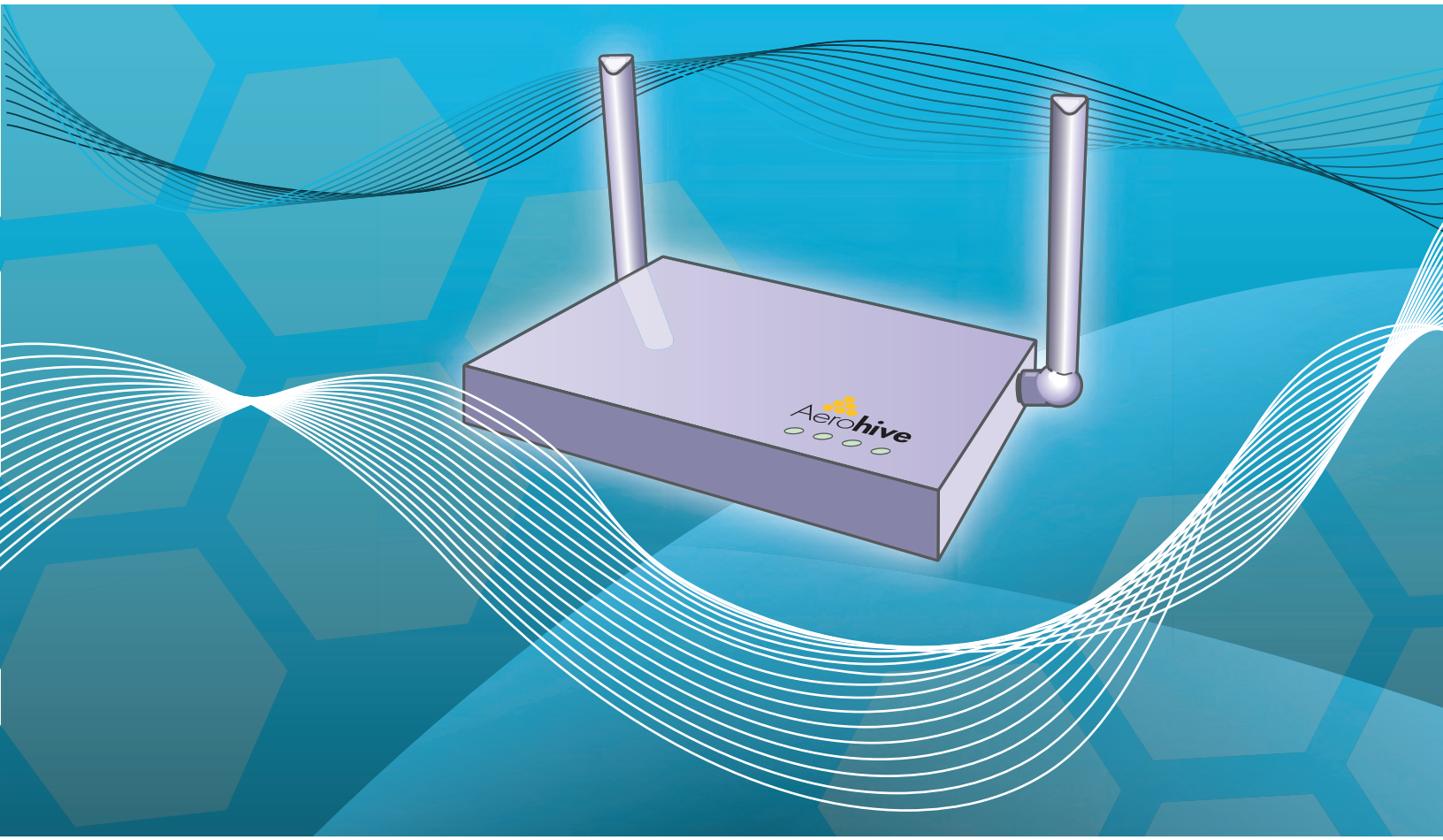
Aerohive Deployment Guide



Aerohive™

Aerohive Deployment Guide

For HiveAP and HiveManager Devices

Aerohive Technical Publications

P/N 330002-05, Rev. A

HiveAP Compliance Information

Federal Communication Commission Interference Statement

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.

Important: FCC Radiation Exposure Statement

This equipment complies with FCC 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.

Wireless 5 GHz Band Statements

High power radars are allocated as primary users (meaning they have priority) of the 5250-5350 MHz and 5650-5850 MHz bands. These radars could cause interference and/or damage to the HiveAP when used in Canada.

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

Industry Canada - 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.

Wi-Fi Certification

The Wi-Fi CERTIFIED™ Logo is a certification mark of the Wi-Fi Alliance®. The Aerohive HiveAP 20 ag has been certified for WPA™, WPA2™, WMM® (Wi-Fi Multimedia™), WMM Power Save, and the following types of EAP (Extensible Authentication Protocol):

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

EC Conformance Declaration

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

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 of operation in the command line interface as described in "Appendix A Country Codes" on page 157.
- 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, you must apply for a license from the national spectrum authority to operate a HiveAP outdoors.
  - In Belgium outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.
  - In France outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7.
- HiveAPs are restricted to indoor use when operated in the European Community using the 5.15 - 5.25 GHz band: Channels 36, 40, 44, 48. Because the frequency ranges 5.25 – 5.35 and 5.47 – 5.725 are affected by DFS (Dynamic Frequency Selection), HiveAPs block channels 52, 56, 60, 64, and 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.
- 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** > **Network Objects**> **Radio Profiles >** *profile* **> Advanced**. 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, Edgecore, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	Valmistaja Edgecore 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 Edgecore 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 Edgecore dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French	Par la présente Edgecore 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 Edgecore 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 Edgecore erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
German	Hiermit erklärt Edgecore, 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". (BMWi) Hiermit erklärt Edgecore 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 παρουσα Edgecore δηλωνει οτι radio LAN device συμμορφωνεται προσ τισ ουσιωδεισ απαιτησεισ και τισ λοιπεσ σΧετικεσ διαταξεισ τησ οδηγιασ 1999/5/εκ
Italian	Con la presente Edgecore 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 Manufacturer 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	Manufacturer 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
	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.
Denmark	The supply plug must comply with Section 107-2-D1, Standard DK2-1a or DK2-5a.
Switzerland	The supply plug must comply with SEV/ASE 1011.
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.
	The mains cord must be <HAR> or <BASEC> marked and be of type HO3VVF3GO.75 (minimum).
Europe	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.

Avertissement: L'installation et la dépose de points d'accès HiveAP doivent être effectuées uniquement par un personnel qualifié.

- 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 boitier 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 cable flexible - AWG No. 18, ou AWG No. 16 pour un cable 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 Gerätenetzkabels 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	Der Cord muß das UL gepruft und war das CSA beglaubigt.
Kanada	Das Minimum spezifikation fur 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 1011Bestimmungen 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 may arise from failing to comply with the instructions in this guide and appropriate electrical codes.

Contents

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:

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 19.

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 should be equivalent or slightly lower than the Aerohive 802.11g radio. If the coverage is correct and has the appropriate density for your deployment, then you simply need 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 intelligence and 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. A fat upgrade 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, that 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 14.

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 software. 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. AirMagnet Laptop Analyzer and Survey are two products that 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 18.)
- **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 (supplicants).
  - 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 will certainly 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 Using 802.11g for Each Access Point	Access Point Density
Coverage (low capacity)	12 Mbps to 24 Mbps	1 access point per 8000 square feet
Standard office deployment	36 Mbps	1 access point per 5000 square feet
Standard office deployment with voice	54 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.

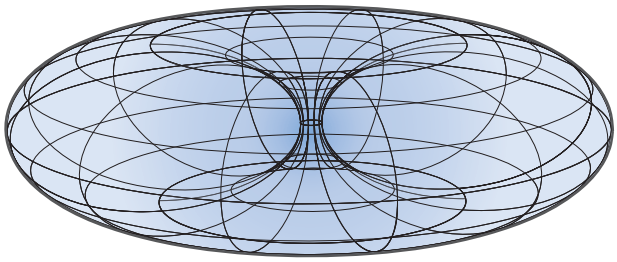
- **Warehouse and Retail**

  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**

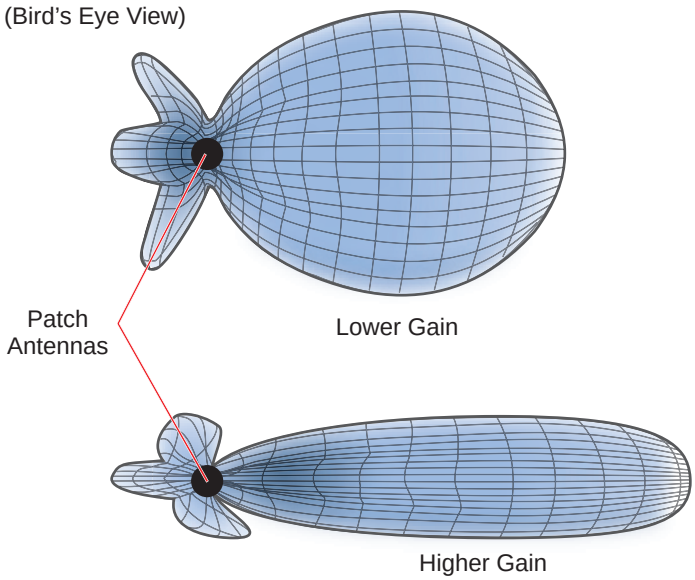
  As anyone who has administered a WLAN system in the past knows, proper configuration of the access point antennas at the outset can save you lots of trouble. HiveAPs come standard with fixed omnidirectional antennas. You typically orient these antennas vertically, positioning the antennas on all HiveAPs in the same direction. Omnidirectional antennas create a coverage area that looks like a doughnut, broadcasting to the sides much more effectively than up or down (see Figure 1 on page 16). 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 Pattern



The HiveAP can accommodate external antennas via coaxial jacks on its chassis (see "Antennas" on page 28). 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. (For an example, see "Example 9: Creating WLAN Policies" on page 107.)

- **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 18), 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 79).

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.

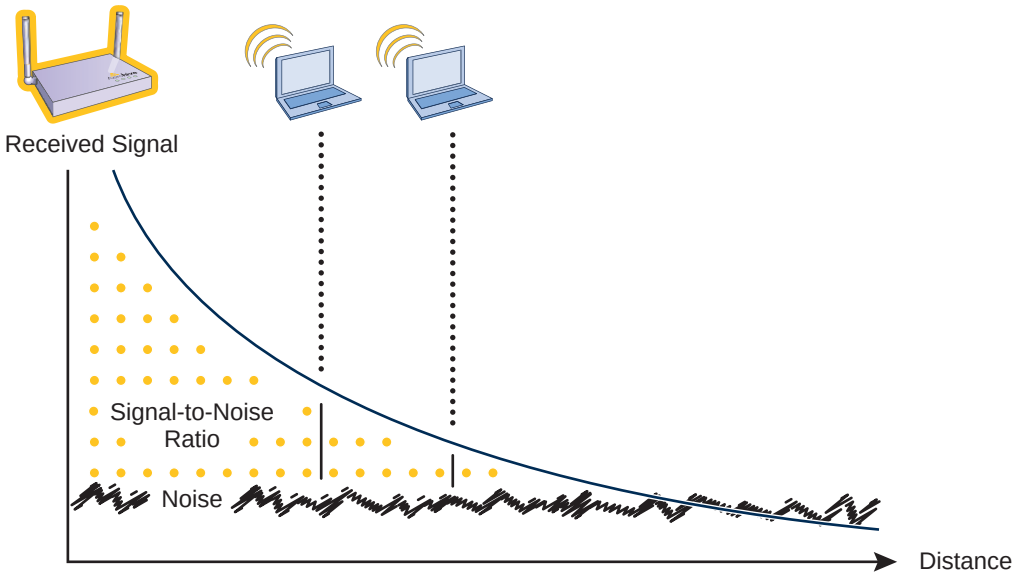
The first thing to know is that Wi-Fi is forgiving. Wi-Fi tends to transmit a bit farther than you expect, and even in cases of interference, it tends to just work. This can be both a blessing and a curse. It is a blessing because people will likely have access to the network, and it is a curse because 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 log10 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 (µW)—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 µW
4 dBm = 2.5 mW	-5 dBm = 316 µW
3 dBm = 2.0 mW	-10 dBm = 100 µW

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 20 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".

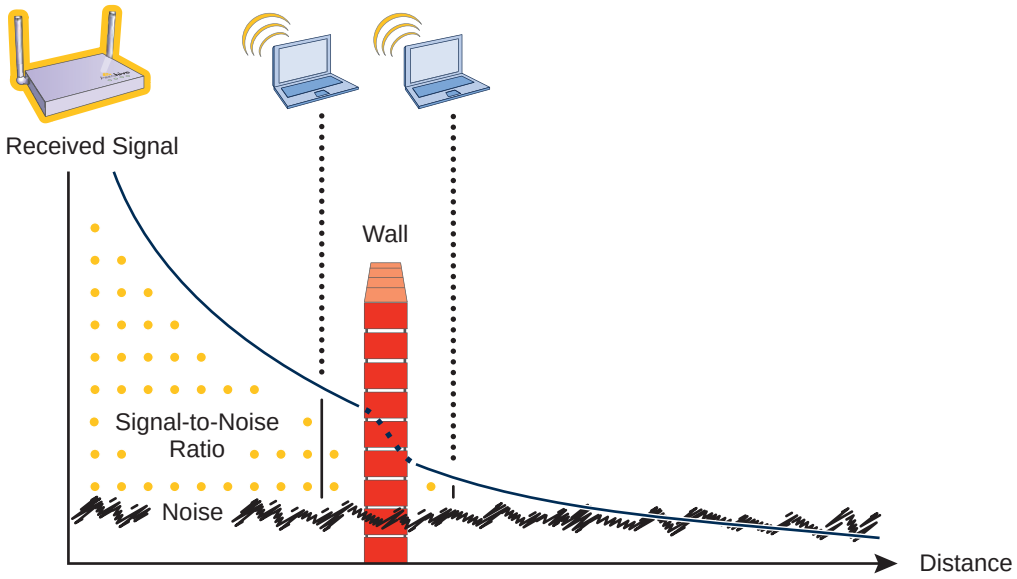
Figure 3 Path Loss in an Open Space



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.

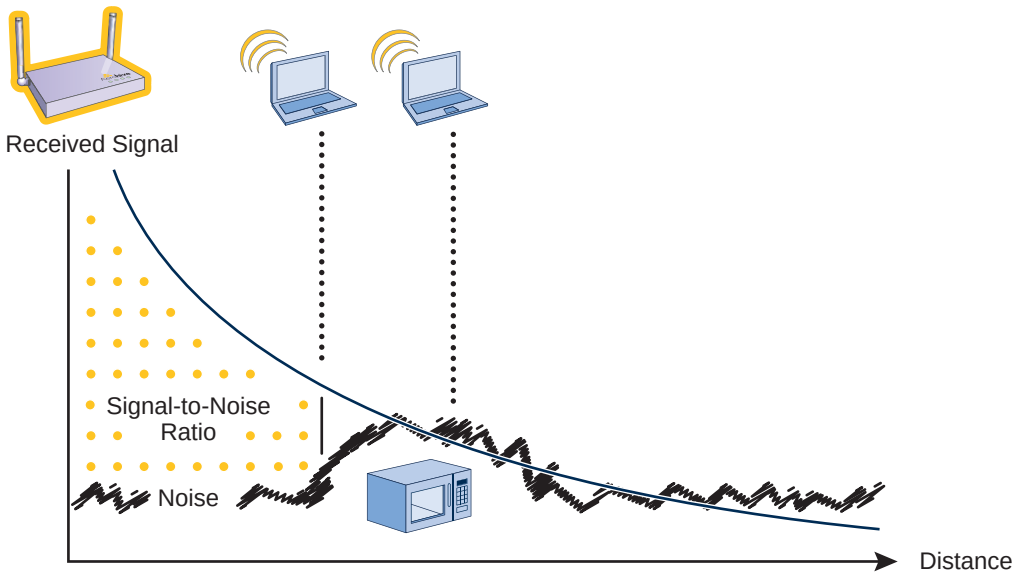
Signal strength not only diminishes over distance but it can also be affected by objects in the way (see Figure 4). This can be a wall, a tree, or even a person. There is a fairly predictable dB drop through most objects that also decreases the SNR, thus decreasing the data rate. While this appears to 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.

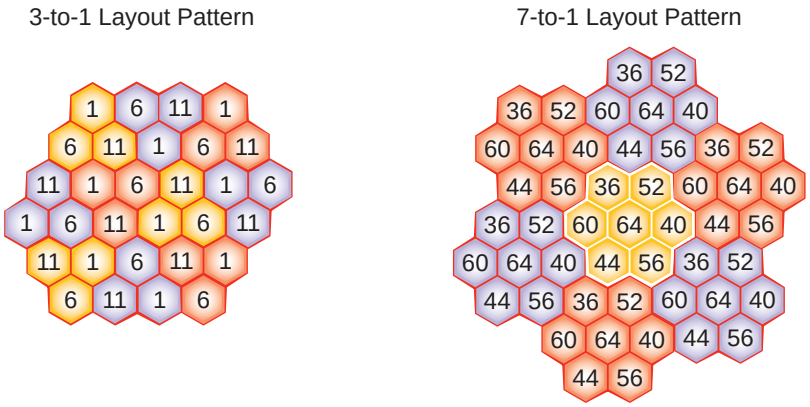
Figure 5 Path Loss with Noise (from Microwave)



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 available in 802.11a/g rather than each being capable of 54-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

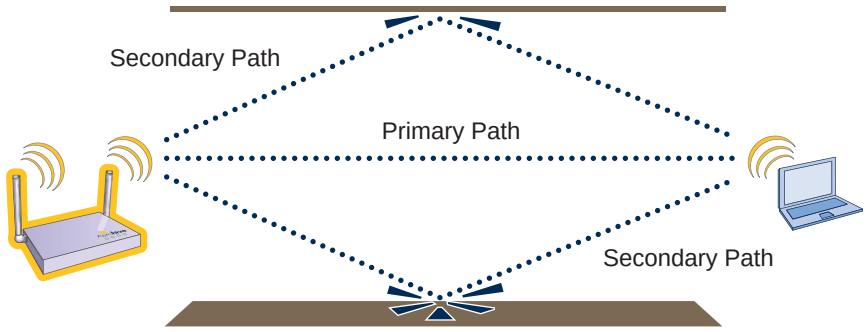


Note: There are alternative 2.4 GHz channel layouts, such as one for four channels using 1, 4, 8 and 11 and another using channels 1, 5, 9 to counter interference from microwaves, which tend to cause interference in the high end of the spectrum. Aerohive recommends alternative channel layouts only for 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 14 channels available for Wi-Fi use. However, in most countries there are at least 8 to work with. 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 21. 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 multipaths. 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.

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 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 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

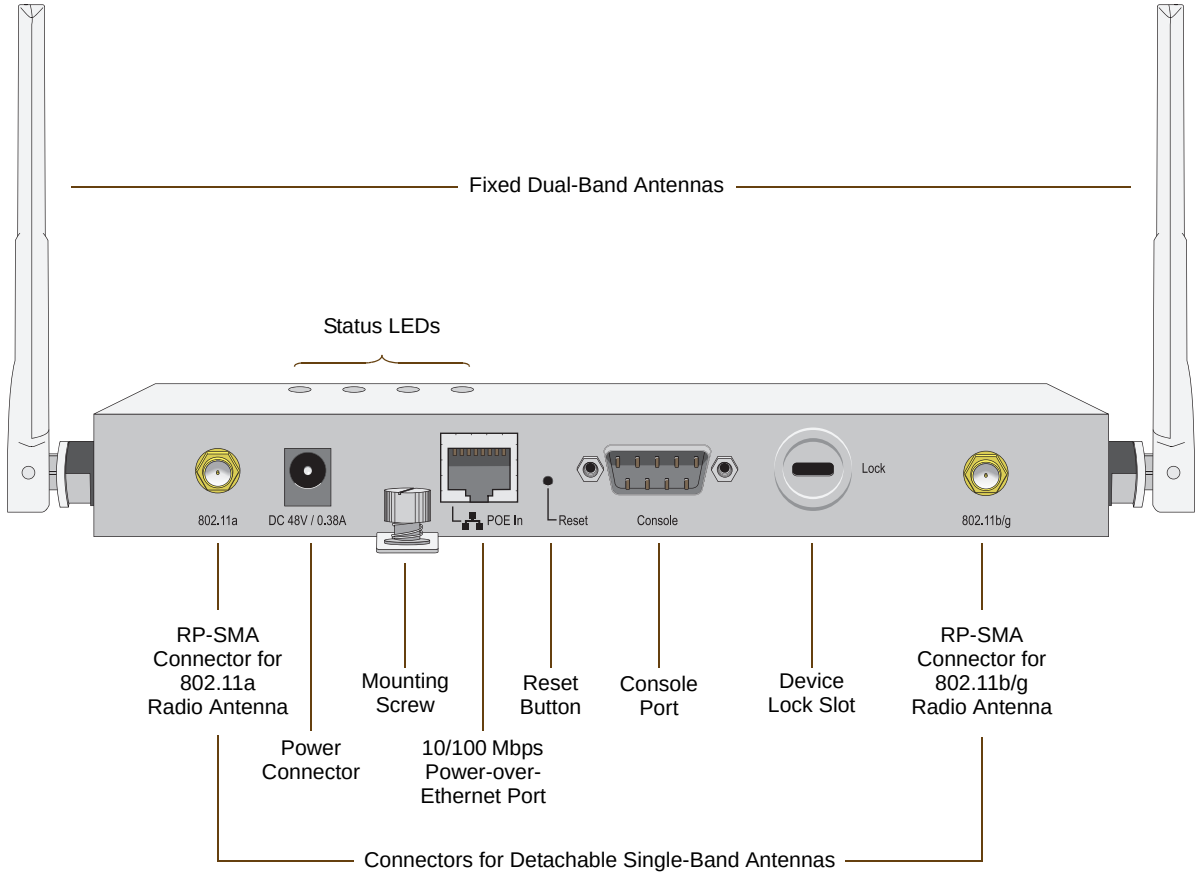


Table 1 HiveAP 20 Component Descriptions

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 28.
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 27.
802.11a RP-SMA Connector	(For future use) You can connect a detachable single-band antenna to the male 802.11a RP-SMA (reverse polarity-subminiature version A) connector. Note that doing so disables the adjacent fixed antenna.

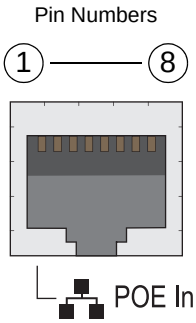
Component	Description
Power Connector	The 48-volt DC power connector (0.38 amps) is one of two methods through which you can power a HiveAP. To connect it to a 100 – 240-volt AC power source, use the AC/DC power adaptor that ships with the product as an extra option. Because the HiveAP does not have an on/off switch, connecting it to a power source automatically powers on the device.
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 29.
10/100 Mbps PoE Port	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 power sourcing equipment (PSE) that is 802.3af-compatible. (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.) 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 26.
Reset Button	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. 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.
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	(For future use) You can connect a detachable single-band antenna 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



(View of the PoE port on the HiveAP)

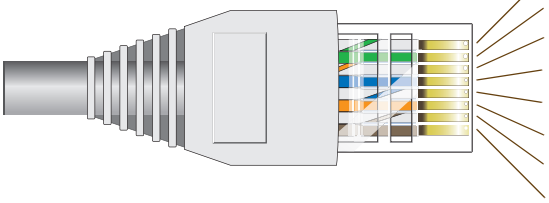
Pin	Data Signal	802.3af Alternative A (Data and Power on the Same Wires)		802.3af Alternative B (Data and Power on Separate Wires)
		MDI	MDI-X	MDI or MDI-X
1	Transmit +	DC+	DC–	– – –
2	Transmit -	DC+	DC–	– – –
3	Receive +	DC–	DC+	– – –
4	(unused)	– – –	– – –	DC+
5	(unused)	– – –	– – –	DC+
6	Receive -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

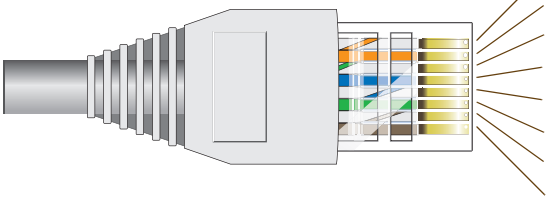
The PoE port is auto-sensing and can automatically adjust to transmit and receive data over straight-through or cross-over Ethernet connections. Likewise, it can automatically adjust to 802.3af Alternative A and B power delivery methods. Furthermore, when the Alternative A method is used, the PoE port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

T568A-Terminated Ethernet Cable with an RJ-45 Connector



Pin	T568A Wire Color
1	White/Green
2	Green
3	White/Orange
4	Blue
5	White/Blue
6	Orange
7	White/Brown
8	Brown

T568B -terminated Ethernet Cable with an RJ-45 Connector



Pin	T568B Wire Color
1	White/Orange
2	Orange
3	White/Green
4	Blue
5	White/Blue
6	Green
7	White/Brown
8	Brown

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.

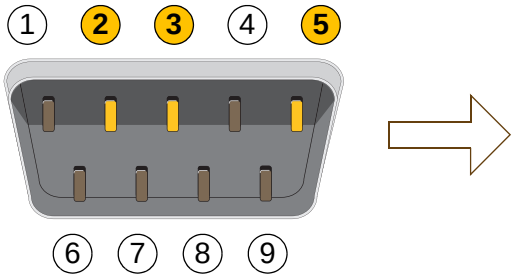
For straight-through Ethernet cables—using either the T568A or T568B standard—the eight wires terminate at the same pins on each end.

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

Male DB-9 Console Port



(View of the console port on the HiveAP)

RS-232 Standard Pin Assignments

Pin	Signal	Direction
1	DCD (Data Carrier Detect)	(unused)
2	**RXD (Received Data)**	**Input**
3	**TXD (Transmitted Data)**	**Output**
4	DTR (Data Terminal Ready)	(unused)
5	**Ground**	**Ground**
6	DSR (Data Set Ready)	(unused)
7	RTS (Request to Send)	(unused)
8	CTS (Clear to Send)	(unused)
9	RI (Ring Indicator)	(unused)

The above pin assignments show a DTE (data terminal equipment) configuration for a DB-9 connector complying with the RS-232 standard. Because this is a console port, only pins **2**, **3**, and **5** need be used.

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 is 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

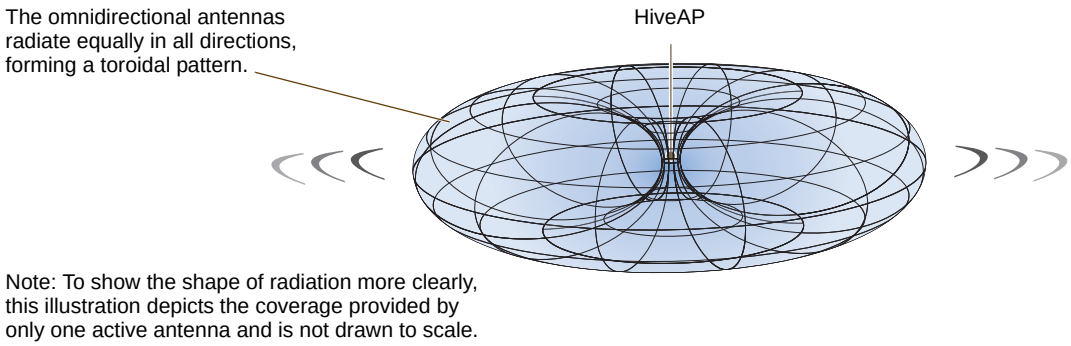
Mesh

- 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

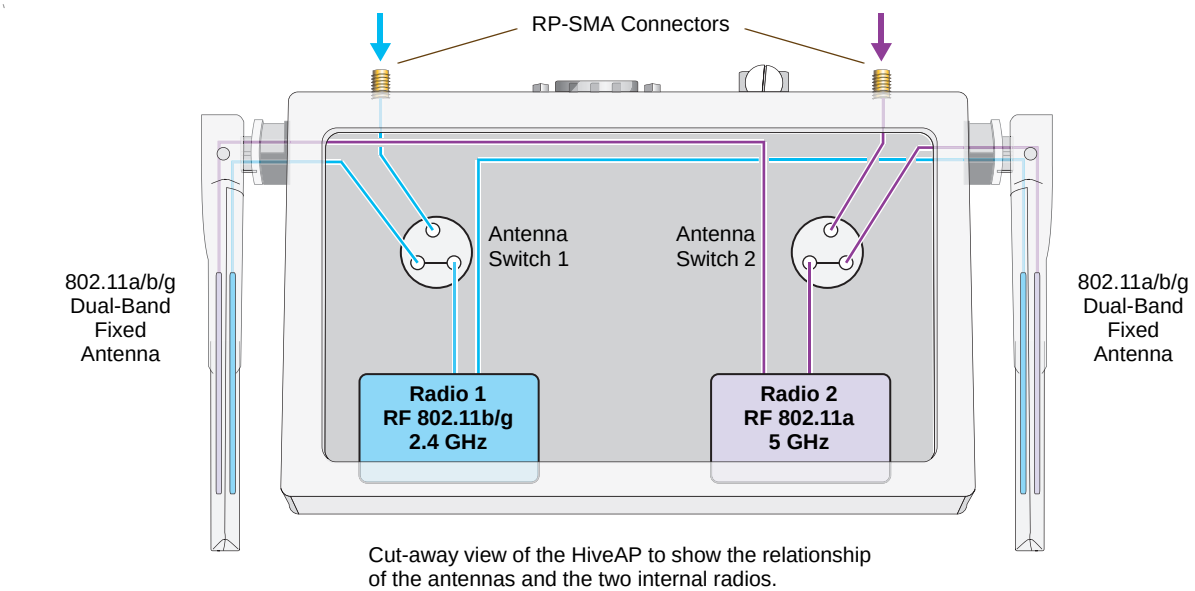
The HiveAP 20 includes two fixed dual-band antennas with 3-dBi gains. These antennas are omnidirectional, providing fairly equal coverage in all directions in a toroidal (donut-shaped) pattern around each antenna. When the antennas are vertically positioned, coverage expands primarily on the horizontal 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 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



After connecting 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, and wifi0.4) 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 28.

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

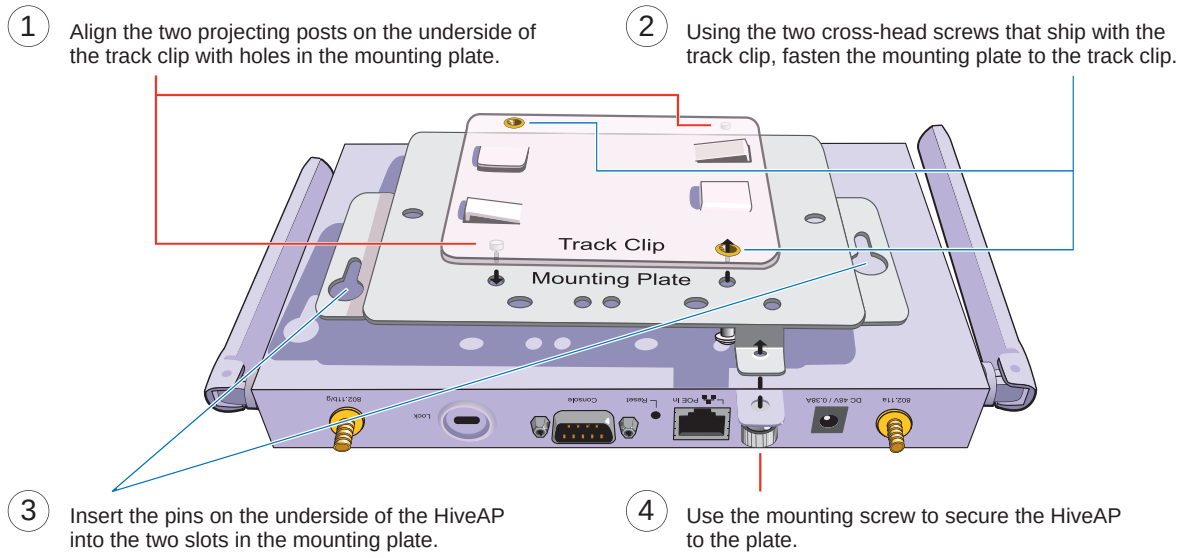
Using the mounting plate and track clip you can mount the HiveAP 20 to the tracks of a dropped ceiling grid. Using just the mounting plate, you can mount the HiveAP to any surface that can support its weight (1.5 lb., 0.68 kg).

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.

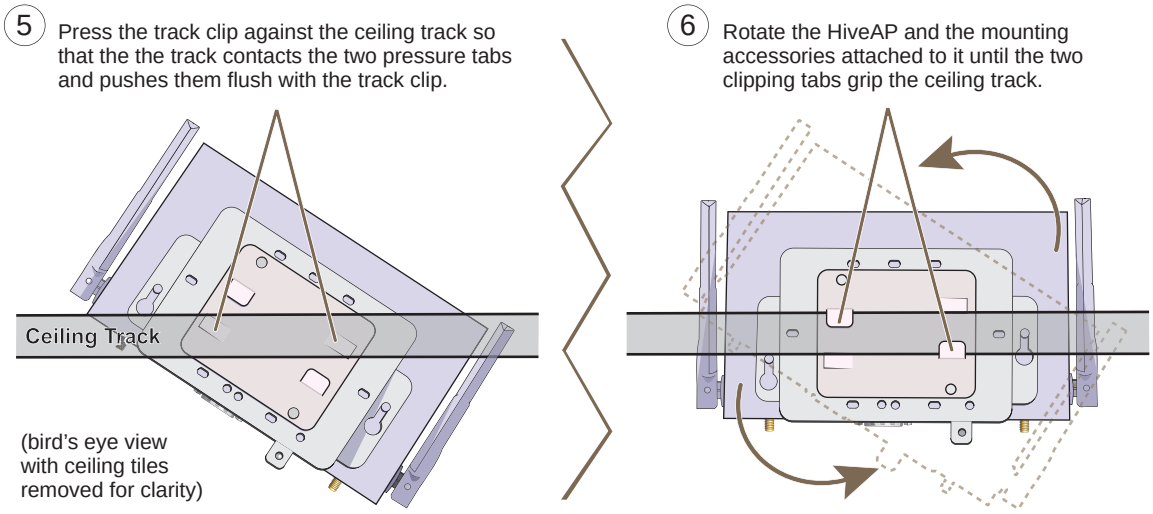
Attach the track clip to the mounting plate, and then attach the clip-plate combination to the HiveAP 20, as shown in Figure 6.

