plane, extending horizontally much more than vertically. See [Figure 4](#), which shows the toroidal pattern emanating from a single vertically positioned antenna. To change coverage to be more vertical than horizontal, position the antennas horizontally. You can also resize the area of coverage by increasing or decreasing the signal strength.

Figure 4 Omnidirectional radiation pattern

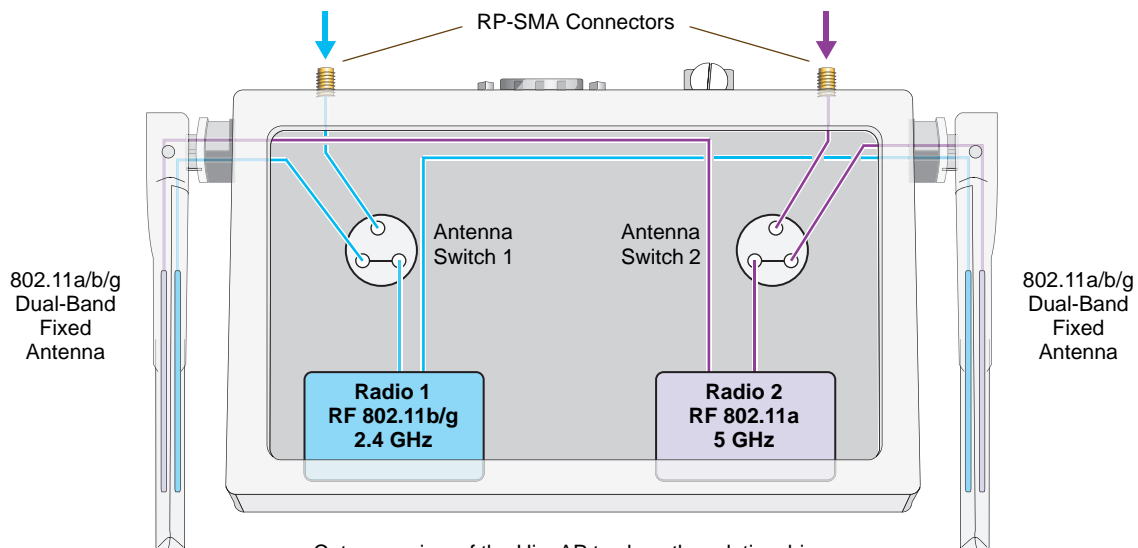
The omnidirectional antennas radiate equally in all directions, forming a toroidal pattern.



Note: To show the shape of radiation more clearly, this illustration depicts the coverage provided by only one active antenna and is not drawn to scale.

The pair of fixed dual-band antennas operate concurrently in two different frequency ranges: 2.4 GHz (IEEE 802.11b/g) and 5 GHz (IEEE 802.11a). Using two different frequency ranges reduces the probability of interference that can occur when numerous channels operate within the same range. Conceptually, the relationship of antennas and radios is shown in [Figure 5](#).

Figure 5 Antennas and radios



Cut-away view of the HiveAP to show the relationship of the antennas and the two internal radios.

If you connect an external antenna to an RP-SMA connector, you must enter the following command to move the appropriate interface from the adjacent fixed antenna to the external antenna:

```
interface interface radio antenna external
```

The wifi0 interface links to radio 1 (frequency range = 2.4 GHz for IEEE 802.11b/g), and the wifi1 interface links to radio 2 (frequency range = 5 GHz for IEEE 802.11a). These interface-to-radio relationships are permanent. However, the interface-to-antenna relationships can be shifted. In other words, you can change which antenna—fixed or external—the wifi0 and wifi1 interfaces use. For example, to link the wifi0 interface to an external antenna connected to the 802.11b/g RP-SMA connector (for radio 1), enter the following command:

```
interface wifi0 radio antenna external
```

If you do not enter this command, the wifi0 interface and all its subinterfaces (wifi0.1, wifi0.2, wifi0.3 ... wifi0.7) continue to use both fixed antennas.

Note: After entering the above command, the radio to which you attached the external antenna uses the external antenna and the fixed antenna on the opposite side of the HiveAP. Attaching an external antenna only disconnects the adjacent fixed antenna. Note the two antenna switches shown in [Figure 5 on page 32](#).

To unlink the wifi0 interface from the external antenna and return it to the fixed antennas, enter this command:

```
interface wifi0 radio antenna internal
```

MOUNTING THE HIVEAP 20

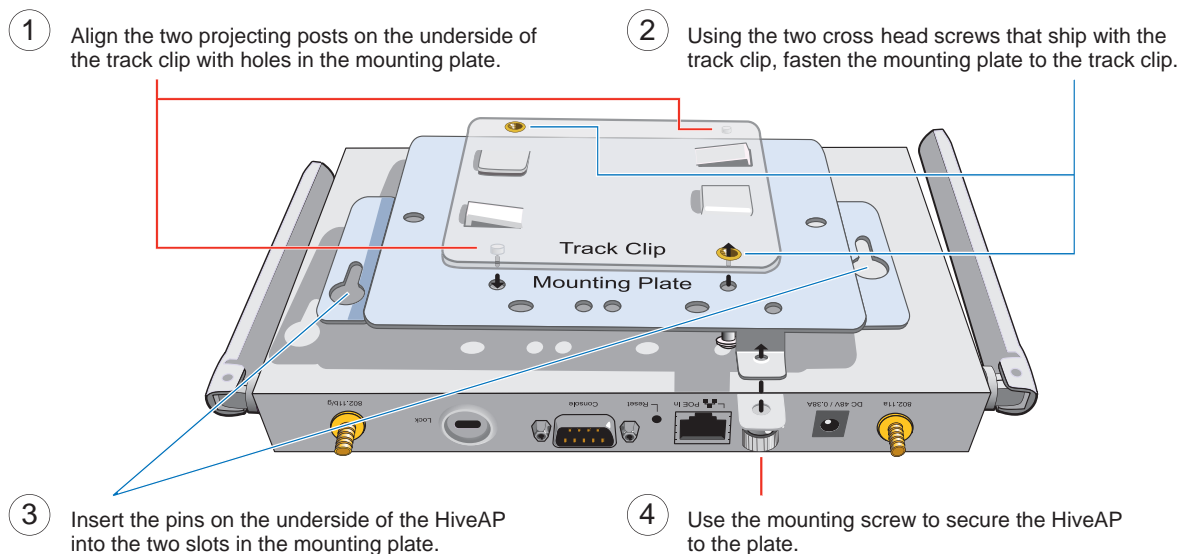
Using the mounting plate and track clip, you can mount the HiveAP 20 to the tracks of a dropped ceiling grid. Using just the mounting plate, you can mount the HiveAP to any surface that can support its weight (1.5 lb., 0.68 kg).

Ceiling Mount

To mount the HiveAP 20 to a track in a dropped ceiling, you need the mounting plate, track clip, and two cross-head screws that ship with the track clip. You also need a cross-head screw driver and—most likely—a ladder.

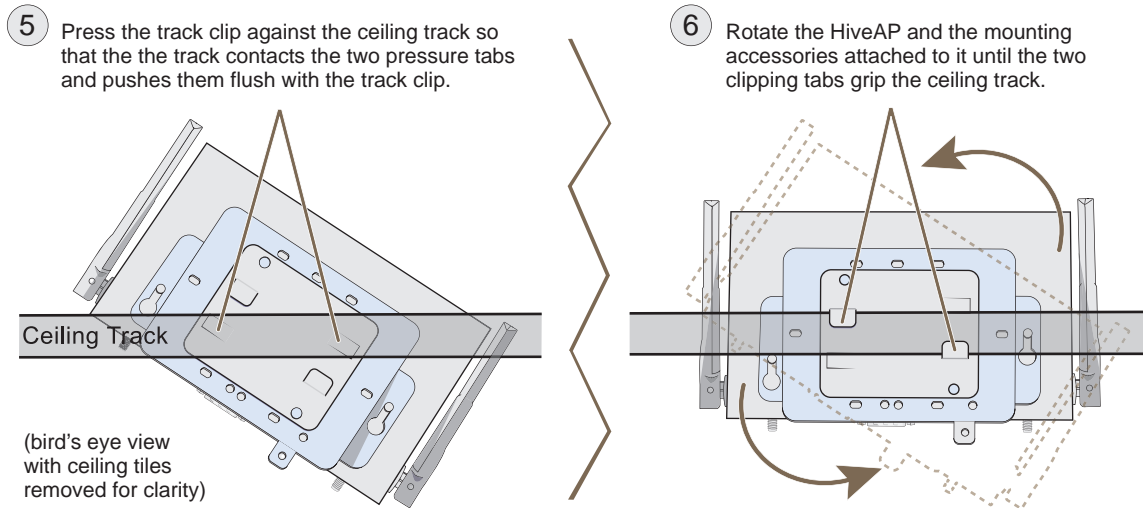
Attach the track clip to the mounting plate, and then attach the clip-plate combination to the HiveAP 20, as shown in [Figure 6](#).

Figure 6 Attaching the HiveAP 20 to the mounting plate and track clip



Nudge the ceiling tiles slightly away from the track to clear some space. Then attach the track clip to the ceiling track as shown in [Figure 7](#). When done, adjust the ceiling tiles back into their former position.

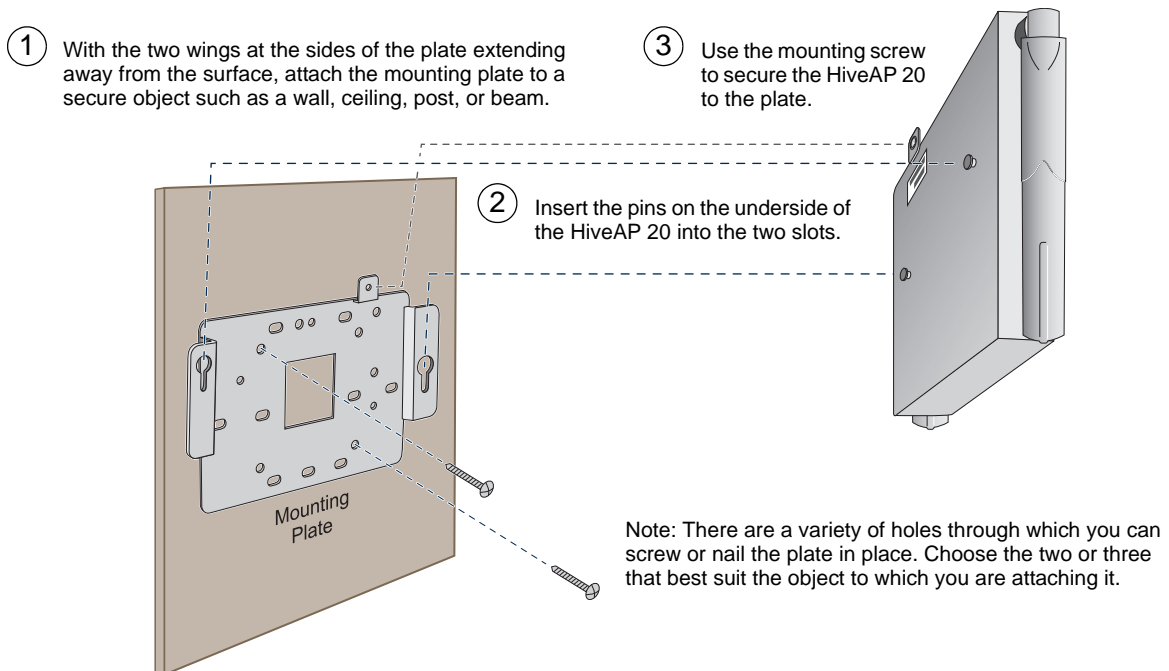
Figure 7 Attaching the HiveAP to a dropped ceiling track



Surface Mount

You can use the mounting plate to attach the HiveAP 20 to any surface that supports its weight, and to which you can screw or nail the plate. First, mount the plate to the surface, and then attach the device to the plate, as shown in [Figure 8](#).

Figure 8 Mounting the HiveAP on a wall



DEVICE, POWER, AND ENVIRONMENTAL SPECIFICATIONS

Understanding the range of specifications for the HiveAP 20 is necessary for optimal deployment and device operation. The following specifications describe the physical features and hardware components, the power adapter and PoE (Power over Ethernet) electrical requirements, and the temperature and humidity ranges in which the device can operate.

Device Specifications

- Chassis dimensions: 8 1/4" W x 1" H x 4 15/16" D (21 cm W x 2.5 cm H x 12.5 cm D)
- Weight: 1.5 lb. (0.68 kg)
- Antennas: Two fixed dual-band 802.11a/b/g antennas, and two RP-SMA connectors for detachable single-band 802.11a or 802.11b/g antennas
- Serial port: DB-9 (bits per second: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none)
- Ethernet port: autosensing 10/100Base-T/TX Mbps, with IEEE 802.3af-compliant PoE (Power over Ethernet)

Power Specifications

- AC/DC power adapter:
 - Input: 100 - 240 VAC
 - Output: 48V/0.38A
- PoE nominal input voltages: 48 V, 0.35A
- RJ-45 power input pins: Wires 4, 5, 7, 8 or 1, 2, 3, 6

Environmental Specifications

- Operating temperature: 32 to 122 degrees F (0 to 50 degrees C)
- Storage temperature: -4 to 158 degrees F (-20 to 70 degrees C)
- Relative Humidity: Maximum 95%

Chapter 3 The HiveAP 28 Outdoor Platform

The Aerohive HiveAP 28 is a new generation wireless access point that is customized for outdoor use. It is mountable in any direction and on any hard surface, post, or wire strand. It can receive power either through an Ethernet cable or power cord.

Note: Do not open the HiveAP 28 chassis. There are no serviceable parts inside.

This guide combines product information, installation instructions, and configuration examples for both the HiveAP and HiveManager platforms. This chapter covers the following topics relating to the HiveAP 28:

- ["HiveAP 28 Product Overview" on page 38](#)
 - ["Ethernet Port" on page 39](#)
 - ["Power Connector" on page 40](#)
 - ["Antennas" on page 41](#)
- ["Mounting the HiveAP 28 and Attaching Antennas" on page 42](#)
 - ["Pole Mount" on page 43](#)
 - ["Strand Mount" on page 44](#)
 - ["Surface Mount" on page 45](#)
 - ["Attaching Antennas" on page 46](#)
- ["Device, Power, and Environmental Specifications" on page 48](#)

HIVEAP 28 PRODUCT OVERVIEW

The HiveAP 28 is a multi-channel wireless AP (access point) for outdoor use. It is compatible with IEEE 802.11b/g (2.4 GHz) and IEEE 802.11a (5 GHz) standards and supports a variety of Wi-Fi (wireless fidelity) security protocols, including WPA (Wi-Fi Protected Access) and WPA2.

You can see the hardware components on the HiveAP 28 in [Figure 1](#). Each component is described in [Table 1](#).

Figure 1 HiveAP 28 hardware components

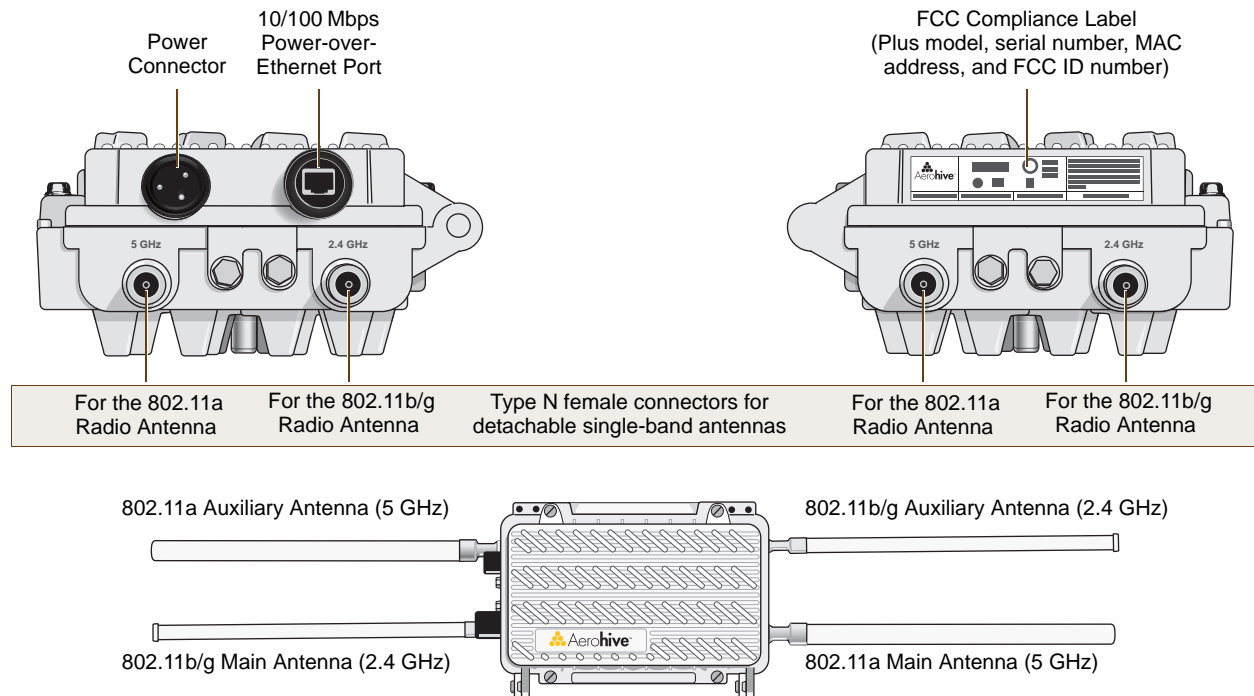


Table 1 HiveAP 28 component descriptions

Component	Description
Detachable Single-Band Antennas	The two pairs of detachable omnidirectional dipole antennas operate at two radio frequencies: one pair at 2.4 GHz (for IEEE 802.11b/g) and the other at 5 GHz (for IEEE 802.11a). For details, see "Antennas" on page 41 .
Type N Connectors (Female)	Attach antennas to the HiveAP 28 through these connectors. For details, see "Attaching Antennas" on page 46 .
Waterproof Power Connector	Using the power connector is one of two methods through which you can power the HiveAP 28. To connect it to a 100 - 240-volt AC power source, use the power cable that ships with the product as an extra option. Because the HiveAP does not have an on/off switch, connecting it to a power source automatically powers on the device. The power source must have a readily accessible service disconnect switch incorporated into the fixed wiring installation so that you have the ability to turn the power on and off. (The other method that the HiveAP can obtain power is through its PoE port.)

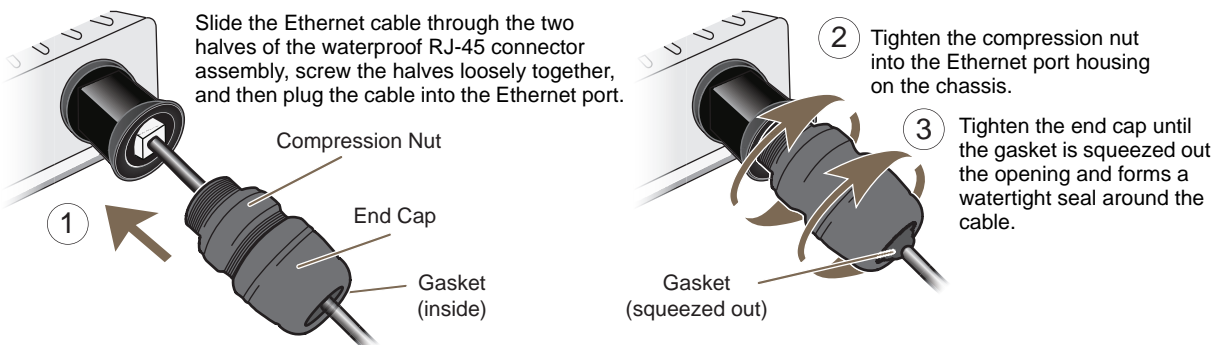
Component	Description
10/100 Mbps PoE Port	<p>The 10/100-Mbps Ethernet port supports IEEE 802.3af PoE (Power over Ethernet) and receives RJ-45 connectors. The HiveAP can receive its power through an Ethernet connection to PSE (power sourcing equipment) that is 802.3af-compatible, such as one of the PoE injectors available as an optional accessory from Aerohive. (If you connect the HiveAP to a power source through the power connector and PoE port simultaneously, the device draws power through the power connector and automatically disables PoE.)</p> <p>The HiveAP 28 can also connect to the wired network or to a wired device (such as a security camera) through this port. It is compatible with 10/100Base-T/TX and automatically negotiates half- and full-duplex connections with the connecting device. It is autosensing and adjusts to straight-through and cross-over Ethernet cables automatically (MDI/MDI-X). It also automatically adjusts for 802.3af Alternative A and B methods of PoE. For details, see "Ethernet Port".</p>

Ethernet Port

The HiveAP 28 has a 10/100Base-T/TX PoE (Power over Ethernet) port. Its pin assignments follow the TIA/EIA-568-B standard (see [Figure 2 on page 30](#)). The PoE port accepts standard types of Ethernet cable—cat3, cat5, cat5e, or cat6—and can receive power over this cable from power sourcing equipment (PSE) that is 802.3af-compatible. Such equipment can be embedded in a switch or router, or it can come from purpose-built devices that inject power into the Ethernet line en route to the HiveAP. Because the PoE port has autosensing capabilities, the wiring termination in the Ethernet cable can be either straight-through or cross-over (MDI/MDI-X). For outdoor deployments use weatherproofed shielded twisted pair (STP) Ethernet cables.

To ensure a waterproof seal for the Ethernet connection, use the RJ-45 connector assembly, which comes in three parts: a compression nut, end cap, and gasket.

Figure 2 Connecting the Ethernet cable



1. Insert one end of the Ethernet cable through the waterproof RJ-45 connector assembly and plug the cable into the Ethernet port.
2. Tighten the compression nut by twisting it clockwise into the Ethernet port housing on the chassis.
3. Tighten the end cap by twisting it clockwise onto the compression nut and tighten until the rubber gasket emerges and wraps itself around the Ethernet cable.

The Ethernet connection is now sealed and waterproof.

4. Connect the other end of the Ethernet cable to PSE (power sourcing equipment) such as a power injector if the HiveAP 28 receives power through PoE, or directly to a network device such as a switch if it receives power through a power cord.

Note: To prevent damage to the HiveAP 28 or power injector when using PoE to provide power, connect the Ethernet cable from the power injector to the HiveAP 28, and connect the injector to a power jack before applying power.

If the Ethernet cable connects the HiveAP to another device that is indoors, you must install appropriate lightning protection at the point before it enters the building. Failing to do so might cause damage to the equipment as well as serious injury or death.

Note: When the HiveAP acts as a mesh point and does not use the Ethernet port, cover the Ethernet port with a connector cap to prevent water intrusion and possible safety hazards.

Power Connector

The HiveAP 28 can receive power through an Ethernet cable using PoE or through a power cord. Aerohive recommends using either PoE or wiring the power cord directly to a 100 – 240-volt AC power source. Only plug the power cord into an electric outlet when configuring the device before deployment or when testing it in the lab.

Note: When the HiveAP receives power through PoE, cover the power connector with a connector cap to prevent water intrusion and possible safety hazards.

To connect the power cord to the HiveAP 28:

1. Align the slot in the power cord plug with the small tab at the top of the three-pin power connector, and slide the plug firmly over the pins until it is fully seated in the power connector.
2. Slide the cover over the connector and tighten it by turning the cover clockwise.
3. Install a lightning protector between the HiveAP 28 and its power source.
4. When possible, run the cord through a conduit to protect it from the elements. Where the cord is exposed, allow enough slack in it to create a drip loop. Leaving some slack in the cord lets water run away from the connections at each end. Use only a weatherproof power cord, such as the cord that ships with the HiveAP 28.
5. Strip the other end of the power cord and wire it directly to a power source, such as a junction box that has a service disconnect switch that you can use to turn the power on and off. Also, because the HiveAP 28 does not have short-circuit (over current) protection built into it, it relies on the protection provided by the power source to which you connect it. Ensure that the protective device, such as a circuit breaker, is not rated greater than 15A. Furthermore, if you need to install the HiveAP 28 in a wet or damp location, the AC branch circuit that is powering it must be provided with ground fault protection (GFCI), as required by Article 210 of the National Electrical Code (NEC).

Note: The HiveAP 28 must be grounded. Do not operate it unless there is a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

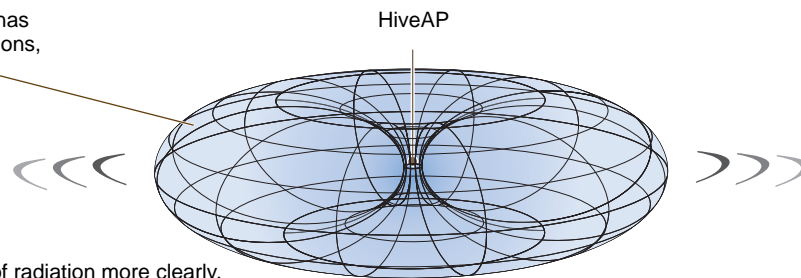
Antennas

The HiveAP 28 includes two detachable single-band antennas with 8dBi gains (802.11b/g) and two detachable single-band antennas with 10dBi gains (802.11a). These antennas are omnidirectional, providing fairly equal coverage in all directions in a toroidal (donut-shaped) pattern around each antenna. When the antennas are vertically positioned, coverage expands primarily on the horizontal plane, extending horizontally much more than vertically. See [Figure 3](#), which shows the toroidal pattern emanating from a single vertically positioned antenna. Note that when high gain antennas are added, the torus shape becomes somewhat elongated or compressed. If the HiveAP 28 is mounted higher than 20 feet the center of the torus curves inward so that the connection quality, directly underneath the center of the HiveAP 28, becomes compromised.

To change coverage to be more vertical than horizontal, position the HiveAP so that the antennas are on a horizontal plane. You can also resize the area of coverage by increasing or decreasing the signal strength.

Figure 3 Omnidirectional radiation pattern

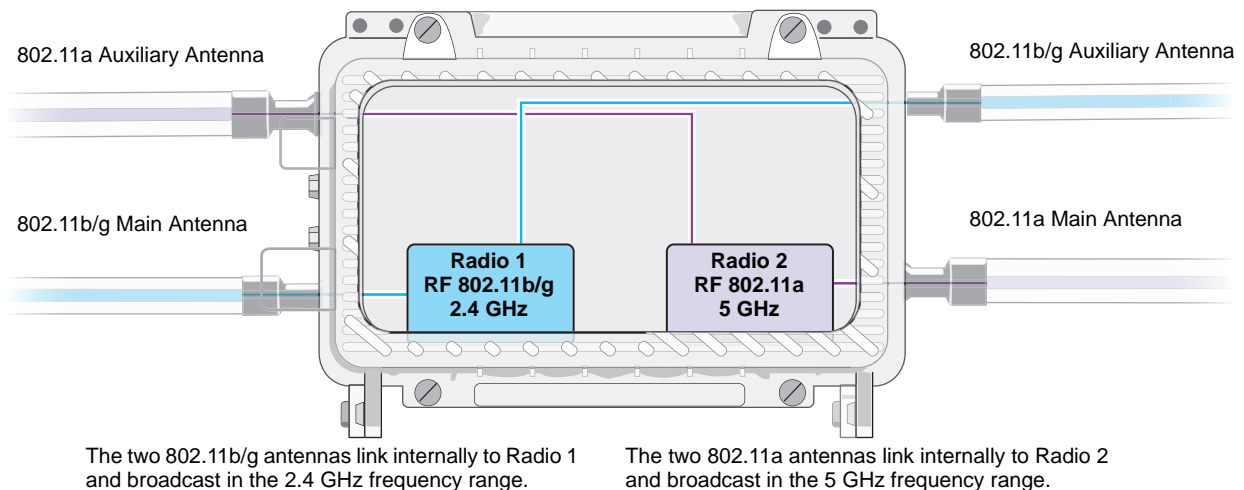
The omnidirectional antennas radiate equally in all directions, forming a toroidal pattern.



Note: To show the shape of radiation more clearly, this illustration depicts the coverage provided by only one active antenna and is not drawn to scale.

The pairs of antennas operate concurrently in two different frequency ranges: 2.4 GHz (IEEE 802.11b/g) and 5 GHz (IEEE 802.11a). Using two different frequency ranges reduces the probability of interference that can occur when numerous channels operate within the same range. Conceptually, the relationship of antennas and radios is shown in [Figure 4](#). (For information about attaching the antennas to the HiveAP 28, see ["Attaching Antennas"](#) on page 46.)

Figure 4 Antennas and radios



Note: The HiveAP 20 uses the `interface interface radio antenna external` command to enable an external antenna attached to it. Entering this command on the HiveAP 28 disables the antenna on the opposite side of the device from the radio to which the interface is linked and results in a loss of diversity.

MOUNTING THE HIVEAP 28 AND ATTACHING ANTENNAS

Using the mounting accessories (available separately) you can mount the HiveAP in various locations:

- ["Pole Mount" on page 43](#) - Mount the HiveAP 28 on a pole such as a street light.
- ["Strand Mount" on page 44](#) - Suspend the HiveAP 28 from a cable or phone line.
- ["Surface Mount" on page 45](#) - Mount the HiveAP 28 on a flat surface such as a wall or beam.

You can mount the HiveAP 28 in any of these locations as long as the object to which you mount it and the attaching screws can support its weight (9 lbs., 4.08 kg).

After mounting the HiveAP 28, attach the antennas as explained in ["Attaching Antennas" on page 46](#).

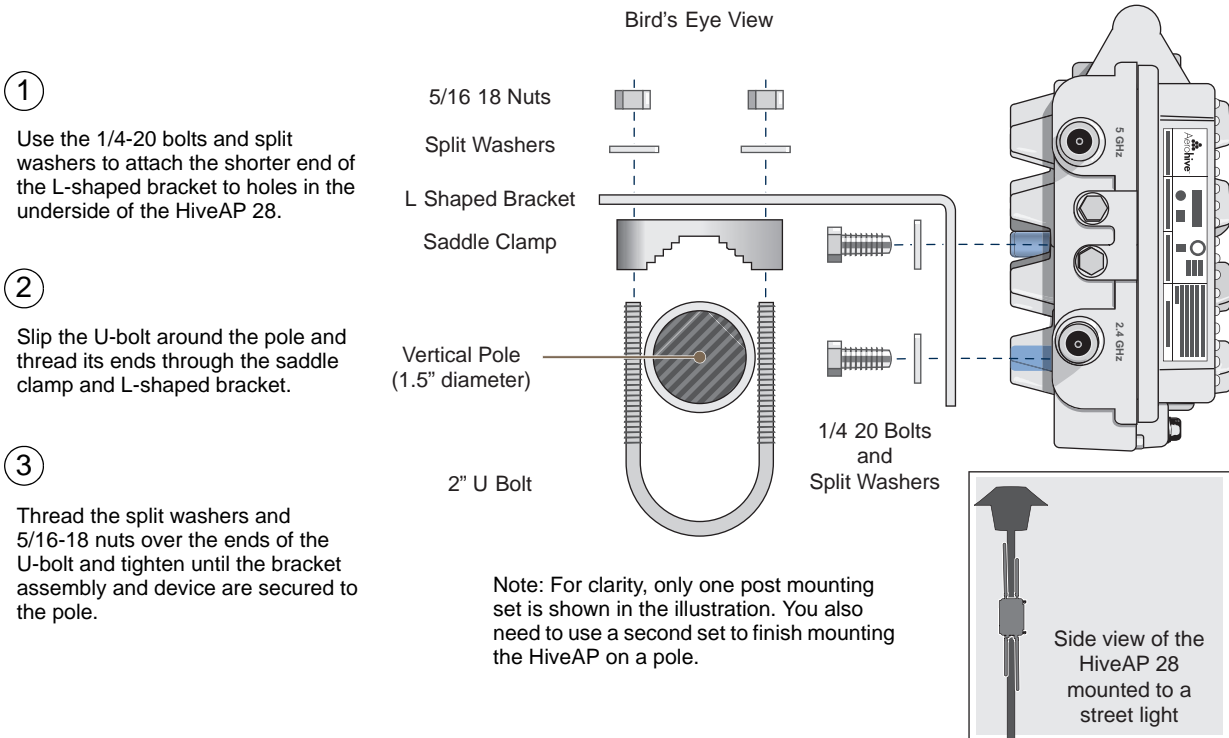
Before you mount the HiveAP 28 and attach antennas, read the following warnings and cautions:

- To install the HiveAP 28, you must be a qualified installation professional, licensed or certified in accordance with local regulations.
- Use lightning arrestors and ground both the HiveAP 28 and any separately mounted antennas.
- Do not connect or disconnect antennas or cables from the HiveAP 28 during periods of lightning activity.
- If you need to place the HiveAP 28 in an explosive environment, such as in an oil refinery, mine, or any place where there is flammable gas, it must first be encased in an ATEX enclosure.
- To comply with RF (radio frequency) exposure limits, do not place antennas within 6.56 feet (2 meters) of people.
- Do not locate antennas near overhead power lines or other electric light or power circuits, or where they can come into contact with such circuits. When installing antennas, take extreme care not to come into contact with these circuits, which might cause serious injury or death. For proper installation and grounding of the antenna, refer to national and local electrical codes: NFPA (National Fire Protection Association) 70, National Electrical Code Article 810 (U.S.); Canadian Electrical Code, Part I, CSA 22.1 and Section 54 (Canada); and if local or national electrical codes are not available, refer to IEC (International Electrotechnical Commission) 364, Part 1 through 7 (other countries).
- To prevent damage, avoid over-tightening the connectors, nuts, and screws used to mount the HiveAP 28 and antennas.

Pole Mount

To mount the HiveAP 28 to a pole with a 1.5-inch diameter, you need two sets of the L-shaped brackets, two 2" U-bolts, saddle clamps, and the nuts, bolts, and washers shown in [Figure 5](#). You also need a wrench to tighten the nuts and bolts securely.

Figure 5 Attaching the HiveAP 28 to a pole



1. Align two of the holes in the shorter end of the bracket with two of the holes in the HiveAP, insert the two bolts through the washers and bracket, and screw them into the holes in the HiveAP 28 chassis, using a wrench to tighten the bolts so that the bracket is securely attached.

Note: Repeat this step to attach the other bracket to the HiveAP. However, this time, place the long end of the bracket in the opposite direction of the first one for better stability. For example, if you attached the first bracket with its long end positioned toward the outside edge of the device, install this second bracket with the long end of the bracket toward the middle.

2. Holding a saddle clamp against the inside of the long end of one of the L-shaped brackets, slip a U-bolt around the pole and thread it through the two holes in the saddle clamp and L-shaped bracket.

Note: One of the holes in the bracket is arc-shaped so that you can adjust the angle of the mounted device if necessary.

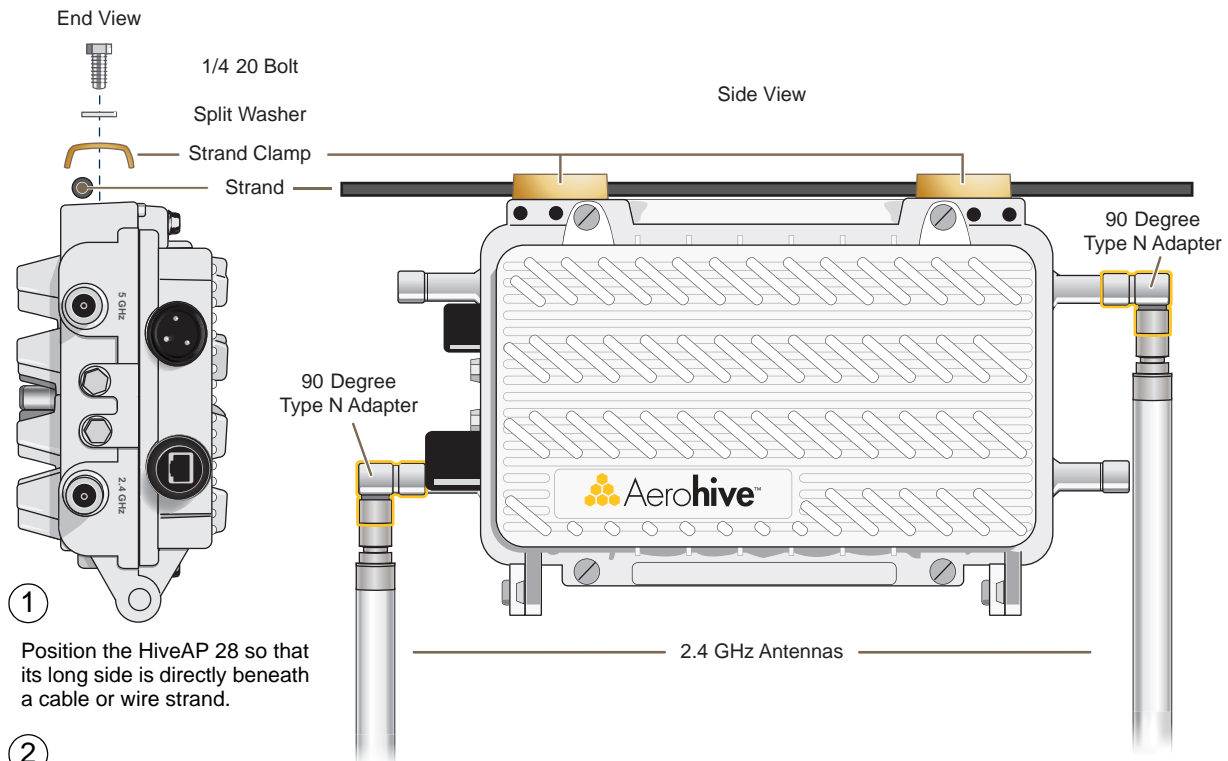
3. Thread a split washer and 5/16-18 nut to each end of the U-bolt, and tighten them with a wrench to secure the U-bolt firmly to the pole.

Note: Repeat steps 2 and 3 to attach the other U-bolt and saddle clamp to the remaining L-shaped bracket and secure the HiveAP 28 to the pole.

Strand Mount

The HiveAP 28 outdoor platform can also be mounted on a cable or strand of wire as shown in [Figure 6](#). When mounted on a wire strand, use 90-degree N type adapters (not included) to orient the antennas vertically. If you do not use the adapters and orient the antennas horizontally, the area covered will be far less.

Figure 6 Clamping the HiveAP 28 to a wire strand

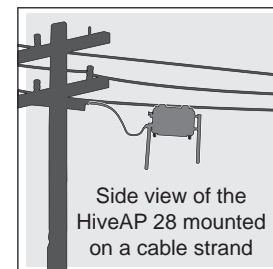


① Position the HiveAP 28 so that its long side is directly beneath a cable or wire strand.

② Place the strand clamps over the wire, and bolt the clamps tightly to the chassis around the strand.

③ Attach 90-degree type N adapters to the 2.4 GHz antenna connectors so that the adapters face downward, and then attach the antennas to the adapters

Note: For clarity, only one bolt, washer, and strand clamp are shown in the illustration on the left. You also need to use a second set of these items to finish clamping the HiveAP to a wire strand.



To mount the HiveAP 28 on a wire or strand, you need a wrench and two 1/4-20 bolts, split washers, strand clamps, and 90-degree type N adapters. In the following instructions, you use only the 2.4 GHz antennas.

1. Position the HiveAP 28 so that its long side (with three holes at each end) is underneath a cable or wire strand running lengthwise along the upper side of the chassis (for the proper orientation, see the inset in [Figure 6](#)).
2. Place the strand clamp over the wire and use the 1/4-20 bolt and split washer to secure the strand between the clamp and chassis.

Note: Repeat the preceding steps to fasten the other end of the HiveAP 28 to the cable or wire strand.

3. Attach the 90-degree type N adapters to the two 2.4 GHz antenna connectors and then attach the antennas to the adapters so that the antennas face downward. For details, see "[Attaching Antennas](#)" on page 46.

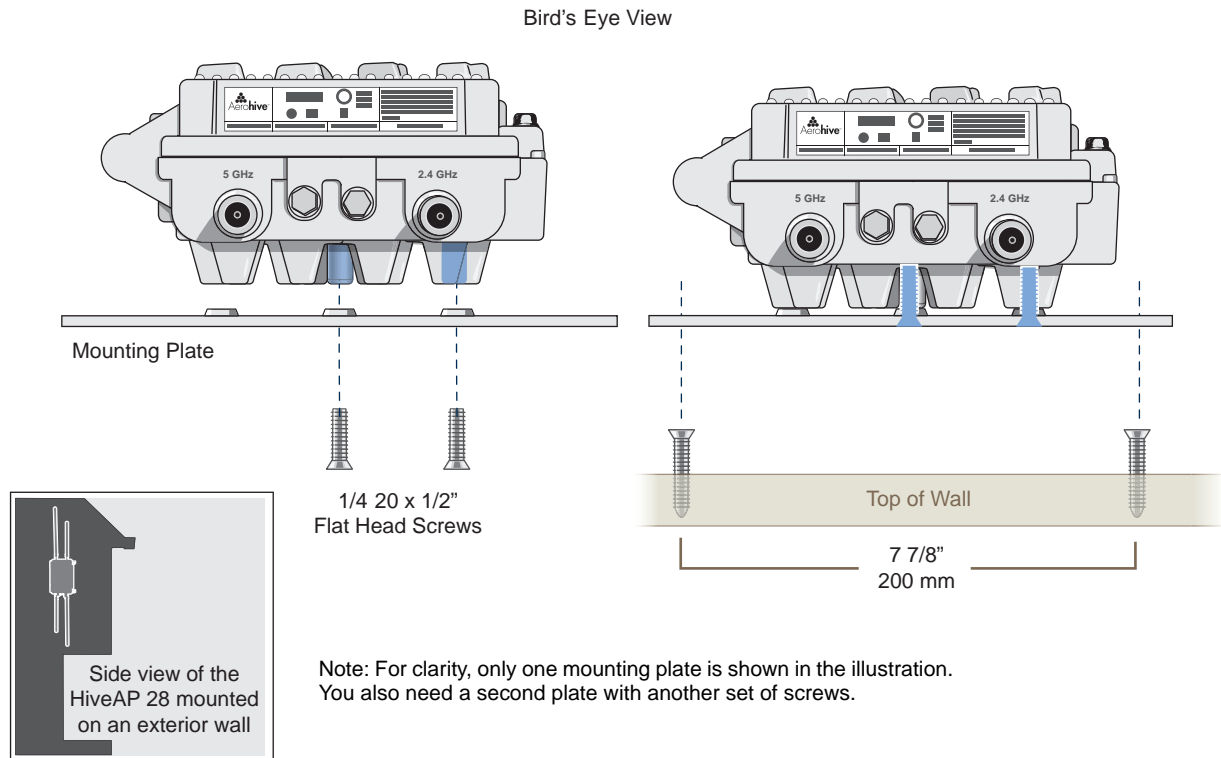
Surface Mount

You can use the mounting plate to attach the HiveAP 28 to any surface that supports its weight (9 lbs., 4.08 kg), and to which you can screw or nail the plate. First, mount the plate to the HiveAP 28, and then attach the plate to the surface, as shown in [Figure 7](#). Note that the screw heads that you attach to the wall or surface must be small enough for the keyholes on the mounting plate to slip over them.

Note: Because the metal in a wall can degrade the radio signal pattern, Aerohive recommends using sector antennas instead of omnidirectional antennas when mounting the device on a wall.

Figure 7 Mounting the HiveAP 28 on a wall

- ① With the ridged edge of the holes on the mounting plates facing the HiveAP 28, use 1/4-20 x 1/2 inch screws to secure the two mounting plates to its underside.
- ② Attach four screws to a secure object such as a wall or beam. Space them 8 1/8" (206 mm) apart vertically and 7 7/8" (200 mm) apart horizontally.
- ③ Guide the screws fastened to the wall through the keyholes in the mounting plates.



To mount the HiveAP 28 to a surface like a wall, you need two mounting plates, four 1/4-20 x 1/2" flat head screws, four screws (no bigger than 5/16"), and a screw driver:

1. Align the ridged edge of one of the mounting plates with two of the holes located on the underside of the HiveAP 28, and use two 1/4-20 x 1/2" flat head screws to secure the plate against the HiveAP 28. Then attach the other mounting plate to the HiveAP 28 in the same way.
2. Attach four 5/16" screws to a wall or beam. They must be 8 1/8" (206 mm) apart vertically and 7 7/8" (200 mm) apart horizontally to accommodate the keyholes on the mounting plates.
3. Guide the keyholes over the screws fastened to the wall and push downward after the screw heads have cleared the keyholes.

Attaching Antennas

You can connect the antennas directly to the HiveAP 28 or mount them separately. Although connecting the antennas directly to the device typically provides better performance, in some cases the location of the HiveAP might not be a good location for the antennas; for example, if the HiveAP 28 is mounted on a reinforced concrete wall that interferes with radio coverage. In such cases, mounting the antennas separately in a more open location can improve coverage; however, bear in mind that cables introduce loss into the overall signal strength and that the longer the cable connecting the antennas to the HiveAP 28, the greater the loss will be.

Note: Cover any unused antenna connectors with a connector cap to prevent water intrusion and possible safety hazards.

Connecting Antennas Directly to the HiveAP 28

The two 2.4 GHz and two 5 GHz antennas that ship with the HiveAP 28 have male Type N connectors that you can connect directly to the female Type N antenna connectors on the HiveAP 28. You can also use self-amalgamating PTFE (polytetrafluoroethylene) tape, which is available separately from Aerohive, to create a waterproof seal at the points of attachment.

To attach the antennas:

1. Remove the antenna connector covers from the HiveAP 28 (leave the covers on any connectors that you do not plan to use), and make sure that the surface of the connectors on the HiveAP 28 and the connectors on the antennas are clean.
2. If you are using PTFE tape, wrap the tape around the threads on the HiveAP 28 antenna connectors as follows:
 - 2.1. Starting at one end of the threads on one of the connectors, stretch the tape and wrap it in half-lap layers until you cover the threads completely.
 - 2.2. Wrap the tape in the opposite direction to bring it back onto itself for one full wrap.
 - 2.3. Place one thumb on the tape at the point of termination and stretch the tape until it breaks.
 - 2.4. Repeat the preceding steps to cover all the connectors to which you will attach antennas.
3. Connect the 2.4 GHz antennas to the 2.4 GHz antenna connectors. (To tighten an antenna, turn the antenna base cap—the textured metal band that encloses the connector—clockwise over the tape-covered threads of the HiveAP antenna connector.)

Their connections are now sealed and waterproof.

4. Repeat the preceding steps to connect the 5 GHz antennas.

Mounting Antennas Separately

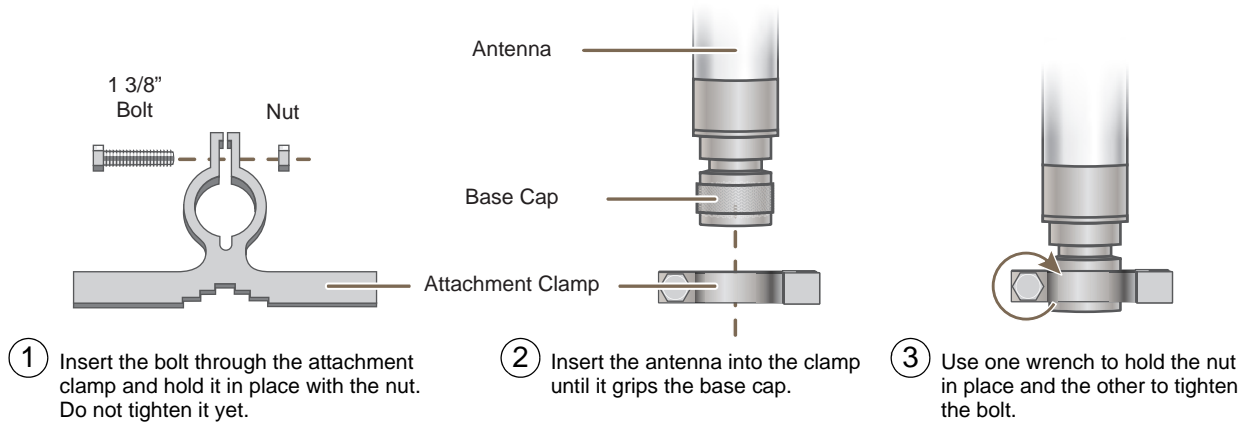
In addition to connecting antennas directly to the HiveAP 28, you can also mount them separately and run a cable between the antennas and the device. Use either male-to-female cables with Type N connectors or use male-to-male or female-to-female cables with cable gender changers. (The antennas have male Type N connectors and the HiveAP 28 has female Type N connectors.)

Note: Using cables to mount antennas separately causes some signal loss and using a cable gender changer can cause even more. The amount of loss varies from product to product, so refer to the documentation accompanying the cables and gender changer you use for information. To minimize loss, Aerohive recommends using LMR400 cables and using the shortest cables possible.

You can mount antennas at the top of a pole as shown in [Figure 8](#) and [Figure 9](#), or to a flat surface. If you must mount the antenna lower on a pole, the pole must be nonmetallic—such as one made from a hard plastic like PVC (polyvinyl chloride)—so that it does not distort the signal. Aerohive recommends that antennas be installed away from power lines and obstructions that can interfere with radio coverage.

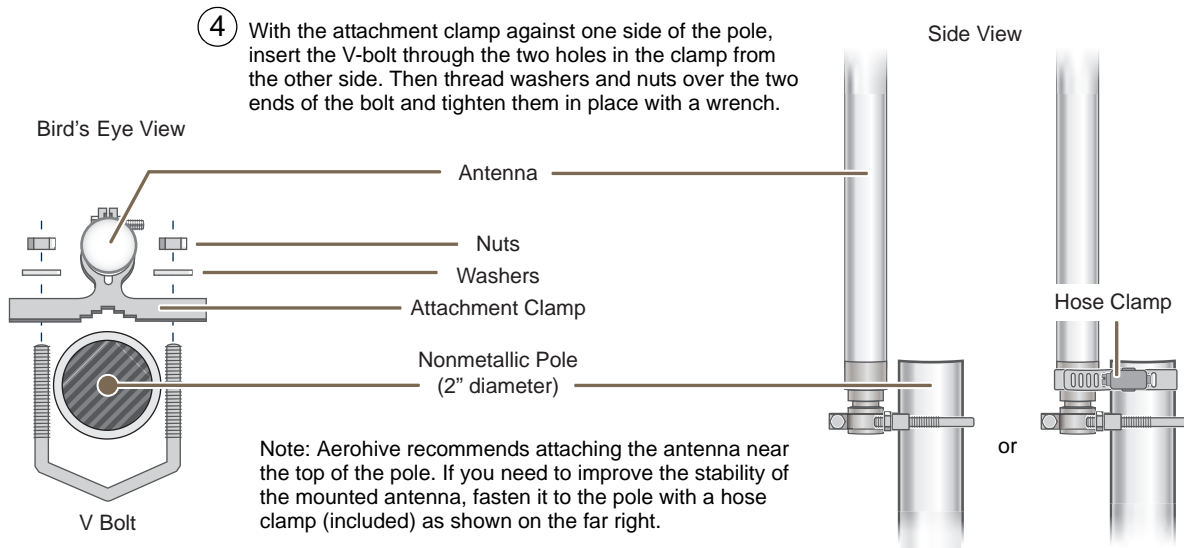
For each antenna that you mount, you need an attachment clamp, a 1 3/8" bolt and nut, a V-bolt, two washers and two nuts, a hose clamp, and two wrenches.

Figure 8 *Securing an antenna to an attachment clamp*



1. Insert the 1 3/8" bolt through the attachment clamp and screw a nut loosely onto its end.
2. Place the antenna base cap inside the attachment clamp.
3. Using a pair of wrenches, tighten the nut to the bolt until the clamp grips the base cap firmly.

Figure 9 *Mounting an antenna to a pole*



4. To mount the antenna on a nonmetallic pole, place the attachment clamp against the pole, thread the V-bolt through the holes on the attachment, the washers, and nuts, and use the wrenches to tighten the nuts to the bolt. (Optional) For added stability, fasten the top of the antenna to the pole with the hose clamp.

To mount the antenna directly to a flat surface, run bolts or screws (not included) through the two holes in the attachment clamp, and fasten them firmly to the surface.

Note: Radio coverage might be limited if the surface acts as an obstruction.

5. Make sure that all the antenna and cable connectors are clean. If you are using PTFE tape, wrap the tape around the threads on the HiveAP 28 antenna connectors as explained in ["Connecting Antennas Directly to the HiveAP 28" on page 46](#).
6. Assuming that you are using male-to-female cables, connect the female Type N connector on the cables to the male connectors on the antennas.
7. Connect the male Type N connectors on the cables to the female antenna connectors on the HiveAP 28.

DEVICE, POWER, AND ENVIRONMENTAL SPECIFICATIONS

Understanding the range of specifications for the HiveAP is necessary for optimal deployment and device operation. The following specifications describe the physical features and hardware components, the power adapter and PoE (Power over Ethernet) electrical requirements, and the temperature and humidity ranges in which the device can operate.

Device Specifications

- Chassis dimensions: 13 13/16" W x 4 3/8" H x 8 3/8" D (35 cm W x 11 cm H x 21 cm D)
- Weight: (9 lbs., 4.08 kg)
- Antennas: Two detachable single-band 8dBi 802.11b/g antennas and two detachable single-band 10dBi 802.11a antennas
- Maximum Transmission Power: 20 dBm
- Ethernet port: autosensing 10/100Base-T/TX Mbps, with IEEE 802.3af-compliant PoE (Power over Ethernet)

Power Specifications

- AC/DC power adapter:
 - Input: 100 - 240 VAC
 - Output: 17 watts
- PoE nominal input voltages: 48 V, 0.35A
- RJ-45 power input pins: Wires 4, 5, 7, 8 or 1, 2, 3, 6
- RF power output:

802.11b RF (8-dBi Omnidirectional Antenna, Model S2406BFNM)			
Frequency	2412 MHz	2437 MHz	2462 MHz
Peak Power Output (dBm)	14.20	14.00	14.20
802.11g RF (8-dBi Omnidirectional Antenna, Model S2406BFNM)			
Frequency	2412 MHz	2437 MHz	2462 MHz
Peak Power Output (dBm)	16.20	16.80	15.00
802.11a RF (10-dBi Omnidirectional Antenna, Model S4908WBF)			
Frequency	5745 MHz	5785 MHz	5825 MHz
Peak Power Output (dBm)	17.80	17.40	17.60

Environmental Specifications

- Operating temperature: -40 to 140 degrees F (-40 to 60 degrees C)
- Storage temperature: -40 to 194 degrees F (-40 to 90 degrees C)
- Relative Humidity: Maximum 100%

Chapter 4 The HiveAP 340 Platform

The Aerohive HiveAP 340 is a high-performance and highly reliable 802.11n wireless access point. The HiveAP 340 provides dual concurrent 802.11b/g/n and 802.11a/n radios for 3x3 MIMO (Multiple In, Multiple Out) and dual 10/100/1000 Ethernet ports for link aggregation or link redundancy. Its power management system uses a concept called smart PoE (Power over Ethernet) to adjust its power consumption automatically in response to the available power in different environments. Smart PoE supports the IEEE 802.3af standard and the 802.3at pre-standard.

This chapter covers the following topics relating to the HiveAP 340:

- ["HiveAP 340 Product Overview" on page 50](#)
 - ["Ethernet and Console Ports" on page 52](#)
 - ["Status LEDs" on page 56](#)
 - ["Antennas" on page 56](#)
- ["Mounting the HiveAP 340" on page 60](#)
 - ["Ceiling Mount" on page 61](#)
 - ["Plenum Mount" on page 63](#)
 - ["Suspended Mount" on page 66](#)
 - ["Surface Mount" on page 68](#)
- ["Device, Power, and Environmental Specifications" on page 69](#)

HIVEAP 340 PRODUCT OVERVIEW

The HiveAP 340 is a multi-channel wireless access point. It is compatible with IEEE 802.11b/g/n (2.4 GHz) and IEEE 802.11a/n (5 GHz) standards and supports a variety of Wi-Fi (wireless fidelity) security protocols, including WPA (Wi-Fi Protected Access) and WPA2.

