AIRFLOW NETWORKS

The AirSwitch 1200

Release 1.0

System Manual

Notice

The information contained in this manual is Proprietary and Confidential. No contents of this document may be disclosed, reproduced, or distributed without the express written permission of the copyright holder, AirFlow Networks, Inc.

All reasonable effort was made to ensure that the information contained in this manual was complete and accurate at the time of publication. However, AirFlow Networks, Inc. cannot be held liable for any errors or omissions. Changes and/or corrections to the information contained in this document will be published in future versions.

Any changes or modifications to the AirSwitch or AirHubs not expressly approved by AirFlow Networks, Inc., may void the user's authority to operate this equipment.

Contact Information

AirFlow Networks, Inc.
455 West Maude Avenue
Sunnyvale, CA 94085

408-524-3100
www.airflownetworks.com

We welcome feedback on this manual: techpubs@airflownetworks.com

Published by AirFlow Networks, Inc.
Sunnyvale, California

DCN: as1200sm-B11

AirFlow NETWORKS

Contents

DCN: as1200sm-B11

DCN: as1200sm-B11

DCN: as1200sm-B11

DCN: as1200sm-B11

DCN: as1200sm-B11

I. Product Features

This manual provides comprehensive information on installing, configuring and using the AirFlow AirSwitch 1200 product family, from AirFlow Networks. We start by providing a high-level description of product features, including:

- an overview of the AirFlow distributed AP architecture;
- a description of AirSwitch and AirHub hardware (page 10); and
- a summary of the AirFlow system's main features (page 13).

Details on configuring and using all features are provided in later chapters of this manual, as indicated by cross-references.

The AirFlow Architecture

The AirFlow AirSwitch provides your enterprise with 802.11b wireless LAN connectivity similar to that of standard Access Point (AP) products available on the market today. There is, however, one critical difference that sets it apart: the AirFlow distributed architecture. Whereas ordinary APs integrate radio and security protocols in a single unit, the AirFlow AP distributes this intelligence across a central AirSwitch connected by Ethernet cables to multiple packet antennas called *AirHubs*. In 802.11 terms, the individual AirHubs are not APs; rather, the whole coverage area of all AirHubs constitutes a single AP, through which wireless clients can roam seamlessly without needing to reauthenticate and reassociate.

Because each of these packet antennas creates a coverage area for wireless clients, they combine to cover a significantly larger area than a standard AP does. Because the AP consists of many overlapping coverage areas, wireless clients can roam among them while the switch monitors signal quality and hands the network connection over from one AirHub to another as the client moves. Because these handovers are completely transparent, mobile users enjoy a wider mobile coverage area than would be possible with standard APs.

Because AirHubs can be more closely spaced than standard APs, clients can be closer on average to an AirHub than they would be to a standard AP, which means faster data rates, higher throughput, and longer battery life. In this situation, wireless clients can be connected to more than one AirHub at the same time, which eliminates the single point of failure characteristic of ordinary APs. And because AirHubs connect to existing Ethernet lines and offer plug-and-play autoconfigura-

tion, they offer unparalleled flexibility in expanding or reshaping your wireless LAN whenever the need arises.

Hardware Description

This section provides a description of the hardware features of the AirSwitch and the AirHubs.

AirSwitch Hardware

Figure 1-1, below, shows the front panel of the AirSwitch 1211. The numbered call-outs in the figure refer to the following text description.

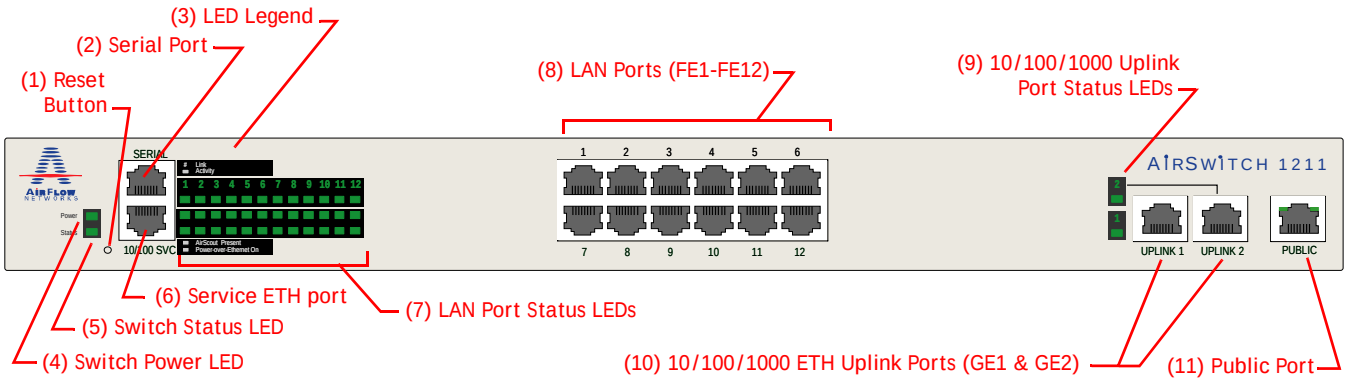
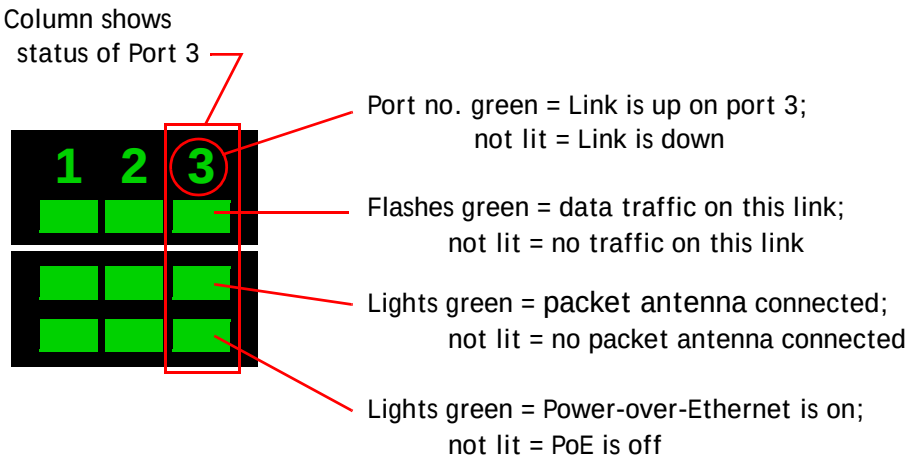


Figure 1-1: AirSwitch, Front Panel Features

1. **Reset Button:** This can be used to force a reboot of the AirSwitch, to original factory defaults.
2. **Serial Port:** Used to connect a serial console for management purposes.
3. **LED legend:** Explains the meanings of the four LAN port status LEDs (see #7 below).
4. **Switch Power LED:** Will light steady green when switch system power is on, not lit when system power is off.
5. **System Status LED:** Will light steady amber during bootup and POST, and steady green when switch system has finished bootup and POST and is running normally. Not lit while system is booting up or is not running for any reason.
6. **Service ETH Port:** Used to connect to a local console for management and diagnostic purposes.
7. **LAN Port Status LEDs:** Display the status of the LAN ports. These LEDs are arranged in a grid with each column representing one LAN port. There are four LED indicators per each port; their meaning is shown in the illustration below.

DCN: as1200sm-B11



8. **LAN Ports:** Used to connect CAT-5 cables to network entities such as packet antennas, PCs, hubs, switches, 3rd-party access points, etc.

9. **Gb Uplink Port Status LEDs:** Display the status of the Gb uplink ports. These work just like the top two LAN port LEDs: port number lights green if link is up on the port, not lit if link is down; rectangular LED rapidly flashes green when data traffic is passing on this link, and is not lit when there is no data traffic.

10. **Gb Uplink Ports:** Used to connect the 10/100/1000 line uplink to the backbone router.

11. **Reserved Port:** This port is reserved for a future release feature.

Switch Fans

The switch chassis is cooled by a set of five DC fan units that vent the chassis from the left side to the right. The fans run at half speed at temperatures below 35° C., and at full speed from 35° to 50° C. When the temperature rises above 50°, an immediate power shutdown will occur, turning off the entire switch, including the fans, and protecting the components from overheating.

AC Power

The power cord on the back of the AirSwitch connects to the power supply unit, which has an integrated On/Off switch that controls all power for the system. The power supply also has an integrated fuse unit.

AirHub 100 Hardware

The AirHubs, by design, are relatively simple devices with very few features. Figure 1-2 and Figure 1-3, below, represent the AirHub back panel and LEDs. The numbered callouts in the figure refer to the text description of all features.

Back Panel

1. **Downlink Bypass Port**: This port is available for plugging in a desktop PC or other network device, if convenient. All traffic to and from this device will be passed through the AirHub without any processing, and with no effect on the performance of either the AirHub or the second device.

2. **Uplink ETH Port**: This is the connection to the LAN wall jack, using a standard Ethernet cable.

3. **Local AC Power**: If you are not using PoE, you can plug in the local AC converter in here. If you are using PoE for this AirHub, the local power port will be disabled.

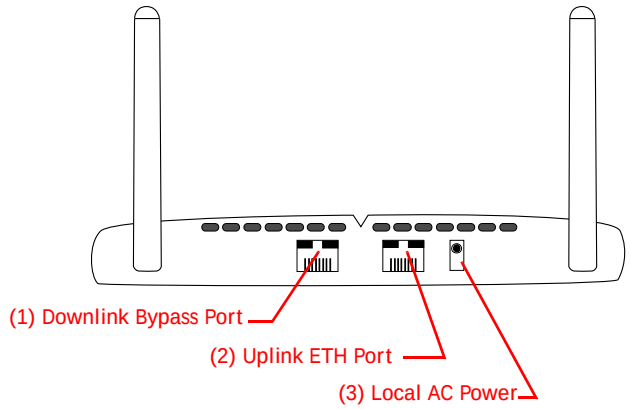


Figure 1-2: AirHub 100, Back Panel

Note: You must **never** use any AC converter other than the one supplied by AirFlow Networks. Using an unapproved adaptor is likely to cause irreparable damage to the AirHub.

LED Functions

1. **Bypass Port Traffic**: Lights solid green when the AirHub detects a normal link to a wired PC, through the Bypass Port.

2. **Radio Transmit Traffic**: Blinks rapidly green when the AirHub is sending RF traffic out across the wireless link.

3. **AirHub Status**:

   - Solid red: power on, awaiting download of firmware from AirSwitch
   - Blinking red: has not received firmware within normal time-out interval

DCN: as1200sm-B11

- Solid amber: download and self-test in progress
- Solid green: download and self-test successful, AirHub in normal operation.

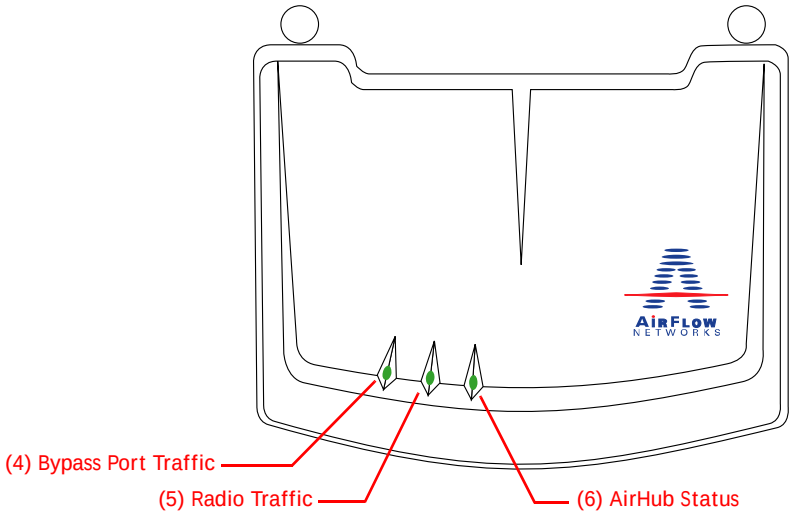


Figure 1-3: AIrHub 100, LED Functions

System Features

The features listed below have been implemented in the 1.0 release of the AirSwitch 1200.

Packet Antenna Support

The current version can support one or multiple AirHubs at each of its twelve 10/100 Ethernet ports. Multiple AirHubs can be connected to a single port by using an external third-party switch or LAN hub. A switch is preferable, as it reduces the extraneous data traffic on each packet antenna.

Power over Ethernet

AirHubs receive power over Ethernet from the AirSwitch. PoE is always available on all ports, but is device-sensitive, and will only be sent if the AirSwitch detects a connection to a device, such as an AirHub or a VoIP phoneset, that requires it. PoE will not be sent to ordinary network devices like PCs or printers.

If you set up an intermediate hub or switch between the AirSwitch and one or more packet antennas, the PoE will terminate at this hub or switch, and will not be available for any packet antennas downlink from it. For this reason, each AirHub is equipped with a power converter for plugging into a local AC power supply, as an alternative to PoE.

Note: You should never use a third-party PoE power injector to send power to an AirHub.

Autostart and AutoRestart

Starting up individual AirHubs requires no action from the system administrator. As soon as the switch is booted up, it detects all connected packet antennas, sends them all required configuration parameters, and places them in Active mode.

From this point on, the switch continuously monitors the status of all attached AirHubs through a heartbeat mechanism. If it detects that a packet antenna has stopped running for any reason, it will automatically resend configuration settings and restart the AirHub.

Bypass Port

Each AirHub has a bypass port that lets you plug it into an Ethernet jack that is already in use by another device. For example, if you need to install an AirHub in a room with only one jack that is already in use by a desktop PC, simply unplug the PC, plug in the AirHub, and plug the PC back into the AirHub's bypass port. The PC's traffic will then pass normally back to the network with no effect on performance, of either the PC or the AirHub.

Wireless Performance

The current version has been satisfactorily tested with a wide variety of wireless devices, client cards, and card drivers. Coverage range is comparable to currently available 802.11b AP products; although it will vary according to your facility's topology, operation should be reliable at a range of 50 to 100 meters. All four standard data rates—1, 2, 5.5, and 11 Mbps—are supported.

Many RF attributes of the AirHubs, such as channel, transmit power, data rate, beacon interval, and so on, are configurable, though not individually. That is, changes to any packet antenna's operational settings will apply to all PAs currently connected to the AirSwitch.

Seamless Roaming

The AirSwitch supports seamless roaming from one active packet antenna to another, based on data transfer quality. When a device moves from one coverage area toward another, the switch detects that the wireless connection is degrading in the first area and improving in the second and hands the connection over to the new PA before the performance drop becomes noticeable to the user. Again, because all coverage areas are part of the same distributed access point, this does not involve disassociation from and reassociation to the network, making the handover completely transparent to the user.

Access Control List

Before any client devices can associate with the AirSwitch, they must be added to the Access Control List. This mechanism provides basic security, guarding against wireless devices in the coverage area casually attaching to the wireless network. However, because this is a relatively low level of security that can be bypassed by a knowledgeable hacker, additional security mechanisms should be installed on the network.

DCN: as1200sm-B11

For a more reliable security solution, AirFlow currently recommends using the AirSwitch in combination with a layered security regimen incorporating technologies such as 802.1x and IPSec.

Individual entries to the ACL can be added one at a time through the CLI. Existing lists can be imported from an Excel spreadsheet, for convenience and accuracy. For details, see “Importing Entries into the ACL” on page 35.

WEP Security

The AirSwitch supports standard 40-bit and 128-bit WEP encryption and authentication, for additional security.

CLI Management Interface

You can view and change your AirSwitch’s configuration settings through an industry-standard Command Line Interface (CLI) on a locally connected console, or remotely via telnet connection. The CLI commands currently enabled are described in detail in Appendix A, "CLI Reference".

Layer 2 Switching Features

The AirSwitch supports the following standard Layer 2 features:

- Port-based VLANs
- Class of Service levels
- Port Mirroring
- Packet Storm Control
- Spanning Tree Protocol

Details on these features are provided in Chapter IX, "Layer 2 Switching Features".

Statistical Monitoring

This release provides a set of statistical counters, which can be viewed via the CLI. These include statistics for individual packet antennas level, individual ports or interfaces, and the switch as a whole.

The statistical monitoring feature is used through the SHOW STATISTICS CLI command, as described in Table A-1 on page 122. All counters can be manually reset as desired. The following statistics are available in this release:

Packet antenna-level statistics:

- PA uptime
- Number of client devices associated
- Number of data frames sent
- Number of data frames received
- Number of retransmits
- Number of CRC errors received
- Number of failed packets
- Number of ACK failures

Interface-level statistics:

- Number of inbound octets, unicast packets, and non-unicast packets received
- Number of outbound octets, unicast packets, and non-unicast packets received

Switch-level statistics:

- Number of beacons sent
- Number of authentication requests received
- Number of authentication requests rejected
- Number of association requests received
- Number of association requests rejected

Current Status Monitoring

In addition to the statistics listed above, y ou can use the CLI to display:

- The current Access Control List
- A list of all currently attached wireless devices
- A list of all currently operating packet antennas, and their status
- Status of all interfaces
- The current settings for all available switch configuration parameters
- Current contents of system log in NVRAM

Configuration Export

You can save and reload multiple switch configurations, in addition to the factory default and the currently running configurations. For details on using this feature, see “Managing Configuration Files” on page 65.

Diagnostic Logging

To aid in toubleshooting, the AirSwitch can generate a diagnostic log of recent switch events and software component statuses, which can be sent to AirFlow technical support engineers to help them analyze and solve potential problems. You can generate these logs with the SHOW TECH command (see “Trouble shooting” on page 56.).

Public Port

This is a special feature that allows visitors to your enterprise to attach to and use the wireless network, through a Gb uplink connection that is completely isolated from the backbone network. Because this port bypasses the network’s firewall and the AirSwitch’s standard VPN termination, visiting users connect directly to the Internet, and have no access to any of your network resources. Because this port is password protected, it lets you provide your visitors with the benefit of simple wireless access from inside your enterprise, on a selective and controlled basis. For details, see “Using the Public Port” on page 57.

DCN: as1200sm-B11

FCC Compliance

The AirSwitch 1200 has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules and ICES 003. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Any changes or modifications to the AirSwitch or AirHubs not expressly approved by AirFlow Networks, Inc., may void the user's authority to operate this equipment.

DCN: as1200sm-B11

II. Planning Your System

Network Architecture

Typically, the AirSwitch 1200 should be installed in your network at the network edge, as an edge switch would be. All AirHubs are connected only to the AirSwitch's 10/100 ports (either directly or through an intermediate hub or switch), rather than to any other devices downstream from the AirSwitch. Desktop PCs or other Ethernet devices may be connected to the AirSwitch as well. Figure 2-1 illustrates a typical deployment.

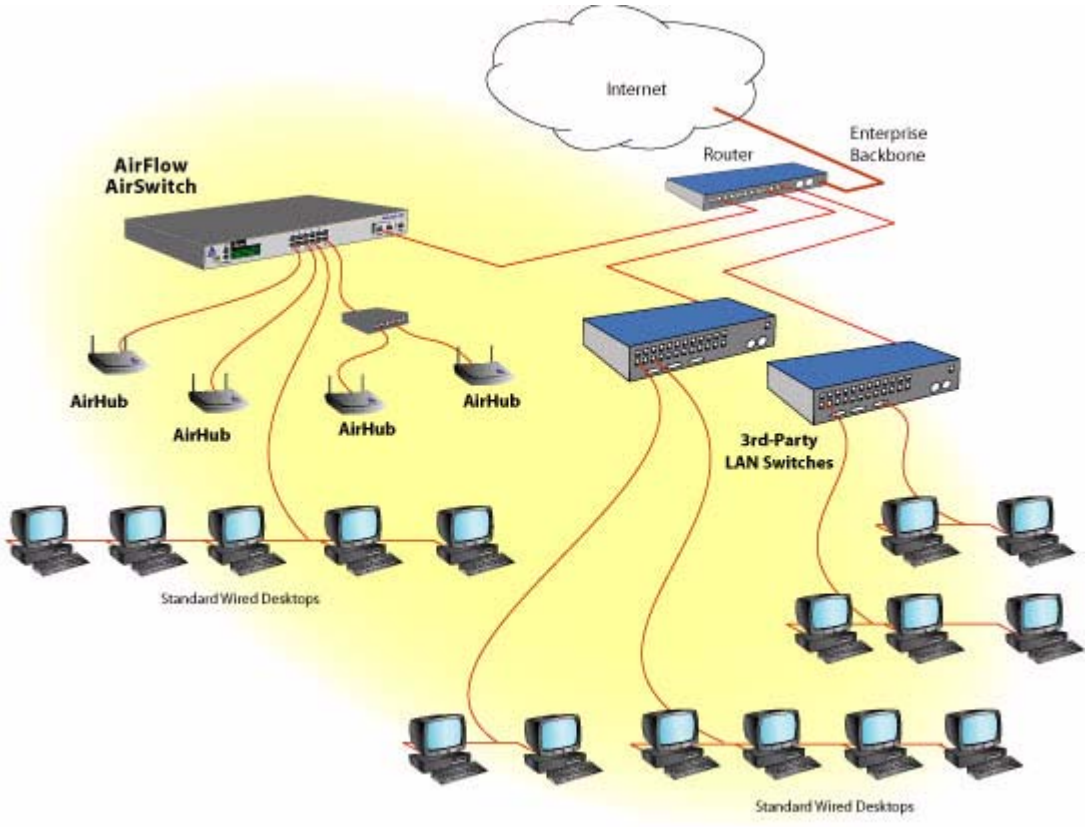


Figure 2-1: Typical AirSwitch Network Architecture

The defining aspect of this design is that all AirFlow Transport Protocol (ATP) traffic between the AirHubs and the AirSwitch passes only through the downlink Ethernet

ports—that is, it terminates at the AirSwitch, and never passes out the uplink Gb port.

Wireless Network Planning

One of the benefits of the AirFlow distributed architecture is that it can be deployed in a large enterprise with very little detailed site planning or technically complex RF surveys. This is so because PAs are relatively inexpensive, and can be distributed with large degrees of overlapping coverage, without concern about interference or maximizing coverage. Moreover, since packet antennas simply plug into existing Ethernet cables and can easily be moved later, there is less concern that they be placed in exactly the optimum location during your initial installation.

Nevertheless, there are a few considerations you should make before you begin your installation. These are discussed in this section.

Packet Antenna Coverage Cells

It is helpful to think of your WLAN like a miniature cell phone network, consisting of overlapping coverage cells. Stationary wireless devices will usually be covered by more than one cell, but will connect to the network through whichever PA is closest and so provides the best data throughput. Moving devices will transparently roam from one cell to another, just as your cell phone does if you use it while you drive.

Cell Shape

For planning purposes these cells may be thought of as basically circular, though technically they are irregularly shaped due to interference from objects in the environment and from other radio signals and noise. Because the radio coverage extends in three dimensions, the cells actually are spherical, and in a multi-floor building will usually extend to the floors above and below. In a multi-floor enterprise this may represent a benefit; if your enterprise only occupies one floor, this overlap is not a problem since AirFlow's multi-level security mechanisms will prevent any unauthorized use of the WLAN.

Cell Size

As with standard 802.11 access points, the wireless coverage of the AirHub 100 is influenced by environmental barriers such as walls, structural supports, elevator banks and so on. In all cases, the coverage radius will be wider in an open space, and will be reduced in more closed spaces. In general, the coverage of a packet antenna is comparable to that of a standard 802.11b access point.

Number of PAs

The standard system starts with one AirSwitch and four PAs. If these are not adequate to cover your enterprise, simply install more PAs, which can be purchased separately.

Technically, each AirSwitch 1200 can support up to 60 PAs. This limitation is primarily driven by processor performance and memory requirements on the system. In future versions, new limits will be provided as the system designs expand. You have the option of connecting each packet antenna either directly to a port on the switch

DCN: as1200sm-B11

(through a patch panel), or indirectly, through an intermediate switch or hub in your network. Because there are 12 ports, you can directly connect a maximum of 12 packet antennas; if you want to connect more, you will need one or more intermediate switches.

Powering the PAs

Power over Ethernet is always available, but is sent as needed. That is, the AirSwitch will send PoE whenever it detects a network device, such as an AirHub, that requires it. If you connect to devices that do not require PoE, such as a switch, PC or a printer, the AirSwitch will recognize it and will not send PoE out that port.

All AirHubs connected directly to the switch can run on PoE. AirHubs connected via an intermediate switch or hub cannot use PoE, but will have to be plugged into local AC wall sockets using the AC adapter unit. This will require a wall socket close enough to the LAN jack where you plug in such AirHubs. Though this will usually not be a problem, it is something to bear in mind when planning your AirHub locations.

Note: You must **never** use any AC adapter other than the one supplied by AirFlow Networks. Using an unapproved adaptor is likely to cause irreparable damage to the AirHub. Also, you should never use a third-party power injector to sent PoE to an AirHub.

Interference Considerations

As you select locations for the AirHubs, bear in mind that like any radio transmitters they will be affected by their physical environment, and you are better off locating them in open areas away from solid barriers. On top of a cubicle partition in the interior of a large, open room, for example, is an ideal position. As you locate your AirHubs, bear in mind the following general guidelines:

- Solid walls such as elevator banks, stairwells, concrete bearing walls, and similar high density impediments will cause more radio interference than non-bearing, interior dividing walls.
- For interior walls, new construction of drywall on metal studs will produce more interference than older walls with wooden studs.
- AirHub performance can be reduced by interference from other radio sources, such as servers and switches (concentrated in your switch closet), and microwaves ovens.

Exterior Walls

Bear in mind that if PAs are placed near exterior walls, potentially large portions of the coverage cells will extend outside the building. This may be desirable—you may want to provide wireless coverage to a courtyard or patio area, for example. If you don't want to do this, however, it represents wasted coverage, and you would do better to place PAs further toward the interior of the space.

Again, no matter how far your coverage extends outside the building, this does not represent a network security threat, as long as you enable at least basic security mechanisms.

FCC Exposure Guidelines

It is the responsibility of the installer and user of the AirFlow AirSwitch 1200 to guarantee that all AirHub 100s are operated at least 20 centimeters from any person. This is necessary to insure that the product is operated in accordance with the RF Guidelines for Human Exposure which have been adopted by the Federal Communications Commission. The device shall not be co-located with other transmitters.

Rearranging and Expanding your Network

Again, because AirHubs are automatically detected and monitored by the AirSwitch, you can simply change their location if you observe any areas of relatively low coverage or performance. You can also extend the coverage area by plugging in new PAs, or increase the density in a current coverage area by adding PAs. The latter should generally improve throughput performance for individual users, since performance is dependent on distance from the PA.

DCN: as1200sm-B11

III. Setting Up Your System

This chapter describes the process of configuring the basic parameters of your AirSwitch, so that wireless clients can begin using it securely.

Your AirSwitch 1200 FlashCard outlines the minimum installation and configuration procedure, using a local console. The present chapter includes all the information in that FlashCard, plus additional detail and instructions on setting up the telnet connection for remote administration.

The process begins as soon as you connect a local console to the management port, and boot up the AirSwitch. At this point the AirSwitch detects that you need to perform an initial configuration, and prompts you with a series of questions which will guide you through the initial, bare minimum configuration you need to start and connect to the switch. Once this is done, the system presents the standard CLI command line, where you can complete your initial configuration.

The entire process should take ten or twenty minutes.

Physical Connections

Once you have mounted the AirSwitch in its rack location, make all the physical wiring connections to the AirSwitch as described below. All connections are represented in Figure 3-1.

1. Power up the AirSwitch

Connect the AC power cord to the power module on the back panel of the AirSwitch, on the far left side. Plug in the cord, and turn on the main power switch.

2. Connect to the Network Backbone

Connect a standard CAT-5 cable to the Gb Ethernet port on the right side of the front panel (labeled UPLINK). Connect the other end to your backbone network router.

3. Connect 10/100 Lines

Plug as many standard CAT-5 Ethernet cables into as many of the front 10/100 ports as you want to use to connect to AirHubs. (Ordinarily these will go through a patch panel.)