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.

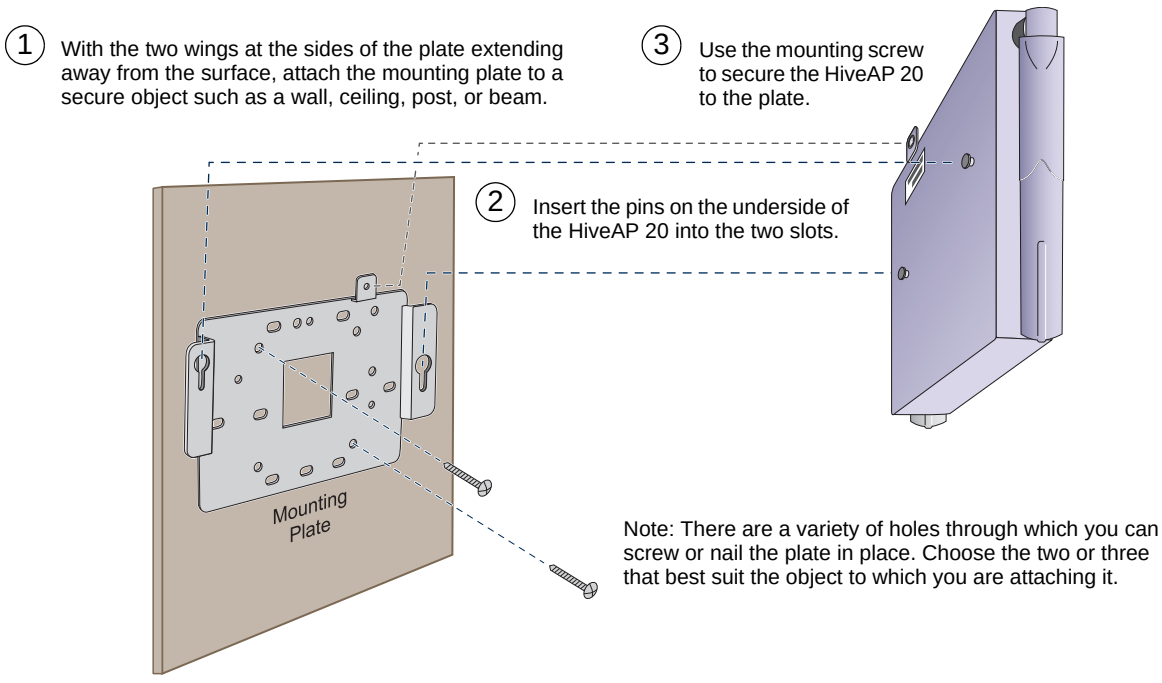
Figure 7 Attaching the HiveAP to a Dropped Ceiling Track



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 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

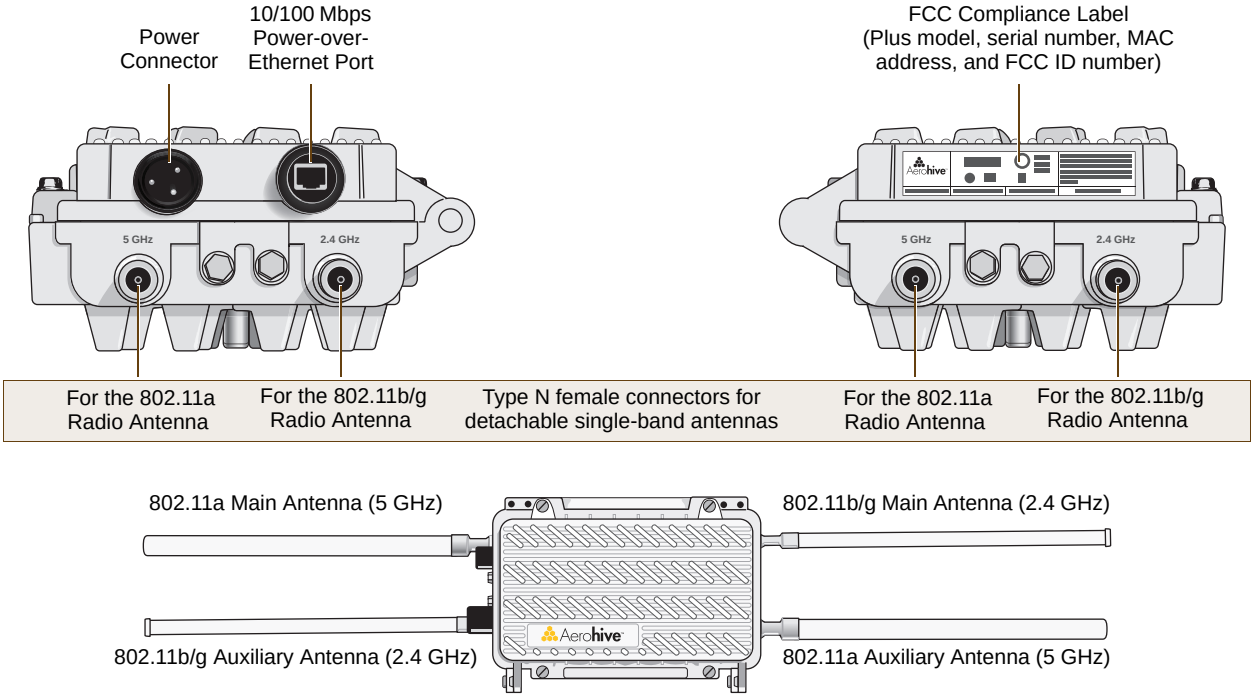


Table 1 HiveAP 28 Component Descriptions

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 37.
Type N Connectors (Female)	Attach antennas to the HiveAP 28 through these connectors. For details, see "Attaching Antennas" on page 42.
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.)

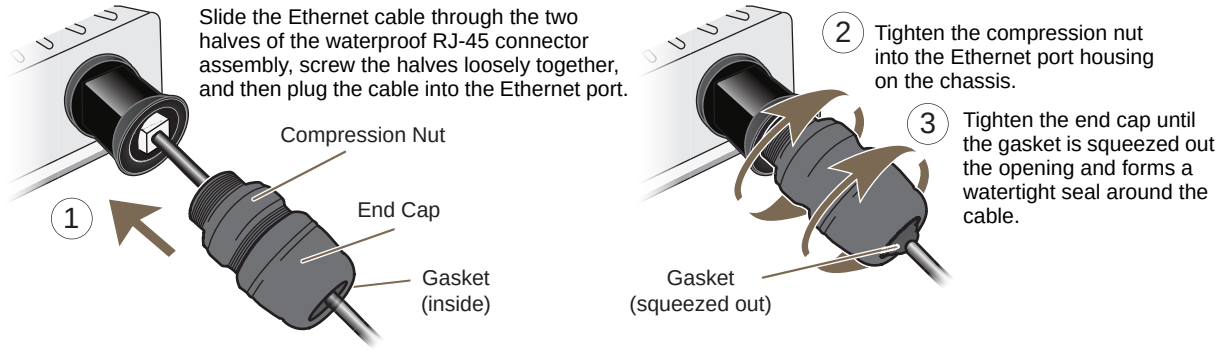
Component	Description
10/100 Mbps PoE Port	The 10/100-Mbps Ethernet port supports IEEE 802.3af PoE (Power over Ethernet) and receives RJ-45 connectors. The HiveAP can receive its power through an Ethernet connection to PSE (power sourcing equipment) that is 802.3af-compatible. (If you connect the HiveAP to a power source through the power connector and PoE port simultaneously, the device draws power through the power connector and automatically disables PoE.) 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".

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 26). 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 wrap 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).

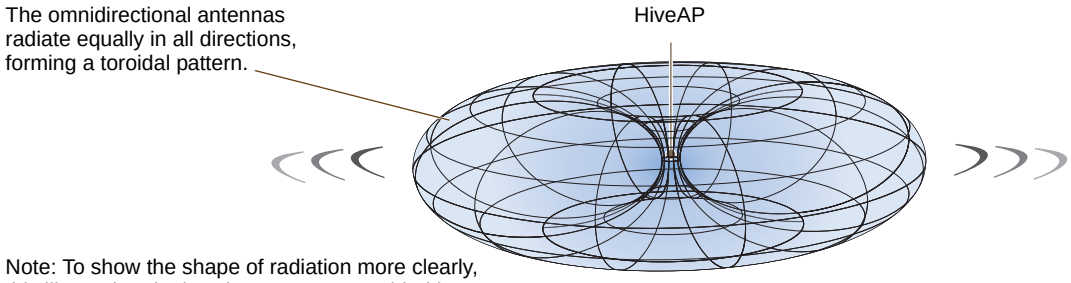
   Note: The HiveAP 28 must be grounded. Do not operate it unless there is a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

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.

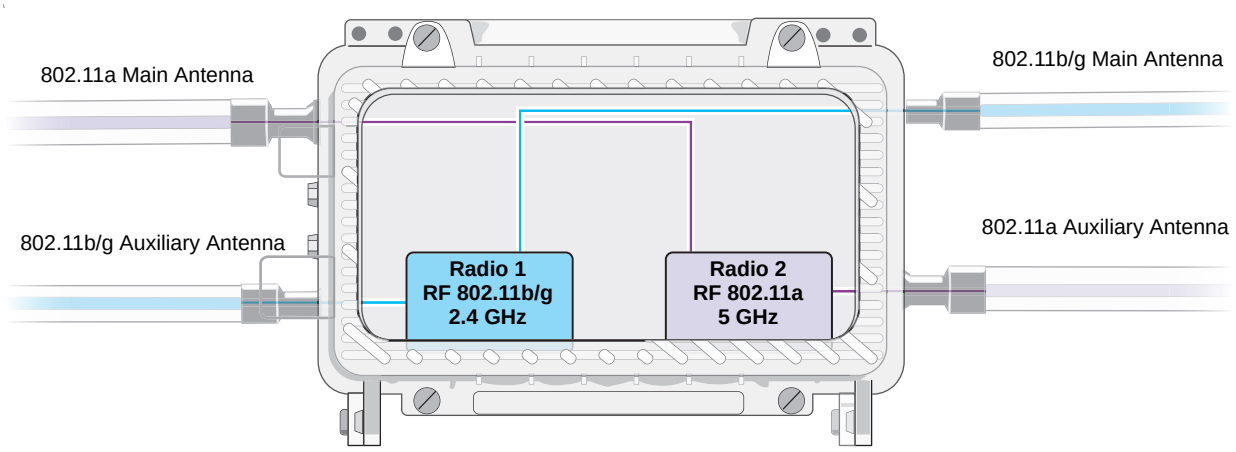
Figure 3 Omnidirectional Radiation Pattern



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 42.)

Figure 4 Antennas and Radios



The two 802.11b/g antennas link internally to Radio 1 and broadcast in the 2.4 GHz frequency range.

The two 802.11a antennas link internally to Radio 2 and broadcast in the 5 GHz frequency range.

Note: The HiveAP 20 uses **`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 39 – Mount the HiveAP 28 on a pole such as a street light.
- "Strand Mount" on page 40 – Suspend the HiveAP 28 from a cable or phone line.
- "Surface Mount" on page 41 – 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 42.

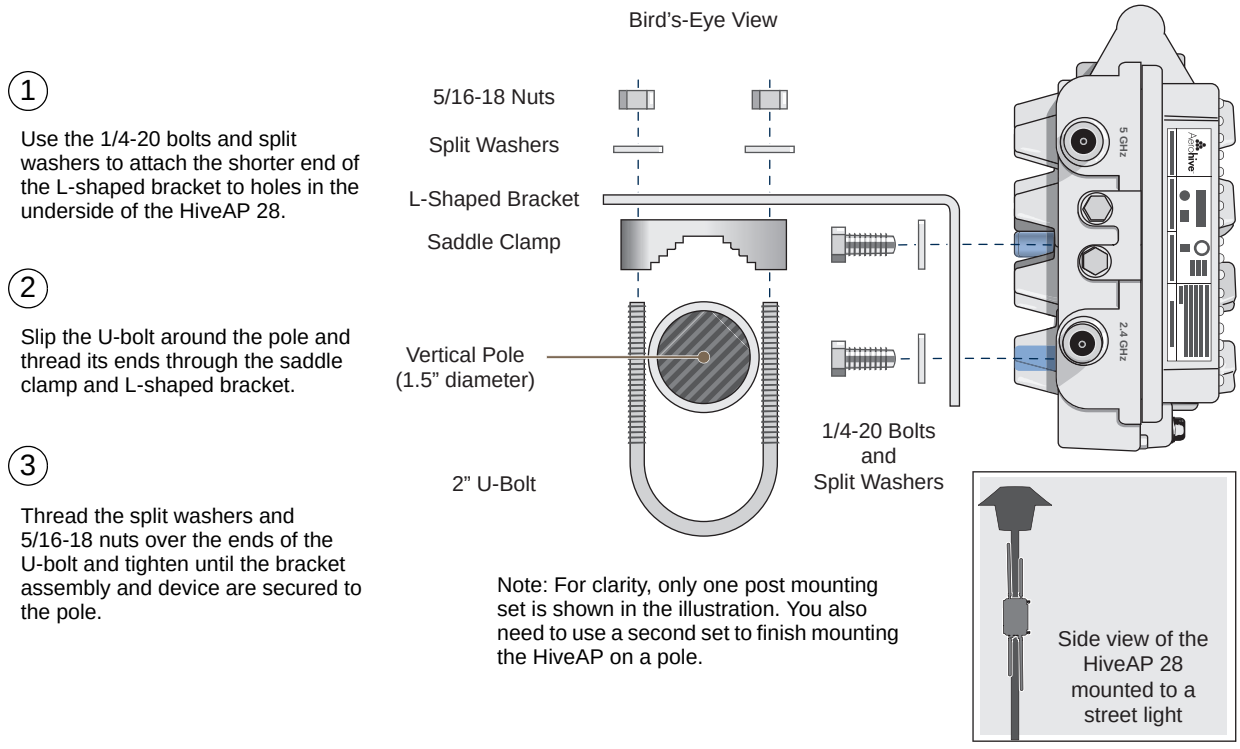
Before you mount the HiveAP 28 and attach antennas, read the following warnings and cautions:

- 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.

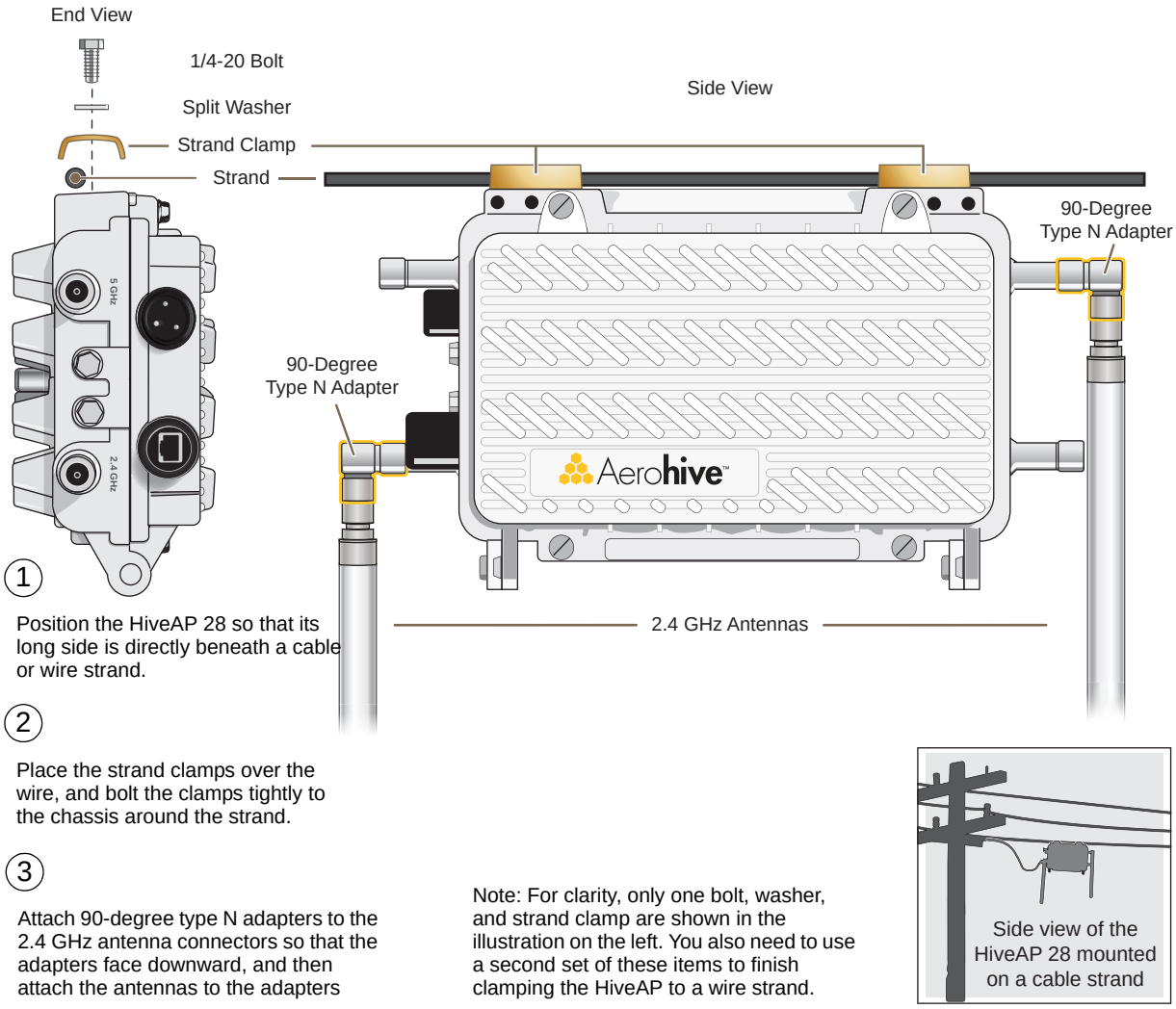
3. Thread a split washer and 5/16-18 nut to each end of the U-bolt, and tighten them with a wrench to secure the U-bolt firmly to the pole.

   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



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.

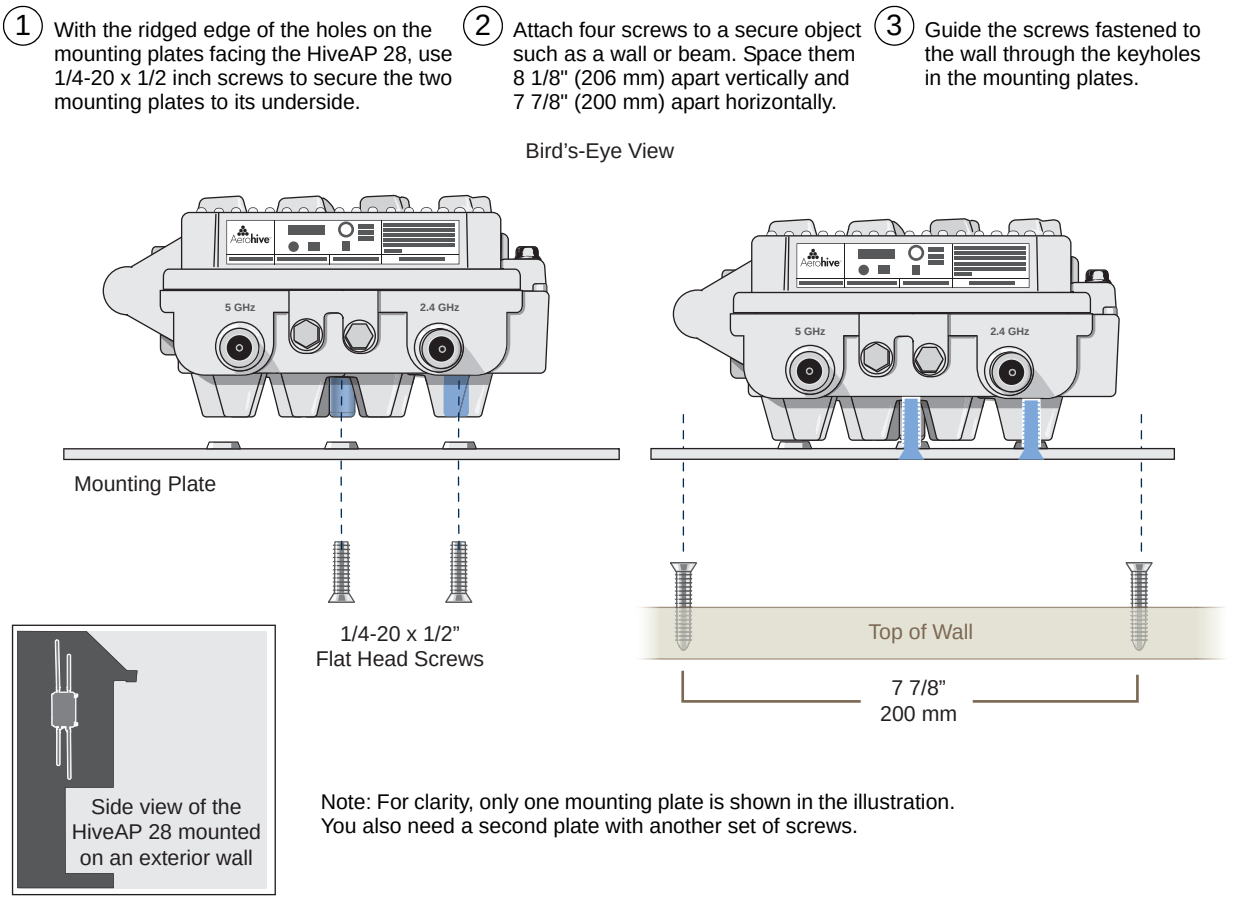
3. Attach the 90-degree type N adapters to the two 2.4 GHz antenna connectors and then attach the antennas to the adapters so that the antennas face downward. For details, see "Attaching Antennas" on page 42.

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



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

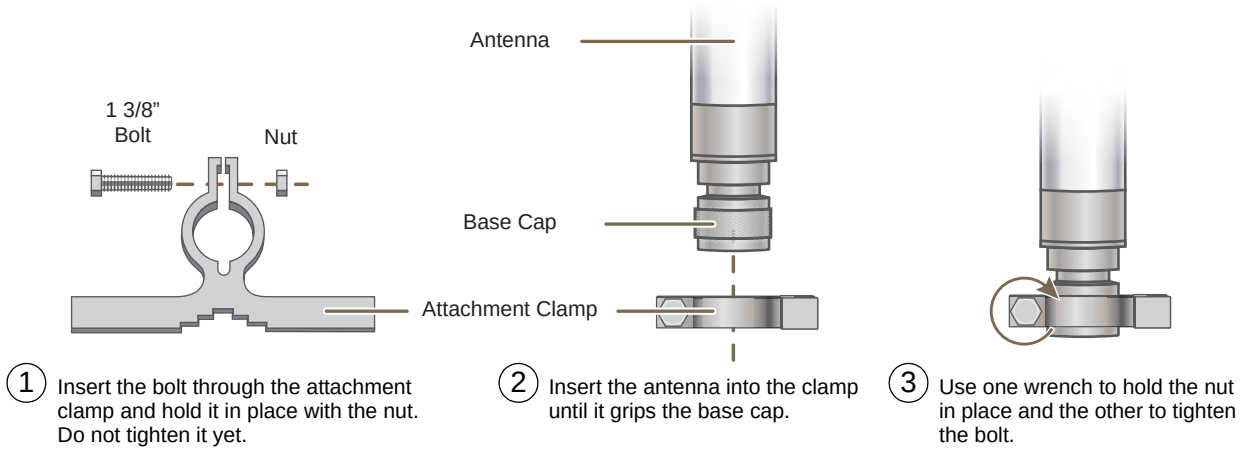
In addition to connecting antennas directly to the HiveAP 28, you can also mount them separately and run a cable between the antennas and the device. Use either male-to-female cables with Type N connectors or use male-to-male or female-to-female cables with cable gender changers. (The antennas have male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

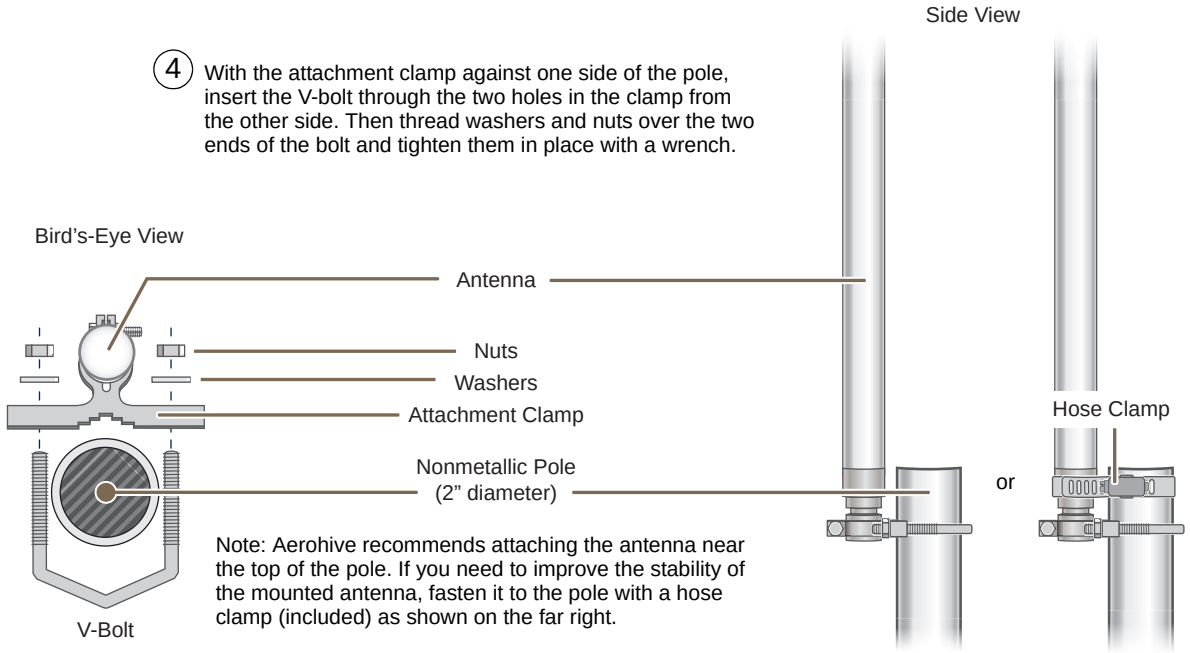
For each antenna that you mount, you need an attachment clamp, a 1 3/8" bolt and nut, a V-bolt, two washers and two nuts, a hose clamp, and two wrenches.

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 42.
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

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 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

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

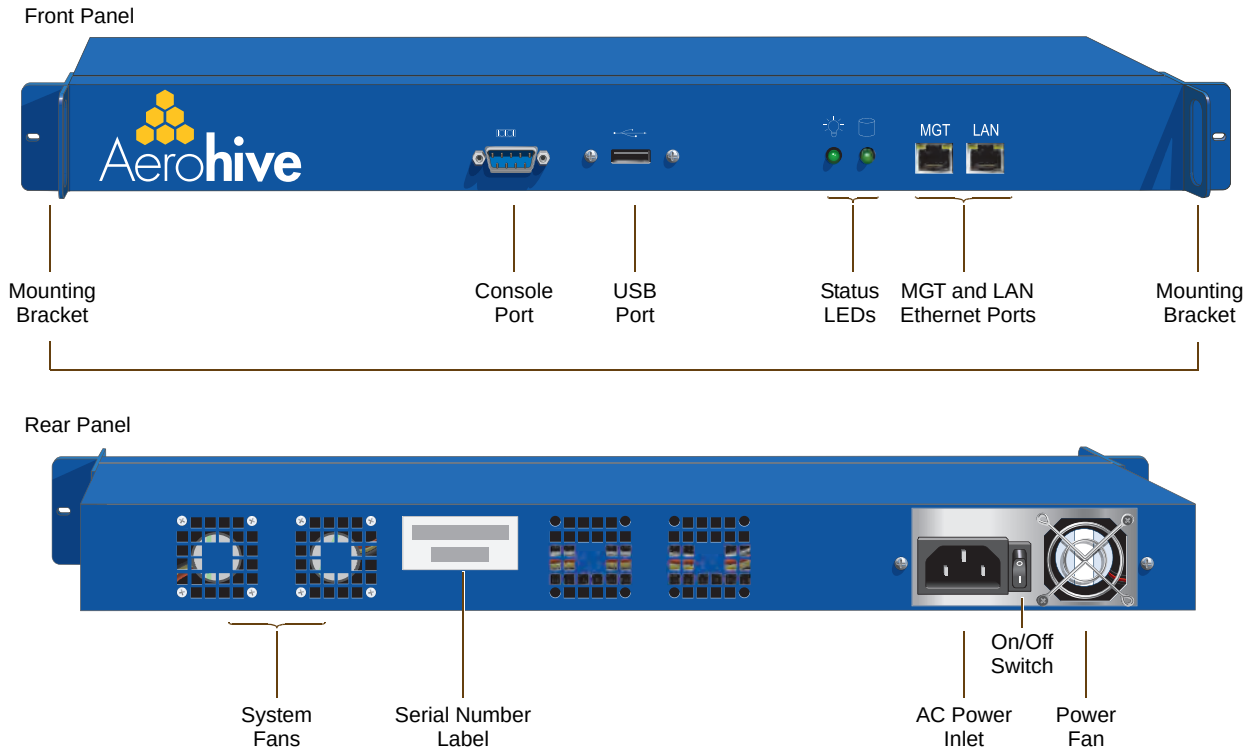


Table 1 HiveManager Component Descriptions

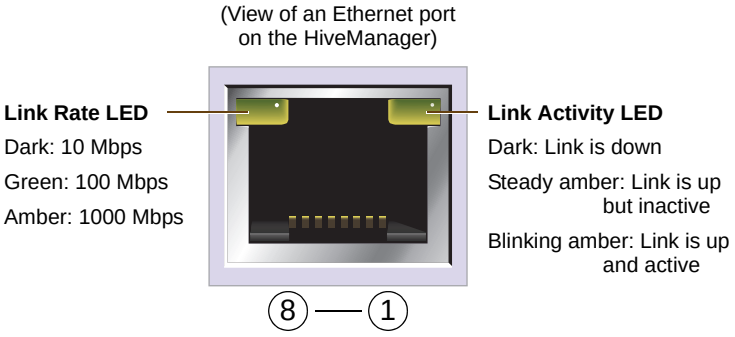
Component	Description
Mounting Brackets	The two mounting brackets allow you to mount the HiveManager in a standard 19" (48.26 cm) equipment rack. You can also move the brackets to the rear of the chassis if you need to reverse mount it.
Console Port	A male DB-9 serial port to which you can make a console 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 26). 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 *admin* and the password is *aerohive*. 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 48.
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 (○) 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



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

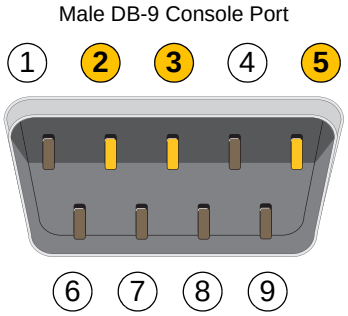
A+/A-, B+/B-, C+/C-, D+/D- = wire pairings

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 26.

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



(View of the console port on the HiveManager)

RS-232 Standard Pin Assignments

Pin	Signal	Direction
1	DCD (Data Carrier Detect)	(unused)
2	**RXD (Received Data)**	**Input**
3	**TXD (Transmitted Data)**	**Output**
4	DTR (Data Terminal Ready)	(unused)
5	**Ground**	**Ground**
6	DSR (Data Set Ready)	(unused)
7	RTS (Request to Send)	(unused)
8	CTS (Clear to Send)	(unused)
9	RI (Ring Indicator)	(unused)

The above pin assignments show a DTE configuration for a DB-9 connector complying with the RS-232 standard. Because this is a console port, only pins **2**, **3**, and **5** need be used.

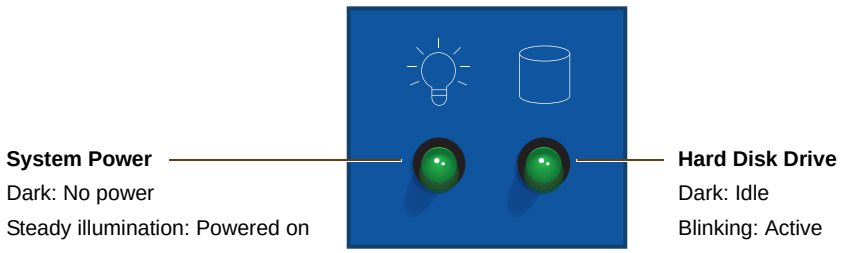
The serial connection settings are as follows:

- 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.

