

Aruba 501 802.11ac Wireless Client Bridge Configuration and Administration Guide



a Hewlett Packard
Enterprise company

Part Number: 5200-3856
Published: June 2017
Edition: 1

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel[®], Itanium[®], Pentium[®], Intel Inside[®], and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft[®] and Windows[®] are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe[®] and Acrobat[®] are trademarks of Adobe Systems Incorporated.

Java[®] and Oracle[®] are registered trademarks of Oracle and/or its affiliates.

UNIX[®] is a registered trademark of The Open Group.

| | |
|---|-----------|
| Chapter 1 Deploying the Aruba 501 | 5 |
| Connecting wired devices to a wireless network | 5 |
| Connecting a wired device using MAC address cloning | 5 |
| Connecting a serial device to a wireless network | 6 |
| Chapter 2 Managing the Aruba 501 | 7 |
| Configuring web server settings | 7 |
| Web server configuration | 7 |
| Administrator login configuration | 8 |
| Managing HTTP SSL certificates | 8 |
| Configuring a management access control list | 10 |
| Configuring SNMP | 11 |
| Configuring SNMPv1 and SNMPv2 | 11 |
| SNMPv3 configuration | 14 |
| Supported MIBs | 16 |
| Automatically configuring the Aruba 501 | 17 |
| Setting the system time | 18 |
| Set system time | 18 |
| Daylight savings | 19 |
| Chapter 3 Wireless configuration | 20 |
| Wireless range | 20 |
| Configuring radio settings | 20 |
| Basic settings | 22 |
| Advanced radio settings | 22 |
| Using station profiles to establish a wireless link | 25 |
| To add or edit a station profile | 26 |
| Security methods | 28 |
| Configuring wireless bridging features | 31 |
| Configuring MAC address cloning | 31 |
| Redirecting unsupported traffic | 32 |
| Configuring frame processing settings | 32 |
| Viewing wireless information | 33 |
| Viewing nearby APs | 33 |
| Viewing wireless statistics for the radio | 34 |
| Viewing the MAC translation table | 35 |
| Chapter 4 Network configuration | 37 |
| IP configuration | 37 |
| IPv4 configuration | 37 |
| IPv6 configuration | 38 |
| Manual link speed settings | 39 |
| Network 802.1X feature descriptions | 40 |
| Viewing Ethernet statistics | 41 |
| TCP serial | 41 |
| TCP connection | 41 |
| Serial port settings | 42 |

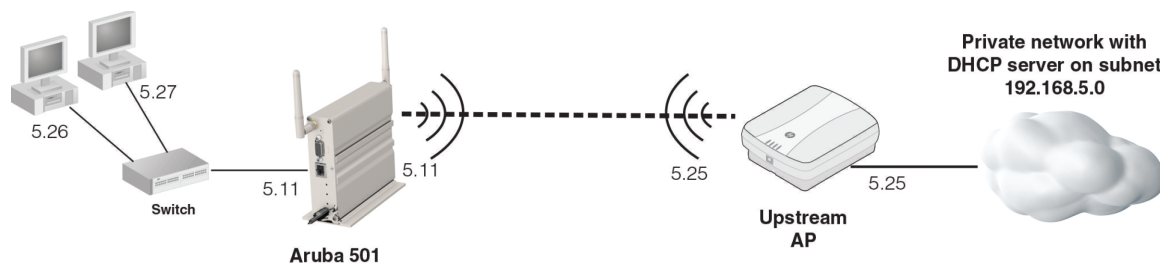
| | |
|---|-----------|
| Viewing TCP serial status and statistics..... | 43 |
| LLDP configuration..... | 44 |
| Loop protection..... | 45 |
| Viewing loop protection statistics..... | 45 |
| Chapter 5 Maintenance..... | 47 |
| Configuration file management..... | 47 |
| Software updates..... | 48 |
| System information..... | 49 |
| Chapter 6 Tools..... | 50 |
| System log..... | 50 |
| System log configuration..... | 50 |
| Remote syslog configuration..... | 51 |
| Events..... | 52 |
| RSSI log..... | 52 |
| Syslog message list..... | 54 |
| Email alert..... | 56 |
| General email alert configuration..... | 57 |
| Mail server configuration..... | 58 |
| Message configuration..... | 58 |
| Sending a test message..... | 58 |
| Viewing email alert status..... | 59 |
| Network trace configuration..... | 59 |
| Overview..... | 59 |
| Packet trace configuration..... | 59 |
| Packet file trace..... | 60 |
| Remote packet trace..... | 61 |
| Packet trace status..... | 63 |
| Packet trace file download..... | 63 |
| Ping..... | 64 |
| Iperf..... | 65 |
| Chapter 7 Websites..... | 67 |
| Chapter 8 Support and other resources..... | 68 |
| Accessing Hewlett Packard Enterprise Support..... | 68 |
| Accessing updates..... | 68 |
| Remote support..... | 68 |
| Warranty information..... | 69 |
| Regulatory information..... | 69 |
| Documentation feedback..... | 70 |
| Resetting to factory defaults..... | 71 |
| Factory reset procedures..... | 71 |
| Using the reset button..... | 71 |
| Using the management tool..... | 71 |

The Aruba 501 securely connects legacy Ethernet or serial communications devices to a wireless local area network (WLAN). It enables the deployment of legacy client devices, such as point-of-sale terminals, servers, and printers, in any location where a WLAN signal is available, thus eliminating the need to install a cabling infrastructure.

The following sections describe various deployment scenarios.

Connecting wired devices to a wireless network

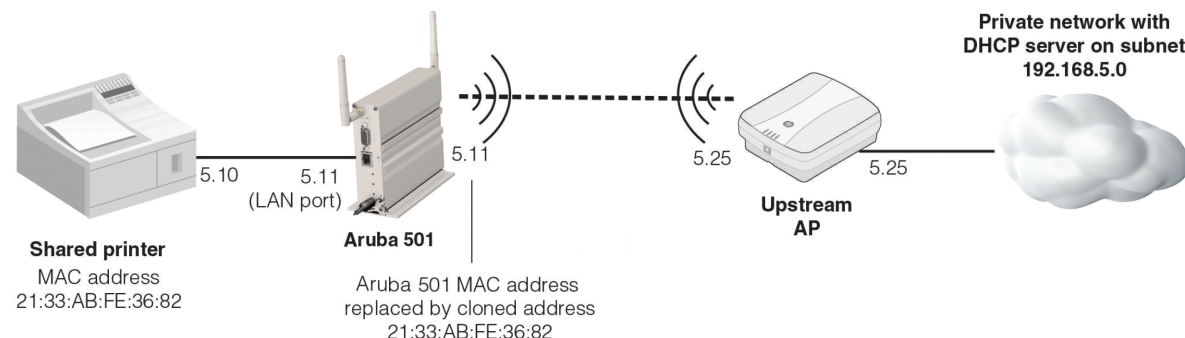
In this scenario, the Aruba 501 connects two wired computers to a private network via a wireless connection. The two computers are connected to a switch that is connected to the Ethernet port on the Aruba 501. A station profile is defined on the Aruba 501 with the name of the wireless network provided by the upstream AP, and the required credentials to log in. Once the Aruba 501 is connected to the private network, the computers obtain an IP address from the DHCP server and can then communicate with resources on the private network.



For configuration instructions, see [Using station profiles to establish a wireless link](#) on page 25.

Connecting a wired device using MAC address cloning

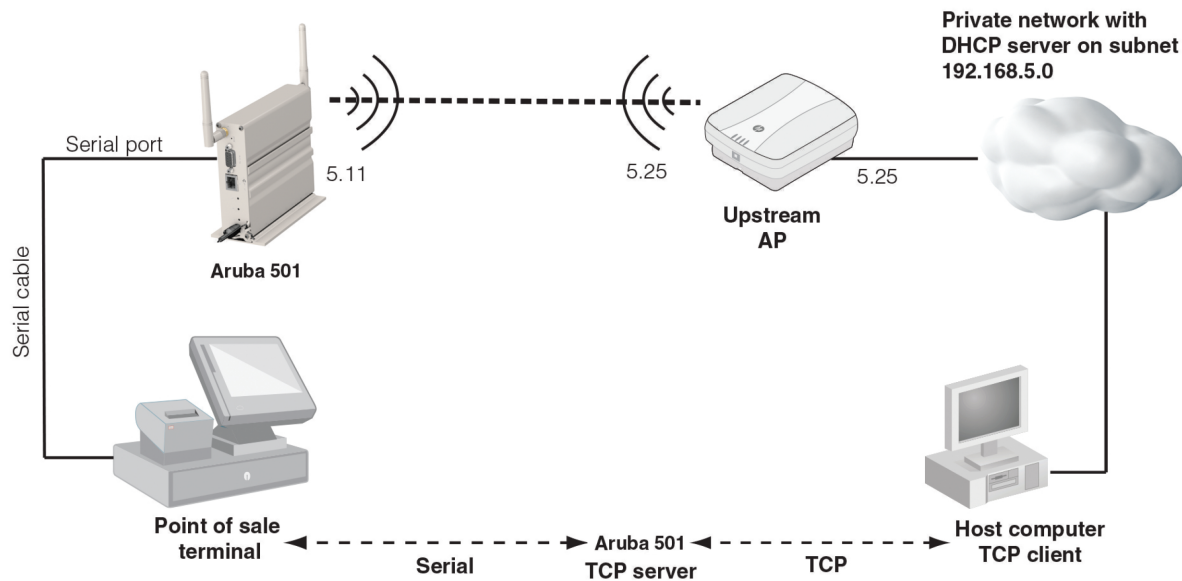
In this scenario, the Aruba 501 makes a wired printer available to clients on the upstream wireless network. Prior to this deployment, the printer's MAC address was known by users from its previous placement on a wired network. Although it is now available through a wireless connection, it is preferable for the wireless clients to continue accessing the printer using the MAC address, so that they do not need to change any settings. The MAC address cloning feature on the Aruba 501 is used to preserve the printer's network identity. With MAC address cloning, the Aruba 501 assigns the printer's MAC address to the Aruba 501 wireless port, making the Aruba 501 appear to be the printer on the upstream wireless network.



For configuration instructions, see [Configuring MAC address cloning](#) on page 31.

Connecting a serial device to a wireless network

TCP serial functionality allows devices that have no native Ethernet or wireless connectivity to access the network through a serial port. In this scenario, the Aruba 501 enables a point-of-sale terminal to exchange traffic with a remote host. The point-of-sale terminal is connected to the serial port on the Aruba 501. To connect it to a wireless network, the Aruba 501 converts traffic between the serial data format and TCP/IP.



For configuration instructions, see [TCP serial](#) on page 41.

The Aruba 501 is managed via its web-based management tool using Microsoft Internet Explorer 8 or later or Mozilla Firefox 17 or later. You can access the Aruba 501 management tool using either HTTP or HTTPS. Using HTTPS is more secure but you will see a security warning until you purchase and install your own certificate. With HTTPS, it is acceptable to choose the option that allows you to proceed through the security warning.

In a web browser, specify either: **http://192.168.1.1** or **https://192.168.1.1**. (By default, HTTP access is disabled and any access from HTTP is automatically redirected to HTTPS.)

For information on launching the management tool for the first time, see the **Aruba 501 802.11ac Wireless Client Bridge Quickstart**.

Configuring web server settings

Select **Management > Management tool** to open the **Configure web server settings** page.

You can configure the web server settings, change the user login name or password, and manage the certificate file required for secure HTTP communication.

Web server configuration

Use this section to configure web access to the management tool.

Web server configuration

| | |
|----------------------|---|
| HTTPS server status: | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| HTTP server status: | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| HTTP port: | <input type="text" value="80"/> (80, 1025-65535) |
| HTTPS port: | <input type="text" value="443"/> (443, 1025-65535) |
| Session timeout: | <input type="text" value="5"/> (1-1440) minutes |

Save

HTTPS server status/HTTP server status

The Aruba 501 software includes HTTP and HTTPS functionality to enable communication with your web browser. Unlike HTTP, HTTPS enables secure sessions using a digital certificate to encrypt data exchanged between the Aruba 501 and your web browser. By default, HTTPS is enabled and HTTP is disabled. When HTTP is disabled, requests from HTTP clients are redirected to use HTTPS.

The Aruba 501 supports only one management session at a time via HTTP or HTTPS.

HTTPS port/HTTP port

By default, the HTTP server uses the well-known logical port number 80 for communication with clients and the HTTPS port uses port number 443. You can specify different port numbers in the range 1025 to 65535 if the default ports are blocked or used for other protocols on your network.

Session timeout

If there is no activity on the management session for the specified time, then the administrator will be automatically logged off. The default timeout is 5 minutes.

Administrator login configuration

The Aruba 501 supports one administrator login. Use this section to change the username and password.

Administrator login configuration

| | | |
|-----------------------|------------------------------------|-----------------|
| Username: | <input type="text" value="admin"/> | 1-32 characters |
| Current password: | <input type="password"/> | |
| New password: | <input type="password"/> | 1-32 characters |
| Confirm new password: | <input type="password"/> | |

Save

Username

The default username is admin. The username can be from 1 to 32 alphanumeric characters including special characters.

Current password

The default password is admin.

New password and Confirm password

Specify a new password for the Aruba 501 administrator account.

The administrator password can be from 1 to 32 alphanumeric characters including special characters. The password cannot begin or end with a space. For security purposes, it is recommended that the password be at least 6 characters.



If you forget the administrator password, the only way to access the administrator account is to reset the Aruba 501 to factory default settings. See [Resetting to factory defaults](#) on page 71.

Managing HTTP SSL certificates

When HTTPS access is enabled, the Aruba 501 must be able to present a Secure Sockets Layer (SSL) certificate to the web browser of a computer that attempts access to the management tool. The certificate assures that the browser is accessing the Aruba 501 with the specified IP address. It also provides information that the Aruba 501 and management computer use to encrypt their communication.

