



**Tsunami MP.11 and QuickBridge.11  
Reference Manual  
Version 4.0.0**



# Contents

<b>CONTENTS</b> .....	<b>2</b>
<b>INTRODUCTION</b> .....	<b>5</b>
<b>COMMAND LINE INTERFACE</b> .....	<b>6</b>
Accessing the Command Line Interface.....	6
Ethernet Port.....	6
Serial Port.....	7
HyperTerminal Connection.....	8
Boot Loader CLI.....	9
CLI Terminology.....	10
Navigation and Special Keys.....	10
Commands.....	11
? (Question Mark).....	12
Clear Command.....	12
Done Command.....	12
Downgrade Command.....	12
Download Command.....	13
Exit Command.....	13
Help Command.....	13
History Command.....	13
Log Command.....	14
Passwd Command.....	14
Ping Command.....	14
Quit Command.....	14
Reboot Command.....	14
Save Command.....	15
Search Command.....	15
Set Command.....	15
Show Command.....	15
Templog Command.....	15
Upload Command.....	16
CLI Basic Management Commands.....	17
Show and Set Parameters.....	18
Antenna Alignment Display Parameters.....	18
Broadcast Filtering Parameters.....	18
DDRS WDRP Parameters.....	19
DFS (Dynamic Frequency Selection) Parameters.....	20
DHCP Relay Parameters.....	20
DHCP Server Parameters.....	21
Ethernet Parameters.....	21
Ethernet Filtering Parameters.....	21
Feature Parameter.....	21
HTTP (WEB BROWSER) Parameters.....	22
Internal Unit Temperature Parameters.....	22
Intra-Cell Blocking Parameters.....	22
IP ARP Parameters.....	22
IP ARP Filtering Parameters.....	22
MAC Access Control Table Parameters.....	23
Network Address Translation (NAT) Parameters.....	23
Network Parameters.....	23
QoS (Quality of Service) Parameters.....	24
Radius Parameters.....	28
RIP Global Parameters.....	28
RIP Interface Parameters.....	28
Roaming Parameters.....	29
Security Parameters.....	29

Serial Parameters.....	29
Site Survey Parameters .....	30
SNMP Parameters .....	30
Spanning Tree Parameters .....	30
Static Mac Address Filter Parameters.....	30
Statistic Parameters .....	31
Station Statistic Parameters .....	31
Storm Threshold Parameters .....	31
System Parameters.....	32
Telnet Parameters.....	32
TFTP Parameters.....	32
VLAN Parameters .....	32
Wireless Interface Parameters.....	34
Wireless Interface Security Parameters.....	35
WORP Parameters.....	35
Show and Set Parameter Examples.....	35
Tables .....	36
Table Parameters.....	36
Entering Strings.....	38
Viewing Table Contents .....	39
Creating a Table Row.....	39
Modifying a Table Entry.....	39
Modifying Several Table Entries .....	39
Enabling, Disabling, or Deleting a Table Row.....	39
<b>EVENT LOG ERROR MESSAGES .....</b>	<b>41</b>
Agere Driver.....	41
Bridge.....	41
CLI .....	41
DFS (Dynamic Frequency Selection) .....	41
DHCP Client.....	41
DHCP Relay.....	43
DHCP Server .....	43
Driver .....	43
Event Log.....	43
Flash .....	43
ICB .....	45
LED .....	45
License.....	45
NAT .....	46
Other Tasks .....	46
QoS (Quality of Service) BSU.....	47
QoS (Quality of Service) SU .....	47
Radar Detection.....	47
RADIUS .....	47
Routing.....	47
SNMP.....	48
System .....	48
Templog .....	48
Titan H/W .....	49
TPC.....	49
TFTP .....	49
VLAN.....	52
WORP.....	52
<b>ALARM TRAPS .....</b>	<b>54</b>
Severity Levels.....	54
Trap Groups.....	54
Configuration Related Trap/Notification Group: oriConfigurationTraps .....	54
Flash Memory Related Trap Group: oriFlashTraps .....	55

Image Related Trap Group: oriImageTraps .....	55
Operational Related Trap Group: oriOperationalTraps .....	56
Security Related Trap Group: oriSecurityTraps .....	57
System Feature Based License Related Trap Group: oriSysFeatureTraps .....	58
TFTP Related Trap Group: oriTFTPTraps .....	59
Wireless Interface Card Related Trap Group: oriWirelessIfTraps.....	59
WORP Related Trap Group oriWORPTraps.....	60
<b>MICROSOFT WINDOWS IAS RADIUS SERVER CONFIGURATION .....</b>	<b>61</b>
<b>ADDITION OF UNITS TO A ROUTED NETWORK.....</b>	<b>65</b>
<b>GLOSSARY .....</b>	<b>67</b>

---

## Introduction

This document supplements the *Installation and Management* manual that shipped with your product. This manual contains the following information:

### Command Line Interface

Documents the text-based configuration utility's keyboard commands and parameters.

### Event Log Error Messages

Documents the error messages that you may see in your Event Log.

### Alarm Traps

Documents the alarm traps that can be set.

### Microsoft Windows IAS Radius Server Configuration

Provides information to assist you in setting up the IAS Radius Server.

### Addition of Units to a Routed Network

Describes how to add more units to your routed network.

### Glossary

Describes terms used in the Tsunami MP.11/QB.11 documentation and in the wireless industry.

---

**IMPORTANT:** Some features/commands described in this document may not be available for your product.

---

The *Installation and Management* manual provides the following information:

- An overview of wireless network topologies and combinations that can be built with the unit.
- Detailed installation instructions.
- Information on accessing the unit for configuration and maintenance.
- The most common settings used to manage the unit.
- A description of the Web Interface in a hierarchical manner, so you can easily find details about each item.
- A set of procedures, including TFTP Server Setup, Configuration Backup, Restore, and Download, Forced Reload, and Reset to Factory Defaults.
- Assistance for isolating and solving problems with your Tsunami MP.11/QB.11 product.
- Supplementary information including country code tables, frequency channels tables, technical specifications, and technical support information.

## Command Line Interface

The Command Line Interface (CLI) is a text-based configuration utility that supports a set of keyboard commands and parameters to configure and manage an MP.11/QB.11 unit. Users enter command statements, composed of CLI commands and their associated parameters. You can issue statements from the keyboard for realtime control or from scripts that automate configuration. For example, when downloading a file, administrators enter the **download** CLI command along with IP address, file name, and file type parameters. For example:

```
download 169.254.128.133 image.bin image
```

You can use the CLI as an alternative to the Web interface. You can, for example, quickly change multiple settings by running commands in a batch.

Administrators use the CLI to control radio operation and monitor network statistics. The MP.11/QB.11 products support two types of CLI—the Boot Loader CLI and the normal CLI. The Boot Loader CLI provides a limited command set and is used when the current Image is bad or missing.

## ACCESSING THE COMMAND LINE INTERFACE

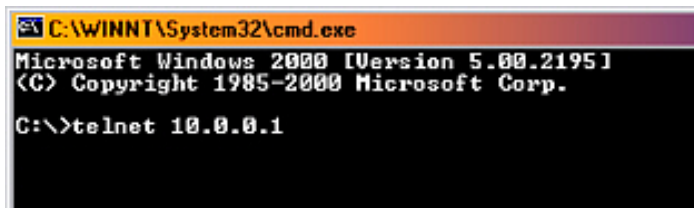
You access the CLI over a HyperTerminal serial connection or through Telnet. During initial configuration, you can use the CLI over a serial port connection to configure the unit's IP address. When accessing the CLI through Telnet, you can communicate with the unit from over your switch or hub, from over the Internet, or with a crossover Ethernet cable connected directly to your computer's Ethernet port.

### Ethernet Port

To use the CLI through the Ethernet port, you must have a telnet program, the CLI password, and the IP address of the unit. On most computers, the telnet program is called **telnet**. (See "Setting the IP Address" in the *Installation and Management manual* for details.)

To access the unit through Ethernet on a Windows PC:

1. Open a DOS command window from the Windows **Start** menu, select **Run**; enter **cmd** and click **OK**.
2. Enter **telnet** followed by the IP address, as shown in the following sample **DOS** command window.



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\>telnet 10.0.0.1
```

3. You are prompted for your password:  
**Please enter password:**
4. Enter the password (the default password is **public**).

You can now use the CLI.

## Serial Port

You can also use the CLI through the serial connection of the unit with a terminal emulation program such as HyperTerminal. You can use this method for cases in which other access methods cannot be used, or when the IP address of the unit cannot be set or retrieved.

To use the CLI through the serial connection of the unit, the following items are required:

- The CLI password of the unit
- An RJ11-to-DB9 connector (included in shipment of BSU)
- An ASCII terminal emulation program, such as HyperTerminal

Proxim recommends you switch off the unit and the computer before connecting or disconnecting the serial cable.

---

**Note:** You can connect to the serial port by connecting the included RJ11 to DB9 connector from the radio (RJ11 connection) to your computer's serial port (DB9 connection).

---

To access the unit through the serial port:

1. Start your terminal emulation program.
2. Set the following connection properties; then connect:

COM port	(For example, COM1 or COM2, to which the unit's serial port is connected.)
Bits per second	9600
Data bits	8
Stop bits	1
Flow control	none
Parity	none
Line ends	carriage return with line feed
3. Disconnect and then reconnect power to reset the unit. The terminal emulation program displays Power On Self Test (POST) messages. After approximately one minute (four minutes if Dynamic Frequency Selection (DFS) is enabled) it displays: **Please enter password:**

---

**Note:** In situations in which the unit is below freezing, it self-heats before turning on. This can take up to 30 minutes.

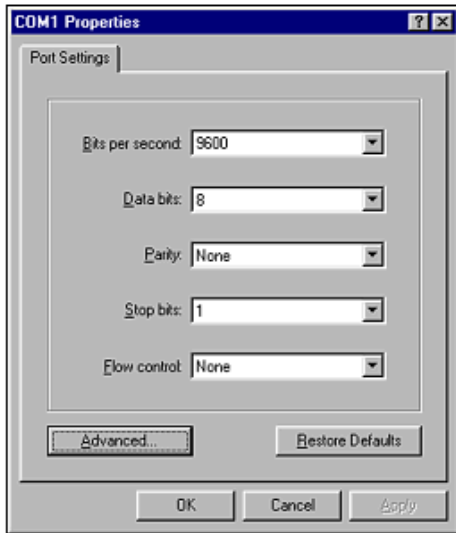
---

4. Enter the password. The default password is `public`. You can now use the CLI.

## HyperTerminal Connection

The serial connection properties can be found in HyperTerminal as follows:

1. Start HyperTerminal and select **Properties** from the **File** menu.
2. In the **Connect using:** drop-down list, select **Direct to Com1** (depending upon the COM port you use) and click **Configure...**; a window such as the following is displayed.

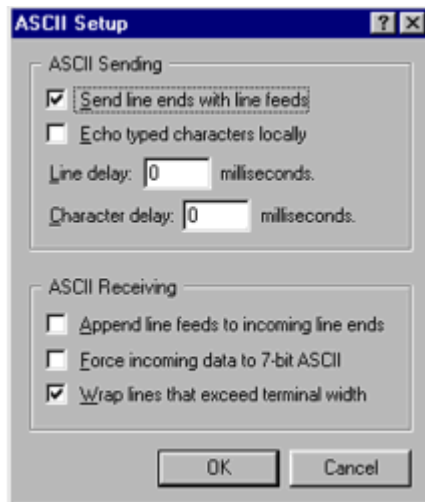



---

**Note:** If this selection is grayed out, the Hyperterminal connection must first be disconnected, then the **Properties** menu re-opened.

---

3. If the COM1 window displayed shows settings other than those above, change as necessary and click **OK**.
4. From the Hyperterminal **Properties** window, click the **Settings** tab; then click **ASCII Setup...**; a window such as the following is displayed:



5. Ensure that **Send line ends with line feeds** is selected and click **OK**.
6. Click **OK** again to exit the **Properties** window.

HyperTerminal is now correctly configured.

## BOOT LOADER CLI

The Boot Loader CLI is a minimal subset of the normal CLI used to perform initial configuration of the unit. The Boot Loader is started when the unit is switched on or reset, and is responsible for starting the embedded software. The Boot Loader CLI is available when the unit's embedded software is not running.

This interface is accessible only through the serial interface if the unit does not contain a software image or a download image command over TFTP has failed.

The Boot Loader CLI lets you configure the initial setup parameters as well as download a software image to the device.

The following commands are supported by the Boot Loader CLI:

- **Set** for configuration of initial device parameters
- **Show** to view the device's configuration parameters
- **Help** to provide additional information about all commands supported by the Boot Loader CLI
- **Reboot** to reboot the device

The parameters supported by the Boot Loader CLI for viewing and modifying are:

- System name
- IP address assignment type
- IP address
- IP mask
- Gateway IP address
- TFTP Server IP address
- Image Filename (including the file extension)

## CLI TERMINOLOGY

### Configuration Files

Database files containing the current configuration information. Configuration items include the IP address and other network-specific values. Configuration files can be downloaded to the unit or uploaded for backup or troubleshooting.

### Download versus Upload

Downloads transfer files to the unit; uploads transfer files from the unit. The TFTP server performs file transfers in both directions.

### Group

A logical collection of network parameter information. For example, the System Group is comprised of several related parameters. Groups also can contain tables. All items for a given group can be displayed with a `show <Group>` CLI command.

### Image File

The unit's software executed from RAM. To update a unit, you typically download a new image file.

### Parameter

A fundamental network value that can be displayed and may be changeable. For example, the unit must have a unique IP address and the wireless interface must be assigned an SSID. Change parameters with the CLI set command and view them with the CLI show command.

### Table

Tables hold parameters for several related items. For example, you can add several potential managers to the SNMP table. All items for a given table can be displayed with a `show <table>` CLI command.

### TFTP

Refers to the TFTP Server, used for file transfers.

## NAVIGATION AND SPECIAL KEYS

The CLI supports these navigation and special key functions to move the cursor along the prompt line:

Key Combination	Description
Delete or Backspace	Delete previous character
Ctrl-A	Move cursor to beginning of line
Ctrl-E	Move cursor to end of line
Ctrl-F	Move cursor forward one character
Ctrl-B	Move cursor back one character
Ctrl-D	Delete the character the cursor is on
Ctrl-U	Delete all text to the left of the cursor
Ctrl-P	Go to the previous line in the history buffer
Ctrl-N	Go to the next line in the history buffer
Tab	Complete the command line
?	List available commands

## COMMANDS

The commands listed in the following table are described in more detail in the following subsections.

Command	Action
?	Lists commands
done	Disconnects and closes the current CLI session
downgrade	Downgrade to a previous software version
download	Transfer files from the TFTP server to the unit
exit	Disconnects and closes the current CLI session
help	View command specifics or control-key sequences you can use to navigate
history	Lists commands previously entered
log	Manage the event log file maintained by the unit
passwd	Change the password used to access the CLI
quit	Disconnects and closes the current CLI session
reboot	Signal the unit to reboot after a specified number of seconds
save	Save the current configuration to flash memory
search	Display the parameter entries in a specified table
set	Change parameter values
show	View parameter and statistical values
templog	View the temperature log
upload	Transfer files from the unit to the TFTP server

Also see “Show and Set Parameters” on page 18 and “Table Parameters” on page 36.

## ? (Question Mark)

You can show CLI help by entering **help** at the command prompt. The CLI also provides context-specific help. For help in a specific situation, enter **?**.

You can get help as follows:

display the command list	?
display commands that start with specified letters	s?  The more letters you enter, the fewer the results returned. Enter one or more letters, then ? with no space between letters and ?
display parameters for set and show commands	download ?  Lets you see every possible parameter for the <b>set</b> or <b>show</b> commands Enter the command, a space, then ?
display prompts for successive parameters	download ? download 169.254.128.133 ? download 169.254.128.133 image.bin ? download 169.254.128.133 image.bin image  Enter the command, a space, and then ?. Then, when the parameter prompt appears, enter the parameter value. The parameter is changed and a new CLI line is echoed with the new value.  After entering one parameter you can add another ? to the new CLI line to see the next parameter prompt, and so on until you have entered all the required parameters.

Note that the Boot Loader CLI does not have command help.

## Clear Command

The **clear** command is used to clear clear interface statistics. You must specify which interface you wish to clear.

```
clear <arptble/learntbl/ethernet/wireless/worp>
```

## Done Command

The **quit**, **done**, and **exit** commands are used to disconnect and close the current CLI session.

## Downgrade Command

The **downgrade** command lets you downgrade to a previous release.

Once you enter this command, the device is downgraded to the specified release and is automatically rebooted.

```
downgrade <TFTPIPAddress> <TFTP filename> <filetype (image)> <Release Number>
```

The **filetype** must be **image**.

## Download Command

The `download` command is used to transfer files from the TFTP server to the unit. Executing download in combination with the asterisk character (\*) makes use of the previously set TFTP parameters. Executing download without parameters displays command help and usage information.

To transfer a file from the TFTP server to the unit:

```
download <tftpserveraddress> <path and filename> <filetype>
```

where <filetype> can be one of these four values:

```
config - Configuration file, the unit's current settings
image - Image file, the unit's embedded software
bootloader - Boot software
license - License file
```

To issue repeated operations, use the asterisk (\*) character in place of the options: `download *`

Previously used optional values for the `download` command is stored in TFTP parameters that you can view and change. See the TFTP parameter table for details.

## Exit Command

The `quit`, `done`, and `exit` commands are used to disconnect and close the current CLI session.

## Help Command

Use the `help` command to view the specifics of certain commands or to view control-key sequences you can use to navigate the command line.

To display how to navigate the command line using special keys:

```
help
```

## History Command

Use the `history` command to show this list of commands. Commands entered in the current session are stored in a Command History Buffer. To avoid re-entering long command statements, use the keyboard up arrow (↑) and down arrow (↓) keys to recall previous statements from the Command History Buffer. When the desired statement reappears, press the **Enter** key to execute, or you can edit the statement before executing it.

