

# Authentication Commands

---

## General Authentication Commands

**aaa bandwidth-contract** *<name>*[kbits|mbits]*<rate>*

This command creates a bandwidth contract with the name specified in the name variable. Use the kbits|mbits parameter to specify the bandwidth. The rate variable must be an integer value between 0 and 65536 for kbits and 0 and 64 for mbits.

```
(Aruba5000) #configure t
Enter Configuration commands, one per line. End with CNTL/Z

(Aruba5000) (config) #aaa bandwidth-contract ?
STRING                               Name of bandwidth contract

(Aruba5000) (config) #aaa bandwidth-contract TestCon ?
kbits                                Specify bandwidth in kbits/second
mbits                                Specify bandwidth in mbits/second

(Aruba5000) (config) #aaa bandwidth-contract TestCon kbits ?
<0..65536>                            Bandwidth in kbits/seconds

(Aruba5000) (config) #aaa bandwidth-contract TestCon kbits 10

(Aruba5000) (config) #show aaa bandwidth-contracts

Bandwidth Contracts
-----
Name      Contract  Rate
----      -
TestCon  1          10240

(Aruba5000) (config) #
```

## **destination** <name> <address> [<netmask>] [**invert**]

This command is used to define a destination alias. The **no** form of the command may be used to delete the destination. However, if the destination is in use by an ACL the destination will not be deleted.

Use the **invert** option to allow all resources *except* the one specified in the arguments.

```
(Aruba5000) (config) # destination Internet 192.168.1.120 255.255.255.255
(Aruba5000) (config) #
```

## **net service** <name> {**tcp** | **udp**} *start-port* [*end-port*]

This command is used to define an alias for a service. The **no** form of the command may be used to delete an alias.

Variations:

- **net service** <name> **tcp** <port> [*end port*]
- **net service** <name> **udp** <port> [*end port*]
- **net service** <name> <protocol>

## **time-range**...

Variations:

- **time-range** <name> **absolute** [**no**] [**start** <start date> <start time>] [**end** <end date> <end time>]
- **time-range** <name> **periodic** <day type> <start time> **to** <end time>
- **time-range** <name> **periodic** <day of week> <start time> **to** [*day of week*] <end time>
- **time-range** <name> **periodic no weekday** <start time> **to** <end time>

Parameters:

*day type*

The following options can be specified:

- **Daily**
- **Weekday**
- **Weekend**

*day of week*

The following options can be specified:

- **Monday**
- **Tuesday**
- **Wednesday**
- **Thursday**
- **Friday**
- **Saturday**

## Role Sub-Mode

To modify a role, enter the Role Mode for a specific role as follows:

```
user-role <role name>
```

```
bandwidth-contract <contract_name> [per-user]
```

Assigns the bandwidth in *contract\_name* parameter to all the users within the current role, users share bandwidth. If the *per-user* key-word is specified, then each user in the role receives the entire bandwidth specified by the bandwidth contract.

```
(Aruba5000) (config-role) # bandwidth-contract TestCon per-user
```

```
dialer <dialer name>
```

Assigns the VPN dialer named by the *dialer name* variable to the current role.

```
[no] session-acl <session ACL name> [location <b.f.l>] [priority <number>]
```

Add the specified session ACL to the role. Use the *no* form of the command to remove the ACL from the role.

Use the *location* parameter to specify a building, floor, and location where the ACL will be applied. If the *location* parameter is not specified, then the ACL will be applied in all locations.

Use the *priority* parameter to specify the priority of the specified *session ACL name* in the list of ACLs configured for the current role. If no *priority* parameter is specified, then the ACL is added at the bottom of the list.

```
(Aruba5000) (config-role) # session-acl TestACL location 1.1.1 priority 4
```

```
pool [l2tp|pptp]<poolname>
```

This command assigns the pool specified in *poolname* to the current role. This command applies only to VPN authentication. Users authenticated in the current role will be assigned an address from the pool specified in *poolname*.

## **reauthentication-interval** <minutes>

This command specifies the interval in *minutes* after which the user must re-authenticate. Use the no form (no *reauthentication-interval*) to disable this function and allow the users in the current role to remain authenticated for an indefinite period of time. Specifying 0 minutes has the same effect as using the no form. The *minutes* variable is an integer.

