SNMP

The *Simple Network Management Protocol* (SNMP) is an Internet standard protocol that facilitates the monitoring and managing of network devices. SNMP lets you monitor events on your network through an SNMP software application.

The following sections describe how to configure SNMP on your network:

- Understanding SNMP
- Navigating to Simple Network Management Protocol
- Enabling and Disabling Simple Network Management Protocol (SNMP)
- Updating Settings
- Configuring Your Network Management System

Understanding SNMP

SNMP defines a standard for recording, storing, and sharing information about network devices. SNMP is a subset of *Transmission Control Protocol/Internet Protocol* (TCP/IP) that facilitates network management, troubleshooting, and maintenance.

Key components of any SNMP-managed network are managed devices, SNMP agents, and a network management system. The agents, store data about their devices in *Management Information Bases* (MIBs) and return this data to the network management system when requested. Managed devices can be network nodes such as access point base stations, routers, switches, bridges, hubs, servers, or printers.

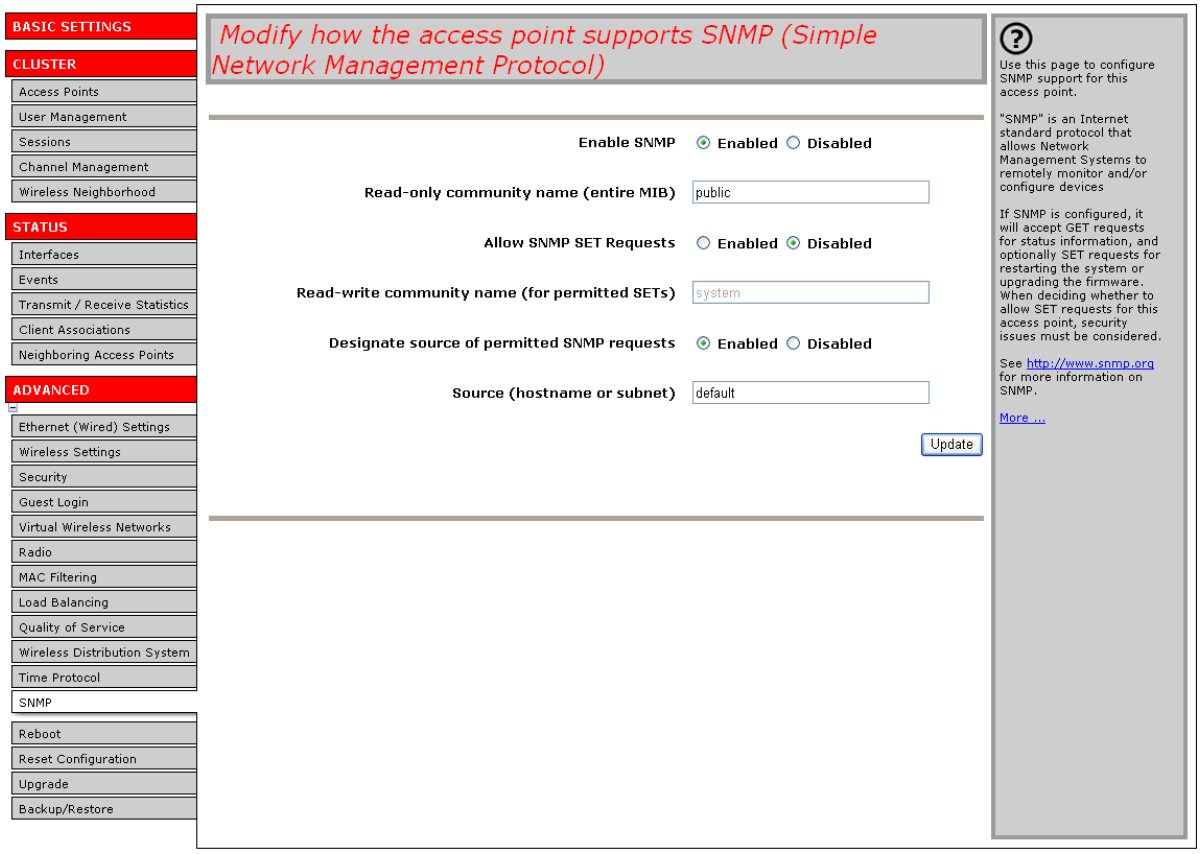
The Professional Access Point can function as an SNMP managed device for seamless integration into network management systems such as HP OpenView. The Professional Access Point supports the following SNMP MIBs:

- Standard SNMP MIBs
    - SNMP v1 and v2 MIBs
    - IEEE802.11 MIB
- Proprietary MIB
    - USR5453-PRODUCTS MIB—stores product identification information.
    - USR5453-SYSTEM MIB—facilitates system-level requests, such as reboot and upgrade.
    - USR5453-WIRELESS-CHAN MIB—maintains channel assignment information for access points in a cluster.
    - USR5453-WIRELESS-MIB—stores information about the wireless system, including peer statistics, beacon report, radio, and client statistics tables.

For more information about SNMP, visit http://www.snmplink.org.

Navigating to Simple Network Management Protocol

To enable SNMP, click the Advanced menu's **SNMP** tab and update the fields as described below.



Enabling and Disabling Simple Network Management Protocol (SNMP)

To configure your access point to use Simple Network Management Protocol (SNMP) server, first *enable* the SNMP option that you want to use, and then provide the name of the community or host that can use

the option.

Field	Description
Enable SNMP	SNMP provides a way for the access point to store management information and to provide the information to a network-management system (NMS). (See http://www.snmplink.org/ for more general information on SNMP.) Choose to either enable (default) or disable use of Simple Network Management Protocol:
Read-only Community Name (entire MIB)	If SNMP is enabled, enter the name of the community that is allowed to make information queries against the MIB. The community name acts an as authentication mechanism. The name functions as a password, and a request is considered authentic if the requester knows the password. The community name is alphanumeric; do not use special characters or spaces.
Allow SNMP SET Requests	Choose to either enable or disable the honouring of SNMP SET requests: • **Enable**—Machines on the network that provide the correct community name can issue SET requests. • **Disable**—(default) SET requests are not honoured. SET requests are restricted to the USR5453-SYSTEM MIB and USR5453-WIRELESS-CHAN MIB..
Read-write community name (for permitted SETs)	If SET requests are enabled, enter the name of the community that is allowed to make SET requests. The community name acts an as authentication mechanism. The name functions as a password, and a request is considered authentic if the requester knows the password. The community name is alphanumeric; do not use special characters or spaces.
Designate source of permitted SNMP requests	Choose to either enable or disable designating the source of the SNMP requests: • **Enable**—(default) A machine must be designated in the **Source** field in order for its requests to be honoured. • **Disable**—Any machine in the network may issue requests.

Field	Description
Source (hostname or subnet)	If source designation is enabled, enter the IP address of the host or subnet that is allowed to issue SNMP requests to the access point. If you use this option, the Professional Access Point honours requests from the specified host or subnet only. If you also enable a read-write community, the specified source must be a member of that community in order for the access point to honour the source's requests. **Note:** Even if you explicitly name a machine or a subnet in this field, any machine issuing a request must also know the proper community name in order to have the request honoured.

To shut down SNMP on the access point, select **Disable** in the **SNMP** field.

Updating Settings

To apply your changes, click **Update**.

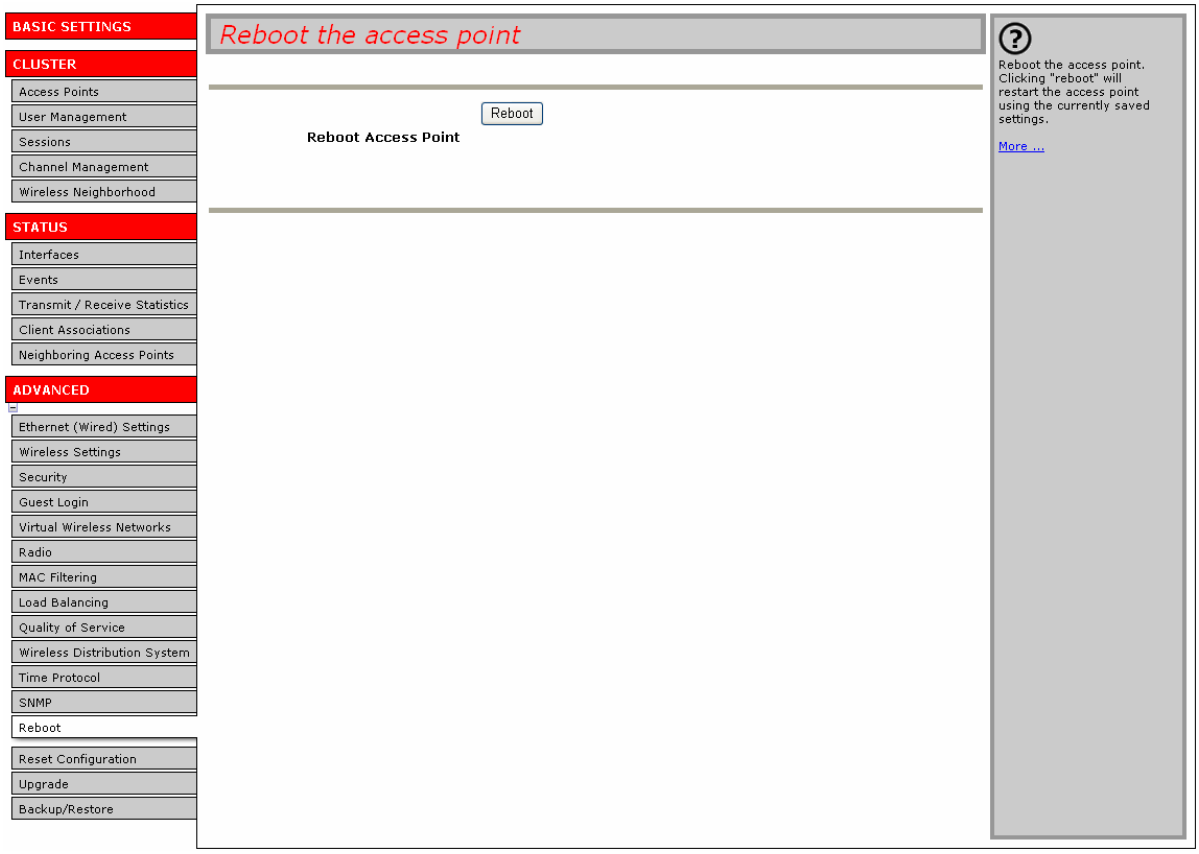
Configuring Your Network Management System

In order to access the USRobotics proprietary MIBs, you need to import the MIBs into your network management system. You can find the MIB files in the Mib folder on the USRobotics CD-ROM. Refer to your network management system for instructions on importing and compiling MIBs.

Reboot

For maintenance purposes or as a troubleshooting measure, you can reboot the Professional Access Point as follows.

1. Click the Advanced menu's **Reboot** tab.



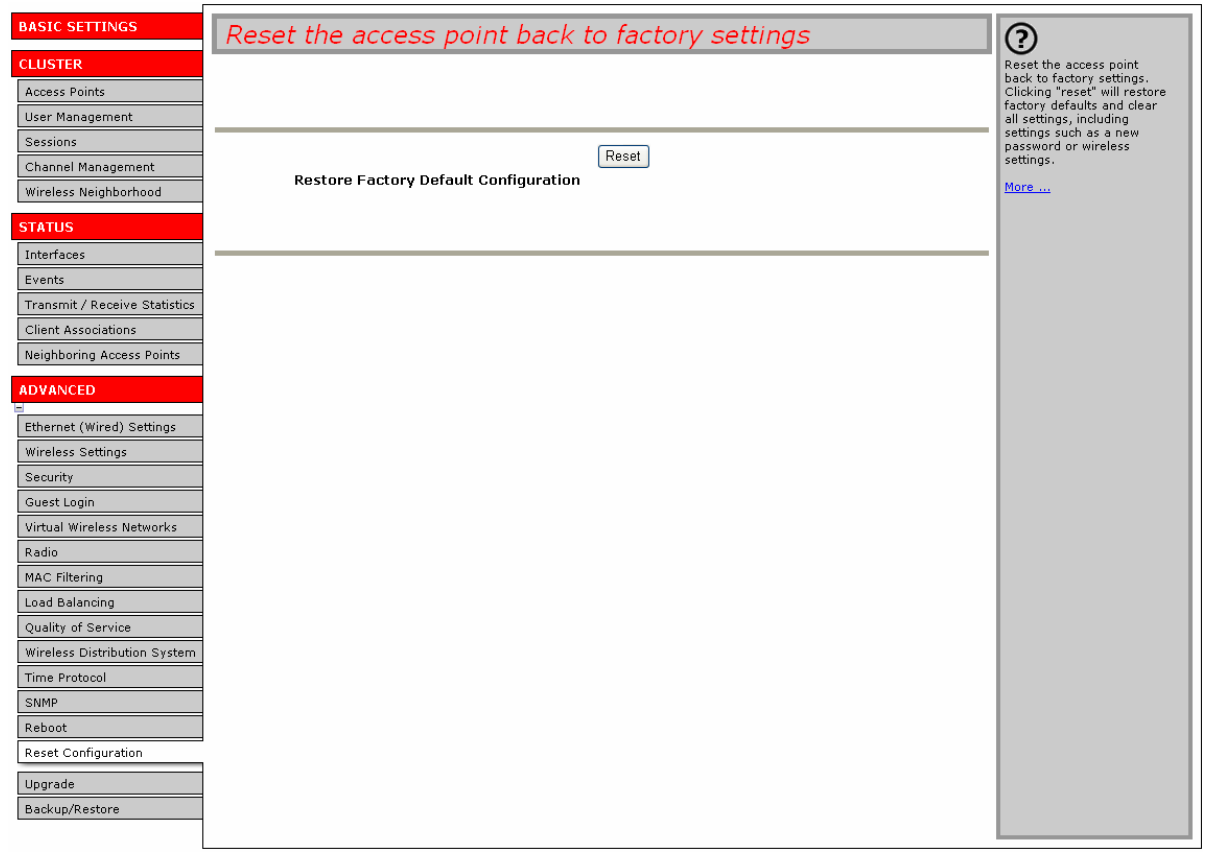
2. Click the **Reboot** button.

   The access point reboots. If the IP address of the access point changes after the reboot, you need to specify the new address in your Web browser in order to access the Web User Interface.

Reset Configuration

If you are experiencing extreme problems with the Professional Access Point and have tried all other troubleshooting measures, use the **Reset Configuration** function. This will restore factory defaults and clear all settings, including settings such as a new password and wireless settings.

1. Click the Advanced menu's **Reset Configuration** tab.



2. Click the **Reset** button.

   Factory defaults are restored.If the IP address of the access point changes after the reset, you need to specify the new address in your Web browser in order to access the Web User Interface.

Note Keep in mind that if you do reset the configuration from this page, you are doing so for this access point only; not for other access points in the cluster.

For information on the factory default settings, see “Default Settings for the Professional Access Point” on page 6.

If you cannot access the Web User Interface, you can reset the access point by using a thin object, such as a paper clip, to press the Reset button until both the LAN and WLAN LEDs turn off briefly.

Upgrade

As new versions of the Professional Access Point firmware become available, you can upgrade the

firmware on your devices to take advantages of new features and enhancements.

Caution Do not upgrade the firmware from a wireless client that is associated with the access point you are upgrading. Doing so will cause the upgrade to fail. Furthermore, all wireless clients will be disassociated and no new associations will be allowed.

If you are reading this section because you already tried to upgrade the firmware through a wireless client, use a wired client to regain access to the access point as follows:

- Create a wired Ethernet connection from a PC to the access point.
- Open the Web User Interface.

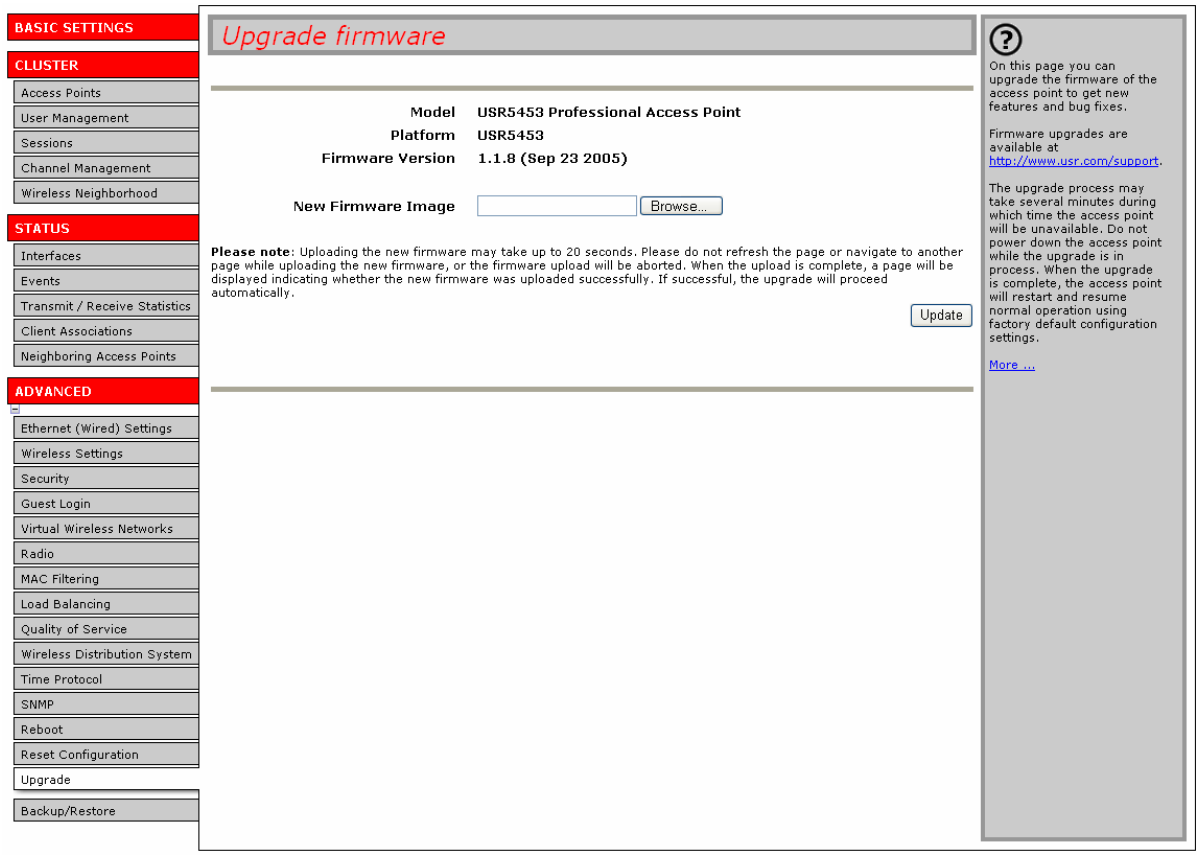
Repeat the upgrade process using with the wired client.

Caution The upgrade process may take several minutes during which time the access point will be unavailable. Do not power down the access point while the upgrade is in process. When the upgrade is complete, the access point will restart and resume normal operation.

Note You must upgrade firmware for each access point; you cannot upgrade firmware automatically across the cluster.

To upgrade the firmware on a particular access point:

1. Navigate to Advanced menu's **Upgrade** tab on the Web User Interface for that access point.



Information about the current firmware version is displayed and an option to upgrade a new firmware image is provided.

2. If you know the path to the **New Firmware Image** file, enter it in the textbox. Otherwise, click the **Browse** button and locate the firmware image file.

3. Click **Update** to apply the new firmware image.

   A confirmation window describes the upgrade process.

4. Click **OK** to confirm the upgrade and start the process.

> **Caution** The firmware upgrade takes approximately 5 minutes, during which the Web User Interface displays a status message and progress bar. Do not power off the access point, and do not navigate away from the upgrade page in your Web browser during the firmware upgrade.

When the upgrade is complete, the Web User Interface redisplays the Upgrade firmware page. You can verify that the ugrade was successful by checking the firmware version shown on that page.

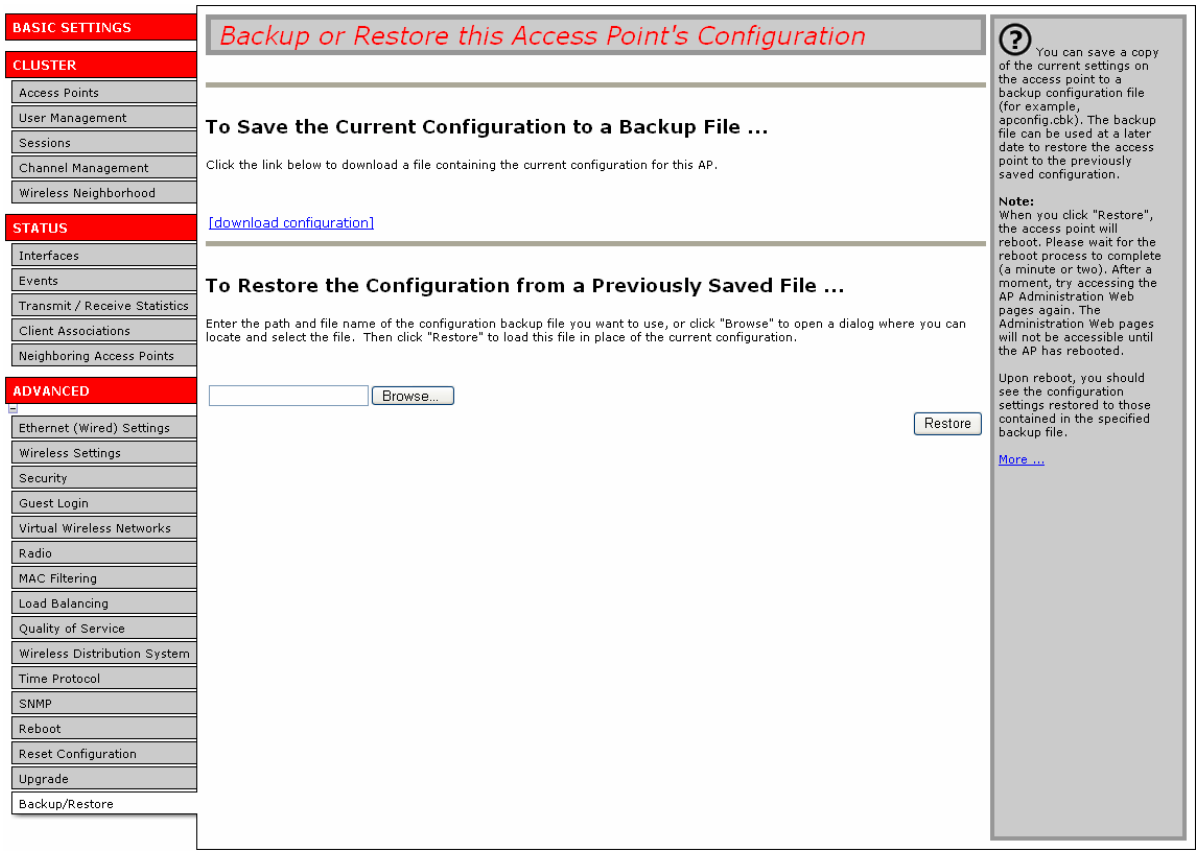
Backup/Restore

You can save a copy of the current settings on the Professional Access Point to a backup configuration file. The backup file can be used at a later date to restore the access point to the previously saved configuration.

- Navigating to Backup and Restore Settings
- Backing up Configuration Setting for an Access Point
- Restoring Access Point Settings to a Previous Configuration

Navigating to Backup and Restore Settings

To backup or restore a configuration for an access point, click the Advanced menu's **Backup and Restore** tab and use the Web User Interface as described below.



Backing up Configuration Setting for an Access Point

To save a copy of the current settings on an access point to a backup configuration file (`.cbk` format):

1. Click the **download configuration** link.

   A File Download or Open dialogue is displayed.

2. Choose the **Save** option on this first dialogue.

   This brings up a file browser.

3. Use the file browser to navigate to the directory where you want to save the file, and click **Save** to save the file.

   You can use the default file name (`apconfig.cbk`) or type a new name for the backup file, but be sure to save the file with a `.cbk` extension.

Restoring Access Point Settings to a Previous Configuration

To restore the configuration on an access point to previously saved settings:

1. Select the backup configuration file you want to use, either by typing the full path and file name in the Restore field or by clicking **Browse**, selecting the file, and clicking **Open**.

   (Only those files that were created with the Backup function and saved as `.cbk` backup configuration files are valid to use with **Restore**; for example, `apconfig.cbk`.)

2. Click the **Restore** button.

   The access point will reboot.

   Note When you click **Restore**, the access point will reboot. A reboot confirmation dialogue and follow-on rebooting status message will be displayed. Wait a minute or two for the reboot process to complete. Then try to access the Web User Interface as described in the next step; the Web User Interface will not be accessible until the access point has rebooted.

3. When the access point has rebooted, access the Web User Interface either by clicking again on one of the tabs (if the Web User Interface is still displayed) or by typing the IP address the Professional Access Point as a URL in the address field of the Web browser. Enter the URL for the access point as `http://`*`IPAddressOfAccessPoint`*.

   The Web User Interface displays the configuration settings restored from the backup file that you selected.

Command Line Interface

In addition to the Web-based user interface, the Professional Access Point includes a command line interface (CLI) for administering the access point. The CLI lets you view and modify status and configuration information.

From the client station perspective, even a single deployed Professional Access Point broadcasting its "network name" to clients constitutes a *wireless network*. Keep in mind that CLI configuration commands, like Web User Interface settings, can affect a single access point running in stand-alone mode or automatically propagate to a network of *clustered* access points that share the same settings. (For more information on clustering, see "Access Points" on page 33. For information on how to set an access point to stand-alone or cluster mode from the CLI, see "Set Configuration Policy for New Access Points" on page 29)

This part of the Professional Access Point Administrator Guide introduces the interface and provides a complete description of classes and their associated fields:

- Class Structure, Commands, and Examples
- Class and Field Reference

Class Structure, Commands, and Examples

The following topics in this appendix provide an introduction to the class structure upon which the CLI is based, CLI commands, and examples of using the CLI to get or set configuration information on an access point or cluster of APs:

- Comparison of Settings Configurable with the CLI and Web User Interface
- How to Access the CLI for an Access Point
  - Telnet Connection to the Access Point
  - SSH2 Connection to the Access Point
- Quick View of Commands and How to Get Help
- Command Usage and Configuration Examples
  - Understanding Interfaces as Presented in the CLI
  - Saving Configuration Changes
  - Basic Settings

- Access Point and Cluster Settings
- User Accounts
- Status
- Ethernet (Wired) Interface
- Wireless Interface
- Security
- Enable/Configure Guest Login Welcome Page
- Configuring Multiple BSSIDs on Virtual Wireless Networks
- Radio Settings
- MAC Filtering
- Load Balancing
- Quality of Service
- Wireless Distribution System
- Time Protocol
- Reboot the Access Point
- Reset the Access Point to Factory Defaults

- Keyboard Shortcuts and Tab Completion Help
- CLI Class and Field Overview

Comparison of Settings Configurable with the CLI and Web User Interface

The command line interface (CLI) and the Web User Interface to the Professional Access Point are designed to suit the preferences and requirements for different types of users or scenarios. Most administrators will probably use both interfaces in different contexts. Some features (such as Clustering) can only be configured from the Web User Interface, and some details and more complex configurations are only available through the CLI.

The CLI is particularly useful in that it provides an interface to which you can write programmatic scripts for access point configurations. Also, the CLI may be less resource-intensive than a Web interface.

The following table shows a feature-by-feature comparison of which settings can be configured through the CLI or the Web User Interface, and which are configurable with either.

