

A Using the Command Line Interface

This appendix explains how to access and interact with the command line interface (CLI). For detailed information on specific commands, see the CLI Reference Manual.

Using the Command Line Interface

To connect to the AP for command line interface access using Secure Shell (SSH), do the following:

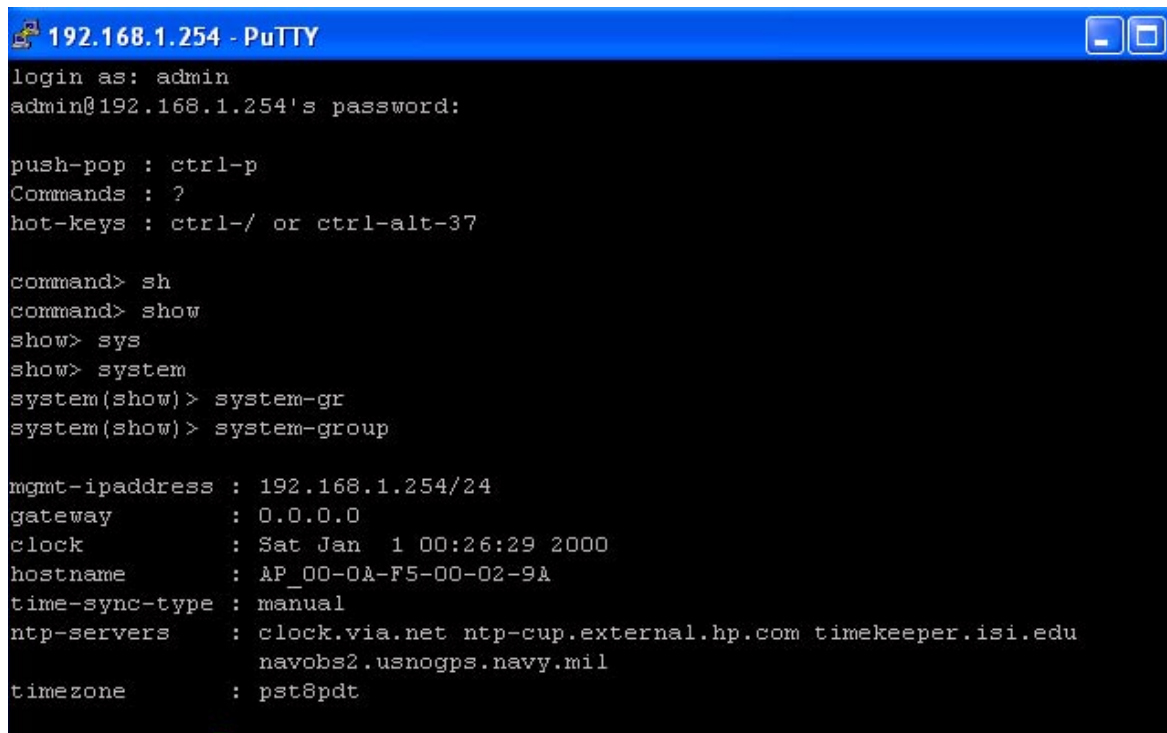
- 1 Launch your SSH client application.

i **NOTE:** SSH Communications provides an SSH client, <http://www.ssh.com>.

- 2 Type `ssh admin@<AP IP address>`, using the AP IP address assigned to the Access Point (or 192.168.1.254 by default) and press Return.

When connected, a screen opens similar to the one shown in Figure 188.

Figure 188: Access Point Serial Console Login Screen



```
192.168.1.254 - PuTTY
login as: admin
admin@192.168.1.254's password:

push-pop : ctrl-p
Commands : ?
hot-keys : ctrl-/ or ctrl-alt-37

command> sh
command> show
show> sys
show> system
system(show)> system-gr
system(show)> system-group

mgmt-ipaddress : 192.168.1.254/24
gateway       : 0.0.0.0
clock         : Sat Jan  1 00:26:29 2000
hostname      : AP_00-0A-F5-00-02-9A
time-sync-type : manual
ntp-servers   : clock.via.net ntp-cup.external.hp.com timekeeper.isi.edu
               : navobs2.usnogps.navy.mil
timezone      : pst8pdt
```

- 3 Enter your login ID and press Return. When prompted next, enter your password. The factory default for administrator access is username: admin. The factory default password is shipped with the AP on a paper insert. Use the password from the insert to log in.

- 4 To see the list of available commands, type a question mark (?). For a list of hot keys (short cuts for console functions, press Ctrl-H.
There are two important modes in console access, one is *show* mode and the other is *config* mode. In show mode, examine the AP's configuration settings and status. Use config mode to change values. To go into either mode from the main `command>` prompt, type either `show` or `config`.
Toggle between *show* and *config* modes by pressing Ctrl-P. Leave a mode and return to the top level command prompt by typing `exit`.
- 5 To log out and close your connection to the command line interface, type `logout` at any prompt.

Using the Console Port for CLI Access

To connect to the AP for command line interface (CLI) access using the built-in console port, do the following:

- 1 Connect your computer to the AP console port using a serial DCE cable (this is typically a 9-pin-to-9-pin cable with the transmit and receive lines crossed over — a null modem cable). A USB-to-Serial adapter may be required if your computer lacks a 9-pin serial port.
- 2 Launch your terminal emulation application. On PCs running Microsoft Windows operating systems, the Microsoft-provided application HyperTerminal will work fine. (This is accessed usually through `Programs > Accessories > Communications > HyperTerminal`. The remainder of this procedure assumes the use of HyperTerminal. Modify the procedures accordingly if using another application.)
- 3 Create a terminal connection profile if one does not already exist. Enter a descriptive name and select any icon from the list provided. Click **OK** when done.
If there is a working HyperTerminal connection profile, select that shortcut instead to launch the connection, and skip to step 7.
- 4 The Connect To screen displays. The important element there is to use the `Connect using:` box, and select the serial port to which the AP is connected. Click OK when done.
- 5 Use the following port settings:
 - Bits per second: 115200
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None
- 6 Click OK when done. When connected, a screen opens similar to the one shown in Figure 188.
- 7 If the console login screen in the HyperTerminal does not open, press **Return** once or twice. If you still see nothing or garbage characters appear, check the cable connection and the terminal connection parameters.
- 8 Enter your login ID and press Return. When prompted next, enter your password. (The AP defaults are login: `admin` and password: `password`, and login: `opr` and password: `opr` for operator (read-only) access.)

- 9 To see the list of available commands, type a question mark. For a list of hot keys (short cuts for console functions, press Ctrl-H.

There are two important modes in console access, one is *show* mode and the other is *config* mode. In show mode, examine the AP's configuration settings and status. Use config mode to change values. To go into either mode from the main `command>` prompt, type either `show` or `config`.

Toggle between show and config modes by pressing Ctrl-P. Leave a mode and return to the top level command prompt by typing `exit`.

To log out and close your connection to the command line interface, type `logout` at any prompt.

B Regulatory and License Information

This appendix contains the regulatory and license information specific to the Airgo Access Point hardware and software.

ID	Access Point Requirement	Details
CERT1	Safety	UL 1950 third edition TUV approval UL-2043 (Fire and Smoke) Compliance
CERT2	EMC	EMC Directive 89/336/EEC (CE Mark)
CERT3	Radio Approvals	FCC CFR47 Part 15, section 15.247 FCC (47CFR) Part 15B, Class B Emissions Canada IC RSS210 Japan MIC Radio Regulations Europe: ETS 300.328

FCC Certifications

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

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



CAUTION: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

The Airgo AP is suitable for use in environmental air space in accordance with Section 300-22(c) of the National Electrical Code, and Sections 2-128, 12-010(3) and 12-100 of the Canadian Electrical Code, Part 1, CSA C22.1.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.

C External Landing Page API

This appendix is a supplement to Chapter 8, “Configuring Guest Access,” which describes the process of authenticating and isolating guest user stations. Guest authentication is a web-based process that requires the user to open a web browser, which then automatically redirects the user to an authentication web page. Two approaches are available:

- Internal Landing Page that is present inside the AP
- External Landing Page

Introduction

This appendix documents the application programming interface (API) between the AP and the External Landing Page Server (ELPS).

Case Studies

- 1 Enterprise Guest Access Scenario: An enterprise will typically support multiple VLANs. Enterprise users are generally strongly authenticated and have direct access to the enterprise VLAN. Untrusted guest users are blocked from enterprise resources by use of an HTTP captive portal. After authenticating to the captive portal, the guest users are allowed on a specific VLAN with access to the Internet, but not to enterprise resources.
- 2 Hotspot Deployment Scenario: All user web browser traffic is initially redirected to a captive portal (walled garden) that allows them to either login or purchase services to obtain a valid login identity. Subsequently, the entitled users are allowed full Internet access through AP association. Connection services may be constrained to a specific duration before reauthentication is required. The ELPS service may also track usage by connection.

AP Configuration

As described in Chapter 8, “Configuring Guest Access,” configuring an AP to support Guest Access using an external authentication web server, requires specifying two configuration parameters:

- The fully qualified URL (IP format) of a page on the external authentication web server, the “landing page.”
- A shared secret code known to both the external authentication web server and the AP. This information is entered into the Guest Access Wizard or the Guest Access Service Panel.

This information is entered into the Guest Access Wizard or the Guest Access Service Panel.

System Description

Three principle entities are involved in user authentication with an external authentication web server.

- The station (STA)
- The Access Point (AP)
- The External Landing Page Server (ELPS)

The station associates to the AP. The AP allows the station to obtain a DHCP based IP address and allows ARP and DNS queries. All other traffic is blocked. Web traffic is blocked and redirected to the ELPS. The ELPS provides web pages to authenticate users and subsequently signals the AP to allow the station access to a broader set of IP addresses (the Internet).

The web server (ELPS) is also able to disconnect any of the previously connected stations. The signaling from the web server to the AP includes a disconnect request. The disconnect request can be used to stop billed connection time at a hot spot. This is often implemented by providing a status web window that displays the users time on-line with a button to provide the logout. The disconnect can also be sent directly from the server to the AP to provide a forced disconnection of the user based on the management functionality in the web server.

The process to enable access (from the ELPS to the AP) is analogous to purchasing a ticket and then entering a theater. The guest station represents the theater patron, the external authentication web server represents the box office, and the AP represents the ticket taker.

Upon entering the theater, the patron is first directed to the box office and presents credentials in order to collect tickets (money or identification for pre-ordered tickets). The patron then takes the ticket to the ticket taker, who validates the ticket and permits entrance. Correct validation includes a check of the timestamp (date and time of performance) and confirmation of the type of performance. In effect, the ticket taker verifies that the ticket has been issued by the box office.

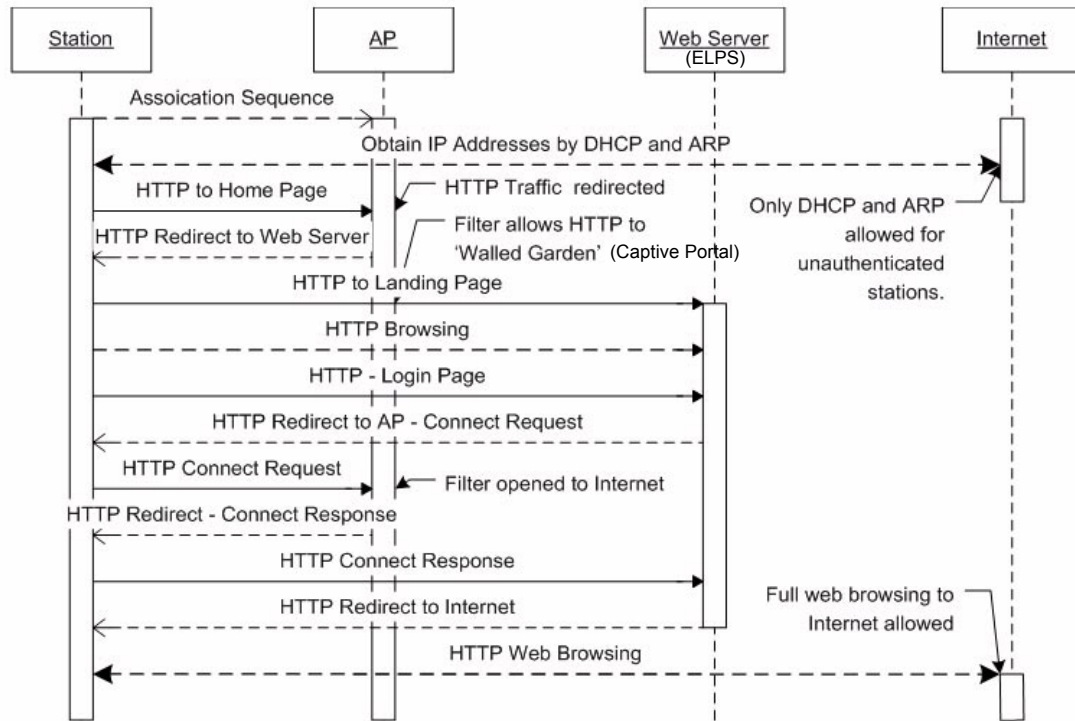
Detailed Signaling Description and API

The application programming interface (API) between the ELPS and the AP supports the following uses:

- Connect Sequence: Capture unauthenticated users and subsequently connect them after a valid authentication
- User Initiated Disconnect: Disconnect a station based on a user request to logout (STA Disconnect)
- Station Forced Disconnect: Force a disconnect from the ELPS (STA Forced Disconnect)

Connect Sequence

The signaling flow for a station associating with the network for the first time is illustrated in Figure 1.

Figure 189: User authentication using the External Landing Page Server

The HTTP filter in the AP allows the station to obtain an IP address, but redirects any HTTP traffic to the web server. The URL used in the redirection provides the server with the MAC address of the station, the SSID used for the association, the IP address of the AP, and the original requested URL. This data is used by the web server to create a connect request to the AP after successful authentication.

Redirected URL generated by an AP:

<http://1.2.3.4/cgi/l?gpm=192.168.254.249&origpage=www.google.com&ssid=myHotspot&stamac=00:af:50:00:00:00>

The URL prefix (<http://1.2.3.4/cgi-bin/l>) was the URL entered in the AP configuration.

The field names and description in the redirected URL are described in Table 18.

Table 18: Fields in the STA-ELPS-to-AP Connection Request

Field	Description
gpm	The IP address of the AP
origpage	The URL originally submitted by the user before the redirection
ssid	The SSID used by the station to associate to the AP
stamac	The MAC address of the station.

Once redirected to the web server, the user is able to browser only in the walled garden. This restricted set of web pages should provide a means to login into the network and optionally a means to obtain an account for first-time users. When a user is successfully authenticated, the ELPS returns a redirection URL that signals the AP to allow unrestricted access for the specific station (a Connection Request).