## **vlan** <VLAN ID>

This command assigns the vlan specified by the *vlan\_id* variable to all users in the current role. The valid range for *vlan\_id* is 1 to 4096.

# IEEE 802.1x Commands

## **dot1x default**

The *dot1x default* command resets the dot1x state machine configuration to its default values.

## **dot1x max-req** <retry>

The *dot1x max-req* command sets the maximum number of attempts the server will make to authenticate a supplicant.

Default: 5

Valid Range: 0 - 10

## **dot1x multicast-keyrotation**

The *dot1x multicast-keyrotation* command enables the rotation of multicast keys. Multicast keys are used to encrypt multicast packets generated for each AP. Multicast keys are issued individually to each bssid tunnel.

Default: Disabled

## **dot1x re-authentication**

The *dot1x re-authentication* command enables the re-authentication of supplicants. Re-authorization occurs after a specific amount of time has elapsed from the last authentication. The time period is specified using the *dot1x timeout reauthperiod* command (see below). Unicast keys are updated after each re-authorization.

Default: Disabled

## **dot1x server**

The `dot1x server` commands are used for setting the back-end authentication server configuration.

### **dot1x server server-retry** *<retry>*

The `dot1x server server-retry` command sets the number of attempts the switch may make to obtain an authentication from the server.

Default: 2

Valid Range: 0 - 3

### **dot1x server server-timeout** *<timeout>*

The `dot1x server server-timeout` command sets the delay period between authentication retrys.

Default: 30 (seconds)

Valid Range: 1 - 65535

## **dot1x timeout**

The `dot1x timeout` commands are used for setting the periods of the timers used in the 802.1x authenticator.

### **dot1x timeout idrequest-period** *<IDR period>*

The `dot1x timeout idrequest-period` command sets the period between each identity request sent to the supplicant by the authenticator. The identity request is sent when a client associates or re-associates with an AP or when the re-authentication timer expires ( see *dot1x re-authentication*, above).

Default: 30 (seconds)

Valid Range: 1 - 65535

### **dot1x timeout mcastkey-rotation-period** *<MKR period>*

The `dot1x timeout mcastkey-rotation-period` command sets the time between each multicast key rotation. A key message is sent by the authenticator to all the stations associated with an AP at the expiration of the period.

Default: 1200 (seconds)

Valid Range: 1-4294967295

**dot1x timeout quiet-period** *<quiet period>*

The state machine enters a quiet period when authentication fails. The *dot1x timeout quiet-period* command sets the time interval during which the authenticator will make no attempt to acquire the supplicant.

Default: 60 (seconds)

Valid Range: 0 - 65535

**dot1x timeout reauthperiod** {*<RA period>* | **server**}

The *dot1x timeout reauthperiod* command sets the period between re-authorization and the last authorization. This period may also be driven by the *Session-Timeout* attribute from the authentication server.

Default: 60 (seconds)

Valid Range: 1-2147483647

# AAA Commands

## General AAA Commands

### aaa captive-portal

Keywords:

- `auth-server <name>`  
`[priority <pos_num>]` Specifies the authentication server to use.  
Use the name of the external RADIUS server configured using the `aaa radius-server` command (see [page 96](#)), or  
Use **Internal** for the internal WLAN switch database.
- `default-role <role_name>` Specifies the default role for all users authenticating via captive portal.
- `guest-logon` Enables users to logon as a guest. Use the `no` form of this keyword ( `no guest-logon`) to disable guest-logons.
- `user-logon` Enables registered users to logon. Default is enabled. To disable use the `no` form.
- `logout-popup-window` Enables the display of a small logout browser window for the user to log out from. The option is enabled by default.
- `protocol-http` Enables the use of HTTP for authentication. The default is HTTPS.
- `redirect-pause <seconds>` After the user authenticates, he/she is sent to the default welcome page (unless an alternate location is specified). This option causes the browser to pause for the specified number of seconds at the default *[internal]* welcome page before the user is redirected from the login page to the URL they originally requested.  
  
This option is only valid when used with the default *[internal]* welcome page.
- `welcome-page [internal | <location>]` After authentication the user is redirected to this webpage. If the default *[internal]* is specified, the `redirect-pause` option may be used.  
  
The default is the internal welcome page.