A default certificate is present on the Aruba 501, based on the default device IP address 192.168.1.1. If you change the Aruba 501 IP address, you must update the certificate to reflect the new address; otherwise, a security warning will display at the start of each new management session. A certificate can also expire, requiring you to obtain a new one.

Generate certificate

Generate a new SSL certificate.

Generate

Certificate status

| | |
|---------------------------------|--------------------------|
| Certificate file present: | yes |
| Certificate expiration date: | Dec 31 00:40:08 2032 GMT |
| Certificate issuer common name: | CN=192.168.5.99 |

Save certificate

Save the current SSL certificate to a backup file.

Download method: ☒ HTTP ☐ TFTP

Download

Upload certificate

Upload a new SSL certificate.

Upload method: ☒ HTTP ☐ TFTP

HTTP SSL certificate file:

Upload

Generate certificate

You can generate a new certificate directly using the Aruba 501 management tool, or you can upload a certificate to the Aruba 501 from a computer or network location.

To generate a new certificate from the **Management tool** page, under **Generate certificate**, click **Generate**.

Certificate status

You can view the following information about the certificate in the **Certificate status** section of the **Management tool** page:

Certificate file present

Indicates whether an HTTP SSL certificate file is present (yes or no).

Certificate expiration date

The date that the HTTP SSL certificate file will expire.

Certificate issuer common name

The common name attribute of the server certificate. The common name is often the fully qualified domain name for the HTTP server, or the IP address equivalent.

Save certificate

You can save the current SSL certificate to a backup file.

Download method

Select a download method (HTTP or TFTP).

- **HTTP:** Select this option to save the certificate on a computer or network location.
- **TFTP:** Select this option to save the certificate on a TFTP server.

HTTP SSL certificate file

The file name of the certificate to be saved.

Server IP

The Server IP location to save the file.

Upload certificate

You can upload a new SSL certificate from another computer or network location:

Upload method

Select an upload method (HTTP or TFTP).

- **HTTP:** Choose this option if the certificate is located on a computer or network location.
- **TFTP:** Choose this option if the certificate is located on a TFTP server.

HTTP SSL certificate file

The file path and file name of the certificate to be uploaded.

Server IP

The Server IP location from which to upload the file.

Configuring a management access control list

You can create an access control list (ACL) that lists hosts that are authorized to access the Aruba 501 management tool. If this feature is disabled, anyone can access the management interface from any network client by supplying the correct user name and password.

Procedure

1. Select **Management > Management ACL** to open the **Management access control list configuration** page.

Management access control list configuration
?

Management access configuration

Management ACL control:
☐ Enabled
☒ Disabled

Allowed IPv4 addresses

Allowed IPv4 addresses:

Remove

IPv4 address:

Add

Allowed IPv6 addresses

Allowed IPv6 addresses:

Remove

IPv6 address:

Add

Save

- Under **Management ACL control**, select **Enabled**.
- Under **Allowed IPv4 addresses** and **Allowed IPv6 addresses**, enter an IPv4 address or IPv6 address and click **Add**. You can add up to five addresses to each list.
- Click **Save**.

Configuring SNMP

Simple Network Management Protocol (SNMP) defines a standard for recording, storing, and sharing information about network devices. SNMP facilitates network management, troubleshooting, and maintenance. The Aruba 501 supports SNMP versions 1, 2, and 3.

Key components of any SNMP-managed network are managed devices, SNMP agents, and a management system. The agents store data about their devices in management information bases (MIBs) and return this data to the SNMP manager when requested. Managed devices can be network nodes such as APs, routers, switches, bridges, hubs, servers, or printers.

Configuring SNMPv1 and SNMPv2

The Aruba 501 provides a robust SNMP v1/v2 implementation supporting both industry-standard MIB II objects and Aruba-specific MIB objects. Read-only or read/write access is supported.

Select **Management > SNMP** to open the **SNMP configuration** page.

SNMP configuration
?

System settings

System name: CN43G5W04G
System location:
System contact:

SNMP configuration

SNMP: ☒ Enabled ☐ Disabled
Read-only community name: public
Port number: 161 (161, 1025-65535)
SNMP set requests: ☒ Enabled ☐ Disabled
Read-write community name: private
SNMP source enable: ☐ Enabled ☒ Disabled
Hostname, address, or subnet:
IPv6 hostname, address, or subnet:

Trap destinations

Community name for traps:

| Enabled | Host Type | Hostname or IP Address |
|--------------------------|-----------|------------------------|
| <input type="checkbox"/> | IPv4 ▼ | |
| <input type="checkbox"/> | IPv4 ▼ | |
| <input type="checkbox"/> | IPv4 ▼ | |

Save

System settings

Under **System settings**, you can define basic properties of the Aruba 501 as an SNMP managed device.

System name

Enter a name to identify the Aruba 501 as an SNMP managed device (63 alphanumeric characters maximum). The default SNMP name is the product serial number.

System location

Enter a description of the physical location of the device (255 alphanumeric characters maximum).

System contact

Specify an email address for a contact person for the Aruba 501 (255 alphanumeric characters maximum).

SNMP configuration

You can configure the following settings in this section. Unless specifically noted, these configuration parameters apply to SNMPv1 and SNMPv2c only.

SNMP

Select a button to enable or disable the SNMP agent. By default, the SNMP agent is enabled. If you disable the agent, the Aruba 501 will not respond to SNMP requests.

Read-only community name

The community name acts as a simple authentication mechanism to restrict the devices on the network that can request data from the device. The name functions as a password, and the request is assumed to be authentic if the sender knows the password.

The valid range is 1 to 256 characters. The community name can be in any alphanumeric format. The default is **public**.

Port number

By default, the Aruba 501 listens to requests from port 161 only. You can configure to another value in the range of 1025 to 65535.

SNMP set requests

When **SNMP set requests** is enabled, SNMP manager devices on the network can make changes to the Aruba 501 configuration by issuing “set” requests for MIB objects. When disabled, SNMP manager devices can only retrieve configuration information by issuing “get” requests for MIB objects. This is enabled by default.

Read-write community name

If you have enabled **SNMP set requests**, you can set a read-write community name.

Setting a community name is similar to setting a password. Only requests from devices that identify themselves with this community name will be accepted.

The valid range is 1 to 256 characters. The community name can be in any alphanumeric format. The default is **private**.

SNMP source enable

Select **Enabled** if you want to restrict the source of permitted SNMP requests to a specified IP address, hostname, or subnet. When disabled, the Aruba 501 accepts requests from any device on the network that is configured with the appropriate community name. It is disabled by default.

Hostname, address, or subnet

If you have enabled the **SNMP source enable** setting, specify the hostname or IPv4 address of a device to enable it to execute get and set requests to the Aruba 501. Or, specify a subnet to enable SNMP access for any device on that subnet.

The valid range is 1 to 256 characters.

As with community names, this setting provides a level of security on SNMP accesses. The SNMP agent accept requests only from the specified device or subnet.

To specify a subnet, enter one or more subnetwork address ranges in the form **address/mask_length**, where **address** is an IP address and **mask_length** is the number of mask bits. Both formats **address/mask** and **address/mask_length** are supported. Individual hosts can also be specified in this manner. For example, a range of 192.168.1.0/24 specifies a subnet with address 192.168.1.0 and a subnet mask of 255.255.255.0. In this example, devices with addresses from 192.168.1.1 through 192.168.1.254 can execute SNMP commands on the Aruba 501. (The address identified by the suffix .0 is reserved for the subnet address, and the address identified by .255 is reserved for the broadcast address).

As another example, if you enter a range of 10.10.1.128/25, machines with IP addresses from 10.10.1.129 through 10.10.1.254 can execute SNMP requests on managed devices. In this example, 10.10.1.128 is the network address and 10.10.1.255 is the broadcast address. A total of 126 addresses are designated.

IPv6 hostname, address, or subnet

Specify the DNS hostname, address, or subnet of the IPv6 devices that can execute get and set requests to the Aruba 501.

Trap destinations

The Aruba 501 generates and stores data about significant events, such as system errors and configuration changes, in the form of SNMP traps. These traps can be forwarded to up to three SNMP manager devices, which you can configure in the Trap destinations section of the page.

Community name for traps

Enter the global community string associated with SNMP traps. Traps sent from the device provide this value as a community name.

The valid range is 1 to 256 characters. The community name can be in any alphanumeric format. Special characters are not permitted.

Enabled

Enable this option to allow configuration of up to three devices to receive traps.

Host type

Select whether the devices use an IPv4 or IPv6 address.

Hostname or IP address

Specify the hostname or IP address of the selected type.

SNMPv3 configuration

SNMPv3 adds security in the form of configurable encryption of data and enhanced authentication of users. You can configure security settings on a per-user basis. You can also configure a user as an SNMPv3 receiver, so that the Aruba 501 sends SNMP trap messages to the user.

Configuring SNMPv3 users

The **SNMPv3 users** page enables the network administrator to define multiple user IDs with different privileges and security levels. A user can be configured to have read or write access with either authentication or encryption or both. Users can also be configured to receive SNMP notifications from the Aruba 501.

To configure SNMPv3 users:

Procedure

1. In the management tool, select **Management > SNMPv3 users**.

SNMPv3 user configuration
?

SNMPv3 user list:

Remove

SNMPv3 user parameters:

| | | | | | | |
|----------------------|-------------|-----------|----------------------|-----------------|----------------------|-----|
| Name | Group level | Auth type | Auth key | Encryption type | Encryption key | |
| <input type="text"/> | RO ▼ | MD5 ▼ | <input type="text"/> | DES ▼ | <input type="text"/> | Add |

Save

2. Enter a **Name**. User names can contain up to 32 alphanumeric characters.
3. Select a **Group level**. The built-in group levels are read-only (**RO**) and read-write (**RW**).
4. Select the type of authentication to use on SNMP requests from the user:
 - **MD5**: Require MD5 authentication on SNMPv3 requests from the user.
 - **None**: SNMPv3 requests from this user require no authentication.
5. If you specified MD5 authentication, enter a value in **Auth key** box. The authentication key can be from 8 to 32 alphanumeric characters.
6. From the **Encryption type** list, select the type of privacy to use on SNMP requests from the user:
 - **DES**: Use DES encryption on SNMPv3 requests from the user.
 - **None**: SNMPv3 requests from this user are not encrypted.
7. If you specified DES encryption, enter a value in the **Encryption key** box. The encryption key can be from 8 to 32 alphanumeric characters.
8. Click **Add**. You can add up to eight SNMPv3 users.
9. When finished adding users, click **Save**.

To remove a configured SNMPv3 user, select the name in the SNMPv3 user list, and then click **Remove**.

Configuring SNMPv3 receivers

The Aruba 501 can send SNMP traps to configured SNMPv3 users. The eligible users must be configured on the **SNMPv3 users** page. On the **SNMPv3 receivers** page, you provide IP information for the users you select to receive traps.

To configure an SNMPv3 receiver:

- In the management tool, select **Management > SNMPv3 receivers**.

SNMPv3 notification receivers
?

SNMPv3 receiver list:

Remove

SNMPv3 receiver parameters:

IPv4/IPv6 address
Port
Users
Add

Save

- In the **IPv4/IPv6 address** field, enter the IP address where the trap will be sent.
- In the **Port** box, enter the logical UDP port number to associate with SNMP receiver messages.
- From the **Users** list, select the user to associate with this IP address and port, and then click **Add**. You can add up to eight receivers.
- When you are finished adding receivers, click **Save**.

To remove a configured SNMPv3 receiver, select the name in the SNMPv3 receiver list, and then click **Remove**.

Supported MIBs

The Aruba 501 supports the following MIBs and MIB objects:

Standard MIBs

The following standard MIBs are supported:

- | | |
|-------------------------|---------------------------|
| • BRIDGE-MIB (802.1d) | • SNMP-USM-DH-OBJECTS-MIB |
| • ENTITY-MIB (RFC 2737) | • SNMPv2-CONF |
| • IANAIfType-MIB | • SNMPv2-MIB (RFC 2418) |
| • IEEE802dot11-MIB | • SNMPv2-SMI |
| • IF-MIB | • SNMPv2-TC |
| • INET-ADDRESS-MIB | • SNMPv2-TM |
| • RFC1155-SMI | • RFC4688 |
| • RFC1213-MIB | • IP-MIB |
| • RFC1215 | • TCP-MIB |
| • SNMP-FRAMEWORK-MIB | • UDP-MIB |
| • SNMP-NOTIFICATION-MIB | • UCD-SNMP-MIB |
| • SNMP-TARGET-MIB | |

Private MIBs

The Aruba 501 supports a private MIB named HP-WLAN-ACCESS-POINT-MIB, with the following organization and contact information:

ORGANIZATION:

Hewlett Packard Enterprise

CONTACT-INFO:

Hewlett Packard Enterprise, 8000 Foothills Blvd. Roseville, CA 95747

This private MIB is linked to the product MIB tree at:

1.3.6.1.4.1.11.2.14.11.6.4.5.1

(iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).hp(11).nm(2).icf(14).hpicfObjects(11).hpicfAccess(6).hpWireless(4).hpWlanProducts(5).hpWlanProduct(1)).

The Aruba 501 sysOID value is:

1.3.6.1.4.1.11.2.3.7.11.162.1

(iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).hp(11).nm(2).hpSystem(3).netElement(7).hpEtherSwitch(11).hpWlan(162).hpWlanClientBridge501(1)).

Automatically configuring the Aruba 501

This task explains how to automatically configure an Aruba 501 at startup with no user intervention using DHCP options 43 and 60. Automatic configuration is supported via both the Ethernet port and wireless port.

Prerequisites

- DHCP server that supports options 43 and 60.
- TFTP server.