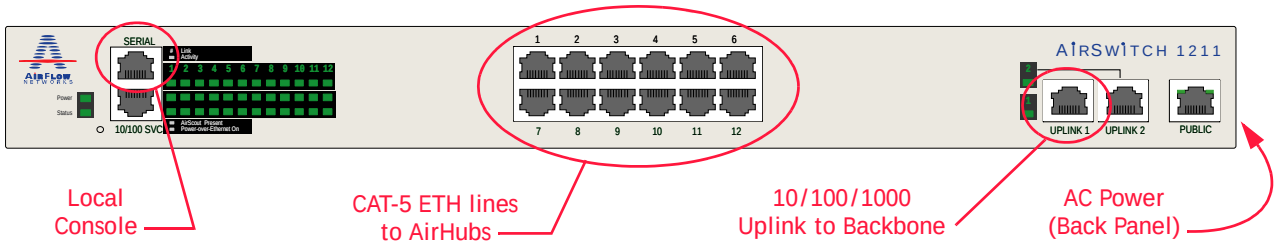


Figure 3-1: Physical Connections

4. Connect a Local Console

Connect a console to the management port on the left side of the front panel (labeled SERIAL), using a standard CAT-5 cable with RJ-45 connector. This is the port you must use for your initial configuration.

5. Connect to the SVC Port

Connect a standard CAT-5 cable to the SVC port on the left side of the front panel, and connect the other end to your backbone network router. Once you assign an IP address to this port during your initial configuration, you can use this connection for routine remote management.

At this point you are ready to begin configuration, using the Initial Configuration Dialog.

The Initial Configuration Dialog

The first time you boot up the AirSwitch, it checks for a configuration file, and if it does not find one it launches a helpful Initial Configuration Dialog. This dialog prompts you for the parameter values that are necessary for the switch to operate and connect to wireless clients.

Default Values

Each line of the dialog presents a prompt. At some prompts, a default value will be displayed in [square brackets]; this means you have the option of accepting that value by pressing Enter, or changing it by providing an alternative and then pressing Enter.

Connecting

In order to provide this configuration information, you must have a local console connected to the management port of the AirSwitch. It is not possible to set up a telnet connection to the switch or use the CLI in any way, until this initial configuration is performed.

DCN: as1200sm-B11

6. Assign Service Port IP Address

If you have a local console connected, when you first power up the AirSwitch you will see the following prompt:

```
************************************************

Welcome to AirSwitch Initial Configuration Dialog!

Enter IP address for SVC Port:
```

Provide the static IP address you want to assign to the AirSwitch's service port. This is the address you will use for establishing a telnet connection, for all management functions. (You can change this later if you like with the IP ADDR command, in the Interface submode.)

You will also be prompted for a subnet mask for this address:

```
Enter network mask for SVC Port:
```

Type the subnet mask for the management address. Ordinarily this will be 255.255.255.0.

7. Set Enable Password

Next, you will be prompted for the Enable password. This is the password that allows administrators to navigate from the initial Main level of the CLI, to the next lower Enabled level. (See "The CLI Structure," on page 93.) The dialog will prompt you to type the password twice:

```
Enter enable password:

Re-enter enable password:
```

You can use up to 30 letters, numbers, symbols and spaces; do not use control characters. If you type the same string twice, the password will be saved and you will see the next prompt.

8. Define the SSID

The next prompt,

```
Enter SSID [AFNworks]:
```

asks you to provide a new SSID, or to accept the default value *AFNworks*. Technically you do not need to change this, but you should replace it with more suitable ID that identifies your company or organization. (For details about SSIDs, see "Managing VLANs, SSIDs, and Interfaces," on page 44.)

If you do not wish to change the default value, press Enter. If you do want to change it, type the new SSID and then press Enter.

9. Choose Installation Type

The next prompt asks

```
Are you installing AirSwitch in a server-type deployment?
[no]:
```

If you are performing a standard installation, leave the default No and press Enter. If you would like a server-type (also referred to as an *appliance-type*) deployment, type Yes and then press Enter. For details on these two deployment types, refer to Application Note 1, *Basic Deployment Types*.

10. Configure Internal VLANs

At this point you will be asked whether you want to change any of the default IDs of the six internal VLANs that the AirSwitch uses for its own packet traffic. (See "Internal VLANs," on page 84.) The only reason you should change any of these is if it conflicts with a VLAN ID you have already defined in your network. If there are no conflicts, you should respond no, and press Enter:

```
Would you like to override the block of 6 internal VLANs
(3072-3077)? [no]: no
```

If you would like to change this block, respond yes, and you will be prompted for the first ID in the range you want to assign. For instance, if you designate 2002, the six VLANs will be reassigned IDs from 2002-2007.

Next, you will be prompted to collapse the six internal VLANs into a single VLAN.

```
Would you like to collapse the block of 6 reserved VLANs into a
   single VLAN? [yes]
```

You should choose the default, *yes*, if your network cannot support multiple VLANs for any reason. If you do, you will see a confirmation message:

```
Internal VLANs have been collapsed into a single VLAN, ID=3072
```

If you type *no*, your six internal VLANs will remain, as shown in the confirmation example below.

11. Confirm Configuration

At this point you will see a summary of the configuration changes so far, and an Exit prompt:

```
The following configuration command script was created:

IP ADDRESS <yourIPaddress> 255.255.255.0

SSID AFNworks CORPORATE VLAN 0 ADVERTISE

VLAN 3072 AFN-RSVD NAME AFN-Reserved
VLAN 3073 AFN-RSVD2 NAME AFN-Reserved2
VLAN 3074 AFN-RSVD3 NAME AFN-Reserved3
VLAN 3075 AFN-RSVD4 NAME AFN-Reserved4
VLAN 3076 AFN-RSVD5 NAME AFN-Reserved5
VLAN 3077 AFN-RSVD6 NAME AFN-Reserved6
```


DCN: as1200sm-B11

```
Would you like to commit the configuration and exit? [yes]:
yes
```

If you type **yes**, as in the example, you will be directed to the Main-level command prompt

```
~AirSwitch~>
```

where you can continue with further initial configuration.

Note: This step commits the configuration settings to system memory, but *does not yet save them to a configuration file*. To do that, you must manually use the **SAVE** CLI command, as instructed at the end of the “Further Initial Configuration” section, below.

If you do not save your settings to a configuration file, the next time the AirSwitch reboots it will revert to factory defaults, and will launch the initial configuration dialog from the beginning.

Examples

An example of the whole dialog for a standard (i.e., switch-type) installation is shown below.

```
Welcome to AirSwitch Initial Configuration Dialog!

                    *********

Enter SVC port IP address [10.0.0.1]: 172.16.129.28

Enter SVC port network mask [255.255.255.0]: 255.255.128.0

Enter enable password:

Re-enter enable password:

Enter SSID [AFNworks]:

Are you installing AirSwitch in a server-type deployment?
[no]:

Would you like to override the block of 6 internal VLANs
(3072-3077)? [no]:

Would you like to collapse the block of 6 reserved VLANs into
a single VLAN? [yes]:

The following configuration has been created:

IP ADDRESS 172.16.129.28 255.255.128.0
SSID AFNworks CORPORATE VLAN 1 ADVERTISE
The internal VLANs are collapsed into VLAN ID = 3072

Would you like to commit the configuration and exit? [yes]:

~AirSwitch~>
```

An example of the whole dialog for a server-type installation is shown below. The difference is that the VLANs are collapsed automatically, and so that prompt is never displayed.

```
Welcome to AirSwitch Initial Configuration Dialog!

                    *********

Enter SVC port IP address [172.16.129.28]:

Enter SVC port network mask [255.255.128.0]:

Enter enable password:

Re-enter enable password:

Enter SSID [AFNworks]:

Are you installing AirSwitch in a server-type deployment?
[no]: yes

Would you like to override the block of 6 internal VLANs
(3072-3077)? [no]: yes

Enter the start of the block [3072]: 1000

The following configuration has been created:

IP ADDRESS 172.16.129.28 255.255.128.0
SSID AFNworks CORPORATE VLAN 1 ADVERTISE
The internal VLANs are collapsed into VLAN ID = 1000

Would you like to commit the configuration and exit? [yes]:

~AirSwitch~>
```

Further Initial Configuration

The initial configuration dialog you have just completed sets the basic minimum of switch parameters needed to run and connect to the switch. However, there are still some required configuration steps before you can use your wireless network. To perform these remaining steps, use the CLI presented at the end of the initial dialog.

12. Populate the Access Control List

Before any wireless clients can connect to the network, you must add them to the Access Control List, or ACL. You do this with the **ACL** command, which creates an entry in the list with the specified MAC address, user name, and device type. The ACL command is available only at the Configure level of the CLI, so you must first navigate to that level. To do so, you will need to supply the enabled password, which you just defined during the initial configuration dialog:

```
~AirSwitch~> enable
Password:
```


DCN: as1200sm-B11

```
~AirSwitch~# config terminal
~AirSwitch(config)~#
```

At this point you can use the ACL command to create ACL entries. For example, the following command would add a device *Bezdomnyi laptop*, of a type *Dell Inspiron 8500* and MAC address c3:aa:c9:ba:16:a5 as an entry in the ACL:

```
~AirSwitch(config)~# ACL c3:aa:c9:ba:16:a5 NAME Bezdomnyi
     laptop TYPE Dell Inspiron 8500
```

Note that only the MAC address and Name fields are technically required; the Type field is provided for the convenience of system administrators, and can be any alphanumeric string you like.

You can also import multiple entries into the ACL from an Excel spreadsheet, to save time and reduce the likelyhood of errors. For a detailed discussion of this and the ACL generally, see "The Access Control List," on page 33.

Once you have entered your wireless clients, you can confirm with the command:

```
~AirSwitch(config)~# SHOW ACL
```

13. Create a Telnet User

While you are performing this initial configuration, you are directly connected to the local management port of the AirSwitch. However, because you or other administrators will eventually need to connect remotely via telnet, you must create a telnet user and password. To do this,

A. If you are in the Configure level, navigate back up to the Enabled level by using the command:

```
exit
```

B. Type the command:

```
user add <username>
```

where <username> is the user you want to create. You can use up to 32 letters and numbers; do not use spaces or special characters.

C. At the next prompt, provide a password for this user. You can use up to 32 letters and numbers; again, no spaces or special characters.

D. When prompted to repeat the password, type it again.

E. If the passwords match, the new user is created and you will see a confirmation message.

Note that the password strings you type do not display onscreen at any time. The whole procedure will look like this:

```
~AirSwitch~> enable
~AirSwitch~# user add Woland
(New) password:
```

```
Retype (New) password:
New user Woland has been added
~AirSwitch~#
```

Note that both usernames and passwords are cap-sensitive, so `afnWorldHQ` is a completely distinct password from, say, `AFNworldHq`.

Once you have created at least one user, you can open a telnet connection to the AirSwitch Command Line Interface from any PC or console with a network connection to the switch's management port, using the static IP address you assigned during the initial configuration dialog.

14. Replace the Default System Name

Each AirSwitch has an overall system name, which displays in all CLI prompts. The default value for this name is *AirSwitch*, as you can see in the command line examples throughout this chapter. Though this is optional, you may want to supply something more specific to your environment, such as your company name. You can use up to 32 letters and numbers; do not use spaces or special characters.

To change the system name, use the command:

```
~AirSwitch(config)~# sysname <NewSystemName>
```

Once you do this, you will see the *NewSystemName* as a part of each CLI prompt. In our examples here, we will continue to use the default system name *AirSwitch*.

15. Create New VLANs

The AirSwitch is shipped with six internal VLANs. If you want to create additional VLANs for your use—for example, if you want to use more than one SSID with associated VLANs—do so now with the command:

```
~AirSwitch(config)~# VLAN <id> NAME <name>
```

(For a detailed discussion of VLANs, see "VLANs," on page 83.)

16. Designate a Management VLAN

As we have seen, you can assign an IP address to the SVC port during the initial setup dialog, to use as your management interface to the switch. You can also assign a management IP address to the Gb uplink ports, but there is an important difference between the Gb ports and the SVC port: If you designate the service port, your IP address will be assigned only to that port, and so you can only open a telnet connection through that single port. If you designate either Gb uplink port, you are actually assigning the IP address to the AirSwitch's internal switching fabric, so that you can open a telnet connection through *either* Gb port, *and* through any of the 12 10/100 Ethernet ports as well, but *not* through the service port.

If you designate the Gb ports as your management interface, you can also assign it to a VLAN, which will keep all your management traffic isolated from all other traffic. This step is optional, and can be done at any time. To do this, navigate to the

DCN: as1200sm-B11

configuration level, create the special management VLAN, and use the MGMT-VLAN command to assign it to the management interface:

```
~AirSwitch~# conf t
~AirSwitch(config)~# vlan 320
~AirSwitch(config-vlan)name mgmt type port-based
~AirSwitch(config-vlan)~# exit
~AirSwitch(config)~# mgmt-vlan 320
~AirSwitch(config)~# end
~AirSwitch~#
```

You can undo this management interface VLAN association with the command:

```
~AirSwitch(config)~# NO MGMT-VLAN
```

Note that his command does not delete the VLAN itself, but only removes the management interface from it.

17. Create Additional SSIDs

As we have seen, each AirSwitch is shipped with one defined SSID, *AFNworks*. Whether you renamed this during the initial configuration dialog or not, you may want to create additional SSIDs, which are useful for segmenting your WLAN.

```
~AirSwitch(config)~# SSID <name> [VLAN <ID>]
```

Note that the VLAN parameter is optional, as indicated by the square brackets, though in most cases you will want to map a VLAN to each SSID. Therefore, in general if you want to create more than one SSID, you will need to define a new VLAN for each before you create the SSIDs.

You can always change VLAN/SSID associations later on, after creating the entities themselves. (For details on this topic, see "Managing VLANs, SSIDs, and Interfaces," on page 44.)

18. Set up WEP Authentication and Encryption

At this point, all clients in the ACL should be able to attach to the WLAN normally. Though the ACL mechanism provides a reasonable level of security, you will want to set up WEP authentication encryption to make your network more secure still. To do this,

A. Define up to four WEP keys:

```
~AirSwitch(config)~# WEP KEY 1 SIZE 40 <key> TRANSMIT-KEY
~AirSwitch(config)~# WEP KEY 2 SIZE 40 <key>
~AirSwitch(config)~# WEP KEY 3 SIZE 40 <key>
~AirSwitch(config)~# WEP KEY 4 SIZE 40 <key>
```

B. Turn on WEP encryption and shared-key authentication:

```
~AirSwitch(config)~# WEP MODE SHARED
```

C. Confirm your settings with the command:

```
~AirSwitch(config)~# SHOW WEP
```

Note that this example sets Key 1 as the Transmit Key, and key size at 40 bits rather than 128. You may want to use 128-bit keys, or to designate a different transmit key. You could also specify Open System authentication, with the command

```
~AirSwitch(config)~# WEP MODE OPEN
```

For complete details on WEP, see "About WEP," on page 37.

19. Save Your Changes

As we mentioned above, when you are finished with this initial configuration you must manually save all settings with the SAVE command, from the Enabled level:

```
~AirSwitch(config)~# exit
~AirSwitch~# SAVE
```

This command will save your settings to a configuration file, with the default name *config.txt*. This file is not present until you save your initial settings, and if the AirSwitch does not find it the next time it reboots, it will start from the beginning of the configuration dialog.

DCN: as1200sm-B11

IV. Securing Your System

The AirSwitch provides network security that operates on two levels, which can be tuned to provide the kind of security you need for your wired and wireless users. These levels include:

- Access Control List
- WEP Authentication (page 38)
- WEP Encryption (page 38)

This chapter describes the operation of these security features.

The Access Control List

The Access Control List (ACL) is a file, *afnacl.csv*, that lists all wireless devices authorized to attach to the wireless LAN. All devices that are authorized to connect to the internal network must be added to this list before they can do so.

You can turn the ACL checking mechanism on or off altogether; by default, it is turned on. To disable ACL checking, uset the command

```
~AirSwitch(config)~# ACL ANY UNBLOCK
```

To turn it back on again, use the command

```
~AirSwitch(config)~# ACL ANY BLOCK
```

Any device entering your network will be allowed to authenticate and associate normally if it is listed here (and not Blocked).

Managing the ACL

To authorize a wireless device, you must add it to the ACL. Each device in this table is defined by three parameters:

- **MAC Address:** The 802.11 MAC address of the authorized device. This will always be unique.
- **Device Name:** Provides a more descriptive name, e.g. *MargoM Laptop, Marketing,* to the authorized device. This parameter is not mandatory.
- **Device Type:** Specifies the type of wireless device, e.g. *Sony Vaio 505TS Notebook*. This parameter is not mandatory, but is provided solely for the management convenience of system administrators.

In addition, a device can be set in either **Blocked** or **Unblocked** status. The default status of all newly created devices is unblocked, but it can be manually changed at any time. This feature allows an administrator to block authorization for a listed device, without deleting it from the list altogether. This is useful if you want to block a device temporarily but be able to easily reauthorize it later.

Adding Entries with the CLI

Access Control List management via the CLI is performed using the **ACL** command. All ACL-related commands are described in Table 4-1.

Table 4-1: ACL Management Commands

Command	Description
SHOW ACL	Shows all entries in the current Access Control List
ACL	Adds a new entry to the Access Control List, which specifies the devices authorized to associate to and use the wireless network. Devices are identified by MAC address and name, and can be in either Blocked or Unblocked status. You can also use this command to change one or more of an existing entry in the list. To do so, add the entry exactly as though it were a new entry, but with one or more different values—for instance, with a Blocked setting rather than Unblocked. Syntax = ACL <mac-addr> [NAME <name>] [TYPE <type>] {BLOCK | UNBLOCKED}
NO ACL <MAC ADDRESS>	Removes an entry, specified by MAC address, from the Access Control List.

For example, the command

```
~AirSwitch(config)~# ACL cc:dd:4C:00:04:ac NAME BerliozLaptop TYPE
       Dell Latitude
```

would add the specified laptop to the ACL. The device would be in Unblocked state, since that is the default if no state is specified.

To place this device in Blocked state, you would type:

```
~AirSwitch(config)~# ACL cc:dd:4C:00:04:ac BLOCK
```

You could also add a BLOCK parameter at the end of the command line that initially created the entry. In this case, the entry would be added, but the laptop would be blocked from connecting to the network until its status is changed.

To remove this entry from the ACL altogether, you can use the NO command and specify either the MAC address or the device name. Thus *either* of the following commands would produce the same result:

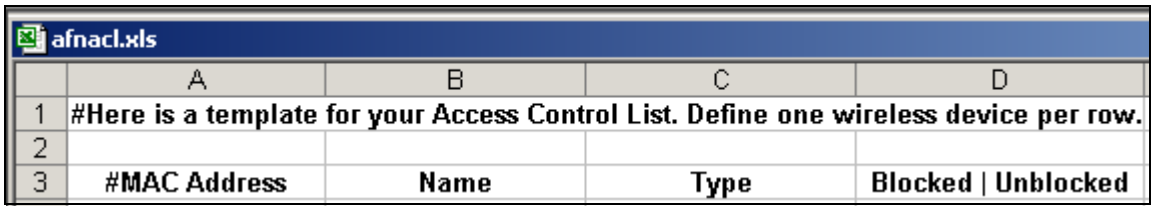
```
NO ACL cc:dd:4C:00:04:ac

NO ACL BerliozLaptop
```


DCN: as1200sm-B11

Importing Entries into the ACL

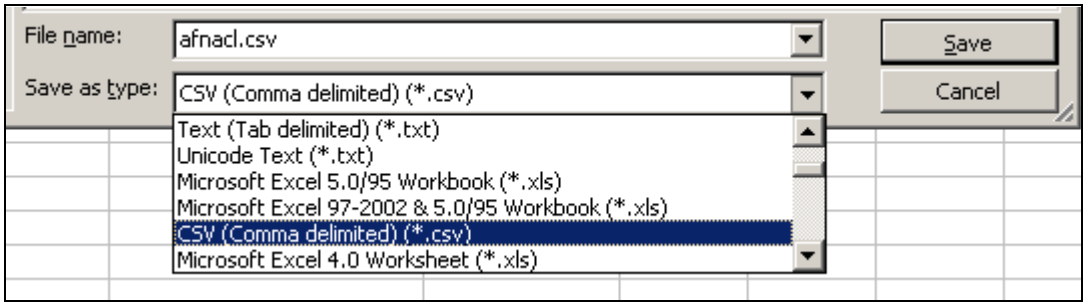
You can add entries to the ACL manually, using the process we just described. However, when more than a few clients are being added this method becomes very tedious and prone to typing errors. For this reason, the AirSwitch allows you to import whole lists of ACL entries from a standard Microsoft Excel spreadsheet. The file must have four columns, thus:



For convenience, AirFlow provides a template file **afnacl.xls**, on the Product Documentation CD. You can use a copy of this file to build your ACL for import, or you can open a new Excel file and set it up with four columns, as shown. If you have wireless client data stored in an existing database, it should be simple to export or paste it into Excel.

To import large numbers of ACL entries the first time, perform the following procedure:

1. Open or create an Excel spreadsheet called **afnacl.xls**, containing the required information on the wireless clients, as shown above.
2. Using the File, Save As command, convert the Excel sheet to .CSV format:



3. Copy the resulting .csv file to the AirSwitch file system, using the standard COPY FTP command (see page 99).
4. Reboot the AirSwitch.

To add large numbers of entries to an existing ACL, you have two options:

A. FTP the file from the AirSwitch with the COPY FTP command, open it directly in Excel, add the new entries as rows in the spreadsheet, save your changes, and copy the file back to the switch via FTP.

B. If you have an existing ACL on the switch and want to keep its contents and add additional entries from another existing .csv file, you can do that with the ACL LOAD feature. After you FTP copy the source file to the switch, use the command

```
~AirSwitch(cofnig)#~ ACL LOAD <filename.acl>
```

It is up to you whether you import entries to the ACL using either of these methods, or add them one at a time through the CLI. For example, some users may choose to create their initial ACL by copying or loading—since that will involve a relatively larger number of users—and use the ACL command to add the occasional new user thereafter.

Important: Every time the switch reboots, it looks for a file called *afnacl.csv* and, if one is present, uses it as the Access Control List. Whenever you work with this file to add or delete users, take care not to change the filename; if you change it, the switch will not be able to use it as an access list.

Viewing the ACL

You can use the **SHOW ACL** command to display the Access Control List, in the format shown below.

```
~AirSwitch~# show acl
ACL             : ENABLE

MAC-ADDR            NAME                    TYPE              STATE
00:0A:F4:9C:4D:20   Dell Demo Conf. room    Dell 200          BLOCKED
00:C4:D0:00:0A:D4   dell-smc                laptop            BLOCKED
00:0A:F4:9C:4B:3F   dellAiroPeek            laptop            UNBLOCKED
00:0A:F4:9C:4D:05   labinspiron8000         CiscoDell         UNBLOCKED
```

The second line in the example indicates that the ACL as a whole is in Enabled state. Beyond that, the ACL displays the following four parameters:

Table 4-2: SHOW ACL Parameters

Parameter	Description
MAC Address	MAC address of the authorized device.
Name	A descriptive name, e.g. Jane Jones Laptop, Marketing, assigned to the authorized device.
Type	Specifies the type of wireless device, e.g. Sony Vaio 505TS.
State	Displays whether the device is in Blocked or Unblocked state.The default status of all newly added devices is Unblocked.

DCN: as1200sm-B11

About WEP

The AirSwitch supports Wireless Equivalent Privacy (WEP) client authentication and data encryption. Both these features are based on the same keys, and they are both enabled and disabled by the same CLI command, `WEP MODE <open|shared>`. When WEP encryption feature is enabled on the switch, it must also be configured and enabled on all wireless clients who wish to connect to the network.

You configure and enable WEP encryption and authentication from the Configure level of the AirSwitch CLI.

WEP Keys

WEP keys are hexadecimal character strings that you define, which are exchanged between the switch and wireless clients and used for encrypting and decrypting data packets. These are defined on the AirSwitch and also on any authorized client devices.

You can define up to four keys, each with a key number assigned—for example, 1 through 4. You can change these keys as often as you like; the more often they are changed, the more secure the encryption mechanism will be.

The switch supports either 40-bit or 128-bit encryption; the difference is the length of the keys. Obviously, 128-bit encryption is more secure than 40-bit. The length of each key is specified with the `SIZE` parameter.

The actual value you must provide for a 40-bit key is a 10-character hexidecimal string, consisting of any digits 0-9 and any letters A-F, in any combination. 128-bit keys are represented by 26-character hexadecimal strings. These strings are not case sensitive.

To define your WEP keys, use the WEP KEY command, also from the Configure mode

```
~AirSwitch(config)#~ WEP KEY <key-no> SIZE <40 | 128> <key>
```

You use this command to define each key, one at a time.

Switch Side and Client Side

For any WEP-enabled client device to communicate with the AirSwitch, the WEP keys on the switch must be stored on client. These keys are compared whenever the device is authenticated. Moreover, this key comparison is performed in both directions, during transmission. That is, one of the switch's keys is designated Transmit key, and this must be matched on the client side for the switch to send packets. On the AirSwitch, this Transmit key is designated with the DEFAULT KEY ID parameter (set to 1 in the SHOW WEP sample output, in Table 4-3).

Similarly, one of the client's keys must also be designated the Transmit key, and it must match one of the four keys on the switch if the client wants to send packets to the switch. The method for configuring WEP keys and designating a Transmit key for any given wireless client is, naturally, specific to the software running on that device. For details, consult the vendor's user documentation. The most important point here is that all keys defined on the switch must match exactly the corresponding keys on the client.

WEP Authentication

Whenever you enable WEP encryption, you must specify which WEP authentication type you want as well: **Open System** or **Shared Key**. Practically speaking, you may think of these as disabling and enabling WEP authentication. Under Open System authentication, authentication is essentially disabled: any client that requests a network connection will be authenticated, without checking whether its keys match those defined on the switch. Under Shared Key authentication, the WEP encryption key will be used as an authentication mechanism, and only clients with correct keys will be authenticated. Thus you cannot enable Shared Key authentication unless you have at least one key defined, and place the switch in WEP MODE.

You can change to Shared Key authentication from the Configure level of the AirSwitch CLI, with the command

```
~AirSwitch(config)#~ WEP MODE SHARED
```

To go back to Open System authentication, use the command

```
~AirSwitch(config)#~ WEP MODE OPEN
```

WEP Encryption

When WEP encryption is enabled, all packets passing in both directions between the AirSwitch and wireless clients will be encrypted, using one of the defined keys.

You enable WEP encryption from the Configure level of the AirSwitch CLI, with the command

```
~AirSwitch(config)#~ WEP MODE <open|shared>
```

(Again, you must specify an authentication type at the same time as you enable encryption.) You disable encryption (alonmg with authentication) with the command

```
~AirSwitch(config)#~ NO WEP MODE <open|shared>
```


DCN: as1200sm-B11

Summary of WEP CLI Commands

Table 4-3 explains the syntax and function of all available WEP commands.

Table 4-3: WEP CLI Commands

CLI Command	Description
WEP KEY	Lets you define up to four secret keys, used for WEP encryption of packets between the switch and clients. These settings will only be used if WEP Mode is Enabled. Syntax: WEP KEY <key-no> SIZE <size> <key> [TRANSMIT-KEY], where:
<key-no>	The ID of the key being defined, from 1 to 4.
<size>	Designates the size of this key, in bits. Valid values are 40 and 128. All four keys must be the same size.
<key>	The actual key, as a hexadecimal string, either 10 or 26 hex digits (depending on the size parameter).
[TRANSMIT-KEY]	An optional flag, TRANSMIT-KEY, that marks this key as the transmit key. May be set only for one of the defined keys at a time.
WEP MODE	Enables WEP encryption for all clients connected to the switch, along with the specified authentication type—open system, or shared key. Authentication type is set only when encryption is enabled; that is, there can be no client authentication without setting the system to WEP MODE. **Syntax:** WEP MODE <open | shared>
NO WEP	Disables WEP encryption and authentication for all clients connected to the switch. Has no parameters. **Syntax:** NO WEP

SHOW WEP	Displays current WEP configuration. WEP mode = Shared means encryption is enabled and authentication is set to Shared Key type; WEP mode = Open means encryption is enabled and authentication is set to Open System type (i.e., no authentication); and WEP mode = Disabled means encryption and authentication are is disabled.
	Sample output of this command (note that the WEP keys themselves never display onscreen):
	`~AirSwitch~(config)# show wep`
	`WEP MODE :ENABLED`
	`DEFAULT KEY ID :1`
	`DEFAULT KEY 1 TYPE :WEP 40 (key set)`
	`DEFAULT KEY 2 TYPE :WEP 40 (key set)`
	`DEFAULT KEY 3 TYPE :WEP 40 (key set)`
	`DEFAULT KEY 4 TYPE :WEP 40 (key set)`

DCN: as1200sm-B11

V. Managing Your System

This chapter describes several routine management procedures administrators may need to perform on the AirSwitch. Topics include:

Using Telnet Connections

As a security feature, the first time you configure the AirSwitch you must do so from a local console, connected directly to the management port (the one labeled SERIAL). You cannot establish a telnet connection to the switch until you connect locally and use the CLI to create a telnet user and password.