Feature or Setting	Configurable from CLI	Configurable from Web User Interface
Basic Settings • Getting/changing Administrator Password • Getting/changing access point name and location • Viewing information like MAC, IP address, and Firmware version	**yes**	**yes**
Access Point and Cluster Settings	Get existing settings only. You cannot set configuration *policy* or other cluster features from the CLI. Use for clustering settings.	**yes**
User Accounts	**yes**	**yes**
User Database Backup and Restore	You cannot backup or restore a user database from the CLI. To restore a user database, use the Web User Interface as described in "Backing Up and Restoring a User Database" on page 46.	**yes**
Sessions	The CLI does not provide session monitoring information. To view client sessions, use the Web User Interface.	**yes**
Channel Management	You cannot configure Channel Management from the CLI. To configure channel management, use the Web User Interface as described in "Channel Management" on page 53.	**yes**
Wireless Neighborhood	You cannot view the cluster-based "Wireless Neighborhood" from the CLI. To view the wireless neighbourhood,use the Web User Interface as described in "Wireless Neighborhood" on page 61.	**yes**
Status	**yes**	**yes**

Feature or Setting	Configurable from CLI	Configurable from Web User Interface
Ethernet (Wired) Interface	**yes** You can configure all Ethernet (Wired) settings from the CLI except "Connection Type". To change the Connection Type from DHCP to Static IP addressing (or vice versa), you must use the Web User Interface.	**yes**
Wireless Interface	**yes**	**yes**
Security	**yes**	**yes**
Set Up Guest Access	**yes**	**yes**
Enable/Configure Guest Login Welcome Page	**yes**	
Configuring Multiple BSSIDs on Virtual Wireless Networks	**yes**	**yes**
Radio Settings	**yes** You can configure all Radio settings from the CLI except for turning on/off Super G.	**yes**
MAC Filtering	**yes**	**yes**
Load Balancing	**yes**	**yes**
Quality of Service	**yes**	**yes**
Wireless Distribution System	**yes**	**yes**
Time Protocol	**yes**	**yes**
Reboot the Access Point	**yes**	
Reset the Access Point to Factory Defaults	**yes**	**yes**
Upgrade the Firmware	You cannot upgrade the firmware from the CLI. To upgrade firmware, use the Web User Interface as described in "Upgrade" on page 160.	**yes**
Backup and Restore	You cannot backup or restore an access point configuration from the CLI. To backup or restore an access point configuration, use the Web User Interface as described in "Backup/Restore" on page 162.	**yes**

How to Access the CLI for an Access Point

Use one of the following methods to access the command line interface (CLI) for the access point or wireless network:

- Telnet Connection to the Access Point
- SSH2 Connection to the Access Point

Telnet Connection to the Access Point

If you already have your network deployed and know the IP address of your access point, you can use a remote Telnet connection to the access point to view the system console over the network.

Notes The default Static IP address is 192.168.1.10. If there is no DHCP server on the network, the access point retains this static IP address at first-time startup. You can use the Detection Utility to find the IP address of the access point. (For more about IP addressing, see "Understanding Dynamic and Static IP Addressing on the Professional Access Point" on page 10)

1. Bring up a command window on your PC.

   (For example, from the Start menu, select **Run** to bring up the Run dialogue, type `cmd` in the Open field, and click **OK**.)

2. At the command prompt, type the following:

   ```
   telnet IPAddressOfAccessPoint
   ```

   where *`IPAddressOfAccessPoint`* is the address of the access point you want to monitor.

   (If your Domain Name Server is configured to map domain names to IP addresses via DHCP, you can also telnet to the domain name of the access point.)

3. You will be prompted for an Administrator user name and password for the access point.

   ```
   USR5453-AP login:
   Password:
   ```

   Enter the default Administrator username and password for the Professional Access Point (`admin`, `admin`), and press "Enter" after each. (The password is masked, so it will not be displayed on the screen.)

   When the user name and password is accepted, the screen displays the Professional Access Point help command prompt.

   ```
   USR5453-AP login: admin
   Password:
   Enter 'help' for help.
   ```

   You are now ready to enter CLI commands at the command line prompt.

SSH2 Connection to the Access Point

If you already have your network deployed and know the IP address of your access point, you can use a remote SSH2 connection to the access point to view the system console over the network.

Notes

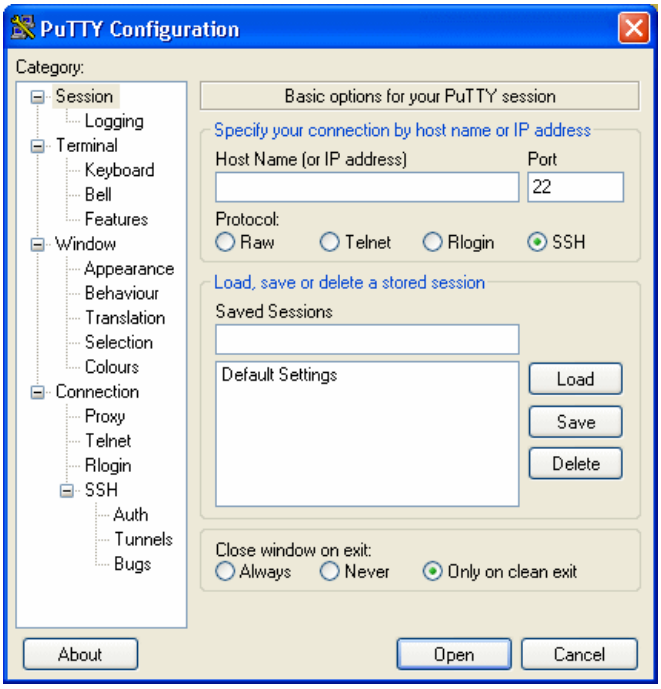
The Professional Access Point supports SSH version 2 only.

The default Static IP address is 192.168.1.10. If there is no DHCP server on the network, the access point retains this static IP address at first-time startup. You can use the Detection Utility to find the IP address of the access point. (For more about IP addressing, see "Understanding Dynamic and Static IP Addressing on the Professional Access Point" on page 10.)

Using an SSH2 connection to the access point is similar to Telnet in that it gives you remote access to the system console and CLI. SSH2 has the added advantage of being a secure connection traffic encrypted.

To use an SSH2 connection, you need to have SSH software installed on your PC (such as PuTTY, which is available at http://www.chiark.greenend.org.uk/~sgtatham/putty/).

1. Start your SSH application. (This example uses PuTTY.)



2. Enter the IP address of the access point and click **Open**.

   (If your Domain Name Server is configured to map domain names to IP addresses via DHCP, you can enter the domain name of the access point instead of an IP address.)

   This brings up the SSH command window and establishes a connection to the access point. The login prompt is displayed.

   ```
   login as:
   ```

3. Enter the default Administrator username and password for the Professional Access Point (`admin`, `admin`), and press "Enter" after each. (The password is masked, so it will not be displayed on the

screen.)

```
login as: admin
admin@10.10.100.110's password:
Enter 'help' for help.
```

When the user name and password is accepted, the screen displays the Professional Access Point help command prompt.

```
USR5453-AP#
```

You are now ready to enter CLI commands at the command line prompt.

Quick View of Commands and How to Get Help

Caution Settings updated from the CLI (with **get**, **set**, **add**, **remove** commands) will not be saved to the startup configuration unless you explicitly save them via the **save-running** command. For a description of configurations maintained on the access point and details on how to save your updates, see "“Saving Configuration Changes” on page 178.

Commands and Syntax

The CLI for the Professional Access Point provides the following commands for manipulating objects.

Notes

- *named_class* is a class of an object from the configuration whose instances are individually named.
- *instance* is a name of an instance of class.
- field values cannot contain spaces unless the value is in quotes

For a detailed class and field reference, see “Class and Field Reference” on page 239.

Command	Description
get	The "get" command allows you to get the field values of existing instances of a class. Classes can be "named" or "unnamed". The command syntax is: **get** *unnamed-class* [*field* ... | **detail**] **get** *named-class* [*instance* | **all** [*field* ... | *name* | **detail**]] The rest of the command line is optional. If provided, it is either a list of one or more *fields*, or the keyword **detail**. An example of using the "get" command on an unnamed class with a single instance is: **get log** (There is only one log on the access point. This command returns information on the log file.) An example of using the "get" command on an unnamed class with multiple instances is: **get log-entry** (There are multiple log entries but they are not named. This command returns all log entries.) An example of using the "get" command on a named class with multiple instances is: **get bss wlan0bssInternal** (There are multiple bss's and they are named. This command returns information on the BSS named "wlan0bssInternal".) An example of using the "get" command on a named class to get all instances: **get radius-user all name** **get radius-user all** **Note:** "wlan0bssInternal" is the name of the basic service set (BSS) on the internal network (wlan0 interface). For information on *interfaces*, see "Understanding Interfaces as Presented in the CLI" on page 177.

Command	Description
set	The "set" command allows you to set the field values of existing instances of a class. **set** *unnamed-class* [**with** *qualifier-field qualifier-value* ... **to**] *field value* . . . The first argument is an unnamed class in the configuration. After this is an optional qualifier that restricts the set to only some instances. For singleton classes (with only one instance) no qualifier is needed. If there is a qualifier, it starts with the keyword **with**, then has a sequence of one or more *qualifier-field qualifier-value* pairs, and ends with the keyword **to**. If these are included, then only instances whose present value of *qualifier-field* is *qualifier-value* will be set. The *qualifier-value* arguments cannot contain spaces. Therefore, you cannot select instances whose desired *qualifier-value* has a space in it. The rest of the command line contains *field-value* pairs. **set** *named-class instance* | **all** [with *qualifier-field qualifier-value* ... **to**] *field value* . . . The first argument is either a named class in the configuration. The next argument is the name of the *instance* to set, or the keyword **all**, which indicates that all instances should be set. Classes with multiple instances can be set consecutively in the same command line as shown in Example 4 below. The *qualifier-value* arguments cannot contain spaces. Here are some examples. (Bold text indicates class names, field names, or keywords; text that is not bold indicates values to which the fields are being set.) 1. **set interface wlan0 ssid** "Vicky's AP" 2. **set radio all beacon-interval** 200 3. **set tx-queue wlan0 with queue data0 to aifs** 3 4. **set tx-queue wlan0 with queue data0 to aifs** 7 **cwmin** 15 **cwmax** 1024 **burst** 0 5. **set bridge-port br0 with interface eth0 to path-cost** 200 **Note:** For information on *interfaces* used in this example (such as `wlan0`, `br0`, or `eth0`) see "Understanding Interfaces as Presented in the CLI" on page 177.
add	The "add" command allows you to add a new instance of a class. **add** *named-class instance* [*field value* ...] **add** *anonymous-class* [*field value* ...] For example: **add radius-user** wally

Command	Description
remove	The "remove" command allows you to remove an existing instance of a class. **remove** *unnamed-class* [*field value* . . .] **remove** *named-class instance* | **all** [*field value* . . .] For example: **remove radius-user** wally

The CLI also includes the following commands for maintenance tasks:

save-running	The **save-running** command saves the running configuration as the startup configuration. For more information, see "Saving Configuration Changes" on page 178.
reboot	The **reboot** command restarts the access point (a soft reboot). For more information, see "Reboot the Access Point" on page 233.
factory-reset	The **factory-reset** command resets the access point to factory defaults and reboots. For more information, see "Reset the Access Point to Factory Defaults" on page 233.

Getting Help on Commands at the CLI

Help on commands can be requested at the command line interface (CLI) by using the TAB key. This is a quick way to see all valid completions for a class.

Hitting TAB once will attempt to complete the current command.

If multiple completions exist, a beep will sound and no results will be displayed. Enter TAB again to display all available completions.

- **Example 1:** At a blank command line, hit TAB twice to get a list of all commands.

```
USR5453-AP#
add              Add an instance to the running configuration
factory-reset    Reset the system to factory defaults
get              Get field values of the running configuration
reboot           Reboot the system
remove           Remove instances in the running configuration
save-running     Save the running configuration
set              Set field values of the running configuration
```

- **Example 2:** Type "**get** " TAB TAB (including a space after **get**) to see a list of all field options for the **get** command.

```
USR5453-AP# get
association      Associated station
basic-rate       Basic rate of the radio
bridge-port      Bridge ports of bridge interfaces
bss              Basic Service Set of the radio
cluster          Clustering-based configuration settings
```

```
cluster-member   Member of a cluster of like-configured access points
config           Configuration settings
detected-ap      Detected access point
dhcp-client      DHCP client settings
dot11            IEEE 802.11
host             Internet host settings
interface        Network interface
ip-route         IP route entry
klog-entry       Kernel log entry
log              Log settings
log-entry        Log entry
mac-acl          MAC address access list item
ntp              Network Time Protocol client
portal           Guest captive portal
radio            Radio
radius-user      RADIUS user
ssh              SSH access to the command line interface
supported-rate   Supported rate of the radio
system           System settings
telnet           Telnet access to the command line interface
tx-queue         Transmission queue parameters
wme-queue        Transmission queue parameters for stations
```

- **Example 3:** Type "**get system v**" TAB. This will result in completion with the only matching field, "**get system version**". Hit ENTER to display the output results of the command.

For detailed examples on getting help, see "Tab Completion and Help" on page 234.

Ready to Get Started?

If you know the four basic commands shown above (**get**, **set**, **remove**, and **add**) and how to get help at the CLI using tab completion, you are ready to get started.

The best way to get up-to-speed quickly is to bring up the CLI on your access point and follow along with some or all of the examples in the next topic "Command Usage and Configuration Examples" on page 175.

Command Usage and Configuration Examples

Understanding Interfaces as Presented in the CLI

The following summary of interface names is provided to help clarify the related CLI commands and output results. These names are not exposed on the Web User Interface, but are used throughout the CLI. You get and set many configuration values on the access point by referring to interfaces. In order to configure the access point through the CLI, you need to understand which interfaces are available on the access point, what role they play (corresponding setting on the Web User Interface), and how to refer to them.

Interface	Description
lo	Local loopback for data meant for the access point itself.
eth0	The wired (Ethernet) interface for the Internal network.
br0	The Internal bridge represents the Internal interface for the access point. To telnet or ssh into the access point, use the IP address for this interface. br0 consists: • eth0 (or vlan*SomeNumber* if you have VLANs configured) • wlan0 The IP address of the access point is provided in the output detail for br0. So, a useful command is **get interface**. This gives you common information on all interfaces. From the output results, you can find the IP address for `br0`. Use this IP address to connect to the access point.
brguest	The Guest bridge, which consists of eth1 and wlan0guest.
brvwn1	The bridge interface for Virtual Wireless Network (VWN) 1. The bridge interface for VWN1 consists of: • `wlan0vwn1` • `vlan`*`VLANID`* where *`VLANID`* is a four-digit VLAN ID that you provided. (For example, if you provided a VLAN ID of 1234, the VLAN interface would be "`vlan1234`"
brvwn2	This is for the second Virtual Wireless Network (VWN) 2. The bridge interface for VWN2 consists of: • `wlan0vwn1` • `vlan`*`VLANID`* where *`VLANID`* is a four-digit VLAN ID that you provided. (For example, if you provided a VLAN ID of 1234, the VLAN interface would be `vlan1234`.)
wlan0	The wireless (radio) interface for the Internal network.
wlan0guest	The wireless (radio) interface for the Guest network.
wlan0vwn1	The wireless interface for Virtual Wireless Network (VWN) 1.
wlan0vwn2	The wireless interface for Virtual Wireless Network (VWN) 2.

Interface	Description
wlan0wds*x*	A wireless distribution system (WDS) interface where "x" indicates the number of the WDS link. (For example, `wlan0wds1`.)

vlanxxxx	A VLAN interface for VLAN ID `xxxx`. To find out what this VLAN interface is (Internal, Guest, VWN1 or VWN2), use the following command to look at the "`role`" field:
	
	`get interface vlan`*`VLANID`* `role`
	
	For example:
	`get interface vlan`1234 `role`

Saving Configuration Changes

The Professional Access Point maintains three different configurations.

- **Factory Default Configuration** - This configuration consists of the default settings shipped with the access point (as specified in "Default Settings for the Professional Access Point" on page 6).

  You can always return the access point to the factory defaults by using the **factory-reset** command, as described in "Reset the Access Point to Factory Defaults" on page 233.

- **Startup Configuration** - The startup configuration contains the settings that the access point will use the next time it starts up (for example, upon reboot).

  To save configuration updates made from the CLI to the *startup* configuration, you must execute the **save-running** or "**set config startup running**" command from the CLI after making changes.

- **Running Configuration** - The running configuration contains the settings with which the access point is currently running.

  When you view or update configuration settings through the command line interface (CLI) using **get**, **set**, **add**, and **remove** commands, you are viewing and changing values on the *running* configuration only. If you do not save the configuration (by executing the **save-running** or "**set config startup running**" command at the CLI), you will lose any changes you submitted via the CLI upon reboot.

The **save-running** command saves the *running* configuration as the startup configuration. (The **save-running** command is a shortcut command for "**set config startup running**", which accomplishes the same thing)

Settings updated from the CLI (with **get**, **set**, **add**, **remove** commands) will not be saved to the startup configuration unless you explicitly save them via the **save-running** command. This gives you the option of maintaining the *startup* configuration and trying out values on the *running* configuration that you can discard (by not saving).

By contrast, configuration changes made from the Web User Interface are automatically saved to both the *running* and *startup* configurations. If you make changes from the Web User Interface that you do not want to keep, your only option is to reset to factory defaults. The previous startup configuration will be lost.

Basic Settings

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 177. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface, or to the Internal or Guest network.

The following CLI command examples correspond to tasks you can accomplish on the Basic Settings tab of the Web User Interface for access points with clustering capabilities. In some cases, the CLI **get** command provides additional details not available through the Web User Interface.

This table shows a quick view of Basic Settings commands and provides links to detailed examples.

Basic Setting	Example

Get the IP Address for the Internal Interface on an Access Point	`get interface br0 ip`
	or
	`get interface`
	
	get interface is a catch-all command that shows common information on all interfaces for the access point such as IP addresses, MAC addresses, and so on. The IP address for the Internal interface (and the one used to access the access point) is that shown for br0. (See "Understanding Interfaces as Presented in the CLI" on page 177)

Get the MAC Address for an Access Point	`get interface br0 mac`
Get Both the IP Address and MAC Address	`get interface br0 mac ip`
Get Common Information on All Interfaces for an Access Point	`get interface`
Get the Firmware Version for the Access Point	`get system version`
Get the Location of the Access Point	`get cluster location`

Set the Location for an Access Point	`set system location` *`NewLocation`*
	
	For example:
	`set system location hallway`
	or
	`set system location "Vicky's Office"`

Get the Current Password	`get system encrypted-password`
Set the Password	`set system password` *`NewPassword`* For example: `set system password admin`
Get the Wireless Network Name (SSID))	`get interface wlan0 ssid`

Basic Setting	Example

Set the Wireless Network Name (SSID)	`set interface wlan0 ssid NewSSiD`
	
	For example:
	`set interface wlan0 ssid Vicky`
	`set interface wlan0 ssid "Vicky's AP"`

Get the IP Address for the Internal Interface on an Access Point

In the following example, the IP address for the access point is: 10.10.55.216. Use the **get** command as shown to obtain the IP address for the Internal network.

```
USR5453-AP# get interface br0 ip
10.10.55.216
```

Get the MAC Address for an Access Point

In the following example, the MAC address for the access point is: 00:a0:c9:8c:c4:7e. Use the **get** command as shown to obtain the MAC address.

```
USR5453-AP# get interface br0 mac
00:a0:c9:8c:c4:7e
```

Get Both the IP Address and MAC Address

The following command returns both the IP address and the MAC address for an access point:

```
USR5453-AP# get interface br0 mac ip
Field  Value
---------------------
ip     10.10.55.216
mac    00:a0:c9:8c:c4:7e
```

Get Common Information on All Interfaces for an Access Point

The following example shows common information (including IP addresses) for all interfaces.

```
USR5453-AP# get interface
name         type          status  mac                ip              mask
-------------------------------------------------------------------------
-----
lo                        up      00:00:00:00:00:00  127.0.0.1       255.0.0.0
eth0                      up      00:02:B3:01:01:01
eth1                      down    00:02:B3:02:02:02
br0          bridge       up      00:02:B3:01:01:01  10.10.100.110
255.255.255.0
brguest      bridge       down    00:00:00:00:00:00
wlan0        service-set  up      00:0C:41:16:DF:A6
wlan0guest   service-set  up
wlan0wds0    wds          down
```

```
wlan0wds1    wds           down
wlan0wds2    wds           down
wlan0wds3    wds           down
USR5453-AP#
```

Get the Firmware Version for the Access Point

In the following example, the access point is running Firmware Version: 1.0.0.9. Use the **get** command as shown to obtain the Firmware Version.

```
USR5453-AP# get system version
1.0.0.9
```

Get the Location of the Access Point

In the following example, the location of the access point has not been set. Use the **get** command as shown to obtain the location of the access point.

```
USR5453-AP# get cluster location
not set
```

Set the Location for an Access Point

To set the location for an access point, use the **set** command as follows:

```
USR5453-AP# set system location hallway
USR5453-AP# set system location "Vicky's Office"
```

To check to make sure that the location was set properly, use the **get** command again to find out the location

```
USR5453-AP# get system location
Vicky’s Office
```

Get the Current Password

```
USR5453-AP# get system encrypted-password
2yn.4fvaTgedM
```

Set the Password

```
USR5453-AP# set system password admin
USR5453-AP# get system encrypted-password
/rYSvxS4Okptc
```

Get the Wireless Network Name (SSID)

```
USR5453-AP# get interface wlan0 ssid
Internal Instant802 Network
```

Set the Wireless Network Name (SSID)

```
USR5453-AP# set interface wlan0 ssid "Vicky’s AP"
USR5453-AP# get interface wlan0 ssid
Vicky’s AP
```

Access Point and Cluster Settings

The command examples in this section show how to get the configuration for a cluster of access points. These settings generally correspond to those on the Cluster menu's Access Points tab in the Web User Interface.

Note You cannot use the CLI to add or remove an access point from a cluster or set the configuration policy. If you want to configure clustering, please use the Web User Interface as described in "Access Points" on page 33

This table provides a quick view of Access Point Cluster commands and provides links to detailed examples.

Cluster Command	Example
Determine whether the Access Point is a Cluster Member or is in Stand-alone Mode	`get cluster detail`
Get MAC Addresses for all Access Points in the Cluster	`get clustered-ap all name`

Determine whether the Access Point is a Cluster Member or is in Stand-alone Mode

This command shows whether the access point is clustered or not. If the command returns 0, the access point is in stand-alone mode (not clustered). If the command returns 1, the access point is a member of a cluster. In the following example, the access point is in stand-alone mode.

```
USR5453-AP# get cluster detail
Field        Value
--------------------
clustered    0
clusterable  0
kickstarted  0
location     not set
formation
```

Get MAC Addresses for all Access Points in the Cluster

```
USR5453-AP# get cluster-member all
name               mac                ip             location  removed
-------------------------------------------------------------------------
00:e0:b8:76:23:b4  00:e0:b8:76:23:b4  10.10.10.248   not set   0
00:e0:b8:76:16:88  00:e0:b8:76:16:88  10.10.10.230   not set   0
```

User Accounts

The following command examples show configuration tasks related to user accounts. These tasks correspond to the Cluster menu's User Management tab in the Web User Interface.

This table shows a quick view of User Management commands and provides links to detailed examples.

User Account Command	Example

Get All User Accounts	To view all usernames:
	`get radius-user all name`
	
	To view all user accounts:
	`get radius-user all`

Add Users	add radius-user *UserName* For example: `add radius-user samantha`
To set the user's real name:	set radius-user *UserName RealName* For example: `set radius-user samantha "Elizabeth Montgomery"` (or `set radius-user samantha Elizabeth`)
To set user's password:	set radius-user *UserName* password *Password* For example: `set radius-user samantha password westport`
Remove a User Account	`remove radius-user` *UserName*

Get All User Accounts

To view all user names:

```
USR5453-AP# get radius-user all name
name
--------
larry
```

To view all user accounts:

```
USR5453-AP# get radius-user all
name      username  disabled  password  realname
-------------------------------------------------------------
larry                                   David White
```

(At the start, "larry" is the only user configured.)

Add Users

In this example, you will add four new users: (1) samantha, (2) endora, (3) darren, and (4) wally. You will set up user names, real names, and passwords for each.

1. Add **username** "samantha":

```
USR5453-AP# add radius-user samantha
```

2. Provide a **real name** (Elizabeth Montgomery) for this user:

```
USR5453-AP# set radius-user samantha realname "Elizabeth Montgomery"
```

3. Set the user **password** for samantha to "westport":

```
USR5453-AP# set radius-user samantha password westport
```

4. Repeat this process to add some other users (endora, darren, and wally):

```
USR5453-AP# add radius-user endora
USR5453-AP# set radius-user endora realname "Agnes Moorhead"
USR5453-AP# set radius-user endora password scotch
USR5453-AP# add radius-user darren
USR5453-AP# set radius-user darren realname "Dick York"
USR5453-AP# set radius-user darren password martini
USR5453-AP# add radius-user wally
USR5453-AP# set radius-user wally realname "Tony Dow"
USR5453-AP# set radius-user wally password sodapop
```

5. After configuring these new accounts, use the "**get**" command to view all users. (Passwords are always hidden.)

```
USR5453-AP# get radius-user all
name      username  disabled  password  realname
-----------------------------------------------------------
larry                                   David White
samantha                                Elizabeth Montgomery
endora                                  Agnes Moorhead
darren                                  Dick York
wally                                   Tony Dow
```

Remove a User Account

To remove a user account, type the following

```
USR5453-AP# remove radius-user wally
```

Use the "**get**" command to view all user names. (You can see "wally" has been removed.)

```
USR5453-AP# get radius-user all name
name
--------
larry
samantha
endora
darren
```

Status

The command tasks and examples in this section show status information on access points. These settings correspond to what is shown on the Status tabs in the Web User Interface. ("Status" on page 67)

This table provides a quick view of all Status commands and links to detailed examples.

Note Make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 177. The interface name you reference in a **get** command determines whether the command output shows a wired or wireless interface or the Internal or Guest network.

This table shows a quick view of Status commands and provides links to detailed examples

Status Command	Example
Understanding Interfaces as Presented in the CLI	Reference of interface names and purposes as described in "Understanding Interfaces as Presented in the CLI" on page 177.
Global command to get all detail on a Basic Service Set (BSS). This is a useful command to use to get a comprehensive understanding of how the access point is currently configured.	`get bss all detail`
Get Common Information on the Internal Interface for the Access Point	`get interface br0`
Get All Wired Settings for the Wired Internal Interface	`get interface br0`

Get Current Settings for the Ethernet (Wired) Guest Interface	`get interface brguest`
	`get interface brguest mac`
	`get interface brguest ssid`

Get the MAC Address for the Wired Internal Interface	`get interface wlan0 mac`
Get the Network Name (SSID) for the Wired Internal Interface	`get interface wlan0 ssid`
Get the Current IEEE 802.11 Radio Mode	`get radio wlan0 mode`
Get the Channel the Access Point is Currently Using	`get radio wlan0 channel`
Get Basic Radio Settings for the Internal Interface	`get radio wlan0` `get radio wlan0 detail`
Get Status on Events	`get log-entry all`

Status Command	Example
Enable Remote Logging and Specify the Log Relay Host for the Kernel Log	As a prerequisite to remote logging, the Log Relay Host must be configured first as described in Setting Up the Log Relay Host. See complete explanation of CLI commands at Enable Remote Logging and Specify the Log Relay Host for the Kernel Log. Here are a few: `set log relay-enabled 1` enables remote logging `set log relay-enabled 1` disables remote logging `get log` `set log` TAB TAB shows values you can set on the log
Get Transmit / Receive Statistics	`get interface all ip mac ssid tx-packets tx-bytes tx-errors rx-packets rx-bytes rx-errors`
Get Client Associations	`get association`
Get neighbouring Access Points	`get clustered-ap`

Get Common Information on the Internal Interface for the Access Point

The following command obtains all information on the internal interface for an access point:

```
USR5453-AP# get interface br0
Field           Value
--------------------
type            bridge
status          up
hello           10
mac             00:a0:c9:8c:c4:7e
ip              192.168.1.1
mask            255.255.255.0
```

Get Current Settings for the Ethernet (Wired) Internal Interface

The following example shows how to use the CLI to get the Ethernet (Wired) settings for the Internal interface for an access point. You can see by the output results of the command that the MAC address is 00:a0:c9:8c:c4:7e, the IP address is 192.168.1.1, and the subnet mask is 255.255.255.0.

Get All Wired Settings for the Wired Internal Interface

```
USR5453-AP# get interface br0
Field           Value
--------------------
mac             00:a0:c9:8c:c4:7e
ip              192.168.1.1
mask            255.255.255.0
```

Get the MAC Address for the Wired Internal Interface

```
USR5453-AP# get interface wlan0 mac
02:0C:41:00:02:00
```

Get the Network Name (SSID) for the Wired Internal Interface

```
USR5453-AP# get interface wlan0 ssid
```

```
elliot_AP
```

Get Current Settings for the Ethernet (Wired) Guest Interface

The following example shows how to use the CLI to get the Ethernet (Wired) settings for the Guest interface for an access point. You can see by the output results of the command that the MAC address is 00:50:04:6f:6f:90, the IP address is 10.10.56.248, and the subnet mask is 255.255.255.0.

```
USR5453-AP# get interface brguest
Field          Value
--------------------
type           bridge
status         up
mac            00:50:04:6f:6f:90
ip             10.10.56.248
mask           255.255.255.0
```

Note You can get specifics on the Guest interface by using the same types of commands as for the Internal interface but substituting `brguest` for `wlan0`. For example, to get the MAC address for the guest interface: `get interface wlan0 ssid`

Get Current Wireless (Radio) Settings

The following examples show how to use the CLI to get wireless radio settings on an access point, such as mode, channel, and so on. You can see by the results of the commands that the access point mode is set to IEEE 802.11g, the channel is set to 6, the beacon interval is 100, and so forth.