Redirection URL generated by the ELPS:

https://192.168.254.249/Forms/ExtCmd_html_1?Xnp=www.google.com&Xcmd=crq&Xts=0410280335&Xssid=myHotspot&Xmac=00%3Aaf%3A50%3A00%3A00%3A00&Xcv=f4eb6692aeffe839&Xdata=480&Xid=bob

The base portion of the URL was formed using the IP address originally passed to the web server as the gpm field (AP IP address). The URL is protected from modification, spoofing, or reuse by the use of a timestamp and a cryptographic check value. The URL must always have the form:

https://<AP IP Address>/Forms/ExtCmd_html_1?<parameters>

The URL that signals the AP to permit access for a particular station uses parameters that are passed in the URL. These form a connection request. The following parameters are supported:

Table 19: Fields in the STA-ELPS-to-AP Connection Request

Field	Description
Xcmd	The command type (connect for this example) For a connect this value MUST be 'crq'
Xnp	Not used
Xid	Optional, the login user id (included in logs)
Xip	Optional, not used for the connect command.
Xssid	The SSID.
Xmac	The MAC address of the station that has been authenticated.
Xdata	Command data. For the connect request should contain the duration of the permitted user connectivity in minutes.
Xts	A time stamp of the form yymmddhhMM, where yy=year, mm=month, dd=day, hh=hours, MM=minutes. To be valid, the time value (in UTC) must be within plus or minus 5 minutes of the AP's time.
Xcv	A SHA1 hash using the shared password.

Upon successful opening of the AP HTTP filter, the user's browser is redirected back to the web server. This permits positive indication of user access for billing purposes on the ELPS. The redirected URL contains the following parameters:

Table 20: Fields in the STA-AP-to-ELPS Connection Response

Field	Description
Xcmd	This MUST be 'crs' for the connection response.
Xnp	Not used
Xid	Not used.

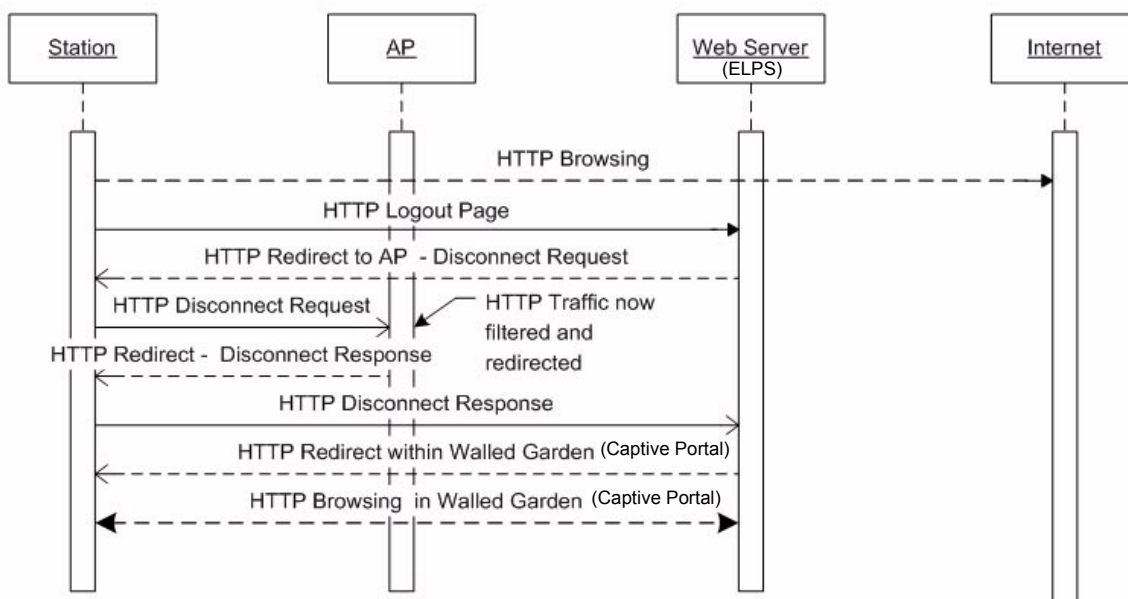
Table 20: Fields in the STA-AP-to-ELPS Connection Response (continued)

Field	Description
Xip	Not used.
Xssid	The SSID.
Xmac	The MAC address of the station that has been authenticated.
Xdata	Should have a value of '3' for a successful connection.
Xts	A time stamp of the form yymmddhhMM, where yy=year, mm=month, dd=day, hh=hours, MM=minutes. To be valid, the time value (in UTC) must be within plus or minus 5 minutes of the AP's time.
Xcv	A SHA1 hash using the shared password.

After the user is redirected to the ELPS, the server can redirect the user's browser to the originally requested URL, or start a status/tracking window to inform the user of their time on-line.

User Initiated Disconnect

Figure 2 illustrates the flow of the signaling for a user initiated disconnect. The user typically will have a status browser window open that includes a log out button.

Figure 190: User initiated Disconnect Request Sequence

The log out takes the user's browser to the ELPS. At the ELPS a redirected URL sends the user's browser back to the AP. The redirected URL includes all parameters required to disconnect the station.

https://192.168.254.249/Forms/ExtCmd_html_1?Xcmd=drq&Xnp=www.hotspot.com&Xts=0410280408&Xmac=00A0AAF5A00A00A00&Xssid=myHotSpot&Xcv=92fbed6322fbd017

The prefix portion of the URL was formed using the IP address originally passed to the web server as the gpm field (AP IP address). The URL is protected from modification, spoofing or reuse by the use of a timestamp and a cryptographic check value. The URL must always have the form:

https://<AP IP Address>/Forms/ExtCmd_html_1?<parameters>

Note that the disconnect request will send the user to a “next page” that can put the user’s browser back into the web servers walled garden. The disconnect leaves the station associated, but returns the station to the unauthenticated state. The HTTP filter in the AP will now redirect any HTTP traffic back to the configured walled garden. Table 21 lists the parameters.

Table 21: Fields in the STA-ELPS-to-AP Disconnect Request

Field	Description
Xcmd	The command type (connect for this example) For a connect this value MUST be 'drq'
Xnp	The next page to send the Users browser
Xid	Optional, the login user id (included in logs)
Xip	Optional, not used for the connect command.
Xssid	The SSID (required).
Xmac	The MAC address of the station that has been authenticated. Required to specify the station to disconnect.
Xdata	Not used for a disconnect command.
Xts	A time stamp of the form yymmddhhMM, where yy=year, mm=month, dd=day, hh=hours, MM=minutes. To be valid, the time value (in UTC) must be within plus or minus 5 minutes of the AP's time.
Xcv	A SHA1 hash using the shared password.

Upon successfully closing of the AP HTTP filter, the user's browser is redirected back to the web server to signal a Disconnect Response. This allows the user to be smoothly transitioned from browsing the Internet back to a known page in the walled garden web. Table 22 lists the parameters in the URL.

Table 22: Fields in the STA-AP-to-ELPS Disconnect Response

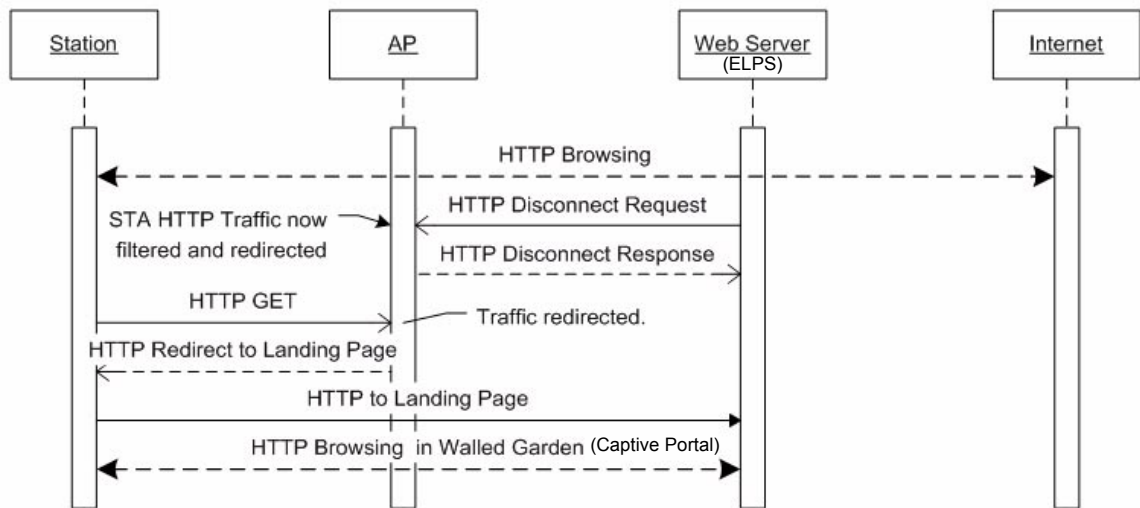
Field	Description
Xcmd	The command type (connect for this example) For a connect this value MUST be 'drs'
Xnp	The next page to send the Users browser
Xid	Optional, the login user id (included in logs)
Xip	Optional Fields in the STA-AP-to-ELPS Disconnect Response, not used for the connect command.
Xssid	The SSID.
Xmac	The MAC address of the station that has been authenticated. Required to specify the station to disconnect.

Table 22: Fields in the STA-AP-to-ELPS Disconnect Response

Field	Description
Xdata	This should have a value of 8 for a successful disconnect.
Xts	A time stamp of the form yymmddhhMM, where yy=year, mm=month, dd=day, hh=hours, MM=minutes. To be valid, the time value (in UTC) must be within plus or minus 5 minutes of the AP's time.
Xcv	A SHA1 hash using the shared password.

Station Forced Disconnect

The web server can directly signal the AP to disconnect a station. Figure 3 illustrates the signal flow for this scenario.

Figure 191: Web server initiated forced disconnect of user

The construction of the disconnect URL is identical to the URL for the user initiated station disconnect. The only difference is that the HTTP request is initiated from the web server to the AP rather than from the station.

Check Value Algorithm

The check value carried in the Xcv field is calculated using the SHA-1 algorithm (FIPS 180-1 standard). The server must create the appropriate time stamp and check value in server side active web pages. The check value will typically be created using active pages on the web server (asp, cgi,.net, etc.). This check value is produced using the following procedure:

- 1 Create a timestamp of the form yymmddhhMM, where yy=year, mm=month, dd=day, hh=hours, MM=minutes. For example, the string '0407041355' corresponds to 2004 July 7 1:55pm. This string must always be 10 characters long and all fields must be zero filled.
- 2 Obtain the parameters from the original redirect URL sent to the server. These are most easily retained as a cookie. The following parameters are required:
 - a The STAs MAC address (e.g. '00:0A:F5:00:09:99')

- b** The SSID that the station used to associate to the AP
 - c** The IP address of the AP
- 3** Have available the server key that is shared with the AP. This secret key authenticates the server to the AP.
- 4** Create the partial URL using the URL parameters of the form:
`Xcmd=<cmd>&Xnp=<nextUrl>&Xid=<userId>&Xip=<ipAddress>&Xssid=<ssid>&Xmac=<staMac>&Xdata=<data>&Xts=<timeStamp>`
Any of the unused option parameters should be included, but the strings should be set to null. The Order of these parameters MUST be the exactly as shown - else the check value will not match.
For example:
`Xcmd=crq&Xnp=www.hotspot.com&Xid=smith&Xip=&Xssid=coffeeShop&Xmac=00:0A:F5:00:00:00&Xdata=60&Xts=0410280408`
- 5** Calculate the SHA1 has algorithm over the string formed by placing the server key before and after the partial URL:
`hash = SHA1(server key | partial URL | server key)`
- 6** Take only the first 8 octets of the hash and convert these octets to hex-ascii. This is the Xcv parameter value.
- 7** Create the full URL by appending all of the above parameters to the base URL of the AP. Unused parameters do NOT have to be included in the final URL sent to the AP. The base URL is always of the form: `https://<AP IP Address>/Forms/ExtCmd_html_1?`
`https://1.2.3.4/Forms/ExtCmd_html_1?Xcmd=crq&Xnp=www.hotspot.com&Xid=smith&Xssid=coffeeShop&Xmac=00:0A:F5:00:00:00&Xdata=60&Xts=0410280408&Xcv=92fbed6322fbd017`

Response Return Codes

The Connect Response (crs) and the Disconnect Response (drs) carry result values to indicate success or possible error conditions. The following response codes are supported:

Response Code	Usage
0	Not used.
1	Invalid command.
2	Login success, filters removed for the station.
3	Digest check value error.
4	Time stamp error.
5	Duration value failure.
6	Connection request failure. Typically caused by station roaming to a different AP.
7	Disconnect succeeded, filters reinstalled for the station.
8	Disconnect failed. Typically caused by the station already being disassociated.
9	Not used.

D Alarms

Alarms generated by the Airgo Access Point are stored persistently on the AP. The Airgo AP can store approximately $130 * 2 = 260$ alarms in total. When the number of alarms exceeds this limit, the oldest alarm set is discarded.

All alarms generated by the Airgo Access Point have the following parameters:

- **Event ID:** The internal event number that uniquely identifies the event.
- **Log-level:** The criticality of the event. All alarms are logged at the same criticality.
- **Log-time:** The time as determined by the clock on the Access point, when the alarm was logged. All forwarded alarms have the log-time set to the clock time on the originating Access point.
- **Module:** The subsystem on the Access point that generated the alarm.
- **Source:** The hostname or IP address of the access point that generated the alarm.
- **Description:** The alarm details.