Procedure

1. Login to the management interface on the Aruba 501 and define the configuration settings needed to successfully deploy the Aruba 501 on your network. (You can further customize these settings later by directly editing the configuration file.)
2. Select **Maintenance > Config file** and save the configuration file to your computer.
3. Edit the configuration file to customize settings as required. The configuration file is an XML document and can be edited with an ASCII text editor (or XML editor, if you have one). If you alter the structure of the file, or define settings that are invalid, the file will be rejected and the configuration settings ignored when it is downloaded by the Aruba 501. A message is written to the log indicating the errors that occur. The following configuration settings are not overwritten when the new configuration file is loaded:
 - serial number
 - mac address
 - system name
 - hostname
4. Configure the DHCP server as follows:
 - Set the Vendor Class Identifier to **Aruba 501 Wireless Client Bridge**.
 - Set sub-option 4 to the IP address of the TFTP Server.
 - Set sub-option 5 to the full path and filename of the configuration file on the TFTP server.
5. Copy the configuration file to the TFTP server in the appropriate directory.
6. Connect the Aruba 501 to the same network as the DHCP server via either the Ethernet port or a wireless connection. To use a wireless connection, you must define a station profile that matches the settings on the wireless network. The Aruba 501 ships with a default network profile that automatically connects to a wireless network with SSID **Aruba 501** and WPA2/PSK key **Aruba 501 Client Bridge**. To modify the default station profile, see **Using station profiles to establish a wireless link** on page 25.
7. Restart the Aruba 501.
 - a. On start up, the Aruba 501 sends an optional parameter, called the Vendor Class Identifier (Option 60) in its DHCP request with a value of **Aruba 501 Wireless Client Bridge**. This request is sent on the Ethernet port and the connected wireless network.
 - b. The DHCP Server checks its configuration settings to find a match for the Option 60 value. If found, it sends a DHCP reply with the name of the configuration file and the IP address of the TFTP server on which it is stored (as part of Option 43).

- c. The Aruba 501 uses the Option 43 values to download the new configuration file.
- d. The Aruba 501 checks that the new configuration file has a different name than the one currently installed, and that it is valid. If so, the Aruba 501 reboots and starts up using the new configuration settings.



Each time you edit the configuration file to implement new configuration settings, you must change the filename of the configuration file on the TFTP server and in the Option 43 definition on the DHCP server. If the filename is not changed, the Aruba 501 will not install the new configuration file.

Setting the system time

Correct system time is important for proper operation of the Aruba 501, especially when using the logs to troubleshoot.

Select **Management > System time** to open the **System time** page. This page enables you to configure time server and time zone information.

System time ?

Set system time

System time (24 HR):
Fri Jan 4 2013 17:03:46 PST

Set system time:
☐ Using network time protocol (NTP)
☒ Manually

System date:
January 4 2013

System time (24 HR):
17 : 03

Time zone:
USA (Pacific)

Daylight savings

Adjust time for daylight savings:
☒

DST start (24 HR):
Second Sunday in March at 02 : 00

DST end (24 HR):
First Sunday in November at 02 : 00

DST offset:
60 minutes

Save

Set system time

This section displays the current system time. You can configure the time manually or have it automatically configured by a Network Time Protocol (NTP) server.

Manually

Select the date, time (in 24-hour notation), and time zone.

Using network time protocol (NTP)

NTP servers transmit Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock. The timestamp is used to indicate the date and time of each event in log messages.

When you select this option, a field displays for you to specify the NTP server. You can specify the NTP hostname or IP address, although it is recommended that you not use the IP address, as these are more likely to change. If you specify a hostname, note the following requirements:

- The length must be from 1 to 63 characters.
- Upper and lower case characters, numbers, and hyphens are accepted.
- The first character must be a letter (a to z or A to Z), and the last character cannot be a hyphen.

An actual NTP server host name, `pool.ntp.org`, is configured by default and provides the time when the Aruba 501 is connected to the Internet.

Daylight savings

Use this section to enable support for daylight savings time, if required for your location. When you select **Adjust time for daylight savings**, additional fields display to enable you to configure the starting and ending dates and times, and the **DST offset**.

The **DST offset** specifies how many minutes to move the clock forward for daylight savings time.

Wireless range

At high power, the Aruba 501 can communicate with APs that are up to about 300 feet away. The achievable range can vary widely depending on the antenna selected, the radio mode, and environmental and other circumstances.

The following factors can affect wireless performance:

- **Radio power:** More radio power means better signal quality and the ability to create bigger wireless cells. However, cell size should generally not exceed the range of transmission supported by client stations. If it does, wireless clients (such as the Aruba 501) can receive signals from the AP, but might not be able to reply, rendering the connection useless.

Governmental regulations in different parts of the world determine the maximum power output of the Aruba 501 radio.

- **Antenna configuration:** Antennas play an important role in determining the shape of the wireless cell and transmission distance. Consult the specifications for the antennas you are using to determine how they affect wireless coverage.
- **Interference:** Interference is caused by other APs or devices (cordless phones, microwaves) that operate in the same 2.4 GHz frequency band as the Aruba 501 when it is set to a 2.4 GHz mode. Such interference can substantially affect throughput. A smaller, but growing number of devices are potential sources of interference in the 5 GHz band.

Information provided by the management tool can help you diagnose interference problems as they occur.

- Select **Wireless > Neighborhood** to view detailed information about all wireless APs operating in the immediate area so that you can effectively set the operating frequencies.
- Select **Status > Wireless** to view detailed information about packets sent and received, transmission errors, and other low-level events.
- **Physical characteristics of the location:** Radio waves have a limited ability to penetrate metal. The steel reinforcing found in concrete walls and floors can block transmissions or reduce signal quality. However, the Aruba 501 is able to transmit through wood or plaster walls and closed windows. To maximize the range of the wireless cell, the Aruba 501 is best installed in an open area with as few obstructions as possible.

Configuring radio settings

To configure the Aruba 501 radio, select **Wireless > Radio**. The **Modify radio settings** page appears.

Modify radio settings
?

Country and Channels

Country:
US - United States

Restrict channels to:
Channel 36, 5.180 GHz
Channel 40, 5.200 GHz
Channel 44, 5.220 GHz
Channel 48, 5.240 GHz

Basic settings

Radio:
☒ Enabled ☐ Disabled

Mode:
IEEE 802.11a/n/ac

Current channel:
1

Advanced radio settings

Roam threshold:
-75
(-99 - -1) dBm

Roam delta:
10
(0 - 100) dBm

Roam motion detection:
0
(0 - 100) dBm, 0 disables

Fragmentation threshold:
2346
(256-2346) bytes, even numbers

RTS threshold:
2347
(0-2347) bytes

Antenna:
Aruba 2dBi Dual-Band Omni Antenna

Transmit power:
100
(1-100) percent

Save

This page enables you to configure the country in which the Aruba 501 operates, basic radio settings such as the radio mode, and advanced radio features.

Country

The country of operation, also known as the regulatory domain, determines the availability of certain wireless settings on the Aruba 501.

If **Country** is set to **Auto**, the Aruba 501 adopts the country setting from the AP it associates with.

When the country is set, the Aruba 501 automatically limits the available wireless channels and channel width, adjusts the radio power level in accordance with the regulations of the selected country, and alters the available options in the Mode list.



NOTE

Selecting the incorrect country can result in illegal operation and can cause harmful interference to other systems. Ensure that the Aruba 501 is operating in accordance with power, indoor/outdoor restrictions, and license requirements for the country of use. If you fail to heed this notice, you can be held liable for violating the local regulatory compliance.

Restrict channels to

Select the channels that the Aruba 501 will scan. By limiting the channels that are scanned, the speed at which the Aruba 501 switches to a new AP can be increased.

To select or delete a channel, hold down the **CTRL** key as you select the channel names.



When toggling between radio modes, you may lose visibility of the restricted channel list. It is recommended that you configure the channel restriction list while in auto mode.

Basic settings

Radio

The wireless radio is enabled by default using the default station profile **Aruba 501**. See [Using station profiles to establish a wireless link](#) on page 25

Mode

Select a mode that is compatible with the upstream AP.

Supported wireless modes are determined by the regulatory domain (country of use). Available options can include one or more of the following:

- **Auto:** The Aruba 501 detects the wireless mode of the upstream AP and automatically selects a compatible mode. When set to **Auto** mode, the Aruba 501 scans both the 2.4 GHz and 5 GHz bands and is capable of connecting with 802.11a/b/g/n/ac APs. This is the default setting.
- **IEEE 802.11a:** The Aruba 501 can connect to an 802.11a or 802.11 a/n/ac AP as an 802.11a client.
- **IEEE 802.11b/g:** (Compatibility mode.) The Aruba 501 can connect to an 802.11b/g or 802.11b/g/n AP as an 802.11b/g client.
- **IEEE 802.11b/g/n:** (Compatibility mode.) The Aruba 501 can connect to an 802.11b, 802.11g, or 802.11b/g/n AP as an 802.11b/g/n client.
- **IEEE 802.11a/n/ac:** (Compatibility mode.) The Aruba 501 can connect to 802.11a, 802.11n, and 802.11ac BSSIDs operating in 5 GHz frequency.


Current channel

This field displays the wireless channel currently in use. The channel defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each mode offers a number of channels, depending on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R).

On the Aruba 501, the channel is determined by the upstream AP with which the Aruba 501 is communicating.

Advanced radio settings

When you click the **+** symbol, next to **Advanced radio settings**, the following settings display:


Advanced radio settings

| | | |
|--------------------------|-------------------------------------|--------------------------------|
| Roam threshold: | <input type="text" value="-75"/> | (-99 - -1) dBm |
| Roam delta: | <input type="text" value="10"/> | (0 - 100) dBm |
| Roam motion detection: | <input type="text" value="0"/> | (0 - 100) dBm, 0 disables |
| Fragmentation threshold: | <input type="text" value="2346"/> | (256-2346) bytes, even numbers |
| RTS threshold: | <input type="text" value="2347"/> | (0-2347) bytes |
| Antenna: | Aruba 2dBi Dual-Band Omni Antenna ▼ | |
| Transmit power: | <input type="text" value="100"/> | (1-100) percent |

Roam threshold/Roam delta

The Aruba 501 periodically detects the strength of wireless signals received on its antennas, including both beacon frames and ordinary traffic. The signal strength value is called the Receive Signal Strength Indicator (RSSI). If the Aruba 501 detects an RSSI value below the configured Roam threshold, the Aruba 501 is triggered to scan for other APs within range. If it finds an AP with a stronger signal by a value greater than the configured Roam delta, the Aruba 501 associates with that AP.

If multiple APs are detected with a stronger signal, preference is given to APs in the 5 GHz band over those in the 2.4 GHz band. The detected strength of each 5 GHz AP is increased by 10 dBm for comparison purposes only. The following examples illustrate the decision process and assume that the **Mode** is set to **Auto**.

- If the Aruba 501 is currently connected to a 5 GHz AP and the Roam delta is set to 15 dBm, when a signal is detected that falls below the Roam threshold:
 - The Aruba 501 will associate with a detected 2.4 GHz AP only if its signal is more than 25 dB stronger than the current AP. Although the Roam delta is only 15 dB, when comparing signal strengths, an additional 10 dB is added to the signal strength of the current 5 GHz AP but not to the signal from the 2.4 GHz AP.
 - The Aruba 501 will associate with another 5 GHz AP if its signal is more than 15 dBm stronger than the current AP, as both APs receive the 10 dB increase.
- If the Aruba 501 is currently associated with a 2.4 GHz AP, and the Roam delta is set to 10 dBm, when a signal is detected that falls below the Roam threshold:
 - The Aruba 501 will associate with a detected 5 GHz AP if its signal is at least 1 dB stronger than the current AP.
 - The Aruba 501 will associate with another 2.4 GHz AP if its signal is more than 10 dB stronger than the current AP, as neither AP receives the 10 dB increase.

You can specify a Roam threshold value from -99 to -1 dBm. The default is -75 dBm. You can specify a Roam delta from 0 to 100 dBm. The default is 10 dBm.



It is recommended that network administrators experiment with these values to determine the optimum roaming performance in your specific environment.



NOTE

Setting the roam threshold too high can degrade performance.

Roam motion detection

Roam motion (of the Aruba 501) detection is based on the RSSI from the current AP. Because the cost of roaming is high, the roam trigger threshold and roam delta parameters are designed to minimize these costs while still locating the best AP available in an area. If motion (of the Aruba 501) is detected, the roam threshold will be more

aggressive and roam delta will be set much lower. This allows the radio to perform a full scan to attempt to locate a better AP.

To detect roaming, RSSI is sampled every second and when the RSSI delta exceeds the configured threshold, motion (of the Aruba 501) is detected. When motion is detected, the roam threshold (10 dB by default) is increased and the roam delta (5 dB by default) is decreased for two minutes. This may trigger a roam to a new and better AP, if possible. After two minutes, roam threshold and roam delta return to the originally configured values.

Fragmentation threshold

Specify a number from 256 to 2,346 (even numbers only) to set the frame size threshold in bytes. The default is 2,346 bytes.

The fragmentation threshold is a way of limiting the size of frames transmitted over the network. If a frame exceeds the fragmentation threshold you set, the fragmentation function is activated and the frame is sent as multiple 802.11 frames.

If the frame being transmitted is equal to or less than the threshold, fragmentation is not used.

Setting the threshold to the largest value (2,346 bytes) effectively disables fragmentation.

Fragmentation involves more overhead because it requires the extra work of dividing up and reassembling frames and it increases message traffic on the network. However, fragmentation can help improve network performance and reliability if properly configured.

Sending smaller frames (by using lower fragmentation threshold) might help with some interference problems; for example, with microwave ovens.

By default, fragmentation is off. It is recommended that you not use fragmentation unless you suspect radio interference. The additional headers applied to each fragment increase the overhead on the network and can greatly reduce throughput.

RTS threshold

Specify a Request to Send (RTS) threshold value from 0 to 2347. The default is 2347 octets.