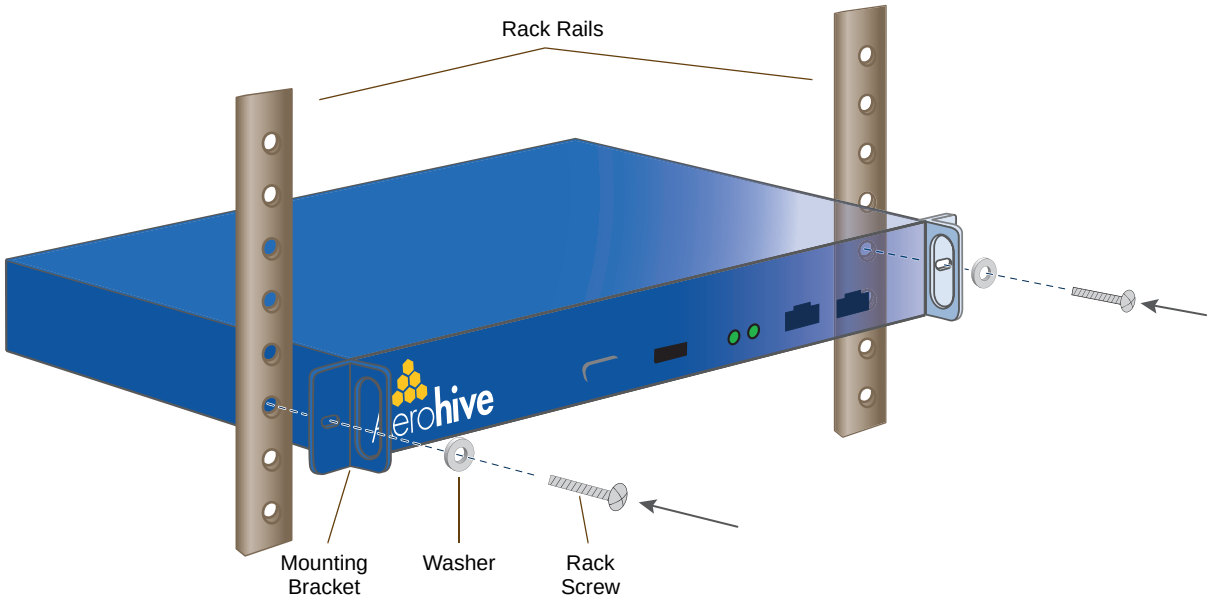
Figure 4 Status LEDs



RACK MOUNTING THE HIVEMANAGER

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 46). 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 5 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

The Aerohive HiveManager High Capacity 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 High Capacity Hardware Components

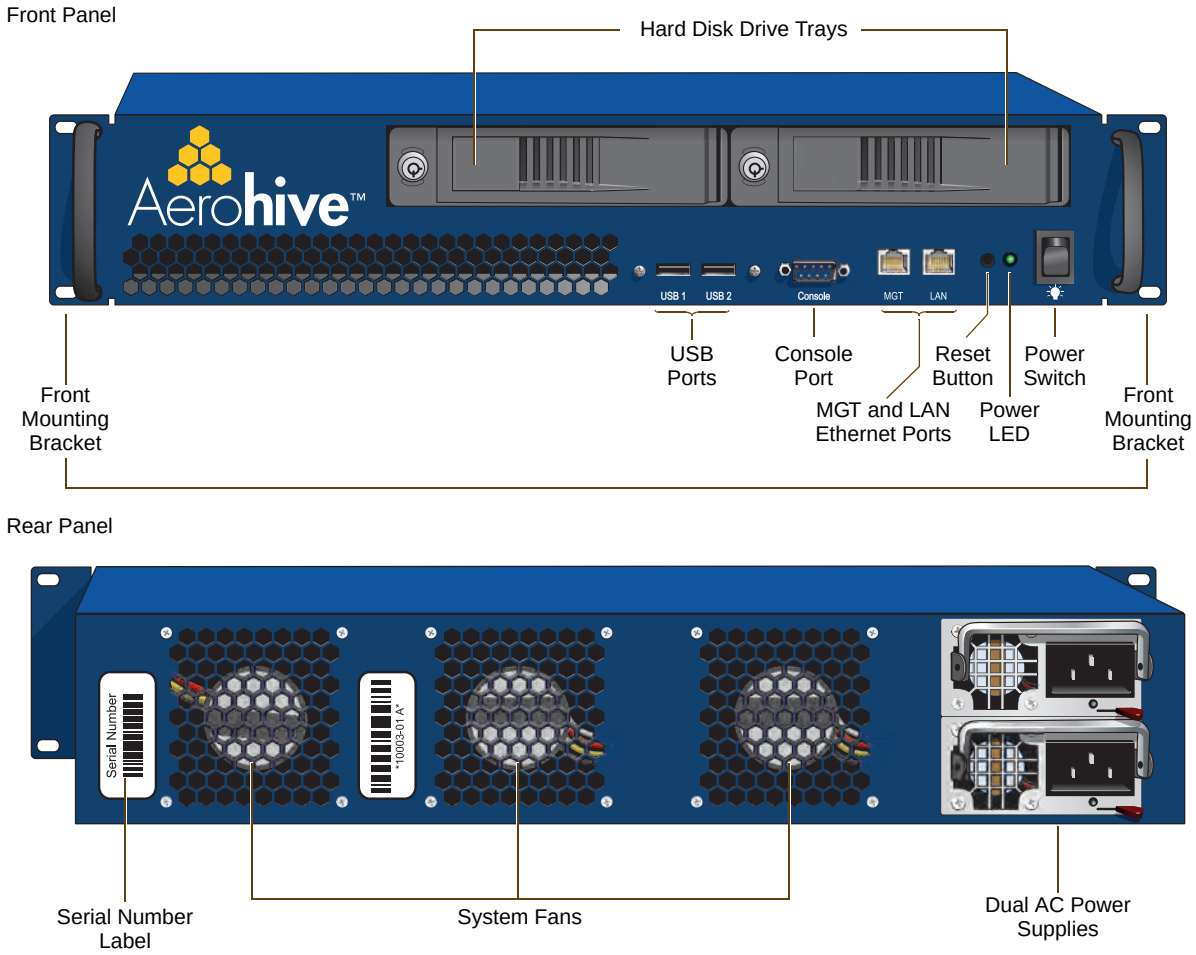


Table 1 HiveManager Component Descriptions

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 54.
USB Ports	The USB ports are reserved for internal use.

Component	Description
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 HiveManager and on the HiveAP (see "Ethernet and Console Ports" on page 26). 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 *admin* and the password is *aerohive*. After making a connection, you can access the Linux operating system.
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. The wiring terminates the same way as that on the standard capacity HiveManager (see "Ethernet and Console Ports" on page 47).
Reset Button	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
Power LED	The power LED conveys the operational states for the system power: dark = no power; steady green = powered on.
On/Off Switch	The on and off switch controls the power to the HiveManager.
Serial Number Label	The serial number label contains the serial number for the device.
System Fans	The three system fans maintain an optimum operating temperature. Be sure that air flow through the system fan vents is not obstructed.
Dual AC Power Supplies	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.

Rack Mounting the High Capacity HiveManager

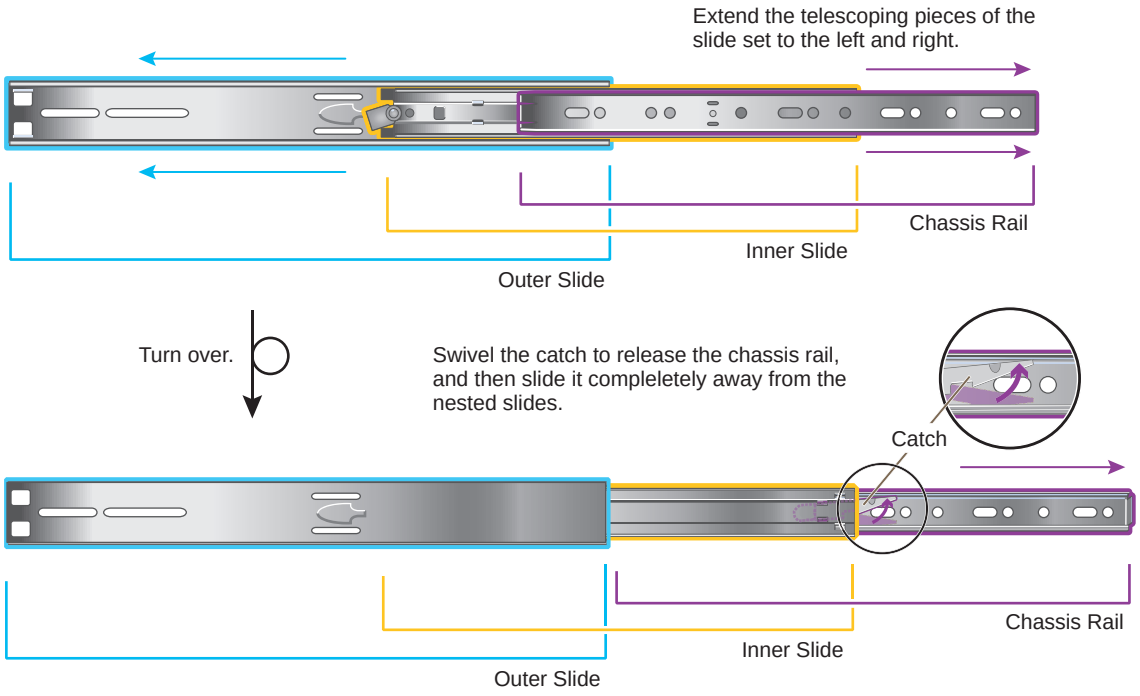
Use the rack mounting kit to mount the High Capacity HiveManager in a standard 19" (48 cm) equipment rack. The rack mounting kit contains the following items:

- (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.

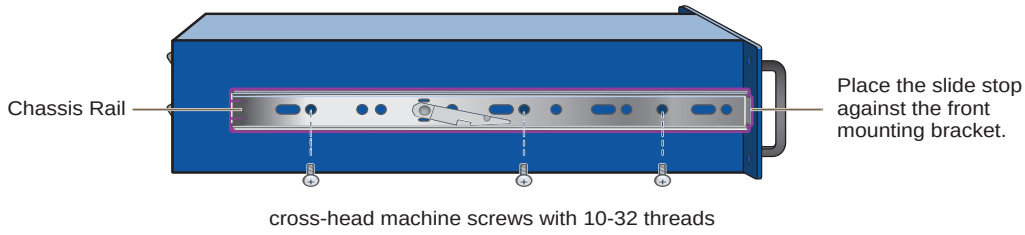
1. After checking that the mounting kit contains the above parts, separate the chassis rails from each slide set, as shown in Figure 2.

Figure 2 Separating the Chassis Rail from the Nested Slides



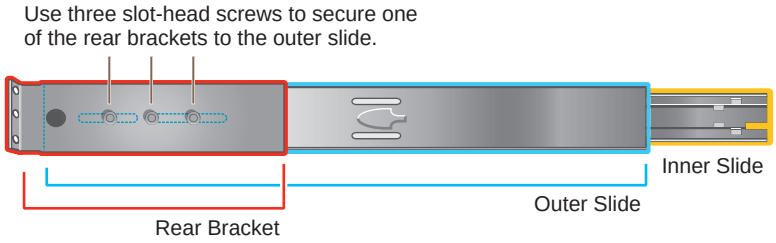
2. Position one of the chassis rails so that the slide stop is near the HiveManager mounting bracket near the front panel and the front and rear holes in the chassis rail align with the holes in the side of the HiveManager. Use three of the cross-head screws to secure the chassis rail to the HiveManager chassis as shown in Figure 3 on page 55.

Figure 3 Attaching the Chassis Rail to the HiveManager



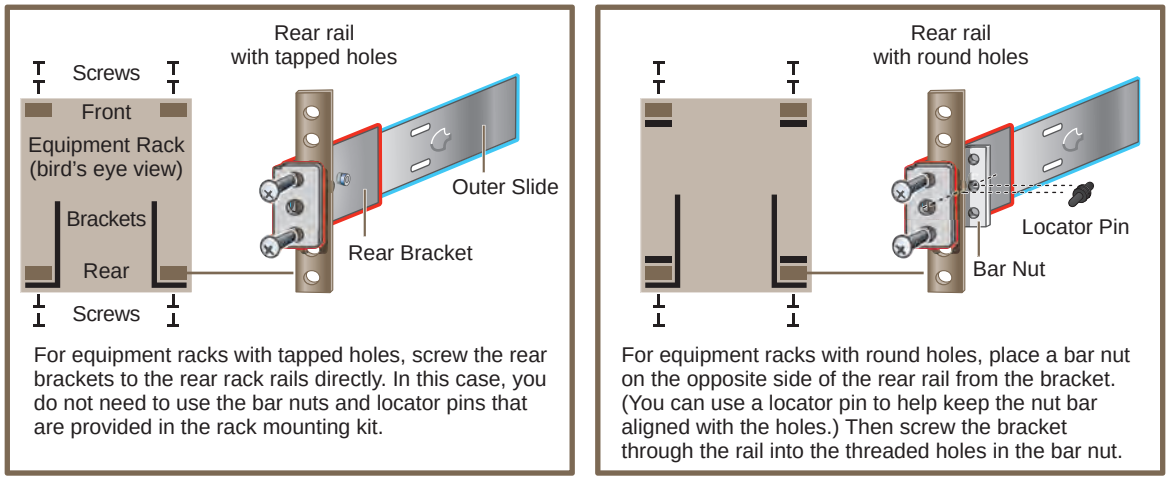
3. Secure the other chassis rail to the other side of the HiveManager.
4. Use three slot-head screws to attach the rear mounting bracket to the outer slide. Insert the screws through the rounded slots in the outer slide into the threaded holes in the bracket and tighten them as shown in Figure 4.

Figure 4 Attaching the Rear Bracket to the Outer Slide



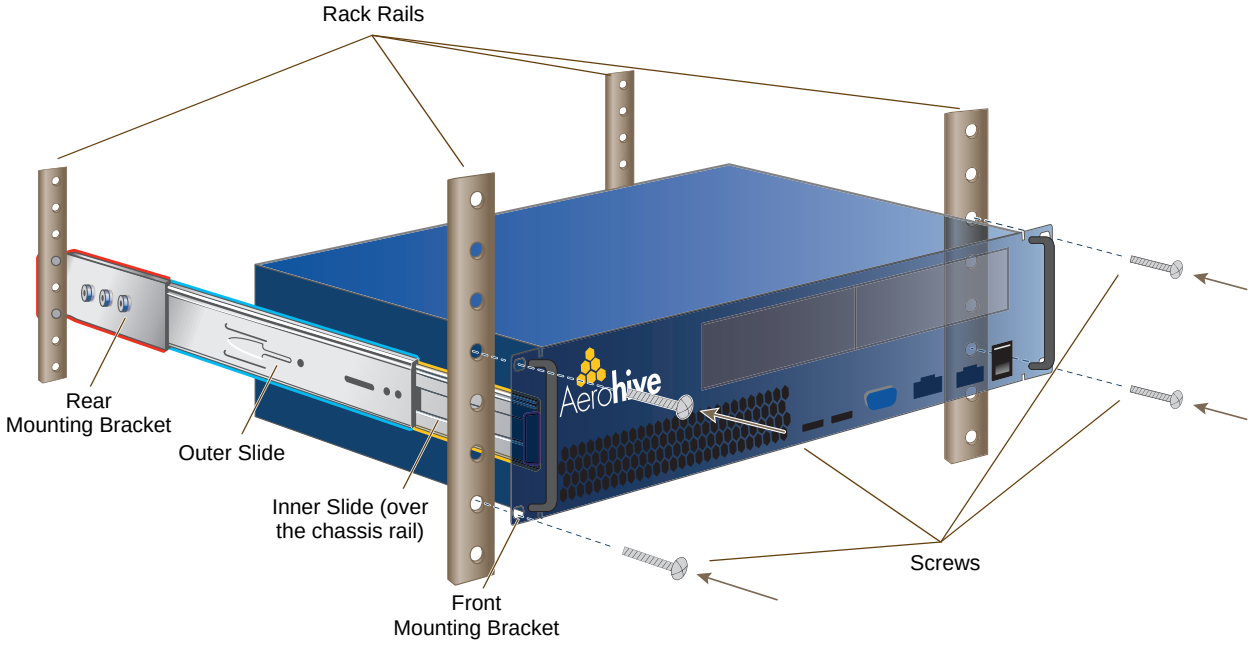
5. Use the remaining three slot-head screws to attach the other rear mounting bracket to the other outer slide.
6. Fasten the rear mounting brackets—and the slides attached to them—to the rear equipment rack rails. Depending on the type of holes in the equipment rack, use one of the following methods:
   - 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



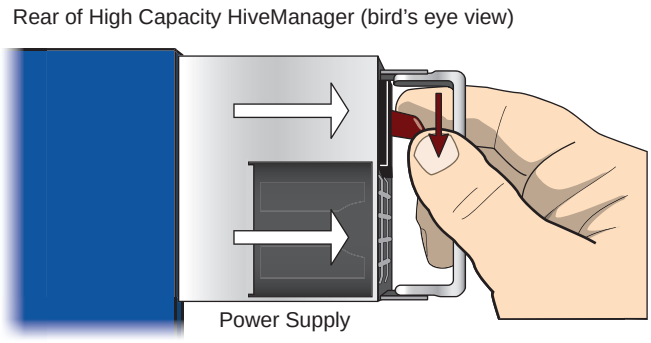
The HiveManager is now securely mounted to the front and rear rails of the equipment rack.

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 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



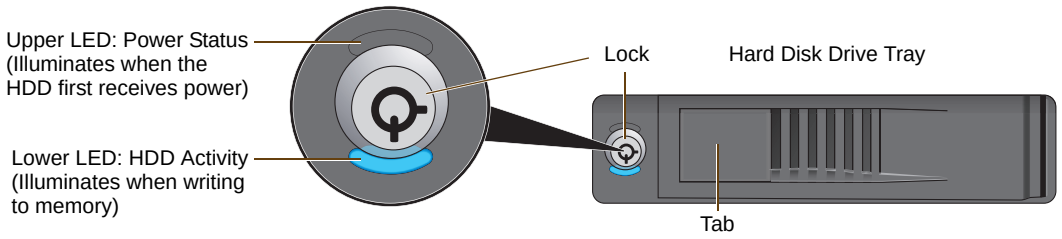
5. Insert a working power supply into the vacant bay and push it straight in until it is fully seated.

   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 63.
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

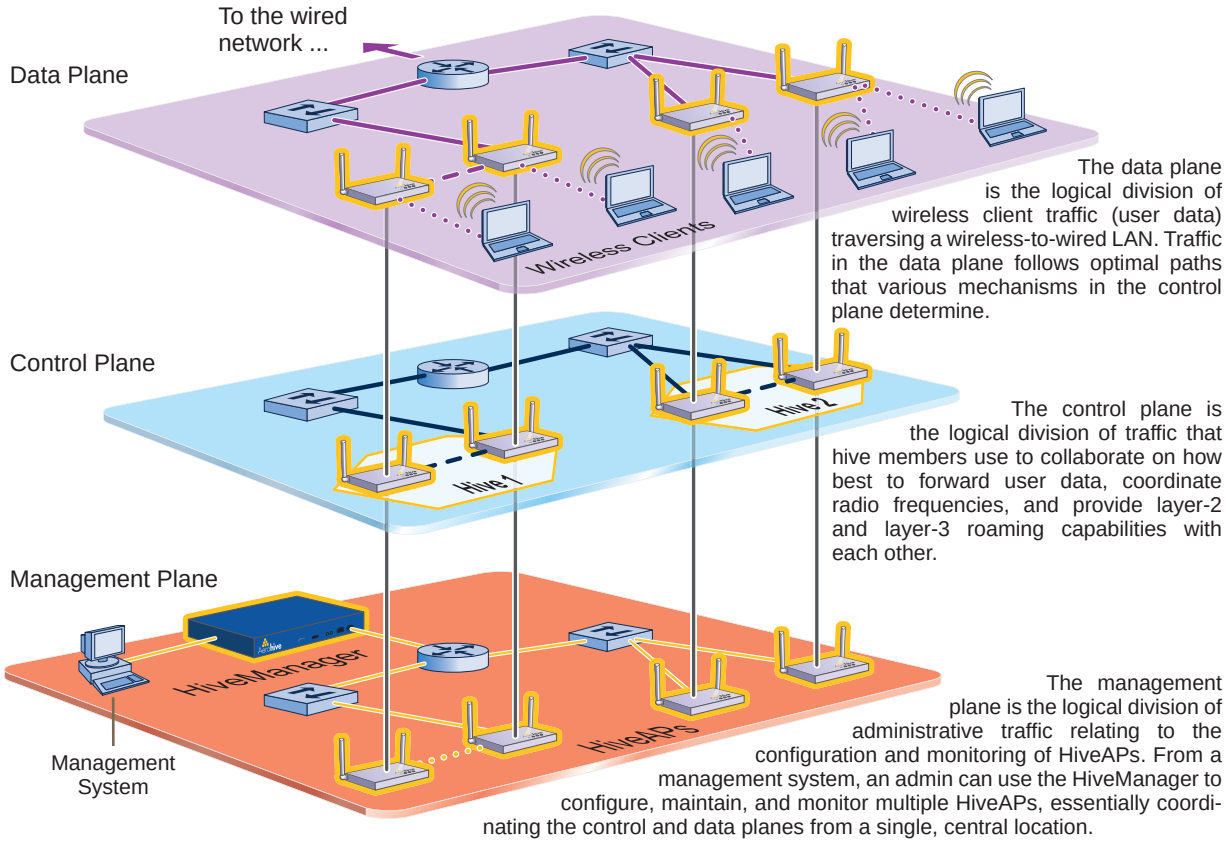
Environmental Specifications

- 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 6 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 and LAN interfaces
- 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

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 and download the GUI application.

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 47.)

The GUI requirements for the management system are as follows:

- Minimum screen resolution of 1024 x 768 pixels
- Standard browser—Aerohive recommends Internet Explorer v7.0 or Mozilla Firefox v2.0.0 or later—with the following enabled:
  - JavaScript (referred to as "active scripting" in Internet Explorer) and the scripting of Java applets; these are required for making SSH connections to managed HiveAPs
  - Flash v9.0 or later; this 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® operating systems).

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 startup wizard that is available through the 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 and offers several options. To change network settings, enter **1**
7. Follow the instructions to configure the IP address and netmask for the MGT (and LAN) interfaces, as well as the default gateway, host name and domain name of HiveManager, and its primary DNS server.

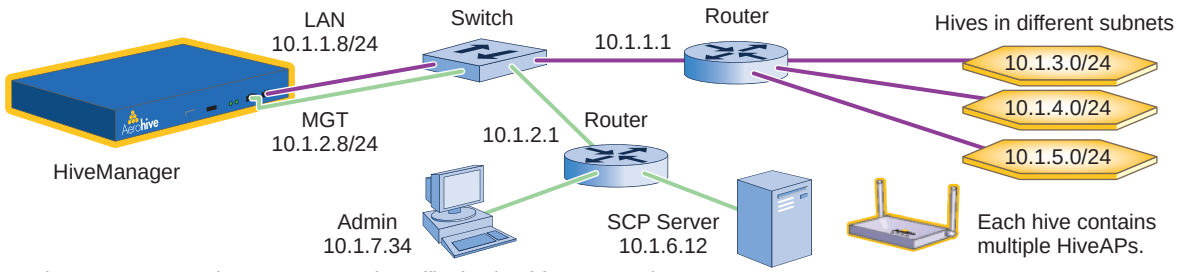
Note: The default IP address/netmask for the MGT interface is 192.168.2.10/24. For the LAN interface, it is 192.168.3.10/24. The default gateway IP address is 192.168.2.1. If you only use the MGT interface, change the LAN interface network settings to 0.0.0.0/0. Do not assign it an IP address and netmask.

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 SCP (Secure Copy) uploads
- HiveAP management traffic for CAPWAP, SNMP monitoring and notifications, and SCP configuration, captive web portal file, and HiveOS firmware uploads 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.

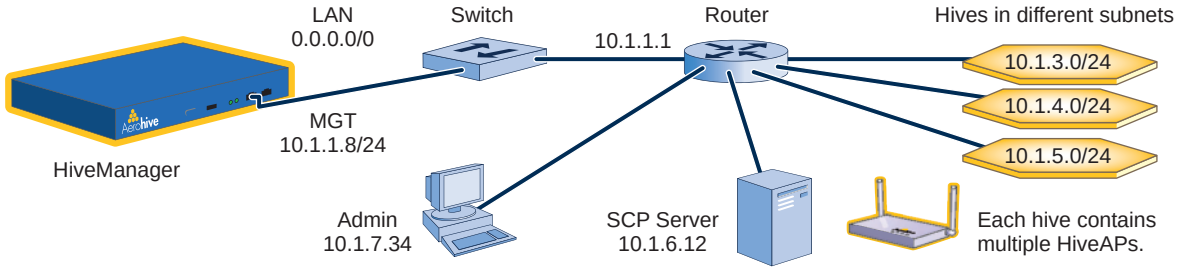
HiveManager sends traffic destined for 10.1.7.0/24 to 10.1.2.1.

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 HM Admin > 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 the two types of management traffic cannot be separated 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, return to the main menu, and reboot the HiveManager appliance by entering **5** (`5 Reboot HM Appliance`).

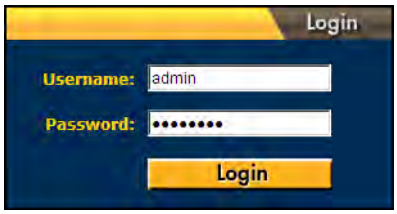
   You can now disconnect the serial cable.

Connecting to the GUI through the MGT Interface

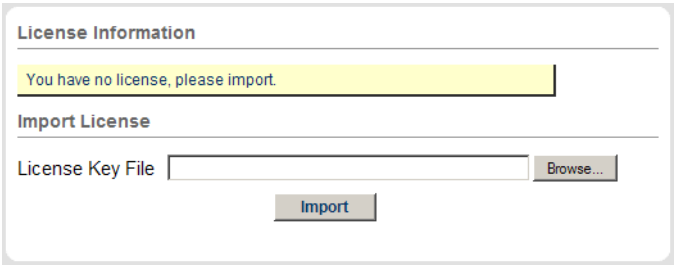
1. Connect Ethernet cables from the MGT interface and LAN interface—if you are using it—to the network.
2. Connect an Ethernet cable from your management system to the network so that you can make an HTTPS connection to the IP address that you set for the MGT interface.
3. Open a web browser and enter 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

   Note: If you ever forget the IP address of the MGT interface and cannot make an HTTP connection to HiveManager, make a serial connection to its console port and enter this command: **`ifconfig`**. *The output displays data about the MGT interface (internally called "eth0"), including its IP address. The serial connection settings are explained in* *"Changing Network Settings" on page 63*.

   A login prompt appears.
4. Type the default user name (*admin*) and password (*aerohive*) in the login fields, and then click **Login**.



5. If prompted to enter a license key, click **Browse**, navigate to and select the text file containing the license key that Aerohive provided when HiveManager was purchased, and then click **OK**.



   You are now logged in to the HiveManager GUI. After logging in, you can check details about the license you installed on the HM Admin > License Management page.

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" on page 69. The GUI consists of several important sections, which are shown in Figure 4.

Figure 4 Important Sections of the HiveManager GUI

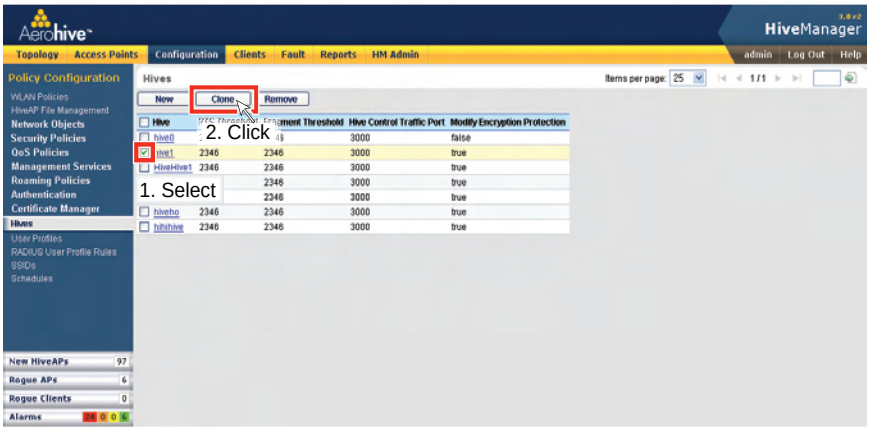
Some convenient aspects that the HiveManager GUI offers are the ability to clone configurations, apply configurations to multiple HiveAPs at once, and sort displayed information. Brief overviews of these functions are presented in the following sections.

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 5 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.



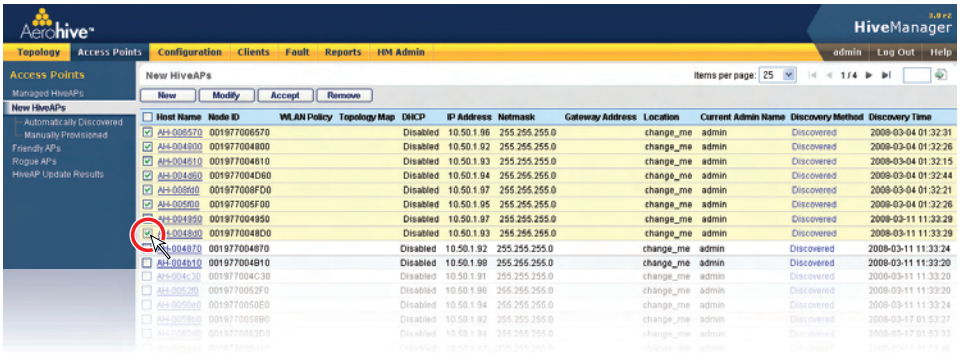
Multiselecting

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

Figure 6 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 **Accept** to accept all the selected HiveAPs for HiveManager management, or click the **Modify** button to configure them with the same settings.



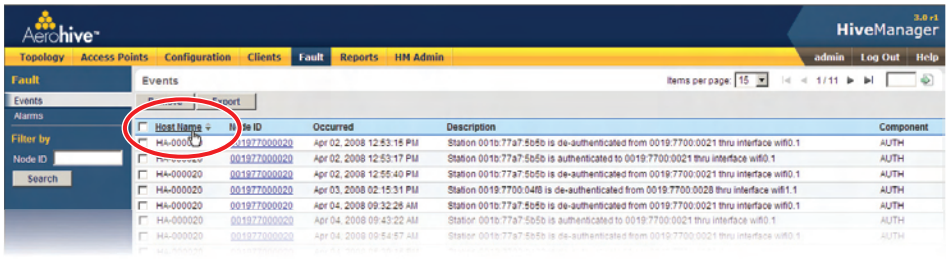
Here, you use the shift-click multiselection method to select a set of the topmost eight HiveAPs in the list; that is, you select the check box for the top HiveAP and hold down the SHIFT key while selecting the check box for the eighth HiveAP from the top.

Sorting Displayed Data

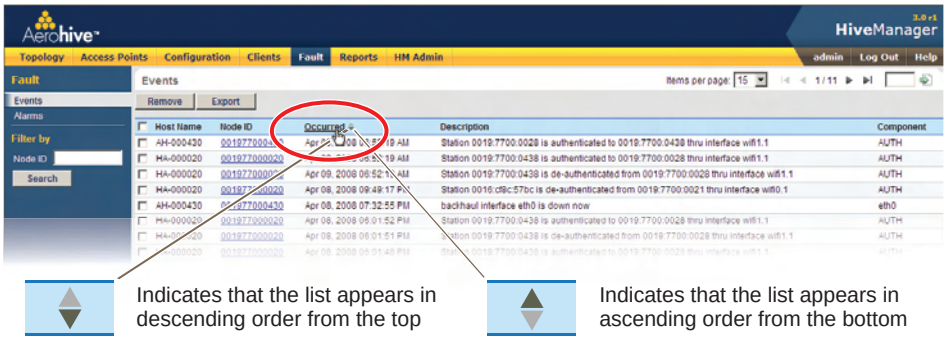
You can control how the GUI displays data in the main panel by clicking a column header. This causes the displayed content to reorder itself alphanumerically or chronologically in either ascending or descending order. Clicking the header a second time reverses the order in which the data is displayed.

Figure 7 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

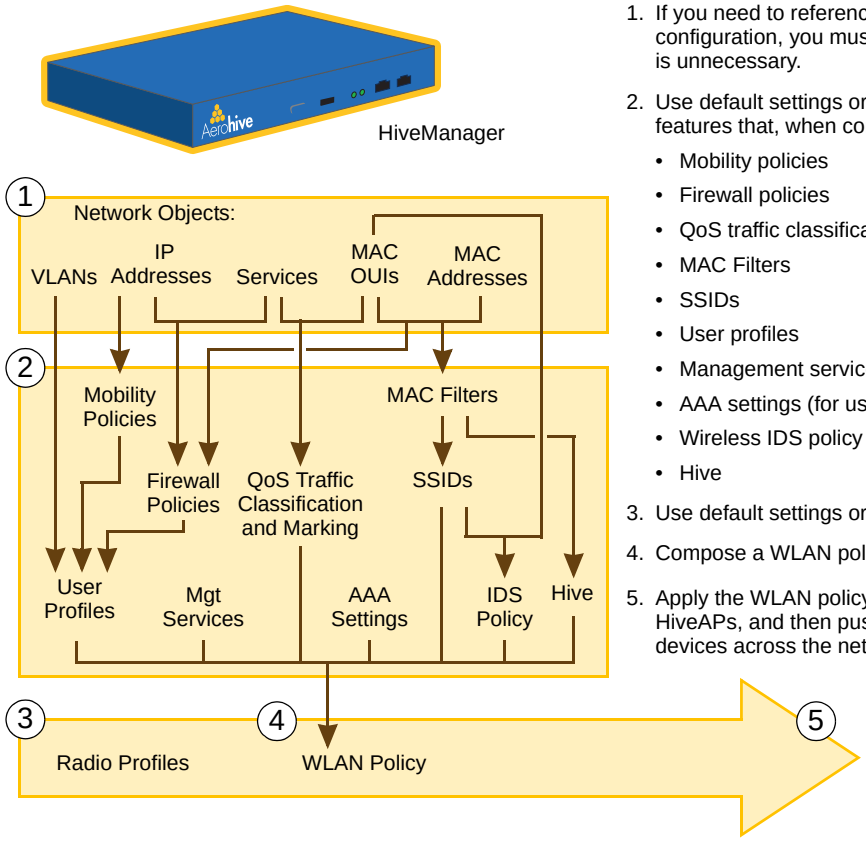
HIVEMANAGER CONFIGURATION WORKFLOW

Assuming that you have already installed your HiveAPs, uploaded maps (see "Setting Up Topology Maps" on page 75), accepted the HiveAPs for management, and decided on the features and settings you want to use, you are now ready to start configuring the HiveAPs through HiveManager[1]. You can configure numerous objects, some of which might need to reference other objects. An efficient configuration strategy is to first define any objects that you will later need to use when configuring others. The typical workflow, shown in Figure 8, proceeds like this:

1. Define network objects. You can then reference them when defining other parts of the configuration. If you do not plan to use network objects, you can skip this step.
2. Configure various features.
3. Define radio profiles (or use default settings).

4 and 5. Compile the features from step 2 into a WLAN policy, assign the radio profiles and WLAN policy to one or more HiveAPs, and then push the configurations to the physical devices on the network.

Figure 8 Configuration Workflow



1. If you need to reference network objects in another part of the configuration, you must define them first. Otherwise, this step is unnecessary.
2. Use default settings or configure new settings for various features that, when combined, constitute a WLAN policy:
   - Mobility policies
   - Firewall policies
   - QoS traffic classification and marking
   - MAC Filters
   - SSIDs
   - User profiles
   - Management services (DNS, NTP, SNMP, syslog, location)
   - AAA settings (for user authentication using IEEE 802.1X)
   - Wireless IDS policy
   - Hive
3. Use default settings or define one or more radio profiles.
4. Compose a WLAN policy by referencing items set in Step 2.
5. Apply the WLAN policy and radio profiles to one or more HiveAPs, and then push the configuration to the physical devices across the network.