You can see the hardware components on the HiveAP in [Figure 1](#). Each component is described in [Table 1](#).

Figure 1 HiveAP 340 hardware components

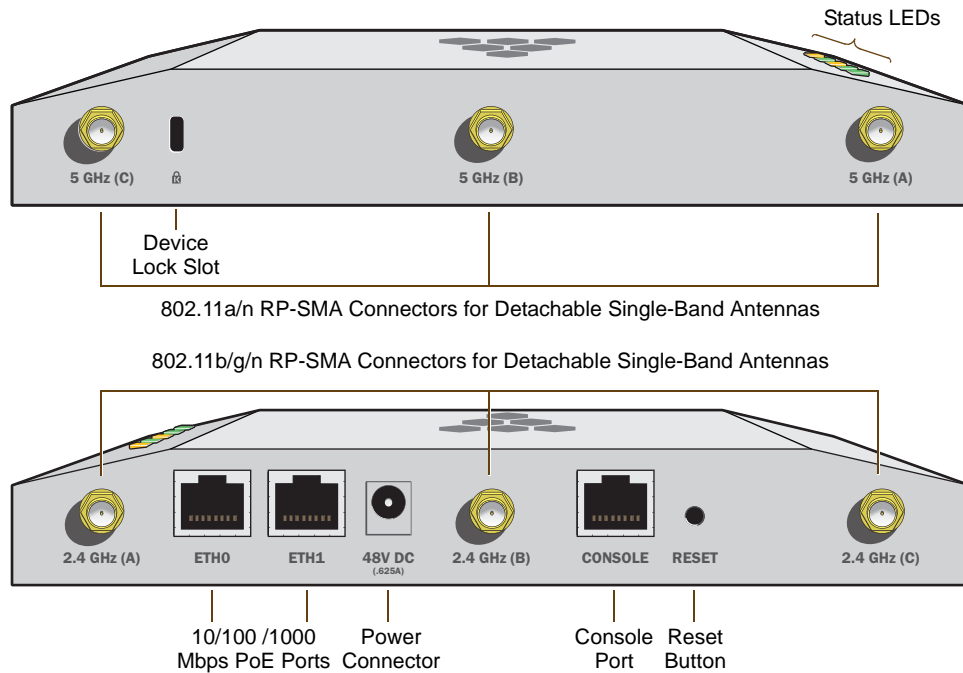


Table 1 HiveAP 340 component descriptions

Component	Description
Status LEDs	The status LEDs convey operational states for system power, firmware, Ethernet interfaces, and radios. For details, see "Status LEDs" on page 56 .
Device Lock Slot	You can physically secure the HiveAP by attaching a lock and cable (such as a Kensington® notebook lock) to the device lock slot or by using the lock adapter that is included in the mounting kit and a padlock. For more information, see "Locking the HiveAP 340" on page 62 .
802.11a/b/g/n RP-SMA Connectors	You can connect up to six detachable single-band antennas to the male 802.11a/b/g/n RP-SMA (reverse polarity-subminiature version A) connectors. Connect the longer antennas, which support 2.4 GHz frequencies (for IEEE 802.11b/g/n), to the connectors on the side panel with the Ethernet ports. Connect the shorter antennas, which support 5 GHz frequencies (for IEEE 802.11a/n), to the connectors on the side panel with the device lock slot. For details, see "Antennas" on page 56 .

Component	Description
10/100/1000 Mbps PoE Ports	<p>The two 10/100/1000-Mbps Ethernet ports—ETH0 and ETH1—support IEEE 802.3af and 802.3at PoE (Power over Ethernet) and receive RJ-45 connectors. The HiveAP can receive power through one or both Ethernet connections from PSE (power sourcing equipment) that is compatible with the 802.3af standard and the forthcoming 802.3at standard, such as one of the PoE injectors available as an optional accessory from Aerohive. (If you connect the HiveAP to a power source through the power connector and PoE ports simultaneously, the device draws power through the power connector and automatically disables PoE.)</p> <p>You can configure ETH0 and ETH1 as two individual Ethernet interfaces, combine them into an aggregate interface to increase throughput, or combine them into a redundant interface to increase reliability. You can connect the HiveAP 340 to a wired network or to a wired device (such as a security camera) through these ports using bridging. They are compatible with 10/100/1000Base-T/TX and automatically negotiate half- and full-duplex connections with the connecting device. They are autosensing and adjust to straight-through and cross-over Ethernet cables automatically. For details, see "Ethernet and Console Ports" on page 52.</p>
Power Connector	<p>The 48-volt DC power connector (0.625 amps) is one of two methods through which you can power the HiveAP 340. To connect it to a 100 - 240-volt AC power source, use the AC/DC power adaptor that is available as an extra option. Because the HiveAP does not have an on/off switch, connecting it to a power source automatically powers on the device.</p>
Console Port	<p>You can access the CLI by making a serial connection to the RJ-45 console port. The management station from which you make a serial connection to the HiveAP must have a VT100 emulation program, such as Tera Term Pro[®] (a free terminal emulator) or Hilgraeve Hyperterminal[®] (provided with Windows[®] operating systems). The following are the serial connection settings: bits per second: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none. For details, see "Ethernet and Console Ports" on page 52.</p>
Reset Button	<p>The reset button allows you to reboot the device or reset the HiveAP to its factory default settings. Insert a paper clip, or something similar, into the Reset pinhole and press the reset button. To reboot the device, hold the button down between 1 and 5 seconds. To return the configuration to the factory default settings, hold it down for at least 5 seconds. After releasing the button, the Power LED goes dark as the system reboots. Then it pulses green while the firmware loads and the system performs a self-test. After the software finishes loading, the Power LED glows steady green.</p> <p>To disable the reset button from resetting the configuration, enter this command: no reset-button reset-config-enable Pressing the button between 1 and 5 seconds will still reboot the HiveAP, but pressing it for more than 5 seconds will not reset its configuration.</p>

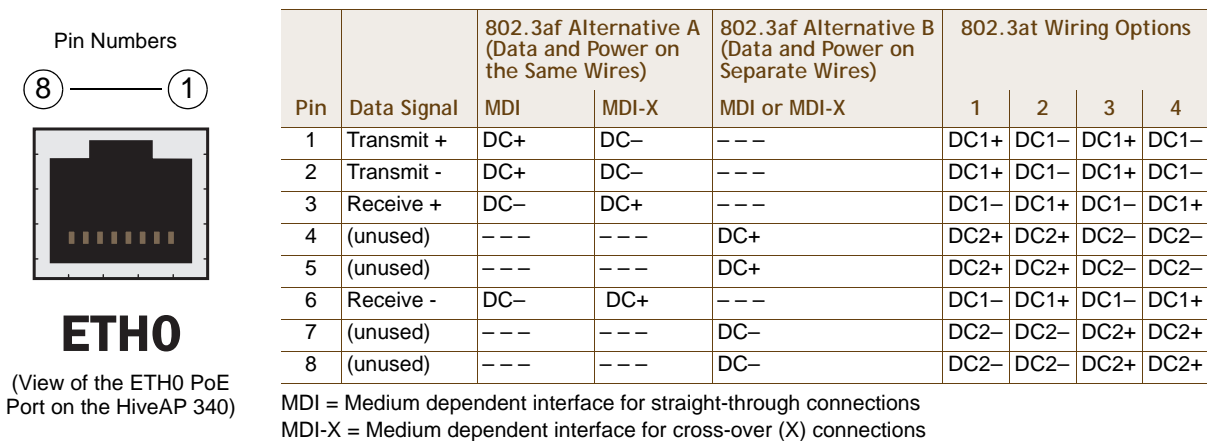
Note: The rear surface of the HiveAP 340 is used for heat dissipation to reduce the internal temperature. Consequently, it can become hot, so use caution when handling it.

Ethernet and Console Ports

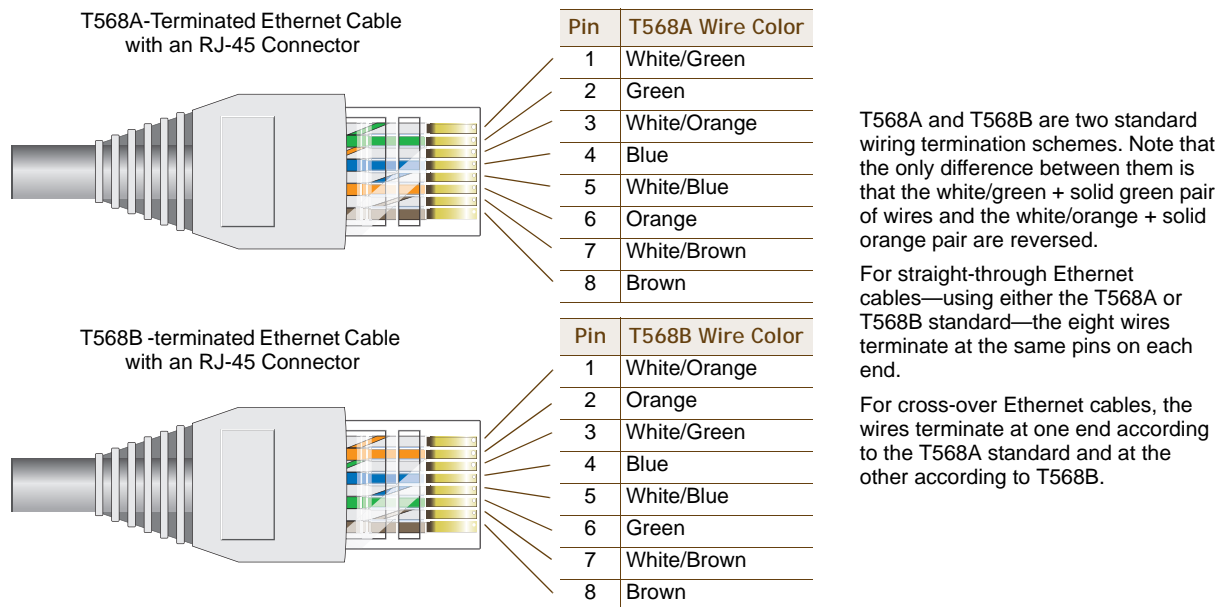
There are three ports on the HiveAP 340: two RJ-45 10/100/1000Base-T/TX Ethernet ports and an RJ-45 console port.

The pin assignments in the PoE (Power over Ethernet) Ethernet ports follow the TIA/EIA-568-B standard (see [Figure 2](#)). The ports accept standard types of Ethernet cable—cat3, cat5, cat5e, or cat6—and can receive power over this cable from power sourcing equipment (PSE) that is 802.3af-compatible. If you use cat5, cat5e, or cat6 cables, the HiveAP 340 can also support 802.3at-compliant PSE. Such equipment can be embedded in a switch or router, or it can come from purpose-built devices that inject power into the Ethernet line en route to the HiveAP. Because the PoE ports have autosensing capabilities, the wiring termination in the Ethernet cable can be either straight-through or cross-over.

Figure 2 PoE wire usage and pin assignments



The PoE ports are auto-sensing and can automatically adjust to transmit and receive data over straight-through or cross-over Ethernet connections. Likewise, they can automatically adjust to 802.3af Alternative A and B power delivery methods. Furthermore, when the Alternative A method is used, the ports automatically allow for polarity reversals depending on their role as either MDI or MDI-X. In 802.3at, the 1/2 and 3/6 wire pairs connect to DC source 1 and 4/5 and 7/8 pairs to DC source 2 in PSE. Although the exact polarity depends on the PSE design, the HiveAP 340 Ethernet ports can support all possible options.



Smart PoE

The HiveAP 300 series applies the Aerohive concept of smart PoE to adjust power consumption as necessitated by varying levels of available power. No adjustments are needed when the power level is 20 W (watts) or higher. If the available power drops to a range between 18 and 20 W, the HiveAP disables the ETH1 interface. If the level drops to the 15 - 18 W range, it then switches from 3x3 MIMO (Multiple In, Multiple Out) to 2x3 (see ["MIMO" on page 57](#)). In rare cases when the power drops between 13.6 and 15 W and further power conservation is necessary, the HiveAP reduces the speed on ETH0 from 10/100/1000 Mbps to 10/100 Mbps. Finally, in the event that there is a problem with the PoE switch or Ethernet cable and the power falls between 0 and 13.6 W, the HiveAP disables its wireless interfaces and returns its ETH0 and ETH1 interfaces to 10/100/1000 Mbps speeds. Through the application of smart PoE, the HiveAP 340 can make power usage adjustments so that it can continue functioning even when the available power level drops.

Aggregate and Redundant Interfaces

By default ETH0 and ETH1 act as two individual Ethernet interfaces. When both interfaces are connected to the network and are in backhaul mode, the HiveAP transmits broadcast traffic only through ETH0. The HiveAP transmits broadcast traffic through ETH1 only when ETH0 does not have network connectivity. When both Ethernet interfaces are connected to the network and are in access mode, then the HiveAP transmits broadcast traffic through all the access interfaces: ETH0, ETH1, and all wireless subinterfaces in access mode.

In addition to using ETH0 and ETH1 as individual interfaces, you can combine them into an aggregate interface (agg0) to increase throughput, or combine them into a redundant interface (red0) to increase reliability. The logical red0 and agg0 interfaces support all the settings that you can configure for Ethernet interfaces except those pertaining to physical link characteristics such as link speed. See the sections below for configuration information.

Aggregate Interface

You can increase throughput onto the wired network by combining ETH0 and ETH1 into a single logically aggregated interface called "agg0". The aggregate interface effectively doubles the bandwidth that each physical interface has when used individually. In this configuration, both Ethernet ports actively forward traffic, the HiveAP applying an internal scheduling mechanism based on the source MAC address of each packet to send traffic through the aggregate member interfaces. To configure an aggregate interface, enter the following commands:

```
interface eth0 bind agg0
interface eth1 bind agg0
```

In addition to configuring the HiveAP, you must also configure the connecting switch to support EtherChannel. For example, the following commands bind two physical Ethernet ports—0/1 and 0/2—to the logical interface port-channel group 1 on a Cisco Catalyst 2900 switch running Cisco IOS 12.2:

```
Switch#conf t

Switch(config)#interface port-channel 1
Switch(config-if)#switchport mode access
Switch(config-if)#spanning-tree portfast
Switch(config-if)#exit

Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#channel-group 1 mode on
Switch(config-if)#spanning-tree portfast
Switch(config-if)#exit
```

```
Switch(config)#int fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#channel-group 1 mode on
Switch(config-if)#spanning-tree portfast
Switch(config-if)#exit
Switch(config)#exit

Switch#wr mem
```

Finally, you must cable the Cisco switch and the HiveAP together: Cisco 0/1 to HiveAP eth0, and Cisco 0/2 to HiveAP eth1.

Redundant Interface

If a single Ethernet link provides sufficient bandwidth and speed, such as a 1000 Mbps link, but you want to ensure link redundancy, you can connect the two Ethernet ports to the same switch—or to two different switches—and configure them to act as a redundant interface called "red0". In this mode, only one Ethernet interface is actively forwarding traffic at any one time. If eth0 is active and eth1 is passive and eth0 loses its connection, the HiveAP switches over to eth1. To configure a redundant interface, enter the following commands:

```
interface eth0 bind red0 primary
interface eth1 bind red0
```

The interface that you specify as primary is the one that the HiveAP uses when both interfaces have network connectivity. Because the HiveAP uses eth0 as the primary interface by default, it is unnecessary to specify "primary" in the first command above. However, it is included to make the role of eth0 as the primary interface obvious.

Note: No extra configuration is necessary on the connecting switch or switches to support a redundant interface.

Interface Selection for the Default Route

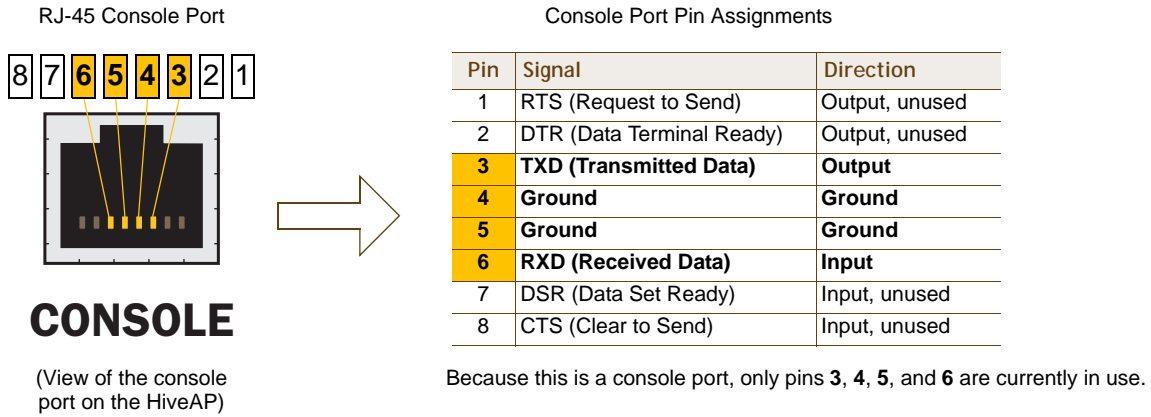
In cases where there are multiple active interfaces in backhaul mode, the HiveAP uses the following logic to choose which interface to use in its default route:

- If there is an Ethernet interface and a wireless interface in backhaul mode, the HiveAP uses the Ethernet interface in its default route.
- If there are multiple Ethernet interfaces in backhaul mode, the HiveAP chooses which one to use in its default route in the following order:
 - It uses red0 or agg0 if one of them has at least one member interface bound to it and its link state is UP.
 - It uses ETH0 if neither red0 nor agg0 has any member interfaces and the link state for ETH0 is UP.
 - It uses ETH1 if neither red0 nor agg0 has any member interfaces, the link state for ETH0 is DOWN, and the link state for ETH1 is UP.

Console Port

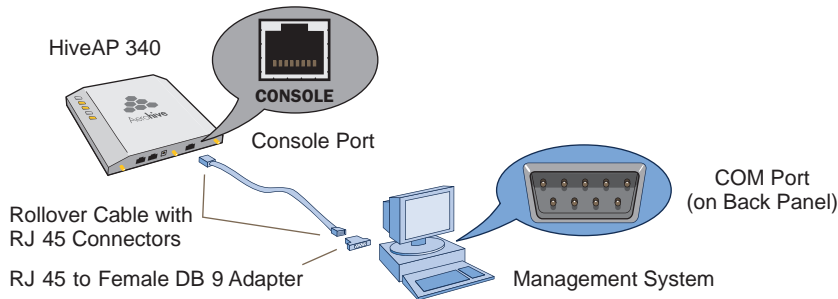
The pin-to-signal mapping in the RJ-45 console port is shown in [Figure 3](#).

Figure 3 Console port pin assignments



To make a serial connection between your management system and the HiveAP, you can use the console cable that is available as an extra accessory. Insert the RJ-45 connector into the HiveAP 340 console port, and attach the DB-9 connector to the serial (or COM) port on your management system. The management system must have a VT100 terminal emulation program, such as Tera Term Pro[®] (a free terminal emulator) or Hilgraeve Hyperterminal[®] (provided with Windows[®] operating systems). If you want to make your own serial cable and adapter, refer to [Figure 3](#).

Figure 4 Wiring details for making a serial cable with an RJ-45-to-Female DB-9 adapter



Console Port (HiveAP 340)	RJ-45-to-RJ-45 Rollover Cable		RJ-45-to-Female DB-9 Adapter		Management System
Signal	RJ-45 Pin	RJ-45 Pin	RJ-45 Pin	DB-9 Pin	Signal
RTS (Request to Send)	1	8	1	8	CTS (unused)
DTR (Data Terminal Ready)	2	7	2	6	DSR (unused)
TXD (Transmitted Data)	3	6	3	2	RXD
Ground	4	5	4	5	Ground
Ground	5	4	5	5	Ground
RXD (Received Data)	6	3	6	3	TXD
DSR (Data Set Ready)	7	2	7	4	DTR (unused)
CTS (Clear to Send)	8	1	8	7	RTS (unused)
-	-	-	-	9	RI (Ring Indicator, unused)

Status LEDs

The five status LEDs on the top of the HiveAP 340 indicate various states of activity through their color (dark, green, amber, and red) and illumination patterns (steady glow or pulsing). The meanings of the various color + illumination patterns for each LED are explained below.

Power

- Dark: No power
- Steady green: Powered on and the firmware is running normally
- Pulsing green: Firmware is booting up
- Steady amber: Firmware is being updated
- Pulsing amber: Alarm indicating a firmware issue has occurred
- Steady red: Alarm indicating a hardware issue has occurred

ETH0 and ETH1

- Dark: Ethernet link is down or disabled
- Steady green: 1000 Mbps Ethernet link is up but inactive
- Pulsing green: 1000 Mbps Ethernet link is up and active
- Steady amber: 10/100 Mbps Ethernet link is up but inactive
- Pulsing amber: 10/100 Mbps Ethernet link is up and active

WIFI0 and WIFI1

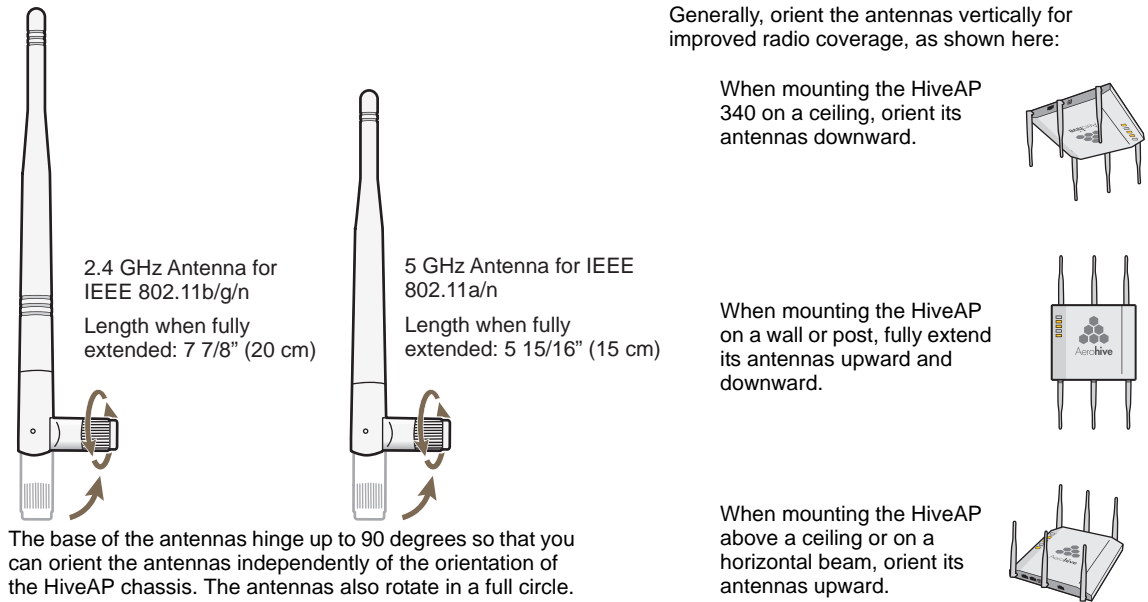
- Dark: Wireless interface is disabled
- Steady green: Wireless interface is in access mode but inactive
- Pulsing green: Wireless interface is in access mode and active
- Steady amber: Wireless interface is in backhaul mode but inactive
- Pulsing amber: Wireless interface is in backhaul mode and is connected with other hive members
- Alternating green and amber: Wireless interface is in backhaul mode and is searching for other hive members

Antennas

Antennas are an integral part of the HiveAP 340. The HiveAP 340 can accept up to six detachable dipole antennas. The three shorter antennas are designed for the 5 GHz band and have a 2-dBi gain. The three longer antennas are designed for the 2.4 GHz band and have a 4.9-dBi gain. These antennas are omnidirectional, providing fairly equal coverage in all directions in a toroidal (donut-shaped) pattern around each antenna (see [Figure 4 on page 32](#)). For greater coverage on a horizontal plane, it is best to orient the antennas vertically. So that you can easily do that whether the HiveAP chassis is mounted horizontally or vertically, the antennas hinge and swivel (see [Figure 5 on page 57](#).)

Although hive members automatically adjust their signal strength according to their environments, you can resize the area of coverage by increasing or decreasing the signal strength manually by entering the `interface { wifi0 | wifi1 } radio power <number>` command, where <number> can be from 1 to 20 and represents a value in dBm.

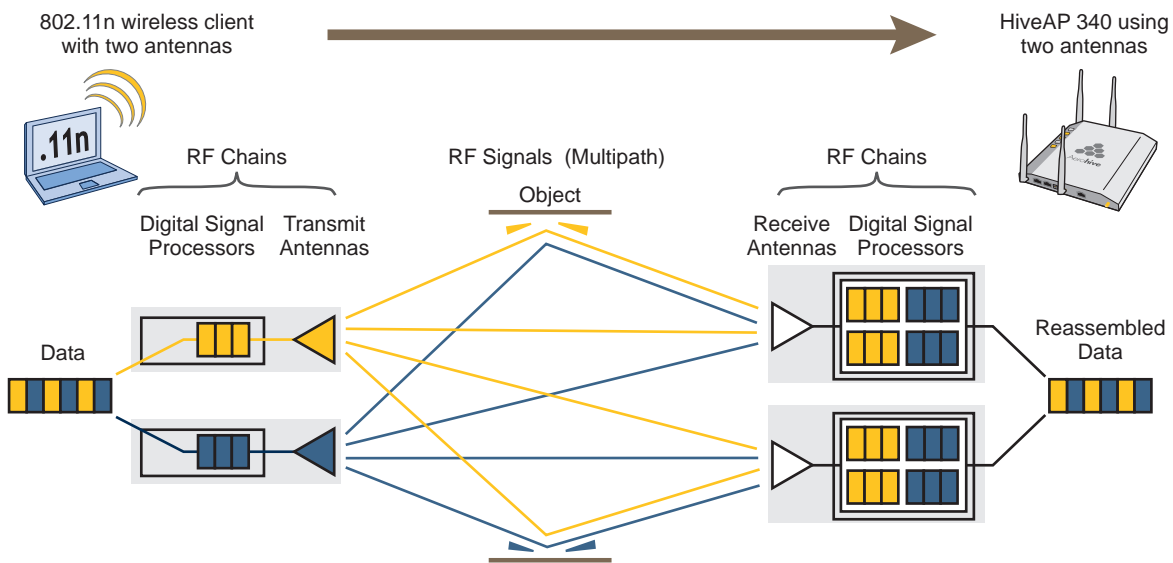
Figure 5 HiveAP 340 antennas



MIMO

MIMO (Multiple In, Multiple Out) is a major WLAN advancement introduced in the IEEE 802.11n standard in which multiple RF links are formed on the same channel between the transmitter and receiver simultaneously. To accomplish this, the transmitter separates a single data stream into multiple spatial streams, one for each RF chain (an antenna + various digital signal processing modules linked to the antenna). The transmit antennas at the end of each RF chain then transmit their spatial streams. The recipient's receive antennas obtain streams from all the transmit antennas. In fact, due to multipath, they receive multiple streams from each transmit antenna. The receive antennas pass the spatial streams to the digital signal processors in their RF chains, which take the best data from all the spatial streams and reassemble them into a single data stream once again (see Figure 6).

Figure 6 2x2 MIMO (2 transmit antennas x 2 receive antennas)



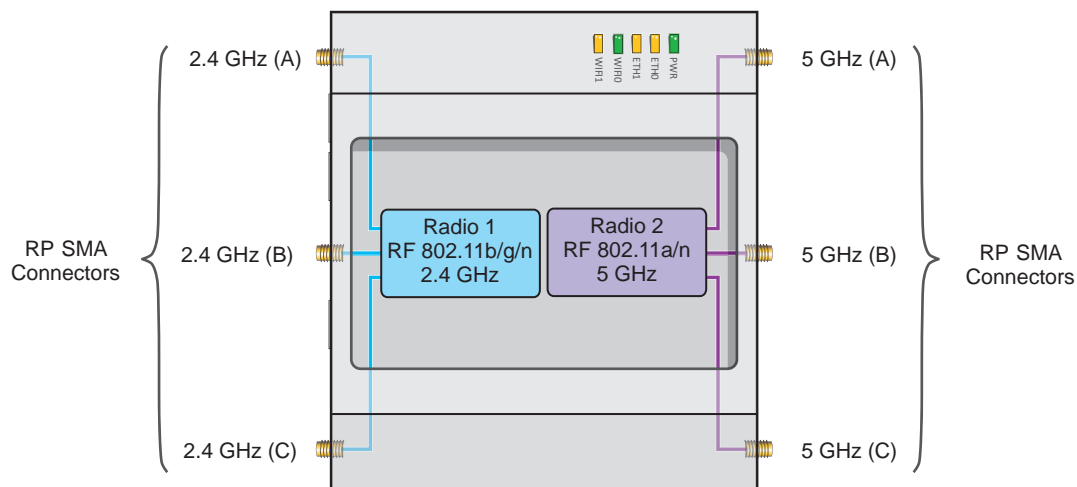
In previous 802.11 standards, access points and clients each employed a single set of components, or RF chain, for transmitting or receiving. Although two antennas are often used for diversity, only the one with the best signal-to-noise ratio is used at any given moment, and that antenna makes use of the single RF chain while the other antenna remains inactive. A significant improvement that MIMO introduces is to permit each antenna to have its own RF chain and for all antennas to function simultaneously. For the HiveAP 340, you can connect up to three antennas per radio and configure the radio to use two or three transmit chains and two or three receive chains.¹ Using two or three transmit and receive chains simultaneously increases the amount of data that can flow across the WLAN and accelerates the processing of that data at each end of the wireless link.

Another major aspect of MIMO is how it turns multipath signals from a curse to a boon. As a radio signal moves through space, some objects reflect it, others interfere with it, and still others absorb it. The receiver can end up receiving multiple copies of the original signal, all kind of muddled together. However, the digital signal processors in the multiple receive chains are able to combine their processing efforts to sort through all the received data and reconstruct the original message. Furthermore, because the transmitter makes use of multiple RF chains, there is an even richer supply of signals for the receive chains to use in their processing. To set the transmit and receive RF chains for a radio profile, enter the following commands:

```
radio profile <name> transmit-chain { 2 | 3 }
radio profile <name> receive-chain { 2 | 3 }
```

There are two sets of antennas—three antennas per set—that operate concurrently in two different frequency ranges: 2.4 GHz (IEEE 802.11b/g/n) and 5 GHz (IEEE 802.11a/n). Using two different frequency ranges reduces the probability of interference that can occur when numerous channels operate within the same range. Conceptually, the relationship of antennas and radios is shown in [Figure 7](#).

Figure 7 Antennas and radios



Cut-away view of the HiveAP 340 to show the relationship of the antennas and the two internal radios

The wlan0 interface links to radio 1 (frequency range = 2.4 GHz for IEEE 802.11b/g), and the wlan1 interface links to radio 2 (frequency range = 5 GHz for IEEE 802.11a). These interface-to-radio relationships are permanent.

When deciding how many antennas to use, consider the types of wireless clients—802.11n only, 802.11g/n, 802.11b/g/n, or 802.11a/n—the area needing coverage, and the RF environment.

1. The convention for presenting the configuration of transmitting and receiving MIMO RF chains is TxR. For example, a HiveAP 340 radio functioning in access mode might be configured to use two RF chains for transmitting and three for receiving. In that case, its configuration can be presented as "2x3". In general, the number of receive antennas is equal to or greater than the number of transmit antennas.

Using MIMO with Legacy Clients

In addition to supporting up to 300-Mbps throughput per radio for 802.11n clients, MIMO (Multiple In, Multiple Out) can improve the reliability and speed of legacy 802.11a/b/g client traffic. When an 802.11a/b/g access point does not receive acknowledgement that a frame it sent was received, it resends that frame, possibly at a somewhat lower transmission rate. If the access point must continue resending frames, it will continue lowering its transmission rate. As a result, clients that could get 54-Mbps throughput in an interference-free environment might have to drop to 48- or 36-Mbps speeds due to multipath interference. However, because MIMO technology makes better use of multipath, an access point using MIMO can continue transmitting at 54 Mbps, or at least at a better rate than it would in a pure 802.11a/b/g environment, thus improving the reliability and speed of 802.11a/b/g client traffic.

Although 802.11a/b/g client traffic can benefit somewhat from an 802.11n access point using MIMO, supporting such legacy clients along with 802.11n clients can have a negative impact on 802.11n client traffic. Legacy clients take longer to send the same amount of data as 802.11n clients. Consequently, legacy clients consume more airtime than 802.11n clients do, causing greater congestion in the WLAN and reducing 802.11n performance.

By default, the HiveAP 340 supports 802.11a/b/g clients. You can restrict access only to clients using the IEEE 802.11n standard. By only allowing traffic from clients using 802.11n, you can increase the overall bandwidth capacity of the access point so that there will not be an impact on 802.11n clients during times of network congestion. To do that, enter the following command:

```
radio profile <string> 11n-clients-only
```

You can also deny access just to clients using the IEEE 802.11b standard, which has the slowest data rates of the three legacy standards, while continuing to support 802.11a and 802.11g clients. To do that, enter the following command:

```
no radio profile <string> allow-11b-clients
```

By blocking access to 802.11b clients, their slower data rates cannot clog the WLAN when the amount of wireless traffic increases.

MOUNTING THE HIVEAP 340

Using the mounting plate and track clips, you can mount the HiveAP 340 to the tracks of a dropped ceiling grid. Using just the mounting plate, you can mount the HiveAP to any surface that can support its weight (3.3 lb., 1.5 kg).

This document covers the following methods for mounting the Aerohive® HiveAP® 340:

- ["Ceiling Mount" on page 61](#) - Using the mounting plate and track clips, you can mount the HiveAP 340 to the tracks of a dropped ceiling grid so that it is suspended upside down against the ceiling.
- ["Plenum Mount" on page 63](#) - Using the mounting plate, hanger clip, and hanger frame, you can mount it in the plenum above a dropped ceiling.
- ["Suspended Mount" on page 66](#) - Using the mounting plate, cable, quad-toggle, and locking device, you can suspend the device from a beam, bracket, or any object that can support its weight (3.3 lb., 1.5 kg)
- ["Surface Mount" on page 68](#) - Using just the mounting plate and some screws or nails, you can mount the HiveAP directly to any surface that can support its weight.

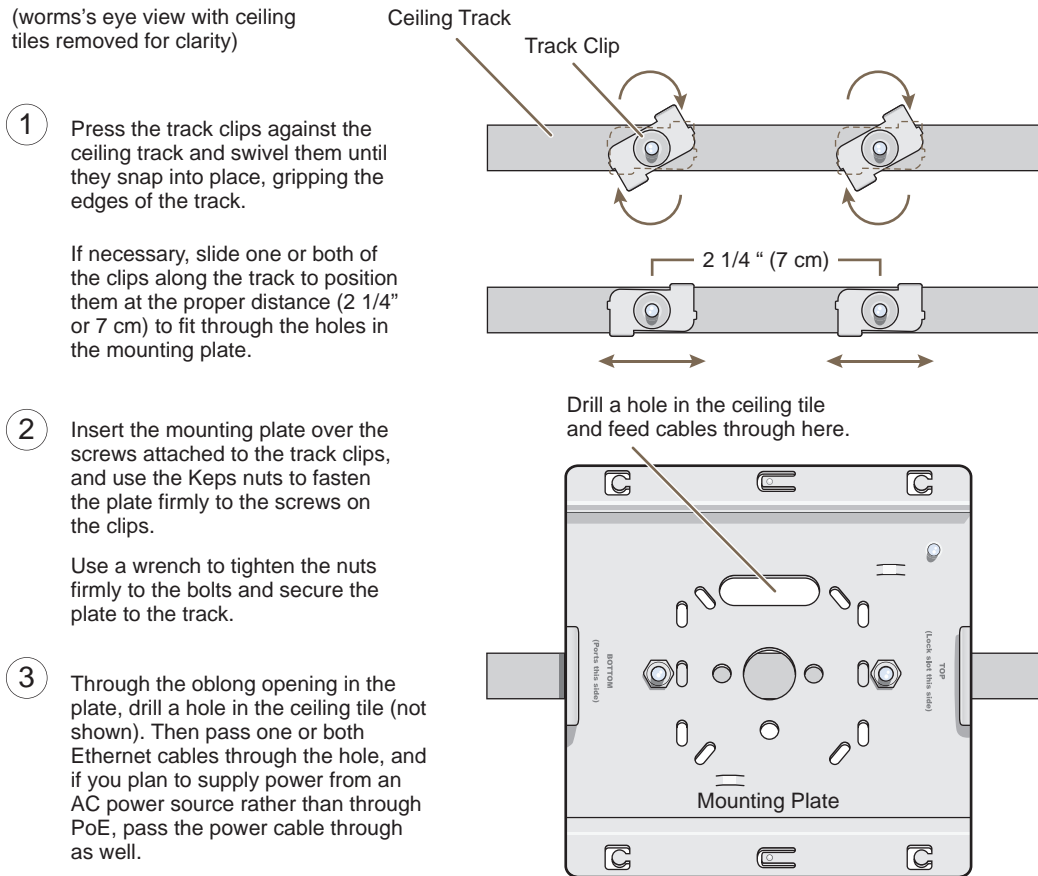
Note: In addition to these methods, you can also mount the HiveAP 340 on a table using the set of four rubber feet that ship with the product. Simply peel the rubber feet off the adhesive sheet and press them against the underside of the HiveAP in its four corners.

Ceiling Mount

To mount the HiveAP 340 to a standard 1"-wide track in a dropped ceiling, you need the mounting plate, two track clips, and two Keps nuts that ship with the HiveAP 340. You also need a drill, a wrench, and—most likely—a ladder.

Nudge the ceiling tiles slightly away from the track to clear some space. Attach the track clips to the ceiling track, and then fasten the mounting plate to the clips, as shown in [Figure 8](#). When you have the mounting plate in the correct location, cut or drill a hole in the ceiling through which you can then pass the Ethernet and power cables.

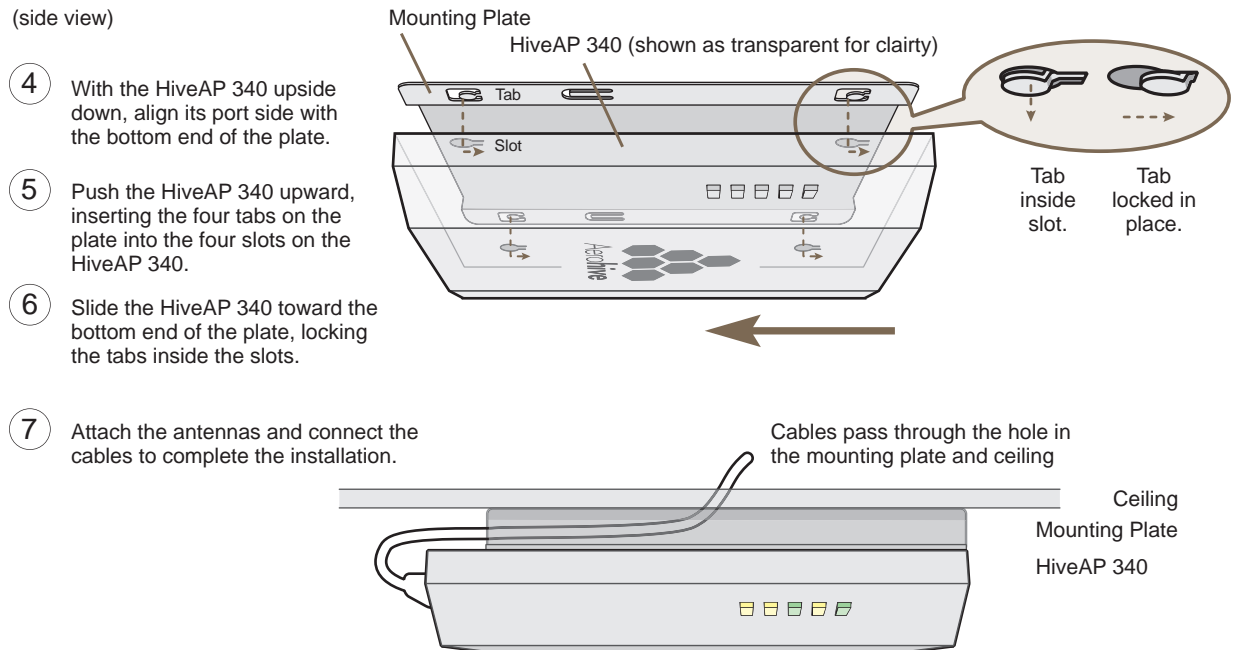
Figure 8 Attaching the track clips and mounting plate to the ceiling track



Attach the HiveAP 340 to the mounting plate and connect the cables, as shown in [Figure 9](#) on page 62.

Note: You can tie the cables to the tie points (small arched strips) on the mounting plate to prevent them from being pulled out of their connections accidentally.

Figure 9 Attaching the HiveAP 340 to the mounting plate and connecting cables



When done, adjust the ceiling tiles back into their former position.

Locking the HiveAP 340

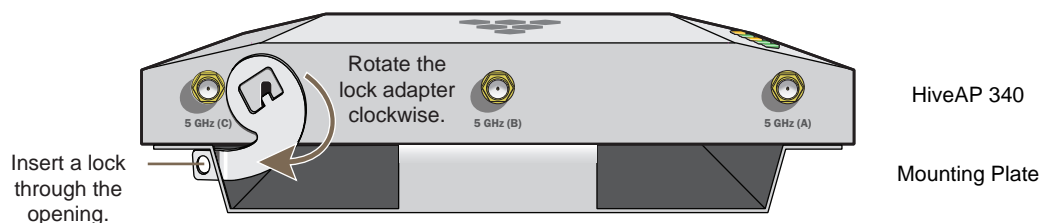
To lock the HiveAP 340 to the mounting plate, use either a Kensington lock or the lock adapter that is included with the mounting kit and a small padlock (not included).

To use a Kensington lock, loop the cable attached to the lock around a secure object, insert the T-bar component of the lock into the device lock slot on the HiveAP, and then turn the key to engage the lock mechanism.

To use the lock adapter :

1. Insert the T-shaped extension on the adapter into the device lock slot, and rotate it clockwise so that the curved section extends through the slot in the mounting plate (see [Figure 10](#)).

Figure 10 Locking the HiveAP 340 to the mounting plate



2. Link a padlock through the opening in the adapter and engage the lock to secure the HiveAP 340 to the mounting plate. The opening is 1/8" (0.3 cm) in diameter at its narrowest.

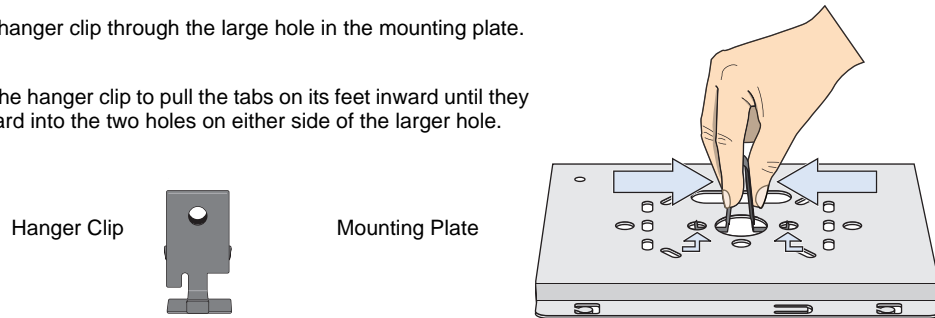
Plenum Mount

To mount the HiveAP 340 in the plenum space above a dropped ceiling grid, you need the mounting plate, hanger clip, and a standard 24"-wide hanger frame, which can be ordered separately (SKU# AH-ACC-BKT-PLENUM).

1. With the recessed side of the mounting plate facing downward, insert the hanger clip through the large hole in the center of the plate.
2. Squeeze the clip until the projecting tabs at the ends of its two feet snap into the smaller holes on both sides of the larger hole (see [Figure 11](#)).

Figure 11 Fitting the hanger clip to the mounting plate

- ① Insert the hanger clip through the large hole in the mounting plate.
- ② Squeeze the hanger clip to pull the tabs on its feet inward until they snap upward into the two holes on either side of the larger hole.



3. Attach the HiveAP 340 to the mounting plate, and then attach the antennas to the connectors (see [Figure 12](#)).

Figure 12 Attaching the HiveAP 340 to the mounting plate

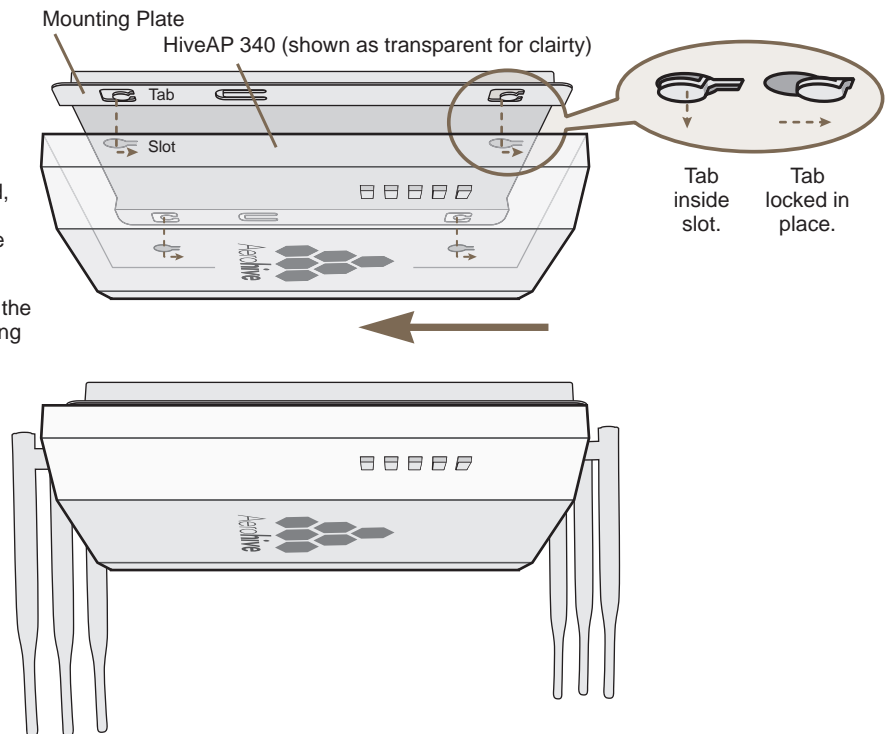
(side view)

- ③ With the HiveAP 340 upside down, align its port side with the bottom end of the plate.

Push the HiveAP 340 upward, inserting the four tabs on the plate into the four slots on the HiveAP 340.

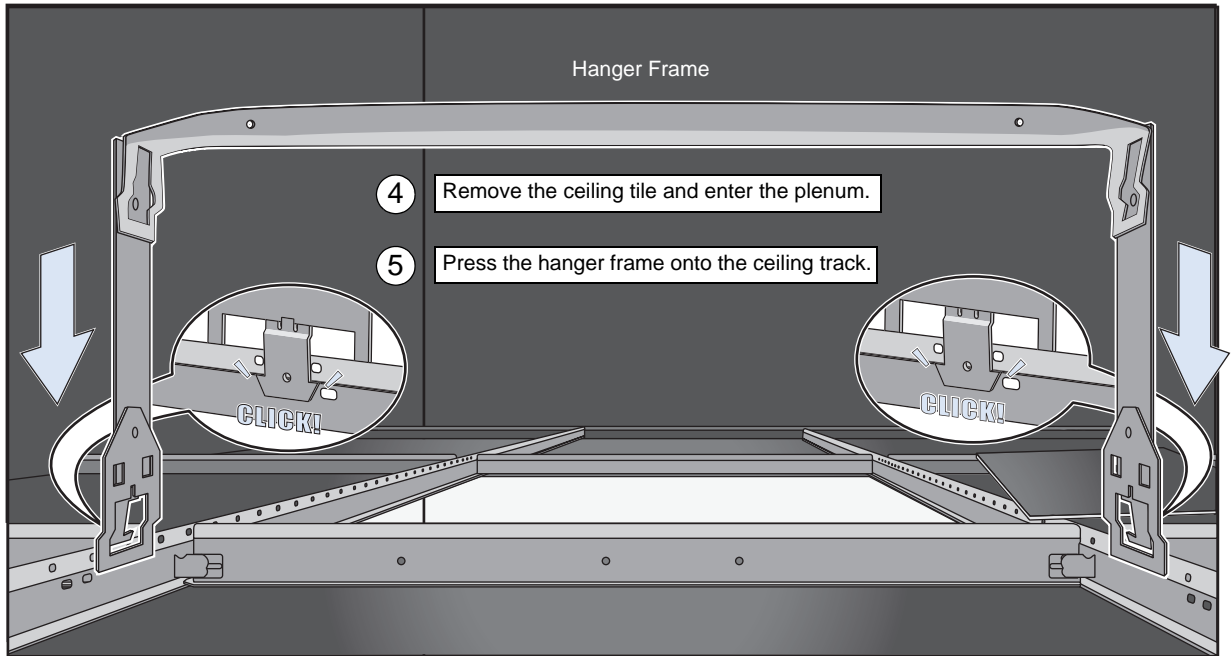
Slide the HiveAP 340 toward the bottom end of the plate, locking the tabs inside the slots.

Attach the antennas to the antenna connectors.



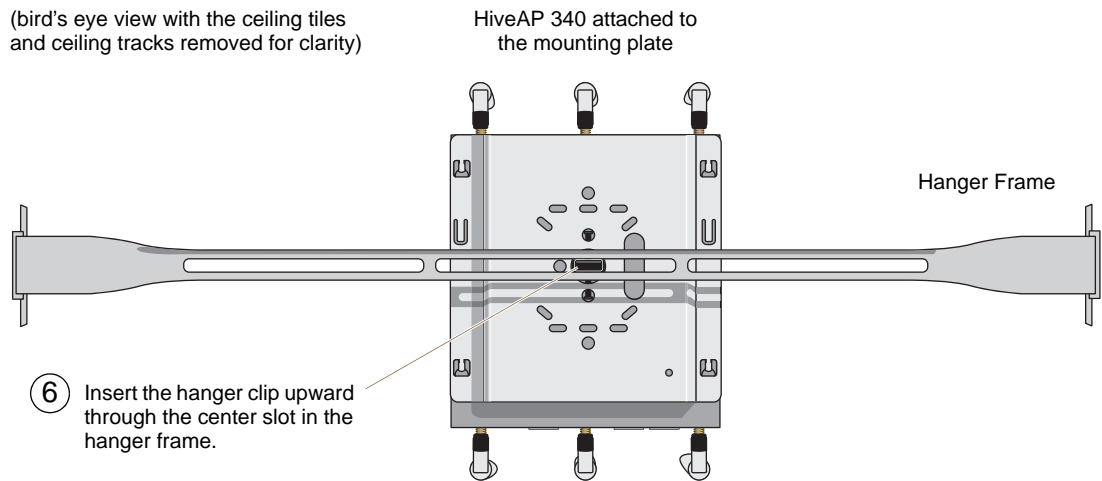
4. Remove the ceiling tile next to the area where you want to mount the device.
5. Press the hanger frame downward into place on the ceiling track until the claws on each leg grips the track below the top ridge (see [Figure 13](#)).

Figure 13 Clipping the hanger frame onto the track

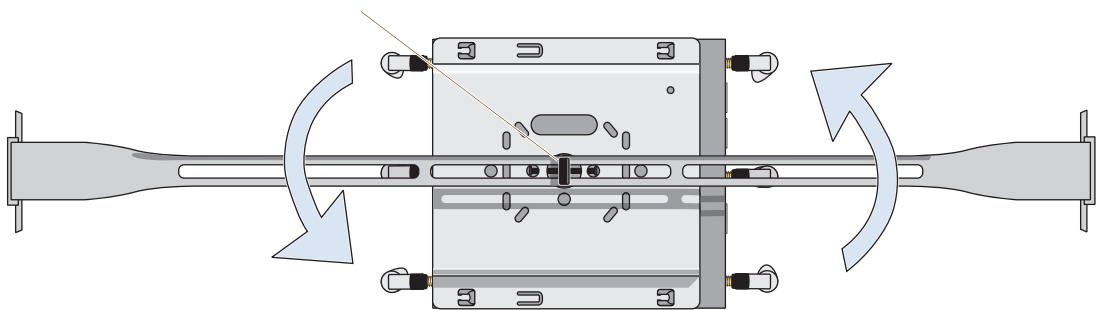


6. Insert the hanger clip upward through the center slot in the hanger frame, and then twist it counterclockwise until the clip snaps into a locked position against the sides of the crossbar (see [Figure 14 on page 65](#)).

Figure 14 Securing the HiveAP 340 to the hanger frame



Rotate the HiveAP 340 and the attached mounting accessories counterclockwise until the clip locks in place against the sides of the crossbar.



7. Connect one or two Ethernet cables to the network, and—if not using PoE—connect the power cord to a power source.
8. Replace the ceiling tile to complete the installation.

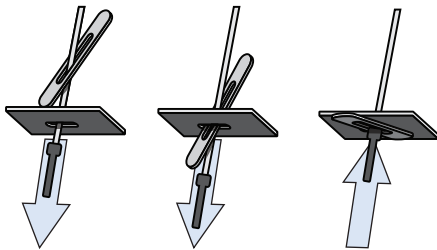
Suspended Mount

You can suspend the HiveAP 340 from a horizontal beam, post, strut, or girder. As well as the mounting plate, you need a quad-toggle, a 1.5 mm (0.059 inch) wire rope with hook, and a locking device. ERICO® supplies these items in its CADDY® SPEED LINK product line. The part number for the quad-toggle is SLD15QT250 and that for the set that includes the wire rope, hook, and locking device is SLD15L2T. These items are available through various suppliers.

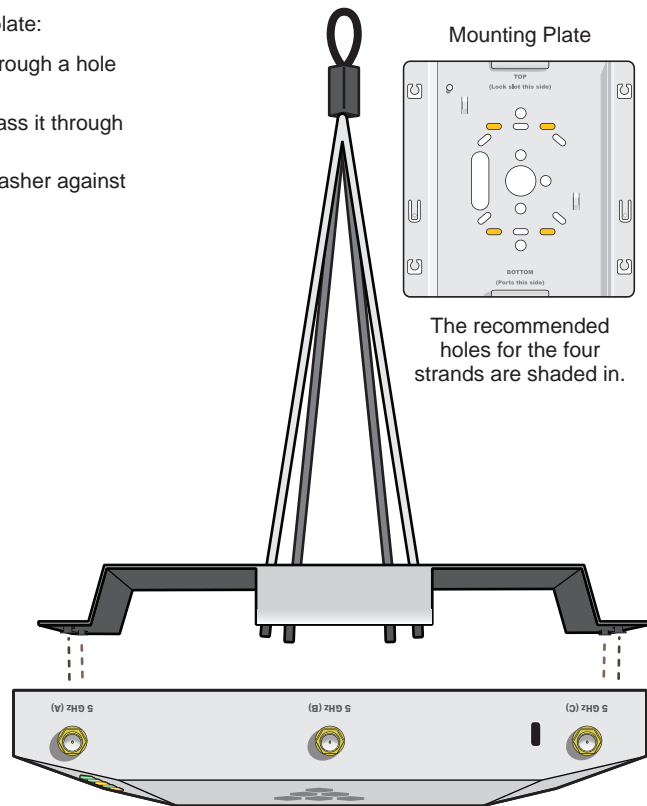
1. With the recessed side of the mounting plate facing downward, insert the four ends of the quad-toggle through holes in the mounting plate.
2. Turn the HiveAP 340 face down and attach it to the mounting plate (see [Figure 15](#)).