If you followed the whole procedure outlined in the System Setup chapter, you have created a new telnet user already. If not, you can create a new user at any time.

Managing Telnet Users

Administrators can create any number of telnet users, change the passwords of existing users, and delete existing users.

Note that whenever you are dealing with passwords, the strings you type do not appear on the console screen at any time.

Adding a New Telnet User

To create a new telnet user:

1. Connect a local console to the management port. When you do this, you will see the AirSwitch's Main level command prompt, which displays the default System Name defined on the switch. If you have not changed the factory default, you will see:

```
~AirSwitch~>
```

2. Navigate to the Enabled level, by using the command

   ```
   enable
   ```

   and providing the enabled password.

3. Type the command

   ```
   user add <username>
   ```

   where <username> is the user you want to create.

4. At the following prompt, provide a password for this user.

5. When prompted to repeat the password, type it again.

6. If the passwords match, the new user is created and you will see a confirmation message.

The whole procedure will look like this:

```
~AirSwitch~> enable
~AirSwitch~# user add begemot
(New) password:
Retype (New) password:
New user begemot has been added
~AirSwitch~#
```

Note that both usernames and passwords are cap-sensitive, so `LetMeIn` is a completely distinct password from, say, `LETmeIN`.

Once you have created at least one user, you can open a telnet connection to the AirSwitch Command Line Interface from any PC or console with a network connection to the switch's management port, using the static IP address you have assigned.

When you make a remote telnet connection, you will see the AirSwitch's Main level command prompt, just as you do from a local console.

Changing a User's Password

To change the telnet password of an existing user, perform the following procedure:

1. Navigate to the Enabled level, using the command:

   ```
   enable
   ```

   At the Enabled prompt, type the command:

   ```
   user change <username>
   ```

   where <username> is the user you want to assign a new password.

2. At the next prompt, type the current password of that user. If you type the current password correctly, the CLI will prompt you for the new password.

DCN: as1200sm-B11

3. When prompted to repeat the new password, type it again.
4. If the passwords match, the new user is created and you will see a confirmation message.

The whole procedure will look like this:

```
~AirSwitch~> enable
~AirSwitch~# user change begemot
(Old) password:
(New) password:
Retype (New) password:
User begemot has been changed
~AirSwitch~#
```

Deleting a Telnet User

To delete an existing user:

1. Navigate to the Enabled level, using the command:

   ```
   enable
   ```

2. At the Enabled prompt, type the command:

   ```
   user delete [username]
   ```

   where [username] is the user you want to delete.

3. At the next prompt, confirm that you really want to delete this user. If you type Y or Yes, the user will be deleted and you will see a confirmation message.

The whole procedure will look like this:

```
~AirSwitch~> enable
~AirSwitch~# user delete begemot
Do you really want to delete user? (y/n) y
User begemot has been deleted
~AirSwitch~#
```

Viewing All Telnet Users

You can view all currently defined telnet users from the Enabled level, with the command

```
~AirSwitch~# show user-database
```

Note that passwords will never display on screen. If you lose a password, delete the user and recreate it, assigning a new password.

Managing VLANs, SSIDs, and Interfaces

Because the functions of VLANs, SSIDs and Interfaces are complex and interrelated, they deserve some detailed explanation. Basically, their relationship may be thought of as linear, downstream from the switch: one or more physical ports are combined as an interface; and each interface may be associated with, or assigned to, a VLAN in the wired segment of the network, which in turn is associated with an SSID for the air segment.

Ports and Interfaces

An *interface* is simply a term for one or more physical ports that are configured identically. For example if you want to set up ports 1-6 to behave one way and 7-12 another way, you could group the first six as a single interface and the latter six as a second interface, considerably simplifying the configuration process. Ports do not need to be contiguous to belong to the same interface.

For the purpose of defining interfaces, there are three categories of ports on the AirSwitch:

- FE1-FE12: These are the twelve 10/100 Ethernet ports.
- GE1 & GE2: These are the two Gb uplink ports.
- SVC: This is the management or service port, labeled 10/100 SVC.

The SERIAL port is only used for local connection, and cannot be included in any interface.

Interfaces do not have their own ID or name, but are identified by their *port list*, which is simply the list of physical ports that constitute the interface. A port list may contain either one port, or more than one.

VLANs and SSIDs

In fact, each SSID is nothing more than an extension of a VLAN from the wired into the wireless medium. VLANs segment the wired network, and SSIDs simply extend this segmentation out into the WLAN. When you create an SSID you can associate a VLAN to it, and then by association with an Interface the resulting SSID/VLAN pair contains or represents one or more physical ports.

The diagram below represents this interrelationship, with reference to the sequence of command lines used to create these entities. Note that VLANs must be created first, so they can then be associated with SSIDs and Interfaces.

DCN: as1200sm-B11

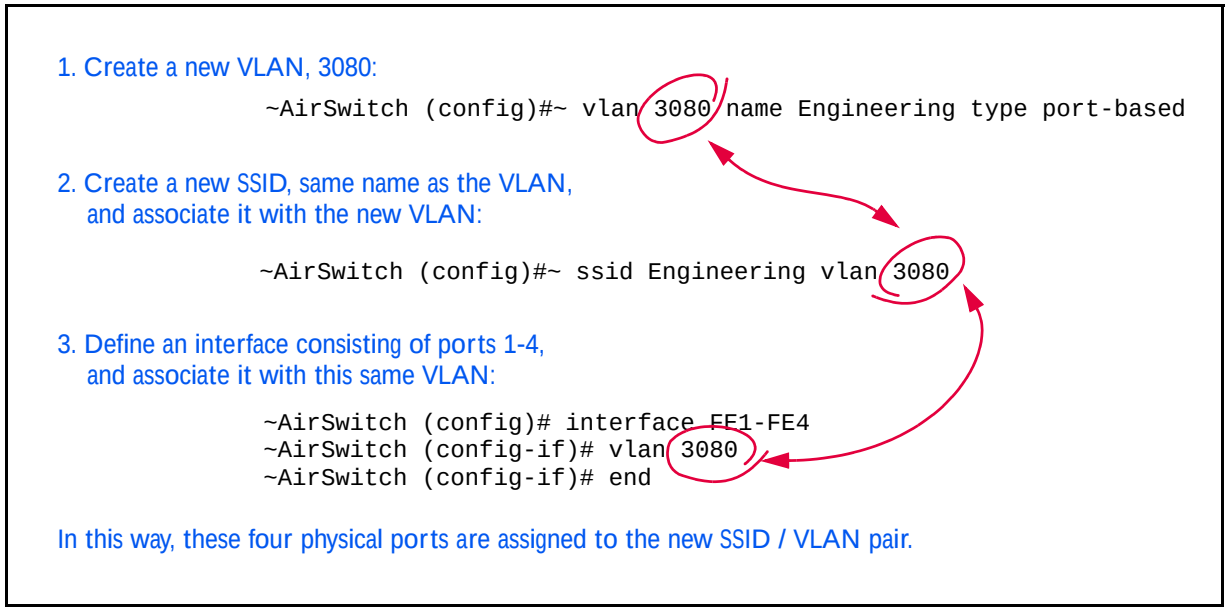


Figure 5-1: Creating VLANs, SSIDs, and Interfaces

SSID Types

Each SSID must be defined as one of two types: either Corporate or Public. The Public SSID is the one associatd with your Public port; there can only be one at any given time. All others must be Corporate, which means they are routed through your internal backbone network, rather than straight to the Intranet. The syntax is:

```
SSID <ssid> VLAN <vlanid> <corporate|public> [advertise]
```

For details, see Chapter VI, "Using the Public Port".

Advertising SSIDs

When a wireless client requests a connection to the network, it must specify an SSID. Access points generally are able to broadcast their SSID, so that devices can request the specific connection. This is referred to as *advertising* the SSID.

If you wish, you can designate one of your SSIDs with an **advertise** parameter. Again, the syntax is:

```
SSID <ssid> VLAN <vlanid> <corporate|public> [advertise]
```

If this parameter is set, the AirSwitch will advertise this SSID to wireless clients requesting association to the network. If it is not set, wireless users will need to know the SSID they want to associate with, which provides a security feature.

You can advertise both types of SSIDs (corporate and public), but bear in mind that you can only set one SSID to advertise at a time. If you try to advertise a second one, the switch will prompt you with an error message.

Making Changes

Once initially defined and associated, you can rearrange these entities in various ways:

You can add physical ports to, or remove them from, an existing interface, by redefining the <port-list>. Bear in mind, however, that each physical port can only belong to one interface at a time.

You can change the interface associated with each VLAN. This is done from the perspective of the interface, so to speak, rather than that of the VLAN, since this association is made in the Interface command (#3 in the figure above: “what VLAN do I belong in?”) rather than in a VLAN command (“what interface belongs to me?”).

You can delete existing SSIDs, with the `NO SSID <ID>` command. However, you must have at least one SSID defined on the switch at all times, and if you try to delete the last SSID, the switch will prompt you with an error message.

You can redefine SSID/VLAN pairs, by assigning a new VLAN value to an existing SSID, in the SSID command line (#2 in the figure above).

You can freely assign new names to existing SSIDs and VLANs. These are simply alias strings for user convenience, and have no software dependencies. Bear in mind, however, that the SSID names are displayed on client devices when they attach to the network.

You can *not* change the ID of an existing VLAN. Rather, you must delete it and redefine a new one from scratch.

Changing Your Management Port

As we described in the System Setup chapter ("Designate a Management VLAN," on page 30), you have the option of assigning the management IP address either to the SVC port, or the Gb uplink ports of the AirSwitch. You do this with the MGMT-MODE command, in the interface submode. Assigning it to *either* Gb uplink port will allow telnet connections to *both* Gb ports *and* all 10/100 Ethernet ports (through the switching fabric); assigning it to SVC port will allow telnet connection only to that single port.

You can confirm which port is set in management mode by typing the SHOW INTERFACE command. Note that for the SVC port, management mode status is the only parameter displayed.

```
~AirSwitch~# show int

GE1       VLAN  ID: 1
          STP COST: 2
          STP PORT-PRIORITY: 128
            MGMT MODE: ON
```


DCN: as1200sm-B11

```
GE2       VLAN  ID: 1
          STP COST: 2
          STP PORT-PRIORITY: 128
           MGMT MODE: ON

SVC        MGMT MODE: OFF
```

You can change this designation if you like, by entering the submode for the interface you want to take out of management mode, and typing the NO MGMT command. You then enter the submode for the interface you want to place into management mode, and use the MGMT-MODE command to enable it. Remember that you must perform both steps—turn off the current interface, then turn on the new one.

To change the status of the interfaces shown in the example above, the procedure would look like this:

```
~AirSwitch~# conf t
~AirSwitch(config)~#  int ge1
~AirSwitch(config-if)~# no mgmt
~AirSwitch(config-if)~# end
~AirSwitch(config)~# int svc
~AirSwitch(config-if)~# mgmt
~AirSwitch(config-if)~# end
~AirSwitch(config)~# show int

GE1       VLAN  ID: 1
          STP COST: 2
          STP PORT-PRIORITY: 128
           MGMT MODE: OFF

GE2       VLAN  ID: 1
          STP COST: 2
          STP PORT-PRIORITY: 128
           MGMT MODE: OFF

SVC        MGMT MODE: ON
```

Note that GE1 and GE2 will always have the same MGMT MODE, so you need only change the settings for one or the other, to affect both.

Changing the CLI Enable Password

The AirSwitch is shipped with a factory default password, **afnafn,** which allows you to navigate to the Enable level. You will be prompted to change this during your initial setup dialog, and you can change it again at any time.

Enabled passwords are cap-sensitive, so MyPassword is entirely distinct from myPASSword. You can use up to 30 alphanumeric characters.

To change the Enable password, perform the following procedure:

1. At the Enabled prompt, type the command:

   ```
   enable password
   ```

2. At the next prompt, type the current password. If you provide the correct password, the CLI will prompt you for a new password.
3. Type the new password at the prompt.
4. When prompted to repeat the new password, type it again.
5. If the passwords match, the CLI password is changed and you will see a confirmation message.

Note that the password strings you type do not display onscreen at any time. The entire procedure looks like this:

```
~AirSwitch~> enable
~AirSwitch~# enable password
(Current) password:
(New) password:
Retype (New) password:
Enable password has been changed
~AirSwitch~#
```

Managing Packet Antennas

The requirements of Packet Antenna management are very simple. Obviously you need to plug the physical PA units into LAN wall jacks, and those jacks need to be connected to 10/100 ports on the AirSwitch. The network administrator will need to keep track of the physical location of each PA so that its configuration can be adjusted, if appropriate, based on considerations connected to its physical location.

As soon as each PA is plugged in, it receives power over Ethernet from the switch, and you should see the power LED light steady red when it detects that it has no firmware loaded yet. It will change to steady amber to indicate that it is receiving the firmware from the AirSwitch. When the download is successful, the LED turns to steady green, indicating the AirHub is operating normally and is in Active status. At this point you should be able to see it listed with all statistics, in the output from the SHOW PA command in the CLI.

DCN: as1200sm-B11

Changing PA State

The AirHub 100 can be in one of two states: Active or Standby. In Active state the PA is receiving and transmitting normally; in Standby state the PA listens for beacons from wireless devices and passes them up to the switch, but does not pass any other kind of uplink data, and does not transmit downlink data of any kind.

The default state is Active, but you can manually place PAs in Standby state with the following command, from the Enabled level:

```
~AirSwitch~# PA NAME <name> STANDBY
```

Packet antennas remain in the same state until they are manually changed, or are rebooted with the RESET command, in which case they always power up in Active state (see below).

Rebooting PAs

One valuable feature of the AirFlow distributed architecture, is that all AirHub firmware upgrades can be centrally handled and greatly simplified. If you need to upgrade AirHub software but would like to test the new version first, you can load the new version to one AirHub, then manually restart using the command

```
~AirSwitch~# PA NAME <name> RESET
```

Redefining PAs

Besides STATE, each PA has several fields, all of which are autopopulated by the AirSwitch during initial autodetection. These include:

- name
- location
- boot image filename
- mode

At any time after bootup, you may wish to replace these default values with something more helpful. The Location field in particular provides a useful descriptive handle, that helps remind you of the physical pattern of your AirHubs around the coverage area.

Note that you can only redefine these parameters at the Configure level of the CLI.

To assign a new name, use the SHOW PA command to display the default name, and then assign a new one by typing

```
~AirSwitch(config)~# PA <default-name> NAME <new-name>
```

To assign a new location description, use the command

```
~AirSwitch(config)~# PA <name> LOCATION <new-location>
```

Preconfiguring PAs

The PA command at the Configure level allows you to manually define as many PAs as you wish, before they are physically plugged into the network. This represents an alternative to letting the AirSwitch autodetect scouts and supply configuration values automatically. If you want to do this, you must supply values for all the parameters of the PA command, including those discussed above plus the MAC Address as well. The complete syntax of this command looks like this:

```
~AirSwitch(config)~# PA <name> [name <newname>] [BOOT <file-name>]
  [LOCATION <location>] [MAC <mac-addr>] [MODE <value>]
```

If you preconfigure a PA, the AirSwitch will recognize that an entry exists for it when the PA is plugged in, and will leave the preconfigured entry unchanged.

Managing Wireless Clients

There are very few things the WLAN administrator needs to do regarding the wireless clients connecting to the AirSwitch. You can view some basic information about them, by displaying the Active Station List. As we have seen, you can view the short version or the detailed version of the ASL, with the commands

```
show asl
```

or

```
show asl details
```

(For details, see "Monitoring Client Connections," on page 71.)

You can also get a general idea of the physical location of a given client, since the ASL shows you what packet antenna the client is using, and the **SHOW PA <name>** command will display a Location parameter for that PA.

Controlling Client Connections

There are four CLI commands related to client connections:

- DISASSOCIATE
- DEAUTHENTICATE
- ASL [name] BLOCK
- NO ASL [name]

All four are used to disconnect a specific client from the WLAN, but there are important differences between them. The state model at right is useful in explaining these differences.

Generally speaking, wireless devices enter the coverage area of your WLAN in State 1, not authenticated and not associated. If the device is listed in the ACL and is not blocked, it will automatically authenticate (State 2), and then associate (State 3). This process happens very quickly—usually in less than a second.

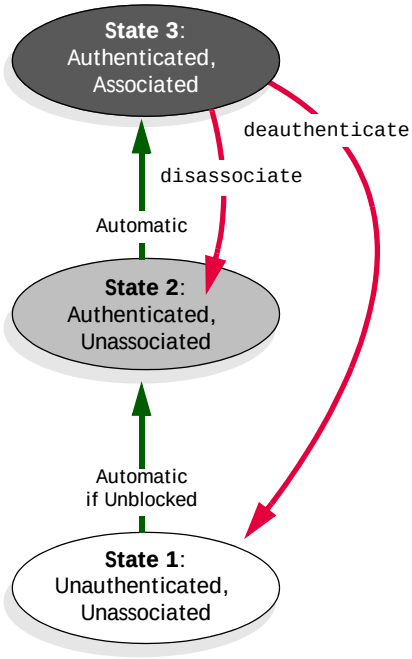


Figure 5-2: Wireless Client State Model

DCN: as1200sm-B11

The Disassociate and Deauthenticate Commands

Once a client is associated, if you type the command

```
DISASSOCIATE <name>
```

the AirSwitch will break the association, and the client will briefly move to State 2. The client will automatically request a reassociation, and since it is already authenticated, the switch will place it back into State 3. The result of this command, then, is a very brief disconnection—again, less than a second—followed automatically by a reconnection.

The purpose of this command is to force a client to reassociate with the network after you have changed one or more operational parameters.

By contrast, if you type the command

```
DEAUTHENTICATE NAME <name>
```

the AirSwitch will both disassociate the device and deauthenticate it, changing it from State 3 to State 1. If the ACL status is not changed, however, the device will promptly reconnect, and return to State 3.

The point of this command is to force a client to reauthenticate, for example if there is something suspicious about the client and you want to confirm that it is a legitimate user.

The ACL Command

If you type the command

```
ACL NAME <name> block
```

where <name> is the name of an existing wireless device, the effect will be to place the specified device in a blocked state. (You can use the MAC address instead of the name, if you prefer.) This does not involve any change in terms of the states represented in Figure 5-2; if the device is associated with the network, it will stay associated. However, if the device is ever deauthenticated, it will not be permitted to reconnect and will remain in State 1, periodically requesting authentication and being rejected.

If you unblock the device with the command

```
ACL NAME <name> unblock
```

it will be permitted to reconnect to the network at its next attempt.

If you type

```
NO ACL NAME <name>
```

the specified device will be deleted from the ACL altogether. The effect will be identical to the BLOCK command; the device will not change state, but will not be

able to reassociate, once disconnected. In order to reenable it to connect, you must add it to the ACL as a new entry.

Summary

The use of these four commands, then, can be summarized as follows: the **disassociate** and **deauthenticate** commands disconnect a client but do not keep it disconnected; the **ACL NAME <name> BLOCK** and **NO ACL NAME <name>** commands do not themselves disconnect a client, but prevent it from reconnecting once it is otherwise disconnected.

Upgrading your System Software

If for any reason you need to upgrade your system software, AirFlow Networks will provide an upgrade image in the form of a .tar file, whose filename reflects the version of the code. For example, the image for Release 1.0.2.11 is named `as1200-1-0-2-11-upgrade.tar`.

To install a new version on your AirSwitch, perform the following procedure:

1. Copy the image to a source location in your network, that is accessible both to your FTP server and to the AirSwitch.

2. At the Enabled level of the AirFlow CLI, use the **COPY** command to copy the image to the switch's flash memory:

   ```
   copy ftp://<user>:<password>@<sourceIPAddress/filename>
   <dest filename>
   ```

   If this is successful, you will see a confirmation message:

   ```
   File [name] transferred successfully.
   ```

3. Untar the image, using the **TAR XF** command:

   ```
   TAR XF <filename>
   ```

   If you receive no error message, the untar was successful.

4. Save your current configuration to file, using the **SAVE** command.

5. Reboot the switch, using the **REBOOT NOW** command. After reboot, you can confirm that you have the new switch image installed by using the **SHOW SWITCH** command to view the switch version.

6. Move to the System submode, and upgrade your bootflash to the new version with the following command sequence:

   ```
   BOOTFLASH UNLOCK
   BOOTFLASH UPDATE <filename>
   ```


DCN: as1200sm-B11

You can use the **DIR** command to find the new bootflash file name; it is the only file with a .hex extension.

7. Once the bootflash upgrade finishes, relock the flash chip:

```
BOOTFLASH LOCK
```

8. Exit the System submode, and reboot the switch again with the **REBOOT NOW** command.

At this point your new image is installed and running. Any wireless clients that had been using the network during the upgrade will automatically reconnect after a momentary disconnection.

Customizing Your Upgrade

Each upgrade .tar file contains a number of files that provide new versions of various individual software components on the AirSwitch: the main switch software, the FPGA processor code, the packet antenna software that is sent down to AirHubs on system bootup, and the PA bootloader software that performs this installation to the packet antennas.

It also contains a file called **env_var**, which contains the instructions for how the switch handles these new versions when it first boots up. The env_var file is organized in key-value pairs, representing the component label and the file name where the component will be copied during the upgrade.

The list in the env_var file represents the files that must be present for the AirSwitch to boot up and run. That does not necessarily mean, however, that all these files must be copied onto the switch every time you upgrade. In practice, you may not want to install all the components provided in a given system upgrade. For example, you may want to upgrade your switch software but not your PAs, since you may already have the latest version of PAs installed. (For help on checking your currently installed version, see "Viewing Installed Versions," on page 55.)

If you are confident you want to do so, you can customize your installation by opening the env_var file, inserting a pound sign (#) to comment out those components in that you do not want to install, and saving your changes. To do this, however, you need to be sure you recognize what is what in the file.

CAUTION: This information is provided for users who are knowledgeable and experienced in using the AirSwitch, and who are confident of the reasons why they want to customize their upgrade. If you have any questions, be sure to consult AirFlow tech support before editing the env_var or any other installation files.

The following figure shows the contents of a sample env_var file. The callouts in the figure refer to the following descriptions of each line. Note that the file contains more than one version of all PA-related installation components, in order to support simultaneous upgrade of several versions of PA hardware in the same network—for example, a mix of 802.11b and 802.11a PAs.

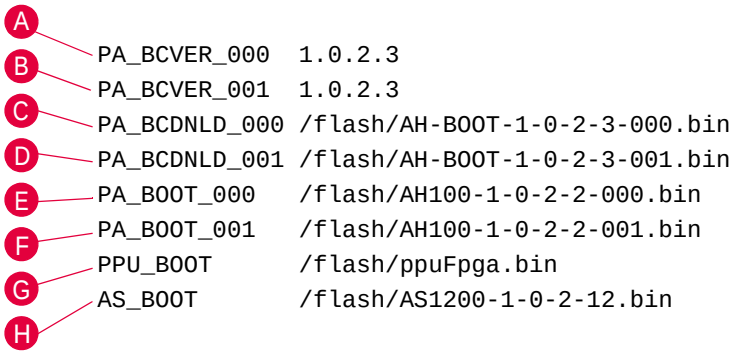


Figure 5-3: Contents of the env_var *File*

A. This line shows the version of the bootloader code provided in this upgrade. (The BCVER signifies **B**oot **C**ode **VER**sion.)

B. Displays version of alternate PA boot code, which supports a different PA hardware version.

C. This is the bootloader code upgrade. The bootloader copies the latest available PA application code from the AirSwitch flash directory down to PA memory, every time a PA is power cycled. (The BCDNLD signifies **B**oot **C**ode **D**ow**NL**oa**D**.) If you want to block the installation of a given version of the PA upgrade, this is the line you should comment out in the env_var file.

D. Alternate PA boot downloader, to support a different PA hardware version.

E. This is the PA application code, that is downloaded by the bootloader when the PA is power cycled. In the file name, the AH100 signifies the model (AirHub 100) and the rest reflects the release version. This is the version displayed when you use the SHOW PA command.

F. Alternate PA application code, to support a different PA hardware version.

G. This is the code for the FPGA processor. This code is always required to boot the AirSwitch, but will very rarely need to be actually upgraded. In the CLI, it is displayed as *PPU FPGA Version*, in response to the SHOW SWITCH command.

H. This is the switch application code, as signified by the model series, AS1200. In the CLI, it is displayed as *SW Version*, in response to the SHOW SWITCH command. You can comment out this line if you do not want to upgrade the switch application software.

DCN: as1200sm-B11

Viewing Installed Versions

If you want to check your currently installed version of these components against the versions specified in your env_var file, you can use the CLI commands SHOW PA and SHOW SWITCH.

```
~AFNworks~# show pa
Packet Antenna:

PA                                          : 1
  Model Number                              : AH 200
  MAC-ADDRESS                               : 00:0B:C8:00:00:72
  Port Number                               : FE1
  STATUS                                    : ON
  Transmit to STA Failures                  : 17
  Transmit retries                          : 21167
  Transmitted frames with multi retries     : 2312
  Received duplicate frames                 : 922
  RTS success                               : 0
  RTS failures                              : 0
  Ack failures                              : 2689
  Received frames                           : 2122326
  FCS errors                                : 21395
  Transmitted frames                        : 15018
  Active tokens                             : 0
  Max active tokens                         : 5
  Software version                          : R20.1.0.2.1
  Boot version                              : AH BOOT 1.0.2.1
  Up time                                   : 0 d 18 h 39 m 33 s
  Name                                      : DemoRoom
  Location                                  : unknown
  Boot filename                             : default
```

PA Application:

PA Bootloader:

Figure 5-4: The SHOW PA Command

```
~AFNworks~# sh sw
SW Version      : 1.0.2.11
IP ADDRESS      : 102.138.108.61 255.255.255.0
Beacons sent    : 1354668
Auth requests   : 53
Auth rejected   : 0
Assoc requests  : 13
Assoc rejected  : 0
WEP Undecrypted : 0
WEP ICV Error   : 0
WEP Excluded    : 2
Up time         : 0 days, 18 hours, 51 minutes, 51 seconds

Model Number    : AS1211
Part Number     : 550-11002-01
Serial Number   : 1232460
DateCode        : 06192003
MAC Address     : 00:AB:B8:80:C1:5A
BSP Version     : 1.0.2.13
BootCode Version: 1.0.2.11
BCOM Version    : 2
HIFN Version    : 4
PPU FPGA Version: 0
DevSup FPGA Version: 35
Regulatory Domain  : FCC
```

Switch Application:

PPU FPGA Code:

Figure 5-5: The SHOW SWITCH Command

Trouble shooting

If you experience technical problems with the AirSwitch during your testing, you may have to generate troubleshooting logs that AirFlow's engineering staff can use to investigate the problem. To do this, go to the CLI prompt (any level) and type:

```
SHOW TECH
```

This command will automatically generate a long body of diagnostic information, which will scroll on your console. When this finishes generating, select all of the text and copy it to a standard text document (preferably in Notepad or Wordpad), save it, and send it to your tech support representative at AirFlow.

Ordinarily you will not need to generate these logs unless asked to do so by your tech support representative.

DCN: as1200sm-B11

VI. Using the Public Port

This chapter describes the configuration and use of the AIrSwitch's public port feature. Topics include:

What is the Public Port?

The public port is a special feature that allows visitors to your enterprise to attach to and use the wireless network, through a Gb uplink connection that is completely isolated from the backbone network. Because this port bypasses the network's firewall and the AirSwitch's standard VPN termination, all visiting users have no access to any network resources. For the same reason, none of the AirSwitch's security features are available to visiting users' traffic, and visitors must rely on VPNs already configured between their clients and their target networks. Visitors get the benefit of simple wireless access from inside your enterprise, but they must provide their own security for that wireless traffic.