1. 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 79.

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 **HM Admin** > **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.
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).*
- *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 **Configuration** > **HiveAP File Management**.
4. On the HiveAP Files page, select **HiveOS Image** for the file type, enter one of the following—depending on how you intend to upload the HiveOS image file to HiveManager—and then click **OK**:

   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 image file, select the file in the "Available Images" list, and then click Remove.

5. Click **Access Points** > **Managed HiveAPs**.
6. In the Managed HiveAPs window, select one or more HiveAPs, and then click **Update > Upload and Activate SW Image**.

   The Upload and Activate SW Image dialog box appears.

7. Enter the following, and then click **Upload**:
   - From the HiveOS Image drop-down list, select the image that you want to load onto managed HiveAPs.
   - In the Activation Time section, select one of the following options, depending on when you want to activate the software—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 software. 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 software and not activate it. The loaded software 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".

- Select the check box for each HiveAP whose software you want to update.

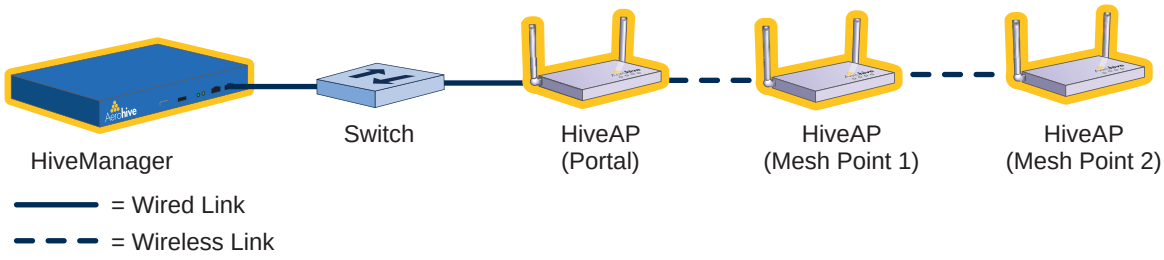
Updating HiveAPs in a Mesh Environment

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 9 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.

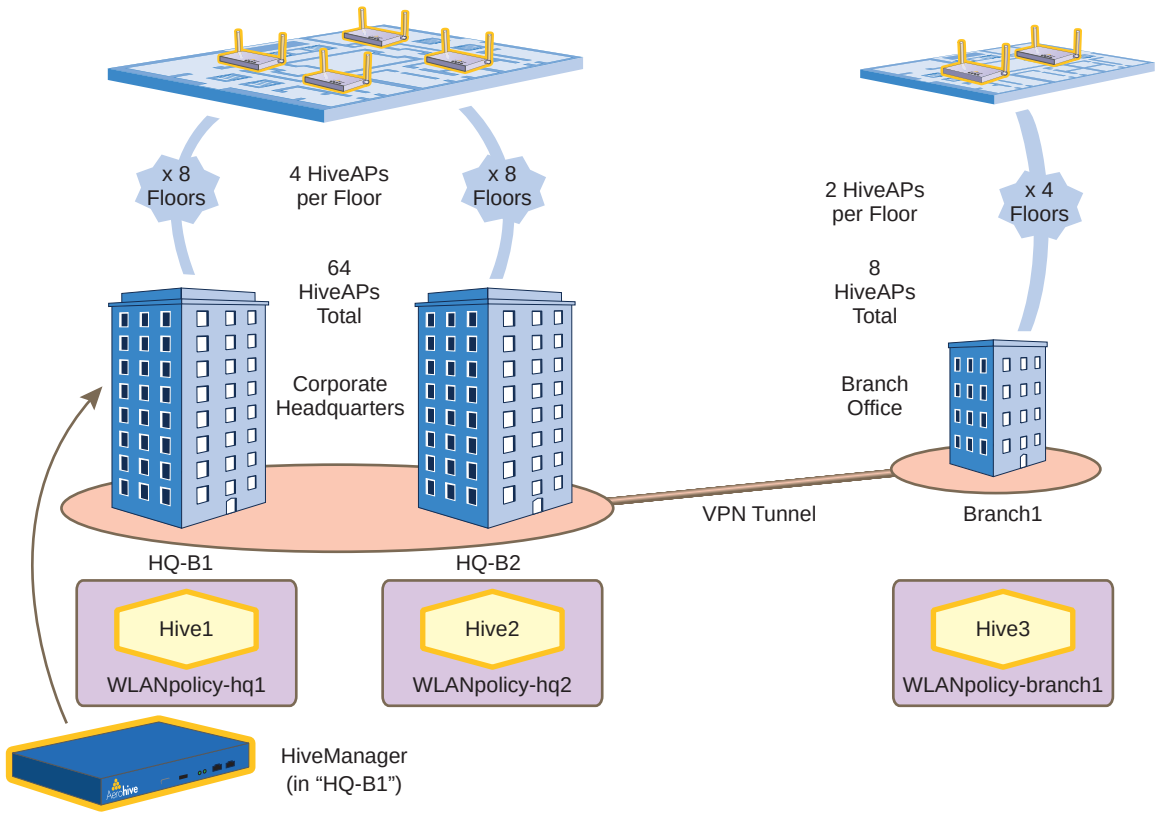
Chapter 7 HiveManager Configuration Examples

The following examples in this chapter show how to install over 70 HiveAPs at three locations in a corporate network, use HiveManager to create configurations for them, and then push the configurations to them over the network. The high-level deployment scheme is as follows:

Headquarters - Building 1 (HQ-B1)	Headquarters - Building 2 (HQ-B2)	Branch Office (Branch1)
32 HiveAPs	32 HiveAPs	8 HiveAPs
1 Hive (hive1)	1 Hive (hive2)	1 Hive (hive3)
1 WLAN policy (WLANpolicy-hq1)	1 WLAN policy (WLANpolicy-hq2)	1 WLAN policy (WLANpolicy-branch1)

The general design of the deployment is shown in Figure 1.

Figure 1 Deployment Overview



You can look at any of the following examples individually to study how to configure a specific feature or view all of them sequentially as a set to study the workflow for deploying large numbers of HiveAPs and configuring them through HiveManager.

This chapter contains a sequential flow of examples that show how to import and organize maps, install HiveAPs on the network and link them to maps, configure typically needed features, assign these features to HiveAPs, and push configurations to the HiveAPs across the network. The examples are as follows:

- "Example 1: Mapping Locations and Installing HiveAPs" on page 75

  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: Defining Network Objects and MAC Filters" on page 81

  Define a MAC OUI (organizationally unique identifier), VLANs, and IP addresses for use by other configuration objects. Define a MAC filter so that QoS classifiers and SSID profiles can reference them. Map the MAC OUI and several services to Aerohive classes.

- "Example 3: Providing Guest Access" on page 88

  Provide controlled and limited network access for guests. Two approaches are presented.

- "Example 4: Creating User Profiles" on page 94

  Define several user profiles, their companion QoS forwarding rates and priorities, and their VLANs.

- "Example 5: Setting SSIDs" on page 98

  Define sets of authentication and encryption services that wireless clients and HiveAPs use when communicating with each other.

- "Example 6: Setting Management Service Parameters" on page 101

  Configure DNS, syslog, SNMP, and NTP settings for HiveAPs.

- "Example 7: Defining AAA RADIUS Settings" on page 104

  Define AAA RADIUS server settings to use when HiveAPs send 802.1X authentication requests.

- "Example 8: Creating Hives" on page 106

  Create hives so that sets of HiveAPs can exchange information with each other over the network to coordinate client access, provide best-path forwarding, and enforce QoS policies.

- "Example 9: Creating WLAN Policies" on page 107

  Define WLAN policies. These are sets of configuration objects (defined in previous examples) that HiveAPs use to control how wireless clients access the network.

- "Example 10: Assigning Configurations to HiveAPs" on page 116

  Assign WLAN policies, radio profiles, and maps to detected HiveAPs so that you can begin managing them through HiveManager.

EXAMPLE 1: MAPPING LOCATIONS AND INSTALLING HIVEAPS

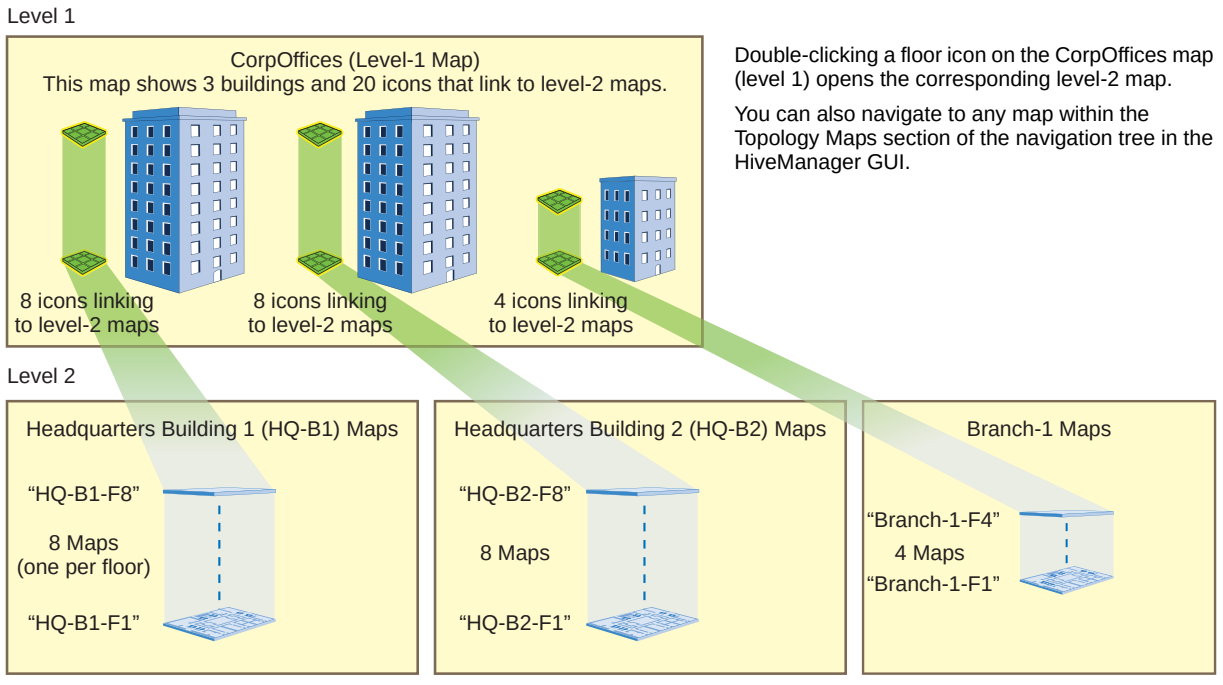
HiveManager allows you to mark the location of HiveAPs on maps so that you can track devices and monitor their status. First, you must upload the maps to HiveManager, and then name and arrange them in a structured hierarchy (see "Setting Up Topology Maps"). After that, you can follow one of two ways to install HiveAPs so that you can later put their corresponding icons on the right maps (see "Preparing the HiveAPs" on page 78).

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

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 of .jpg files of drawings or blueprints showing the layout of each floor. Also, as an easy means of organizing the maps in 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.

Figure 2 Organizational Structure of Level-1 and -2 Maps

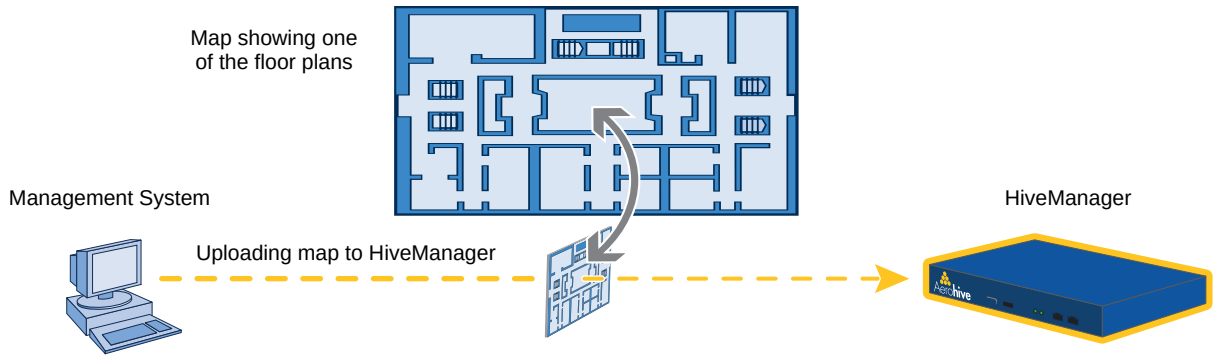


Uploading Maps

1. Log in to the HiveManager GUI as explained in " Installing and Connecting to the HiveManager GUI" on page 63.
2. Click **Topology,** right-click **World**, and then choose **Add/Delete Image** from the pop-up menu that appears.
3. In the Add/Delete Image window, click **Browse**, navigate to the directory containing the image files that you want to upload, and select one of them.
4. Click **Upload**.

The selected image file is transferred from your management system to HiveManager as shown in Figure 3.

Figure 3 Uploading a Map of a Building Floor Plan



5. Repeat this for all the image files that you need to load. In this example, you load 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 "World", and then choose **Edit** from the pop-up menu that appears.
2. In the Edit Map - World dialog box, enter the following, and then click **Update**:
   - Map Name: **CorpOffices** (Note that spaces are not allowed in map level names.)
   - Map Icon: **Building**
   - Background Image: Choose **corp_offices.png** from the drop-down list.
3. Click **Topology**, right-click the top level map "CorpOffices", and then choose **New** from the pop-up menu that appears.
4. In the New Map (Submap for CorpOffices) dialog box, enter the following, and then click **Create**:
   - Map Name: **HQ-B1-F**
   - Map Icon: **Floor**
   - Background Image: Choose **HQ-B1-F1.png** from the drop-down list.

   A white 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.
5. Click **Unlock**, select the icon, drag it to the location you want, and then click **Save**.
6. Click **Topology**, right-click the top level map "CorpOffices", and then choose **New** from the pop-up menu that appears.
7. In the New Map (Submap for CorpOffices) dialog box, enter the following, and then click **Create**:
   - Map Name: **HQ-B1-F2**
   - Map Icon: **Floor**
   - Background Image: Choose **HQ-B1-F2.png** from the drop-down list.

   A white 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.
8. Click **Unlock**, select the icon, drag it to the location you want, and then click **Save**.

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.

9. 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 as many levels as necessary to the map hierarchy. You can also delete maps as long as they do not have any submaps or HiveAP icons on them.

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. With the first 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. The second approach ("Using MAC Addresses" on page 79) 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.

Note: For a summary of how HiveAPs use CAPWAP to discover and connect to HiveManager, see "How HiveAPs Connect to HiveManager" on page 79.

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:
    1. Make a serial connection to the console port, and log in (see "Log in through the console port" on page 130).
    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 the name of a map is not unique, then include the map hierarchy in the string until the path to the map is unique. For example, if you have two maps named "floor-1", and the one you want to use is nested under a higher level map named "building-1" while the other is nested under "building-2", then enter the command as follows: **snmp location northwest_corner@floor-1@building-1**. Similarly, if there are two maps named "building-1" nested under higher level maps for two different sites ("campus-1" and "campus-2", for example), then include that next higher level in the string to make it unique:
       snmp location northwest_corner@floor-1@building-1@campus-1
    3. Mount and cable the HiveAP to complete its installation. (For mounting details, see "Mounting the HiveAP 20" on page 29. For information about the PoE port on the HiveAP, see "Ethernet and Console Ports" on page 26.)

When a HiveAP connects to HiveManager, HiveManager checks its SNMP location. When you accept the HiveAP for management, then HiveManager 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 Access Points > New HiveAPs > Automatically Discovered window in the HiveManager GUI, you can sort detected HiveAPs by map name to assign them more easily to WLAN policies, hives, and radio profiles.

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 you uploaded to HiveManager, label them, and take them with you 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 in the Access Points > New HiveAPs > Automatically Discovered window. 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, a WLAN policy, and two radio profiles.

How HiveAPs Connect to HiveManager

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

When HiveAPs and HiveManager are in different subnets, the HiveAPs will not be able to discover HiveManager 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 configure them so that they can learn it through DHCP or DNS. When HiveAPs have the HiveManager IP address, they then send unicast CAPWAP Discovery Request messages to that address.

- Log in to the CLI on each HiveAP and enter the HiveManager IP address with the following command, in which the variable *ip_addr* is the address of the interface through which HiveManager communicates with HiveAPs:

  hivemanager *ip_addr*

- Configure the DHCP server to supply the HiveManager domain name as DHCP option 225 or its IP address as option 226 in its DHCPOFFER. (If you use a domain name, the authoritative DNS server for that domain must also be configured with an A record that maps the domain name to an IP address for HiveManager.) HiveAPs request DHCP option 225 and 226 by default when they broadcast 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 on each HiveAP with a different option number for the variable number:

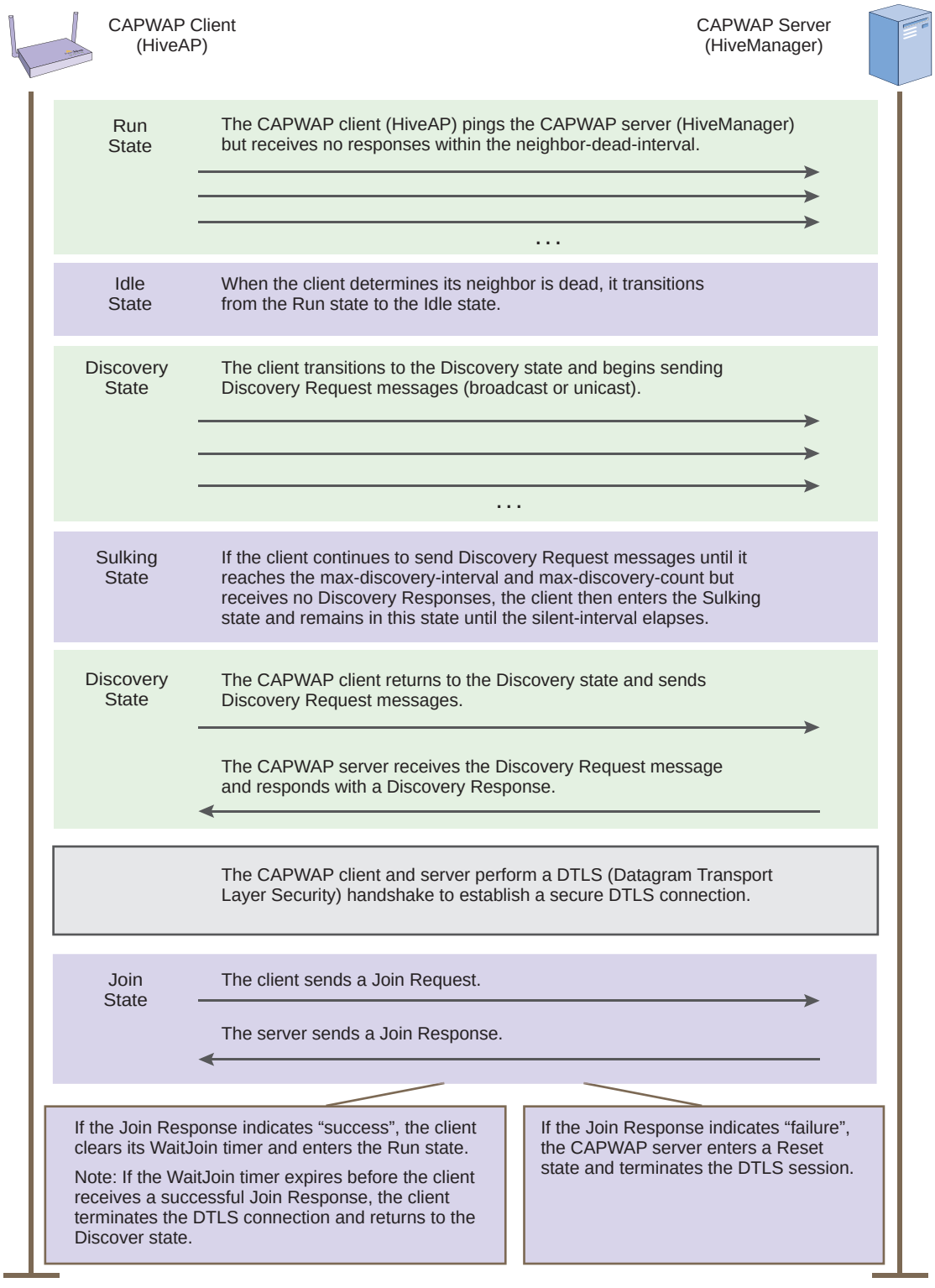
  interface mgt0 dhcp client option custom hivemanager *number* **{ ip | string }**

- If HiveManager continues to use its default domain name ("hivemanager"), configure the local authoritative DNS server with an A record that resolves that name to an IP address. If the HiveAPs do not have a static IP address configured for HiveManager and do not receive an address or domain name returned in a DHCP option, then they try to resolve the domain name "hivemanager" to an IP address.

Within the framework of the CAPWAP protocol, HiveAPs are CAPWAP clients and HiveManager is a CAPWAP server. The client proceeds through a series of CAPWAP states. These states and the basic events that trigger the client to transition from one state to another are shown in Figure 6 on page 80.

Note: To illustrate all possible CAPWAP states, Figure 6 on page 80 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 been configured with (or has discovered) the HiveManager IP address—it begins in the Discovery state.

Figure 6 CAPWAP Process—Beginning from the Run State



EXAMPLE 2: DEFINING NETWORK OBJECTS AND MAC FILTERS

Network objects are the most basic objects that you can configure and only function when other objects such as QoS classifiers, SSID profiles, and firewall policy rules reference them. IP addresses, network services (HTTP, SMTP, FTP, ...), MAC addresses, MAC OUIs (organizationally unique identifiers), VLANs, Ethernet profiles, and radio profiles are network objects that make no reference to any other previously defined object.

You define the following network objects that you reference in other examples later in this chapter:

- MAC OUI for filtering VoIP phone traffic
- VLANs that you can apply to user profiles
- IP addresses that you can assign to management services and RADIUS servers

In addition, you define a MAC filter to control access to the SSID for VoIP traffic.

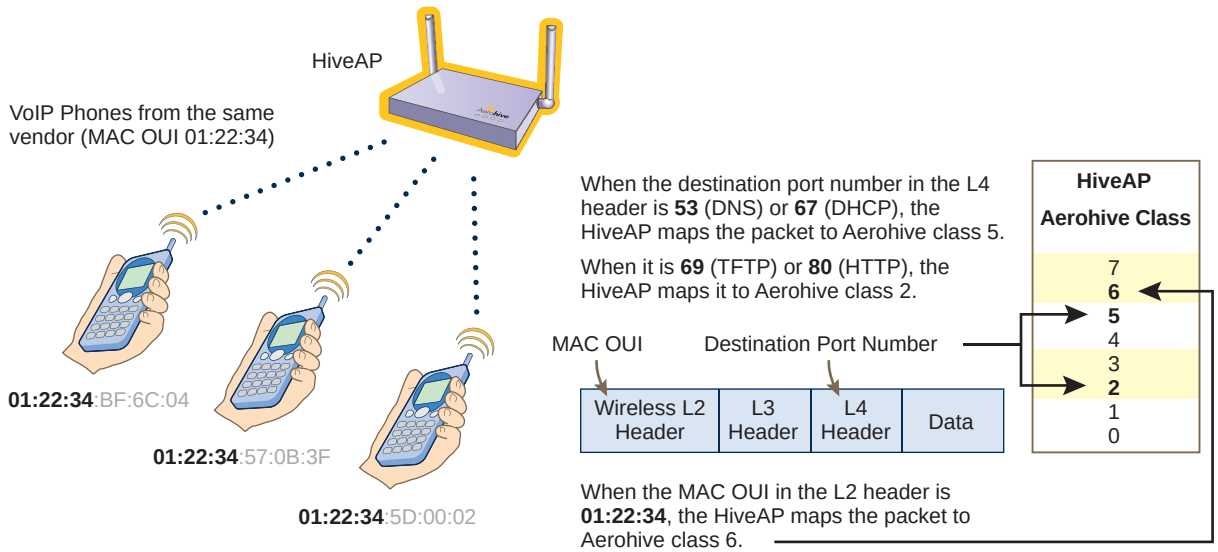
Defining a MAC OUI

You define a MAC OUI for the type of VoIP (Voice over IP) phones in use in the network and assign traffic from it to Aerohive class 6. Other critical IP telephony services are DHCP and DNS for address and domain name assignments, and TFTP and HTTP for configuration downloads and software updates. You map traffic using destination port numbers 53 (DNS) and 67 (DHCP) to Aerohive class 5. This is a fairly high priority level because these services are vital for VoIP to work properly; however, they are not as high as that for the voice traffic itself. Finally, you map traffic using destination port numbers 69 (TFTP) and 80 (HTTP) to Aerohive class 2. This is a much lower priority level, but it is appropriate for these resilient and less time-sensitive services. HiveAPs check if an incoming packet matches a classifier map by checking for matches in the following order. They then use the first match found:

1. Service
2. MAC OUI
3. Ingress interface
4. Existing priorities used by various standard QoS classification systems (802.11e, 802.1p, and DSCP)

After VoIP clients associate with an SSID and begin sending traffic, the HiveAP maps all DNS and DHCP traffic to class 5, all TFTP and HTTP traffic to class 2, and all remaining traffic—voice traffic in this case—to class 6 (see Figure 7).

Figure 7 MAC OUI and Service Classifier Maps for VoIP Phones



By distinguishing voice traffic by the clients' OUI and mapping it to class 6, HiveAPs can prioritize it above other traffic types (see "Example 4: Creating User Profiles" on page 94).

1. Log in to the HiveManager GUI.
2. Click **Configuration** > **Network Objects** > **MAC Addresses/OUIs** > **New**.
3. Enter the following, and then click **Save**:
   - MAC OUI: (**select**)
   - MAC Name: Type a name such as "VoIP_Phones". You cannot include any spaces when defining a MAC name.

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

     - MAC Entry: Type the OUI for the VoIP phones used in the network; that is, type the first six numbers constituting the vendor prefix of the MAC address. For example, if a MAC address is 01:22:34:AB:6C:04, the OUI is 01:22:34. Type only the hexadecimal numerals without any formatting symbols such as colons or dashes. If you do type such symbols, the GUI ignores—and does not display—them.
     - Type: Choose **Global** because you do not need to restrict this network object to a particular set of HiveAPs, which is what the other three options allow you to do.
     - Description: Type a meaningful comment for the MAC OUI, such as the vendor that the OUI identifies.

Note: If there are phones from more than one vendor, make a separate MAC OUI entry for each one.

Mapping the MAC OUI and Services to Aerohive Classes

First, map VoIP phone MAC OUIs to Aerohive class 6. Next, map DNS and DHCP services to Aerohive class 5 and TFTP and HTTP services to class 2. Because voice traffic is the only remaining type of traffic from phones whose MAC OUIs you have already mapped to class 6, HiveAPs map voice traffic from those phones to class 6. Although all these services are critical for IP telephony to function properly, voice traffic is the least resistant to delay, and TFTP and HTTP file downloads are the most resistant. Therefore, you prioritize the different types of traffic accordingly.

1. Click **Configuration** > **QoS Policies** > **Classifiers and Markers** > **New**.

   The New Classifiers and Markers dialog box appears.
2. Enter the following, and then click **Save**:
   - Name: **VoIP-QoS** (You cannot include any spaces when defining a QoS policy name.)
   - Description: Add a descriptive comment, such as "Mapping for VoIP phone traffic".
   - Network Services: (**select**)
   - MAC OUIs: (**select**)
3. Click **Configuration** > **QoS Policies** > **Classifier Maps** > **New** > **General**.

   The New Classifier Maps dialog box appears.
4. Enter the following on the General page:
   - Name: **VoIP-Mapping** (You cannot include any spaces when defining the name of a classifier map.)
   - Description: Add a descriptive comment, such as "Mapping services and OUIs for VoIP phone traffic".
   - Network Services: (**select**)
   - MAC OUIs: (**select**)

5. Click the **Network Services** tab, enter the following, and then click **Apply**:
   - Service: **DNS**
   - QoS Class: **5 - Video**
   - Action: **Permit**
   - Logging: Select the check box to enable HiveAPs to log traffic that matches the service-to-Aerohive class mapping. (HiveAPs log traffic whether the action is permit or deny.) The main use of logging traffic is to see if the HiveAPs are receiving expected—or unexpected—types of traffic when you debug connectivity issues. You can see the log entries in the event log on the HiveAPs (`show logging buffered`). Also, if you configure the HiveAP to send event logs to a syslog server, you can see the log entries there (see "Example 6: Setting Management Service Parameters" on page 101).
6. Enter the following, and then click **Apply**:
   - Service: **DHCP-Server**
   - QoS Class: **5 - Video**
   - Action: **Permit**
   - Logging: Select the check box to enable traffic logging, or clear the check box to disable it.
7. Enter the following, and then click **Apply**:
   - Service: **TFTP**
   - QoS Class: **2 - Best Effort 1**
   - Action: **Permit**
   - Logging: Select the check box to enable traffic logging, or clear the check box to disable it.
8. Enter the following, and then click **Apply**:
   - Service: **HTTP**
   - QoS Class: **2 - Best Effort 1**
   - Action: **Permit**
   - Logging: Select the check box to enable traffic logging, or clear the check box to disable it.
9. Click the **MAC OUIs** tab, click **New**, enter the following, and then click **Apply**:
   - MAC OUIs: Choose the name of the MAC OUI that you defined in "Defining a MAC OUI", such as "VoIP_Phones".
   - QoS Class: **6 - Voice**
   - Action: **Permit**
   - Comment: Enter a meaningful comment about the MAC OUI for future reference.
   - Logging: Select the check box to enable log traffic that matches the MAC OUI-to-Aerohive class mapping, or clear the check box to disable it.
10. To save the configuration and close the dialog box, click **Save**.

Defining VLANs

You define three VLANs that you will later assign to various user profiles (see "Example 4: Creating User Profiles" on page 94). By assigning different VLANs to different user roles, their traffic remains isolated from each other; that is, voice traffic never shares a broadcast domain with data traffic; and data traffic from guests never shares the same broadcast domain with employee data traffic. The result is that you can provide access for certain types of traffic to select areas of the network while blocking unauthorized access to other areas.

The VLAN IDs and the user profiles to which you will assign them are as follows:

- VLAN ID 1 for the Emp and IT user profiles (and for users not yet registered through a captive web portal)[1]
- VLAN ID 2 for the VoIP user profile
- VLAN ID 3 for the Guests user profile

Note: When defining the following VLANs, choose Global as the VLAN type because you do not need to restrict these VLANs to a particular set of HiveAPs, which is what the other three options allow you to do.

1. Click **Configuration > Network Objects > VLANs > New**, enter the following, and then click **Save**:
   - VLAN Name: **VLAN-1-EmployeeData**
   - Enter the following, and then click **Apply**:
     - VLAN ID: **1**
     - Type: **Global**
     - Description: **VLAN for Emp, IT, and unregistered CWP users**
2. Click **Configuration** > **Network Objects** > **VLANs >** (check box) **VLAN-1-EmployeeData > Clone**, make the following changes, and then click **Save**:
   - VLAN Name: **VLAN-2-EmployeeVoice**
   - VLAN ID: **2**
   - Type: **Global**
   - Description: **VLAN for VoIP traffic**
3. Click **Configuration** > **Network Objects** > **VLANs >** (check box) **VLAN-2-VoIP > Clone**, make the following changes, and then click **Save**:
   - VLAN Name: **VLAN-3-Guests**
   - VLAN ID: **2**
   - Type: **Global**
   - Description: **VLAN for guests visiting corporate**

1. There is a predefined VLAN definition for VLAN ID 1, so it is not really necessary to create a new VLAN object for it. However, because later examples in this chapter refer to VLAN 1 by the name defined here ("VLAN-1-EmployeeData"), its purpose will hopefully be clearer than if it were referred to by the simpler name of the predefined VLAN ("1").

Creating IP Addresses

You use the IP addresses that you create here when defining management services for the HiveAPs (see "Example 6: Setting Management Service Parameters" on page 101). The IP addresses are used for DNS, SNMP, syslog, and NTP servers. To understand the locations of the different servers on the network, see Figure 14 on page 101.

DNS Servers

1. Click **Configuration > Network Objects > IP Addresses > New**, and after entering all the following, click **Save**:
   - Address Name: **DNS-Primary**

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

   — IP Address: **10.1.1.25**
   — Netmask: **255.255.255.255**
   — Type: **Classifier**
   — Value: Tag 1: **hq**

   By classifying the IP address definition as "hq" and then later classifying all HiveAPs deployed at headquarters as "hq", only those HiveAPs will use the 10.1.1.25 address for their primary DNS server.

   — Description: **Primary DNS server located at HQ**

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

   — IP Address: **10.2.2.251**
   — Netmask: **255.255.255.255**
   — Type: **Classifier**
   — Value: Tag 1: **branch1**

   By classifying the IP address definition as "branch1" and then later classifying all HiveAPs deployed at the branch site as "branch1", only those HiveAPs will use the 10.2.2.251 address for their primary DNS server. Classifying the different IP address definitions within the same IP address object allows you to use this one object in multiple locations that have different addressing schemes.

2. Click **Configuration > Network Objects > IP Addresses > New**, and after entering all the following, click **Save**:
   - Address Name: **DNS-Secondary**

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

   — IP Address: **10.1.1.26**
   — Netmask: **255.255.255.255**
   — Type: **Global**

   Because all the HiveAPs at both the headquarters and branch site use the same secondary DNS server, you classify it as Global. The server is located at headquarters and HiveAPs at the branch site reach it through a VPN tunnel.