To ensure that sufficient bandwidth is available to send a frame, the Aruba 501 can send an RTS packet to the upstream AP and await for a Clear to Send (CTS) reply. When the Aruba 501 receives the CTS, it sends the frame. The RTS/CTS handshake itself consumes bandwidth, so it is generally not desirable to perform the handshake prior to a large percentage of data exchanges. The RTS threshold indicates how large a frame must be in order for the Aruba 501 to send an RTS packet. For frames below this value, an RTS/CTS handshake is not performed.

Changing the RTS threshold can help control traffic flow through the Aruba 501. If you specify a low threshold value, RTS packets are sent more frequently. This consumes more bandwidth and reduces packet throughput. However, sending more RTS packets can help the network recover from interference or collisions that might occur on a busy network or on a network experiencing electromagnetic interference.

Antenna

Select the antenna to use.



When antennas other than the default are used, some channels and radio modes might not be supported. For restrictions, see the *Aruba 501 802.11ac Wireless Client Bridge Quickstart*.

Transmit power

Enter a percentage value for the transmit power level.

The default value of 100% gives the Aruba 501 a maximum broadcast range.

To increase the capacity of the network, place the Aruba 501 closer to the upstream AP and reduce the value of the transmit power. This helps reduce overlap and interference among the Aruba 501 and APs in the area. A

lower transmit power setting can also keep your network more secure because weaker wireless signals are less likely to propagate outside the physical location of your network.

Using station profiles to establish a wireless link

A station profile contains the configuration settings that the Aruba 501 uses to establish a wireless connection with an AP.

Station profiles are defined on the **Wireless > Station profiles** page. A profile called **Aruba 501** is created by default. (It has an SSID of **Aruba 501** and a WPA2 key of **Aruba 501 Client Bridge**.)



HPE recommends that once you define one or more custom profiles, you delete the default profile.

Station profiles configuration ?

Station profiles

| Status | Active Scanning | Priority | Name | SSID | Security |
|--------|-----------------|----------|---------------------------|-----------|---------------------|
| | Enabled | ▲ ▼ | Aruba 501 | Aruba 501 | WPA2 personal (PSK) |

Edit Station profile

Name:

Enabled: ☒

SSID:

Active Scan: ☒

Security:

WPA versions: ☐ WPA ☒ WPA2

Key: 8-63 characters

Confirm key:

Each profile contains the definitions for a wireless connection. The Aruba 501 supports multiple station profiles, enabling it to automatically connect with different wireless networks. For example:

| Station profiles | | | | | |
|------------------|-----------------|----------|---------------------------|-----------|---------------------|
| Status | Active Scanning | Priority | Name | SSID | Security |
| | Enabled | ▲ ▼ | Aruba 501 | Aruba 501 | WPA2 personal (PSK) |
| | Enabled | ▲ ▼ | Office_1 | Office_1 | WPA personal (PSK) |
| | Disabled | ▲ ▼ | Office_2 | Office_2 | WPA personal (PSK) |

The Aruba 501 uses the profile definitions in the following order when it attempts to find an AP with which to establish a wireless link:

- First, all profiles with **Active scanning enabled** are sequentially checked in the order that they are listed, from top to bottom. The Aruba 501 actively sends probe requests to the SSID defined in each profile.
- Next, all profiles in the table are sequentially checked in the order that they are listed, from top to bottom. The Aruba 501 uses information collected by passively scanning the wireless neighborhood to find a match for the SSID defined in each profile.

Status

The Status column indicates whether the wireless profile is **Associated** (blue bars) with a wireless network, or **Disconnected** (white bars).

Active Scanning

Shows whether **Active Scanning** is enabled or disabled on a station profile.

Priority

Change profile priority by clicking the up/down arrows in the **Priority** column.

Name

The name identifying a station profile.

SSID

Specify the SSID of the wireless network to be bridged with the wired network. You can click the icon to the right of the text box to select an SSID from a list of available wireless networks. (You can manually enter an SSID even if it does not appear in the list.)

Security

The Aruba 501 supports the following authentication and encryption options for protection of wireless transmissions. Select the option that is required to authenticate with the upstream AP:

- **None:** No security options are applied.
- **Static WEP:** The Aruba 501 authenticates using a WEP key configured on the Aruba 501 and the upstream AP. This mode is available only when the configured radio mode does not support 802.11ac or 802.11n.
- **WPA/WPA2 Personal:** The Aruba 501 authenticates using a preshared key (PSK) configured on the upstream AP.
- **WPA/WPA2 Enterprise:** Select this option if the upstream AP uses a remote authentication server to handle authentication requests.

See **Security methods** on page 28 for additional instructions.

To add or edit a station profile

Select **Wireless > Station profiles** and do the following:

- To add a new profile, click **Add**.
- To edit a profile, select its name in the list.

In either case, the Station profiles - Add/Edit Station profile page opens.

Edit Station profile

Name:

Office_1

Enabled:

☒

SSID:

Office_1

Active Scan:

☒

Security:

WPA/WPA2 Personal

WPA versions:

☒ WPA ☐ WPA2

Key:

••••••••

8-63 characters

Confirm key:

••••••••

Delete

Cancel

Save

Configure station profile settings as follows:

Name

Specify a name to uniquely identify the station profile.

Enabled

To enable the station profile, select **Enabled**.

SSID

Specify the SSID of the wireless network to which this profile will connect.

Active scan

In active scanning mode, the Aruba 501 sends out **probe request** frames in an attempt to solicit responses from APs that are within range. This enables the Aruba 501 to establish a connection with an AP that does not broadcast an SSID.


Some countries prohibit active scanning on some channels. In these countries, probe requests are not sent on prohibited channels.

Security

Available security method options are outlined in the following section.

Security methods

Edit Station profile

| | |
|---------------|--|
| Name: | <input type="text" value="Office_1"/> |
| Enabled: | <input checked="" type="checkbox"/> |
| SSID: | <input type="text" value="Office_1"/>  |
| Active Scan: | <input checked="" type="checkbox"/> |
| Security: | <div>WPA/WPA2 Personal ▼</div> <div>None</div> <div>Static WEP</div> <div>WPA/WPA2 Personal</div> <div>WPA/WPA2 Enterprise</div> |
| WPA versions: | |
| Key: | <input type="text" value=""/> 8-63 characters |
| Confirm key: | <input type="password" value=""/> |

Delete Cancel Save

Configure station profile settings as follows:

None

Select **None** to provide no security option for station profiles.

Static WEP

The Aruba 501 authenticates using a WEP key configured on the Aruba 501 and the upstream AP. This mode is available only when the configured radio mode does not support 802.11ac or 802.11n.

This method uses a WEP key that is configured on both the Aruba 501 and the upstream AP. It is the least secure method of protecting wireless transmissions. WEP is provided so you can authenticate with an upstream AP that does not support WPA.



WEP cannot be used when the radio operating mode supports 802.11a/n/ac or 802.11n.

Key length

Select one of the following values as the length of the encryption key, based on the settings on the upstream AP:

- **64 bits:** The key can be 5 ASCII characters or 10 hexadecimal digits.
- **128 bits:** The key can be 13 ASCII characters or 26 hexadecimal digits.

Key type

Select the format used to specify the encryption key, based on the settings on the upstream AP:

- **ASCII:** ASCII keys are much weaker than carefully chosen hexadecimal keys. You can include ASCII characters from 32 through 126 in the key.
- **Hex:** Hex keys must include only the following hexadecimal characters: 0–9, a–f, A–F.

WEP key

Enter a key of the specified format and length, and re-enter the key in the **Confirm WEP key** box.

WPA/WPA2 Personal

WPA Personal provides for secure login using a preshared key (PSK) and data encryption. The key must match the key configured on the upstream AP. If you select this method, specify the following:

WPA versions

Select **WPA** or **WPA2**, depending on the version supported by the upstream AP.



WPA is not supported for 802.11n or 802.11ac operation.

Key

Specify the preshared key (PSK) configured on the upstream AP. The key must be from 8 to 63 alphanumeric characters. Re-enter the key in the **Confirm key** box.

WPA/WPA2 Enterprise

Select this option if the upstream AP uses a remote authentication server to handle authentication requests. If you select this method, specify the following:

WPA versions

Select **WPA** or **WPA2**, depending on the version supported by the upstream AP.



WPA is not supported for 802.11n or 802.11ac operation.

EAP methods

Select one of the following extensible authentication protocol (EAP) methods:

- **PEAP:** With this method, the Aruba 501 username and password credentials are provided to the upstream AP, which forwards them to the authentication server for verification. Specify the following:

Username

Enter a value from 1 to 64 alphanumeric characters.

Password

Enter a value from 1 to 64 alphanumeric characters.

- **TLS:** Choose **TLS** for EAP-TLS authentication using certificates. Specify the following:

Identity field

The username that is used for the **radius user account** and must match. (Username and password are usually the same.)

Private key

The **passphrase** that protects the private key. You need to provide this to load the private key. Enter a value from 1 to 64 characters.

Edit Station profile

Name:

Office_1

Enabled:

☒

SSID:

Office_3

Active Scan:

☒

Security:

WPA/WPA2 Enterprise ▼

WPA versions:

☒ WPA ☐ WPA2

EAP method:

☐ PEAP ☒ TLS

Identity:

Private key:

1-64 characters

Confirm private key:

Certificate file present:

No

Certificate expiration date:

Not Present

Certificate file:

HTTP upload ▼

Upload filename:

Choose File

No file chosen

Delete

Cancel

Save

Certificate file

The **Certificate Chain file** that contains the **CA Certificate**, **SSL certificate** and, **Private Key** components, in base-64 format, with a .pem extension.

PKCS#12 formatted certificates are supported using .pfx or .p12 file extensions.

Certificate components

These are the SSL components that you need to acquire or generate, depending on the source of your SSL Public Key Infrastructure (PKI). These components can be generated from a Public PKI (for example, GoDaddy, Entrust, or Thawte), or from a private PKI such as MS Certificate Server.

- A **Certificate Signing Request (CSR)**. This can be generated by OpenSSL, or by MS Certificate Server, for instance.
- A **Private Key**. The CSR will also generate a Private Key (.key file) for your SSL certificate.
- A **Certificate Authority (CA)**. The CA (such as GoDaddy or MS Certificate server), is used to sign your CSR, and this will produce your SSL certificate.
- An **SSL Certificate**. This is the resulting certificate that is created when the CA signs your CSR, which will be installed on the Aruba 501 with your Private Key.
- A **Certificate Chain**. This is a text file that contains your **CA Certificate**, **SSL Certificate**, and your **Private key** components in base-64 format, with the .pem file extension.
- PKCS#12 certificates contain both public and private certificate pairs. Unlike PEM, PKCS#12 files are fully encrypted.

Radius Server configuration

Your Radius server requires the following steps setup to support EAP-TLS.

- **CA Certificate.** This is the same CA certificate that signs the SSL certificate installed in the Aruba 501.
- **SSL Certificate.** This is an SSL certificate signed by the above-mentioned CA Certificate.
- **Private Key.** This is the private key associated with the above-mentioned SSL certificate.

Configuring wireless bridging features

Configuring MAC address cloning

The Aruba 501 supports cloning the MAC address of a single connected wired device, thereby minimizing the impact on the network configuration when the device is converted to wireless by the addition of the Aruba 501. MAC cloning is useful when the upstream AP does not accept requests for more than one IP address per wireless MAC address. It also allows remote devices upstream to access the connected wired device by its MAC address. MAC cloning renders the Aruba 501 transparent on the wireless network, as it adopts the MAC address of the connected device for all communication with the upstream AP.

Only one wired client MAC address can be cloned at a time. MAC address cloning is disabled by default. When enabled, the Aruba 501 management interfaces are inaccessible unless the management traffic interception feature is configured.

To configure MAC address cloning, select **Wireless > Bridging**.

In the **Ethernet MAC cloning** section of the **Wireless bridging** page, configure the following settings:

Ethernet MAC cloning

Enable or disable MAC cloning. When enabled, the Aruba 501 disassociates from the upstream AP and reassociates using the MAC address you configure instead of the default DHCP-assigned IP address.

Ethernet MAC address to clone

Specify the MAC address to clone.

You can select **MAC address** and manually specify the address of a client. Or, you can select **Discovered MAC mode** for the Aruba 501 to discover the address of the device connected to the Ethernet port.

Management traffic interception

A limitation of Ethernet MAC cloning is that, when the cloned MAC address is used to establish the wireless connection, the bridge itself is no longer accessible through the wireless connection. The management traffic interception feature allows the wireless bridge to intercept wireless traffic on specific logical ports and redirect it to the management interfaces, instead of forwarding it to the cloned device.

Select any of the following types of management traffic to be intercepted:

- Management tool (TCP ports 80 and 443)
- SNMP agent (UDP port 161)
- Network time (UDP port 123)

Redirecting unsupported traffic

The Aruba 501 sends and receives only IPv4 traffic on the wireless link. By default, all other traffic is unsupported and is dropped. In some cases, you might want to forward the unsupported traffic to a wired device connected to the Ethernet port.

You can configure the Aruba 501 to redirect non-IPv4 traffic received on the wireless port to the specified MAC address on the wired network.



NOTE

This feature cannot be used when MAC cloning is enabled.

To enable this feature, select **Wireless > Bridging**.

Redirect unsupported traffic

Redirect unsupported traffic to:

☐ Enabled ☒ Disabled

MAC address:

00:00:00:00:00:00

Save

In the **Redirect unsupported traffic** section of the **Wireless bridging** page, select **Enabled**. Enter the **MAC address** of the station to forward non-IPv4 traffic to, and then click **Save**.

Configuring frame processing settings

The following settings can be configured in the Frame processing section of the **Wireless bridging** page:

Frame processing

Act like a DHCP relay agent:

☐ Enabled ☒ Disabled

IP forwarding:

☐ Enabled ☒ Disabled

Save

Act like a DHCP relay agent

A device connected to the Ethernet port can acquire its IP address from a DHCP server that is accessed over the wireless network. DHCP requests from the device, and the replies from the DHCP server, are handled by the upstream AP.