This feature is of great practical benefit in providing a wireless Internet connection to temporary visitors whom you might not want to authorize in the standard way, through RADIUS or the AirSwitch's access list. Such users might include customers, visiting sales representatives, OEM partners and suppliers, job candidates in for interviews, new hires attending training activities on your site, employees visiting from other locations in your firm, and so forth.

Visitors must provide a username and password to access the public port. When users log on, they get Internet access for a limited duration that is configurable. This means you have selective control over who will be able to use the public, and for how long.

The public port route feature identifies all visiting users, assigns dynamic IP addresses from its internal DHCP server, grants them Internet access through an isolated Gb uplink port, and routes all their traffic through that port using a reserved SSID/VLAN pair. You are free to use the factory default SSID/VLAN, called *Public*, or you can create your own.

DCN: as1200sm-B11

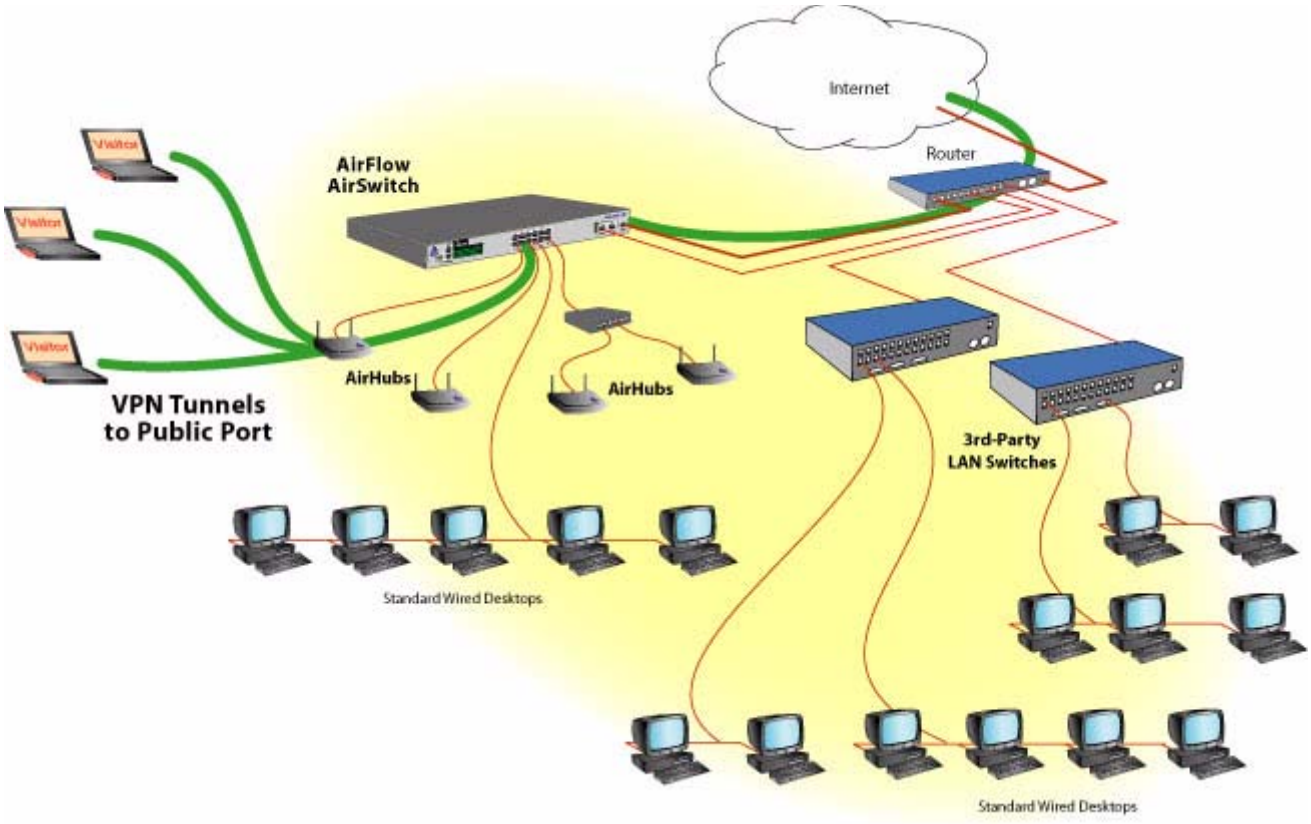


Figure 6-1: The Public Port

Using the Public Port

With all wireless LANs, everyone requesting a connection must specify the SSID they want in their wireless client utility, either by typing it, or by selecting it from their client's displayed list of all detected networks. The AirSwitch uses this requested SSID to distinguish between authorized users, who can connect to the backbone network, and visiting users, who can use only the public port.

Visitors arriving at your enterprise must be given the SSID of the public network, along with a username and password they will need to log on. When they request a connection to the SSID of the public port, the AirSwitch responds with a logon web page. If visitors provide a valid user name and password, they are connected to the Internet via the public port. As a security feature, users have three chances to provide a username and password; if all three are incorrect, they will be disconnected from the network.

DCN: as1200sm-B11

In addition to username and password, each user must supply his e-mail address when logging on, as Figure 6-2 shows. This allows administrators to identify who is actually logging on, and to track statistical history of public port users. (For details, refer to "Monitoring Public Port Use," on page 63.)

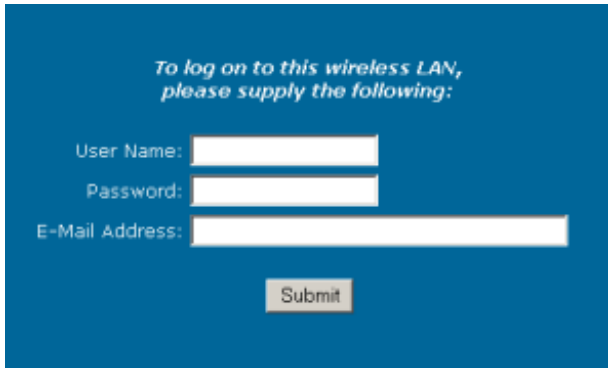


Figure 6-2: Public Port Logon Screen

Visiting users have access to the public port for a limited duration; by default this is set at 24 hours, but it can be configured as described below.

The public port SSID, like any other, can be set either to advertise or not. If set to advertise, it will appear in the wireless client's list of detected networks; if not, the visitor will have to type it in. You use the **SSID** command to change this; for details, see page 111.

Authorized system administrators can view the configuration settings for all current user groups (as described below), as well as information on who is currently using the public port and historical statistics on public port use.

Public Port Setup Requirements

The setup process for the public port comprises four component areas. We will explain each of these in turn, and then describe in detail the entire public port configuration procedure.

DHCP Server

The AirSwitch has an internal DHCP server dedicated to allocating dynamic IP addresses to visiting clients who need to use the public port. This DHCP server must be configured with one or more ranges of IP addresses available to assign to clients. You can designate a single range of contiguous addresses as a pool, or several non-contiguous ranges, each with an assigned pool ID. You must also specify the default gateway for these address pools.

Visitor Groups

The public port relies on the concept of *visitor groups*, each assigned a single username and password. Each visitor group can configured in a wide variety of ways to best suit its members needs and your administrative and security requirements. You can configure the following for each group:

- maximum number of users
- password length band duration
- access start time, duration, and renewal policy

For example, if your company is hosting a week-long sales training seminar for channel partners, you could create a group called *ChannelTraining*, with username *partner* and a static password *LRN2SELL*. You could configure their public port access to be available starting Monday morning from 8 a.m. to 5 p.m., and to automatically renew four times, after which it expires. Alternatively, if you want to provide a generic group for miscellaneous visitors, you would probably prefer to have the group's access indefinitely renewed every day, and with a password that has a longer duration—from 6 a.m. to midnight, say—but is valid only for one day, to be replaced a new one randomly generated every morning.

Note that however many visitor groups you define, they will all use the same public SSID to initially connect to the network, since only one SSID can be assigned to the physical port at a time.

Port Configuration

If you are going to use the Public Port, you need to set a number of Interface configuration settings, just as you do for other kinds of interfaces. These include assigning a static IP address and an SSID, enabling the port for use, and (optionally) assigning a VLAN to the port.

Administrative Users

All visitors must obtain the public SSID, a username and a password from someone in your organization—for example, the receptionist at the main entrance, or the instructor of a training seminar. Whoever is responsible for distributing this information obviously needs access to the current group definition, so they can give it to visitors as appropriate. This is especially true of groups whose password autogenerates every day.

To provide this access, you must create one or more administrative users, who are authorized to connect to the AirSwitch and view current group definitions. This is analogous to creating authorized telnet users, and in fact uses the same Enabled-level CLI command, USER ADD, but with type = public, rather than telnet:

```
~AirSwitch~# USER ADD oper-type <name>
(New) password:
Retype (New) password:
User <name> has been created.
~AirSwitch~#
```

Users created with this command will be able to navigate to a special submode, called **Public**, where they have read-only access to all currently defined visitor groups. For this reason, we will refer to them as *read-only administrators*.

Viewing Current Visitor Groups

Read-only administrators must telnet to the switch as any system administrator does However, because they may not have access to any of the Enabled- or Config-level CLI commands, they can navigate to the Public submode straight from the Main CLI level, using the command PUBLIC. Users must provide a username and password to enter this submode. Because it exists only to provide information on public groups, it provides only two commands: SHOW GROUP, and EXIT:

```
~AirSwitch~> public
~AirSwitch~> Username: Admin
```


DCN: as1200sm-B11

```
~AirSwitch~> Password:
~AirSwitch-public~> ?
show group     exit
~AirSwitch-public~> exit
~AirSwitch~>
```

The SHOW GROUP command displays four parameters:

- group name
- password
- access start time
- access duration

When used with the optional [name] parameter,

```
~AirSwitch-public~> show group [name]
```

it will display this information only for the specified group. Without the [name] parameter, it displays this information for all currently defined visitor groups.

Configuring the Public Port

To configure your public port, perform the procedure described below. You can do this either as a part of your initial system configuration, or at any later time. As we mentioned, you can configure and save all settings regardless of whether the public port is set to access mode or not.

1. Configure the DHCP Server

To define one or more IP address pools for use by the DHCP server, navigate to the configure level and use the command:

```
~AirSwitch(config)~# DHCP-SERVER
```

You need to specify at least one pool of dynamic IP addresses and the default gateway, along with the DNS server if you are using one. Use the syntax:

```
~AirSwitch(config)~# dhcp-server pool <name> <startIP-addr> <endIP-
   addr> dns [dns-server-addr] droute [default-gateway]
```

For details on these parameters, see **REF**.

2. Set up the Public SSID

Next, create a dedicated SSID for the public port. Although it is not required, ordinarily you will create a dedicated VLAN and add this port to it, as in our example below; this will isolate the visitors' traffic from the rest of your network. Note that you must specify SSID type = pub and VLAN type = pub, and add the PUB Interface to this VLAN.

If you use a VLAN, the process should look like this (substituting your own values, of course):

```
~AirSwitch(config)#~ VLAN 1099
~AirSwitch(config-vlan)#~ name Visitors_1
~AirSwitch(config-vlan)#~ type pub
~AirSwitch(config-vlan)#~ end
```

= create VLAN, type = pub

```
~AirSwitch(config)#~ SSID Visitors type pub vlan 1099 advertise
```

= create advertised SSID, type = pub, and add to this VLAN

```
~AirSwitch(config)#~ interface pub
~AirSwitch(config-if)#~ vlan 1099
~AirSwitch(config-if)#~ end
```

= add Public port to this VLAN

If you do not want to use a VLAN, you need only the SSID command:

```
~AirSwitch(config)#~ SSID Visitors type pub advertise
```

Because type = pub, this SSID is automatically linked to the Public Port, and no interface settings are required.

3. Define a Public Group

Once the port is set up, you need to define at least one group of users and set up their public port access rules. You do this in the Group submode, when you create a new group. For each group, you can specify:

- password type (user-defined or auto-generated)
- password string, if user-defined
- password length, if auto-generated
- start time and duration of access period
- number of times access period will be renewed after it expires

Complete details on these settings are provided under **REF**.

Example 1: You are expecting a group of executives from a friendly rival company, CessCo Systems, to come for a full day of meetings to discuss the possibility of an acquisition deal. In this case you might create a group called *CessCo*, with the password *lets_talk* and group access enabled from 8:00 a.m. to 8:00 p.m., after which the group would expire and not be renewed. The configuration of this group would look like the following:

```
~AirSwitch(config)~# group CessCo
~AirSwitch(config-group)~# password lets_talk
~AirSwitch(config-group)~# access start 0800
```


DCN: as1200sm-B11

```
~AirSwitch(config-group)~# access duration 12
~AirSwitch(config-group)~# access renewal none
~AirSwitch(config-group)~# end
~AirSwitch(config)~#
```

Example 2: You want to create a generic public access group, that would be available to unexpected visitors, employees visiting from your other corporate offices, or any other visitors not included in a specifically created group. This group would have the generic name *Visitor*, with a 5-character random password that would be autogenerated every day. You might want access for this group to be available every day from 6 a.m. till 10 p.m., and be automatically renewed every day indefinitely. This configuration would be the following:

```
~AirSwitch(config)~# group Visitor
~AirSwitch(config-group)~# password auto
~AirSwitch(config-group)~# password length 5
~AirSwitch(config-group)~# access start 0600
~AirSwitch(config-group)~# access duration 16
~AirSwitch(config-group)~# access renewal daily
~AirSwitch(config-group)~# end
~AirSwitch(config)~#
```

Note that you can give the same SSID to all the groups you create, or you can create separate SSIDs (on separate VLANs) for different groups. Naturally, the DHCP address pools you configure will be used by all groups.

Monitoring Public Port Use

The AirSwitch maintains historical information on all visitors using the public port, and stores them in log files that you can etc. The information is available to system administrators from the Configure level; it is *not* accessible by read-only administrators using the Public submode. The following information can be displayed for each group:

- user e-mail address
- username & password used
- time of connection to network
- duration of connection
- other stats here??

Note that the SHOW GROUP [name] command, described above on page 61, can also be used from the Config level. In addition, authorized system administrators can view a snapshot of visitors currently using the public port, use the command

```
~AirSwitch(config)~# SHOW GROUP [name] USER
```

To view a more extensive list of user statistics, administrators can use the command

```
~AirSwitch(config)~# SHOW GROUP [name] USER DETAILS
```

Here too the optional [name] parameter limits the display to the requested group; if omitted, all members of all groups will be displayed.

DCN: as1200sm-B11

VII. Handling System Files

This chapter describes several procedures available to help administrators manage system files the AirSwitch. Topics include:

Managing Configuration Files

Every time it boots up, the AirSwitch receives its configuration information from a flat file called *config.txt*, which is stored at a default location in the file directory in flash memory. To change your default configuration, you need only replace this file with another one that contains the configuration settings you want. You do this by setting up your desired configuration and exporting it to a file that you then rename *config.txt*.

Remember that, unlike CLI commands themselves, file names are case-sensitive: *Config.txt* is **not** the same as *config.txt*.

To enable you to manage your configuration files, the CLI provides several file management commands, all available only at the Enabled level. These include:

- **CHMOD** allows you to change the file mode from read-write to read-only, or vice versa.
- **COPY** copies the specified file; also used to rename a file.
- **DELETE** deletes the specified file.
- **DIR** displays all files currently in the flash directory.
- **LOAD** loads the settings in a specified file as the current configuration.
- **RENAME** renames the specified file.
- **SAVE** saves all current running configuration settings in the *config.txt* file.
- **TYPE** displays the contents of a specified file.

Use the following procedure to save your current configuration:

1. When you boot up the switch, it automatically loads the configuration from *config.txt*. This is now the running configuration.

2. When you make any changes to the current configuration—reduce the PA transmit power, let's say—the running configuration is now different from the default configuration. If you don't save the changed running config, it will revert to the default the next time the switch boots.

3. To save this configuration as the default, use the SAVE command. If you type

   ```
   SAVE
   ```

   the running configuration will be saved with the default filename, and the former default settings will be lost. (The file was overwritten.) If you do not want to do this, you can save the default settings in another file first, with the command:

   ```
   COPY config.txt oldconfig.conf
   ```

   (Of course you can use any name you like, in place of *oldfconfig.conf*.)

4. At this point when you SAVE the running configuration, you will be able to restore the old settings at some time in the future, if you like. To do this, type:

   ```
   LOAD oldconfig.conf
   ```

   and your the old settings will be loaded as the running configuration, which you can then resave as the default config, or as another file.

   Thus by combining the COPY, SAVE, and LOAD commands you can archive multiple configurations and use them to best suit your needs. If you are saving multiple configuration files, be sure to give them recognizable names that will help cue you to their content.

   You can use the DIR command to view the names of all config files you have saved, TYPE to check the contents of backup files, and DELETE to remove files you no longer need.

DCN: as1200sm-B11

Using FTP and TFTP

You can use FTP or TFTP protocols to transfer files to and from the AirSwitch—for example, if you want to archive configuration files, or when importing ACL entries from an Excel spreadsheet (see "Importing Entries into the ACL," on page 35). This section describes the commands available for using FTP and TFTP from the CLI.

FTP Commands

Administrators can use the **COPY FTP** command to copy files via FTP and the **USER** command to change the default username and password for FTP connections to the switch. Table 7-1 explains the FTP-related CLI commands that are available under the Enabled mode.

Mandatory parameters are shown in <angle brackets>; optional parameters are shown in [square brackets].T

Table 7-1: FTP CLI Commands

To do this:	Use this command:
Copy a local file to remote host	`copy <source-filename> ftp://<username>:<passwd@host>/<directory>/ <target-filename> [binary|ascii]`
Copy a file from remote host to local file system	`copy ftp://<username>:<passwd@host>/<directory>/<source-filename> <target-filename> [binary|ascii]`
Create a new FTP user	`user add <username>`
Delete factory default FTP user	`user delete afnafn`
Change the password for an existing FTP user	`user change <username>`
	The transfer mode is ASCII by default. For transferring AirSwitch image files, you must specify binary mode.
Examples	
FTP configuration file to remote system	`~AirSwitch~# copy config.txt ftp://SwAdmin:OpenSesame@169.120.118.20/ cfg-bkups/cfg-bak-1.txt binary verbose`
	This operation will save the *config.txt* file as *cfg-bak-1.txt*, on the remote directory called *cfg-bkups*, at host address 169.120.118.20. The administrator will log on to the remote system using username *SwAdmin* and password *OpenSesame*. The copy will use binary transfer mode.
FTP configuration file from remote system	`~AirSwitch~# copy ftp://SwAdmin:OpenSesame@169.120.118.20/cfg-bkups/cfg-bak-1.txt config.txt binary verbose`
	This operation will copy the file *cfg-bak-1.txt* from the remote directory called *cfg-bkups* on host 169.120.118.20, to the AirSwitch's flash file system as *config.txt*. This will overwrite the existing version of config.txt. The administrator will log on to the remote system using username *SwAdmin* and password *OpenSesame*. The copy will use binary transfer mode.
Get system image from remote host	`~AirSwitch~# copy ftp://SwAdmin:OpenSesame@169.120.118.20/AirSwitch-images/AirSwitch-1-0-2-11.tar AirSwitch-1-0-2-11.tar binary verbose`
	This command will write a copy of the binary image file named *AirSwitch-1-0-2-11.tar* from the *AirSwitch-images* directory *remote_directory* on remote host *169.120.118.20,* onto the AirSwitch's local file system with the filename unchanged. The administrator will log on to the remote system using username *SwAdmin* and password *OpenSesame*. The copy will use binary transfer mode.

TFTP Commands

You can also copy files via TFTP, using the COPY TFTP command. This command is also available from Enabled mode. The main difference between FTP and TFTP, is that the latter is not password protected.

Table 7-2: TFTP CLI Commands

To do this:	Use this command:
Copy a local file to remote host	`copy <source-filename> tftp://<host>/<directory>/<target-filename> [binary|ascii]`
Copy a file from remote host to local file system	`copy ftp://<host>/<directory>/<source-filename> <target-filename> [binary|ascii]`
Examples	
TFTP configuration file to remote system	`~AirSwitch~# copy config.txt ftp://SwAdmin:OpenSesame@169.120.118.20/cfg-bkups/cfg-bak-1.txt binary verbose`
This operation will copy the *config.txt* file as *cfg-bak-1.txt*, on the remote directory called *cfg-bkups*, at host address 169.120.118.20. The copy will use binary transfer mode.	
TFTP configuration file from remote system	`~AirSwitch~# copy ftp://169.120.118.20/cfg-bkups/cfg-bak-1.txt config.txt binary verbose`
This operation will copy the file *cfg-bak-1.txt* from the remote directory called *cfg-bkups* on host 169.120.118.20, to the AirSwitch's flash file system as *config.txt*. This will overwrite the existing version of config.txt. The copy will use binary transfer mode.	
Get system image from remote host, via TFTP	`~AirSwitch~# copy tftp://169.120.118.20/AirSwitch-images/AirSwitch-1-0-2-11.tar AirSwitch-1-0-2-11.tar binary verbose`
This command will write a copy of the binary image file named *AirSwitch-1-0-2-11.tar* from the *AirSwitch-images* directory *remote_directory* on remote host *169.120.118.20,* onto the AirSwitch's local file system with the filename unchanged. The copy will use binary transfer mode.	

Upgrading System Software

From time to time you may need to install an upgrade version of the AirSwitch system software. AirFlow delivers these upgrade images in the form of tar files. To install an upgrade,

1. Navigate to the Enabled level of the CLI.
2. Place the upgrade tar file on some host in your network, accessible from the AirSwitch.
3. Use the COPY FTP command to download the upgrade tar file to the switch from the remote host. (As a security precaution, FTP can only be used from within with CLI to "pull" files onto the switch or "push" them out from the switch to a remote location; you cannot FTP files down to the switch from another location.)

   AirFlow recommends that you do not change the filenames when you FTP files onto the AirSwitch.
4. Once the file is copied, use the TAR XF command to untar it. The component files inside will automatically be copied to correct locations.

DCN: as1200sm-B11

5. Use the REBOOT command to restart the switch. This will automatically replace the old version with the new one, and will also distribute upgraded AirHub software to all packet antennas, if required for the system upgrade.

As an example, the following set of commands would install an upgrade from a tar file called **upgrade.tar**.

```
~AirSwitch~> enable
Password:
~AirSwitch~# copy ftp://<username>:<passwd@host>/<direc-
   tory>/upgrade.tar dst binary
~AirSwitch~# tar xf airswitch_upgrade.tar
The image successfully unpacked!
~AirSwitch~# reboot
```

Updating your Boot Flash

The System submode has a command, BOOTFLASH, that allows you to update the system boot code that resides on the AirSwitch's bootflash chip. This is the code that runs whenever you power cycle the switch.

If you need to find out your current bootrom version, you can display it with the SHOW SWITCH command. You can also use the DIR command and check the label of the bootrom image itself (the only one with a .hex extension), which reflects the version number.

The BOOTFLASH command has three parameters—LOCK | UNLOCK, and UPDATE—which are used for loading a new bootflash image. These commands can *only* be used with a local serial connection; they are not available over telnet. Once you connect a serial console and navigate to the CLI's System submode, the process requires three steps:

1. Unlock bootflash with the BOOTFLASH UNLOCK command (By default, the bootflash files are locked and cannot be overwritten unless they are manually unlocked.)

2. Use the BOOTFLASH UPDATE <filename> command to load your new bootrom image.

3. After the upgrade, you use the BOOTFLASH LOCK command to relock the bootflash.

WARNING: Because the bootrom image is fundamental to starting your system, your AirSwitch could be altogether disabled if it is damaged or overwritten by mistake. Accordingly, you should *never* use this command unless specifically instructed to do so by an AirFlow technical support representative.

The following is an example of the updating procedure, in which the bootflash is updated with a file named *bootrom-1-0-2-9.hex*:

```
~AirSwitch~# conf t
Enter configuration commands, one per line. End with 'exit'
~AirSwitch~(config)# system
Step 1: ~AirSwitch~(config-sys)# bootflash unlock
Step 2: ~AirSwitch~(config-sys)# bootflash update bootrom-1-0-2-
9.hex
Update operation will destroy all data in "bootflash:"
ARE YOU SURE YOU WANT TO DO THIS ? (y/n)y
Erasing chip.....done
Verify chip erase - Verifyinflash.....done
Opening file /flash/bootrom-1-0-2-9.hex ... Done
Size of file /flash/bootrom-1-0-2-9.hex = 1134684
        Reading file...done
        Binary record size 394656 bytes.
        Verify area is erased - Verifying flash....done
        Programming flash.....done
        Programming MAC address.....done
        Verifying programming.....done
bootrom code in the bootflash: device has been updated suc-
cessfully
Step 3: ~AFNworks~(config-sys)# bootflash lock
~AirSwitch~(config-sys)# exit
~AirSwitch~(config)#
```


DCN: as1200sm-B11

VIII. Monitoring Your System

The current release of the AirSwitch 1200 allows system administrators to monitor various critical aspects of the system's operation. The present chapter describes these system monitoring features, organized in the following categories:

Monitoring Client Connections

The AirSwitch constantly monitors the status and activity of all wireless clients attached to the network. Administrators can view this information as the Active Station List, or ASL. (In 802.11 terminology, wireless client devices are referred to as *stations*.) The ASL provides a snapshot of all currently attached clients, including, MAC and IP addresses, owner, connection status, data rate, and other information.

Viewing the ASL

You have a choice of viewing either a short or a more detailed version of the ASL. The **SHOW ASL** command will return the short version, in the format shown below.

```
~AirSwitch~# sh asl

ASL:
MAC Address           IP Address         State          PA       Name

00:40:96:29:FE:E9   202.198.108.151    ASSOCIATED       1       Neo

00:09:5B:10:0E:BE   202.198.108.107    ASSOCIATED       0      Trinity
```

As the example shows, the short version of the ASL displays the following five parameters:

Table 8-1: SHOW ASL, Short Version

Parameter	Description
MAC Address	MAC address of the connected device.

Table 8-1: SHOW ASL, Short Version

Parameter	Description
IP Address	The IP address of the connected device.
State	Current status of the device: • Not authenticated or associated • Authenticated (but not associated) • Associated
PA	ID of the packet antenna currently maintaining the connection with the device.
Name	Name assigned to the device. This is the configurable text string you can assign in the Access Control List.

The **SHOW ASL DETAILS** command will return the more technically detailed version of the ASL, in the format shown below.

```
~AirSwitch~# sh asl details
ASL:

MAC               AID     IP           State   PA CRate SRate  PMode  Cap  Inactivity  Auth
00:40:96:29:FE:E9  461  262.108.128.154  3    1   8    8     200     1    10   1   open sys
00:09:5B:10:0E:BE  463  262.108.128.177  3    0   8    8      1      1    27   2   open sys
```

As the example shows, the ASL displays the following parameters:

Table 8-2: SHOW ASL Details

Parameter	Description
MAC Address	MAC address of the connected device.
AID	Association ID—a unique numeric ID assigned incrementally to every instance of a device associating with the WLAN. Refers to the association itself, rather than the device.
IP	The IP address of the connected device.
State	Current status of the device: • 1 = Not authenticated or associated • 2 = Authenticated but not associated • 3 = Authenticated and associated
PA	ID of the packet antenna currently maintaining the connection with the device.
CRate	Current data transfer rate to and from this client.
SRate	Supported data rates to and from this client.
PMode	Powersave status. (Not supported in current release.)
Cap	Reserved parameter, for internal use.
Inactivity	Inactivity timer, displays the amount of time, in seconds, since any traffic was received from this client. If this reaches the limit set by the Inactivity TImeout config parameter (default is 1000), the AirSwitch assumes the client has left the network, and removes it from the ASL.

DCN: as1200sm-B11

Table 8-2: SHOW ASL Details

Parameter	Description
Auth	WEP authentication type the device used to attach to the network: Open System, or Shared Key.

Viewing System Information

Several of the SHOW commands can be used to display information and statistics on the AirSwitch system. These include:

- SHOW PA
- SHOW INTERFACE
- SHOW SWITCH

These commands require a more detailed explanation.

Viewing Statistics

The **SHOW** command can be used for viewing several basic measurements of the performance of your switch and packet antennas. There are three categories of statistics:

- SHOW PA <name> will show current statistics for packet antennas only. You can use the optional [name] parameter to display statistics for one or more specific PAs at a time. If you do not specify an ID, the CLI will display information for all PAs.
- SHOW INTERFACE <port-list | port no>
- **SHOW SWITCH** will display statistics for the switch only.