   — Description: **Secondary DNS server located at HQ**

Syslog Server

Click **Configuration > Network Objects > IP Addresses > New**, and after entering all the following, click **Save**:

- Address Name: **Syslog-Server**

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

— IP Address: **10.1.1.23**

  - Netmask: **255.255.255.255**
  - Type: **Global**

    Because all the HiveAPs at both the headquarters and branch site use the same syslog server, you classify it as Global. The HiveAPs at the branch site reach the syslog server, which is also located at headquarters, through a VPN tunnel.
  - Description: **Syslog server at HQ**

SNMP Server

Click **Configuration > Network Objects > IP Addresses >** (check box) **Syslog-Server > Clone**, change the following settings, click **Save**:

- Address Name: **SNMP-Server**
  - IP Address: **10.1.1.24** (This is the IP address of the SNMP management system to which the SNMP agent running on the HiveAPs sends SNMP traps.)
  - Description: **SNMP server at HQ**

NTP Server

Click **Configuration > Network Objects > IP Addresses >** (check box) **SNMP-Server > Clone**, change the following settings, click **Save**:

- Address Name: **NTP-Server**
  - IP Address: **207.126.97.57**
  - Description: **NTP admin wjones@time.org**

RADIUS Servers

1. Click **Configuration > Network Objects > IP Addresses > New**, and after entering all the following, click **Save**:
   - Address Name: **RADIUS-Server-Primary**

   Enter the following, and then click **Apply**:
   - IP Address: **10.1.1.15**
   - Netmask: **255.255.255.255**
   - Type: **Global**

     Because all the HiveAPs at both the headquarters and branch site use the same RADIUS servers, you classify them as Global. The HiveAPs at the branch site reach the RADIUS servers, which are also located at headquarters, through a VPN tunnel.
   - Description: **Primary RADIUS server at HQ**
2. Click **Configuration > Network Objects > IP Addresses >** (check box) **RADIUS-Server-Primary > Clone**, and after making the following changes, click **Save**:
   - Address Name: **RADIUS-Server-Secondary**
     - IP Address: **10.1.2.16**
     - Description: **Secondary RADIUS server at HQ**

Creating a MAC Filter

A MAC filter is a type of security policy that you can apply to an SSID to allow or deny access to clients attempting to form associations based on their source MAC addresses. In this example, you define a MAC filter based on the VoIP phone OUI and apply it to the SSID to which you want VoIP clients to associate. HiveAPs can then filter association requests and respond only to clients whose OUI matches that in the filter (see "Example 5: Setting SSIDs" on page 98).

The MAC filter that you create here becomes useful when you define the SSID for voice traffic (see "voip SSID" on page 99). You apply this filter to the SSID so that only VoIP phones with the MAC OUI 01:22:34 can form an association with the HiveAPs.

1. Click **Configuration** > **Security Policies** > **MAC Filters** > **New**.

   The New MAC Filters dialog box appears.

2. Enter the following name and description for the MAC filter:
   - Name: **corpVoIPphones** (You cannot include any spaces when defining a MAC filter name.)
   - Description: **Use this filter for "voip" SSID**

   Choose the name that you gave the OUI, such as "VoIP_Phones" (see "Defining a MAC OUI" on page 81) from the MAC Address/OUI drop-down list, choose **Permit** as the action, and then click **Apply**.

3. To save the MAC filter configuration and close the dialog box, click **Create**.

EXAMPLE 3: PROVIDING GUEST ACCESS

As a convenience for guests visiting the corporate headquarters or branch office, you provide them with wireless network access. To preserve bandwidth for employees, the rate limit for guests is somewhat minimized. To maintain security, visitors are restricted to accessing just the public LAN.

Two approaches are presented in this section:

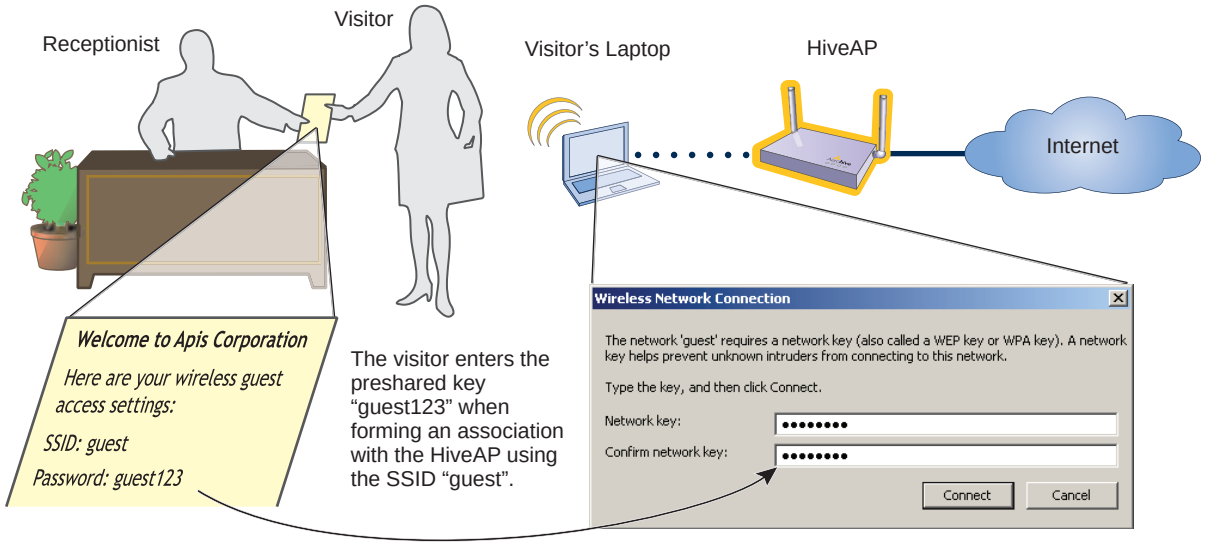
- "Guest Access with Preshared Keys": This approach provides visitors with secured network access by using WPA or WPA2 with preshared keys and TKIP or CCMP (AES) encryption. It does not include a means for enforcing visitors to accept a network usage policy before receiving network access.
- "Guest Access with Captive Web Portal" on page 89: A captive web portal is a way to control network access by requiring users to authenticate or register before assigning them network and user profile settings that allow them network access beyond the HiveAP with which they associated. With this approach, registered visitors' activity can be tracked and stored in historical logs on a syslog server for security and compliance auditing.

For the first approach, no extra configuration is necessary other than configuring a guest user profile and SSID. For the second approach, you might want to customize the registration form used on the captive web portal. To do that, see "Customizing the Registration Page" on page 90 and "Loading Customized Captive Web Portal Files" on page 92.

Guest Access with Preshared Keys

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 8.

Figure 8 Guest Access Using a Preshared Key

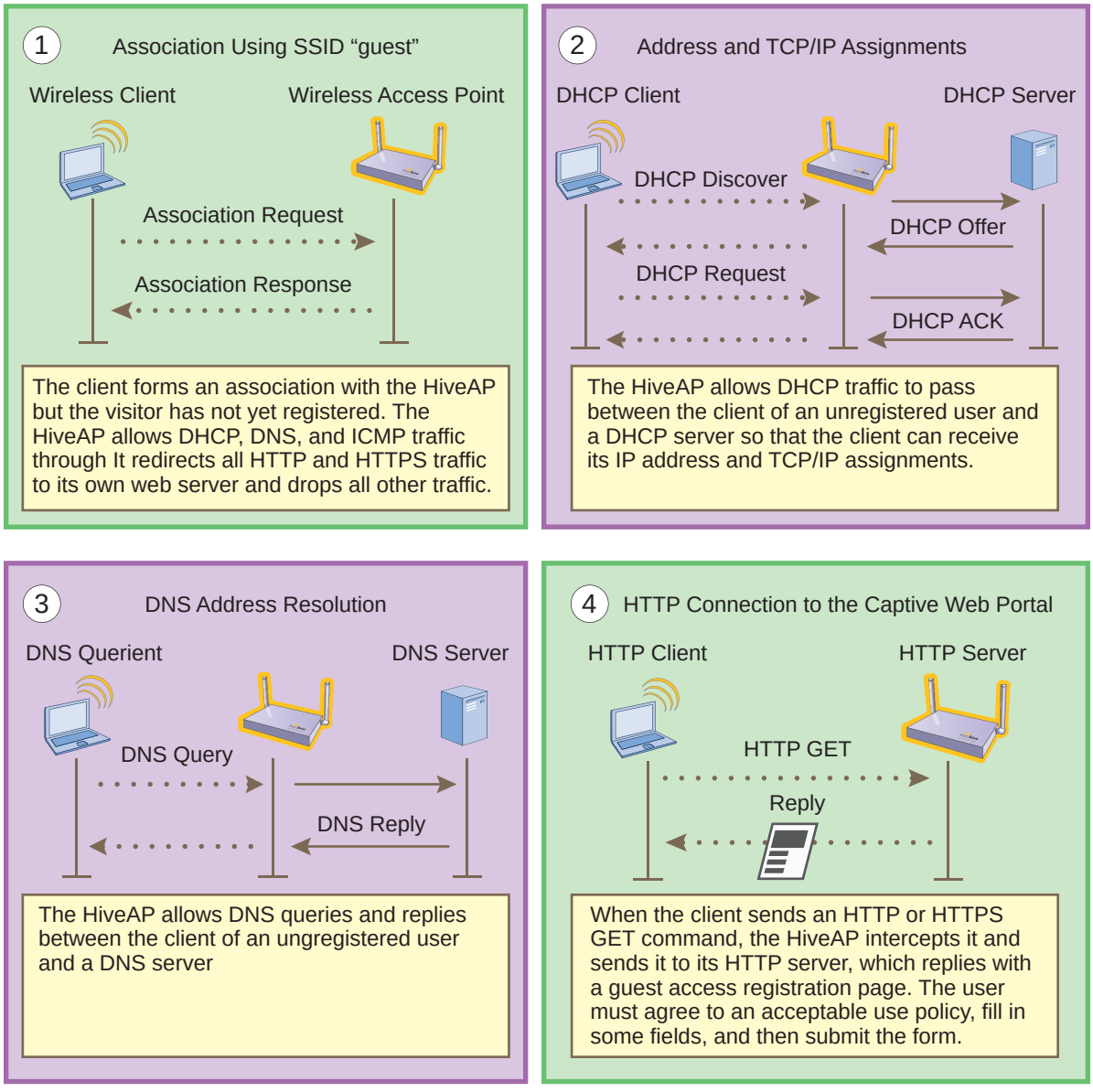


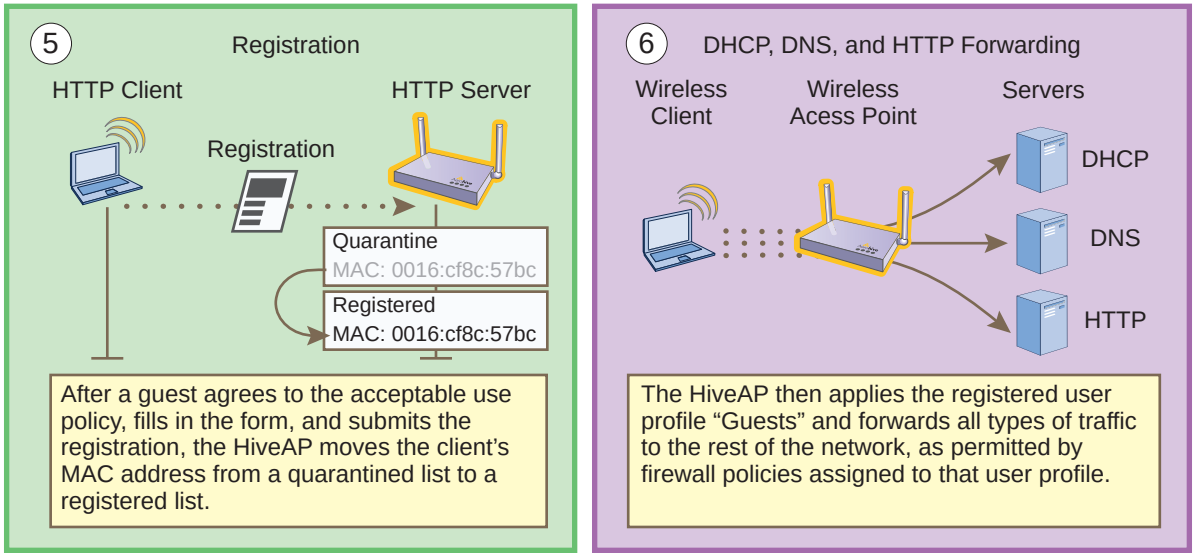
The guest SSID provides secure network access for visitors. Also, by linking visitors to the guest SSID, you can differentiate them from employees—who associate with other SSIDs (voip and corp)—so that you can apply one set of QoS (Quality of Service) settings for visitors and other settings for employees. In addition, the user profiles for employees and guests further separate their traffic into two different VLANs. For instructions on setting up guest access with a preshared key, see "Guests QoS and User Profile" on page 96 and "guest SSID" on page 100.

Guest Access with Captive Web Portal

A captive web portal provides registered users with network access while containing unregistered users. When the client of a previously unregistered visitor first associates with the guest SSID, the HiveAP assigns the "Unregistered-Guests" user profile to the visitor. It 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 "Guests" 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 9.

Figure 9 Captive Web Portal Exchanges





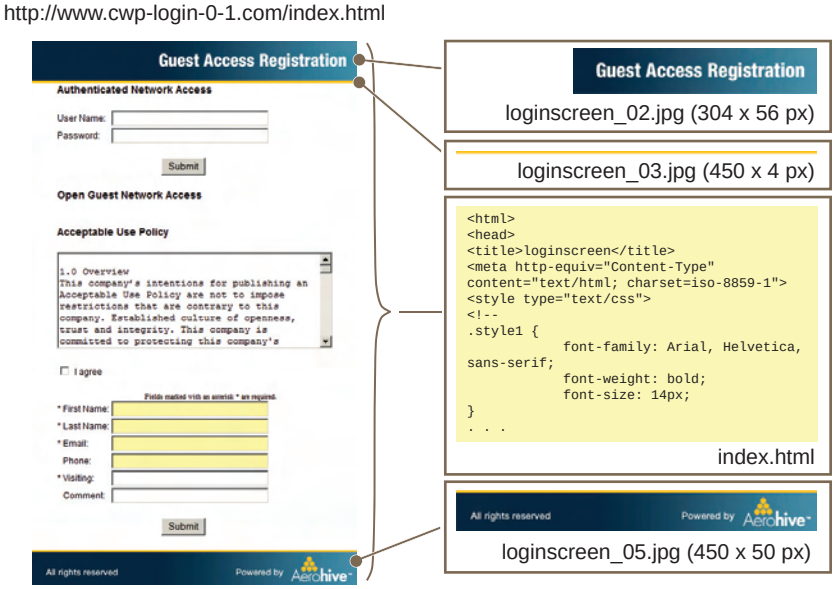
Note: Unlike the captive web portal implementation in earlier HiveOS releases where you can assign different VLANs to the unregistered and registered user profiles, in HiveOS 3.0r2 they must use the same VLAN.

Customizing the Registration Page

Although Aerohive provides .html and .jpg files for use on the captive web portal server, you might want to customize them to better suit your organization. There are six files, four of which are shown in Figure 10:

- index.html (the main registration page)
- success.html (page that appears after registering)
- reg.php (script stored on internal web server)
- loginscreen_02.jpg (image at the top of web pages)
- loginscreen_03.jpg (yellow line near top of web pages)
- loginscreen_05.jpg (image at bottom of index.html)

Figure 10 Captive Web Portal Registration Page



To modify the registration page, do the following:

1. Set up a captive web portal on an SSID.
2. Acting as a client, make an association with that SSID.
3. When you see the registration page in your browser, save it and its accompanying images.
4. Use a graphics program to create new .jpg images.
5. Use a text editor to modify the text in the index.html file.
6. Upload the files to the HiveAP.

Note: The resolution for all images is 96 dpi. The bit depth is 24.

Unregistered users' browsers are redirected to the registration page (index.html) of the captive web portal for the SSID to which they associate (the guest SSID in the examples here). You can have a different registration page for each SSID.

To access the default set of .html and .jpg files on a HiveAP, do the following:

1. Configure a guest SSID as explained in "guest SSID" on page 100 and complete the rest of the HiveAP steps explained in this chapter to bring a HiveAP under HiveManager management.

   Note: An alternative approach is to log in to the console port of an individual HiveAP that you have connected to the network—see "Step 1 Log in through the console port" on page 130—and enter the following commands:

   ```
   ssid guest
   ssid guest security additional-auth-method captive-web-portal
   interface wifi0 ssid guest
   save config
   ```

2. Position your management system near the HiveAP and form an association with it using the guest SSID.
3. Open a web browser. When it tries to open its home page, the HiveAP intercepts the HTTP traffic and redirects it to the captive portal web server.
4. Save the registration page to your local system. In Microsoft Internet Explorer®, for example, click **File** > **Save As**, name it *index*, and in the Save as type field, choose **Webpage, complete (*.htm, *.html)**.
5. Open the directory where you saved the index.html file.

   In addition to the index.html file, there is also an images directory containing the three .jpg files that index.html references: loginscreen_02.jpg, loginscreen_03.jpg, and loginscreen_05.jpg.
6. Because the directory structure in the HiveAP is different, move the three .jpg files to the same directory as index.html. Optionally, delete those three images and create your own new images, saving them in the same directory as the index.html file.
7. Open index.html with a text editor and make the following changes:
   - Remove the string `index_files/` from the image source definitions of the three images:

     ```
     <img src="index_files/loginscreen_02.jpg" width="304" height="56" alt="">
     <img src="index_files/loginscreen_03.jpg" width="450" height="4" alt="">
     <img src="index_files/loginscreen_05.jpg" width="450" height="50" alt="">
     ```

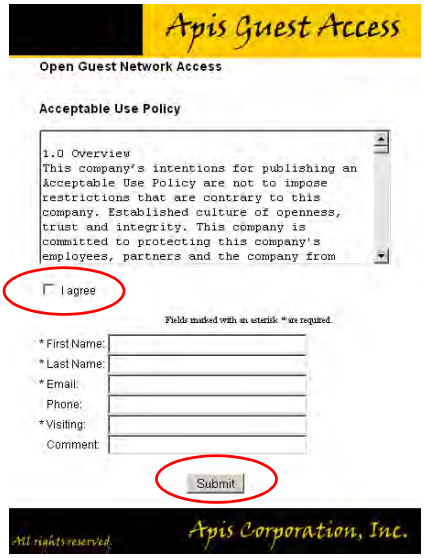
     Note: When working on image files, make sure that they match the above dimensions.

   - To change the color in the bar in the upper left corner, find `<td width="146" bgcolor="002740">` and enter a different color definition. For example, to make it black, enter `"000000"`.
   - If you want to change the acceptable use policy, find the section that begins with the words `"1.0 Overview"`, and then either replace the text with your own policy or edit the existing one.
   - To remove the Authenticated Network Access section at the top of the page, delete the HTML code from "`<FORM name=form2 action=reg.php method=post>`" to "`</DIV></FORM>`".

     Note: If you want to use the Authenticated Network Access section to authenticate employees through the captive web portal, store their user accounts on the RADIUS server that you configure in "Example 7: Defining AAA RADIUS Settings" on page 104. The HiveAPs hosting the captive web portal will forward their user name and password entries to that RADIUS server for the authentication check.

Figure 11 on page 92 shows the result of editing the text in the acceptable use policy, changing the color in the top left bar in the index.html file, creating two new images for loginscreen_02.jpg and loginscreen_05.jpg, and removing the Authenticated Network Access section.

Figure 11 Modified Registration Page



Notes

The default registration page contains two forms: an upper form for user authentication (through an external RADIUS server) and a lower form for user registration. In this example, you remove the upper form so that the page is simply for guest registration.

The total number of fields in the customized file shown here is the same as that in the default index.html file. If you want, you can edit the HTML code to change the number of required and optional fields. (Fields identified as "INPUT id=field<number>" are required, and "INPUT id=opt_field<number>" are optional.) If you change the number of fields in the HTML code, you must also change them in the captive web portal section of the SSID configuration.

There are two elements that cannot be removed from this file: the "I agree" check box—and its name must remain as “checkbox” in the code—and the Submit button.

8. To edit the "Successful Registration" page, which follows the registration page, click **I agree**, fill in the fields, and then click **Submit Query**.

   The browser opens the "Successful Registration" page.

9. Save the page as a file named success.html to the same directory as the index.html file.
10. Open it with a text editor, make your changes, and then save the modified file.

Loading Customized Captive Web Portal Files

To load your edited or new files onto one or more HiveAPs, you first create a directory on HiveManager and then upload the files from your management system or SCP (Secure Copy) server into that directory. From there, you can send the files to one or more managed HiveAPs when you push the configuration that references the files.

To create a directory on HiveManager and upload files into it, do the following:

1. In the HiveManager GUI, click **Configuration** > **HiveAP File Management**.
2. In the HiveAP File Management window, select **Captive Portal Page** for file type.

   Two display areas (Available Directories and Available CWP Files) and a new field (Directory Name) appear.

3. In the Directory Name field, type a name such as **guestCWP**, and then click **Create**.

   A directory named "guestCWP" appears in the Available Directories list.

4. Depending on how you upload the files, select **guestCWP**, enter one of the following, and then click **Upload**:

   To load files from a directory on your local management system:

   - Local File: (**select**); type the directory path and a file name; or click **Browse**, navigate to one of the files, and select it.

or

To load a 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 directory path and file name. If the files are 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.

Note: After you load a file, it appears in the Available CWP Files display area. If you accidentally load the wrong file, select the file name and then click Remove.

5. Repeat either the Local or SCP method of uploading each file you need into the guestCWP directory.

Defining a Captive Web Portal

Define the following captive web portal for use when creating an SSID for guest registration (see "guest SSID" on page 100). The definition below references the web directory "guestCWP" and the HTML files that you modified and uploaded in the previous section—login.html and success.html.

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

- Name: **CWP-guest1**
- Description: **Captive web portal for guest registration**
- Use default file settings: (**clear**)
- Web Files Directory: **guestCWP**
- Web Page Name: **login.html**
- Result Page Name: **success.html**

Perform the following tasks to finish setting up the captive web portal:

- Configure two user profiles—one for successfully registered users and another for the unsuccessful (see "Guests QoS and User Profile" on page 96 and "Unregistered-Guests QoS and User Profile" on page 97)
- Configure an SSID with captive web portal functionality (see "guest SSID" on page 100)
- Link the user profiles to the SSID in a WLAN policy (see "Example 9: Creating WLAN Policies" on page 107)
- Push the files and configuration to managed HiveAPs on which you want to run the portal (see "Example 10: Assigning Configurations to HiveAPs" on page 116)

Note: You can also use the Aerohive GuestManager to provide network access to wireless visitors. An administrator, called an operator, sets up visitors' account on GuestManager. Then GuestManager uses its built-in RADIUS server to authenticate those users. For more information, see the Aerohive GuestManager Getting Started Guide.

EXAMPLE 4: CREATING USER PROFILES

User profiles contain a grouping of settings that determine the QoS (Quality of Service), VLAN, firewall policies, and mobility policy that you want HiveAPs to apply to traffic from a specific group of users. In this example, you define user profiles and their companion QoS forwarding rates and VLANs for VoIP phone users ("VoIP"), IT staff ("IT"), corporate employees ("Emp"), and corporate visitors ("Guests"[2]). The user profile settings, maximum traffic forwarding rates per user, and the VLAN for each profile are shown in Figure 12.

Note: 802.11n radio options appear in anticipation of an upcoming release. They are not yet functional.

Figure 12 User Profiles, Forwarding Rates per User, and Default VLANs

User Profiles	Maximum Data Forwarding Rates per User	Default VLANs
Name: VoIP Attribute: 2	512 Kbps	2
Name: IT Attribute: 3	54000 Kbps	1
Name: Emp Attribute: 4	54000 Kbps	1
Name: Guests Attribute: 5	2000 Kbps	3

Notes: Because individual VoIP calls use relatively little bandwidth (~128 Kbps, depending on the voice compression codex used), a single VoIP user does not need as much bandwidth as a user transmitting other types of traffic.

Corporate employees—IT and Emp—receive the highest maximum data forwarding rates.

Guests receive enough bandwidth to satisfy basic network access but not enough to interfere with employee traffic.

Regarding VLAN assignments, each user role is securely isolated in its own VLAN (IT and Emp being divisions within the larger role of employee). Note: The link connecting the HiveAP Ethernet interface to the interface on the connecting switch must be an 802.1Q trunk port configured to allow traffic on these VLANs from the HiveAPs.

VoIP QoS and User Profile

1. Click **Configuration > QoS Policies > Rate Control & Queuing > New**, enter the following, and then click **Save**:
   - Name: **QoS-VoIP**
   - Per User Rate Limit (for 802.11 a/b/g): **512** Kbps

     This is the maximum amount of bandwidth that a single user belonging to this profile can use. It supports a single 128-Kbps VoIP session—depending on the voice codec used—while reserving bandwidth for other required telephony services.
   - Description: Enter a useful comment for future reference, such as "QoS for VoIP traffic per user".
   - Per User Queue Management: Enter the following items that appear in **bold**:

Class Number - Name	Scheduling Type	Scheduling Weight	Weight % (Read Only)	Policing Rate Limit (Kbps) (802.11a/b/g)
7 - Network Control	Strict	0	0%	**128**
6 - Voice	Strict	0	0%	**128**
5 - Video	Weighted Round Robin	60	28%	**512**
4 - Controlled Load	Weighted Round Robin	50	23%	**512**
3 - Excellent Effort	Weighted Round Robin	40	19%	**512**

2. For guest access using a captive web portal, there must be two user profiles: one for guests that register successfully ("Guests") and another for guests have not registered or whose registration attempt failed ("Unregistered-Guests").

Class Number - Name	Scheduling Type	Scheduling Weight	Weight % (Read Only)	Policing Rate Limit (Kbps) (802.11a/b/g)
2 - Best Effort 1	Weighted Round Robin	30	14%	**512**
1 - Best Effort 2	Weighted Round Robin	20	9%	**512**
0 - Background	Weighted Round Robin	10	4%	**512**

Because you use strict rate limiting for voice traffic, it is always assured the maximum bandwidth rate of 128 Kbps—even if the VoIP phone is updating its software or is otherwise engaged in activity other than voice traffic. The other telephony services (DHCP and DNS mapped to Aerohive class 5, and HTTP and TFTP mapped to class 2) can function at the remaining bandwidth rate.

Note: The default rate limit for Aerohive class 6 (voice) is 512 Kbps, which is large enough to support conference calls, but for typical one-to-one communications, 128 Kbps is sufficient.

2. Click **Configuration** > **User Profiles** > **New > General**, enter the following, and then click **Save**:
   - Name: **VoIP** (You cannot include any spaces when defining a user profile name.)
   - Attribute: **2**

     Each user profile must have a unique attribute number. When using a local authentication mechanism, this attribute links the profile to an SSID so that the HiveAP applies the QoS settings for the profile to all traffic using that SSID.
   - Attribute Group: Leave this field empty.

     An attribute group is a way to assign various RADIUS users with different attribute numbers to the same user profile. Because VoIP users are not authenticated from a RADIUS server, this option is not applicable here.
   - QoS Setting: **QoS-VoIP**
   - Default VLAN: **VLAN-2-EmployeeVoice** (previously defined; see "Defining VLANs" on page 84)

     HiveAPs assign users matching the VoIP user profile to VLAN 2. This separates all employee voice traffic from employee data traffic, which will be on VLAN 1. Guest traffic will be on VLAN 3, separating it from both employee data and voice traffic.
   - Description: **Employees using VoIP**

IT Staff QoS and User Profile

1. Click **Configuration > QoS Policies > Rate Control & Queuing > New**, enter the following, and then click **Save**:
   - Name: **QoS-ITdata**
   - Per User Rate Limit (for 802.11 a/b/g): **54000** Kbps (default)

     This is the maximum amount of bandwidth that a single user belonging to this profile can use. It is the maximum so that even if only one IT staff member is on the network, he or she can use all the available bandwidth if needed.
   - Description: **QoS per IT staff member**
   - Per User Queue Management: Keep all the settings at their default values.
2. Click **Configuration** > **User Profiles** > **New > General**, enter the following, and then click **Save**:
   - Name: **IT** (You cannot include any spaces when defining a user profile name.)
   - Attribute: **3**

     Because the attribute number for the def-user and VoIP user profiles are 1 and 2, enter "3" here. This number can be any unique number from 3 to 63. Because you will later map this profile to an SSID that uses IEEE 802.1X authentication, you must configure the user profile attribute that you set here as an attribute on the RADIUS server as explained in "RADIUS Server Attributes" on page 105.

- Attribute Group: Leave this field empty.
- QoS Setting: **QoS-ITdata**
- Default VLAN: **VLAN-1-EmployeeData** (previously defined; see "Defining VLANs" on page 84)

  HiveAPs assign users matching the IT user profile to VLAN 1. This separates all employee data traffic from employee voice traffic, which will be on VLAN 2. Guest traffic will be on VLAN 3, separating it from both employee data and voice traffic.
- Description: **IT staff**

Emp (Employees) QoS and User Profile

1. Click **Configuration > QoS Policies > Rate Control & Queuing >** (check box) **QoS-ITdata > Clone**, change the following settings, and then click **Save**:
   - Name: **QoS-EmployeeData**
   - Description: **QoS per regular employee**
   - Per User Queue Management: Keep all the settings at their default values.

   Note: Although the "per user rate limit" and the "per user queue management" settings are the same as those for QoS-ITdata, you must create this QoS profile so that you can later assign different weights to QoS-ITdata and QoS-EmployeeData (see "Example 9: Creating WLAN Policies" on page 107).

2. Click **Configuration** > **User Profiles >** (check box) **IT > Clone**, make the following changes, and then click **Save**:
   - Name: **Emp** (You cannot include any spaces when defining a user profile name.)
   - Attribute: **4**

     Because the attribute numbers for the def-user, VoIP, and IT profiles are 1, 2, and 3 respectively, enter "4" here. This number can be any unique number from 4 to 63. Because you will later map this profile to an SSID that uses IEEE 802.1X authentication, you must configure the user profile attribute set here as an attribute on the RADIUS server as explained in "RADIUS Server Attributes" on page 105.
   - QoS Setting: **QoS-EmployeeData**
   - Description: **Regular employees**

Guests QoS and User Profile

1. Click **Configuration > QoS Policies > Rate Control & Queuing > New**, enter the following, and then click **Save**:
   - Name: **QoS-Guests**
   - Per User Rate Limit (for 802.11 a/b/g): **2000** Kbps

     This is the maximum amount of bandwidth that a single user belonging to this profile can use. It is far less than that for employees, but should be sufficient for basic Internet and e-mail access.
   - Description: **QoS per guest**
   - Per User Queue Management: Enter the following items in **bold**. Leave all other cloned settings unchanged.

Class Number - Name	Scheduling Type	Scheduling Weight	Weight % (Read Only)	Policing Rate Limit (Kbps) (802.11a/b/g)
7 - Network Control	Strict	0	0%	**64**
6 - Voice	Strict	0	0%	**64**
5 - Video	Weighted Round Robin	60	28%	**2000**
4 - Controlled Load	Weighted Round Robin	50	23%	**2000**

Class Number - Name	Scheduling Type	Scheduling Weight	Weight % (Read Only)	Policing Rate Limit (Kbps) (802.11a/b/g)
3 - Excellent Effort	Weighted Round Robin	40	19%	**2000**
2 - Best Effort 1	Weighted Round Robin	30	14%	**2000**
1 - Best Effort 2	Weighted Round Robin	20	9%	**2000**
0 - Background	Weighted Round Robin	10	4%	**2000**

2. Click **Configuration** > **User Profiles >** (check box) **Emp > Clone > General**, enter the following, and then click **Save**:
   - User Profile Name: **Guests**
   - Attribute: **5**

     Each user profile must have a unique attribute number. Because the attributes for the def-user, VoIP, IT, and Emp profiles are 1, 2, 3, and 4 respectively, enter "5" here. This number can be any unique number from 5 to 63.
   - Attribute Group: Leave this field empty.
   - QoS Setting: **QoS-Guests**
   - Default VLAN: **VLAN-3-Guests** (previously defined; see "Defining VLANs" on page 84)

     HiveAPs assign users matching the VoIP user profile to VLAN 2. This separates all employee voice traffic from employee data traffic, which will be on VLAN 1. Guest traffic will be on VLAN 3, separating it from both employee data and voice traffic.
   - Description: **Visiting guests**

Unregistered-Guests QoS and User Profile

Enter the following if you are using the captive web portal approach for providing guest access (see "Guest Access with Captive Web Portal" on page 89). A HiveAP applies this profile to users who have not yet registered, or do not successfully register, through the captive web portal.

Click **Configuration** > **User Profiles >** (check box) **Guests > Clone > General**, enter the following, and then click **Save**:

- User Profile Name: **Unregistered-Guests**
- Attribute: **6**

  Because each user profile attribute number must be unique and 1 – 5 have already been assigned, enter "6" here. This number can be any unique number from 6 to 63.
- Attribute Group: Leave this field empty.
- QoS Setting: **QoS-Guests**
- QoS Setting: **VLAN-3-Guests**
- Description: **CWP unregistered guests**

Note: So that the clients of registered users can continue to use the network settings that they received while they were still unregistered, you must configure both the Guests and Unregistered-Guests profiles with the same VLAN.