Figure 15 Connecting the quad-toggle and HiveAP 340 to the mounting plate

- 1 To secure each of the four strands to the mounting plate:
 1. Insert the metal cleat at the end of a strand through a hole in the plate.
 2. Sliding the oblong washer along the strand, pass it through the hole.
 3. Pull the strand upward to lock the cleat and washer against the underside of the plate.



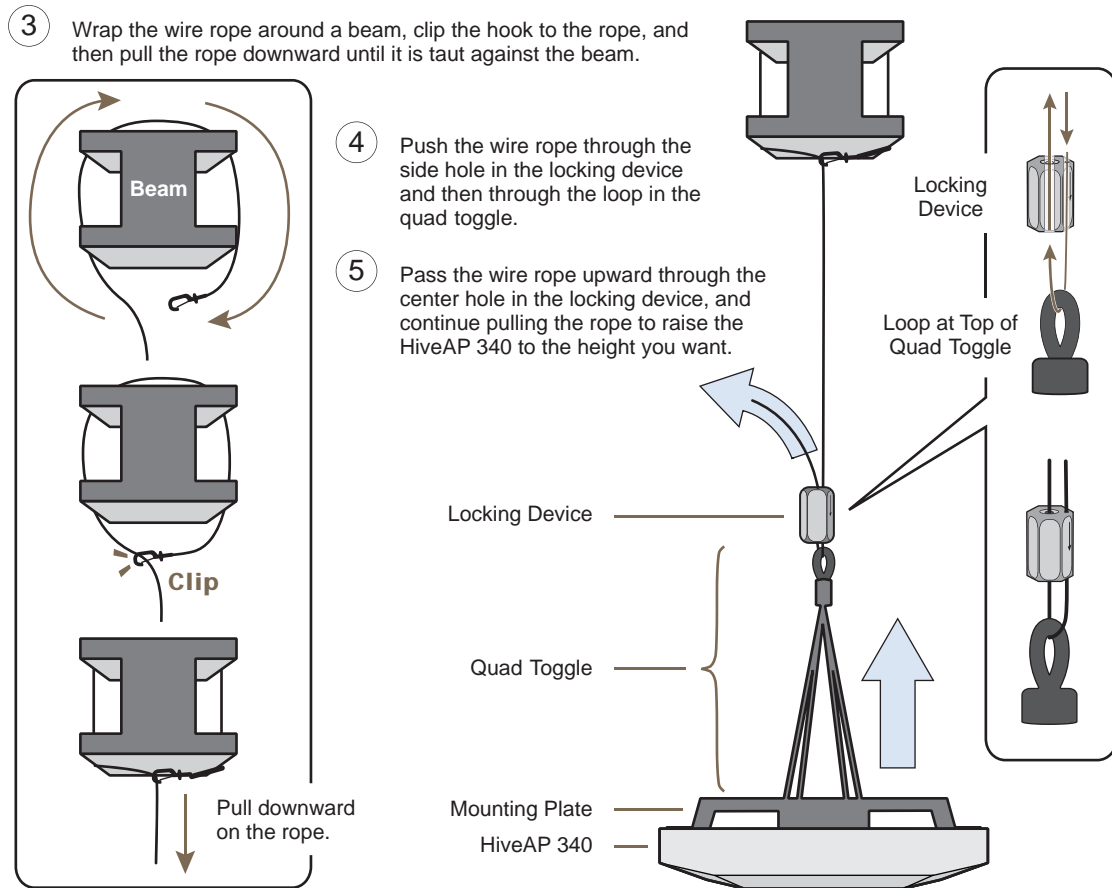
- 2 To attach the HiveAP 340 to the mounting plate:
 1. Align the tabs on the plate with the wider, circular section of the keyhole shaped slots on the underside of the device, which is face down as shown.
 2. Push the tabs into the slots and slide the HiveAP 340 toward its port panel. This repositions the tabs in the narrower, rectangular section of the slots and holds the device firmly in place below the mounting plate.



3. Draw the wire rope over a support beam, fasten the hook around the wire, and pull the wire until the hook is snug against the underside of the beam.
4. Push the plain end of the wire rope—the end without the hook—through the side hole in the locking device in the direction indicated by the arrow on its side, and then pass it through the loop at the end of the quad-toggle.
5. Insert the wire rope back through the center hole in the locking device, and then continue pulling it through the locking device until the HiveAP 340 is suspended at the height you want (see [Figure 16 on page 67](#)).

The center tube that runs through the locking device is designed to allow you to pull the rope wire up through it while preventing the rope from slipping back down. If you ever pull too much rope through and need to pull it back down, use a tool such as a screw driver to press against the inner tube in the locking device to release the rope. Then you can pull it back out (see ["Height Correction" on page 67](#)).

Figure 16 Suspending the HiveAP 340

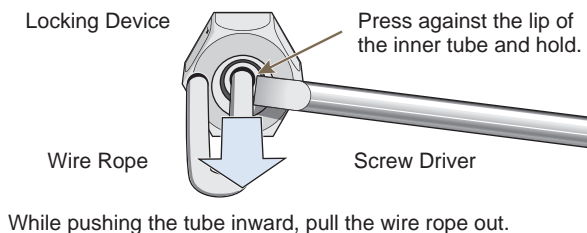


6. Attach antennas to the antenna connectors on the HiveAP 340, connect one or two Ethernet cables to the network, and—if not using PoE—connect the power cord to a power source.

Height Correction

If you accidentally pull too much wire rope through the locking device, raising the HiveAP 340 too high, and you then need to lower it, do the following: Take a tool, such as a screw driver with a 1/8" flat tip, and press it against the lip of the inner tube in the opposite direction from the arrow on the outside of the locking device (see [Figure 17](#)). This releases its grip on the rope, allowing you to pull the rope out the same way it was inserted. While maintaining pressure on the tube, adjust the rope until the HiveAP 340 is at the height you want. When you are satisfied, stop pressing against the tube so that it can regain its grip on the rope.

Figure 17 Releasing the wire rope from the locking device



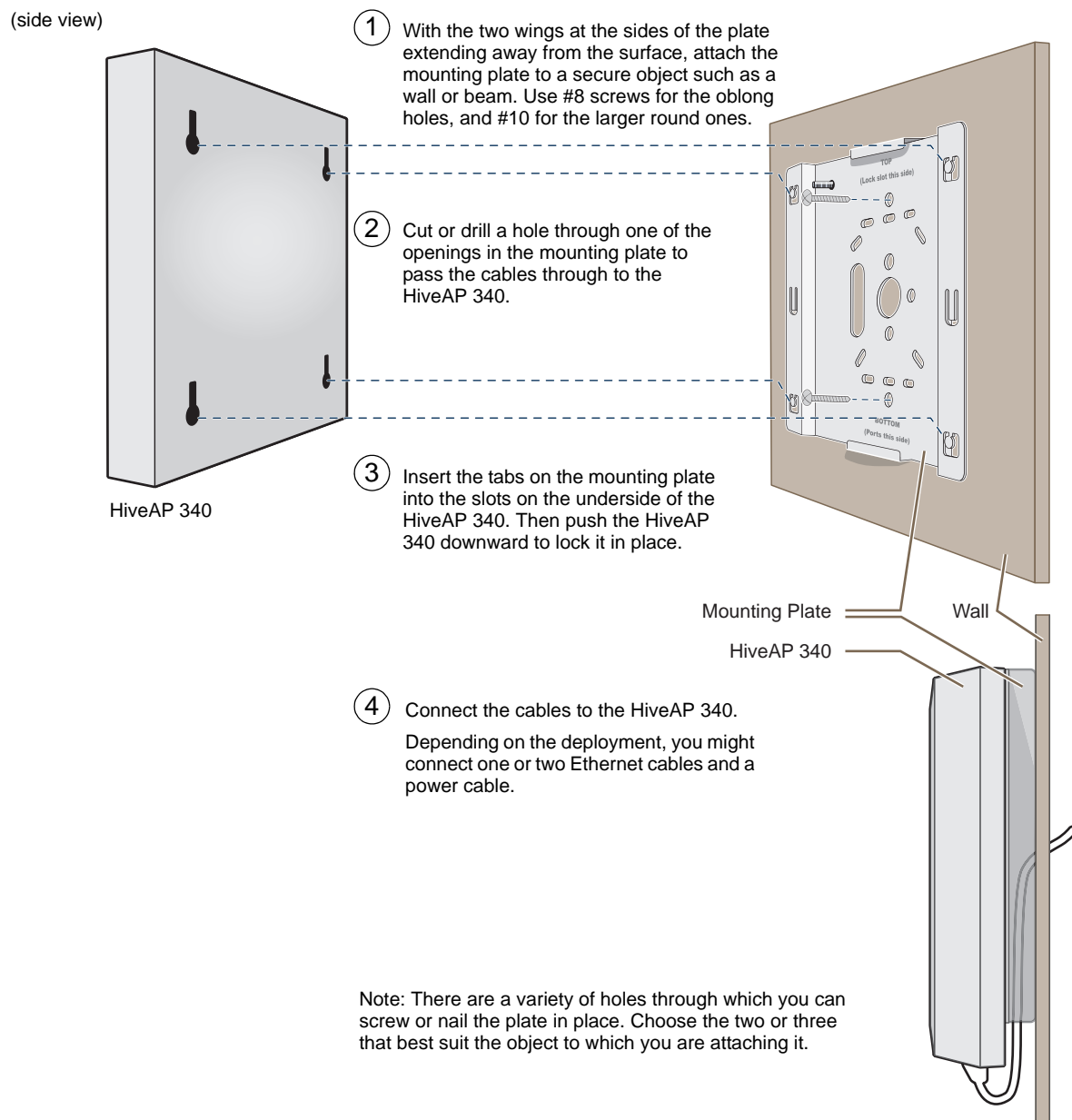
Surface Mount

You can use the mounting plate to attach the HiveAP 340 to any surface that supports its weight, and to which you can screw or nail the plate. First, mount the plate to the surface. Then, through one of the two large openings in the plate, make a hole in the wall so that you can pass the cables through to the HiveAP.

Note: You can tie the cables to the tie points on the mounting plate to prevent them from being pulled out of their connections accidentally.

Finally, attach the device to the plate, and connect the cables, as shown in [Figure 18](#).

Figure 18 Mounting the HiveAP on a wall



DEVICE, POWER, AND ENVIRONMENTAL SPECIFICATIONS

Understanding the range of specifications for the HiveAP 340 is necessary for optimal deployment and device operation. The following specifications describe the physical features and hardware components, the power adapter and PoE (Power over Ethernet) electrical requirements, and the temperature and humidity ranges in which the device can operate.

Device Specifications

- Chassis dimensions: 8 1/2" W x 1 1/4" H x 8" D (21.5 cm W x 3.2 cm H x 20.3 cm D)
- Weight: 3 lb. (1.36 kg)
- Antennas: Three omnidirectional 802.11b/g/n antennas, and three omnidirectional 802.11a/n antennas
- Serial port: RJ-45 (bits per second: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none)
- Ethernet ports: autosensing 10/100/1000 Base-T/TX Mbps; both ports are compliant with the IEEE 802.3af standard and the forthcoming 802.at standard for PoE (Power over Ethernet)

Power Specifications

- AC/DC power adapter:
 - Input: 100 - 240 VAC
 - Output: 48V/0.38A
- PoE nominal input voltages:
 - 802.3af: 48 V/0.35A
 - Pre-802.3at: 48 V/0.625A
- RJ-45 power input pins: Wires 4, 5, 7, 8 or 1, 2, 3, 6

Environmental Specifications

- Operating temperature: -4 to 131 degrees F (-20 to 55 degrees C)
- Storage temperature: -40 to 176 degrees F (-40 to 80 degrees C)
- Relative Humidity: Maximum 95%

Chapter 5 The HiveAP 320 Platform

The Aerohive HiveAP 320 is a high-performance and highly reliable 802.11n wireless access point. The HiveAP 320 provides dual concurrent 802.11b/g/n and 802.11a/n radios for 3x3 MIMO (Multiple In, Multiple Out) and dual 10/100/1000 Ethernet ports for link aggregation or link redundancy. Its power management system uses a concept called smart PoE (Power over Ethernet) to adjust its power consumption automatically in response to the available power in different environments. Smart PoE supports the IEEE 802.3af standard and the 802.3at pre-standard.

This chapter covers the following topics relating to the HiveAP 320:

- ["HiveAP 320 Product Overview" on page 72](#)
 - ["Ethernet and Console Ports" on page 74](#)
 - ["Status LEDs" on page 74](#)
 - ["Antennas" on page 75](#)
- ["Mounting the HiveAP 320" on page 76](#)
 - ["Ceiling Mount" on page 76](#)
 - ["Surface Mount" on page 78](#)
- ["Device, Power, and Environmental Specifications" on page 79](#)

Note: The HiveAP 320 supports all same 802.11n features as the HiveAP 340. Of particular interest is its support of MIMO (Multiple Input, Multiple Output). For more information, see ["MIMO" on page 57](#) and ["Using MIMO with Legacy Clients" on page 59](#).

HIVEAP 320 PRODUCT OVERVIEW

The HiveAP 320 is a multi-channel wireless access point. It is compatible with IEEE 802.11b/g/n (2.4 GHz) and IEEE 802.11a/n (5 GHz) standards and supports a variety of Wi-Fi (wireless fidelity) security protocols, including WPA (Wi-Fi Protected Access) and WPA2.

You can see the hardware components on the HiveAP in [Figure 1](#). Each component is described in [Table 1](#).

Figure 1 HiveAP 320 hardware components

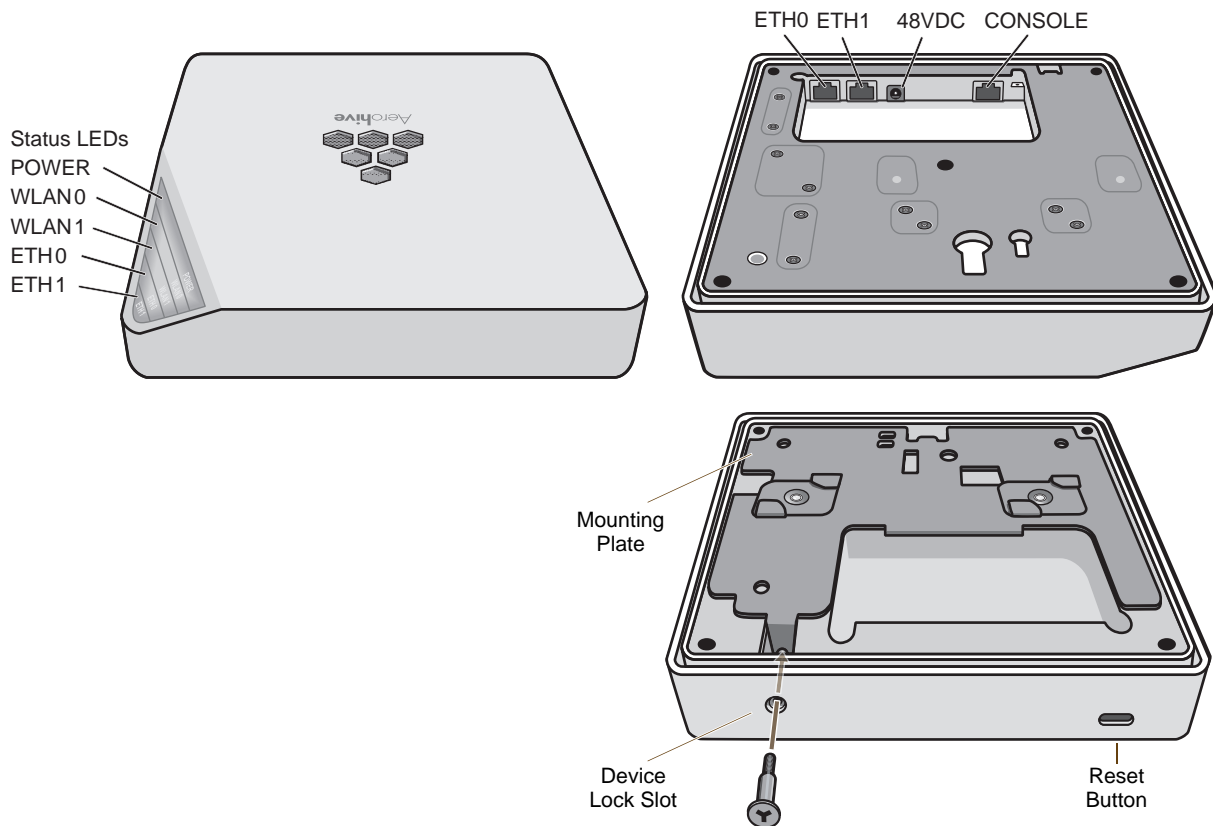


Table 1 HiveAP 320 component descriptions

Component	Description
Status LEDs	The status LEDs convey operational states for system power, firmware, Ethernet interfaces, and radios. For details, see "Status LEDs" on page 74 .
ETH0 10/100/1000 Mbps PoE Port and ETH1 10/100/1000 Mbps Port	The two 10/100/1000-Mbps Ethernet ports—ETH0 and ETH1—receive RJ-45 connectors. The HiveAP can receive power through an Ethernet connection to the ETH0 port from PSE (power sourcing equipment) that is compatible with the 802.3af standard and the forthcoming 802.3at standard. Aerohive provides suitable PoE injectors as an optional accessory. (If you connect the HiveAP to a power source through the power connector and the ETH0 PoE port simultaneously, the device draws power through the power connector and automatically disables PoE.)

Component	Description
	You can configure ETH0 and ETH1 as two individual Ethernet interfaces, combine them into an aggregate interface to increase throughput, or combine them into a redundant interface to increase reliability. You can connect the HiveAP 320 to a wired network or to a wired device (such as a security camera) through these ports using bridging. They are compatible with 10/100/1000Base-T/TX and automatically negotiate half- and full-duplex connections with the connecting device. They are autosensing and adjust to straight-through and cross-over Ethernet cables automatically. For details, see "Ethernet and Console Ports" on page 74.
48VDC Power Connector	The 48-volt DC power connector (0.625 amps) is one of two methods through which you can power the HiveAP 320. To connect it to a 100 - 240-volt AC power source, use the AC/DC power adaptor that is available as an extra option. Because the HiveAP does not have an on/off switch, connecting it to a power source automatically powers on the device.
Console Port	You can access the CLI by making a serial connection to the RJ-45 console port. The management station from which you make a serial connection to the HiveAP must have a VT100 emulation program, such as Tera Term Pro [®] (a free terminal emulator) or Hilgraeve Hyperterminal [®] (provided with Windows [®] operating systems). The following are the serial connection settings: bits per second: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none. For details, see "Ethernet and Console Ports" on page 74.
Device Lock Slot	You can physically secure the HiveAP by attaching it to a mounting plate that is clipped to a ceiling track and then using a screw with a unique head design to fasten the HiveAP to the mounting plate through the device lock slot. The screw and special screw driver that fits the slot on the screw head are included in the mounting kit. For more information, see "Locking the HiveAP 320" on page 77.
Reset Button	<p>The reset button allows you to reboot the device or reset the HiveAP to its factory default settings. Insert a paper clip, or something similar, into the Reset pinhole and press the reset button. To reboot the device, hold the button down between 1 and 5 seconds. To return the configuration to the factory default settings, hold it down for at least 5 seconds. After releasing the button, the Power LED goes dark as the system reboots. Then it pulses green while the firmware loads and the system performs a self-test. After the software finishes loading, the Power LED glows steady green.</p> <p>To disable the reset button from resetting the configuration, enter this command: no reset-button reset-config-enable Pressing the button between 1 and 5 seconds will still reboot the HiveAP, but pressing it for more than 5 seconds will not reset its configuration.</p>

Note: The rear surface of the HiveAP 320 is used for heat dissipation to reduce the internal temperature. Consequently, it can become hot, so use caution when handling it.

Ethernet and Console Ports

There are three ports on the HiveAP 320: two RJ-45 10/100/1000Base-T/TX Ethernet ports and an RJ-45 console port.

The pin assignments in the PoE (Power over Ethernet) Ethernet ports follow the TIA/EIA-568-B standard (see [Figure 2 on page 52](#)). The ports accept standard types of Ethernet cable—cat3, cat5, cat5e, or cat6. The ETH0 port can receive power over the Ethernet cable from power sourcing equipment (PSE) that is 802.3af-compatible. If you use cat5, cat5e, or cat6 cables, the ETH0 port can also support 802.3at-compliant PSE. Such equipment can be embedded in a switch or router, or it can come from purpose-built devices that inject power into the Ethernet line en route to the HiveAP. Because the PoE ports have autosensing capabilities, the wiring termination in the Ethernet cable can be either straight-through or cross-over.

The HiveAP 320 supports the following features on its Ethernet ports:

- The HiveAP 320 supports smart PoE on its ETH0 port to adapt its power consumption to changes in the amount of power available to it over Ethernet from PSE (power sourcing equipment). For more information, see ["Smart PoE" on page 53](#).
- The two Ethernet interfaces can be configured as aggregate interfaces for increased throughput and redundant interfaces for increased reliability. For more information, see ["Aggregate and Redundant Interfaces" on page 53](#).

Through the RJ-45 console port, you can make a serial connection between your management system and the HiveAP. The pin-to-signal mapping of the RJ-45 console port is the same as that for the HiveAP 340, which is shown in [Figure 3 on page 55](#). Similarly, cabling and connection details for the HiveAP 320 are same as those for the HiveAP 340 (see [Figure 4 on page 55](#)).

Status LEDs

The five status LEDs on the top of the HiveAP 320 indicate various states of activity through their color (dark, green, amber, and red) and illumination patterns (steady glow or pulsing). The meanings of the various color + illumination patterns for each LED are explained below.

Power

- Dark: No power
- Steady green: Powered on and the firmware is running normally
- Pulsing green: Firmware is booting up
- Steady amber: Firmware is being updated
- Pulsing amber: Alarm indicating a firmware issue has occurred
- Steady red: Alarm indicating a hardware issue has occurred

ETH0 and ETH1

- Dark: Ethernet link is down or disabled
- Steady green: 1000 Mbps Ethernet link is up but inactive
- Pulsing green: 1000 Mbps Ethernet link is up and active
- Steady amber: 10/100 Mbps Ethernet link is up but inactive
- Pulsing amber: 10/100 Mbps Ethernet link is up and active

WIFI0 and WIFI1

- Dark: Wireless interface is disabled
- Steady green: Wireless interface is in access mode but inactive
- Pulsing green: Wireless interface is in access mode and active
- Steady amber: Wireless interface is in backhaul mode but inactive
- Pulsing amber: Wireless interface is in backhaul mode and is connected with other hive members
- Alternating green and amber: Wireless interface is in backhaul mode and is searching for other hive members

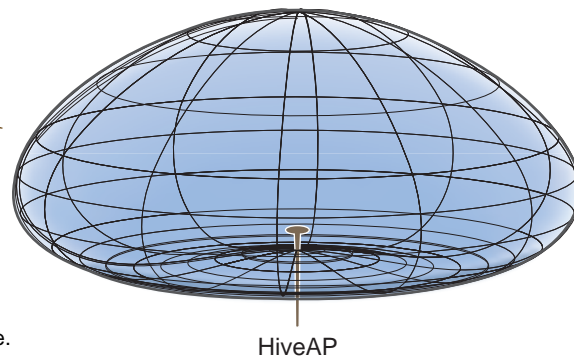
Antennas

Antennas are an integral part of the HiveAP 320. The HiveAP 320 has six internal single-band antennas. Three of the antennas operate in the 2.4-GHz band (IEEE 802.11b/g/n) and have a 2-dBi gain. The other three antennas operate in the 5-GHz band (IEEE 802.11a/n) and have a 3-dBi gain. All antennas are omnidirectional, providing fairly equal coverage in all directions in a cardioid (heart-shaped) pattern around each antenna (see [Figure 2](#)).

Figure 2 *Cardioid radiation pattern*

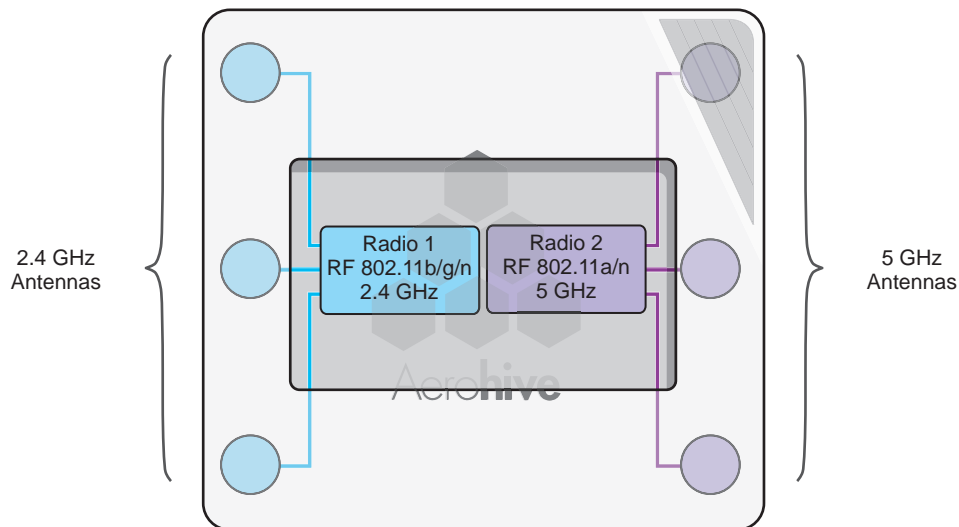
The omnidirectional antennas radiate fairly equally in all directions, forming a cardioid pattern.

Note: To show the shape of radiation more clearly, this illustration depicts the coverage provided by only one active antenna pointing upward and is not drawn to scale.



The three 2.4-GHz antennas link to radio 1, and the three 5-GHz antennas link to radio 2. Conceptually, the relationship of antennas and radios is shown in [Figure 3](#).

Figure 3 *Antennas and radios*



Cut-away view of the HiveAP 320 to show the relationship of the antennas and the two internal radios

The wifi0 interface links to radio 1 (frequency range = 2.4 GHz for IEEE 802.11b/g), and the wifi1 interface links to radio 2 (frequency range = 5 GHz for IEEE 802.11a). These interface-to-radio relationships are permanent.

Although hive members automatically adjust their signal strength according to their environments, you can resize the area of coverage by increasing or decreasing the signal strength manually by entering the `interface { wifi0 | wifi1 } radio power <number>` command, where <number> can be from 1 to 20 and represents a value in dBm.

MOUNTING THE HIVEAP 320

Using the mounting plate and track clips, you can mount the HiveAP 320 to the tracks of a dropped ceiling grid. Using just the mounting plate, you can mount the HiveAP to any surface that can support its weight (2 lb., 0.9 kg).

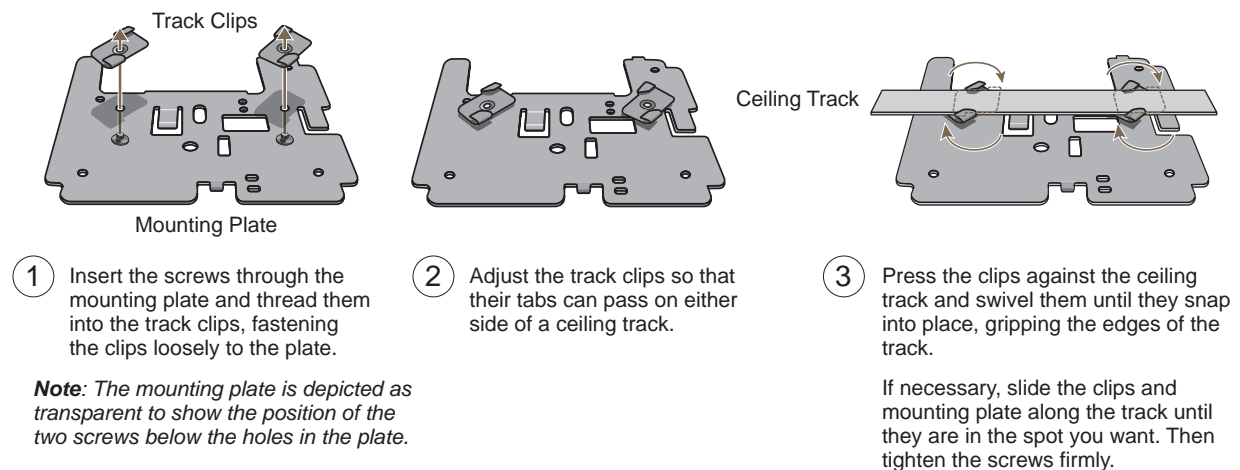
Note: In addition to these methods, you can also mount the HiveAP 320 on a table using the set of four rubber feet that ship with the product. Simply peel the rubber feet off the adhesive sheet and press them against the underside of the HiveAP in its four corners.

Ceiling Mount

To mount the HiveAP 320 to a track in a dropped ceiling, you need the mounting plate, two track clips, and two Keps nuts, all of which ship as an option with the HiveAP 320. You also need a screwdriver and—most likely—a ladder.

Nudge the ceiling tiles slightly away from the track to clear some space. Fasten the track clips to the mounting plate, and then attach them to the ceiling track, as shown in [Figure 4](#).

Figure 4 Attaching the track clips and mounting plate to the ceiling track

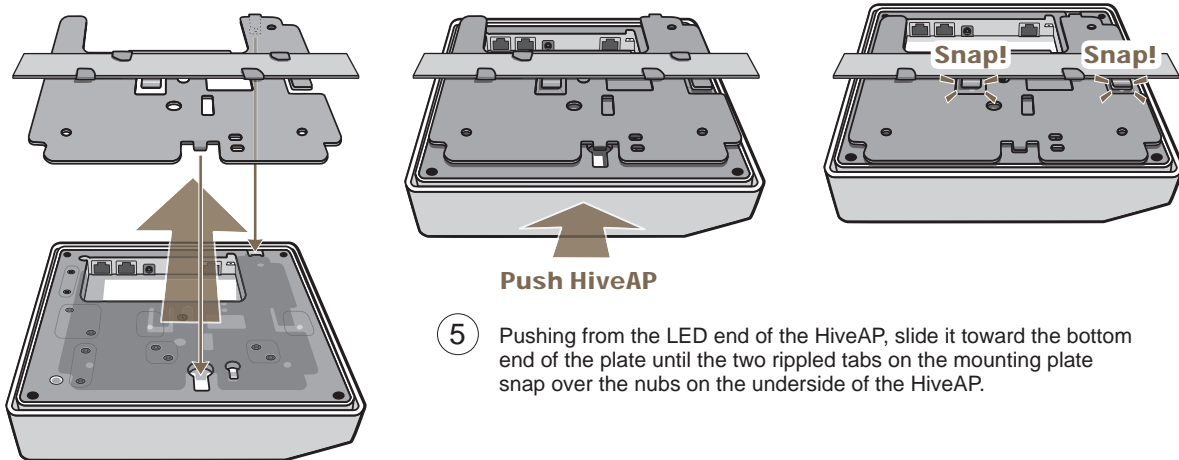


When you have the mounting plate in the correct location, cut or drill a hole in the ceiling through which you can then pass the Ethernet and power cables. Pass the cables through the hole and attach them to the HiveAP 320, leaving some slack so that you can easily maneuver the HiveAP into place, attaching it to the mounting plate as shown in [Figure 5](#) on page 77.

Note: For clarity, the power and Ethernet cables are not shown in the illustrations.

Figure 5 Attaching the HiveAP 320 to the mounting plate

- ④ With the HiveAP 320 upside down, align the round tab and security screw hole extension on the mounting plate with the keyhole opening and security screw cavity on the HiveAP 320, and press the HiveAP upward.



- ⑤ Pushing from the LED end of the HiveAP, slide it toward the bottom end of the plate until the two rippled tabs on the mounting plate snap over the nubs on the underside of the HiveAP.

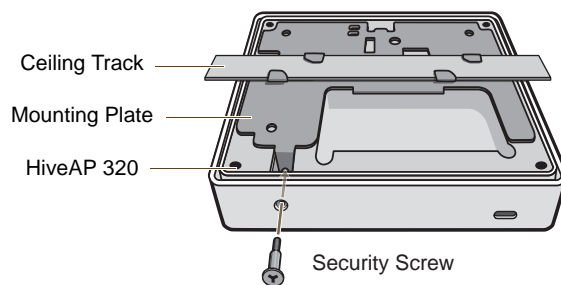
When done, adjust the ceiling tiles back into their former position.

Locking the HiveAP 320

To lock the HiveAP 320 to the mounting plate, use the security screw, which is included in the mounting kit. You also need a Torx tri-wing torsion insert bit for size #1 tri-wing security screws and a screw driver that will accept the bit. The correct bits are available from Aerohive in sets of three (AH-ACC-SEC-BIT-3PK).

1. Insert the security screw through the hole in the HiveAP 320 and begin to thread it into the hole in the mounting plate (see [Figure 6](#)).

Figure 6 Locking the HiveAP 320 to the Mounting Plate



Note: The ceiling tiles are removed for clarity.

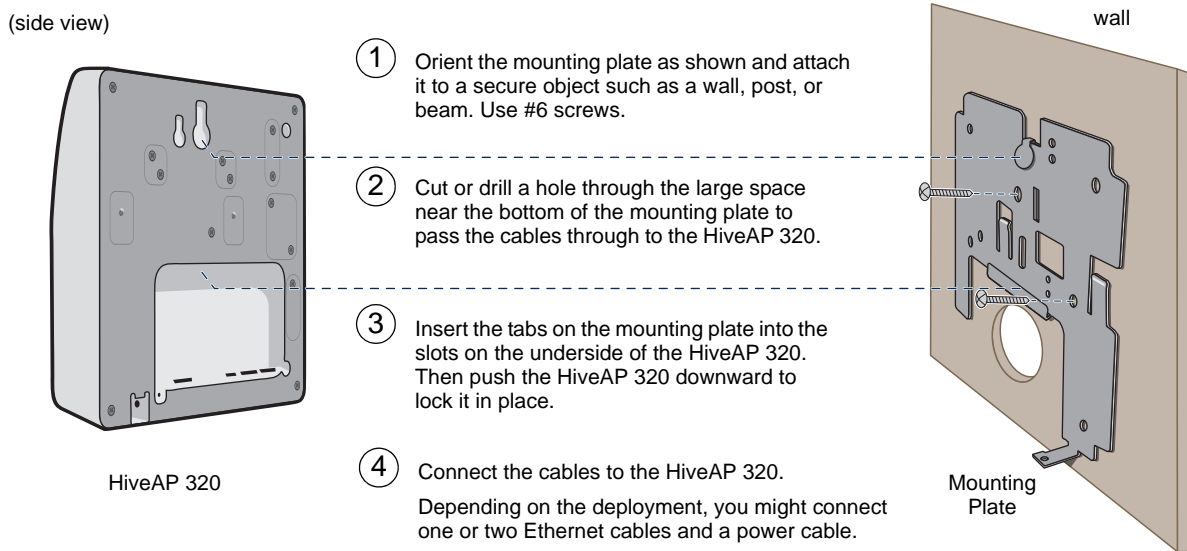
2. With the insert bit in a screw driver, tighten the screw into place, securing the HiveAP to the mounting plate.

Surface Mount

You can use the mounting plate to attach the HiveAP 320 to any surface that supports its weight, and to which you can screw or nail the plate. First, mount the plate to the surface. Then, through the large opening in the lower part of the plate, make a hole in the wall so that you can pass the cables through to the HiveAP.

Finally, attach the device to the plate, and connect the cables, as shown in [Figure 7](#).

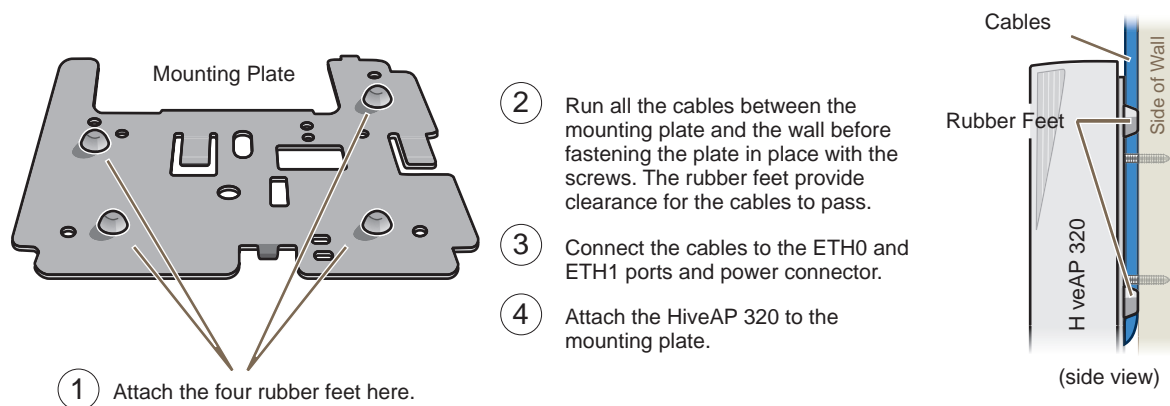
Figure 7 Mounting the HiveAP 320 on a wall



Note: You can use the locking screw to secure the HiveAP 320 to the mounting plate. For information, see "Locking the HiveAP 320" on page 77.

If you do not pass the cables through a hole, you can run them along the wall between the wall and the mounting plate. To create space for the cables, attach the rubber feet to the mounting plate before attaching it to the wall. The recommended positions for the four rubber feet and the mounting instructions are shown in [Figure 8](#).

Figure 8 Using the rubber feet to provide clearance for cables



DEVICE, POWER, AND ENVIRONMENTAL SPECIFICATIONS

Understanding the range of specifications for the HiveAP 320 is necessary for optimal deployment and device operation. The following specifications describe the physical features and hardware components, the power adapter and PoE (Power over Ethernet) electrical requirements, and the temperature and humidity ranges in which the device can operate.

Device Specifications

- Chassis dimensions: 8" W x 1.5" H x 8" D (20 cm W x 3.8 cm H x 20 cm D)
- Weight: 2 lb. (0.9 kg)
- Antennas: Three omnidirectional 802.11b/g/n antennas, and three omnidirectional 802.11a/n antennas
- Serial port: RJ-45 (bits per second: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none)
- Ethernet ports: two autosensing 10/100/1000 Base-T/TX Mbps ports; the ETH0 port is compliant with the IEEE 802.3af standard and the forthcoming 802.at standard for PoE (Power over Ethernet)

Power Specifications

- AC/DC power adapter:
 - Input: 100 - 240 VAC
 - Output: 48V/0.38A
- PoE nominal input voltages:
 - 802.3af: 48 V/0.35A
 - Pre-802.3at: 48 V/0.625A
- RJ-45 power input pins: Wires 4, 5, 7, 8 or 1, 2, 3, 6

Environmental Specifications

- Operating temperature: 32 to 104 degrees F (0 to 40 degrees C)
- Storage temperature: -4 to 158 degrees F (-20 to 70 degrees C)
- Relative Humidity: Maximum 95%

Chapter 6 HiveAP 100 Series Platforms

The Aerohive HiveAP 110 and 120 platforms are high-performance wireless access points suitable for small offices, mobile employees, and telecommuters. The HiveAP 110 has one dual-band 802.11a/b/g/n radio, and the HiveAP 120 has two radios—one for 802.11a/n and one for 802.11b/g/n, which can both operate concurrently. Both platforms provide 2x2 MIMO (Multiple In, Multiple Out) and a single 10/100/1000 Ethernet port through which they can be powered using PoE (Power over Ethernet) that follows the IEEE 802.3af standard or the 802.3at pre-standard. Optionally, they can be powered by an AC/DC desktop power adapter.

This chapter covers the following topics relating to the HiveAP 100 series:

- ["HiveAP 110 and 120 Product Overview" on page 82](#)
 - ["Ethernet Port" on page 83](#)
 - ["Status Indicator" on page 84](#)
 - ["Antennas" on page 84](#)
- ["Mounting a HiveAP 100 Series Device" on page 85](#)
 - ["Ceiling Mount" on page 85](#)
 - ["Surface Mount" on page 87](#)
- ["Device, Power, and Environmental Specifications" on page 88](#)

Note: HiveAP 100 series devices support the same 802.11n features as the HiveAP 300 series. Of particular interest is their support of 2x2 MIMO (Multiple Input, Multiple Output). For more information, see ["MIMO" on page 57](#) and ["Using MIMO with Legacy Clients" on page 59](#).

HIVEAP 110 AND 120 PRODUCT OVERVIEW

The HiveAP 110 and 120 are both multi-channel wireless access points. The HiveAP 110 contains a dual-band radio that can operate at either 2.4-GHz or 5-GHz—but not in both bands simultaneously. The HiveAP 120 contains a 2.4-GHz radio and a 5-GHz radio that can operate concurrently through four internal antennas. The HiveAP 100 series supports a variety of Wi-Fi (wireless fidelity) security protocols, including WPA (Wi-Fi Protected Access) and WPA2.

You can see the hardware components on the HiveAP in [Figure 1](#). Each component is described in [Table 1](#).

Figure 1 HiveAP 110 and 120 hardware components

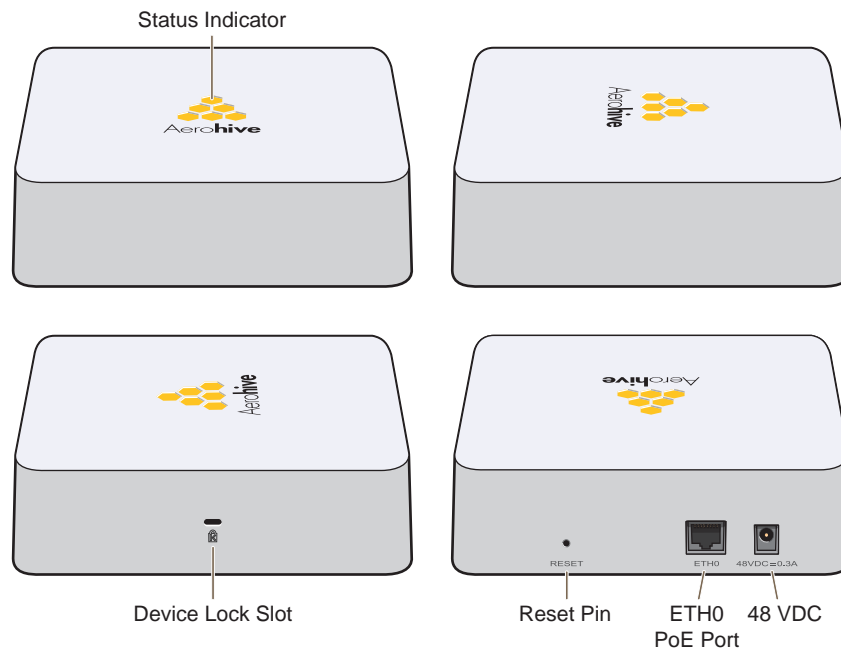


Table 1 HiveAP 110 and 120 component descriptions

Component	Description
Status Indicator	The status indicator conveys operational states for system power, firmware updates, Ethernet and wireless interface activity, and major alarms. For details, see "Status Indicator" on page 84 .
Device Lock Slot	You can physically secure the HiveAP by attaching a Kensington lock and cable to the device lock slot. For more information, see "Locking the HiveAP" on page 87 .

Component	Description
Reset Button	<p>The reset button allows you to reboot the device or reset the HiveAP to its factory default settings. Insert a paper clip, or something similar, into the Reset pinhole and press the reset button. To reboot the device, hold the button down between 1 and 5 seconds. To return the configuration to the factory default settings, hold it down for at least 5 seconds. After releasing the button, the status indicator goes dark as the system reboots. Then it glows blue while the device boots and the system performs a self-test. After the firmware finishes loading and the HiveAP is ready to serve clients, the status indicator glows white.</p> <p>To disable the reset button from resetting the configuration, enter this command: no reset-button reset-config-enable Pressing the button between 1 and 5 seconds will still reboot the HiveAP, but pressing it for more than 5 seconds will not reset its configuration.</p>
ETH0 PoE Port	<p>The 10/100/1000-Mbps Ethernet port—ETH0—receives an RJ-45 connector. The HiveAP can receive power through an Ethernet connection to the ETH0 port from PSE (power sourcing equipment) that is compatible with the 802.3af standard and the forthcoming 802.3at standard. Aerohive provides suitable PoE injectors as an optional accessory. (If you connect the HiveAP to a power source through the power connector and the ETH0 PoE port simultaneously, the device draws power through the power connector and automatically disables PoE.)</p> <p>The ETH0 port is compatible with 10/100/1000Base-T/TX and automatically negotiates half- and full-duplex connections with the connecting device. It is autosensing and adjusts to straight-through and cross-over Ethernet cables automatically. For details, see "Ethernet Port" on page 83.</p>
48VDC Power Connector	<p>The 48-volt DC power connector (0.3 amps), with a voltage range of 36 to 57 volts DC, is one of two methods through which you can power the HiveAP (the other is PoE). To connect it to a 100 - 240-volt AC power source, use the AC/DC power adaptor that is available as an extra accessory. Because the HiveAP does not have an on/off switch, connecting it to a power source automatically powers on the device.</p>

Ethernet Port

The pin assignments in the PoE (Power over Ethernet) 10/100/1000Base-T/TX Ethernet port follow the TIA/EIA-568-B standard (see [Figure 2 on page 52](#)). The port accepts standard types of Ethernet cable—cat3, cat5, cat5e, or cat6—and can receive power over the Ethernet cable from power sourcing equipment (PSE) that is 802.3af-compatible. If you use cat5, cat5e, or cat6 cables, the ETH0 port can also support 802.3at-compliant PSE. Such equipment can be embedded in a switch or router, or it can come from purpose-built devices that inject power into the Ethernet line en route to the HiveAP. Because the PoE port has autosensing capabilities, the wiring termination in the Ethernet cable can be either straight-through or cross-over.

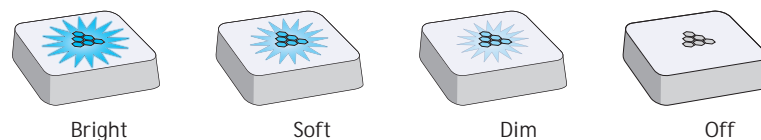
Status Indicator

The status indicator has been incorporated into the Aerohive logo on the top of the HiveAP 110 and 120. It is illuminated by various colors to indicate different states of activity. The meanings of the colors are as follows:

- **Dark:** There is no power or the status indicator is disabled.
- **Blue:** (solid) The device is booting up or there is no backhaul link; (flashing) the device is shutting down.
- **Green:** The default route is through the backhaul Ethernet interface, but not all conditions for normal operations (white) have been met.
- **Yellow:** The default route is through a backhaul wifi interface, but not all conditions for normal operations (white) have been met.
- **White:** The device is powered on and the firmware is operating normally; that is, a wireless interface in access mode is up, a wired or wireless backhaul link is up, and the HiveAP has a CAPWAP connection to either HiveManager or a management AP.
- **Purple:** A new image is being loaded from HiveManager or a management AP.
- **Orange:** An alarm indicating a firmware or hardware issue has occurred.

For locations where the status indicator might be a distraction or attract unwanted attention, you can adjust its brightness level from bright (the default) to soft to dim. You can even turn it off completely. In HiveManager, choose the brightness level that you want from the LED Brightness drop-down list on the Configuration > Management Services > Management Options page. Through the CLI, enter `[no] system led brightness { soft | dim | off }`. The four settings are represented graphically in [Figure 2](#).

Figure 2 Adjustable status indicator brightness levels

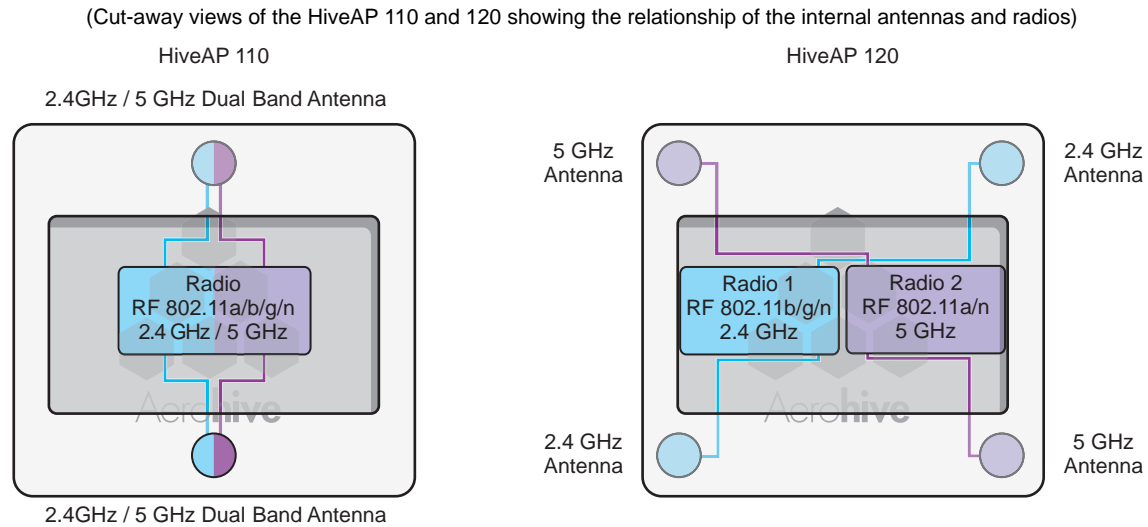


Antennas

Antennas are an integral part of both the HiveAP 110 and HiveAP 120. The HiveAP 110 has two internal dual-band antennas. The HiveAP 120 has four internal single-band antennas. Two of the antennas operate in the 2.4-GHz band (IEEE 802.11b/g/n) and have a 0-dBi gain. The other two antennas operate in the 5-GHz band (IEEE 802.11a/n) and have a 3-dBi gain. All antennas are omnidirectional, providing fairly equal coverage in all directions in a cardioid (heart-shaped) pattern around each antenna (see [Figure 2 on page 75](#)).

On the HiveAP 110, the two dual-band antennas link to a dual-band radio, which can operate in the 2.4-GHz band for 802.11b/g/n or the 5-GHz band for 802.11a/n, but not in both bands simultaneously. On the HiveAP 120, the two 2.4-GHz antennas link to one radio, and the two 5-GHz antennas link to the other radio, both of which can operate concurrently. Conceptually, the relationship of antennas and radios is shown in [Figure 3 on page 85](#).

Figure 3 Antennas and radios



MOUNTING A HIVEAP 100 SERIES DEVICE

Using one of the track clips included in the box with the HiveAP, you can mount it to a track in a dropped ceiling grid. To mount the HiveAP to any flat surface that can support its weight (1.75 lb., 0.8 kg), use two #6 or #8 screws to mount it on a wall and three screws to mount it on a ceiling.

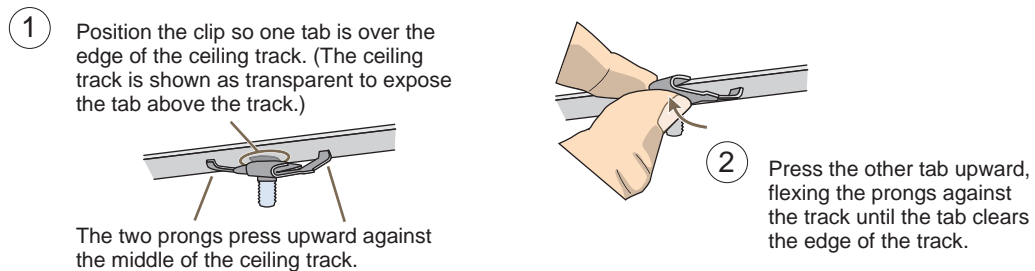
Note: In addition to these methods, you can also mount the HiveAP on a table using the set of four rubber feet that ship with the product. Simply peel the rubber feet off the adhesive sheet and press them against the underside of the HiveAP in its four corners.

Ceiling Mount

To mount a HiveAP series device to a track in a dropped ceiling, use the appropriate track clip for the width of the ceiling track. Two clips ship with the HiveAP: one for 1" (2.54 cm) tracks and one for 1/2" (1.27 cm) tracks.

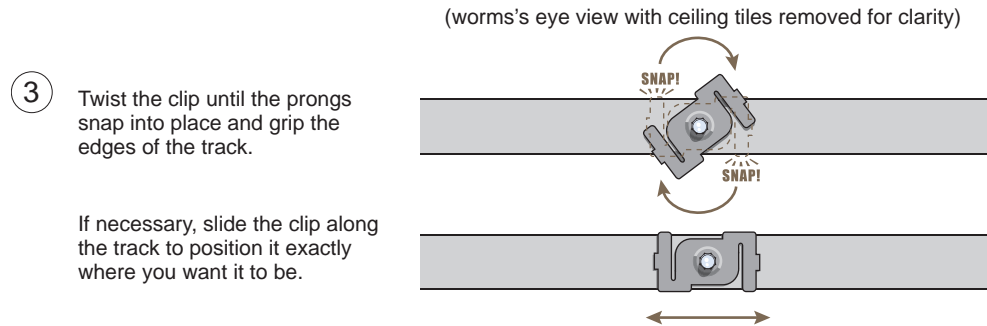
1. Nudge the ceiling tiles slightly away from the track to clear some space, and slide one tab of the track clip over the edge of the track.
2. With the tips of the track clip prongs positioned against the middle of the track, press upward on the other tab until it clears the track edge, as shown in Figure 4. Keeping the prongs away from the track edges until both tabs grip the track ensures that the clip does not snap into place prematurely with only one tab in position.

Figure 4 Attaching the track clip to the ceiling track



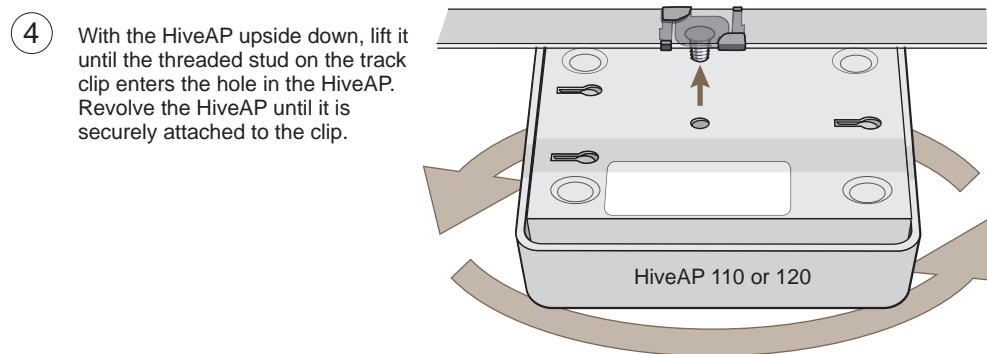
- Twist the track clip until it snap onto the ceiling track, as shown in [Figure 5](#). You can then slide the clip along the track to reposition it if necessary.

Figure 5 Securing the clip to the track and repositioning it if necessary



- Holding the HiveAP upside down, raise it until the threaded stud on the track clip enters the hole on the HiveAP. Then revolve the HiveAP until it is firmly attached to the clip (see [Figure 6](#)).