```
history
```

## Log Command

Use the `log` command to manage the event log file maintained by the unit.

To append a user-specified string to the event log, enter:

```
log addstring <anyString>
```

To append a user-specified string multiple times to the event log, enter:

```
log addmany <numMsgs> <anyString>
```

To reset the event log, enter the following. Note that this generates an event log message stating that the log has been reset intentionally.

```
log reset
```

To display the contents of the entire event log, enter:

```
log dump
```

To display the current number of log entries:

```
log count
```

To display the log entry corresponding to the specified number, enter:

```
log display <msgNum>
```

The first log entry is numbered 0. If no parameter is supplied, the entire event log is displayed.

## Passwd Command

Use the `passwd` command to change the password used to access the CLI.

```
passwd <old password> <new password> <new password>
```

Enter the new password twice to ensure no mistake was made when specifying the new password. If you forget the CLI password, there is no way to retrieve it from the unit and the CLI cannot be accessed. In this case, the unit must be reset to factory defaults. The default password for the CLI is **public**.

## Ping Command

Use the `ping` command to test the accessibility of a network device.

```
ping <Host IP address> <number of times>
```

## Quit Command

The `quit`, `done`, and `exit` commands are used to disconnect and close the current CLI session.

## Reboot Command

Use the `reboot` command to signal the unit to reboot after a specified number of seconds.

```
reboot <number of seconds>
```

The `<number of seconds>` parameter must be positive. Specify a value of 0 (zero) for an immediate reboot.

## Save Command

Use the **save** command to save the current configuration of the unit to flash memory.

```
save config
```

## Search Command

Use the **search** command to list the parameters supported by the specified table. This list corresponds to the table information displayed in the HTTP interface.

```
search <table name>
```

See “Table Parameters” on page 36 for details.

## Set Command

The **set** command lets you change parameter values. You can set a single parameter value, or you can set a group of parameters or a table with parameters. If a parameter requires more than one value, the values must be separated by spaces.

For example, to set the unit IP address parameter:

```
set ipaddrtype static
set ipaddr 1 ipaddress 10.0.0.12
```

Some parameter values change only when the unit is rebooted. In these cases, the CLI warns you that a reboot is required for the change to take effect.

See “Show and Set Parameters” on page 18 for a list of parameters that can be used with the **set** command.

## Show Command

The **show** command lets you view parameter and statistical values. You can view a single parameter, a group of parameters, or a table with parameters. (A table consists of rows with similar parameters.)

To see a definition and syntax example, enter only **show**. To see a list of available parameters, enter a question mark after show (example **show ?**).

To view the current values of all system parameters: **show system**

See “Show and Set Parameters” on page 18 for a list of parameters that can be used with the **show** command.

## Templog Command

The **templog** command is used to display the temperature log for the radio. The temperature log is a file in flash memory that holds the temperature data.

<b>templog dump</b>	Displays the temperature log
<b>templog reset</b>	Resets the temperature log
<b>upload &lt;target ip&gt; &lt;filename&gt; templog</b>	Export the log to a text file for further analysis

- Maximum number of entries in the log is 576 (2 days with the refresh time of 5 minutes).
- The log is exportable to a text file for further analysis.
- The range of the internal unit temperature (IUT) is from 0° C to 55° C

- The range of the recording interval of IUT is from 1 to 60 minutes, configurable in 5-minute increments (1, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60)

---

**Note:** If a **walk** operation is performed on the MIB variable **oriTempLogTableEntry** using SNMP V2 default settings, log entries are repeated about 10 times (as the maximum repetitions in SNMP V2 is 10). Set the maximum repetitions value to **1** or uncheck the **Use Get Bulk** option for all entries to be displayed without any repetitions in the MIB browser.

---

## Upload Command

The **upload** command is used to transfer files from the unit to the TFTP server.

To upload a file from the unit to the TFTP server:

```
upload <tftpserveraddress> <path and filename> <filetype>
```

where <filetype> can be one of these four values:

```
config - Configuration file, the unit's current settings
templog - Temperature log
eventlog - Event log
```

To issue repeated operations, use the asterisk (\*) character in place of the options:

```
upload *
```

Previously used optional values for the **upload** command is stored in TFTP parameters that you can view and change. See the TFTP parameter table for details.

## CLI BASIC MANAGEMENT COMMANDS

Proxim recommends setting up the following basic configuration parameters immediately when you receive the unit.

Task	Commands
Set System Name, Location, and Contact information	<pre>show system set sysname &lt;name&gt; set sysloc &lt;location&gt; set sysctname &lt;contact name&gt; set sysctemail &lt;contact email&gt; set sysctphone &lt;contact phone&gt; set syscountrycode &lt;country code&gt;</pre>
Shows the type of hardware being used	<pre>show syshwtype hardwaretype</pre>
Set IP address for the unit	<pre>set ipaddrtype &lt;static   dynamic&gt; set ipaddr 1 ipaddress &lt;ip address&gt; set ipaddr 1 ipsubmask &lt;subnet mask&gt; For example: set ipaddr 1 ipaddress &lt;ip address&gt; ipsubmask &lt;subnet mask&gt;</pre>
Set default gateway	<pre>set ipgw &lt;gateway address&gt;</pre>
Configure Wireless Interface	<pre>set wif 3 channel 10 set wif 3 netname &lt;network name&gt;</pre> <p>For more Wireless Interface parameters, see "Wireless Interface Parameters" on page 34</p>
Configure Ethernet Interface	<pre>show ethernet set Ethernet 1 etherspeed &lt;autospeedauto   autospeedhalf   100auto   100full   100 half   10full   10half&gt;</pre>
Set Encryption for the Wireless interface	<pre>show wifsec set wifsec 3 encryptoption &lt;wep aes none&gt; set wifsec 3 encryptkey1 &lt;key 1&gt; set wifsec 3 encryptallowdeny &lt;enable   disable&gt;</pre>
Set Telnet Password	<pre>show telnet set telifbitmask &lt;0-15&gt; set tellogintout &lt;login timeout&gt; set telport &lt;port number&gt; set telsessiontout &lt;inactivity timeout&gt;</pre>
Set Web Interface Password	<pre>show http set httpifbitmask &lt;0-15&gt; set httppasswd &lt;password&gt; set httpport &lt;port number&gt;</pre>
Set SNMP Password	<pre>show snmp (displays the read password, read/write password, IP Access Table entries, and SNMP Interface Bitmask) set snmprpasswd &lt;read password&gt; set snmprpasswd &lt;read/write password&gt; set snmpifbitmask &lt;0-15&gt;</pre>
Download a configuration file from your TFTP server	<pre>Download &lt;ipaddr&gt; &lt;tftpfilename&gt; &lt;tftpfiletype&gt; show tftp (to ensure the entries are correct) download * reboot 0</pre>
Backup your configuration file	<pre>upload &lt;ipaddr&gt; &lt;tftpfilename&gt; &lt;tftpfilename&gt; show tftp (to ensure the entries are correct) upload *</pre>
Reboot	<pre>reboot [&lt;number of seconds&gt;]</pre>
Reset to Factory Defaults	<pre>set sysresettodefaults 1</pre>

## SHOW AND SET PARAMETERS

The following table details the non-table parameters available to be viewed and set within the unit CLI.

R = Read-only      W = Write-only      RW = Read-Write

### Antenna Alignment Display Parameters

Antenna Alignment Display (AAD) provides a measurement of signal quality in an easy-to-interpret manner (a numeric printed signal value at the CLI and serial ports). The SNR is displayed numerically on the CLI or serial port by two decimal characters representing a number from 00 to 99. On the serial port, AAD is enabled by default after booting.

To start the display, you must enable AAD and a wireless link must be established between the Base Station and SU.

aad	RW	<p><b>set aad enable local</b></p> <p>Enables display of the local SNR. Local SNR is the SNR measured by the receiver at the near end.</p> <p><b>set aad enable remote</b></p> <p>Enables display of the remote SNR. Remote SNR is the SNR as measured by the receiver at the far end.</p> <p><b>set aad enable average</b></p> <p>Enables display of the average SNR. The average SNR is the average of the local and remote SNR.</p> <p><b>set aad disable</b></p> <p>Disables Antenna Alignment Display. Also, ctrl-c disables AAD.</p> <p>AAD is automatically disabled 30 minutes after it is enabled to remove the load of extra messages on the wireless interface. The default telnet timeout is 900 seconds (15 minutes). In this case, AAD auto stops in 15 minutes. If AAD is required to run for the full 30 minutes, change the default telnet timeout to a value greater than 30 minutes (greater than 1800 seconds). This restriction is for telnet connections only and not for the serial interface. The serial interface never times out.</p>
-----	----	---

### Broadcast Filtering Parameters

broadcastflttbl	RW	Broadcast Filter Table
index	R	Index
protoname	R	Protocol name
direction	RW	Filtering Direction [1=ethernet to wireless, 2=wireless to ethernet, 3=both]
status	RW	Status of table entry [1=enable, 2=disable]

## DDRS WORP Parameters

ddrs	R	WORP DDRS Group
ddrsstatus	RW	Status of WORP DDRS [1=enable, 2=disable]. This variable is only used on the Base Station; the SU ignores this variable. Default value is disabled.
ddrsdefdatarate	RW	The data rate at which the BSU starts communication with all SUs to begin the registration process. This value can be configured only on the Base Station and not the SU. Possible values are (normal mode): 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps.
ddrsmaxdatarate	RW	The maximum data rate that can be dynamically set by DDRS. Possible values are (normal mode): 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps.
ddrsrateupavgsnrthr	RW	The average SNR threshold in the calculation for data rate increase. Default value is 4 dB.
ddrsrateupreqsnrthr	RW	The required SNR threshold in the calculation for data rate increase. Default value is 6 dB.
ddrsratedownreqsnrthr	RW	The required SNR threshold in the calculation for data rate reduction. Default value is 3 dB.
ddrsminreqsnr11an	RW	Minimum SNR required in normal mode 6 Mbps - 6 dB, 9 Mbps - 7 dB, 12 Mbps - 9 dB 18 Mbps - 11 dB, 24 Mbps - 14 dB, 36 Mbps - 18 dB
ddrsminreqsnr11an6mbps	RW	Minimum required SNR for data rate of 6 Mbps, normal mode. Configurable limits: 1-50.
ddrsminreqsnr11an9mbps	RW	Minimum required SNR for data rate of 9 Mbps, normal mode. Configurable limits: 1-50.
ddrsminreqsnr11an12mbps	RW	Minimum required SNR for data rate of 12 Mbps, normal mode. Configurable limits: 1-50.
ddrsminreqsnr11an18mbps	RW	Minimum required SNR for data rate of 18 Mbps, normal mode. Configurable limits: 1-50.
ddrsminreqsnr11an24mbps	RW	Minimum required SNR for data rate of 24 Mbps, normal mode. Configurable limits: 1-50.
ddrsminreqsnr11an36mbps	RW	Minimum required SNR for data rate of 36 Mbps, normal mode. Configurable limits: 1-50.
ddrsminreqsnr11an48mbps	RW	Minimum required SNR for data rate of 48 Mbps, normal mode. Configurable limits: 1-50.
ddrsminreqsnr11an54mbps	RW	Minimum required SNR for data rate of 54 Mbps, normal mode. Configurable limits: 1-50.
ddrsrateincpercentthr	RW	If the number of retransmissions out of the last 128 transmissions is bigger than this percentage, DDRS will increase the TX data rate.
ddrsratedecpercentthr	RW	If the number of retransmissions out of the last 128 transmissions is less than this percentage, DDRS will decrease the TX data rate.

## DFS (Dynamic Frequency Selection) Parameters

dfsblstchn	RW	Set channel status in DFS blacklist channel table, or display DFS blacklisted channels. <b>set dfsblstchn 3.&lt;channel&gt; blackliststatus &lt;value&gt;</b> <b>show dfsblstchn</b> where value can be: enable; disable. Ex: set dfsblstchn 3.100 blackliststatus enable
dfsprioritychannel	RW	Set DFS priority channel, or display DFS priority channel. <b>set dfsprioritychannel &lt;channel_number&gt;</b> <b>show dfsprioritychannel.</b>

## DHCP Relay Parameters

dhcprelay	R	DHCP Relay Group
dhcprelaystatus	RW	DHCP Relay Status [1=enable, 2=disable]
dhcprelayipaddr	RW	DHCP Server IP address
dhcprelaycmt	RW	Comment

## DHCP Server Parameters

dhcp	R	DHCP Server Group
dhcpstatus	RW	DHCP Server Status. [1=enable, 2=disable].
dhcpgw	RW	DHCP Server Gateway IP address.
dhcpsubnetmask	R	DHCP Server Gateway Subnet Mask.
dhcppridnsipaddr	RW	DHCP Server Primary DNS IP address.
dhcpsecdnsipaddr	RW	DHCP Server Secondary DNS IP address.
dhcpiptooltbl	RW	DHCP Server IP Pool Table
index	R	Index
startipaddr	RW	Start IP address in the form xxx.xxx.xxx.xxx.
endipaddr	RW	End IP address in the form xxx.xxx.xxx.xxx.
defleasetm	RW	Default lease time. 3600-86400.
maxleasetm	RW	Maximum lease time. 3600-86400.
comment	RW	Comment. 1-255 characters.
status	RW	Status of table entry. [1=enable, 2=disable, 3 = delete, 4 = create]

## Ethernet Parameters

ethernet	RW	Ethernet Configuration Table
index	R	Index
etherspeed	RW	Speed [1=10M Half Duplex 2=10M Full Duplex 3=10M Auto Duplex 4=100M Half Duplex, 5=100M Full Duplex 6=Auto Speed Half Duplex 7=Auto Speed Auto Duplex]

## Ethernet Filtering Parameters

etherflt	R	Ethernet Filtering Group
etherflttbl	RW	Ethernet Filter Table
index	R	Index
proto	RW	Ethernet Filtering Protocol
cmt	RW	Comment {1-255 characters}
status	RW	Status of table entry {1=enable, 2=disable}
etherfltoptype	RW	Operation type [1=allow, 2=deny]
etherfltifbitmask	RW	Interface bitmask

## Feature Parameter

featuretbl	R	Table of supported features on current image file
------------	---	---

## HTTP (WEB BROWSER) Parameters

http	R	HTTP Group
httpport	RW	HTTP port
httppasswd	W	HTTP password
httpifbitmask	RW	HTTP interface bitmask
httphelplink	RW	Help link

## Internal Unit Temperature Parameters

internalunittemp	R	Internal unit temperature
iutlogginginterval	RW	IUT logging interval

## Intra-Cell Blocking Parameters

**Note:** *Intra-cell blocking is configured on the BSU only..*

### Limitations:

- Telnet Server supports only 32 arguments; therefore, any command comprising greater than 32 arguments results in an error.
- When **sh intra** is used to show commands relating to Intra-cell blocking, some of the commands displayed are too long to be shown with clear boundaries when all the commands are shown on the CLI.

intracellblockingstatus	RW	Enable or disable Intra-Cell blocking.
intracellgrptbl	RW	Intra-Cell Group Table. Defines the filter groups.
index	R	Index
grpname	RW	Name of the Intra-Cell group, 1-255 characters.
grpstatus	RW	Status of table entry [1=enable, 2=disable, 3=delete].
intracellmactbl	RW	Intra-Cell MAC Address Table. Enables or disables a MAC address and assigns it to a specific filter group.
index	R	Index
mac	RW	MAC Address of the SU.
grpidl (to grpid16)	RW	Status of group entry [1=active, 2=inactive, 3=delete].
macstatus	RW	Status of table entry [1=enable, 2=disable, 3=delete] Default is enable.
intracellsecuritygwstatus	RW	Enable or disable packet forwarding to an external Security Gateway.
intracellsecuritygwmac	RW	MAC address of the Security Gateway.

## IP ARP Parameters

parp	R	Proxy ARP Group
parpstatus	RW	Proxy ARP status [1=enable, 2=disable]

## IP ARP Filtering Parameters

IPARP	R	IP ARP Group
iparpfltaddr	RW	IP address
iparpfltstatus	RW	Status [1=enable, 2=disable]
iparpfltsubmask	RW	Subnet mask

## MAC Access Control Table Parameters

macacl	R	MAC Access Control Group
macacлтаbl	RW	MAC Access Control Table
index	R	Index
macaddr	RW	MAC address
cmt	RW	Comment of 1-255 characters.
status	RW	Status of table entry [1=enable, 2=disable, 3=delete]
macaclstatus	RW	Status [1=enable, 2=disable]
macacloptype	RW	Operation type [1=allow, 2=deny]

## Network Address Translation (NAT) Parameters

**Note:** NAT parameters are configured on the SU in routing mode only.

nat	R	NAT Group
natstatus	RW	Status of NAT [1=enable, 2=disable]. Default is disable.
natstaticbindstatus	RW	Status of NAT Static [1=enable, 2=disable]. Default is disable.
natstaticporttbl	RW	NAT Static Port Bind Table
index	R	Index
localipaddr	RW	Local IP address in the form xxx.xxx.xxx.xxx.
porttype	RW	Port type. [1=TCP, 2=UDP, 3 = both]
startport	RW	Local port number. 1-65535.
endport	RW	Public port number. 1-65535.
status	RW	Status of table entry [1=enable, 2=disable, 3 = delete, 4 = create]

## Network Parameters

network	R	Network Group
ip	R	IP Group (same as Network Group)
ipaddr	RW	IP Address Table
index	R	Index [1=Ethernet, 2=loopback, 3=wireless]
ipaddress	RW	IP address
ipsubmask	RW	Subnet mask
ipaddrtype	RW	Address type [1=static, 2=dynamic]
ipgw	RW	Default Router IP address
ipttl	RW	Default time-to-live
iproutes	RW	IP Route Table (Routing mode only).
ipaddr	R	IP address
metric	RW	Routing metric
routetype	RW	Route Type
ipsubmask	RW	Subnet Mask
ipgw	RW	Gateway IP address
<p>Example: This command changes the first entry in the IP Address table:  set ipaddr 1 ipaddress 150.80.0.1 ipsubmask 255.255.255.0</p>		

## QoS (Quality of Service) Parameters

**Note:** QoS parameters are configured on the BSU only.

qossutbl	R	To display all SUs. <b>show qossutbl</b> Note: there is no command to show individual table entries. The "Invalid index" error message will be printed if a "show qossutbl <index>" command is used.
qossutbl	W	To add a new SU. <b>set qossutbl 0 sumacaddr &lt;SU MAC address&gt; qosclsindex &lt;index&gt;</b> Note: both the MAC address and the QoS class index must be entered. The order does not matter.
qossutbl	W	To delete an SU. <b>set qossutbl &lt;index&gt; suqosstatus delete</b>
qossutbl	W	To update the SU table entry. <b>set qossutbl &lt;index&gt; param1 &lt;value&gt; ----- param2 &lt;value&gt;</b> where: param =           sumacaddr qosclsindex suqosstatus
qosclstbl	R	To display all QoS classes. <b>show qosclstbl</b> Note: there is no command to show individual table entries. The "Invalid index" error message will be printed if a "show qosclstbl <index>" command is used.
qosclstbl	W	To add a new QoS class. <b>set qosclstbl 0 classname &lt;class name&gt; sfvalue &lt;SFC index&gt; pirvalue &lt;PIR index&gt;</b> Ex: set qosclstbl 0 classname test sfvalue 1 pirvalue 3 Note: SFC 1 and PIR 3 must have been defined beforehand.
qosclstbl	W	To add SFC "X" identified by PIR "Y" to QoS class "Z". <b>set qosclstbl Z.0 sfvalue X pirvalue Y</b> Ex: set qosclstbl 5.0 sfvalue 1 pirvalue 3 Note: SFC 1 and PIR 3 must have been defined beforehand.
qosclstbl	W	To add PIR "Y" to identify SFC "X" of class "Z". <b>set qosclstbl Z.X.0 pirvalue Y</b> Ex: set qosclstbl 5.1.0 pirvalue 3 Note: PIR 3 must have been defined beforehand.
qosclstbl	W	To disable QoS class "Z". <b>set qosclstbl Z.0 qosclsstatus disable</b> Ex: set qosclstbl 5.0 qosclsstatus disable
qosclstbl	W	To delete QoS class "Z". <b>set qosclstbl Z.0 qosclsstatus delete</b> Ex: set qosclstbl 5.0 qosclsstatus delete
qosclstbl	W	To delete SFC "X" of QoS class "Z" <b>set qosclstbl Z.X.0 qosclsstatus delete</b> Ex: set qosclstbl 5.1.0 qosclsstatus delete
sfclstbl	R	To display all SF classes <b>show sfclstbl</b> Note: there is no command to show individual table entries. The "Invalid index" error message will be printed if a "show sfclstbl <index>" command is used.
sfclstbl	W	To add a new SF class <b>set sfclstbl 0 sfclassname &lt;SFC name&gt;</b>
sfclstbl	W	To delete a SF class <b>set sfclstbl &lt;index&gt; sfclsstatus delete</b> Note: the entry will not be deleted if it is used by a QoS class.

sfclstbl	W	<p>To update an SF class</p> <pre><b>set sfclstbl &lt;index&gt; param1 &lt;value&gt; ----- param3 &lt;value&gt;</b></pre> <p>where param =sfclassname  schtype  sfdir  sfstate  msr  minresrate(cir)  maxlatency  tolerablejitter  trafficpriority  multiburstframes  sfclsstatus</p> <p>Ex: set sfclstbl 4 multiburstframes 3</p>
pirtbl	R	<p>To show all PIRs</p> <pre><b>show pirtbl</b></pre> <p>Note: there is no command to show individual table entries. The "Invalid index" error message will be printed if a "show pirtbl &lt;index&gt;" command is used.</p>
pirtbl	W	<p>To add a new PIR</p> <pre><b>set pirtbl 0 rulename &lt;PIR name&gt;</b></pre> <p>Ex: set pirtbl 0 rulename test</p> <p>Note: this command actually creates the first subrule of the PIR (X.1) because the shared fields must be stored somewhere even if there are no subrules. The 7 fields of the subrule are initialized to default values. Later on, when explicitly creating the first subrule (see the next command), the X.1 record will be modified. This command can not be used to create X.2, X.3, X.4 (the last 3 subrules of the PIR).</p>

pirtbl	W	<p>To add 4 subrules to PIR "X" (the numbers on the right are for reference only)</p> <pre> set pirtbl X.0 ipprotid &lt;protocol ID&gt; 1 set pirtbl X.0 ipprotid &lt;protocol ID&gt; 2 set pirtbl X.0 ipprotid &lt;protocol ID&gt; 3 set pirtbl X.0 ipprotid &lt;protocol ID&gt; 4 </pre> <p>Note: The first 4 commands above are mandatory.</p> <pre> set pirtbl X.0 srcportstart &lt;port #&gt; srcportend &lt;port #&gt; 1 set pirtbl X.0 srcportstart &lt;port #&gt; srcportend &lt;port #&gt; 2 set pirtbl X.0 srcportstart &lt;port #&gt; srcportend &lt;port #&gt; 3 set pirtbl X.0 srcportstart &lt;port #&gt; srcportend &lt;port #&gt; 4  set pirtbl X.0 destportstart &lt;port #&gt; destportend &lt;port #&gt; 1 set pirtbl X.0 destportstart &lt;port #&gt; destportend &lt;port #&gt; 2 set pirtbl X.0 destportstart &lt;port #&gt; destportend &lt;port #&gt; 3 set pirtbl X.0 destportstart &lt;port #&gt; destportend &lt;port #&gt; 4  set pirtbl X.0 srcipaddr &lt;IP addr&gt; srcipmsk &lt;IP msk&gt; 1 set pirtbl X.0 srcipaddr &lt;IP addr&gt; srcipmsk &lt;IP msk&gt; 2 set pirtbl X.0 srcipaddr &lt;IP addr&gt; srcipmsk &lt;IP msk&gt; 3 set pirtbl X.0 srcipaddr &lt;IP addr&gt; srcipmsk &lt;IP msk&gt; 4  set pirtbl X.0 destipaddr &lt;IP addr&gt; destipmsk &lt;IP msk&gt; 1 set pirtbl X.0 destipaddr &lt;IP addr&gt; destipmsk &lt;IP msk&gt; 2 set pirtbl X.0 destipaddr &lt;IP addr&gt; destipmsk &lt;IP msk&gt; 3 set pirtbl X.0 destipaddr &lt;IP addr&gt; destipmsk &lt;IP msk&gt; 4  set pirtbl X.0 srcmacaddr &lt;MAC addr&gt; srcmacmsk &lt;MAC msk&gt; 1 set pirtbl X.0 srcmacaddr &lt;MAC addr&gt; srcmacmsk &lt;MAC msk&gt; 2 set pirtbl X.0 srcmacaddr &lt;MAC addr&gt; srcmacmsk &lt;MAC msk&gt; 3 set pirtbl X.0 srcmacaddr &lt;MAC addr&gt; srcmacmsk &lt;MAC msk&gt; 4  set pirtbl X.0 destmacaddr &lt;MAC addr&gt; destmacmsk &lt;MAC msk&gt; 1 set pirtbl X.0 destmacaddr &lt;MAC addr&gt; destmacmsk &lt;MAC msk&gt; 2 set pirtbl X.0 destmacaddr &lt;MAC addr&gt; destmacmsk &lt;MAC msk&gt; 3 set pirtbl X.0 destmacaddr &lt;MAC addr&gt; destmacmsk &lt;MAC msk&gt; 4 </pre> <p>Note: if you need only 3/2/1 subrules then there will be only 3/2/1 commands for each of the 7 fields. The new subrule is created only when setting ipprotid (which is mandatory). Subrules can not be modified. They must be deleted and redefined.</p>
--------	---	---