For information on how to configure Radio settings through the CLI, see "Radio Settings" on page 217.

(Radio settings are fully described in "Configuring Radio Settings" on page 120.)

Get the Current IEEE 802.11 Radio Mode

```
USR5453-AP# get radio wlan0 mode
g
```

Get the Channel the Access Point is Currently Using

```
USR5453-AP# get radio wlan0 channel
2
```

Get Basic Radio Settings for the Internal Interface

```
USR5453-AP# get radio wlan0
Field                     Value
------------------------------
status                    up
max-bsses                 2
channel-policy            best
channel                   6
static-channel            9
mode                      g
fragmentation-threshold   2346
rts-threshold             2347
ap-detection              on
beacon-interval           100
```

Get All Radio Settings on the Internal Interface

```
USR5453-AP# get radio wlan0 detail
Field                                          Value
-----------------------------------------------------
status                                         up
description                                    IEEE 802.11
mac
max-bss                                        2
channel-policy                                 best
mode                                           g
static-channel                                 11
channel                                        2
tx-power                                       100
tx-rx-status                                   up
beacon-interval                                100
rts-threshold                                  2347
fragmentation-threshold                        2346
load-balance-disassociation-utilization        0
load-balance-disassociation-stations           0
load-balance-no-association-utilization        0
ap-detection                                   on
station-isolation                              off
frequency                                      2417
wme                                            on
```

Get Status on Events

```
USR5453-AP# get log-entry all
Number  Time              Priority  Daemon
        Message
-------------------------------------------------------
1       Apr 20 21:39:55    debug     udhcpc
        Sending renew...
2       Apr 20 21:39:55    info      udhcpc
        Lease of 10.10.55.216 obtained, lease time 300
3       Apr 20 21:37:25    debug     udhcpc
        Sending renew...
4       Apr 20 21:37:25    info      udhcpc
        Lease of 10.10.55.216 obtained, lease time 300
5       Apr 20 21:34:55    debug     udhcpc
        Sending renew...
6       Apr 20 21:34:55    info      udhcpc
        Lease of 10.10.55.216 obtained, lease time 300
```

Enable Remote Logging and Specify the Log Relay Host for the Kernel Log

The Kernel Log is a comprehensive list of system even its and kernel messages such as error conditions like dropping frames. To capture Access Point Kernel Log messages you need access to a remote syslog server on the network. The following sections describe how to set up remote logging for the access point.

1. Prerequisites for Remote Logging
2. View Log Settings
3. Enable / Disable Log Relay Host

4. Specify the Relay Host
5. Specify the Relay Port
6. Review Log Settings After Configuring Log Relay Host

Prerequisites for Remote Logging

To capture Kernel Log messages from the access point system, you must first set up a remote server running a syslog process and acting as a syslog "log relay host" on your network. (For information on how to set up the remote server, see “Setting Up the Log Relay Host” on page 70.)

Then, you can use the CLI to configure the Professional Access Point to send its syslog messages to the remote server.

View Log Settings

To view the current log settings:

```
USR5453-AP# get log
Field          Value
-------------------------
depth          15
relay-enabled 0
relay-host
relay-port     514
```

When you start a new access point, the Log Relay Host is disabled. From the above output for the "`get log`" command, you can identify the following about the Log Relay Host (syslog server):

- The syslog server is *disabled* (because "relay-enabled" is set to "0")
- No IP address or Host Name is specified for the syslog server.
- The access point is listening for syslog messages on the default port 514

Enable / Disable Log Relay Host

To enable the Log Relay Host:

```
USR5453-AP# set log relay-enabled 1
```

To disable the Log Relay Host:

```
USR5453-AP# set log relay-enabled 0
```

Specify the Relay Host

To specify the Relay Host, provide either the IP Address or a DNS name for the Log Relay Host as parameters to the "**set log relay-host**" command as shown below.

Note If you are using Instant802 Conductor, the Repository Server should receive the syslog messages from all access points. In this case, use the IP address of the Conductor Repository Server as the Relay Host.

- To specify an IP address for the syslog server:

```
set log relay-host IP_Address_Of_LogRelayHost
```

Where *IP_Address_Of_LogRelayHost* is the IP Address of the Log Relay Host.

For example:

```
USR5453-AP# set log relay-host 10.10.5.220
```

- To specify a Host Name for the syslog server:

```
set log relay-host Host_Name_Of_LogRelayHost
```

Where *Host_Name_Of_LogRelayHost* is the a DNS name for the Log Relay Host.

For example:

```
USR5453-AP# set log relay-host myserver
```

Specify the Relay Port

To specify the Relay Port for the syslog server:

```
set log relay-port Number_Of_LogRelayPort
```

Where *Number_Of_LogRelayPort* is the port number for the Log Relay Host.

For example:

```
USR5453-AP# set log relay-port 514
```

Review Log Settings After Configuring Log Relay Host

To view the current log settings:

```
USR5453-AP# get log
Field          Value
-------------------------
depth          15
relay-enabled  1
relay-host     10.10.5.220
relay-port     514
```

From the above output for the "`get log`" command, you can identify the following about the Log Relay Host (syslog server):

- The syslog server is *enabled* (because "relay-enabled" is set to "1")
- The syslog server is at the IP address `10.10.5.220`
- The access point is listening for syslog messages on the default port 514

Get Transmit / Receive Statistics

```
USR5453-AP# get interface all ip mac ssid tx-packets tx-bytes tx-errors rx-packets
rx-bytes rx-errors
```

```
Name         Ip             Mac                 Ssid                Tx-packets
             Tx-bytes  Tx-errors  Rx-packets  Rx-bytes  Rx-errors
------------------------------------------------------------------------------
lo           127.0.0.1      00:00:00:00:00:00                      1319
              151772   0           1319        151772   0
eth0                        00:A0:C9:8C:C4:7E                      4699
             3025566   0          11323       1259824   0
eth1         0.0.0.0        00:50:04:6F:6F:90                       152
               49400   0           6632        664298   0
br0          10.10.55.216   00:A0:C9:8C:C4:7E                      4699
             3025566   0          10467        885264   0
brguest      10.10.56.248   00:50:04:6F:6F:90                       152
               48032   0           5909        293550   0
wlan0        0.0.0.0        02:0C:41:00:02:00  AAP1000 (Trusted)   6483
              710681   0              0             0   0
wlan0guest   0.0.0.0        02:0C:41:00:02:01  AAP1000 (Guest)     5963
              471228   0              0             0   0
wlan0wds0
wlan0wds1
wlan0wds2
wlan0wds3
```

Get Client Associations

```
USR5453-AP# get association
Interf Station            Authen Associ Rx-pac Tx-pac Rx-byt Tx-byt Tx-rat
wlan0  00:0c:41:8f:a7:72  Yes    Yes    126    29      9222   3055  540
wlan0  00:09:5b:2f:a5:2f  Yes    Yes    382    97     16620  10065  110
USR5453-AP# get association detail
Inter  Station            Authe Assoc Rx-pa Tx-pa Rx-byt Tx-byt Tx-ra Liste
wlan0  00:0c:41:8f:a7:72  Yes   Yes   126   29     9222   3055  540   1
wlan0  00:09:5b:2f:a5:2f  Yes   Yes   382   97    16620  10065  110   1
```

Get neighbouring Access Points

The Neighboring access point view shows wireless networks within range of the access point. These commands provide a detailed view of neighboring access points including identifying information (SSIDs and MAC addresses) for each, and statistical information such as the channel each access point is broadcasting on, signal strength, and so forth.

To see the kinds of information about access point neighbours you can search on, type **`get detected-ap`** TAB TAB.

```
USR5453-AP# get detected-ap
[Enter]           * Get common fields *
band              Frequency band
beacon-interval   Beacon interval in kus (1.024 ms)
capability        IEEE 802.11 capability value
channel           Channel
detail            * Get all fields *
erp               ERP
last-beacon       Time of last beacon
mac               MAC address
```

```
num_beacons       Number of beacons received
phy-type          PHY mode detected with
privacy           WEP or WPA enabled
rate              Rate
signal            Signal strength
ssid              Service Set IDentifier (a.k.a., Network Name)
supported-rates   Supported rates list
type              Type (AP, Ad hoc, or Other)
wpa               WPA security enabled
```

To get the neighbouring access points, type **`get detected-ap`**.

```
USR5453-AP# get detected-ap
Field    Value
---------------------------------------
mac      00:e0:b8:76:28:e0
type     AP
privacy  On
ssid     Purina
channel  6
signal   2

Field    Value
---------------------------------------
mac      00:0e:81:01:01:62
type     AP
privacy  Off
ssid     Internal Instant802 Network
channel  6
signal   1

Field    Value
---------------------------------------
mac      00:e0:b8:76:1a:f6
type     AP
privacy  Off
ssid     domani
channel  6
signal   3

Field    Value
---------------------------------------
mac      00:e0:b8:76:28:c0
type     AP
privacy  Off
ssid     domani
channel  6
signal   4
```

Ethernet (Wired) Interface

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 177. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network.

This table shows a quick view of commands for getting and setting values for the Wired interface and provides links to detailed examples.

Wired Interface Command	Example
Get Summary View of Internal and Guest Interfaces	`get bss`
Get the DNS Name	`get host id`

Set the DNS Name	`set host id HostName`
	
	For example:
	`set host id vicky-ap`

Get Current Settings for the Ethernet (Wired) Internal Interface	`get interface br0`
Get Current Settings for the Ethernet (Wired) Guest Interface	`get interface brguest`
Set Up Guest Access	Setting up Guest Access consists of configuring Internal and Guest Wired interfaces on VLANs. For detailed examples, see "Set Up Guest Access" on page 195.
Find out if Guest Access is enabled and configured.	`get interface brguest status` (will be "up" or "down")
Get/Change the Connection Type (DHCP or Static IP)	See detailed example in "Get/Change the Connection Type (DHCP or Static IP)" on page 198.
Re-Configure Static IP Addressing Values	For detailed examples see: "Set the Static IP Address" on page 199 "Set the Static Subnet Mask Address" on page 199 "Set the Static Subnet Mask Address" on page 199
Set DNS Nameservers to Use Static IP Addresses (Dynamic to Manual Mode)	See example below.
Set DNS Nameservers to Use DHCP IP Addressing (Manual to Dynamic Mode)	See example below.

Get Summary View of Internal and Guest Interfaces

```
USR5453-AP# get bss
name              status  radio  beacon-interface  mac
------------------------------------------------------------------
wlan0bssInternal  up      wlan0  wlan0             00:0C:41:16:DF:A6
wlan0bssGuest     down    wlan0  wlan0guest
```

Get the DNS Name

```
USR5453-AP# get host id
USR5453-AP
```

Set the DNS Name

```
USR5453-AP# set host id vicky-ap
bob# get host id
vicky-ap
```

Get Wired Internal Interface Settings

See "Get Current Settings for the Ethernet (Wired) Internal Interface" on page 187 under Status.

Get Wired Guest Interface Settings

See "Get Current Settings for the Ethernet (Wired) Guest Interface" on page 188 under Status.

Set Up Guest Access

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 177. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network.

Configuring a Guest interface from the CLI is a complex task. Unless this is your area of expertise, you may find it easier to use the Web User Interface to set up Guest Access. For information on how to set up Guest Access from the Web User Interface, see "Ethernet (Wired) Settings" on page 79 and "Guest Login" on page 111.

Before configuring guest or internal interface settings, make sure you are familiar the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 177.

Note After you configure the Guest Network (as described in the sections below), you can enable a "captive portal" Welcome page for guest clients who are using the Web over your Guest network. You can modify the Welcome page text that is displayed to guests when they log on to the Web. For more information, see "Enable/Configure Guest Login Welcome Page" on page 215.

The following Guest Access configuration examples are provided:

- Enable / Configure Guest Access on VLANs

- Disable Guest Access on VLANs
- Change VLAN IDs (VLANs Must Be Enabled Already)

Enable / Configure Guest Access on VLANs

Caution

- You cannot use an ssh or telnet connection to configure VLANs, because you will lose network connectivity to the access point when you remove the bridge-port. Therefore, you cannot configure VLANs through the CLI.
- Be sure to verify that the switch and DHCP server you are using can support VLANs per the 802.1Q standard. After configuring the VLAN on the Advanced menu's Ethernet (Wired) Settings page, physically reconnect the Ethernet cable on the switch to the tagged packet (VLAN) port. Then, re-connect via the Web User Interface to the new IP address. (If necessary, check with the infrastructure support administrator regarding the VLAN and DHCP configurations.)

This example assumes you start with Guest Access "disabled" and provides commands to enable it on VLANs.

1. Get the current status of Guest Access (it is "down" or disabled initially):

```
USR5453-AP# get interface brguest status
down
```

2. Enable Guest and remove bridge-port:

```
USR5453-AP# set bss wlan0bssGuest status up
USR5453-AP# set bss wlan1bssGuest status up
USR5453-AP# set interface brguest status up
USR5453-AP# set portal status up
USR5453-AP# remove bridge-port br0 interface eth0
```

3. Enable VLANs:

```
USR5453-AP# add interface vlan1111 type vlan status up vlan-id 1111 vlan-interface
eth0
USR5453-AP# add bridge-port br0 interface vlan1111
USR5453-AP# add interface vlan2222 type vlan status up vlan-id 2222 vlan-interface
eth0
USR5453-AP# add bridge-port brguest interface vlan2222
```

4. Check the current settings:

```
USR5453-AP# get bss
name              status  radio  beacon-interface  mac
------------------------------------------------------------------
wlan0bssInternal  up      wlan0  wlan0             00:01:02:03:04:01
wlan0bssGuest     up      wlan0  wlan0guest        00:01:02:03:04:02

USR5453-AP# get interface brguest
Field   Value
------------------------
type    bridge
status  up
mac     00:01:02:03:04:02
```

```
ip      10.10.56.248
mask    255.255.255.0
```

Disable Guest Access on VLANs

This example assumes you start with Guest Access "enabled" on VLANs and provides commands to disable it.

1. Get the current status of Guest Access (it is "up" or enabled initially):

   ```
   USR5453-AP# get interface brguest status
   up
   ```

   The output for the following commands show that VLANs are configured for the Internal and Guest interfaces (because both interfaces are VLANs: "`brguest`" is `vlan2222` and "`br0`" is `vlan1111`):

   ```
   USR5453-AP# get bridge-port brguest
   Name     Interface
   -------------------
   brguest  wlan0
   brguest  vlan2222

   USR5453-AP# get bridge-port br0
   Name  Interface
   ---------------
   br0   wlan0guest
   br0   vlan1111
   ```

2. The following series of commands reconfigures the Internal interface to use an Ethernet port (by setting `br0` to `eth0`), disables Guest Access, and removes the two VLANs.

   ```
   USR5453-AP# add bridge-port br0 interface eth0
   USR5453-AP# set bss wlan0bssGuest status down
   USR5453-AP# set bss wlan1bssGuest status down
   USR5453-AP# remove bridge-port br0 interface vlan1111
   USR5453-AP# remove interface vlan1111
   USR5453-AP# remove bridge-port brguest interface vlan2222
   USR5453-AP# remove interface vlan2222
   USR5453-AP# set interface brguest status down
   USR5453-AP# set portal status down
   ```

Change VLAN IDs (VLANs Must Be Enabled Already)

1. Check the current configuration of Wired interfaces.

   The output of the following command shows that the Guest interface is already configured on VLANs:

   ```
   USR5453-AP# get bridge-port br0
   Name  Interface
   ---------------
   br0   wlan0guest
   br0   vlan1111
   ```

2. Set up a new VLAN and remove the old one:

```
USR5453-AP# set interface vlan1111 vlan-id 1112
Error: vlan-id cannot be changed after insert.
USR5453-AP# remove bridge-port br0 interface vlan1111
USR5453-AP# remove interface vlan1111
USR5453-AP# add interface vlan1113 type vlan status up vlan-id 1113 vlan-interface
eth0
```

Get/Change the Connection Type (DHCP or Static IP)

Note For more information on DHCP and Static IP connection types, see the topic ""Understanding Dynamic and Static IP Addressing on the Professional Access Point" on page 10.

To get the connection type:

```
USR5453-AP# get dhcp-client status
up
```

You cannot use the CLI to reset the connection type from DHCP to Static IP because you will lose connectivity during the process of assigning a new static IP address. To make such a change, use the Web User Interface on a computer connected to the access point with an Ethernet cable.

To reset the connection type from Static IP to DHCP:

```
USR5453-AP# set dhcp-client status up
```

To view the new settings:

```
USR5453-AP# get interface br0 detail
Field             Value
----------------------------------
type              bridge
status            up
description       Bridge - Internal
mac               00:E0:B8:76:23:B4
ip                10.10.12.221
mask              255.255.255.0
static-ip         10.10.12.221
static-mask       255.255.255.0
nat
```

Re-Configure Static IP Addressing Values

Note This section assumes you have already set the access point to use Static IP Addressing and set some initial values as described in "Get/Change the Connection Type (DHCP or Static IP)" on page 198.

If you are using static IP addressing on the access point (instead of DHCP), you may want to reconfigure the static IP address, subnet mask, default gateway, or DNS name servers.

The following examples show how to change these values from the CLI. With the exception of DNS name servers, these values can only be reconfigured if you are using Static IP Addressing mode.

You do have the option of manually configuring DNS name servers for either a DHCP or Static IP connection type, so that task is covered in a separate section following this one.

Set the Static IP Address

1. Check to see what the current static IP address is. (In this example, the current static IP address is the factory default.)

```
USR5453-AP# get interface br0 static-ip
10.10.12.221
```

2. Re-set to a new static IP address:

```
USR5453-AP# set interface br0 static-ip 10.10.12.81
```

Set the Static Subnet Mask Address

1. Check to see the current Subnet Mask. (In this example, the current subnet mask is the factory default.)

```
USR5453-AP# get interface br0 static-mask
255.255.255.0
```

2. Re-set to a new static Subnet Mask:

```
USR5453-AP# set interface br0 static-mask 255.255.255.128
```

Set the IP Address for the Default Gateway

This example sets the Default Gateway to 10.10.12.126:

```
USR5453-AP# set ip-route with gateway 10.10.12.126 in-use yes
```

Set DNS Nameservers to Use Static IP Addresses (Dynamic to Manual Mode)

This example shows how to reconfigure DNS Nameservers from *Dynamic* mode (where name server IP addresses are assigned through DHCP) to *Manual* mode, and specify static IP addresses for them.

1. Check to see which mode the DNS Name Service is running in. (In this example, DNS naming is running in DHCP mode initially because the following command returns `up` for the mode.)

```
USR5453-AP# get host dns-via-dhcp
up
```

2. Turn off Dynamic DNS Nameservers and re-check the settings:

```
USR5453-AP# set host dns-via-dhcp down
USR5453-AP# get host dns-via-dhcp
down
```

3. Get the current IP addresses for the DNS Nameservers:

```
USR5453-AP# get host static-dns-1
10.10.3.9

USR5453-AP# get host static-dns-2
10.10.3.11
```

4. Re-set the IP addresses for the DNS Nameservers as desired:

```
USR5453-AP# set host static-dns-1 10.10.3.10
USR5453-AP# get host static-dns-1
10.10.3.10

USR5453-AP# set host static-dns-2 10.10.3.12
USR5453-AP# get host static-dns-2
10.10.3.12
```

Set DNS Nameservers to Use DHCP IP Addressing (Manual to Dynamic Mode)

To switch DNS Nameservers from Manual (static IP addresses) to Dynamic mode (nameserver addresses assigned by DHCP), use the reverse command and check to see the new configuration:

```
USR5453-AP# set host dns-via-dhcp up
USR5453-AP# get host dns-via-dhcp
up
```

Wireless Interface

To set up a wireless (radio) interface, configure the following on each interface (Internal or Guest) as described in other sections of this CLI document.

- Configure the Radio Mode and Radio Channel as described in “Configure Radio Settings” on page 219.
- Configure the Network Name as described in “Set the Wireless Network Name (SSID)” on page 182.

Security

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 177. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network.

The following sections show examples of how to use the CLI to view and configure security settings on the access point. These settings correspond to those available in the Web User Interface on the Advanced menu’s Security tab. For a detailed discussion of concepts and configuration options, see“Security” on page 91.

This section focuses on configuring security on the *Internal* network. (Security on the *Guest* network defaults to **None**. See “When to Use No Security” on page 92.)

This table shows a quick view of Security commands and links to detailed examples.

Security Command	Example
Get the Current Security Mode	`get interface wlan0 security`

Security Command	Example

Get Detailed Description of Current Security Settings	`get bss wlan0bssInternal detail`
	
	`get interface wlan0 detail`

Set the Broadcast SSID (Allow or Prohibit)	`set bss wlan0bssInternal ignore-broadcast-ssid on`
	
	`set bss wlan0bssInternal ignore-broadcast-ssid off`

Enable / Disable Station Isolation	
Set Security to None	`set interface wlan0 security plain-text`
Set Security to Static WEP	See detailed example in "Set Security to Static WEP" on page 202.
Set Security to IEEE 802.1x	See detailed example in"Set Security to IEEE 802.1x" on page 206.
Set Security to WPA/WPA2 Personal (PSK)	See detailed example in "Set Security to WPA/WPA2 Personal (PSK)" on page 208.
Set Security to WPA/WPA2 Enterprise (RADIUS)	See detailed example in "Set Security to WPA/WPA2 Enterprise (RADIUS)" on page 210.

Get the Current Security Mode

```
USR5453-AP# get interface wlan0 security
none
```

Get Detailed Description of Current Security Settings

```
USR5453-AP# get bss wlan0bssInternal detail
Field                          Value
---------------------------------------------
status                         up
description                    Internal
radio                          wlan0
beacon-interface               wlan0
mac                            00:0C:41:16:DF:A6
dtim-period
max-stations
ignore-broadcast-ssid          off
mac-acl-mode                   deny-list
mac-acl-name                   wlan0bssInternal
radius-accounting
radius-ip                      127.0.0.1
radius-key                     secret
open-system-authentication
shared-key-authentication
wpa-cipher-tkip
wpa-cipher-ccmp
wpa-allowed                    off
wpa2-allowed                   off
rsn-preauthentication
```

Set the Broadcast SSID (Allow or Prohibit)

To set the Broadcast SSID to on (allow):

```
USR5453-AP# set bss wlan0bssInternal ignore-broadcast-ssid on
```

To set the Broadcast SSID to off (prohibit):

```
USR5453-AP# set bss wlan0bssInternal ignore-broadcast-ssid off
```

Enable / Disable Station Isolation

```
USR5453-AP# get radio wlan0 station-isolation
off
USR5453-AP# set radio wlan0 station-isolation off
USR5453-AP# get radio wlan0 detail
Field                                          Value
-------------------------------------------------------------------
status                                         up
description                                    Radio 1 - IEEE 802.11g
mac
max-bss                                        4
channel-policy                                 static
mode                                           g
static-channel                                 6
channel                                        6
tx-power                                       100
tx-rx-status                                   up
beacon-interval                                100
rts-threshold                                  2347
fragmentation-threshold                        2346
load-balance-disassociation-utilization        0
load-balance-disassociation-stations           0
load-balance-no-association-utilization        0
ap-detection                                   off
station-isolation                              off
frequency                                      2437
wme                                            on
```

Set Security to None

```
USR5453-AP# set interface wlan0 security none
```

Set Security to Static WEP

1. Set the Security Mode

```
USR5453-AP# set interface wlan0 security static-wep
```

2. Set the Transfer Key Index

The following commands set the Transfer Key Index to 4.

```
USR5453-AP# set interface wlan0 wep-default-key 1
USR5453-AP# set interface wlan0 wep-default-key 2
USR5453-AP# set interface wlan0 wep-default-key 3
USR5453-AP# set interface wlan0 wep-default-key 4
```

3. Set the Key Length

For the CLI, valid values for Key Length are 40 bits or 104 bits.

Note The Key Length values used by the CLI do not include the initialisation vector in the length. On the Web User Interface, longer Key Length values may be shown which include the 24-bit initialisation vector. A Key Length of 40 bits (not including initialisation vector) is equivalent to a Key Length of 64 bits (with initialisation vector). A Key Length of 104 bits (not including initialisation vector) is equivalent to a Key Length of 128 bits (which includes the initialisation vector).

To set the WEP Key Length, type one of the following commands:

To set the WEP Key Length to 40 bits:	`set interface wlan0 wep-key-length 40`
To set the WEP Key Length to 104 bits:	`set interface wlan0 wep-key-length 104`

In this example, you will set the WEP Key Length to 40.

```
USR5453-AP# set interface wlan0 wep-key-length 40
```

4. Set the Key Type

Valid values for Key Type are ASCII or Hex. The following commands set the Key Type.

To set the Key Type to ASCII:	`set interface wlan0 wep-key-ascii yes`
To set the Key Type to Hex:	`set interface wlan0 wep-key-ascii no`

In this example, you will set the Key Type to ASCII:

```
USR5453-AP# set interface wlan0 wep-key-ascii yes
```

5. Set the WEP Keys

Note The number of characters required for each WEP key depends on how you set Key Length and Key Type:

- If Key Length is 40 bits and the Key Type is "ASCII", then each WEP key be 5 characters long.
- If Key Length is 40 bits and Key Type is "Hex", then each WEP key must be 10 characters long.
- If Key Length is 104 bits and Key Type is "ASCII", then each WEP Key must be 13 characters long.
- If Key Length is 104 bits and Key Type is "Hex", then each WEP Key must be 26 characters long.

Although the CLI will allow you to enter WEP keys of any number of characters, you must use the correct number of characters for each key to ensure a valid security configuration.

```
USR5453-AP# set interface wlan0 wep-key-1 abcde
USR5453-AP# set interface wlan0 wep-key-2 fghi
USR5453-AP# set interface wlan0 wep-key-3 klmno
USR5453-AP# set interface wlan0 wep-key-4
```

6. Set the Authentication Algorithm

The options for the authentication algorithm are Open System, Shared Key or Both:

To set Authentication Algorithm to **Open System**:	`set bss wlan0bssInternal open-system-authentication on`
	
	`set bss wlan0bssInternal shared-key-authentication off`

To set Authentication Algorithm to **Shared Key**:	`set bss wlan0bssInternal open-system-authentication off`
	
	`set bss wlan0bssInternal shared-key-authentication on`

To set Authentication Algorithm to **Both**:	`set bss wlan0bssInternal open-system-authentication on`
	
	`set bss wlan0bssInternal shared-key-authentication on`

In this example, you will set the authentication algorithm to Shared Key:

```
USR5453-AP# set bss wlan0bssInternal shared-key-authentication on
USR5453-AP# set bss wlan0bssInternal open-system-authentication off
```

7. Get Current Security Settings After Re-Configuring to Static WEP Security Mode

Now you can use the "get" command again to view the updated security configuration and see the results of your new settings.

The following command gets the security mode in use on the Internal network:

```
USR5453-AP# get interface wlan0 security
static-wep
```

The following command gets details on how the internal network is configured, including details on Security.

```
USR5453-AP# get bss wlan0bssInternal detail
Field                       Value
```

```
-------------------------------------------
status                      up
description                 Internal
radio                       wlan0
beacon-interface            wlan0
mac                         00:0C:41:16:DF:A6
dtim-period                 2
max-stations                2007
ignore-broadcast-ssid       off
mac-acl-mode                deny-list
mac-acl-name                wlan0bssInternal
radius-accounting           off
radius-ip                   127.0.0.1
radius-key                  secret
open-system-authentication  off
shared-key-authentication   on
wpa-cipher-tkip             off
wpa-cipher-ccmp             off
wpa-allowed                 off
wpa2-allowed                off
rsn-preauthentication       off
```

The following command gets details on the interface and shows the WEP Key settings, specifically.

```
USR5453-AP# get interface wlan0 detail
Field             Value
-----------------------------------------
type              service-set
status            up
description       Wireless - Internal
mac               00:0C:41:16:DF:A6
ip                0.0.0.0
static-ip         0.0.0.0
static-mask
nat
rx-bytes          0
rx-packets        0
rx-errors         0
rx-drop           0
rx-fifo           0
rx-frame          0
rx-compressed     0
rx-multicast      0
tx-bytes          259662
tx-packets        722
tx-errors         0
tx-drop           0
tx-fifo           0
tx-colls          0
tx-carrier        0
tx-compressed     0
ssid              Vicky's AP
bss               wlan0bssInternal
security          static-wep
```

```
wpa-personal-key
wep-key-ascii      yes
wep-key-length     104
wep-default-key    4
wep-key-1          abcde
wep-key-2          fghij
wep-key-3          klmno
wep-key-4
vlan-interface
vlan-id
radio
remote-mac
wep-key
```

Set Security to IEEE 802.1x

1. Set the Security Mode

```
USR5453-AP# set interface wlan0 security dot1x
```

2. Set the Authentication Server

You can use the built-in authentication server on the access point or an external RADIUS server.