Figure 6 Attaching the HiveAP to the track clip



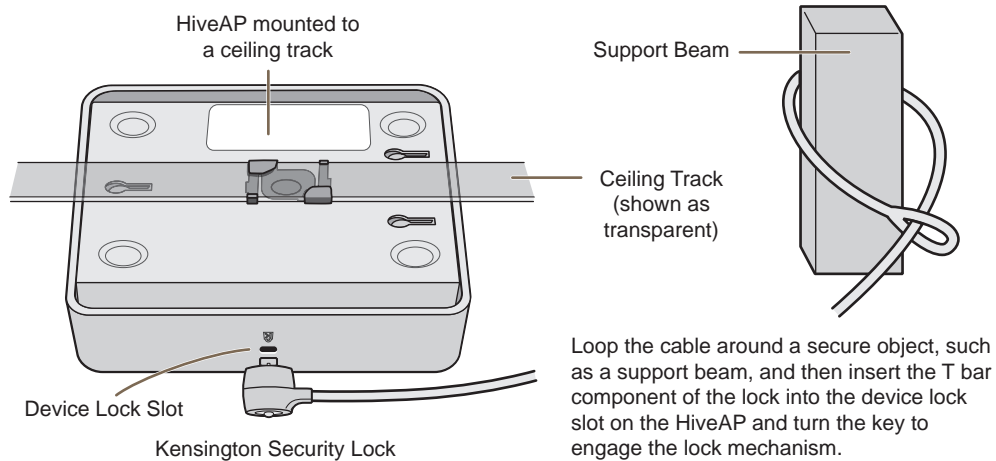
- When you have the HiveAP in the correct location, cut or drill a hole in the ceiling through which you can then pass the Ethernet and power cables. Pass the cables through the hole and attach them to the HiveAP.
- When done, adjust the ceiling tiles back into their former position.

Note: You can also mount the HiveAP 100 series device to a solid ceiling—or the underside of any horizontal object such as a cross beam—using three #6 or #8 screws. Position the three screws in a T-shaped layout: two screws 2" (5 cm) apart from each other and the third screw center-aligned between them and 4.75" (12 cm) away. Then attach the HiveAP to the screws as explained in "Surface Mount" on page 87.

Locking the HiveAP

To lock the HiveAP to a secure object, use a Kensington lock and cable. Loop the cable around a securely anchored object, insert the Kensington lock in the device lock slot in the HiveAP, and engage the locking mechanism (Figure 7).

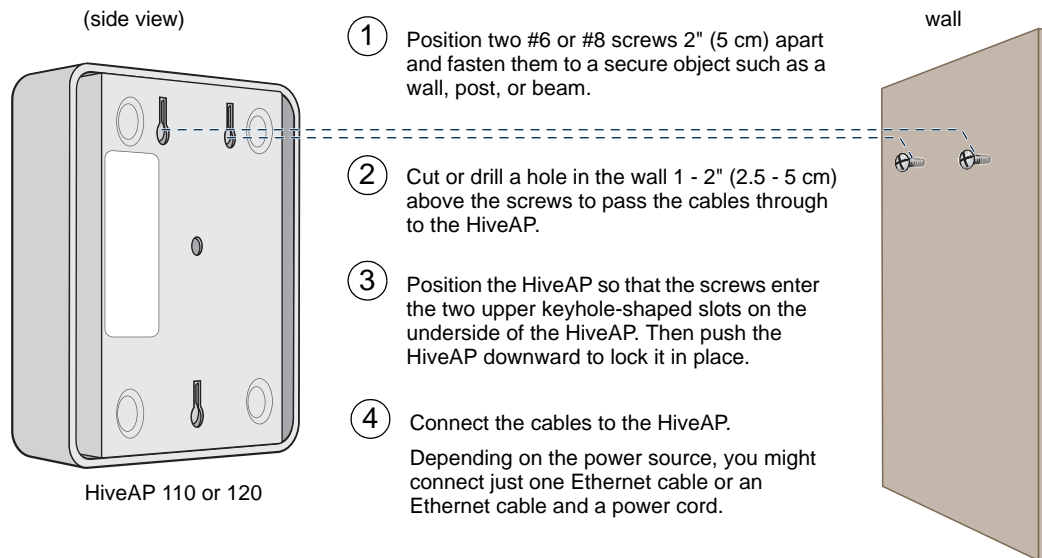
Figure 7 Locking the HiveAP with a Kensington security lock



Surface Mount

You can attach the HiveAP 110 or 120 to any flat surface that supports its weight. First, attach two screws to the surface. Then, make a hole in the wall a few inches or centimeters above the screws so that you can pass the cables through the wall to the HiveAP. Finally, attach the device to the screws, and connect the cables (see Figure 8).

Figure 8 Mounting the HiveAP on a wall



Instead of passing the cables through a hole in the wall, you can also simply run them along the wall from the port side of the HiveAP, which is located at the top of the device when it is mounted on a wall.

Note: You can use a Kensington lock to secure the HiveAP to a stationary object. For information, see "Locking the HiveAP" on page 87.

DEVICE, POWER, AND ENVIRONMENTAL SPECIFICATIONS

Understanding the specifications for the HiveAP 100 series platforms is necessary for optimal deployment and device operation. The following specifications describe the physical features and hardware components, the power adapter and PoE (Power over Ethernet) electrical requirements, and the temperature and humidity ranges in which the device can operate.

Device Specifications

- Chassis dimensions: 6.5" W x 2" H x 6.5" D (16.3 cm W x 4.6 cm H x 16.3 cm D)
- Weight: 1.75 lb. (0.8 kg)
- Antennas:
 - HiveAP 110: two dual-band omnidirectional 802.11a/b/g/n antennas
 - HiveAP 120: two omnidirectional 802.11b/g/n antennas, and two omnidirectional 802.11a/n antennas
- Ethernet port: one autosensing 10/100/1000 Base-T/TX Mbps port; compliant with the IEEE 802.3af standard and the forthcoming 802.at standard for PoE (Power over Ethernet)

Power Specifications

- DC Input: 36 - 57VDC (48 V/0.3A)
- PoE input:
 - 802.3af
 - Pre-802.3at
- RJ-45 power input pins: Wires 4, 5, 7, 8 or 1, 2, 3, 6

Environmental Specifications

- Operating temperature: 32 to 104 degrees F (0 to 40 degrees C)
- Storage temperature: -40 to 185 degrees F (-40 to 85 degrees C)
- Relative Humidity: Maximum 95% noncondensing

Chapter 7 The HiveManager Platform

The HiveManager Network Management System provides centralized configuration, monitoring, and reporting for multiple HiveAPs. The following are a few of the many benefits that a HiveManager offers:

- Simplified installations and management of up to 500 HiveAPs
- Profile-based configurations that simplify the deployment of large numbers of HiveAPs
- Scheduled firmware upgrades on HiveAPs by location
- Exportation of detailed information on HiveAPs for reporting

This chapter covers the following topics related to the HiveManager platform:

- ["Product Overview" on page 90](#)
 - ["Ethernet and Console Ports" on page 91](#)
 - ["Status LEDs" on page 92](#)
- ["Rack Mounting the HiveManager" on page 93](#)
- ["Device, Power, and Environmental Specifications" on page 94](#)

PRODUCT OVERVIEW

The Aerohive HiveManager is a central management system for configuring and monitoring HiveAPs. You can see its hardware components in [Figure 1](#) and read a description of each component in [Table 1](#).

Figure 1 HiveManager hardware components

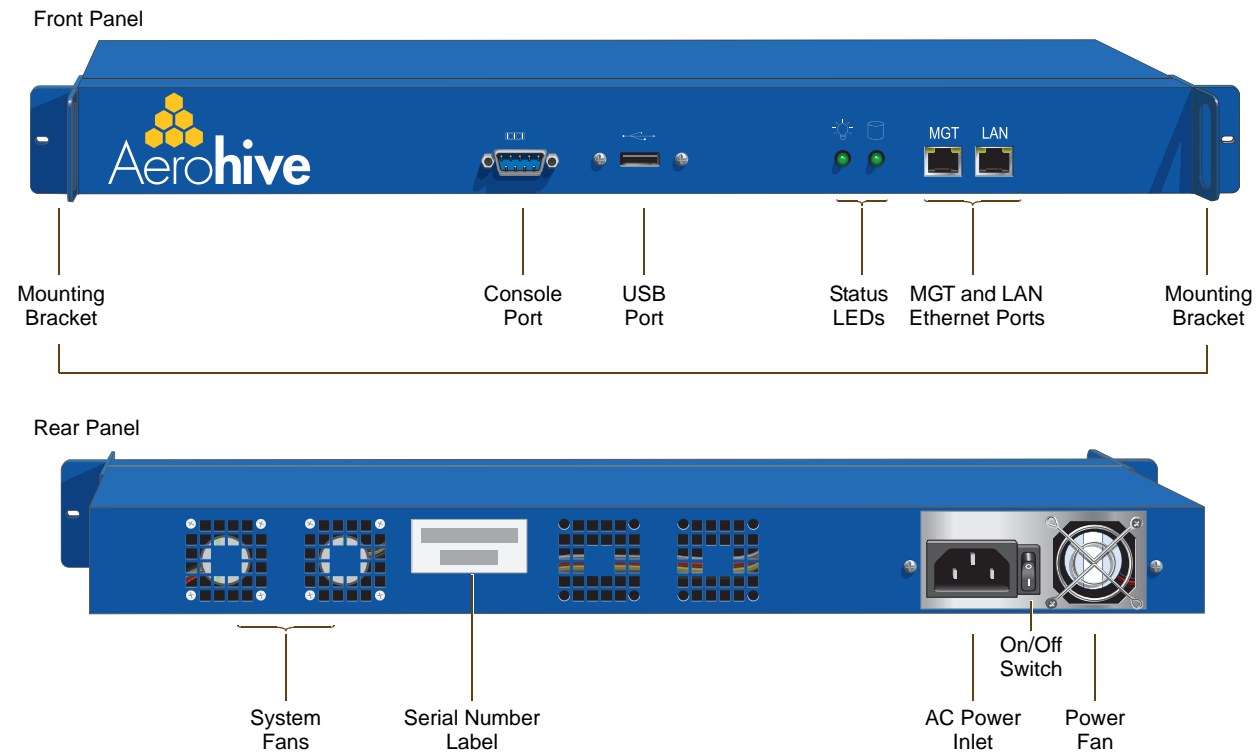


Table 1 HiveManager component descriptions

Component	Description
Mounting Brackets	The two mounting brackets allow you to mount the HiveManager in a standard 19" (48.26 cm) equipment rack. You can also move the brackets to the rear of the chassis if you need to reverse mount it.
Console Port	A male DB-9 serial port to which you can make a console connection using an RS-232 (or "null modem") cable. The pin assignments are the same as those on the HiveAP (see "Ethernet and Console Ports" on page 30). The management station from which you make a serial connection to the HiveManager must have a VT100 emulation program, such as Tera Term Pro [®] (a free terminal emulator) or Hilgraeve Hyperterminal [®] (provided with Windows [®] operating systems). The following are the serial connection settings: bits per second: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none. The default login name is <i>admin</i> and the password is <i>aerohive</i> . After making a connection, you can access the Linux operating system.

Component	Description
USB Port	The USB port is reserved for internal use.
Status LEDs	The status LEDs convey operational states for the system power and hard disk drive. For details, see "Status LEDs" on page 92.
MGT and LAN Ethernet Ports	The MGT and LAN Ethernet ports are compatible with 10/100/1000-Mbps connections, automatically negotiate half- and full-duplex mode with the connecting devices, and support RJ-45 connectors. They are autosensing and automatically adjust to straight-through and cross-over Ethernet cables. The two ports allow you to separate traffic between the HiveManager and its administrators from traffic between the HiveManager and the HiveAPs it manages.
System Fans	The two system fans maintain an optimum operating temperature. Be sure that air flow through the system fan vents is not obstructed.
Serial Number Label	The serial number label contains the FCC compliance stamp, model number, input power specifications, and serial number for the device.
AC Power Inlet	The three-prong AC power inlet is a C14 chassis plug through which you can connect a HiveManager to a 100 - 240-volt AC power source using the 10-amp/125-volt IEC power cord that ships with the product.
On/Off Switch	The on () and off (O) switch controls the power to the HiveManager.
Power Fan	The fan that maintains the temperature of the power supply.

Ethernet and Console Ports

The two 10/100/1000-Mbps Ethernet ports on the HiveManager labeled MGT and LAN use standard RJ-45 connector pin assignments that follow the TIA/EIA-568-B standard (see Figure 2). They accept standard types of Ethernet cable—cat3, cat5, cat5e, or cat6. Because the ports have autosensing capabilities, the wiring termination in the Ethernet cables can be either straight-through or cross-over.

Figure 2 Ethernet port LEDs and pin assignments

(View of an Ethernet port on the HiveManager)

Link Rate LED
 Dark: 10 Mbps
 Green: 100 Mbps
 Amber: 1000 Mbps

Link Activity LED
 Dark: Link is down
 Steady amber: Link is up but inactive
 Blinking amber: Link is up and active

⑧ — ①
Pin Numbers

Pin	10/100Base-T Data Signal	1000Base-T Data Signal
1	Transmit +	BI_DA+
2	Transmit -	BI_DA-
3	Receive +	BI_DB+
4	(unused)	BI_DC+
5	(unused)	BI_DC-
6	Receive -	BI_DB-
7	(unused)	BI_DD+
8	(unused)	BI_DD-

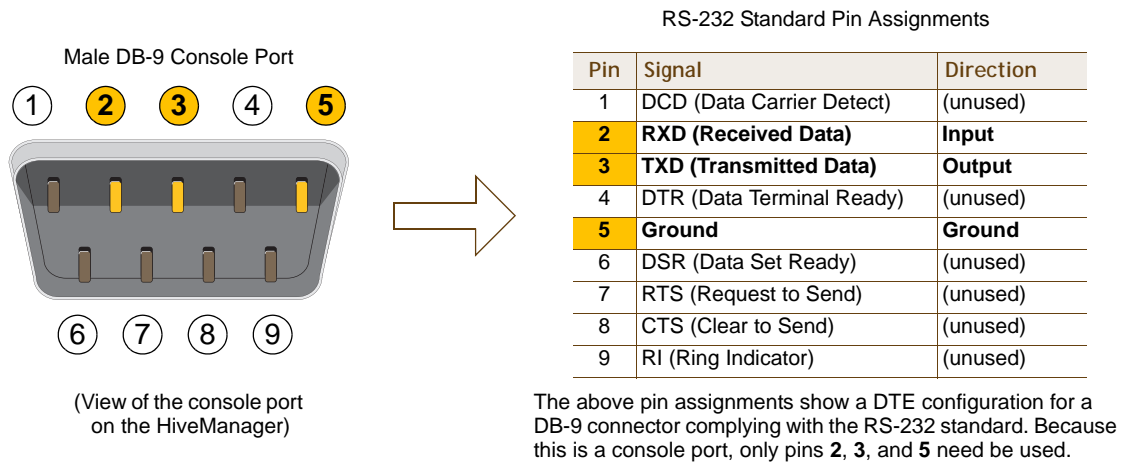
Legend: BI_D = bidirectional
 A+/A-, B+/B-, C+/C-, D+/D- = wire pairings

The Ethernet ports are auto-sensing and can automatically adjust to transmit and receive data over straight-through or cross-over Ethernet connections. For a diagram showing T568A and T568B wiring, see "Ethernet and Console Ports" on page 30.

Note: The default IP address/netmask for the MGT interface is 192.168.2.10/24. For the LAN interface, the default IP address/netmask is 192.168.3.10/24. The IP address of the default gateway is 192.168.2.1.

The pin assignments in the male DB-9 console port follow the EIA (Electronic Industries Alliance) RS-232 standard. To make a serial connection between your management system and the console port on the HiveManager, you can use a null modem serial cable, use another serial cable that complies with the RS-232 standard, or refer to the pin-to-signal mapping shown in Figure 3 to make your own serial cable. Connect one end of the cable to the console port on the HiveManager and the other end to the serial (or COM) port on your management system. The management system must have a VT100 terminal emulation program, such as Tera Term Pro[®] (a free terminal emulator) or Hilgraeve Hyperterminal[®] (provided with Windows[®] operating systems).

Figure 3 Console port pin assignments



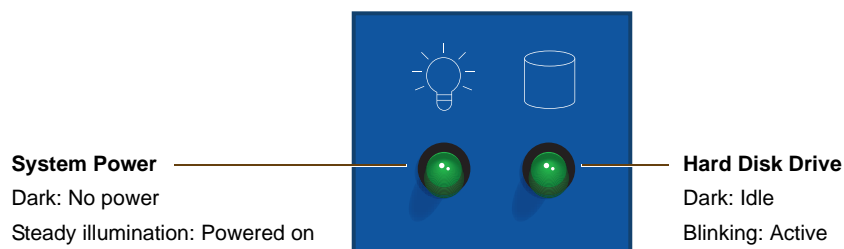
The serial connection settings are as follows:

- Bits per second: 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none

Status LEDs

The two status LEDs on the front of the HiveManager indicate various states of activity through their color (dark, green, amber) and illumination patterns (steady glow or blinking). The meanings of the various color + illumination patterns for each LED are shown in Figure 4.

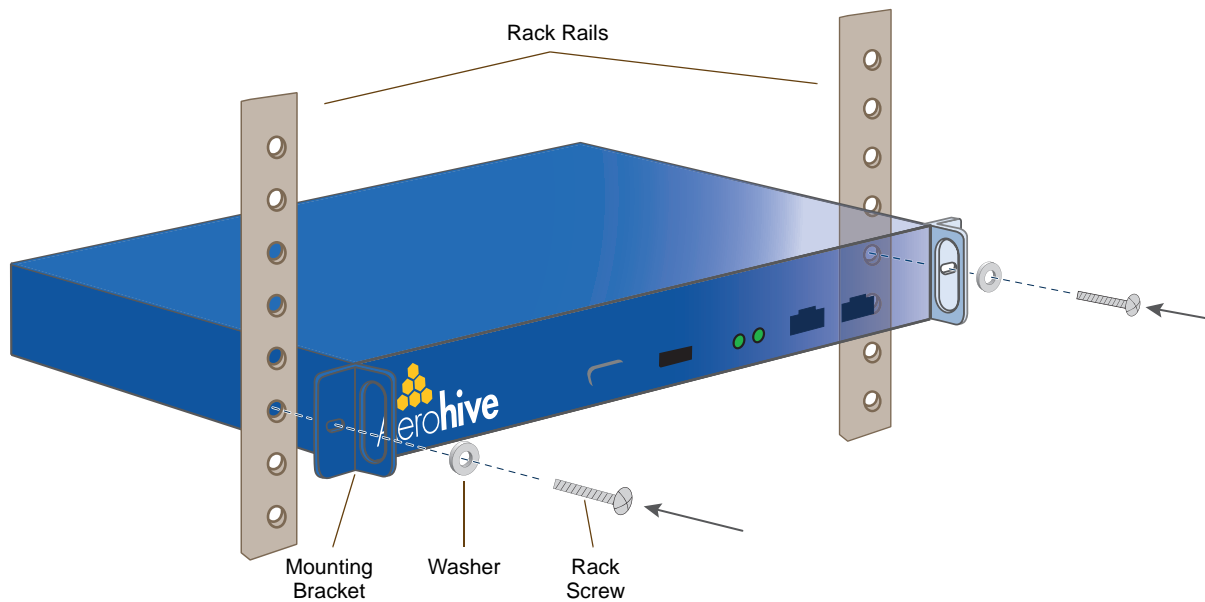
Figure 4 Status LEDs



RACK MOUNTING THE HIVE MANAGER

You can mount the HiveManager in a standard 19" (48 cm) equipment rack with two rack screws—typically 3/4", 1/2", or 3/8" long with 10-32 threads. The HiveManager ships with mounting brackets already attached to its left and right sides near the front panel (see [Figure 1 on page 90](#)). In this position, you can front mount the HiveManager as shown in [Figure 5](#). Depending on the layout of your equipment rack, you might need to mount the HiveManager in reverse. To do that, move the brackets to the left and right sides near the rear before mounting it.

Figure 5 Mounting the HiveManager in an equipment rack



1. Position the HiveManager so that the holes in the mounting brackets align with two mounting holes in the equipment rack rails.
2. Insert a screw through a washer, the hole in one of the mounting brackets, and a hole in the rail.
3. Tighten the screw until it is secure.
4. Repeat steps 2 and 3 to secure the other side of the HiveManager to the rack.

DEVICE, POWER, AND ENVIRONMENTAL SPECIFICATIONS

Understanding the range of specifications for the HiveManager is necessary for optimal deployment and operation of the device. The following specifications describe the physical features and hardware components, the electrical requirements for the power supply and cord, and the temperature and humidity ranges in which the device can operate.

Device Specifications

- Form factor: 1U rack-mountable device
- Chassis dimensions: 16 13/16" W x 1 3/4" H x 15 13/16" D (42.7 cm W x 4.4 cm H x 40.2 cm D)
- Weight: 13.75 lb. (6.24 kg)
- Serial port: male DB-9 RS-232 port (bits per second:9600, data bits: 8, parity: none, stop bits: 1, flow control: none)
- USB port: standard Type A USB 2.0 port
- Ethernet ports: MGT and LAN – autosensing 10/100/1000Base-T Mbps

Power Specifications

- ATX (Advanced Technology Extended) autoswitching power supply with PFC (power factor corrector):
 - Input: 100 - 240 VAC
 - Output: 250 watts
- Power supply cord: Standard three conductor SVT 18AWG cord with an NEMA5-15P three-prong male plug and three-pin socket

Environmental Specifications

- Operating temperature: 32 to 140 degrees F (0 to 60 degrees C)
- Storage temperature: -4 to 176 degrees F (-20 to 80 degrees C)
- Relative Humidity: 10% - 90% (noncondensing)

Chapter 8 The High Capacity HiveManager Platform

The High Capacity HiveManager is a management system that provides centralized configuration, monitoring, and reporting for multiple HiveAPs. The following are a few of the many benefits that a HiveManager offers:

- Simplified installations and management of up to 5000 HiveAPs
- Profile-based configurations that simplify the deployment of large numbers of HiveAPs
- Scheduled firmware upgrades on HiveAPs by location
- Exportation of detailed information on HiveAPs for reporting
- Hot swappable power supplies
- Cold swappable hard disk drives

This chapter covers the following topics related to the High Capacity HiveManager platform:

- ["Product Overview" on page 96](#)
- ["Rack Mounting the High Capacity HiveManager" on page 98](#)
- ["Replacing Power Supplies" on page 101](#)
- ["Replacing Hard Disk Drives" on page 102](#)
- ["Device, Power, and Environmental Specifications" on page 103](#)

PRODUCT OVERVIEW

The Aerohive High Capacity HiveManager is a central management system for configuring and monitoring HiveAPs. You can see its hardware components in [Figure 1](#) and read a description of each component in [Table 1](#).

Figure 1 High Capacity HiveManager hardware components

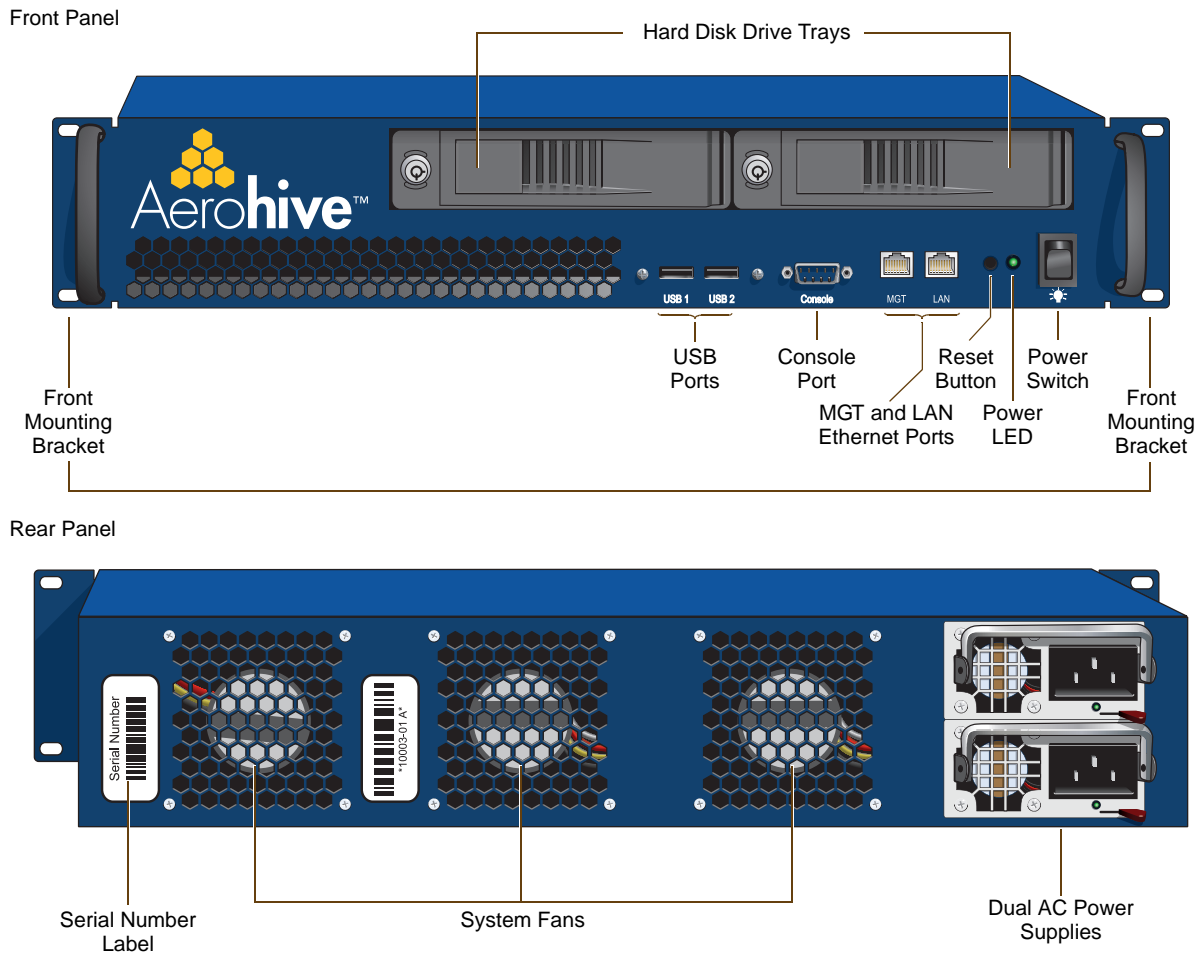


Table 1 High Capacity HiveManager component descriptions

Component	Description
Hard Disk Drive Trays	The two hard disk drive trays contain first-level RAID (Redundant Array of Independent Drives) mirrored hard disk drives to provide fault tolerance, data reliability, and increased performance.
Front Mounting Brackets	When used with the rack mounting kit, the two front mounting brackets allow you to mount the High Capacity HiveManager in a standard 19" (48.26 cm) equipment rack. For rack mounting instructions, see "Rack Mounting the High Capacity HiveManager" on page 98.
USB Ports	The USB ports are reserved for internal use.

Component	Description
Console Port	<p>A male DB-9 serial port to which you can make a console connection using an RS-232 (or "null modem") cable. The pin assignments are the same as those on the HiveManager and on the HiveAP (see "Ethernet and Console Ports" on page 30).</p> <p>The management station from which you make a serial connection to the HiveManager must have a VT100 emulation program, such as Tera Term Pro[®] (a free terminal emulator) or Hilgraeve Hyperterminal[®] (provided with Windows[®] operating systems). The following are the serial connection settings: bits per second: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none. The default login name is <i>admin</i> and the password is <i>aerohive</i>. After making a connection, you can access the Linux operating system.</p>
MGT and LAN Ethernet Ports	<p>The MGT and LAN Ethernet ports are compatible with 10/100/1000-Mbps connections, automatically negotiate half- and full-duplex mode with the connecting devices, and support RJ-45 connectors. They are autosensing and automatically adjust to straight-through and cross-over Ethernet cables. The two ports allow you to separate traffic between the HiveManager and its administrators from traffic between the HiveManager and the HiveAPs it manages. The wiring terminates the same way as that on the standard capacity HiveManager (see "Ethernet and Console Ports" on page 91).</p>
Reset Button	<p>The reset button allows you to reboot the High Capacity HiveManager. Insert a paper clip, or something similar, into the hole and press the reset button between 1 and 5 seconds. After releasing the button, the Power LED goes dark, and then glows steady amber while the software loads and the system performs a self-test. After the software finishes loading, the Power LED glows steady green.</p>
Power LED	<p>The power LED conveys the operational states for the system power: dark = no power; steady green = powered on.</p>
On/Off Switch	<p>The on and off switch controls the power to the HiveManager.</p>
Serial Number Label	<p>The serial number label contains the serial number for the device.</p>
System Fans	<p>The three system fans maintain an optimum operating temperature. Be sure that air flow through the system fan vents is not obstructed.</p>
Dual AC Power Supplies	<p>There are two power supplies. Each three-prong AC power inlet is a C14 chassis plug through which you can connect the HiveManager to a 100 - 240-volt AC power source using the 10-amp/125-volt IEC power cords that ship with the product. By cabling each power supply to a different source, they provide redundancy in the event of a single power failure. Each power supply has a fan that maintains its temperature. It is important that nothing obstructs the air flow to these fans so that the power supplies do not overheat.</p>

RACK MOUNTING THE HIGH CAPACITY HIVEMANAGER

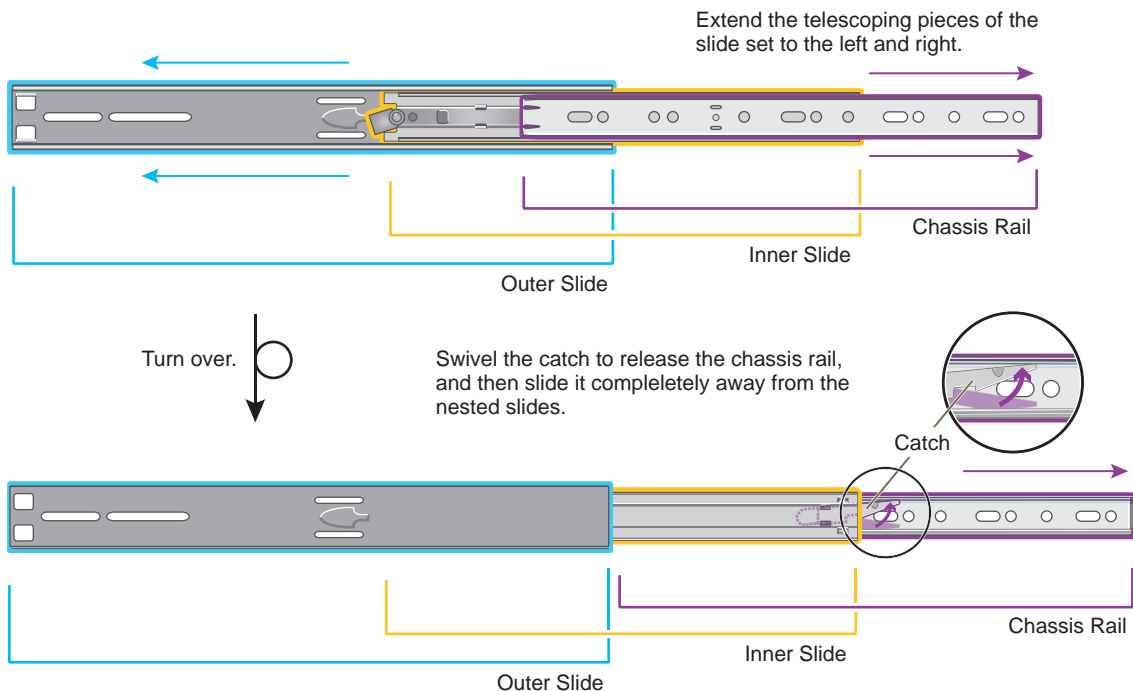
Use the rack mounting kit to mount the High Capacity HiveManager in a standard 19" (48 cm) equipment rack. The rack mounting kit contains the following items:

- (2) slide sets (each consisting of an outer slide, inner slide, and chassis rail)
- (2) rear mounting brackets
- (4) bar nuts
- (4) locator pins
- (6) slot-head machine screws with 8-32 threads - for attaching the mounting brackets to the outer slides
- (14) cross-head machine screws with 10-32 threads - for attaching the chassis rails to the HiveManager, and the front and the rear mounting brackets to equipment rack rails with tapped holes or to the enclosed bar nuts when the rack rails have round holes

Note: Because of the weight of the device (34 lb./ 15.42 kg without rails) , two people are required to rack mount it safely.

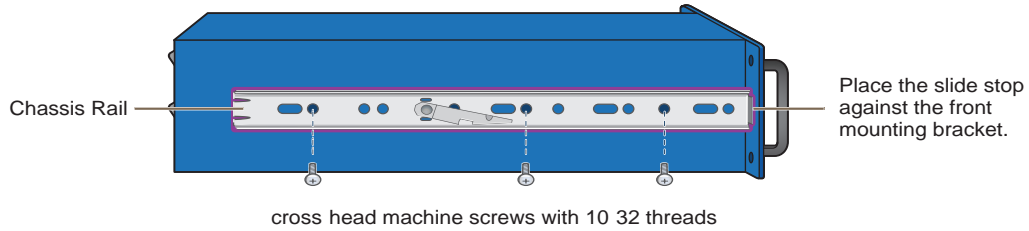
1. After checking that the mounting kit contains the above parts, separate the chassis rails from each slide set, as shown in [Figure 2](#).

Figure 2 Separating the chassis rail from the nested slides



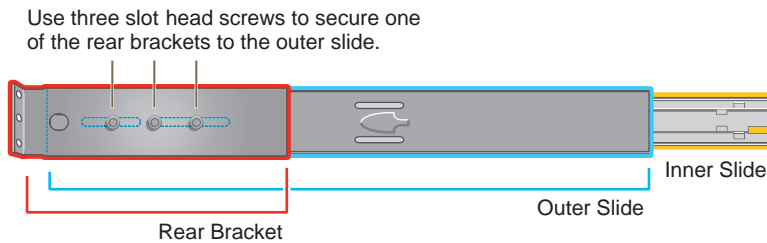
2. Position one of the chassis rails so that the slide stop is near the HiveManager mounting bracket near the front panel and the front and rear holes in the chassis rail align with the holes in the side of the HiveManager. Use three of the cross-head screws to secure the chassis rail to the HiveManager chassis as shown in [Figure 3 on page 99](#).

Figure 3 Attaching the chassis rail to the HiveManager



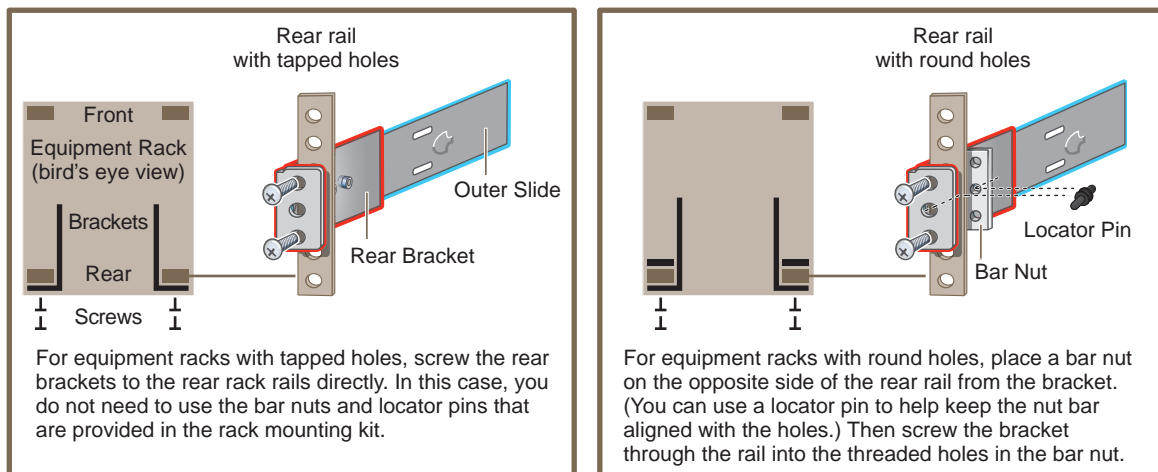
3. Secure the other chassis rail to the other side of the HiveManager.
4. Use three slot-head screws to attach the rear mounting bracket to the outer slide. Insert the screws through the rounded slots in the outer slide into the threaded holes in the bracket and tighten them as shown in Figure 4.

Figure 4 Attaching the rear bracket to the outer slide



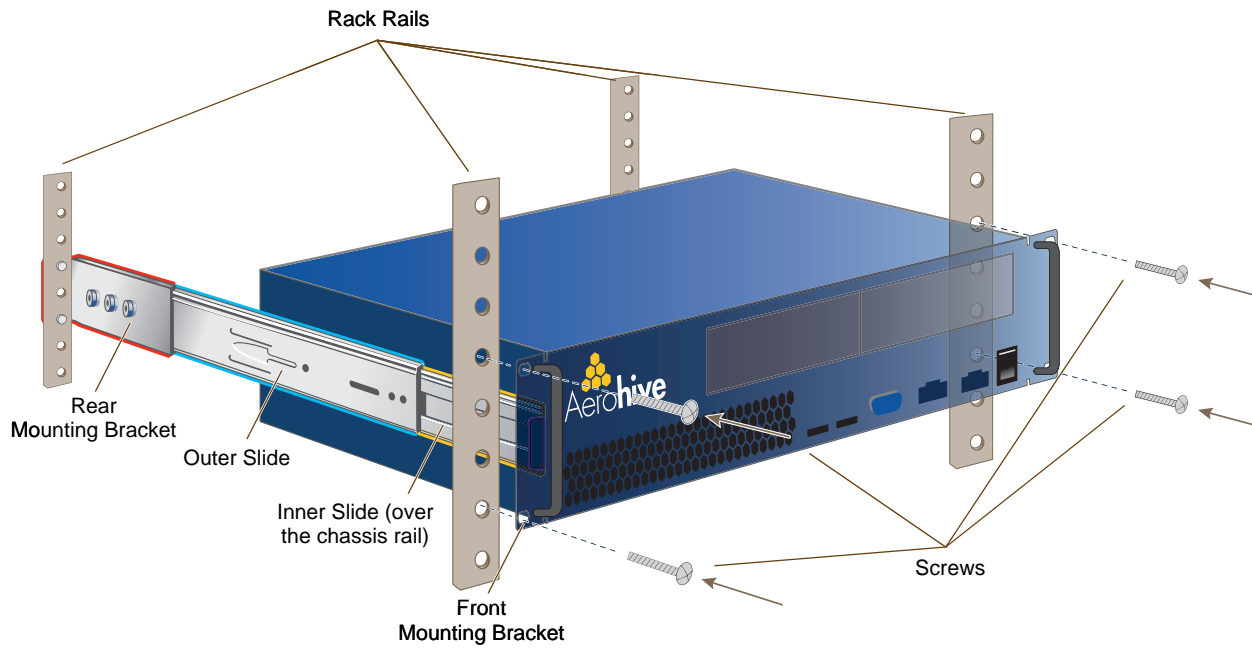
5. Use the remaining three slot-head screws to attach the other rear mounting bracket to the other outer slide.
6. Fasten the rear mounting brackets—and the slides attached to them—to the rear equipment rack rails. Depending on the type of holes in the equipment rack, use one of the following methods:
 - For tapped (threaded) holes, use two screws to fasten the brackets directly to the rack rails. Use the cross-head screws (with 10-32 threads) if they fit the holes in the rack.
 - For round holes, use the cross-head screws to fasten the brackets through the holes in the rack rails to the bar nuts. You can use the locator pins to help keep the bar nuts aligned to the holes. See Figure 5.

Figure 5 Fastening the rear mounting brackets to the rack rails



7. From the front of the equipment rack, guide the chassis rails on the sides of the HiveManager into the inner slides. Then push the HiveManager into the rack until the front mounting brackets are flush against the front rack rails.
8. Using four screws—two for each of the front brackets—fasten the HiveManager to the equipment rack as shown in [Figure 6](#). If the rack has round holes, use the two remaining nut bars (and locator pins) and thread the screws through the rack rails into them.

Figure 6 Mounting the HiveManager in an equipment rack



The HiveManager is now securely mounted to the front and rear rails of the equipment rack.

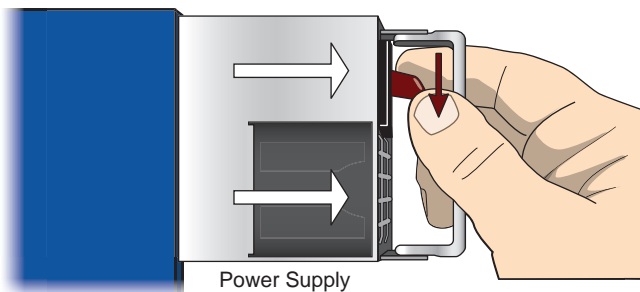
REPLACING POWER SUPPLIES

The high capacity HiveManager has a pair of redundant, hot-swappable power supplies. If one of the power supplies fails, the other will continue to power the device. When a power supply fails, a continuous beeping alarm sounds and the power LED glows amber. To replace the failed power supply, do the following:

1. Disconnect the failed power supply from the power source.
2. Lower the handle to a horizontal position.
3. With your index finger, press the red release lever to the left.
4. While holding the release lever to the left, grip the handle between your thumb and second finger, and pull the power supply straight out. See [Figure 7](#).

Figure 7 Removing a power supply

Rear of High Capacity HiveManager (bird's eye view)

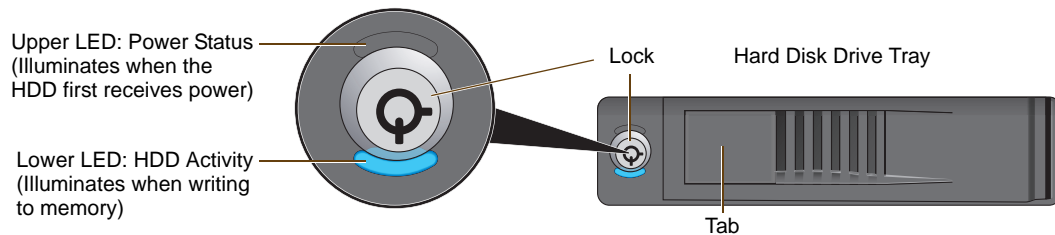


5. Insert a working power supply into the vacant bay and push it straight in until it is fully seated.
The red release automatically slides back to the right to secure the power supply in place.
6. Connect the power supply to the power source.

REPLACING HARD DISK DRIVES

To provide fault tolerance from disk errors and single disk failure, the high capacity HiveManager uses level 1 RAID (Redundant Array of Independent Drives) HDDs (hard disk drives). Each HDD holds identical data, the data that is written to one disk being mirrored to the other. The lower LEDs on the front of each HDD flash in unison to indicate that they are writing data to memory. The upper LEDs indicate that they have power. See [Figure 8](#).

Figure 8 Hard disk drive LEDs



If you notice that only one of the lower LEDs is flashing while the other is dark, then there is a HDD failure. Although the HiveManager can continue with just one operational HDD, you should replace the faulty HDD soon.

Note: HiveManager HDDs are not hot swappable. You must turn off the power before replacing a HDD.

1. Turn off the HiveManager.
2. Unlock the HDD tray door for the disk that you want to replace.
3. Pull the tab on the left side of the door, and open the door, swivelling it on the hinge along its right side.
As you open the door, the HDD tray automatically extends.
4. Remove the failed HDD and insert a replacement

Note: The replacement disk drive must be new or, if it has been used, there must not be a root file system on it. Also, it must be the same size as or bigger than the other disk drive.

5. Close the door and lock it again.
6. Connect a serial cable to the console port
7. Connect one end of an RS-232 serial cable to the male DB-9 console port on the HiveManager and other end to the serial port (or COM port) on your management system.
8. Start a serial connection as explained in "[Changing Network Settings](#)" on page 109.
9. Turn on the HiveManager.
10. While it is booting up, press and hold down the CTRL+A keys until the utility console appears.
11. From the main menu, select **Manage Arrays**. (An array is the logical representation of a physical HDD unit.)
12. From the list of arrays, select the one that you want to rebuild.
13. Press CTRL+R to rebuild it.

The rebuild process takes about 30 minutes. When done, the utility console notifies you with a message.

14. Confirm that the process is complete.

The HiveManager continues booting up with the new HDD replacement in operation.

DEVICE, POWER, AND ENVIRONMENTAL SPECIFICATIONS

Understanding the range of specifications for the high capacity HiveManager is necessary for the optimal deployment and operation of the device. The following specifications describe the physical features and hardware components, the electrical requirements for the power supply and cord, and the temperature and humidity ranges in which the device can operate.

Device Specifications

- Form factor: 2U rack-mountable device
- Chassis dimensions: 16 13/16" W x 3 1/2" H x 17" D (42.7 cm W x 8.9 cm H x 43.2 cm D)
- Weight: 34 lb. (15.42 kg)
- Serial port: male DB-9 RS-232 port (bits per second:9600, data bits: 8, parity: none, stop bits: 1, flow control: none)
- USB port: standard Type A USB 2.0 port
- Ethernet ports: MGT and LAN – autosensing 10/100/1000Base-T Mbps

Power Specifications

- Redundant ATX (Advanced Technology Extended) autoswitching power supplies with PFC (power factor corrector):
 - Input: 100 - 240 VAC
 - Output: 700 watts
- Power supply cords: Standard three conductor SVT 18AWG cords with an NEMA5-15P three-prong male plug and three-pin socket

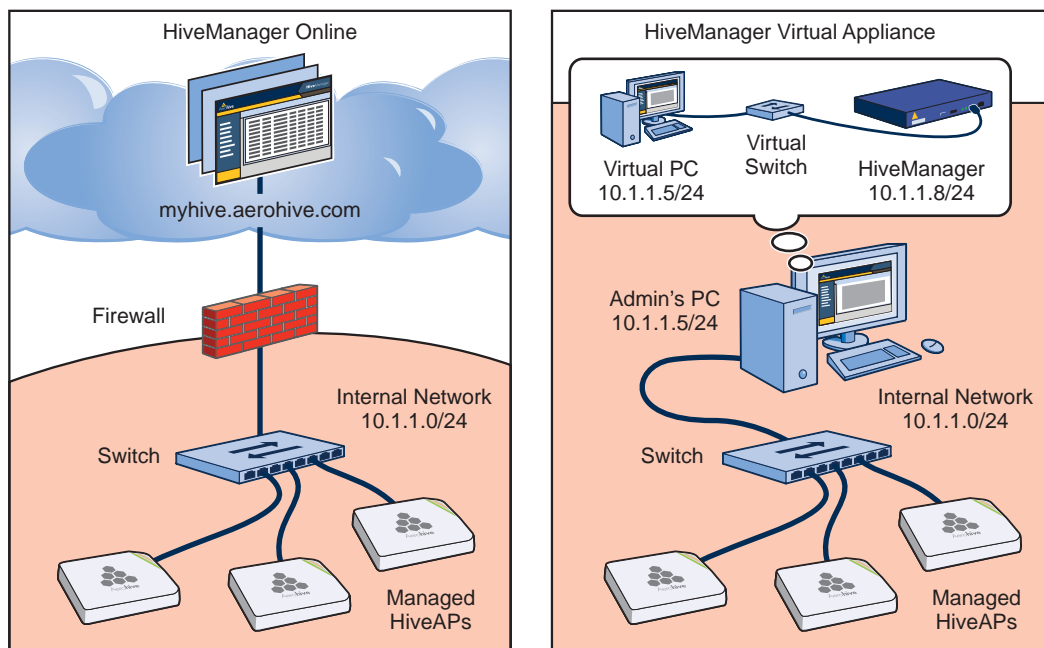
Environmental Specifications

- Operating temperature: 32 to 140 degrees F (0 to 60 degrees C)
- Storage temperature: -4 to 176 degrees F (-20 to 80 degrees C)
- Relative Humidity: 10% - 90% (noncondensing)

Chapter 9 HiveManager Online and HiveManager Virtual Appliance

In addition to a physical HiveManager appliance, the HiveManager network management system is available in two other forms. HiveManager Online is a cloud-based service running on hardware hosted and maintained by Aerohive and HiveManager Virtual Appliance is VMware that you can install and run on a computer on your network (see Figure 1). These two management systems provide cost-effective alternatives for managing WLAN networks that might not require the investment of a physical HiveManager appliance.

Figure 1 HiveManager Online and HiveManager Virtual Appliance



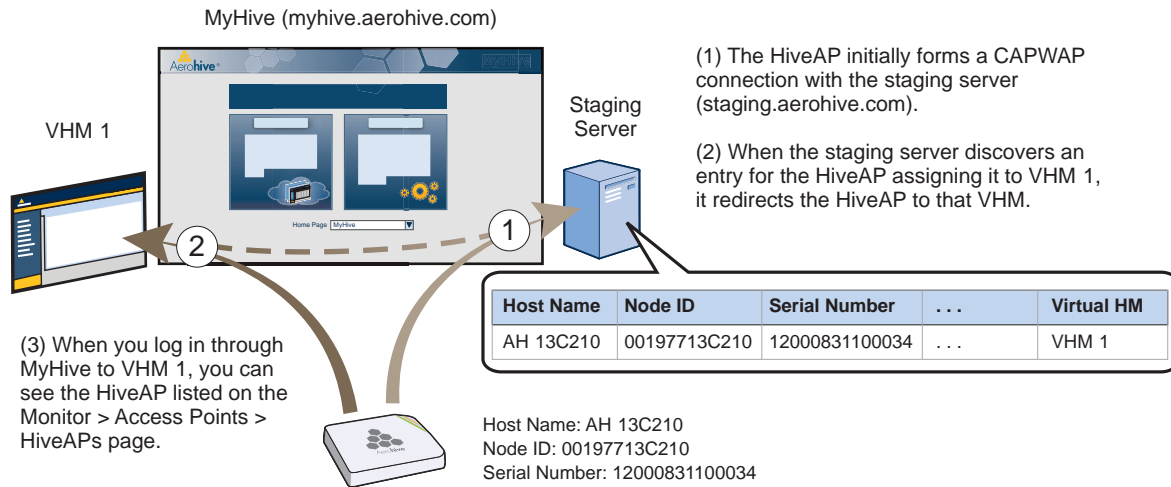
HIVEMANAGER ONLINE

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 HiveAPs. 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 HiveAPs.

After purchasing HiveManager Online, 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 staging server and your VHM.

Through your VHM, you can manage HiveAPs deployed remotely. By default, HiveAPs first try to connect to a local HiveManager. If they cannot find one locally, they then automatically try to reach the staging server, and if the MAC address or serial number of the HiveAP is already assigned to a VHM, the staging server redirects the HiveAP to it (see [Figure 2](#)).

Figure 2 MyHive



If the HiveAP MAC address or serial number is in the staging server but not yet assigned to the VHM, the HiveAP that forms a CAPWAP connection with the staging server remains connected to it. If the HiveAP MAC address or serial number is not in the staging server, then the staging server does not respond to the CAPWAP connection attempts from that HiveAP. For details about the initial CAPWAP connection process, see ["How HiveAPs Connect to HiveManager"](#) on page 133.

HIVEMANAGER VIRTUAL APPLIANCE

HiveManager Virtual Appliance (HM VA) is similar to a physical HiveManager appliance except that it is available as VMware that you load onto a computer of your choice. HM VA ships as VMware on a USB flash drive.

Figure 3 HiveManager Virtual Appliance ships as VMware on a USB flash drive



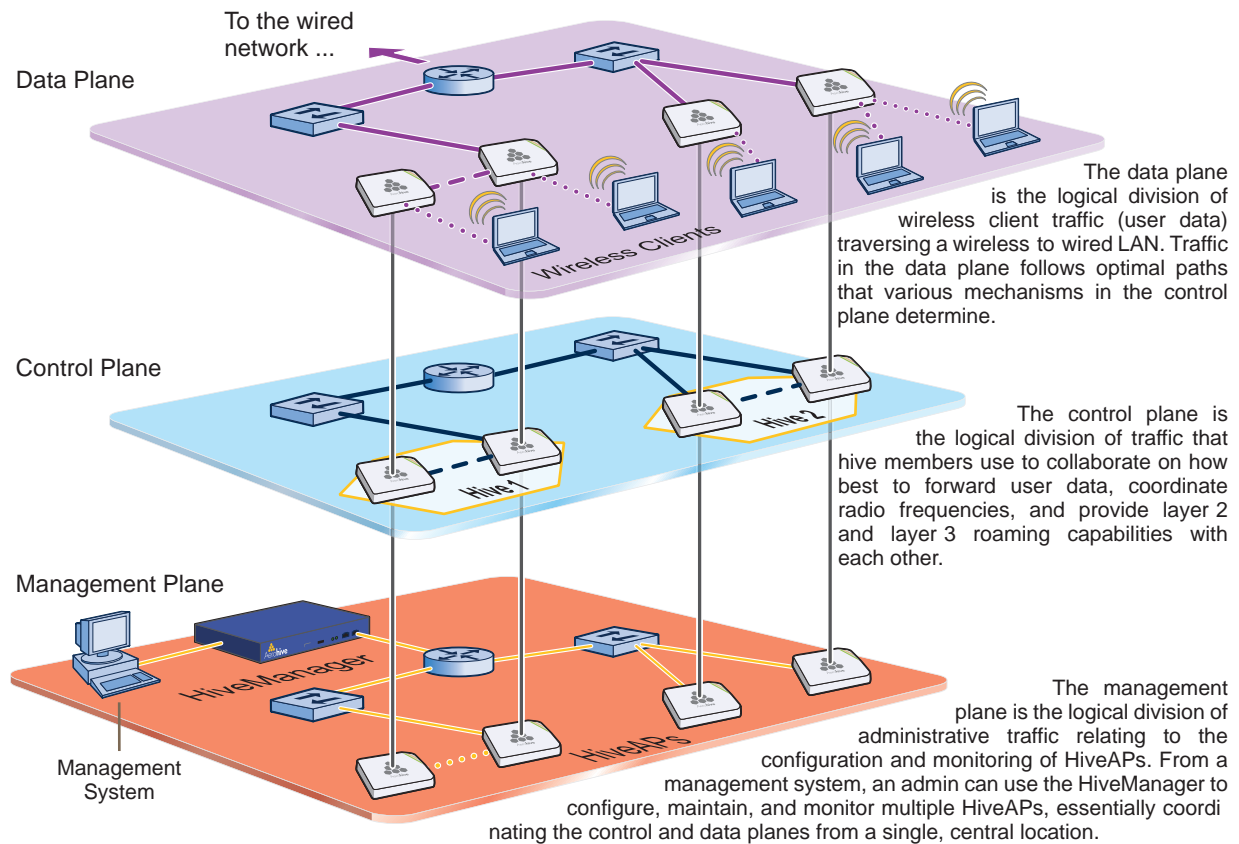
You must first install a VMware product such as VMware Workstation or VMware Player on your computer. Then install HM VA on the VMware workstation or player, where it runs like a virtual server inside your computer. HM VA forms a virtual layer 2 connection to your computer—much as if the two were connected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

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

Chapter 10 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 HiveAPs. On the control plane, HiveAPs 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 HiveAPs. 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 HiveAPs it manages only affects HiveAP 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 HiveAP firmware. The sections are as follows:

- ["Installing and Connecting to the HiveManager GUI" on page 109](#)
- ["Introduction to the HiveManager GUI" on page 113](#)
 - ["Viewing Reports" on page 114](#)
 - ["Searching" on page 115](#)
 - ["Multiselecting" on page 116](#)
 - ["Cloning Configurations" on page 116](#)
 - ["Sorting Displayed Data" on page 117](#)
- ["HiveManager Configuration Workflow \(Enterprise Mode\)" on page 118](#)
- ["Updating Software on HiveManager" on page 119](#)
- ["Updating HiveOS Firmware" on page 120](#)
 - ["Updating HiveAPs in a Mesh Environment" on page 121](#)

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.