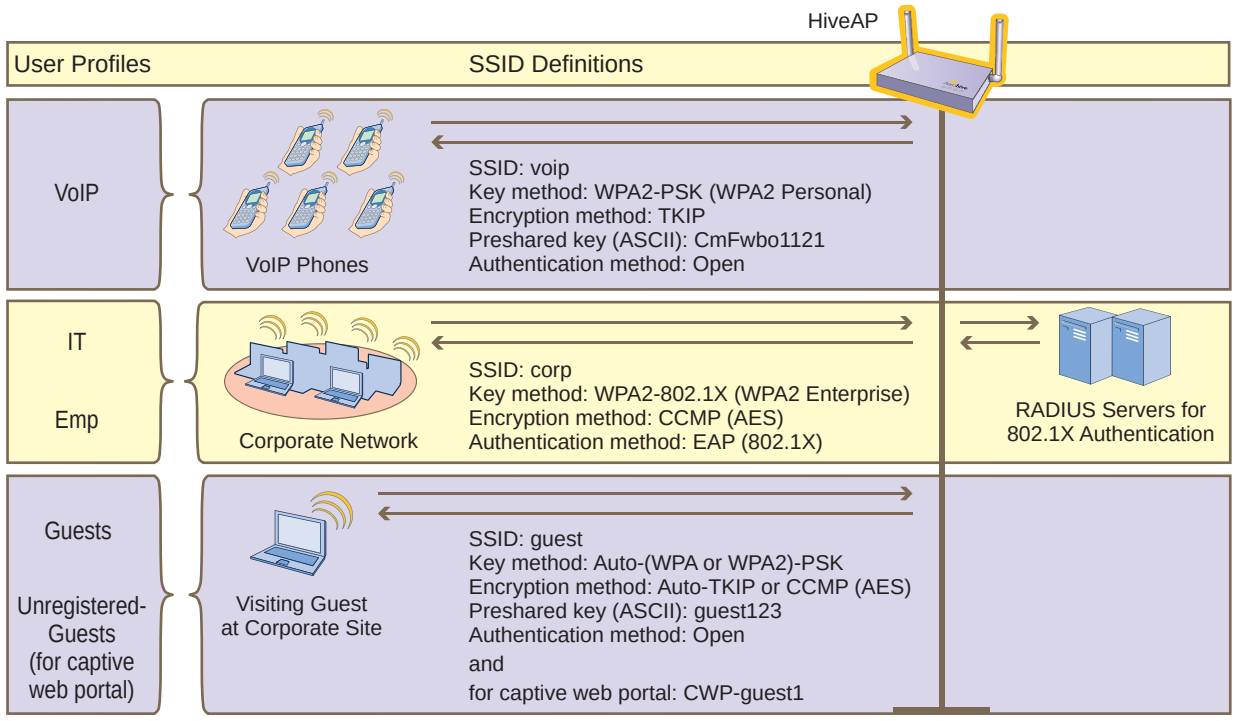
EXAMPLE 5: SETTING SSIDS

An SSID (service set identifier) is an alphanumeric string that identifies a set of authentication and encryption services that wireless clients and access points use when communicating with each other. In this example, you define the following three SSIDs, which are also shown in Figure 13:

SSID Name	Security Protocol	Other
voip	Key method: WPA2-PSK Encryption method: TKIP Preshared key (ASCII): CmFwbo1121 Authentication method: Open	A MAC filter restricts access only to VoIP phones specified in the filter.
corp	Key method: WPA2-EAP (802.1X) Encryption method: CCMP (AES) Authentication method: EAP (802.1X)	Employees use the RADIUS server specified in "Example 7: Defining AAA RADIUS Settings" on page 104 to authenticate themselves using IEEE 802.1X.
guest	Key method: Auto-(WPA or WPA2)-PSK Encryption method: Auto-TKIP or CCMP (AES) Preshared key (ASCII): guest123 Authentication method: Open and for captive web portal: CWP-guest1	For guest access using a preshared key, the receptionist supplies guests with the SSID name and configuration details, including the preshared key, when they arrive.

Note: You can define up to seven SSIDs for a single radio in access mode. If hive members use one radio for wireless backhaul communications, then they must use the other radio in access mode. In this case, a HiveAP can have a maximum of seven SSIDs. If hive members send backhaul traffic completely over wired links, then both radios can be in access mode and a HiveAP can have a maximum of 14 SSIDs.

Figure 13 SSIDs Providing Network Access to Different Users



Employees that belong to the "IT" and "Emp" profiles can use SSIDs "voip" and "corp". The SSID with which they associate is based on how they are attempting to access the network. If they use a VoIP phone, then they associate with the voip SSID because that is the SSID configured on their phones. If they use a wireless client on a computer, then they associate with the corp SSID because that is the SSID configured on the wireless client on their computers.

In contrast, visitors can only associate with the guest SSID. The receptionist provides configuration details and the preshared key for the guest SSID when visitors arrive. The guest SSID is the only wireless network choice available to which visitors' wireless clients can connect. When the captive web portal option is in use, HiveAPs assign visitors who register successfully to the "Guests" profile and those who do not to the "Unregistered-Guests" profile.

Note: You can also use Aerohive GuestManager to provide network access to wireless visitors. For information about GuestManager, see the Aerohive GuestManager Getting Started Guide.

voip SSID

1. Click **Configuration** > **SSIDs** > **New** > **General**, enter the following, and leave all other values at their default settings:
   - SSID: **voip** (You cannot include any spaces when defining the name of an SSID.)
   - Description: **SSID exclusively for VoIP phones**
   - Key Management: **WPA2-PSK**
   - Encryption Method: **TKIP**
   - Authentication Method: **Open**
   - Key Type: **ASCII Key**
   - Key Value: **CmFwbo1121** (The key length can be from 8 to 63 characters.)
2. Click the **Advanced** tab.
3. In the Available MAC Filters list, click **corpVoIPphones >**, to move it to the Selected MAC Filters list, set the Default Action as **Deny**, and then click **Save**.

   By applying a MAC filter to the voip SSID, you restrict access to VoIP phones matching the specified OUI. The corpVoIPphones MAC filter is defined in "Creating a MAC Filter" on page 87.

corp SSID

1. Click **Configuration** > **SSIDs** > **New** > **General**, enter the following, and leave all other values at their default settings:
   - SSID: **corp**
   - Description: **SSID for corporate employees**
   - Key Management: **WPA2-EAP (802.1X)**
   - Encryption Method: **CCMP (AES)**
   - Authentication Method: **EAP (802.1X)**

guest SSID

1. Click **Configuration** > **SSIDs** > **New** > **General**, enter the following, and leave all other values at their default settings:
   - SSID: **guest**
   - Description: **SSID for company guests**
   - Key Management: **Auto-(WPA or WPA2)-PSK**
   - Encryption Method: **Auto-TKIP or CCMP (AES)**
   - Authentication Method: **Open**
   - Key Type: **ASCII Key**
   - Key Value: **guest123**

   or

   On the General page, enter the following:
   - SSID: **guest**
   - Description: **SSID for registering company guests**
   - Captive Web Portal: **CWP-guest1**
   - Key Management: **Auto-(WPA or WPA2)-PSK**
   - Encryption Method: **Auto-TKIP or CCMP (AES)**
   - Authentication Method: **Open**
   - Key Type: **ASCII Key**
   - Key Value: **guest123**

EXAMPLE 6: SETTING MANAGEMENT SERVICE PARAMETERS

Management services include the settings for DNS, syslog, SNMP, NTP, and location servers. HiveAPs use these services for network communications and logging activities. In addition, you can set HiveAP admin access parameters.

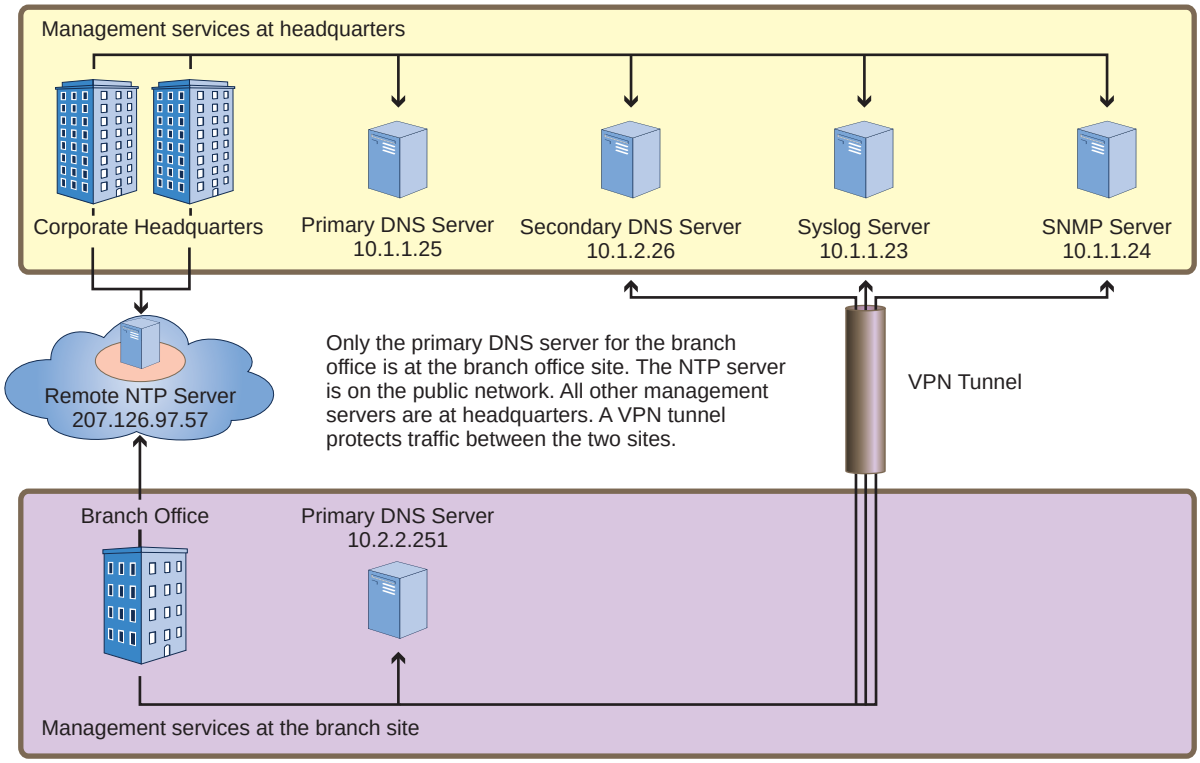
In this example, you configure the management services that you later reference in WLAN policies (see "Example 9: Creating WLAN Policies" on page 107). Two WLAN policies are for HiveAPs at the corporate HQ site and the third is for HiveAPs at the remote branch office. You define the following management services:

- Three DNS (Domain Name Service) servers—one primary server at HQ, one primary server at the branch site, and one secondary server at HQ. HiveAPs at the branch site connect to the secondary DNS server through a VPN tunnel.

  Although there are three DNS servers, there are only two IP address objects. The IP address object for the primary DNS server has two IP address definitions. By using the classifier tags "hq" and "branch1", all HiveAPs deployed at headquarters and classified as "hq" use the "hq" address definition, while all those deployed at the branch site and classified as "branch1" use the "branch1" definition. Because all HiveAPs use the secondary DNS server (at headquarters), its IP address definition is classified as Global; that is, it is the same for all HiveAPs.
- One syslog server and one SNMP (Simple Network Management Protocol) server—both at headquarters. HiveAPs at the branch office connect to these through a VPN tunnel.
- One NTP (Network Time Protocol) server—located on the public network. HiveAPs synchronize the time on their system clocks with this server.

The various servers and their relationship to the two sites is shown in Figure 14.

Figure 14 Location of Servers in Relation to Each WLAN Policy



DNS Assignment

Click **Configuration** > **Management Services** > **DNS Assignments** > **New**, and after entering all the following, click **Save**:

- Name: **DNS-Primary-HQ**
- Domain Name: **apis.com** (This is the domain name of the corporation in this example.)
- Description: **Primary and secondary DNS servers**

To specify a previously defined IP address object for the primary DNS server, enter the following, and then click **Apply**:

- IP Address: **DNS-Primary**
- Description: **Primary DNS server tagged "hq" and "branch1"**

To specify a previously defined IP address object for the secondary DNS server, click **New**, enter the following, and then click **Apply**:

- IP Address: **DNS-Secondary**
- Description: **Secondary DNS server 10.1.1.26**

Syslog Assignment

Click **Configuration** > **Management Services** > **Syslog Assignments** > **New**, and after entering all the following, click **Save**:

- Name: **Syslog-Server**
- Facility: From the drop-down list, choose a syslog facility with which to tag event log messages from the HiveAPs. By specifying a particular facility, the syslog server can differentiate all messages from the same source from messages from other sources.
- Description: **Syslog server at HQ**

To specify a previously defined IP address object for the syslog server, enter the following, and then click **Apply**:

- Type: **IP Address**
- Syslog Server: **Syslog-Server**
- Severity: Choose the minimum severity level for messages that you want to send to the syslog server. HiveAPs send messages of the level you choose plus messages of all severity levels above it. For example, if you choose critical, the HiveAP sends the syslog server all messages whose severity level is critical, alert, or emergency. If you choose emergency, the HiveAPs send only emergency-level messages.
- Description: Type a useful note, such as "Log critical - emergency events".

SNMP Assignment

Click **Configuration** > **Management Services** > **SNMP Assignments** > **New**, and after entering all the following, click **Save**:

- Name: **SNMP-Server**
- SNMP Contact: Type contact information for the person to contact if you need to reach a HiveAP admin. (You cannot include any spaces in the SNMP contact definition.)
- Description: **SNMP server at HQ**
- Enable SNMP Service: (**select**)

To specify a previously defined IP address object for the SNMP server, enter the following, and then click **Apply**:

- Type: **IP Address**
- SNMP Server: **SNMP-Server**
- Version: From the drop-down list, select the version of SNMP that is running on the management system you intend to use: **V1** or **V2C**.
- Operation: From the drop-down list, choose the type of activity that you want to permit between the specified SNMP management system and the HiveAPs in the WLAN policy to which you (later) assign this management services profile:

  get – get commands sent from the management system to a HiveAP to retrieve MIBs (Management Information Bases), which are data objects indicating the settings or operational status of various HiveOS components

  trap – messages sent from HiveAPs to notify the management system of events of interest

  get and trap – permit both get commands and traps

  none – cancel all activity, disabling SNMP activity for the specified management system
- Community String: Enter a text string that must accompany queries from the management system. The community string acts similarly to a password. (HiveAPs only accept queries from management systems that send the correct community string. The default string is "hivecommunity".)

NTP Assignment

Click **Configuration** > **Management Services** > **NTP Assignments** > **New**, and after entering all the following, click **Save**:

- Name: **NTP-Server**
- Sync Interval: Set an interval for polling the NTP (Network Time Protocol) server so that HiveAPs can synchronize their internal system clock with the server. The default interval is 1440 minutes (once a day). The possible range is from 60 minutes (once an hour) to 10,080 minutes (once a week).
- Time Zone: From the drop-down list, choose the time zone for the HiveAPs to which you intend to apply the management services.
- Description: Enter useful information, such as contact details for the NTP server admin.
- Enable NTP client service: (**select**)
- Sync Clock with HiveManager: (**clear**)

  Because you want the HiveAPs to use an NTP server, this option must be cleared. Select this only if you want the HiveAPs to synchronize their times with that set on HiveManager.

To specify a previously defined IP address object for the NTP server, enter the following, and then click **Apply**:

- Type: **IP Address**
- NTP Server: **NTP-Server**
- Description: Type a useful note, such as the location of the NTP server.

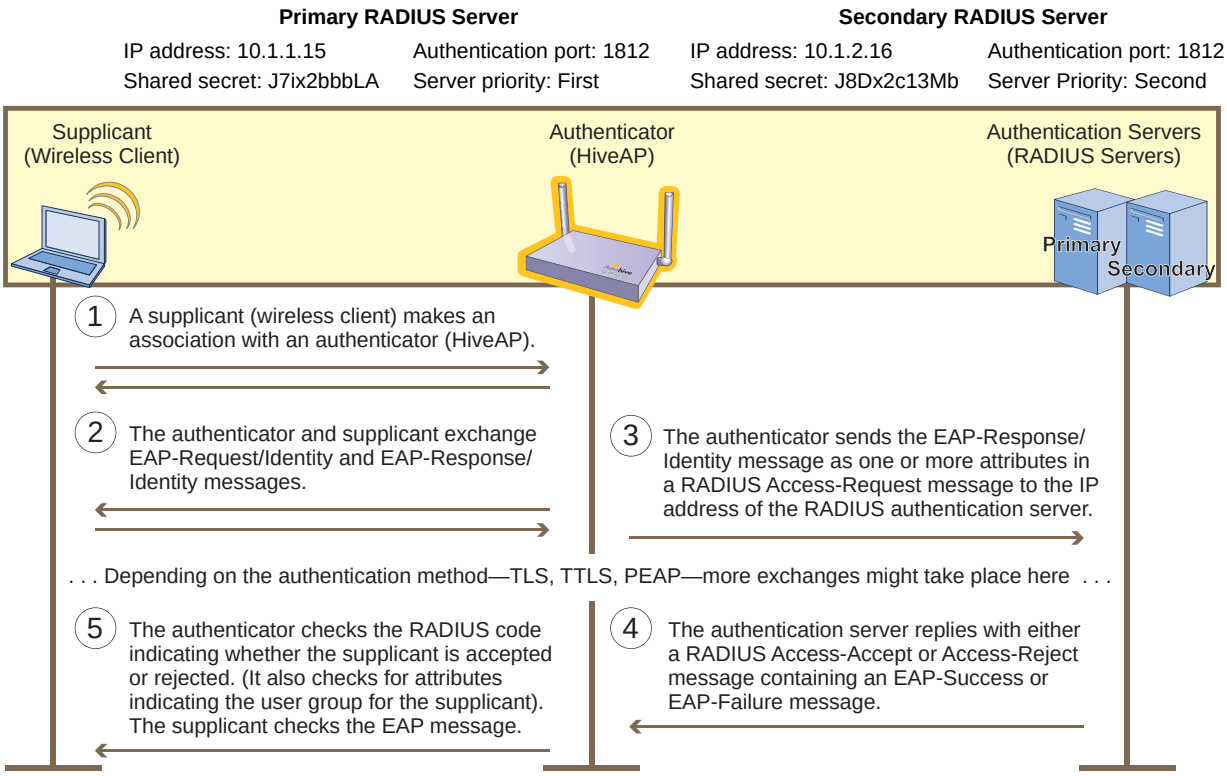
EXAMPLE 7: DEFINING AAA RADIUS SETTINGS

In this example, you define the connection settings for a RADIUS server so that HiveAPs can send RADIUS authentication requests to the proper destination.

After corporate employees associate with HiveAPs, they gain network access by authenticating themselves to a RADIUS server. The authentication process makes use of the IEEE 802.1X standard. Within this context, wireless clients act as supplicants, HiveAPs as authenticators, and the RADIUS server as the authentication server. The roles of each participant, packet exchanges, and connection details for the RADIUS server are shown in Figure 15.

Note: You can define a HiveAP as a RADIUS server. A HiveAP RADIUS server only supports 802.1X authentication, so you cannot use it to authenticate users through a captive web portal.

Figure 15 IEEE 802.1X Authentication Process



1. Click **Configuration > Authentication > AAA Client Settings > New > General**, and then enter the following:
   - RADIUS Name: **RADIUS-Servers** (You cannot use spaces in the RADIUS profile name.)
   - Retry Interval: **1800** (Seconds)

     Enter the period of time that a HiveAP waits before retrying a previously unresponsive primary RADIUS server. If a primary RADIUS server does not respond to three consecutive attempts—where each attempt consists of ten authentication requests sent every three seconds (30 seconds for a complete request)—and a backup RADIUS server has been configured, the HiveAP sends further authentication requests to the backup server. The default is 600 seconds (or 10 minutes). The minimum is 60 seconds and the maximum is

100,000,000 seconds. Generally, you want to make the retry interval fairly large so that supplicants (that is, wireless clients requesting 802.1X authentication) do not have to wait unnecessarily as a HiveAP repeatedly tries to connect to a primary server that is down for an extended length of time.

- Accounting Interim Update Interval: **20** (default)

  This is the interval in seconds for updating the RADIUS accounting server with the cumulative length of a client's session. Because this example does not make use of RADIUS accounting, leave the default setting.

- Description: **802.1X authentication for corp employees**

2. Click the **RADIUS Servers** tab, enter the following, and then click **Apply**:
   - Type: **IP Address**
   - Server IP/Name: **RADIUS-Server-Primary** (previously configured in "RADIUS Servers" on page 86)
   - Shared Secret: **J7ix2bbbLA**
   - Confirm Secret: **J7ix2bbbLA**

     Note: The shared secret is a case-sensitive alphanumeric string that must be entered on the RADIUS authentication server exactly as shown above.

   - Authentication Port: **1812** (default RADIUS authentication port number)
   - Enable Accounting: (**clear**)
   - Server Priority: **Primary**
   - Description: **Primary RADIUS server**

   - Click **New**, enter the following, and then click **Apply**:
     - Type: **IP Address**
     - Server IP/Name: **RADIUS-Server-Secondary** (previously configured in "RADIUS Servers" on page 86)
     - Shared Secret: **J8Dx2c13Mb**
     - Confirm Secret: **J8Dx2c13Mb**
     - Authentication Port: **1812** (default RADIUS authentication port number)
     - Enable Accounting: (**clear**)
     - Server Priority: **Backup1**
     - Description: **Backup (Secondary) RADIUS server**
3. To save the configuration and close the dialog box, click **Save**.

RADIUS Server Attributes

On the two RADIUS servers (also referred to as "RADIUS home servers"), define the HiveAPs as RADIUS clients.[3] Also, configure the following attributes for the realms to which user accounts matching the two user profiles belong:

Realm for IT (User Profile Attribute = 3)	Realm for Emp (User Profile Attribute = 4)
Tunnel Type = GRE (value = 10)	Tunnel Type = GRE (value = 10)
Tunnel Medium Type = IP (value = 1)	Tunnel Medium Type = IP (value = 1)
Tunnel Private Group ID = 3	Tunnel Private Group ID = 4

The RADIUS server returns one of the above sets of attributes based on the realm to which an authenticating user belongs. HiveAPs then use the combination of returned RADIUS attributes to assign users to profile 3 ("IT"), or 4 ("Emp"). Note that these attributes do not create a GRE tunnel, which the tunnel type might seem to indicate.

3. If you use RADIUS proxy servers, then direct RADIUS traffic from the HiveAPs to them instead of the RADIUS home servers. This approach offers the advantage that you only need to define the proxy servers as clients on the RADIUS home servers. You can then add and remove multiple HiveAPs without having to reconfigure the RADIUS home servers after each change.

EXAMPLE 8: CREATING HIVES

A hive is a set of HiveAPs that exchange information with each other to form a collaborative whole. In this example, you define three hives: two for the two buildings at headquarters and a third for the branch site. Later, in "Example 9: Creating WLAN Policies" on page 107, you assign the hives to WLAN policies, which in turn, you assign to HiveAP devices in "Example 10: Assigning Configurations to HiveAPs" on page 116.

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.

Hive1

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

- Hive: **Hive1** (You cannot use spaces in the name of a hive.)
- Description: Enter a meaningful comment, such as "Hive for HQ, Bldg 1"
- Modify Encryption Protection: (**select**); **g3r4oU7a#x**

  The password string is what hive members use when authenticating themselves to each other over the wireless backhaul link using WPA-PSK CCMP (AES). It can be from 8 to 63 characters long and contain special characters. If you do not enter a password string, HiveManager derives a default password from the hive name.

Hive2

Click **Configuration > Hives >** (check box) **Hive1 > Clone > General**, change the following, leave the other options at their previously defined settings, and then click **Save**:

- Hive: **Hive2**
- Description: Modify the description for Hive2 to something appropriate, such as "Hive for HQ, Bldg 2".
- Modify Encryption Protection: (**select**); **wWaG8U!3#2**

Hive3

Click **Configuration > Hives >** (check box) **Hive2 > Clone > General**, change the following, leave the other options at their previously defined settings, and then click **Save**:

- Hive: **Hive3**
- Description: Modify the description for Hive3 to something appropriate, such as "Hive for branch site".
- Modify Encryption Protection: (**select**); **C!8vGg5Jo3**

EXAMPLE 9: CREATING WLAN POLICIES

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

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

A WLAN policy is an assembly of policy-based 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, connectivity-based configurations are more appropriately applied to smaller sets of devices or to individual devices themselves.

In this example, you create "WLANpolicy-hq1" and "WLANpolicy-hq2" for the two buildings at corporate headquarters and "WLANpolicy-branch1" for the branch site. You add a hive, management server assignments, SSID profile–radio mode–user profile mappings, plus the QoS settings for each user group.

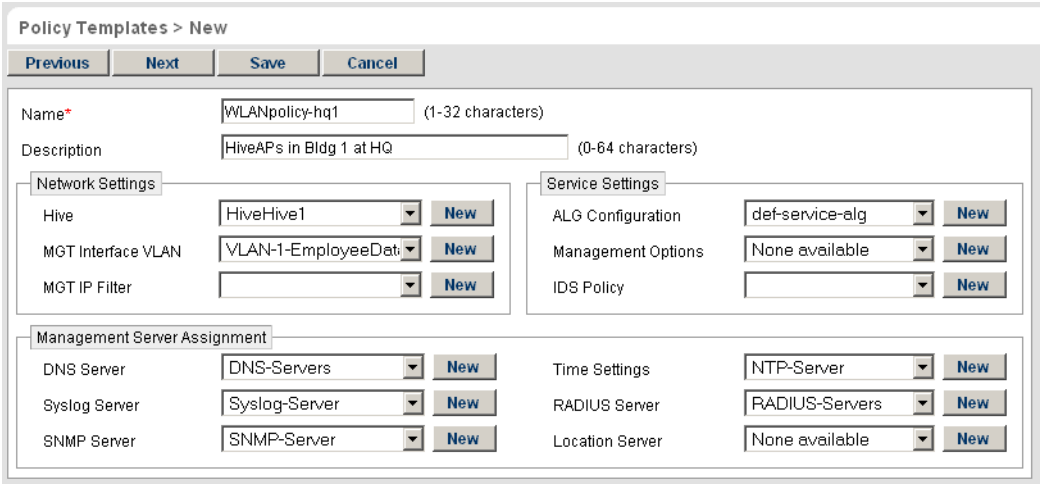
WLANpolicy-hq1

This WLAN policy is for all the HiveAPs in Building 1 at the corporate headquarters depicted in Figure 1 on page 73. The New WLAN Policy dialog box consists of several pages. The configuration of the items on each page is presented individually and in detail. The other WLAN policies are clones of this one with only minor changes.

WLANpolicy-hq1 (Page 1)

On the first page of the new WLAN policy dialog box, you define the name and a description of the WLAN policy, and set network settings, service settings, and management server assignments for the HiveAPs to which you will apply this WLAN policy. See Figure 16.

Figure 16 First Page of the WLAN Policy Dialog Box



1. Click **Configuration > WLAN Policies > New**, enter the following on the first page of the new WLAN policy dialog box:
   - Name: **WLANpolicy-1** (You cannot use spaces in the WLAN policy name.)
   - Description: Enter a useful description, such as "HiveAPs in Bldg1 at HQ".

Network Settings

2. Enter the following in the Network Settings section. (Note that the hive and VLAN were previously configured in "Example 8: Creating Hives" on page 106 and "Defining VLANs" on page 84.)
   - Hive: **Hive1**
   - MGT Interface VLAN: **1** (or **VLAN-1-EmployeeData**)

     In this example, the MGT interface is in VLAN 1, the same VLAN as that for employee data traffic. You can specify either the predefined VLAN "1" or "VLAN-1-EmployeeData", which was previously created.
   - MGT IP Filter: leave empty. A management IP address filter defines addresses from which admins are permitted administrative access to HiveAPs. This filter was not configured in the preceding examples.

Service Settings

3. Leave the Service Settings fields at their default values or empty. None of these options were modified or configured in the preceding examples.

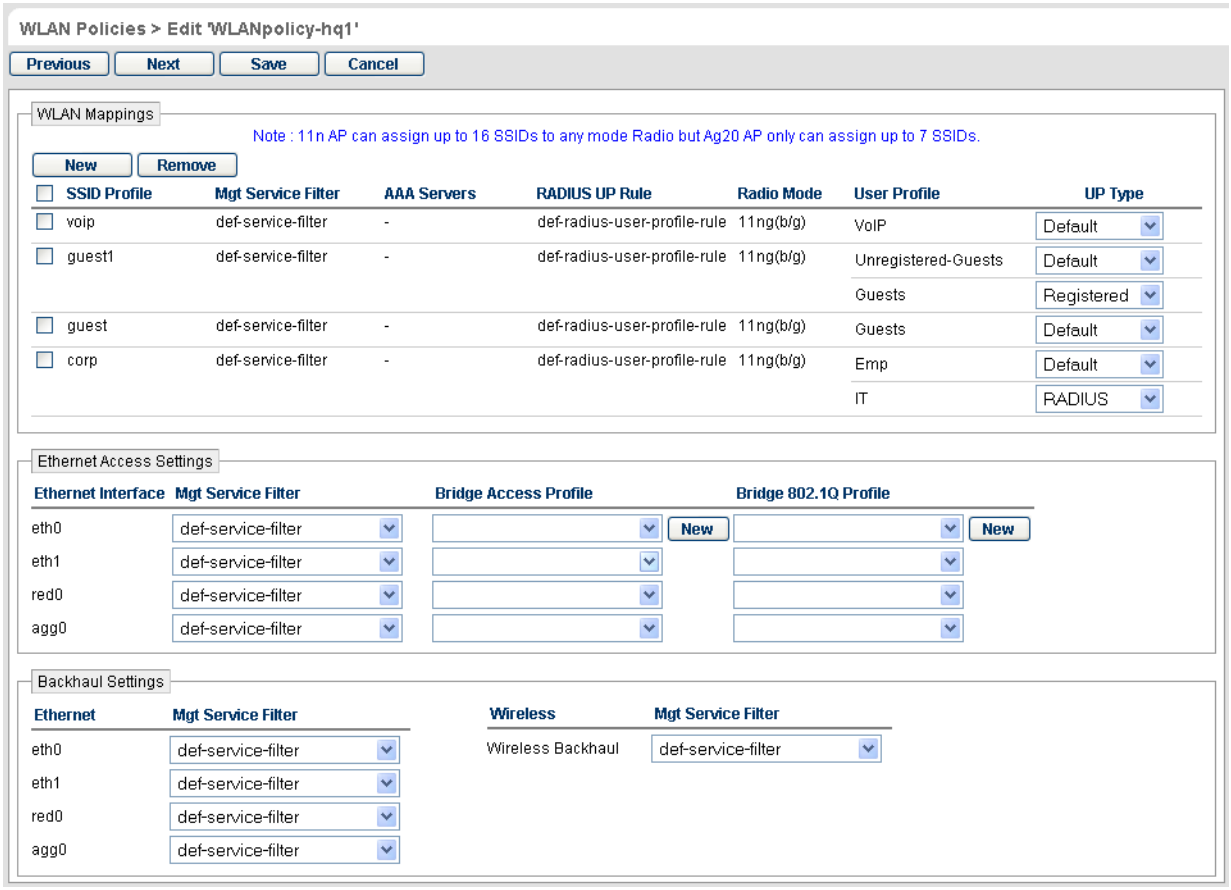
Management Server Assignment

4. Enter the following in the Management Server Assignment section. (Note that the following settings were previously configured in "Example 6: Setting Management Service Parameters" on page 101 and "Example 7: Defining AAA RADIUS Settings" on page 104.)
   - DNS Server: **DNS-Servers**
   - Syslog Server: **Syslog-Server**
   - SNMP Server: **SNMP-Server**
   - Time Settings: **NTP-Server**
   - RADIUS Server: **RADIUS-Servers**
   - Location Server: None available (this option was not configured in the preceding examples)
5. To proceed to the next page, click **Next**.

WLANpolicy-hq1 (Page 2)

On the second page of the new WLAN policy dialog box, you can map SSIDs to management service filters, AAA servers, radio modes, and user profiles. In addition, you can set the Ethernet interface in access mode (Bridge-Access or Bridge-802.1Q) and assign management service filters to the Ethernet and wireless backhaul interfaces. (Note that because no management service filters were set in the previous examples, you only configure WLAN mappings below.) See Figure 17.

Figure 17 Second Page of the WLAN Policy Dialog Box



WLAN Mappings

Configure the WLAN mappings of SSIDs to radio modes and user profiles. (The SSIDs were previously configured in "Example 5: Setting SSIDs" on page 98, and the user profiles were configured in "Example 4: Creating User Profiles" on page 94.)

SSID: voip

1. Enter the following to define the WLAN mappings for the voip SSID, and then click **Apply**:
   - SSID Profile: **voip**
   - MGT Service Filter: **def-service-filter** (default)
   - AAA Servers: (leave empty; this setting is for overriding the RADIUS server setting on the previous page of this dialog box, and, in any case, is not applicable to SSIDs using preshared keys)

- RADIUS UP Rule: **def-radius-user-profile-rule** (default)

  This setting essentially controls which users authenticated by a RADIUS server can access the SSID. Because the voip SSID does not use RADIUS authentication, the setting is not applicable.

- Radio Mode: **11ng(b/g)**

Note: 802.11n radio options appear in anticipation of an upcoming release. They are not yet functional.

In this example, you want to use IEEE 802.11b/g for network access traffic because a broader range of wireless clients support IEEE 802.11b than IEEE 802.11a, which came out two years later (despite its alphabetical precedence), and it provides slightly greater coverage.

The three choices in the Radio Mode drop-down list are as follows:

11na+11ng(a+b/g): This binds the SSID to two subinterfaces, each linked to a different radio operating in separate frequency bands. Radio 1 supports IEEE 802.11b/g and operates in the 2.4 GHz band, and radio 2 supports IEEE 802.11a and operates in the 5 GHz band.

This is a good approach if the HiveAPs need to interoperate with some wireless clients that only support 802.11b/g and others that only support 802.11a. In this case, both of the wifi interfaces—wifi0 and wifi1—must be in access mode. On the other hand, if hive members need to support wireless backhaul communications, then you cannot take this approach because one interface (wifi1 by default) will need to be in backhaul mode and its subinterfaces (wifi1.1 – wifi1.4), therefore, cannot support an SSID.

11ng(b/g): This binds the SSID to a subinterface linked to a radio operating at 2.4 GHz for the IEEE 802.11b or IEEE 802.11g standards.

11na(a): This binds the SSID to a subinterface using an antenna operating at 5 GHz for the IEEE 802.11a standard.

- User Profile: **VoIP**

2. After you click **Apply**, a drop-down list appears for the user profile type. Choose **Default**.

SSID: corp

1. Click **New**, enter the following to define the WLAN mappings for the corp SSID, and then click **Apply**:
   - SSID Profile: **corp**
   - MGT Service Filter: **def-service-filter** (default)
   - AAA Servers: (leave empty; you want to use the RADIUS servers set on the previous page)
   - RADIUS UP Rule: **def-radius-user-profile-rule** (default)

     The default RADIUS user profile rule allows all users authenticated by the same RADIUS server to access the SSID. In this example, only corporate employee accounts are stored on the RADIUS server, so there is no need to restrict access to a smaller set of users.

   - Radio Mode: **11ng(b/g)**
   - User Profile: **IT** and **Emp** (SHIFT-click or CTRL-click to make multiple selections.)
2. After you click **Apply**, a drop-down list appears for the user profile type. Choose **RADIUS** for IT, and choose **Default** for Emp.

   When authenticating users through 802.1X to a RADIUS server, there can be multiple user profiles, and the RADIUS server will indicate which one the HiveAP applies to each user. However, if the RADIUS server does not have a set of attributes configured for some users, then the HiveAP applies the user profile that you mark as the default. One of the two user profile types must be marked as default and the other as RADIUS.