## **aaa derivation-rules {user|server <server-name>}**

This commands configures rules to derive user rules. Rules can be configured based on user attributes returned by the AP or user attributes returned by the authentication server subsequent to a successful user authentication.

```
(Aruba5000) (config) #aaa derivation-rules user
(Aruba5000) (user-rule) #
```

## **(user-rule) set role condition {bssid|encryption-type|ssid|location|macaddr}**

This set of commands are used to set the rules upon which a user is assigned a specific user role. Each condition has its own set of attributes and operators.

The user-rule option employs predetermined attributes which are described below.

Example.

```
(Aruba5000) (user-rule) #set role condition macaddr equals 00:03:2f:02:bc:4d
set-value employee
(Aruba5000) (user-rule) #
```

**BSSID attribute**

```
(Aruba5000) (user-rule) #set role condition bssid contains 01:02:03:04:05:06
set-value foo_user
(Aruba5000) (user-rule) #
```

*BSSID Operators:*

- contains
- ends-with
- equals
- not-equals
- starts-with

### encryption-type attribute

```
(Aruba5000) (user-rule) #set role condition encryption-type equals  
open set-value foo_role  
  
(Aruba5000) (user-rule) #
```

### *Encryption-type Operators:*

- equals
- not-equals

### *Encryption-type Operands*

- dynamic-tkip
- dynamic-wep
- open
- static-tkip
- static-wep

### ssid attribute

```
(Aruba5000) (user-rule) #set role condition ssid contains  
foo_ssid set-value foo_role  
  
(Aruba5000) (user-rule) #
```

### *SSID Operators:*

- contains
- ends-with
- equals
- not-equals
- starts-with

### location attribute

```
(Aruba5000) (user-rule) #set role condition location equals 1.1.1
set-value pubs_foo

(Aruba5000) (user-rule) #
```

#### *Location Operators:*

- equals
- not-equals

### macaddr attribute

```
(Aruba5000) (user-rule) #set role condition macaddr equals
01:02:03:04:05:06 set-value pubs_foo

(Aruba5000) (user-rule) #
```

#### *Macaddr Operators:*

- contains
- ends-with
- equals
- not-equals
- starts-with

# Access Control List Commands

---

## General ACL Commands

```
ip nat pool <name> <start_ip_addr> <end_ip_addr>
```

This command creates a named IP address pool with the start and end addresses specified by the *start\_ip\_addr* and *end\_ip\_addr* variables.

## Session ACL Mode

To add or modify a Session ACL, enter the Session ACL Mode for a specific ACL as follows:

```
ip access-list session <acname>
```

```
[no] <source> <destination> <port> <action> [<options>...]
```

Use this command to add a rule to the ACL. Use the **no** form of the command to remove a rule from the ACL.

Parameters:

*source* Source parameters are specified as follows:

- **alias** <source alias>
- **any**
- **host** <address>
- **network** <IP address> <subnet mask>
- **user**

*destination* Destination parameters are specified as follows:

- <string>
- **any**
- **host** <address>
- **network** <IP address> <subnet mask>
- **user**

*port*

Port parameters are specified as follows:

- *<IP protocol>*
- *<string>*
- **any**
- **tcp** *<port1>* [*<port2>*]
- **udp** *<port>* [*<port2>*]

*action*

Action parameters are specified as follows:

- **deny**
- **dst-nat** *<port>*
- **permit**
- **redirect** *<opcode>*
- **src-nat** {*<natpoolname>*} See [ip nat pool command, page 102](#).

*options*

Option parameters are specified as follows:

- **log**
- **time-range** *<name>*
- **queue** *<low|high>*
- **priority** *<number>*

# Intrusion Detection Commands

---

## **ids-policy mode [enable | disable]**

This command enables or disables the Intrusion Detection System. You may enter the wms: ids-policy mode by typing **ids-policy <cr>**.

```
(rbalay-master) (config) #ids-policy
(rbalay-master) (wms:ids-policy) #
```

## **adhoc-check [enable | disable]**

This command enables and disables ad-hoc checking functionality, which looks for adhoc networks within the range of any air monitor attached to the switch.

The adhoc-check feature is disabled by default and must be explicitly enabled using this command.