Note: 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 HiveAP 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. (For more details, see "[Ethernet and Console Ports](#)" on page 91.)

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 HiveAP 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).

You also need an order ID or, for a physical HiveManager appliance, a license key. You can obtain these by sending an email request to Aerohive Support at orders@aerohive.com. Include your sales order ID and—for a physical HiveManager appliance or HiveManager Virtual Appliance—a HiveManager system ID. Aerohive will send you back an order ID or license key.

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.

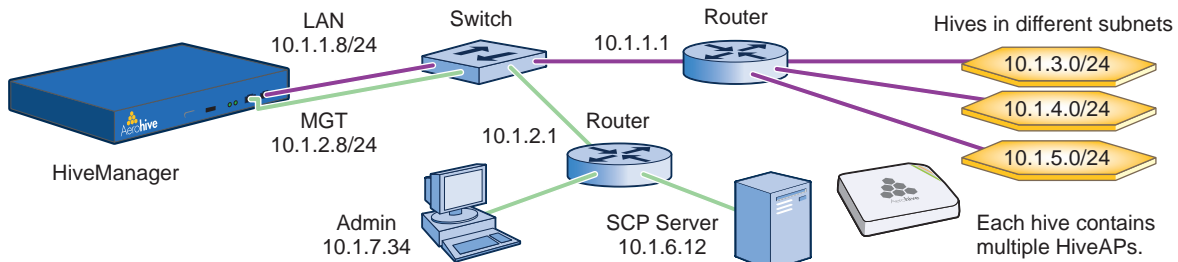
Note: The default IP address/netmask for the MGT interface is 192.168.2.10/24. The default gateway IP address is 192.168.2.1. The LAN interface is disabled by default and does not have a default IP address. You can define network settings for the LAN interface through the HiveManager GUI after you log 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
- HiveAP management traffic and configuration, file, and HiveOS image downloads to managed HiveAPs

When you enable both interfaces, HiveManager management traffic uses the MGT interface while HiveAP management traffic uses the LAN interface, as shown in [Figure 2](#).

Figure 2 Using both MGT and LAN interfaces



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

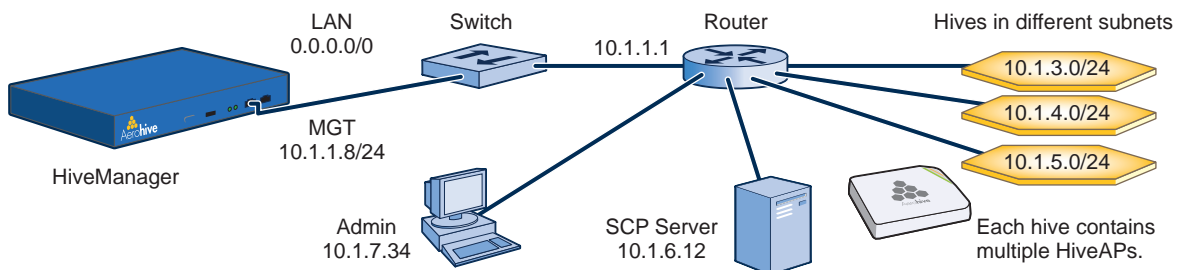
HiveManager sends traffic destined for 10.1.7.0/24 to 10.1.2.1.

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

Note: 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.

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 HiveAP management traffic would need to flow on the operational network because HiveManager would need to communicate with the HiveAPs from its MGT interface (see [Figure 3](#)). 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 3 Using just the MGT interface



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

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`

Note: 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 109.

A login prompt appears.

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

5. If you have not yet installed a HiveManager license on your HiveManager appliance, a prompt to enter an order ID or install a HiveManager license key appears (as shown below). For HiveManager Virtual Appliance, a prompt to enter an order ID appears immediately after logging in. For HiveManager Online, you first enter MyHive after logging in. Then the prompt to enter an order ID appears after you click the HiveManager Online button.

For a HiveManager appliance with Internet access, select **Enter Order ID**. Copy the order ID text string that Aerohive sent you in an email message, paste it in the Order ID field, and then click **Enter**. For HiveManager Online and HiveManager Virtual Appliance, copy the order ID text string, paste it in the Order ID field, and then click **Enter**. HiveManager transmits the order ID to the online Aerohive license server, which replies with all licenses associated with that order ID.

For a physical HiveManager appliance, you also have the option of installing a HiveManager license key, which is particularly 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 **Install**.

If you do not have an order ID or license yet, you can request that Aerohive send it to you. To accomplish this, HiveManager must have Internet access and email settings configured. If this is the first time to log in to HiveManager, you can access a limited area of the GUI to configure its email settings. Click **Continue**, navigate to Home > Administration > HiveManager Services, and select **Update Email Service Settings**. Enter the IP address or domain name of the SMTP server, enter an email address for HiveManager in the From Email field, and enter your own email address in the To Email 1 field. Also, configure any additional port, encryption, and authentication settings that your SMTP server requires. When done, click **Email Test**. If you receive an email message with the subject "testing", the settings are correct. Click **Update** to save them, and then click **Log Out** in the upper right corner of the GUI to return to the login prompt. After logging back in, the HiveManager License Information dialog box appears again. To generate an email containing the sales order number and system ID, simply click the [click here](#) hyperlink. In the Send Email to Aerohive dialog box that appears, enter the four-digit sales order number in the field provided, and then click **Send**. Optionally you can type the sales order number and system ID into an email of your own composition and send it to orders@aerohive.com. After you receive the order ID or license key in an email response, select **Install License Key**, copy the license key text string that Aerohive sent, paste it in the License Key field, and then click **Install**.

6. After entering an order ID or installing a license key, the Aerohive Networks, Inc. End User License Agreement appears. Read it over, and if you agree with its content, click **Agree**.

You are now logged in to the complete HiveManager GUI. Later, after completing the Start Here page in the next steps, you can check details about the order ID and licenses you installed on the Home > Administration > License Management page. You can also enter more licenses there, such as a User Manager license if necessary.

7. On the Start Here page, HiveManager presents a choice of administrative modes: **Express** or **Enterprise**. Express mode provides a simple set of configuration components designed for managing a single simple network. Enterprise mode provides a complete set of configuration components for managing multiple networks that require more advanced settings. Because the examples throughout this guide are based on Enterprise mode, select **Enterprise (recommended for more advanced networks)**.¹
8. After selecting Enterprise mode, you have the option of changing the root admin password for logging in to HiveAPs and HiveManager. The default password for both logins is *aerohive*. To set different passwords, enter them in the New HiveAP Password and New HiveManager Password fields, and then enter them again in the Confirm Password fields. The HiveAP password can be any alphanumeric string from 5 to 32 characters long, and the HiveManager password can be any alphanumeric string from 1 to 32 characters long.

If you want, you can change just one password at this time, or leave them both as the default and change them later. To see the password string that you enter, clear **Obscure Password**.

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.

9. To save your settings and enter the HiveManager GUI in Enterprise mode, click **Save**.
10. A message appears prompting you to confirm your selection of Enterprise mode. After reading the confirmation message, click **Yes**.

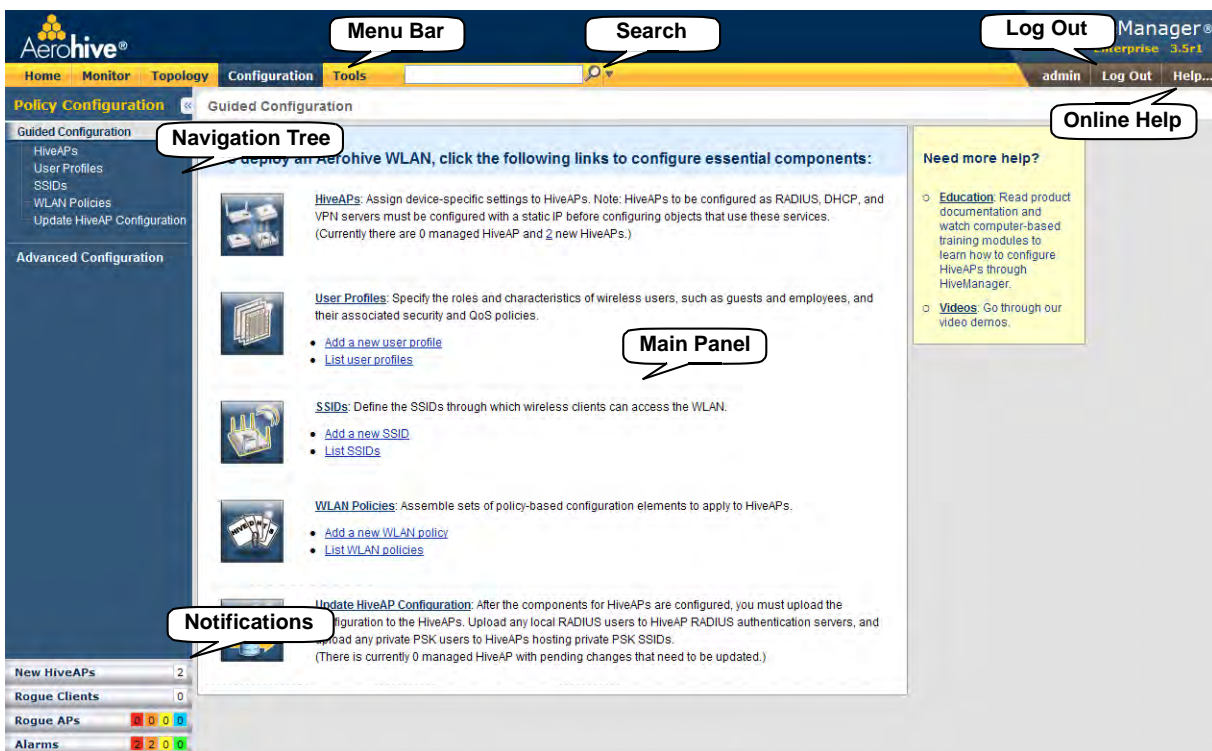
HiveManager displays the Guided Configuration page to assist you with the main configuration steps:

- Device-level settings for HiveAPs
- The three major WLAN policy-level configuration objects, which reference all other configuration objects: user profiles, SSIDs, and WLAN policies
- The transfer of the device- and policy-level settings from HiveManager to HiveAPs

INTRODUCTION TO THE HIVEMANAGER GUI

Using the HiveManager GUI, you can set up the configurations needed to deploy, manage, and monitor large numbers of HiveAPs. The configuration workflow is described in "[HiveManager Configuration Workflow \(Enterprise Mode\)](#)" on page 118. The GUI consists of several important sections, which are shown in [Figure 4](#).

Figure 4 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.

Search: This is a tool for finding a text string anywhere in the GUI (except in Reports). You can do a global search or confine a search to a specific part 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 computer-based training modules 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.

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

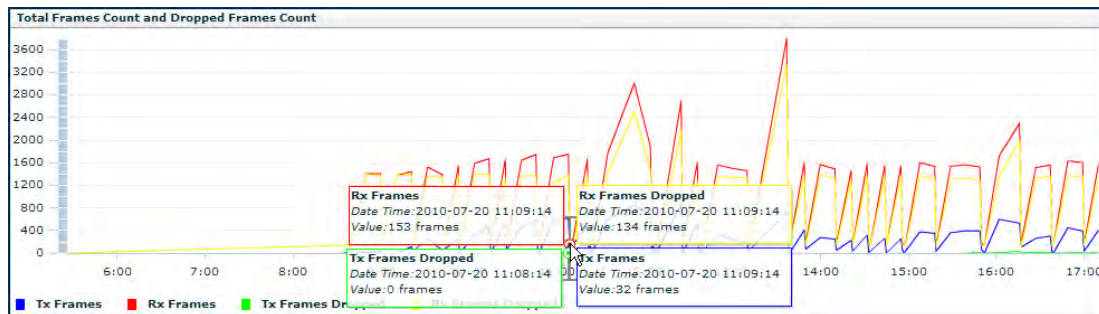
Notifications: HiveManager displays a summary of new HiveAPs, rogue clients, rogue APs, and alarms detected on managed HiveAPs here. Clicking a displayed number opens the relevant page with more details.

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

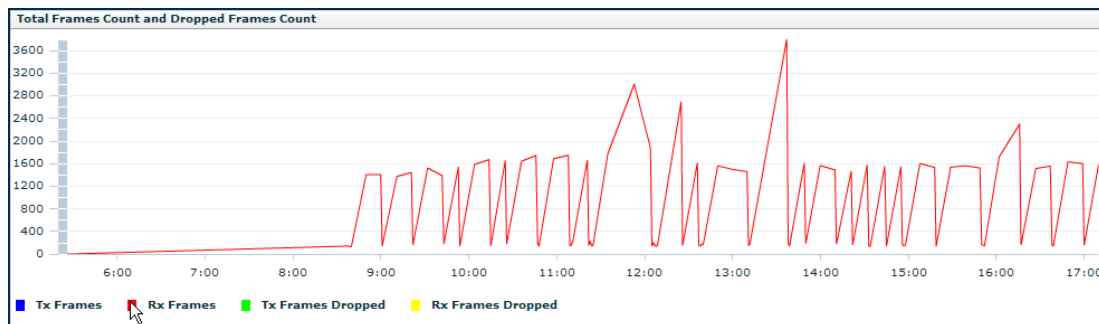
Viewing Reports

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*) or a report defined as a "New Report Version", moving your mouse over a color box in the legend hides all other lines except the one matching that color (see Figure 5).

Figure 5 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.

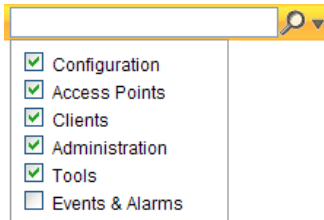


In the graph showing details for a selected active client, moving the mouse over a colored box in the legend hides all other lines except the one that is the same color as the box under the mouse. Here HiveManager only shows the red line for transmitted frames because the mouse is over the red box next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

Searching

The HiveManager GUI provides a search feature that you can use to find 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 6](#)).

Figure 6 Search tool



The following items are ignored when using the 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 7](#)).

Figure 7 Search results

Profile Name	SSID	Access Security	CWP Used	Enable MAC Authentication	Maximum Client Limit	Description
ssid0	ssid0	Open	false	false	100	default SSID profile
(For-Cloning)-Symbol-Scanner	(For-Cloning)-Symbol-Scanner	Open	false	false	100	SSID profile template
(For-Cloning)-SpectralLink	(For-Cloning)-SpectralLink	Open	false	false	100	SSID profile template
(For-Cloning)-Legacy-Clients	(For-Cloning)-Legacy-Clients	Open	false	false	100	SSID profile template
(For-Cloning)-HighCapacity-a/g/n	(For-Cloning)-HighCapacity-a/g/n	Open	false	false	100	SSID profile template
(For-Cloning)-BlackBerry	(For-Cloning)-BlackBerry	Open	false	false	100	SSID profile template

Note: 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.

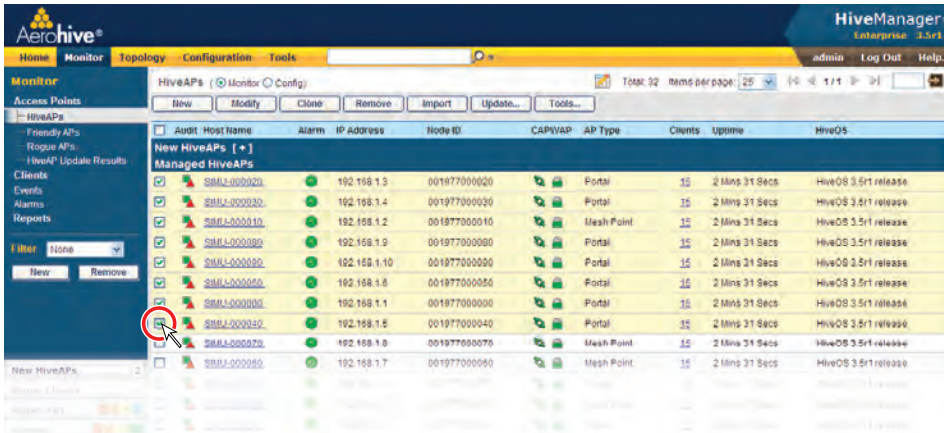
Multiselecting

You can select multiple objects to make the same modifications or perform the same operation to all of them at once.

Figure 8 Selecting multiple new HiveAPs

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.



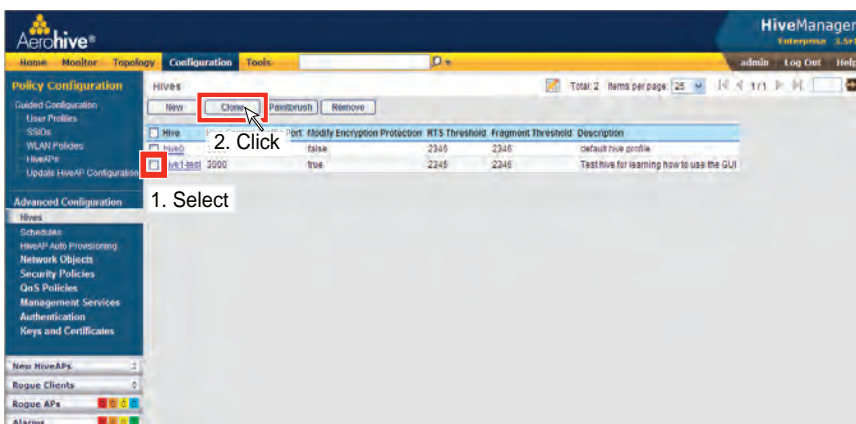
Here, you use the shift-click multiselection method to select a set of the topmost eight HiveAPs in the list; that is, you select the check box for the top HiveAP and hold down the SHIFT key while selecting the check box for the eighth HiveAP from the top.

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.

Figure 9 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.

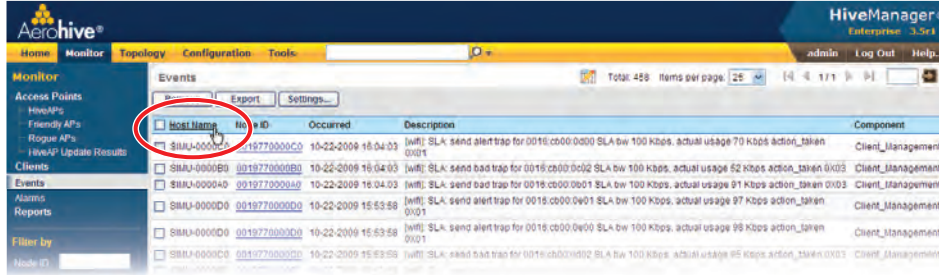


Sorting Displayed Data

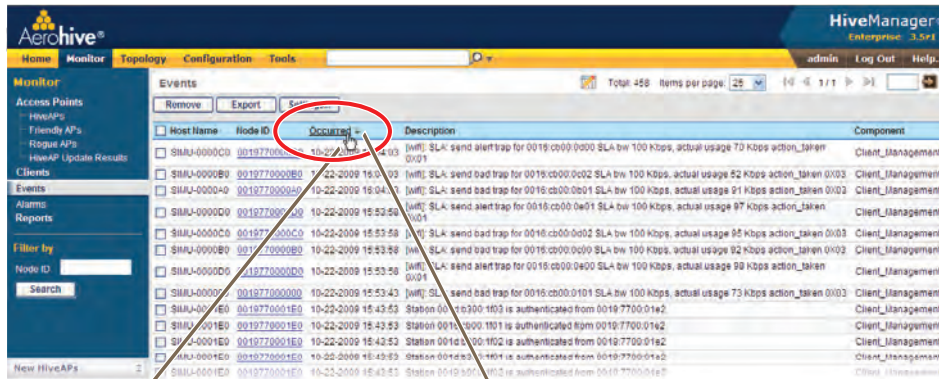
You can control how the GUI displays data in the main panel by clicking a column header. This causes the displayed content to reorder itself alphanumerically or chronologically in either ascending or descending order. Clicking the header a second time reverses the order in which the data is displayed.

Figure 10 Sorting event log entries by HiveAP 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 from the top



Indicates that the list appears in ascending order from the bottom

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 HiveAPs, which are now connected to HiveManager, you can start configuring the HiveAPs through HiveManager.² You can configure numerous objects, some of which might need to reference other objects. An efficient configuration strategy is first to define any objects that you will later need to use when configuring other objects. If one object must reference another that has not yet been defined, there is usually a "New" button that you can click, define the object you need, and then return to the first dialog box to continue with its configuration.

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

The typical workflow proceeds like this:

1. Use default settings or configure new settings for various features that, when combined, constitute a user profile, an SSID, and a WLAN policy. These are the three main objects that reference most of the other ones. Together these features define policies that you can apply to multiple HiveAPs.

User Profile →	SSID →	WLAN Policy
OoS Rate Control & Queuing	user profiles	SSIDs
IP firewall rules	captive web portal (possibly including a RADIUS server profile and certificates)	hive (possibly including MAC filters and MAC DoS)
MAC firewall rules	MAC filters	management options
GRE and VPN tunnel policies	schedules	QoS classifier and marker maps, dynamic airtime scheduling
VLAN	IP DoS	traffic filters
SLA (service-level agreement) settings	MAC DoS	VPN service
attribute number		DNS, NTP, SNMP, syslog, location services
User Manager control		service settings for WIPS, virtual access console, ALG services, Mgt IP filter, LLDP/CDP link discovery protocols, and IP tracking

2. Define various device-level configuration objects to apply to individual HiveAPs. These include map, CAPWAP servers, radio profiles, scheduled configuration audits, RADIUS authentication server settings, and DHCP server or DHCP relay agent settings.
3. Apply the policy-level settings (contained within a WLAN policy) and device-level settings to one or more HiveAPs, and then push the configurations to physical HiveAP devices across the network.

2. When HiveAPs 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 HiveAPs. If the HiveAPs and HiveManager are in different subnets, then you can use one of several approaches to enable HiveAPs to connect to HiveManager. For information about these options, see ["How HiveAPs Connect to HiveManager" on page 133](#).

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, send an email request to support@aerohive.com to set one up.
2. When you have login credentials, visit 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 HiveAPs. First, you obtain new HiveAP firmware from Aerohive Support and upload it onto HiveManager. Then you push the firmware to the HiveAPs and activate it by rebooting them.

Note: When upgrading both HiveManager software and HiveOS firmware, do so in this order:

- Upgrade HiveManager (HiveManager can manage HiveAPs running the current version of HiveOS and also previous versions going back two major releases).
- Upload the new HiveOS firmware to the managed HiveAPs, and reboot them to activate it.
- Reload the HiveOS configurations to the managed HiveAPs—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 > Access Points > HiveAPs**.
4. In the HiveAPs window, select one or more HiveAPs, 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.

*Note: 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 HiveAPs and requires a manual reboot of the HiveAPs 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 HiveAPs, 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 HiveAPs—after HiveManager finishes loading it:

- **Activate at:** Select and set the time at which you want the HiveAPs to activate the firmware. To use this option accurately, make sure that both HiveManager and managed HiveAP clocks are synchronized.
- **Activate after:** Select to load the firmware on the selected HiveAPs 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 to load the firmware and not activate it. The loaded firmware gets activated the next time the HiveAP reboots.

Note: When choosing which option to use, consider how HiveManager connects to the HiveAPs it is updating. See "Updating HiveAPs in a Mesh Environment".

10. 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 HiveAPs, HiveManager will again apply the default settings.
11. Select the file you just loaded from the HiveOS Image drop-down list, select one or more HiveAPs 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 > Access Points > HiveAP Update Results page.

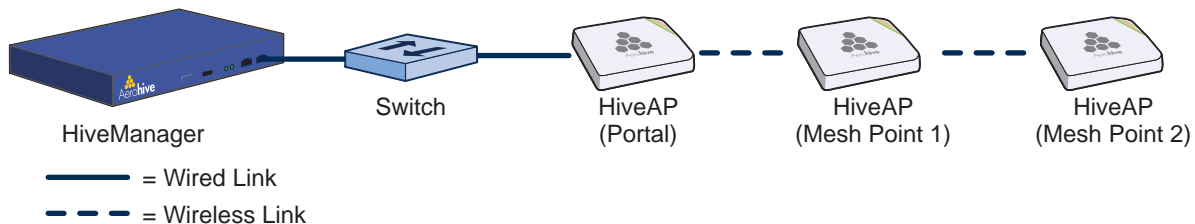
Updating HiveAPs in a Mesh Environment

When updating hive members in a mesh environment, be careful of the order in which the HiveAPs 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.

Note: 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 11 HiveAPs in a mesh environment

When updating HiveAPs 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 HiveAPs in such an environment, it is important to keep the path from the HiveManager to all HiveAPs clear so that the data transfer along that path is not disrupted. Therefore, when updating a firmware image or configuration on HiveAPs 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 HiveAP 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 HiveAPs have the firmware, rebooting any HiveAPs between them and HiveManager becomes inconsequential.

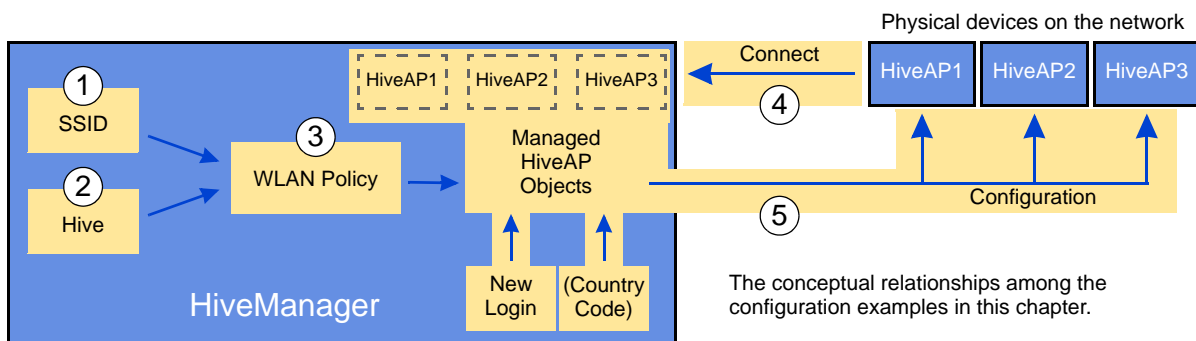
Chapter 11 Basic Configuration Examples

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

Note: Although maps provide a convenient method for organizing and managing your HiveAP deployment, they are not strictly required and are not covered in this chapter. For information about using maps, see "Example 1: Mapping Locations and Installing HiveAPs" on page 140.

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 HiveAPs through HiveManager. The examples are as follows:

- "Example 1: Defining an SSID" on page 124
Define the security and network settings that wireless clients and HiveAPs use to communicate.
- "Example 2: Creating a Hive" on page 127
Create a hive so that the HiveAPs can exchange information with each other to coordinate client access, provide best-path forwarding, and enforce QoS policy.
- "Example 3: Creating a WLAN Policy" on page 128
Define a WLAN policy, which contains the SSID and hive defined in the first two examples.
- "Example 4: Connecting HiveAPs to HiveManager" on page 129
Cable two HiveAPs to the network to act as portals and set up a third one as a mesh point. Put the HiveAPs on the same subnet as HiveManager and allow them to make a CAPWAP connection to HiveManager.
- "Example 5: Assigning the Configuration to HiveAPs" on page 135
Assign the WLAN policy to the HiveAPs. Also, change HiveAP login settings and—if necessary—country codes.



In the first three examples, you define configuration objects in the Configuration section of the GUI. In the last two examples, you connect some HiveAPs to the network, enable them to make a CAPWAP connection to HiveManager, and then manage them in the Monitor section of the GUI.

EXAMPLE 1: 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 define the following SSID, which uses a PSK (preshared key) for client authentication and data encryption:

SSID name: test1-psk

SSID access security: WPA/WPA2 PSK (Personal)

Preshared key: CmFwb01121

A PSK is the simplest way to provide client authentication and data encryption: simply configure an SSID with the same PSK on the HiveAP and its clients. A PSK authenticates clients by the simple fact that the clients and HiveAP have the same key. For data encryption, both the HiveAP 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 HiveAP and all its clients. With a large number of clients, this can be very time-consuming. For examples of key management solutions that are more suitable for large-scale deployments, see the 802.1X and private PSK examples in ["Common Configuration Examples" on page 139](#). For the present goal of showing how to use HiveManager to configure an SSID, the PSK method works well.

To configure the SSID, log in to the HiveManager GUI (see ["Installing and Connecting to the HiveManager GUI" on page 109](#)), click **Configuration > SSIDs > New**, enter the following, 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 reference a captive web portal; include default or modified data rate settings; apply DoS (denial of service) policies, MAC filters, and schedules; and specify the SSID name that the HiveAP 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 Available SSIDs list in the WLAN Policy dialog box. You will later choose this SSID when defining a WLAN policy in ["Example 3: Creating a WLAN Policy" on page 128](#).

When you type in 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 HiveAP 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.

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)

Use Default WPA/WPA2 PSK Settings: (select)

By default, when a HiveAP hosts a WPA/WPA2 PSK (Personal) SSID, it negotiates with clients over the use of WPA or WPA2 for key management and TKIP or CCMP (AES) for encryption, and uses whichever methods each client supports. Also, the PSK text string is in ASCII format by default.

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

With these settings, the HiveAP 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)

User profile assigned to users that associate with this SSID: **default-profile**

The predefined user profile "default-profile" applies the standard Aerohive Quality of Service level through the predefined QoS policy "def-user-qos" and assigns user traffic to VLAN 1.

SSID Broadcast Band: **2.4 GHz (11n/b/g)**

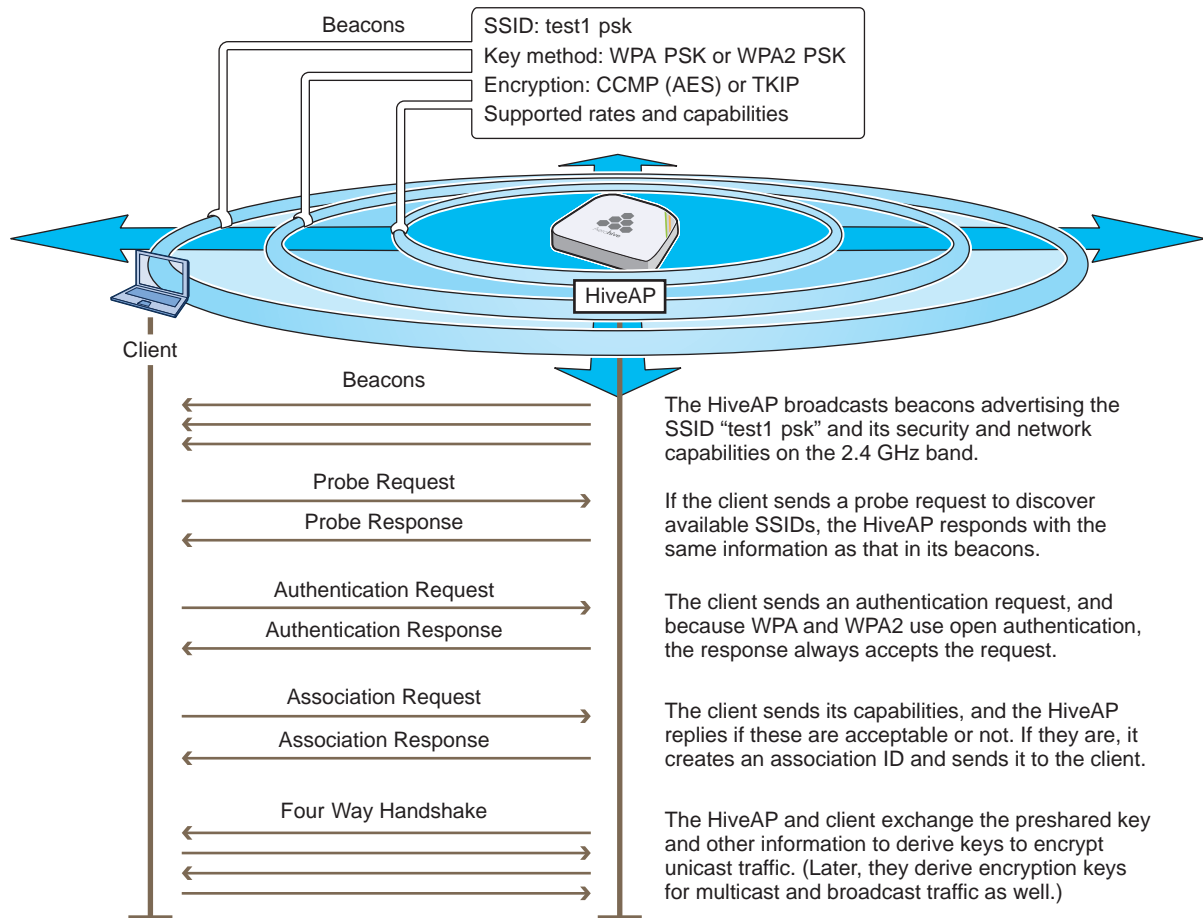
HiveAPs have two radios: a 2.4 GHz radio, which supports 802.11n/b/g, and a 5 GHz radio, which supports 802.11n/a. On all HiveAP models except the HiveAP 110, both radios can function concurrently. This setting broadcasts the SSID on the wifi0 interface, which is bound to the 2.4 GHz radio. (There is an assumption that your clients support at least one of the following IEEE standards: 802.11n, 802.11g, or 802.11b.)

As will be seen later in this chapter, one HiveAP will be deployed as a mesh point; that is, it will not have an Ethernet connection but will connect to the wired network over a wireless backhaul link through another HiveAP that does have an Ethernet connection (see ["Example 5: Assigning the Configuration to HiveAPs" on page 135](#)). Because of this, the HiveAPs must use one radio for wireless backhaul communications and the other radio for client access. By default, both the 2.4 GHz and 5 GHz radios are in access mode.

In the series of examples in this chapter, you set the 5 GHz radio in backhaul mode, and the 2.4 GHz radio in access mode. Therefore, you assign the SSID to the 2.4 GHz band.

To see how the different SSID settings determine the way that the HiveAP advertises the SSID and how clients form associations with it, see [Figure 1 on page 126](#).

Figure 1 How a client discovers the SSID and forms a secure association



EXAMPLE 2: CREATING A HIVE

A hive is a group of HiveAPs that exchange information with each other to form a collaborative whole. Through 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 HiveAP in the internal network to another HiveAP 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 open authentication and CCMP (AES) encryption. CCMP is a rough acronym for "Counter Mode with Cipher Block Chaining Message Authentication Code Protocol" that makes use of AES (Advanced Encryption Standard). This is very similar to the security provided by the SSID in the preceding example.

In this example, you define a hive and name it "hive-test1". Later, in ["Example 3: Creating a WLAN Policy" on page 128](#), you assign the hive to a WLAN policy, which in turn, you assign to HiveAP devices in ["Example 5: Assigning the Configuration to HiveAPs" on page 135](#).

Note: A WLAN policy is different from a hive. Whereas the members of a WLAN policy share a set of policy-based configurations, the members of a hive communicate with each other and coordinate their activities as access points. WLAN policy members share configurations. Hive members work together collaboratively.

Click **Configuration > Advanced Configuration > Hives > New**, enter the following, leave the other options at their default settings, and then click **Save**:

Hive: **hive1-test** (You cannot include spaces in the name of a hive.)

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

As was done in the previous example, this note and the name "hive1-test" are intended to act as reminders to replace this configuration later with a hive name that you really intend to use.

Modify Encryption Protection: **(select)**

Automatically generate password: **(select)**

The password is what hive members use when authenticating themselves to each other over the wireless backhaul link using WPA-PSK CCMP (AES). As an admin, you never need to see or know what this string is; therefore, using the automatic password generation method saves you the trouble of inventing a long—up to 63 characters—and random alphanumeric string.

Optional Settings: Leave the optional settings as they are by default. For information about these settings, and about any setting in the GUI for that matter, see the HiveManager online Help system.

EXAMPLE 3: CREATING A WLAN POLICY

Through 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 WLAN policy is an assembly of policy-level feature configurations that HiveManager pushes to all HiveAPs 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 WLAN policy that includes the SSID and hive configured in the previous two examples. Although the New WLAN Policy dialog box consists of several pages, for this basic configuration, you only need to configure items on the first page (see [Figure 2](#)).

Figure 2 WLAN policy general settings

WLAN Policy Name and Description

Hive

SSID Profile

SSID Profile	SSID	Captive Web Portal	AAA Servers	Radio	User Profile	User Profile Role
test1-psk	test1-psk	-	-	2.4 GHz (11n/b/g)	default-profile	Default

Click **Configuration > WLAN Policies > New**, enter the following on the first page of the new WLAN policy dialog box, leave all the other settings as they are, and then click **Save**:

Name: **wlan-policy-test1** (You cannot use spaces in the WLAN policy name.)

Description: **Test WLAN policy for learning how to use the GUI; remove later**

Hive: **hive1-test** (The hive was previously configured in ["Example 2: Creating a Hive" on page 127.](#))

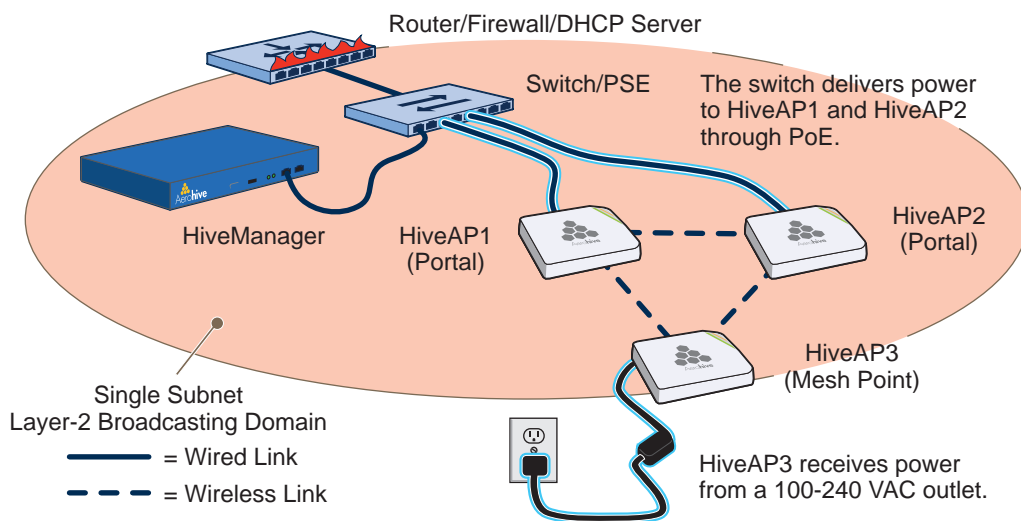
SSID Profiles: Click **Add/Remove SSID Profile**, choose **test1-psk** in the Available SSID Profiles list, click the right arrow (>) to move it to the Selected SSID Profiles list, and then click **Apply**. (The SSID was previously configured in ["Example 1: Defining an SSID" on page 124.](#))

The creation of a WLAN policy that puts the HiveAPs to which you apply it in a hive and provides them with an SSID is complete. In the following examples, you deploy several HiveAPs on a network, accept them for HiveManager management, and then apply the WLAN policy to them.

EXAMPLE 4: CONNECTING HIVEAPs TO HIVEMANAGER

In this example, you set up three HiveAPs for management through HiveManager. Cable two of the HiveAPs—HiveAP1 and HiveAP2—to the network. Run an Ethernet cable from the eth0 port on each HiveAP to a switch so that they are in the same subnet as the IP address of the MGT interface on HiveManager. (Neither the HiveAP 300 eth1 port nor the HiveManager LAN port are used in this example.) You can use AC/DC power adaptors 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 adaptors and PoE injectors are available from Aerohive as options.) Place the third HiveAP—HiveAP3—within range of the other two, and use a power adaptor to connect it to an AC power source. See [Figure 3](#), in which the switch uses PoE to provide power to HiveAPs 1 and 2.

Figure 3 Connecting HiveAPs to the network



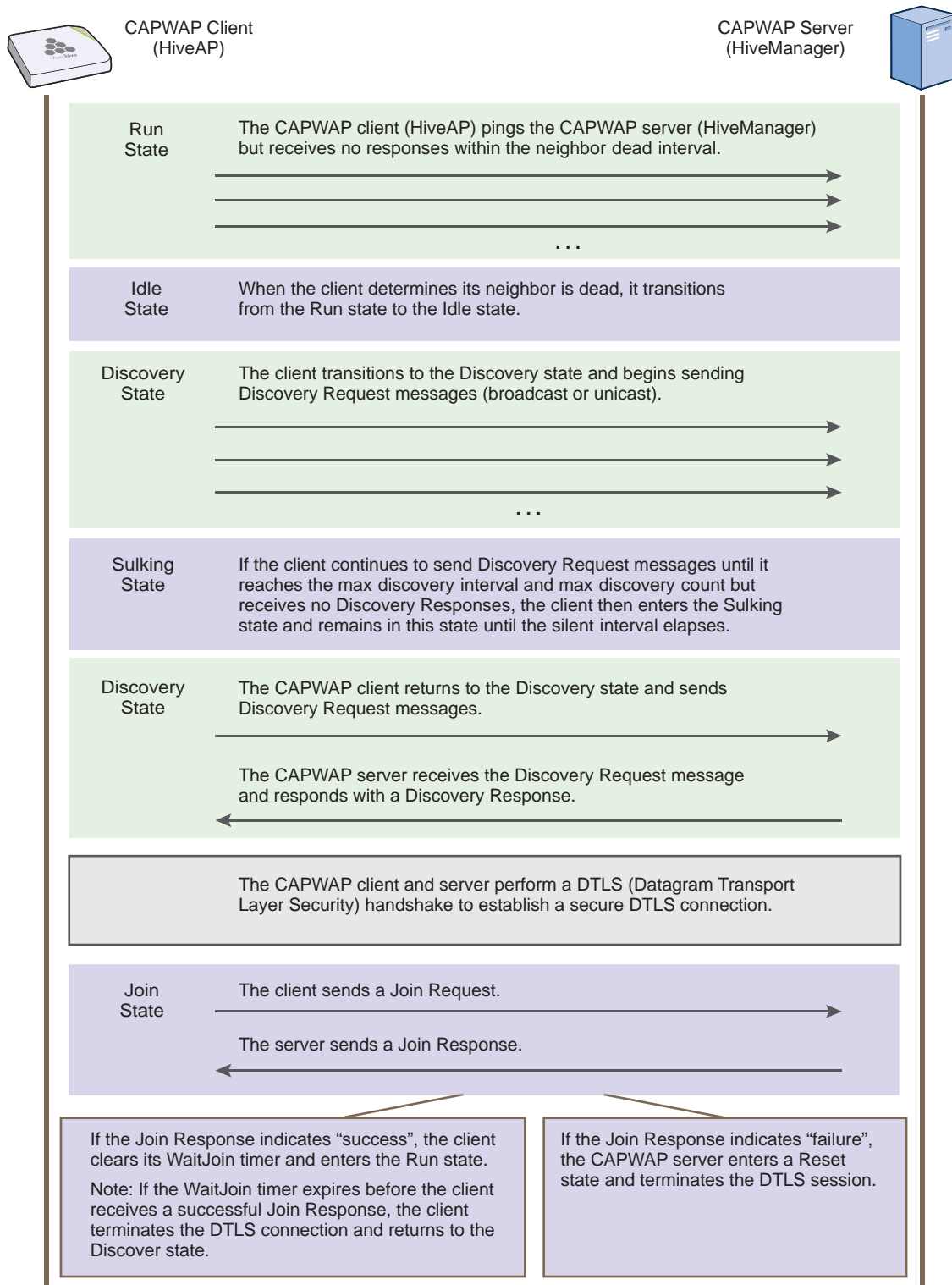
By default, the HiveAPs obtain their network settings dynamically from a DHCP server. HiveAP3 reaches the DHCP server after first forming a wireless link with the other two HiveAPs. (A HiveAP in the position of HiveAP3 is referred to as a mesh point, and HiveAPs such as HiveAP1 and 2 are called portals.)

Within the framework of the CAPWAP (Control and Provisioning of Wireless Access Points) protocol, HiveAPs act as CAPWAP clients and HiveManager as 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 4 on page 130](#).

Note: To illustrate all possible CAPWAP states, [Figure 4 on page 130](#) begins by showing a HiveAP and HiveManager already in the Run state. When a HiveAP first attempts to discover a HiveManager—after the HiveAP 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 HiveAPs 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 HiveAPs Connect to HiveManager" on page 133](#).

Figure 4 CAPWAP Connection process—beginning from the run state



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

Click **Monitor > Access Points > HiveAPs**.

The page displays the three HiveAPs that you put on the network. If you see the three HiveAPs, refer to [Figure 5 on page 132](#). If you do not see them, check the following:

- Do the HiveAPs 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 a HiveAP 320 or 340 is pulsing green, it is still loading the HiveOS firmware. The Power LED on the HiveAP 20 indicates that it is loading firmware by glowing steady amber. If the PWR status LED is dark, the device does not have power. If a HiveAP is getting power through PoE from the switch or from a power injector, make sure that the PSE is configured and cabled correctly. If a HiveAP is powered from an AC outlet, make sure that the power cable is firmly attached to the power connector, the AC/DC power adaptor, and the outlet.

- Are the two portals—HiveAP1 and HiveAP2—connected to the Ethernet network?

When the devices are properly connected, the ETH0 status LED on the HiveAP 300 series device pulses green to indicate a 1000 Mbps link or amber for a 10/100 Mbps link. On the HiveAP 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 HiveAP and switch ports. If the ETH0 or LAN status LED is still dark, try a different cable.

- Did the HiveAPs receive network settings from a DHCP server? At a minimum, each HiveAP 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 HiveAPs,¹ and do the following:

To check the IP address, netmask, and default gateway of the mgt0 interface on a HiveAP, 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 (HiveAP3) 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 HiveAP 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 HiveAP has been discovered, but there is a mismatch with its hive ID.

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

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

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

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

Auth (Authenticated) - The HiveAP 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.

1. To make a physical console connection, connect a console cable to the HiveAP as explained in several of the HiveAP platform chapters. A virtual access console is an SSID that the HiveAP 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 HiveAP through this SSID, check the IP address of the default gateway that the HiveAP assigns to your wireless client, and then make an SSH or Telnet connection to the HiveAP 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 HiveAPs 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 HiveAP. For a list of country codes, see "[Appendix A Country Codes](#)" on page 213.

If the HiveAP 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 HiveAP 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 HiveAP.

- Are the HiveAPs in the same subnet as HiveManager?

HiveAPs 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 HiveAPs 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 HiveAPs to contact HiveManager, but not by broadcasting CAPWAP messages. For a list of other connection options, see ["How HiveAPs Connect to HiveManager" on page 133](#).
- Can the HiveAPs ping the IP address of the HiveManager MGT interface?

Enter the `ping <ip_addr>` command on the HiveAP, 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 HM Admin > HiveManager Settings > Interface Settings in the HiveManager GUI).
- What is the status of the CAPWAP client running on the HiveAP?

To check the CAPWAP status of a HiveAP, enter the `show capwap client` command. Compare the "RUN state" with the CAPWAP states explained in [Figure 4 on page 130](#). Check that the HiveAP has an IP address for itself and the correct address for HiveManager. If for some reason, the HiveAP 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 HiveAPs have contacted HiveManager, they appear in the Monitor > Access Points > HiveAPs page, as shown in [Figure 5](#).

Figure 5 Monitor > Access Points > HiveAPs (view mode: Monitor)

Audit icon
Green square + red triangle: The configuration on a HiveAP does not match that on HiveManager.
Two green squares: They match.

CAPWAP connection and security icons:
Green linked chain/red unlinked chain: The HiveAP is connected or disconnected.
Green locked padlock/red unlocked padlock: Connection is secured through 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	IP Address	Node ID	Connection	AP Type	Clients	Uptime	HiveOS
	HiveAP-1		10.45.1.38	0019770E5580		Portal	0	1 Days, 10 Hrs 3 Mins 48 Secs	HiveOS 3.5r1
	HiveAP2		10.45.1.33	001977000190		Portal	0	8 Days, 6 Hrs 16 Mins 58 Secs	HiveOS 3.5r1
	HiveAP3		10.45.1.38	00197725BC20		Mesh Point	0	1 Days, 10 Hrs 3 Mins 48 Secs	HiveOS 3.5r1

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-0E5580)

The AP type for HiveAP1 and HiveAP2 is "Portal"; they have Ethernet connections to the network. HiveAP3 is "Mesh Point"; it connects to the network through a portal.

Note: If you see a different group of HiveAP settings, make sure that Monitor is selected as the view mode at the top of the HiveAPs page. The GUI provides two view modes for HiveAPs, one that focuses on monitoring HiveAPs (Monitor) and another that focuses on configuring them (Config).

How HiveAPs Connect to HiveManager

If CAPWAP (Control and Provisioning of Wireless Access Points) clients are in the same layer 2 broadcast domain as the CAPWAP server—as they are in the previous example—the clients broadcast CAPWAP Discovery Request messages to discover and establish a secure connection with the server automatically. There is no need for any extra configuration on your part.

However, if the CAPWAP clients and server are in different subnets, the clients cannot discover the server by broadcasting CAPWAP Discovery Request messages. In this case, you can use one of the following methods to configure HiveAPs with the HiveManager IP address or domain name, or configure them so that they can learn it through DHCP or DNS. When HiveAPs have the HiveManager IP address or domain name, they can then send unicast CAPWAP Discovery Request messages to it.

- Log in to the CLI on the HiveAP and enter the IP address or domain name of the CAPWAP server:

```
capwap client server name <string>
```
- Configure the DHCP server to supply the HiveManager domain name 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 the HiveManager IP address.) A HiveAP requests options 225 and 226 by default when it broadcasts DHCPDISCOVER and DHCPREQUEST messages.

Note: If you need to 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 HiveAPs belong, configure an authoritative DNS server with an A record that resolves "hivemanager.<local_domain>" to an IP address. If a HiveAP does not have an IP address or domain name configured for the CAPWAP server and does not receive an address or domain name returned in a DHCP option, then it tries to resolve the domain name to an IP address.

If you are using HiveManager Online instead of a physical HiveManager appliance or HiveManager Virtual Appliance and the HiveAPs go online for the first time without any specific CAPWAP server configuration entered manually or received as a DHCP option, they progress through the following cycle of CAPWAP connection attempts. First, they try to connect with a CAPWAP server at hivemanager.<local_domain>. If that is unsuccessful, they next try to elicit a response from the broadcast of CAPWAP Discovery messages on their local subnet. If neither of these efforts produce a response, they try to connect to HiveManager Online, first using the CAPWAP UDP port 12222 and then using CAPWAP over the HTTP TCP port of 80. This cycle is shown in [Figure 6 on page 134](#).

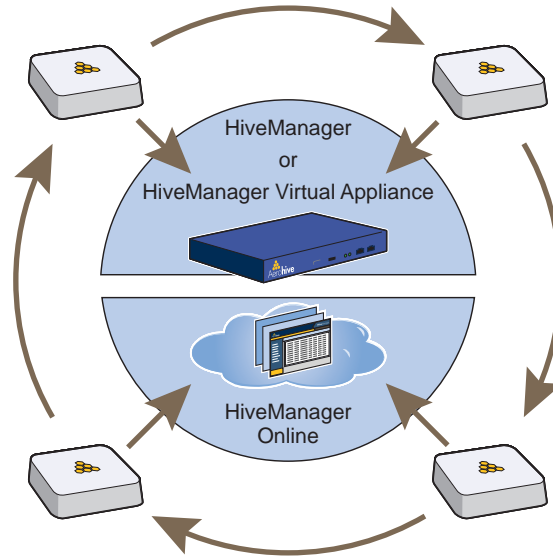
Figure 6 Discovering the CAPWAP server

①

The HiveAP tries to connect to HiveManager using the following default domain name: `hivemanager.<local_domain>`, where "`<local_domain>`" is the domain name that a DHCP server supplied to the HiveAP. If a DNS server has been configured with an A record to resolve that domain name to an IP address, the HiveAP and HiveManager then form a secure CAPWAP connection.

④

If the HiveAP cannot make a CAPWAP connection to HiveManager Online using UDP port 12222, it tries to reach it by using TCP port 80: `staging.aerohive.com:80`. If that proves unsuccessful, the HiveAP returns to its initial search through a DNS lookup and repeats the cycle.



②

If the DNS server cannot resolve the domain name to an IP address, the HiveAP broadcasts CAPWAP Discovery messages on its local subnet for a CAPWAP server (HiveManager). If HiveManager is on the local network and responds, they form a secure CAPWAP connection.

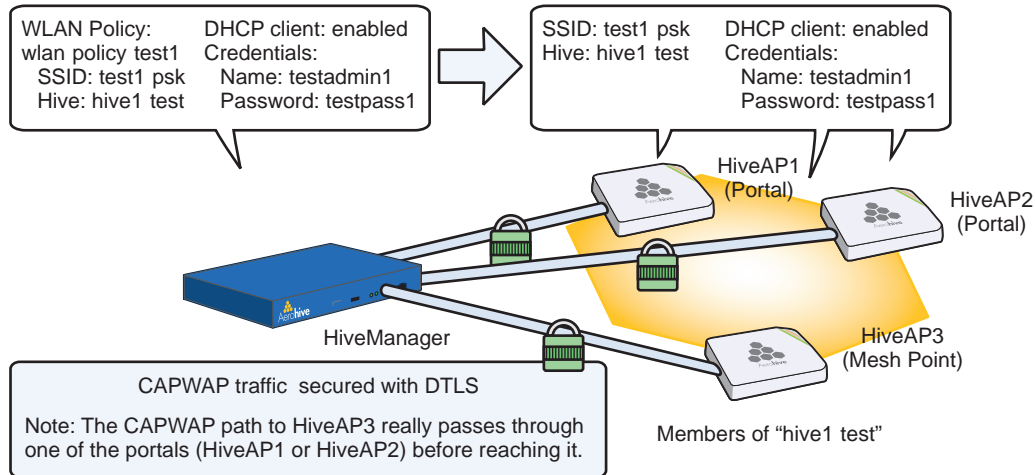
③

If the first two searches for a local HiveManager produce no results, the HiveAP broadens its search even wider and tries to contact HiveManager Online at `staging.aerohive.com:12222`. If the staging server has a serial number or MAC address for that HiveAP, it responds and they form a secure CAPWAP connection.

EXAMPLE 5: ASSIGNING THE CONFIGURATION TO HIVEAPs

After completing the steps in the previous examples, you now assign the WLAN policy to the HiveAPs. In addition, you set one radio in access mode and one in backhaul mode, and you change their login settings (and country code if necessary). Finally, you push the configuration to the HiveAPs. The transfer of HiveAP configuration assignments is presented conceptually in [Figure 7](#).

Figure 7 HiveAP configuration assignments



Assigning Configurations

1. Click **Monitor > Access Points > HiveAPs (View mode: Config)**.
2. Because you can only set radio modes on individual HiveAPs, click one of their names, select **Use one radio (2.4 GHz) for client access and one radio (5 GHz) for a mesh link**, and then click **Save**. Repeat this step for all the other HiveAPs as well.
3. To modify all the HiveAPs at the same time, select the check box in the header to the left of **Host Name**, which selects the check boxes of all the HiveAPs, and then click **Modify**.

The **HiveAPs > Modify (Multiple)** dialog box appears.