Use the Airgo AP CLI to display the alarm table as follows:

Examples: `system(show) > alarm-table`

```
event-id   : 102
log-level  : 2
log-time   : Tue Jan  4 16:14:01 2000
module     : WSM
source-ip  : AP_00-0A-F5-00-02-1F
description : Device ID AP_00-0A-F5-00-02-1F radio 6 is enabled, its operational
              state is 2 operating on 11
-----
event-id   : 103
log-level  : 2
log-time   : Tue Jan  4 17:04:28 2000
module     : WSM
source-ip  : AP_00-0A-F5-00-02-1F
description : Device Id AP_00-0A-F5-00-02-1F radio 4 disabled
-----
```

The following section describes in detail the alarm syntax and alarm parameters. The alarm and its parameters together are shown as “description” above. The following alarms are described:

- “Discovery: Discovered new node” on page 275
- “Discovery: Node deleted from network” on page 275
- “Discovery: Managed nodes limit exceeded” on page 276
- “Enrollment: Node enrolled” on page 277
- “Enrollment: Node un-enrolled” on page 278
- “Policy: Policy download successful” on page 278

- “Policy: Policy Download Failed” on page 279
- “Software Download: Image download succeeded” on page 280
- “Software Download: Image download failed” on page 280
- “Software Download: Software distribution succeeded” on page 281
- “Wireless: Radio enabled (BSS enabled)” on page 282
- “Wireless: Radio disabled (BSS disabled)” on page 283
- “Wireless: BSS enabling failed” on page 283
- “Wireless: Frequency changed” on page 284
- “Wireless: STA association failed” on page 285
- “Wireless: STA associated” on page 286
- “Wireless: STA disassociated” on page 287
- “Wireless: WDS failed” on page 288
- “Wireless: WDS up” on page 289
- “Wireless: WDS down” on page 290
- “Security: Guest authentication succeeded” on page 291
- “Security: Guest authentication failed” on page 291
- “Security: User rejected by RADIUS server” on page 292
- “Security: BP rejected by RADIUS server” on page 293
- “Security: RADIUS server timeout” on page 294
- “Security: Management user login success” on page 295
- “Security: Management User login failure” on page 296
- “Security: STA failed EAPOL MIC check” on page 297
- “Security: STA attempting WPA PSK – no pre-shared key is set for SSID” on page 298
- “Security: Auth server Improperly configured on this SSID” on page 298
- “Security: STA failed to send EAPOL-start” on page 299
- “Security: RADIUS sent a bad response” on page 300
- “Security: RADIUS timeout too short” on page 301
- “Security: STA authentication did not complete in time” on page 302
- “Security: Upstream AP is using an untrusted auth server” on page 303
- “Security: Upstream AP is using a non-portal node as its auth server” on page 304
- “Security: Upstream AP failed MIC check during BP authentication” on page 305
- “Security: Premature EAP-success received” on page 306
- “Security: Profile not configured for user-group” on page 306
- “Security: STA has failed security enforcement check” on page 307
- “Security: AP detected bad TKIP MIC” on page 308
- “Security: BP detected bad TKIP MIC on incoming unicast” on page 309
- “Security: BP detected bad TKIP MIC on incoming multicast/broadcast” on page 310
- “Security: STA detected bad TKIP MIC on incoming unicast” on page 311
- “Security: STA detected bad TKIP MIC on incoming multicast/Broadcast” on page 311
- “Security: TKIP counter-measures lockdown period started” on page 312
- “Security: EAP user-ID timeout” on page 313
- “Security: EAP response timeout” on page 314

- “Security: EAPOL key exchange – message 2 timeout” on page 315
- “Security: EAPOL key exchange – message 4 timeout” on page 316
- “Security: EAPOL Group 2 key exchange timeout” on page 317
- “L3 Mobility: Peer Mobility Agent Up” on page 318
- “L3 Mobility: Peer Mobility Agent Down” on page 318

Discovery: Discovered new node

Alarm generated when a new Airgo AP is discovered in the network

Syntax

```
DeviceId %s discovered node [deviceId=%s, IP=%s, Subnet=%s] .
```

Alarm Parameters

DeviceID	The Portal’s device ID
deviceId	The discovered node’s device ID
IP	The discovered node’s IP address
Subnet	The subnet to which the discovered node belongs

Alarm Severity

Severity	Critical
----------	----------

Description

This alarm is generated when an Airgo AP is discovered by the NM Portal the first time.

Usage Guidelines

Informational log

Examples

```
DeviceId AP_00-0A-F5-00-02-1F discovered node [deviceId=AP_00-0A-F5-00-01-B0,  
IP=192.168.75.244, Subnet=255.255.254.0] .
```

See Also

```
<Node deleted from network>
```

Discovery: Node deleted from network

Generated when a node is deleted from the Portal network

Syntax

```
DeviceId %s Node [Ip=%s, persona=%d] deleted from database.
```

Alarm Parameters

DeviceId	The device ID of the NM Portal
----------	--------------------------------

Ip	The IP address of the node being deleted
----	--

Persona	The persona of the node being deleted.
---------	--

Alarm Severity

Severity	Critical
----------	----------

Description

This alarm is generated when the discovered node is deleted from the system. When a node is deleted, all information about that node is erased from the Portal. If the node's IP address falls within the discovery scope, then the node will be re-discovered and added back to the set of the discovered nodes on the next discovery sweep.

Usage Guidelines

Informational log

Examples

```
DeviceId AP_00-0A-F5-00-02-1F Node [Ip=192.168.74.210, persona=6] deleted from database.
```

See Also

```
<Discovered new node>
```

Discovery: Managed nodes limit exceeded

Generated when the number of nodes discovered exceeds the predefined limit on the NM portal.

Syntax

```
On Device %s Node[Ip=%s] managed node limit exceeded. Current managed nodes limit is %d.
```

Alarm Parameters

Device	The device ID of the NM Portal
--------	--------------------------------

IP	The IP address of the node being deleted
----	--

Node Limit	The current limit imposed on the discovery server
------------	---

Alarm Severity

Severity	Critical
----------	----------

Description

This alarm is generated when the number of discovered nodes exceeds the predefined limit. The current limit on the number of access points discovered is 50. This limit can be configured to be lower.

Usage Guidelines

If this alarm occurs, the discovery server will not discover nor track any new nodes once this limit is reached. In such a case, delete unwanted nodes and manually add the nodes to the discovery database so they may be managed.

Examples

On Device AP_00-0A-F5-00-02-1F Node[Ip=192.168.74.245] managed node limit exceeded. Current managed nodes limit is 10.

See Also**Enrollment: Node enrolled**

Alarm generated when an Airgo AP is enrolled into the network

Syntax

NMPortal with **DeviceId** %s has successfully enrolled a remote node having **ApDeviceId**=%s **NodeIp**=%s and **Persona**=%d

Alarm Parameters

DeviceId	The device ID of the NMPortal
ApDeviceId	The device ID of the remote AP
NodeIp	The IP address of the remote AP
Persona	The persona of the remote AP 6 = Security Portal 2 = Normal AP

Alarm Severity

Severity	Critical
----------	----------

Description

This alarm is generated when the Airgo AP has been successfully enrolled into the network.

Usage Guidelines

Informational log

Examples

NMPortal with DeviceId AP_00-0A-F5-00-01-77 has successfully enrolled a remote node having DeviceIdId=AP_00-0A-F5-00-01-7A NodeIp=172.16.12.4 and persona=2

See Also

<Node Unenrolled>

Enrollment: Node un-enrolled

Alarm generated when the Airgo AP is rejected (un-enrolled) from the network

Syntax

NMPortal with **DeviceId** %s has successfully unenrolled the remote node having **ApDeviceId**=%s **NodeIp**=%s and **Persona**=%d

Alarm Parameters

DeviceId	The device ID of the NMPortal
ApDeviceId	The device ID of the remote AP
NodeIp	The IP address of the remote AP
Persona	The persona of the remote AP 6 = Security Portal 2 = Normal AP

Alarm Severity

Severity	Critical
----------	----------

Description

This alarm is generated when the Airgo AP has been successfully rejected (un-enrolled) from the network.

Usage Guidelines

Informational log

See Also

NMPortal with DeviceId AP_00-0A-F5-00-01-77 has successfully enrolled a remote node having DeviceIdId=AP_00-0A-F5-00-01-7A NodeIp=172.16.12.4 and persona=2

See Also

<Node Enrolled>

Policy: Policy download successful

Alarm generated when a policy is successfully downloaded to an AP

Syntax

For accesspoint **Node** %s The **policy** [%s] **from** [%s] was successfully downloaded at **time**[%s]

Alarm Parameters

Node	The device ID of the remote AP
policy	The policy name

from	The device ID of the source of the policy
time	The time at which the policy was consumed
Alarm Severity	
Severity	Critical

Description

This alarm is generated when a policy is successfully downloaded to an AP.

Usage Guidelines

Informational log

Examples

```
For accesspoint Node AP_00-0A-F5-00-01-77 The policy [security.xml] from
[TrustedManager] was successfully downloaded at time[Thu Jan 6 04:27:45 2000 ]
```

See Also

<Policy Download Failed>

Policy: Policy Download Failed

Alarm generated when a policy download to an AP has failed

Syntax

```
For accesspoint Node %s the policy [%s] from [%s] could not be downloaded due
to error %d at time[%s]
```

Alarm Parameters

Node	The device ID of the remote AP
policy	The policy name
from	The device ID of the source of the policy
error	The failure error code
time	The time at which the policy was consumed

Alarm Severity

Severity	Critical
----------	----------

Description

This alarm is sent when a policy downloaded to an AP could not be consumed correctly due to an error in the policy, software version mismatch, or another error.

Usage Guidelines

Informational log

Examples

For accesspoint Node AP_00-0A-F5-00-01-7D The policy [defaultpolicy.xml] from [TrustedManager] could not be downloaded due to error 22549 at time[Wed Feb 11 17:28:38 2004]

See Also

<Policy Download Successful>

Software Download: Image download succeeded

Alarm generated when an image is successfully downloaded and applied to an AP

Syntax

For accesspoint **Node** %s the software **image** [%s] **from** [%s] was successfully downloaded at **time**[%s]

Alarm Parameters

Node	The device ID of the remote AP
image	The image version information
from	The device ID of the source of the image
time	The time at which the image was consumed

Alarm Severity

Severity	Critical
----------	----------

Description

This alarm is generated when an image is successfully downloaded and applied to an AP.

Usage Guidelines

Informational log

Examples

For accesspoint Node AP_00-0A-F5-00-01-77 The software image [1.1.0, build 3278, AGN1dev, Airgo Networks Inc.,] from [AP_00-0A-F5-00-01-77] was successfully downloaded at time[Fri Jan 7 06:04:47 2000]

See Also

<Image Download Failed, Software Distribution Succeeded>

Software Download: Image download failed

Alarm generated when an image is unsuccessfully downloaded and applied to an AP

Syntax

For accesspoint **Node** %s The software **image** [%s] **from** [%s] could not be downloaded due to **error** %d at **time**[%s]

Alarm Parameters

Node	The device ID of the remote AP
image	The image version
from	The device ID of the source of the image
error	The failure error code
time	The time at which the error occurred

Alarm Severity

Severity	Critical
----------	----------

Description

This alarm indicates that an image is unsuccessfully downloaded and applied to an AP.

Usage Guidelines

Image download failures can happen due to corrupted images, invalid length images or connectivity failures.

Examples

```
For accesspoint Node AP_00-0A-F5-00-01-77 The software image [] from [AP_00-0A-F5-00-01-77 ] could not be downloaded due to error 24581 at time[Fri Jan 7 04:12:35 2000 ]
```

See Also

<Image Download Succeeded, Software Distribution Succeeded>

Software Download: Software distribution succeeded

Alarm generated when an image distribution is completed

Syntax

On **DeviceId** %s, the Software **image** [%s] distribution request from **portal**[%s] using the Distribution **TaskId**=%s and with **status**=%s completed at **time**[%s]

Alarm Parameters

DeviceId	The device ID of the remote AP
image	The image version
portal	The device ID of the source of the image (NMS or NMPortal)
TaskId	The task ID of the distribution
status	The distribution status (success or failure) of the selected APs
time	The time at which the distribution was done

Alarm Severity

Severity	Critical
----------	----------

Description

This alarm is when an image distribution is completed.

Usage Guidelines

Informational log

Examples

```
On DeviceId AP_00-0A-F5-00-01-77 , the Software image [0.7.0, build A.2286,
AGN1dev, Airgo Networks Inc., ] distribution request from portal[AP_00-0A-F5-
00-01-77 ] using the Distribution TaskId=000000 and with status=172.16.12.4, ,
0, 947304168, 947304183, invalid image file. completed at time[Tue Jan 6
21:32:18 1970 ]
```

See Also

<Image Download Failed, Image Download Succeeded>

Wireless: Radio enabled (BSS enabled)

Notification that an AP radio has been enabled

Syntax

```
"Device ID %s radio %d is enabled, its operational state is %d operating on
%d"
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Radio	Identifies radio by interface ID on the AP
Operational Mode	This indicates the operational mode of the radio whether it is 802.11a, 802.11b, or 802.11g.
Channel ID	This indicates the channel on which the AP is operating.

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when an AP radio (BSS) is enabled.

Usage Guidelines

This indicates the successful start of a BSS and also provides the channel on which the AP radio will be operating.

Examples

Device ID AP_00-0A-F5-00-01-B6 radio 4 is enabled, its operational mode is 1 and operating on 64

See Also**Wireless: Radio disabled (BSS disabled)**

Notification that an AP radio has been disabled

Syntax

"Device Id %s radio %d disabled"

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Radio	Identifies radio by interface ID on the access point

Alarm Severity

Severity	Critical
----------	----------

Description

This notification indicates that an AP radio has been disabled.

Usage Guidelines

The AP radio can be disabled for several reasons such as:

- User triggered (administrative disabling)
- Radio reset caused due to application of wireless specific configuration
- Radio reset triggered by hardware
- Radio reset due to change in SSID

Examples

Device Id AP_00-0A-F5-00-01-B6 radio 4 disabled

See Also

<List of other alarms>

Wireless: BSS enabling failed

Notification that indicates the AP radio (BSS) enabling failed

Syntax

"Bss enabling failed for DeviceId %s radio %d CauseCode %d"

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Radio	Radio interface on the AP
Cause Code	Reason for AP radio enabling failure

Alarm Severity

Severity	Critical
----------	----------

Description

This notification indicates that AP radio enabling has failed.

Usage Guidelines

The AP radio enabling can fail for reasons that are indicated by the Cause code parameter:

- 0 Unspecified reason
- 1 System timeout attempting to enable BSS

Examples

Bss enabling failed for Device Id AP_00-0A-F5-00-01-B6 radio 4 Cause Code 1

See Also

<List of other alarms>

Wireless: Frequency changed

Notification that indicates the frequency of operation changed on the AP

Syntax

"Frequency changed for DeviceId %s radio %d channelId %d CauseCode %d"

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Radio	Radio identified by interface ID on the AP
Channel ID	Channel on which the AP is operating
Cause Code	Reason why frequency changed

Alarm Severity

Severity	Critical
----------	----------

Description

This is a notification generated when operating frequency is changed for an AP radio due to either user triggers or events such as periodic DFS. The reason code can have a value of 0m, indicating that the reason is unspecified. The new channel ID is also provided.

Reason Code	Description
0	Triggered due to DFS
1	User triggered

Usage Guidelines

Informational log

Examples

```
Frequency Changed for Device ID AP_00-0A-F5-00-01-B6 radio 4 channelId 64
CauseCode 0
```

See Also**Wireless: STA association failed**

Notification that indicates the association failed for an 802.11 station

Syntax

```
"Station association failed for DeviceId %s radio %d station MAC %s station
status %d CauseCode"
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Radio	Radio interface ID on the AP
STA MAC Address	MAC address of 802.11 station
STA status	Association or reassociation
Cause Code	Reason why station association failed

Alarm Severity

Severity	Critical
----------	----------

Description

This is a notification generated when an association from an 802.11 station fails with the AP radio. The reasons for the failure are encapsulated in the cause code parameter and are as follows:

- 1 - Invalid parameters received from station in association request
- 2 - Only stations are allowed to associate with this AP based on current configuration
- 3 - Only backhauls can be formed with this AP based on current configuration
- 4 - Maximum backhaul limit is reached based on the 'Max Trunks' configuration for AP admission

criteria

- 5 - Maximum station limit is reached based on the 'Max Stations' configuration for SSID
- 6 - SSID received in association request does not match SSID in AP configuration. This can occur more often when the AP is not broadcasting SSID in beacon (either due to SSID being suppressed or multiple SSIDs being configured) and station is associating with an AP with a different SSID.
- 7 - Authentication and encryption requested by station does not match security policy of the AP
- 8 - Multi Vendor Station are not allowed to associate based on AP admission criteria
- 9 - 802.11b stations are not allowed to associate based on AP admission criteria
- 10 - Station is not allowed to associate and transferred to another AP Radio due to Load Balancing
- 11 - Station is not allowed to associate because node does not have network connectivity

Usage Guidelines

The reason for the association failure can be used to determine any configuration issue in the system that may be causing the association failures.