Table 8-3 and Table 8-4, below, describe the available PA and switch information. As the Type columns show, most of the available statistics are cumulative in nature: the switch begins monitoring and saving statistics as soon as it boots up, and when you enter any of these commands, the CLI will display cumulative statistics as a total number since that time.

You can use the **CLEAR STATISTICS** command to reset the counters for cumulative statistics, at which time all statistical accumulation restarts from zero. Thus when we refer to the Statistical Period, we mean the time elapsed *either* since the switch was booted, *or* since the CLEAR STATISTICS command was used—whichever occurred more recently.

Viewing Packet Antenna Information

You can use the **SHOW PA** command to display information for all currently attached packet antennas. If you do not specify any ID, information on all detected PAs will be

displayed. If you do specify a packet antenna ID, the request will return information for the specified PA only, as in the following example:

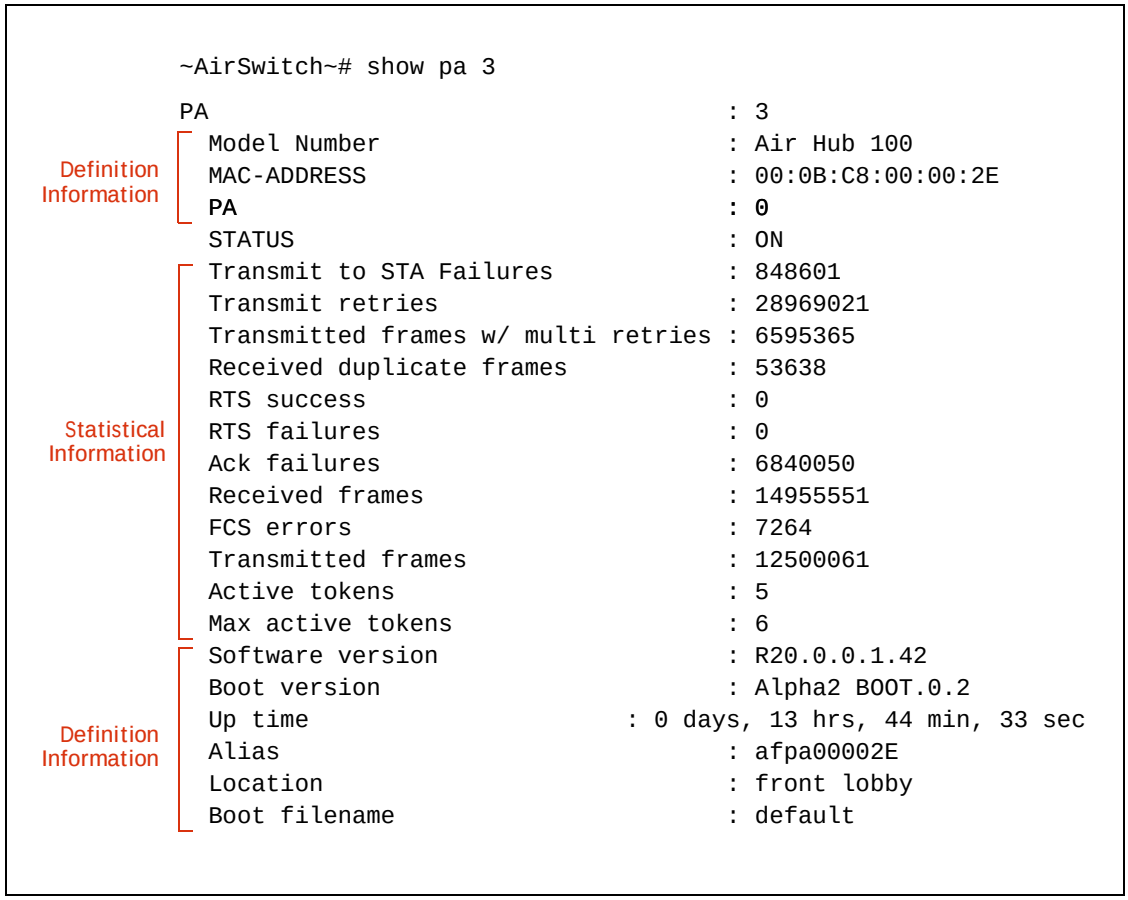


Figure 8-1: Sample Packet Antenna Information

As the example shows, the command returns two kinds of information: definition information, and statistical information. The definition type are self explanatory; the meanings of the statistics are described in the table below.

Table 8-3: Packet Antenna Statistics

Name	Description	Type
Transmit to STA failures	Total unsuccessful attempts to transmit packets to stations attached to this PA.	Cumulative
Transmit retries	Total retry messages detected by this PA since the beginning of the statistical period.	Cumulative
Transmitted frames w/ multi retries	Total multiple retry attempts detected by this PA since the beginning of the statistical period.	Cumulative

DCN: as1200sm-B11

Table 8-3: Packet Antenna Statistics

Name	Description	Type
Received duplicate frames	Total duplicate frames detected by this PA since the beginning of the statistical period.	Cumulative
RTS successes	Total successful RTS (request-to-send) messages detected by this PA since the beginning of the statistical period.	Cumulative
RTS failures	Total unsuccessful RTS (request-to-send) message detected by this PA since the beginning of the statistical period.	Cumulative
ACK failures	Total acknowledgment message failures detected by this PA since the beginning of the statistical period.	Cumulative
Received frames	Total message fragments received by this PA since the beginning of the statistical period. Used only when fragmentation/defragmentation is enabled.	Cumulative
FCS errors	Total FCS errors detected by this PA since the beginning of the statistical period.	Cumulative
Transmitted frames	Total data frames transmitted by this PA since the beginning of the statistical period.	Cumulative
Active tokens	Number of wireless devices currently connected to the WLAN using this PA.	Snapshot
Max active tokens	Highest number of wireless devices simultaneously connected to the WLAN using this PA, at any time since the beginning of the statistical period.	Greatest value over time
Up time	Interval since this PA was last booted up.	Cumulative

Viewing Switch Information

As we mentioned, the **SHOW SWITCH** command will display information on the switch. As with the packet antenna information, this includes both definitional information and statistics.

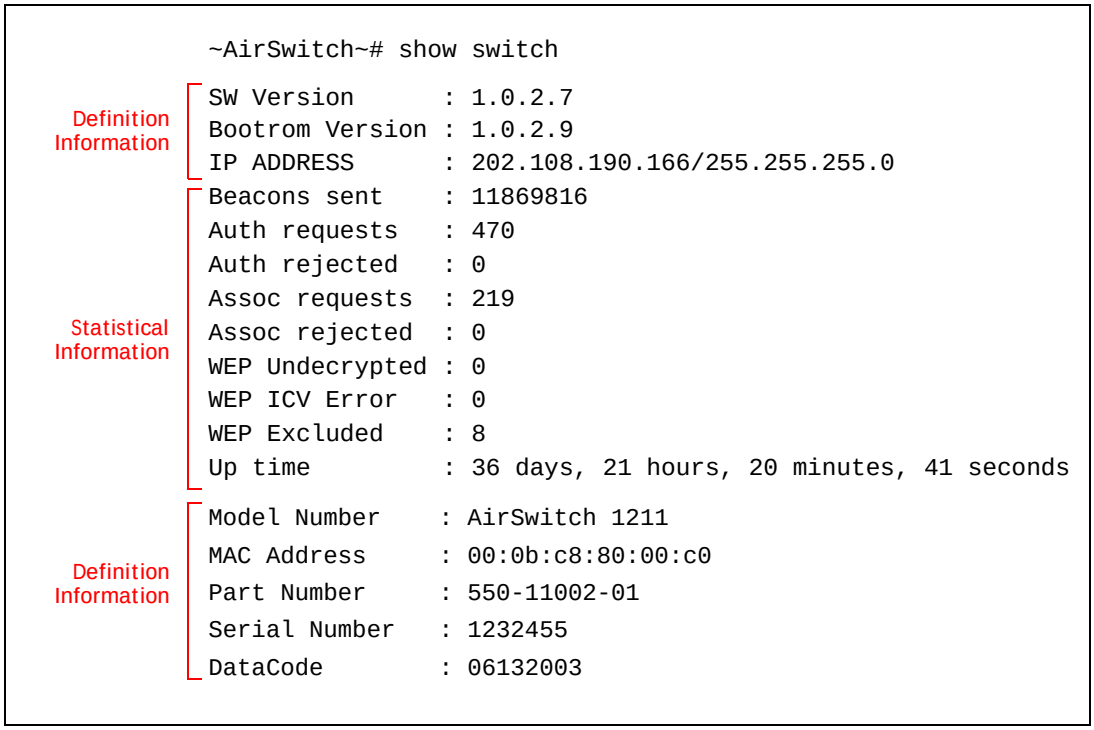


Figure 8-2: Sample Switch Information

Table 8-4 provides a description of the available switch statistics.

Table 8-4: Switch Statistics

Name	Description	Type
Beacons sent	Total number of beacons transmitted by this switch since the beginning of the statistical period.	Cumulative
Auth requests	Total number of authorization requests received by this switch from wireless devices since the beginning of the statistical period.	Cumulative
Auth rejected	Total number of wireless device authorization requests rejected by this switch since the beginning of the statistical period. A request will be rejected when a device not listed in the Access List attempts to connect to the network.	Cumulative
Assoc requests	Total number of association requests received by this switch from wireless devices since the beginning of the statistical period.	Cumulative
Assoc rejected	Total number of wireless device authorization requests rejected by this switch since the beginning of the statistical period. A request may be rejected for various reasons, including incompatible data rates.	Cumulative
WEP Undecrypted	Total number of WEP-encrypted frames the switch received but was unable to decrypt—for example because the keys were not set properly, or the frame was generally corrupted.	Cumulative

DCN: as1200sm-B11

Table 8-4: Switch Statistics

Name	Description	Type
WEP ICV Error	Total number of Integrity Check Value errors detected. (ICV is a checksum mechanism, similar to CRC32 but specific to WEP.)	Cumulative
WEP Excluded	Total number of clear packets that were dropped because WEP is enabled. (When WEP is enabled, the AirSwitch will accept only encrypted traffic and will drop all unencrypted packets.	Cumulative
Up time	Total time elapsed since the last time this switch was rebooted. Displayed in days, hours, minutes and seconds.	Cumulative

Viewing the Entire Configuration

There are two special SHOW commands that give you a snapshot of current configuration settings. You can use the SHOW RUNNING CONFIGURATION command to display a summary of current configuration settings. It will return the parameters as displayed in the following example:

```
~AirSwitch~# show run

# AirSwitch Running Configuration
ANTENNA TX 3
ANTENNA RX 3
BEACON-INTERVAL 100
BEACON-OFFSET 7
BSSID 00:ab:1c:ab:1c:00
CCA-MODE 4
CHANNEL 11
DTIM 2
ED-THRESHOLD 31
HEARTBEAT 1
IP ADDRESS 10.100.100.111 255.255.255.0
LONG-RETRY-LIMIT 4
OPRATE 11
NO PREAMBLE-SHORT
SCOUT afpa00003D LOCATION unknown BOOT default MODE
   1 MAC 00:0B:C8:00:00:3D
SCOUT afpa000038 LOCATION unknown BOOT default MODE
   1 MAC 00:0B:C8:00:00:38
SCOUT afpa00002E LOCATION unknown BOOT default MODE
   1 MAC 00:0B:C8:00:00:2E
SHORT-RETRY-LIMIT 7
SSID SystemTest4 VLAN 0 ADVERTISE
SSID guest PUBLIC VLAN 0
STATION-TIMEOUT 20
SYSNAME AirSwitch
TX-POWER-LEVEL 100
VLAN 3072 AFN-RSVD NAME AFN-Reserved
VLAN 3073 AFN-RSVD NAME2 AFN-Reserved2
VLAN 3074 AFN-RSVD3 NAME AFN-Reserved3
VLAN 3075 AFN-RSVD4 NAME AFN-Reserved4
VLAN 3076 AFN-RSVD5 NAME AFN-Reserved5
VLAN 3077 AFN-RSVD6 NAME AFN-Reserved6
```

```
WEP AUTHENTICATION SHARED
WEP KEY 1 SIZE 128 01010101010101010101010101
   TRANSMIT-KEY
WEP KEY 2 SIZE 40 0000000000
WEP KEY 3 SIZE 40 0000000000
WEP KEY 4 SIZE 40 0000000000

# End of Running Configuration
```

You can also use the SHOW ALL command, which returns an even more extensive list of configuration settings and statistical information.

Restarting Statistical Counting

You can use the CLEAR STATISTICS command to reset the statistical counting period for the switch, PAs, or both. (This command is available only from the Enabled level.) The variations on this command are shown in the table below.

Table 8-5: Restarting Switch and PA Satatitstics

To Reset:	Use Command:
AirSwitch only	`~AirSwitch~# clear stat sw`
All PAs only	`~AirSwitch~# clear stat pa`
Specified PA	`~AirSwitch~# clear stat pa <name>`
AirSwitch and all PAs	`~AirSwitch~# clear stat all`

Viewing Interface Information

The AirSwitch allows you to display the status of all switch interfaces at any time. To view interface status, navigate to the Enable mode and type

```
show interface [port-list]
```

For the optional [port-list] parameter, you may specify one or more defined interfaces, by port list. If you do not specify individual interfaces, the switch displays only VLAN association and STP settings for all ports, in the format shown in the left side of Figure 8-3.

If you do specify one or more interfaces, the switch returns more detailed statistical information on packet traffic into and out of the specified interfaces. A sample output from this command is shown in the right side of Figure 8-3.

DCN: as1200sm-B11

```
~AirSwitch #~ show interface

FE11: VLAN  ID: 1
     STP COST: 19
     STP PORT-PRIORITY: 128

FE12: VLAN  ID: 1
     STP COST: 19
     STP PORT-PRIORITY: 128

GE2: VLAN  ID: 1
     STP COST: 2
     STP PORT-PRIORITY: 128
     MGMT MODE: ON

GE2: VLAN  ID: 1
     STP COST: 1
     STP PORT-PRIORITY: 128
     MGMT MODE: ON

SVC: MGMT MODE: OFF
```

```
~AirSwitch #~ show interface fe4-fe5

FE4
IP ADDR: 121.82.115.200
VLAN  ID: 1
STP COST: 19
STP PORT-PRIORITY: 128
Speed:          0 Mb/s
Duplex:         HalfDuplex
LinkState:      Up
AdminState:     Up
InOctets:       0
InUCastPkts:    0
InNUCastPkts:   0
OutOctets:      64
OutUCastPkts:   1
OutNUCastPkts: 1

FE5
IP ADDR: 121.82.115.200
VLAN  ID: 1
STP COST: 19
STP PORT-PRIORITY: 128
Speed:          0 Mb/s
Duplex:         HalfDuplex
LinkState:      Down
AdminState:     Up
InOctets:       0
InUCastPkts:    0
InNUCastPkts:   0
OutOctets:      64
OutUCastPkts:   1
OutNUCastPkts: 1
```

Figure 8-3: Show Interface Output, Global and Detailed

Table 8-6 provides descriptions of the statistics provided in the more detailed output.

Table 8-6: Interface Statistics

Element	Description
IP ADDR	IP address assigned to this port.
VLAN ID	The VLAN with which this port or ports is currently associated (see "The Interface Submode," on page 116.
STP COST	STP Cost value currently assigned to this port or ports (see "The Interface Submode," on page 116.
STP PORT-PRIORITY	STP port priority value currently assigned to this port or ports (see "The Interface Submode," on page 116.
Speed	Current data transmission speed of this port or ports.
Duplex	Duplex type currently assigned to this port or ports, either half- or full-duplex.
LinkState	Current link status of this port or ports. Up = there is currently an Ethernet connection to a network device from this port. Down = no Ethernet connection is currently detected at this interface.

Table 8-6: Interface Statistics

Element	Description
AdminState	Shows whether the administrative state of this port or ports, either Up (not blocked) or Down (blocked).
InOctets	Number of inbound octets received by the interface since the last reboot of the switch.
InUCastPkts	Number of inbound unicast packets received by the interface since the last reboot of the switch.
InNUCastPkts	Number of inbound non-unicast packets received by the interface since the last reboot of the switch.
OutOctets	Number of outbound octets received by the interface since the last reboot of the switch.
OutUCastPkts	Number of outbound unicast packets received by the interface since the last reboot of the switch.
OutNUCastPkts	Number of outbound non-unicast packets received by the interface since the last reboot of the switch.

Restarting Interface Statistics

You can use the CLEAR COUNTERS command to reset the statistical counting period for interfaces. (This command is available only from the Configure level.) If you want to restart counting for a specific interface, specify it by port list, thus:

```
~AirSwitch (config)~# clear counters FE2-FE4
```

The System Log

The AirSwitch constantly maintains a system event log, recording and describing the major system events of interest to users. This log is always saved to system NVRAM, and also optionally printed to the console. Console logging is enabled by default, but you can turn it off with the command

```
NO LOGGING CONSOLE
```

Displaying System Log Settings

You can use the SHOW LOGGING command to display current configuration of event logging. Here are the default settings:

```
~AFNworks~# sh log
LOGGING CONSOLE : ENABLE
LOGGING NVRAM   : ENABLE
NVRAM SIZE      : 320
LOGGING SERVER  : DISABLE

TASK            : LEVEL
tRootTask     : FATAL
tNetTask      : FATAL
tTelnetd      : FATAL
tSender       : FATAL
```


DCN: as1200sm-B11

```
tBeacon       : FATAL
tRepeaterMgmt : FATAL
tTokenMgmt    : FATAL
tSignaling    : FATAL
tData         : FATAL
tDnld         : FATAL
tWebSerGA     : FATAL
tControl      : FATAL
tAslAgeing    : FATAL
tTelnetC0     : FATAL
```

The first line, `logging console Enable`, shows that the current event log is be displayed on the system console. Note that this refers both to the a local console, connected directly to the management port (labeled SERIAL), and to any console connected remotely via telnet.

The second and third lines show that event logs are saved in NVRAM, in a 320-line circular buffer. When the log reaches this size, the oldest events are deleted as new ones are added. NVRAM logging cannot be disabled. You can change the buffer size, but this is not recommended.

The remaining lines display the event level set for each individual software task. This information is for internal debugging and troubleshooting by AirFlow technicians, and may be disregarded.

Logging Timestamps

By default, each log entry is timestamped with in YYYY-MM-DD HH-MM-SS format. You can disable log timestamps with the CLI command:

```
~AirSwitch(config)~# no logging timestamp
```

Timestamping can be re-enabled with the following command:

```
~AirSwitch(config)~# logging timestamp
```

Bear in mind that the LOGGING TIMESTAMP command controls timestamping to the log in NVRAM, whether or not it is being sent to the console.

Viewing Log Contents

You can use the SHOW LOGGING command to view the contents of the current system log in NVRAM. If you specify a positive number of lines, you will view that number of entries, starting with the lastest one and moving backwards in time. For example, to see the last twenty entries, type

```
~AirSwitch(config)~# logging nvram 20
```

If you specify a negative number, the list will start with the oldest entry in the log and move forwared in time. Thus the command

```
~AirSwitch(config)~# logging nvram -50
```

would display the fifty earliest entries.

Saving System Log Contents

You can write the current contents of the NVRAM log buffer to a file, using the command

```
LOGGING SAVE-FILE <filename>
```

where <filename> is the name of the log file you want to save. You can then use the file handling commands to view the contents of this file, rename it, or send it from the switch to a remote host.

DCN: as1200sm-B11

IX. Layer 2 Switching Features

The current release of the AirSwitch supports a number of features connected with Layer 2 switching. These features include:

- VLANs (page 83)
- Spanning Tree Protocol (STP) (page 85)
- Class of Service (page 88)
- Port Mirroring (page 89)
- Packet Storm Control (page 90)

VLANs

The AirSwitch 1200 supports Virtual LANs, or VLANs, which improve performance by dividing network traffic based on categories. There are two types of VLANs: *Internal*, which are present by default and cannot be deleted or renamed; and *Port-Based*, which you can create to suit your needs, edit, and delete.

Viewing VLANs

You can view the current VLAN configuration settings through the CLI, using the SHOW VLAN command. The following sample shows the command and the results it returns:

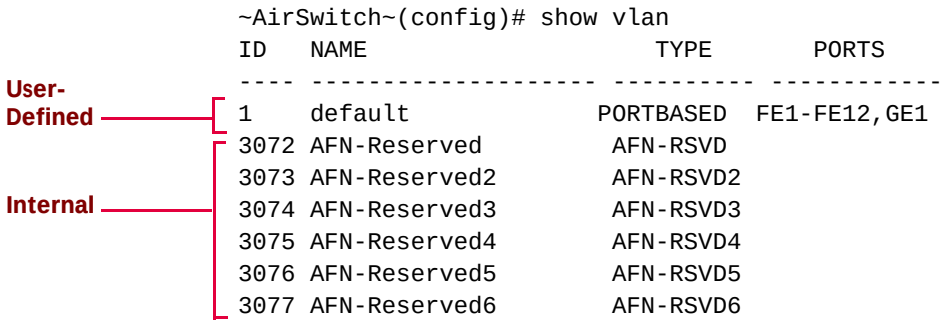


Figure 9-1: Viewing VLANS

This example illustrates the two types of VLANs. User-defined VLANs have type = PORTBASED; all other types are internal VLANs.

Internal VLANs

The current version of the AirSwitch supports six internal VLANs, one for each type of traffic specific to the AirFlow converged network.

These six, with IDs from 3072 through 3077, are automatically present when you first boot up the switch. They are for internal use, and only the ID field is editable. You may assign a new ID if one of these default values conflicts with another VLAN you have already set up in your network; otherwise you should just ignore them.

Collapsing Internal VLANs

During the initial setup dialog, you will have a chance to collapse the six internal VLANs into a single VLAN:

```
Would you like to collapse the block of 6 reserved VLANs into
a single VLAN? [yes]
```

If your network does not allow multiple VLANs—for example, if you have separated the AirSwitch from the PAs with a switch or other device that does not support multiple VLANs—you will need to choose this option. (You also need to do this if you are using server mode.)

If you accept the default Yes at this step in the dialog, your internal VLANs will be collapsed into one—specifically, the first one in the list:

```
3072    AFN-Reserved      AFN-RSVD
```

If you assign new IDs to these VLANs, the single collapsed VLAN will be the first in the ID block you assign. For instance, if during the setup dialog you choose to override the default block and create a block starting with 2002, then the collapsed VLAN will be ID 2002.

Note that this affects only the six internal VLANs. You will still be able to create and use port-based VLANs.

You can collapse your VLANs, or restore them once collapsed, at any time after the setup dialog, using the SYSVLAN command (page 120).

User-Defined VLANs

Besides the internal VLANs described above, you can define up to 16 configurable VLANs, allowing you to segment wireless user traffic according to categories that make sense in your specific context. For example, you might define one VLAN for use by all members of your company's Engineering organization, other for the Product Training group, and so on.

VLANs are defined by association with an Interface in the AirSwitch. This association is not defined in the VLAN itself, but in the Interface. VLANs are created independently, and then associated to an interface as one of the interface's definition parameters.

The AirSwitch is factory-set with one default port-based VLAN, VLAN1. Until you make any changes, all interfaces belong to this VLAN, meaning that the network is not segmented. The sample in Figure 9-1 illustates this default situation.

DCN: as1200sm-B11

When you create new port-based VLANs and associate FE interfaces (i.e. the twelve 10/100 ETH ports) with them, these interfaces are removed from the default VLAN1, since FE interfaces can only belong to one VLAN at a time. By contrast, GE interfaces (the two Gb uplink ports) can belong to multiple VLANs, as well as in the default VLAN1.

Setting up VLANs

To configure VLAN features in the CLI, you must navigate to the Configure level. and type the command **VLAN [ID]**. This will move you to the VLAN submode, where you can set parameters for the individual VLAN represented by the specified ID. If the specified ID exists, you can make changes to the VLAN. If it does not exist already, you are creating a new VLAN.

A VLAN is defined by three parameters: ID, Name, and Type. For internal VLANs, only the ID field is editable; for existing user-defined VLANs, you can change any of the parameters except Type.

The VLAN type for all User-Defined VLANs must be PORT-BASED—you cannot create new internal VLANs. Note that these values are not case-sensitive.

You use the command **END** to exit the submode and return to global Configure level.

Example

The following example would create a new VLAN with ID 3190, and return to Config level.

```
~AirSwitch~> enable
~AirSwitch~# config t
~AirSwitch~# (config)~# VLAN 3190
~AirSwitch~# (config-vlan)~# name SystemTest
~AirSwitch~# (config-vlan)~# type Port-Based
~AirSwitch~# (config-vlan)~# end
~AirSwitch~# (config)~#
```

The commands for creating a new VLAN are the same as for changing one or more parameters of an existing one. If the specified ID does not exist yet, a new VLAN will be defined; if it does already exist, it will be changed to reflect any new parameter values.

Note that you can also use the **NO** and **SHOW** commands from inside VLAN submode. For complete list of all commands, see "The VLAN Submode," on page 120.

Spanning Tree Protocol (STP)

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that ensures redundant links between end stations while protecting against the creation of data loops. It does this by comparing priority levels assigned to all switches in the network, and to all ports within those switches. In addition, it considers the assigned data speed (referred to as the *port cost*) of each port in the network. Whenever a switch detects two or more redundant paths between end stations, the spanning

tree algorithm uses priorities and cost values to assign one path as primary and place it in forwarding state, and then places all redundant paths in blocked state.

The current release of the AirSwitch allows administrators to configure the following settings:

Switch priority: A global configuration parameter, which assigns a priority to the whole switch vis-a-vis other switches in the network. This is an integer value from 1 to 65535; the lower the integer, the higher the priority. The default priority is 32768. Because this is a global parameter, governing the switch as a whole, it is set at the Configure level of the CLI.

Port priority: Assigns a priority for one or more specified ports, defined as an interface, within the switch. This is an integer value from 1 to 65535; the lower the integer, the higher the priority. Default priority is 128. Because this is an interface-specific parameter, it is set in the interface submode (see "The Interface Submode," on page 116.)

Port cost: This value represents a bandwidth or media speed assigned to the specified interface. Because this is an interface-specific parameter, it is set in the interface submode (see "The Interface Submode," on page 116.)

Hello time: All network switches participating in the spanning tree must identify one another and exchange information about their own and their ports' priority settings. The Hello Time parameter represents the interval, in seconds, at which this switch will broadcast these so-called "hello" messages. Valid values are 1 through 10; default is 2. Because this is a global parameter, governing the switch as a whole, it is set at the Configure level of the CLI.

Forwarding delay time: When the switch receives new information in hello messages, it pauses in listening and learning states before it proceeds to forward data packets. This parameter sets the length of that delay, in seconds. Valid values are 4 to 30; default is 15. Because it is a global parameter, governing the switch as a whole, it is set at the Configure level of the CLI.

Maximum aging time: Sets the maximum duration, in seconds, that this switch will store STP information it receives about other ports in the network. Valid values are 6 through 40; default is 20. Because this is a global parameter, governing the switch as a whole, it is set at the Configure level of the CLI.

You can set up STP operation through CLI commands.

Configuring STP

To set STP features in the CLI, you must navigate to the Configure level. The command for controlling STP features is **STP**.

All STP commands are described in table below. Note that most are global configuration commands, meaning that they govern the switch as a whole; however, there are two exceptions—STP PORT-PRIORITY and STP COST—that operate at the individual interface level, and so must be set in the Interface submode (see "The Interface Submode," on page 116).

Table 9-1: STP CLI Commands

Parameter	Description
STP MODE	Enables STP, if already disabled.
NO STP MODE	Disables STP, if already enabled.
STP PRIORITY	Sets the STP priority of the entire switch. Syntax = STP PRIORITY <priority>, where:
<priority>	priority value of the switch, as an integer from 0 - 65535; lower value is higher priority
STP PORT-PRIORITY	Sets the STP priority of individual ports. Because it operates at the individual interface level, it must be set in the Interface submode. Syntax = STP PORT-PRIORITY <priority>, where:
<priority>	priority value of specified port(s), as an integer from 0 - 65535; lower value is higher priority. Defaults: FE ports 128, GE ports 64.
STP COST	Sets the STP cost of individual ports. Because it operates at the individual interface level, it must be set in the Interface submode. Syntax = STP COST <cost>, where:
<cost>	cost value of specified port(s), as an integer from 1 -200 000 000; lower value is higher speed. Defaults: FE ports 19, GE ports 4.
STP HELLO	Sets the hello time for the entire switch. Syntax = STP HELLO <hello-time>, where:
<hello-time>	hello-time value in seconds, as an integer from 1 - 10. Default value is 2.
STP FORWARD	Sets the duration of the forward delay timer for the entire switch. Syntax = STP FORWARD <fwd-time>, where:
<fwd-time>	forward delay timer value in seconds, as an integer from 4 - 30. Default value is 15.
STP AGE	Sets the duration of the age time for the entire switch. Syntax = STP AGE <age-time>, where:
<age-time>	age-time value in seconds, as an integer from 6 - 40. Default value is 20.