4. From the **WLAN Policy** drop-down list, choose **wlan-policy-test1**. This is the WLAN policy that you created in ["Example 3: Creating a WLAN Policy"](#) on page 128. Do not modify any of the other basic settings.
5. In the **Optional Settings** section, expand **Credentials**, and then enter the following in the **Root Admin Configuration** section:

New Admin Name: testadmin1

This is the root admin name that HiveManager uses to make SSH connections and upload a full configuration to managed HiveAPs. The default root admin name and password is *admin* and *aerohive*.

New Password: testpass1

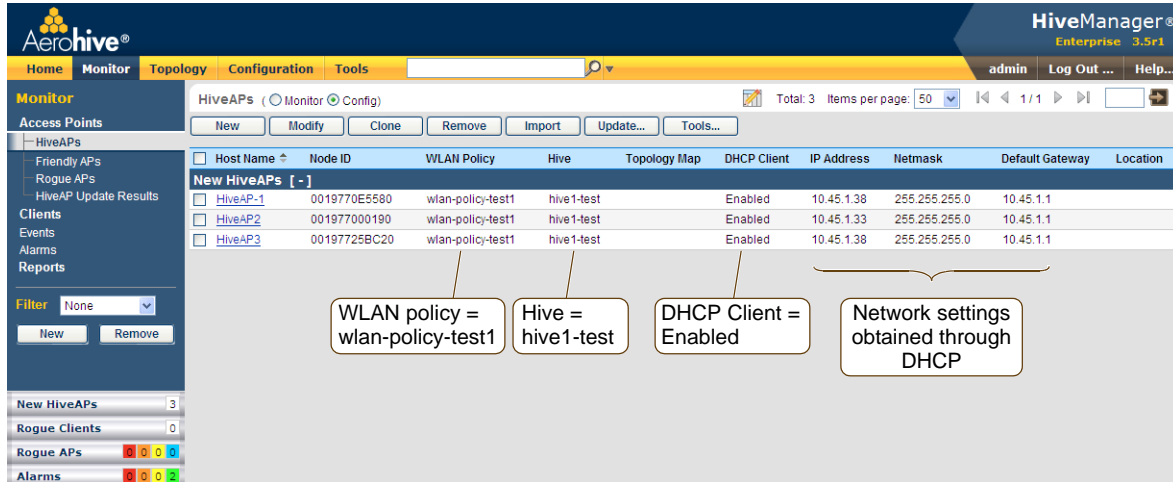
Confirm New Password: testpass1

Although changing the login credentials is not necessary, it is good practice, which is why it is included here. When you are ready to deploy the HiveAPs on your network, change the admin name and password again.

Note: To see the text strings that you enter, clear the **Obscure Password** check box.

- Leave the other settings as they are, and then click **Save** to save your configuration and close the dialog box.
- Check your settings in the HiveAPs window (see [Figure 8 on page 136](#)).

Figure 8 Monitor > Access Points > HiveAPs (view mode: Config)



Updating the Country Code

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

- On the Monitor > Access Points > HiveAPs page, select the check box for HiveAP3, and then click **Update > Update Country Code**.²
- In the Update Country Code dialog box, enter the following, and then click **Upload**:
 - Choose the country where they are deployed from the New Country Code drop-down list.

Note: Be sure to choose the correct country. An incorrect choice might result in illegal radio operation and cause harmful interference to other systems.

- In the Activate after field, set an interval in seconds after which the HiveAP reboots to activate the updated country code settings.
- Make sure that the check box for HiveAP3 is selected.

HiveManager updates the country code on HiveAP3 and then reboots it after the activation interval that you set elapses. After HiveAP3 reboots, it puts the appropriate radio settings for the updated country code into effect.

- Select the check boxes for the two portals HiveAP1 and HiveAP2, and then repeat the previous steps to update their country codes.

After they reboot, all the HiveAPs will have the correct country code, will reform into a hive, and reconnect to HiveManager.

- When updating the country code on HiveAPs 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 HiveAPs in a Mesh Environment" on page 121](#).

Uploading HiveAP Configurations

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

Because HiveAP3 is a mesh point and the update involves changing its hive—from hive0 to hive1-test—you must make sure to update its configuration before updating the configurations on HiveAP1 and HiveAP2. 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 (hive1-test) 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 HiveAPs in a Mesh Environment](#)" on page 121.

1. On the Monitor > Access Points > HiveAPs page, select the check box for HiveAP3, and then click **Update > Upload and Activate Configuration**.

The Upload and Activate Configuration dialog box appears.

2. When initially sending the configuration to HiveAPs, 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 HiveAP stored on HiveManager with that running on the HiveAP and then uploading only the parts that are different. The three options (found in the Settings section) for uploading configurations are as follows:

Complete Upload: This option uploads the complete configuration to the selected HiveAPs 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 HiveAPs from HiveManager.

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

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

Note: If there is any failure when performing a delta upload, use a complete upload the next time.

3. Click **Settings**, select **Activate after**, leave the default interval of 5 seconds, and then click **Save**. 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 HiveAPs 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 HiveAPs need to have NTP enabled.

Activate after: Select this option to load a configuration on the selected HiveAPs 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 HiveAP reboots.

4. Select **Upload and activate configuration** (the other items that can be uploaded are inapplicable at this point), make sure that HiveAP3 is selected, and then click **Upload**.

HiveManager begins transferring the configuration to HiveAP3 and displays the Monitor > Access Points > HiveAP Update Results page where you can observe the progress and the result of the operation.

After HiveAP3 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 hive1-test hive while its portals—HiveAP1 and 2—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.

5. Repeat the previous steps to update HiveAP1 and HiveAP2.

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

Chapter 12 Common Configuration Examples

Through the use of examples, this chapter shows how to use HiveManager in Enterprise mode to configure several features that are somewhat more advanced than those covered in the previous chapter. The examples cover topics such as topological maps, IEEE 802.1X authentication, captive web portals, and the HiveManager concept of classifier tags, which is a method for assigning the different definitions of a single network object to various managed HiveAPs. By trying out these examples—or perhaps just reading them—you can better familiarize yourself with the HiveManager GUI and how to use it to manage and configure HiveAPs.

The following examples in this chapter show how to use HiveManager to configure the following features:

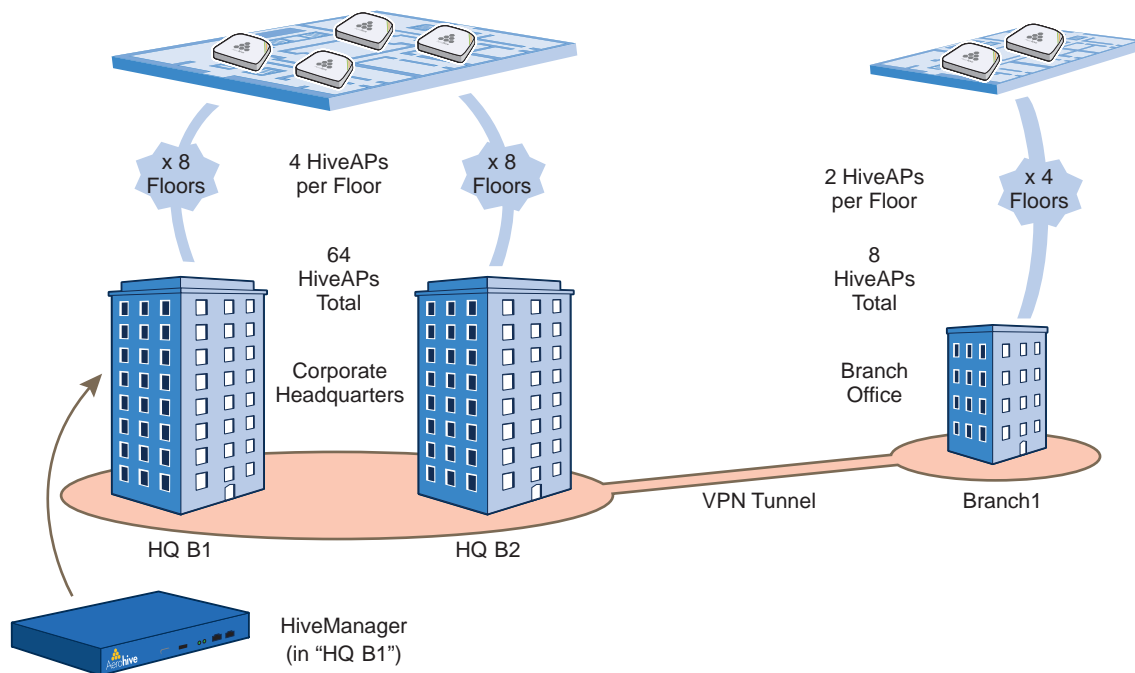
- ["Example 1: Mapping Locations and Installing HiveAPs" on page 140](#)
Upload image files of topology maps to HiveManager and use one of two ways to associate physical HiveAPs with their corresponding icons on the maps.
- ["Example 2: IEEE 802.1X with an External RADIUS Server" on page 145](#)
Configure an IEEE 802.1X SSID and enable HiveAPs to act as RADIUS authenticators, forwarding authentication requests from their wireless clients to an external RADIUS authentication server.
- ["Example 3: Providing Guest Access through a Captive Web Portal" on page 151](#)
Provide controlled and limited wireless network access for guests. This example includes the configuration of a captive web portal, QoS policy, IP firewall policy, user profile, and SSID.
- ["Example 4: Private PSKs" on page 165](#)
Import a file of user names, email addresses, and other data to create private PSK users. Assign the users to a private PSK SSID, and distribute the private PSK data to users through email.
- ["Example 5: Using HiveAP Classifiers" on page 170](#)
Define a single VLAN object with three different definitions, each definition marked with a classifier tag so that the HiveAPs similarly tagged at different sites can apply the appropriate VLAN for their location.

EXAMPLE 1: MAPPING LOCATIONS AND INSTALLING HIVEAPs

HiveManager allows you to mark the location of HiveAPs on maps so that you can track devices and monitor their status. First, you must upload the maps to HiveManager, and then name and arrange them in a structured hierarchy (see "Setting Up Topology Maps"). After that, you can follow one of two ways to install HiveAPs so that you can later put their corresponding icons on the right maps (see "Preparing the HiveAPs" on page 144).

In this example, you set up maps and install over 70 HiveAPs at three locations in a corporate network. After that, you can use HiveManager to create configurations for them, and then push the configurations to them over the network. The general design of the deployment is shown in [Figure 1](#).

Figure 1 Deployment overview

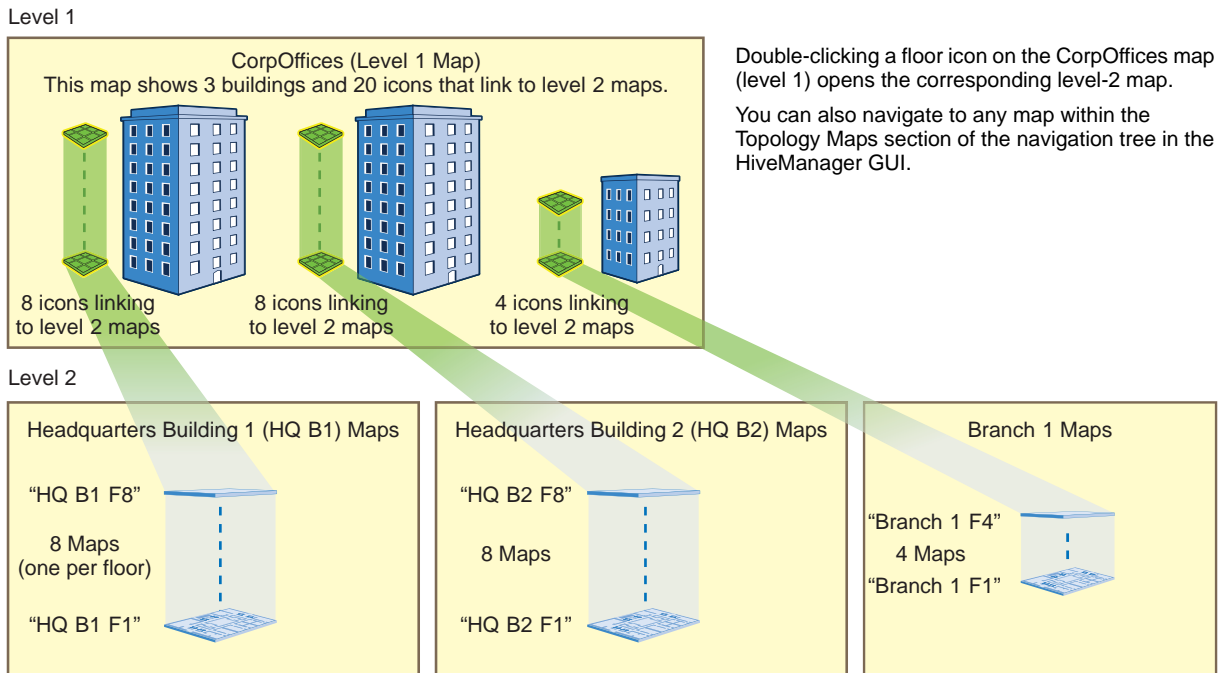


Setting Up Topology Maps

In this example, you upload maps to HiveManager showing floor plans for three office buildings and organize them in a hierarchical structure. You need to make .png or .jpg files of drawings or blueprints showing the layout of each floor. Also, as an easy means of organizing the maps in the HiveManager GUI, you create a file showing the three buildings HQ-B1, HQ-B2, and Branch-1. By using this drawing at the top topographical level, you can display icons for each floor of each building. You can then click an icon to link to its corresponding map. This is shown in [Figure 2](#) on page 141.

Note: Instead of using an illustration of buildings, you can also set the image of the root map as None and use the Add Wall tool to draw three simple rectangles. This option is useful when you have floor plans but not an illustration depicting the external buildings.

Figure 2 Organizational structure of level-1 and -2 maps



Uploading Maps

Note: All image files that you upload to HiveManager must be in .png or .jpg format.

1. Log in to the HiveManager GUI as explained in "Installing and Connecting to the HiveManager GUI" on page 109.
2. To begin using maps, you must first set the root map, which will be at the top level of all the maps you add under it. Click **Topology**, enter the following, and then click **Update**:

Root Map Name: **CorpOffices** (Note that spaces are not allowed in map level names. This will be the map at the top of a hierarchical structure of maps. After defining this map, you can then add other maps beneath it.)

Operational Environment: Because the CorpOffices "map" does not contain any HiveAP icons—it is an illustration of three buildings that you use to organize the submaps of the floors in each building—the environment setting is irrelevant. Leave it at its default, **Office**.

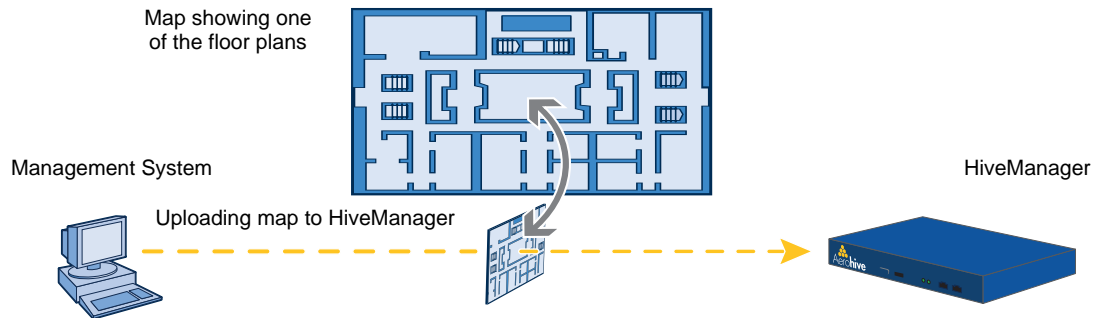
Background Image: Click **Import > Upload**, navigate to **corp_offices.png** and select it. Then choose **corp_offices.png** from the Background Image drop-down list.

Map Size and HiveAP Installation Height: Because the **corp_offices.png** depicts buildings instead of a floor plan, it is not necessary to specify the size of the image or the HiveAP installation height.

3. To add maps below the root map, click **Topology**, right-click **CorpOffices**, and then choose **Add/Delete Image** from the pop-up menu that appears. In the Add/Delete Image window, click **Upload**, navigate to the directory containing the image files that you want to upload, select up to five of them, and then click **Open**.

The selected image files are transferred from your management system to HiveManager as shown in [Figure 3 on page 142](#).


Figure 3 Uploading a map of a building floor plan



4. Repeat this for all the image files that you need to load, and then close the dialog box when done. For this example, you load these 21 files:
 - 8 maps for the eight floors in HQ-B1 (Headquarters Building 1)
 - 8 maps for the eight floors in HQ-B2 (Headquarters Building 2)
 - 4 maps for the four floors in Branch-1
 - 1 file (named "corp_offices.png" in this example) that shows a picture of the three buildings

Naming and Arranging Maps within a Structure

1. Click **Topology**, right-click the top level map "CorpOffices", and then choose **New** from the pop-up menu that appears.
2. In the New Map (Submap for CorpOffices) dialog box, enter the following, and then click **Create**:
 - Map Name: HQ-B1-F1
 - Map Icon: **Floor**
 - Environment: Because the environment is that of a typical office building, choose **Office**. The environment assists in the prediction of signal strength and attenuation shown in the heat maps.
 - Background Image: Choose **HQ-B1-F1.png** from the drop-down list.
 - Map Width (optional): 120 feet (HiveManager automatically calculates map height using the aspect ratio of the image.)
 - HiveAP Installation Height: 13 feet; a fairly standard ceiling height in offices

A floor icon () labeled "HQ-B1-F1" appears on the CorpOffices image, and a new entry named "HQ-B1-F1" appears nested under "CorpOffices" in the navigation tree.
3. Select the icon, and drag it to the location you want.
4. Click **Topology**, right-click the top level map "CorpOffices", and then choose **New** from the pop-up menu that appears.
5. In the New Map (Submap for CorpOffices) dialog box, enter the following, and then click **Create**:
 - Map Name: HQ-B1-F2
 - Map Icon: **Floor**
 - Environment: **Office**
 - Background Image: Choose **HQ-B1-F2.png** from the drop-down list.
 - Map Width (optional): 120 feet
 - HiveAP Installation Height: 13 feet

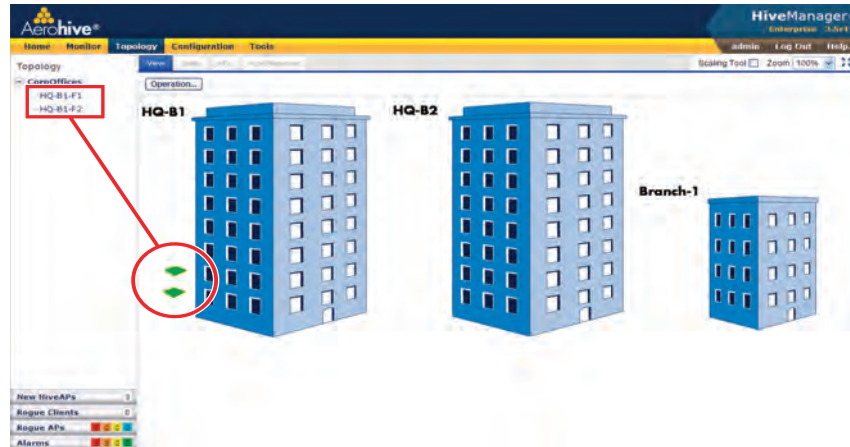
A floor icon labeled "HQ-B1-F2" appears on the CorpOffices image, and a new entry named "HQ-B1-F2" appears nested under "CorpOffices" in the navigation tree.

6. Select the icon and drag it to the location you want.

After adding the CorpOffices "map" (really an illustration showing three buildings), two floor plans for the first and second floors of "HQ-B1", and dragging the floor icons into position, the display of the CorpOffices map looks similar to that in [Figure 4](#).

Figure 4 CorpOffice map (level 1) with links to level-2 maps HQ-B1-F1 and HQ-B1-F2

The submaps in the navigation tree and the icons on this map link to other maps. Click a submap or double-click an icon to open the map to which it links.



7. Repeat this process until you have arranged all the maps and icons in place as shown in [Figure 5](#).

Figure 5 CorpOffice map with links to all level-2 maps



Note: You can add up to seven levels to the map hierarchy. You can also remove maps as long as they do not have any submaps or HiveAP icons on them. To remove a map from the hierarchy, right-click it in the Map Hierarchy list, select Remove from the short-cut menu that pops up, and then click Yes.

Preparing the HiveAPs

There are several approaches that you can take when mapping the location of installed HiveAP devices. Two possible approaches are presented below. The first approach ("[Using MAC Addresses](#)" on page 144) allows you to install HiveAPs without needing to do any extra configurations, but you later have to match each HiveAP with the right map in HiveManager manually. With the second approach ("[Using SNMP](#)"), HiveManager automatically assigns HiveAPs to maps. This approach does require a small amount of configuration of each HiveAP up front, but after the HiveAPs form a CAPWAP connection with HiveManager, the automatic assignment of HiveAPs to their appropriate maps on HiveManager occurs without any further effort.

Note: For a summary of how HiveAPs use CAPWAP to discover and connect to HiveManager, see "[How HiveAPs Connect to HiveManager](#)" on page 133.

Using MAC Addresses

With this approach, you write down the MAC address labelled on the underside of each HiveAP and its location while installing the HiveAPs throughout the buildings. The MAC address on the label is for the mgt0 interface. Because the MAC addresses of all HiveAPs begin with the Aerohive MAC OUI 00:19:77, you only need to record the last six numerals in the address. For example, if the MAC OUI is 0019:7700:0120, you only need to write "000120" to be able to distinguish it from other HiveAPs later.

1. Make copies of the maps uploaded to HiveManager, label them, and take them along when installing the HiveAPs.
2. When you install a HiveAP, write the last six digits of its MAC address at its location on the map.

When HiveAPs automatically connect with HiveManager, HiveManager displays them on the Monitor > Access Points > HiveAPs page. You can differentiate them in the displayed list by MAC address (node ID), which allows you to match the HiveAPs in the GUI with those you noted during installation so that you can properly assign each one to a map.

Using SNMP

This approach makes use of the SNMP (Simple Network Management Protocol) sysLocation MIB (Management Information Base) object, which you define on HiveAPs. HiveManager can use this information to associate a HiveAP with a map and provide a description of where on the map each HiveAP belongs.

1. Make copies of the maps you uploaded to HiveManager, label them, and take them with you for reference when installing the HiveAPs.
2. For each HiveAP that you install, do the following:
 - 2.1 Make a serial connection to the console port, and log in (see "[Log in through the console port](#)" on page 182).
 - 2.2 Enter the following command, in which *string1* describes the location of the HiveAP on the map (in open format) and *string2* is the name of the map:

```
snmp location string1@string2
```

For example, if you install a HiveAP in the northwest corner on the first floor of building 1, enter **snmp location northwest_corner@HQ-B1-F1**. If you want to use spaces in the description, surround the entire string with quotation marks: **snmp location "northwest corner@HQ-B1-F1"**.

If you want, you can include some or all of the map hierarchy in the SNMP location string. For example, if a map named "floor-1" is nested under a higher level map named "building-1", then enter the command as follows: **snmp location northwest_corner@floor-1@building-1**. Similarly, if these two maps are nested under a higher level map named "campus-1", then include that next higher level in the SNMP location string: **snmp location northwest_corner@floor-1@building-1@campus-1**. Although including the map hierarchy is unnecessary to identify a map in HiveManager—all map names must be unique—including the map hierarchy in the SNMP location can provide a simple way to check that preconfigured HiveAPs get distributed to various sites correctly before they are installed.

- 2.3 Mount and cable the HiveAP to complete its installation. (For mounting instructions, see the mounting section in the chapter for the HiveAP platform that you are installing.)

When a HiveAP connects to HiveManager, HiveManager checks its SNMP location and automatically associates it with the map specified in its SNMP location description. You can then click the icon to see its location and drag it to the specified location on the map. Also, on the Monitor > Access Points > HiveAPs page (view mode: Config), you can sort detected HiveAPs by map name to assign them more easily to WLAN policies.

Note: The first approach—using MAC addresses—makes the deployment considerably easier for installers, whereas the second approach—using SNMP—makes new HiveAP management easier for the HiveManager administrator. You can decide which approach makes the most sense for your team.

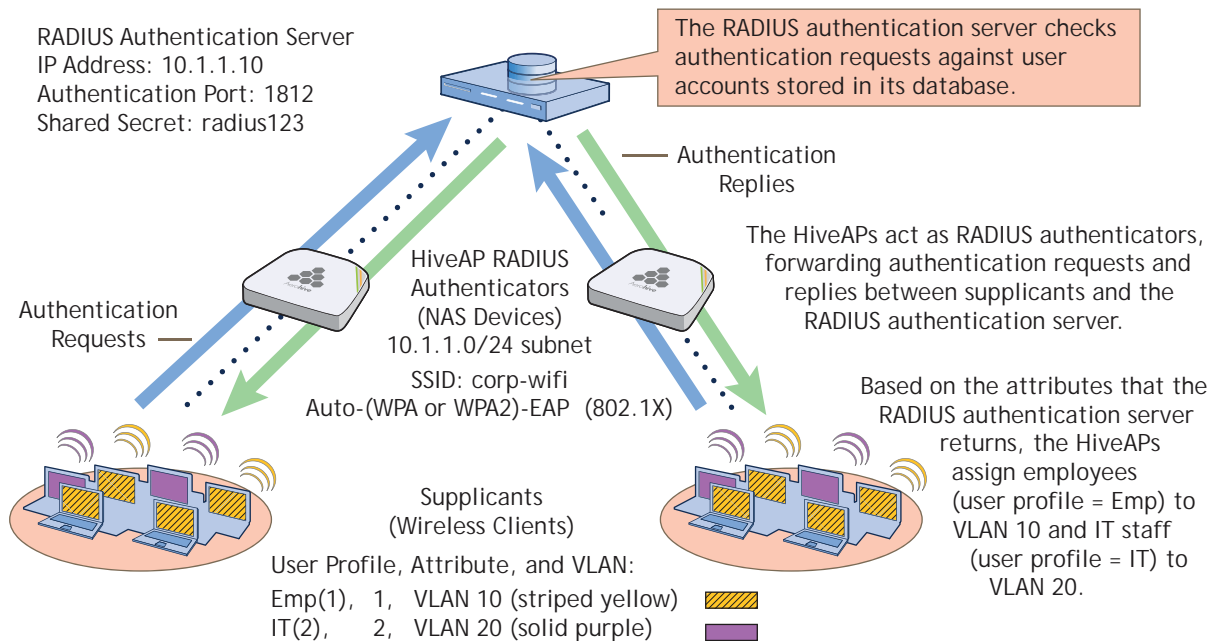
EXAMPLE 2: IEEE 802.1X WITH AN EXTERNAL RADIUS SERVER

You can configure HiveAPs to act as RADIUS authenticators, also known as RADIUS clients or NAS (network access server) devices. They forward IEEE 802.1X/EAP user authentication requests and responses between wireless supplicants and up to four RADIUS authentication servers (a primary and three backups). In this example, you configure two HiveAPs to act as RADIUS authenticators. They provide network access to wireless clients/RADIUS supplicants and pass authentication requests between the supplicants and a RADIUS authentication server.

Note: This example makes several assumptions about the RADIUS authentication server: (1) user accounts are already stored on it; (2) it listens on UDP port 1812 for authentication requests; (3) it uses "t6bEdmNfot3vW9vVr6oAz48CNCsDtInd" as its shared secret; (4) it allows RADIUS authentication requests from NAS devices in the 10.1.1.0/24 subnet. For configuration details, consult the product documentation for your RADIUS server.

You also configure an SSID that makes use of IEEE 802.1X/EAP authentication on the HiveAP authenticators. Because an SSID using 802.1X/EAP authentication can support numerous user profiles, the example shows how two groups of users—employees and IT staff—can access the same SSID but be assigned to two different VLANs. See [Figure 6](#).

Figure 6 Authentication requests and replies for wireless clients on two HiveAPs



This example assumes that you have already accepted the HiveAPs for HiveManager management, assigned them to a WLAN policy that includes a hive and at least one SSID, and pushed that configuration to them. In other words, the HiveAPs are already under HiveManager management by the time you begin the configuration in this example. If that is not yet the case, see ["Basic Configuration Examples" on page 123](#) before continuing.

VLANS and User Profiles

To begin, you create two VLAN objects and then two user profiles, each of which references one of the VLANs. When you configure the SSID later, you reference both user profiles in the SSID configuration. With this approach, the HiveAPs apply different VLANs to traffic from different users based on their corresponding user profiles.

1. To create a VLAN object for employee traffic, click **Configuration > Advanced Configuration > Network Objects > VLANs > New**, and then enter the following in the VLANs dialog box:

VLAN Name: **VLAN-10**

Enter the following, and then click **Apply**:

VLAN ID: **10**

Type: **Global**

Setting the type as "Global" means that HiveManager applies the VLAN entry to all HiveAPs that include the VLAN object in their configuration—unless you add another VLAN entry to this VLAN object and assign it a more specific classification type such as a classifier tag, map, or HiveAP. Then the HiveAP applies the other VLAN entry if it has the same classifier tag, is on the specified map, or is the specified HiveAP.

Description: **VLAN for employees**

2. To save the configuration and close the VLANs dialog box, click **Save**.
3. To create a VLAN object for IT staff traffic, select the check box for the newly created VLAN object "VLAN-10" in the list on the **Configuration > Advanced Configuration > Network Objects > VLANs** page, and then click **Clone**.

The VLANs dialog box appears with the settings for VLAN-10.

4. For VLAN Name, enter **VLAN-20**; in the VLAN ID field, change **10** to **20**; modify the Description field to **VLAN for IT staff**; and then click **Save**.

You can see the two newly created VLAN objects on the **Configuration > Advanced Configuration > Network Objects > VLANs** page.

5. To create a user profile for employees, click **Configuration > User Profiles > New**, enter the following, leave the other settings as they are, and then click **Save**:

Name: **Emp(1)**

Including the attribute number "(1)" as part of the user profile name is helpful when troubleshooting and when configuring the RADIUS server. The name "Emp(1)" serves as reminder to use 1 as the Tunnel-Private-Group-ID attribute when configuring the RADIUS server. HiveAPs use a combination of three RADIUS attributes to determine which user profile to assign to an authenticated user: Tunnel-Type = GRE (10), Tunnel-Medium-Type = IP (1), and Tunnel-Private-Group-ID = <number>. If a HiveAP receives all three attributes and the third one matches a user profile attribute, it then applies that user profile to traffic from the authenticated user. Including the attribute number in the user profile name makes configuring the RADIUS server a bit simpler.

Attribute Number: **1**

Default VLAN: **VLAN-10**

Description: **For employees to use VLAN 10**

- To create a user profile for IT staff, select the check box of the user profile that you just created, "Emp(1)", and then click **Clone**.

The User Profiles dialog box appears with the settings for Emp(1).

- For Name, enter **IT(2)**; for Attribute Number, enter **2**; for Default VLAN, choose **VLAN-20**, modify the text in the Description field to **For IT staff to use VLAN 20**, and then click **Save**.

HiveAPs as RADIUS Authenticators

HiveAP RADIUS authenticators provide network access to wireless clients and pass authentication requests between the wireless clients acting as RADIUS supplicants and a RADIUS authentication server. In this section, you configure the settings that control how the HiveAPs communicate with the RADIUS authentication server.

Click **Configuration > Advanced Configuration > Authentication > AAA Client Settings > New**, and enter the following:

RADIUS Name: **RADIUS-10.1.1.10**

This is a name for the RADIUS configuration object on HiveManager. Provide it with a useful name that easily identifies it to you. The name can be up to 32 characters and cannot contain spaces.

Description: **HQ RADIUS server with employee accounts**

Enter a useful comment about the configuration. It can be up to 64 characters, including spaces.

In the RADIUS Servers section, enter the following to define the necessary network and security settings for making secure connections with the RADIUS authentication server:

Click the **New** icon to the right of the IP Address/Domain Name drop-down list, and define the IP address of the RADIUS authentication server in the IP Objects/Host Names dialog box that appears:

IP Address: (**select**; this setting automatically applies a netmask of 255.255.255.255)

Object Name: **AuthServer-10.1.1.10**

Enter the following, and then click **Apply** to add the IP address to the address configuration:

IP Entry: **10.1.1.10**

Type: **Global**

Setting the type as "Global" means that HiveManager applies the IP entry to all HiveAPs that include the IP address/host name object in their configuration.

Description: **RADIUS auth server at 10.1.1.10**

Click **Save** to save the address configuration and return to the AAA Client Settings page.

IP Address/Domain Name: **AuthServer-10.1.1.10** (This is the address that you just created.)

Server Type: **Authentication**

You can define the service that the RADIUS server provides: authentication, accounting, or both (auth/acct). In this example, the server only authenticates users, so there is no need to enable accounting. When RADIUS accounting is enabled, the RADIUS authenticators report the status and cumulative length of RADIUS supplicant sessions to the RADIUS authentication server. Accounting is often used to track client activity so that users can be accurately charged for network use. It is also sometimes used to gather statistics about general network usage.

Shared Secret: **t6bEdmNfot3vW9vVr6oAz48CNCsDtInd**

Confirm Secret: **t6bEdmNfot3vW9vVr6oAz48CNCsDtInd**

The shared secret that you enter here must exactly match that on the RADIUS authentication server. Because the authentication server and authenticators use it to verify each other's identities

when establishing a RADIUS session, it is important that the shared secret be fairly strong. Therefore, you use the longest string possible—32 alphanumeric characters—randomly arranged. To see the text strings that you enter, clear the **Obscure Password** check box.

Server Role: Primary

To provide server redundancy, you can configure up to four RADIUS servers, designating one as the primary server and the others as backup servers. The RADIUS authenticators only send RADIUS authentication requests to the backup servers when the primary server becomes unreachable. Because only one RADIUS server is configured in this example, it must be designated as the primary.

To add the RADIUS authentication server to the AAA client settings configuration, click **Apply**.

In the **Advanced Settings** section, you can change the RADIUS authentication port number, enable RADIUS accounting, and change the RADIUS accounting port number. For this example, keep their default values.

Authentication Port: 1812

UDP port 1812 is the default port number on which RADIUS servers listen for authentication requests. In this example, the RADIUS server is using the default port number. If your RADIUS server listens on a different port, make sure that you enter that port number here.

Accounting Port: 1813

UDP port 1813 is the default port number on which RADIUS accounting servers listen for accounting reports. In this example, accounting is not enabled, so this setting is irrelevant.

You can expand the **Optional Settings** section at the bottom of the page to modify additional settings pertaining to RADIUS; however, the default settings work well for this example and do not need to be changed.

Retry Interval: 600 seconds (the default setting)

This field is only relevant when both primary and backup RADIUS authentication servers are configured. The retry interval defines how long a HiveAP RADIUS authenticator waits before retrying a previously unresponsive primary RADIUS server, even if the current backup server is responding. When there is only a single RADIUS authentication server, as in this example, the retry interval does not matter.

Accounting Interim Update Interval: 20 seconds (the default setting)

This setting defines the interval for sending RADIUS accounting updates to report the status and cumulative length of RADIUS supplicant sessions. This setting is important when enforcing RADIUS accounting, which is not involved in the present example. Therefore, this setting is irrelevant here.

Permit Dynamic Change of Authorization Messages (RFC 3576): (clear; the default setting)

This option allows HiveAP RADIUS authenticators to accept unsolicited disconnect and CoA (Change of Authorization) messages from the RADIUS authentication server by enabling the dynamic authorization extension provided in *RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*. "Disconnect" messages terminate a user's session immediately, and CoA messages modify session authorization attributes such as VLANs and user profile IDs. The ability for HiveAP RADIUS authenticators to accept these messages from the RADIUS authentication server is not required in this example, so it remains disabled.

To save the configuration as "RADIUS-10.1.1.10" and close the dialog box, click **Save**.

Defining an SSID with 802.1X/EAP Authentication

Define an SSID that supports 802.1X/EAP authentication and directs the HiveAP RADIUS authenticators to forward authentication requests from RADIUS supplicants to the RADIUS authentication server that you just defined.

Click **Configuration > SSIDs > New**, enter the following, leave all other values at their default settings, and then click **Save**:

Profile Name: **corp-wifi**

SSID: **corp-wifi**

Description: **Employee and IT WLAN access; 802.1X**

SSID Access Security: **WPA/WPA2 802.1X (Enterprise)**

Use Default 802.1X Settings: **(select)**

By default, when a HiveAP hosts a WPA/WPA2 802.1X (Enterprise) SSID, it negotiates with clients over the use of WPA or WPA2 for key management and TKIP or CCMP (AES) for encryption, and uses whichever methods each client supports. The HiveAP and client use EAP (802.1X) for authentication through an external RADIUS server.

RADIUS Server: **RADIUS-10.1.1.10**

User profile assigned if no attribute is returned from RADIUS after successful authentication: **Emp(1)**

The HiveAP RADIUS authenticator applies the user profile "Emp(1)" to users if the RADIUS authentication server successfully authenticates them and returns a Tunnel-Private-Group-ID attribute that matches the attribute for this user profile (1). The HiveAP also applies this profile to users if the RADIUS authentication server does not return any attributes.

If the RADIUS server authenticates a user and returns attributes that do not match an existing user profile, the user profile lookup will fail and HiveAP will reject the client.

User profiles assigned via attributes returned from RADIUS after successful authentication: Click **IT(2)** in the Available User Profiles list, and then click the right arrow (>) to move it to the Selected User Profiles list.

The HiveAP RADIUS authenticator applies the "IT(2)" user profile only if the RADIUS authentication server returns a Tunnel-Private-Group-ID attribute matching the attribute for this user profile (2).

Only the selected user profiles can be assigned via RADIUS for use with this SSID: **(clear)**

When cleared, this setting allows access to authenticated users even when the Tunnel-Private-Group-ID attribute that the RADIUS authentication server returns matches another user profile configured on the HiveAP but not specified for this SSID. If you do not mind granting access to all valid user accounts on the RADIUS authentication server, disable this option by clearing the check box. This is the default setting.

On the other hand, if you want to restrict access to authenticated users only when the RADIUS authentication server returns attributes that match one of the specified user profiles for the SSID, enable this option by selecting the check box and then specifying the action that you want the HiveAP to take: ban the client for a period of time, ban it indefinitely, or simply disconnect it. You might want to enable this if the RADIUS authentication server contains accounts for users other than employees and IT staff—perhaps there are accounts for contractors and guests. Even though the server would approve authentication requests from such users if they submitted a correct user name and password, you might not want them to use this SSID to access the WLAN.

SSID Broadcast Band: **2.4 GHz (11n/b/g)**

Assigning an SSID to the 2.4 GHz radio in access mode allows HiveAPs to use their second radio, which operates at 5 GHz, for wireless backhaul communications.

Applying the RADIUS and SSID Settings to HiveAPs

1. Click **Configuration > WLAN Policies >** (select the name of a WLAN policy that has already been applied to the HiveAPs) **> Add/Remove SSID Profile**, select **corp-wifi** in the Available SSID Profiles list, click the right arrow (**>**) to move it to the Selected SSID Profiles list, click **Apply** to add the SSID to the WLAN policy, and then click **Save** to save the modified policy and close its dialog box.
2. Click **Monitor > Access Points > HiveAPs >** (check boxes for the two HiveAP RADIUS authenticators) **> Update > Upload and Activate Configuration**, enter the following, and then click **Upload**:
Upload and activate configuration: (select)
Upload and activate CWP pages and Server key: (clear)
Upload and activate certificate for RADIUS and VPN services: (clear)
Upload and activate employee, guests, and contractor credentials: (clear)
Check boxes for both HiveAPs: (select)

Connecting Supplicants to the WLAN

The 802.1X authentication process is somewhat different depending on the operating system on which the RADIUS supplicant is running and whether the client uses the user's login credentials to authenticate itself on a domain.

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 **corp-wifi**.
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.

Note: 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.

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): **corp-wifi**
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 **corp-wifi**.
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 stored on the RADIUS server, and then click **OK**.

If the supplicant is on a Macintosh computer and is not on a domain, view the available SSIDs in the area, and select **corp-wifi**. Then click **Join Network**, and accept the certificate that the RADIUS server provides, assuming it is from a trustworthy source. After the RADIUS server validates your identity, the client connects to the WLAN.

EXAMPLE 3: PROVIDING GUEST ACCESS THROUGH A CAPTIVE WEB PORTAL

A captive web portal is a way to control network access by requiring users to authenticate their identity or complete a registration form before assigning them network and user profile settings that allow them network access beyond the HiveAP with which they associated. A captive web portal provides registered users with network access while containing unregistered users. Because the Aerohive captive web portal feature is very flexible, you will have a number of choices to make when configuring it. Several of these are examined first—"Registration Types", "Providing Network Settings", and "Modifying Captive Web Portal Pages"—and then a complete configuration example is presented.

Registration Types

There are five types of registration (four are shown in Figure 7) that a captive web portal can require of users:

Self-Registration: With this option, users must complete a registration form and accept a network use policy before being allowed to pass through the captive web portal. This is a good choice when you cannot know in advance who will be attempting to make a network connection through the captive web portal and simply want to keep a record of the users, or if user authentication is unimportant.




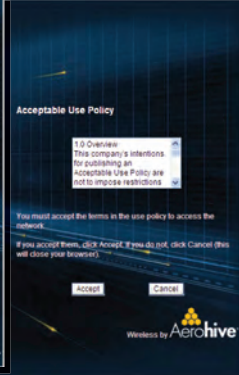
User Authentication: With this option, users must enter and submit a valid user name and password to log in. The HiveAP acts as a RADIUS authenticator or RADIUS client and forwards the submitted login credentials to a RADIUS server for authentication. The RADIUS authentication server can either be an internal server on a HiveAP or an external RADIUS server on the network. This is a good choice when you can set up a RADIUS authentication server with user accounts before the users attempt to access the network.

Both (Auth/Self-reg): This is a combination of the previous two registration types. Users can authenticate themselves by submitting a user name and password or complete and submit a registration form.

Use Policy Acceptance: With this option, the user is presented with a network use policy, and only has to click Accept to gain network access.

External Authentication: HiveAPs redirect unregistered users' HTTP and HTTPS traffic to a captive web portal on an external server, such as the amigopod Visitor Management Appliance.

Figure 7 Four types of registration through a captive web portal running on a HiveAP

<p>Self-Registration</p> <p>The user self-registers by entering data that can then be saved to a syslog server for tracking and auditing.</p>	<p>User Authentication</p> <p>The user submits a name and password, which are sent to a RADIUS server for authentication.</p>	<p>Both (Auth/Self-reg)</p> <p>Authentication at the top and self-registration at the bottom (the user submits one of them)</p>	<p>Use Policy Acceptance</p> <p>The user must accept a network use policy to gain network access</p>
			

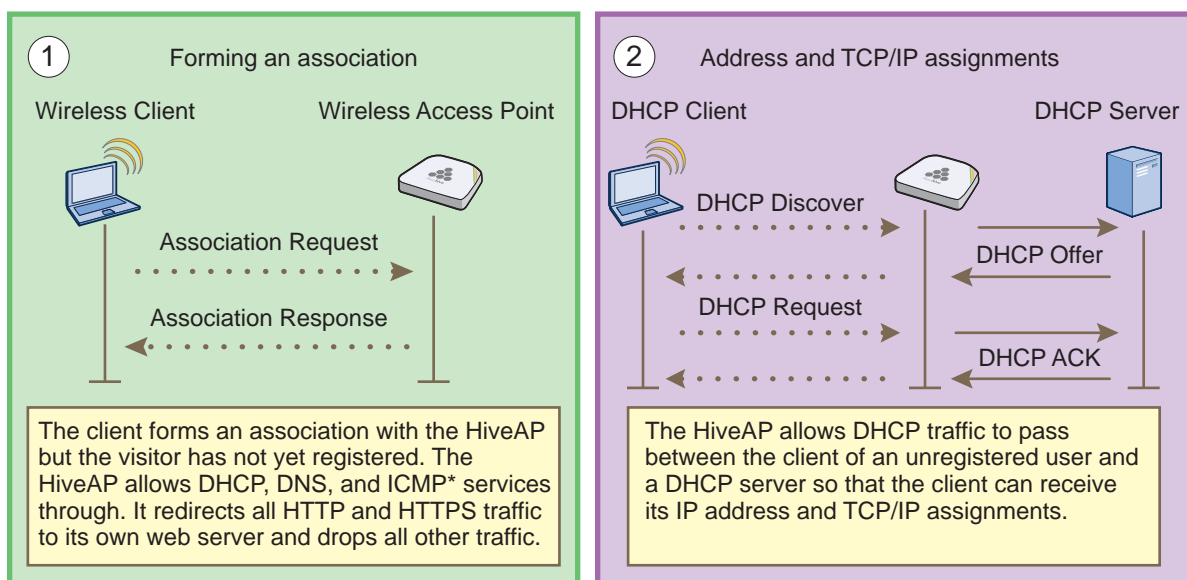
Providing Network Settings

In addition to various registration types, Aerohive offers two approaches to providing captive web portal clients with network settings. One approach uses external DHCP and DNS servers on the network, and the other uses internal DHCP and DNS servers on the HiveAP itself.

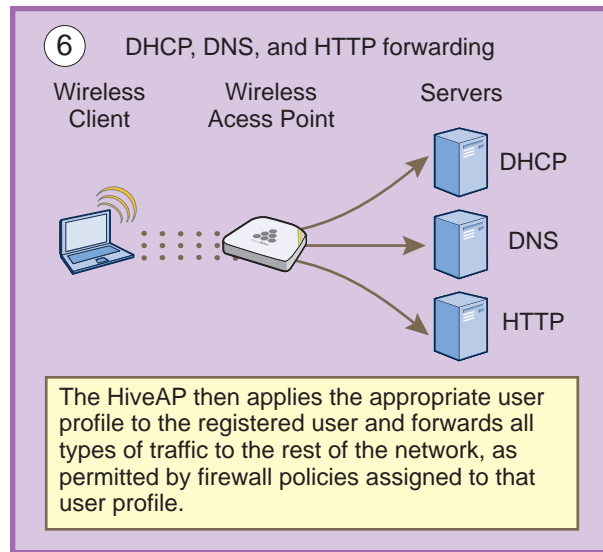
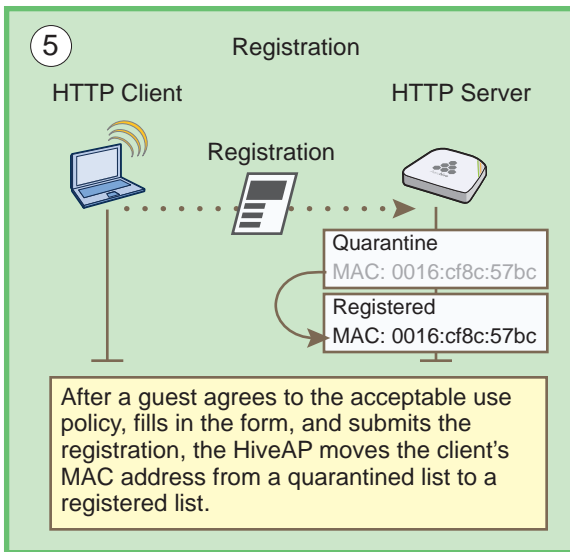
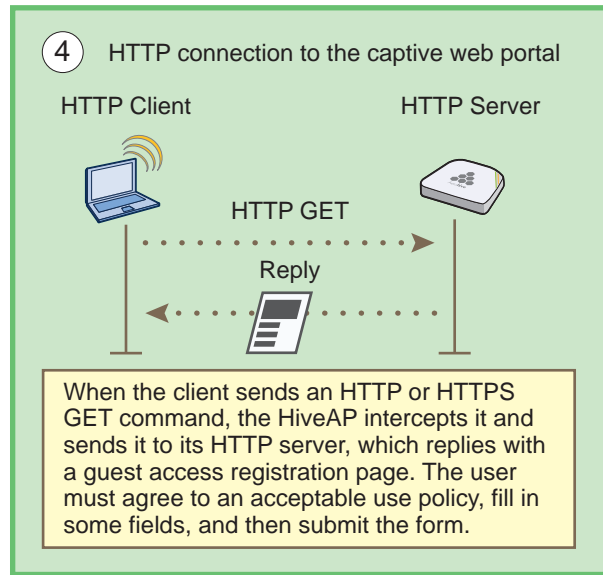
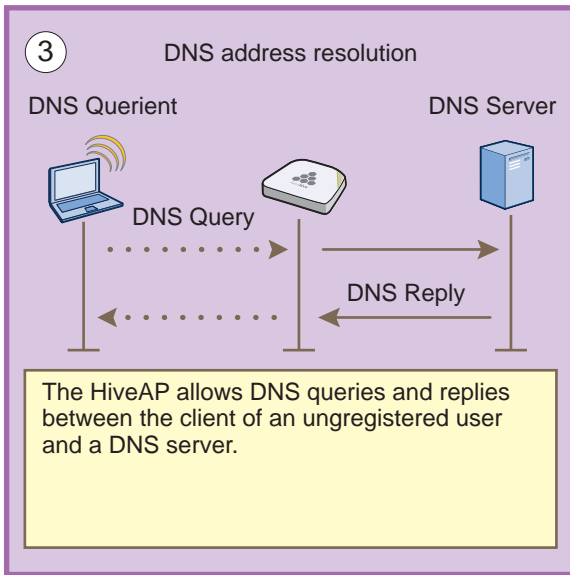
Captive Web Portal with External DHCP and DNS Servers

With this approach, when the client of a previously unregistered visitor first associates with the guest SSID, the HiveAP allows DHCP and DNS traffic to pass through so that the client can receive its address and TCP/IP assignments and resolve domain names to IP addresses. It also allows ICMP traffic for diagnostic purposes. However, the HiveAP intercepts all HTTP and HTTPS traffic from that client—and drops all other types of traffic—thereby limiting its network access to just the HiveAP with which it associated. No matter what website the visitor tries to reach, the HiveAP directs the visitor’s browser to a registration page. After the visitor registers, the HiveAP stores the client’s MAC address as a registered user, applies the appropriate user profile to the visitor, and stops keeping the client captive; that is, the HiveAP no longer intercepts HTTP and HTTPS traffic from that MAC address, but allows the client to access external web servers. The entire process is shown in [Figure 8](#).

Figure 8 Captive web portal exchanges using external DHCP and DNS servers



* If the HiveAP enforces a firewall policy that blocks ICMP services from registered users, it will also block them from unregistered users. In contrast to ICMP, DHCP and DNS are essential services that must always be permitted by the HiveAP firewall.

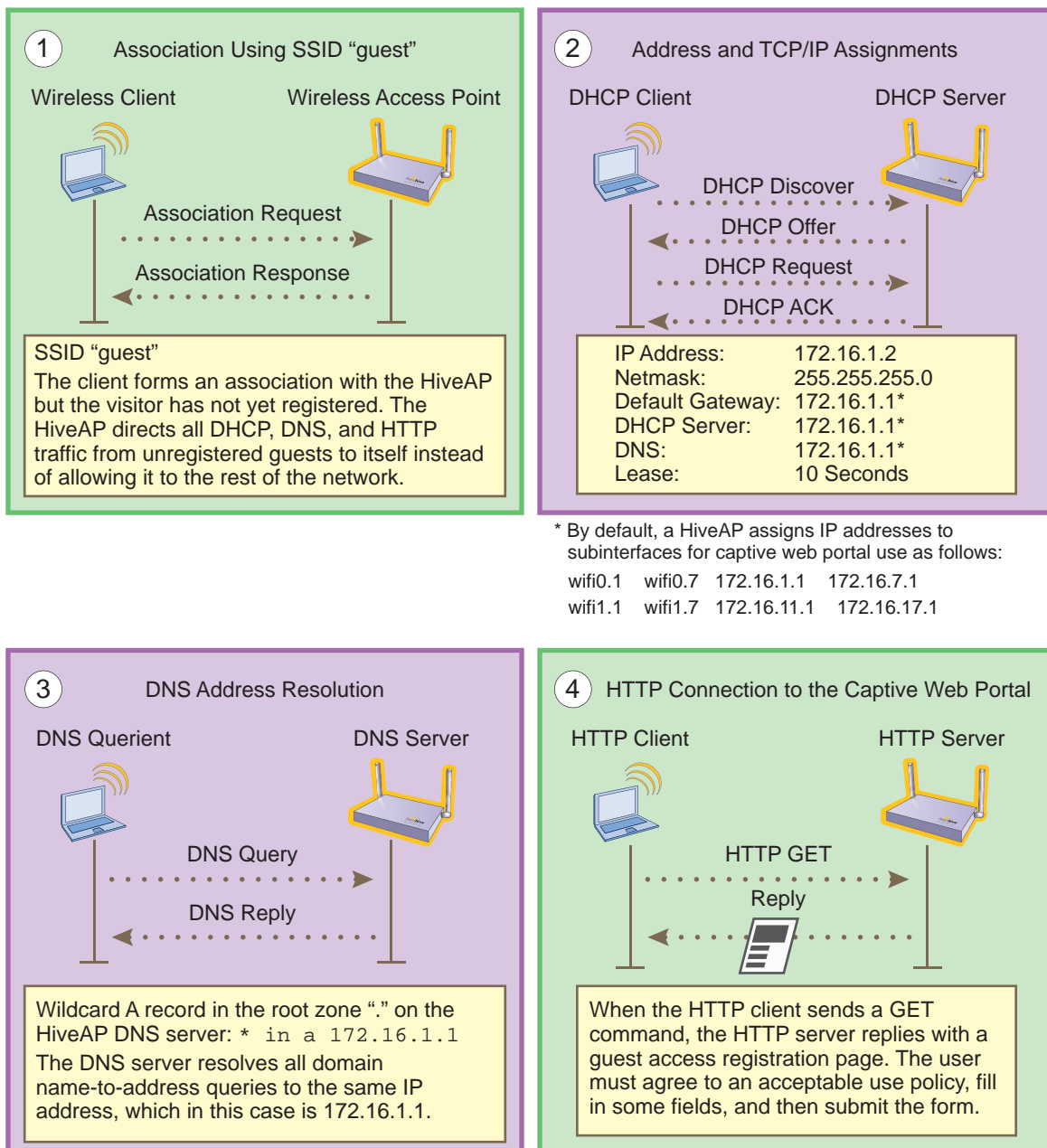


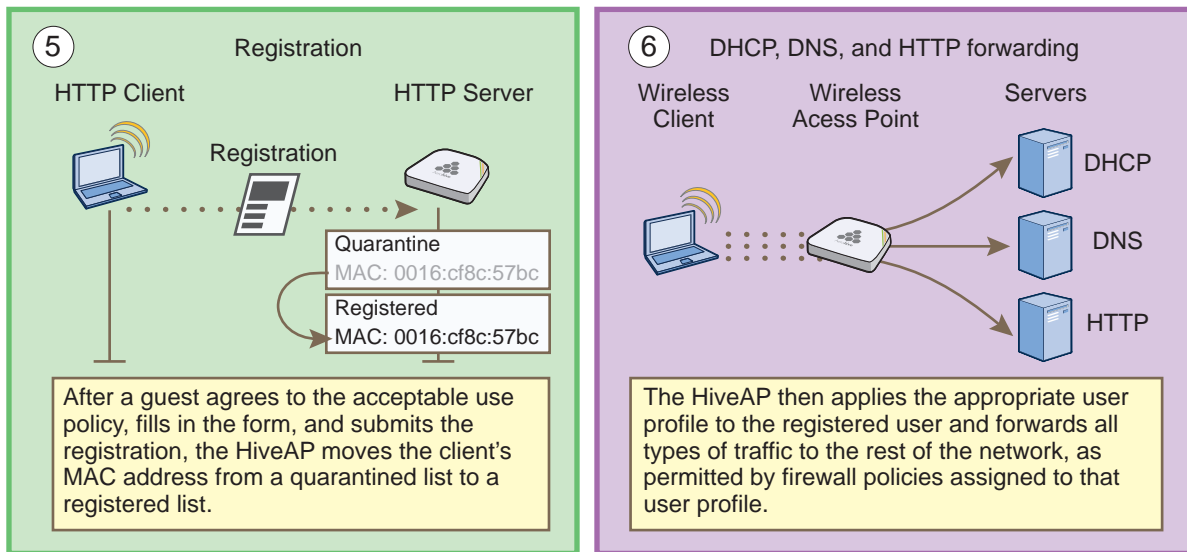
To enable the captive web portal to forward DHCP and DNS traffic from unregistered users to external servers on the network, click **Configuration > Advanced Configuration > Authentication > Captive Web Portals > New**, and select **Use external DHCP and DNS servers on the network**.