Examples

```
Station association failed for Device ID AP_00-0A-F5-00-01-B6 radio 4 station
MAC 00:0a:f5:00:3a:fe CauseCode 2
```

See Also

Wireless: STA associated

Notification that indicates the association and authentication was successful for an 802.11 station

Syntax

```
"Station associated for DeviceId %s radio %d station MAC %s, Station status %d
userId %s station count %d"
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Radio	Radio interface ID on the AP
STA MAC Address	MAC address of 802.11 station
STA status	Association or reassociation
User ID	Identifies user by user name or MAC address
Station Count	Current count of associated users with AP

Alarm Severity

Severity	Critical
----------	----------

Description

This is a notification generated when an association and authentication from an 802.11 station succeeds with the AP radio. In addition, count of current associated stations, type of association, and user ID is provided. User ID is user name if RADIUS authentication is used and MAC address otherwise.

Usage Guidelines

Informational log

Examples

```
Station associated for Device ID AP_00-0A-F5-00-01-B6 radio 4 station MAC
00:0a:f5:00:3a:fe, Station status 1 userId John Doe station count 10
```

See Also**Wireless: STA disassociated**

Notification that indicates an 802.11 station disassociated

Syntax

```
"Station disassociated from AP for DeviceId %s radio %d station MAC %s
CauseCode %d"
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Radio	Radio interface on the AP
STA MAC Address	MAC address of 802.11 station
Cause Code	Reason Code for disassociation

Alarm Severity

Severity	Critical
----------	----------

Description

This is a notification generated when an 802.11 station is disassociated either by the network or the station.

Description

Reason Code	Description
0	STA initiated disassociation
1	Station has handed off to another AP
2	Disassociation triggered due to authentication failure after ULAP timeout

Reason Code	Description
3	Disassociation triggered due to user action

Usage Guidelines

Informational log

Examples

```
Station disassociated for Device ID AP_00-0A-F5-00-01-B6 radio 4 station MAC  
00:0a:f5:00:3a:fe, CauseCode 0
```

See Also

Wireless: WDS failed

Notification that indicates a failure in formation of wireless backhaul

Syntax

```
"WDS trunk brought down for DeviceId %s radio %d remote MAC %s CauseCode %d"
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Radio	Radio interface ID on the AP
Remote MAC Address	MAC address of remote end of backhaul link
Cause Code	Reason code for WDS formation failure

Alarm Severity

Severity	Critical
----------	----------

Description

This is a notification generated when a wireless backhaul formation fails. The remote end's MAC address is provided. This notification is generated by AP node.

Reason Code	Description
0	System failure
1	Maximum BP count has been reached (this relevant only for AP)
2	Join attempt to the uplink AP failed (relevant only on BP side)

Usage Guidelines

This can be used to track any losses in connectivity of network.

Examples

```
WDS trunk brought down for Device ID AP_00-0A-F5-00-01-B6 radio 4 remote MAC
00:0a:f5:00:3a:fb, CauseCode 0
```

See Also

Wireless: WDS up

Notification that indicates successful formation of wireless backhaul

Syntax

```
"WDS trunk established for DeviceId %s radio %d remote mac %s TrunkPort count
%d CauseCode %d"
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Radio	Radio interface on the AP
Remote MAC Address	MAC address of remote end of backhaul link
Backhaul Count	Number of backhauls that are formed to this AP radio
Cause Code	Indicates whether backhaul was a retrunk or not

Alarm Severity

Severity	Critical
----------	----------

Description

This is a notification generated when a wireless backhaul formation succeeds. The remote end's MAC address is provided.

Reason Code	Description
0	Trunk has been established
1	Trunk has been optimized (re-established based on better connectivity)

Usage Guidelines

Informational log

Examples

```
WDS trunk established for Device ID AP_00-0A-F5-00-01-B6 radio 4 remote MAC
00:0a:f5:00:3a:fb TrunkPort count 2 CauseCode 0
```

See Also

Wireless: WDS down

Notification that indicates a wireless backhaul link has gone down

Syntax

```
"WDS trunk brought down for DeviceId %s radio %d remote MAC %s CauseCode %d"
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Radio	Radio interface on the AP
Remote MAC Address	MAC address of remote end of backhaul link
Cause Code	Indicates why backhaul link was brought down

Alarm Severity

Severity	Critical
----------	----------

Description

This is a notification generated when a wireless backhaul has gone down. The remote end's MAC address is provided.

Reason Code	Description
0	System reason (unspecified)
1	Loss of link (applies to BP side only)
2	Trunk brought down by uplink AP (applies to BP side only)
3	User retrunk issued (this can occur due to new backhaul configuration being applied on BP)
4	Trunk has reformed with another AP (AP side only)
5	Trunk brought down by BP (applies to AP side only)

Usage Guidelines

Informational log

Examples

```
WDS trunk brought down for Device ID AP_00-0A-F5-00-01-B6 radio 4 remote MAC 00:0a:f5:00:3a:fb CauseCode 0
```

See Also

Security: Guest authentication succeeded

Notification that indicates a Guest Access Station has been successfully authenticated

Syntax

```
"For device-id %s , Guest authentication succeeded for STA %s on radio %d with
SSID %s using captive portal %s and guest mode %d"
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Station	MAC address of the Guest STAtion
Radio	Radio interface on the AP
SSID	SSID on this AP with which the Guest has associated
Captive Portal	Landing page that has accomplished authentication of the Guest STA, either the internal landing page, or a URL identifying the external landing page that performed the authentication
Guest Mode	Currently, always set to 4.

Alarm Severity

Severity	Normal
----------	--------

Description

This notification is generated when a guest station is authenticated.

Usage Guidelines

This indicates the successful start of a guest access Stations communications session. This Guest STA will be offered the communications services specified in the Guest Profile that has been configured for the specified SSID.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , Guest authentication succeeded for STA
00:0a:f5:00:05:f0 on radio 0 with SSID NewYorkRoom using captive portal
Internal and guest mode 4
```

See Also

Security: Guest Authentication Failed

Security: Guest authentication failed

Notification that indicates a guest access station has failed authentication

Syntax

```
"For device id %s, Guest authentication failed for STA %s on radio %d with SSID %s
using captive portal %s and guest mode %d due to %d"
```

Alarm Parameters

DeviceId	The device ID of the AP
Station	MAC address of the Guest Station
Radio	Radio interface on the AP
SSID	SSID on the AP with which the guest has associated
Captive Portal	Landing page that has accomplished authentication of the Guest STA, either the internal landing page, or a URL identifying the external landing page that performed the authentication
Guest Mode	Currently, always set to 4.
Reason code	Currently, always set to 0

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when a guest station fails authentication.

Usage Guidelines

This indicates that a guest station did not present the appropriate “credentials” (currently simple password) upon request.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , Guest authentication failed for STA
00:0a:f5:00:05:f0 on radio 0 with SSID NewYorkRoom using captive portal
Internal and guest mode 4 due to 0
```

See Also

Security: Guest Authentication Succeeded

Security: User rejected by RADIUS server

Notification that indicates the AP has determined a user has been rejected by RADIUS

Syntax

```
"For device-id %s, the RADIUS SERVER %s:%d from auth zone %s rejected the STA
%s on radio %d with user-id %s and SSID %s"
```

Alarm Parameters

DeviceId	The device ID of the AP
RADIUS server	IP address of the RADIUS server

Port	The port used to communicate with the RADIUS server
Auth Zone	The name of the Auth Zone on this AP of which this RADIUS server is a member
Station	MAC address of the Station
Radio	Radio interface on the AP
User ID	The Username
SSID	SSID on this AP with which the station has associated

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when user authentication fails. The context of the AP radio and the RADIUS server that rejected the User are also provided.

Usage Guidelines

This indicates that the AP has determined that RADIUS has rejected a user authentication attempt.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812
from auth zone BldgOne rejected rejected the STA 00:0a:f5:00:05:cc on radio 0
with user-id paul and SSID NewYorkRm
```

See Also

Security: BP rejected by RADIUS server

Notification that indicates the AP has determined that a RADIUS server has rejected this BP's authentication attempt

Syntax

```
"For device-id %s, the RADIUS SERVER %s:%d from auth zone %s rejected the node
%s on radio %d with device-id %s and SSID %s"
```

Alarm Parameters

DeviceId	The device ID of the AP
RADIUS server	The IP address of the RADIUS server
Port	The port used to communicate with the RADIUS server
Auth Zone	The name of the Auth Zone on this AP of which this RADIUS server is a member

Node	The MAC address of the BP node
Radio	Radio interface on the AP
Device ID	The device ID of the BP node
SSID	SSID on the AP to which the station has associated

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when a Bridge Portal (radio) authentication fails. The context of the BP radio and the RADIUS server that rejected the BP radio are also provided. A BP attempts authentication when a wireless backhaul is being established.

Usage Guidelines

This indicates that a security portal has rejected a BP authentication attempt with this AP. Usually it means that the BP is not enrolled in the same network as the AP. It may also mean that the BP was just enrolled, and the enrollment database has not yet been synced across the network to all security portals.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812
from auth zone BldgOne rejected the node 00:0a:f5:00:06:22 on radio 0 with
device-id AP_00-0A-F5-00-01-89 and SSID NewYorkRm
```

See Also

Security: RADIUS server timeout

Notification that indicates the AP has determined that a RADIUS server has failed to respond within the RADIUS timeout

Syntax

```
"For device-id %s, the RADIUS server %s:%d from auth zone %s failed to respond
within %d seconds and %d attempts while authenticating STA %s on radio %d with
user-id %s and SSID %s"
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
RADIUS server	The IP address of the RADIUS server
Port	The port used to communicate with the RADIUS server.
Auth Zone	The name of the Auth Zone on this AP of which this RADIUS server is a member

RADIUS timeout	The current setting of the RADIUS timeout
RADIUS retries	The number of retries performed
Station	MAC address of the station
Radio	Radio interface on the AP
User	Supplicant user ID established during EAPOL Authentication exchange
SSID	SSID on the AP to which the station has associated

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when the RADIUS server fails to respond within a certain timeout period.

Usage Guidelines

This indicates that the AP has determined that a RADIUS server has failed to respond within the RADIUS timeout. This may mean that the RADIUS server is unreachable over the network, or the shared secret with the RADIUS server is mis-configured on the AP. Usually, RADIUS servers do not respond when clients attempt to communicate with bad shared secrets. If multiple RADIUS servers are configured in this auth zone, the AP will switch to using the next one in the list.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812
from auth zone BldgOne failed to respond within 5 seconds and 3 attempts while
authenticating STA 00:0a:f5:00:05:f0 on radio 0 with user-id paul and SSID
NewYorkRm
```

See Also

Security: Management user login success

Notification that indicates the AP has determined that a management user login has succeeded

Syntax

```
"For device-id %s, the management user '%s' with privilege level %d logged in
succesfully via %d"
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
----------	-------------------------------

Management User	Username of management user
Privilege Level	The privilege level of the management user (ignore in this release)
Login access	Type of access, console, or SSH (ignore in this release)

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated whenever a management user tries to log in to the local AP.

Usage Guidelines

This indicates that the AP has determined that a management user login has succeeded.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , the management user 'admin' with
privilege level 1 logged in successfully via 1
```

See Also

Security: Management User login failure

Notification that indicates the AP has determined that a management user login has failed

Syntax

```
"For device-id %s, the management user '%s' failed to login successfully via
%d"
```

DeviceId	The device ID of the Airgo AP
Management User	Username of management user.
Login access	Type of access, console, or SSH (ignore in this release)

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when a management user login attempt is unsuccessful.