SHOW STP	Displays the currently configured STP settings. Sample output from this command:
	`STP Mode:  ON`
	`Switch Priority: 32768`
	`Hello Interval: 2 seconds`
	`Max. Aging Time: 20 seconds`
	`Forward Delay: 15 seconds`

Class of Service

The current release of the AirSwitch supports eight Class of Service levels, mapped to four levels of egress queues. Users can map the CoS levels to queues in the AirSwitch, and define the way the AirSwitch will handle packets with those levels assigned, as well as how it will handle packets with no CoS tags assigned.

Configuring CoS

To set CoS features in the CLI, you must navigate to the global Configure level. The use of **CoS** commands is described in the table below.

Table 9-2: CoS CLI Commands

Parameter	Description
COS BANDWIDTH	Assigns a bandwidth value to each of the four queues. This value represents the number of packets for one queue sent per number of packets in other queues; valid values are 0-255. If this value is set to anything but zero, the AirSwitch will assign the specified priorities to the four queues, which then handle tagged packets in a weighted round robin treatment. If all four are set to the default value, 0, the priority is set to strict priority treatment. This means that rather than applying a round robin treatment the switch will always handle packets from the highest level queue only, and will never handle packets from lower queues as long as there are any waiting in a higher one. Syntax = CoS BANDWIDTH <weight1 weight 2 weight 3 weight 4>, where:
<weight 1>	The priority assigned to queue 1.
<weight 2>	The priority assigned to queue 2.
<weight 3>	The priority assigned to queue 3.
<weight 4>	The priority assigned to queue 4.
NO COS BANDWIDTH	Removes any configured round-robin bandwidth settings, and restores the default value of all zeros (i.e., strict priority).
COS MAP	Used to map the eight priority levels in the packet tags, to the four port-based queues in the AirSwitch. You can map one or more CoS levels to each port-based queue. You must specify the mapping for each of the four queues separately. Syntax = COS MAP <queue> <cos-list>, where:
<queue>	The number of an AirSwitch queue.
<cos-list>	The one or more CoS levels mapped to that queue.
COS UNTAGGED	Specifies what kind of treatment will be applied to packets that arrive without any CoS tags attached. When you set some value here, the AirSwitch will treat all untagged packets as though they were tagged with that value. Syntax = CoS UNTAGGED <cos>, where:
<cos>	One of the eight CoS packet tags.

SHOW COS	Displays the currently configured CoS settings. Sample output from this command:
	`Untagged CoS:  7`
	`Priority:      weighted round robin`
	`Queue      CoS      Bandwidth`
	`1        0,1        75`
	`2        2,3        150`
	`3        4,5        200`
	`4        6,7        255`

DCN: as1200sm-B11

Example

To set up the CoS configuration shown in the SHOW COS sample in the last row of the table above, you would use the following command sequence:

```
~AirSwitch (config)~# cos bandwidth 75 150 200 255
~AirSwitch (config)~# cos untagged 7
~AirSwitch (config)~# cos map 1 0,1
~AirSwitch (config)~# cos map 2 2,3
~AirSwitch (config)~# cos map 3 4,5
~AirSwitch (config)~# cos map 4 6,7
~AirSwitch (config)~# exit
~AirSwitch ~#
```

Port Mirroring

Port Mirroring refers to the ability to copy all data packets moving to and from one or more switch ports, and direct that copied traffic to a specified different port where they can be analyzed by a packet analyzer. The port or ports where the traffic will be copied is referred to as the *source port* and the port where the packet analyzer will receive them is called the *destination port*.

The AirSwitch 1200 allows administrators to configure port mirroring through the Enabled CLI level.

Configuring Port Mirroring

To set port mirroring features in the CLI, you must navigate to the Configure level. The command for controlling port mirroring features is **MIRROR**. This command has two parameters, Source and Destination, whose use is described in the table below. Note that you can also use the **NO** and **SHOW** commands with **MIRROR**.

Table 9-3: Port Mirroring CLI Commands

Parameter	Description
MIRROR SOURCE	Designates a specified port list as source to be mirrored. Note that you must designate a DEST port first, then your SOURCE ports. Syntax = MIRROR SOURCE <source-port-list> [both | rx | tx], where:
<source-port-list>	The physical port or ports you wish to mirror, from FE1-FE12. May be represented as a single port, a range of contiguous ports (e.g. FE4-FE7), or a comma-delimited set of non-contiguous ports (e.g. FE3,FE5,FE10).
[both | rx | tx]	Direction of packet traffic you wish to mirror from this port list: transmit only, receive only, or both transmit and receive.
NO MIRROR SOURCE	Disables port mirroring at the specified source, in the specified direction. You can use this command to disable mirroring of only Tx or only Rx packets, while continuing to mirror the other (Rx or Tx, respectively). Syntax = MIRROR SOURCE <source-port-list> [both | rx | tx], where:
<source-port-list>	Comma delineated list of one or more ports, whose traffic you wish to mirror.
[both | rx | tx]	Direction of the packet traffic you wish to stop mirroring from this port list: transmit only, receive only, or both transmit and receive.
MIRROR DEST	Specifies the mirrored-to port for port mirroring. Note that you must designate this port first, before you set any SOURCE ports. Syntax = MIRROR DEST <destination-port>, where:

Table 9-3: Port Mirroring CLI Commands

Parameter	Description
<destination-port>	Number of the port to which you wish to send the mirrored traffic from the source port(s).
NO MIRROR DEST	Stops mirroring to the specified destination port.

SHOW MIRROR	Displays current Port Mirroring settings. Sample output of this command:
	`Rx mirroring ports: 5`
	`Tx mirroring ports: 1,3,5`
	`Destination Port: 12`

As a rule, you will generally use mirror commands in pairs, to specify the source and the destination. For example, if you wanted to disable the mirroring setup shown in the **SHOW MIRROR** example in the table, you would have to type two commands:

```
~AirSwitch~ # no mirror source 1,3,5
~AirSwitch~ # no mirror dest 12
```

The first command will stop both the Rx and Tx mirroring. There is no need to specify traffic direction, since Both is the default, but you could stop mirroring only to one or the other if you wished.

When setting up mirroring, you must define the Destination port before you set the Source port or ports. When disabling, the sequence does not matter. Lastly, be sure you do not define a port as both DEST and SOURCE.

Packet Storm Control

The current release of the AirSwitch provides a Packet Storm Control feature which, when enabled, prevents overload levels of data traffic through individual ports. The storm control mechanism constantly monitors traffic levels and drops excess packets when levels reach a specified threshold, expressed as a percentage of the port's available bandwidth. When levels drop back below the specified threshold, the port resumes switching all packets normally.

This feature applies to all kinds of packets—broadcast, multicast, and unicast. By default, it is disabled until you turn it on.

Configuring Storm Control

To set storm control features in the CLI, you must navigate to the Configure level. The command for controlling this feature is **STORM-CONTROL**. All storm control settings apply to the entire switch, rather than to individual VLANs.

DCN: as1200sm-B11

All storm control commands are described in table below.

Table 9-4: Storm Control CLI Commands

Parameter	Description
STORM-CONTROL	Enables storm control feature at a specified level, if already disabled. (Available at the Configure level only.) Syntax = STORM-CONTROL <level>, where:
<level>	Control level as a percent of each port's available bandwidth. Valid values are 0-99. The default value of 0 means storm control is disabled.
NO STORM-CONTROL	Disables storm control, if already enabled. This is the same as setting the level to 0%.
SHOW STORM-CONTROL	Displays the currently configured storm control settings. Sample output from this command: `Storm-control level: 5%`

DCN: as1200sm-B11

A. CLI Reference

This Appendix provides a complete overview of how to use the AirSwitch's command line interface, followed by descriptions of all available commands. Commands are listed in alphabetical order, grouped according to the three levels of the CLI structure as shown in Figure A-1, below. Note that the command prompt itself is slightly different on each level, providing a helpful visual cue for users.

It is organized in the following sections:

Using the Command Line Interface

This section provides a brief description of the AirFlow command line interface, or CLI. You can type these commands from a locally connected console, or remotely through a telnet connection.

Because the AirSwitch has a line-based rather than character-based CLI, you should avoid using standard CTRL keyboard functions. For example, if you accidentally press CTRL+S, you will lock console scrolling; you can release it with CTRL+Q.

Note that although they are shown in block capitals in this manual and onscreen, all commands and parameters are cap-insensitive, so *beacon-interval*, *Beacon-Interval*, and *BEACON-INTERVAL* will all invoke the same function.

The CLI Structure

Figure A-1, below, shows all CLI commands and their structure. As the figure shows, the CLI structure comprises a hierarchy of three command levels, plus a sub-mode level:

- Main Commands

- Enabled Commands
- Configuration Commands
  - Individual submodes

Note that the five commands shown in bold in the figure—**?**, **Help**, **CLS**, **Ping**, and **Show**—are available at all three levels.

Angle brackets indicate **<**mandatory**>** parameters; square brackets indicate [optional] parameters.

About Submodes

Submodes may be thought of as sub-levels below Configure, used for configuring individual entities rather than global settings. You enter a submode by command lines that refer to the specific entity you are configuring. For example, some Interface-related configuration parameters are global for all interfaces, and so can be set from the configure level like any other commands; but others are specific to individual interfaces, and so to configure these you must enter the submode for the individual interface, specified by port list. When you are finished with changes, you use the END command to navigate back up to the configure level.

In the current version there are two submodes, for Interfaces and VLANs. More detailed information on using them is provided in the specific Command Line descriptions (see "Submode Commands," on page 114).

Navigating through the CLI

When you first connect to the switch by a serial console or telnet connection, you will begin at the Main command level. The CLI utility will prompt you for a password before you can use the Enabled- and Configure-level commands. The factory default password is **afnafn**; the first time you use it you will be prompted to change it to something more suitable. For detailed information on doing this, see "Changing the CLI Enable Password," on page 48.

In Figure A-1, the commands for navigating between levels are indicated by red arrows. As a navigation cue for users, the command prompt differs slightly from level to level:

- Main level: `~AirSwitch~>`
- Enabled level: `~AirSwitch~#`
- Configuration level: `~AirSwitch~(config)#`
- Submodes: `~AirSwitch~(config-if)#`
  `~AirSwitch~(config-vlan)#`

DCN: as1200sm-B11

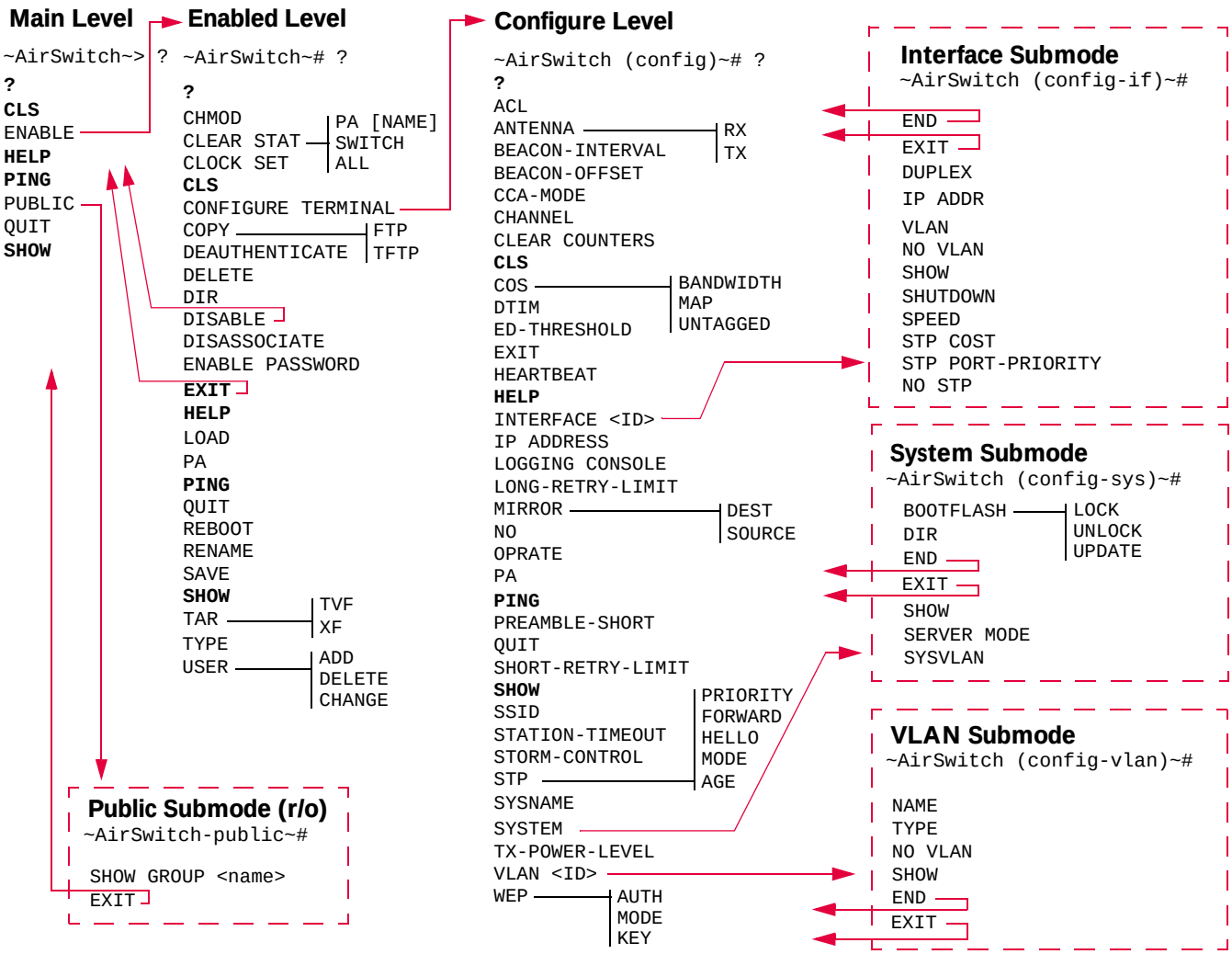


Figure A-1: Command Line Architecture

Abbreviated Commands

For ease of use, the AirFlow CLI is equipped with an intelligent assistant, which recognizes the full command as soon as the user types enough characters to provide a unique identification. This means that instead of typing the whole string for any given command, you can always use the shortest abbreviation unique to that command at that level. For example, at the Enabled level instead of typing out

```
show switch
```

you can return the same result with the command

```
sh sw
```

This is so because at this level two characters are sufficient to provide a unique abbreviation for each: SHOW is the only command starting with "sh", and SWITCH is the only SHOW parameter starting with "sw".

If you type an abbreviated command that is not unique, the switch will prompt you for clarification. For example, when you are at the Configure level "sh" is not unique to the SHOW command, and will result in the following response:

```
~AirSwitch~(config)# sh sw
sh: ambiguous command
```

CLI Help Commands

In addition, if you type a string of characters and then a ?, the CLI will return a list of all commands that begin with that string. For example, if you type

```
di?
```

the CLI will display all commands beginning with "di":

```
DIR          Display all file names
DISABLE      Exit Enabled Mode
DISASSOCIATE Disassociate this station
```

and you can then choose the command you were looking for.

Note that you must not type a space before the question mark. If you do type a space before the question mark, the CLI will return the syntax of all parameters available with that command.

If you type only a ? from the command prompt, the CLI will display a list of all available commands, as described in the following section. This is the same result as typing the HELP command.

Bear in mind that these queries will return different results depending on the level you are working at—Main, Enabled, or Configuration.

DCN: as1200sm-B11

Main Commands

As the figure shows, there are six commands available at the top, or main, level of the AirFlow CLI.

? Displays a list of all available commands, just as the **HELP** command does. This command is available from all three levels.

cls Clears the current terminal screen, leaving only the CLI prompt. This command is available from all three levels.

enable Navigation command; moves authorized user down to the Enabled-level commands. This command will return a password prompt; user must supply a password before moving to the Enabled level.

help Displays a list of all available commands, just as the **?** command does. This command is available from all three levels.

ping Sends a network ping to a specified IP address, without exiting the CLI.

Syntax: PING <IP address> [SIZE <size>], where:

<IP address> = Target host that you wish to ping.

[SIZE <size>] = Size of the ping packet, in bits. Default is 64; valid range is 8 to 4000.

public Navigation command; moves authorized users down to the Public submode. This command will return a password request; user must supply a password before moving to a special submode prompt:

```
~AirSwitch-public~>
```

At this submode, you can use the SHOW GROUP [name] command to view current visitor group definitions, for the public port.

quit Disconnects from AirSwitch and ends telnet session.

show Displays the current value of various settings for this switch; these Show Parameters are listed in Table A-1. This command is available from all three levels. You can use multiple parameters with one Show command, and the CLI will display all requested values. Use the special **SHOW ALL** command to display the entire running configuration.

Enabled Commands

All commands available at the Enabled level are listed below, with functional description and required syntax (if applicable). Note that in the syntax descriptions, angle brackets indicate **<**mandatory parameters**>**; square brackets indicate [optional parameters]. Where appropriate, examples are also provided.

? Displays a list of all available commands. Same function as **Help** command. This command is available from all three levels.

chmod Allows you to change the mode of a specified file from read-write to read-only, or vice versa. Read-only files cannot be overwritten or deleted. Most of the time you will want system files to be read-only, to prevent accidental overwriting or deletion; but if you need to upgrade your firmware you will need to change them to read/write.

Syntax: CHMOD { [rd | rw] } [filename], where:

[rd | rw] = new mode you want to assign to the specified file, and

[filename] = the name of the file you want to change.

clear statistics Resets the collection of PA and switch statistics. In response to this command, the statistical monitoring mechanism will clear its memory and begin collecting cumulative statistics from this moment.

Syntax: CLEAR STATISTICS { SWITCH | PA [NAME] | ALL }

Note the variations of this command: you can clear the switch statistics only, all PA statistics only, statistics of a single PA specified by name, or all stats for switch and all PAs.

clock set Resets the AirSwitch system clock.

Syntax: CLOCK SET <hh:mm:ss> <month> <dd> <yyyy>

cls Clears the current terminal screen, leaving only the CLI prompt. This command is available from all three levels.

configure Navigation command; moves user down to the Configure-level commands as described below (see "Configure Commands," on page 104).

Syntax: CONFIGURE <terminal>

<terminal> = Specifies meaning as CLI navigation command. Currently the only parameter for the CONFIGURE command; others will be enabled in future releases.

DCN: as1200sm-B11

copy Used for managing configuration files. Copies the specified file to a new or existing file.

Syntax: COPY <sourceFileName> <destFileName>, where:

<sourceFileName> = Name of the file you wish to copy from;

destFileName> = Name of the file you wish to copy to. If this file already exists, it will be overwritten; if not, a new file is created.

copy ftp Used for downloading files from a remote host to the switch via FTP, or for uploading files from the switch to a remote location. May be used for configuration files, upgrade software tar files, or Access Control Lists.

Syntax: COPY FTP://<username>:<passwd>@<sourcehost>/<source directory>/<sourcefilename> <targetfilename> [binary|ascii] [verbose], where:

<username> = FTP username for connecting to the remote host;

<passwd> = FTP password for connecting to the remote host;

<sourcehost> = IP address of the remote host from which you are copying the file;

<sourcedirectory> = Directory path on the remote host where the desired file is located;

<sourcefilename> = Name of the file you wish to download;

<targetfilename> = Name of the file as you want it to be written to the AirSwitch file system (usually this will be the same as the sourcefile);

[binary|ASCII] = Optional parameter, specifies if file transfer mode is binary or ASCII. Default is ASCII.

[verbose] = a flag that, when set, sends a series of characters to the console while the file copies, as a visual cue that the process is underway.

copy tftp Used for downloading files to the switch via TFTP. Similar to COPY FTP, but without any username or password parameters.

Syntax: COPY TFTP://<sourcehost>/<source directory>/<sourcefilename> <target-filename> [binary|ascii]

deauthenticate Manually deauthenticates a specified wireless device, forcing it to reauthenticate (see "Controlling Client Connections," on page 50).

Syntax: DEAUTHENTICATE <mac>, where:

<mac> = MAC address of the device you want to deauthenticate.

delete Used for managing configuration files. Deletes the specified file.

Syntax: DELETE <filename>

dir Displays names of all files in the current file directory (useful when saving config files, to avoid unintended overwriting).

disable Navigation command; moves user back up to the Main-level commands (see "Main Commands," on page 97).

disassociate Manually disassociates a specified wireless device (see "Controlling Client Connections," on page 50).

Syntax: DISASSOCIATE <mac>, where:

<mac> = MAC address of the device you want to deauthenticate.

After you disassociate a device, it remains authenticated and will promptly reassociate to the network. If you want to prevent it from reconnecting the the network, use the **ACL <mac> BLOCK** command, then disassociate the device.

enable password Changes the CLI password, required for navigating from Main to Enabled level. This command has no parameters, but is followed by a prompt for current password (see "Changing the CLI Enable Password," on page 48). Maximum permitted length of password is 30 characters.

Syntax: ENABLE PASSWORD

help Displays a list of all available commands, just as the **?** command does. This command is available from all three levels.

load Loads the configuration parameters from an existing config file, which had been created by the Save command.

Syntax: LOAD [filename], where:

[filename] = Name of the configuration file you want to load. If no file name is specified, the switch will look for the default file name *config.txt*.

quit Disconnects from the AirSwitch and ends the current telnet session.

pa Used to change the operational state of an already connected and operating packet antenna.

Both **activate** and **reset** will place the PA in an active state; **standby** will place it in standby. This is an optional parameter; default state is Active.

DCN: as1200sm-B11

The **reset** parameter will also force a hard restart, at which time the PA will load any software upgrades that may have been sent down by the AirSwitch.

Syntax: PA name {ACTIVATE | RESET | STANDBY}, where:

[name] = Name of the PA you wish to configure or reset. Names are automatically assigned during bootup, based on MAC addresses; but you can replace these default names with something more descriptive and helpful. You can use an alphanumeric string up to 16 characters.

[location] = Like the name, this is a default value that you can manually replace with a description of the physical location of this PA.

For more details on changing these parameters, see "Managing Packet Antennas," on page 48.

`ping` Sends a network ping to a specified IP address, without exiting the CLI.

Syntax: PING <IP address> [SIZE <size>], where:

<IP address> = Target host that you wish to ping

[SIZE <size>] = Size of the ping packet, in bits. Default is 64; valid range is 8 to 4000.

`reboot` Reboots the switch. When the switch reboots, it will draw configuration values from the default file called **config.txt**.

Syntax: REBOOT <now>, where:

<now> = Tells the switch to reboot immediately. Currently the only parameter for the REBOOT command; others will be enabled in future releases.

`rename` Used for managing configuration files. Renames a specified file with the specified new name.

Syntax: RENAME <oldfilename> <newfilename>

`save` Saves the current configuration to a config file, stored in flash memory on the switch.

Syntax: SAVE [filename], where:

[filename] = Name of the configuration file where you want the running configuration to be saved. If no file name is specified, the configuration will be saved by default in a file called *config.txt*. If the specified file already exists, it will be overwritten with the current configuration.

show Displays the current value of various settings for this switch; these Show Parameters are listed in Table A-1. This command is available from all three levels.

You can use multiple parameters with one SHOW command, and the CLI will display all requested values. Use the special SHOW ALL command to display the entire running configuration.

sysname Assigns a system name to this AirSwitch, which will display in the CLI prompt at all levels.

Syntax: SYSNAME <name>, where:

<name> = Name assigned to the server, as an alphanumeric string up to 16 characters. Default value is *AirSwitch*.

tar tvf Displays the list of files contained in a specified tar file, without actually untarring it.

Syntax: TAR TVF <filename>, where:

<filename> = Tar file whose contents you want to view.

tar xf Unpacks all files contained in a specified tar file. This command is used to install an upgrade of system software.

Syntax: TAR XF <filename>, where:

<filename> = Tar file whose contents you want to view.

type Displays the content of a specified text file. This is useful for reviewing backed up config files, to check contents.

Syntax: TYPE [filename], where:

[filename] = Name of the file whose content you want to display.

user add Creates a new administrative user.

Syntax: USER ADD [{telnet | oper-type}] <USERNAME> , where:

{telnet | public} = user type; oper-type have read-only access to current public port user group configurations and visiting user statistics (see"Viewing Current Visitor Groups," on page 60); telnet type have general telnet access (see "Managing Telnet Users," on page 41). Default type is telnet.

<username> = The new user you want to create. You can use up to 32 letters, numbers, symbols and spaces; do not use control characters. When you press Return, you will be prompted for a password for this user, and then prompted to retype the new password.

DCN: as1200sm-B11

user change Changes the password of an existing administrative user.

Syntax: USER CHANGE <{telnet | oper-type}> <USERNAME>, where:

{telnet | public} = Type assigned to this user. Because you can have two users with the same name but different types, you must specify oper-type if that is the one you mean. If no type is specified, the telnet is assumed.

<username> = The existing user whose password you want to change. When you press Return, you will be prompted for the old password for this user, and then prompted to type and then retype the new password. You can use up to 32 letters, numbers, symbols and spaces; do not use control characters.

user delete Deletes an existing administrative user.

Syntax: USER DELETE <{telnet | oper-type}> <USERNAME> , where:

{telnet | public} = Type assigned to this user. Because you can have two users with the same name but different types, you must specify oper-type if that is the one you mean. If no type is specified, the telnet is assumed.

<username> = The existing user you want to delete. When you press Return, you will be prompted for the old password for this user. If you provide it correctly, the user will be deleted.

Configure Commands

All commands available at the Configure level are listed below, with functional description and required syntax (if applicable). Note that in the syntax descriptions, angle brackets indicate **<**mandatory**>** parameters; square brackets indicate [optional] parameters. Where appropriate, examples are also provided.

? Displays a list of all available commands, just as the **Help** command does. This command is available from all three levels.

acl Adds a new entry to the Access Control List, which specifies the devices authorized to associate to and use the wireless network. Devices are identified by MAC address and name, and can be in either Blocked or Unblocked status.

You can also use this command to change one or more of an existing entry in the list. To do so, add the entry exactly as though it were a new entry, but with one or more different values—for instance, with a Blocked setting rather than Unblocked.

Syntax: ACL <mac-addr> [NAME <name>] [TYPE <type>] [BLOCK | UNBLOCKED], where:

<mac-addr> = MAC Address of the wireless device being added to the access list.

NAME <name> = Recognizable name of the device—for example, *JoeSmith laptop*. May be any alphanumeric string, up to 33 characters.

TYPE <type> = Recognizable description of type of device—for example, *Compaq Presario 8100*. May be any alphanumeric string, up to 33 characters.

{BLOCK | UNBLOCKED} = Sets status of this device. Blocked status allows you to temporarily block the device from associating from the network without actually removing it from the access list; unblocked means the device will associate normally.

This parameter is not required; if no value is specified, newly added entries will be Unblocked by default.

You can use also the special syntax ACL ANY UNBLOCKED to disable the ACL altogether, so that the switch will allow all devices to attach to the network without checking the access control table. Re-enable ACL checking with the command ACL ANY BLOCKED.

antenna rx Specifies the receive antenna to be used by all PAs connected to this switch.

Syntax: ANTENNA RX <AP> <value>, where:

<value> = Active receive antenna for all PAs: 1 (right), 2 (left), or 3 (diversity, i.e. both antennas)

DCN: as1200sm-B11

antenna tx

Specifies the transmit antenna to be used by all PAs connected to this switch.

Syntax: ANTENNA TX <value>, where:

<value> = Active transmit antenna for all PAs: 1 (right), 2 (left), or 3 (diversity, i.e. both antennas). Right and Left refer to the PA as viewed from the front.

beacon-interval

Sets the beacon interval for all PAs attached to this air switch.