SSID: guest

1. Click **New**.
2. Depending on which guest access method you used (see "Example 3: Providing Guest Access" on page 88), enter either of the following to define the WLAN mappings for the guest SSID, and then click **Apply**:

   For guest access using a preshared key:

   - SSID Profile: **guest**
   - MGT Service Filter: **def-service-filter** (default)
   - AAA Servers: (leave empty)
   - RADIUS UP Rule: **def-radius-user-profile-rule** (default)
   - Radio Mode: **11ng(b/g)**
   - User Profile: **Guests**

   After you click **Apply**, choose **Default** as the user profile type.

   or

   For guest access using a captive web portal:

   - SSID Profile: **guest**
   - MGT Service Filter: **def-service-filter** (default)
   - AAA Servers: (leave empty)
   - RADIUS UP Rule: **def-radius-user-profile-rule** (default)
   - Radio Mode: **11ng(b/g)**
   - User Profile: **Guests** and **Unregistered-Guests**

   After you click **Apply**, choose **Default** as the user profile type for Unregistered-Guests. Choose **Registered** as the user profile type for Guests.

WLANpolicy-hq1 (Page 3)

On the third page of the new WLAN policy dialog box, you can assign QoS classifier and marker maps to SSIDs and specify user profile-based QoS data forwarding rate limits and weights. (Note that no marker maps were configured previously, so this option is unavailable.)

To view the third page of the WLAN policy dialog box configured with the SSID "guest" with and without a captive web portal, see Figure 18.

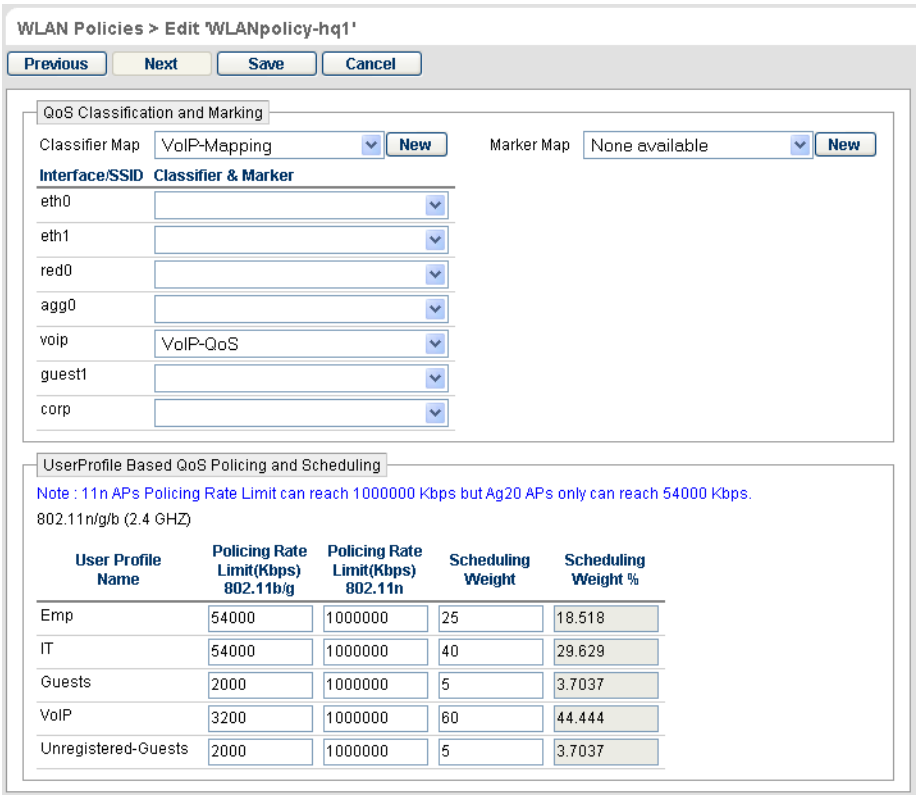
Figure 18 Third Page of the WLAN Policy Dialog Box (SSID "guest" with and without a Captive Web Portal)

When the SSID "guest" uses a captive web portal, there are two user profiles:

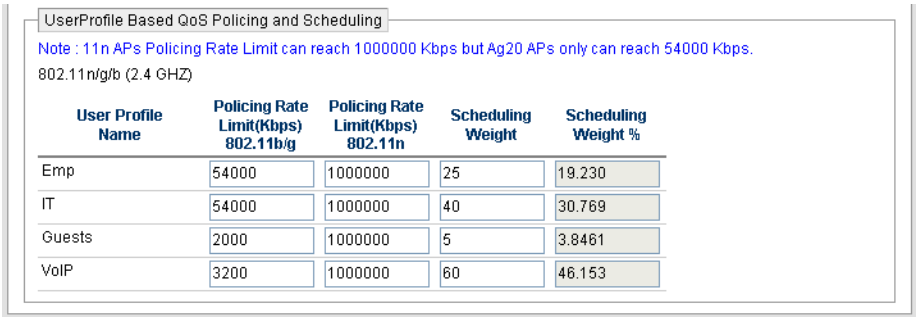
"Guests" (Registered)

"Unregistered-Guests" (Default)

You must set the same policing rate limits and scheduling weights for both of these profiles.



When the SSID "guest" does not use a captive web portal, there is only one user profile: "Guests"



The User profile settings, maximum traffic forwarding rates per user profile, and the WRR (weighted round robin) weights for each profile are shown in Figure 19 on page 113.

Figure 19 User Profiles, Forwarding Rates, and Weights

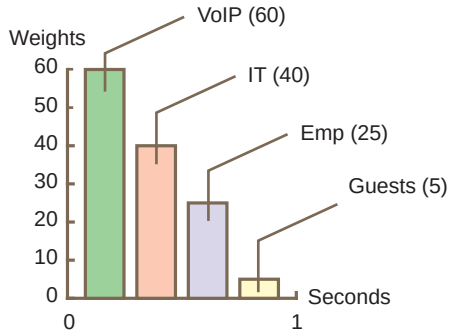
User Profiles	Maximum Traffic Forwarding Rates	
	Per Profile	Per User
Name: VoIP ID: 2	3200 Kbps	128 Kbps
Name: IT ID: 3	54000 Kbps	54000 Kbps
Name: Emp ID: 4	54000 Kbps	54000 Kbps
Name: Guests ID: 5	2000 Kbps	2000 Kbps

Note: Unregistered-Guests (ID 6) is not shown.

For IT, Emp, and Guests users, the maximum traffic forwarding rates are the same for the entire user profile as they are for an individual user. By keeping them the same, a single online user is not restricted to a smaller rate than that of the profile to which he or she belongs. (The individual user rate can be the same as or smaller than its profile rate.)

For VoIP users, because individual calls use relatively little bandwidth (~128 Kbps), a single user does not need as much as that for the entire VoIP user profile. A 3200 Kbps/profile maximum allows up to 25 concurrent voice sessions at 128 Kbps per HiveAP (3200 ÷ 128 = 25). If a stronger voice compression codex is used, the number of concurrent voice sessions can increase proportionately.

User Profile Weights
(for traffic forwarding using WRR)



Note: Weights do not apply to strict traffic forwarding.

The bar chart indicates the ratio of allotted bandwidth among the four user profiles based on their respective weights. During the course of one second, a HiveAP allots 12 times more bandwidth for VoIP users, 8 times more for IT users, and 5 times more for Emp users than it allots for Guests.

Bandwidth rationing only occurs when usage is at maximum capacity.

1. Enter the following in the QoS Classification and Marking section:
   - Classifier Map: **VoIP-Mapping**
   - voip: **VoIP-QoS**

   The QoS map and policy were previously configured in "Mapping the MAC OUI and Services to Aerohive Classes" on page 82, and as part of user profiles in "Example 4: Creating User Profiles" on page 94.
2. Enter the following in the User Profile Based QoS Policing and Scheduling section, and then click **Save**:

   SSID "guests" without a captive web portal (only one user profile)

User Profile Name	Policing Rate Limit (Kbps) 802.11b/g	Scheduling Weight	Scheduling Weight % (read-only)
Guests	2000	5	3.8461
VoIP	3200	60	46.153
IT	54000	40	30.769
Emp	54000	25	19.230

SSID "guests" with a captive web portal (two user profiles)

User Profile Name	Policing Rate Limit (Kbps) 802.11b/g	Scheduling Weight	Scheduling Weight % (read-only)
Guests	2000	5	3.7037
Unregistered-Guests	2000	5	3.7037
VoIP	3200	60	44.444
IT	54000	40	29.629
Emp	54000	25	18.518

Some notes about the settings for each user profile:

Guests user profile

- Entire User Profile Rate Limit: **2000** Kbps

  This is a limited amount of bandwidth that all users belonging to this profile can use. This setting provides guests with a basic amount of available traffic.

- Entire User Profile Weight: **5**

  Because wireless access for guests is mainly a convenience and not a necessity, you assign it the lowest weight to give it the lowest priority. The weight defines a preference for forwarding traffic. It does not specify a percentage or an amount. Its value is relative to other weights. However, you can see an automatically calculated percentage of this weight versus those of other user profiles in the far right column.

VoIP user profile

- Entire User Profile Rate Limit: **3200** Kbps

  This is the maximum amount of bandwidth that all users belonging to this profile can use. The typical bandwidth consumption for VoIP is about 128 Kbps depending on the speech codec used. This setting supports up to 25 concurrent VoIP sessions using 128-Kbps compression (3200 Kbps / 128 Kbps = 25 sessions).

- Entire User Profile Weight: **60**

  Because you want HiveAPs to favor VoIP traffic over all other types, you give this profile the highest weight.

IT user profile

- Entire User Profile Rate Limit: **54000** Kbps (default)

  This is the maximum amount of bandwidth that all users belonging to this profile can use. This setting provides IT staff members with the maximum amount of available traffic.

- Entire User Profile Weight: **40**

  Because you want the HiveAPs to favor IT staff traffic over employee and guest traffic, you give this profile a higher weight than those, but a lower one than that for VoIP traffic.

Emp user profile

- Entire User Profile Rate Limit: **54000** Kbps (default)

  This is the maximum amount of bandwidth that all users belonging to this profile can use. This setting provides employees with the maximum amount of available traffic.

- Entire User Profile Weight: **25**

  Because you want the HiveAPs to prioritize VoIP traffic first, IT staff traffic second, employee traffic third, and guest traffic last, you give this profile a weight of 25. This weight is less than that for VoIP traffic (60) and IT staff traffic (40), and more than what you are going to assign to guest traffic (5) next. These weights skew the rate at which the HiveAPs forward queued traffic using the WRR (weighted

round robin) scheduling discipline. Roughly, for every 5 bytes of guest traffic per second, a HiveAP forwards 25 bytes of employee traffic, 40 bytes of IT traffic, and 60 bytes of VoIP traffic. These numbers are not exact because HiveAPs also have internal weights per class that also affect the amount of traffic that a HiveAP forwards.

Unregistered-Guests profile

Although the Unregistered-Guests user profile is required for the configuration of the "guest" SSID using a captive web portal, the HiveAP never applies the QoS settings for this user profile because it never forwards traffic from unregistered guests.

WLANpolicy-hq2

This WLAN policy is for all the HiveAPs in Building 2 at the corporate headquarters depicted in Figure 1 on page 73. Because this policy consists of nearly identical elements to those in WLANpolicy-hq1, you clone the first WLAN policy and simply change the WLAN policy name and description, and the hive in the configuration.

Click **Configuration > WLAN Policies >** (check box) **WLANpolicy-hq1 > Clone**, change only the following, and then click **Save**:

- Name: **WLANpolicy-hq2**
- Description: **HiveAPs in Bldg 2 at HQ**
- Hive: **Hive2**

WLANpolicy-branch1

This WLAN policy is for all the HiveAPs at the branch site depicted in Figure 1 on page 73. Because this policy consists of nearly identical elements to those in WLANpolicy-hq1 and WLANpolicy-hq2, you can clone either policy and simply change the WLAN policy name and description, and the hive in the configuration.

Click **Configuration > WLAN Policies >** (check box) **WLANpolicy-hq2 > Clone**, change only the following, and then click **Save**:

- Name: **WLANpolicy-branch1**
- Description: **HiveAPs at the branch site**
- Hive: **Hive3**

EXAMPLE 10:ASSIGNING CONFIGURATIONS TO HIVEAPS

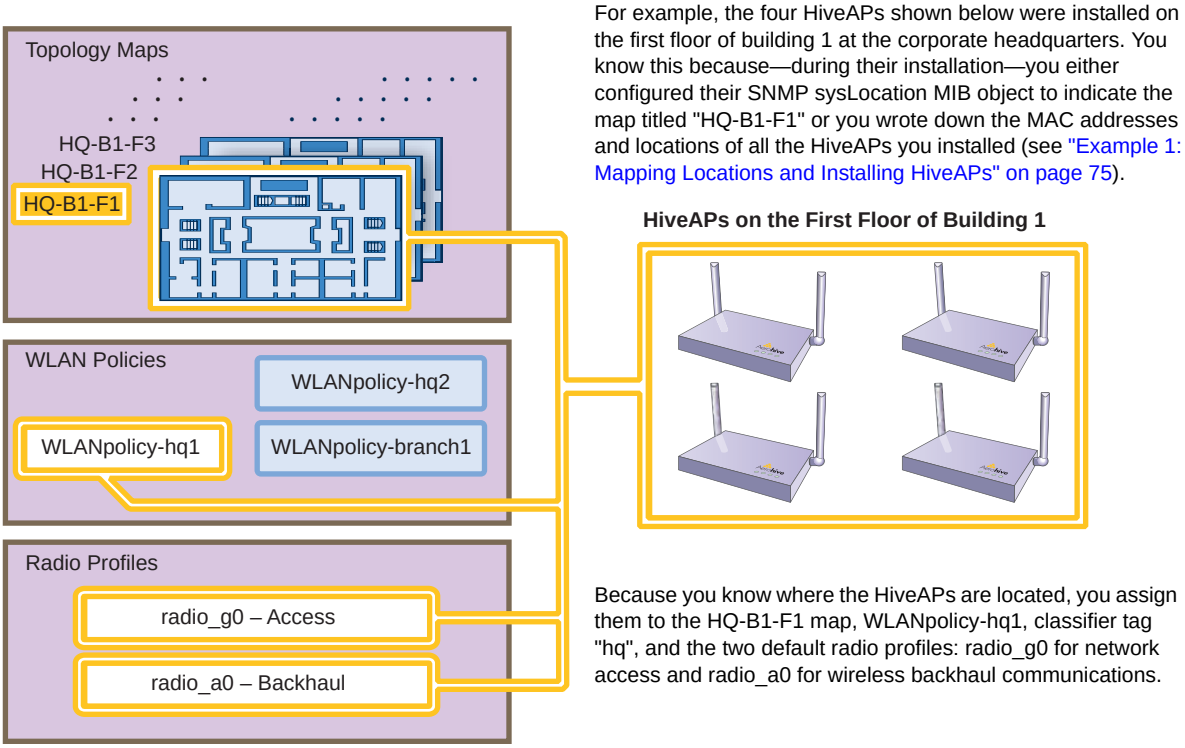
After completing the steps in the previous examples, you can now assign the following configurations as appropriate to each HiveAP:

- WLAN policy (created in "Example 9: Creating WLAN Policies" on page 107)
- Radio profiles (default radio profiles)
- Map (uploaded in "Example 1: Mapping Locations and Installing HiveAPs" on page 75)

As the above list indicates, this example makes use of the two default radio profiles: radio_g0 for the wifi0 interface in access mode, and radio_a0 for the wifi1 interface in backhaul mode.

The HiveAP configuration assignments are presented conceptually in Figure 20.

Figure 20 HiveAP Configuration Assignments



In addition to assigning the above configurations to the HiveAPs, you also change their login settings (and country code if necessary) and apply the classifier tags "hq" and "branch1" so that the HiveAPs at HQ and the branch site use the correct DNS servers.

Finally, you update the HiveAPs with the new configuration settings—and captive web portal files, if a captive web portal is a part of the configuration—to complete their deployment.

Assigning Configurations

1. Click **Access Points** > **Automatically Discovered**.
2. Select a group of HiveAPs associated with the same map.

   If you defined SNMP sysLocation MIB objects as you installed the HiveAPs as explained in "Using SNMP" on page 78, each HiveAP listed in the Automatically Discovered window will now include a map title in the Topology Map column. By clicking the Topology Map column header, you can sort HiveAPs by topology map. You can then select all the HiveAPs belonging to the same map (shift-click the check boxes to select multiple contiguous HiveAPs) and assign the same WLAN policy, radio profiles, and classifier tags to them.

   If you tracked HiveAPs by writing their MAC addresses on the maps as explained in "Using MAC Addresses" on page 79, you can sort the HiveAPs in the Automatically Discovered window by MAC address. Click the Node ID column header to display the HiveAPs numerically by MAC address. By referring to the MAC addresses and the title of the map on which you wrote them during the installation, you can then select all the HiveAPs belonging to the same map and assign the same map, WLAN policy, radio profiles, and classifier tags to them.
3. Click **Modify > General**, and then enter the following:
   - WLAN Policy: Choose the WLAN policy that you want to assign to the selected HiveAPs. In these examples, there are three WLAN policies. Assign WLANpolicy-hq1 to all HiveAPs in Building 1 at corporate headquarters, WLANpolicy-hq2 to all HiveAPs in Building 2 at corporate headquarters, and WLANpolicy-branch1 to all HiveAPs at the branch office.
   - Topology Map: Choose the map that you want to assign to the selected HiveAPs. (If you used the SNMP sysLocation MIB definition to associate HiveAPs with maps, HiveManager has automatically chosen the correct map already.) The maps allow you to organize the HiveAPs by site (HQ or Branch1), then at HQ by building (HQ-B1 or HQ-B2), and then by floor (HQ-B1-F1, HQ-B1-F2, HQ-B1-F3, and so on).
   - Gateway Address: Leave as is.
   - Location: If you set the SNMP sysLocation MIB when you installed the HiveAPs, leave this field as is. If not, enter a description for the location of each HiveAP individually.
   - Native VLAN: **1** (for control traffic among hive members on the wired backhaul interface)
   - LAN Interface: Leave the settings as they are.
   - WLAN Interface: Set the radio profile for wifi0 as **radio_g0** and the radio profile for wifi1 as **radio_a0**. Leave the values for the other fields as they are.
   - HiveAP Classification: For HiveAPs at headquarters, type **hq** in the Tag1 field. For HiveAPs at the branch site, type **branch1** in the Tag1 field. By classifying the HiveAPs with these tags, they will receive the similarly tagged IP address for the primary DNS server on the network at their respective locations. (The two IP addresses are tagged in "DNS Servers" on page 85.)
4. Click **Credentials**, enter the following in the Root Admin Configuration section, and then click **Save**:

   Root Admin Configuration

   - New Admin Name: 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*. To change the login settings on the HiveAPs, click **Change Login Credentials**, and then enter a new admin name. The admin name can be any alphanumeric string from 3 to 20 characters long.
   - New Password: Although the password is obscured, the default password is *aerohive*. To change the default password on the HiveAPs, enter a new password here. The password can be any alphanumeric string from 5 to 16 characters.
   - Confirm New Password: If you entered a password in the above field, enter it again to confirm accuracy.

DTLS Passphrase

HiveManager and HiveAPs use the DTLS (Datagram Transport Layer Security) passphrase to derive a preshared key that they then use to mutually authenticate each other when making a CAPWAP connection. By default, when a HiveAP first makes a CAPWAP connection to HiveManager, they use a predefined bootstrap DTLS passphrase combined with several other values to derive a shared key that they then use to authenticate each other. To change the DTLS passphrase, click **Change Passphrase**.

Note: When you click Change Passphrase, HiveManager immediately generates a new, random passphrase. You can override this by typing your own passphrase, which can be from 16 to 32 characters long.

5. Repeat this procedure with the HiveAPs associated with all the other maps until they are all configured.
6. To accept all the HiveAPs for management through HiveManager, select the top check box to the left of "Host Name" in the header in the Automatically Discovered window, and then click **Accept**.

   HiveManager displays accepted HiveAPs in the Access Points > Managed HiveAPs window.

Updating the Country Code

When the preset region code for a managed HiveAP is "World", you must set the appropriate country code to control the radio channel and power selections that that HiveAP can use. 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 the region code for any of the managed HiveAPs is "World", set the country code as follows:

1. Click **Access Points > Managed HiveAPs >** (check box) *hiveap* **> Update > Update Country Code**.
2. In the Update Country Code dialog box , enter the following, and then click **Upload**:
   - Select the check box for the HiveAPs whose country code you want to change.[4]
   - Choose the country where they are deployed from the New Country Code 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 after which the HiveAP reboots to activate the updated country code settings.

   HiveManager updates the country code on the selected HiveAPs. To put the radio settings for the updated country code in effect, they reboot after the activation interval that you set elapses. After the HiveAPs reboot, they then apply the appropriate radio settings for the newly updated country code.

4. 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 72.

Uploading HiveAP Configurations

At this point, you have assigned configurations to the HiveAPs, accepted them for management, changed their login settings, and possibly the country code as well. Now, you can push their configurations from HiveManager to the HiveAPs.

1. Click **Access Points** > **Managed HiveAPs** > **Update** > **Upload and Activate Configuration (Wizard)**.

   The Upload and Activate Configuration (Wizard) dialog box appears.

2. If you have an SSID using captive web portal files, the first step in the upload process is to upload these pages and a server key, if the captive web portal uses HTTPS to secure guest registrations. To upload these files, select the HiveAPs to which you want to send the files, and then click **Upload**.

   The HiveAP Update Results page appears so that you can monitor the progress of the upload procedure.

Note: If a managed HiveAP already has the maximum number of captive web portal directories (8), you must delete at least one of them before you can add a new one. To see how many directories are already on a HiveAP and delete a directory if necessary, do the following:

1. *Make an SSH connection to the managed HiveAP by finding an icon of the HiveAP on a map, right-clicking the icon, and choosing SSH to HiveAP*
2. *Enter the following command to see the number of existing directories and their names:* **`show web-directory`**
3. *Delete a directory by entering the following command, in which* `<string>` *is the name of the directory that you want to delete:* **`no web-directory`** `<string>`

3. After the files are successfully uploaded, click the **Back** button in your browser to return to the Upload and Activate Configuration dialog box.
4. To continue to the next step, click **Next**.
5. There are two options for uploading configurations to HiveAPs:
   - Complete Upload, which uploads the complete configuration to the managed HiveAPs and which requires them to reboot to activate the new configuration
   - Delta Upload, which uploads only the parts of the configuration that were not pushed to the managed HiveAP in a previous configuration update

   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 upload delta configurations. When initially sending the configuration to HiveAPs, you must choose **Complete Upload**.

   Note: If there is any failure when performing a delta upload, the next upload must be a full upload.

6. Select the HiveAPs whose configurations you want to update, select one of the following options for controlling when the uploaded configurations are activated (by rebooting the HiveAPs), and then click **OK**:
   - **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 the 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 to load the 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 60 seconds.
   - **Activate at next reboot**: Select to load the configuration and not activate it. The loaded configuration is 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" on page 72.

   HiveManager pushes the configuration to all the selected HiveAPs. After they reboot to activate their new configurations, they reconnect with HiveManager. To check the status of their CAPWAP connections, see the Status and CAPWAP columns on the Access Points > Managed HiveAPs page. From this point, you can upload delta configurations, which do not require the HiveAPs to reboot to activate a configuration update.

7. To check that the HiveAP is using the new files for its captive web portal, make an association with the HiveAP using the guest SSID and then open a browser as described in step 2 to step 3 on page 91.

   Note: If you still see the default .html and .jpg files, try clearing your browser cache and then closing and reopening the browser.

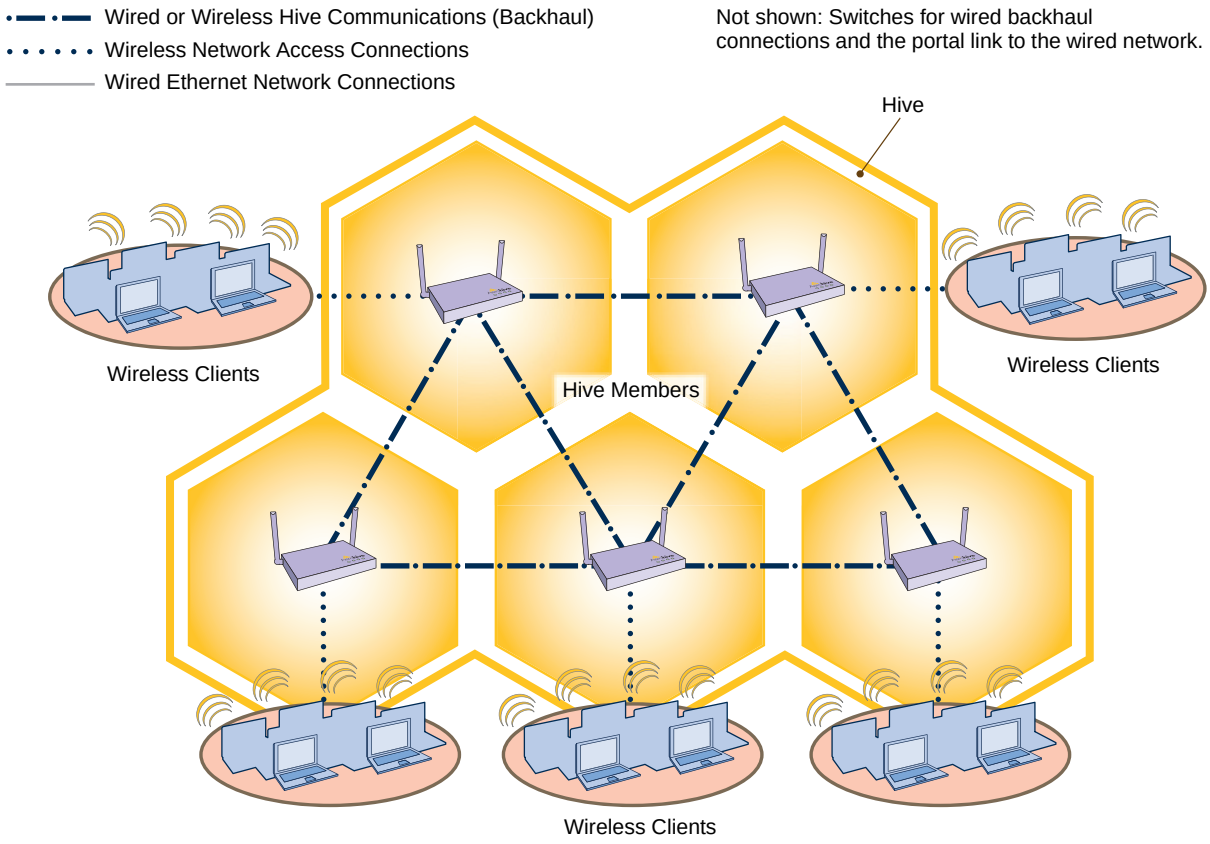
   If you customize captive web portal pages and then later want to return to the default set of files, enter this command: **`reset web-directory`** `<string>`
   where `<string>` *is the name of the directory whose contents you want to return to the default files.*

Chapter 8 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



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 its security protocol suite, 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:

	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 a different VLAN ID: **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*
Default QoS policy	def-user-qos policy: user profile rate = 54,000 Kbps user profile weight = 10 user rate limit = 54,000 Kbps mode = weighted round robin for Aerohive classes 0 - 5; strict forwarding for classes 6 - 7 classes 0 - 4 rate limit = 54,000 Kbps class 5 rate limit = 10,000 Kbps classes 6 - 7 rate limit = 512 Kbps	To change the default QoS policy: **qos policy def-user-qos qos** *ah_class* { **strict** *rate_limit* **0** | **wrr** *rate_limit weight* } **qos policy def-user-policy user-profile** *rate_limit weight* **qos policy def-user-policy user** *rate_limit*
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 129, 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 124. 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`* **`group-id`** *`number`* **`qos-policy`** *`string`* **`vlan-id`** *`number`*

  For hive communications:

  `hive` *`string`* **`native-vlan`** *`number`*

  For the mgt0 interface:

  `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

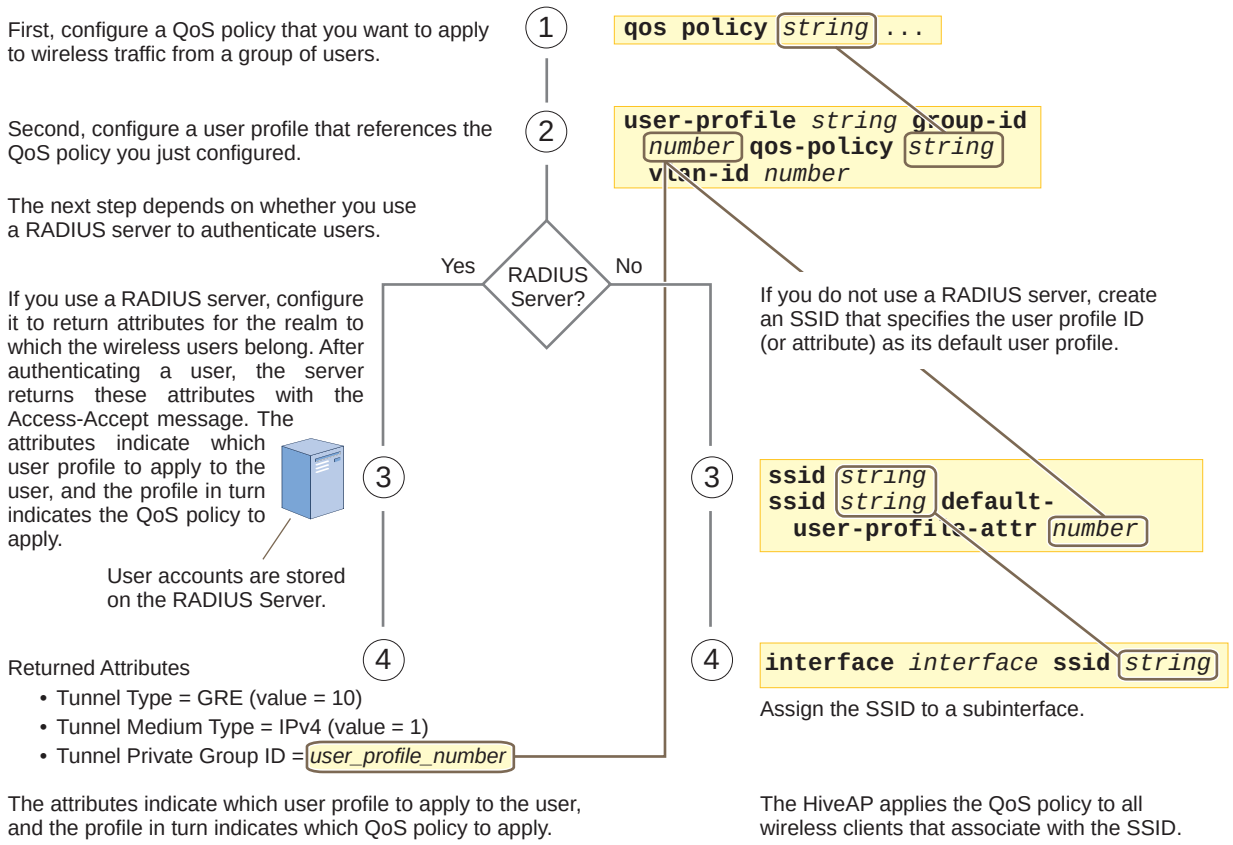
  ssid *string* **…**

- 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 a subinterface 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.

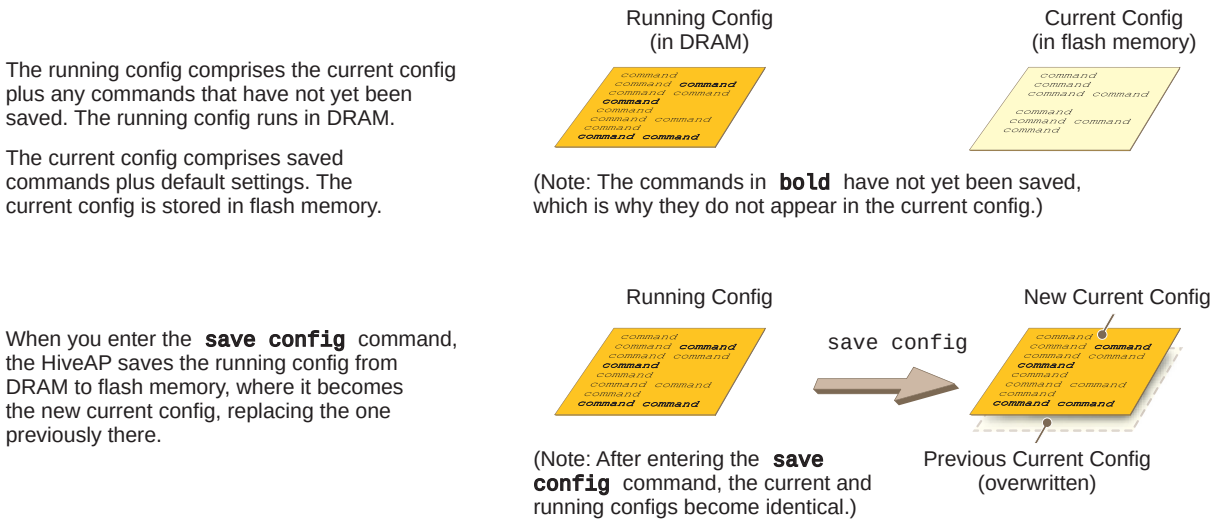
The **running** configuration (config) is the configuration that is actively running in DRAM. During the bootup process, a HiveAP loads the running config from one of up to four config files stored in flash memory:

- **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 126 and Figure 5 on page 126.
- **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 128.
- **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 128.

Note: There is also a failed config file, which holds any backup config that fails to load. See Figure 5 on page 126.