Usage Guidelines

This indicates that the AP has determined that a management user login has failed. Too many failed logins in succession might indicate that someone is trying to break into your AP.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , the management user 'admin' failed to
login successfully via 1
```

See Also**Security: STA failed EAPOL MIC check**

Notification that indicates the AP has determined that a STA has failed a MIC check during the EAPOL authentication exchange

Syntax

```
"For device-id %s, the STA %s[%d] on radio %d with user-id %s and SSID %s
failed an EAPOL-MIC check with auth-type %d during key exchange %d. (If using
WPA-PSK, check the PSK on the STA.)"
```

DeviceId	The device ID of the Airgo AP
Station	The MAC address of the station
bpIndicator	BP (1) or a STA (0) supplicant
Radio	Radio interface on the AP
User	Supplicant user ID established during EAPOL authentication exchange
SSID	SSID on the AP to which the station has associated
Authentication Type	The valid types include: WPA PSK (3), WPA EAP (4)
Key Exchange	0 for pairwise key exchange, and 1 for group key exchange

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when the MIC fails during EAPOL key exchange process.

Usage Guidelines

This indicates that the AP has determined that a STA has failed a MIC check during the EAPOL authentication exchange. If the authentication type is WPA PSK and the failure happened during the pairwise key exchange, this is most likely due to a misconfiguration of the WPA pre-shared key on the station. Otherwise, it might mean that an attacker's station is attempting to masquerade as a legal station.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0
with user paul and SSID NewYorkRm failed an EAPOL-MIC check with auth-type 4
during key exchange 2. (If using WPA-PSK, check the PSK on the STA.)
```

See Also

Security: STA attempting WPA PSK – no pre-shared key is set for SSID

Notification that indicates the AP has determined that a STA is attempting WPA-PSK authentication, but no Pre-shared Key has been configured for the SSID

Syntax

```
"For device-id %s, the STA %s on radio %d attempted to do WPA-PSK based auth on the SSID %s but no pre-shared key is set."
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Station	The MAC address of the station
Radio	Radio interface on the AP
SSID	SSID on the AP to which the station has associated

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is sent when a Station attempts to do a WPA-PSK based authentication on a given SSID, but no WPA pre-shared key is set up for that SSID.

Usage Guidelines

This indicates that the AP has determined that a station is attempting to perform WPA-PSK authentication, but no WPA pre-shared key has been configured on this AP for that SSID. Recall that WPA-PSK is configured per SSID.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 on radio 0 attempted to do WPA-PSK based auth on the SSID NewYorkRm but no pre-shared key is set.
```

See Also

Security: Auth server Improperly configured on this SSID

Notification that indicates the AP has determined that a STA requires authentication servers and these are not configured properly on this SSID

Syntax

```
"For device-id %s, Auth servers are improperly configured for the SSID %s and are needed for authenticating STA %s on radio %d with RADIUS usage %d"
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
SSID	SSID on the AP to which the station has associated
Station	The MAC address of the station
Radio	Radio interface on the AP
RADIUS Usage	The RADIUS server required for: Legacy 8021.x for dynamic WEP (1), WPA EAP authentication (2), MAC address based ACL lookup (3)

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is sent when authentication servers are improperly configured for a given SSID.

Usage Guidelines

This indicates that the AP has determined that a STA requires authentication servers to be configured and there are none configured on this SSID. Generally authentication servers are needed for EA-based authentication, or for MAC address based ACL lookups.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , Auth servers are improperly configured
for the SSID NewYorkRm and are needed for authenticating STA 00:0a:f5:00:05:f0
on radio 0 with RADIUS 2
```

See Also

Security: STA failed to send EAPOL-start

Notification that indicates the STA has failed to send an EAPOL-Start even though it was expected for EAP based authentication

Syntax

```
"For device-id %s, the STA %s on radio %d and SSID %s failed to send an EAPOL-
Start in order to begin auth of type %d"
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Station	The MAC address of the station
Radio	Radio interface on the AP

SSID	SSID on the AP to which the station has associated
------	--

Authentication Type	LEGACY 802.1.x (2) or WPA EAP (4)
---------------------	-----------------------------------

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is sent during authentication when the station fails to send an EAPOL-Start in order to begin the authentication using WPA-EAP or legacy 802.1X protocols.

Usage Guidelines

This indicates that the AP has determined that a STA has failed to send an EAPOL-Start. This might indicate a misconfiguration on the STA. The AP expects the STA to send an EAPOL-Start if the authentication type is deemed to be EAP based. This can happen when WPA EAP authentication is negotiated, or when WEP is enabled on the AP and no manual WEP keys are configured.

Examples

For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 on radio 0 and SSID NewYorkRm failed to send an EAPOL-Start in order to begin auth of type 4

See Also

Security: RADIUS sent a bad response

Notification that indicates the AP has determined that a RADIUS server has sent a bad response

Syntax

"For device-id %s, the RADIUS server %s:%d sent back a bad response due to %d"

Alarm Parameters

DeviceId	The device ID of the AP
----------	-------------------------

RADIUS server	The IP address of the RADIUS server
---------------	-------------------------------------

Port	The port used to communicate with the RADIUS server.
------	--

Response	Reason codes: BAD SIGNATURE BASED ON SHARED SECRET (0), UNEXPECTED RESPONSE TYPE WHEN DOING EAP AUTH (1), UNEXPECTED RESPONSE TYPE WHEN DOING MAC-ACL LOOKUP (2), LEGAL MS-MPPE KEYS NOT PRESENT (3), BAD ENCODING FOR USER GROUP ATTRIBUTE (5)
----------	---

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is sent during authentication, when the RADIUS server sends a bad response. The aniNotifCauseCode identifies the reason associated with this bad response.

Usage Guidelines

This indicates that the AP has determined that a RADIUS server has sent a bad or unexpected response. The response could be bad because the cryptographic signature check might have failed or because an attribute might be missing or badly encoded.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812
sent back a bad response due to 7
```

See Also

Security: RADIUS timeout too short

Notification that indicates the AP has determined that a RADIUS server has sent a late response. This indicates that the AP RADIUS timeout might need to be increased

Syntax

```
"For device-id %s, the RADIUS server %s:%d sent a late response - you might
need to increase your RADIUS timeout of %d seconds"
```

Alarm Parameters

DeviceId	The device ID of the AP
RADIUS server	The IP address of the RADIUS server
Port	The port used to communicate with the RADIUS server
RADIUS timeout	The current setting of the RADIUS timeout

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when the AP receives a late response from the RADIUS server, as opposed to not receiving any response at all. The AP may have attempted multiple retries or may have switched to another RADIUS server by this time. This indicates that due to higher latencies in the network, it might be better to increase the timeout associated with the authentication server.

Usage Guidelines

This indicates that the AP has determined that a RADIUS server has sent a late response.

Examples

For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812 sent a late response - you might need to increase your RADIUS timeout of 4 seconds

See Also

Security: STA authentication did not complete in time

Notification that indicates the AP has determined that a station has failed to complete the proper sequence of authentication exchanges in a timely manner

Syntax

"For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not complete its auth sequence in time with auth-type %d and enc-type %d due to reason code %d"

Alarm Parameters

DeviceId	The device ID of the Airgo AP
AP	The MAC address of the upstream AP
Station	The MAC address of the station
bpIndicator	BP (1) or a STA (0) supplicant
Radio	Radio interface on the AP
User	Supplicant User ID, if exchanged the during EAPOL authentication
SSID	SSID on the AP to which the station has associated
Authentication Type	LEGACY 802.1x (2), WPA PSK (3), or WPA EAP (4)
Encryption Type	WEP-64 (1), WEP-128 (2), TKIP (5), or AES (6)
Reason Code	The reason for the failure: EAP-REQUEST NOT RECEIVED FROM AUTHENTICATION SERVER (2)

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when the station authentication sequence did not complete in time.

Usage Guidelines

This indicates that the AP has determined the station authentication sequence did not complete in time.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0
with user paul and SSID NewYorkRm did not complete its auth sequence in time
with auth-type 4 and enc-type 6 due to reason code 6
```

See Also

EAP User-ID timeout, EAP Response Timeout

Security: Upstream AP is using an untrusted auth server

Notification that indicates the local BP has determined that the upstream AP is using an un-trusted auth server

Syntax

```
"For device-id %s, the upstream AP %s with SSID %s authenticating via local BP
radio %d is using an untrusted auth server %s with certificate SHA-1
thumbprint %s : IT MIGHT BE A ROGUE AP"
```

Alarm Parameters

DeviceId	The device ID of the AP
AP	The MAC address of the upstream AP
SSID	SSID on the AP to which the station has associated
Radio	Radio interface on the AP
Node	The device ID (X.509 Certificate CN) of the entity used by the upstream AP as an auth server
Thumbprint	The SHA-1 thumbprint of the certificate for this purported portal

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when the local BP has determined that the upstream AP is using an untrusted auth server.

Usage Guidelines

This indicates that the local BP has determined the upstream AP is using an un-trusted auth server. This may indicate that the upstream AP is a rogue AP. It is safe to say that the upstream AP and the downstream AP are not enrolled in the same network. If the downstream AP was previously enrolled elsewhere, then reset it and re-enroll it in the new network.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , the upstream AP 00:0a:f5:00:06:22 with
SSID NewYorkRm authenticating via local BP radio 0 is using an untrusted auth
server 00:0a:f5:00:01:45 with certificate SHA-1 thumbprint
98:72:a8:6d:56:f8:92:a8:f3:97:ec:3f:fa:0b:66:4e : IT MIGHT BE A ROGUE AP
```

See Also

Security: Upstream AP is using a non-portal node as its auth server

Notification that indicates the local BP has determined that the upstream AP is using a non-portal node as an auth server

Syntax

```
"For device-id %s, the upstream AP %s with SSID %s authenticating via local BP
radio %d is using a non portal node %s with certificate SHA-1 thumbprint %s as
its auth server: YOUR ENROLLMENT DATABASE MIGHT BE OUT OF SYNC."
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
AP	The MAC address of the upstream AP
SSID	SSID on the AP to which the station has associated
Radio	Radio interface on the AP
Node	The device ID (X.509 Certificate CN) of the entity used by the upstream AP as an auth server
Thumbprint	The SHA-1 thumbprint of the certificate for this purported portal

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when the local BP has determined that the upstream AP is using a node that is not a security portal as its auth server. This indicates that the BP knows about the other Airgo Networks node, but does not believe it is authorized to be a Security Portal.

Usage Guidelines

This indicates that the local BP has determined that the upstream AP is out-of-sync with respect to the identity of legitimate portal APs and the enrollment databases are out of sync on the downstream AP and the upstream AP.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , the upstream AP 00:0a:f5:00:06:22 with
SSID NewYorkRm authenticating via local BP radio 0 is using a non portal node
00:0a:f5:00:01:45 with certificate SHA-1 thumbprint
98:72:a8:6d:56:f8:92:a8:f3:97:ec:3f:fa:0b:66:4e as its auth server: YOUR
ENROLLMENT DATABASE MIGHT BE OUT OF SYNC
```

See Also

Security: Upstream AP failed MIC check during BP authentication

Notification that indicates the local BP has determined that the upstream AP has failed a MIC check on a received frame

Syntax

```
"For device-id %s, the upstream AP %s with SSID %s authenticating via local BP radio %d failed an EAPOL-MIC check with auth-type %d during key exchange %d"
```

Alarm Parameters

DeviceId	The device ID of the AP
AP	The MAC address of the upstream AP
SSID	SSID on the AP to which the station has associated
Radio	Radio interface on the AP
Authentication Type	RSN PSK (3) or RSN EAP (4)
Key Exchange	Pairwise key exchange (0) or group key exchange (1)

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when the MIC fails during EAPOL key exchange process via a BP radio.

Usage Guidelines

This indicates that a frame with a MIC failure has been received during the EAPOL Key exchange process.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , the upstream AP 00:0a:f5:00:06:22 with SSID NewYorkRm authenticating via local BP radio 0 failed an EAPOL-MIC check with auth-type 4 during key exchange 3
```

See Also

Security: Premature EAP-success received

Notification that indicates the local BP has received an EAP-Success before authentication has completed

Syntax

"For device-id %s, the upstream AP %s with SSID %s authenticating via local BP radio %d sent EAP-Success before authentication completed : IT MIGHT BE A ROGUE AP"

Alarm Parameters

DeviceId	The device ID of the Airgo AP
AP	The MAC address of the upstream AP
SSID	SSID on the AP to which the station has associated
Radio	Radio interface on the AP

Alarm Severity

Severity	Critical
----------	----------

Description

Description: This notification is generated when an upstream AP sends an EAP success before authentication is completed. This may be a rogue AP trying to force an AP to join even before authentication is complete.

Usage Guidelines

This indicates that the local BP has received an EAP-success before authentication has even been completed.

Examples

For device-id AP_00-0A-F5-00-01-89 , the upstream AP 00:0a:f5:00:06:22 with SSID NewYorkRm authenticating via local BP radio 0 sent EAP-Success before authentication completed : IT MIGHT BE A ROGUE AP

See Also

Security: Profile not configured for user-group

Notification that indicates the AP has determined that a station is a member of a group for which a corresponding service profile has not been configured in this SSID

Syntax

"For device-id %s, the STA %s on radio %d with user %s is in group %s but SSID %s has no profile configured for that group"

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Station	The MAC address of the station
Radio	Radio interface on the AP
User	User ID
Group	Group tag for this user (determined from RADIUS configuration)
SSID	SSID on the AP to which the station has associated

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated during Station authentication when no service profile has been configured for a given Group.

Usage Guidelines

This indicates that the AP has detected a STA is authenticating that is a member of a group for which no service profile has yet been configured in this SSID.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:cc on radio 0
with user paul is in group employee but SSID NewYorkRm has no profile
configured for that group.
```

See Also

Security: STA has failed security enforcement check

Notification that indicates the AP has determined that a STA has failed the security enforcement checks for its service profile

Syntax

```
"For device-id %s, the STA %s on radio %d with user %s and SSID %s of group %s
failed the security enforcement check with auth-type %d and enc-type %d at
enforcement level %d"
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Station	The MAC address of the station
Radio	Radio interface on the AP

User	Supplicant User ID
SSID	SSID on the AP to which the station has associated.
Group	Group tag for this user (determined from RADIUS configuration)
Authentication Type	NONE (0), SHARED KEY (1), LEGACY EAP (2), RSN PSK (3), or RSN EAP (4)
Encryption Type	TNONE (0), WEP-64 (1), WEP-128 (2), TKIP (5), or AES (6)
Enforcement Level	The security enforcement level configured in the service profile: AES ONLY (1) TKIP OR AES (2), WEP ONLY (3), NO ENCRYPTION (4), DEFAULT ENFORCEMENT (5)

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated if the STA fails the security enforcement checks for its service profile.

Usage Guidelines

This indicates that the STA is attempting to use an encryption type that is not allowed in its service profile. The service profile is determined based on the SSID and user group of the STA. Note that the AP may advertise multiple encryption capabilities, but different STAs might be restricted to different subsets of encryption capabilities based on their service profiles.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:cc on radio 0
with user paul and SSID NewYorkRm of group employee failed the security
enforcement check with auth-type 4 and enc-type 5 at enforcement level 1
```

See Also

Security: AP detected bad TKIP MIC

Notification that indicates the AP has detected a BAD TKIP MIC value in an incoming frame encrypted with the pairwise/uniastr key

Syntax

```
"For device-id %s, a bad TKIP MIC was detected on an incoming unicast packet
from STA %s on radio %d"
```

Alarm Parameters

DeviceId	The device ID of the AP
Station	The MAC address of the station

Radio Radio interface on the AP

Alarm Severity

Severity Critical

Description

This notification is generated when a bad TKIP MIC is detected on an incoming frame from a STA that is encrypted with the pairwise/unicast key.