Note To use the built-in authentication server, set the RADIUS IP address to that used by the built-in server (`127.0.0.1`) and turn RADIUS accounting off (because it is not supported by the built-in server)

RADIUS Option	Example
To set the AP to use the **Built-in** Authentication Server:	`set bss wlan0bssInternal radius-ip 127.0.0.1`
To set the AP to use an **External** RADIUS Server:	`set bss wlan0bssInternal radius-ip` *`RADIUS_IP_Address`* where *`RADIUS_IP_Address`* is the IP address of an external RADIUS server.

In this example, you will set it to use the built-in server:

```
USR5453-AP# set bss wlan0bssInternal radius-ip 127.0.0.1
```

3. Set the RADIUS Key (For External RADIUS Server Only)

If you use an external RADIUS server, you must provide the RADIUS key. (If you use the built-in authentication server the RADIUS key is automatically provided.)

This command sets the RADIUS key to `secret` for an external RADIUS server.

```
USR5453-AP# set bss wlan0bssInternal radius-key secret
```

4. Enable RADIUS Accounting (External RADIUS Server Only)

You can enable RADIUS Accounting if you want to track and measure the resources a particular user has consumed such system time, amount of data transmitted and received, and so on.

Note RADIUS accounting is not supported by the built-in server, so if you are using the built-in server make sure that RADIUS accounting is off.

To enable RADIUS accounting:	`set bss wlan0bssInternal radius-accounting on`
To disable RADIUS accounting:	`set bss wlan0bssInternal radius-accounting off`

In this example, you will disable RADIUS accounting since you are using the built-in server:

```
USR5453-AP# set bss wlan0bssInternal radius-accounting off
```

5. Get Current Security Settings After Re-Configuring to IEEE 802.1x Security Mode

Now you can use the "get" command again to view the updated security configuration and see the results of your new settings.

The following command gets the security mode in use on the Internal network:

```
USR5453-AP# get interface wlan0 security
dot1x
```

The following command gets details on how the internal BSS is configured, including details on Security.

```
USR5453-AP# get bss wlan0bssInternal detail
Field                          Value
---------------------------------------------
status                         up
description                    Internal
radio                          wlan0
beacon-interface               wlan0
mac                            00:0C:41:16:DF:A6
dtim-period                    2
max-stations                   2007
ignore-broadcast-ssid          off
mac-acl-mode                   deny-list
mac-acl-name                   wlan0bssInternal
radius-accounting              off
radius-ip                      127.0.0.1
radius-key                     secret
open-system-authentication     off
shared-key-authentication      on
wpa-cipher-tkip                off
wpa-cipher-ccmp                off
wpa-allowed                    off
wpa2-allowed                   off
```

```
rsn-preauthentication       off
```

Set Security to WPA/WPA2 Personal (PSK)

1. Set the Security Mode

```
USR5453-AP# set interface wlan0 security wpa-personal
```

2. Set the WPA Versions

Select the WPA version based on what types of client stations you want to support.

WPA Option	Example

WPA: If all client stations on the network support the original WPA but none support the newer WPA2, then use WPA.
 	
To support WPA clients:
	`set bss wlan0bssInternal wpa-allowed on`
	
	`set bss wlan0bssInternal wpa2-allowed off`

WPA2: If all client stations on the network support WPA2, we suggest using WPA2 which provides the best security per the IEEE 802.11i standard.
 	
To support WPA2 clients:
	`set bss wlan0bssInternal wpa-allowed off`
	
	`set bss wlan0bssInternal wpa2-allowed on`

Both: If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select "Both". This lets both WPA and WPA2 client stations assoicate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.
 	
To support both WPA and WPA2 clients:
	`set bss wlan0bssInternal wpa-allowed on`
	
	`set bss wlan0bssInternal wpa2-allowed on`

In this example, you will set the access point to support **Both** WPA and WPA2 client stations:

```
USR5453-AP# set bss wlan0bssInternal wpa-allowed on
USR5453-AP# set bss wlan0bssInternal wpa2-allowed on
```

3. Set the Cipher Suites

Set the cipher suite you want to use. The options are:

Cipher Suite Option	Example

TKIP: Temporal Key Integrity Protocol (TKIP), which is the default.
 	
To set the cipher suite to **TKIP only**:
	`set bss wlan0bssInternal wpa-cipher-tkip on`
	
	`set bss wlan0bssInternal wpa-cipher-ccmp off`

CCMP (AES) - Counter mode/ CBC-MAC Protocol (CCMP) is an encryption method for IEEE 802.11i that uses the Advanced Encryption Algorithm (AES).
 	
To set the cipher suite to **CCMP (AES) only**:
	`set bss wlan0bssInternal wpa-cipher-tkip off`
	
	`set bss wlan0bssInternal wpa-cipher-ccmp on`

Both - When the authentication algorithm is set to "**Both**", both TKIP and AES clients can associate with the access point. WPA clients must have either a valid TKIP key or a valid CCMP (AES) key to be able to associate with the AP.
 	
To set the cipher suite to **Both**:
	`set bss wlan0bssInternal wpa-cipher-tkip on`
	
	`set bss wlan0bssInternal wpa-cipher-ccmp on`

In this example, you will set the cipher suite to **Both**:

```
USR5453-AP# set bss wlan0bssInternal wpa-cipher-tkip on
USR5453-AP# set bss wlan0bssInternal wpa-cipher-ccmp on
```

4. Set the Pre-shared Key

The *Pre-shared Key* is the shared secret key for WPA-PSK. Enter a string of at least 8 characters to a maximum of 63 characters. Following are two examples; the first sets the key to "`SeCret !`", the second sets the key to "`KeepSecret`".

```
Ex 1. USR5453-AP# set interface wlan0 wpa-personal-key "SeCret !"
```

or

```
Ex 2. USR5453-AP# set interface wlan0 wpa-personal-key KeepSecret
```

Note Shared secret keys can include spaces and special characters if the key is placed inside quotation marks as in the first example above. If the key is a string of characters with no spaces or special characters in it, the quotation marks are not necessary as in the second example above..

5. Get Current Security Settings After Re-Configuring to WPA/WPA2 Personal (PSK)

Now you can use the "get" command again to view the updated security configuration and see the results of your new settings.

The following command gets the security mode in use on the Internal network:

```
USR5453-AP# get interface wlan0 security
wpa-personal
```

The following command gets details on how the internal network is configured, including details on Security.

```
USR5453-AP# get bss wlan0bssInternal detail
Field                          Value
---------------------------------------------
status                         up
description                    Internal
radio                          wlan0
beacon-interface               wlan0
mac                            00:0C:41:16:DF:A6
dtim-period
max-stations
ignore-broadcast-ssid          off
mac-acl-mode                   deny-list
mac-acl-name                   wlan0bssInternal
radius-accounting
radius-ip                      127.0.0.1
radius-key                     secret
open-system-authentication
shared-key-authentication
wpa-cipher-tkip                on
wpa-cipher-ccmp                on
wpa-allowed                    on
wpa2-allowed                   on
rsn-preauthentication
```

Set Security to WPA/WPA2 Enterprise (RADIUS)

8. Get Current Security Settings After Re-Configuring to WPA/WPA2 Enterprise (RADIUS)

1. Set the Security Mode

```
USR5453-AP# set interface wlan0 security wpa-enterprise
```

2. Set the WPA Versions

Select the WPA version based on what types of client stations you want to support.

WPA Option	Example

WPA: If all client stations on the network support the original WPA but none support the newer WPA2, then use WPA.
 	
To support WPA clients:
	`set bss wlan0bssInternal wpa-allowed on`
	
	`set bss wlan0bssInternal wpa2-allowed off`

WPA2: If all client stations on the network support WPA2, we suggest using WPA2 which provides the best security per the IEEE 802.11i standard.
 	
To support WPA2 clients:
	`set bss wlan0bssInternal wpa-allowed off`
	
	`set bss wlan0bssInternal wpa2-allowed on`

Both: If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select "Both". This lets both WPA and WPA2 client stations assoicate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.
 	
To support both WPA and WPA2 clients:
	`set bss wlan0bssInternal wpa-allowed on`
	
	`set bss wlan0bssInternal wpa2-allowed on`

In this example, you will set the access point to support WPA client stations only:

```
USR5453-AP# set bss wlan0bssInternal wpa-allowed on
USR5453-AP# set bss wlan0bssInternal wpa2-allowed off
```

3. Enable Pre-Authentication

If you set WPA versions to "WPA2" or "Both", you can enable *pre-authentication* for WPA2 clients.

Enable pre-authentication if you want WPA2 wireless clients to send pre-authentication packet. The pre-authentication information will be relayed from the access point the client is currently using to the target access point. Enabling this feature can help speed up authentication for roaming clients who connect to multiple access points. To enable pre-authentication for WPA2 clients:	`set bss wlan0bssInternal rsn-preauthentication on`
To disable pre-authentication for WPA2 clients:	set bss wlan0bssInternal rsn-preauthentication on

This option does not apply if you set the WPA Version to support "WPA" clients only because the original WPA does not support this pre-authentication

In this example, you will disable pre-authentication.

```
USR5453-AP# set bss wlan0bssInternal rsn-preauthentication off
```

4. Set the Cipher Suites

Set the cipher suite you want to use. The options are:

Cipher Suite Option	Example

TKIP: Temporal Key Integrity Protocol (TKIP), which is the default.
 	
To set the cipher suite to **TKIP only**:
	`set bss wlan0bssInternal wpa-cipher-tkip on`
	
	`set bss wlan0bssInternal wpa-cipher-ccmp off`

CCMP (AES) - Counter mode/ CBC-MAC Protocol (CCMP) is an encryption method for IEEE 802.11i that uses the Advanced Encryption Algorithm (AES).
 	
To set the cipher suite to **CCMP (AES) only**:
	`set bss wlan0bssInternal wpa-cipher-tkip off`
	
	`set bss wlan0bssInternal wpa-cipher-ccmp on`

Cipher Suite Option	Example

Both - When the authentication algorithm is set to "**Both**", both TKIP and AES clients can associate with the access point. WPA clients must have either a valid TKIP key or a valid CCMP (AES) key to be able to associate with the AP.
 	
To set the cipher suite to **Both**:
	`set bss wlan0bssInternal wpa-cipher-tkip on`
	
	`set bss wlan0bssInternal wpa-cipher-ccmp on`

In this example, you will set the cipher suite to **TKIP Only**:

```
USR5453-AP# set bss wlan0bssInternal wpa-cipher-tkip on
USR5453-AP# set bss wlan0bssInternal wpa-cipher-ccmp off
```

5. Set the Authentication Server

You can use the built-in authentication server on the access point or an external RADIUS server.

Note To use the built-in authentication server, set the RADIUS IP address to that used by the built-in server (`127.0.0.1`) and turn RADIUS accounting off (because it is not supported by the built-in server)

RADIUS Option	Example
To set the AP to use the **Built-in** Authentication Server:	`set bss wlan0bssInternal radius-ip 127.0.0.1`
To set the AP to use an **External** RADIUS Server:	`set bss wlan0bssInternal radius-ip` *`RADIUS_IP_Address`* where *`RADIUS_IP_Address`* is the IP address of an external RADIUS server.

In this example, you will use an external RADIUS server with an IP address of 142.77.1.1:

```
USR5453-AP# set bss wlan0bssInternal radius-ip 142.77.1.1
```

6. Set the RADIUS Key (For External RADIUS Server Only)

If you use an external RADIUS server, you must provide the RADIUS key. (If you use the built-in authentication server the RADIUS key is automatically provided.)

This command sets the RADIUS key to `KeepSecret` for an external RADIUS server.

```
USR5453-AP# set bss wlan0bssInternal radius-key KeepSecret
```

7. Enable RADIUS Accounting (External RADIUS Server Only)

You can enable RADIUS Accounting if you want to track and measure the resources a particular user has

consumed such system time, amount of data transmitted and received, and so on.

Note RADIUS accounting is not supported by the built-in server, so if you are using the built-in server make sure that RADIUS accounting is off.

To enable RADIUS accounting:	`set bss wlan0bssInternal radius-accounting on`
To disable RADIUS accounting:	`set bss wlan0bssInternal radius-accounting off`

For this example, you will enable RADIUS accounting for your external RADIUS server:

```
USR5453-AP# set bss wlan0bssInternal radius-accounting on
```

8. Get Current Security Settings After Re-Configuring to WPA/WPA2 Enterprise (RADIUS)

Now you can use the "get" command again to view the updated security configuration and see the results of your new settings.

The following command gets the security mode in use on the Internal network:

```
USR5453-AP# get interface wlan0 security
wpa-enterprise
```

The following command gets details on how the internal network is configured, including details on Security.

```
USR5453-AP# get bss wlan0bssInternal detail
Field                         Value
--------------------------------------------
status                        up
description                   Internal
radio                         wlan0
beacon-interface              wlan0
mac                           00:0C:41:16:DF:A6
dtim-period                   2
max-stations                  2007
ignore-broadcast-ssid         off
mac-acl-mode                  deny-list
mac-acl-name                  wlan0bssInternal
radius-accounting             on
radius-ip                     142.77.1.1
radius-key                    KeepSecret
open-system-authentication    on
shared-key-authentication     off
wpa-cipher-tkip               on
wpa-cipher-ccmp               off
wpa-allowed                   on
wpa2-allowed                  off
rsn-preauthentication         off
```

Enable/Configure Guest Login Welcome Page

Guest Welcome Option	Example
View Guest Login Settings:	`get portal`
Enable/Disable the Guest Welcome Page	`set portal status`
Set Guest Welcome Page TextI:	`set portal welcome-screen-text "`*`Welcome Screen Text`*`"` Where "*`Welcome Screen Text`*" is the content of the Welcome message you want displayed on the Guest Welcome Web Page. The Welcome message must be in quotes if it contains spaces, punctuation, and special characters."

Note Guest Login settings are only relevant if you have first configured a Guest Network. For information about configuring a Guest Network, see "Set Up Guest Access" on page 195.

You can set up a "captive portal" that Guest clients will see when they log on to the Guest network. or modify the Welcome screen guest clients see when they open a Web browser or try to browse the Web.

View Guest Login Settings

To view the current settings for Guest Login:

```
USR5453-AP# get portal
Field                Value
-------------------------------------------------------------------------------
status               down
welcome-screen       on
welcome-screen-text  Thank you for using wireless Guest Access as provided
by this U.S. Robotics Corporation wireless AP. Upon clicking "Accept", you
will gain access to our wireless guest network. This network allows complete
access to the Internet but is external to the corporate network. Please note
that this network is not configured to provide any level of wireless
security.
```

Enable/Disable the Guest Welcome Page

To enable the Guest welcome page:

```
USR5453-AP# set portal status up
```

To disable the Guest welcome page:

```
USR5453-AP# set portal status down
```

Set Guest Welcome Page Text

To specify the text for the Guest welcome page:

```
USR5453-AP# set portal welcome-screen-text "Welcome to the Stephens Network"
```

Review Guest Login Settings

The following example shows the results of the "`set portal`" command after specifying some new settings:

```
USR5453-AP# get portal
Field                Value
-----------------------------------------------------
status               up
welcome-screen       on
welcome-screen-text  Welcome to the Stephens Network
```

Configuring Multiple BSSIDs on Virtual Wireless Networks

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 177. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network,.

Configuring Virtual Wireless Network "One" on Radio One

1. Configure these settings from the Web User Interface first:

   - On Advanced menu's Ethernet (Wired) Settings tab on the Web User Interface, enable Virtual Wireless Networks as described in "Enabling and Disabling Virtual Wireless Networks on the Access Point" on page 82.

   - On Advanced menu's Virtual Wireless Networks tab on the Web User Interface, provide a VLAN ID as described in "Configuring VLANs" on page 116.

2. Use the CLI to configure Security on the interface.

   The following example shows commands for configuring WPA/WPA2 Enterprise (RADIUS) security mode, allowing "Both" WPA and WPA2 clients to authenticate and using a TKIP cipher suite:

```
USR5453-AP# set bss wlan0bssvwn1 open-system-authentication on
USR5453-AP# set bss wlan0bssvwn1 shared-key-authentication on
USR5453-AP# set bss wlan0bssvwn1 wpa-allowed on
USR5453-AP# set bss wlan0bssvwn1 wpa2-allowed on
USR5453-AP# set bss wlan0bssvwn1 wpa-cipher-tkip on
USR5453-AP# set bss wlan0bssvwn1 wpa-cipher-ccmp off
USR5453-AP# set bss wlan0bssvwn1 radius-ip 127.0.0.1
USR5453-AP# set bss wlan0bssvwn1 radius-key secret
USR5453-AP# set bss wlan0bssvwn1 status up
USR5453-AP# set interface wlan0vwn1 security wpa-enterprise
```

3. Use the CLI to set the Network Name (SSID) for the new Virtual Wireless Network:

```
USR5453-AP# set interface wlan0vwn1 ssid my-vwn-one
```

Creating VWN 'Two' on Radio One with WPA security

To configure the second Virtual Wireless Network, repeat steps 1-3 as described above (in Configuring Virtual Wireless Network "One" on Radio One) with the following differences:

- Create a second VLAN ID from the Web User Interface with a new SSID
- In the CLI commands, replace `wlan0bssvwn1` with `wlan0bssvwn2`.

Radio Settings

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 177. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network.

This table shows a quick view of Radio Settings commands and provides links to detailed examples.

Radio Setting Command	Example

Get Radio Settings	`get radio`
	`get radio wlan0`
	`get radio wlan0 detail`

Get IEEE 802.11 Radio Mode	`get radio wlan0 mode`
Get Radio Channel	`get radio wlan0 channel`
Get Basic Radio Settings	`get radio wlan0`
Get All Radio Settings	`get radio wlan0 detail`
Get Supported Rate Set	`get supported-rate`
Get Basic Rate Set	`get basic-rate`
Configure Radio Settings	See detailed examples in: "1. Turn the Radio On or Off" on page 220 "2. Set the Radio Mode" on page 220 "3. Enable or Disable Super G" on page 220 "4. Set the Beacon Interval" on page 220 "5. Set the DTIM Period" on page 220 "6. Set the Fragmentation Threshold" on page 220 "7. Set the RTS Threshold" on page 221 "8. Configure Basic and Supported Rate Sets" on page 221

Get IEEE 802.11 Radio Mode

To get the current setting for radio Mode:

```
USR5453-AP# get radio wlan0 mode
g
```

(The radio in this example is using IEEE 802.11g mode.)

Get Radio Channel

To get the current setting for radio Channel:

```
USR5453-AP# get radio wlan0 channel
6
```

(The radio in this example is on Channel 6.)

Get Basic Radio Settings

To get basic current Radio settings:

```
USR5453-AP# get radio wlan0
Field           Value
----------------------
status          up
mac
channel-policy  static
mode            g
static-channel  6
channel         6
tx-rx-status    up
```

Get All Radio Settings

To get all current Radio settings: get radio wlan0 detail

```
USR5453-AP# get radio wlan0 detail
Field                                       Value
------------------------------------------------
status                                      up
description                                 IEEE 802.11
mac
max-bss                                     2
channel-policy                              static
mode                                        g
static-channel                              6
channel                                     6
tx-power                                    100
tx-rx-status                                up
beacon-interval                             100
rts-threshold                               2347
fragmentation-threshold                     2346
load-balance-disassociation-utilization     0
load-balance-disassociation-stations        0
load-balance-no-association-utilization     0
ap-detection                                off
station-isolation                           off
frequency                                   2437
```

```
wme                                     on
```

Get Supported Rate Set

The *Supported Rate Set* is what the access point supports. The access point will automatically choose the most efficient rate based on factors like error rates and distance of client stations from the access point.

```
USR5453-AP# get supported-rate
name   rate
-----------
wlan0  54
wlan0  48
wlan0  36
wlan0  24
wlan0  18
wlan0  12
wlan0  11
wlan0  9
wlan0  6
wlan0  5.5
wlan0  2
wlan0  1
```

Get Basic Rate Set

The *Basic Rate Set* is what the access point will advertise to the network for the purposes of setting up communication with other APs and client stations on the network. It is generally more efficient to have an access point broadcast a subset of its supported rate sets.

```
USR5453-AP# get basic-rate
name   rate
-----------
wlan0  11
wlan0  5.5
wlan0  2
wlan0  1
```

Configure Radio Settings

Note To get a list of all fields you can set on the access point radio, type the following at the CLI prompt: set radio wlan0 [SpaceKey] [TAB] [TAB]

1. Turn the Radio On or Off

To turn the radio on:	`set radio wlan0 status up`
To turn the radio off:	`set radio wlan0 status down`

2. Set the Radio Mode

Valid values depend on the capabilities of the radio. Possible values and how you would use the CLI to set each one are shown below.

IEEE 802.11b	set radio wlan0 mode **b**
IEEE 802.11g	set radio wlan0 mode **g**

The following command sets the Wireless Mode to IEEE 802.11g:

```
USR5453-AP# set radio wlan0 mode g
```

3. Enable or Disable Super G

You cannot enable/disable Super G from the CLI. You must set this from the Web User Interface. For information on how to set this option, please see the field description for this option in "Configuring Radio Settings" on page 120.

4. Set the Beacon Interval

The following command sets the beacon interval to 80.

```
USR5453-AP# set radio wlan0 beacon-interval 80
```

5. Set the DTIM Period

The Delivery Traffic Information Map (DTIM) period indicates how often wireless clients should check to see if they have buffered data on the access point awaiting pickup. The measurement is in beacons. Specify a DTIM period within a range of 1 - 255 beacons. For example, if you set this to "1" clients will check for buffered data on the access point at every beacon. If you set this to "2", clients will check on every other beacon.

The following command sets the DTIM interval to 3.

```
USR5453-AP# set bss wlan0bssInternal dtim-period 3
```

To get the updated value for DTIM interval after you have changed it:

```
USR5453-AP# get bss wlan0bssInternal dtim-period
3
```

6. Set the Fragmentation Threshold

You can specify a fragmentation threshold as a number between 256 and 2,346 to set the frame size threshold in bytes. The fragmentation threshold is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold set here, the fragmentation function will be activated and the packet will be sent as multiple 802.11 frames. If the packet being transmitted is equal to or less than the threshold, fragmentation will not be used. Setting the threshold to the largest value

(2,346 bytes) effectively disables fragmentation.

The following command sets the fragmentation threshold to 2000.

```
USR5453-AP# set radio wlan0 fragmentation-threshold 2000
```

7. Set the RTS Threshold

You can specify an RTS Threshold value between 0 and 2347. The RTS threshold specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the access point, especially one with a lot of clients.

The following command sets the RTS threshold at

```
USR5453-AP# set radio wlan0 rts-threshold 2346
```

8. Configure Basic and Supported Rate Sets

Add a basic rate set	`add basic-rate` *`WirelessInterface`* `rate` *`SomeRate`* For example: `add basic-rate wlan0 rate 48`
Get current basic rates	`get basic-rate`
Add supported rate	`add supported-rate` *`WirelessInterfaceName`* `rate` *`SomeRate`* For example: `add supported-rate wlan0 rate 9`
Get current supported rates	`get supported-rate wlan0`

The following command adds "`48`" as a basic rate to `wlan0` (the internal, wireless interface):

```
USR5453-AP# add basic-rate wlan0 rate 48
```

To get the basic rates currently configured for this access point:

```
USR5453-AP# get basic-rate
name   rate
-----------
wlan0  11
wlan0  5.5
wlan0  2
wlan0  1
wlan1  24
wlan1  12
wlan1  6
wlan0  48
```

The following command adds "`9`" as a supported rate to `wlan0` (the internal, wireless interface):

```
USR5453-AP# add supported-rate wlan0 rate 9
```

To get the supported rates currently configured for this access point (using "`wlan0`" as the interface for this example):

```
USR5453-AP# get supported-rate wlan0
rate
----
1
2
5.5
6
11
12
18
24
36
48
54

9
```

Note You can use the **get** command to view current rate sets from the CLI as described in "Get Supported Rate Set" on page 219 and "Get Basic Rate Set" on page 219. However, cannot reconfigure Supported Rate Sets or Basic Rate Sets from the CLI. You must use the Advanced menu's Radio page on the Web User Interface to configure this feature.

MAC Filtering

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 177. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network.

You can control access to Professional Access Point based on *Media Access Control* (MAC) addresses. Based on how you set the filter, you can *allow* only client stations with a listed MAC address or *prevent* access to the stations listed.

Specify an Accept or Deny List

To set up MAC filtering you first need to specify which type of list you want to configure

To set up an **Accept** list: (With this type of list, client stations whose MAC addresses are listed will be allowed access to the access point.)	`set bss wlan0bssInternal mac-acl-mode accept-list`

To set up a **Deny** list: (With this type of list, the access point will prevent access to client stations whose MAC addresses are listed.)	`set bss wlan0bssInternal mac-acl-mode deny-list`

Add MAC Addresses of Client Stations to the Filtering List

To add a MAC address to the list:

```
add mac-acl wlan0bssInternal mac MAC_Address_Of_Client
```

Where *MAC_Address_Of_Client* is the MAC address of a wireless client you want to add to the MAC filtering list.

For example, to add 4 new clients to the list with the following MAC addresses:

```
USR5453-AP# add mac-acl wlan0bssInternal mac 00:01:02:03:04:05
USR5453-AP# add mac-acl wlan0bssInternal mac 00:01:02:03:04:06
USR5453-AP# add mac-acl wlan0bssInternal mac 00:01:02:03:04:07
USR5453-AP# add mac-acl wlan0bssInternal mac 00:01:02:03:04:08
```

Remove a Client Station's MAC Address from the Filtering List

To remove a MAC address from the list:

```
remove mac-acl wlan0bssInternal mac MAC_Address_Of_Client
```

Where *MAC_Address_Of_Client* is the MAC address of a wireless client you want to remove from the MAC filtering list.

For example:

```
USR5453-AP# remove mac-acl wlan0bssInternal mac 00:01:02:03:04:04
```

Get Current MAC Filtering Settings

Get the Type of MAC Filtering List Currently Set (Accept or Deny)

The following command shows which type of MAC filtering list is currently configured:

```
USR5453-AP# get bss wlan0bssInternal mac-acl-mode
accept-list
```

Get MAC Filtering List

The following command shows the clients on the MAC filtering list:

```
USR5453-AP# get mac-acl
name              mac
-----------------------------------
wlan0bssInternal  00:01:02:03:04:05
```

```
wlan0bssInternal  00:01:02:03:04:06
wlan0bssInternal  00:01:02:03:04:07
wlan0bssInternal  00:01:02:03:04:08
```

Load Balancing

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 177. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network.

Load balancing parameters affect the distribution of wireless client connections across multiple access points. Using load balancing, you can prevent scenarios where a single access point in your network shows performance degradation because it is handling a disproportionate share of the wireless traffic. (For an overview of Load Balancing, see "Load Balancing" on page 129.)

The access point provides default settings for load balancing.

The following command examples reconfigure some load balancing settings and get details on the configuration:

```
USR5453-AP# set radio wlan0 load-balance-disassociation-stations 2
USR5453-AP# get radio wlan0 load-balance-disassociation-stations
2
USR5453-AP# set radio wlan0 load-balance-disassociation-utilization 25
USR5453-AP#
USR5453-AP# get radio wlan0 load-balance-disassociation-utilization
25
USR5453-AP# set radio wlan0 load-balance-no-association-utilization 50
USR5453-AP#
USR5453-AP# get radio wlan0 load-balance-no-association-utilization
50
```

Quality of Service

Note Before configuring this feature from the CLI, make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 177 The interface name referenced in a command determines if a setting applies to a wired or wireless interface or to the Internal or Guest network.

Quality of Service (QoS) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like *Voice-over-IP* (VoIP), other types of audio, video, and streaming media as well as traditional IP data over the Professional Access Point.