pirtbl (cont'd)	W	<p>Example 1 shows the creation of 4 subrules:</p> <pre> set pirtbl 7.0 ipprotid 27 set pirtbl 7.0 ipprotid 56 set pirtbl 7.0 ipprotid 70 set pirtbl 7.0 ipprotid 90  set pirtbl 7.0 srcportstart 15 srcportend 16 set pirtbl 7.0 srcportstart 50 srcportend 51 set pirtbl 7.0 srcportstart 60 srcportend 61 set pirtbl 7.0 srcportstart 25 srcportend 29  set pirtbl 7.0 destportstart 15 destportend 35 set pirtbl 7.0 destportstart 50 destportend 39 set pirtbl 7.0 destportstart 60 destportend 21 set pirtbl 7.0 destportstart 25 destportend 42  set pirtbl 7.0 srcipaddr 10.0.0.0 srcipmask 255.0.0.0 set pirtbl 7.0 srcipaddr 11.0.0.0 srcipmask 255.0.0.0 set pirtbl 7.0 srcipaddr 12.0.0.0 srcipmask 255.0.0.0 set pirtbl 7.0 srcipaddr 13.0.0.0 srcipmask 255.0.0.0  set pirtbl 7.0 destipaddr 14.0.0.0 destipmask 255.0.0.0 set pirtbl 7.0 destipaddr 15.0.0.0 destipmask 255.0.0.0 set pirtbl 7.0 destipaddr 16.0.0.0 destipmask 255.0.0.0 set pirtbl 7.0 destipaddr 17.0.0.0 destipmask 255.0.0.0  set pirtbl 7.0 srcmacaddr 00112233445566 srcmacmask ff00ff00ff00 set pirtbl 7.0 srcmacaddr 00117839945566 srcmacmask ff00ff00ff00 set pirtbl 7.0 srcmacaddr 00111234555667 srcmacmask ff00ff00ff00 set pirtbl 7.0 srcmacaddr 00112237896566 srcmacmask ff00ff00ff00  set pirtbl 7.0 destmacaddr 00112233445566 destmacmask ff00ff00ff00 set pirtbl 7.0 destmacaddr 00117839945566 destmacmask ff00ff00ff00 set pirtbl 7.0 destmacaddr 00111234555667 destmacmask ff00ff00ff00 set pirtbl 7.0 destmacaddr 00112237896566 destmacmask ff00ff00ff00 </pre> <p>Example 2 shows the creation of 1 subrule:</p> <pre> set pirtbl 7.0 ipprotid 27 set pirtbl 7.0 srcportstart 15 srcportend 16 set pirtbl 7.0 destportstart 15 destportend 35 set pirtbl 7.0 srcipaddr 10.0.0.0 srcipmask 255.0.0.0 set pirtbl 7.0 destipaddr 14.0.0.0 destipmask 255.0.0.0 set pirtbl 7.0 srcmacaddr 00112233445566 srcmacmask ff00ff00ff00 set pirtbl 7.0 destmacaddr 00112233445566 destmacmask ff00ff00ff00 </pre>
-----------------	---	---

pirtbl	W	To delete PIR "X" <b>set pirtbl X.0 pirstatus delete</b> Note: the entry will not be deleted if it is used by a QoS Class.
pirtbl	W	To disable PIR "X" <b>set pirtbl X.0 pirstatus disable</b>
pirtbl	W	To modify one of the shared fields of PIR "X" <b>set pirtbl X.0 param &lt;value&gt;</b> OR <b>set pirtbl X.0 param1 &lt;value&gt; param2 &lt;value&gt;</b> where param =rulename iptoslow iptoshigh iptosmask ethprilow ethprihigh vlanid ethtype ethvalue Ex: set pirtbl 7.0 iptoslow 1 iptoshigh 2 set pirtbl 7.0 rulename test

## Radius Parameters

radius	R	RADIUS Group
radiustbl	RW	RADIUS Authentication Server Table
index	R	Index
status	RW	RADIUS Server Status [1=enable, 2=disable]
ipaddr	RW	IP address
port	RW	Authentication port
ssecret	W	Shared Secret
responsetm	RW	Response Time [1-4 seconds]
maxretx	RW	Maximum retransmissions [1-10]
type	R	Server type
radcliinvsvraddr	R	Client Invalid Server Address
radauthlifetm	RW	Authentication Lifetime [0, 900 - 42300]
radmacacctrl	RW	MAC Access Control

## RIP Global Parameters

queries	R	RIP v2 Global Queries
routechg	R	RIP v2 Global Route Changes

## RIP Interface Parameters

**Note:** RIP parameters are configured in routing mode only.

ripifcfg	RW	RIP Interface Configuration Table
authtype	RW	Authentication Type [1 = No Authentication, 2 = Simple Password]
authkey	RW	Authentication Key
ifconf	RW	RIP Interface Configuration [1 = Enable, 2 = Disable]. This enables/disables RIP for interfaces with specified IP address.

txmode	RW	Transmission Mode (Advertise) [1 = Do Not Send, 2 = RIP v1, 3 = RIP1 compatible, 4 = RIP v2]
rxmode	RW	Receiving Mode [1 = RIP v1, 2 = RIP v2, 3 = RIP v1 or v2]
defmetric	RW	Default Metric

## Roaming Parameters

roaming	R	To show Roaming parameters.
roamstatus	RW	Status of Roaming. <b>set roamstatus &lt;value&gt;</b> <b>show roamstatus</b> where value can be: enable; disable. Default value is disable.
announcementperiod	RW	Announcement Period. <b>set announcementperiod &lt;value&gt;</b> <b>show announcementperiod</b> where value=25-100 ms in 5 ms increments. Default value is 100 ms.
multiframebursting	RW	Multi-Frame Bursting. <b>set multiframebursting &lt;value&gt;</b> <b>show multiframebursting</b> where value can be: 1=Enable, 2=Disable
roamscanchantbl	RW	Auto Scanning Channel Priority Table. <b>set roamscanchantbl &lt;index&gt; &lt;value&gt;</b> <b>show roamscanchantbl</b> where value can be: 1=Active, 2=Active High, 3=Inactive.
slowscanthreshold	RW	Slow Scan Threshold. 0-50 dB in 1 dB increments. Default value is 12dB. This parameter applies to SUs only.
fastscanthreshold	RW	Fast Scan Threshold. 0-50 dB in 1 dB increments. Default value is 6 dB. This parameter applies to SUs only.
roamthreshold	RW	Roaming Threshold. 0-50 dB in 1 dB increments. Default value is 3 dB. This parameter applies to SUs only.
slowscanpercentthreshold	RW	Slow Scan Percent Threshold. Used to manage retransmission calculation. Default is 2 percent.
fastscanpercentthreshold	RW	Fast Scan Percent Threshold. Used to manage retransmission calculation. Default is 10 percent.

## Security Parameters

security	R	Security Configuration Group
seconfig	RW	Security configuration
secenckeylentbl	RW	Encryption Key Length Table
index	R	Index
enckeylen	RW	Encryption Key Length

## Serial Parameters

serial	R	Serial Group
serbaudrate	RW	Baud rate [1=2400, 2=4800, 3=9600, 4=19200, 5=38400, 6=57600]
serdatabits	RW	Data bits
serparity	RW	Parity
serstopbits	RW	Stop bits
serflowctrl	RW	Flow control [1=xonxoff, 2=none]

## Site Survey Parameters

sitesurvey	R	Site Survey Group
sitesurveytbl	R	Site Survey Table

## SNMP Parameters

snmp	R	SNMP Group
snmpipaccesstbl	RW	SNMP IP Access Table
index	R	Index
ipaddr	RW	IP address
submask	RW	Subnet mask
if	RW	Interface [0=None, 1=Ethernet, 4=Wireless, 15=All]
cmt	RW	Comment of 1-255 characters.
status	RW	Status of table entry [1=enable, 2=disable, 3=delete]
snmptraphosttbl	RW	SNMP Trap Host Table
index	R	Index
ipaddr	RW	IP address
passwd	W	Password
cmt	RW	Comment of 1-255 characters.
status	RW	Status of table entry [1=enable, 2=disable, 3=delete]
snmprpasswd	W	Read password
snmprpasswd	W	Read/write password
snmpifbitmask	RW	SNMP Interface Bitmask (0-15)
SNMP Example: This command adds and enables a new entry to the SNMP IP Access Table with IP address 10.0.0.2, subnet mask 255.255.255.0 on an Ethernet interface.		
set snmpipaccesstbl 0 ipaddr 10.0.0.2 submask 255.255.255.0 if 1 status 1		

## Spanning Tree Parameters

stp	R	Spanning Tree Group
stptbl	RW	Spanning Tree Table
index	R	Index
priority	RW	Bridge priority
pathcost	RW	Path cost
status	RW	Status of table entry [1=enable, 2=disable]
stpstatus	RW	Spanning Tree status [1=enable, 2=disable]
stppriority	RW	Bridge priority
stpmaxage	RW	Maximum age
stpbridgehellotime	W	Hello time
stpfwddelay	RW	Forward delay

## Static Mac Address Filter Parameters

staticmactbl	RW	Static MAC Address Filter Table
index	R	Index
wiredmacaddr	RW	Static MAC address on wired network
wiredmask	RW	Static MAC address mask on wired network
wirelessmacaddr	RW	Static MAC address on wireless network
wirelessmask	RW	Static MAC address on wireless network
cmt	RW	Comment [1-255 characters]
status	RW	Status of table entry [1=enable, 2=disable]

## Statistic Parameters

statarptbl	R	ARP Table
statbridgetbl	R	Bridge Learn Table
statif	R	Interface Statistics
statradius	R	RADIUS Authentication Statistics
statripglobal	R	RIP Global Statistics
statripif	R	RIP Interface Statistics
staticmp	R	ICMP Statistics

## Station Statistic Parameters

On SUs, these parameters show statistics of the BSU to which the SU is registered. On the BSU, they show statistics of all the SUs connected to the BSU.

statworp	R	Displays WOPR statistics.
statworpbsu	R	Displays station statistics of the BSU (must be executed from the SU).
statworpstbl	R	Displays station statistics parameters of connected SUs (must be executed from the BSU).
statworpbsumac	R	Displays the MAC address of the device.
statworpbsulrxrate	R	Displays the transmission rate of the local device.
statworpbsurtxrate	R	Displays the transmission rate of the remote device.
statworpbsuls	R	Displays the local signal statistics.
statworpbsuln	R	Displays the local noise statistics.
statworpbsurs	R	Displays the remote signal statistics.
statworpbsurn	R	Displays the remote noise statistics.
statstations	R	Displays station statistics.

## Storm Threshold Parameters

stmthres	R	Storm Threshold Group
stmbrdthres	RW	Broadcast Address Threshold [4-250]
stmmultithres	RW	Multicast Address Threshold [4-250]
stmthrestbl	RW	Storm Threshold Table
index	R	Index
bcast	RW	Broadcast Address Threshold [4-250]
multrate	RW	Multicast Address Threshold [4-250]

## System Parameters

system	R	System group
sysname	RW	Name
sysmode	RW	Mode [1=bridge, 2=router]
sysloc	RW	Location
syscountrycode	RW	System country code
sysctname	RW	Contact name
sysctemail	RW	Contact email
sysctphone	RW	Contact phone
sysdescr	R	Description
sysoid	R	OID
syservices	R	Services
sysuptime	R	Up time
sysflashbkint	RW	Flash backup interval (seconds)
sysflashupdate	RW	Flash update [1=write flash]
sysresettodefaults	RW	Resets to factory defaults. [1=reset and immediate reboot] Example: To set the unit to Routing mode: <b>set sysmode 2</b>
sysinvmgmt	R	Inventory Management Group
sysinvmgmtcmpiftbl	R	Inventory Interface Table
sysinvmgmtcmptbl	R	Inventory Component Table

## Telnet Parameters

telnet	R	Telnet Group
telifbitmask	RW	Telnet interface bitmap
telport	RW	Telnet port
tellogintout	RW	Telnet login timeout (seconds)
telsessionout	RW	Telnet session timeout (seconds)
Example: To change the login timeout and the session timeout: <b>set tellogintout 200</b> <b>telsessionout 1800</b>		

## TFTP Parameters

tftp	R	TFTP Group
tftpfilename	RW	TFTP file name
tftpfiletype	RW	TFTP file type
tftpipaddr	RW	TFTP Server IP address

## VLAN Parameters

**Note:** VLANs are configured on the BSU only.

vlanmode	RW	<p>BSU VLAN mode.</p> <p><b>show vlanmode</b> <b>set vlanmode &lt;value&gt;</b> where <b>value</b> can be: 1=Access mode, 2=Trunk mode, 3=Transparent mode. The default value is 3 for Transparent mode.</p> <p>SU VLAN mode.</p> <p><b>show vlanmode &lt;index no.&gt;</b> <b>set vlanmode &lt;index no.&gt; &lt;value&gt;</b> where <b>index no.</b> refers to the particular SU whose VLAN mode you want to assign and where <b>value</b> can be: 1=Access mode, 2=Trunk mode, 3=Transparent mode. The default value is 3 for Transparent mode.</p>
----------	----	--

vlanmgmtid	RW	<p>BSU VLAN management ID.  <b>show vlanmgmtid</b>  <b>set vlanmgmtid &lt;vlanid&gt;</b>  where <b>vlanid</b> can be 0 for no management, or <b>VLAN1 ... VLAN4095</b>  The default value is 0.</p> <p>SU management VLAN ID.  <b>show vlanmgmtid &lt;index no.&gt;</b>  <b>set vlanmgmtid &lt;index no.&gt; &lt;vlanid&gt;</b>  where <b>index no.</b> refers to the specific SU and <b>vlanid</b> is an integer from 1 to 4095. A value of 0 indicates no management VLAN. The default value is 0.</p>
vlanmgmtpri	RW	<p>BSU VLAN management priority.  <b>show vlanmgmtpri</b>  <b>set vlanmgmtpri &lt;value&gt;</b>  where <b>value</b> can be an integer from 0 to 7. The default value is 2.</p> <p>SU management VLAN priority.  <b>show vlanmgmtpri &lt;index no.&gt;</b>  <b>set vlanmgmtpri &lt;index no.&gt; &lt;value&gt;</b>  where <b>index no.</b> refers to a specific SU and <b>value</b> can be an integer from 0 to 7. The default value is 2.</p>
vlantrunktbl	RW	<p>BSU Trunk VLAN Table.  <b>show vlantrunktbl</b>  <b>set vlantrunktbl &lt;index no.&gt;</b>  where <b>index no.</b> refers to the specific BSU to which this trunk table applies. There can be up to 16 values in the BSU trunk table. There is no default value for this parameter.</p> <p>SU trunk VLAN table.  <b>show vlantrunktbl &lt;index no.&gt;</b>  <b>set vlantrunktbl &lt;index no1&gt;&lt;index no2&gt;</b>  where <b>index no.</b>, <b>index no1</b>, and <b>index no2</b> refer to a specific SU.</p>
vlanaccessid	RW	<p>SU Access VLAN ID. This parameter applies only when the SU is in Access mode.  <b>show vlanaccessid &lt;index no.&gt;</b>  <b>set vlanaccessid &lt;index no.&gt; &lt;vlanid&gt;</b>  where <b>index no.</b> refers to the specific SU and <b>vlanid</b> is an integer from 1 to 4095. The default value is 1.</p>
vlanaccesspri	RW	<p>SU VLAN access priority. This parameter applies only when the SU is in Access mode.  <b>show vlanaccesspri &lt;index no.&gt;</b>  <b>set vlanaccesspri &lt;index no.&gt; &lt;value&gt;</b>  where <b>index no.</b> refers to the specific SU and <b>value</b> is an integer from 0-7. The default value is 2.</p>

## Wireless Interface Parameters

wif	RW	Wireless Interface Group																																				
index	R	Index [3]																																				
antennagain	RW	Antenna Gain [0 - 35]																																				
autochannel	RW	Auto channel select status [1=enable, 2=disable]																																				
channel	RW	Frequency channel. Example: set wif 3 channel 149																																				
chbandwidth	RW	Channel bandwidth. 0 Bandwidth 40 - turbo 20 - 20 MHz (Turbo mode is valid for non-DFS 5054-R models sold in the US only.) 1 Bandwidth 20 - 20 MHz 2 Bandwidth 10 - 10 MHz 3 Bandwidth 5 - 5 MHz Example: set wif 3 chbandwidth <x>																																				
closedsys	RW	Closed system [1=enable, 2=disable]																																				
dtimperiod	RW	DTIM period																																				
interrobust	RW	Interference Robustness [1=enable, 2=disable]																																				
ldbalance	R	Load balancing [1=enable, 2=disable]																																				
macaddr	R	MAC address																																				
mcast	RW	Multicast rate (megabits per second)																																				
medres	RW	RTS/CTS Medium Reservation																																				
meddendistrib	R	Medium Density Distribution [1=enable, 2=disable]																																				
multrate	RW	Multicast rate (megabits per second)  <table border="1"> <thead> <tr> <th>Chnl Speed Value</th> <th>5 MHz</th> <th>10 MHz</th> <th>20 MHz</th> </tr> </thead> <tbody> <tr><td>1</td><td>1.5</td><td>3</td><td>6</td></tr> <tr><td>2</td><td>2.25</td><td>4.5</td><td>9</td></tr> <tr><td>3</td><td>3</td><td>6</td><td>12</td></tr> <tr><td>4</td><td>4.5</td><td>9</td><td>18</td></tr> <tr><td>5</td><td>6</td><td>12</td><td>24</td></tr> <tr><td>6</td><td>9</td><td>18</td><td>36</td></tr> <tr><td>7</td><td>12</td><td>24</td><td>48</td></tr> <tr><td>8</td><td>13.5</td><td>27</td><td>54</td></tr> </tbody> </table>	Chnl Speed Value	5 MHz	10 MHz	20 MHz	1	1.5	3	6	2	2.25	4.5	9	3	3	6	12	4	4.5	9	18	5	6	12	24	6	9	18	36	7	12	24	48	8	13.5	27	54
Chnl Speed Value	5 MHz	10 MHz	20 MHz																																			
1	1.5	3	6																																			
2	2.25	4.5	9																																			
3	3	6	12																																			
4	4.5	9	18																																			
5	6	12	24																																			
6	9	18	36																																			
7	12	24	48																																			
8	13.5	27	54																																			
netname	RW	Network name																																				
opermode	R	Operational mode																																				
phytype	R	Physical layer type																																				
preambletype	R	Preamble type																																				
protmech	R	Protection mechanism status																																				
regdomain	R	Regulatory Domain List																																				
satdensity	RW	Satellite density (1=large, 2= medium, 3=small, 4=mini, 5=micro]																																				
suppchannels	R	Supported channels																																				
suppdatarates	R	Supported data rates																																				
tpcmode	RW	TPC mode [0=0 dB, 3=3 dB, 6=6 dB, 9=9 dB, 12=12 dB, 15=15 dB, 18=18 dB]																																				
turbomode	RW	Turbo mode [1=enable, 2=disable] (Turbo mode can be enabled only for non-DFS US units and only for the 5054-R.)																																				
txrate	RW	Transmit rate [0=auto fallback, 1-255=(<value>/2) megabits per second]																																				

wifrxbwlimit	RW	Incoming bandwidth limit
wiftxbwlimit	RW	Outgoing bandwidth limit
Example: To disable closed system and enable turbo mode: set wif 3 closedsys 2 turbomode 1		

## Wireless Interface Security Parameters

wifsec	RW	Wireless Interface Security Table
index	R	Index
encryptoption	RW	Encryption option [1=none, 2=wep, 3=rcFour128, 4=aes]
encryptkey1	W	Encryption key 1
encryptkey2	W	Encryption key 2
encryptkey3	W	Encryption key 3
encryptkey4	W	Encryption key 4
encryptkeytx	RW	Currently used key [0-4=Keys 1-5, respectively]
While setting the key to encrypt data, the index to key name mapping is: (0-key1), (1-key2), (2-key3), (3-key4). (4-key5). Example: To set the encryption option to <b>aes</b> , set a new string for <b>key2</b> , and set it as the key used for encryption: <b>set wifsec 3 encryptoption 4 encryptkey2 abcdefghi encryptkeytx 1</b>		

## WORP Parameters

worp	R	WORP Group
worpcfg	RW	WORP Interface Configuration
index	R	Index
mode	RW	Mode [1=disabled, 2=ap, 3=base, 4=subscriber]
netname	RW	Network Name (2 to 32 characters in length)
basename	RW	Base Station Name (2 to 32 characters in length)
maxsatellites	RW	Maximum number of SUs allowed
multrate	RW	Multicast rate
nosleepmode	RW	No sleep mode; 1 = enable, 2 = disable Example: set worpcfg 3 nosleepmode 1
regtimeout	RW	Registration Time Out (seconds) [1-10]
retries	RW	Number of times data is retransmitted [1-10]
ssecret	W	Shared Secret

## SHOW AND SET PARAMETER EXAMPLES

<i>Show and Set Parameter Examples</i>	
Set the IP address parameter	<p><b>Syntax:</b> set &lt;parameter name&gt; &lt;parameter value&gt;</p> <p><b>Example:</b> set ipaddr 1 ipaddress &lt;ip address&gt; set ipaddr 1 ipaddress 10.0.0.3</p>
Create a table row or entry	<p><b>Syntax:</b> set &lt;table name&gt; &lt;table index&gt; &lt;element 1&gt; &lt;value 1&gt; ... &lt;element n&gt; &lt;value n&gt;</p> <p><b>Example:</b> set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0</p>
Modify a	<p><b>Examples:</b></p>

table entry or row	<pre>set mgmtipaccesstbl 1 ipaddr 10.0.0.11 set mgmtipaccesstbl 1 ipaddr 10.0.0.12 ipmask 255.255.255.248 cmt "First Row"</pre>
Show the group parameters	<p><b>Syntax:</b></p> <pre>show &lt;group name&gt;</pre> <p><b>Example:</b></p> <pre>show network</pre>
Show individual and table parameters	<p><b>Syntax:</b></p> <pre>show &lt;parameter name&gt;   show &lt;table name&gt;</pre> <p><b>Examples:</b></p> <pre>show ipaddr               show mgmtipaccesstbl</pre>
Enable, disable, or delete a table entry or row	<p><b>Syntax:</b></p> <pre>set &lt;Table&gt; index status &lt;enable, disable, delete&gt; set &lt;Table&gt; index status &lt;1=enable, 2=disable, 3=delete&gt;</pre> <p><b>Examples:</b></p> <pre>set mgmtipaccesstbl 2 status enable set mgmtipaccesstbl 2 status disable set mgmtipaccesstbl 2 status delete set mgmtipaccesstbl 2 status 2</pre>

## TABLES

In some cases, parameters are stored in tables whose rows contain similar parameters. Command arguments involving tables have the following syntax:

```
<table name> <row> <parameter 1 name> <value 1> ... <parameter n name> <value n>
```

Every table parameter supported in the unit's CLI and an example of a row entry for that table are listed in the following table.

### Table Parameters

<b>broadcastflttbl</b>		
index	R	Index
protoname	R	Protocol Name
direction	RW	Filtering direction [1=Ethernet-to-wireless, 2=wireless, 3=both]
status	RW	Status of table entry [1=enable, 2=disable]
<b>dhcprelaytbl</b>		
index	R	Index
dhcprlyipaddr	RW	DHCP Server Address
dhcprlycmt	RW	Comment
dhcprelaystatus	RW	Status of table entry [1=enable, 2=disable, 3=delete]
<b>dhcpserverippooltable</b>		
index	R	Index
startipaddr	RW	Start IP address in the form xxx.xxx.xxx.xxx.
endipaddr	RW	End IP address in the form xxx.xxx.xxx.xxx.
Defleasetm	RW	Default lease time. 3600-86400.

maxleasetm	RW	Maximum lease time. 3600-86400.
comment	RW	Comment. 1-255 characters.
status	RW	Status of table entry. [1=enable, 2=disable, 3=delete, 4=create]
<b>etherflttbl</b>		
index	R	Index
proto	RW	Ethernet filtering protocol
cmt	RW	Comment [1-255 characters]
status	RW	Status of table entry [1=enable, 2=disable, 3=delete]
<b>macacltbl</b>		
index	R	Index
macaddr	RW	MAC Address
cmt	RW	Comment [1-255 characters]
status	RW	Status of table entry [1=enable, 2=disable, 3=delete]
<b>intracellgrptbl</b>		
index	R	Index
grpname	RW	Name of the Intra-Cell group, 1-255 characters.
grpidl (to grpidl6)	RW	Status of table entry [1=enable, 2=disable, 3=delete]
<b>intracellmactbl</b>		
index	R	Index
mac	RW	MAC Address of the SU.
grptbl status	RW	Status of group entry [1=active, 2=inactive, 3=delete].
macstatus	RW	Status of table entry [1=enable, 2=disable, 3=delete]. Default is enable.
<b>natstaticportbindtable</b>		
index	R	Index
localipaddr	RW	Local IP address in the form xxx.xxx.xxx.xxx.
porttype	RW	Port type. [1=TCP, 2=UDP, 3 = both]
startport	RW	Local port number. 1-65535.
endport	RW	Public port number. 1-65535.
status	RW	Status of table entry [1=enable, 2=disable, 3 = delete, 4 = create]
<b>radiustbl</b>		
index	R	Index
status	RW	Status of table entry [1=enable, 2=disable]
ipaddr	RW	Server IP address
port	RW	Authentication Port
secret	W	Shared Secret
responsetm	RW	Response time [1-4 seconds]
maxretx	RW	Maximum retransmissions [1-10]
type	R	Service type
<b>secenckeylentbl</b>		
index	R	Index
enckeylen	RW	Encryption Key Length
<b>snmpipaccesstbl</b>		

index	R	Index
ipaddr	RW	IP address
submask	RW	Subnet mask
if	RW	Interface [1=Ethernet, 2=PC card A]
cmt	RW	Comment [1-255 characters]
status	RW	Status of table entry [1=enable, 2=disable, 3=delete]
<b>snmptraphosttbl</b>		
index	R	Index
ipaddr	RW	IP address
passwd	W	Password
cmt	RW	Comment [1-255 characters]
status	RW	Status of table entry [1=enable, 2=disable, 3=delete]
<b>staticmactbl</b>		
index	R	Index
wiredmacaddr	RW	Static MAC address on Ethernet (wired) network
wiredmask	RW	Static MAC address mask on wired network
wirelessmacaddr	RW	Static MAC address on wireless network
wirelessmask	RW	Static MAC address mask on wireless network
cmt	RW	Comment [1-255 characters]
status	RW	Status of table entry [1=enable, 2=disable]
<b>stmthrestbl</b>		
index	R	Index
bcast	RW	Broadcast address threshold [4-250]
mcast	RW	Multicast address threshold [4-250]
<b>sptbl</b>		
index	R	Index
priority	RW	Priority
pathcost	RW	Path cost
status	RW	Status of table entry [1=enable, 2=disable]

## Entering Strings

To enter a string with spaces, use single or double quotes. For example, there is no need for quotes in the following command because the string contains no spaces:

```
set sysname Lobby
```

The following string, however, requires quotes because of the space between the words **Front** and **Lobby**.

```
set sysname "Front Lobby"
```

## Viewing Table Contents

You can view the contents of a table as follows:

```
show <table name>
```

**Example:** This command displays all parameter values of the SNMP IP access table (`snmpipaccesstbl`).

```
show snmpipaccesstbl
```

## Creating a Table Row

You can create a table row as follows:

```
set <table name> 0 <parameter 1 name> <value 1> ... <parameter n name> <value n>
```

When you create a table row, you must use 0 as row index. Only the mandatory parameters are required. Optional parameters automatically receive the default value unless a value is given.

**Example:**

```
set snmpipaccesstbl 0 ipaddr 10.0.0.10 submask 255.255.0.0
```

This command adds a row to the SNMP IP access table (`snmpipaccesstbl`) with the IP address (`ipaddr`) and subnet mask (`submask`) parameters, which are respectively assigned `10.0.0.10` and `255.255.0.0`.

## Modifying a Table Entry

If you want to change a table entry, you must indicate the index of the table row and the parameter that must be modified.

**Example:**

```
set snmpipaccesstbl 1 ipaddr 10.0.0.11
```

This command changes the IP address (`ipaddr`) at row index 1 of the SNMP IP access table (`snmpipaccesstbl`) into `10.0.0.11`.

## Modifying Several Table Entries

You can also modify several table entries at once by indicating the index of the table row and the parameters that must be modified. With the `search` command, you can see which parameters are in the table.

**Example:**

```
set snmpipaccesstbl 1 ipaddr 10.0.0.12 submask 255.255.255.248 cmt "First Row"
```

## Enabling, Disabling, or Deleting a Table Row

You can also enable, disable, or delete a row in a table. The syntax of this command is:

```
<table name> <row> <enable/disable/delete>, or  
<table name> <row> status <1/2/3>
```

**Example 1:** The following command enables the row at index 2 of the SNMP IP access table (`snmpipaccesstbl`).