Usage Guidelines

This indicates that the AP has detected an invalid TKIP MIC value on an incoming frame. All packets received by the AP are always encrypted with the pairwise/unicast key.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected on an
incoming unicast packet from STA 00:0a:f5:00:05:cc on radio 0
```

See Also

Security: BP detected bad TKIP MIC on incoming unicast

Notification that indicates the BP has detected a BAD TKIP MIC value in an incoming frame from the AP that is encrypted with the pairwise/unicast key

Syntax

```
"For device-id %s, a bad TKIP MIC was detected by local BP radio %d on an
incoming unicast packet from the AP %s"
```

Alarm Parameters

DeviceId The device ID of the AP

Radio Radio interface on the AP

AP MAC address The MAC address of the source AP

Alarm Severity

Severity Critical

Description

This notification is generated when a bad TKIP MIC is detected by a local BP radio, identified by aniApRadioIndex, on an incoming unicast packet from the AP, where the packet is encrypted with the pairwise/unicast key.

Usage Guidelines

This indicates that the BP has detected an invalid TKIP MIC value on an incoming frame encrypted with the pairwise/unicast key.

Examples

For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected by local BP radio 0 on an incoming unicast packet from the AP 00:0a:f5:00:06:22

See Also

BP Detected Bad TKIP MIC on Incoming Multicast/Broadcast

Security: BP detected bad TKIP MIC on incoming multicast/broadcast

Notification that indicates the BP has detected a BAD TKIP MIC value in an incoming frame from the AP that is encrypted with the group/multicast/broadcast key

Syntax

"For device-id %s, a bad TKIP MIC was detected by local BP radio %d on an incoming multicast/broadcast packet from the AP %s"

Alarm Parameters

DeviceId	The device ID of the AP
Radio	Radio interface on the AP
AP MAC address	The MAC address of the source AP

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when a bad TKIP MIC is detected by a local BP radio, identified by aniApRadioIndex, on an incoming multicast or broadcast packet from the AP where the packet is encrypted with the group/multicast/broadcast key.

Usage Guidelines

This indicates that the BP has detected an invalid TKIP MIC value on a received multicast/broadcast frame.

Examples

For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected by local BP radio 0 on an incoming multicast/broadcast packet from the AP 00:0a:f5:00:06:22

See Also

BP Detected Bad TKIP MIC on Incoming Unicast

Security: STA detected bad TKIP MIC on incoming unicast

Notification that indicates a STA associated with this AP has detected a BAD TKIP MIC value in a frame it received from the AP encrypted with the pairwise/unicast key

Syntax

```
"For device-id %s, a bad TKIP MIC was detected by STA %s on radio %d on an incoming unicast packet from the AP"
```

Alarm Parameters

DeviceId	The device ID of the AP
Station	The MAC address of the station
Radio	Radio interface on the AP

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when a bad TKIP MIC is detected by an STA associated with this AP on an incoming unicast packet from the AP, where the packet is encrypted with the pairwise/unicast key.

Usage Guidelines

This indicates that the STA has detected an invalid TKIP MIC value on an incoming frame encrypted with the pairwise/unicast key.

Examples

```
For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected by STA 00:0a:f5:00:05:f0 on radio 0 on an incoming unicast packet from the AP
```

See Also

STA Deteted Bad TKIP MIC on Incoming Multicast/Broadcast

Security: STA detected bad TKIP MIC on incoming multicast/Broadcast

Notification that indicates a STA associated with this AP has detected a BAD TKIP MIC value in a multicast/broadcast frame it received from the AP

Syntax

```
"For device-id %s, a bad TKIP MIC was detected by STA %s on radio %d on an incoming multicast/broadcast packet from the AP"
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
----------	-------------------------------

Station	The MAC address of the station
---------	--------------------------------

Radio	Radio interface on the AP
-------	---------------------------

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when a bad TKIP MIC is detected by an STA associated with a radio, identified by aniApRadioIndex, on an incoming multicast or broadcast packet from the AP where the packet is encrypted with the group/multicast/broadcast key.

Usage Guidelines

This indicates that the STA has detected an invalid TKIP MIC value on a received, multicast frame.

Examples

For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected by STA 00:0a:f5:00:05:f0 on radio 0 on an incoming multicast/broadcast packet from the AP

See Also

STA Detected Bad TKIP MIC on Incoming Unicast

Security: TKIP counter-measures lockout period started

Notification that indicates the AP is taking active counter measures against an attempted compromise of TKIP.

Syntax

"For device-id %s, the TKIP counter-measures lockout period has started for 60 seconds."

Alarm Parameters

DeviceId	The device ID of the AP
----------	-------------------------

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when a TKIP counter measures lockout period for 60 seconds is started.

Usage Guidelines

This indicates that the AP has determined that an attempt is underway to compromise the secure operation of TKIP. This happens if two MIC failures are detected within a 60 second

interval. If this happens, the AP disassociates all STAs and prevents new STAs from associating for a period of 60 seconds.

Examples

For device-id AP_00-0A-F5-00-01-89 , the TKIP counter-measures lockdown period has started for 60 seconds.

See Also

Security: EAP user-ID timeout

Notification that indicates the STA has failed to respond in a timely manner with its user ID during the authentication exchange

Syntax

```
"For device-id %s, the STA %s[%d] on radio %d and SSID %s did not send its
user-id in time to complete its auth sequence with auth-type %d and enc-type
%d."
```

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Station	The MAC address of the station
bpIndicator	BP (1) or STA (0) supplicant
Radio	Radio interface on the AP
SSID	SSID on the AP to which the station has associated
Authentication type	TLEGACY 8021.x (2) or WPA EAP (4)
Encryption Type	WEP-64 (1), WEP-128 (2), TKIP (5), or AES (6)

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when an STA fails to send its user ID in time to complete its authentication sequence using the specified authentication type.

Usage Guidelines

This indicates the failure of a STA to complete the EAP authentication exchange in a timely fashion. The two authentication modes that require the STA to send its user ID are WPA EAP and legacy 8021.x for dynamic WEP. This trap might indicate that a user prompt is not attended to on the client side.

Examples

For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 and SSID NewYorkRm did not send its user-id in time to complete its auth sequence with auth-type 4 and enc-type 6

See Also

EAP Response Timeout, STA Authentication Timeout

Security: EAP response timeout

Notification that indicates the STA has failed to respond in a timely manner with an EAP response during the authentication exchange

Syntax

"For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not send an EAP-Response in time to complete its auth sequence with auth-type %d and enc-type %d"

Alarm Parameters

DeviceId	The device ID of the Airgo AP
Station	The MAC address of the station
bpIndicator	BP (1) or STA (0) supplicant
Radio	Radio interface on the AP
User	Supplicant user ID established during EAPOL Authentication exchange
SSID	SSID on the AP to which the station has associated.
Authentication type	LEGACY 802.1x (2) or WPA EAP (4)
Encryption Type	WEP-64 (1), WEP-128 (2), TKIP (5), or AES (6)

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when an STA fails to send an EAP response in time to complete its authentication sequence using the specified authentication type and encryption. This is an EAP response other than the User-ID.

Usage Guidelines

This indicates the failure of a STA to complete its EAP authentication exchange in a timely fashion. The two authentication modes that require the STA to send EAP responses are WPA EAP and legacy 802.1x for dynamic WEP. This trap might indicate that a user prompt is not attended to on the client side. It may also indicate that the client silently rejected a EAP request

sent from the RADIUS server – perhaps because it did not trust the RADIUS server's credentials.

Examples

For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm did not send an EAP-Response in time to complete its auth sequence with auth-type 4 and enc-type 6

See Also

EAP User-ID Timeout, STA Authentication Timeout

Security: EAPOL key exchange – message 2 timeout

Notification that indicates the STA has failed to respond in a timely manner with EAPOL 4-way handshake message number 2

Syntax

"For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not send the WPA EAPOL-Key Pairwise Messg #2 in time where auth-type %d and enc-type %d"

Alarm Parameters

DeviceId	The device ID of the AP
Station	The MAC address of the station
bpIndicator	BP (1) or STA (0) supplicant
Radio	Radio interface on the AP
User	User ID established during EAPOL Authentication exchange (if applicable)
SSID	SSID on the AP to which the station has associated
Authentication type	WPA PSK (3) or WPA EAP (4)
Encryption Type	TKIP (5) or AES (6)

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when an STA fails to send the WPA EAPOL-key Pairwise Message #2 in time to complete the pairwise key exchange.

Usage Guidelines

This indicates the failure of a STA to complete the EAPOL 4-way key exchange in a timely fashion.

Examples

For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm did not send the WPA EAPOL-Key Pairwise Messg #2 in time where auth-type 4 and enc-type 6

See Also**Security: EAPOL key exchange – message 4 timeout**

Notification that indicates the STA has failed to respond in a timely manner with EAPOL 4-way handshake message number 4

Syntax

"For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not send the WPA EAPOL-Key Pairwise Messg #4 in time where auth-type %d and enc-type %d"

Alarm Parameters

DeviceId	The device ID of the AP
Station	The MAC address of the station
bpIndicator	BP (1) or STA (0) supplicant
Radio	Radio interface on the AP
User	User ID established during EAPOL Authentication exchange (if applicable)
SSID	SSID on the AP to which the station has associated.
Authentication type	WPA PSK (3) or WPA EAP (4)
Encryption Type	TKIP (5) or AES (6)

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when an STA fails to send the WPA EAPOL-key Pairwise Message #4 in time to complete its authentication sequence with a radio, using the specified authentication type and encryption.

Usage Guidelines

This indicates the failure of a STA to complete the EAPOL 4-way key exchange in a timely fashion.

Examples

For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm did not send the WPA EAPOL-Key Pairwise Messg #4 in time where auth-type 4 and enc-type 6

See Also

Security: EAPOL Group 2 key exchange timeout

Notification that indicates the STA has failed to respond in a timely manner with EAPOL Group key exchange message number 2

Syntax

"For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not send the WPA EAPOL-Key Group Messg #2 in time where auth-type %d and enc-type %d"

Alarm Parameters

DeviceId	The device ID of the AP
Station	The MAC address of the station
bpIndicator	BP (1) or STA (0) supplicant
Radio	Radio interface on the AP
User	User ID established during EAPOL Authentication exchange (if applicable)
SSID	SSID on the AP to which the station has associated.
Authentication type	WPA PSK (3) or WPA EAP (4)
Encryption Type	TKIP (5) or AES (6)

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when an STA fails to send the WPA EAPOL-key group message #2 in time to complete its authentication sequence with a radio, using the specified authentication type and encryption.

Usage Guidelines

This indicates the failure of a STA to complete the group key exchange in a timely fashion.

Examples

For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm did not send the WPA EAPOL-Key Group Messg #2 in time where auth-type 4 and enc-type 6

L3 Mobility: Peer Mobility Agent Up

Notification which indicates that the local Mobility Agent has established contact with a peer Mobility Agent

Syntax

```
Device %s detected Layer-3 Mobility Agent %s/%d is up
```

Alarm Parameters

DeviceId	The device ID of the AP
MA IP Address	The IP Address of the peer Mobility Agent
MA IP Maskbits	The number of bits in the Mobility Agent's subnet mask

Alarm Severity

Severity	Critical
----------	----------

Description

This notification is generated when a peer Mobility Agent responds to keep-alives in a timely fashion.

Usage Guidelines

This indicates that the local Mobility Agent is able to communicate with the peer Mobility Agent.

Examples

```
Device AP_00-0A-F5-00-01-89 detected Layer-3 Mobility Agent 192.168.75.23/24  
is up
```

See Also

L3 Mobility: Peer Mobility Agent Down

L3 Mobility: Peer Mobility Agent Down

Notification that indicates that the local Mobility Agent has lost contact with a peer Mobility Agent

Syntax

```
Device %s detected Layer-3 Mobility Agent %s/%d is down
```

Alarm Parameters

DeviceId	The device ID of the AP
MA IP Address	The IP Address of the peer Mobility Agent
MA IP Maskbits	The number of bits in the Mobility Agent's subnet mask

Alarm Severity

Severity Critical

Description

This notification is generated when a peer Mobility Agent fails to respond to keep-alives in a timely fashion.

Usage Guidelines

This indicates that the local Mobility Agent is no longer able to communicate with the peer Mobility Agent.

Examples

Device AP_00-0A-F5-00-01-89 detected Layer-3 Mobility Agent 192.168.75.23/24 is down

See Also

L3 Mobility: Peer Mobility Agent Up

Glossary

This glossary defines terms that apply to wireless and networking technology in general and Airgo Networks products in particular.

802.1x

Standard for port-based authentication in LANs. Identifies each user and allows connectivity based on policies in a centrally managed server.

802.11

Refers to the set of WLAN standards developed by IEEE. The three commonly in use today are 802.11a, 802.11b, and 802.11g, sometimes referred to collectively as Dot11.

access control list (ACL)

A list of services used for security of programs and operating systems. Lists users and groups together with the access awarded for each.

access point (AP)

An inter-networking device that connects wired and wireless networks together. Also, an 802.11x capable device that may support one or more 802.11 network interfaces in it and coordinates client stations to establish an Extended Service Set 802.11 network.

Advanced Encryption Standard (AES)

An encryption algorithm developed for use by U.S. government agencies; now incorporated into encryption standards for commercial transactions.

ad-hoc network

A group of nodes or systems communicating with each other without an intervening access point. Many wireless network cards support ad-hoc networking modes.

authentication server

A central resource that verifies the identity of prospective network users and grants access based on predefined policies.

authentication zone

A administrative grouping of resources for user authentication.

backhaul

The process of getting data from a source and sending it for distribution over the main backbone network. Wireless backhaul refers to the process of delivering data from a node on the wireless network back to the wired network. Also referred to as WDS.x.

Basic Service Set (BSS)

The set of all wireless client stations controlled by a single access point.

bridge

A connection between two (or more) LANs using the same protocol. Virtual bridges are used as a means of defining layer 2 domains for broadcast messages. Each virtual bridge uniquely defines a virtual local area network (VLAN).

Class of Service (COS)

A method of specifying and grouping applications into various QoS groups or categories.

client utility

This application executes on a station and provides management and diagnostics functionality for the 802.11 network interfaces.

Differentiated Services Code Point (DSCP)

A system of assigning Quality of Service “Class of Service” tags.

Domain Name Service (DNS)

A standard methodology for converting alphanumeric Internet domain names to IP addresses.

Dynamic Host Configuration Protocol (DHCP)

A communications protocol enabling IP address assignments to be managed both dynamically and centrally. With DHCP enabled on a node (a system, device, network card, or access point), when it boots or is connected to a network, an address is automatically assigned. Each assigned address is considered to be “leased” to a specific node; when the lease expires, a new IP can be requested and/or automatically reassigned. Without DHCP, IP addresses would need to be entered manually for each and every device on the network.

dynamic IP address

A TCP/IP network address assigned temporarily (or dynamically) by a central server, also known as a DHCP server. A node set to accept dynamic IPs is said to be a “DHCP client.”

Extensible Authentication Protocol (EAP)

Standard that specifies the method of communication between an authentication server and the client, or supplicant, requesting access to the network. EAP supports a variety of authentication methods.