For a complete conceptual overview of QoS, see"Quality of Service" on page 133.

This table shows a quick view of QOS commands and provides links to detailed examples.

QoS Command	Example

Enable/Disable Wi-Fi Multimedia	`set radio wlan0 wme off`
	`set radio wlan0 wme on`
	`get radio wlan0 wme`

About Access Point and Station EDCA Parameters	See "About Access Point and Station EDCA Parameters" on page 226.
Understanding the Queues for Access Point and Station	See "Understanding the Queues for Access Point and Station" on page 226.
Distinguishing between Access Point and Station Settings in QoS Commands	See ""Distinguishing between Access Point and Station Settings in QoS Commands" on page 226.
Get QoS Settings on the Access Point	`get tx-queue`
Get QoS Settings on the Client Station	`get wme-queue`
Set Arbitration Interframe Spaces (AIFS)	On the access point: `set wme-queue wlan0 with queue` *`Queue_Name`* `to aifs` *`AIFS_Value`* On a client station: `set wme-queue wlan0 with queue` *`Queue_Name`* `to aifs` *`AIFS_Value`* See examples in "Set Arbitration Interframe Spaces (AIFS)" on page 227
Setting Minimum and Maximum Contention Windows (cwmin, cwmax)	On the access point: `set tx-queue wlan0 with queue` *`Queue_Name`* `to cwmin` *`cwmin_Value`* `cwmax` *`cwmax_Value`* On a client station: `set wme-queue wlan0 with queue` *`Queue_Name`* `to cwmin` *`cwmin_Value`* `cwmax` *`cwmax_Value`* See examples in "Setting Minimum and Maximum Contention Windows (cwmin, cwmax)" on page 228.
Set the Maximum Burst Length (burst) on the Access Point	`set tx-queue wlan0 with queue` *`Queue_Name`* `to burst` *`burst_Value`* See examples in "Set the Maximum Burst Length (burst) on the Access Point" on page 229.
Set Transmission Opportunity Limit (txop-limit) for WMM client stations	`set wme-queue wlan0 with queue` *`Queue_Name`* `to txop-limit` *`txop-limit_Value`* See examples in "Set Transmission Opportunity Limit (txop-limit) for WMM client stations" on page 230.

Enable/Disable Wi-Fi Multimedia

By default, Wi-Fi MultiMedia (WMM) is enabled on the access point. With WMM enabled, QoS settings on

the Professional Access Point control both *downstream* traffic flowing from the access point to client station (access point EDCA parameters) and *upstream* traffic flowing from the station to the access point (station EDCA parameters). Enabling WMM essentially activates station-to-access-point QoS control.

Disabling WMM will deactivates QoS control of "station EDCA parameters" on *upstream* traffic flowing from the station to the access point. With WMM disabled, you can still set downstream access-point-to-station QoS parameters but no station-to-access-point QoS parameters.

- To disable WMM:

```
USR5453-AP# set radio wlan0 wme off
USR5453-AP# get radio wlan0 wme
off
```

- To enable WMM:

```
USR5453-AP# set radio wlan0 wme on
USR5453-AP# get radio wlan0 wme
on
```

About Access Point and Station EDCA Parameters

AP Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the access point to the client station (access-point-to-station).

Station Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the client station to the access point (station-to-access-point). Keep in mind that station-to-access-point parameters apply only when WMM is enabled as described in "Enable/Disable Wi-Fi Multimedia" on page 225.

Understanding the Queues for Access Point and Station

The same types of queues are defined for different kinds of data transmitted from access-point-to-station and station-to-access-point but they are referenced by differently depending on whether you are configuring access point or station parameters.

Data	Access Point	Station
Voice - Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.	`data0`	`vo`
Video - High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.	`data1`	`vi`
Best Effort - Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.	`data2`	`be`
Background - Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).	`data3`	`bk`

Distinguishing between Access Point and Station Settings in QoS Commands

Access Point - To get and set QoS settings on the access point, use "**tx-queue**" class name in the command.

Station - To get and set QoS settings on the client station, use the "**wme-queue**" class name in the command.

Get QoS Settings on the Access Point

To view the current QoS settings and queue names for access-point-to-station parameters:

```
USR5453-AP# get tx-queue
name   queue  aifs  cwmin  cwmax  burst
--------------------------------------
wlan0  data0  1     3      7      1.5
wlan0  data1  1     7      15     3.0
wlan0  data2  3     15     63     0
wlan0  data3  7     15     1023   0
```

Get QoS Settings on the Client Station

To view the current QoS settings queue names for station-to-access-point parameters:

```
USR5453-AP# get wme-queue
name   queue  aifs  cwmin  cwmax  txop-limit
-----------------------------------------
wlan0  vo     2     3      7      47
wlan0  vi     2     7      15     94
wlan0  be     3     15     1023   0
wlan0  bk     7     15     1023   0
```

Set Arbirtation Interframe Spaces (AIFS)

Arbitration Inter-Frame Spacing (AIFS) specifies a wait time (in milliseconds) for data frames.

Valid values for AIFS are 1-255.

Set AIFS on the Access Point

To set AIFS on access-point-to-station traffic:

```
set tx-queue wlan0 with queue Queue_Name to aifs AIFS_Value
```

Where *Queue_Name* is the queue on the access point to which you want the setting to apply and *AIFS_Value* is the wait time value you want to specify for AIFS.

For example, this command sets the AIFS wait time on the access point Voice queue (data0) to 13 milliseconds.

```
USR5453-AP# set tx-queue wlan0 with queue data0 to aifs 13
```

View the results of this configuration update (bold in the command output highlights the modified value):

```
USR5453-AP# get tx-queue
name   queue  aifs  cwmin  cwmax  burst
--------------------------------------
```

```
wlan0   data0   13     3       7       1.5
wlan0   data1   1      7       15      3.0
wlan0   data2   3      15      63      0
wlan0   data3   7      15      1023    0
```

Set AIFS on the Client Station

To set the AIFS on station-to-access-point traffic:

```
set wme-queue wlan0 with queue Queue_Name to aifs AIFS_Value
```

Where *Queue_Name* is the queue on the station to which you want the setting to apply and *AIFS_Value* is the wait time value you want to specify for AIFS.

For example, this command sets the AIFS wait time on the station Voice queue (vo) to 14 milliseconds.

```
USR5453-AP# set wme-queue wlan0 with queue vo to aifs 14
```

View the results of this configuration update (bold in the command output highlights the modified value):

```
USR5453-AP# get wme-queue
name    queue   aifs   cwmin   cwmax   txop-limit
-----------------------------------------------
wlan0   vo      14     3       7       47
wlan0   vi      2      7       15      94
wlan0   be      3      15      1023    0
wlan0   bk      7      15      1023    0
```

Setting Minimum and Maximum Contention Windows (cwmin, cwmax)

The *Minimum Contention Window* (`cwmin`) sets the upper limit (in milliseconds) of the range from which the initial random backoff wait time is determined. For more details, see "Random Backoff and Minimum / Maximum Contention Windows" on page 136.)

Valid values for the "`cwmin`" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. The value for "`cwmin`" must be lower than the value for "`cwmax`".

The *Maximum Contention Window* (`cwmax`) sets the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. For more details, see "Random Backoff and Minimum / Maximum Contention Windows" on page 136.)

Valid values for the "`cwmax`" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. The value for "`cwmax`" must be higher than the value for "`cwmin`".

Set cwmin and cwmax on the Access Point

To set the Minimum and Maximum Contention Windows (cwmin, cwmax) on access-point-to-station traffic:

```
set tx-queue wlan0 with queue Queue_Name to cwmin cwmin_Value cwmax cwmax_Value
```

Where *Queue_Name* is the queue on the access point to which you want the setting to apply and *cwmin_Value* and *cwmax_Value* are the values (in milliseconds) you want to specify for contention back-off windows.

For example, this command sets the access point Video queue (data1) `cwmin` value to 15 and `cwmax` value to 31.

```
USR5453-AP# set tx-queue wlan0 with queue data1 cwmin 15 cwmax 31
```

View the results of this configuration update (bold in the command output highlights the modified values):

```
USR5453-AP# get tx-queue
name   queue  aifs  cwmin  cwmax  burst
---------------------------------------
wlan0  data0  13    3      7      1.5
wlan0  data1  1     15     31     3.0
wlan0  data2  3     15     63     0
wlan0  data3  7     15     1023   0
```

Set cwmin and cwmax on the Station

To set the Minimum and Maximum Contention Windows (cwmin, cwmax) on station-to-access-point traffic:

```
set wme-queue wlan0 with queue Queue_Name to cwmin cwmin_Value cwmax
cwmax_Value
```

Where *Queue_Name* is the queue on the station to which you want the setting to apply and *cwmin_Value* and *cwmax_Value* are the values (in milliseconds) you want to specify for contention back-off windows.

For example, this command sets the client station Video queue (vi) `cwmin` value to 15 and `cwmax` value to 31.

```
USR5453-AP# set wme-queue wlan0 with queue vi cwmin 7 cwmax 15
```

View the results of this configuration update (bold in the command output highlights the modified values):

```
USR5453-AP# get wme-queue
name   queue  aifs  cwmin  cwmax  txop-limit
-------------------------------------------
wlan0  vo     14    3      7      47
wlan0  vi     2     7      15     94
wlan0  be     3     15     1023   0
wlan0  bk     7     15     1023   0
```

Set the Maximum Burst Length (burst) on the Access Point

The *Maximum Burst Length* (`burst`) specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The `burst` applies only to the access point (access-point-to-station traffic).

Valid values for maximum burst length are 0.0 through 999.9.

To set the maximum burst length on access-point-to-station traffic:

```
set tx-queue wlan0 with queue Queue_Name to burst burst_Value
```

Where *Queue_Name* is the queue on the access point to which you want the setting to apply and *burst_Value* is the wait time value you want to specify for maximum burst length.

For example, this command sets the maximum packet burst length on the access point Best Effort queue (data2) to 0.5.

```
USR5453-AP# set tx-queue wlan0 with queue data2 to burst 0.5
```

View the results of this configuration update (bold in the command output highlights the modified value):

```
USR5453-AP# get tx-queue
name   queue  aifs  cwmin  cwmax  burst
---------------------------------------
wlan0  data0  13    3      7      1.5
wlan0  data1  1     15     31     3.0
wlan0  data2  3     15     63     0.5
wlan0  data3  7     15     1023   0
```

Set Transmission Opportunity Limit (txop-limit) for WMM client stations

The *Transmission Opportunity Limit* (`txop-limit`) specifies an interval of time (in milliseconds) when a WMM client station has the right to initiate transmissions on the wireless network. The `txop-limit` applies only to the client stations (station-to-access-point traffic).

To set the `txop-limit` on station-to-access-point traffic:

```
set wme-queue wlan0 with queue Queue_Name to txop-limit txop-limit_Value
```

Where *`Queue_Name`* is the queue on the station to which you want the setting to apply and *`txop-limit_Value`* is the value you want to specify for the `txop-limit`.

For example, this command sets the `txop-limit` on the station Voice queue (vo) to 49.

```
USR5453-AP# set wme-queue wlan0 with queue vo to txop-limit 49
```

View the results of this configuration update (bold in the command output highlights the modified value):

```
USR5453-AP# get wme-queue
name   queue  aifs  cwmin  cwmax  txop-limit
-------------------------------------------
wlan0  vo     14    3      7      49
wlan0  vi     2     7      15     94
wlan0  be     3     15     1023   0
wlan0  bk     7     15     1023   0
```

Wireless Distribution System

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 177. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network.

This table shows a quick view of WDS commands and links to detailed examples.

WDS Command	Example
Configuring a WDS Link	See detailed command example below.
Configuring a WDS Link	`get interface wlan0wds0 detail`

Configuring a WDS Link

To set up a Wireless Distribution System (WDS) link between two wireless networks:

1. Enable the WDS interface (`wlan0wds0`) on the current access point:

```
USR5453-AP# set interface wlan0wds0 status up
USR5453-AP# set interface wlan0wds0 radio wlan0
```

2. Provide the MAC address of the remote access point to which you want to link:

```
USR5453-AP# set interface wlan0wds0 remote-mac MAC_Address_Of_Remote_AP
```

For example:

```
USR5453-AP# set interface wlan0wds0 remote-mac 00:E0:B8:76:1B:14
```

Getting Details on a WDS Configuration

Verify the configuration of the WDS link you just configured by getting details on the WDS interface:

```
USR5453-AP# get interface wlan0wds0 detail
Field             Value
------------------------------------------------------
type              wds
status            up
description       Wireless Distribution System - Link 1
mac               00:E0:B8:76:26:08
ip
mask
static-ip
static-mask
rx-bytes          0
rx-packets        0
rx-errors         0
rx-drop           0
rx-fifo           0
```

```
rx-frame          0
rx-compressed     0
rx-multicast      0
tx-bytes          0
tx-packets        0
tx-errors         0
tx-drop           0
tx-fifo           0
tx-colls          0
tx-carrier        0
tx-compressed     0
ssid
bss
security
wpa-personal-key
wep-key-ascii     no
wep-key-length    104
wep-default-key
wep-key-1
wep-key-2
wep-key-3
wep-key-4
vlan-interface
vlan-id
radio             wlan0
remote-mac        00:E0:B8:76:1B:14
wep-key
```

Time Protocol

The *Network Time Protocol* (NTP) is an Internet standard protocol that synchronizes computer clock times on your network. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock. The timestamp will be used to indicate the date and time of each event in log messages. See http://www.ntp.org for more general information on NTP.

To enable the Network Time Protocol (NTP) server on the access point do the following:

1. Enable the NTP Server

```
set ntp status up
```

2. Provide the Host Name or Address of an NTP Server

```
set ntp server NTP_Server
```

Where *NTP_Server* is the host name or IP address of the NTP server you want to use. (USRobotics recommends using the host name rather than the IP address, since IP addresses these change more frequently.)

For example, this command sets the NTP server by host name to "ntp.instant802.com"

```
set ntp server ntp.instant802.com
```

3. Get Current Time Protocol Settings

```
USR5453-AP# get ntp detail
```

```
Field   Value
-------------------------
status  up
server  ntp.instant802.com
```

Reboot the Access Point

To reboot the access point, simply type "`reboot`" at the command line:

```
USR5453-AP# reboot
```

Reset the Access Point to Factory Defaults

If you are experiencing extreme problems with the Professional Access Point and have tried all other troubleshooting measures, you can reset the access point. This will restore factory defaults and clear all settings, including settings such as a new password or wireless settings.

The following command resets the access point from the CLI:

```
USR5453-AP# factory-reset
```

Note Keep in mind that the `factory-reset` command resets only the access point you are currently administering; not other access points in the cluster.

For information on the factory default settings, see "Default Settings for the Professional Access Point" on page 6.

Keyboard Shortcuts and Tab Completion Help

The CLI provides keyboard shortcuts to help you navigate the command line and build valid commands, along with "tab completion" hints on available commands that match what you have typed so far. Using the CLI will be easier if you use the tab completion help and learn the keyboard shortcuts.

- Keyboard Shortcuts
- Tab Completion and Help

Keyboard Shortcuts

Action on CLI	Keyboard Shortcut
Move cursor to the beginning of the current line	Ctrl-a Home
Move cursor to the end of the current line	Ctrl-e End
Move cursor back on the current line, one character at a time	Ctrl-b Left Arrow key
Move the cursor forward on the current line, one character at a time	Ctrl-f Right Arrow Key
Start over at a blank command prompt (abandons the input on the current line)	Ctrl-c
Remove one character on the current line.	Ctrl-h
Remove the last word in the current command. (Clears one word at a time from the current command line, always starting with the last word on the line.)	Ctrl-W
Remove characters starting from cursor location to end of the current line. (Clears the current line from the cursor forward.)	Ctrl-k
Remove all characters before the cursor. (Clears the current line from the cursor back to the CLI prompt.)	Ctrl-U
Clear screen but keep current CLI prompt and input in place.	Ctrl-l
Display previous command in history. (Ctrl-p and Ctrl-n let you cycle through a history of all executed commands like Up and Down arrow keys typically do. Up/Down arrow keys also work for this.)	Ctrl-p Up Arrow key
Display next command in history. (Ctrl-p and Ctrl-n let you cycle through a history of all executed commands like Up and Down arrow keys typically do. Up/Down arrow keys also work for this.)	Ctrl-n Down Arrow key
Exit the CLI. (At a blank command prompt, typing Ctrl-d closes the CLI.) (Typing Ctrl-d within command text also removes characters, one at a time, at cursor location like Ctrl-h.)	Ctrl-d

Tab Completion and Help

Help on commands can be requested at the command line interface (CLI) by using the TAB key. (See also "Basic Settings" on page 179.)

Hitting TAB once will attempt to complete the current command.

If multiple completions exist, a beep will sound and no results will be displayed. Enter TAB again to display all available completions.

- **Example 1:** At a blank command line, hit TAB twice to get a list of all commands.

```
USR5453-AP#
add              Add an instance to the running configuration
factory-reset    Reset the system to factory defaults
get              Get field values of the running configuration
reboot           Reboot the system
remove           Remove instances in the running configuration
save-running     Save the running configuration
set              Set field values of the running configuration
```

- **Example 2:** Type "**get** " TAB TAB (including a space after **get**) to see a list of all field options for the **get** command.

```
USR5453-AP# get
association       Associated station
basic-rate        Basic rate of the radio
bridge-port       Bridge ports of bridge interfaces
bss               Basic Service Set of the radio
cluster           Clustering-based configuration settings
cluster-member    Member of a cluster of like-configured access points
config            Configuration settings
detected-ap       Detected access point
dhcp-client       DHCP client settings
dot11             IEEE 802.11
host              Internet host settings
interface         Network interface
ip-route          IP route entry
klog-entry        Kernel log entry
log               Log settings
log-entry         Log entry
mac-acl           MAC address access list item
ntp               Network Time Protocol client
portal            Guest captive portal
radio             Radio
radius-user       RADIUS user
ssh               SSH access to the command line interface
supported-rate    Supported rates of the radio
system            System settings
telnet            Telnet access to the command line interface
tx-queue          Transmission queue parameters
wme-queue         Transmission queue parameters for stations
```

- **Example 3:** Type "**get system v**" TAB. This will result in completion with the only matching field, "**get system version**". (Hit ENTER to get the output results of the command.)

```
USR5453-AP# get system v
USR5453-AP# get system version
```

- **Example 4:** Type "**set**" TAB TAB (including a space after **set**) to get a list of all field options for the **set** command.

```
USR5453-AP# set
bss               Basic Service Set of the radio
cluster           Clustering-based configuration settings
cluster-member    Member of a cluster of like-configured access po
config            Configuration settings
```

```
dhcp-client      DHCP client settings
dot11            IEEE 802.11
host             Internet host settings
interface        Network interface
ip-route         IP route entry
log              Log settings
mac-acl          MAC address access list item
ntp              Network Time Protocol client
portal           Guest captive portal
radio            Radio
radius-user      RADIUS user
ssh              SSH access to the command line interface
system           System settings
telnet           Telnet access to the command line interface
tx-queue         Transmission queue parameters
wme-queue        Transmission queue parameters for stations
```

- **Example 5:** Type "**set mac**" TAB, and the command will complete with the only matching option:

```
USR5453-AP# set mac-acl
```

- **Example 6:** Type "**set cluster**" TAB TAB, and the two matching options are displayed:

```
USR5453-AP# set cluster
cluster          Clustering-based configuration settings
cluster-member   Member of a cluster of like-configured access points
```

- **Example 7:** Type "**add**" TAB TAB (including a space after **add**) to get a list of all field options for the **add** command.

```
USR5453-AP# add
basic-rate       Basic rate of the radio
bridge-port      Bridge ports of bridge interfaces
bss              Basic Service Set of the radio
interface        Network interface
mac-acl          MAC address access list item
radius-user      RADIUS user
supported-rate   Supported rate of the radio
```

- **Example 8:** Type "**remove**" TAB TAB (including a space after **remove**) to get a list of all field options for the **remove** command

```
USR5453-AP# remove
basic-rate       Basic rate of the radio
bridge-port      Bridge ports of bridge interfaces
bss              Basic Service Set of the radio
interface        Network interface
ip-route         IP route entry
mac-acl          MAC address access list item
radius-user      RADIUS user
supported-rate   Supported rates of the radio
```

CLI Class and Field Overview

The following is an introduction to the CLI classes and fields. For a complete reference guide, see “Class

and Field Reference" on page 239.

Configuration information for the Professional Access Point is represented as a set of classes and objects.

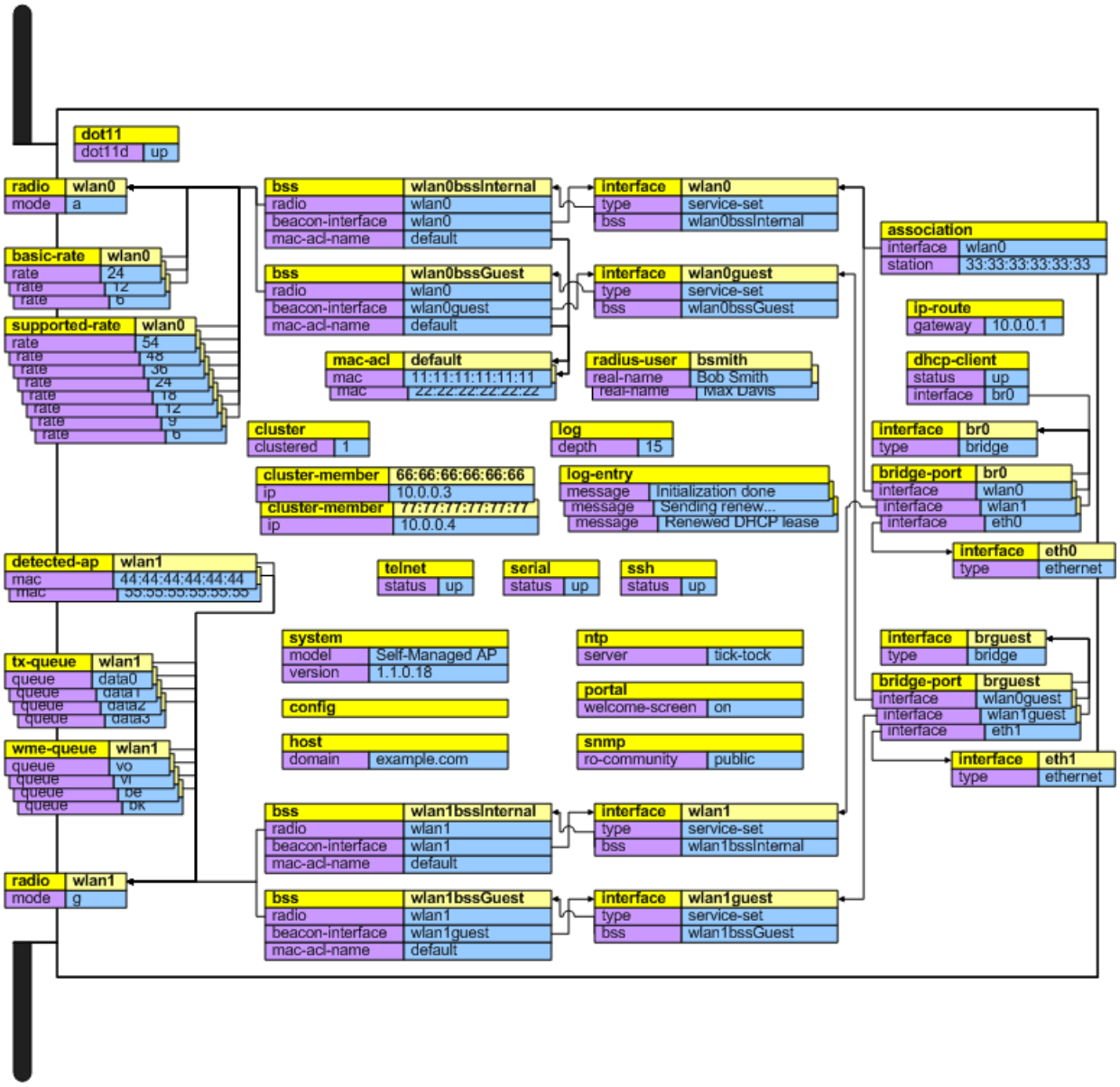
Different kinds of information uses different classes. For example, information about a network interface is represented by the "interface" class, while information about an NTP client is represented by the "ntp" class.

Depending on the type of class, there can be multiple instances of a class. For example, there is one instance of the "interface" class for each network interface that the access point has (Ethernet, radio, and so on), while there is just a singleton instance of the "ntp" class, since an access point needs only a single NTP client. Some classes require their instances to have names to differentiate between them; these are called *named classes*. For example, one interface might have a name of `eth0` to indicate that it is an Ethernet interface, while another interface could have a name of `wlan0` to indicate it is a wireless LAN (WLAN) interface. Instances of singleton classes do not have names, since they only have a single instance. Classes that can have multiple instances but do not have a name are called anonymous classes. Together, singleton and anonymous classes are called unnamed classes. Some classes require their instances to have names, but the multiple instances can have the same name to indicate that they are part of the same group. These are called group classes.

has name? \ # of instances?	one	multiple
no	singleton	anonymous
yes - unique	n/a	unique named
yes - non-unique	n/a	group named

Each class defines a set of fields, that describe the actual information associated with a class. Each instance of a class will have a value for each field that contains the information. For example, the interface class has fields such as "ip" and "mask". For one instance, the `ip` field might have a value of 192.168.1.1 while the `mask` field has a value of 255.255.0.0; another instance might have an `ip` field with a value of 10.0.0.1 and `mask` field with a value of 255.0.0.0.

Figure 10. CLI Class Relationships



Class and Field Reference

Class Index

Class	Description
association	An associated station.
basic-rate	A radio rate.
bridge-port	A port that is a member of a bridge.
bss	A BSS of a radio.
cluster	Stores arbitrary data.
cluster-member	Stores arbitrary data.
config	Config settings.
detected-ap	A detected access point.
dhcp-client	The handler for the DHCP client class.
dot11	802.11 settings (all radios).
host	IP host settings.
interface	A network interface.
ip-route	An IP route.
jvm	Java Virtual Machine.
kickstartd	The handler for the kickstartd class
log	Access point log settings.
log-entry	An entry in the log.
mac-acl	A MAC access list entry.
ntp	Network Time Protocol client settings.
portal	Guest captive portal settings.
radio	A physical radio.
radius-user	A local authentication server user.
serial	The handler for the serial class.
snmp	SNMP server.
ssh	The handler for the ssh class.
supported-rate	A radio rate.
system	System-wide settings.
telnet	The handler for the telnet class.
traphost	An SNMP trap destination host.
tx-queue	A transmission queue.
web-ui	Web user interface settings.
wme-queue	A WME station queue.

association

Persistent: No.
Purpose: An associated station.

Field Index

Field	Description
interface	The interface with which the station is associated.
station	The MAC address of the station.
authenticated	Whether the station is authenticated.
associated	Whether the station is associated.
rx-packets	The number of packets received from the station.
tx-packets	The number of packets transmitted by the station.
rx-bytes	The number of bytes received from the station.
tx-bytes	The number of bytes transmitted by the station.
tx-rate	The transmission rate.
listen-interval	The listen interval.

interface

Purpose The interface with which the station is associated.
Valid values Linux network interface name.

station

Purpose The MAC address of the station.
Valid values Six colon-separated octets in hexadecimal.

authenticated

Purpose Whether the station is authenticated.
Valid values "Yes" or "-".

associated

Purpose Whether the station is associated.
Valid values "Yes" or "-".

rx-packets

Purpose The number of packets received from the station.
Valid values Positive integer.

tx-packets

Purpose The number of packets transmitted by the station.
Valid values Positive integer.

rx-bytes

Purpose The number of bytes received from the station.
Valid values Positive integer.

tx-bytes

Purpose The number of bytes transmitted by the station.
Valid values Positive integer.

tx-rate

Purpose The transmission rate.
Valid values A rate, in 100 kbps.

listen-interval

Purpose The listen interval.
Valid values A time, in ms.

basic-rate

Persistent: Yes.
Purpose: A radio rate.
Description: Used to set the rate sets of radios.

Field Index

Field	Description
rate	A radio rate in MBps.

rate

Purpose A radio rate in MBps. Note that you cannot change an existing rate field; you can only insert or delete the entire instance.
Valid values Positive integer, or 5.5.

bridge-port

Persistent: Yes.
Purpose: A port that is a member of a bridge.