```
set snmpipaccesstbl 2 enable
```

**Example 2:** The following command disables the row at index 2 of the SNMP IP access table (`snmpipaccesstbl`). The status codes have the following meaning: 1 is enable, 2 is disable, 3 is delete.

```
set snmpipaccesstbl 2 status 2
```

## Event Log Error Messages

### AGERE DRIVER

Error Type	Message	Description	Corrective Action
Alert	tWlcTask0 taskNameTold failed.	Task name to ID for Agere 11b driver failed	None
Alert	tWlcTask0 taskSuspend failed, id = 0x%x.	Task suspend for agere 11b driver failed	None
Alert	tNetTask tWlcTask0 taskResume failed.	Task resume for agere 11b driver failed	None
Alert	usrAppInit: ERROR initWlcInitString ()	Driver init failed for agere driver	Specify valid init parameters for driver

### BRIDGE

Error Type	Message	Description	Corrective Action
Alert	fnControlTask Serious failure, fnInitializeBridgeMemory() failed.	Init of memory for bridge failed	None
Alert	fnControlTask Serious failure, Mblk Conatiner not initialized.	Unable to initialize memory blocks for bridge	None
Alert	Bridge semCreate failed	Semaphore creation for bridge failed	None
Alert	Control Task:Error while Initializing Bridge.	Bridge init failed	Check bridge init parameters
Critical	Init of filtering grp flash Failed ....	Init of filtering group failed	Check filtering group init parameters

### CLI

Error Type	Message	Description	Corrective Action
Error	getIntFromStr passed invalid hex digit 0x%d.	Converting string to integer has invalid specified hex value	None

### DFS (DYNAMIC FREQUENCY SELECTION)

Error Type	Message	Description	Corrective Action
Info	Radar detected on channel <x> and is blacklisted	A radar signal is detected on a channel	None
Info	Radar detected on DFS preferred channel <x> and is blacklisted.	A radar signal is detected on DFS preferred channel	None
Info	Blacklisted channel <x> moved back to DFS channel list	A blacklisted channel returns to "Active" status in the DFS channel list after a 30 minute period	None
Critical	All "Active" channels are blocked due to Radar interference, wireless interface is disabled.	None of the channels in the DFS channel list is usable because they all have become blacklisted.	None

### DHCP CLIENT

Error Type	Message	Description	Corrective Action
Info	values were ip 0x%x netmask 0x%x	Specifies the initial IP address and subnet mask for DHCP client	None
Info	values are ip 0x%x netmask 0x%x	Specifies the current IP address and subnet mask for DHCP client	None
Info	Started DHCP Client.	Started DHCP client	None

Error Type	Message	Description	Corrective Action
Alert	executedDHCPClient() failed.	DHCP client execution failed	Check DHCP client /Server settings
Info	Static IP Address.	Indicates that the system has static IP address	None
Alert	DHCP interface not specified.	DHCP interface not specified.	Specify proper DHCP interface
Alert	DHCP interface not found '%s'.	Specified DHCP interface is not found	Specify proper DHCP interface
Alert	dhcpcInit failed for interface '%s'.	DHCP client init failed for the specified interface	Check DHCP init parameters
Alert	dhcpcEventHookAdd failed for interface '%s'.	DHCP client event hook add for specified interface failed	None
Alert	DHCP : failed to set _DHCP_ROUTER_TAG	DHCP client failed to set router tag	None
Alert	DHCP : failed to set _DHCP_DNS_SERVER_TAG	DHCP client failed to set DNS server tag	None
Alert	DHCP : failed to set _DHCP_SUBNET_MASK_TAG	DHCP client failed to set subnet mask tag	None
Alert	DHCP : failed to set _DHCP_HOSTNAME_TAG	DHCP client failed to set hostname tag	None
Info	DHCP client ID is %s	Specifies the DHCP client ID	None
Alert	DHCP : failed to set _DHCP_CLIENT_ID_TAG	DHCP client failed to set	None
Alert	fnnDhcpInit() gDhcpHookRequestSem semCreate FAILED.	Semaphore creation for DHCP client request failed	None
Alert	fnnDhcpInit() gDhcpHookResponseSem semCreate FAILED.	Semaphore creation for DHCP client response failed	None
Alert	fnnDhcpInit() tDhcpRequest failed to spawn task.	DHCP client request task failed	None
Alert	fnnDhcpInit() tDhcpResponse failed to spawn task.	DHCP client response task failed	None
Warning	DHCP Lease has expired.	DHCP lease has expired	None
Warning	dhcpParamsGet() call failed, errno 0x%x.	Specifies that the parameters to get for DHCP client failed	None
Warning	Restart of failed fnnDhcpInit() call failed, errno 0x%x.	Restart of Init of DHCP client failed	None
Alert	DHCP interface not specified.	DHCP interface is not specified.	None
Alert	[Dhcp] dhcpLibInit failed!	Init of DHCP library failed	None
Critical	ifAddrDelete() failed in DHCP client.	DHCP client failed to delete IP address	None
Critical	ifMaskSet() failed in DHCP client.	DHCP client failed to set IP subnet mask	None
Critical	ifAddrSet() failed in DHCP client.	DHCP client failed to set IP address	None
Info	New IP Address: %s	Specifies the new IP address	None
Info	New Subnet mask: 0x%x	Indicates the subnetmask	None
Critical	DHCP Client Subnet Mask Option get Failed	DHCP client failed to get subnetmask	Check DHCP client/Server settings
Critical	DHCP Client Router Option get Failed	DHCP client failed to get Router address	Check DHCP client/Server settings
Critical	Error in params get	Indicates error in getting DHCP parameters	Check DHCP client/Server settings
Critical	[Dhcp] Gateway IP Address supplied by DHCP Server is NULL, Gateway IP = Target IP	Gateway IP Address supplied by DHCP Server is NULL	Check DHCP client/Server settings
Info	DHCP Successful	DHCP client successful	None

Error Type	Message	Description	Corrective Action
Info	IP Address: %s	Indicates the DHCP IP address obtained	None
Info	SubnetMask: %s	Specifies the subnetmask	None
Info	Gateway IP Address: %s	Specifies the gateway Ip address	None
Warning	Unable to Add Default Route, so trying to delete and trying again	Unable to Add Default Route, so trying to delete and trying again	None
Critical	routeDelete is not successful	Deleting route was not successful	None
Critical	Unable to Add the Default route	Unable to add default route	

## DHCP RELAY

Error Type	Message	Description	Corrective Action
Critical	DHCP Relay Agent Init Failed.	DHCP Relay Agent Init Failed.	Specify proper init parameters
Info	DHCP Relay Agent Init Success.	DHCP Relay Agent Init was successful	None

## DHCP SERVER

Error Type	Message	Description	Corrective Action
Alert	Control task:Error while Initialistion of dhcp.	Init of DHCP failed	Specify proper init parameters

## DRIVER

Error Type	Message	Description	Corrective Action
Alert	initWlcDriver -- failed	Driver init failed	Specify valid init parameters for driver

## EVENT LOG

Error Type	Message	Description	Corrective Action
Info	The Event Log has been intentionally reset.	The event log file is reset	None
Info	System startup elf file does not exist (stat).	Event log file does not open	None
Info	System startup elf file does not exist (fopen).	Event log file does not open	None
Alert	System startup elf incorrect size, recover failed, start with new file: was %d is %d.	Event log file has incorrect size and specifies the size of old log file and new log file	Check for proper event log file
Alert	System startup elf incorrect size, recovered file: was %d is %d	Event log file has incorrect size and specifies the size of old log file and new log file	Check for proper event log file
Alert	System startup elf incorrect size, start with new file: was %d is %d.	Event log file has incorrect size and specifies the size of old log file and new log file	Check for proper event log file
Alert	Initial file missing start or end: start %d and end %d will start with empty file.	Event log file has missing start or end and specifies the start and end of the file	Check for proper event log file

## FLASH

Error Type	Message	Description	Corrective Action
Alert	ERROR fnnInitFLASHData() failed	Init of flash data failed	None
Alert	FlashControl semCreate failed	Creation of flash control semaphore failed	None

Error Type	Message	Description	Corrective Action
Alert	Control task:Error taskSpawn() fnFlashControl failed.	Spawing a task for flash control failed	None
Alert	fnReadFromFlash() failed, CheckSum %c %c %c %c	Specifies the Checksum value that failed for the file	None
Alert	Unable to write country code from factory defaults	Unable to write country code from factory defaults	None
Notice	fnnWriteDataToFLASH() Write to FLASH Failed	Writing to flash failed	Check flash device
Notice	fnnWriteDataToFLASH() FLASH disabled .....	Flash is disabled	Check flash device
Notice	fnnWriteDataToFLASH() FLASH semTake failed .....	Semaphore take failed	None
Notice	FLASH fnnFlashInit() semCreate failed.	Creating semaphore failed	None
Notice	fnnDeleteNGAPflashFiles() semTake failed.	Semaphore take failed	None
Notice	fnnDeleteNGAPflashFiles() Deleting existing CONFIG file.	Existing configuration file is deleted	None
Info	Config File does not exist, creating with default values.	Creating default configuration file	None
Notice	fnnSNMPFlashRegister() open create file %s failed.	Open failed for the specified file	None
Notice	fnnSNMPFlashRegister() fnnWriteHeaderAndDataToFLASH() failed.	Writing header and data to flash file failed	None
Critical	Checksum failed, Deleting existing CONFIG file.	Checksum for existing config file failed and hence will be deleted	None
Info	Config File has: Top %d Bot %d, we are currently at Top %d Bot %d.	Specifies the existing and current top and Bottom values for config file	None
Info	Incomptable config versions, reset to factory defaults	The device shall be reset to factory defaults due to incompatible config versions	None
Info	Config File has: Top %d Bot %d, we are currently at Top %d Bot %d.	Specifies the existing and current top and Bottom values for config file	None
Info	Calling data Translation function.		None
Info	DATA File does not exist, creating with default values.	Data file does not exist and hence shall be created with default values	None
Critical	Interface and Component IDs does not match	Interface and component IDs do not match	None
Critical	DATA file Length is invalid, updating the file	Data file length is invalid and hence the file shall be updated	None
Critical	Checksum Failed for LTV DATA file header	Checksum Failed for LTV DATA file header	None
Critical	Failed reading FlashFormat from DATA file, creating a default one	Failed reading FlashFormat from DATA file, creating a default one	None
Critical	Forced Reload Deleting existing CONFIG file.	Forced Reload Deleting existing CONFIG file.	None
Critical	Init of SNMP Setup Group Failed	Init of SNMP Setup Group Failed	Specify proper init values for SNMP
Critical	Init of DHCP Group Failed	Init of DHCP Group Failed	Specify proper init values for DHCP
Critical	Init of filtering grp def Failed .	Init of filtering grp def Failed	Specify proper init values for filtering
Critical	Init of Intra-Cell Blocking Grp Failed	Init of Intra-Cell Blocking Grp Failed	Specify proper init values for ICB
Critical	Init of Temp Log Failed	Init of Temp Log Failed	Specify proper init values for temp log

Error Type	Message	Description	Corrective Action
Critical	Network Grp Init failed	Network Grp Init failed	Specify proper init values for network group
Critical	IpRouteTbl Grp Init failed	IP route table Grp Init failed	Specify proper init values for route table
Critical	Init of link test group failed	Init of link test group failed	Specify proper init values for link test
Critical	System Grp Init failed	System Grp Init failed	Specify proper init values for system group
Critical	Init of fnnMIB2Init Group Failed	Init of MIB2 Group Failed	Specify proper MIB 2 init values
Critical	TFTP Grp Init failed	TFTP Grp Init failed	Specify proper values for TFTP group
Critical	fnnSetEthernetSettings : returned Error	Setting Ethernet returned error	Specify proper ethernet settings
Critical	fnnLtvDataFlashRegister() failed.	Writing LTV data to flash failed	Specify proper LTV data
Critical	fnnSNMPFlashRegister() failed.	Writing SNMP to flash failed	Specify proper SNMP values
Critical	Init of 802dot11 group failed	Init of 802dot11 group failed	Specify proper values for 802.11 group

## ICB

Error Type	Message	Description	Corrective Action
Error	Not able to get the Mblk Container	Not able to allocate memory blocks	None

## LED

Error Type	Message	Description	Corrective Action
Alert	LED Watchdog could not be started	LED Watchdog could not be started	None
Alert	LED Watchdog could not be created	LED Watchdog could not be created	None
Alert	LED Watchdog could not be deleted	LED Watchdog could not be deleted	None

## LICENSE

Error Type	Message	Description	Corrective Action
Alert	ERROR fnnProcessLicenseFiles() failed.	Processing of license files failed	Specify valid license files in flash
Alert	ERROR fnnCheckRadioSupport() failed	The radio check failed	Check radio
Alert	Zero License Files present in the FLASH	Zero license files present in the FLASH	Provide a valid license file in device
Alert	From factory default base is licensed, so set to base mode.	From factory default base is licensed, so set to base mode	None
Warning	Unable to write base mode from factory defaults	Unable to write base mode from factory defaults	None
Alert	License Correction: change from base station mode to satellite mode.	License Correction: change from base station mode to satellite mode.	None
Alert	Max stations licensed must be > 0 for a base station mode.	Max stations licensed must be greater than zero for a base station mode.	Provide a valid license file in device
Alert	License Correction: Change Input Bandwidth from %d to %d.	Specifies the existing and current input bandwidth	None
Alert	License Correction: Change Output Bandwidth from %d to %d.	Specifies the existing and current output bandwidth	None

Error Type	Message	Description	Corrective Action
Alert	License Correction: Change Max Satellites from %d to %d.	Specifies the existing and current value for max satellites	None
Info	Processing license file %s.	Specifies the license file being processed	None
Error	Unable to read %s License File header.	Unable to read header of specified License File	Use valid license file
Error	Invalid Header for %s License file	Invalid Header for the specified License file	Use valid license file
Error	Duplicate License file %s.	Specifies that the license file is duplicate	None
Error	Unable to read features of %s License file.	Unable to read features of the specified License file.	None
Critical	License file %s has more than MAX features.	Specified license file has more than MAX features.	None
Error	No licensed features in %s for this unit.	The specified file has no licensed features for this unit.	None
Info	No of features in %s = %d	Specifies the license file and the number of features in the license file	None
Error	Unable to read signature for %s License file	Unable to read signature for the specified License file	Use valid license file
Error	%s License file Verification Failed	License file Verification Failed failed for specified license file	Use valid license file
Info	Updated features for %s	Updated features for the specified license file	None
Error	No license files were processed.	No license files were processed.	None
Error	Unable to store to activation file header	Unable to store to activation file header	None
Info	License File processing done	License File processing done	None
Error	Invalid component ID %d	Specifies the Invalid component ID	None
Error	Invalid Variant %d	Specifies the Invalid Variant ID	None
Error	Invalid Major Version	Invalid Major Version	None
Error	Invalid Minor Version	Invalid Minor Version	None
Error	Invalid File size	Invalid File size	None

## NAT

Error Type	Message	Description	Corrective Action
ELF_SYS_ST_L1	Failed to create natInitSync semaphore	Failed to create semaphore for NAT	None
ELF_SYS_ST_L1	rwos_task_main() failed.	Init of rwos failed	None
ELF_SYS_ST_L1	setSingleNatIPStaticEntry, NAT fails to rebind the new WAN IP (from DHCP, PPPoE or PPPoA)	NAT fails to rebind the new WAN IP from DHCP, PPPoE or PPPoA	None

## OTHER TASKS

Error Type	Message	Description	Corrective Action
Alert	tNetTask taskNameTold failed	Network task name to ID failed	None
Alert	tNetTask taskSuspend failed, id = 0x%x.	Network task suspend failed	None
Alert	fnControlTask Serious failure, fnnNetDevInit() unsuccessful.	Network device init failed	Specify proper network init values
Info	fnnNetDevInit() successful.	Network device init is successful	None
Alert	tNetTask taskResume failed	Resuming Network task failed	None
Alert	rebootHookAdd -- failed	Adding reboot hook failed	None

Error Type	Message	Description	Corrective Action
Alert	Control task:Error taskSpawn() fnReloadControlTask failed.	Task spawn for reload control failed	None
Info	reboot Hook called.	Reboot is called	None
Alert	fnSystemDefault() stMyDirEnt is NULL.	Flash does not contain any files	None
Error	Task Monitor Rebooting: task %s id 0x%x is suspended.	Rebooting as the specified task is in suspend state	None

## QOS (QUALITY OF SERVICE) BSU

Error Type	Message	Description	Corrective Action
Info	SU with <MAC address> does not have QoS support	BSU registers an SU without QoS support	None
Warning	Total CIR for active service flows of all SUs is <x kbps> and exceeds available bandwidth of <y kbps>	Total CIR for active service flows of all SUs exceeds the available bandwidth	None
Warning	Unable to provide the CIR for service flow <x> of <SU name>	Unable to provide the required CIR for a service flow of an SU	None
Warning	Dropping packets for service flow <x> of <SU Name>	On dropping packets for a service flow of an SU in the BSU	None

## QOS (QUALITY OF SERVICE) SU

Error Type	Message	Description	Corrective Action
Info	BSU does not have QoS support	SU registers to a BSU without QoS support	None
Info	BSU provides QoS support	SU registers to a BSU with QoS support	None
Warning	Dropping packets for service flow <x>	On dropping packets for a service flow	None

## RADAR DETECTION

Error Type	Message	Description	Corrective Action
Alert	apReboot() rebooting system due to radar detection.	Indicates that reboot is due to radar detection	None
Alert	REBOOTING, radarDetection Alert: unit %d channel %d freq %d	Indicates the unit, channel and frequency for which the radar was detected	None
Info	fnControlTask() started.	Control task has started	None

## RADIUS

Error Type	Message	Description	Corrective Action
Alert	Radius semCreate failed	Creating semaphore for RADIUS failed	None
Alert	Control Task:Error while Initialistion of Radius	Init of Radius failed	Specify proper init parameters

## ROUTING

Error Type	Message	Description	Corrective Action
Alert	fnControlTask Serious failure, m2IpInit() failed	Init of static routes failed	Check for proper static routes
Critical	Failed to update Static Routing Entries.	Failed to update Static Routing Entries.	Check for proper static routes
Info	System is in Gateway mode	System is in Gateway mode	None
Critical	fnnUpdateFLASHwithRIP : returned ERROR.	Updating flash with RIP Routing enteries failed	Check for proper RIP routing entries

Error Type	Message	Description	Corrective Action
Critical	fnnUpdateRIPEntries: returned ERROR.	Updating RIP Routing Entries failed	Check for proper RIP routing entries
Critical	Failed to update Static Routing Entries.	Updating flash with static Routing Entries failed	Check for proper static routes

## SNMP

Error Type	Message	Description	Corrective Action
Alert	fnnSNMPNGAPInit -- failed	Init of Flash failed	Specify proper flash init parameters
Alert	first SNMP semCreate failed	Creation of SNMP semaphore failed	None

## SYSTEM

Error Type	Message	Description	Corrective Action
Warning	fnpGetWifRebootParams returned NULL : GET Failed	SNMP get for Wireless reboot parameters returned NULL	Check wireless reboot parameters set
Warning	oriWirelessIfPropertiesEntry_get_value: NO SUCH OBJECT : GET Failed	Mib object does not exist	Check if the MIB object exists
Warning	oriWirelessIfPropertiesEntry_test : Card is NOT present : TEST Failed	Wireless card is not present	Insert the wireless card
Warning	oriWirelessIfPropertiesEntry_test : oriWirelessIfAutoChannelSelect Status is NOT supported by this Image : TEST Failed	AutoChannelSelectStatus is NOT supported by this Image	None
Warning	oriWirelessIfPropertiesEntry_test : NO SUCH OBJECT : TEST Failed	Mib object does not exist	Check if the MIB object exists
Warning	fnnTestOriWirelessAntennaGain: Test Failed	Test for Antenna gain failed	Specify proper antenna gain
Warning	sysname len =%d , valid length should be 1 to %d.	The length of sysname is invalid and specifies the current length and the valid length of the sysname	Enter sysname of valid length

## TEMPLOG

Error Type	Message	Description	Corrective Action
Alert	TEMPLOG_TASK can not be created.	Temp logging task could not be created	None
Info	The Temp Log has been intentionally reset.	Temp log has been reset	None
Info	System startup tlf file does not exist (stat).	Temp log file does not exist	None
Info	System startup tlf file does not exist (fopen).	Temp log file does not exist	None
Alert	System startup tlf incorrect size, start with new file: was %d is %d	Specifies the incorrect size of the Temp log file and size of the new file created	None
Alert	Initial file missing start or end: start %d and end %d, we will start with empty file.	Specifies the start and end of the temp log file that has missing start or end	None
Critical Warning	Temp is %d C or is %4.1f F.	Indicates the temp in degrees and ferheneit that is out of limit	Maintain temp within limits

## TITAN H/W

Error Type	Message	Description	Corrective Action
Alert	I2C init failed	I2C bus init in Titan Hardware failed	Check I2C bus
Alert	I2C TimeOut Set failed	I2C bus timeout in Titan Hardware failed	Check I2C bus

## TPC

Error Type	Message	Description	Corrective Action
Info	Final Output Power Setting for channel %d MHz	Specifies the channel for which the output power settings shall be provided (given in next two messages)	None
Info	Scaled Power @ %dMb %d dBm, MaxRD: %d dBm, MaxEdge %d dBm, - TPC Scale %d dBm - Ant Red %d dBm	Specifies the multicast rate, scaled power, Maximum RD Power, maximum edge power, TPC scale reduction and Antenna reduction	None

## TFTP

Error Type	Message	Description	Corrective Action
Info	Image Digital Signature checking FAILED	Digital signature check for the file failed	Info
Info	fnnUp_Download: Invalid File Type for TFTP = %d	TFTP download failed due to invalid file type	None
Info	fnnUp_Download: Invalid TFTP operation requested value = %d	TFTP download failed due to invalid TFTP operation	None