Extensible Authentication Protocol Over LAN (EAPOL)

Protocol used for 802.1x authentication.

EAP-TLS

EAP using Transport Layer Security. EAP-based authentication method based on X.509 certificates, which provides mutual, secure authentication. Certificates must be maintained in the authentication server and supplicant.

EAP-PEAP

Protected EAP-based authentication method based on X.509 certificates. Uses a two-phase approach in which the server is first authenticated to the supplicant. This establishes a secure channel over which the supplicant can be authenticated to the server.

Extended Service Set (ESS)

A set of multiple connected BSSs. From the perspective of network clients, the ESS functions as one wireless network; clients are able to roam between the BSSs within the ESS.

ESSID

Name or identifier of the ESS used in network configuration.

hostname

The unique, fully qualified name assigned to a network computer, providing an alternative to the IP address as a way to identify the computer for networking purposes.

Hypertext Transfer Protocol (HTTP)

Protocol governing the transfer of data on the World Wide Web between servers and browser (and browser enabled software applications).

Hypertext Transfer Protocol over SSL (HTTPS)

A variant of HTTP that uses Secure Sockets Layer (SSL) encryption to secure data transmissions. HTTPS uses port 443, while HTTP uses port 80.

Independent Basic Service Set (IBSS)

A set of clients communicating with each other or with a network via an access point.

Internet Protocol (IP)

The network layer protocol for routing packets through the Internet.

IP address

32-bit number, usually presented as a period-separated (dotted decimal) list of three-digit numbers, which identifies an entity on the Internet according to the Internet Protocol standard.

local area network (LAN)

A group of computers, servers, printers, and other devices connected to one another, with the ability to share data between them.

management information bases (MIBs)

A database of objects that can be monitored by a network management system. Both SNMP and RMON use standardized MIB formats that allows any SNMP and RMON tools to monitor any device defined by a MIB.

maskbits

Number of bits in the subnet prefix for an IP address, (provides the same information as subnet mask). Each triplet of digits in an IP address consists of 8 bits. To specify the subnet in maskbits, count the number of bits in the prefix. To specify using a subnet mask, indicate the masked bits as an IP address. Example: subnet mask 255.255.255.0 is equivalent to 24 maskbits, which is the total number of bits in the 255.255.255 prefix.

Media Access Control (MAC) address

A unique hardware-based equipment identifier, set during device manufacture. The MAC address uniquely identifies each node of a network. Access points can be configured with MAC access lists, allowing only certain specific devices to connect with the LAN through them, or to allow certain MAC-identified network cards or devices access only to certain resources.

MAC address authentication

Method of authenticating clients by using the MAC address of the client station rather than a user ID.

Network Address Translation (NAT)

The translation of one IP address used within a network to another address used elsewhere. One frequent use of NAT is the translation of IPs used inside a company, versus the IP addresses visible to the outside world. This feature helps increase network security to a small degree, because when the address is translated, it is an opportunity to authenticate the request and/or to match it to known, authorized types of requests. NAT is also used sometimes to map multiple nodes to a single outwardly visible IP address.

Network Interface Card (NIC)

Generic term for network interface hardware that includes wired and wireless LAN adapter cards, PC Cardbus PCMCIA cards, and USB-to-LAN adapters.

network management system (NMS)

Software application that controls a network of multiple access points and clients.

node

Generic term for a network entity. Includes an access point, network adapter (wireless or wired), or network appliance (such as a print server or other non-computer device).

Network Time Protocol (NTP)

NTP servers are used to synchronize clocks on computers and other devices. Airgo APs have the capability to connect automatically to NTP servers to set their own clocks on a regular basis.

Packet Internet Groper (PING)

A utility that determines whether a specific IP address is accessible, and the amount of network time (measured in milliseconds) needed for response. PING is used primarily to troubleshoot Internet connections.

policy-based networking

The management of a network with rules (or policies) governing the priority and availability of bandwidth and resources, based both on the type of data being transmitted and the privileges assigned to a given user or group of users. This allows network administrators to control how the network is used in order to help maximize efficiency.

Power over Ethernet (PoE)

Power supplied to a device by way of the Ethernet network data cable instead of an electrical power cord.

preamble type

The preamble defines the length of the cyclic redundancy check (CRC) block for communication between the access point and a roaming network adapter. All nodes on a given network should use the same preamble type.

Quality of Service (QoS)

QoS is a term encompassing the management of network performance, based on the notion that transmission speed, signal integrity, and error rates can be managed, measured, and improved. In a wireless network, QoS is commonly managed through the use of policies.

Remote Authentication Dial-In User Service (RADIUS)

A client/server protocol and software that enables remote access servers to communicate with a central server in order to authenticate users and authorize service or system access. RADIUS permits maintenance of user profiles in a central repository that all remote servers can share.

Radio Frequency (RF)

The electromagnetic wave frequency radio used for communications applications.

roaming

Analogous to the way cellular phone roaming works, roaming in the wireless networking environment is the ability to move from one AP coverage area to another without interruption in service or loss in connectivity.

rogue AP

An access point that connects to the wireless network without authorization.

Secure Shell (SSH)

Also known as the Secure Socket Shell, SSH is a UNIX-based command line interface for secure access to remote systems. Both ends of a communication are secured and authenticated using a digital certificate, and any passwords exchanged are encrypted.

Service Set Identifier (SSID)

The SSID is a unique identifier attached to all packets sent over a wireless network, identifying

one or more wireless network adapters as “belonging” to a common group. Some access points can support multiple SSIDs, allowing for varying privileges and capabilities based on user roles.

Secure Sockets Layer (SSL)

A common protocol for message transmission security on the Internet. Existing as a program layer between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers, SSL is a standard feature in Internet Explorer, Netscape, and most web server products.

Simple Mail Transfer Protocol (SMTP)

Protocol used to transfer email messages between email servers.

Simple Network Management Protocol (SNMP)

An efficient protocol for network management and device monitoring.

SNMP trap

A process that filters SNMP messages and saves or drops them, depending upon how the system is configured.

Spanning Tree Protocol (STP)

A protocol that prevents bridging loops from forming due to incorrectly configured networks.

Station (STA)

An 802.11-capable device that supports only one 802.11 network interface, capable of establishing a Basic Service Set 802.11 network (i.e., peer-to-peer network).

static IP address

A permanent IP address assigned to a node in a TCP/IP network.

subnet

A portion of a network, designated by a particular set of IP addresses. Provides a hierarchy for addressing in LANs. Also called a subnetwork.

subnet mask

A TCP/IP addressing method for dividing IP-based networks into subgroups or subnets (compare with maskbits). Each triplet of digits in an IP address consists of 8 bits. To specify using a subnet mask, indicate the masked bits as an IP address. To specify the subnet in maskbits, count the number of bits in the prefix. Example: subnet mask 255.255.255.0 is equivalent to 24 maskbits, which is the total number of bits in the 255.255.255 prefix.

Temporal Key Integrity Protocol (TKIP)

Part of the IEEE 802.11i encryption standard, TKIP provides improvements to WEP encryption, including per-packet key mixing, message integrity check, and a re-keying mechanism.

Traffic Class Identifier (TCID)

Part of the standard 802.11 frame header. The 3-bit TCID is used for mapping to class-of-service values.

Transmission Control Protocol/Internet Protocol (TCP/IP)

One of the most commonly used communication protocols in modern networking. Addresses used in TCP/IP usually consist of four triplets of digits, plus a subnet mask (for example, 192.168.25.3, subnet 255.255.255.0).

Transport Layer Security (TLS)

A protocol that provides privacy protection for applications that communicate with each other and their users on the Internet. TLS is a successor to the Secure Sockets Layer (SSL).

True MIMO™

The Airgo Networks, Inc. implementation of the data multiplexing technique known as Multiple Input Multiple Output (MIMO). MIMO uses multiple spatially-separated antennas to increase wireless throughput, range, and spectral efficiency by simultaneously transmitting multiple data streams on the same frequency channel.

Trunk

In telecommunications, a communications channel between two switching systems. In a wireless network, a trunk is a wireless connection from one Access Point to another.

Type of Service (ToS)

Sometimes also called IP Precedence, ToS is a system of applying QoS methodologies, based on headers placed into transmitted IP packets.

User Datagram Protocol (UDP)

A connectionless protocol similar to TCP/IP, but without the same level of error checking. UDP is commonly used when some small degree of error and packet loss can be tolerated without losing program integrity, such as for online games.

Virtual LAN (VLAN)

A local area network with a definition that addresses network nodes on some basis other than physical location or even whether the systems are wired together or operating using the same local equipment. VLANs are, on average, much easier to manage than a physically implemented LAN. In other words, moving a user from one VLAN to another is a simple change in software, whereas on a regular LAN, the computer or device would need to be connected physically to a different switch or router to accomplish the same thing. Network management software of some sort is used to configure and manage the VLANs on a given network.

Wired Equivalent Privacy (WEP)

Security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. Uses dynamically or manually assigned keys for encryption and authentication, as dictated by the capabilities of the client station. The WEP algorithms are vulnerable to compromise; therefore, WEP security is only recommended for legacy clients that do not support the newer generation security standards.

Windows Internet Name Server (WINS)

The Windows implementation of DNS, which maps IP addresses to computer names (NetBIOS names). This allows users to access resources by computer name instead of by IP address.

Wi-Fi

A play on the term “HiFi,” Wi-Fi stands for Wireless Fidelity, a term for wireless networking technologies.

Wireless Local Area Network (WLAN)

A type of local area network that employs radio frequencies to transmit data (usually encrypted), much like LANs transmit data over wires and fiber optic cables.

Index

Numerics

- 128-bit encryption 147
- 64-bit encryption 147
- 802.11
 - 802.11a,802.11b,802.11g 7
 - definition 321
 - extensions 74
 - mode in 2.4 GHz band 74
 - policy configuration 74
- 802.11i 12
- 802.1p 8
- 802.1Q 8
- 802.1x 12, 147, 321

A

- access control list (ACL) 321
- access points (APs)
 - beacon name 63, 141
 - candidate 141
 - components 27
 - configuration management 245
 - definition 321
 - description 1
 - enrollment 181
 - hostname 35
 - interfaces 105
 - introduction 1
 - mode, selecting 66
 - placement 29
 - rebooting 239
 - rogue 190
 - security 145
- access, open 152
- accessing
 - access points (APs) 33
 - NM Portal 47, 180
- ack mode 71
- activating DHCP server 207
- add to discovery database 201
- address resolution protocol (ARP)
 - table 108
- ad-hoc network 321
- Admin State 66
- administrative users 223
- administrator

- authentication 157
 - email address 39
 - password 39, 157
 - security 145, 157, 158
- admission
 - backhaul criteria 73
 - criteria 215, 286
 - multi-vendor criteria 73
- advanced
 - radio configuration 74
 - RADIUS parameters 163
- advanced encryption standard (AES)
 - definition 321
 - description 12
 - statistics 95
 - with WPA 151
- alarms
 - count 211
 - filter 219
 - ID 211
 - list and description 273
 - logging time 211
 - panel 40
 - summary 210, 211
 - table 210, 211
 - total 211
- AP. *see* access points (APs)
- ARP. *see* address resolution protocol (ARP) table
- assigning IP address to interface 129
- association status 93
- association status and type 92, 94
- asterisk next to field name 33
- authentication
 - diagnostics 159, 162
 - means 5
 - server 153, 321
 - status and type 92
 - timeout 163
 - user 12, 147
 - zones 14, 155, 321
- authorization state 187
- auto/manual identification 186
- auto-discovery 202
- automatic channel selection 69

- automatically generated
 - password 169, 174
- auto-select channel 63
- auto-sync database 204
- auxiliary manager 244

B

- background scanning 63
- backhaul
 - admission criteria 73
 - AP and BP radios 134
 - applications 133
 - authentication 133
 - candidate APs 141
 - configuration 133
 - definition 321
 - link criteria 138
 - security 136
 - trunk 135, 141
 - uplink criteria 140
 - viewing topology 184
- backhaul point (BP)
 - description 59
 - mode, selecting 66
- backup 245, 250
- backup/restore portal databases 206
- band 69
- basic rate set 75
- basic service set (BSS)
 - definition 321
 - type 188
- beacon
 - name 63, 141
 - period 77
- bootstrapping
 - AP 34
 - NM Portal 180
 - policy 198
 - security mode 37
- BP. *see* backhaul point (BP)
- br1 bridge name 107
- br4094 bridge name 107
- branch office installation 16
- Bridge and STP tab 106
- bridges

- definition 321
- details table 107
- forwarding table 107
- name prefix 107
- statistics 108
- bridging services 106
- broadcast SSID in beacon 86
- BSS. *see* basic service set (BSS)
- BSSID criteria 140
- burst ack 74
- buzzer 244, 245
- byte statistics 94

C

- cabling requirements 28
- campus installation 16
- candidate APs 141
- captive portal 167
- cell size and range management 4
- certificate 222
- channels
 - configuration 37, 44, 68
 - ID 185
 - list 69
 - management 4
 - selecting automatically 69
 - set 69
- choosing access point locations 27
- class 188
- class of service (COS)
 - assigning to packets 117
 - class order 118, 122
 - COS-to-TCID 120
 - definition 321
 - IP value 118
 - levels 6, 117, 120
 - mappings 6
 - overview 6
 - priority settings 6
 - values assigned to service
 - profile 88
- client LAN adapter 1
- client stations, managing 91
- Client Utility 322
- clock 45
- command conventions xi
- command line interface (CLI)
 - getting help 260
 - management support 8
 - using 259
- common problems and solutions 256
- compatibility status 82
- configuration
 - bridging services 106
 - DHCP server 206
 - interfaces 33, 128
 - network discovery 200
 - packet filters 126
 - portals 203
 - quality of service 117
 - RADIUS parameters 163
 - reports 247
 - resetting 249
 - SNMP 130
 - syslog 241
 - VLANs 111
 - wireless backhaul 138
 - zone privacy 164
- console port
 - command line interface (CLI)
 - access 260
 - connection 27
 - settings 260
- conventions, command xi
- COS. *see* class of service (COS)
- country code 44, 62
- coverage and capacity
 - requirements 10
- cyclic redundancy check (CRC)
 - block 324

D

- data encryption
 - options 147
 - overview 12
 - types of 5
- data rates supported 7
- date setting 36, 45
- default portal flag 187
- defaults
 - gateway 35, 36
 - SSID 83
 - VLAN 111, 114
- defer threshold 74
- delivery traffic indication message (DTIM) 77
- deployment environment 44, 63
- destination 185
- detection time 188
- device ID 183, 186
- DHCP. *see* dynamic host configuration protocol (DHCP)
- diagnostics authentication 162