Field Index

Field	Description
path-cost	The path cost.
priority	The port priority.

path-cost

Purpose The path cost. Used only when STP is on.
Valid values 1-65535.

priority

Purpose The port priority. Used only when STP is on.
Valid values 0-255.

bss

Persistent: Yes.
Purpose: A BSS of a radio.
Description: Represents a basic service set.

Field Index

Field	Description
status	Controls whether this is on or off.
description	A human-readable description of the interface.
radio	The radio this is part of.
beacon-interface	The service-set interface to send beacons for.
mac	The MAC address of the interface.
dtim-period	Delivery Traffic Information Map period.
max-stations	Maximum number of stations.
ignore-broadcast-ssid	Do not send SSID in beacons and ignore probe requests.
mac-acl-mode	MAC address Access Control List mode.
mac-acl-name	The name of the mac access control list to use.
radius-accounting	Whether RADIUS accounting is enabled.
radius-ip	The RADIUS server IP address.
radius-key	The RADIUS server shared secret.
open-system-authentication	Whether Open System authentication is permitted.
shared-key-authentication	Whether Shared Key authentication is permitted.
wpa-cipher-tkip	Whether TKIP is permitted as a WPA cipher.
wpa-cipher-ccmp	Whether CCMP is permitted as a WPA cipher.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

description

Purpose A human-readable description of the interface.
Valid values an ASCII string.

radio

Purpose The radio this is part of.
Valid values The name of an existing radio instance.

beacon-interface

Purpose The service-set interface to send beacons for.
Valid values The name of an existing interface instance with type of service-set.

mac

Purpose The MAC address of the interface. Read-only; value is determined by the starting MAC of the radio.
Valid values 6 colon-separated hexadecimal digit pairs.

dtim-period

Purpose Delivery Traffic Information Map period.
Valid values 1-225.

max-stations

Purpose Maximum number of stations.
Valid values 0-2007.

ignore-broadcast-ssid

Purpose Do not send SSID in beacons and ignore probe requests.
Valid values "on" or "off".

mac-acl-mode

Purpose MAC address Access Control List mode.
Valid values "deny-list": deny only stations in list. "accept-list": accept only stations in list. */

mac-acl-name

Purpose The name of the mac access control list to use.
Valid values the name of existing mac-acl instances.

radius-accounting

Purpose Whether RADIUS accounting is enabled. If unset defaults to "off".
Valid values "on" or "off".

radius-ip

Purpose The RADIUS server IP address.
Valid values An IP address.

radius-key

Purpose The RADIUS server shared secret.
Valid values A string.

open-system-authentication

Purpose Whether Open System authentication is permitted.
Valid values "on" or "off".

shared-key-authentication

Purpose Whether Shared Key authentication is permitted.
Valid values "on" or "off".

wpa-cipher-tkip

Purpose Whether TKIP is permitted as a WPA cipher.
Valid values "on" or "off".

wpa-cipher-ccmp

Purpose Whether CCMP is permitted as a WPA cipher.
Valid values "on" or "off".

channel-planner

Persistent: Yes.
Purpose: Stores arbitrary data.

Field Index

This class has the same fields as class cluster-member.

cluster

Persistent: Yes.
Purpose: Stores arbitrary data.

Field Index

This class has the same fields as class cluster-member.

cluster-member

Persistent: Yes.

Purpose: Stores arbitrary data.
Description: No services are restarted.

config

Persistent: Yes.
Purpose: Configuration settings.
Description: Used for configuration fields.

Field Index

Field	Description
startup	Configuration at boot time.
default	Configuration after factory reset.
no-external-updates	Prevent external configuration updates

startup

Purpose Configuration at boot time.
Write-only.
Valid values "default": Reset to factory defaults.
"rescue": Reset to rescue.
"running": Save running configuration.

default

Purpose Configuration after factory reset.
Write-only.
Valid values "rescue": Reset to rescue.
"running": Save running configuration.

no-external-updates

Purpose Prevent external configuration updates.
Valid values "up" or "down".

debug

Persistent: Yes.
Purpose: Access point debug settings.
Description: The debugging parameters of the access point.

Field Index

Field	Description
level	Level of debugging information.
timestamp	Add a timestamp to debugging information.
klevel	Level of kernel debugging information.
olevel	Level of Orchestrator debugging information.
ologhost	Host for Orchestrator to send syslogs to.

level

Purpose Level of debugging information.
Valid values 0-5.

timestamp

Purpose Add a timestamp to debugging information.
Valid values "on" or "off".

klevel

Purpose Level of kernel debugging information.
Valid values 1-8.

olevel

Purpose Level of Orchestrator debugging information.
Valid values 0-7.

ologhost

Purpose Host for Orchestrator to send syslogs to.
Valid values IP address.

detected-ap

Persistent: No.
Purpose: A detected access point.
Description: Represents an access point that has been detected by passive scanning.

Field Index

Field	Description
mac	The MAC address of the AP.
radio	The radio that detected the AP.
beacon-interval	The beacon interval of the AP in kus (1.
capability	The capabilities of the AP.
type	The type of device detected.
privacy	Whether privacy (WEP or WPA) is enabled.
ssid	The SSID of the AP.
wpa	Whether WPA security is enabled.
phy-type	The mode our radio was in when the AP was detected.
band	The RF band the AP was detected in.
channel	The channel of the AP.
rate	The rate of the AP.
signal	The signal of the AP.
erp	The ERP of the AP.
beacons	The number of beacons received from this AP.
last-beacon	The time of the last beacon received from this AP.
supported-rates	The supported rates of the AP.

mac

Purpose The MAC address of the AP.
Valid values Six colon-separated octets in hexadecimal.

radio

Purpose The radio that detected the AP.
Valid values Linux network interface name.

beacon-interval

Purpose The beacon interval of the AP in kus (1.024 ms).
Valid values Positive integer.

capability

Purpose *The capabilities of the AP.*
Valid values C-formatted hexadecmial bitflag.

type

Purpose The type of device detected.
Valid values "AP", "Ad hoc", or "Other".

privacy

Purpose Whether privacy (WEP or WPA) is enabled.
Valid values "On" or "Off".

ssid

Purpose The SSID of the AP.
Valid values String of up to 32 octets.

wpa

Purpose Whether WPA security is enabled.
Valid values "On" or "Off".

phy-type

Purpose The mode your radio was in when the AP was detected.
Valid values 4: IEEE 802.11b.
7: IEEE 802.11g.

band

Purpose The RF band the AP was detected in.
Valid values "2.4" or "5".

channel

Purpose The channel of the AP.
Valid values Positive integer.

rate

Purpose The rate of the AP.
Valid values Positive integer.

signal

Purpose The signal of the AP.
Valid values Positive integer.

erp

Purpose The ERP of the AP.
Valid values C-formatted hexadecimal number.

beacons

Purpose The number of beacons received from this AP.
Valid values Positive integer.

last-beacon

Purpose The time of the last beacon received from this AP.
Valid values Date and time, in Unix time format.

supported-rates

Purpose The supported rates of the AP.
Valid values Bracketed list of hexadecimal rate codes.

dhcp-client

Persistent: Yes.
Purpose: The handler for the DHCP client class.
Description: Represents a DHCP client.

Field Index

Field	Description
status	Controls whether this is on or off.
interface	The interface to perform DHCP on.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

interface

Purpose The interface to perform DHCP on.
Valid values The name of an existing interface instance. */

dot11

Persistent: Yes.
Purpose: 802.11 settings (all radios).
Description: Represents the wireless functions of the access point.

Field Index

Field	Description
status	Controls whether 802.
debug	The debugging level for 802.
dot11d	Whether AP should enable 802.

status

Purpose Controls whether 802.11 is in use.
Valid values "up" or "down".

debug

Purpose The debugging level for 802.11.
Valid values 0-3.

dot11d

Purpose Whether AP should enable 802.11d
Valid values "up" or "down".

host

Persistent: Yes.
Purpose: IP host settings.
Description: Used for IP host fields.

Field Index

Field	Description
dns-[12]	Domain name servers in use.
domain	Domain name in use.
id	The host name.
static-dns-[12]	Domain name servers to use when not obtained through DHCP.
static-domain	Domain name to use when not obtained through DHCP.
dns-via-dhcp	Whether DNS parameters are obtained through DHCP.

dns-[12]

Purpose Domain name servers in use.
Valid values IP address.

domain

Purpose Domain name in use.
Valid values DNS domain name.

id

purpose The host name.
Valid values DNS domain name.

static-dns-[12]

Purpose Domain name servers to use when not obtained through DHCP.
Valid values IP address.

static-domain

Purpose Domain name to use when not obtained through DHCP.
Valid values DNS domain name.

dns-via-dhcp

Purpose Whether DNS parameters are obtained through DHCP.
Valid values "up" or "down".

interface

Persistent: Yes.
Purpose: A network interface.
Description: Used for per-interface fields.

Field Index

Field	Description
ip	The actual IP address of this interface.
mask	The actual netmask of this interface.
status	Controls whether this is on or off.
type	The type of the interface.
description	A human-readable description of the interface.
mac	The MAC address of the interface.
static-ip	The static IP address of this interface.
static-mask	The static netamsk of this interface.
rx-bytes	Received bytes.
rx-packets	Received packets.
rx-errors	Received packets with errors.
rx-drop	Received packets that were dropped.
rx-fifo	Received packets with FIFO overflows.
rx-frame	Received packets with frame errors.
rx-compressed	Received packets with compression.
rx-multicast	Received packets that were multicast.
tx-bytes	Transmitted bytes.
tx-packets	Transmitted packets.
tx-errors	Transmitted packets with errors.
tx-drop	Transmitted packets that were dropped.
tx-fifo	Transmitted packets with FIFO overflows.
tx-colls	Transmitted packets will collisions.
tx-carrier	Transmitted packets with carrier errors.
tx-compressed	Transmitted packets with compression.

ip

Purpose The actual IP address of this interface. Read-only.
Valid values IP address.

mask

Purpose The actual netmask of this interface.
Read-only.

Valid values Netmask in dotted-decimal notation.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

type

Purpose The type of the interface. Used to determine what additional fields are available. Read-only.
Valid values "service-set", "bridge", "vlan", "wds", "pptp", "pppoe".

description

Purpose A human-readable description of the interface.
Valid values an ASCII string.

mac

Purpose The MAC address of the interface.
Valid values 6 colon-separated hexadecimal digit pairs.

static-ip

Purpose The static IP address of this interface. Used when DHCP is not in use.
Valid values IP address.

static-mask

Purpose The static netamsk of this interface. Used when DHCP is not in use.
Valid values Netmask in dotted-decimal notation.

rx-bytes

Purpose Received bytes.
Valid values Integer.

rx-packets

Purpose Received packets.
Valid values Integer.

rx-errors

Purpose Received packets with errors.
Valid values Integer.

rx-drop

Purpose *Received packets that were dropped*
Valid values Integer.

rx-fifo

Purpose Received packets with FIFO overflows.
Valid values Integer.

rx-frame

Purpose Received packets with frame errors.
Valid values Integer.

rx-compressed

Purpose Received packets with compression.
Valid values Integer.

rx-multicast

Purpose Received packets that were multicast.
Valid values Integer.

tx-bytes

Purpose Transmitted bytes.
Valid values Integer.

tx-packets

Purpose Transmitted packets.
Valid values Integer.

tx-errors

Purpose Transmitted packets with errors.
Valid values Integer.

tx-drop

Purpose Transmitted packets that were dropped.
Valid values Integer.

tx-fifo

Purpose Transmitted packets with FIFO overflows.

Valid values Integer.

tx-colls

Purpose Transmitted packets will collisions.
Valid values Integer.

tx-carrier

Purpose Transmitted packets with carrier errors.
Valid values Integer.

tx-compressed

Purpose Transmitted packets with compression.
Valid values Integer.

ip-route

Persistent: Yes.
Purpose: An IP route.
Description: An IP route.

Field Index

Field	Description
in-use	Whether the route is currently in use.
destination	The destination network prefix.
mask	The mask of the destination network prefix.
gateway	The router by which the destination is reachable.

in-use

Purpose Whether the route is currently in use. Read-only.
Valid values "up" or "down".

destination

Purpose The destination network prefix.
Valid values IP address prefix.

mask

Purpose The mask of the destination network prefix.

Valid values Netmask.

gateway

Purpose The router by which the destination is reachable.
Valid values IP address.

jvm

Persistent: No.
Purpose: Java Virtual Machine.
Description: Represents a JVM.

Field Index

Field	Description
status	Controls whether this is on or off.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

kickstartd

Persistent: No.
Purpose: The handler for the kickstartd class.
Description: Represents a kickstartd process.

log

Persistent: Yes.
Purpose: Access point log settings.
Description: Access point log messages.

Field Index

Field	Description
depth	The number of log entries to keep

depth

Purpose The number of log entries to keep.
Valid values Positive integer.

log-entry

Persistent: No.
Purpose: An entry in the log.
Description: An entry in the log.

Field Index

Field	Description
number	The entry number.
priority	The priority of the log entry.
time	The time of the message.
daemon	The daemon the message is associated with.
message	The message.

number

Purpose The entry number.
Valid values A non-zero integer.

priority

Purpose The priority of the log entry.
Valid values A non-zero integer.

time

Purpose The time of the message.
Valid values A Unix-format time.

daemon

Purpose The daemon the message is associated with.
Valid values String.

message

Purpose The message.
Valid values String.

mac-acl

Persistent: Yes.
Purpose: A MAC access list entry.
Description: Each instance represents a single MAC address. All instances with the same name form a list. This list can be used by BSSes.

Field Index

Field	Description
mac	A MAC address.

mac

Purpose A MAC address.
Valid values 6 colon-separated hexadecimal digit pairs. */

ntp

Persistent: Yes.
Purpose: Network Time Protocol client settings.

Field Index

Field	Description
status	Controls whether this is on or off.
server	The NTP server IP address.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

server

Purpose The NTP server IP address.
Valid values An IP address.

portal

Persistent: Yes.
Purpose: Guest captive portal settings.
Description: Represents a portal. When a portal is run on an interface, traffic entering that interface does not have unconditional access to the AP - they must satisfy some portal requirements, such as clicking through a welcome screen, before access is given.

Field Index

Field	Description
status	Controls whether this is on or off.
welcome-screen	Whether the welcome screen is shown to guest users.
welcome-screen-text	Text to display on the welcome screen.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

welcome-screen

Purpose Whether the welcome screen is shown to guest users.
Valid values "on" or "off".

welcome-screen-text

Purpose Text to display on the welcome screen.
Valid values HTML.

radio

Persistent: Yes.
Purpose: A physical radio.
Description: Represents a physical radio.

Field Index

Field	Description
status	Controls whether the radio is on or off.
description	A human-readable description of the interface.
mac	The MAC address of the radio.
max-bss	The maximum number of BSSes permitted on this radio.
channel-policy	The channel policy of this radio.
mode	The wireless mode of this radio.
super-g	Whether Super G is enabled.
static-channel	The static channel of this radio.
tx-power	The transmit power of this radio.
tx-rx-status	Whether the radio transmits and receives data.
beacon-interval	The beacon interval for this radio in kus (1.
rts-threshold	The size of frames at which RTS/CTS will be used.
fragmentation-threshold	The size of frames at which they will be fragmented.
load-balance-disassociation-utilization	The load that must be exceeded in order for a station to be disassociated.
load-balance-disassociation-stations	The number of associated stations that must be exceeded for a station to be disassociated.
load-balance-no-association-utilization	The load that must be exceeded in order for new stations to be prohibited from associating.
ap-detection	Whether AP detection is performed.
station-isolation	Whether stations are isolated.
wme	Whether WME is enabled.
wme_wifi_noack_test	Mode for Wi-Fi noack test.

status

Purpose Controls whether the radio is on or off
Valid values "up" or "down".

description

Purpose A human-readable description of the interface.
Valid values an ASCII string.

mac

Purpose The MAC address of the radio. If blank, obtains the MAC address of the radio from hard-

ware. This will be used as the starting MAC address for the BSSes.

Valid values 6 colon-separated hexadecimal digit pairs.

max-bss

Purpose The maximum number of BSSes permitted on this radio. This limits the number of bss instances whose radio field can be this radio's name.

Valid values Positive integers.

channel-policy

Purpose The channel policy of this radio.

Valid values static: Use static-channel.
best: Select the best channel.

mode

Purpose The wireless mode of this radio.

Valid values The Valid values depend on the capabilities of the radio:
b: IEEE 802.11b.
g: IEEE 802.11g.

super-g

Purpose Whether Super G is enabled. If unset defaults to "no".

Valid values "yes" or "no".

static-channel

Purpose The static channel of this radio. Used when channel policy is static.

Valid values Depends on regulatory-domain and mode. All channels are positive integers.

tx-power

Purpose The transmit power of this radio.

Valid values A percentage.

tx-rx-status

Purpose Whether the radio transmits and receives data.

Valid values "up" or "down".

beacon-interval

Purpose The beacon interval for this radio in kus (1.024 ms).

Valid values 20-2000.

rts-threshold

Purpose The size of frames at which RTS/CTS will be used.
Valid values 0-2347.

fragmentation-threshold

Purpose The size of frames at which they will be fragmented.
Valid values 256-2346.

load-balance-disassociation-utilization

Purpose The load that must be exceeded in order for a station to be disassociated. The condition for load-balance-disassociation-stations must also be satisfied, if it is non-zero.
Valid values A non-zero percentage, or 0 to disable.

load-balance-disassociation-stations

Purpose The number of associated stations that must be exceeded for a station to be disassociated. The condition for load-balance-disassociation-utilization must also be satisfied, if it is non-zero.
Valid values 1-2007, or 0 to disable.

load-balance-no-association-utilization

Purpose The load that must be exceeded in order for new stations to be prohibited from associating.
Valid values A non-zero percentage, or 0 to disable.

ap-detection

Purpose Whether AP detection is performed. If on, the detected APs will be represented by instances of the detected-ap class.
Valid values "on" or "off".

station-isolation

Purpose Whether stations are isolated. If on, then stations on this radio cannot exchange data with other stations on this radio.
Valid values "on" or "off".

wme

Purpose Whether WME is enabled. Determines whether wme-queue values will be sent to clients.
Valid values "on" or "off".

wme_wifi_noack_test

Purpose Mode for Wi-Fi noack test.

Valid values "on" or "off".

radius-user

Persistent: Yes.
Purpose: A local authentication server user.
Description: Handles username/password and generates password hash

serial

Persistent: Yes.
Purpose: The handler for the serial class.
Description: Represents the serial access to the CLI.

snmp

Persistent: Yes.
Purpose: SNMP server.
Description: Represents a SNMP server.

Field Index

Field	Description
status	Controls whether this is on or off.
ro-community	The read-only community name.
rw-community	The read-write community name.
ip	The IP address of the interface to listen on.
engine-id	The engine identifier.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

ro-community

Purpose The read-only community name.
Valid values String.

rw-community

Purpose The read-write community name.
Valid values String.

ip

Purpose The IP address of the interface to listen on.
Valid values IP address.

engine-id

Purpose The engine identifier.
Valid values A string.

ssh

Persistent: Yes.
Purpose: The handler for the ssh class.
Description: Represents the SSH.

supported-rate

Persistent: Yes.
Purpose: A radio rate.

Field Index

This class has the same fields as class basic-rate.

system

Persistent: Yes.
Purpose: System-wide settings.
Description: Used for system-wide fields.

Field Index

Field	Description
password	The login password.
encrypted-password	The login password, crypted.
password-initialized	Whether the password has been initialized since first boot.
reboot	Reboot the system.

password

Purpose The login password.
Write-only.
Valid values String.

encrypted-password

Purpose The login password, crypted.
Valid values String.

password-initialized

Purpose Whether the password has been initialized since first boot.
Valid values 1, or blank.

reboot

Purpose Reboot the system.
Write-only.
Valid values "yes" to reboot.

telnet

Persistent: Yes.
Purpose: The handler for the telnet class.
Description: Represents Telnet access to the CLI.

traphost

Persistent: Yes.
Purpose: An SNMP trap destination host.
Description: Represents a trapsink, trap2sink and informsink commands in SNMPD configuration file.

Field Index

Field	Description
host	The host to send traps to.
community	The community to send the traps with.
type	The type of traps to send.

host

Purpose The host to send traps to.
Valid values IP address.

community

Purpose The community to send the traps with.
Valid values A string.

type

Purpose The type of traps to send.
Valid values "trapsink", "trap2sink", or "informsink".

tx-queue

Persistent: Yes.
Purpose: A transmission queue.
Description: Represents transmission queue parameters of a radio. The name of the instance must be the same as the name of the radio it represents.

Field Index

Field	Description
queue	The queue.
aifs	Adaptive Inter-Frame Space.
cwmin	Minimum contention window.
cwmax	Maximum contention window.
burst	Maximum burst length.

queue

Purpose The queue.
Valid values "data0", "data1", "data2", "data3", "mgmt", "after_beacon", or "beacon".

aifs

Purpose Adaptive Inter-Frame Space.
Valid values 1-255.

cwmin

Purpose Minimum contention window.
Valid values 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024.

cwmax

Purpose Maximum contention window.
Valid values 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024.

burst

Purpose Maximum burst length.
Valid values 0.0-999.9.

web-ui

Persistent: No.
Purpose: Web user interface settings.
Description: Represents the web user interface of the AP.

Field Index

Field	Description
status	Controls whether this is on or off.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

wme-queue

Persistent: Yes.
Purpose: A WME station queue.
Description: Represents queue parameters of a WME station. The name of the instance must be the same as the name of the radio to whose stations it applies to.

Troubleshooting

This part of the Professional Access Point Administrator Guide addresses installation and post-installation troubleshooting issues as follows:

- Installation and Connectivity Troubleshooting
    - The installation procedure does not begin when I insert the Installation CD-ROM.
    - The Professional Access Point Detection Utility does not find the access point.
    - I cannot access the Web User Interface.
    - I need to configure the access point with an operating system other than Windows.
    - My wireless device cannot find the wireless network.
    - I changed the access point settings, and now my wireless device does not establish a wireless connection.
    - I am experiencing poor wireless link quality.
- Configuration Troubleshooting
    - Wireless Distribution System (WDS) Problems and Solutions
    - Cluster Recovery

Installation and Connectivity Troubleshooting

The installation procedure does not begin when I insert the Installation CD-ROM.

Possible Solution:

You may be running a program that interferes with the autolaunch feature of the CD-ROM. Navigate to your CD-ROM drive and launch **Startup.exe**.

The Professional Access Point Detection Utility does not find the

access point.

Possible Solution 1:

1. Ensure that all cables are plugged in firmly, and verify that the access point's power indicator is lighted.

2. In the Detection Utility, click **Back** and then click **Next** to restart the discovery process.

Possible Solution 2:

You can open the access point's Web User Interface without using the Detection Utility by typing the IP address in your Web browser's navigation or address bar. To find the IP address of the access point,

1. Using the configuration program for the networking device to which the access point is connected, view the device's client list.

2. Find the MAC address of the access point in the client list.

3. Note the IP address the corresponds to the MAC address of the access point.

Possible Solution 3:

The access point and the administrator machine may not be connected to the same subnet. Bypass your local area network by connecting the access point directly to the administrator computer, then start the Detection Utility again. If the Detection Utility finds the access point, either the two machines were on different subnets or the problem lies within your LAN.

If you are unable to connect the Access Point and the administrator computer to the same subnet, you can perform Access Point configuration by using the direct connection. For more information about using this method, see "Setting Up and Launching Your Wireless Network" on page 13.

I cannot access the Web User Interface.

Possible Solution 1:

Verify that you are entering the correct IP address in your Web browser.

Possible Solution 2:

Reboot the access point by disconnecting and then reconnecting its power adapter.

Possible Solution 3:

Verify the connection setting of your Web browser, and verify that the HTTP Proxy feature of your Web browser is disabled.

Internet Explorer users:

1. Click **Tools**, click **Internet Options**, and then click the **Connections** tab.

2. Select **Never dial a connection**, and then click the **LAN Settings** button.

3. Clear all the checkboxes and click **OK**.

4. Click **OK** again to apply the connection setting

Netscape Navigator users:

1. Click **Edit**, **Preferences**, and then double-click **Advanced** in the Category window.

2. Click **Proxies**, select **Direct connection to the Internet**, and then click **OK**.

Possible Solution 4:

Note Resetting the access point returns all settings to their factory defaults. You will have to re-enter your configuration settings or restore your configuration backup after resetting the access point.

Reset the access point by using a thin object, such as a paper clip, to press the Reset button until both the LAN and WLAN LEDs turn off briefly.

I need to configure the access point with an operating system other than Windows.

Possible Solution:

You must configure the access point through its Web User Interface as follows:

1. Find the access point's IP address:

    1) Using the configuration program for the networking device to which the access point is connected, view the device's client list.

    2) Find the MAC address of the access point in the client list.

    3) Note the IP address the corresponds to the MAC address of the access point.

2. Launch a Web browser, type the IP address of the access point in the browser's navigation bar, and press Enter.

3. You can now log in and perform access point configuration.

My wireless device cannot find the wireless network.

Possible Solution 1:

Move the wireless device closer to the access point. The device may be out of the access point's range.

Possible Solution 2:

Ensure that the wireless device is set to **Infrastructure** mode and has the following settings in common with the access point:

- SSID, also called **Network Name**.
- Kind of security (for example, WPA)
- Security key value
- 802.11 mode

If you change the settings on the access point, remember to change the settings on your wireless devices also.

Possible Solution 3:

Ensure that the access point is broadcasting its SSID:

1. Open the Web User Interface of the access point.
2. From the **Advanced** menu, select **Security**.
3. Verify that **Broadcast SSID** is set to **Allow**.
4. Click **Update** to save any change.

Possible Solution 4:

If you use MAC filtering on the access point, verify that the MAC address of the client is allowed to access your wireless network:

1. Open the Web User Interface of the access point.
2. From the **Advanced** menu, select **MAC Filtering**.
3. If you selected **Allow only stations in list**, verify that the client's MAC address is included in the Stations List.

   If you selected **Allow any station unless in list**, verify that the client's MAC address is not included in the Stations List.

Possible Solution 5:

Reboot the access point by disconnecting and then reconnecting its power adapter.

Possible Solution 6:

Note Resetting the access point returns all settings to their factory defaults. You will have to re-enter your configuration settings or restore your configuration backup after resetting the access point.

Reset the access point by using a thin object, such as a paper clip, to press the Reset button press the Reset button until both the LAN and WLAN LEDs turn off briefly.

I changed the access point settings, and now my wireless device does not establish a wireless connection.

Possible Solution:

Ensure that the client device is using the correct Pass phrase and encryption options. If you changed the settings in the configuration of the Professional Access Point, you must also change the settings of every wireless adapter that needs access to the wireless network. The settings of the wireless PC cards, PCI adapters, or USB adapters must match the new settings of the Professional Access Point.

I am experiencing poor wireless link quality.

Possible Solution 1:

Reposition the access point or the wireless device so that environmental factors, such as lead-based paint or concrete walls, do not interfere with your wireless signal.

Possible Solution 2:

Create a wireless connection on a different channel so that electronic devices, such as 2.4 GHz phones, do not interfere with your wireless signal. For more information about changing channels, see “Channel Management” on page 53.

Configuration Troubleshooting

Wireless Distribution System (WDS) Problems and Solutions

If you are having trouble configuring a WDS link, be sure that you have read the notes and cautions in “Configuring WDS Settings” on page 146. These notes are reprinted here for your convenience. The most common problem that administrators encounter with WDS setups is forgetting to set both access points in the link to the same radio channel and IEEE 802.11 mode. That prerequisite, as well as others, is listed in

the notes below.

Notes

- The only security mode available on the WDS link is Static WEP, which is not particularly secure. Therefore, USRobotics recommends using WDS to bridge the Guest network only. Do not use WDS to bridge access points on the Internal network unless you are not concerned about the security risk for data traffic on that network.
- When using WDS, be sure to configure WDS settings on *both* access points participating in the WDS link.
- You can have only one WDS link between any pair of access points. That is, a remote MAC address may appear only once on the WDS page for a particular access point.
- Both access points participating in a WDS link must be on the same radio channel and use the same IEEE 802.11 mode. (See “Radio” on page 119 for information on configuring the Radio mode and channel.)
- **Do not create loops** with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges. *Spanning Tree Protocol* (STP), which manages path redundancy and prevent unwanted loops, is not available in the Professional Access Point. Keep these rules in mind when working with WDS on the access point:

  Any two access points can be connected by only a single path; either a WDS bridge (wireless) or an Ethernet connection (wired), but not both.

  Do not create backup links.

  If you can trace more than one path between any pair of APs going through any combination of Ethernet or WDS links, you have a loop.

  You can only extend or bridge either the Internal or Guest network but not both.