Some DHCP servers respond to DHCP requests using the MAC address of the requesting station to identify the recipient. In this case, the upstream AP might not recognize the MAC address, as it does not identify a device on the wireless network. The AP can then discard the DHCP reply.

To avoid this problem, you can configure the Aruba 501 to modify all DHCP requests from the Ethernet interface so that, when forwarded to the wireless network, they appear to come from a DHCP relay agent. When enabled, the upstream AP sends DHCP replies from the server back to the Aruba 501 for forwarding to the wired device.

This feature is disabled by default. To enable, select **Enabled**, and then click **Save**.



The DHCP relay agent feature is not supported when MAC address cloning is enabled.

IP forwarding

Ethernet devices that do not send any IP packets at startup have no entry in the Aruba 501 wireless-to-MAC translation table. As a result, the Aruba 501 cannot route incoming IPv4 wireless traffic to these devices.

When the IP forwarding option is enabled, the Aruba 501 sends an ARP request on the Ethernet port whenever a packet with an unknown destination IP address is received on the wireless interface. After receiving an ARP response from the device on the Ethernet port, the Aruba 501 can forward the packet to the intended device.

This feature is disabled by default. To enable, select **Enabled**, and then click **Save**.

Viewing wireless information

The Aruba 501 provides several pages where you can view information related to wireless operation.

Viewing nearby APs

To view information on all APs operating within range of the Aruba 501, select **Wireless > Neighborhood**.

The following information is displayed for each detected AP:

| Field | Description |
|--------------------|--|
| MAC | The MAC address of the AP (also called the BSSID). |
| Beacon int. | APs periodically send out management frames called beacons to advertise their presence and some configuration data to other wireless devices. The beacon interval is the number milliseconds between beacons. |
| Type | The type of AP: <ul style="list-style-type: none">• AP indicates the neighboring device is an AP that supports the IEEE 802.11 Wireless Networking Framework in Infrastructure Mode.• Ad hoc indicates a neighboring station running in Ad hoc Mode. Stations set to ad hoc mode communicate with each other directly, without the use of a traditional AP. Ad hoc mode is an IEEE 802.11 Wireless Networking Framework also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS). |
| SSID | The wireless network name. |
| Privacy | Indicates whether there is any security enabled on the neighboring AP. <ul style="list-style-type: none">• Off indicates that no security is enabled on the AP.• On indicates that the neighboring device has some security in place. |
| WPA | Indicates whether WPA security is on or off for this AP. |
| Mode | Indicates the operating mode of the AP: 802.11a, b, g, n, or ac, or a combination of modes. |
| Channel | The channel the AP is operating on. |

Table Continued

| Field | Description |
|---------------|---|
| Rate | The rate in megabits per second at which the AP is currently beaconing. |
| Signal | A bar chart indicating the signal strength. |

The Aruba 501 regularly performs scans to detect beacon frames sent by APs within range. These are referred to as passive scans. When the Aruba 501 is not associated with an AP, the duration of the passive scan is lengthened to more quickly build the available AP list. To display the latest detected APs, click **Refresh**.

You can click **Clear All** to remove all APs from the list. This button is disabled when the radio is disabled.

You can click **Start Scan** to initiate an active scan. An active scan sends probe requests to detect nearby APs rather than passively waiting to receive beacons from them. Therefore, the active scan may populate the AP list more quickly. The scan is performed on all available channels in the frequency band currently in use. If the radio mode is Auto, both the 2.4 GHz and 5 GHz frequency bands are scanned. The active scan does not send probes to channels that are reserved due to regulations in the selected country of operation.

The Aruba 501 sends two probes on each channel and collects the responses. It does not attempt to associate with another AP in this scan—the scan only collects data for display. Information for existing APs in the list is updated, and newly discovered APs are added to the bottom of the list. A single scan may not find all available APs. If you suspect additional APs are available, perform another scan.



If the Aruba 501 is currently associated with an AP, the scan disrupts the connection for up to 8 seconds, depending on how many channels are scanned (which varies by country and radio mode).

If a scan is initiated while the Aruba 501 is in the process of associating with an AP, or while it is roaming to associate with another AP, the scan request may be ignored. **Start Scan** is disabled when the radio is disabled or when AP profiles are configured but in a disconnected state.

Viewing wireless statistics for the radio

Select **Status > Wireless** to view wireless interface statistics. The statistics are accumulated from the time of the last reset. This page displays the following items:

| Field | Description |
|--------------------------------------|---|
| WLAN packets received | Total packets received by the Aruba 501. |
| WLAN bytes received | Total bytes received by the Aruba 501. |
| WLAN packets transmitted | Total packets transmitted by the Aruba 501. |
| WLAN bytes transmitted | Total bytes transmitted by the Aruba 501. |
| WLAN packets receive dropped | Number of packets received by the Aruba 501 that were dropped. |
| WLAN bytes receive dropped | Number of bytes received by the Aruba 501 that were dropped. |
| WLAN packets transmit dropped | Number of packets transmitted by the Aruba 501 that were dropped. |
| WLAN bytes transmit dropped | Number of bytes transmitted by the Aruba 501 that were dropped. |

Table Continued

| Field | Description |
|-------------------------------------|---|
| Fragments received | Count of successfully received MPDU frames of type data or management. |
| Fragments transmitted | Number of transmitted MPDU with an individual address or an MPDU with a multicast address of type data or management. |
| Multicast frames received | Count of MSDU frames received with the multicast bit set in the destination MAC address. |
| Multicast frames transmitted | Count of successfully transmitted MSDU frames where the multicast bit is set in the destination MAC address. |
| Duplicate frame count | Number of times a frame is received and the Sequence Control field indicates it is a duplicate. |
| Failed transmit count | Number of times an MSDU is not transmitted successfully due to transmit attempts exceeding either the short retry limit or the long retry limit. |
| Transmit retry count | Number of times an MSDU is successfully transmitted after one or more retries. |
| Multiple retry count | Number of times an MSDU is successfully transmitted after more than one retry. |
| RTS success count | Count of CTS frames received in response to an RTS frame. |
| RTS failure count | Count of CTS frames not received in response to an RTS frame. |
| ACK failure count | Count of ACK frames not received when expected. |
| FCS error count | Count of FCS errors detected in a received MPDU frame. |
| Transmitted frame count | Count of each successfully transmitted MSDU. |
| WEP undecryptable count | Count of encrypted frames received and the key configuration of the transmitter indicates that the frame should not have been encrypted or that frame was discarded due to the receiving station not implementing the privacy option. |
| Cloned MAC address | If MAC address cloning is enabled for a device on the Ethernet port, the MAC address displays here. |

Viewing the MAC translation table

You can select **Status > MAC translation** to view the MAC address/IP address associations for clients on the Ethernet network. The following fields display:

| Field | Description |
|----------------------|--|
| MAC address | The MAC address of the client on the wired network. |
| IP address | The IP address of the client on the wired network. |
| Tx/Rx packets | Total packets transmitted from the Aruba 501 to the client or received by the Aruba 501 from the client. |

Click **Clear MAC table** to delete all entries from the list.

IP configuration

The Aruba 501 can connect to up to 15 wired Ethernet clients through a switch or hub connected to its Ethernet port. Use the **IP configuration** page to view the Ethernet port MAC address and configure IPv4 and IPv6 settings. To display this page, select **Network > IP**.

The **Ethernet configuration** section of the page shows the **MAC address** assigned to the Ethernet port and to the wireless interface. The MAC address is also printed on the Aruba 501 label.

IPv4 configuration

Use the **IPv4 configuration** section of the page to assign an IPv4 address from a DHCP server on your network to the Aruba 501, or to statically configure an IPv4 address.

IPv4 configuration

Connection type: Static IP ▼

Static IP address: . . .

Subnet mask: . . .

Default gateway: . . .

DNS nameservers: ☐ Dynamic ☒ Manual

. . .

. . .

Automatically assigning an IP address (default method)

By default, Connection type is set to DHCP and the Aruba 501 operates as a DHCP client. This means that if the wired or wireless network has a DHCP server, the Aruba 501 automatically receives a new IP address in place of its default IP address (192.168.1.1) upon connecting to the network.



- The Aruba 501 can receive an address from a DHCP server on either the wireless or wired network. To avoid conflicts, however, a DHCP server should reside on only one of these networks.
- The DHCP server assigns an address from its pool of available addresses. You can find the IP address of the 501 by looking for its Ethernet base MAC address in the DHCP server log. The Ethernet MAC address is printed on the 501 label identified as Ethernet Base MAC, or listed on the management tool IP page as MAC address.
- To have the DHCP server assign a specific IP address to the Aruba 501, you must pre-configure the DHCP server to associate the IP address you want to use with the MAC address of the Ethernet port on the Aruba 501.
- When operating as a DHCP client, the Aruba 501 supports DHCP options 43 and 60, providing the ability to download a configuration file during start up without user intervention. See **Automatically configuring the Aruba 501 using DHCP options 43 and 60**.

Static IP configuration

You can manually assign an IP address to the Ethernet port. This requires that you also define the address of the default gateway and DNS server that are in use on your network.

Connection type

Select **Static IP** from the list to manually configure an IPv4 Ethernet address.

Static IP address

Set an address that is on the same subnet as the network to which the Aruba 501 will connect when installed. Respect any DHCP server-mandated static address ranges.

Subnet mask

Specify the mask for the IP address.

Default gateway

Set the IP address of the gateway on the network.

DNS nameservers

Select **Dynamic** to have the DNS nameservers assigned through DHCP, or select **Manual** to configure up to two static DNS nameserver addresses.

IPv6 configuration

If the attached network uses the IPv6 protocol, use the **IPv6 configuration** section of the page to enable IPv6 support on the Aruba 501. IPv6 functionality is enabled by default.

IPv6 configuration

IPv6:

☒ Enabled ☐ Disabled

Static IPv6 address:

Static IPv6 address prefix length:

(0-128)

Default IPv6 gateway:

IPv6 DNS nameservers:

☒ Dynamic ☐ Manual

Static IPv6 address status:

IPv6 link local address:

fe80::8a51:fbff:fe77:9053/64

DHCPv6:

☒ Enabled ☐ Disabled

IPv6 auto configuration:

☒ Enabled ☐ Disabled

IPv6 autoconfigured global addresses:

IPv6

Enable or disable the ability to use IPv6 addressing to access the web user interface for Aruba 501 configuration. This setting does not enable or disable IPv6 functionality on the network itself.

Static IPv6 address

The Aruba 501 can have a static IPv6 address, even if addresses have already been configured automatically. Enter an address in the form **XXXX:XXXX:XXXX:XXXX**.

Static IPv6 address prefix length

The prefix length must be an integer in the range from 0 to 128 bits. The prefix length determines the part of the IPv6 address that identifies the network to which the Aruba 501 is attached.

Default IPv6 gateway

The default gateway address for IPv6 traffic destined outside the network.

IPv6 DNS nameservers

You can configure up to two IPv6 DNS nameservers for resolving domain names to IP addresses. If you select **Dynamic**, be sure to enable DHCPv6 functionality in the field below. If you select **Manual**, enter up to two IPv6 addresses in the text boxes provided.

Static IPv6 address status

The operational status of the static IPv6 address assigned to the Aruba 501 management interface. The possible values are as follows:

- **Operational:** The IP address has been verified as unique on the LAN and is usable on the interface.
- **Tentative:** The Aruba 501 initiates a duplicate address detection (DAD) process automatically when a static IP address is assigned. An IPv6 address is in the tentative state while it is being verified as unique on the network. While in this state, the IPv6 address cannot be used to transmit or receive traffic, except to exchange messages with other network nodes to verify the uniqueness of the address.
- **Blank (no value):** No IP address is assigned or the assigned address is not operational.

IPv6 link local address

The IPv6 link local address is the IPv6 address used by the local physical link. The link local address is not configurable and is assigned by using the IPv6 Neighbor Discovery process.

DHCPv6

In addition to statically configuring IPv6 addresses, you can enable this feature to have IPv6 addresses assigned by a DHCPv6 server on the network.

IPv6 auto configuration

When IPv6 auto configuration is enabled, the Aruba 501 processes the Router Advertisements received on the LAN port to determine its IPv6 addresses. The Aruba 501 can have multiple autoconfigured IPv6 addresses. The autoconfigured addresses coexist with the statically configured address. The Aruba 501 can be accessed using either the statically configured or the automatically obtained IPv6 address.

IPv6 autoconfigured global addresses

If the Aruba 501 has been assigned one or more IPv6 addresses automatically, the addresses are listed.

Manual link speed settings

To display this page, select **Network > Port**.

Port 1 configuration
?

Link

Autonegotiation:
☒ Enabled
☐ Disabled

Link speed:
1000 Mbps

Duplex mode:
Full duplex

(Currently: 100 Mbps Full Duplex)

Save

Autonegotiation

Use this setting to enable or disable automatic port negotiation. It is enabled by default.

Link speed

With autonegotiation disabled, you can specify the particular link speed to be used. Supported speeds are 10 Mbps, 100 Mbps and 1000 Mbps.

Duplex mode

With autonegotiation disabled, you can specify the particular duplex mode to be used. Supported modes are Half duplex and Full duplex with the exception of 1000 Mbps which can only be set to Full duplex.

Network 802.1X feature descriptions

The Aruba 501 features a built-in 802.1X authenticator for authenticating wired devices connected to the Ethernet port. When enabled, a wired device will not be given access to the upstream AP network without first successfully completing an 802.1X authentication exchange. The Aruba 501 relays the authentication frames to the configured upstream RADIUS server.

Wired RADIUS server settings
?

RADIUS server settings

Wired LAN 802.1X authenticator:
☐ Enabled
☒ Disabled

RADIUS IP address type:
☒ IPv4
☐ IPv6

RADIUS IP port:
1812

RADIUS IP address-1:

RADIUS IP address-2:

RADIUS key-1:
(1-64) characters

RADIUS key-2:

Save

Wired LAN 802.1X authenticator

Enable the authenticator feature to require authentication for all wired devices. If disabled, all traffic from wired devices will be directly bridged to the upstream AP network.