Info	TFTP download image SUCCESS.	Image download is successful	None
Info	TFTP downgrade FAILED! Could not allocate memory.	Downgrade through TFTP failed due to insufficient memory	None
Info	TFTP downgrade FAILED! Access to Flash Failed	Downgrade through TFTP failed as flash could not be accessed	Check flash device
Info	TFTP downgrade FAILED! File Open Failed.	Downgrade through TFTP failed as file could not be opened	None
Info	TFTP downgrade FAILED! Header Write Failed	Downgrade through TFTP failed as file header could not be written	None
Info	TFTP downgrade FAILED! Date Write Failed.	Downgrade through TFTP failed as data could not be written to file	None
Info	TFTP downgrade FAILED! File Rename Failed.	Downgrade through TFTP failed as file could not be renamed	None
Info	TFTP downgrade SUCCESS!	Downgrade through TFTP was successful	None
Info	TFTP download image failed.	Image download through TFTP failed	None
Info	TFTP download image failed, created failed for backup file	Image download through TFTP failed as backup file could not be created	None
Info	TFTP download image failed, Firmware could not be read error %d lastTftpStatus %d	Image download through TFTP failed as image could not be read	None
Info	TFTP download image failed, Firmware size is greater than 2MB.	Image download through TFTP failed as image size was greater than 2 MB	None
Info	TFTP download image failed, Firmware could not be written error %d lastTftpStatus %d	Image download through TFTP failed as image could not be written	None
Info	TFTP download image failed, image size zero.	Image download through TFTP failed as image size was zero	None

Error Type	Message	Description	Corrective Action
Info	TFTP download image failed, errno %d error string '%s'	Image download through TFTP failed	None
Info	TFTP download image SUCCESS.	Image download through TFTP was successful	None
Info	TFTP download license failed, Max License files limit reached.	License file download through TFTP failed as the number of existing license files is maximum	None
Info	TFTP download license failed, tftpXfer failed.	License file download through TFTP failed as the TFTP transfer failed	Check TFTP transfer
Info	TFTP download license failed, create failed for license file.	License file download through TFTP failed as the new license file could not be created	None
Info	TFTP download license failed, open failed for license file.	License file download through TFTP failed as the new license file could not be opened	None
Info	TFTP download license failed, file could not be read, error %d lastTftpStatus %d	License file download through TFTP failed as the new license file could not be read	None
Info	TFTP download license failed, file could not be written, error %d lastTftpStatus %d	License file download through TFTP failed as the new license file could not be written	None
Info	TFTP download license failed, errno %d error string '%s'	License file download through TFTP failed	None
Info	TFTP download license failed, zero size file.	License file download through TFTP failed as the new license file file size was zero	None
Info	TFTP download license failed, File open Failed for file: %s	License file download through TFTP failed as the specified file could not be opened	None
Info	TFTP download license failed, zero size file. Read failed for Licensefile	License file download through TFTP failed due to zero file size	None
Info	TFTP download license failed, License File verification failed.	License file download through TFTP failed as license file verification failed	Use valid license file
Info	TFTP download license successful	License file download was successful	None
Info	TFTP upload file failed, could not open the file	TFTP upload failed as file could not be opened	None
Info	TFTP upload config file failed, tftpXfer failed	TFTP upload of config file failed as TFTP transfer failed	Check TFTP transfer
Info	TFTP upload eventlog file failed, tftpXfer failed	TFTP upload of event log file failed as TFTP transfer failed	Check TFTP transfer
Info	TFTP upload templog file failed, tftpXfer failed	TFTP upload of temp log file failed as TFTP transfer failed	Check TFTP transfer
Info	TFTP upload config file failed, File could not be read: error %d lastTftpStatus %d	TFTP upload of config file failed as file could not be read	Check for proper config file
Info	TFTP upload eventlog file failed, File could not be read: error %d lastTftpStatus %d	TFTP upload of event log file failed as file could not be read	Check for proper eventlog file
Info	TFTP upload templog file failed, File could not be read: error %d lastTftpStatus %d	TFTP upload of temp log file failed as file could not be read	Check for proper temp log file
Info	TFTP upload config file failed, write to file failed: error %d lastTftpStatus %d	TFTP upload of config file failed as file write failed	Check for proper config file

Error Type	Message	Description	Corrective Action
Info	TFTP upload eventlog file failed, write to file failed: error %d lastTftpStatus %d	TFTP upload of event log file failed as file write failed	Check for proper eventlog file
Info	TFTP upload templog file failed, write to file failed: error %d lastTftpStatus %d\	TFTP upload of temp log file failed as file write failed	Check for proper temp log file
Info	TFTP upload config file failed, TFTP operation failed: errno %d error string '%s'	TFTP upload of config file failed due to TFTP failure and specifies the error no and reason	Check TFTP transfer
Info	TFTP upload eventlog file failed, TFTP operation failed: errno %d error string '%s'	TFTP upload of eventlog file failed due to TFTP failure and specifies the error no and reason	Check TFTP transfer
Info	TFTP upload templog file failed, TFTP operation failed: errno %d error string '%s'	TFTP upload of templog file failed due to TFTP failure and specifies the error no and reason	Check TFTP transfer
Info	TFTP upload config file failed, Zero bytes uploaded.	TFTP upload of config file failed due to zero bytes transferred	Check TFTP transfer
Info	TFTP upload eventlog file failed, Zero bytes uploaded	TFTP upload of eventlog file failed due to to zero bytes transferred	Check TFTP transfer
Info	TFTP upload templog file failed, Zero bytes uploaded.	TFTP upload of templog file failed due to to zero bytes transferred	Check TFTP transfer
Info	TFTP upload config file successful	TFTP upload of config file was successful	None
Info	TFTP upload eventlog file successful	TFTP upload of eventlog file was successful	None
Info	TFTP upload templog file successful.	TFTP upload of templog file was successful.	None
Info	TFTP upload config file failed, could not open the DATA file	TFTP upload of config file failed due to failure to open config file	Check for proper config file
Info	TFTP upload config file failed, tftpXfer failed	TFTP upload of config file failed due to TFTP failure	Check TFTP transfer
Info	TFTP upload config file failed, File could not be read: error %d lastTftpStatus %d	TFTP upload of config file failed due to failure to read config file and specifies the error no and status	Check for proper config file
Info	TFTP upload config file failed, write to file failed: error %d lastTftpStatus %d	TFTP upload of config file failed due to failure to write config file and specifies the error no and status	Check for proper config file
Info	TFTP upload config file failed, TFTP operation failed: errno %d error string '%s'	TFTP upload of config file failed due to TFTP failure and specifies the error no and reason	Check TFTP transfer
Info	TFTP upload config file failed, Zero bytes uploaded.	TFTP upload of config file failed due to to zero bytes transferred	Check TFTP transfer
Info	TFTP upload config file successful.	TFTP upload of config file was successful	None
Info	TFTP download config file failed, tftpXfer failed.	TFTP download of config file failed due to failure of TFTP transfer	Check TFTP transfer
Info	TFTP download config file failed, File creation failed for %s. TFTP operation aborted.	TFTP download of config file failed due to failure to create specified backup config file	None
Info	TFTP download config file failed, File could not be read: error %d lastTftpStatus %d	TFTP download of config file failed due to failure to read config file and specifies the error no and status	Check for proper config file
Info	TFTP download config file failed, write to file failed: error %d lastTftpStatus %d	TFTP download of config file failed due to failure to write config file and specifies the error no and status	Check for proper config file

Error Type	Message	Description	Corrective Action
Info	TFTP download config file failed, TFTP operation Failed: errno %d error string %s	TFTP download of config file failed due to failure of TFTP operation and specifies the error number and the reason	Check TFTP transfer
Info	TFTP download config file failed, TotalBytes Transfered is %d	TFTP download of config file failed and specifies the total number of bytes transferred	Download valid config file
Info	TFTP download config file failed, Incompatible Configuration Type.	TFTP download of config file failed due to incompatible configuration type	Download valid config file
Info	TFTP download config file successful	TFTP download of config file was successful	None

## VLAN

Error Type	Message	Description	Corrective Action
Info	VLAN mode of the BSU upon boot up	Access, Trunk, or Transparent	N/A
Info	Change of VLAN mode during runtime	BSU VLAN mode has changed from Transparent to Trunk or from Trunk to Transparent mode.	N/A
Info	VLAN configuration applied (RADIUS server/Flash/Default)	BSU configuration changes have been applied. VLAN configuration for BSU is obtained from RADIUS or from that stored in its Flash, or it has come up with the default VLAN configuration.	N/A
Info	Upon deleting VLAN configuration of unregistered SU automatically	The VLAN configuration for an unregistered SU has been deleted. When all the entries in the SU table are full and it contains entries for unregistered SUs, and then a new SU is associated, the VLAN configuration of unregistered SUs are deleted automatically.	Register SU with BSU and re-configure.
Info	VLAN mode of the SU on boot up	Access, Trunk, or Transparent	N/A
Info	Change of VLAN mode during runtime	SU VLAN mode has changed from Transparent to Trunk mode or from Trunk to Access mode, or from Access to Trunk mode.	N/A
Info	VLAN configuration applied (RADIUS server/Flash/Default)	SU configuration changes have been applied. VLAN configuration for an SU have been obtained from RADIUS or from that stored in the BSU's Flash, or it has come up with the default VLAN configuration.	N/A

## WORP

Error Type	Message	Description	Corrective Action
Error	Invalid interface type for unit %d interface type %d	Specifies the invalid unit and interface type	Specify proper interface
Alert	initWorp -- failed	WORP init failed	Specify proper WORP init parameters
Alert	fnSUStatUpdater() failed.	SU statistics updation failed	None
Alert	UsrAppInit:Error Initializing Mutual Authentication	Error Initializing Mutual Authentication	Specify proper init parameters for mutual authentication
Error	WORP MTU could not be set	WORP MTU could not be set	Check for proper WORP MTU

<b>Error Type</b>	<b>Message</b>	<b>Description</b>	<b>Corrective Action</b>
Alert	fnnGetRateInMbps: Illegal value from WORP.	Illegal value of data Rate	Use valid data rate value
Alert	Update of SU Statistics failed!	Update of SU Statistics failed!	None

## Alarm Traps

The following trap types are documented in this section:

- Configuration-related traps
- Flash memory related traps
- Image related traps
- Operational related traps
- Security related traps
- System feature based license related traps
- TFTP related traps
- Wireless Interface Card related traps
- WORP related traps

These alarm groups can be enabled or disabled through the Web Interface.

## SEVERITY LEVELS

There are three severity levels for system alarms: Critical, Major, and Informational

Critical alarms will often result in severe disruption in network activity or an automatic reboot of the unit.

Major alarms are usually activated due to a breach in the security of the system. Clients cannot be authenticated because an attempt at unauthorized access into the unit has been detected.

Informational alarms provide the network administrator with some general information about the activities the unit is performing.

## TRAP GROUPS

### Configuration Related Trap/Notification Group: oriConfigurationTraps

oriTrapDNSIPNotConfigured

This trap is generated when the DNS IP Address has not been configured.

Severity: Major

oriTrapRADIUSAuthenticationNotConfigured

This trap is generated when the RADIUS authentication information has not been configured.

Severity: Major

oriTrapRADIUSAccountingNotConfigured

This trap is generated when the RADIUS accounting information has not been configured.

Severity: Major

oriTrapDuplicateIPAddressEncountered

This trap is generated when the device has encountered another network device with the same IP address.

Severity: Major

oriTrapDHCPRelayServerTableNotConfigured

This trap is generated when the DHCP relay agent server table is empty or not configured.

Severity: Major

**oriTrapWORPIfNetworkSecretNotConfigured**

This trap is generated when the system network authentication shared secret is not configured.

Severity: Major

**oriTrapVLANIDInvalidConfiguration**

This trap is generated when VLAN ID configuration is invalid.

Severity: Major

**oriTrapAutoConfigFailure**

This trap is generated when the auto configuration failed.

Severity: Minor

**oriTrapBatchExecFailure**

This trap is generated when the CLI Batch execution fails for the following reasons:

- Illegal Command is parsed in the CLI Batch File
- Execution error is encountered while executing CLI Batch file
- Bigger File Size than 100 Kbytes

Severity: Minor

**oriTrapBatchFileExecStart**

This trap is generated when the CLI Batch execution begins after file is uploaded.

Severity: Minor

**oriTrapBatchFileExecEnd**

This trap is generated when the execution of CLI batch files ends.

Severity: Minor

## Flash Memory Related Trap Group: oriFlashTraps

**oriTrapFlashMemoryEmpty**

This trap is generated when there is no data present in flash memory, either on the flash card on the onboard flash memory.

Severity: Informational

**oriTrapFlashMemoryCorrupted**

This trap is generated when the data content of flash memory is corrupted.

Severity: Critical

**oriTrapFlashMemory RestoringLastKnownGoodConfiguration**

This trap is generated when the current/original configuration data file is found to be corrupted; therefore, the device will load the last known good configuration file.

Severity: Informational

## Image Related Trap Group: oriImageTraps

**oriTrapZeroSizeImage**

This trap is generated when a zero size image is loaded on the device.

Severity: Major

**oriTrapInvalidImage**

This trap is generated when an invalid image is loaded on the device.

#### oriTrapImageTooLarge

This trap is generated when the image loaded on the device exceeds the size limitation of flash.

Severity: Major

#### oriTrapIncompatibleImage

This trap is generated when an incompatible image is loaded on the device.

#### oriTrapInvalidImageDigitalSignature

This trap is generated when an image with an invalid Digital Signature is loaded in the device.

Severity: Major

## Operational Related Trap Group: oriOperationalTraps

#### oriTrapUnrecoverableSoftwareErrorDetected

This trap is generated when an unrecoverable software error has been detected. This trap can signify that a problem/error has occurred with one or more software modules. This error would cause the software watchdog timer to expire, which would then cause the device to reboot.

Severity: Critical

#### oriTrapRADIUSServerNotResponding

This trap is generated when no response is received from a RADIUS server or servers for authentication requests sent from the RADIUS client in the device.

Severity: Major

#### oriTrapModuleNotInitialized

This trap is generated when a certain software or hardware module has not been initialized or has failed to be initialized.

Severity: Major

#### oriTrapDeviceRebooting

This trap is generated when the device has received a request to be rebooted.

Severity: Informational

#### oriTrapTaskSuspended

This trap is generated when a task in the device has suspended.

Severity: Critical

#### oriTrapBootPFailed

This trap is generated when a response to the BootP request is not received, hence the device is not dynamically assigned an IP address.

Severity: Major

#### oriTrapDHCPFailed

This trap is generated when a response to the DHCP client request is not received, hence the device is not dynamically assigned an IP address.

Severity: Major

#### oriTrapDNSClientLookupFailure

This trap is generated when the DNS client attempts to resolve a specified hostname (DNS lookup) and a failure occurs. This could be the result of the DNS server being unreachable or returning an error for the hostname lookup. This trap specified the hostname that was being resolved.

Severity: Major

**oriTrapMaximumNumberOfSubscribersReached**

This trap is generated when the maximum number of subscribers has been reached.

Severity: Major

**oriTrapSSLInitializationFailure**

This trap is generated when the SSL initialization fails.

Severity: Major

**oriTrapWirelessServiceShutdown**

This trap is generated when the Wireless Service Shutdown object is configured to down; that is, the wireless interface has shut down services for wireless clients.

Severity: Informational

**oriTrapWirelessServiceResumed**

This trap is generated when the Wireless Service Shutdown object is configured to go up; that is, the wireless interface has resumed service and is ready for wireless client connections.

Severity: Informational

**oriTrapSSHInitializationFailure**

This trap is generated when the SSH initialization fails.

Severity: Major

**oriTrapVLANIDUserAssignment**

This trap is generated when a user is assigned a VLAN ID from the RADIUS server.

Severity: Informational

**oriTrapDHCPLeaseRenewal**

This trap is generated when the device does a DHCP renewal request and receives new information from the DHCP server. The variables/objects bound to this trap will provide information about the DHCP server IP address that replied to the DHCP client request, and the IP address, subnet mask, and gateway IP address returned from the DHCP server.

Severity: Informational

**oriTrapTemperatureAlert**

This trap is generated when the temperature crosses the limit of –30 to –60 degrees Celsius.

Severity: Major

## Security Related Trap Group: oriSecurityTraps

**oriTrapInvalidEncryptionKey**

This trap is generated when an invalid encryption key has been detected.

Severity: Critical

**oriTrapAuthenticationFailure**

This trap is generated when a client authentication failure has occurred. The authentication failures can range from:

MAC Access Control Table

RADIUS MAC Authentication

802.1x Authentication specifying the EAP-Type

WORP Mutual Authentication

SSID Authorization Failure specifying the SSID

VLAN ID Authorization Failure specifying the VLAN ID

Severity: Major

**oriTrapUnauthorizedManagerDetected**

This trap is generated when an unauthorized manager has attempted to view or modify parameters.

Severity: Major

**oriTrapRADScanComplete**

This trap is generated when a RAD scan is successfully completed.

Severity: Informational

**oriTrapRADScanResults**

This trap is generated in order to provide information about the RAD Scan results.

Severity: Informational

**oriTrapRogueScanStationDetected**

This trap is generated when a rogue station is detected.

Severity: Informational

**oriTrapRogueScanCycleComplete**

This trap is generated when a rogue scan is successfully completed.

Severity: Informational

## System Feature Based License Related Trap Group: oriSysFeatureTraps

**oriTrapIncompatibleLicenseFile**

This trap is generated when a license file in the device's flash memory is not compatible with the current bootloader.

Type: Major

**oriTrapFeatureNotSupported**

This trap is generated when a feature present in the license codes is not supported by the current embedded software image. A newer embedded software image could support the feature or there are more licenses needed.

Type: Informational

**oriTrapZeroLicenseFiles**

This trap is generated when a single license file is not present in flash. This causes the device to operate in default mode with very limited features enabled.

Type: Critical

**oriTrapInvalidLicenseFile**

This trap is generated when a license file in the device's flash memory has an invalid signature and will be ignored.

Type: Minor

**oriTrapUselessLicense**

This trap is generated when a license code file does not contain any valid feature code. The probable reason for this is that, after verification, not any of the features was meant for this unit's MAC address.

## TFTP Related Trap Group: oriTFTPTraps

### oriTrapTFTPFailedOperation

This trap is generated when a failure has occurred with the TFTP operation.

Severity: Major

### oriTrapTFTPOperationInitiated

This trap is generated when a TFTP operation has been initiated.

Severity: Informational

### oriTrapTFTPOperationCompleted

This trap is generated when a TFTP operation has been completed.

Severity: Informational

## Wireless Interface Card Related Trap Group: oriWirelessIfTraps

### oriTrapWLCNotPresent

This trap is generated when a wireless interface card is not present in the device.

Severity: Informational

### oriTrapWLCFailure

This trap is generated when a general failure has occurred with the wireless interface card.

Severity: Critical

### oriTrapWLCRemoval

This trap is generated when the wireless interface card has been removed from the device.

Severity: Critical

### oriTrapWLCIncompatibleFirmware

This trap is generated when the firmware of the wireless interface card is incompatible.

Severity: Critical

### oriTrapWLCVoltageDiscrepancy

This trap is generated when other than a 5-volt card or a 3.3 volt wireless interface card is inserted in the device.

Severity: Critical

### oriTrapWLCIncompatibleVendor

This trap is generated when an incompatible wireless vendor card is inserted or present in the device.

Severity: Critical

### oriTrapWLCFirmwareDownloadFailure

This trap is generated when a failure occurs during the firmware download process of the wireless interface card.