Cluster Recovery

In cases where the access points in a cluster become out of sync or an access point cannot join or be removed from a cluster, the following methods for cluster recovery are recommended.

Reboot or Reset Access Point

Apply these recovery methods in the order in which they are listed. In all but the last case (stop clustering), you only need to reset or reboot the access point whose configuration is out of synchronization with other cluster members or that cannot join or be removed from the cluster.

1. Reboot the access point by disconnecting and then reconnecting the power cable.

2. Reset the access point through its Web User Interface. To do this, go to `http://IPAddressOfAccessPoint`, navigate to the Advanced menu’s **Reset Configuration** tab, and click the **Reset** button. (IP addresses for APs are on the Cluster menu’s Access Points page for any cluster member.)

3. Reset the access point by pressing the reset button on the device until both the LAN and WLAN LEDs turn off briefly.

4. In extreme cases, rebooting or resetting may not solve the problem. In these cases, follow the procedure described next in “Stop Clustering and Reset Each Access Point in the Cluster” to recover every

access point on the subnet.

Stop Clustering and Reset Each Access Point in the Cluster

If the previous reboot or reset methods do not solve the problem, do the following to stop clustering and reset all APs.

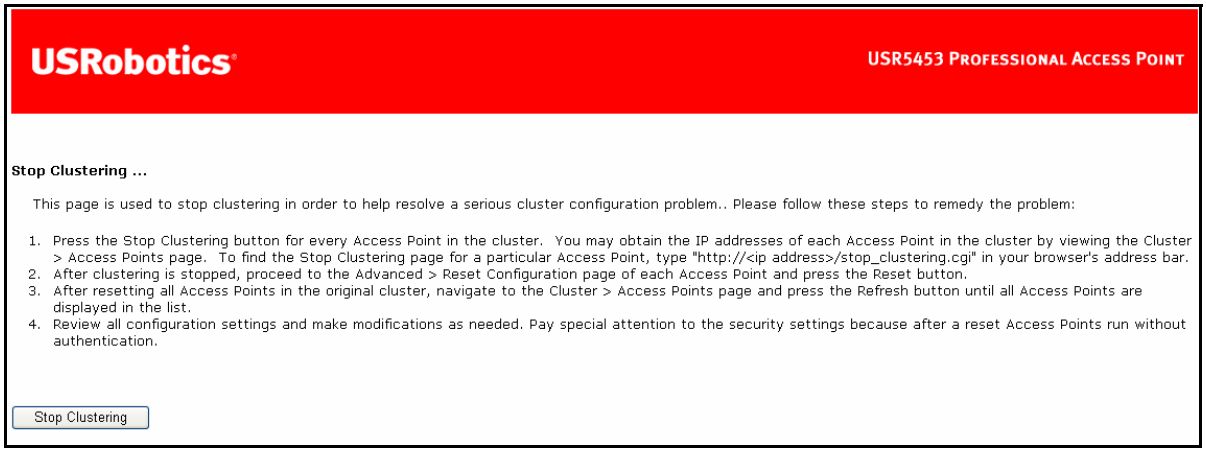
1. Stop clustering on each access point in the cluster.

   To do this, enter the Stop Clustering URL in the address bar of your Web browser as follows:

   `http://IPAddressOfAccessPoint/stop_clustering.cgi`

   Where *IPAddres0sOfAccessPoint* is the IP address of the access point that you want to stop clustering. You can find the IP addresses for the cluster members on the Cluster menu's Access Points page for any of the clustered access points. USRobotics recommends making a note of all IP addresses at this point.

   The Stop Clustering page for this access point is displayed.



   Click **Stop Clustering**.

   Repeat this "stop clustering" step for every access point in the cluster.

> **Caution** Do not proceed to the next step of resetting access points until you have stopped clustering on all access points. Make sure that you first stop clustering on every access point on the subnet, and only then perform the next part of the process of resetting each access point to the factory defaults.

2. Reset each access point.

   To do this, go to the Web User Interface of the access point you want to reset by entering its URL into the address bar of your Web browser:

   `http://IPAddressOfAccessPoint/`

   Where *IPAddres0sOfAccessPoint* is the IP address of the access point you want to reset.

Support Information

If you are having trouble with the configuration or operation of your access point:

1. Refer to the "Troubleshooting" section in this guide.

2. Go to the Support section of the USRobotics Web site at www.usr.com/support/. Many of the most common difficulties that users experience have been addressed in the FAQ and Troubleshooting Web pages for your product. The product number of the Professional Access Point is 5453. You may need to know this to obtain information on the USRobotics Web site.

3. Submit your technical support question using an online form at www.usr.com/emailsupport/.

4. Contact the USRobotics Technical Support Department. To receive assistance, you need your serial number.

Country	Webmail	Voice	Support Hours
United States	www.usr.com/emailsupport	(888) 216-2850	8:00 A.M.–6:00 P.M. M–F, Central Time
Canada	www.usr.com/emailsupport	(888) 216-2850	8:00 A.M.–6:00 P.M. M–F, Central Time
Austria	www.usr.com/emailsupport/de	+43 07 110 900 116	8:00–18:00, M–F
Belgium (Flemish)	www.usr.com/emailsupport/bn	+32 70 23 3545	8:00–18:00, M–F
Belgium (French)	www.usr.com/emailsupport/be	+32 70 23 3546	8:00–18:00, M–F
Czech Republic	www.usr.com/emailsupport/cz		
Denmark	www.usr.com/emailsupport/ea	+45 70 10 4030	8:00–18:00, M–F
Finland	www.usr.com/emailsupport/ea	+358 98 171 0015	8:00–18:00, M–F
France	www.usr.com/emailsupport/fr	+33 082 5070 693	8:00–18:00, M–F
Germany	www.usr.com/emailsupport/de	+49 0180 567 1548	8:00–18:00, M–F
Hungary	www.usr.com/emailsupport/hu	+49 0180 567 1548	9:00–17:00, M–F
Ireland	www.usr.com/emailsupport/uk	+353 1890 252 130	8:00–18:00, M–F
Italy	www.usr.com/emailsupport/it	+39 848 80 9903	8:00–18:00, M–F
Luxembourg	www.usr.com/emailsupport/be	+352 342 080 8318	8:00–18:00, M–F
Middle East/Africa	www.usr.com/emailsupport/me	+44 870 844 4546	8:00–18:00, M–F
Netherlands	www.usr.com/emailsupport/bn	+31 (0) 900 202 5857	8:00–18:00, M–F
Norway	www.usr.com/emailsupport/ea	+47 23 50 0097	8:00–18:00, M–F
Poland	www.usr.com/emailsupport/pl		
Portugal	www.usr.com/emailsupport/pt	+351 (0) 21 415 4034	8:00–18:00, M–F
Russia	www.usr.com/emailsupport/ru	+7 8 800 200 200 1	10:00–18:00, M–F
Spain	www.usr.com/emailsupport/es	+34 902 11 7964	8:00–18:00, M–F
Sweden	www.usr.com/emailsupport/ea	+46 (0) 77 128 1020	8:00–18:00, M–F
Switzerland	www.usr.com/emailsupport/de	+41 0848 840 200	8:00–18:00, M–F

Country	Webmail	Voice	Support Hours
Turkey	www.usr.com/emailsupport/tk		
UAE	www.usr.com/emailsupport/me	+971 0800 877 63	12:00–22:00, M–F
UK	www.usr.com/emailsupport/uk	+44 0870 844 4546	8:00–18:00 M–F

For current support contact information, go to www.usr.com/support.

Regulatory Information

Manufacturer’s Declaration of Conformity

U.S. Robotics Corporation
935 National Parkway
Schaumburg, IL 60173
U.S.A.

declares that this product conforms to the FCC’s specifications:
Part 15, Class B

Operation of this device is subject to the following conditions:
1) this device may not cause harmful electromagnetic interference, and
2) this device must accept any interference received including interference that may cause undesired operations.

This equipment complies with FCC Part 15 for Home and Office use.

Caution to the User: Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

Detachable Antenna Information

FCC Part 15, Subpart C, Section 15.203 Antenna requirement

USR5453 users: An intentional radiator shall be designed to ensure that no antenna other than that furnished by the responsible party shall be used with the device. The use of a permanently attached antenna or of an antenna that uses a unique coupling to the intentional radiator shall be considered sufficient to comply with the provisions of this section. The manufacturer may design the unit so that a broken antenna can be replaced by the user, but the use of a standard antenna jack or electrical connector is prohibited.

FCC Radiation Exposure Statement

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

Radio and Television Interference:

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

to try to correct the interference by one or more of the following measures:

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

USR declares USR 5453 is limited in CH1~11 from 2412 to 2462 MHz by specified firmware controlled in USA.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

UL Listing/CUL Listing:

For External products:
This information technology equipment is UL Listed and C-UL Listed for both the US and Canadian markets respectively for the uses described in the User Guide.

For Internal products:
This information technology equipment is UL Listed and C-UL Listed for both the US and Canadian markets respectively for use with UL-Listed personal computers that have installation instructions detailing user installation of card accessories.

For Laptop/Notebook products:
This information technology equipment is UL Listed and C-UL Listed for both the US and Canadian markets respectively for use only with UL Listed laptop or notebook computers.

For Canadian Users

Industry Canada (IC)

This equipment complies with the Industry Canada Spectrum Management and Telecommunications policy, RSS-210, standard Low Power License-Exempt Radio Communication Devices.

Operation is subject to the following two conditions:

1. This device may cause interference.

2. This device must accept any interference, including interference that may cause undesired operation of the device.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

This device has been designed to operate with an antenna having a maximum gain of 5 dBi. Attaching an antenna with a higher gain to this device is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the Equivalent Isotropic Radiated Power (EIRP) is not more than that required for successful communication.

Caution: Users should not attempt to make electrical ground connections by themselves, but should contact the appropriate inspection authority or an electrician, as appropriate.

CE Compliance

Manufacturer's Declaration of Conformity

We, U.S. Robotics Corporation of 935 National Parkway, Schaumburg, Illinois, 60173-5157 USA, declare under our sole responsibility that the product, U.S. Robotics Professional Access Point, Model 5453, to which this declaration relates, is in conformity with the following standards and/or other normative documents.

EN300 328
EN301 489-1
EN301 489-17
EN60950
EN61000-3-2
EN61000-3-3
EN50392

We, U.S. Robotics Corporation, hereby declare the above named product is in compliance and conformity with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The conformity assessment procedure referred to in Article 10(3) and detailed in Annex II of Directive 1999/5/EC has been followed.

This equipment is in compliance with the European recommendation 1999/519/ECC, governing the exposure to the electromagnetic radiation.

This product can be used in the following countries:

UK, Ireland, Spain, Portugal, Germany, France, Luxembourg, Italy, Switzerland, Austria, Netherlands, Belgium, Norway, Sweden, Denmark, Finland, Czech Republic, Poland, Hungary, and Greece.

Regarding IEEE 802.11g we currently have the following information about restrictions in the R&TTE countries:

Country	Frequency band	Output power
France	2454-2483.5 MHz	10 mW EIRP outdoor

Regulatory Channel Frequency

Channel	Frequency (MHz)	FCC	Canada	ETSI
1	2412	X	X	X
2	2417	X	X	X
3	2422	X	X	X
4	2427	X	X	X
5	2432	X	X	X
6	2437	X	X	X
7	2442	X	X	X
8	2447	X	X	X
9	2452	X	X	X
10	2457	X	X	X
11	2462	X	X	X
12	2467			X
13	2472			X

EU Health Protection

This device complies with the European requirements governing exposure to electromagnetic radiation. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body. This wireless device is a transmitter/receiver and has been designed and manufactured to comply with the exposure limits recommended by the Council of the European Union and the International Commission on Non-Ionizing Radiation Protection (ICNIRP, 1999) for the entire population. The exposure standard for portable equipment uses the "Specific Absorption Rate" as unit of measure. The maximum SAR value of this wireless device measured in the conformity test is 0.52 W/kg.

EU Detachable Antenna Information

This U.S. Robotics wireless device has been designed to operate with the antenna included in this package only. Together this device and antenna combination has been tested and approved by a European Agency conforming with the European R&TTE directive 1999/5/EC to meet the radiated power level requirement of 100mW e.i.r.p. Replacement of this antenna must only be done with an authorized U.S. Robotics component that has been designed and tested with the unit to the requirements of directive 1999/5/EC. Please refer to the U.S. Robotics Web site to get product antenna ordering information.

Operating Channels:	• IEEE 802.11g compliant • 11 channels (US, Canada) • 13 channels (ETSI)

Go to www.usr.com to see the most recent channel restriction information.

U.S. Robotics Corporation Two (2) Year Limited Warranty

1.0 GENERAL TERMS:

1.1 This Limited Warranty is extended only to the original end-user purchaser (CUSTOMER) and is not transferable.

1.2 No agent, reseller, or business partner of U.S. Robotics Corporation (U.S. ROBOTICS) is authorised to modify the terms of this Limited Warranty on behalf of U.S. ROBOTICS.

1.3 This Limited Warranty expressly excludes any product that has not been purchased as new from U.S. ROBOTICS or its authorised reseller.

1.4 This Limited Warranty is only applicable in the country or territory where the product is intended for use (As indicated by the Product Model Number and any local telecommunication approval stickers affixed to the product).

1.5 U.S. ROBOTICS warrants to the CUSTOMER that this product will be free from defects in workmanship and materials, under normal use and service, for TWO (2) YEARS from the date of purchase from U.S. ROBOTICS or its authorised reseller.

1.6 U.S. ROBOTICS sole obligation under this warranty shall be, at U.S. ROBOTICS sole discretion, to repair the defective product or part with new or reconditioned parts; or to exchange the defective product or part with a new or reconditioned product or part that is the same or similar; or if neither of the two foregoing options is reasonably available, U.S. ROBOTICS may, at its sole discretion, provide a refund to the CUSTOMER not to exceed the latest published U.S. ROBOTICS recommended retail purchase price of the product, less any applicable service fees. All products or parts that are exchanged for replacement will become the property of U.S. ROBOTICS.

1.7 U.S. ROBOTICS warrants any replacement product or part for NINETY (90) DAYS from the date the product or part is shipped to Customer.

1.8 U.S. ROBOTICS makes no warranty or representation that this product will meet CUSTOMER requirements or work in combination with any hardware or software products provided by third parties.

1.9 U.S. ROBOTICS makes no warranty or representation that the operation of the software products provided with this product will be uninterrupted or error free, or that all defects in software products will be corrected.

1.10 U.S. ROBOTICS shall not be responsible for any software or other CUSTOMER data or information contained in or stored on this product.

2.0 CUSTOMER OBLIGATIONS:

2.1 CUSTOMER assumes full responsibility that this product meets CUSTOMER specifications and requirements.

2.2 CUSTOMER is specifically advised to make a backup copy of all software provided with this product.

2.3 CUSTOMER assumes full responsibility to properly install and configure this product and to ensure proper installation, configuration, operation and compatibility with the operating environment in which this product is to function.

2.4 CUSTOMER must furnish U.S. ROBOTICS a dated Proof of Purchase (copy of original purchase receipt from U.S. ROBOTICS or its authorised reseller) for any warranty claims to be authorised.

3.0 OBTAINING WARRANTY SERVICE:

3.1 CUSTOMER must contact U.S. ROBOTICS Technical Support or an authorised U.S. ROBOTICS Service Centre within the applicable warranty period to obtain warranty service authorisation.

3.2 Customer must provide Product Model Number, Product Serial Number and dated Proof of Purchase (copy of original purchase receipt from U.S. ROBOTICS or its authorised reseller) to obtain warranty service authorisation.

3.3 For information on how to contact U.S. ROBOTICS Technical Support or an authorised U.S. ROBOTICS Service Centre, please see the U.S. ROBOTICS corporate Web site at: www.usr.com

3.4 CUSTOMER should have the following information / items readily available when contacting U.S. ROBOTICS Technical Support:

- Product Model Number
- Product Serial Number
- Dated Proof of Purchase
- CUSTOMER contact name & telephone number
- CUSTOMER Computer Operating System version
- U.S. ROBOTICS Installation CD-ROM
- U.S. ROBOTICS Installation Guide

4.0 WARRANTY REPLACEMENT:

4.1 In the event U.S. ROBOTICS Technical Support or its authorised U.S. ROBOTICS Service Centre determines the product or part has a malfunction or failure attributable directly to faulty workmanship and/or materials; and the product is within the TWO (2) YEAR warranty term; and the CUSTOMER will include a copy of the dated Proof of Purchase (original purchase receipt from U.S. ROBOTICS or its authorised reseller) with the product or part with the returned product or part, then U.S. ROBOTICS will issue CUSTOMER a Return Material Authorisation (RMA) and instructions for the return of the product to the authorised U.S. ROBOTICS Drop Zone.

4.2 Any product or part returned to U.S. ROBOTICS without an RMA issued by U.S. ROBOTICS or its authorised U.S. ROBOTICS Service Centre will be returned.

4.3 CUSTOMER agrees to pay shipping charges to return the product or part to the authorised U.S. ROBOTICS Return Centre; to insure the product or assume the risk of loss or damage which may occur in transit; and to use a shipping container equivalent to the original packaging.

4.4 Responsibility for loss or damage does not transfer to U.S. ROBOTICS until the returned product or part is received as an authorised return at an authorised U.S. ROBOTICS Return Centre.

4.5 Authorised CUSTOMER returns will be unpacked, visually inspected, and matched to the Product Model Number and Product Serial Number for which the RMA was authorised. The enclosed Proof of Purchase will be inspected for date of purchase and place of purchase. U.S. ROBOTICS may deny warranty service if visual inspection of the returned product or part does not match the CUSTOMER supplied information for which the RMA was issued.

4.6 Once a CUSTOMER return has been unpacked, visually inspected, and tested U.S. ROBOTICS will, at its sole discretion, repair or replace, using new or reconditioned product or parts, to whatever extent it deems necessary to restore the product or part to operating condition.

4.7 U.S. ROBOTICS will make reasonable effort to ship repaired or replaced product or part to CUSTOMER, at U.S. ROBOTICS expense, not later than TWENTY ONE (21) DAYS after U.S. ROBOTICS receives the authorised CUSTOMER return at an authorised U.S. ROBOTICS Return Centre.

4.8 U.S. ROBOTICS shall not be liable for any damages caused by delay in delivering or furnishing repaired or replaced product or part.

5.0 LIMITATIONS:

5.1 THIRD-PARTY SOFTWARE: This U.S. ROBOTICS product may include or be bundled with third-party software, the use of which is governed by separate end-user license agreements provided by third-party software vendors. This U.S. ROBOTICS Limited Warranty does not apply to such third-party software. For the applicable warranty refer to the end-user license agreement governing the use of such software.

5.2 DAMAGE DUE TO MISUSE, NEGLECT, NON-COMPLIANCE, IMPROPER INSTALLATION, AND/OR ENVIRONMENTAL FACTORS: To the extent permitted by applicable law, this U.S. ROBOTICS Limited Warranty does not apply to normal wear and tear; damage or loss of data due to interoperability with current and/or future versions of operating system or other current and/or future software and hardware; alterations (by persons other than U.S. ROBOTICS or authorised U.S. ROBOTICS Service Centres); damage caused by operator error or non-compliance with instructions as set out in the user documentation or other accompanying documentation; damage caused by acts of nature such as lightning, storms, floods, fires, and earthquakes, etc. Products evidencing the product serial number has been tampered with or removed; misuse, neglect, and improper handling; damage caused by undue physical, temperature, or electrical stress; counterfeit products; damage or loss of data caused by a computer virus, worm, Trojan horse, or memory content corruption; failures of the product which result from accident, abuse, misuse (including but not limited to improper installation, connection to incorrect voltages, and power points); failures caused by products not supplied by U.S. ROBOTICS; damage cause by moisture, corrosive environments, high voltage surges, shipping, abnormal working conditions; or the use of the product outside the borders of the country or territory intended for use (As indicated by the Product Model Number and any local telecommunication approval stickers affixed to the product).

5.3 TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. U.S. ROBOTICS NEITHER ASSUMES NOR AUTHORISES ANY OTHER PERSON TO ASSUME FOR IT ANY

OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, WARRANTY, OR USE OF ITS PRODUCTS.

5.4 LIMITATION OF LIABILITY. TO THE FULL EXTENT ALLOWED BY LAW, U.S. ROBOTICS ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF U.S. ROBOTICS OR ITS AUTHORISED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT U.S. ROBOTICS OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

6.0 DISCLAIMER:

Some countries, states, territories or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to CUSTOMER. When the implied warranties are not allowed by law to be excluded in their entirety, they will be limited to the TWO (2) YEAR duration of this written warranty. This warranty gives CUSTOMER specific legal rights, which may vary depending on local law.

7.0 GOVERNING LAW:

This Limited Warranty shall be governed by the laws of the State of Illinois, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

U.S. Robotics Corporation
935 National Parkway
Schaumburg, IL, 60173
U.S.A.

Glossary

0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0-9

802

IEEE 802 (IEEE Std. 802-2001) is a family of standards for peer-to-peer communication over a LAN. These technologies use a shared-medium, with information broadcast for all stations to receive. The basic communications capabilities provided are packet-based. The basic unit of transmission is a sequence of data octets (8-bits), which can be of any length within a range that is dependent on the type of LAN.

Included in the 802 family of IEEE standards are definitions of bridging, management, and security protocols.

802.1x

IEEE 802.1x (IEEE Std. 802.1x-2001) is a standard for passing EAP packets over an 802.11 wireless network using a protocol called *EAP Encapsulation Over LANs* (EAPOL). It establishes a framework that supports multiple authentication methods.

IEEE 802.1x authenticates users not machines.

802.2

IEEE 802.2 (IEEE Std. 802.2.1998) defines the LLC layer for the 802 family of standards.

802.3

IEEE 802.3 (IEEE Std. 802.3-2002) defines the MAC layer for networks that use CSMA/CA. Ethernet is an example of such a network.

802.11

IEEE 802.11 (IEEE Std. 802.11-1999) is a medium access control (MAC) and physical layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area. It uses direct sequence spread spectrum (DSSS) in the 2.4 GHz ISM band and supports raw data rates of 1 and 2 Mbps. It was formally adopted in 1997 but has been mostly superseded by 802.11b.

IEEE 802.11 is also used generically to refer to the family of IEEE standards for wireless local area networks.

802.11a

IEEE 802.11a (IEEE Std. 802.11a-1999) is a PHY standard that specifies operating in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 6 to 54 Mbps.

802.11b

IEEE 802.11b (IEEE Std. 802.11b-1999) is an enhancement of the initial 802.11 PHY to include 5.5 Mbps and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) in the 2.4 GHz ISM band as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps.

802.11d

IEEE 802.11d defines standard rules for the operation of IEEE 802.11 wireless LANs in any country without reconfiguration. PHY requirements such as provides frequency hopping tables, acceptable channels, and power levels for each country are provided. Enabling support for IEEE 802.11d on the access point causes the access point to broadcast which country it is operating in as a part of its beacons. Client stations then use this information. This is particularly important for access point operation in the 5GHz IEEE 802.11a bands because use of these frequencies varies a great deal from one country to another.

802.11e

IEEE 802.11e is a developing IEEE standard for MAC enhancements to support QoS. It provides a mechanism to prioritize traffic within 802.11. It defines allowed changes in the Arbitration Interframe Space, a minimum and maximum Contention Window size, and the maximum length (in kμsec) of a burst of data.

IEEE 802.11e is still a draft IEEE standard (most recent version is D5.0, July 2003). A currently available subset of 802.11e is the *Wireless Multimedia Enhancements* (WMM) standard.

802.11f

IEEE 802.11f (IEEE Std. 802.11f-2003) is a standard that defines the inter access point protocol (IAPP) for access points (wireless hubs) in an extended service set (ESS). The standard defines how access points communicate the associations and reassociations of their mobile stations.

802.11g

IEEE 802.11g (IEEE Std. 802.11g-2003) is a higher speed extension (up to 54 Mbps) to the 802.11b PHY, while operating in the 2.4 GHz band. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps.

802.11i

IEEE 802.11i is a comprehensive IEEE standard for security in a wireless local area network (WLAN) that describes Wi-Fi *Protected Access 2* (WPA2). It defines enhancements to the MAC Layer to counter the some of the weaknesses of WEP. It incorporates stronger encryption techniques than the original Wi-Fi *Protected Access* (WPA), such as Advanced Encryption Standard (AES).

The original WPA, which can be considered a subset of 802.11i, uses *Temporal Key Integrity Protocol* (TKIP) for encryption. WPA2 is backwards-compatible with products that support the original WPA

IEEE 802.11i / WPA2 was finalized and ratified in June of 2004.

802.11k

IEEE 802.11k is a developing IEEE standard for wireless networks (WLANs) that helps auto-manage network Channel selection, client Roaming, and Access Point utilization. 802.11k capable networks will automatically load balance network traffic across APs to improve network performance and prevent under or over-utilization of any one access point. 802.11k will eventually complement the 802.11e quality of service (QoS) standard by ensuring QoS for multimedia over a wireless link.

802.1Q

IEEE 802.1Q is the IEEE standard for *Virtual Local Area Networks* (VLANs) specific to wireless technologies. (See http://www.ieee802.org/1/pages/802.1Q.html.)

The standard addresses the problem of how to break large networks into smaller parts to prevent broadcast and multicast data traffic from consuming more bandwidth than is necessary. 802.11Q also provides for better security between segments of internal networks. The 802.1Q specification provides a standard method for inserting VLAN membership information into Ethernet frames.

A

Access Point

An *access point* acts as a communication hub for the devices on a WLAN, providing a connection or bridge between wireless and wired network devices. It supports a Wireless Networking Framework called Infrastructure Mode.

When one access point is connected to wired network and supports a set of wireless stations, it is referred to as a basic service set (BSS). An extended service set (ESS) is created by combining two or more BSSs.

Ad-hoc Mode

Ad-hoc mode is a Wireless Networking Framework in which stations communicate directly with each other. It is useful for quickly establishing a network in situations where formal infrastructure is not required.

Ad-hoc mode is also referred to as *peer-to-peer mode* or an independent basic service set (IBSS).

AES

The *Advanced Encryption Standard* (AES) is a symmetric 128-bit block data encryption technique developed to replace DES encryption. AES works at multiple network layers simultaneously.

Further information is available on the NIST Web site.

B

Basic Rate Set

The *basic rate set* defines the transmission rates that are mandatory for any station wanting to join this wireless network. All stations must be able to receive data at the rates listed in this set.

Beacon

Beacon frames announce the existence of the wireless local area network and enable stations to establish and maintain communications in an orderly fashion. A beacon frame carries the following information, some of which is optional:

- The *Timestamp* is used by stations to update their local clock, enabling synchronization among all associated stations.
- The *Beacon interval* defines the amount of time between transmitting beacon frames. Before entering power save mode, a station needs the beacon interval to know when to wake up to receive the beacon.
- The *Capability Information* lists requirements of stations that want to join the WLAN. For example, it indicates that all stations must use WEP.
- The *Service Set Identifier* (SSID).
- The Basic Rate Set is a bitmap that lists the rates that the WLAN supports.
- The optional *Parameter Sets* indicates features of the specific signaling methods in use (such as frequency hopping spread spectrum, direct sequence spread spectrum, etc.).
- The optional *Traffic Indication Map* (TIM) identifies stations, using power saving mode, that have data frames queued for them.

Bridge

A connection between two local area networks (LANs) using the same protocol, such as Ethernet or IEEE 802.1x.

Broadcast

A *Broadcast* sends the same message at the same time to everyone. In wireless networks, broadcast usually refers to an interaction in which the access point sends data traffic in the form of IEEE 802.1x Frames to all client stations on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also Unicast and Multicast.

Broadcast Address

See IP Address.

BSS

A *basic service set* (BSS) is an Infrastructure Mode Wireless Networking Framework with a single access point. Also see extended service set (ESS) and independent basic service set (IBSS).

BSSID

In Infrastructure Mode, the *Basic Service Set Identifier* (BSSID) is the 48-bit MAC address of the wireless interface of the Access Point.

C

CCMP

Counter mode/CBC-MAC Protocol (CCMP) is an encryption method for 802.11i that uses AES. It employs a *CCM* mode of operation, combining the Cipher Block Chaining Counter mode (CBC-CTR) and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.

AES-CCMP requires a hardware coprocessor to operate.

CGI

The *Common Gateway Interface* (CGI) is a standard for running external programs from an HTTP server. It specifies how to pass arguments to the executing program as part of the HTTP request. It may also define a set of environment variables.

A CGI program is a common way for an HTTP server to interact dynamically with users. For example, an HTML page containing a form can use a CGI program to process the form data after it is submitted.