RADIUS IP address type

Specify the type of IP network that should be used to communicate with the RADIUS server. Supported types are IPv4 and IPv6. The RADIUS IP address-1 and RADIUS IP address-2 fields below should be configured with corresponding IP addresses.

RADIUS IP port

Specify the RADIUS port on which the upstream RADIUS server is listening.

RADIUS IP address-1

Specify the primary RADIUS server IP address.

RADIUS IP address-2

Specify the secondary/backup RADIUS server IP address.

RADIUS key-1

Specify the shared secret to be used when communicating with the primary RADIUS server.

RADIUS key-2

Specify the shared secret to be used when communicating with the secondary RADIUS server.

Viewing Ethernet statistics

To view statistics on Ethernet packets transmitted and received on the wired and wireless ports, select **Status > Ports**.

The statistics accumulate until the Aruba 501 is rebooted.

Port

The LAN port is listed as Port 1. The wireless port displays as Wireless. The up/down status of the port displays to the left of the port name.

Packets

The total number of packets received or transmitted on the interface.

Dropped

The number of packets dropped upon receipt or transmission.

Errors

The number of packets received or transmitted that had errors.

TCP serial

TCP connection

The Aruba 501 has an external serial port which can be used to enable a device with a serial connection to communicate with a remote host over the wireless network. This is useful for devices that do not have wireless or Ethernet functionality.

To configure a TCP-over-serial connection, in the Management tool, select **Network > TCP serial**.

Ensure that the serial port is configured as required for communication with the attached device (see **Serial port settings** on page 42). Then, in the **TCP connection** section, configure these settings:

TCP connection

TCP over serial:

☐ Enabled
☒ Disabled

Mode:

Server ▼

Remote IP address:

TCP port:

8000 (1000-65535)

Transmit timeout:

☐ Enabled
☒ Disabled

100 (1-30000) ms

Idle timeout:

☐ Enabled
☒ Disabled

30 (5-86400) seconds

TCP over serial

Enables and disables this functionality. It is disabled by default.

Mode

Configures the Aruba 501 to act as either a TCP client or a TCP server.

- **Client:** The Aruba 501 acts as a TCP client and initiates a connection to the specified remote IP address using the specified TCP port. Serial data received from the serial device is packaged and transmitted on the specified TCP port and is destined for the remote TCP server.
- **Server:** The Aruba 501 acts as a TCP server and listens for an incoming connection from a TCP client on the specified TCP port. When TCP is enabled, this mode is the default.

TCP connections can be initiated from either the wired or wireless network.

Remote IP address

The IP address of the remote TCP client or server that communicates with the serial device.

TCP port

The logical port number on which the Aruba 501 listens for TCP connections and transmits data from the serial device. The default port number is 8000.

Transmit timeout

The length of time, in milliseconds, that traffic on the serial port will be buffered. The range is 100 to 30000 ms and the default is 100 ms.

Idle timeout

The amount of time, in seconds, that the TCP connection can remain idle before it is disconnected by the Aruba 501. The range is 30 to 86400 seconds and the default is 30 seconds.

Statistics for the TCP serial feature are available on the **Status > TCP serial** page.

Serial port settings

Use the settings in this section to configure the communication settings for the serial port. Ensure that the settings are compatible with those on the attached serial device.

| Serial port | |
|------------------------|------------------------|
| Data bits: | 8 ▼ |
| Parity bit: | None ▼ |
| Stop bits: | 1 ▼ |
| Baud rate: | 38400 ▼ |
| Software flow control: | None ▼ |
| Hardware flow control: | None ▼ |
| Max receive buffer: | 1024 (1024-8192) bytes |

Data bits

The number of data bits. The default is 8 bits.

Parity bit

Whether the parity bit is even or odd, or no parity bit is used. The default is None.

Stop bits

The number of stop bits. The default is 1 stop bit.

Baud rate

The baud rate in bits per second. The default is 38400 bps.

Software flow control

Select one of the following values:

- **None:** The Aruba 501 does not provide flow control. Instead, flow control is performed end-to-end by the remote TCP device and the locally connected serial device. This is the default value.
- **XON/XOFF:** Flow control is performed locally using XON/XOFF. In this case, the attached serial device must also support software flow control.

Hardware flow control

Select one of the following values:

- **None:** The Aruba 501 does not provide flow control. Instead, flow performed end-to-end by the remote TCP device and the locally connected serial device.
- **RTS/CTS:** Flow control is performed locally using RTS (Request To Send)/CTS (Clear To Send). In this case, the attached serial device must also support hardware flow control.

Max receive buffer

Receive buffer size in bytes. If the buffer becomes full, data is discarded until space can be freed up. The range is from 1024 to 8192 bytes and the default is 1024 bytes.

Viewing TCP serial status and statistics

Use the **Status > TCP serial** page to view information on the state of the TCP connection and transmit and receive statistics.

State

The TCP connection state. Possible values are:

- **Listen:** When the TCP Mode is set to Server, this value indicates that the Aruba 501 is waiting for the remote TCP client to establish the connection.
- **Connecting:** When the TCP Mode is set to Client, this value indicates that the Aruba 501 is attempting to establish a connection with the remote TCP server. If this state persists, then it indicates that the remote TCP server is not reachable. The Aruba 501 will periodically attempt to establish the connection.
- **Active:** The connection has been established and data is being transferred.
- **Idle:** The connection has been established but no data is currently being transferred.
- **Disabled:** TCP functionality is administratively disabled on the serial port.

Remote IP address

The configured IP address of the remote device that can communicate with the serial device.

Connection time

The duration of the current TCP connection.

Tx (kbytes)

The number of kilobytes of data transmitted from the serial device to the remote device.

Rx (kbytes)

The number of kilobytes of data received by the serial device from the remote device.

LLDP configuration

The Aruba 501 can use the Link-Layer Discovery Protocol (LLDP) to advertise information about itself, such as the system name, port name, and system capabilities, to devices on the wired network (LLDP information is not sent on the wireless network). This information can be useful for network management and monitoring purposes.

The information contained in LLDP frames includes the device model and configured system name, the base MAC address and IPv4 address, the Ethernet port speed and duplex, and the maximum power needed by the device in milliwatts.

To configure LLDP settings, select **Network > LLDP** in the management tool. You can configure the following settings:

LLDP mode

Enables or disables LLDP advertisements. By default, LLDP operation is enabled.

Transmit interval

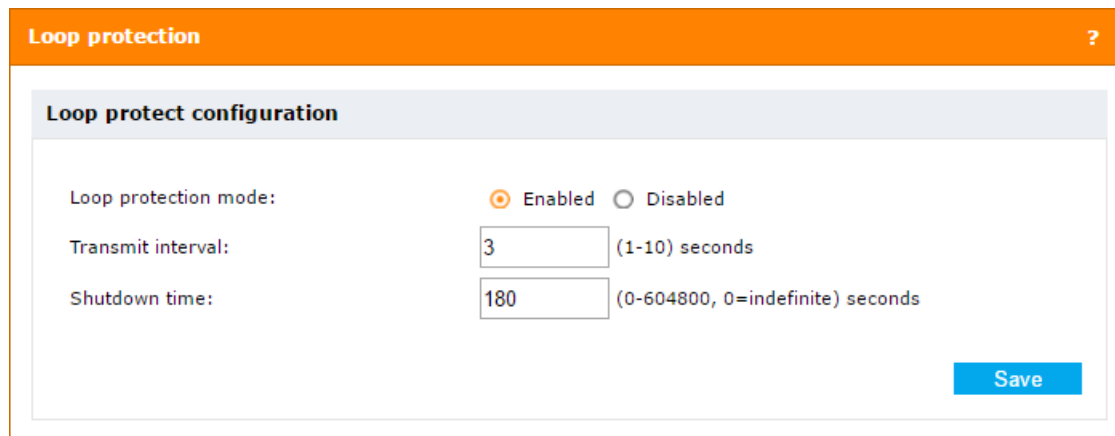
The number of seconds between LLDP message transmissions. The default is 30 seconds.

Loop protection

The Aruba 501 supports loop protection, which prevents configuring both the wired and wireless interfaces to use the same subnet.

When enabled, the software periodically sends loop protection packets to a reserved multicast address on the wireless interface. If the multicast packet comes back to the Aruba 501 on the Ethernet interface (with a source MAC addresses that identifies the wireless interface) within a specified time, the software determines that a loop has occurred. The Ethernet interface is shut down for a configured period, and a log entry is created.

To configure loop protection settings, select **Network > Loop protection** in the management tool.

The screenshot shows the 'Loop protection' configuration page. At the top is an orange header with the text 'Loop protection' and a question mark icon. Below this is a light gray box titled 'Loop protect configuration'. Inside this box, there are three settings: 'Loop protection mode:' with radio buttons for 'Enabled' (selected) and 'Disabled'; 'Transmit interval:' with a text input field containing '3' and a label '(1-10) seconds'; and 'Shutdown time:' with a text input field containing '180' and a label '(0-604800, 0=indefinite) seconds'. A blue 'Save' button is located at the bottom right of the configuration box.

You can configure the following settings:

Loop protection mode

Enables and disables loop protection. It is enabled by default.

Transmit interval

The number of seconds between loop protection packets sent. The range is from 1 to 10 seconds and the default is 3 seconds.

Shutdown time

The number of seconds the Ethernet interface is shut down when a loop is detected. The range is from 0 to 604800 seconds and the default is 180 seconds. If you specify a value of 0, the Ethernet interface is shut down indefinitely.

Viewing loop protection statistics

The following status and statistics for the loop protection feature are available on the **Status > Loop protection** page.

Loop protection status

Indicates whether the feature is enabled or disabled.

Number of packets sent/received

The number of loop protection packets sent and received since the last reboot.

Shut down interface

If the Ethernet interface is currently in the shut down state, eth0 appears in this field.

Remaining shutdown time

If the Ethernet port has been shut down due to the discovery of a loop, this field shows the number of seconds it will remain shut down.

Loop detection count

The total number of loops detected since the Aruba 501 was last reset.

Time of last loop detection

The date and time of the most recent detected loop.

Configuration file management

The configuration file contains all the settings that customize the operation of the Aruba 501. You can save and restore the configuration file by selecting **Maintenance > Config file management**.

Config file management ?

Reset

Restore the factory default configuration.

Reset

Save

Save the current configuration to a backup file.

Download method: ☒ HTTP ☐ TFTP

Download

Restore

Restore the configuration from a previously saved file.

Upload method: ☒ HTTP ☐ TFTP

Configuration file:

Restore

Reboot

Reboot the device.

Reboot

Reset

See [Resetting to factory defaults](#) on page 71 for information about restoring the factory default configuration.

Save

The Save feature enables you to back up your configuration settings so that they can be easily restored in case of failure.

Before you install new software, it is recommended that you always back up your current configuration.

To start the process, select a **Download method**, and then click **Download**.

For HTTP downloads, you are prompted for the location in which to save the configuration file. For TFTP downloads, specify the file name and the TFTP server IP address.

Restore

The Restore feature enables you to load a previously saved configuration file.

- For an HTTP restore, browse to choose the configuration file you want to restore, and then click

Restore.

- For a TFTP restore, specify the file path and file name on the TFTP server and enter the TFTP server address, and then click

Restore.



After restoring the configuration file, the system automatically reboots.

Reboot

For maintenance purposes or as a troubleshooting measure, you can reboot the Aruba 501 by clicking **Reboot**.

The process can take several minutes during which time the Aruba 501 is unavailable. The Aruba 501 resumes normal operation with the same configuration settings it had before the reboot.

Software updates

To update the Aruba 501 software, select **Maintenance > Software updates**. The **Manage software** page displays.

Manage software ?

Software information

Active image: V2.0.0.0-Aruba501-B0010.cim

Backup image: V1.0.1.2-HP501-B0009.cim

Switch

Software upgrade

Upload method: ☒ HTTP ☐ TFTP

New software image: Choose file

Upgrade

Software information

The Aruba 501 maintains both an active software image and a backup image. The Aruba 501 always tries to boot with the active image. If it fails to load, the backup image is used. Whenever such a failover occurs, the system creates a log message to help you troubleshoot the software failure.

The Software information area shows the active image and backup image versions. To make the backup image the active image, and the active image the backup image, click **Switch**.

The Aruba 501 reboots with the new image. The process can take several minutes, during which time the Aruba 501 is unavailable. Do not power down the Aruba 501 while the image switch is in progress. When the image switch is complete, the Aruba 501 restarts. The Aruba 501 resumes normal operation with the same configuration settings it had before the upgrade.

Software upgrade



- Before updating, be sure to read the Release Notes.
- Even though configuration settings are preserved during software updates, it is recommended that you back up your configuration settings before updating. See [Configuration file management](#) on page 47 .

To update the Aruba 501 software using HTTP, click **Choose file** to locate the software file (with the extension .tar), and then click **Upgrade**.

To update the software using TFTP, specify the file path and file name on the TFTP server, enter the TFTP server address, and then click **Upgrade**.

At the end of the update process, the Aruba 501 automatically restarts, disconnecting the current management session. After the Aruba 501 resumes operation, you can reconnect.

System information

The **System** page enables you to download logs, settings, system tools outputs, and other information that customer support uses to diagnose problems.

To download system information, select **Maintenance > System**.

The screenshot shows the 'System' page of the Aruba 501 web interface. The page has an orange header with the word 'System' and a question mark icon. Below the header, there are two sections: 'Show tech' and 'Save system information'. Each section contains a description of the download and a 'Download' button.

| System | |
|---|--------------------------|
| Show tech | |
| Download system information for technical support. | Download |
| Save system information | |
| Download system information for troubleshooting purposes. | Download |

Show tech

In the Show tech area, you can download a file that can be read in a text editor. The file contains configuration settings, including those that have been customized by the user. The file is named `showtech.rtf` by default.