- differentiated services code point (DSCP) 123, 322
- diffServ code point (DSCP)-to-COS mapping 118
- disassociating a station 93
- discovered radios 187
- discovery
 - configuration 200, 201, 202
 - interval 201
 - method 188
 - scope 202
 - seed 202
- discovery database, adding to 201
- domain name service (DNS)
 - and guest access 169
 - configuration 36
 - definition 322
 - IP address 241
- dot11 QoS 70, 73
- downlink statistics 94
- downloading software 251
- DSCP. *see* differentiated services code point (DSCP)
- DTIM. *see* delivery traffic indication message
- dynamic host configuration protocol (DHCP)
 - definition 322
 - IP address 241
 - lease 209
 - server
 - activating 207
 - configuration 206
 - use flag 35

E

- EAP-PEAP 147, 322
- EAP-TLS 147, 322
- egress COS 118, 120
- encapsulation configuration 130
- encryption type 92, 94
- encryption, open 147
- enhanced
 - data rates 8, 70, 73
 - rate set 74
- enrollment
 - database 216
 - description 12
 - factory default state 182
 - identifying rogue APs 145
 - identity information automatically entered 136

- implementing 181 to 184
- manual 146
- process 181
- server options 146
- status 205
- enrollment portals
 - description 4
 - flag 187
- enrollment state 187
- ESSID 322
- eth0 interface 105
- extended service set (ESS) 322
- extensible authentication protocol (EAP) 147, 322
- external landing page 56, 171
- external RADIUS server 153
 - settings 157

F

- factory default portal flag 187
- factory defaults
 - AP configuration 249
 - resetting radio 66
- fault management 210
- field asterisk 33
- filter
 - alarm 219
 - statistics 128
 - table 126
- filters 126
- fragmentation threshold 77

G

- gateway IP address 241
- generating bootstrap policy 198
- global radio configuration 61
- graph, link test 101
- group key retries 163
- group name 92
- guest access
 - configuration 173
 - external landing page 56
 - internal landing page 54
 - overview 7, 167
 - panel 174
 - security 145, 176
 - shared secret 56
 - task overview 15
 - URL 56
 - VLANs and 56, 173
 - wireless security and 173

- wizard 53
- guest password 169, 174
- guest service profile 173
- guest table 174

H

- hardware options 244
- help, command line interface 260
- highest node priority 140
- Home 180
- home panel 40
- hop count, lowest 140
- hostname 35, 322
- https download 253
- hypermode 70, 73
- hypertext transfer protocol (HTTP) 146, 322
- hypertext transfer protocol over SSL (HTTPS) 323

I

- IAPP. *see* Inter-Access Point Protocol (IAPP)
- IBSS. *see* independent basic service set (IBSS)
- ICMP ping 131
- IEEE802.1x 147
- independent basic service set (IBSS) 323
- ingress QoS 118, 119
- initializing
 - normal AP 35
 - portal AP 38
- installation
 - AP 28
 - planning 9
 - requirements 27
 - scenarios 16
- integration with existing network 8
- Inter-Access Point Protocol (IAPP)
 - configuration 95
 - service 96
 - statistics 98
 - topology 97
- interdependencies
 - channel configuration 72
 - global radio 67
- interface
 - configuration 128
 - statistics 130
 - tab 114

- table 129
- virtual 105
- interface-to-COS mapping 117
- internal landing page 54, 169
- internet protocol (IP)
 - configuration 240
 - definition 323
 - IP-DSCP tab 123
 - Precedence tab 126
 - precedence-to-COS mapping 117
 - Protocol tab 125
 - protocol-to-COS mapping 117
 - rogue discovery 190
 - routing
 - configuration 109
 - description 6
 - subnet criteria 140
 - topology 186
- IP address
 - assigning to interface 129
 - definition 323
 - link for AP 184
 - of AP 35

L

- landing page
 - description 167
 - external 171
 - internal 169
- large office installation 16
- lease time 207
- LEDs 30
- levels of COS 6
- license key 245
- license management 243
- link
 - criteria 138
 - statistics 93
 - test 100
 - test, adding 101
 - test, graph 101
- link statistics 93
- load balancing 74
- local area network (LAN) 323
- logging in to web interface 33
- logging module name 213
- logical interfaces 105
- long retry limit 77
- lowest hop count 140
- lowest weighted cost 140

M

- MAC address
 - association to AP 92
 - authentication 323
 - configuration 76
 - in topology window 186
- MAC-ACL users 225
- management
 - interface options 8
 - VLAN 111
- management information base (MIB) 130
- management IP address 241
- management portal
 - description 4
 - system requirements 27
- management VLAN 112
- managing
 - faults 210
 - users 221
- maskbits 323
- maximum number of leases 207
- media access control (MAC)
 - address 323
- menu tree 39, 180
- MIB. *see* management information base (MIB)
- mid-size office installation 16
- mobility management 4
- model number 47
- module name, logging 213
- multi domain support 44, 62
- multiple SSIDs 83, 90
- multiple VLANs 6

N

- NAT. *see* network address translation (NAT)
- navigating web interface 39
- neighbors 187
- network
 - connectivity parameters 62
 - default settings 105
 - density 62
 - discovery 200
 - information requirements 28
 - management 12, 179
 - radio neighbors 187
 - topology 181, 221
- network address translation (NAT) 323

- network density 37
- network interface card (NIC) 323
- network management system (NMS)
 - configuration 243
 - definition 323
- network time protocol (NTP) 324
 - server 207
- networking services 105
- NIC. *see* network interface card (NIC)
- NM Explorer Home panel 180
- NM Portal
 - access 47
 - features 179
 - initializing 38
 - supported services 4
- NM services 197
- NMS. *see* network management system (NMS)
- NMS-Professional
 - features 2, 179
 - interface options 8
- node 324
- normal AP 133
- NTP. *see* network time protocol (NTP)

O

- open access 152
- open encryption 147
- open security, quick-start option 37
- operating band 37
- operating bands 37, 44
- operational state 186
- options, hardware 244

P

- packet filters 126
- password authentication procedure (PAP) 157
- passwords
 - administrator 157
 - AP 183
- path selection criteria 140
- performance configuration 70, 73
- persona 66
- ping test 131
- planning your installation 9
- policy
 - bootstrapping 198
 - defining 198
 - management 197
 - table 197

- policy-based networking 324
- port number 155
- portal
 - architecture 4
 - configuration 203
 - database backup/restore 206
 - database version 204
 - secure backup 205
 - services overview 4
 - services, configured 187
 - table 204
- portal AP, initializing 38
- power over Ethernet (PoE) 29, 324
- power requirements 28
- preamble type 324
- primary manager 244
- problems and solutions 256
- product features 2
- product suite 1
- profile table 89
- protocols, data rates, and coverage 10
- PuTTY application 27

Q

- quality of service (QoS)
 - advanced features 121
 - class order 118, 122
 - definition 324
 - features 117
 - overview 6
 - statistics 121
 - task overview 15
 - user group-based 6
- Quick Start 34, 42

R

- radio
 - advanced configuration 74
 - channel configuration 68
 - configuration panel 60
 - diagnostics 99
 - discovered 187
 - interface 37, 44
 - neighbors 82, 187
 - operating band 37
 - resource management 4
 - state 77
 - statistics 77, 79
- radio frequency (RF) 324
- RADIUS. *see* Remote Authentication Dial-In User Service (RADIUS)

- rate adaptation 70, 73
 - real-time clock (RTC) 244, 245
 - rebooting AP 239
 - receiver rate adaptation 74
 - redundant security portal 204
 - regulatory and license information 263
 - Remote Authentication Dial-in User Service (RADIUS)
 - advanced configuration 163
 - definition 324
 - servers, list of 153
 - use of 147
 - remote authentication dial-in user service (RADIUS)
 - authentication zones 155
 - group attribute 163
 - server 155
 - server settings 157
 - with backhaul 133
 - remote MAC address 141
 - reporting AP 188
 - reports, configuration 247
 - required field 33
 - requirements
 - cabling 28
 - coverage and capacity 10
 - installation 27
 - network information 28
 - power 28
 - system 27
 - reset
 - AP 31
 - radio 66
 - to factory defaults 31
 - resetting
 - configuration 249
 - subsystems 249
 - to factory defaults 249
 - restore 206, 245, 250
 - re-trunk count 185
 - re-trunking 135
 - retry limits 77
 - retry statistics 94
 - roaming 324
 - rogue APs
 - definition 324
 - description 190
 - discovery 190
 - features 7
 - identifying 145
 - management overview 7
 - reasons for label 191
 - unclassified 191, 194
 - RTS threshold 77
- ## S
- scanning, background 63
 - scope/seed 201
 - secure backup of NM Portal 205
 - secure shell (SSH) 146, 259, 324
 - secure sockets layer (SSL) 325
 - security
 - access points (APs) 145
 - administrator 145, 157, 158
 - backhaul 136
 - certificate 222
 - data encryption 12
 - enforcement 88
 - enrollment 12
 - features 5
 - guest access 145
 - guest access and 176
 - mode 150
 - open 37
 - overview 11
 - statistics 93, 159
 - user 145
 - wireless 150
 - security portal
 - description 4
 - enrolling 183
 - flag 187
 - redundant 204
 - seed 201
 - selecting method 12
 - serial number 47
 - service profile 84
 - add or modify 90
 - bind to SSID 84
 - change binding 88
 - guest 173
 - SSID binding 88
 - task overview 15
 - service set identifier (SSID)
 - association 92
 - authentication 152
 - binding to service profile 88
 - broadcast in beacon 86
 - configuration 83
 - criteria 140
 - default 83
 - definition 324
 - details 87
 - example 83
 - information 85
 - max stations 85
 - multiple 7, 90
 - name 36
 - service profiles and 84
 - service type attribute 158
 - shared secret
 - authentication zones 155
 - for guest access 56
 - short retry limit 77
 - signal quality 188
 - signal strength 188
 - simple mail transfer protocol (SMTP)
 - community 131
 - definition 325
 - server 39
 - server address 46
 - trap 131
 - simple network management protocol (SNMP) 130, 146, 325
 - site surveys 11
 - small office installation 16
 - SMTP. *see* simple mail transfer protocol (SMTP)
 - SNMP. *see* simple network management protocol (SNMP)
 - software
 - distribution 254
 - distribution, cancelling 255
 - download status 255
 - downloading 251
 - image file 252
 - image recovery 256
 - upgrade 251
 - solutions to common problems 256
 - source
 - AP name 185
 - radio 185
 - spanning tree protocol (STP) 106, 107, 325
 - SSH. *see* secure shell (SSH)
 - SSID. *see* service set identifier (SSID)
 - SSL. *see* secure sockets layer (SSL)
 - standards supported 7
 - start discovery 201
 - state, admin 66
 - static IP address 325
 - station
 - definition 325
 - disassociating 93
 - link statistics 93
 - MAC address 94
 - management 91

- statistics
 - links 93
 - security 93
- statistics, supplicant 159, 160
- status of association 93
- STP. *see* spanning tree protocol (STP)
- subnet 325
- subnet mask 325
- supplicant statistics 159, 160
- supported standards and data rates 7
- syslog
 - configuration 241
 - viewing 220
- system
 - configuration, managing 240
 - requirements 27
- system-determined band 69

T

- tagged VLAN 112
- task roadmaps 14
- TCID. *see* traffic class identifier (TCID)
- TCP/IP. *see* transmission control protocol/internet protocol (TCP/IP)
- Telnet 27
- temporal key integrity protocol (TKIP) 151, 325
- TFTP download 254
- TFTP server 245, 250
- thumbprint 183, 186, 187
- time
 - discovered 186
 - setting 36, 45
 - zone setting 36, 45
- timeout statistics 94
- TLS. *see* transport layer security (TLS)
- ToS. *see* type of service (ToS)
- traffic class identifier (TCID) 117, 325
- transmission control protocol/internet protocol (TCP/IP) 325
- transport layer security (TLS) 325
- trap 131
- trunk
 - backhaul 135
 - definition 326
 - statistics 142
 - table 141
- type of service (ToS) 326

U

- UDP. *see* user datagram protocol (UDP)
- unauthenticated users 167
- unclassified rogue APs 191, 194
- unenroll an AP 184
- upgrading software 251, 252
- uplink
 - configuration 140
 - statistics 94
- URL for guest access 56
- user
 - authentication 12, 147
 - group 15, 87
 - name 92
 - VLAN 114
- user datagram protocol (UDP) 326
- user security 145
- user security wizard
 - description 47
 - open access 48, 52
 - WEP 48, 51
 - WPA-EAP 48
 - WPA-PSK 48, 50
- users
 - adding administrative users 223
 - adding MAC-ACL users 225
 - managing 221
 - unauthenticated 167
 - wireless 221
- using NM Portal 180

V

- vendor specific attribute 158
- verifying AP installation 30
- version table 47
- virtual local area network (VLAN)
 - 4094 bridge 107
 - assigned to service profile 87
 - definition 326
 - example 111
 - guest 173
 - guest access and 6, 56
 - ID 112, 114
 - interface 6
 - multiple 6
 - name 112
 - statistics 116
 - tag 112
 - task overview 15, 21, 23
 - user 6, 114

- VLAN-to-COS mapping 117

W

- walk test 103
- web browser
 - interface 8
 - logging in 33
 - navigating interface 39
- weighted cost, lowest 140
- WEP. *see* wired equivalent privacy (WEP)
- Wi-Fi 326
- Wi-Fi Protected Access (WPA)
 - description 12
 - quick-start option 37
- Windows internet name server (WINS) 326
- wired equivalent privacy (WEP)
 - definition 326
 - description 12
 - dynamic 147
 - encryption options 147
 - keys 37, 152
 - no authentication security 147
 - quick start options 37
 - security 152
 - statistics 95
- wireless
 - network example 9
 - security 150
 - users 221
- wireless backhaul
 - AP and BP radios 134
 - applications 133
 - candidate APs 141
 - configuration 138
 - direct AP connection 133
 - link criteria 138
 - security 136
 - trunks 135, 141
 - uplink criteria 140
 - viewing topology 184
- wireless local area network (WLAN) 326
 - adapter 1
- wireless rogue discovery 190
- wizard
 - guest access 53
 - user security 47
- WLAN. *see* wireless local area network (WLAN)
- wlan0 and wlan1 interfaces 105

- world mode
 - country code 44, 62
 - influence on channels 69
 - multi domain support 44, 62
- WPA security 151
- WPA-AES 147
- WPA-EAP 151
- WPA-PSK 147, 151
- WPA-PSK passphrase 37
- WPA-TKIP 147

Z

- zone privacy 164