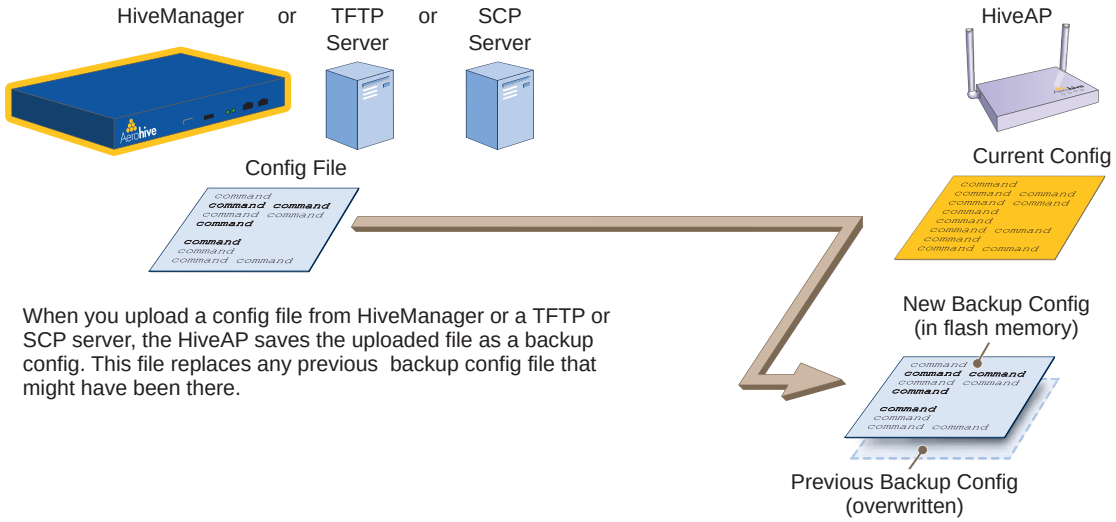
When using the CLI, the two most frequently accessed config types are the running config and current config. When you enter a command in the running config, the HiveAP performs it immediately. However, because the running config is stored in volatile memory (DRAM), the commands are not yet permanent 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



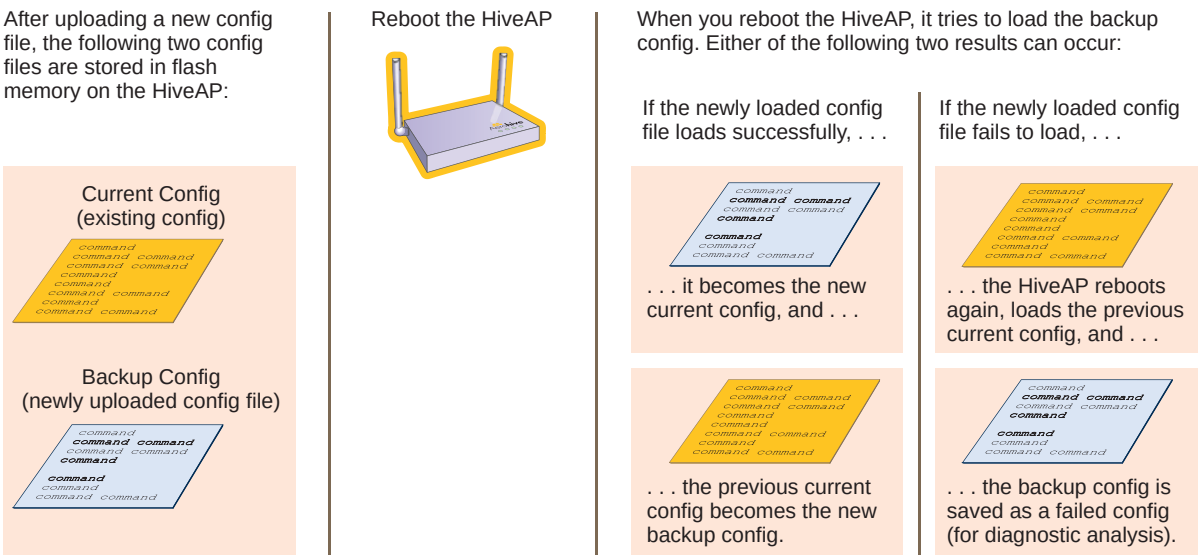
When you upload a configuration file from HiveManager or from a TFTP or SCP server, the HiveAP stores the uploaded file in the backup config partition in flash memory, where it remains until the HiveAP reboots. If there is a backup config file already stored in flash, the newly uploaded file overwrites 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 119. 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 25) 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.

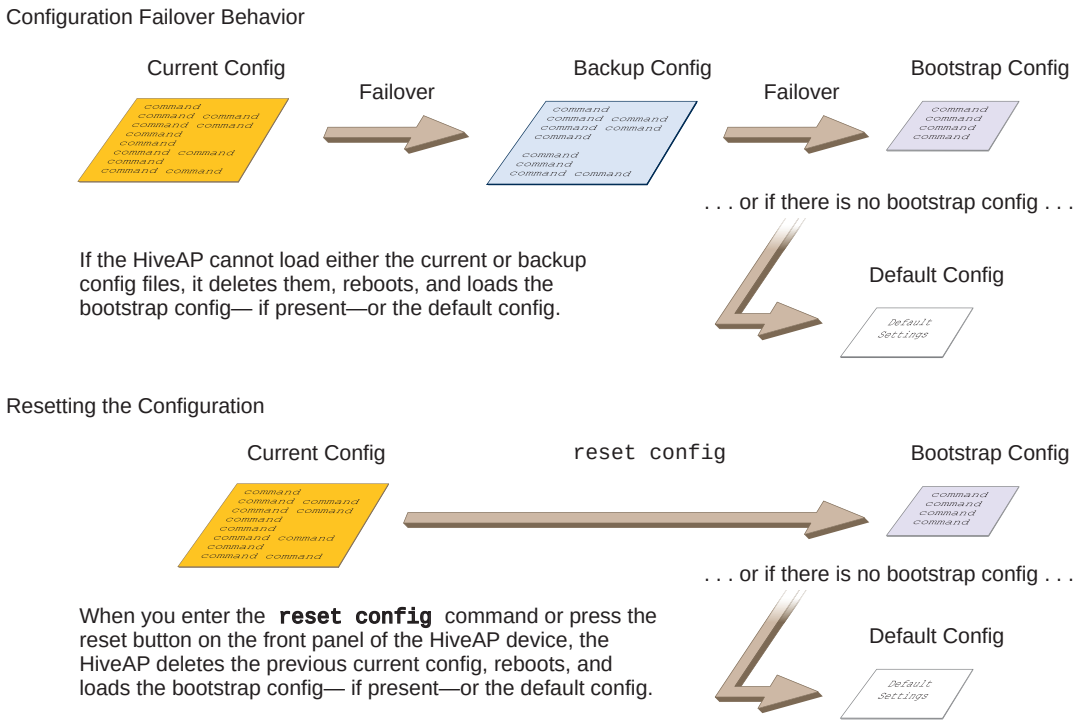
Note: You can disable the ability of the reset button to reset the configuration by entering this command: **`no reset-button reset-config-enable`**

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 128.

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



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 147). 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 9 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 130, 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 133, 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 138, 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 141, 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 147, 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 150. 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 option with the HiveAP product. 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.

- 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

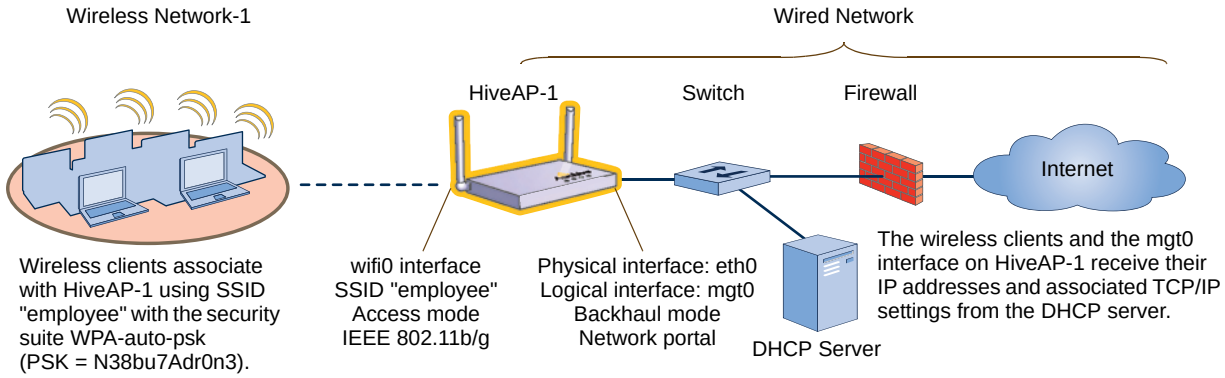
In this example, you deploy one HiveAP (HiveAP-1) to provide network access to a small office with 15 – 20 wireless clients. You only need to define the following SSID (service set identifier) parameters on the HiveAP and clients:

- **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 operates at 2.4 GHz (in accordance with the IEEE 802.11b and 802.11g standards). This example assumes that the clients also support either 802.11b or IEEE 802.11g.

Note: By default, the wifi1 interface is in backhaul mode and operates at 5 GHz to support IEEE 802.11a. To put wifi1 in access mode so that both interfaces provide access—the wifi0 interface at 2.4 GHz and the wifi1 interface 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 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 157.
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. (A HiveAP can create up to seven subinterfaces per interface—14 total.) A HiveAP uses one or two interfaces in access mode to communicate with wireless clients accessing the network, and an 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 superuser.

   `admin root-admin mwebster password 3fF8ha`

   As a safety precaution, you change the default superuser 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 16 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 "Mounting the HiveAP 20" on page 29.
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 (labeled "POE In" for "Power over Ethernet" on the chassis), 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 10.50.1.35 11    54M   -38   wpa2-psk  aes ccm  00:00:56  1     Yes   0     11g
```

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

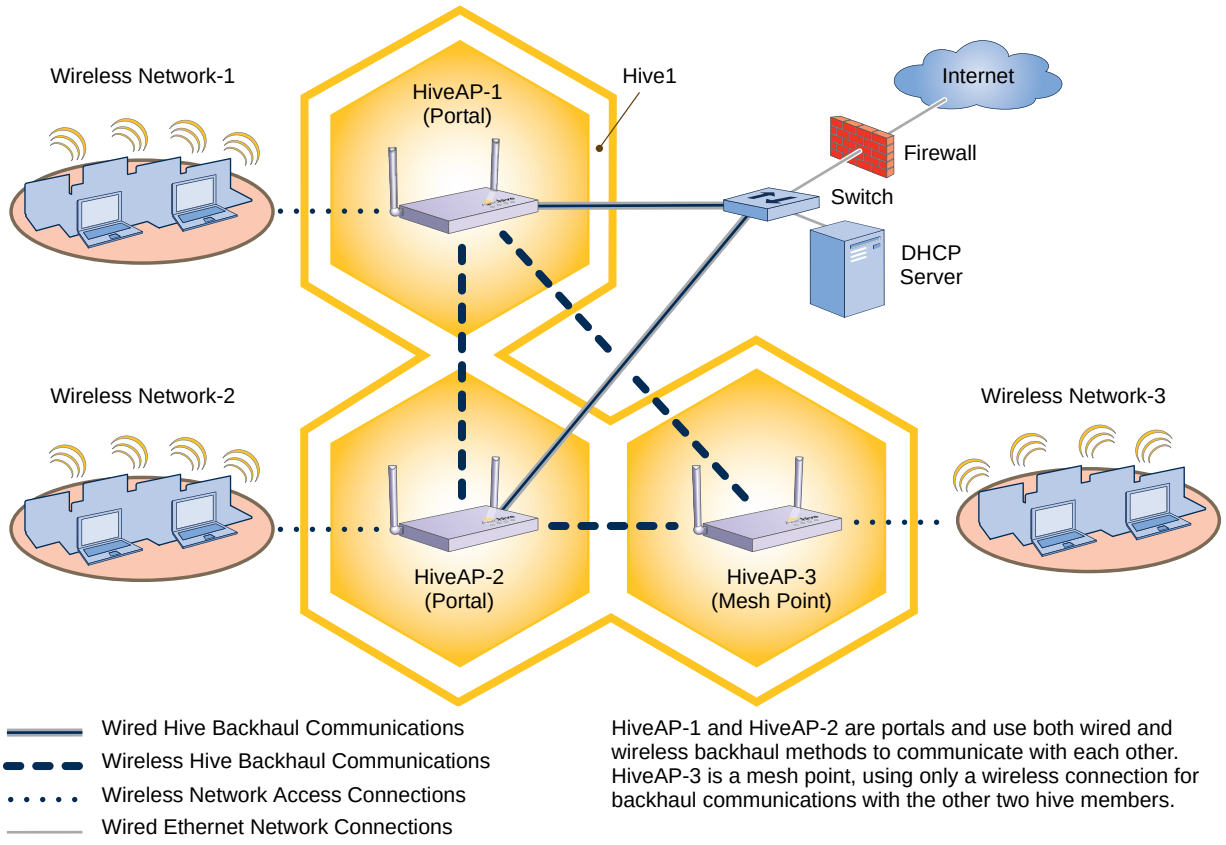
Building on "Deploying a Single HiveAP" on page 130, the office network has expanded and requires more HiveAPs to provide greater coverage. In addition to the basic configuration covered in the previous example, you configure all three HiveAPs to form a hive within the same layer 2 switched network. 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

1. Using the connection settings described in the first example, log in to HiveAP-1.
2. 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 s1r70ckH07m3s`

   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`

3. 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_g0    -       -
Wifi0.1   0019:7700:0024   access     U     11    -     radio_g0  hive1   employee
Wifi1     0019:7700:0028   backhaul   U     149   -     radio_a0    -       -
Wifi1.1   0019:7700:0028   backhaul   U     149   1     radio_a0  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_a0. This is a profile for radio2, which operates in the 5 GHz frequency range (IEEE 802.11a).

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 s1r70ckH07m3s

   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.

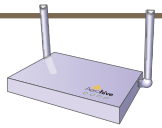
   After HiveAP-2 finishes booting up (indicated when the Power LED changes from steady amber to steady green), it automatically discovers another member of hive1 (HiveAP-1). The two members use a preshared key based on their shared secret (*s1r70ckH07m3s*) to authenticate each other and AES to encrypt 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:

HiveAP-3



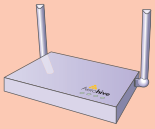
```
show hive hive1 neighbor

Chan=channel number; Pow=Power in dbm;

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

Conn-Time=Connected time; Hstate=Hive State;


Mac Addr        Chan   Rate    Pow    A-Mode   Cipher  Conn-Time  Hstate  Hive
--------------  ----   ----    ----   ------   ------  ---------  ------  -----
0019:7700:0028  149    54M     -16    psk      aesccm  00:04:15   Auth    hive1
0019:7700:0438  149    54M     -16    psk      aesccm  00:04:16   Auth    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 neighbors` command, you can see hive-level and member-level information.

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 assocation process in progress.

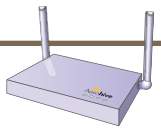
Assocd (Associated) - A HiveAP has associated with the local HiveAP and can now start the authentication process.

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

7. 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

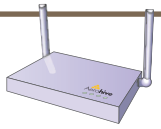


```
show ssid employee station
Chan=channel number; Pow=Power in dbm;
A-Mode=Authentication mode; Cipher=Encryption mode;
A-Time=Associated time; Auth=Authenticated;
UPID=User profile Identifier; Phymode=Physical mode;

Mac Addr        IP Addr     Chan  Rate  Pow  A-Mode    Cipher   A-Time    VLAN  Auth UPID Phymode
--------------  ----------  ----  ----  ---  --------  -------  --------  ----  ---- ----  -------
0016:cf8c:57bc  10.50.1.73  1     54M   -40  wpa2-psk  aes ccm  00:01:46  1     Yes  0     11g

Total station count: 1
```

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

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

   HiveAP-2



MATCH!

```
show roaming cache
Roaming Cache Table:
UID=User profile group ID; PMK=Pairwise Master Key;
TLC=PMK Time Left in Cache; Life=PMK Life;

Roaming for this HiveAP: enabled
Maximum Caching Time:    240 seconds
Roaming hops:            1
Caching update interval: 60 s
Caching update times:    4

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

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.

   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).

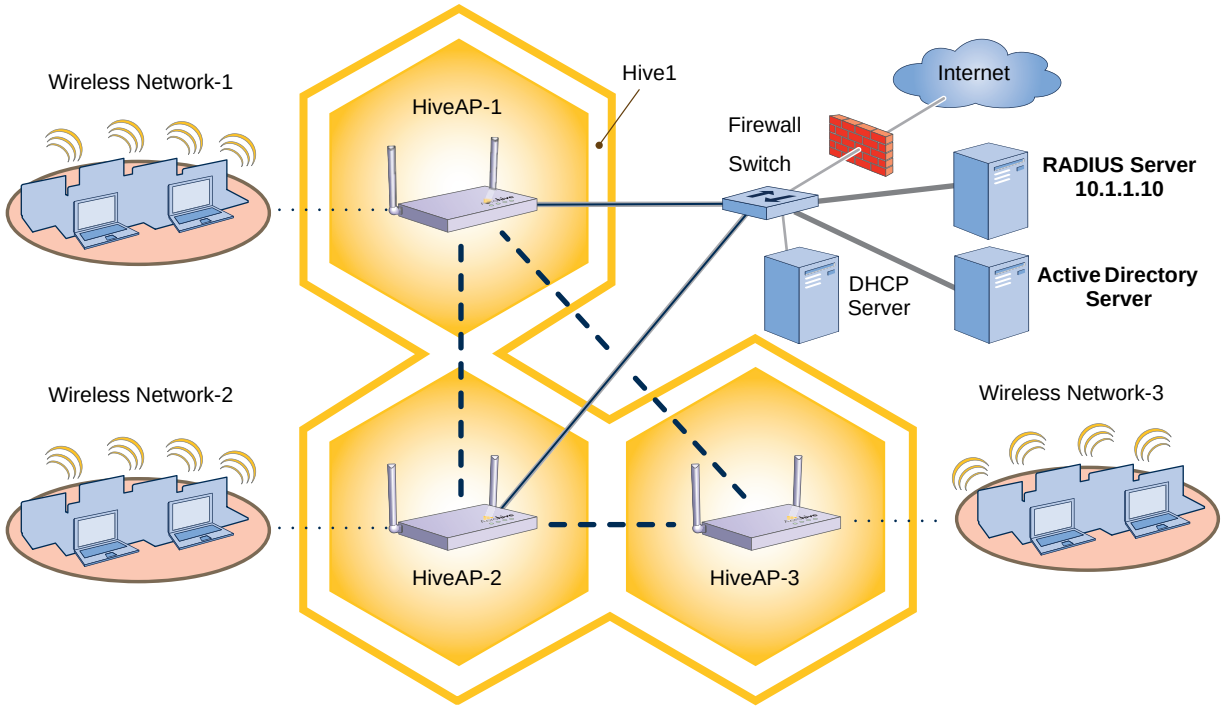
EXAMPLE 3: USING IEEE 802.1X AUTHENTICATION

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



The HiveAPs receive PEAP (Protected EAP) authentication requests from clients and forward them inside RADIUS authentication packets to the RADIUS server at 10.1.1.10. The RADIUS server is in turn linked to the database of the Active Directory server on which all the user accounts have previously been created and stored.

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 s3cr3741n4bl0X
```

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 5).

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 5.

   ```
   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 s3cr3741n4bl0X
   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 5.

   ```
   exit
   ```

4. Log in to HiveAP-3 and enter the same commands.

Step 4 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.

Step 5 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 mgt0 IP addresses (or fully-qualified domain names) and shared secret.

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  Rate  Pow  A-Mode    Cipher   A-Time   VLAN  Auth  UPID  Phymode
--------------  ----------  ----  ----  ---  --------  -------  --------  ----  ----  ----  -------
0016:cf8c:57bc  10.50.1.73  1     54M   -40  8021x     aes ccm  00:02:34  1     Yes   0     11g

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 limited number of voice calls 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 142 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 eight concurrent 64-Kbps VoIP calls:
512 Kbps maximum rate ÷ 64 Kbps/call = 8 calls maximum (more if the codec provides greater compression)

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 increase the bandwidth available for streaming media when there is no competition for it (the default rate for class 5 is 10,000 Kbps). However, you do not set the maximum rate (54,000 Kbps) to ensure that streaming media does not consume all available bandwidth even if it is available.

Class 3 (e-mail)

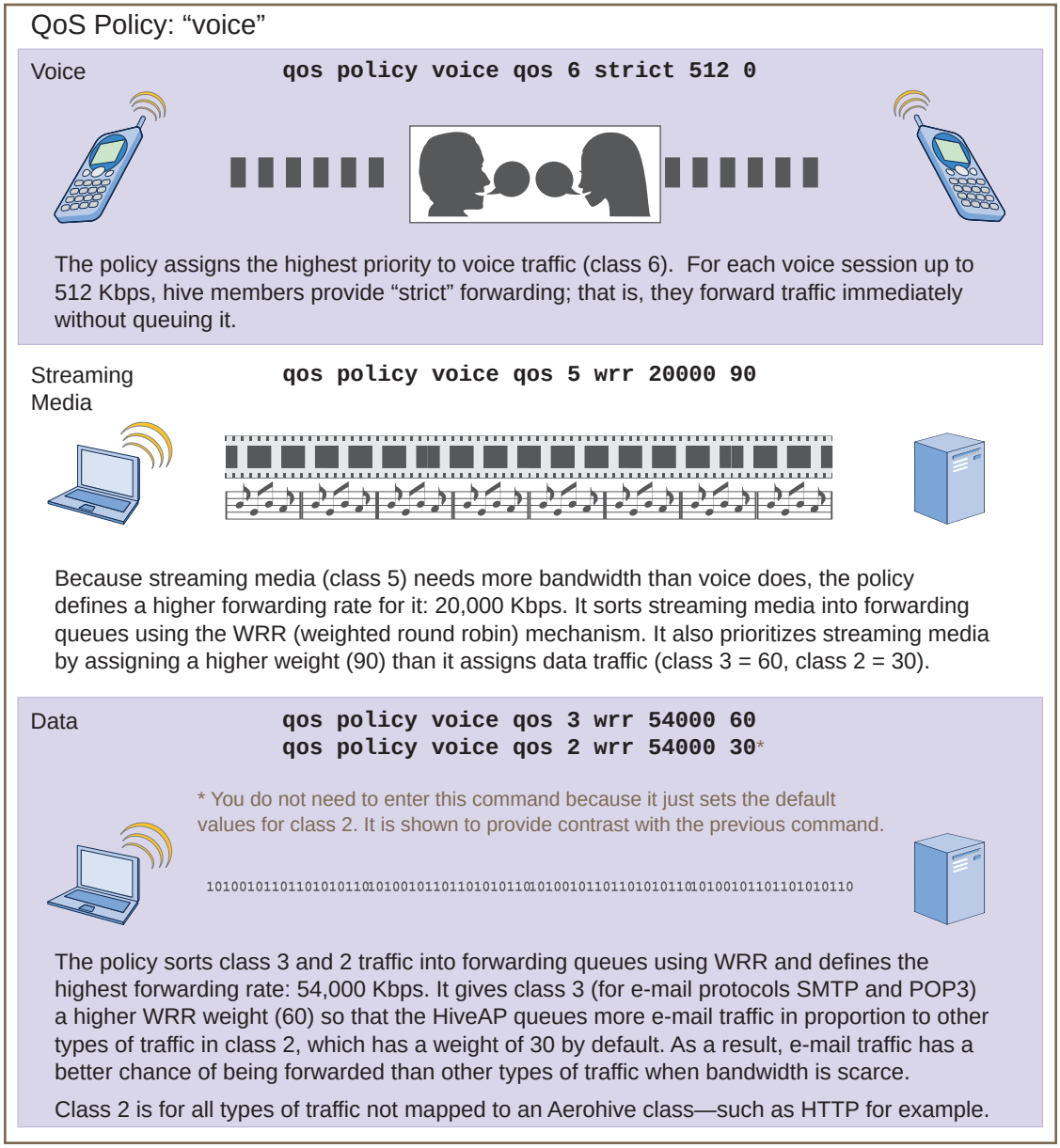
Forwarding: WRR with a weight of 60

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 Kbps (the default)

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 Kbps.

Figure 4 QoS Policy "voice" for Voice, Streaming Media, and Data



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.

2. 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 802.11p 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

1. Create a QoS policy.

   qos policy voice qos 5 wrr 20000 90

   qos policy voice qos 3 wrr 54000 60

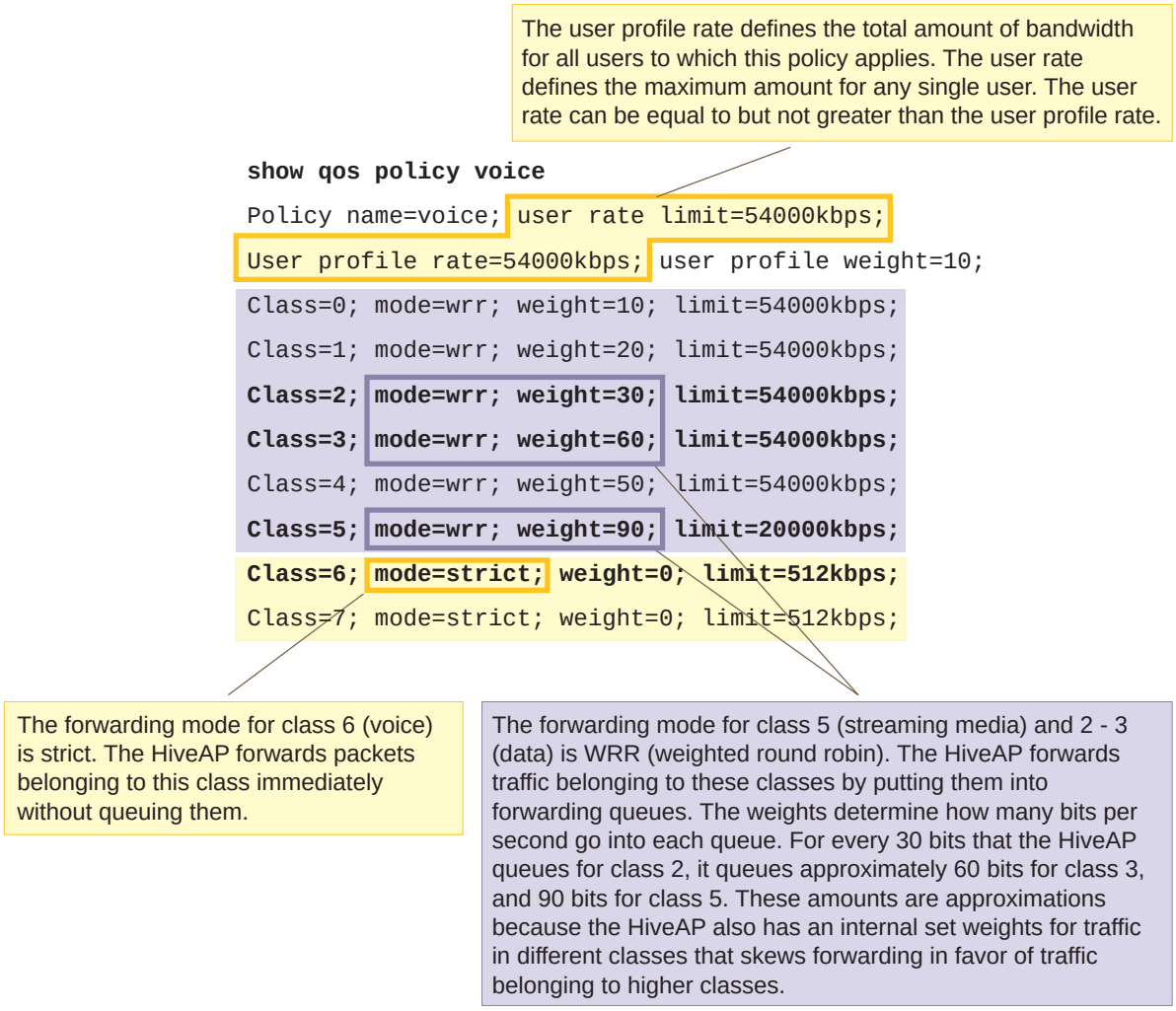
   By default, a newly created QoS policy attempts to forward traffic mapped to classes 6 and 7 immediately upon receipt. This immediate forwarding of received traffic is called "strict" forwarding. To assign strict forwarding to VoIP traffic from phones whose MAC OUI is mapped to class 6, you simply retain the default (top priority) settings for class 6 traffic. 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 for the user group. You also leave the maximum bandwidth for a single user at 54,000 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 on page 145. Note that 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 rate of 54,000 Kbps by default. Because nothing is mapped to classes 0, 1, 4, and 7, their settings are irrelevant.

Figure 5 QoS Policy "voice"



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

   `user-profile employee-net group-id 2 qos-policy voice`

   You apply the QoS policy "voice" to all users belonging to the user-profile "employee-net" with group ID 2. On the RADIUS server, you must configure group ID 2 as one of the RADIUS attributes that the RADIUS server returns when authenticating users (see step 5 on page 146).

   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-id 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
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 54000 60
user-profile employee-net group-id 2 qos-policy voice
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 125, 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 Cwb12o11siNIm8vhD2hs password 8wDamKC1`

   You use the maximum number of alphanumeric characters for the login name (20 characters) and password (16 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 s1r70ckH07m3s`

   `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 130 (*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 130:

```
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 133:

HiveAP-1

```
hive hive1
hive hive1 password s1r70ckH07m3s
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 s1r70ckH07m3s
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 s1r70ckH07m3s
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 138:

HiveAP-1

```
aaa radius-server first 10.1.1.10 shared-secret s3cr3741n4bl0X
ssid employee security protocol-suite wpa-auto-8021x
save config
```

HiveAP-2

```
aaa radius-server first 10.1.1.10 shared-secret s3cr3741n4bl0X
ssid employee security protocol-suite wpa-auto-8021x
save config
```

HiveAP-3

```
aaa radius-server 10.1.1.10 shared-secret s3cr3741n4bl0X
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 141:

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
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 54000 60
user-profile employee-net group-id 2 qos-policy voice
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
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 54000 60
user-profile employee-net group-id 2 qos-policy voice
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
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 54000 60
user-profile employee-net group-id 2 qos-policy voice
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 147:

bootstrap-security.txt

```
admin root-admin Cwb12o11siNIm8vhD2hs password 8wDamKC1
hive hive1
hive hive1 password s1r70ckH07m3s
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 10 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
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
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 HiveManager Management of HiveAPs

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
CAPWAP*	HiveAP mgt0 interface	HiveManager MGT or LAN port	17 UDP	12222	12222	Required for HiveAPs to discover the HiveManager and send it various reports
NTP	HiveAP mgt0 interface	HiveManager MGT or LAN port	17 UDP	1024 - 65535	123	Required for HiveAP time synchronization with the HiveManager

* Control and Provisioning of Wireless Access Points

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
SNMP	HiveAP mgt0 interface	HiveManager MGT or LAN ports, or SNMP manager	17 UDP	1024 - 65535	161	Required for reporting alarms and events to HiveManager and to an SNMP manager
SNMP traps	HiveAP mgt0 interface	HiveManager MGT or LAN ports, or SNMP manager	17 UDP	1024 - 65535	162	Required for sending SNMP traps to HiveManager or an SNMP manager
SSHv2	HiveManager MGT port	HiveAP mgt0 interface	6 TCP	1024 - 65535	22	Required for the HiveManager to manage and upload files to HiveAPs

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.
FTP (control)	HiveManager MGT port	FTP server	6 TCP	1024 - 65535	21	Required for updating HiveManager software from an FTP server
FTP (data)	FTP server	HiveManager MGT port	6 TCP	20	1024 - 65535	Required for updating HiveManager software from an FTP server
HTTPS	management system	HiveManager MGT port	6 TCP	1024 - 65535	443	Required for administration through the HiveManager GUI
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 admins
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
Telnet	management system	HiveAP mgt0 interface	6 TCP, 17 UDP	1024 - 65535	23	Required 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 and downloading files from HiveAPs

* This is the default destination 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.

The following list of country codes is provided for your convenience.

Countries and Country Codes

Albania 8

Algeria 12

Argentina 32

Armenia 51

Australia 36

Austria 40

Azerbaijan 31

Bahrain 48

Belarus 112

Belgium 56

Belize 84

Bolivia 68

Bosnia and Herzegovina 70

Brazil 76

Brunei Darussalam 96

Bulgaria 100

Canada 124

Chile 152

China (People's Republic of China) 156

Colombia 170

Costa Rica 188

Croatia 191

Cyprus 196

Czech Republic 203

Denmark 208

Dominican Republic 214

Ecuador 218

Egypt 818

El Salvador 222

Estonia 233

Faeroe Islands 234

Finland 246

France 250

France2 255

Georgia 268

Germany 276

Greece 300

Guatemala 320

Honduras 340

Hong Kong (S.A.R., P.R.C) 344

Hungary 348

Iceland 352

India 356

Indonesia 360

Iran 364

Iraq 368

Ireland 372

Israel 376

Italy 380

Jamaica 388

Japan 392

Japan1 (JP1) 393

Japan2 (JP0) 394

Japan3 (JP1-1) 395

Japan4 (JE1) 396

Japan5 (JE2) 397

Japan6 (JP6) 399

Japan7 (J7) 4007

Japan8 (J8) 4008

Japan9 (J9) 4009

IJapan10 (J10) 4010

Japan11 (J11) 4011

Japan12 (J12) 4012

Japan13 (J13) 4013

Japan14 (J14) 4014

Japan15 (J15) 4015

Japan16 (J16) 4016

Japan17 (J17) 4017

Japan18 (J18) 4018

Japan19 (J19) 4019

Japan20 (J20) 4020

Japan21 (J21) 4021

Japan22 (J22) 4022

Japan23 (J23) 4023

Japan24 (J24) 4024

Jordan 400

Kazakhstan 398

Kenya 404

Korea (North Korea) 408

Korea (South Korea, ROC) 410

Korea (South Korea, ROC2) 411

Korea (South Korea, ROC3) 412

Kuwait 414

Latvia 428

Lebanon 422

Libya 434

Liechtenstein 438

Lithuania 440

Luxembourg 442

Macau 446

Macedonia (The Former Yugoslav Republic of Macedonia) 807

Malaysia 458

Malta 470

Mexico 484

Monaco (Principality of Monaco) 492

Morocco 504

Netherlands 528

New Zealand 554

Nicaragua 558

Norway 578

Oman 512

Pakistan (Islamic Republic of Pakistan) 586

Panama 591

Paraguay 600

Peru 604

Philippines (Republic of the Philippines) 608

Poland 616

Portugal 620

Puerto Rico 630

Qatar 634

Romania 642

Russia 643

Saudi Arabia 682

Singapore 702

Slovakia (Slovak Republic) 703

Slovenia 705

South Africa 710

Spain 724

Sri Lanka 144

Sweden 752

Switzerland 756

Syria 760

Taiwan 158

Thailand 764

Trinidad y Tobago 780

Tunisia 788

Turkey 792

U.A.E. 784

Ukraine 804

United Kingdom 826

United States 840

United States (Public Safety; FCC49) 842

Uruguay 858

Uzbekistan 860

Venezuela 862

Vietnam 704

Yemen 887

Zimbabwe 716