Captive Web Portal with Internal DHCP and DNS Servers

With this approach, when the client of an unregistered user first associates with the HiveAP, it acts as a DHCP, DNS, and web server, limiting the client's network access to just the HiveAP with which it is associated. No matter what website the user tries to reach, the HiveAP directs the browser to a registration page. After the user registers, the HiveAP stores the client's MAC address as a registered user and stops keeping the station captive; that is, the HiveAP no longer acts as a DHCP, DNS, and web server for traffic from that MAC address, but allows the client to access external servers. The entire process is shown in [Figure 9](#).

Figure 9 Captive web portal exchanges using internal servers





To enable the captive web portal to forward DHCP and DNS traffic from unregistered users to its internal servers, click **Configuration > Advanced Configuration > Authentication > Captive Web Portals > New**, and select **Use internal DHCP and DNS servers on the HiveAP**. By default, the internal DHCP server issues leases with a ten-second lifetime, and if a client with a nonexistent lease requests a lease renewal, the HiveAP responds by broadcasting a DHCP NAK. You can change the HiveAP response so that it sends a unicast NAK or ignores the request completely (Keep Silent).

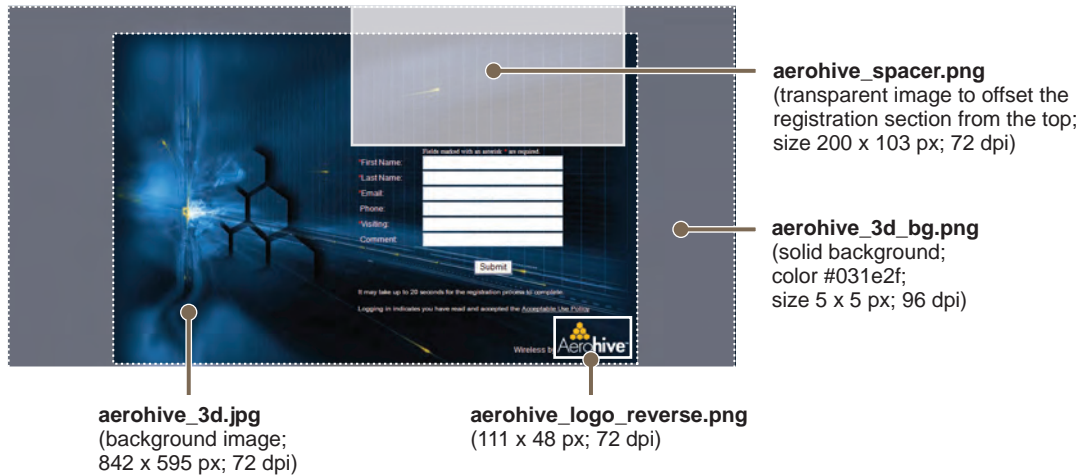
Modifying Captive Web Portal Pages

Aerohive provides .html files and images for use on the captive web portal server and a tool in the GUI to modify the supplied text, colors, and images to better suit the needs of your organization. The various file names and their purposes are as follows. An example of the default web page components is shown in [Figure 10 on page 156](#):

- registration.html (the main login page for self-registration)
- auth-reg.html (the main login page for either self-registration or user authentication)
- success.html (the page that appears after registering successfully)
- failure.html (the page that appears after an unsuccessful registration attempt)
- reg.php (a file that the HiveAP generates automatically and stores on its internal web server)
- aerohive_spacer.png (a transparent image that provides space at the top of web pages; size 200 x 103 px)
- aerohive_3d_bg.png (an image that provides blue filler as background around the main image; size 5 x 5 px)
- use-policy.html (the page that appears when you click the Acceptable Use Policy link on the registration.html or auth-reg.html pages)
- authentication.html (the main login page for user authentication)
- eula.html (the login page for the acceptable use policy)
- aerohive_3d.jpg (default main image on the web pages)
- aerohive_hex_light.jpg (optional background image)
- aerohive_hex_dark.jpg (optional background image)
- aerohive_logo_reverse.png (Aerohive logo with white text at the bottom of the web pages; size 111 x 48 px)
- aerohive_logo.png (Aerohive logo with dark text; size 111 x 48 px)

Figure 10 Components of the captive web portal self-registration page

The registration.html page with Self registered set as the registration type (When you set the registration type as Authenticated or Both, there are different fields for the user to complete than those shown here.)



Unregistered users' browsers are redirected to the login page of the captive web portal for the SSID to which they associate. The login page might be registration.html, authentication.html, or auth-reg.html, depending on the registration method that you configure the portal to use. You can have a different registration page for each SSID.

To modify the default set of .html and image files for a captive web portal, do the following:

1. Click **Configuration > Advanced Configuration > Authentication > Captive Web Portals > New**.
2. Enter a name for the captive web portal configuration, and choose one of the following methods from the Registration Type drop-down list:

User Authentication: Requires users to submit a valid user name and password to log in. The HiveAP then forwards the submitted login credentials to a RADIUS server for authentication.

Self-registration: Requires users to enter data and accept a network use policy before being allowed to pass through the captive web portal.

Both (Auth/Self-reg): Requires users to submit either one of the two types of registration.

Use Policy Acceptance: Requires users to accept a network usage policy before accessing the network.

There is also a fifth option, External Authentication, which redirects unregistered users' HTTP and HTTPS traffic to a captive web portal on an external server instead of redirecting it to an internal captive web portal on a HiveAP. For information about configuring it, see the HiveManager online Help.)

Note: You can use Aerohive GuestManager or User Manager to provide network access to wireless users. A GuestManager administrator, called an operator, sets up user accounts on GuestManager. Then GuestManager uses its built-in RADIUS server to authenticate them. For information, see the Aerohive GuestManager Getting Started Guide. With User Manager, an admin or operator can create permanent or temporary user accounts based on private PSK accounts previously defined by a HiveManager admin. Information about setting up User Manager can be found in the HiveManager online Help.

- To modify the login page, expand **Captive Web Portal Login Page Settings**, select **Modify automatically generated web pages**, click **Customize Login Page**, modify any of the following settings to customize the look of the captive web portal pages, and then click **Save**:

Background Image: You have three preloaded image files to use—`aerohive_3d.jpg` (default), `aerohive_hex_dark.jpg`, and `aerohive_hex_light.jpg`—and you can also import an image file of your choice.

To import a background image, click **Add/Remove** to open the **Add/Remove CWP Web Page Resources** page. Click **Browse**, navigate to the image file and select it, and then click **Upload**.

Whatever size the background image is, it eventually tiles. If you use an image that tiles seamlessly, the tiling cannot be noticed. See the two alternative background images with hexagons in the **Background Image** drop-down list for examples.

Foreground Color: The foreground color controls the color of the text that appears on the page. By default, it is white (RGB 255, 255, 255), which shows up clearly against the dark blue of the default background image `aerohive_3d.jpg`. If you change the background image to something with lighter colors, such as `aerohive_hex_light.jpg`, you can make the foreground color darker to provide greater contrast.

Header Image: This image file is empty and acts as a shim or spacer to offset the form from the top of the page. By default, the header image is `aerohive_spacer.png`, and it is 200 x 103 px at 72 dpi. If you want to increase or decrease the space above the form, you can replace this with a different `.png` file. The file format is PNG (Portable Network Graphics) because it supports transparency. You can also replace it with a file containing an image if you prefer.

Footer Image: By default, this is a graphic of the Aerohive logo. The file name is `aerohive_logo_reverse.png` and its dimensions are 111 x 48 px at 72 dpi. If you replace this with a different image, make sure it has the same or nearly the same dimensions to avoid distortion.

Use Policy: This is a text file that states the company policy for network usage. A user can view the policy by clicking the "Acceptable Use Policy" link on the registration page during the captive web portal registration process. A generic policy is provided in the "use-policy.txt" file. You can export this file, edit it, and import the edited file, or replace it with a completely different file.

*Note: You can check how your customizations affect page appearance by clicking **Preview**.*

- In a similar manner, you can also modify the automatically generated pages that appear after a successful login and after an unsuccessful one. These pages appear after a user successfully registers or fails to register. The file names are `success.html` and `failure.html` and are called by the internal script `reg.php`. The background image, foreground color, header image, and footer image function similarly to those on the Login page. You can specify the same images or different ones on the result pages, and you can use preloaded images or import others to use instead.

Notice: The main difference between the success page and the login page is the notice that is displayed to users. By default, the notice on the is "You are now connected to the wireless network." You can modify this to a different message as long as it has fewer than 256 characters. You can click inside the text box and edit the text onscreen or copy text from an external source and paste it into the text box.

*Note: In addition to modifying the images and text for the preloaded HTML files and importing new image files, you can also import entire web pages. In the sections for the login page, success page, and failure page, select **Import custom web pages**, click **Add/Remove**, browse to the files that you want to import, and then click **Upload**.*

*You can also export the default captive web portal HTML and image files from HiveManager and use them for reference when designing new ones. To do that, click the **Export** option at the top of the **Configuration > Advanced Configuration > Authentication > Captive Web Portals > New page**.*

Configuring a Captive Web Portal

In this example, you configure a captive web portal to provide guests with wireless network access. The configuration includes the following elements:

"[Captive Web Portal](#)" - Define a captive web portal that uses self-registration, the auto-generated web pages provided in HiveManager, and external DHCP and DNS servers.

"[QoS Rate Limiting](#)" - To preserve bandwidth for employees, reduce the rate limit for guests somewhat.

"[Firewall Policy](#)" on page 159 - To maintain security, restrict visitors to accessing just the public network.

"[User Profile](#)" on page 161 - Apply the QoS rate limiting and firewall policy to the user profile that the HiveAP applies to traffic from successfully registered users.

"[SSID](#)" on page 163 - Configure an SSID that secures wireless traffic with a preshared key and permits access to the public network only through the captive web portal.

"[WLAN Policy](#)" on page 164 - Add the SSID to a WLAN policy.

"[Files and Configuration Upload](#)" on page 164 - Push the captive web portal files and the WLAN policy to the managed HiveAPs.

Guests use a preshared key to secure wireless traffic between their wireless clients and HiveAPs. After forming a secure association with a HiveAP, the HiveAP intercepts all outbound traffic—except DHCP, DNS, and ICMP traffic—and presents them with a self-registration page. The guests must complete a form and accept a network usage policy before being allowed to access the public network. Registered visitors' activity can be tracked and stored in historical logs on a syslog server for security and compliance auditing.

Captive Web Portal

To create a captive web portal requiring users to self-register to gain network access, click **Configuration > Advanced Configuration > Authentication > Captive Web Portals > New**, enter the following, leave all the other values at their default settings, and then click **Save**:

Name: **CWP-guest1**

Registration Type: **Self-registration**

Description: **Captive web portal for guest registration**

Leaving everything else at its default setting creates a captive web portal configuration that uses all the predefined web files and the default network settings. The DHCP, DNS, and ICMP traffic from the clients of unregistered users is allowed to pass through the HiveAP to external servers.

QoS Rate Limiting

To allot guests with enough bandwidth to satisfy basic network access but not enough to interfere with employee traffic, click **Configuration > Advanced Configuration > QoS Policies > Rate Control & Queuing > New**, enter the following, and then click **Save**:

Name: **QoS-Guests**

Per User Rate Limit: **2000 Kbps for 802.11a/b/g; 2000 Kbps for 802.11n**

This is the maximum amount of bandwidth that a single user belonging to this profile can use. It is far less than the bandwidth you can reserve for other users such as employees, but it should be sufficient for basic web access for visitors.

Description: **QoS per guest**

Per User Queue Management: Enter the following items in **bold**, and leave all other settings unchanged:

Class Number - Name	Scheduling Type	Scheduling Weight	Weight % (Read Only)	Policing Rate Limit (Kbps) (802.11a/b/g)	Policing Rate Limit (Kbps) (802.11n)
7 - Network Control	Strict	0	0%	0	0
6 - Voice	Strict	0	0%	0	0
5 - Video	Weighted Round Robin	60	28%	2000	2000
4 - Controlled Load	Weighted Round Robin	50	23%	2000	2000
3 - Excellent Effort	Weighted Round Robin	40	19%	2000	2000
2 - Best Effort 1	Weighted Round Robin	30	14%	2000	2000
1 - Best Effort 2	Weighted Round Robin	20	9%	2000	2000
0 - Background	Weighted Round Robin	10	4%	2000	2000

The rate limit for network control and voice is 0 Kbps because guests are not permitted to run any applications that would generate network control traffic or use VoIP applications. In this example, guests are expected to use cell phones or other phones provided for them. (If you want to provide VoIP for guests, then you must enable the SIP ALG, add another rule to the firewall policy permitting SIP traffic, and set the rate limit for voice at 128 Kbps.)

Firewall Policy

You create a firewall policy that permits outgoing HTTP and HTTPS traffic from within the corporate network to the public network but not to the corporate network itself. When applying the policy to a user profile, you apply a default action that denies all incoming traffic and all other unspecified types of outgoing traffic.

Address Objects

To make address objects for use in firewall rules to block traffic to private IP address space in the internal network, click **Configuration > Advanced Configuration > Network Objects > IP Objects/Host Names > New**, enter the following, and then click **Apply**:

Network: (select)

Object Name: **10.0.0.0/8**

In the IP Entry field, enter **10.0.0.0** for the IP address, **255.0.0.0** for the netmask, choose **Global** for the type, enter a useful description such as **Deny RFC 1918 (private addresses)**, and then click **Apply**.

To save the address and close the dialog box, click **Save**.

Repeat the above to create two more address objects, one for **172.16.0.0/12** (IP address = 172.16.0.0; netmask = 255.240.0.0) and another for **192.168.0.0/16** (IP address = 192.168.0.0; netmask = 255.255.0.0).

Custom Service

To make a custom service for NAT-T (NAT Traversal) to permit IKE traffic when traversing a NAT device, click **Configuration > Advanced Configuration > Network Objects > Network Services > New**, enter the following, and then click **Save**:

Name: **NAT-T**

Description: **NAT Traversal**

IP Protocol: **UDP (17)**

Port Number: **4500**

Service Idle Timeout: **1800**

ALG Type: (leave blank)

Firewall Policy Rules

To create an IP firewall policy to control outgoing traffic, click **Configuration > Advanced Configuration > Security Policies > IP Policies > New**, and enter the following:

Policy Name: **guest-IP-policy-from-access**

Description: **Allow guests to access the public network**

To add rules to permit DHCP, DNS, HTTP, HTTPS, IKE, and NAT-T to the public network while denying any type of traffic to the internal network, enter the following (CTRL-click to select multiple services):

(Action)	Source	Destination	Service	Action	Logging*	(Action)
	[-any-] [†]	[-any-] [†]	DHCP-Server, DNS [‡]	Permit	Off	Click Apply .
Click New .	[-any-]	10.0.0.0/8	[-any-]	Deny	Dropped Packets	Click Apply .
Click New .	[-any-]	172.16.0.0/12	[-any-]	Deny	Dropped Packets	Click Apply .
Click New .	[-any-]	192.168.0.0/16	[-any-]	Deny	Dropped Packets	Click Apply .
Click New .	[-any-]	[-any-]	HTTP, HTTPS, IKE, NAT-T	Permit	Both	Click Apply .
Click New .	[-any-]	[-any-]	[-any-]	Deny	Dropped Packets	Click Apply .

* You do not enable logging for DHCP and DNS services because they would generate too many log entries. You enable logging for packets that HiveManager drops due to the enforcement of rules that deny traffic (Dropped Packets) and the logging of session initiation and termination (Both) for traffic permitted by policy rules.

† Because the source for DHCPDISCOVER and DHCPREQUEST messages does not yet have an IP address and the destination is 255.255.255.255 for broadcast traffic, both the source and destination IP addresses must be set as "[-any-]".

‡ Press the SHIFT key while selecting multiple contiguous services, and the CTRL key while selecting multiple contiguous or noncontiguous services. When you click **Apply**, HiveManager generates a separate rule for each service.

HiveManager adds new rules to the bottom of the rule list, so that if you enter the rules in the order presented above, they will already be in the correct positions, as shown in [Figure 11](#). The HiveAP firewall checks policy rules from top to bottom and applies the first match that it finds.

Figure 11 Firewall policy rules

The screenshot shows the 'IP Policies > New' configuration window. It includes a 'Policy Name' field with the value 'guest-IP-policy-from-access' and a 'Description' field with the value 'Allow guests to access the public network'. Below these fields is a 'Policy Rule' section with a table of rules. The table has columns for 'Rule ID', 'Source IP', 'Destination IP', 'Service', 'Action', and 'Logging'. There are 10 rules listed, each with a checkbox on the left and 'Up' and 'Down' buttons on the right.

Rule ID	Source IP	Destination IP	Service	Action	Logging
<input type="checkbox"/> 1	[-any-]	[-any-]	DHCP-Server	Permit	Off
<input type="checkbox"/> 2	[-any-]	[-any-]	DNS	Permit	Off
<input type="checkbox"/> 3	[-any-]	10.0.0.0/8	[-any-]	Deny	Dropped Packets
<input type="checkbox"/> 4	[-any-]	172.16.0.0/12	[-any-]	Deny	Dropped Packets
<input type="checkbox"/> 5	[-any-]	192.168.0.0/16	[-any-]	Deny	Dropped Packets
<input type="checkbox"/> 6	[-any-]	[-any-]	HTTP	Permit	Both
<input type="checkbox"/> 7	[-any-]	[-any-]	HTTPS	Permit	Both
<input type="checkbox"/> 8	[-any-]	[-any-]	IKE	Permit	Both
<input type="checkbox"/> 9	[-any-]	[-any-]	NAT-T	Permit	Both
<input type="checkbox"/> 10	[-any-]	[-any-]	[-any-]	Deny	Dropped Packets

Note: If you need to rearrange a set of policy rules, select the check box to the left of a rule, and then click the **Up** and **Down** buttons on the right to move the selected rule to a new position.

The rules in this policy allow clients to access a DHCP and DNS server to get their network settings and resolve DNS queries so that they can access the captive web portal. They deny traffic to all private IP address spaces, thus blocking access to the internal network. Rules 7-9 allow HTTP and HTTPS traffic so that guests can browse the public network and they allow IKE and NAT-T traffic so that they can make VPN connections back to their corporate sites. Finally, rule 10 logs all outgoing packets that HiveAPs drop because the firewall blocked them.

To save the firewall policy and close the dialog box, click **Save**.

Note: You do not have to create a policy to control incoming traffic because you will set the default action to deny all incoming and outgoing traffic not specified in any of the policy rules.

User Profile

A user profile contains the rate control and queuing QoS settings, VLAN, firewall policies, tunnel policy, and schedules that you want the HiveAP to apply to traffic from certain users. Because the SSID in this example uses a preshared key for user authentication, you can assign a single user profile to it.¹ The HiveAP then applies the various settings in the user profile to all traffic on this SSID.

To define a user profile so that HiveAPs can apply the appropriate QoS settings, VLAN, and firewall policies to all traffic on that SSID, click **Configuration > User Profiles > New**, enter the following, leave the other settings as they are, and then click **Save**:

Name: Self-reg-guests(3)

The number 3 is included as part of the user profile name so that you can easily know its attribute number when looking at the user profile name.

Attribute Number: 3

You must enter an attribute number that is unique for the WLAN policy to which the user profile is attached. Although you can define different user profiles with the same attribute number in HiveManager, the attribute number must be unique for each user profile that appears in the same WLAN policy. You can set an attribute number between 1 and 4095. (The default user profile "default-profile", which cannot be deleted, uses attribute 0.)

In this example, you only associate the user profile to an SSID that authenticates users with a preshared key, so the attribute number is not used here. It becomes important if you use a remote RADIUS authentication server for IEEE 802.1X authentication. When replying to a successful user authentication request, the server returns a set of attributes, and HiveAPs use a combination of three of them to determine which user profile to assign to traffic from an authenticated user:

Tunnel-Type = GRE (10)

Tunnel-Medium-Type = IP (1)

Tunnel-Private-Group-ID = <number>

If a HiveAP receives all three attributes and the Tunnel-Private-Group-ID matches the attribute of a user profile, it then applies that user profile to traffic from the authenticated user. Regardless of its ultimate use in an SSID using a preshared key or 802.1X, the attribute number for a user profile is a required setting.

Default VLAN: 1

Description: Visiting guests

Manage users for this profile via User Manager: (clear)²

1. An SSID using a preshared key supports a single user profile. An SSID using 802.1X authentication can support multiple user profiles.
2. Although not a component in this example, User Manager is an excellent option for guest management. Information about setting up and managing users through User Manager is available in the HiveManager online Help. You can perform a search for "User Manager", or navigate through the TOC to Home > Administration > User Manager.

Expand **Firewalls**, and enter the following in the IP Firewall Policy section:

From-Access: **guest-IP-policy-from-access**

This is the policy that you created in ["Firewall Policy" on page 159](#).

To-Access: (nothing)

Default Action: **Deny**

Expand **QoS Settings**, and enter the following:

Rate Control & Queuing Policy: **QoS-Guests**

This is the policy that you created in ["QoS Rate Limiting" on page 158](#). The HiveAP applies these rates and scheduling to users that belong to this user profile on an individual basis.

CAC Guaranteed Airtime: **0** (default)

CAC (Call Admission Control) monitors the HiveAP resource load and airwaves for congestion, and then determines whether to allow additional VoIP calls using SIP (Session Initiation Protocol) or Vocera services to initiate on that HiveAP. If the HiveAP and airwaves are already over-utilized, then a new caller is not permitted to start a call. Because this user policy will not be applied to voice traffic, it is unnecessary to set this.

Policing Rate Limit a/b/g mode (0-54000 Kbps): **2000**

Policing Rate Limit 11n mode (0-2000000 Kbps): **2000**

The maximum traffic policing rate for the entire user profile is the same as that for an individual user. By keeping the two rates the same, a single online user is not restricted to a smaller rate than that of the profile to which he or she belongs. (These rates can be the same as or greater than the individual user rates.)

Setting a rate limit of 2000 Kbps provides guests with a basic amount of available bandwidth without interfering with the bandwidth usage of other users, such as employees.

Scheduling Weight: **5**

The weight defines a preference for forwarding traffic. It does not specify a percentage or an amount. Its value is relative to the weights of QoS schedules in other user profiles in the same WLAN policy.

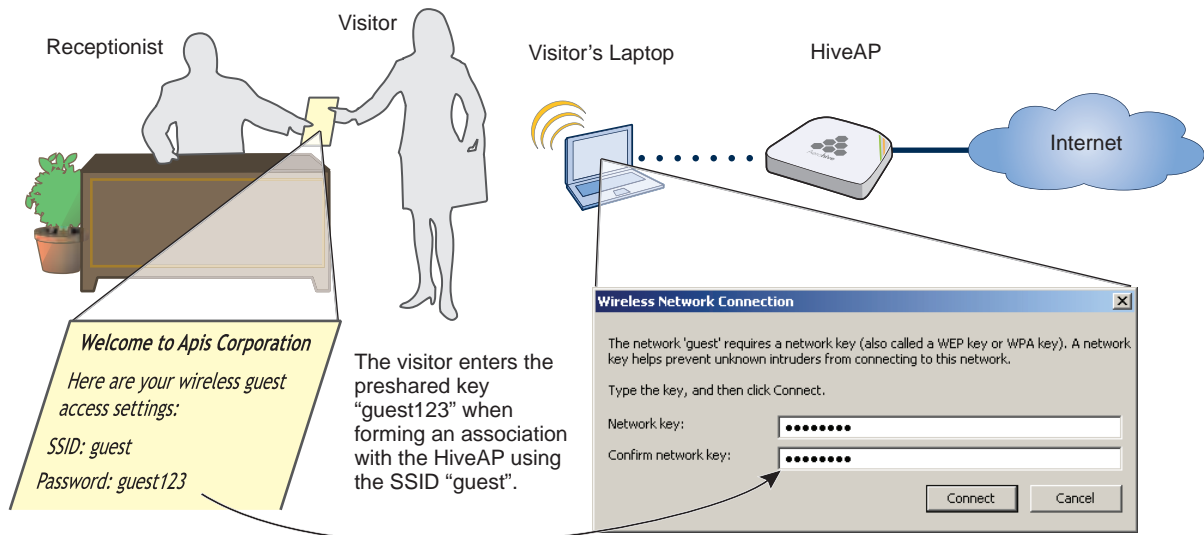
Because wireless access for guests is mainly a convenience and not a necessity, you assign it a weight that is low in comparison to the weights of other user profiles to give guests the lowest priority. In this example, 5 is used. Because this setting is a relative weight, modify it as necessary based on the weights of the other user profiles present.

Note: Although HiveAPs apply policing at all times, they only apply scheduling weights when usage is at maximum capacity.

SSID

You can provide visitors with secure but unregistered network access by issuing them a preshared key to use when associating with the guest SSID. A receptionist can provide visitors with the preshared key along with access instructions upon their arrival, as shown in Figure 12. This approach provides visitors with secured network access by using WPA or WPA2 with preshared keys and TKIP or CCMP (AES) encryption.

Figure 12 Guest access using a preshared key



The guest SSID provides secure network access for visitors. Also, by linking visitors to the guest SSID, you can differentiate them from employees—who associate with other SSIDs—so that you can apply one group of settings for visitors and another for employees. In addition, by assigning employees and guests to different VLANs, you can separate their traffic.

To create an SSID for guest access, click **Configuration > SSIDs > New**, enter the following, leave all other values at their default settings, and then click **Save**:

- Profile Name: **guest**
- SSID: **guest**
- Description: **SSID for registering company guests**
- SSID Access Security: **WPA/WPA2 PSK (Personal)**
- Use Default WPA/WPA2 PSK Settings: **(select)**
- Key Value and Confirm Value: **guest123**
- Enable Captive Web Portal: **(select); CWP-guest1**
- Self-Registration Access: User Profile: **Self-reg-guests(3)**
- SSID Broadcast Band: **2.4 GHz (11n/b/g)**

WLAN Policy

To add the SSID to an existing WLAN policy, click **Configuration > WLAN Policies > wlan_policy**, enter the following and then click **Save**:

In the SSID Profiles section, click **Add/Remove SSID Profile**, select **guest** in the Available SSID Profiles list, click the right arrow (>) to move the SSID profile to the Selected SSID Profiles list, and then click **Apply**.

Files and Configuration Upload

To push the files and configuration to the managed HiveAPs on which you want to provide guest access, click **Monitor > Access Points > HiveAPs > (select HiveAPs) > Update > Upload and Activate Configuration**, enter the following, and then click **Upload**:

Upload and activate configuration: (select)

Upload and activate CWP pages and Server key: (select)

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

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

List of all HiveAPs selected on the Monitor > Access Points > HiveAPs page: (select)

Because the WLAN policy for the selected HiveAPs contains an SSID using captive web portal files, upload and activate the files required for the captive web portal to function and also the configuration. HiveManager uploads the captive web portal files first followed by the configuration.

The HiveAP Update Results page appears so that you can monitor the progress of the upload procedure. When complete, "100%" appears in the Upload Rate column and "Successful" appears in the Update Result column.

Note: *If a managed HiveAP already has the maximum number of captive web portal directories (8), you must remove at least one of them before you can add a new one. To see how many directories are already on a HiveAP and remove a directory if necessary, do the following:*

1. Click **Monitor > Access Points > HiveAPs > (select a HiveAP) > Update > Remove Captive Web Page Directory > Remove Specific Web Page Directory**.
2. Select the check box of the directory that you want to remove, and then click **Submit**.

To test the captive web portal:

1. Take a wireless client near one of the HiveAPs, and form an association with the guest SSID, entering *guest123* when prompted for the preshared key.
2. After the client has formed an association, open a web browser.

The HiveAP intercepts the HTTP or HTTPS traffic from your browser to the URL of its home page and redirects it to the login page (*registration.html*) on the captive web portal.

3. Complete the registration form, and then click **Submit**.

After a successful registration, the "Login Successful" page appears.

4. Close the web page and open a new browser instance.

The browser successfully opens to its home page, and you can visit other sites on the public network. If there is any web server on the local network, try to browse to it and you will find that it is not possible. Similarly, if you try to ping the default gateway or a remote website (*www.aerohive.com*, for example), you will find that you do not receive any responses because the firewall does not permit ICMP traffic to either the internal or external network. On the other hand, if there is a remote IKE peer to which you can build a VPN tunnel, you will find that you will be able to do so.

EXAMPLE 4: PRIVATE PSKS

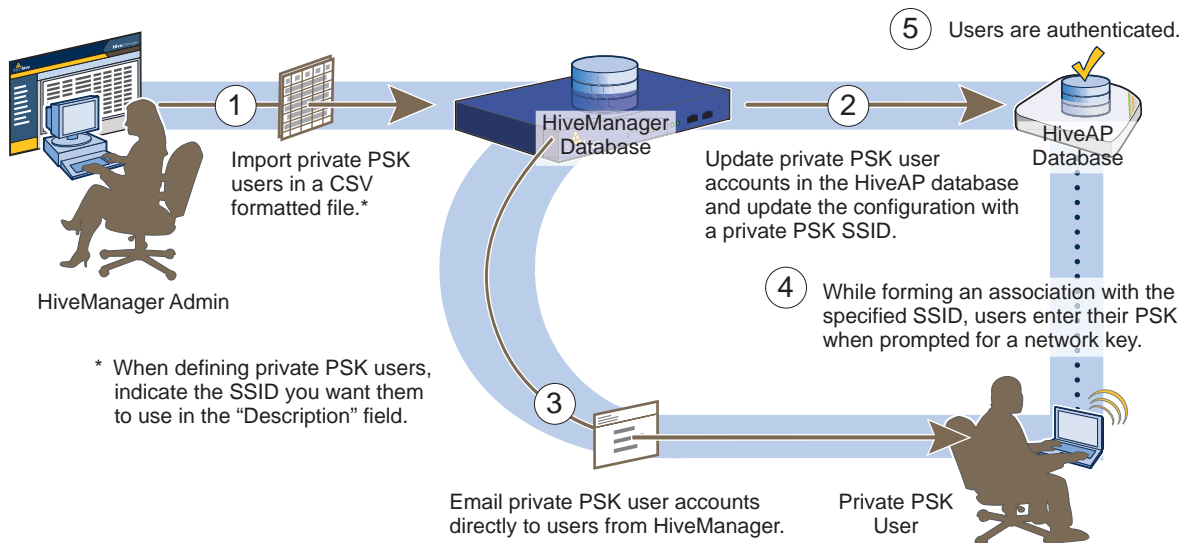
Private PSKs are unique preshared keys created for individual users on the same SSID.³ They offer unique keys per user and user profile flexibility (similar to 802.1X) with the simplicity of preshared keys. For this example, the steps for generating, applying, and distributing private PSK user data are as follows:

1. Define two user profiles.
2. Create two private PSK user groups. Each group includes an attribute that links it to one of the user profiles.
3. Import manually created private PSK users and assign them to one of the two private PSK user groups.
4. Create an SSID that references the private PSK groups and user profiles to which the PSK groups link.
5. Reference the SSID in a WLAN policy.
6. Push the configuration and user database to managed HiveAPs.
7. Email private PSK user data to individuals to use when connecting to the network through the SSID.

Note: Before you can email the private PSK user data, you must configure the SMTP server and From Email settings in the Update Email Service Settings section on the Home > Administration > HiveManager Services page.

An overview of the process is shown in [Figure 13](#).

Figure 13 Private PSK configuration, application, distribution, and usage



3. It is also possible for groups of users to use the same private PSK. For example, you might find it expedient to create a single private PSK user for visitors. You then email the private PSK user data to the lobby ambassador to hand out to all visitors that arrive that week. If you set the validity period so that it recurs on a weekly basis, HiveManager and the HiveAPs generate a new PSK for that private PSK user each week. With this approach, the HiveAPs update the PSK automatically at the start of each new week, and you simply email the new data from HiveManager to the lobby ambassador to distribute to that week's visitors. (Note that it is important that the system clocks on HiveManager and the HiveAPs be synchronized for this to work properly.)

User Profiles

Unlike a traditional PSK SSID, a private PSK SSID can support multiple user profiles. For this example, you create two user profiles, one for employees with full network access and another for contractors with limited access.

To define a user profile for employees, click **Configuration > User Profiles > New**, enter the following, leave the other settings as they are, and then click **Save**:

Name: **Employees(30)**

The number 30 is included as part of the user profile name so that you can easily know its attribute.

Attribute Number: **30**

The HiveAP uses this attribute number to link the user profile to a user group with the same attribute. You can use any number between 1 and 4095.

Default VLAN: **1**

Description: **Corporate employees**

To define a user profile for contractors with a firewall policy that allows basic network protocols to the public network while blocking access to the internal network, click **Configuration > User Profiles > New**, enter the following, leave the other settings as they are, and then click **Save**:

Name: **Contractors(35)**

Attribute Number: **35**

Default VLAN: **1**

Description: **short-term contractors**

Expand **Firewalls**, and enter the following in the IP Firewall Policy section:

From-Access: Click the **New** icon to open the IP Firewall Policy dialog box, and then enter the following:

Policy Name: **contractors-outgoing-IP-policy**

Description: **Apply to contractor user profiles**

Policy Rules:

To add rules permitting only DHCP, DNS, HTTP, and HTTPS to the public network while denying any type of traffic to the internal network, enter the following (use CTRL-click or SHIFT-click to select multiple services):

(Click ...)	Source	Destination *	Service	Action	Logging	(Click ...)
	[-any-]	[-any-]	DHCP-Server, DNS	Permit	Off	Apply.
New.	[-any-]	10.0.0.0/8	[-any-]	Deny	Dropped Packets	Apply.
New.	[-any-]	172.16.0.0/12	[-any-]	Deny	Dropped Packets	Apply.
New.	[-any-]	192.168.0.0/16	[-any-]	Deny	Dropped Packets	Apply.
New.	[-any-]	[-any-]	HTTP, HTTPS	Permit	Both	Apply.

* The three addresses "10.0.0.0/8", "172.16.0.0/12", and "192.168.0.0/16" that define private network address space were created in a previous example. See ["Address Objects" on page 159](#).

Click **Save** to save the IP firewall policy and return to the User Profile dialog box.

From-Access: **contractors-outgoing-IP-policy** (This is the firewall policy that you just created.)

To-Access: (nothing)

Default Action: **Deny**

Private PSK User Groups

You next create two private PSK user groups, one for employees and another for contractors.

To create a private PSK user group for employees, click **Configuration > Advanced Configuration > Authentication > Local User Groups > New**, enter the following, and then click **Save**:

User Group Name: **Employees(30)**

Including the attribute number in the private PSK user group name and in the user profile name makes it easier to match them when configuring the SSID.

Description: **Corp employees**

User Type: **Manually created private PSK users**

User Profile Attribute: **30**

This must be the same number as the user profile "Employees(30)".

VLAN ID: **1**

If you leave this field empty, the HiveAP applies the VLAN ID set in the Employees(30) user profile, which is already set as 1. If you set a different VLAN ID here than the one in the user profile, this setting takes precedence over the one in user profile.

Reauthorization Time: **1800** (default)

This setting is only used when private PSK user accounts are stored on a RADIUS server and a reauthorization interval is not set on the server for those users. If user accounts are stored on a RADIUS server that returns a reauthorization interval attribute, the HiveAPs use that value instead of this one. If user accounts are stored locally on HiveAPs, the HiveAPs ignore this setting.

To create a private PSK user group for contractors, click **Configuration > Advanced Configuration > Authentication > Local User Groups > New**, enter the following, and then click **Save**:

User Group Name: **Contractors(35)**

Description: **Contractors at corp**

User Type: **Manually created private PSK users**

User Profile Attribute: **35**

VLAN ID: **1**

Reauthorization Time: **1800** (default)

Note: If you want to define advanced options, click + to expand the Private PSK Advanced Options section. You can modify the characteristics of keys that HiveManager generates, such as their length, the types of characters used in them, the method of their generation, and the period of time during which they are valid. This example uses the default settings, one of which is the requirement that the password in the imported .csv file must contain letters, digits, and special characters. This requirement has significance in the next section, "Importing Private PSK Users" on page 168

Importing Private PSK Users

Create a list of private PSK users in a .csv file, assign them to the two private PSK user groups Employees(30) and Contractors(35), and import the file to HiveManager.

1. Define a set of private PSK users in a CSV-formatted file, and save it to your management system. The left-to-right order of columns in file must be as follows:

User Name, User Type (3), User Group Name, Password, Email, Description, Virtual HiveManager Name

The value 3 indicates that the user type is a manually defined private PSK user. When using the default settings, the password must contain letters, digits, and special characters.⁴ Multiple email addresses (up to 128 characters total) must be separated by semicolons without spaces before or after the semicolons. The text in the Description column is included in the email sent to users, so you use it to identify the SSID. The last column is only required if there is at least one virtual HiveManager system and you are logged in to "All VHM's" as an admin with superuser privileges. Otherwise, omit it.

The following is a sample of a few private PSK user definitions:

```
#User Name, User Type 3, User Group Name, Password, Email, Description, VHM
Bob Lai, 3, Employees(30), hon;VP#243, hm-admin@apis.com;blai@apis.com, Use SSID star, home
Jenny Lo, 3, Employees(30), loN#953d:)n, hm-admin@apis.com;jlo@apis.com, Use SSID star, home
Phil Wei, 3, Contractors(35), meX18ca1#!, hm-admin@apis.com;mgr@apis.com, Use SSID star, home
Bill Li, 3, Contractors(35), Cm$7)3b01!, hm-admin@apis.com;mgr@apis.com, Use SSID star, home
```

Notice that the private PSK user definitions for employees are sent directly to the people who will use them, but those for contractors are sent to a department manager for dissemination. All definitions are also sent to the HiveManager administrator as a backup.

2. Click **Configuration > Advanced Configuration > Authentication > Local Users > Import > Browse**, navigate to the file containing the private PSK user definitions, select it, and then click **Import**.

Private PSK SSID

To configure an SSID for the private PSK users that you have created, click **Configuration > SSIDs > New**, enter the following, and then click **Save**:

Profile Name: **star**

SSID: **star**

The profile name is the name that you reference in the WLAN policy and contains the SSID and related configuration objects, such as user profiles and user groups. The SSID is the name that HiveAPs broadcast. Although they can be different so that you can create different profiles for the same SSID for use at different locations, the two names are the same in this example.

Description: **Use for both employees and contractors**

SSID Access Security: **Private PSK**

Use Default Private PSK Settings: **(select)**

Private PSK User Groups: Select **Employees(30)** and **Contractors(35)** in the Available Private PSK User Groups list and then click the right arrow (>) to move them to the Selected Private PSK groups list.

User Profiles for Traffic Management: Select **Employees(30)** and **Contractors(35)** in the Available User Profiles list and then click the right arrow to move them to the Selected User Profiles list.

SSID Broadcast Band: **2.4 GHz (11n/b/g)**

This is the broadcast band for the radio operating in access mode.

4. If you do not include a password string in the imported file, HiveManager automatically generates a random string during the import process. For example, if the first entry omits the password, it would be as follows (note the empty space between the commas): Bob Lai, 3, Employees(30), , hm-admin@apis.com;blai@apis.com, Use SSID star, home

WLAN Policy

To add the SSID to a WLAN policy, click **Configuration > WLAN Policies > *wlan_policy_name* > Add/Remove SSID Profile**, select **star** in the Available SSID Profiles list, click the right arrow (>) to move it to the Selected SSID Profiles list, click **Apply**, and then click **Save**.

To push the private PSK user groups, users, and WLAN policy configuration to the HiveAPs on which you want to provide guest access, click **Monitor > Access Points > HiveAPs > (select HiveAPs) > Update > Upload and Activate Configuration**, enter the following, and then click **Upload**:

Upload and activate configuration: (select)

Upload and activate CWP pages and Server key: (clear)

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

Upload and activate employee, guests, and contractor credentials: (select)

List of all HiveAPs selected on the Monitor > Access Points > HiveAPs page: (select)

Because the WLAN policy for the selected HiveAPs contains an SSID using captive web portal files, upload and activate the files required for the captive web portal to function and also the configuration. HiveManager uploads the captive web portal files first followed by the configuration.

The HiveAP Update Results page appears so that you can monitor the progress of the upload procedure. When complete, "100%" appears in the Upload Rate column and "Successful" appears in the Update Result column.

Email Notification

To distribute the private PSK user definitions to the employees and the manager in charge of the contractors, click **Configuration > Advanced Configuration > Authentication > Local Users**, select the users, and then click **Email PSK**. The specified recipients receive a separate email message for each private PSK user, with content like the following:

PSK: hon;VP#243

Description: Use SSID star

User Name: Bob Lai

Start Time:

End Time:

If you define a lifetime for a private PSK user (configurable in the Private PSK Advanced Options section in the Local User Group dialog box), start and end times are also listed here. This can be useful if you want to provide users—such as the contractors in this example perhaps—with WLAN connectivity for a fixed period of time.

Instead of sending the private PSK users through email, you can also export them in a .csv file. To do that, select the users that you want to export, click the **Export PSK** button, and then save it to a directory of your choice. You can open the file using a spreadsheet program such as Microsoft Excel.

EXAMPLE 5: USING HIVEAP CLASSIFIERS

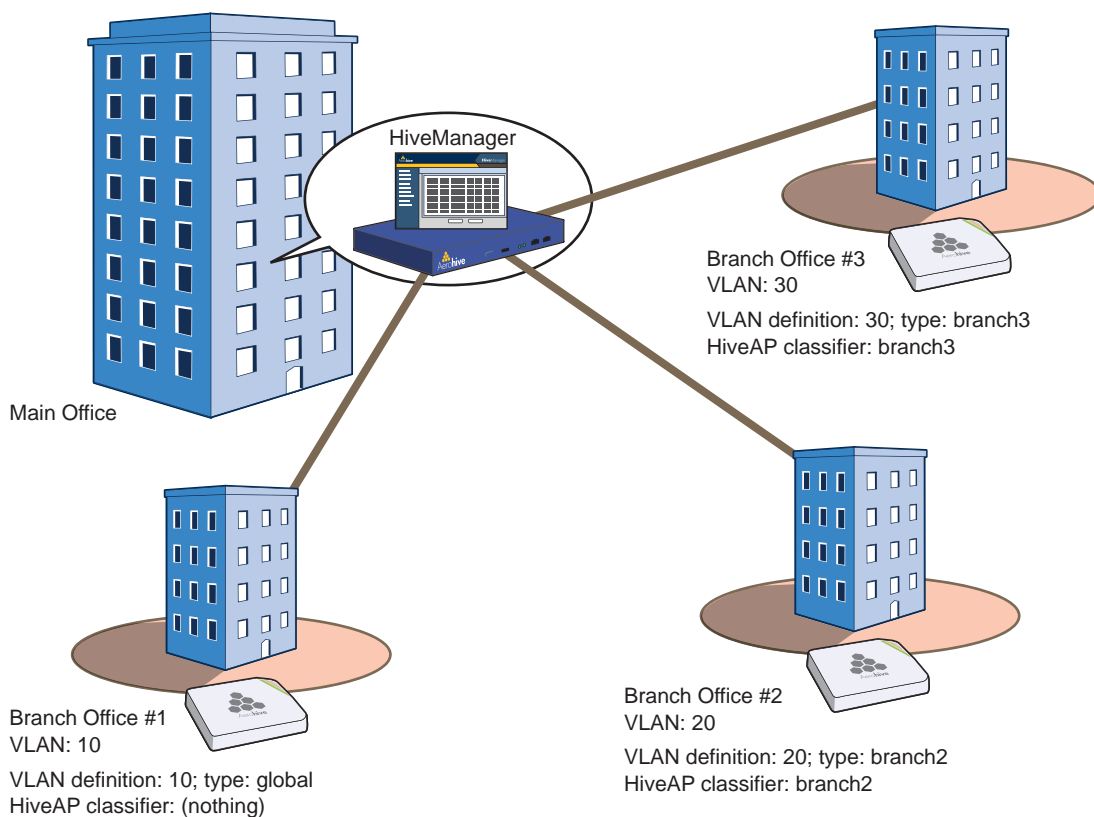
In HiveManager, some network objects can support multiple definitions as long as each definition is uniquely classified by a map name, HiveAP name, or classifier tag—and one of the definitions is classified as global. The definition classified as global is what HiveManager applies when none of the other more specific classification types are applicable. When you then assign a WLAN policy that includes that one network object to various HiveAPs, HiveManager applies the appropriate definition based on the location, name, or tag of each HiveAP. The network objects that support multiple definitions are IP addresses/host names, MAC addresses/OUIs, and VLANs.

In this example, there are four sites: a main office and three branch offices. You assign the same WLAN policy to the HiveAPs at all branch offices. However, the network at each office uses a different VLAN for its wireless clients:

- Branch office 1: VLAN 10
- Branch office 2: VLAN 20
- Branch office 3: VLAN 30

To continue using a single WLAN policy for all branch offices while supporting their different VLANs, you use HiveAP classifiers. You do not classify HiveAPs at branch office 1. As a result, they will use the VLAN definition classified as global. You classify the HiveAPs at branch offices 2 and 3 as "branch2" and "branch3". You also classify two VLAN definitions as "branch2" and "branch3" so that HiveManager will apply them to the HiveAPs with the same classifiers. The classification scheme is shown in Figure 14.

Figure 14 HiveAP classifiers and VLANs



Note: It is assumed that the HiveAPs have already been assigned to maps in the Topology section of the GUI.

The configuration steps are as follows:

1. Classify HiveAPs at branch offices 2 and 3.
2. Create a VLAN object with three definitions for VLANs 10, 20, and 30.
3. Reference the VLAN object in a user profile that is used in an SSID that is part of the WLAN policy used by the HiveAPs at each branch office.
4. Update all the HiveAPs and note how the user profile at each site has the correct VLAN definition.

Set HiveAP Classifiers

Click **Monitor > Access Points > HiveAPs (view mode: Config)**, and then click the column heading **Topology Map** to group the managed HiveAPs by the map to which they are assigned.

Multiselect the HiveAPs belonging to all the maps at branch office 2,⁵ click **Modify**, expand **Advanced Settings**, enter **branch2** in the Tag1 field, and then click **Save**.

Multiselect the HiveAPs belonging to all the maps at branch office 3, click **Modify**, expand **Advanced Settings**, enter **branch3** in the Tag1 field, and then click **Save**.

Create a VLAN Object with Three Definitions

Click **Configuration > Advanced Configuration > Network Objects > VLANs > New**, enter the following, and then click **Apply**:

VLAN Name: **branchVLAN-10-20-30**

VLAN ID: **10**

Type: **Global**

Description: **VLAN at branch office #1**

Click **New**, enter the following, and then click **Apply**:

VLAN ID: **20**

Type: **Classifier**

Value: **branch2**

Description: **VLAN at branch office #2**

Click **New**, enter the following, and then click **Apply**:

VLAN ID: **30**

Type: **Classifier**

Value: **branch3**

Description: **VLAN at branch office #3**

To save your settings and close the dialog box, click **Save**.

5. To multiselect all the HiveAPs on the same map, click the first HiveAP assigned to a map and then SHIFT-click the last one. This example assumes that you have used a naming convention that allows you to select HiveAPs on multiple maps at the same site because all the maps at that site begin with the same word, such as "branch2-floor1", "branch2-floor2", and so on.

Reference the VLAN Object

To assign the VLAN object to a user profile that is used in an SSID that is part of the WLAN policy assigned to the HiveAPs at all the branch offices:

Click **Configuration > User Profiles > *user_profile_name***, choose **branchVLAN-10-20-30** from the Default VLAN drop-down list, and then click **Save**.

The relationships among the objects from the HiveAPs down to each VLAN definition are as follows:

HiveAP > WLAN policy > SSID > user profile > VLAN object > VLAN definition	
—	VLAN 10; Type: global
branch2	VLAN 20; Type: classifier = branch2
branch3	VLAN 30; Type: classifier = branch3

Update HiveAPs

To apply the VLAN definitions to the HiveAPs at all the branch offices, click **Monitor > Access Points > HiveAPs**, multiselect the HiveAPs at all branch offices, click **Update > Upload and Activate Configuration**, and then enter the following:

Upload and activate configuration: (select)

Upload and activate CWP pages and Server key: (clear)

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

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

List of all HiveAPs selected on the Monitor > Access Points > HiveAPs page: (select)

The HiveAP Update Results page appears so that you can monitor the progress of the upload procedure. When complete, "100%" appears in the Upload Rate column and "Successful" appears in the Update Result column.

Check that the VLANs are being applied properly:

In the Upload and Activate Configuration dialog box, click the host name of a HiveAP at branch office 1, and then select **View Configuration**. Notice the VLAN ID that appears in the View Configuration-*hiveap_name* window that pops up:

```
user-profile name vlan-id 10
```

Close the Configuration Details window, and then click the host name of a HiveAP at branch office 2. The VLAN ID for the same user profile is 20:

```
user-profile name vlan-id 20
```

If you click the host name for a HiveAP at branch office 3, you can see that its VLAN ID is 30:

```
user-profile name vlan-id 30
```

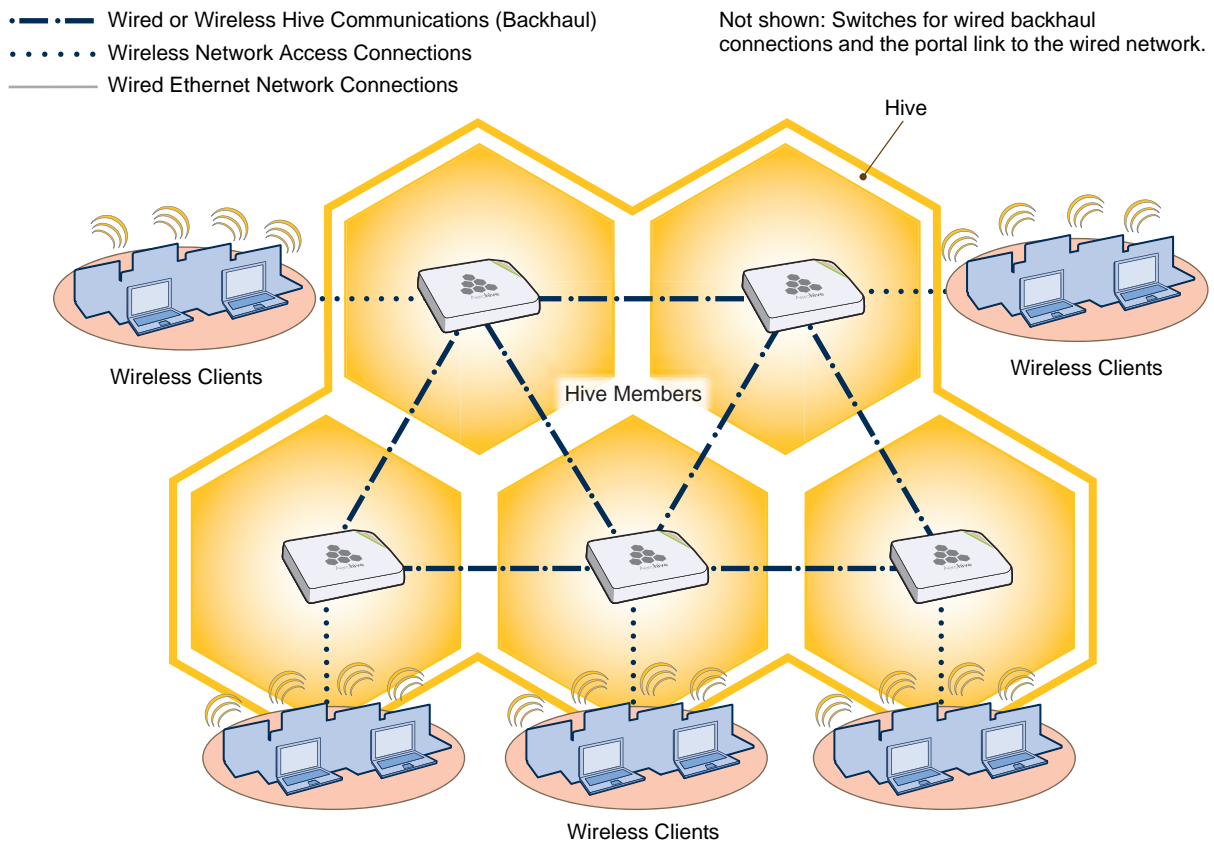
Make sure that all the HiveAPs in the list at the bottom of Upload and Activate Configuration page are selected, and then click **Upload**.

Chapter 13 HiveOS

You can deploy a single HiveAP and it will provide wireless access as an autonomous AP (access point). However, if you deploy two or more HiveAPs in a hive, you can provide superior wireless access with many benefits. A hive is a set of HiveAPs that exchange information with each other to form a collaborative whole (see [Figure 1](#)). Through coordinated actions based on shared information, hive members can provide the following services that autonomous APs cannot:

- Consistent QoS (Quality of Service) policy enforcement across all hive members
- Coordinated and predictive wireless access control that provides fast roaming to clients moving from one hive member to another
- Best-path routing for optimized data forwarding
- Automatic radio frequency and power selection

Figure 1 HiveAPs in a hive



HiveOS is the operating system that runs on HiveAPs.

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 HiveAPs belonging to that hive automatically initiate and maintain communications with each other.

Additionally, there are many default settings that simplify the setup of a HiveAP 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 HiveAP, management traffic between HiveAPs 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 181](#), you can enter a minimum of three commands to deploy a single HiveAP, 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 HiveAPs falls into two main areas: ["Device-Level Configurations"](#) and ["Policy-Level Configurations" on page 176](#). Consider your deployment plans and then refer to the following sections for guidance on the commands you need to configure them.