## **ap-flood-check [enable | disable]**

This command enables and disables ap-flood checking functionality in the air monitors attached to the switch.

The ap-flood-check feature is disabled by default and must be explicitly enabled using this command

## **ap-flood-inc-time <intervals>**

This command sets the maximum number of one second intervals that the ap count may exceed its limit before generating an ap-flood event.

## **ap-flood-quiet\_time <time>**

This command sets the time, in seconds, that the air monitor will wait after an ap-flood event has been generated before it resumes checking for ap-floods.

## **ap-flood-threshold <number>**

This function specifies the maximum number of spurious AP on the network.

### **ap-flood-wait-time** <time>

The time in seconds to wait after the air monitor initializes before checking for AP flood attacks.

### **dsta-check mode** [enable | disable]

This command enables or disables the IDS deauth station check functionality of the AirOS software on the Aruba 5000 switch.

### **eap-rate-threshold** <packets>

The maximum number of eap handshake packets that may be seen on a channel in the time interval specified by the *eap-rate-time-interval* command before an eap-rate event is generated.

### **eap-rate-time-interval**<time>

This command defines the length, in seconds, of the eap-rate-time-interval used in conjunction with the *eap-rate-threshold* command. The maximum value for the time argument is 300 seconds.

### **mac-oui-check** [enable | disable]

This command enables and disables the mac-oui-check feature. The feature checks the OUI (Organizationally Unique Identifier) of the MAC addresses of source or destination of frames seen by the air monitor. The function examines the packets for known valid OUIs.

### **rate-check mode** [enable | disable]

This command enables or disables the IDS rate anomaly check functionality of the AirOS software on the Aruba 5000 switch.

The rate-check function in the AirOS software checks for anomalous rates of the following frame types:

- Associate frames
- Dissassociate frames
- Authenticate frames
- De-authentication frames
- Probe request frames

- Probe response frames

## **rate-frame-type-param**

This command sets the parameters upon which a Frame Rate attack is detected. The arguments are the same for all 6 options .

### Options

- **assoc** This option specifies the parameters for the detection of an association frame rate attack.
- **auth** This option specifies the parameters for the detection of an authentication frame rate attack.
- **deauth** This option specifies the parameters for the detection of a de-authentication frame rate attack.
- **disassoc** This option specifies the parameters for the detection of a dis-association frame rate attack.
- **probe-request** This option specifies the parameters for the detection of a probe-request frame rate attack.
- **probe-response** This option specifies the parameters for the detection of a probe-response frame rate attack.

### Arguments

- **channel-inc-time** This argument specifies the maximum number of consecutive one second intervals that the channel-threshold argument may exceed its limit.  
  
If a threshold is exceeded for the number of consecutive one second intervals specified in this argument, the event is considered an anomaly and an event is generated.
- **channel-threshold** This argument specifies the maximum number of type specific frames on the channel in a one second interval.
- **node-threshold** This argument specifies the maximum number of type specific frames from an access point or station in a one second interval.

- **node-time interval** This argument specifies the maximum number of consecutive one second intervals that the note-threshold argument may exceed its limit.

If a threshold is exceeded for the number of consecutive one second intervals specified in this argument, the event is considered an anomaly and an event is generated.

### **rate-wait-time [enable | disable]**

The time in seconds to wait after the air monitor initializes before checking for rate anomalies.

### **sequence-check mode [enable | disable]**

This command enables or disables the IDS sequence check functionality of the AirOS software on the Aruba 5000 switch.

The sequence-check function of the AirOS software monitors the sequence number values of incoming frames for specific values, identifying known sequences generated by network penetration clients.

### **sequence-diff <number>**

### **sequence-time-tolerance <timediff>**

two packets from same source.... should be close together in time...if time is exceeded then the seq-diff check is not continued for (only) those two packets.

### **wbridge-check [enable | disable]**

This command enables and disables wireless bridge checking functionality, which looks for wireless bridges within the range of any air monitor attached to the switch.

The wbridge-check feature is disabled by default and must be explicitly enabled using this command.

## **signature-check mode [enable | disable]**

This command enables or disables the IDS signature analysis functionality of the AirOS software on the Aruba 5000 switch.

The signature-check function of the AirOS software examines packet payloads for known signatures of known network penetration tools, such as NetStumbler.