When you click **Download**, you are prompted to select a location to save the file.

Save system information

In the Save system information area, you can download an encrypted binary file. Although you cannot read this file, you can provide it to customer support to assist in debugging efforts. This file contains additional configuration and device information. It is named `showdev.out` by default.

When you click **Download**, you are prompted to select a location to save the file.

System log

The system log is a comprehensive list of system messages and kernel messages, which may indicate error conditions such as dropped frames. The Aruba 501 stores up to 512 system error messages in volatile memory (RAM). You can view these events using the Aruba 501 management tool, and you can configure Aruba 501 to relay them as syslog messages to a syslog server residing on the network.

You can also configure the Aruba 501 to store up to 512 messages in nonvolatile memory (flash). When full, the oldest log message gets overwritten by the new log message. Logged messages often indicate severe errors in Aruba 501 operation, and they can prove useful in diagnosing system crashes. All log messages are time stamped.

To configure system log settings, and view a limited number of log messages from RAM, select **Tools > System log**.

System log configuration

Use the **System log configuration** section of the **System log** page to configure the size of the system log and specify which system events result in messages to store in the log, based on their severity level.

System log configuration

Persistence: ☐ Enabled ☒ Disabled

Severity: Warning ▼

Facility ID: 1 ▼

Depth: 4096 (1-4096) entries

Save

You can configure the following log settings:

Persistence

If the system unexpectedly reboots, log messages can be useful to diagnose the cause. However, log messages in volatile memory are lost when the system reboots. You can enable persistent logging to store log messages in flash memory so that they are retained after a reboot.

Select **Enabled** to save system logs to flash memory. Select **Disabled** to save system logs to volatile memory only. The default is **Disabled**.



Persistent logging can eventually deteriorate the flash memory and degrade network performance. It is recommended that you enable persistent logging only to debug a problem. Make sure you disable persistent logging after you finish debugging the problem.

Severity

Specify the severity level of the log messages to write to the system logs. This setting applies to messages stored in RAM and flash memory. The severity levels are listed from most severe (top) to least severe (bottom):

- **Emergency** indicates that the system is unusable. It is the highest level of severity.
- **Alert** indicates action must be taken immediately.
- **Critical** indicates critical conditions.
- **Error** indicates error conditions.
- **Warning** indicates warning conditions.
- **Notice** indicates normal but significant conditions.
- **Informational** indicates informational messages.
- **Debug** indicates debug-level messages.

For example, if you specify **Critical**, only critical, alert, and emergency messages are written to the log(s).

Depth

RAM and flash memory can store up to 512 messages each, which is the default. When the depth value you configure is reached, the oldest log message is overwritten by the new log message.

Remote syslog configuration

You can view up to 512 messages stored in RAM in the **Events** section of the **System log** page. To view a longer history of messages, you must set up a remote syslog server that acts as a syslog log relay host on your network. Then, you can configure the Aruba 501 to send syslog messages to the remote server. The Severity level setting configured in the **System log configuration** section determines which messages are stored in RAM and are available for relay to a remote syslog server.

Using the remote syslog feature provides these benefits:

- Allows aggregation of syslog messages from multiple Aruba 501s. The MAC address of the sending AP displays at the start of each message.
- Stores a longer history of messages than those that are kept on a single Aruba 501.
- Can trigger scripted management operations and alerts.

The procedure for configuring a remote log host depends on the type of system you use as the remote host.

Use the **Remote syslog configuration** section of the **System log** page to configure Aruba 501 remote log settings.

Remote syslog configuration

Syslog mode:

☐ Enabled
 ☒ Disabled

Syslog server:

Syslog port:

514

(1-65535)

Save

Remote syslog

Use this setting to enable or disable this feature. It is disabled by default. When enabled, messages of the selected **Severity** level or higher are sent to the configured syslog server. When disabled, a limited number of these messages is stored locally and can be viewed in the **Events** section of the **System log** page.

Syslog server

Specify the IP address or DNS name of the remote log server.

Syslog port

The syslog process uses logical port 514 by default. It is recommended that you keep this default. If you specify a different port number, ensure that the port number is not being used by another protocol on your network, and that your syslog server is also configured to use that port.

Events

The **Events** section of the **System log** page shows real-time system events on the Aruba 501, such as DHCP address assignments to the Aruba 501. The log shows the date the event occurred, its severity level, the software program or process that caused the event message, and the message text.

You can click **Refresh** to display the most recent data from the Aruba 501, or **Clear All** to remove all entries from the list.

RSSI log

The Aruba 501 can determine the strength of the wireless signal received from an upstream AP. Administrators can use this value, called received signal strength indicator (RSSI), when determining the optimal physical location and configuration of APs and to diagnose network traffic issues.

Up to 1024 RSSI values can be stored in the RSSI log. When the log is full, new entries overwrite older entries. You can configure the Aruba 501 to send certain log entries to a Syslog server for permanent storage or further analysis.

To configure RSSI log settings, select **Tools > RSSI log**.

Syslog message list

The following table lists the syslog messages generated by the Aruba 501. The MAC address of the Aruba 501 is automatically added to the beginning of every syslog entry.

| Message | Description | Severity |
|---|---|---------------|
| The AP startup configuration was updated successfully. | Configuration settings were changed and subsequently saved. | Informational |
| Loop Protect: A loop detected on interface eth0. | A loop was detected. | Critical |
| DHCP6-client: Interface x obtained lease on new address x . | The specified DHCPv6 address was obtained on the listed interface (new address). | Warning |
| DHCP-client: Interface x obtained lease on new address x . | The specified DHCP address was obtained on the listed interface (new address). | Warning |
| DHCP6-client: Interface x obtained lease on new address x . | The specified DHCPv6 address was obtained on the listed interface (same address). | Informational |
| DHCP-client: Interface x obtained lease on new address x . | The specified DHCP address was obtained on the listed interface (same address). | Informational |
| Auto country detected and adopted country XX from AP. | The Country setting is Auto and the country code was adopted from the upstream AP. | Notice |
| Download-Copy: Starting configuration upgrade | Upgrade is in progress. | Informational |
| Download-Copy: Failed to write filename | Upload failed because the Aruba 501 failed to write to the downloaded file or the log file. This may occur due to a lack of space on the device or other system error. | Error |
| Download-Copy: Failed to Open filename | Upload failed because the Aruba 501 was unable to open the downloaded file or the log file. | Error |
| Download-Copy: Failed to Validate Config File | Validation of the configuration file failed. The downloaded configuration file has parameters that are not valid. For example, the model name in the configuration file is invalid. | Warning |
| Download-Copy: Failure in parsing url | The IP address or path to the configuration file returned by the DHCP server is invalid. | Warning |
| Download-Copy: Failed to download Config From location | The configuration file could not be downloaded. | Error |
| Download-Copy: Startup config and the uploaded config are identical | The new configuration file is the same as the one that is currently active on the Aruba 501. | Warning |

Table Continued

| Message | Description | Severity |
|--|---|---------------|
| TSB: Connection established with TCP xx at IP xx port xx . | TCP serial connection established. | Informational |
| TSB: Disconnection from TCP TCP xx xx port xx . | TCP serial connection terminated. | Informational |
| TSB: Idle timeout on TCP xx , xx disconnected. | TCP serial connection disconnected due to idle timeout. | Informational |
| TSB: Closing incoming connection from TCP client at IP xx port xx . A connection has already been established. | Ignoring incoming TCP serial connection, since a connection has already been established. | Warning |
| TSB: tcpserialbridge connect to xx:xx failed errno= xx(xx) , will keep trying. | Remote TCP serial connection failed and will retry. | Warning |
| TSB: Aborting connection from TCP client xx port xx (cause: new connection request from same IP address). | Aborting previous TCP serial connection with the same IP address since the connection was closed. | Warning |
| TSB: Server on port xx | TCP serial server is listening on port xx . | Informational |
| Association to SSID x and BSSID x unsuccessful | Work group bridge connection established. | Notice |
| Deauthenticated from BSSID x with reason xx . | Work group bridge connection terminated due to receiving a disassociation frame. | Notice |
| Roamed to BSSID x for reason x:x . | Work group bridge roamed to a new BSSID. | Notice |
| Lost connection with BSSID x . | Work group bridge abruptly lost contact with the BSSID. | Notice |
| Association failed with status x :Reason. | Association failed with status code and reason given. Likely reasons are: <ul style="list-style-type: none"> Failed due to no matching network found. Protocol failure: packet not acknowledged. Operation failed. | Notice |
| Last firmware upgrade did not complete so still running the previous image. | The attempted firmware upgrade did not complete, and the system reverted to the previous image. | Error |
| The primary image failed to load so the secondary image was loaded. | The primary image could not be loaded, and the system loaded the secondary image. | Error |
| Connected to <ssid> on channel <channel>. | The system associates with a different upstream network. | Informational |

Table Continued

| Message | Description | Severity |
|--|--|---------------|
| Certificate file upload success. | A certificate file has been successfully uploaded for a station profile. | Informational |
| Certificate file upload failed. | A certificate file upload attempt fails. | Error |
| Certificate file validation failed. | A certificate file validation attempt fails. | Warning |
| WPA supplicant failed to reload. | A station profile configuration change triggers a WPA supplicant reload but the operation fails. | Error |
| Trying to associate with SSID <ssid>. | The system attempts to join a station profile network. | Informational |
| invalid 802.1x configuration. | The system attempts to start the 802.1X authenticator but fails due to an invalid configuration. | Error |
| RADIUS server failover. | The system switches to the next RADIUS server after the current server failed to respond. | Notice |
| Adding STA <MACAddress> to 802.1x access list. | A new wired client has been successfully authenticated with the 802.1X authenticator. | Notice |
| Removing STA <MACAddress> from 802.1x access list. | An existing wired client has been de-authenticated from the 802.1X authenticator. | Notice |
| Roamed from BSSID <MACAddress>(RSSI: xx) to BSSID <MACAddress> (RSSI: xx) for reason (xx) | The Aruba 501 roamed from one AP to another. | Notice |
| RSSI log entry - AP:<MACAddress> RSSI: xx <SNR: xx > Channel: xx | RSSI information, channel, and SNR of the AP to which the Aruba 501 is currently connected. | Info |

Email alert

The Email alert feature allows the Aruba 501 to automatically send email messages when an event at or above the configured severity level occurs. To configure email alert settings, select **Tools > Email alert**.

General email alert configuration

General

Email alert:

☐ Enabled ☒ Disabled

From address:

Urgent message severity:

Alert ▼

Non urgent severity:

Warning ▼

Non urgent log duration:

(30-1440) minutes

Email alert

Globally enable or disable the Email alert feature. It is disabled by default.

From address

Specify the email address that appears in the From field of alert messages sent from the Aruba 501, for example AP23@company.com. It is recommended that you use an email address that exits on your own network, so that the address is notified if an email from the Aruba 501 is undeliverable, and to prevent spam filters on the network from blocking the sending or delivery of emails from the Aruba 501.

The address can be a maximum of 255 characters and can contain only printable characters. By default, no address is configured.

Urgent message severity

This setting determines the severity level for log messages that are considered to be urgent. Messages in this category are sent immediately upon being generated. The security level you select and all higher levels are considered urgent:

- **Emergency** indicates that the system is unusable. It is the highest level of severity.
- **Alert** indicates action must be taken immediately.
- **Critical** indicates critical conditions.
- **Error** indicates error conditions.
- **Warning** indicates warning conditions.
- **Notice** indicates normal but significant conditions.
- **Informational** indicates informational messages.
- **Debug** indicates debug-level messages.

Non-urgent severity

This setting determines the severity level for log messages that are considered to be non-urgent. Messages in this category are collected and sent in a digest form at the time interval specified by the non-urgent log duration. The security level you select and all levels up to but not including the lowest urgent level are considered non-urgent. Messages below the security level you specify are not sent via email.

Non urgent log duration

This setting determines how frequently the non-urgent message logs are sent to the email (SMTP) server. The range is 30 to 1440 minutes. The default is 30 minutes.

Non-urgent messages are sent when the time duration is reached or the number of messages exceeds the configured Depth value on the **System log** page, whichever occurs first.

Mail server configuration

| Mail server | |
|-----------------------|---|
| Mail server address: | <input type="text"/> |
| Mail server security: | Open ▼ |
| Mail server port: | <input type="text" value="25"/> (0-65535) |

Mail server address

Specify the IP address or hostname of the SMTP server on the network.

Mail server security

Specify whether to use SMTP over SSL (**TLSv1**) or no security (**Open**) for authentication with the mail server. The default is Open.

Mail server port

Configure the TCP port number for SMTP. The range is a valid port number from 0 to 65535. The default is 25, which is the standard port for SMTP.

Username

The username and password fields display only when the **Mail server security** setting is **TLSv1**. Specify the username to use for authentication with the mail server. The username can be from 1 to 64 characters long and can include any printable characters.

Password

Specify the password associated with the username configured in the previous field. The password can be 1 to 64 characters long and can include any printable characters.

Message configuration

| Message | |
|----------------|---|
| To address 1: | <input type="text"/> |
| To address 2: | <input type="text"/> |
| To address 3: | <input type="text"/> |
| Email subject: | <input type="text" value="Log message from WCB"/> |

To address 1, 2, 3

Configure up to three email addresses to which alert messages are sent. Email addresses must be in valid format, for example abc@def.com. By default, no addresses are configured.

Email subject

Specify the text to be displayed in the subject line of the email alert message. The subject can contain up to 255 alphanumeric characters. The default subject is "Log message from WCB".

Sending a test message

To validate the configured email server credentials, click **Test Mail**.