Severity: Critical

### oriTrapWLCFirmwareFailure

This trap is generated when a failure occurs in the wireless interface card firmware.

Severity: Critical

### oriTrapWLCRadarInterferenceDetected

This trap is generated when radar interference is detected on the channel being used by the wireless interface. The generic trap variable provides information about the channel at which interference was

detected.

Severity: Major

## **WORP Related Trap Group oriWORPTraps**

### **oriWORPStationRegister**

This trap is generated when a WORP SU has registered on an interface of a BSU.

Type: Informational

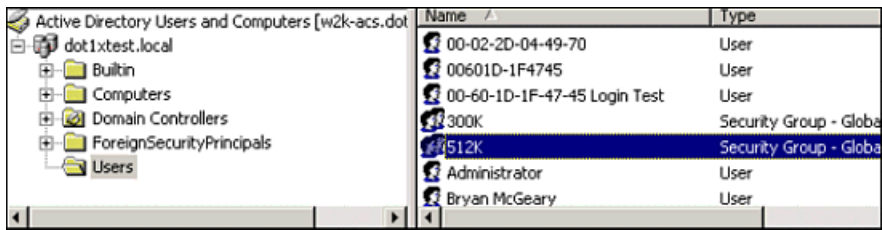
### **oriWORPStationDeRegister**

This trap is generated when a WORP SU has been deleted from an interface of a base.

Type: Informational

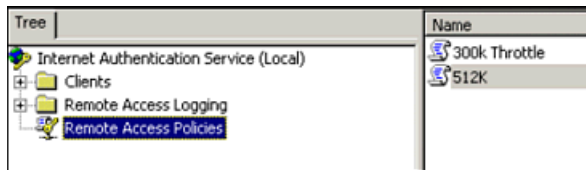
## Microsoft Windows IAS RADIUS Server Configuration

This example uses Active Directory users and groups to authenticate for bandwidth throttling. Create your users with MAC addresses as the **Login IDs**; in this example, we group 512k.

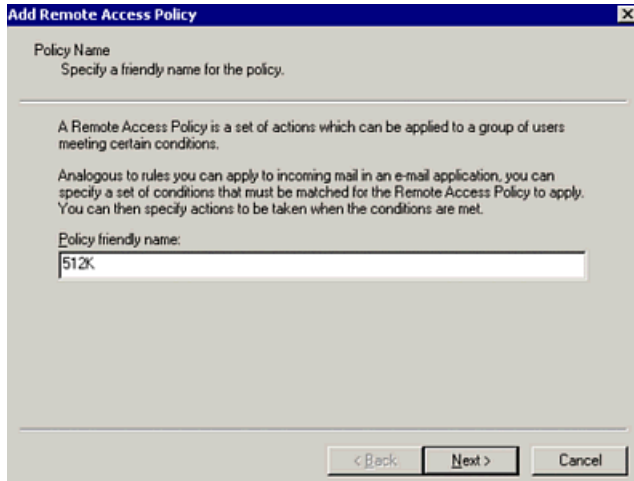


When a new user or Subscriber Unit is to be added, add the user to the Active Directory using the MAC address of its radio card as the Login ID, and make it a member of the group that corresponds to the bandwidth desired (in this case, we will be configuring for 512k). This makes more sense when you see the Internet Authentication Services (IAS) Remote Access policy configuration.

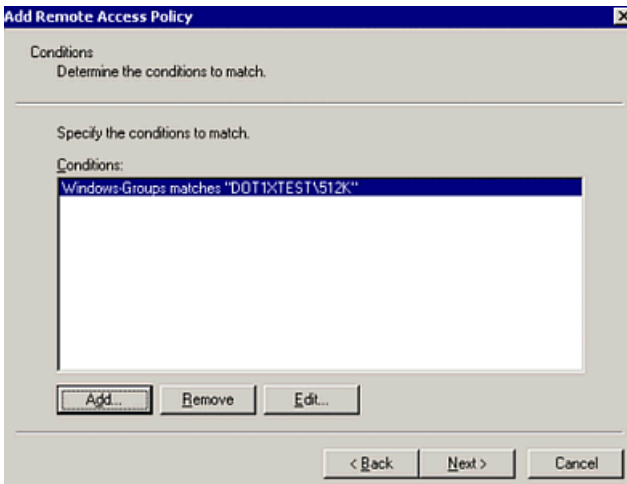
1. Start the Internet Authentication Service applet:



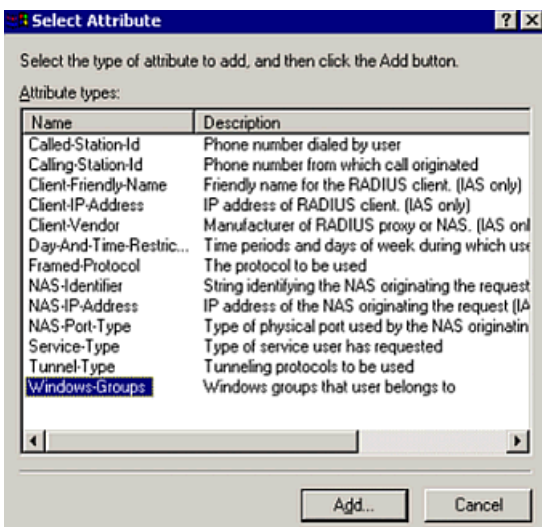
2. Highlight **Remote Access Policies**; right-click and select **new remote access policy**; the following window is displayed:



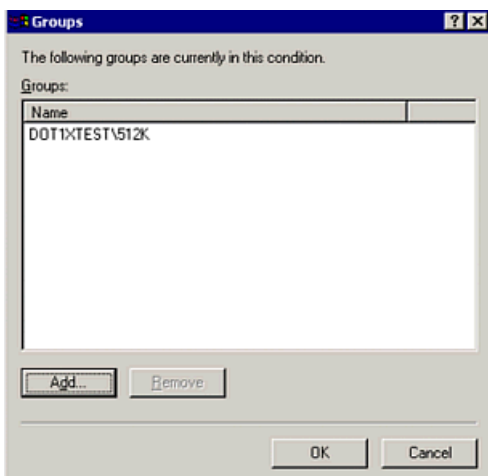
3. Enter **512K** as the name for this policy and click **Next**. Assuming that **dot1xtest** group already exists in Active Directory, the following window is displayed:



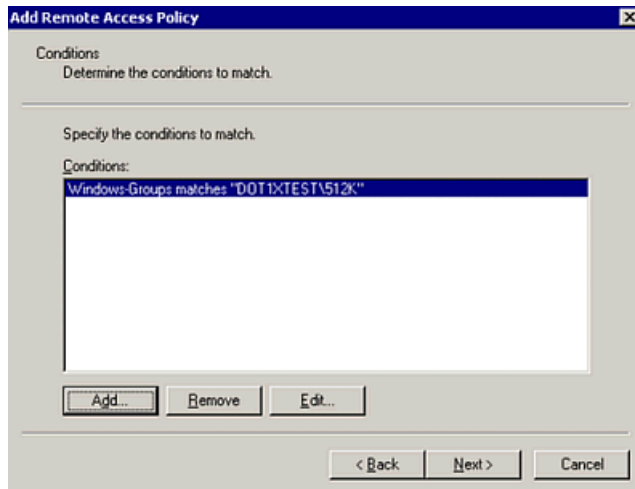
4. Click **Add**; the following window is displayed:



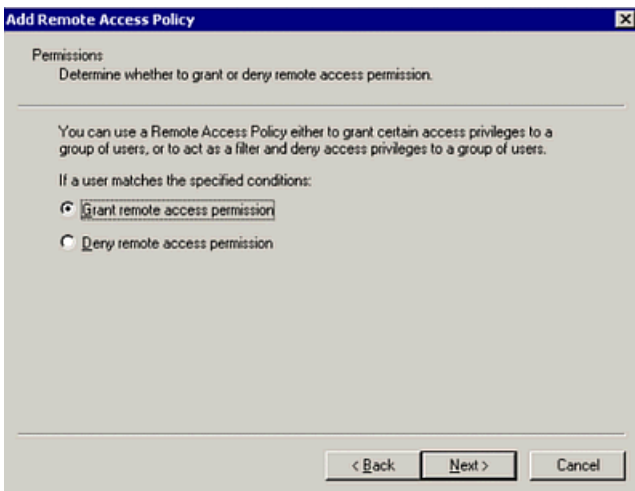
5. Select **Windows-Groups** and click **Add**; the following window is displayed:



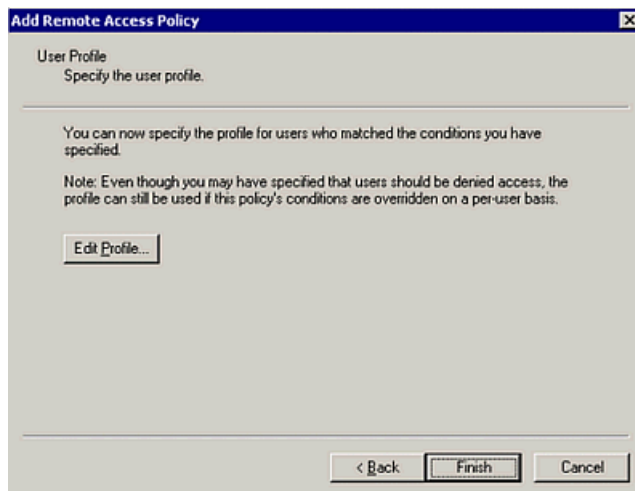
- Click **Add** and select the group that you want to associate with this new security policy. This is what “matches” the group created earlier with the security policy in IAS. Click **OK** and the following window is displayed:



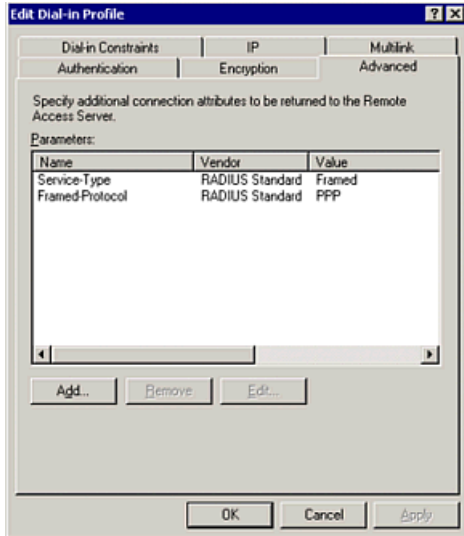
- Click **Next**; the following window is displayed:



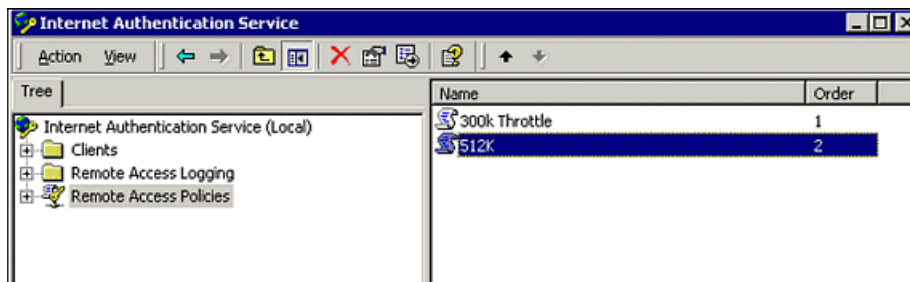
- Ensure that **Grant remote access** is selected (as this is the group to which we would like to grant permissions, and at 512k). Click **Next**; the following window is displayed:



9. Click **Edit Profile**; the following window is displayed:



10. At this point, you must add Vendor Specific values. Click the **Add** button to enter Proxim's vendor code values; the **RADIUS Attributes** window is displayed.
- Select **Vendor Specific RADIUS Standard**; the **Multivalued Attribute Information** window is displayed.
  - Select **Add** to get **Vendor Specific Attribute** Information.
  - Click the **Specify Network Access Server Vendor** radio button and enter **841** for Proxim code.
  - Click the **Yes. It conforms** radio button under the **Specify whether the attribute conforms to RADIUS RFC specification for vendor specific Attributes** area.
  - Click **Configure Attribute** to display the **Configure USA (RFC Compliant) values** window.
  - In the **Vendor Assigned Attribute number** area select either **(1)** for **Input/Uplink** or **(2)** for **Output/Downlink**.
  - For **Attribute Format** select **Decimal**.
  - For **Attribute value** select the Kbps value being tested, for example **64** for 64Kbps.
  - Select **OK** to save configuration.
  - Select **Apply to RADIUS Attributes configuration**.
  - Click **OK**; the following window is displayed:



Your configuration should be complete.

---

## Addition of Units to a Routed Network

The following describes how additional units can be added to a routed network:

1. Log into the BSU by placing its IP address into a Web browser address field.
2. When the Web interface is displayed, click on the **Configure** button.
3. Select the **System** tab and change the mode of operation from the drop down menu to **Routing**. The unit reconfigures itself to Routing mode without the need to click **OK**.
4. Click on the **Commands** button. Select the **Reboot** tab and click on **Reboot**.
5. Wait for the timer to count to zero and you are returned to the Web configuration automatically.
6. Click the **Configure** button. Select the **Network** tab.
7. In the **IP Configuration** sub-tab, you should see that each interface has an IP address. The Ethernet IP address should be the address the unit had previously. The wireless address is now configurable.

---

**Note:** *To make this work, ALL units must have wireless IPs in the same subnet. The default router address must be the IP address of the device that is to provide Internet services to the BSU.*

---

8. Click **OK**.
9. On the **RIP** tab, set **Advertise** and **Receive** drop down menus to RIPv2.
10. Click **OK**.
11. Click on the **Commands** button.
12. Select the **Reboot** tab; click **Reboot**.

We now move on to the SU. First, enable the SU for Routing mode:

13. Log into the SU by placing its IP address into a Web browser address field.
14. When the Web interface is displayed, click on the **Configure** button.
15. Select the **System** tab and change the mode of operation from the drop down menu to **Routing**. The unit reconfigures itself to Routing mode without the need to click **OK**.
16. Click on the **Commands** button. Select the **Reboot** tab and click on **Reboot**.
17. Wait for the timer to count to zero and you are returned to the Web configuration automatically.
18. Click the **Configure** button. Select the **Network** tab.
19. On the **Network** tab, you will see that its previous IP address is now the Ethernet Address and Wireless IP is now configurable. Set the Wireless IP to the same subnet as the BSU, and set the Ethernet IP to be compatible with the target site's subnet.

---

**Note:** *The default router's address must be the BSU's Ethernet IP address when the Internet connection is located there.*

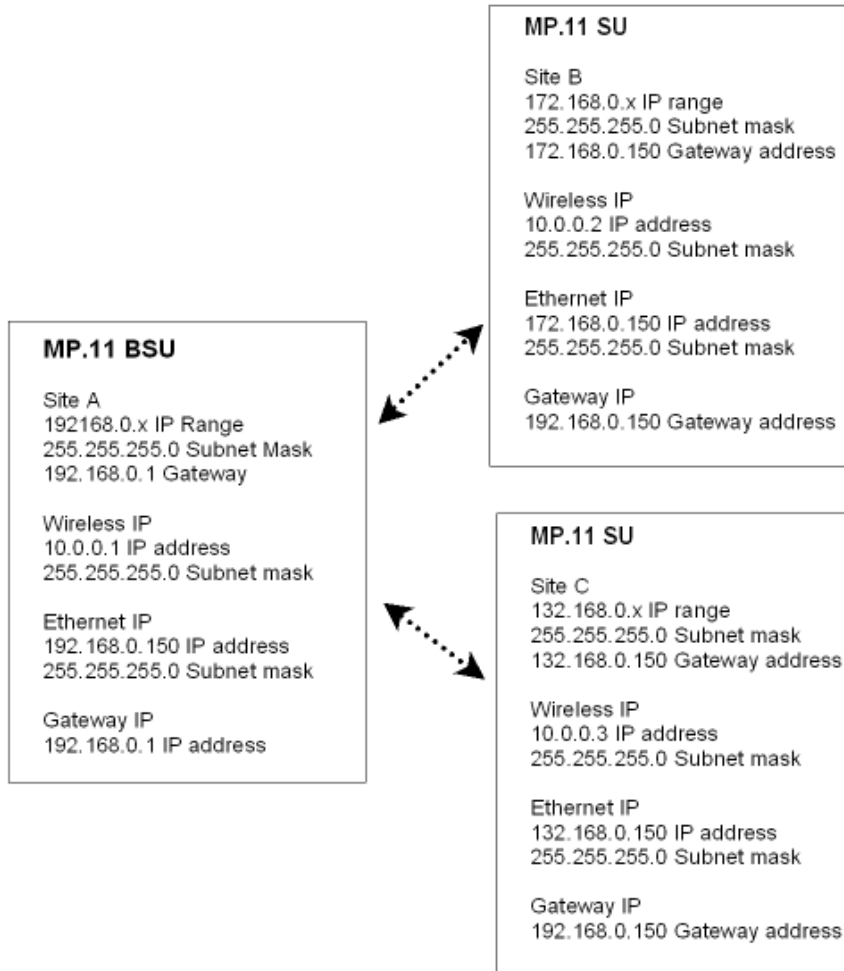
---

20. Click **OK**.
21. On the **RIP** tab, set **Advertise** and **Receive** dropdown menus to RIPv2.
22. Click **OK**.
23. Click on the **Commands** button.

24. Select the **Reboot** tab and click **Reboot**.

The SU should now be configured for routing mode. Repeat these steps for any additional units. For an example, see the following diagram, which shows the IP configuration of a BSU and SUs where the units will be routing different subnets at their target locations. RIPv2 is set for Advertise on all units.

The key to understanding how RIP builds the correct routes is in the Gateway's IP setting. The SU's gateway is the Ethernet IP address of the BSU. The BSU's gateway is the Internet source; that is, switch, router. The Clients at site B and C have their gateway set to the Ethernet IP address of their respective SU.



---

# Glossary

**Address Realm**

An address realm is a network domain in which the network addresses are uniquely assigned to entities such that datagrams can be routed to them.

**Antenna Beamwidth**

Antenna beamwidth is the peak-to-peak angle overlaying the maximum gain beam of the antenna at which its gain is reduced by 3 dB. Contrary to popular belief, the 3 dB gain beam-width of an antenna does not represent its interference beam-width, which is significantly wider. For example, a typical 2-foot parabolic antenna at 5.8 GHz has 28 dBi of gain, and a typical beam-width of 6 degrees. However, as an interference source, it radiates with 25 dBi of gain over a 6 degree area, 10 dBi of gain over a 32 degree area, and 2 dBi gain over a 170 degree area.

**Antenna Gain**

Antenna gain is the amount of increase in signal strength (in decibels) that results from an antenna concentrating its radiated signal into a given direction, when compared to the gain of a reference antenna. As antenna gain increases in a given direction, its radiated "beam-width" becomes narrower in one or more aspects.

**Application Level Gateway (ALG)**

An Application Level Gateway is an application-specific translation agent that provides the required transparency for an application running on a host in a private network to connect to its counterpart running on a host in the public network. The NAT feature requires an ALG to support certain applications.

**ARP**

The Address Resolution Protocol (ARP) is intended to find the MAC address belonging to an IP address.

**Authentication Method**

The process the unit uses to decide whether a station that wants to register is allowed or not. IEEE 802.11 specifies two forms of authentication: open system and shared key; WOPR only supports shared key because of security constraints.

**Authentication Server "Shared Secret"**

This is a kind of password shared between the unit and the RADIUS authentication server. This password is used to encrypt important data exchanged between the unit and the RADIUS server

**Authentication Server Authentication Port**

This is a UDP port number (default is 1812), which is used to connect to the authentication server for obtaining authentication information.

**Auto-Negotiation**

A signaling method that lets each node define its operational mode and detect the operational mode of the adjacent node. Auto-negotiation can be used in dual-function 10/100 Mbps Ethernet adapters. The process happens out-of-band with no loss of network throughput.

**Backbone**

The central part of a network; the backbone network connects all remote and sub networks to each other and to the central infrastructure (such as the mail server, Internet gateway, and so on).

**Base**

If an interface is running in Outdoor mode (WOPR), it is either a base or a subscriber interface. A base interface controls the communication on the channel and is located in the central part of the network cell. Multiple SUs can connect to one base; two bases cannot communicate with each other.

**Broadcast Storm**

A broadcast storm is a large series of broadcast packets (most often caused by wrong network configuration) that severely impact the network performance.

**Client IP Address Pool**

This is a pool of IP addresses from which the unit can assign IP addresses to clients, which perform a DHCP Request.

**Configuration Files**

A configuration file contains the unit configuration details. Configuration items include among others the IP address and other network-specific values. Configuration files may be uploaded to a TFTP server for backup and downloaded into the unit for restoring the configuration.

**DHCP Relay Agent**

A feature of the unit that intercepts DHCP requests from clients and forwards them to a DHCP server. For the client, the DHCP Relay Agent of the unit functions like a DHCP server. This enables DHCP requests to pass router boundaries; for example, it is not required to have a DHCP server on every IP subnet.

**Domain Name Server (DNS)**

A domain name server is an Internet service that translates domain names into IP addresses. For example, [www.ietf.org](http://www.ietf.org) is translated into 4.17.168.6.

**Download**

Downloading a file means copying a file from a remote server to a device or host. In case of the unit downloading means transferring a file from a TFTP server to the unit.

**Downstream**

Downstream means a data stream from the central part of the network to the end user. See also upstream.

**Dynamic Host Configuration Protocol**

Dynamic Host Configuration Protocol (DHCP) is a method to dynamically assign IP addresses. If DHCP is enabled, the device or computer broadcasts a request that is answered by a DHCP Server.

**Earth Ground**

A proper earth ground is a conductive attachment point that presents very low impedance, path to earth ground that has broadband characteristics. The power utility ground does not necessarily constitute (although in some cases it may) a proper earth ground for communication systems, since it is only intended to be a safety return path for the 60 Hz commercial AC power system.

**Encryption**

Encryption is a means of coding data with a key before sending it across a network. The same key must be used to decode the information at the receiver. This way prevents unauthorized access to the data that is sent across the network.

**Ethernet**

Ethernet is the most widely installed Local Area Network (LAN) technology. The unit supports both 10 and 100 Mbps and half and full duplex.

**Gateway**

A gateway is network device that connects multiple (IP) networks to each other. A gateway can perform protocol conversion.

**Group**

A group is a logical collection of network parameters. For example, the System Group is composed of several parameters and tables giving system information of the unit. All items for a group are grouped under one tab of the Web Interface and start with the same prefix for the command line interface.

**HTTP**

Hypertext Transfer Protocol (HTTP) is the protocol to transport Web pages. When you access the Internet with your browser, the HTTP protocol is used for data transport (<http://www.Tsunamiwireless.com>). When you access the unit using the Web Interface, HTTP is used to transport the information.

**ICMP**

Internet Control Message Protocol (ICMP) is used by computers and devices to report errors encountered during processing packets, and to perform other IP-layer functions, such as diagnostics ('ping').

**Image**

The image is the binary executable of the embedded unit software. To update the unit you must download a new image file.

**IP Address**

A unique numerical address of a computer attached to the Internet or Intranet. An IP (Internet Protocol) address consists of a network part and part for a host (computer) number. An IP address is represented by four numbers in the range 0 - 255 separated by dots: for example 10.0.10.1 and 172.21.43.214. See also subnet mask.

**LAN**

A Local Area Network (LAN) is a network of limited size to which computers and devices can connect so that they can communicate with each other.

**License file**

A license file is used to enable certain features of the unit. The unit already has a license file when it is shipped. When more features become available, you can purchase a license file and download it to the unit to enable these additional features.

**MAC**

Media Access Control.

**MAC Address**

A MAC (Media Access Control) address is a globally unique network device address, which is hardware bound. It used to identify a network device in a LAN. A MAC address is represented by six two-digit hexadecimal numbers (0 - 9 and A - F) separated by colons: for example 00:02:2D:47:1F:71 and 00:D0:AB:00:01:AC.

**Management Information Block (MIB)**

A Management Information Block (MIB) is a formal description of a set of network objects that can be managed with the Simple Network Management Protocol (SNMP). A MIB can be loaded by a management application so that it knows the unit specific objects.

**Media Independent Interface (MII)**

A standard interface between the MAC layer and any of the three physical layers (100 Base-TX, 100 Base-T4, and 100 Base-FX) for Fast Ethernet, similar to the AUI interface for traditional Ethernet.

**Network Address Translation**

Network Address Translation is a method by which IP addresses are mapped from one address realm to another, providing transparent routing to end hosts.

**Network Mask**

See subnet mask.

**Parameter**

A parameter is fundamental value that can be displayed and changed. For example, the unit must have a unique IP address and the PC Cards must know which channels to use. You can view and change parameters with the Web Interface, command line interface and SNMP.

**Password**

The unit is password protected. To access the unit you need to enter a password before you can view or change its settings. The default password is 'public'.

**Ping**

Ping is a basic Internet program that lets you verify if a particular computer or device with a certain IP address is reachable. If the computer or device receives the ping packet, it responds which gives the ping program the opportunity to display the round-trip time.

**Remote**

A remote is a base or a subscriber interface. For a base interface, the number of remotes is the number of SUs registered; for a subscriber interface, there is only one remote, which is the base.

**RIP**

Routing Information Protocol (RIP) is used between routers to update routing information so that a router automatically 'knows' which port to use for a certain destination IP address.

**Router**

Routers forward packets from one network to another based on routing information. A router uses a dynamic routing protocol like RIP or static routes to base its forwarding decision on.

**ScanTool**

A computer program that can be used to retrieve or set the IP address of a locally connected unit.

**Simple Network Management Protocol (SNMP)**

A protocol used for the communication between a network management application and the devices it is managing. The network management application is called the SNMP manager; the devices it manages have implemented SNMP agents. Not only the unit but also almost every network device contains a SNMP agent. The manageable objects of a device are arranged in a Management Information Base, also called MIB. The Simple Network Management Protocol (SNMP) allows managers and agents to communicate for accessing these objects.

**Spanning Tree Protocol (STP)**

The Spanning Tree Protocol (STP) can be used to create redundant networks ("hot standby") and to prevent loops. If enabled, spanning tree prevents loops by disabling redundant links; if a link fails, it can automatically enable a backup link.

**STP**

Shielded Twisted Pair

**Subnet Mask**

A subnet mask is a bit mask that defines which part of an IP address is used for the network part and which part for a host (computer) number. A subnet mask is like an IP address represented by four numbers in the range 0 - 255 separated by dots. When the IP address 172.17.23.14 has a subnet mask of 255.255.255.0, the network part is 172.17.23 of the host number is 14. See also IP address.

**Subscriber Unit**

If an interface is running in outdoor mode (WORP), it is either a base or a subscriber interface. Subscriber interface behavior is controlled by the base to which it is registered. SUs are located in the remote locations of a network cell. Multiple SUs can connect to one base; two SUs cannot communicate with each other. See also WORP and base.

### **System Gain**

Radio system gain is the sum of transmitter gain plus its corresponding receiver gain. For example, a transmitter having a power output of 20 dBm combined with a receiver having a threshold sensitivity of – 80 dBm results in a radio system gain of 100 dB.

### **Antenna System Gain**

Antenna system gain is the net (combined) gain of a transmitting antenna plus the gain of a receiving antenna, minus the loss of the cables that connect the transmitter and receiver to their respective antennas. For example, at 5.8 GHz, a two-foot dish antenna has a nominal gain of 28 dBi, and low-loss cable has a loss of 6 dB/100 feet. Therefore the antenna system gain for a pair of two-foot dishes and 100 feet of low-loss cable would be 50 dB (28 + 28 – 6).

### **Total System Gain**

Total system gain is the sum of antenna system gain plus radio system gain.

### **Net System Gain**

Net system gain is amount of system gain left after the effect of free-space and all other propagation losses have been subtracted from the total system gain. The net system gain (if a positive number) is also referred to as Fade Margin.

### **System Ground**

The purpose of a system ground is to provide a low impedance path to ground for electronic noise, energy from lightning strikes, and potential “differences of potential” between the different pieces of equipment at an installation site. Electronic noise can range in frequency from just above DC to well over 100 MHz. The energy in lightning is distributed across a frequency range of 10 KHz to well over 100 MHz. Therefore, an effective ground path for this “broad band” of energy has to be much wider than the “narrow band” 60 Hz AC power utility ground requirements.

### **Table**

Tables hold parameters for several related items. For example, you can add several potential managers to the SNMP IP access table. Tables can be displayed using the Web Interface, command line interface, and SNMP.

### **Topology**

Topology is the physical layout of network components (cable, stations, gateways, hubs, and so on).

### **Transparent Routing**

Transparent routing refers to routing a datagram between disparate address realms, by modifying address contents in the IP header to be valid in the address realm into which the datagram is routed.

### **Trap**

A trap is used within SNMP to report an unexpected or unallowable condition.

### **Trivial File Transfer Protocol (TFTP)**

Trivial File Transfer Protocol (TFTP) is a lightweight protocol for transferring files that is like a simple form of File Transfer Protocol (FTP). A TFTP client is implemented on the unit; using the upload and download commands, the unit can respectively copy a file to or from a TFTP server. TFTP server software is provided on the product CD-ROM.

### **Upload**

Uploading a file means copying a file from a network device to a remote server. In case of the unit uploading means transferring a file from the unit to a TFTP server. See also download.

### **Upstream**

Upstream means a data stream from the end users to the central part of the network. See also downstream.

### **UTP**

Unshielded Twisted Pair

### **WEP**

The Wired Equivalent Privacy (WEP) algorithm is the standard encryption method used to protect wireless communication from eavesdropping.

### **WORP**

The Wireless Outdoor Router Protocol (WORP) was designed to optimize long distance links and multipoint networks with Hidden Node effect to eliminate collisions and loss of bandwidth.