Syntax: BEACON-INTERVAL <msec>, where:

<msec> = Value of the beacon interval, in milliseconds. Default is 100; valid range is 50-10000.

beacon-offset

Sets the beacon offset period for all PAs attached to this air switch.

Syntax = BEACON-OFFSET <msec>, where:

<msec> = Value of the beacon offset, in milliseconds. Default is 10; valid range is from 5 to 1000. **Note:** Be sure the Beacon Offset value is never set to more than 10% of your Beacon Interval value.

cca-mode

Sets the Clear Channel Assessment mode, which works in conjunction with the ED Threshold. There are three modes:

- CCA Mode 1: Energy above threshold. CCA shall report a busy medium upon detection of any energy above the ED threshold.
- CCA Mode 2: Carrier sense only. CCA shall report a busy medium only upon detection of a DSSS signal. This signal may be above or below the ED threshold.
- CCA Mode 4: Carrier sense with energy above threshold. CCA shall report a busy medium upon detection of a DSSS signal with energy above the ED threshold.

Syntax: CCA-MODE <value>, where:

<value> = The CCA mode. Default is 2; valid values are 1, 2 and 4.

channel

Sets the radio channel on which all PAs for the current switch are operating.

Syntax: CHANNEL <number>, where:

<number> = Channel number. Valid range is 1 through 11, though channels 1, 6, and 11 are least susceptible to interference from other radio sources. Default setting is 6.

clear counters

Restarts the statistical counting period for interfaces. This command is analogous to the way the RESET STATISTICS command works for the switch and PAs.

Syntax: CLEAR COUNTERS [port-list], where:

[port-list] = a specific interface you want to clear, identified by port list. If no value is specified, all interface counters will be restarted.

`cls` Clears the current terminal screen, leaving only the CLI prompt. This command is available from all three levels.

`cos bandwidth` Used to assign queue priorities for weighted round robin packet handling, in connection with class of service. For details, see "Class of Service," on page 88.

Syntax: COS BANDWIDTH <weight1 weight 2 weight 3 weight 4>, where:

<weight N> = You can set up to four weights, which represent the number of packets for one queue sent per number of packets in other queues. Valid values are 0-255; default is 255. If all four are set to zero, queues will be treated with strict priority rather than weighted round-robin.

`cos map` Used to map the four port-based queues to the eight levels of CoS packet tags. The four must be defined one at a time. For details, see "Class of Service," on page 88.

Syntax: COS MAP <queue cos-list>, where:

<queue cos-list> = Maps the specified queue (1-4) to one or more CoS levels (0-7). If mapping to more than one CoS level, expressed as a comma-delimited string.

`cos untagged` Specifies a CoS level, which will be used to treat all untagged packets as though they were tagged. For details, see "Class of Service," on page 88.

Syntax: CoS UNTAGGED <cos>, where:

<cos> = CoS level (0-7) you want to apply to all untagged packets.

`dhcp-server` Used to assign one or more pools of IP addresses that the DHCP server can assign dynamically to visiting clients using the public port. If you want to assign just one contiguous range of addresses, you need only one pool; if you want to use more than one non-contiguous range, create a pool for to each range. For details, see **REF**.

Syntax: DHCP-SERVER pool <name> <start-IPaddr> <end-IPaddr> DNS [dns-server-addr] DROUTE [default-gateway] , where:

<name> = ID for this range of IP addresses. Max length = 8 characters

<IPaddr1> = starting address of the range in this pool

<IPaddr2> = ending address of the range in this pool

DCN: as1200sm-B11

[dns-server] = IP address of your network's DNS server, if you want to use it for IP address resolution

[default-gateway] = Specifies the default gateway for all traffic to and from this range of addresses. If you define more than one pool, you should use the same default gateway address for all pools.

You can delete existing DHCP address pools with the command

```
~AirSwitch(config)~# NO DHCP-SERVER <name>
```

Note: You must reboot the system for address pool deletions to take effect. (The CLI will display awarning to this effect when you use this command.) This is true even though the deleted pool will no longer be displayed in response to the SHOW DHCP-SERVER command.

dtim Sets the value of the DTIM interval for this switch.

Syntax: DTIM <period>, where:

<period> = DTIM interval, in milliseconds. Default is 2; valid range is 1-20.

ed-threshold Sets the value for the Energy Detect Threshold. This is the level of radio transmissions detected on the wireless medium that the switch uses to decide whether the air medium is busy or available. If the current level is above this threshold, the switch considers the medium busy and tries another channel. If it is below this threshold, the switch allows PAs to transmit and receive at the assigned channel.

Syntax: ED-THRESHOLD <value>, where:

<value> = Value of the Energy Detect Threshold, expressed as a relative value from 0 to 100. Default value is 1.

group Creates a new user group for the public port feature, and moves to the Group sub-mode, where you can set parameters for this group.

Syntax: GROUP <name>, where:

<name> = The name assigned to this group.

For complete information, see **REF**.

exit Navigation command; moves user back up to the Enabled-level commands as described under "Enabled Commands," on page 98.

heartbeat Specifies the interval, in seconds, at which PAs send heartbeat notification messages to the AirSwitch. The switch expects to receive heartbeats at this interval, and when it fails to detects this three in a row, it assumes the PA has malfunctioned and will initiate restart procedure. The default value is 1.

help Displays a list of all available commands, just as the **?** command does. This command is available from all three levels.

interface Navigation command, used to go to the interface submode to configure an interface, expressed as a port list.

Syntax: INTERFACE <port-list>, where:

<port-list> = One or more physical ports you wish to configure as an interface.

For complete information, see "The Interface Submode," on page 116.

logging nvram Displays the contents of the system log in NVRAM. (For a detailed description, see "The System Log," on page 80.)

Syntax: LOGGING NVRAM { no_lines | -no_lines | ALL }, where:

[no_lines] = A positive number will display this number of entires in the system log, from the most recent entry and moving backwards.

[-no_lines] = A negative number will display this number of entries in the system log, from the oldest event and moving forward.

ALL = Displays the entire contents of system log entries currently in NVRAM.

logging save-file Writes the current contents of the system log buffer to a file in flash memory, of a specified filename.

Syntax: LOGGING SAVE-FILE <filename>, where:

<filename> = Name of the log file you want to save.

Once this file is created, you can use the COPY FTP command to upload it to a remote host.

long-retry-limit Sets the Long Retry Limit value, which determines the number of times the switch will retry sending long data frames.

Syntax: LONG-RETRY-LIMIT <value>, where:

<value> = Value of the long retry limit, in milliseconds. Default is 1.

mirror dest Specifies the destination port for port mirroring, i.e. the port where you will connect the packet analyzer. Note that you must designate a DEST port first, then your SOURCE ports.

Syntax: MIRROR DEST <dest-port-list> [both | rx | tx], where:

DCN: as1200sm-B11

<dest-port-list> = One or more mirroring destination ports, corresponding to the physical 10/100 ports on the front of the AirSwitch. Valid values are FE1-FE12. List may be expressed as comma-delimited strings (such as FE3,FE6,FE12) or a range (for example, FE2—FE6).

[both | rx | tx] = Specifies whether you want to mirror the source port's transmit packets, receive packets, or both.

To change the mirroring destination, use the NO MIRROR DEST command to un-designate any current port (port number is not required), and then the MIRROR DEST <port-no> to specify a new destination.

mirror source Specifies the source port for port mirroring, i.e. the port whose traffic you want to monitor with a packet analyzer. Note that you must designate a DEST port first, then your SOURCE ports.

Syntax: MIRROR SOURCE <source-port-list> [both | rx | tx], where:

<source-port-list> = One or more mirroring source ports, corresponding to the physical 10/100 ports on the front of the AirSwitch. Valid values are FE1-FE12. List may be expressed as comma-delimited strings (e.g. FE3,FE6,FE12) or a range, such as FE2—FE6.

[both | rx | tx] = Specifies whether you want to mirror the source port's transmit packets, receive packets, or both.

You can turn off mirroring from one or more individual source ports with the command NO MIRROR SOURCE <port-list>.

no Deletes a configuration entity, or turns off a feature, specified by the required parameter. For detailed description of this command, see "The NO Command," on page 126.

oprate Specifies all data rates supported by the switch. More than one value can be specified.

Syntax: OPRATE <value>, where:

<value> = Operational data rate, in Mbps. Default is 2; valid values are 1, 2, 5.5, and 11.

pa Used to change various parameters of PAs that were autodetected by the switch, or to assign all values if defining PAs manually. You cannot use this command to change the operational state of PAs; that can be done only from the Enabled level.

Syntax: PA <name> [name <newname>] [BOOT <file-name>] [LOCATION <location>] [MAC <mac-addr>] [MODE <value>], where:

<newname> = New name you wish to assign to the specified PA. Names are automatically assigned during bootup, based on MAC addresses; but you can replace these default names with something more descriptive and helpful. You can use an alphanumeric string up to 16 characters.

<file-name> = name of the firmware image you want the specified PA to load when it restarts. This feature is useful when upgrading or back-revving firmware versions.

<location> = Like the name, this is a default value that you can manually replace with a description of the physical location of this PA.

<mac-addr> = Allows you to manually preconfigure a PA, before the physical unit is actually plugged in. Normally, though, the contents of this field will be autodetected by the AirSwitch.

MODE <value> = Allows you to change the mode of the PA: Active, Standby, or Disabled.

For more details on changing these parameters, see "Managing Packet Antennas," on page 48.

preamble-short Turns on short-preamble mode, for traffic at 2 Mbps or faster. The preamble is a required bitstring in 802.11 packet headers, used for synchronization. Data traveling at 1 Mbps must use only long-preamble format; faster traffic may be set to use short-preamble format. By default this is disabled; normally you should not enable it unless instructed to do so by Airflow Tech Support.

Syntax: PREAMBLE-SHORT

To take the system back out of short-preamble mode once enabled, use the command

```
no preamble-short
```

short-retry-limit Sets the Short Retry Limit value, which is the number of times the switch will retry sending short data frames.

Syntax: SHORT-RETRY-LIMIT <value>, where:

<value> = Value of the short retry limit, in milliseconds. Default is 7.

show Displays the current value of various settings for this switch; these Show Parameters are listed in Table A-1. This command is available from all three levels.

You can use multiple parameters with one Show command, and the CLI will display all requested values. Use the special SHOW ALL command to display the entire running configuration.

DCN: as1200sm-B11

ssid Creates a Service Set Identifier, or SSID, for this switch. SSIDs may be thought of as virtual WLANs: they provide a useful way of segmenting your wireless LAN in much the same way VLANs segment a wired LAN. In fact, multiple SSIDs are implemented based on mapping to already created VLANs in your AirSwitch, since each SSID is associated with a VLAN when it is created. In other works, in effect they are just extensions of standard wired VLANs out into the wireless network. When clients connect to the network, they connect to a particular SSID and its component network resources, and are excluded from network resources belonging to other SSIDs.

Once you create an SSID here, it is available for wireless clients to request an association. You can set one SSID to broadcast so that it is visible to wireless clients (using the Advertise flag); for all others, clients must know the SSID and specifically request an association with it. If you try to advertise an more than one SSID, the switch will prompt you with an error message.

Syntax: SSID <ssid> VLAN <vlanid> <corporate|public> [advertise], where:

<ssid> = SSID, as an alphanumeric string up to 33 characters.

<vlanid> = ID of the VLAN that maps to this SSID.

<corporate|public> = designates this SSID as either public (i.e. assigned to the public port), or corporate (all other SSIDs).

[advertise] = a flag that, when set, will broadcast the SSID to wirelsss clients requesting association to the network. If this flag is not set, wireless users will need to know the SSID they want to associate with, which provides a security feature.

Example: If you need to create a new internal SSID called *engineering*, mapped to VLAN 3080, that will be advertised to clients, type following command line:

```
ssid engineering vlan 3080 corporate advertise
```

To delete an existing SSID, use the `NO SSID <ID>` command. You must have at least one SSID defined on the switch; if you try to delete the last SSID, the switch will return an error message.

station-timeout Sets a timeout limit for inactivity of wireless clients connected to the WLAN. When the switch stops detecting packets from a client, it starts this timer running, and when the limit is reached. the switch assumes the client has left the network and removes it from the Active Station List. (The inactivity counter is displayed for each active client, as the Inactivity column in the ASL.)

Syntax: STATION-TIMEOUT <limit>, where:

<limit> = Timeout limit, in seconds. Default value is 1000, or 16 minutes and 40 seconds.

storm-control Enables the packet storm control feature, and sets a storm control level. (This feature is disabled with the NO STORM-CONTROL command.)

Syntax: STORM-CONTROL <level>, where:

<level> = Level of storm control, as a percentage of each port's available bandwidth.

For details on this feature, see "Packet Storm Control," on page 90.

stp age Sets the duration of the STP aging time for the entire switch.

Syntax: STP AGE <age-time>, where:

<age-time> = Maximum aging time, in seconds, as an integer from 6 - 40. Default value is 20.

stp forward Sets the duration of the STP forward delay timer for the entire switch.

Syntax: STP FORWARD <fwd-time>, where:

<fwd-time> = Forward delay timer value in seconds, as an integer from 4 - 30. Default value is 15.

stp hello Sets the STP hello time for the entire switch.

Syntax: STP HELLO <hello-time>, where:

<hello-time> = Hello-time value in seconds, as an integer from 1 - 10. Default value is 2.

stp mode Enables STP, if currently disabled. To disable STP, use the command

```
no stp mode
```

stp priority Assigns the STP priority of the entire switch.

Syntax: STP PRIORITY <priority>, where:

<priority> = Priority value of the switch, as an integer from 0 - 65535; lower value represents higher priority

sysname Assigns a system name to this AirSwitch, which will display in the CLI prompt at all levels.

Syntax: SYSNAME <name>, where:

<name> = Name assigned to the server, as an alphanumeric string up to ??? characters. Default value is *AirServer*.

tx-power-level Sets the global transmit power level of all PAs currently attached to this switch.

DCN: as1200sm-B11

Syntax: TX-POWER-LEVEL <value>, where:

<value> = Transmit power level, as a relative value from minimum to maximum. Valid range is 0 to 100; default is 100, i.e. maximum power.

`vlan` Navigation command to move to VLAN submode, where you can create new VLANs or changes one or more parameters in an existing VLAN, as described under "VLANs," on page 83.

Syntax: VLAN <vlanid> where:

<vlanid> = ID, as a numeric string up to 4 characters.

For details on the VLAN submode, see "The VLAN Submode," on page 120.

`wep key` Lets you define up to four secret keys, used for WEP encryption of packets between the switch and clients. These settings will only be used if WEP Mode is Enabled.

Syntax: WEP KEY <key-no> SIZE <size> <key> [TRANSMIT-KEY], where:

<key-no> = The number of the key being defined, from 1 to 4;

<size> = Designates the size of this key, in bits. Valid values are 40 and 128.

<key> = The actual key, as a hexadecimal string, either 10 or 26 hex digits (depending on the size parameter);

<TRANSMIT-KEY> = Marks this key as the transmit key. Should be set only for one of the defined keys at a time.

For details, see "WEP Keys," on page 37

`wep mode` Enables WEP encryption for all clients connected to the server, with the specified authentication type—either Open System or Shared Key. Authentication type is set only when encryption is enabled; that is, there can be no client authentication without setting the system to WEP MODE.

Syntax: WEP MODE <open|shared>, where:

<open|shared> = Authentication mode. This is a mandatory parameter.

To disable WEP encryption and authentication, use the command

```
no wep mode
```

For details, see "WEP Encryption," on page 38.

Submode Commands

Submodes may be thought of as a sub-level below Configure, used either for defining individual entities rather than global configuration settings, or for other specialized configuration features. For example, some Interface-related configuration parameters are global for all interfaces, and so can be set from the configure level like any other commands; but others are specific to individual interfaces, and so to configure these you must enter the submode for the individual interface. When you are finished with changes, you use the END command to navigate back up to the Configure level.

The current version of the AirSwitch 1200 has the following submodes:

- The Group Submode
- The Interface Submode (page 116)
- The Public Submode (page 118)
- The System Submode (page 119)
- The VLAN Submode (page 120)

The Group Submode

The Group submode is another lower branch of the Configure CLI level, used for creating and configuring visitor groups with access to the public port. You navigate to the group submode by going to the Configure level and typing the command **GROUP <name>**, where:

<name> = The name of the group you are defining or changing, as an alphanumeric string up to 18 characters. If a specified name does not already exist, a new group is created. If it does already exist, it will be redefined with any changed parameters.

The Group submode also has a special command line, to help with navigation:

```
~AirSwitch (config-group)#~
```

This submode has the following commands, specific to the selected group:

`access start`

Sets the time when this group's access to the public port will begin. Time is expressed as 24-hr format, referring to the current day. If the start time specified has already passed, access will begin at that time on the following day.

Syntax: ACCESS START {<hh:mm> | now}, where:

<hh:mm> = Start time, as hours and minutes of current day, in 24-hr format. Default value is 06:00.

now = Group access begins as soon as current configuration settings are saved.

DCN: as1200sm-B11

access duration Sets the duration of this group's access to the public port. Access begins at the time specified by ACCESS START, and lasts for the number of hours specified here.

Syntax: ACCESS DURATION <value>, where:

<value> = Number of hours this group will have public port access, starting from the ACCESS START time, as a positive integer from 1 to 24; default is 24.

access renewal Controls whether, and how many times, the access configured for this group will be automatically renewed after it expires. Default setting is daily.

Syntax: ACCESS RENEWAL {none | daily | <value>}, where:

none = Access will not be renewed.

daily = Access will be renewed every day, indefinitely.

<value> = Number of times access will be renewed once it expires, as a positive integer from 1 to 30. This is not the total number of days, but the number of renewals; thus an ACCESS RENEWAL 4 setting will give a group public port access for five days, during the hours defined by the ACCESS START and ACCESS DURATION parameters.

max-users Specifies the maximum number of visitors that can connect to the public port as members of this group.

Syntax: MAX-USERS <value>, where:

<value> = Positive integer, from 1 to 1024; default is 5.

password Assigns a specific login password for this group, or specifies that the AirSwitch generate a random string as a password.

Syntax: PASSWORD {<permanent-password>|auto}, where:

<permanent-password> = Password all members of this group will use to log in to the public port, as an alphanumeric string of up to 12 characters. If you define your own password, it will not change if the group access is renewed.

auto = The AirSwitch will generate a random string as password, of a length specified by the PASSWORD LENGTH parameter. Auto-generated ones will be regenerated upon group renewal. For example, if you specify PASSWORD AUTO and ACCESS RENEWAL DAILY, the AirSwitch will renew the group's access and generate a new random password every day, at the ACCESS START time.

password length Sets the maximum length of the login password for this group, if they are auto-generated. If password is permanent, this parameter is not used and need not be set.

Syntax: PASSWORD LENGTH <length>, where:

<length> = Positive integer, from 1 to 12; default is 4.

DCN: as1200sm-B11

show Displays the current settings of this group. For details, see REF.

Syntax: SHOW <name>, where:

<name> = Group name, as an alphanumeric string up to 18 characters.

The Interface Submode

The Interface submode is a lower branch of the Configure CLI level, used for configuring individual interfaces. You navigate to the interface submode by going to the configure level and typing the command **INTERFACE <port-list>**, where:

<port-list> = One or more physical ports: FE1-FE12, GE1, GE2, SVC, or PUB. If the list contains more than one port, it may be expressed as a comma-delineated string (such as FE3,FE6,FE12) or a range (such as FE2—FE6).

It has a special command line, to help with navigation:

```
~AirSwitch (config-if)#~
```

The submode has the following commands, which apply to the specified interface as defined by port list.

access mode Used with the PUB interface only: enables the switch's public port feature, for all groups. (For details on the public port, see "Using the Public Port," on page 58.) To disable this feature, use the command NO ACCESS MODE, also at the PUB interface submode only:

```
~AirSwitch (config)#~ interface pub
~AirSwitch (config-if)#~ no access mode
```

You can configure all other public port-related options at any time, regardless of whether the public port is in access mode or not. For details, see "Configuring the Public Port," on page 61.

duplex Sets the duplex mode for this interface, either Full or Half. Default is Half.

Syntax: DUPLEX <full | half>

end Navigation command, exits Interface submode and moves back up to the global Configure level.

exit Navigation command, exits the Interface submode and moves back up to the global Configure level.

ip addr Assigns an IP address to this interface, for management purposes. This is the address you will use to set up a telnet connection to the CLI. Generally you set this for the SVC port during your initial configuration dialog. If you ever need to change it after

that, or to assign an address to the GE ports, you will have to reboot the AirSwitch for the new address to take effect.

In the current version of the AirSwitch, when you assign an address to either GE port, it will also apply to the other GE port and all FE ports as well, since all are connected through the internal switching fabric. Thus in practice there are two possible IP addresses: the SVC port alone, and the GE1-GE2-FE1/12 combined.

Bear in mind that ports do not need an IP address for connection to AirHubs; the only reason for an IP address is as a management interface.

Syntax: IP ADDRESS <address> <subnet mask>, where:

<address> = New IP Address you want to assign to this interface, in standard dot-delimited format.

<subnet mask> = Subnet mask of the management IP address.

show Displays the current settings for this interface.

shutdown Changes the administrative state of this interface to Down, i.e. blocks the link on this interface. This command has no parameters.

Syntax: SHUTDOWN

Revesed with the NO SHUTDOWN command.

no shutdown Changes the administrative state of this interface to Up if already blocked, i.e. unblocks the link on this interface. This command has no parameters.

Syntax: NO SHUTDOWN

speed Sets the speed for data transfer over this interface. Available only for FE and GE ports; differs for the two types. Default is the highest available speed.

Syntax (FE ports): SPEED <10 | 100>

Syntax (GE ports): SPEED <10 | 100 | 1000>

stp cost Assigns an STP cost value to the specified interval. For details on STP costs, see "Configuring STP," on page 87.

Syntax: STP COST <value>, where:

<value> = The STP cost value assigned to this individual interface.

stp port-priority Assigns an STP port priority value to the specified interval. For details on STP port priorities, see "Configuring STP," on page 87.

Syntax: STP PORT-PRIORITY <value>, where:

<value> = The STP port priority value assigned to this individual interface.

no stp Resets the STP Cost and STP Priority settings for this interface back to factory default values. Default Cost settings: FE ports 19, GE ports 4.; default Priority settings: FE ports 128, GE ports 64. This command has no parameters.

Syntax: NO STP

vlan Associates this interface with a specified VLAN. A VLAN must have been previously defined with the **VLAN <ID>** command before it can be associated with an interface.

Syntax: VLAN <ID>, where:

<ID> = ID of the existing VLAN you want to associate with this interface.

no vlan Clears any VLAN association previously defined for this interface, and resets the association to the default value VLAN 1. This parameter has no parameters.

Syntax: NO VLAN

The Public Submode

The Public submode is unusual in that it is entered from the Main rather than the Configure level, and is password protected. (This username and password are set with the USER NEW command; see page 102.)This submode is used only for viewing the curerntly configured public port visitor groups, and statistics on public port usage. All settings here can only be displayed, not changed.

Access to this submode is controlled by a different password than access to the Enabled level; thus you can tightly restrict access to sensitive public port configuration information, while allowing employees who are not authorized to change any Enabled- or Configure-level settings (for example, a receptionist who distributes usernames and passwords to visitors) to view it.

You navigate to the Public submode with the command PUBLIC, followed by a valid username and password. Note that this submode also has a special command line, to help with navigation.

```
~AirSwitch-> PUBLIC
Username:
Password:
Retype password:
~AirSwitch-public->
```

show group Displays summary of the currently defined groups, including name, password, start time, and access duration.

DCN: as1200sm-B11

Syntax: SHOW GROUP [name], where:

[name] = the group you want to display. In this parameter is not specified, information on all currently defined groups will be displayed.

end Navigation command, moves user out of Public submode back up to Main CLI level.

The System Submode

The System submode is a lower branch of the Configure CLI level, used for configuring a special set of system-level properties. You navigate to the interface submode by going to the configure level and typing the command **SYSTEM.** You use the EXIT or END commands to return to the global Configuration level.

The following commands are available in the System submode.

bootflash lock Locks the bootflash chip so it cannot be accidentally erased and updated. Bootflash is locked by factory default; you need this command only if you have already used the UNLOCK command.

As a security precaution, this command cannot be used through a telnet connection, but is only available from a locally connected console.

Syntax: BOOTFLASH LOCK

bootflash update Loads a specified file into bootflash memory. Should only be used if specifically requested to do so by an AirFlow tech support representative.

As a security precaution, this command cannot be used through a telnet connection, but is only available from a locally connected console.

Syntax: BOOTFLASH UPDATE <filename>, where:

<filename> = the bootflash file you wish to load.

To use this command, you must first unlock your bootflash with the BOOTFLASH UNLOCK command. If you try to upgdate with bootflash still locked, you will see the following error message:

```
Cannot erase bootflash device, please try again!
```

bootflash unlock Unlocks the bootflash chip so all files can be erased and updated. You need to do this before you can use the BOOTFLASH UPDATE command.

As a security precaution, this command cannot be used through a telnet connection, but is only available from a locally connected console.

Syntax: BOOTFLASH UNLOCK

dir Displays names of all files currently in the system file directory, which is helpful in determining your current bootrom version. The bootrom file will be the only one with the .hex extension, and the file name reflects the version number—for example, `bootrom-1-0-2-9.hex`.

end Navigation command, exits the System submode and moves back up to the global Configure level.

exit Navigation command, exits the System submode and moves back up to the global Configure level.

server mode Places the AirSwitch into server mode, which means it can be used in a server-type topology, with ATP packets passing in both directions through the Gb port. This is a non-standard mode; details are available in the *AirSwitch 1200 Application Note 1: Basic Deployment Types*.

You can take the AirSwitch out of server mode—that is, back to standard switch mode—with the command `no server mode`.

show Displays current system submode settings. Currently this includes the server mode (on or off) and the sysvlan mode (single or multi).

sysvlan Allows you to collapse the six internal VLANs into a single VLAN, or to restore them if they have been collapsed. For details, see "Collapsing Internal VLANs," on page 84.

Syntax: SYSVLAN <{single | multi}>, where:

single = The VLANs will be collapsed into one, which will always be the AirSwitch-PA type.

multiple = Your system will have the six default internal VLANs.

The VLAN Submode

The VLAN submode is used for creating and configuring individual VLANs. You navigate to the VLAN submode from the Configure level, with the command **VLAN <ID>**, where:

<ID> = The ID of the VLAN you are defining or changing, expressed as an integer up to four digits. (Note that the six internal VLAN IDs, 3072 through 3077, are reserved.) If a specified ID does not already exist, a new VLAN is created. If it does already exist, it will be redefined with any changed parameters.

It also has a special command line, to help with navigation:

```
~AirSwitch (config-vlan)#~
```

This submode has the following commands, specific to the specified VLAN:

DCN: as1200sm-B11

name Assigns a name to this VLAN.

Syntax: NAME <name>, where:

<name> = VLAN name, as an alphanumeric string up to 18 characters.

no vlan Deletes the specified VLAN. Although you can change an existing VLAN name, there is no such thing as changing VLAN IDs; rather, you must delete an existing one and create a new one with the specified ID. This command has no parameters.

Syntax: NO VLAN

Note that you can also delete an existing VLAN from the global Configure level, by specifying the ID:

```
~AirSwitch (config-vlan)~# no vlan <id>
```

show Displays the current settings for this VLAN. Returns the same result as the following command from the global Configure level:

```
~AirSwitch (config-vlan)~# show vlan <id>
```

type Specifies a type for this VLAN.

Syntax: VLAN type <type>, where:

<type> = VLAN type. Valid types are `SW-SW, SC-SC, SW-SC, SW-SC-DATA, UNSECURED, DESKTOP, Port-Based, and PUB`. All user-defined VLANs must be defined as type = Port-Based, or PUB (if for the public port); the other types are reserved for internal VLANs and should not be used.

end Navigation command, exits the VLAN submode and moves back up to the global Configure level.

exit Navigation command, exits the VLAN submode and moves back up to the global Configure level.

The SHOW Command

The SHOW command displays the current value of various settings for this switch. This command is available from all three levels, as well as from all submodes. Bear in mind that the information it returns is highly dependent on the level where it is used.

Syntax = SHOW <parameter>, used with the available parameters described below in Table A-1. Note that some of the parameters themselves have optional parameters.