The following example shows a sample email alert sent from the Aruba 501 to the network administrator:

```
From: AP-192.168.1.1@mailserver.com
Sent: Wednesday, February 08, 2012 11:16 AM
To: administrator@mailserver.com
Subject: log message from AP
TIME          Priority    Process Id      Message
Feb 8 03:48:25  info      login[]         root login on 'tty0'
Feb 8 03:48:26  info      mini_http-ssl[1175]  Max concurrent connections
                                     of 20 reached
```

Viewing email alert status

You can select **Status > Email alert** to view the status of the email alert feature and information about past activity.

Email alert status

Indicates whether the Email alert feature is enabled or disabled.

Number of emails sent

The number of alert emails sent since the feature was enabled.

Number of emails failed

The number of alert emails sent since the feature was enabled that did not reach the intended destination.

Time since last email sent

The date and time of the last alert email sent.

Network trace configuration

Overview

Network administrators can perform network traces to capture and analyze network traffic. Network trace operates in two modes:

- **Packet file trace mode:** Captured packets are stored in a file on the Aruba 501. The Aruba 501 can transfer the file to a local PC or network location using HTTP or to a TFTP server. The file is formatted in pcap format and can be examined using tools such as Wireshark and OmniPeek.
- **Remote packet trace mode:** The captured packets are redirected in real time to an external PC running the Wireshark tool.

The Aruba 501 can trace the following types of packets:

- 802.11 packets received and transmitted on radio interfaces. Packets captured on radio interfaces include the 802.11 header.
- 802.3 packets received and transmitted on the Ethernet interface.

To configure network trace settings and initiate packet captures, select **Tools > Network trace**.

Packet trace configuration

Use this section to configure parameters that affect how packet trace functions on the radio interface.

Packet trace configuration

Trace beacons:
☒ Enabled
☐ Disabled

Promiscuous trace:
☐ Enabled
☒ Disabled

Client filter enable:
☐

Client filter MAC address:

Save

Trace beacons

Enable to trace the 802.11 beacons detected by the radio. It is recommended that you also enable Promiscuous trace when performing a beacon trace.

Promiscuous trace

Enable to place the radio in promiscuous mode when the trace is active.

In promiscuous mode, the radio receives all traffic on the channel, including traffic that is not destined to the Aruba 501. Packets not destined to the Aruba 501 are not forwarded.

As soon as the trace is completed, the radio reverts to non-promiscuous mode operation.

Client filter enable

Enable to use the WLAN client filter to trace only frames that are transmitted to, or received from, a WLAN client with a specified MAC address.

Client filter MAC address

Specify a MAC address for WLAN client filtering. The MAC filter is active only when a trace is performed on the radio1 interface.



Changes to packet trace settings take effect after a packet trace is restarted. Modifying the parameters while a packet trace is running does not affect the current packet trace session. To begin using new parameter values, an existing packet trace session must be stopped and restarted.

Packet file trace

In packet file trace mode, the Aruba 501 stores captured packets internally in a file.

Upon activation, the packet trace proceeds until one of the following occurs:

- The trace time reaches the configured duration.
- The trace file reaches its maximum size.
- The administrator stops the trace.

During the trace, you can monitor the trace status, elapsed trace time, and the current trace file size. You can click **Refresh** to update this information while the trace is in progress.

Capture packets and store them in a file

Procedure

1. Select **Tools > Network trace**.

Packet file trace

Trace interface:

radio1 ▼

Trace duration:

60

(10-3600) seconds

Max trace file size:

1024

(64-4096) KB

Start Trace

Save

2. Select a **Trace interface**. The following Aruba 501 interfaces are available for packet trace:
 - **brtrunk**: Traffic on the bridge interface destined to the management IP address.
 - **eth0**: 802.3 traffic on the Ethernet port.
 - **radio1**: Traffic on the radio captured in 802.11 format. Captured 802.11 traffic may be encrypted, based on the configured security settings.
3. Specify the following parameters:
 - **Trace duration**: The time duration in seconds for the trace (range 10 to 3600).
 - **Max trace file size**: The maximum allowed size for the trace file in KB (range 64 to 4096).

If you change either of these values, you must click **Save** before initiating a trace.

4. Click **Start Trace**.

The trace session runs for the specified duration. You can view the trace status in the **File trace status** section. Click **Refresh** to see updated trace time and file size values. You can click **Stop Trace** to stop a trace before the specified duration has elapsed.

Remote packet trace

Remote packet trace enables you to specify a remote port as the destination for packet captures. This feature works, for example, in conjunction with the Wireshark network analyzer tool for Windows. A packet trace server runs on the Aruba 501 and sends the captured packets via a TCP connection to the Wireshark tool.



- When MAC cloning is enabled, remote packet trace does not work for remote wireless clients.
- When the remote trace mode is in use, the Aruba 501 does not store any captured data locally in its file system.
- Wireshark is an open source tool available from www.wireshark.org.
- Remote packet trace is not standard on the Linux version of Wireshark. The Linux version does not work with the Aruba 501.

Setting up Wireshark sessions

You can trace up to five interfaces on the Aruba 501 at the same time. However, you must start a separate Wireshark session for each interface. You can configure the IP port number used for connecting Wireshark to the Aruba 501. The default port number is 2002. The system uses five consecutive port numbers starting with the configured port for the packet trace sessions.

If a firewall is installed between the Wireshark PC and the Aruba 501, these ports must be allowed to pass through the firewall. The firewall must also be configured to allow the Wireshark PC to initiate a TCP connection to the Aruba 501.

After you start remote trace on the Aruba 501, you can configure Wireshark to use the Aruba 501 as the source for captured packets. To do this, you must specify the remote interface in the **Capture Options** menu. For example, to trace packets on an Aruba 501 with IP address 192.168.1.10 on the radio interface using the default IP port, specify the following interface:

```
rpcap://192.168.1.10/radio1
```

To trace packets on the Ethernet interface of the Aruba 501 and on the radio interface using IP port 58000, start two Wireshark sessions and specify the following interfaces:

```
rpcap://192.168.1.10:58000/eth0  
rpcap://192.168.1.10:58000/radio1
```

When you are capturing traffic on the radio interface, you can disable beacon trace, but other 802.11 control frames are still sent to Wireshark. You can set up a display filter to show only the following:

- Data frames in the trace.
- Traffic on specific BSSIDs.

The following are examples of useful display filters:

- Exclude beacons and ACK/RTS/CTS frames:

```
!(wlan.fc.type_subtype == 8 || wlan.fc.type == 1)
```

- Data frames only:

```
wlan.fc.type == 2
```

- Traffic on a specific BSSID:

```
wlan.bssid == 00:02:bc:00:17:d0
```



If you stop the remote trace on the Aruba 501, restarting it will not resume the Wireshark capture automatically. You must restart the capture in Wireshark after you restart the remote trace in Aruba 501.

Performance and security considerations

In remote packet trace mode, traffic is sent to the PC running Wireshark via one of the Aruba 501 network interfaces. Depending on where the Wireshark tool is located, the traffic can be sent on an Ethernet interface or the radio. To avoid a traffic flood caused by tracing the trace packets, the Aruba 501 automatically installs a trace filter to filter out all packets destined to the Wireshark application. For example, if the Wireshark IP port is configured to be 58000, the following trace filter is automatically installed on the Aruba 501:

```
not portrange 58000-58004
```

Enabling the packet trace feature impacts Aruba 501 performance, even if there is no active Wireshark session. Performance is negatively impacted to a greater extent when packet trace is in progress.

Due to performance and security issues, the packet trace mode is not saved in nonvolatile memory on the Aruba 501. If the Aruba 501 resets, the trace mode is disabled and you must re-enable it to resume capturing traffic. Packet trace parameters (other than mode) are saved in nonvolatile memory.

To minimize performance impact on the Aruba 501 while traffic trace is in progress, it is recommended that you install trace filters to limit the traffic sent to the Wireshark tool. When capturing 802.11 traffic, a large portion of the captured frames tend to be beacons (typically sent every 100 ms by all APs). Although Wireshark supports a display filter for beacon frames, it does not support a trace filter to prevent the Aruba 501 from forwarding captured beacon packets to the Wireshark tool. To reduce the performance impact of capturing the 802.11 beacons, you can disable the trace beacons mode.

The remote packet trace facility is a standard feature of the Wireshark tool for Windows.

Performing a remote packet trace

To perform a remote packet trace:

Procedure

1. Set up the Wireshark session as described in [Setting up Wireshark sessions](#) on page 61.
2. On the Aruba 501 management tool, select **Tools > Network trace**.

Remote packet trace

Remote trace port:
(1025-65530)

Start Remote Trace
Save

3. In the **Remote packet trace** section, specify the Remote trace port to use as the destination for packet captures. The range is 1 to 65530 and the default port is 2002. If you change this value, you must click **Save** prior to starting the remote trace.
4. Click **Start Remote Trace**.
5. The trace session runs for the specified duration. You can view the trace status in the **Packet trace status** section. Click **Refresh** to see the updated trace time. You can click **Stop Trace** to stop a trace before the specified duration has elapsed.

Packet trace status

This section enables you to view the status of the packet trace on the Aruba 501.

Packet trace status

Current trace status:
Not started

Packet trace time:
00:00:00

Packet trace file size:
0 KB

Stop Trace
Refresh

Current trace status

Whether a packet trace is running or is stopped.

Packet trace time

The elapsed trace time for a trace in progress.

Packet trace file size

The current trace file size.

Packet trace file download

For packet traces saved by Packet file trace, you can download the file by TFTP to a TFTP server, or by HTTP(S) to a PC or network location. A trace is automatically stopped when the trace file download command is triggered.

HTTP download

Select **HTTP** to download to your PC or a network location.

Packet trace file download

Download method:
☒ HTTP
☐ TFTP

TFTP server filename:

Server IP:

Download

Click **Download**, and browse to the desired location.

TFTP download

Select **TFTP** to download to a TFTP server.

Packet trace file download

Download method:
☐ HTTP
☒ TFTP

TFTP server filename:

Server IP:

Download

TFTP server filename

Enter the TFTP server name and path where the file is to be saved.

Server IP

Enter the IP address of the TFTP server.

Click **Download**. A progress bar displays to indicate download status.

Ping

The Aruba 501 supports ping functionality to enable basic diagnostics of network devices. To ping another device, select **Tools > Ping**.

Ping
?

Address to ping:

Timeout:
 (1-15) seconds

Result:

Ping

Address to ping

You can specify an IPv4 address, an IPv6 address, or a hostname.

Timeout

Specify the amount of time in seconds after which an unsuccessful ping will time out. The range is 1 to 15 seconds and the default is 5 seconds.

Result

The result window shows the size and number of each packet sent and, if the host is reached, the size and number of each packet received in response and its round-trip time. It also displays statistics about packet loss and, if the host is reached, the average round-trip time for all packets.

Iperf

The Aruba 501 supports Iperf for testing the performance of a network connection. The Aruba 501 can function as either an Iperf client or Iperf server.

- Only one Iperf connection (client or server) can be active at a time.
- The Aruba 501 runs Iperf version 3. Make sure that the remote Iperf device is running the same version.

To use Iperf, select **Tools > Iperf**.

Iperf?

Iperf Client

Remote Iperf server address:

0.0.0.0

Test duration:

15

(1-1800) seconds

Parallel client thread:

1

(max. 2)

TCP/SCTP maximum segment size:

88

(88-9216) bytes

Client port:

5201

(1-65535)

Stream type:

☒ TCP ☐ UDP

Start

Stop

Iperf Server

Server port:

5201

(1-65535)

Start

Stop

Result

Status:

None

Result:

Iperf client

When operating as an Iperf client, the Aruba 501 establishes a connection to an Iperf server.

Remote Iperf server address

Specify the IPv4 or IPv6 address of the Iperf server. Default: 0.0.0.0.

Test duration

Specify the test duration in seconds. Range: 1 to 1800 seconds. Default: 15 seconds.

Parallel client thread

Specify the number of parallel client streams to be run. Range: 1 or 2. Default: 1.

TCP/SCTP maximum segment size

Specify the maximum segment size in bytes. Range: 88 to 9216 bytes. Default: 88 bytes.

Client port

Specify the port on which the client will establish the connection. The server and the client must use the same port settings. Range: 1 to 65535. Default: 5201.

Stream type

Select the stream type: TCP or UDP. Default: TCP.

Start/Stop

Click to start and stop the test.

Iperf server

When operating as an Iperf client, the Aruba 501 establishes a connection to an Iperf server.

- The Iperf server supports a maximum test duration of 1800 seconds at which point the test is automatically terminated.

Server port

Specify the port on which the server will listen for client connections. The server and the client must use the same port settings. Range: 1 to 65535. Default: 5201.

Result

Status

Test status.

Result

Test results.

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

www.hpe.com/storage/spock

Storage white papers and analyst reports

www.hpe.com/storage/whitepapers

For additional websites, see [Support and other resources](#).

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
<http://www.hpe.com/assistance>
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
<http://www.hpe.com/support/hpesc>

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

Hewlett Packard Enterprise Support Center

www.hpe.com/support/hpesc

Hewlett Packard Enterprise Support Center: Software downloads

www.hpe.com/support/downloads

Software Depot

www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:
www.hpe.com/support/e-updates
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:
www.hpe.com/support/AccessToSupportMaterials



Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett

Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty for your product, see the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* document, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Factory reset procedures

To force the Aruba 501 into its factory default state, follow one of the procedures in this section.



Resetting the Aruba 501 to factory defaults deletes all configuration settings, resets the manager user name and password to **admin**, and enables the DHCP client on the Ethernet port. If no DHCP server assigns an address to the Aruba 501, its address defaults to 192.168.1.1.

Using the reset button

Insert a tool such as a paper clip into the Reset button hole, and press and hold the reset button for a few seconds until the status LEDs flash three times.

Using the management tool

Procedure

1. Launch the management tool (default <https://192.168.1.1>).
2. Select **Maintenance > Config file management**.
3. In the **Reset** section, click **Reset**.

Reset

Restore the factory default configuration.

Reset