Note: 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 a HiveAP and its connectivity to wireless clients, the wired 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 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

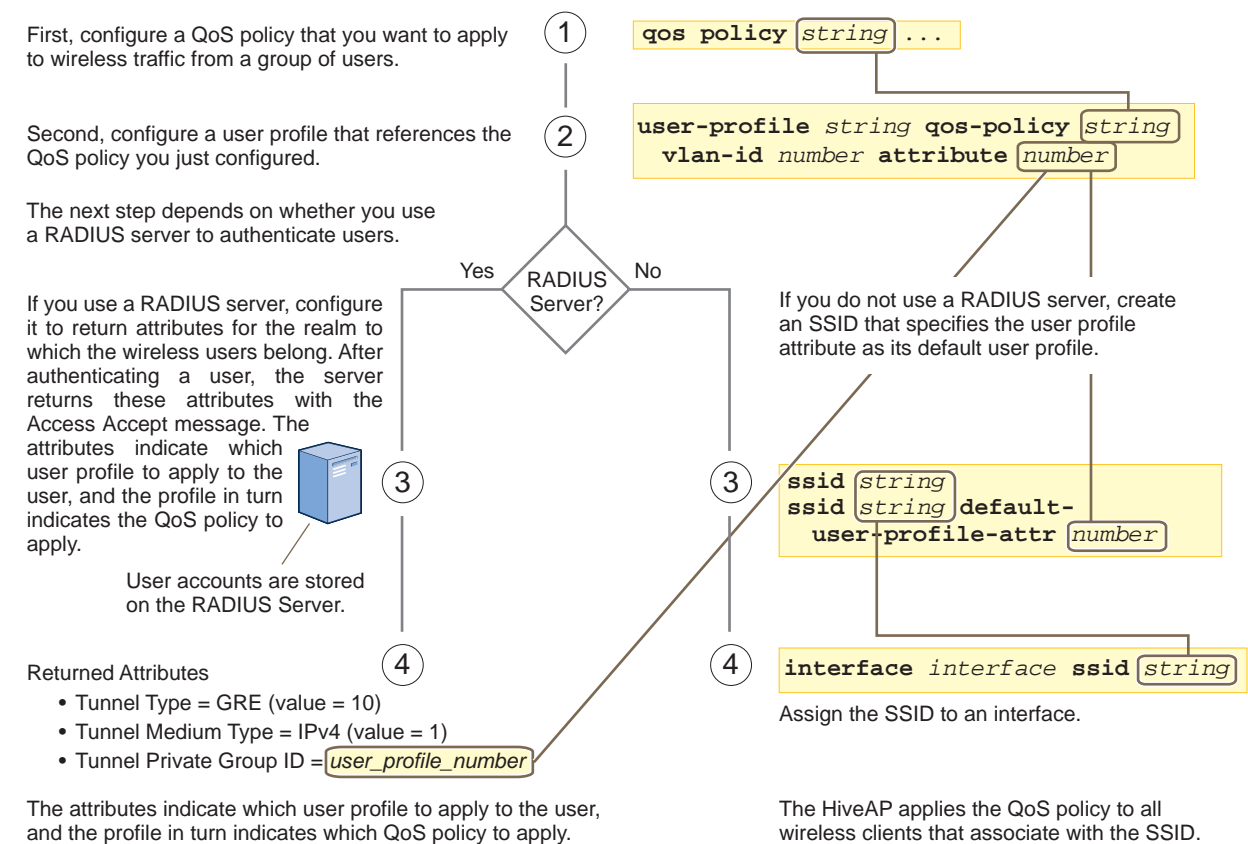

```
user-profile string ...
```
- SSIDs


```
ssid 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.

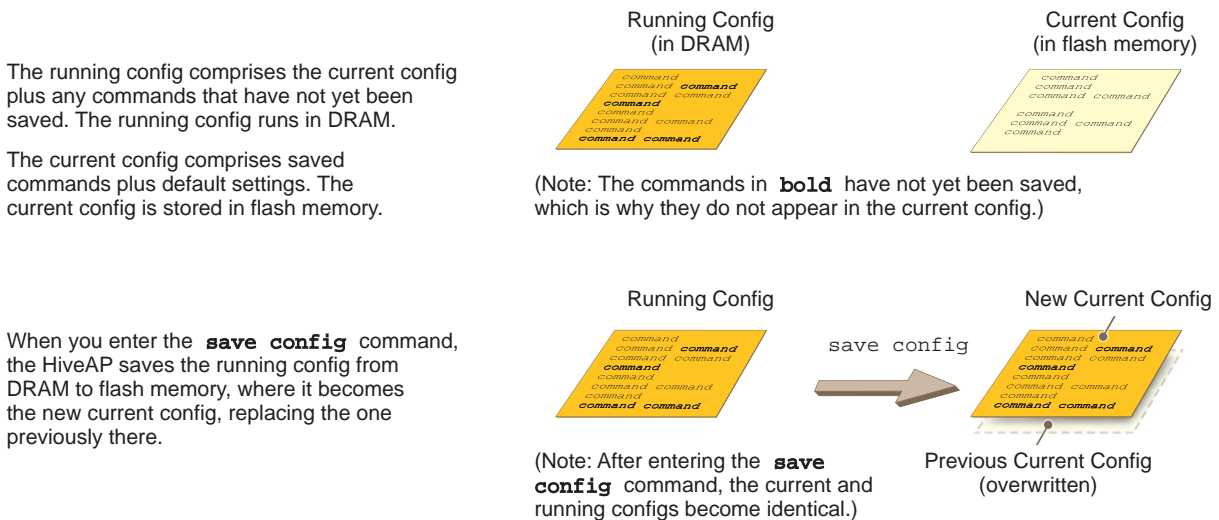
The **running** configuration (config) is the configuration that is actively running in DRAM. During the bootup process, a HiveAP loads the running config from one of up to four config files stored in flash memory:

- **current**: a flash file containing a combination of default and admin-defined settings. During the bootup process, this is the first config that the HiveAP 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 HiveAP 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 178](#) and [Figure 5 on page 178](#).
- **bootstrap**: a flash file containing a second config composed of a combination of default and admin-defined settings. The HiveAP 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 180](#).
- **default**: a flash file containing only default settings. If there is no bootstrap config, the HiveAP 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 180](#).

Note: There is also a failed config file, which holds any backup config that fails to load. See [Figure 5 on page 178](#).

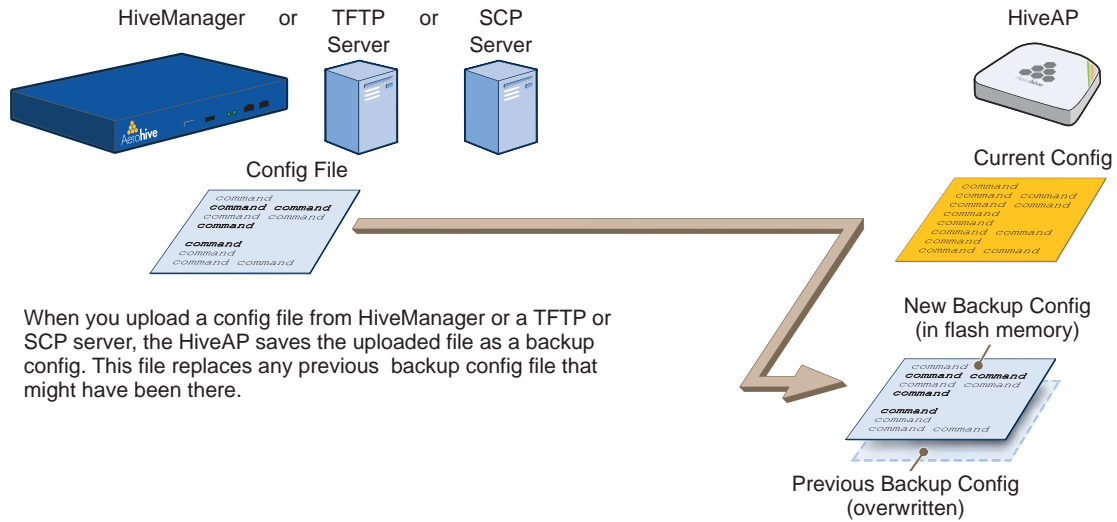
When using the CLI, the two most frequently accessed config types are the running config and current config. When you enter a command in the running config, the HiveAP performs it immediately. However, because the running config is stored in volatile memory (DRAM), the commands are not yet permanent and will be lost when the HiveAP 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



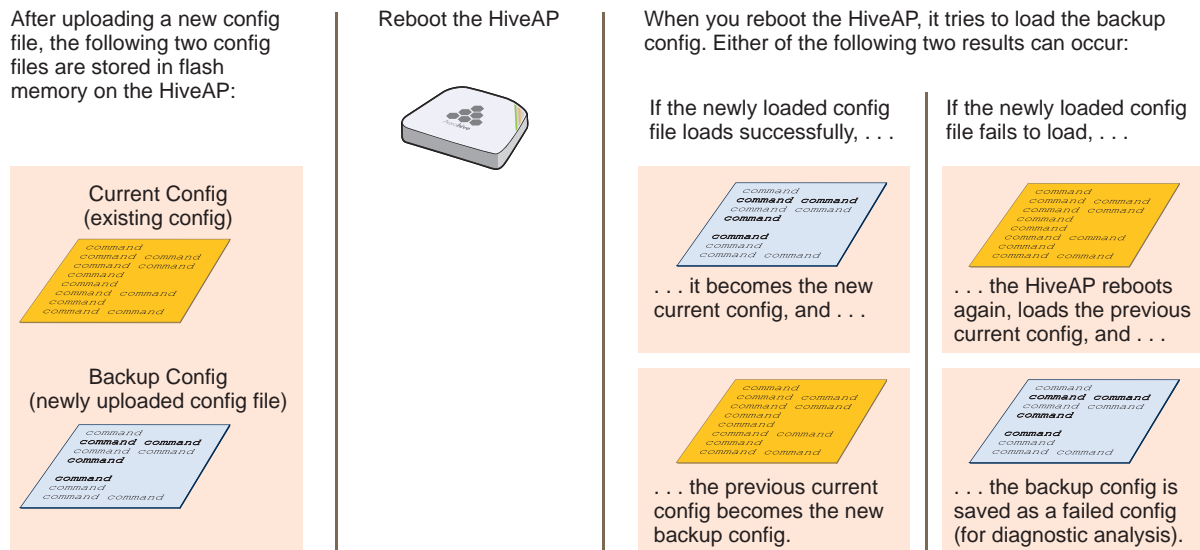
When you upload a configuration file from HiveManager or from a TFTP or SCP server, the HiveAP stores the uploaded file in the backup config partition in flash memory, where it remains until the HiveAP reboots. If there is a backup config file already stored in flash, the newly uploaded file overwrites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

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



When the HiveAP reboots, it attempts to load the the newly uploaded config file. If the file loads successfully, the HiveAP 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 HiveAP reboots again and loads the previous current config file. The HiveAP 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 a HiveAP



Note: To upload and activate a config file from HiveManager, see "Uploading HiveAP Configurations" on page 137. 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 a HiveAP 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 HiveAP 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 (see "Reset Button" on page 29, page 51, and page 73) or enter the **reset config** command. A HiveAP 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.

*Note: You can disable the ability of the reset button to reset the configuration by entering this command: **no reset-button reset-config-enable***

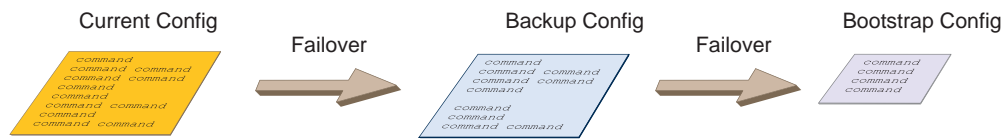
Reverting to the default config can be very useful, especially in the early stages when you are still learning about HiveOS and are likely to be experimenting with different settings. However, retaining the ability of a HiveAP to revert to its default settings after its deployment can present a problem if it is a mesh point in a hive. If the HiveAP 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 HiveAP 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 a HiveAP loads when you reset the configuration. See [Figure 6 on page 180](#).

Note: 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

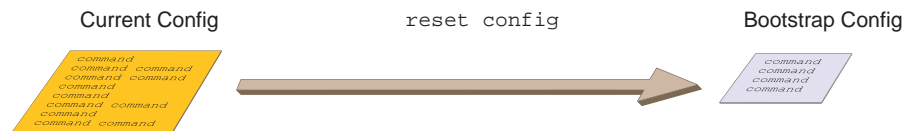


... or if there is no bootstrap config ...

If the HiveAP 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



... or if there is no bootstrap config ...

When you enter the **reset config** command or press the reset button on the front panel of the HiveAP device, the HiveAP 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 HiveAP to load as its bootstrap configuration (for an example, see ["Loading a Bootstrap Configuration" on page 200](#)). 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
```

Note: 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 14 Deployment Examples (CLI)

This chapter presents several deployment examples to introduce the primary tasks involved in configuring HiveAPs through the HiveOS CLI.

In ["Deploying a Single HiveAP" on page 182](#), you deploy one HiveAP 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 185](#), you add two more HiveAPs 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 HiveAP and on each wireless client.

In ["Using IEEE 802.1X Authentication" on page 190](#), you change the user authentication method. Taking advantage of existing Microsoft AD (Active Directory) user accounts, the HiveAPs 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 194](#), 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.

Note: 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 200](#), you load a bootstrap config file on the HiveAPs. 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. This example shows how 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 HiveAPs.

If you want to view just the CLI commands used in the examples, see ["CLI Commands for Examples" on page 203](#). 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 HiveAP
 - VT100 emulator on the management system
 - Serial cable (also called a "null modem cable") that ships as an optional accessory (AH-ACC-Serial-DB9). You use this to connect your management system to the HiveAP.

Note: You can also access the CLI by using Telnet or SSH (Secure Shell). After connecting a HiveAP 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 HiveAP 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 an AD (Active Directory) server and RADIUS server

EXAMPLE 1: DEPLOYING A SINGLE HIVEAP

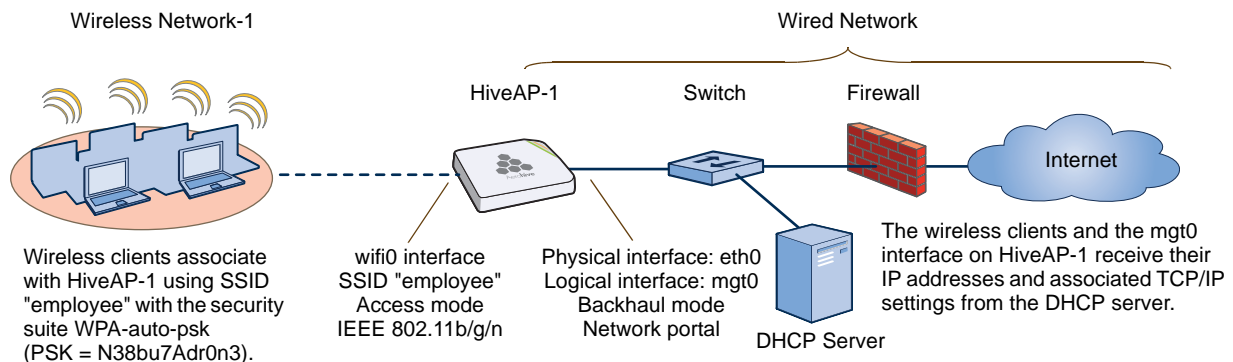
In this example, you deploy one HiveAP (HiveAP-1) to provide network access to a small office with 15 - 20 wireless clients. You only need to define the following SSID (service set identifier) parameters on the HiveAP and clients:

- 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 HiveAP
 - 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 HiveAP both already have
- Preshared key: N38bu7Adr0n3

After defining SSID "employee" on HiveAP-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.

Note: 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 HiveAP 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 HiveAP to the AC/DC power adaptor that ships with the device as an option, and connect that to a 100 - 240-volt power source.

Note: If the switch supports PoE (Power over Ethernet), the HiveAP 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 HiveAP.

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 HiveAPs set with "FCC" as the region code, the Initial CLI Configuration Wizard appears. For HiveAPs set with "world" as the region code, a prompt appears to set the country code for the location where you intend to deploy the HiveAP. 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 ["Appendix A Country Codes" on page 213](#).

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 HiveAP

1. Create an SSID and assign it to an interface.

```
ssid employee
```

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

You first create an SSID named "employee" and then define its protocol suite and preshared key (N38bu7Adr0n3) in standard ASCII (American Standard Code for Information Interchange) text.

```
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 HiveAP 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 HiveAP 300 series supports up to eight per interface for a possible maximum total of 16.) A HiveAP 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 HiveAPs when in a hive (see subsequent examples).

2. (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.

*Note: 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.)*

3. (Optional) Change the host name of the HiveAP.

```
hostname HiveAP-1
```

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

```
save config
```

```
exit
```

The HiveAP 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 HiveAP

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

When you power on the HiveAP, 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

1. To check that a client can associate with the HiveAP 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.
2. Log in to the HiveAP 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.

Note: 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 HiveAP is complete. Wireless clients can now associate with the HiveAP using SSID "employee" and access the network.

EXAMPLE 2: DEPLOYING A HIVE

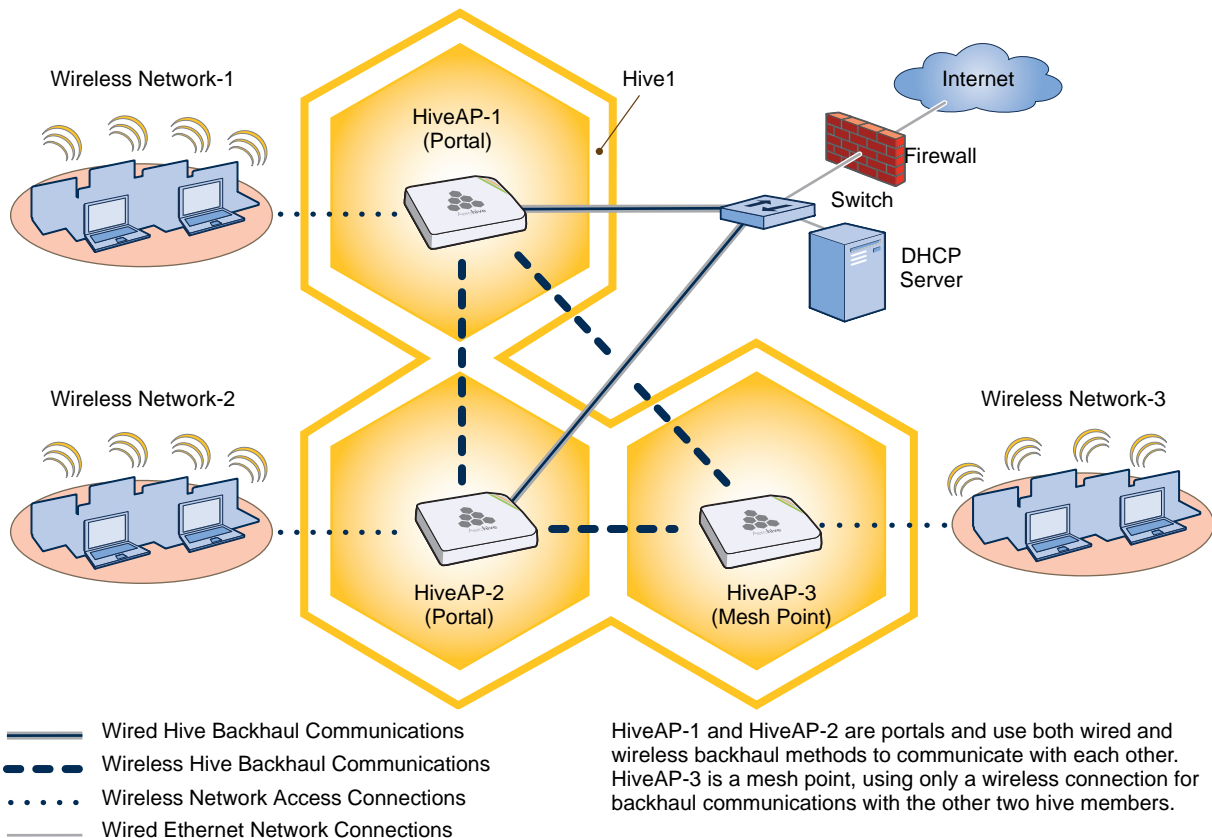
Building on "Deploying a Single HiveAP" on page 182, the office network has expanded and requires more HiveAPs to provide greater coverage. In addition to the basic configuration covered in the previous example, you configure all three HiveAPs to form a hive within the same layer 2 switched network. The following are the configuration details for the hive:

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

Note: The security protocol suite for hive communications is WPA-AES-psk.

HiveAP-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, HiveAP-3 only communicates with HiveAP-1 and -2 over a wireless link (see Figure 2). Because HiveAP-1 and -2 connect to the wired network, they act as portals. In contrast, HiveAP-3 is a mesh point.

Figure 2 Three HiveAPs in a hive



Note: 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 HiveAP-1

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

```
hive hive1
```

You create a hive, which is a set of HiveAPs 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 HiveAP-1 to the hive.

```
save config
```

- Before closing the console session, check the radio channel that HiveAP-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 HiveAP 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.

HiveAP-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 HiveAP-2 and -3, make sure that they also use this channel for backhaul communications.

```
exit
```

Step 2 Configure HiveAP-2 and HiveAP-3

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

```
ssid employee
ssid employee security protocol-suite wpa-auto-psk ascii-key N38bu7Adr0n3
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 HiveAP-2 uses the same channel as HiveAP-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 HiveAP-3.

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

1. Place HiveAP-2 within range of its clients and within range of HiveAP-1. This allows HiveAP-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 HiveAP-2 to the network switch.
3. Power on HiveAP-2 by connecting it to a power source.

After HiveAP-2 finishes booting up (indicated when the Power LED changes from steady amber to steady green), it automatically discovers another member of hive1 (HiveAP-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 HiveAP-3 within range of its wireless clients and one or both of the other hive members.
5. Power on HiveAP-3 by connecting it to a power source.

After HiveAP-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. HiveAP-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—HiveAP-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 mgt0 interface.

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

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

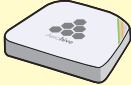
```

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 Phymode 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

HiveAP-1



wifi1.1 MAC Address
0019:7700:0028

HiveAP-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 HiveAPs 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 HiveAP-3 learned them over a wireless backhaul link.

The following are the various hive states that can appear:

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

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

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


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

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

Auth (Authenticated) - The HiveAP 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 HiveAP-1 (the SSID "employee" is already defined on clients in wireless network-1; see "Deploying a Single HiveAP"). Then check if HiveAP-1 forwards the client's MAC address to the others to store in their roaming caches.

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



HiveAP-1

```

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
    
```

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

Note: On HiveAPs 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 HiveAP sends an RTS frame), or "disabled" (always use spatial streams for 11n clients).

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



HiveAP-2

```

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 HiveAP: 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
    
```

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

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



MATCH!

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

Repeat this to confirm that HiveAP-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 HiveAPs using SSID "employee" and access the network. The HiveAPs communicate with each other to share client associations (to support fast roaming) and routing data (to select optimal data paths).

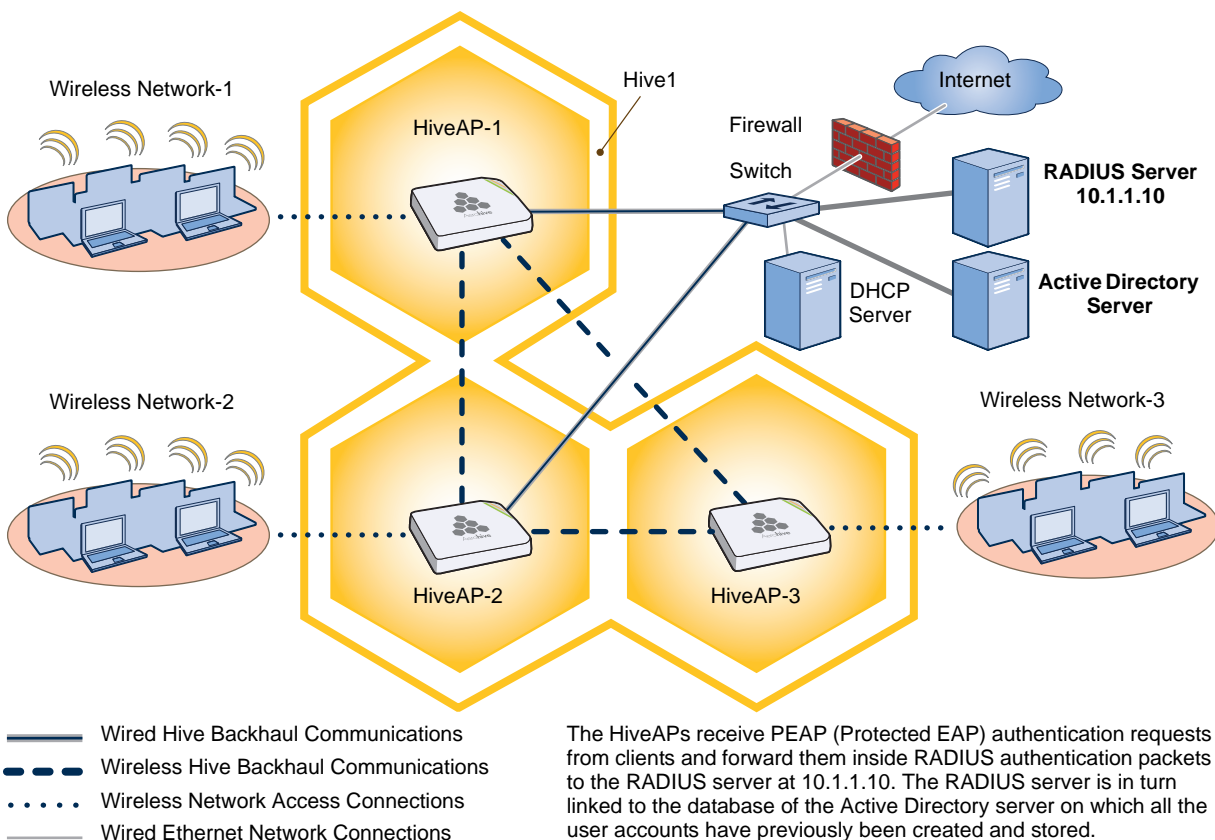
EXAMPLE 3: USING IEEE 802.1X AUTHENTICATION

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 HiveAPs
- Change the SSID parameters on the HiveAPs and wireless clients to use IEEE 802.1X

The basic network design is shown in [Figure 3](#).

Figure 3 Hive and 802.1X authentication



Note: 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 HiveAPs.

Step 1 Define the RADIUS server on the HiveAP-1

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

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

The IP address of the RADIUS server is 10.1.1.10, and the shared secret that HiveAP-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 HiveAPs as access devices (see step 4).

Step 2 Change the SSID on HiveAP-1

1. Change the authentication method in the SSID.

```
ssid 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 HiveAP-1 as an access device on the RADIUS server in step 4.
- ```
exit
```

---

### Step 3 Configure HiveAP-2 and HiveAP-3

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

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

---

*Note: Although all HiveAPs 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 HiveAP-3 and enter the same commands.

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

Log in to the RADIUS server and define the three HiveAPs 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.

Note: 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.

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

1. To check that a client can associate with a HiveAP 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.
2. Log in to the HiveAP 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.

Note: 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 HiveAP 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 195](#) 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 HiveAPs that do not support the IEEE 802.11n standard and 50,000 Kbps on HiveAPs that do. However, you do not set the maximum rate (54,000 or 1,000,000 Kbps, depending on the HiveAP 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).

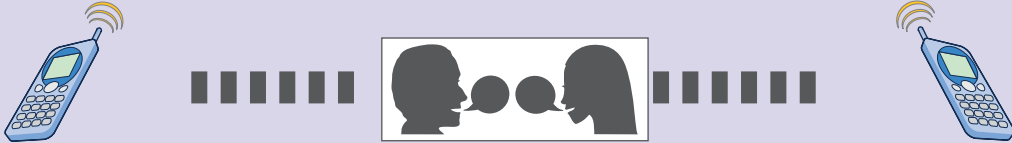
Maximum traffic rate for all class 3 traffic: 54,000 or 1,000,000 Kbps (the default, depending on the HiveAP)

Note: The HiveAP 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 HiveAP.

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

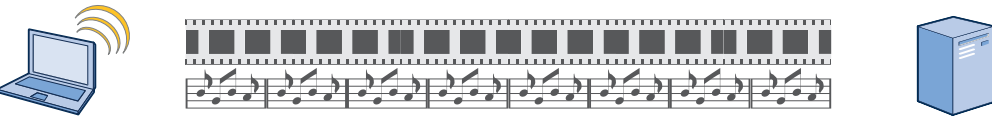
QoS Policy: "voice"

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.

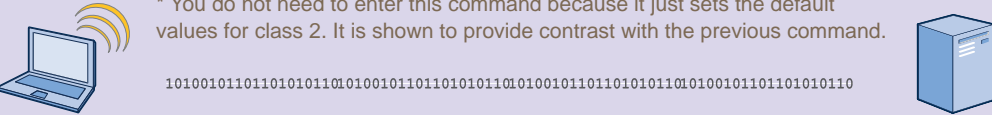
Streaming Media `qos policy voice qos 5 wrr 20000 90`



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.



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.

Note: 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 HiveAPs.

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 HiveAP-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 HiveAP-1 receives traffic from a client whose source MAC address contains this OUI, it assigns it to Aerohive class 6.

2. Define the custom services that you need.

```
service mms tcp 1755
```

```
service smtp tcp 25
```

```
service pop3 tcp 110
```

The MMS (Microsoft Media Server) protocol can use several transports (UDP, TCP, and HTTP). However, for a HiveAP 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 a HiveAP can use to map the service to an Aerohive class.

Therefore, you define a custom service for MMS using TCP port 1755. You also define custom services for SMTP and POP3 so that you can map them to Aerohive class 3. By doing so, you can prioritize e-mail traffic above other types of traffic that the HiveAP assigns to class 2 by default.

3. Map services to Aerohive classes.

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

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

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

Unless you map a specific service to an Aerohive QoS class, a HiveAP maps all traffic to class 2. 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 HiveAP-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 HiveAP-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.

- Associate the classifier profiles with the employee SSID and the eth0 interface so that HiveAP-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, HiveAP-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.

Note: 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 HiveAP-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 HiveAP-1

- Create a QoS policy.

For HiveAPs supporting IEEE 802.11a/b/g:

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

For HiveAPs 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 HiveAPs supporting 802.11a/b/g data rates. For HiveAPs 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 HiveAP 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 HiveAP 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 HiveAP 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 HiveAP 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 HiveAP 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 HiveAPs that support 802.11n data rates. For other HiveAPs, 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 HiveAP 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 HiveAP queues for class 2, it queues approximately 60 bits for class 3, and 90 bits for class 5. These amounts are approximations because the HiveAP 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 200).

Note: When HiveAP-1 does not use RADIUS for user 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 HiveAP-2 and HiveAP-3

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

```
qos classifier-map oui 00:12:3b qos 6
service mms tcp 1755
service smtp tcp 25
service pop3 tcp 110
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 HiveAPs supporting IEEE 802.11a/b/g:

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

For HiveAPs 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 HiveAP-3 and enter the same commands.

Step 5 Configure RADIUS server attributes

1. Log in to the RADIUS server and define the three HiveAPs 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 HiveAP 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 HiveAP 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 177](#), a bootstrap config file is typically a small set of commands to which a HiveAP can revert when the configuration is reset or if the HiveAP cannot load its current and backup configs. If you do not define and load a bootstrap config, the HiveAP 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 a HiveAP acting as a mesh point in a hard-to-reach location—such as a ceiling crawlspace—the HiveAP 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 HiveAP.
- If the location of a HiveAP 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 HiveAP 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.

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

Step 1 Define the bootstrap config on HiveAP-1

1. Make a serial connection to the console port on HiveAP-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.

Note: 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 HiveAP-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 HiveAPs 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 HiveAPs using the bootstrap config can rejoin the grid.

```
hive hive1
```

```
hive hive1 password slr70ckH07m3s
```

```
interface mgt0 hive hive1
```

When a HiveAP 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 HiveAP-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, HiveAP-1 or HiveAP-2.

7. Save the configuration as a bootstrap config.

```
save config running bootstrap
```

If anyone resets the current configuration, the HiveAP 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 HiveAP-1 finishes rebooting, log back in using the login parameters you set in ["Example 1: Deploying a Single HiveAP" on page 182](#) (*mwebster, 3fF8ha*).
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 HiveAP addresses.

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

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

1. Make a serial connection to the console port on HiveAP-2 and log in.
2. Upload the bootstrap-hive1.txt config file from the TFTP server to HiveAP-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 HiveAP-3.

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

CLI COMMANDS FOR EXAMPLES

This section includes all the CLI commands for configuring the HiveAPs 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 HiveAPs in each example and paste them at the command prompt.

Note: The following sections omit optional commands, such as changing the login name and password, and commands used to check a configuration.

Commands for Example 1

Enter the following commands to configure the SSID "employee" on the single HiveAP in ["Deploying a Single HiveAP" on page 182](#):

```
ssid employee
ssid employee security protocol-suite wpa-auto-psk ascii-key N38bu7Adr0n3
interface wifi0.1 ssid employee
save config
```

Commands for Example 2

Enter the following commands to configure three HiveAPs as members of "hive1" in ["Deploying a Hive" on page 185](#):

HiveAP-1

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

HiveAP-2

```
ssid employee
ssid employee security protocol-suite wpa-auto-psk ascii-key N38bu7Adr0n3
interface wifi0.1 ssid employee
hive hive1
hive hive1 password slr70ckH07m3s
interface mgt0 hive hive1
save config
```


HiveAP-3

```
ssid employee
ssid employee security protocol-suite wpa-auto-psk ascii-key N38bu7Adr0n3
interface wifi0.1 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 190](#):

HiveAP-1

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

HiveAP-2

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

HiveAP-3

```
aaa radius-server 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 194](#):

HiveAP-1

```
qos classifier-map oui 00:12:3b qos 6
service mms tcp 1755
service smtp tcp 25
service pop3 tcp 110
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 HiveAPs supporting IEEE 802.11a/b/g

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

For HiveAPs 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
```

HiveAP-2

```
qos classifier-map oui 00:12:3b qos 6
service mms tcp 1755
service smtp tcp 25
service pop3 tcp 110
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 HiveAPs supporting IEEE 802.11a/b/g

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

For HiveAPs 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
```

HiveAP-3

```
qos classifier-map oui 00:12:3b qos 6
service mms tcp 1755
service smtp tcp 25
service pop3 tcp 110
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 HiveAPs supporting IEEE 802.11a/b/g

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

For HiveAPs 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 200](#):

bootstrap-security.txt

```
admin root-admin Cwb12o11siNI8vhD2hs password 8wDamKC1Lo53Ku71
hive hive1
hive hive1 password slr70ckH07m3s
interface mgt0 hive hive1
```

HiveAP-1

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

HiveAP-2

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

HiveAP-3

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


Chapter 15 Traffic Types

This is a list of all the types of traffic that might be involved with a HiveAP and HiveManager 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 Wireless Clients

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
Active Directory	HiveAP RADIUS server mgt0 interface	Active Directory domain controller or global catalog server	6 TCP	1024-65535	139, and 445 or 3268	Required for a HiveAP RADIUS server to contact a domain controller on port 445 or a global catalog server on port 3268
			17 UDP	1024-65535	389	
DHCP	unregistered wireless client	HiveAP wifi subinterface in access mode	17 UDP	68	67	Required for captive web portal functionality
DNS	unregistered wireless client	HiveAP wifi subinterface in access mode	17 UDP	53, or 1024 - 65535	53	Required for captive web portal functionality
GRE	HiveAP mgt0 interface	HiveAP mgt0 interface	47 GRE	N.A.	N.A.	Required to support DNX* and layer 3 roaming between members of different hives
HTTP	unregistered wireless client	HiveAP wifi subinterface in access mode	6 TCP	1024 - 65535	80	Required for captive web portal functionality
HTTPS	unregistered wireless client	HiveAP wifi subinterface in access mode	6 TCP	1024 - 65535	443	Required for captive web portal functionality using a server key
IKE	HiveAP VPN client mgt0 interface	HiveAP VPN server mgt0 interface	17 UDP	500 and 4500 for NAT-Traversal	500 and 4500 for NAT-Traversal	Required for HiveAP VPN clients to connect to HiveAP VPN servers
IPsec ESP	HiveAP VPN client or server mgt0 interface	HiveAP VPN server or client mgt0 interface	50 ESP	N.A.	N.A.	Required for IPsec VPN traffic to flow between HiveAP VPN clients and servers
IPsec ESP with NAT-Traversal enabled	HiveAP VPN client or server mgt0 interface	HiveAP VPN server or client mgt0 interface	17 UDP	4500	4500	Required for VPN traffic to flow when a NAT device is detected inline

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
LDAP	HiveAP RADIUS server mgt0 interface	OpenLDAP server	6 TCP	1024-65535	389	Required for a HiveAP RADIUS server to contact an OpenLDAP server
LDAPS	HiveAP RADIUS server mgt0 interface	OpenLDAP server	6 TCP	1024-65535	636	Required for a HiveAP RADIUS server to make an encrypted connection to an OpenLDAP server
RADIUS accounting	HiveAP mgt0 interface	RADIUS server	17 UDP	1024 - 65535	1813 [†]	Required to support RADIUS accounting
RADIUS authentication	HiveAP mgt0 interface	RADIUS server	17 UDP	1024 - 65535	1812 [†]	Required for 802.1X authentication of users

* DNX = dynamic network extensions

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

Traffic Supporting Management of HiveAPs

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
CAPWAP*	HiveAP mgt0 interface	HiveManager	17 UDP	12222	12222	Required for HiveAPs to discover the HiveManager and send it alarms, events, reports, and traps
Distributed HiveOS image download	HiveAP mgt0 interface	HiveAP mgt0 interface	6 TCP	1024-65535	3007	Required for downloading a HiveOS image from HiveManager to one HiveAP and from there to all others
Iperf	mgt0 interface on Iperf client	mgt0 interface on Iperf server	6 TCP	1024-65535	5001 [†]	Required for performing diagnostic testing of network performance
NTP	HiveAP mgt0 interface	HiveManager	17 UDP	1024 - 65535	123	Required for HiveAP time synchronization with HiveManager
Remote Sniffer	Admin workstation	HiveAP mgt0 interface	6 TCP	1024 - 65535	2002 [†]	Used when capturing packets on HiveAP interfaces
SNMP	SNMP managers	HiveAP mgt0 interface	17 UDP	1024 - 65535	161	Required for SNMP managers to contact HiveAPs
SNMP traps	HiveAP mgt0 interface	SNMP managers	17 UDP	1024 - 65535	162	Required for sending SNMP traps to configured SNMP managers
SSHv2	HiveAP mgt0 interface	HiveManager	6 TCP	1024 - 65535	22	Required for the HiveManager to upload files to HiveAPs
TFTP	HiveAP mgt0 interface	HiveManager	17 UDP	1024 - 65535	69	Used for uploading packet capture files from HiveAPs to HiveManager

* Control and Provisioning of Wireless Access Points

† 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	HiveAP mgt0 interface	HiveAP mgt0 interface	17 UDP	3000*	3000*	Required for hive communications and operates at layer 3
Aerohive Cooperative Control Messages	HiveAP wifi1.1 or eth0 interface	HiveAP wifi1.1 or eth0 interface	N.A.	N.A.	N.A.	Required for hive communications and operates at the LLC (Logical Link Control) sublayer of layer 2
AeroScout Reports	AeroScout engine	HiveAP mgt0 interface	17 UDP	1024 - 65535	1144	Required to report tracked devices to an AeroScout engine
DHCP	HiveAP mgt0 interface	DHCP server	17 UDP	68	67	By default, a HiveAP gets its IP address through DHCP.
Ekahau	Ekahau Positioning Engine (EPE)	HiveAP mgt0 interface	17 UDP	1024 - 65535	8552, 8553, 8554	Required for HiveAPs to communicate with EPE
HTTP	management system	HiveManager MGT port	6 TCP	1024 - 65535	80	Redirected to HTTPS (8443) when accessing the HiveManager GUI; redirected to HTTPS (443) when accessing the HiveManager Online GUI or GuestManager GUI; used for uploading image files for maps to HiveManager Online
HTTP	management system	HiveManager MGT port	6 TCP	1024 - 65535	8080	Redirected to HTTPS (8443) when accessing the HiveManager GUI; used for uploading image files for maps to HiveManager
HTTPS	management system	HiveManager MGT port	6 TCP	1024 - 65535	443	Redirected to HTTPS (8443) when accessing the HiveManager GUI and loading image files for captive web portals (CWPs) to HiveManager; used for accessing the HiveManager Online GUI and uploading CWP image files to HiveManager Online
HTTPS	management system	HiveManager MGT port	6 TCP	1024 - 65535	8443	Used when accessing the HiveManager GUI and uploading CWP image files to HiveManager
NTP	HiveAP mgt0 interface or HiveManager MGT port	NTP server	6 TCP	1024 - 65535	123	Required for time synchronization with an NTP server
SMTP	HiveManager MGT port	SMTP server	6 TCP	1024 - 65535	25	Required for the HiveManager to send e-mail alerts to administrators
SSHv2	management system	HiveAP mgt0 interface or HiveManager MGT port	6 TCP	1024 - 65535	22	Used for secure network access to the HiveAP or HiveManager CLI, and (SCP) for uploading files to and downloading files from HiveAPs
syslog	HiveAP mgt0 interface	syslog server	17 UDP	1024 - 65535	514	Required for remote logging to a syslog server

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
Telnet	management system	HiveAP mgt0 interface	6 TCP, 17 UDP	1024 - 65535	23	Used for unsecured network access to the HiveAP CLI
TFTP	TFTP server or mgt0	HiveAP mgt0 or TFTP server	17 UDP	1024 - 65535	69	Used for uploading files to HiveAPs and downloading files from them

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

Appendix A Country Codes

When the region code on a HiveAP is preset as "world", you must set a country code for the location where you intend to deploy the HiveAP. This code determines the radio channels and power settings that the HiveAP can use when deployed in that country. For HiveAPs intended for use in the United States, the region code is preset as "FCC"—for "Federal Communications Commission"—and the country code is preset for the United States. You can see the region code in the output of the `show boot-param` command.

To set a country code when the region is "world", enter the following command, in which *number* is the appropriate country code number: `boot-param country-code number`

Note: Be sure to enter the correct country code. An incorrect entry might result in illegal radio operation and cause harmful interference to other systems.

To apply radio settings for the updated country code, reboot the HiveAP by entering the `reboot` command.

To see a list of the available channels available for the country code that you have set on the HiveAP, enter the following command: `show interface { wifi0 | wifi1 } channel`. For example, the output for the `show interface wifi0 channel` command on a HiveAP whose region code is FCC and country code is 840 (United States) shows that channels 1 through 11 are available. If a channel does not appear in this list, you cannot configure the radio to use it.

The following list of country codes is provided for your convenience.

Countries and Country Codes

Albania 8	Brunei Darussalam 96
Algeria 12	Bulgaria 100
Argentina 32	Canada 124
Armenia 51	Chile 152
Australia 36	China (People's Republic of China) 156
Austria 40	Colombia 170
Azerbaijan 31	Costa Rica 188
Bahrain 48	Croatia 191
Belarus 112	Cyprus 196
Belgium 56	Czech Republic 203
Belize 84	Denmark 208
Bolivia 68	Dominican Republic 214
Bosnia and Herzegovina 70	Ecuador 218
Brazil 76	Egypt 818

Appendix A Country Codes

El Salvador 222	Japan14 (J14) 4014
Estonia 233	Japan15 (J15) 4015
Faeroe Islands 234	Japan16 (J16) 4016
Finland 246	Japan17 (J17) 4017
France 250	Japan18 (J18) 4018
France2 255	Japan19 (J19) 4019
Georgia 268	Japan20 (J20) 4020
Germany 276	Japan21 (J21) 4021
Greece 300	Japan22 (J22) 4022
Guatemala 320	Japan23 (J23) 4023
Honduras 340	Japan24 (J24) 4024
Hong Kong (S.A.R., P.R.C) 344	Jordan 400
Hungary 348	Kazakhstan 398
Iceland 352	Kenya 404
India 356	Korea (North Korea) 408
Indonesia 360	Korea (South Korea, ROC) 410
Iran 364	Korea (South Korea, ROC2) 411
Iraq 368	Korea (South Korea, ROC3) 412
Ireland 372	Kuwait 414
Israel 376	Latvia 428
Italy 380	Lebanon 422
Jamaica 388	Libya 434
Japan 392	Liechtenstein 438
Japan1 (JP1) 393	Lithuania 440
Japan2 (JP0) 394	Luxembourg 442
Japan3 (JP1-1) 395	Macao 446
Japan4 (JE1) 396	Macedonia (The Former Yugoslav Republic of Macedonia) 807
Japan5 (JE2) 397	Malaysia 458
Japan6 (JP6) 399	Malta 470
Japan7 (J7) 4007	Mauritius 480
Japan8 (J8) 4008	Mexico 484
Japan9 (J9) 4009	Monaco (Principality of Monaco) 492
Japan10 (J10) 4010	Morocco 504
Japan11 (J11) 4011	Netherlands 528
Japan12 (J12) 4012	New Zealand 554
Japan13 (J13) 4013	

Nicaragua 558	Sri Lanka 144
Norway 578	Sweden 752
Oman 512	Switzerland 756
Pakistan (Islamic Republic of Pakistan) 586	Syria 760
Panama 591	Taiwan 158
Paraguay 600	Thailand 764
Peru 604	Trinidad y Tobago 780
Philippines (Republic of the Philippines) 608	Tunisia 788
Poland 616	Turkey 792
Portugal 620	U.A.E. 784
Puerto Rico 630	Ukraine 804
Qatar 634	United Kingdom 826
Romania 642	United States 840
Russia 643	United States (Public Safety; FCC49) 842
Saudi Arabia 682	Uruguay 858
Singapore 702	Uzbekistan 860
Slovakia (Slovak Republic) 703	Venezuela 862
Slovenia 705	Vietnam 704
South Africa 710	Yemen 887
Spain 724	Zimbabwe 716

Index

A

- access points
 - associated costs 18
 - autonomous access points 173
 - fat access points 14
 - thin access points 14
- admin
 - bootstrap login credentials 201
 - login credentials, changing 183
 - lost credentials, one-time login key 179
- Aerohive Cooperative Control Messages 211
- AeroScout Reports 211
- aggregate interface 53
- antennas
 - omnidirectional 19
 - See also individual platform entries

B

- bootstrap config 177, 179-180, 200-202
 - defining 201
 - login credentials, changing (CLI) 201
 - saving to a TFTP server 202
 - uploading from a TFTP server 202

C

- CAC (Call Admission Control) 162
- captive web portal 151-164
 - authentication 151
 - creating 158
 - defined 151
 - exporting default files 157
 - external DHCP and DNS servers 152-153
 - importing files 157
 - internal DHCP and DNS servers 154-155
 - login page, modifying 157
 - modifying web pages 155-157
 - removing web directories 164
 - result page, modifying 157
 - self-registration 151
 - testing 164
- CAPWAP 118
 - CAPWAP traffic 210
 - checking status 132
 - states 130
- channels, layout pattern 25
- classifier tags, See HiveManager
- CLI
 - admin system requirements 181
 - admins, creating 175
 - common commands 174
 - default user profile 174
 - disabling the reset button 179
 - layer 2 and 3 forwarding 175
 - logging 175
 - QoS settings 176
 - radio profiles 174

- resetting the configuration 29, 51, 73, 83, 179
 - updating HiveAP country codes 183
 - uploading a configuration file 179
 - user profiles 176
- clock synchronization 118
- configuration file types
 - backup 177, 178
 - bootstrap 177, 179-180, 200-202
 - bootstrap config, defining 201
 - current 177, 178
 - default 177, 179
 - failed 177, 178
- console, See individual platform entries
- cooperative control 107
- country codes
 - list of country codes 213
 - updating through HiveManager 136
 - updating through the CLI 183
- custom services, creating 159

D

- default login credentials
 - HiveAP 183
 - HiveManager 111
- DHCP 209, 211
- DNS 209

E

- EC conformance declaration 3
- Ekahau 211

F

- FCC compliance 2
- firewall
 - policy rules 159-161, 166
 - stateful 21

G

- GRE 209
- GuestManager 156, 211

H

- hive 127
 - backhaul communications 187
 - checking member connectivity 189
 - defined 173
 - deploying 185-190
 - member communications 185
 - neighbor states 131, 188
 - password 186
 - secured communications 127
- HiveAP 100 series 81-88
 - antennas 84, 88
 - environmental specifications 88
 - Ethernet port 83, 88
 - locking 82, 87

- mounting 85-87
- mounting, surface 87
- PoE 83, 88
- power connector 83
- power specifications 88
- radios 84
- reset button 83
- status indicator 82, 84
- HiveAP 20 ag 27-35
 - antennas 28, 32, 35
 - console 29, 31, 35
 - environmental specifications 35
 - Ethernet port 30, 35
 - LEDs 28, 31
 - locking 29
 - mounting 29
 - mounting, ceiling 33
 - mounting, surface 34
 - PoE 29, 30, 35
 - power connector 29
 - power specifications 35
 - radios 32
 - reset button 29
- HiveAP 28 37-48
 - antennas 38, 41, 48
 - antennas, mounting 46
 - environmental specifications 48
 - Ethernet port 39, 48
 - mounting 42-45
 - mounting, pole 43
 - mounting, strand 44
 - mounting, surface 45
 - PoE 39, 48
 - power connector 38, 40
 - power specifications 48
 - radios 41
- HiveAP 320 71-79
 - antennas 75, 79
 - console 73, 74
 - environmental specifications 79
 - Ethernet ports 72, 74, 79
 - LEDs 72, 74
 - locking 73, 77
 - mounting 76-78
 - mounting, ceiling 76
 - mounting, surface 78
 - PoE 72, 74, 79
 - power connector 73
 - power specifications 79
 - radios 75
 - reset button 73
- HiveAP 340 49-69
 - antennas 50, 56, 69
 - console 51, 55
 - environmental specifications 69
 - Ethernet ports 51, 52, 53
 - LEDs 50, 56
 - locking 62
 - mounting 60-68
 - mounting, ceiling 61
 - PoE 51, 52
 - power connector 51
 - power specifications 69
 - radios 58
 - reset button 51
- HiveAPs as RADIUS authenticators 147
- HiveManager
 - accepting HiveAPs for management 131
 - changing HiveAP login credentials 135
 - classifier tags 146, 170-172
 - CLI shell 109
 - cloning configuration objects 116
 - complete configuration uploads 137
 - configuration workflow 118
 - connecting HiveAPs to HiveManager 129, 133
 - console 90, 92, 94, 109
 - default IP addresses 109
 - default login credentials 111
 - delta configuration uploads 137
 - device-level configuration objects 118
 - environmental specifications 94
 - Ethernet ports 91, 109-110
 - GUI 113-117
 - GUI requirements 109
 - HiveAP classifiers 170-172
 - HiveAP Update Results 164, 169, 172
 - installing 109
 - LAN port 91, 109-110
 - LEDs 91, 92
 - license key 111
 - linking HiveAPs to maps by MAC address 144
 - linking HiveAPs to maps through SNMP 144
 - logging in to the GUI 111
 - maps 140-145
 - maps, arranging and modifying 142
 - maps, uploading 141
 - MGT port 91, 109-110
 - multiselecting configuration objects 116
 - order ID 111
 - policy-level configuration objects 118
 - power fan 91
 - rack mounting 93
 - recovering the IP address 111
 - relationship of configuration objects 118
 - search tool 115
 - serial number 91
 - software updates 119
 - sorting data 117
 - synchronize clocks 118
 - system fans 91
 - troubleshooting HiveAP connectivity issues 131
 - updating HiveAP country codes 136
 - uploading a configuration 164, 169
 - uploading files 164
 - uploading HiveAP configurations 137
 - uploading users 169
- HiveManager Online 105-106, 133
- HiveManager Virtual Appliance 105-106, 133
- HiveManager, High Capacity
 - console 97, 103
 - environmental specifications 103
 - Ethernet ports 97

- hard disk drives 96, 102
- LEDs 97
- power supplies 97
- power supplies, replacing 101
- rack mounting 96, 98-100
- reset button 97
- serial number 97
- system fans 97
- HiveOS
 - backup config 177, 178
 - bootstrap config 177, 179-180, 200-202
 - bootstrap config, defining 201
 - bootstrap login credentials 201
 - changing login credentials 183
 - common CLI commands 174
 - configuration file types 177-180
 - current config 177, 178
 - default config 177, 179
 - default login credentials 183
 - default settings 174
 - device-level configurations 175
 - failed config 177, 178
 - firmware updates 120
 - policy-level configurations 176
- HTTP 209
- HTTPS 209, 211
- I**
- IEEE 802.1X 145, 149
 - returned RADIUS attributes 161
 - SSID (CLI) 190-193
 - supplicants 150, 192
- Industry Canada compliance 2
- interfaces
 - aggregate 53
 - default states 201
 - redundant 54
- IP address objects, creating 159
- L**
- LEDs, See individual platform entries
- login credentials
 - changing (CLI) 183
 - default (HiveAP) 183
 - default (HiveManager) 111
 - if lost, one-time login key 179
- M**
- maps, See HiveManager maps
- mesh points 121, 129, 137, 200
- MIMO (Multiple In, Multiple Out) 57
- multipath 26
- N**
- NTP 118, 210, 211
- P**
- PoE 129
 - smart PoE 53
- portals 121, 129, 137
- private PSK 165-169
 - groups of users 165
 - overview 165
 - SSID 168
 - user groups 167
 - user profiles 166
- PSK 124
- Q**
- QoS
 - applying QoS (CLI) 194-200
 - classifier maps 196
 - classifier profiles 196
 - data traffic 194
 - policing rate limit 162
 - rate limiting 158
 - scheduling weight 162
 - streaming media 194
 - strict forwarding 194
 - voice traffic 194
 - WRR (weighted round robin) 194
- R**
- radio profiles 174
- radios
 - access 125, 182
 - backhaul 125, 182
 - broadcasting SSIDs 125
 - channel layout pattern 25
 - power 23
 - See also individual HiveAP entries
 - signal strength and throughput 23
- RADIUS authentication 21, 145
 - accounting 147
 - accounting interim update interval 148
 - accounting traffic 210
 - authentication port 148
 - authentication traffic 210
 - RADIUS authenticators 147, 191
 - retry interval 148
 - returned RADIUS attributes 161, 200
 - RFC 3576 148
 - server connectivity settings 147
 - server connectivity settings (CLI) 191
 - server priority 148
 - shared secret 147
 - supplicants 150, 192
 - use only selected user profiles 149
- reboot, HiveAPs 29, 51, 73, 83
- redundant interfaces 54
- region codes 213
- reset button, disabling 179, 200
- reset config 29, 51, 73, 83, 179
- RFC 3576 148
- RoHS compliance 3
- routes, default route selection 54
- S**
- serial port, See individual platform entries
- signal-to-noise 24
- site surveys 16

Index

- smart PoE 53
- SMTP 211
- SNMP 210
- SNMP traps 210
- SSHv2 210, 211
- SSID 124
 - 802.1X 145, 149, 190-193
 - 802.1X, testing 193
 - binding to an interface 183
 - captive web portal 163
 - client configuration (PSK) 190
 - creating with a PSK 183
 - private PSK 168
 - radios and rates 149
 - SSID names 124
 - SSID profiles 124
 - testing 184
 - user profiles 161
- status LEDs, See individual platform entries
- syslog 211
- T**
- Telnet 212
- TFTP 210, 212
- traffic types 209-212
- troubleshooting, HiveAP-HiveManager connectivity 131
- Turbo Mode 3
- U**
- updates
 - activation 121, 137, 179
 - HiveManager software 119
 - HiveOS firmware 120
 - portals and meshpoints 121
 - recommended sequence 120
- user groups
 - attribute number 167
 - manually created private PSK users 167
 - reauth time 167
 - VLAN ID 167
- User Manager 156, 161
- user profiles
 - attribute number 146, 161
 - creating 161
 - default user profile 174
- V**
- VLAN 21, 146
 - classified VLAN object definitions (HiveManager) 171
 - default VLAN 174
 - mgt0 interface (CLI) 175
 - native VLAN 174
 - user profiles (CLI) 175
- W**
- WEEE compliance 3
- Wi-Fi certification 3
- WLAN deployment
 - access point density 19
 - bandwidth 18
 - connecting HiveAPs to HiveManager 129
 - considering interference 15, 25
 - data rates 19
 - determining requirements 14
 - fine tuning 22
 - new, or greenfield 15
 - noise 25
 - noise floor 23
 - open space 19
 - single HiveAP 182-184
 - site surveys 16
 - troubleshooting 22
 - upgrading existing Wi-Fi 14
 - warehouse and retail 19
- WLAN policy
 - assigning a WLAN policy to HiveAPs 135, 164, 169
 - defined 128
 - QoS settings 162
 - SSID, adding 164