Channel

The *Channel* defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each 802.11 standard offers a number of channels, dependent on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC), the European Telecommunications Standards Institute (ETSI), the Korean Communications Commission, or the Telecom Engineering Center (TELEC).

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a low-level network arbitration/ contention protocol. A station listens to the media and attempts to transmit a packet when the channel is quiet. When it detects that the channel is idle, the station transmits the packet. If it detects that the channel is busy, the station waits a random amount of time and then attempts to access the media again.

CSMA/CA is the basis of the IEEE 802.11e Distributed Control Function (DCF). See also RTS and CTS.

The CSMA/CA protocol used by 802.11 networks is a variation on CSMA/CD (used by Ethernet networks). In CSMA/CD the emphasis is on collision *detection* whereas with CSMA/CA the emphasis is on collision *avoidance*.

CTS

A *clear to send* (CTS) message is a signal sent by an IEEE 802.11 client station in response to an *request to send* (RTS) message. The CTS message indicates that the channel is clear for the sender of the RTS message to begin data transfer. The other stations will wait to keep the air waves clear. This message is a part of the IEEE 802.11 CSMA/CA protocol. (See also RTS.)

D

DCF

The *Distribution Control Function* is a component of the IEEE 802.11e Quality of Service (QoS) technology standard. The DCF coordinates channel access among multiple stations on a wireless network by controlling wait times for channel access. Wait times are determined by a random backoff timer which is configurable by defining minimum and maximum contention windows. See also EDCF.

DHCP

The *Dynamic Host Configuration Protocol* (DHCP) is a protocol specifying how a central server can dynamically provide network configuration information to clients. A DHCP server offers a lease (for a pre-configured period of time—see Lease Time) to the client system. The information supplied includes the client's IP addresses and netmask plus the address of its DNS servers and Gateway.

DNS

The *Domain Name Service* (DNS) is a general-purpose query service used for translating *fully-qualified names* into Internet addresses. A fully-qualified name consists of the hostname of a system plus its domain name. For example, `www` is the host name of a Web server and `www.usr.com` is the fully-qualified name of that server. DNS translates the domain name `www.usr.com` to an IP address, for example `66.93.138.219`.

A *domain name* identifies one or more IP addresses. Conversely, an IP address may map to more than one domain name.

A domain name has a suffix that indicates which *top level domain* (TLD) it belongs to. Every country has its own top-level domain, for example `.de` for Germany, `.fr` for France, `.jp` for Japan, `.tw` for Taiwan, `.uk` for the United Kingdom, `.us` for the U.S.A., and so on. There are also `.com` for commercial bodies, `.edu` for educational institutions, `.net` for network operators, and `.org` for other organizations as well as `.gov` for the U. S. government and `.mil` for its armed services.

DOM

The *Document Object Model* (DOM) is an interface that allows programs and scripts to dynamically access and update the content, structure, and style of documents. The DOM allows you to model the objects in an HTML or XML document (text, links, , tables), defining the attributes of each object and how they can be manipulated.

Further details about the DOM can be found at the W3C.

DTIM

The *Delivery Traffic Information Map* (DTIM) message is an element included in some Beacon frames. It indicates which stations, currently sleeping in low-power mode, have data buffered on the Access Point awaiting pick-up. Part of the DTIM message indicates how frequently stations must check for buffered data.

Dynamic IP Address

See IP Address.

E

EAP

The *Extensible Authentication Protocol* (EAP) is an authentication protocol that supports multiple methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication, and smart cards.

Variations on EAP include EAP Cisco Wireless (LEAP), Protected EAP (PEAP), EAP-TLS, and EAP Tunnelled TLS (EAP-TTLS).

EDCF

Enhanced Distribution Control Function is an extension of DCF. EDCF, a component of the IEEE Wireless Multimedia (WMM) standard, provides prioritized access to the wireless medium

ESS

An *extended service set* (ESS) is an Infrastructure Mode Wireless Networking Framework with multiple access points, forming a single subnetwork that can support more clients than a basic service set (BSS). Each access point supports a number of wireless stations, providing broader wireless coverage for a large space, for example, an office.

Ethernet

Ethernet is a local-area network (LAN) architecture supporting data transfer rates of 10 Mbps to 1 Gbps. The Ethernet specification is the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. It uses the CSMA/CA access method to handle simultaneous demands.

Ethernet supports data rates of 10 Mbps, *Fast Ethernet* supports 100 Mbps, and *Gigabit Ethernet* supports 1 Gbps. Its cables are classified as "*X*base*Y*", where *X* is the data rate in Mbps and *Y* is the category of cabling. The original cable was *10base5* (Thicknet or "Yellow Cable"). Some others are *10base2* (Cheapernet), *10baseT* (Twisted Pair), and *100baseT* (Fast Ethernet). The latter two are commonly supplied using *CAT5* cabling with *RJ-45* connectors. There is also *1000baseT* (Gigabit Ethernet).

ERP

The *Extended Rate Protocol* refers to the protocol used by IEEE 802.11g stations (over 20 Mbps transmission rates at 2.4GHz) when paired with Orthogonal Frequency Division Multiplexing (OFDM). Built into ERP and the IEEE 802.11g standard is a scheme for effective interoperability of IEEE 802.11g stations with IEEE 802.11b nodes on the same channel.

Legacy IEEE 802.11b devices cannot detect the ERP-OFDM signals used by IEEE 802.11g stations, and this can result in collisions between data frames from IEEE 802.11b and IEEE 802.11g stations.

If there is a mix of 802.11b and 802.11g nodes on the same channel, the IEEE 802.11g stations detect this via an ERP flag on the access point and enable *request to send* (RTS) and *clear to send* (CTS) protection before sending data.

See also CSMA/CA protocol.

F

Frame

A *Frame* consists of a discrete portion of data along with descriptive meta-information packaged for transmission on a wireless network. Each frame includes a source and destination MAC address, a control field with protocol version, frame type, frame sequence number, frame body (with the actual information to be transmitted) and frame check sequence for error detection. A Frame is similar in concept to a Packet, the difference being that a packet operates on the Network layer (layer 3 in the OSI model) whereas a frame operates on the Data-Link layer (layer 2 in the OSI model).

G

Gateway

A *gateway* is a network node that serves as an entrance to another network. A gateway also often provides a proxy server and a firewall. It is associated with both a router, which use headers and forwarding tables to determine where packets are sent, and a switch or bridge, which provides the actual path for the packet in and out of the gateway.

Before a host on a LAN can access the Internet, it needs to know the address of its *default gateway*.

H

HTML

The *Hypertext Markup Language* (HTML) defines the structure of a document on the World Wide Web. It uses tags and attributes to hint about a layout for the document.

An HTML document starts with an `<html>` tag and ends with a `</html>` tag. A properly formatted document also contains a `<head>...</head>` section, which contains the metadata to define the document, and a `<body>...</body>` section, which contains its content. Its markup is derived from the *Standard Generalized Markup Language* (SGML), which is defined in ISO 8879:1986.

HTML documents are sent from server to browser via HTTP. Also see XML.

HTTP

The *Hypertext Transfer Protocol* (HTTP) defines how messages are formatted and transmitted on the World Wide Web. An HTTP message consists of a URL and a command (`GET`, `HEAD`, `POST`, etc.), a request followed by a response.

I

IAPP

The *Inter Access Point Protocol* (IAPP) is an IEEE standard (802.11f) that defines communication between the access points in a "distribution system." This includes the exchange of information about mobile stations and the maintenance of bridge forwarding tables, plus securing the communications between access points.

IBSS

An *independent basic service set* (IBSS) is an Ad-hoc Mode Wireless Networking Framework in which stations communicate directly with each other.

IEEE

The Institute of Electrical and Electronic Engineers (IEEE) is an international standards body that develops and establishes industry standards for a broad range of technologies, including the 802 family of networking and wireless standards. (See 802, 802.1x, 802.11, 802.11a, 802.11b, 802.11e, 802.11f, 802.11g, and 802.11i.)

For more information about IEEE task groups and standards, see http://standards.ieee.org/.

Infrastructure Mode

Infrastructure Mode is a Wireless Networking Framework in which wireless stations communicate with each other by first going through an Access Point. In this mode, the wireless stations can communicate with each other or can communicate with hosts on a wired network. The access point is connected to a wired network and supports a set of wireless stations.

An infrastructure mode framework can be provided by a single access point (BSS) or a number of access points (ESS).

Intrusion Detection

The *Intrusion Detection System* (IDS) inspects all inbound network activity and reports suspicious patterns that may indicate a network or system attack from someone attempting to break into the system. It reports access attempts using unsupported or known insecure protocols.

IP

The *Internet Protocol* (IP) specifies the format of packets, also called datagrams, and the addressing scheme. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and reassembly. It is combined with higher-level protocols, such as TCP or UDP, to establish the virtual connection between destination and source.

The current version of IP is *IPv4*. A new version, called IPv6 or IPng, is under development. IPv6 is an attempt to solve the shortage of IP addresses.

IP Address

Systems are defined by their *IP address*, a four-byte (octet) number uniquely defining each host on the Internet. It is usually shown in the form `192.168.2.254`. This is called dotted-decimal notation.

An IP address is partitioned into two portions: the network prefix and a host number on that network. A Subnet Mask is used to define the portions. There are two special host numbers:

- The Network Address consists of a host number that is all zeroes (for example, `192.168.2.0`).
- The Broadcast Address consists of a host number that is all ones (for example, `192.168.2.255`).

There are a finite number of IP addresses that can exist. Therefore, a local area network typically uses one of the IANA-designated address ranges for use in private networks. These address ranges are:

10.0.0.0 to 10.255.255.255
172.16.0.0 to 172.31.255.255
192.168.0.0 to 192.168.255.255

A Dynamic IP Address is an IP address that is automatically assigned to a host by a DHCP server or similar mechanism. It is called dynamic because you may be assigned a different IP address each time you establish a connection.

A Static IP Address is an IP address that is hard-wired for a specific host. A static address is usually required for any host that is running a server, for example, a Web server.

IPSec

IP Security (IPSec) is a set of protocols to support the secure exchange of packets at the IP layer. It uses shared public keys. There are two encryption modes: Transport and Tunnel.

- *Transport* mode encrypts only the data portion (payload) of each packet, but leaves the headers untouched.
- The more secure *Tunnel* mode encrypts both the header and the payload.

ISP

An *Internet Service Provider* (ISP) is a company that provides access to the Internet to individuals and companies. It may provide related services such as virtual hosting, network consulting, Web design, etc.

J

Jitter

Jitter is the difference between the latency (or delay) in packet transmission from one node to another across a network. If packets are not transmitted at a consistent rate (including Latency), QoS for some types of data can be affected. For example, inconsistent transmission rates can cause distortion in VoIP and streaming media. QoS is designed to reduce jitter along with other factors that can impact network performance.

L

Latency

Latency, also known as *delay*, is the amount of time it takes to transmit a Packet from sender to receiver. Latency can occur when data is transmitted from the access point to a client and vice versa. It can also occur when data is transmitted from access point to the Internet and vice versa. Latency is caused by *fixed network* factors such as the time it takes to encode and decode a packet, and also by *variable network* factors such as a busy or overloaded network. QoS features are designed to minimize latency for high priority network traffic.

LAN

A *Local Area Network* (LAN) is a communications network covering a limited area, for example, the computers in your home that you want to network together or a couple of floors in a building. A LAN connects multiple computers and other network devices such as storage and printers. Ethernet is the most common technology implementing a LAN.

Wireless Ethernet (802.11) is another very popular LAN technology (also see WLAN).

LDAP

The *Lightweight Directory Access Protocol* (LDAP) is a protocol for accessing on-line directory services. It is used to provide an authentication mechanism. It is based on the X.500 standard, but less complex.

Lease Time

The *Lease Time* specifies the period of time the DHCP Server gives its clients an IP Address and other required information. When the lease expires, the client must request a new lease. If the lease is set to a short span, you can update your network information and propagate the information provided to the clients in a timely manner.

LLC

The *Logical Link Control* (LLC) layer controls frame synchronization, flow control, and error checking. It is a higher level protocol over the PHY layer, working in conjunction with the MAC layer.

M

MAC

The *Media Access Control* (MAC) layer handles moving data packets between NICs across a shared channel. It is a higher level protocol over the PHY layer. It provides an arbitration mechanism in an attempt to prevent signals from colliding.

It uses a hardware address, known as the *MAC address*, that uniquely identifies each node of a network. IEEE 802 network devices share a common 48-bit MAC address format, displayed as a string of twelve (12) hexadecimal digits separated by colons, for example `FE:DC:BA:09:87:65`.

MIB

Management Information Base (MIB) is a database of objects used for network management. SNMP agents along with other SNMP tools can be used to monitor any network device defined in the MIB.

MSCHAP V2

Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) provides authentication for PPP connections between a Windows-based computer and an Access Point or other network access device.

MTU

The *Maximum Transmission Unit* is the largest physical packet size, measured in bytes, that a network can

transmit. Any messages larger than the MTU are fragmented into smaller packets before being sent.

Multicast

A *Multicast* sends the same message to a select group of recipients. Sending an e-mail message to a mailing list is an example of multicasting. In wireless networks, multicast usually refers to an interaction in which the access point sends data traffic in the form of IEEE 802.1x Frames to a specified set of client stations (MAC addresses) on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also Unicast and Broadcast.

N

NAT

Network Address Translation is an Internet standard that masks the internal IP addresses being used in a LAN. A NAT server running on a gateway maintains a translation table that maps all internal IP addresses in outbound requests to its own address and converts all inbound requests to the correct internal host.

NAT serves three main purposes: it provides security by obscurity by hiding internal IP addresses, enables the use of a wide range of internal IP addresses without fear of conflict with the addresses used by other organizations, and it allows the use of a single Internet connection.

Network Address

See IP Address.

NIC

A *Network Interface Card* is an adapter or expansion board inserted into a computer to provide a physical connection to a network. Most NICs are designed for a particular type of network, protocol, and media, for example, Ethernet or wireless.

NTP

The *Network Time Protocol* assures accurate synchronization of the system clocks in a network of computers. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. An NTP client sends periodic time requests to servers, using the returned time stamp to adjust its clock.

O

OSI

The *Open Systems Interconnection* (OSI) reference model is a framework for network design. The OSI model consists of seven layers:

- Layer 1, the Physical layer, identifies the physical medium used for communication between nodes. In the case of wireless networks, the physical medium is air, and radio frequency (RF) waves are a com-

ponents of the physical layer.

- Layer 2, the Data-Link layer, defines how data for transmission will be structured and formatted, along with low-level protocols for communication and addressing. For example, protocols such as CSMA/CA and components like MAC addresses, and Frames are all defined and dealt with as a part of the Data-Link layer.

- Layer 3, the Network layer, defines the how to determine the best path for information traversing the network. Packets and logical IP Addresses operate on the network layer.

- Layer 4, the Transport layer, defines connection oriented protocols such as TCP and UDP.

- Layer 5, the Session layer, defines protocols for initiating, maintaining, and ending communication and transactions across the network. Some common examples of protocols that operate on this layer are network file system (NFS) and structured query language (SQL). Also part of this layer are communication flows like single mode (device sends information bulk), half-duplex mode (devices take turns transmitting information in bulk), and full-duplex mode (interactive, where devices transmit and receive simultaneously).

- Layer 6, the Presentation layer, defines how information is presented to the application. It includes meta-information about how to encrypt/decrypt and compress/decompress the data. JPEG and TIFF file formats are examples of protocols at this layer.

- Layer 7, the Application layer, includes protocols like hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), and file transfer protocol (FTP).

P

Packet

Data and media are transmitted among nodes on a network in the form of *packets*. Data and multimedia content is divided up and packaged into *packets*. A packet includes a small chunk of the content to be sent along with its destination address and sender address. Packets are pushed out onto the network and inspected by each node. The node to which it is addressed is the ultimate recipient.

Packet Loss

Packet Loss describes the percentage of packets transmitted over the network that did not reach their intended destination. A 0 percent package loss indicates no packets were lost in transmission. QoS features are designed to minimize packet loss.

PHY

The Physical Layer (PHY) is the lowest layer in the network layer model (see OSI). The Physical Layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a medium, including defining cables, NICs, and physical aspects.

Ethernet and the 802.11 family are protocols with physical layer components.

PID

The *Process Identifier* (PID) is an integer used by Linux to uniquely identify a process. A PID is returned by

the `fork()` system call. It can be used by `wait()` or `kill()` to perform actions on the given process.

Port Forwarding

Port Forwarding creates a 'tunnel' through a firewall, allowing users on the Internet access to a service running on one of the computers on your LAN, for example, a Web server, an FTP or SSH server, or other services. From the outside user's point of view, it looks like the service is running on the firewall.

PPP

The *Point-to-Point Protocol* is a standard for transmitting network layer datagrams (IP packets) over serial point-to-point links. PPP is designed to operate both over asynchronous connections and bit-oriented synchronous systems.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a specification for connecting the users on a LAN to the Internet through a common broadband medium, such as a single DSL or cable modem line.

PPtP

Point-to-Point Tunneling Protocol (PPtP) is a technology for creating a *Virtual Private Network* (VPN) within the *Point-to-Point Protocol* (PPP). It is used to ensure that data transmitted from one VPN node to another are secure.

Proxy

A *proxy* is server located between a client application and a real server. It intercepts requests, attempting to fulfill them itself. If it cannot, it forwards them to the real server. Proxy servers have two main purposes: improve performance by spreading requests over several machines and filter requests to prevent access to specific servers or services.

PSK

Pre-Shared Key (PSK), see Shared Key.

Public Key

A *public key* is used in public key cryptography to encrypt a message which can only be decrypted with the recipient's private or secret key. Public key encryption is also called asymmetric encryption, because it uses two keys, or Diffie-Hellman encryption. Also see Shared Key.

Q

QoS

Quality of Service (QoS) defines the performance properties of a network service, including guaranteed throughput, transit delay, and priority queues. QoS is designed to minimize Latency, Jitter, Packet Loss, and network congestion, and provide a way of allocating dedicated bandwidth for high priority network traffic.

The IEEE standard for implementing QoS on wireless networks is currently in-work by the 802.11e task

group. A subset of 802.11e features is described in the WMM specification.

R

RADIUS

The *Remote Authentication Dial-In User Service* (RADIUS) provides an authentication and accounting system. It is a popular authentication mechanism for many ISPs.

RC4

A symmetric stream cipher provided by RSA Security. It is a variable key-size stream cipher with byte-oriented operations. It allows keys up to 2048 bits in length.

Roaming

In IEEE 802.11 parlance, *roaming clients* are mobile client stations or devices on a wireless network (WLAN) that require use of more than one a as they move out of and into range of different base station service areas. IEEE 802.11f defines a standard by which APs can communicate information about client associations and disassociations in support of roaming clients.

Router

A *router* is a network device which forwards packets between networks. It is connected to at least two networks, commonly between two local area networks (LANs) or between a LAN and a wide-area network (WAN), for example, the Internet. Routers are located at gateways—places where two or more networks connect.

A router uses the content of headers and its tables to determine the best path for forwarding a packet. It uses protocols such as the Internet Control Message Protocol (ICMP), Routing Information Protocol (RIP), and Internet Router Discovery Protocol (IRDP) to communicate with other routers to configure the best route between any two hosts. The router performs little filtering of data it passes.

RSSI

The *Received Signal Strength Indication* (RSSI) an 802.1x value that calculates voltage relative to the received signal strength. RSSI is one of several ways of measuring and indicating *radio frequency* (RF) signal strength. Signal strength can also be measured in mW (milliwatts), dBms (decibel milliwatts), and a percentage value.

RTP

Real-Time Transport Protocol (RTP) is an Internet protocol for transmitting real-time data like audio and video. It does not guarantee delivery but provides support mechanisms for the sending and receiving applications to enable streaming data. RTP typically runs on top of the UDP protocol, but can support other transport protocols as well.

RTS

A *request to send* (RTS) message is a signal sent by a client station to the access point, asking permission to send a data packet and to prevent other wireless client stations from grabbing the radio waves. This message is a part of the IEEE 802.11 CSMA/CA protocol. (See also RTS Threshold and CTS.)

RTS Threshold

The *RTS threshold* specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the access point, and is especially useful for performance tuning on an access point with a many clients.

S

Shared Key

A *shared key* is used in conventional encryption where one key is used both for encryption and decryption. It is also called *secret-key* or *symmetric-key* encryption.

Also see Public Key.

SNMP

The *Simple Network Management Protocol* (SNMP) was developed to manage and monitor nodes on a network. It is part of the TCP/IP protocol suite.

SNMP consists of managed devices and their agents, and a management system. The agents store data about their devices in *Management Information Bases* (MIBs) and return this data to the SNMP management system when requested.

SSID

The *Service Set Identifier* (SSID) is a thirty-two character alphanumeric key that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. There are no restrictions on the characters that may be used in an SSID.

Static IP Address

See IP Address.

STP

The *Spanning Tree Protocol* (STP) an IEEE 802.1 standard protocol (related to network management) for MAC bridges that manages path redundancy and prevents undesirable loops in the network created by multiple active paths between client stations. Loops occur when there multiple routes between access points. STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN

Subnet Mask

A *Subnet Mask* is a number that defines which part of an IP address is the network address and which part is a host address on the network. It is shown in dotted-decimal notation (for example, a 24-bit mask is shown as `255.255.255.0`) or as a number appended to the IP address (for example, `192.168.2.0/24`).

The subnet mask allows a router to quickly determine if an IP address is local or needs to be forwarded by performing a bitwise AND operation on the mask and the IP address. For example, if an IP address is `192.168.2.128` and the netmask is `255.255.255.0`, the resulting Network address is `192.168.2.0`.

The bitwise AND operator compares two bits and assigns 1 to the result only if both bits are 1. The following table shows the details of the netmask:

IP address	`192.168.2.128`	`11000000 10101000 00000010 10000000`
Netmask	`255.255.255.0`	`11111111 11111111 11111111 00000000`
Resulting network address	`192.168.2.0`	`11000000 10101000 00000010 00000000`

Supported Rate Set

The *supported rate set* defines the transmission rates that are available on this wireless network. A station may be able to receive data at any of the rates listed in this set. All stations must be able to receive data at the rates listed in the Basic Rate Set.

T

TCP

The *Transmission Control Protocol* (TCP) is built on top of Internet Protocol (IP). It adds reliable communication (guarantees delivery of data), flow-control, multiplexing (more than one simultaneous connection), and connection-oriented transmission (requires the receiver of a packet to acknowledge receipt to the sender). It also guarantees that packets will be delivered in the same order in which they were sent.

TCP/IP

The Internet and most local area networks are defined by a group of protocols. The most important of these is the *Transmission Control Protocol over Internet Protocol* (TCP/IP), the de facto standard protocols. TCP/IP was originally developed by Defense Advanced Research Projects Agency (DARPA, also known as ARPA, an agency of the US Department of Defense).

Although TCP and IP are two specific protocols, TCP/IP is often used to refer to the entire protocol suite based upon these, including ICMP, ARP, UDP, and others, as well as applications that run upon these protocols, such as telnet, FTP, etc.

TKIP

The *Temporal Key Integrity Protocol* (TKIP) provides an extended 48-bit initialization vector, per-packet key construction and distribution, a Message Integrity Code (MIC, sometimes called "Michael"), and a rekeying mechanism. It uses a RC4 stream cipher to encrypt the frame body and CRC of each 802.11 frame before transmission. It is an important component of the WPA and 802.11i security mechanisms.

ToS

TCP/IP packet headers include a 3-to-5 bit Type *of Service* (ToS) field set by the application developer that indicates the appropriate type of service for the data in the packet. The way the bits are set determines whether the packet is queued for sending with minimum delay, maximum throughput, low cost, or mid-way "best-effort" settings depending upon the requirements of the data. The ToS field is used by the Professional Access Point to provide configuration control over *Quality of Service* (QoS) queues for data transmitted from the access point to client stations.

U

UDP

The *User Datagram Protocol* (UDP) is a transport layer protocol providing simple but unreliable datagram services. It adds port address information and a checksum to an IP packet.

UDP neither guarantees delivery nor does it require a connection. It is lightweight and efficient. All error processing and retransmission must be performed by the application program.

Unicast

A *Unicast* sends a message to a single, specified receiver. In wireless networks, unicast usually refers to an interaction in which the access point sends data traffic in the form of IEEE 802.1x Frames directly to a single client station MAC address on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also Multicast and Broadcast.

URL

A *Uniform Resource Locator* (URL) is a standard for specifying the location of objects on the Internet, such as a file or a newsgroup. URLs are used extensively in HTML documents to specify the target of a hyperlink which is often another HTML document (possibly stored on another computer). The first part of the URL indicates what protocol to use and the second part specifies the IP address or the domain name where that resource is located.

For example, `ftp://ftp.usr.com/downloads/myfile.tar.gz` specifies a file that should be fetched using the FTP protocol; `http://www.usr.com/index.html` specifies a Web page that should be fetched using the HTTP protocol.

V

VLAN

A *virtual* LAN (VLAN) is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be. The nodes in a VLAN share resources and bandwidth, and are isolated on that network. The Professional Access Point supports the configuration of a wireless VLAN. This technology is used on the access point for the virtual guest network feature.

VPN

A *Virtual Private Network* (VPN) is a network that uses the Internet to connect its nodes. It uses encryption and other mechanisms to ensure that only authorized users can access its nodes and that data cannot be intercepted.

W

WAN

A *Wide Area Network* (WAN) is a communications network that spans a relatively large geographical area, extending over distances greater than one kilometer. A WAN is often connected through public networks, such as the telephone system. It can also be connected through leased lines or satellites.

The Internet is essentially a very large WAN.

WDS

A *Wireless Distribution System* (WDS) allows the creation of a completely wireless infrastructure. Typically, an Access Point is connected to a wired LAN. WDS allows access points to be connected wirelessly. The access points can function as wireless repeaters or bridges.

WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption. It uses a RC4 stream cipher to encrypt the frame body and CRC of each 802.11 frame before transmission.

Wi-Fi

A test and certification of interoperability for WLAN products based on the IEEE 802.11 standard promoted by the Wi-Fi Alliance, a non-profit trade organization.

WINS

The *Windows Internet Naming Service* (WINS) is a server process for resolving Windows-based computer names to IP addresses. It provides information that allows these systems to browse remote networks using the *Network Neighborhood*.

Wireless Networking Framework

There are two ways of organizing a wireless network:

- Stations communicate directly with one another in an Ad-hoc Mode network, also known as an independent basic service set (IBSS).
- Stations communicate through an Access Point in an Infrastructure Mode network. A single access point creates an infrastructure basic service set (BSS) whereas multiple access points are organized in an extended service set (ESS).

WLAN

Wireless Local Area Network (WLAN) is a LAN that uses high-frequency radio waves rather than wires to communicate between its nodes.

WMM

Wireless Multimedia (WMM) is a IEEE technology standard designed to improve the quality of audio, video and multimedia applications on a wireless network. Both access points and wireless clients (laptops, consumer electronics products) can be WMM-enabled. WMM features are based on is a subset of the WLAN IEEE 802.11e draft specification. Wireless products that are built to the standard and pass a set of quality tests can carry the "Wi-Fi certified for WMM" label to ensure interoperability with other such products. For more information, see the WMM page on the Wi-Fi Alliance Web site: http://www.wi-fi.org/OpenSection/wmm.asp.

WPA

Wi-Fi Protected Access (WPA) is a Wi-Fi Alliance version of the draft IEEE 802.11i standard. It provides more sophisticated data encryption than WEP and also provides user authentication. WPA includes TKIP and 802.1x mechanisms.

WPA2

Wi-Fi Protected Access (WPA2) is an enhanced security standard, described in IEEE 802.11i, that uses Advanced Encryption Standard (AES) for data encryption.

The original WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption. WPA2 is backwards-compatible with products that support the original WPA.

WPA2, like the original WPA, supports an *Enterprise* and *Personal* version. The Enterprise version requires use of IEEE 802.1x security features and *Extensible Authentication Protocol* (EAP) authentication with a RADIUS server.

The Personal version does not require IEEE 802.1x or EAP. It uses a *Pre-Shared Key* (PSK) password to generate the keys needed for authentication.

WRAP

Wireless Robust Authentication Protocol (WRAP) is an encryption method for 802.11i that uses AES but another encryption mode (OCB) for encryption and integrity.

X

XML

The *Extensible Markup Language* (XML) is a specification developed by the W3C. XML is a simple, flexible text format derived from *Standard Generalized Markup Language* (SGML), which is defined in ISO 8879:1986, designed especially for electronic publishing.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W