Table A-1: SHOW Command Parameters

SHOW Parameter	Function

ACL	Shows the current Access Control List (see "The Access Control List," on page 33). Sample output of this command:
	`~AirSwitch~(config)# show acl`
	`ACL : ENABLE`
	
	`MAC-ADDR NAME TYPE STATE`
	`00:30:BD:D0:57:2D Belkin FAxxxx UNBLOCKED`
	`00:0A:F4:9C:4D:05 Cisco PCM350 UNBLOCKED`
	`00:04:E2:46:AA:7B SMC 2632Wv2 UNBLOCKED`

ALL	Shows all parameters of running configuration.

ANTENNA RX	Shows Rx antenna for specified AP. Sample output:
	`~AirSwitch~(config)# show an r`
	`ANTENNA RX: 3`

ANTENNA TX	Shows which antenna is being used for transmit, for all PAs. Valid values are 1 (right antenna), 2 (left antenna), or 3 (both antennas). Sample output:
	`~AirSwitch~(config)# show an t`
	`ANTENNA TX: 3`

ASL	Shows the shorter version of the Active Station List (see "Viewing the ASL," on page 71). Sample output:
	`~AirSwitch~(config)# show asl`
	`ASL:`
	`MAC Address IP Address State Scout Name`
	`00:0B:FD:9A:C1:2B 10.109.11.118 ASSOCIATED 2 hbims`
	`00:0C:85:64:2E:5F 10.109.11.113 ASSOCIATED 2 bmachlin`

ASL DETAIL	Shows the more technically detailed version of the Active Station List. For sample output, see "Monitoring Client Connections," on page 71).

BEACON-INTERVAL	Shows current beacon interval, in ms.:
	`~AirSwitch~(config)# show beacon-i`
	`BEACON-INTERVAL : 100`

BEACON-OFFSET	Shows current beacon offset value, in ms.:
	`~AirSwitch~(config)# show beacon-o`
	`BEACON-OFFSET : 7`

BSSID	Displays the basic service set ID, or BSSID, of this switch. The BSSID is one of the MAC addresses of the switch, derived from the base MAC address by adding 3. It is a read-only value, factory defined.
	`~AirSwitch~(config)# show bss`
	`BSSID : 00:ab:1c:ab:1c:00`

CCA-MODE	Shows Clear Channel Assessment mode currently in use:
	`~AirSwitch~(config)# show cca`
	`CCA-MODE : 4`

DCN: as1200sm-B11

Table A-1: SHOW Command Parameters (Continued)

SHOW Parameter	Function

CHANNEL	Shows channel currently in use:
	`~AirSwitch~(config)# show ch`
	`CHANNEL : 11`

CLOCK	Shows current AirSwitch system time, in <day><hh:mm:ss> <month> <dd> <yyyy> format. Sample output:
	`~AirSwitch~# show clock`
	`CLOCK : Friday 12:52:03 June 13, 2003`

COS	Displays current CoS settings. Sample output from this command:
	`~AirSwitch~# show cos`
	`Untagged CoS: 7`
	`Priority: weighted round robin`
	`Queue CoS Bandwidth`
	`1 0,1,3 50`
	`2 3,4,5 100`
	`3 6 150`
	`4 7 250`

DHCP-SERVER	Shows Delivery Traffic Identification Message period. Sample output: `~AirSwitch~(config)# show dhc` **`GET ACTUAL SAMPLE FOR THIS!!!`**

DTIM	Shows Delivery Traffic Identification Message period. Sample output:
	`~AirSwitch~(config)# show dt`
	`DTIM : 2`

ED-THRESHOLD	Shows current energy detect threshold:
	`~AirSwitch~# show ed`
	`ED-THRESHOLD : 31`

FILE	Displays names of all files currently in AirSwitch flash memory. (Identical to the DIR command.)
	`~AFNworks~# show fi`
	`Listing Directory /flash/:`
	`-rwxrwxrwx 1 0 0 849 Jun 16 12:25 config.txt`
	`-rwxrwxrwx 1 0 0 2616893 May 4 21:31 vxWorks`
	`drwxrwxrwx 1 0 0 1024 May 4 21:06 html/`
	`-rwxrwxrwx 1 0 0 178340 May 4 21:20 PA240.bin`
	`-rwxrwxrwx 1 0 0 140 May 4 21:25 env_var`
	`-rwxrwxrwx 1 0 0 1089 May 4 21:40 pa_config.txt`
	`-rwxrwxrwx 1 0 0 1680 Jun 16 12:25 accessListConfig`

GROUP [ID]	Shows the name, password, start time and access duration for the specified public port group. If no ID is specified, displays a summary of all groups currently defined: `~AirSwitch(config)~# show group` **`GET ACTUAL SAMPLE FOR THIS!!!`** This command is available from the Public submode, as well as from Enabled and Config levels. For details, see REF.
GROUP [ID] USER [DETAILS]	Shows statistical public port usage information on all individual members of the specified public port group, identified by e-mail address. If no ID is specified, displays a summary of all members of all groups currently defined. The : `~AirSwitch(config)~# show group` **`GET ACTUAL SAMPLE FOR THIS!!!`** This command is available from the Public submode, as well as from Enabled and Config levels. For details, see REF.

HEARTBEAT	Shows the current heartbeat notification threshold:
	`~AirSwitch~# show heart`
	`HEARTBEAT : 1`

Table A-1: SHOW Command Parameters (Continued)

SHOW Parameter	Function
INTERFACE [ID]	Shows detailed information on the specified AirSwitch port or ports. If no ID is specified, displays summary information for all ports. (For sample output, see see Figure 8-3 on page 79.)

IP	Displays the static IP address currently assigned to the switch.
	`~AirSwitch~# show ip`
	`ip address 10.122.108.67`

LOGGING	Shows current logging levels for all software tasks; used for internal debugging purposes.

LONG-RETRY-LIMIT	Shows current long retry limit setting:
	`~AirSwitch~# show long`
	`LONG-RETRY-LIMIT: 4`

MIRROR	Displays current Port Mirroring settings:
	`~AirSwitch~# show mir`
	`Rx mirroring ports:  5`
	`Tx mirroring ports:  1,3,5`
	`Destination Port:  22`

OPRATE	Shows current operational rate of the switch:
	`~AirSwitch~# show opr`
	`OPRATE  : 11 Mbps`

PA [NAME]	With the optional [NAME] parameter, displays information for one specific PA. Used without the [NAME] parameter, shows information on all currently detected PAs. (For sample output, see "Viewing Packet Antenna Information," on page 73.)
RUNNING-CONFIG	Displays all configuration settings currently in effect. (For sample output, see "Viewing the Entire Configuration," on page 77.)

SHORT-RETRY-LIMIT	Shows short retry limit. Sample output:
	`~AirSwitch~# show short`
	`SHORT-RETRY-LIMIT: 7`

SSID	Shows definition of all currently defined Service Set IDs. Sample output:
	`SSID SystemTest4 CORPORATE VLAN 0 ADVERTISE`
	`SSID guest PUBLIC VLAN 0`

STORM-CONTROL	Displays the currently configured storm control settings. Sample output: `Storm-control level: 5%`

STP	Displays the currently configured STP settings. Sample output:
	`~AirSwitch~(config)# show stp`
	`Spanning Tree Display`
	`STP Mode:  OFF`
	`Switch Priority:  32768`
	`Hello Interval:  2 seconds`
	`Max. Aging Time:  20 seconds`
	`Forward Delay:  15 seconds`

DCN: as1200sm-B11

Table A-1: SHOW Command Parameters (Continued)

SHOW Parameter	Function

SWITCH	Shows the current operational statistics of the switch, as described below (see "Viewing Switch Information," on page 76). Sample output:
	`~AirSwitch~> sho sw`
	`SW Version : 1.32`
	`Bootrom version : 1.0.2.9`
	`IP ADDRESS : 15.123.150.101 255.255.255.0`
	`Beacons sent : 440466`
	`Auth requests : 46`
	`Auth rejected : 0`
	`Assoc requests : 15`
	`Assoc rejected : 0`
	`WEP Undecrypted : 0`
	`WEP ICV Error : 0`
	`WEP Excluded : 0`
	`Up time : 0 days, 2 hours, 1 minutes, 25 seconds`
	`Model Number : AirSwitch 1200`
	`MAC Address : 00:0b:c8:80:00:c0`
	`Part Number : 550-11002-01`
	`Serial Number : 1232455`
	`DataCode : 06132003`

SYSVLAN	In the System submode, displays current status of internal VLANs, either Single (i.e. collapsed) or Multi (not collapsed).
TECH-SUPPORT	Generates a detailed diagnostic log of recent switch events, providing a valuable troubleshooting tool for technical support engineers (see "Trouble shooting," on page 56).

TX-POWER-LEVEL	Shows transmit power level set for all PAs currently operating with this switch, expressed as a percentage of full power. Sample output:
	`~AirSwitch~# show tx`
	`TX-POWER-LEVEL : 100 %`

VLAN	Shows current parameters for all VLANs defined on this switch (see "Viewing VLANs," on page 83). Sample output:
	`VLAN 3072 NAME AFN-Reserved TYPE AFN-RSVD`
	`VLAN 3073 NAME AFN-Reserved2 TYPE AFN-RSVD2`
	`VLAN 3074 NAME AFN-Reserved3 TYPE AFN-RSVD3`
	`VLAN 3075 NAME AFN-Reserved4 TYPE AFN-RSVD4`
	`VLAN 3076 NAME AFN-Reserved5 TYPE AFN-RSVD5`
	`VLAN 3077 NAME AFN-Reserved6 TYPE AFN-RSVD6`

WEP	Shows current WEP encryption and authentication settings (see "About WEP," on page 37). WEP mode = Shared means encryption is enabled and authentication is set to Shared Key type; WEP mode = Open means encryption is enabled and authentication is set to Open System type (i.e., no authentication); and WEP mode = Disabled means encryption and authentication are is disabled.
	Sample output:
	`~AirSwitch~# show we`
	`WEP MODE :DISABLED`
	`DEFAULT KEY ID :1`
	`WEP AUTHENTICATION :SHARED KEY`
	`DEFAULT KEY 1 TYPE :WEP 128 (KEY SET)`
	`DEFAULT KEY 2 TYPE :WEP 40 (KEY NOT SET)`
	`DEFAULT KEY 3 TYPE :WEP 40 (KEY NOT SET)`
	`DEFAULT KEY 4 TYPE :WEP 40 (KEY NOT SET)`

The NO Command

The NO command is used to delete configuration entities, turn off various features, or reset the configuration of specified features in certain ways. Bear in mind that the No commands are generally specific to CLI levels, and many are available only in certain submodes.

All available uses of the NO command are described below in Table A-2.

Table A-2: NO Commands

NO Commands	Function
NO ACCESS MODE	Disables the public port feature, for all defined groups. For details, see "Using the Public Port," on page 58.
NO ACL <MAC ADDRESS>	Removes an entry, specified by MAC address, from the Access Control List. For details, see "Managing the ACL," on page 33.
NO COS BANDWIDTH	Removes any defined weighted round robin CoS queue priority, and resets to the default strict priority. For details, see "Configuring CoS," on page 88.
NO DHCP-SERVER POOL <name>	Deletes the specified DHCP IP address pool. Note that this change will not take effect until you reboot the system. This is true even though the deleted pool will no longer be displayed in response to the SHOW DHCP-SERVER command.
NO LOGGING CONSOLE	Stops sending event log to the console. For details on logging features, see "The System Log," on page 80.
NO MGMT-VLAN	Removes the management interface from whatever management VLAN it had belonged to. This command does not delete the VLAN itself, but only removes the interface from it.
NO MIRROR DEST	Disables port mirroring to any ports currently set as destination. For details, see "Configuring Port Mirroring," on page 89.
NO MIRROR SOURCE <source-port-list>	Disables port mirroring from one or more specified source interfaces. For details, see "Configuring Port Mirroring," on page 89.
NO SERVER MODE	From System submode: takes the AirSwitch out of server mode, and places it back into stardard switch mode.
NO STORM-CONTROL	Disables storm control, if already enabled. This is the same as setting the level to 0%. For details, see "Configuring Storm Control," on page 90.
NO STP	From Interface submode only: resets STP Cost and STP Priority settings back to default values, for the specified interface.
NO SHUTDOWN	From Interface submode: places the interface back in Up administrative state—i.e., unblocks the port or ports if they had been blocked. For details, see "no shutdown," on page 117.
NO STP MODE	Disables STP for all interfaces, if already enabled. For details, see "Configuring STP," on page 87.

DCN: as1200sm-B11

Table A-2: NO Commands

NO Commands	Function
NO VLAN <ID>	From global configure level: Deletes the VLAN specified by the ID parameter. From VLAN submode: same result, but the [ID] parameter is not needed. From Interface submode: removes the association between the specified interface and this VLAN. For details, see "The VLAN Submode," on page 120.
NO WEP	Turns off WEP encryption and authentication for all devices attached to the switch. Works only if WEP is enabled.For details, see "About WEP," on page 37.

DCN: as1200sm-B11

A. How Do I . . .?

This Appendix offers a quick reference to a wide variety of tasks administrators may need to perform in managing the AirFlow network, and the CLI commands for those tasks. We provide the full commands here, but remember that you can use abbreviated shortcuts for nearly all commands.

The tasks are grouped in the following tables:

The expressions `@enable`, `@config`, and `@submode <name>` indicate that the command is only available from the Enabled, Configure, or Submode levels, respectively. Otherwise, the command is available from any level.

As usual, angle brackets indicate <required parameters>, while square brackets indicate [optional parameters].

For your convenience, each command is accompanied by a cross-reference to a detailed explanation elsewhere in this manual. For descriptions of all CLI commands, organized alphabetically, refer to Appendix A, "CLI Reference".

Table A-1: Navigate the CLI

How Do I Navigate from . . .	Use This Command:
Main level down to enabled level?	`enable (page 97)`
Enabled level down to configure level?	`configure terminal (page 98)`
Configure level down to a submode?	`<submode> [entity-id] (page 114)`
a submode up to global configure level?	`exit OR end (page 94)`
Configure level up to enabled level?	`exit (page 107)`
Enabled level up to main level?	`exit OR disable (page 100)`

Table A-2: Display Current Status

How do I display my current . . .	Use This Command:
switch software version?	show switch (page 76)
switch hardware part number?	show switch (page 76)
packet antenna software version?	show pa <ID> (Table A-1 on page 122)
bootrom version?	show switch OR dir (page 69)
switch IP address?	show switch (page 76)
system time?	show clock (Table A-1 on page 122)
WEP configuration?	show wep (page 122)
STP configuration?	show stp (page 87)
defined VLANs?	show vlan (page 83)
defined interfaces?	show interface (page 78)
access control list?	show acl (page 36)
event log?	logging console enabled (page 80)
associated wireless clients?	show asl (page 71)
names of backup config files?	@enable: dir (page 100)
packet antennas connected to this switch?	show pa (page 73)
all settings of all config parameters?	show all (page 77)

Table A-3: Display Cumulative Statistics

How do I display cumulative . . .	Use This Command:
beacons sent from all PAs?	show switch (page 76)
authentication requests received by switch?	show switch (page 76)
authentication requests rejected by switch?	show switch (page 76)
association requests received by switch?	show switch (page 76)
association requests rejected by switch?	show switch (page 76)
uptime of switch?	show switch (page 76)
uptime of PAs?	show pa [ID] (page 73)
undecrypted WEP packets?	show switch (page 76)
WEP ICV errors?	show switch (page 76)
PA performance statistics?	show pa [ID] (page 73)
switch performance statistics?	show switch (page 76)
individual port statistics?	@configure: show interface [port-list](page 78)

DCN: as1200sm-B11

Table A-4: Change and Redefine

How do I change the . . .	Use This Command:
IP address of a port?	@interface: ip addr <new address> (page 116)
system time and date?	@enable: clock set <hh:mm:ss> <month> <dd> <yyyy> (page 98)
name of a backup config file?	@enable: rename <oldname> <newname> (page 101)
heartbeat interval?	@config: heartbeat <interval> (page 107)
transmit power level?	@config: tx-power-level <level> (page 112)
transmit antenna?	@config: antenna tx <1 | 2 | 3> (page 105)
telnet password?	@enable: user change (page 103)
mode of a file to read-only?	@enable: chmod rd <filename> (page 98)
mode of a file to read/write?	@enable: chmod rw <filename> (page 98)
VLAN assigned to an SSID?	@config: SSID <name> VLAN <newID>(page 46)
speed of an Ethernet port?	@interface: SPEED <value> (page 117)
duplex mode of an Ethernet port?	@config: SSID <name> VLAN <newID>(page 116)

Table A-5: Create and Delete

How do I . . .	Use This Command:
create an error log for Tech Support?	show tech (page 56)
create a new telnet user?	@config: user add <username> (page 41)
delete an existing telnet user?	@config: user delete <username> (page 43)
create a new entry in the ACL?	@config: acl <mac-addr> [name <name>] [type <type>] (page 34)
delete an entry from the ACL?	@config: no acl name <name> (page 104)
create a new VLAN?	@config: vlan <ID> type port-based <name> (page 85)
delete an existing VLAN?	@config: no vlan <ID> (page 85)
create a new SSID?	@config: ssid <newID> VLAN <vlanID> (page 44)
delete an SSID?	@config: no ssid <ID> (page 44)

Table A-6: Do General Functions

How do I . . .	Use This Command:
reboot the switch?	@enable: reboot (page 101)
save the current configuration?	@enable: save [filename] (page 101)
load a different configuration?	@enable: load <filename> (page 100)
unlock my bootflash?	@system submode: bootflash unlock (page 69)
upgrade my bootflash?	@system submode: bootflash upgrade (page 69)
temporarily block a wireless client's access to the network?	@config: acl name <name> blocked (page 34)

Table A-6: Do General Functions

How do I . . .	Use This Command:
restore temporarily blocked wireless client?	`@config: acl name <name> unblocked` (page 34)
disassociate a wireless client from the network (that is, force it to reassociate)?	`@config: disassociate <mac-addr>` (page 51)
deauthenticate a wireless client (that is, force it to reauthenticate)?	`@config: deauthenticiate <mac-addr>` (page 51)
disable ACL security?	`@config: acl any unblocked` (page 104)
enable ACL security, if disabled?	`@config: acl any blocked` (page 104)
reset counters for switch and PA statistics?	`@enable: clear statistics` (page 78)
reset counters for interface statistics?	`@configure: clear counters interface` (page 80)
view the last N entries in the system log?	`@configure: show logging N` (page 81)
copy the system log from NVRAM to a file?	`@configure: logging file-save <filename>` (page 82)
collapse all internal VLANs into one?	`@system submode: sysvlan single` (page 84)
restore internal VLANs that have been collapsed?	`@system submode: sysvlan multi` (page 84)
block an Ethernet port?	`@interface submode: shutdown` (page 117)
unblock an Ethernet port?	`@interface submode: no shutdown` (page 117)

DCN: as1200sm-B11

A. Technical Information

This appendix contains various categories of technical information that may be helpful as reference to users. It includes:

AirSwitch MAC Addresses

The AirSwitch has one factory-assigned MAC base address, which is permanent and is printed on the back of the chassis. It is not itself used by the system, but provides the basis for deriving the three usable MAC addresses on the switch, as follows:

MAC Address of:	Derived from:
Service Port	Base MAC + 1
Gb Port(s)	Base MAC address + 2 (if there are two Gb ports, both use same MAC address)
BSSID of Switch	Base MAC address + 4

These derivations refer to the last digit of the MAC address. For example, if your base address is 09:ab:3c:ab:2c:**05**,

- the SVC port will be 09:ab:3c:ab:2c:**06**
- the Gb ports will both be 09:ab:3c:ab:2c:**07**
- the BSSID will be 09:ab:3c:ab:2c:**09**

The MAC address displayed in response to the SHOW SWITCH command is the base address:

```
Model Number    : AS1211
Part Number     : 550-11002-01
Serial Number   : 1232460
DateCode        : 06192003
MAC Address     : 09:5B:C8:80:A1:1B
BSP Version     : 1.0.2.13
BootCode Version: 1.0.2.11
BCOM Version    : 2
HIFN Version    : 4
PPU FPGA Version: 0
DevSup FPGA Version: 35
Regulatory Domain  : FCC
```

Regulatory Compliance

The AirSwitch has been certified as complying with the requirements of the following organizations, as specified.

US FCC

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules and ICES 003. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Any changes or modifications to the AirSwitch or AirHubs not expressly approved by AirFlow Networks, Inc., may void the user's authority to operate this equipment.

DCN: as1200sm-B11

AirSwitch 1200 Hardware

AirFlow AirSwitch 1211 Specifications

Specification	Details
Physical Size	1-RU standard rack mounted chassis, 17" wide x 19" deep
Network Architecture	Infrastructure, star topology
LAN Ports	1 Gigabit Ethernet uplink 12 downstream 10/100MB Ethernet 1 unsecure upstream 10/100M, for public port 1 RS232 Serial management port 1 10/100 local service port All connections on front of chassis
Wireless Coverage	Dependent on number of AirScouts attached
Max PAs Supported	Point-to-Point: 12 With intermediate hubs or switches: 5/port, 60/switch
Max WLAN Clients Supported	*Attached*: Unlimited *Active*: 1200 (20/scout, 60 scouts per switch)
Power over Ethernet	Internal Standards-based IEEE 802.3af (Class 0 Power), not user configurable
Power Supply	300W power supply, terminal block mounted Active power factor correction Universal Power Input (VAC = 100-240V) Power output: 48VDC @6.5A UL, cUL & TUV recognition
Status LEDs	Switch: power, status Ports: link status, Tx/Rx traffic, PoE status, AirScout attached status
Address Lists	Wireless client access list: 8K MAC addresses, with aging and automatic learning Layer 2 addresses: up to 128K Layer 3 addresses: up to 64K Routing table: up to 256K entries
Environmental Specifications	*Operating*: 0° to 50° C.; max rel. humidity 95%, non-condensing *Storage*: -20° to 75° C.
Compliance	FCC part 15, UL, Wi-Fi

AirHub 100 Hardware

AirFlow AirHub 100 Specifications

Specification	Details
Physical Size	5.9” wide, 5.5” long, 1.2” high
Network Standard	IEEE 802.11b
Wireless Medium	Direct Sequence Spread Spectrum (DSSS) (DBPSK, DQPSK, CCK)
Installation Positions	Unmounted or mounted horizontal (desktop, shelf, ceiling), mounted vertical (wall, partition, furniture)
Max WLAN Clients Supported	*Attached*: Unlimited *Active*: 20
Data Rates Supported	1, 2, 5.5, 11 Mbps
Radio Channels	North America: 11 total, 3 non-overlapping
Transmit Power	min. = 3 mW, max. = 100 mW
Receive Sensitivity	-92 dBm 1 Mbps; -84 dBm 11 Mbit (typical)
Typical Coverage Range (max. power)	200 ft. (66m) @ 11 Mbps 500 ft. (166 m) @ 1 Mbps
Antenna Scheme	2 polarized omnidirectional diversity antennas, adjustable position
LEDs	Power/Status, Wireless Traffic, LAN Traffic
LAN Interface	Two 10/100 base-T ports: 1 for LAN connection; 1 for PC pass-through
Power Requirement	Power over Ethernet (802.3af) or AC/DC wall adapter, 2A/5V ***only***
Environmental Specifications	*Operating*: 0° to 40° C.; max rel. humidity 95%, non-condensing *Storage*: -20° to 75° C.
Compliance	FCC part 15, UL, Wi-Fi

System File Description

You can use the DIR command to view all files currently in flash memory directory of your AirSwitch. You may need to do this when you are manipulating files, such as during an upgrade or backing up config files or your ACL. As a rule, you should be very careful when directly manipulating files, and never delete or rename a file unless you are confident you know what it does and what the results will be. If you have any doubts, consult AirFlow technical support.

The following information provides a general description of the files you will see when you use the DIR command. Even if you are consulting with AirFlow tech sup-

DCN: as1200sm-B11

port, you should familiarize yourself with this information, and be able to recognize the different kinds of files residing on the switch based on their names.

Note that this is an example, and actual file names will change to reflect software versions. The naming conventions of the various file types, however, will be consistent and recognizable.

Also bear in mind that this example assumes that the filenames were not changed during the ftp procedure. AirFlow strongly recommends that, whenever you FTP files onto the switch, you keep the same name on all target filename as the source file.

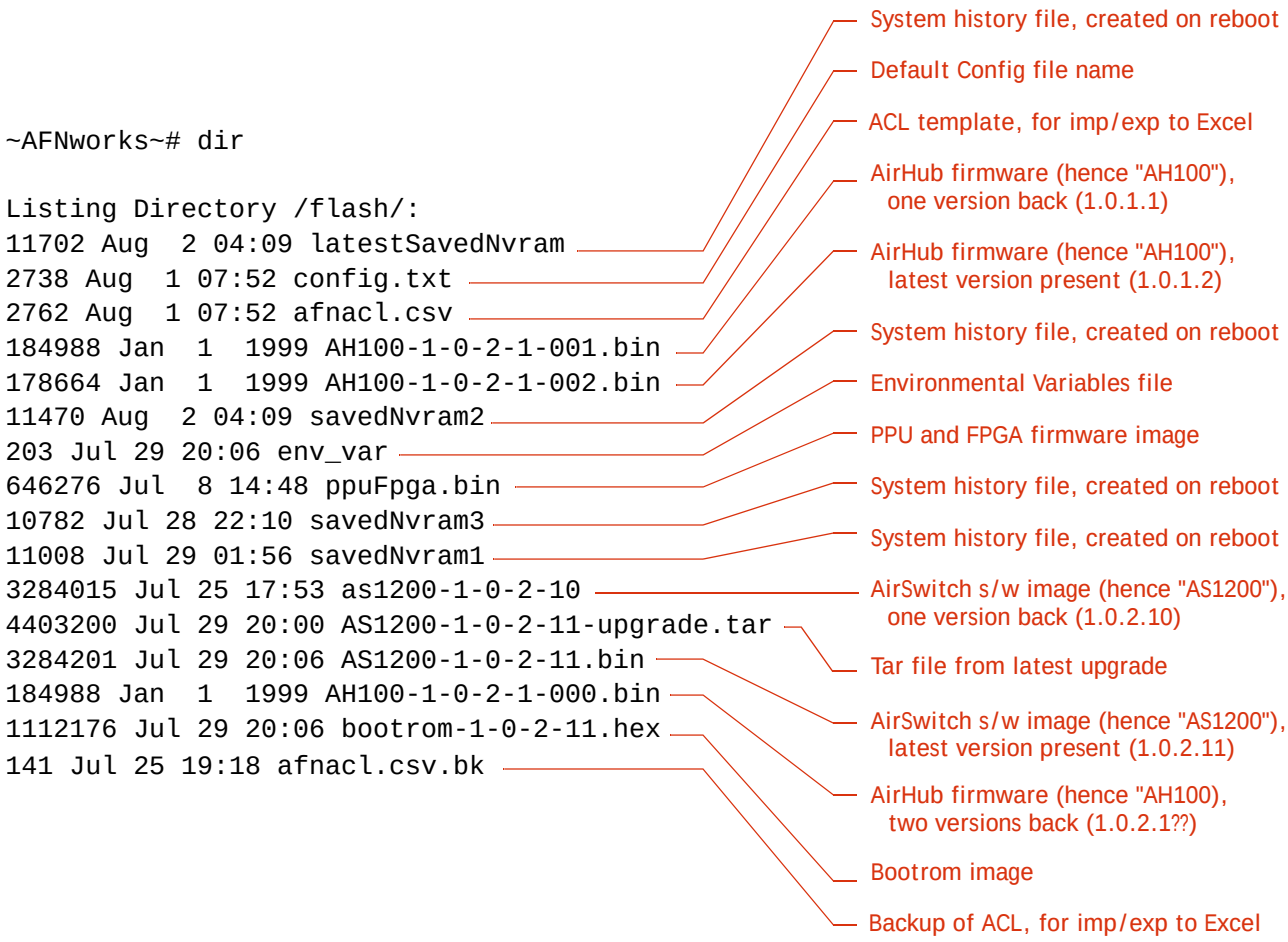


Figure 1-1: Example of AirSwitch System File Types

DCN: as1200sm-B11

I. Index

A

B

C

D

E

F

G

H

I

DCN: as1200sm-B11

K

L

M

N

O

P

DCN: as1200sm-B11

T

U

V

W

DCN: as1200sm-B11

DCN: as1200sm-B11