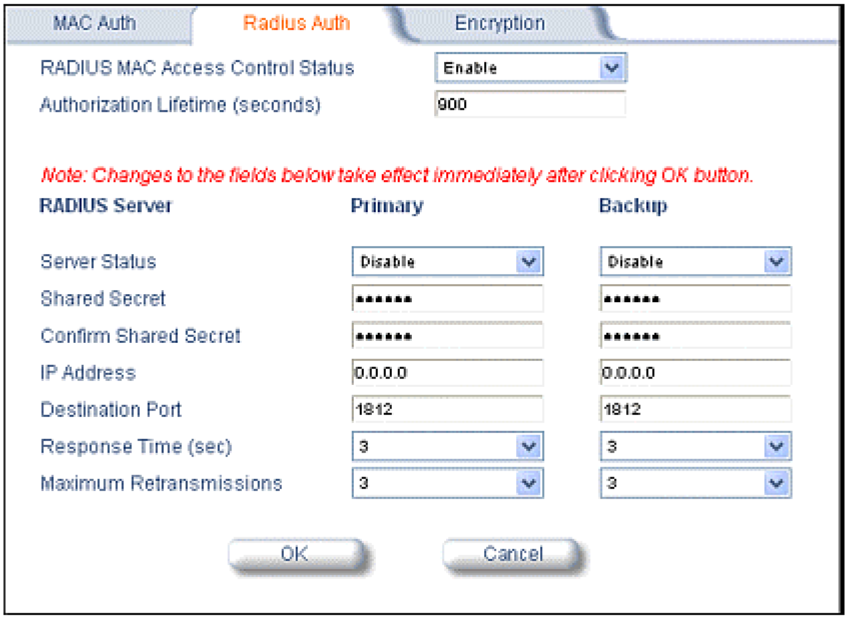
RADIUS Authentication

Click the **Configure** button, the **Security** tab, and the **Radius Auth** sub-tab to set the IP address of the RADIUS server containing the central list of MAC addresses allowed to access the network.



RADIUS MAC Access Control Status	Enable
Authorization Lifetime (seconds)	900

Note: Changes to the fields below take effect immediately after clicking OK button.

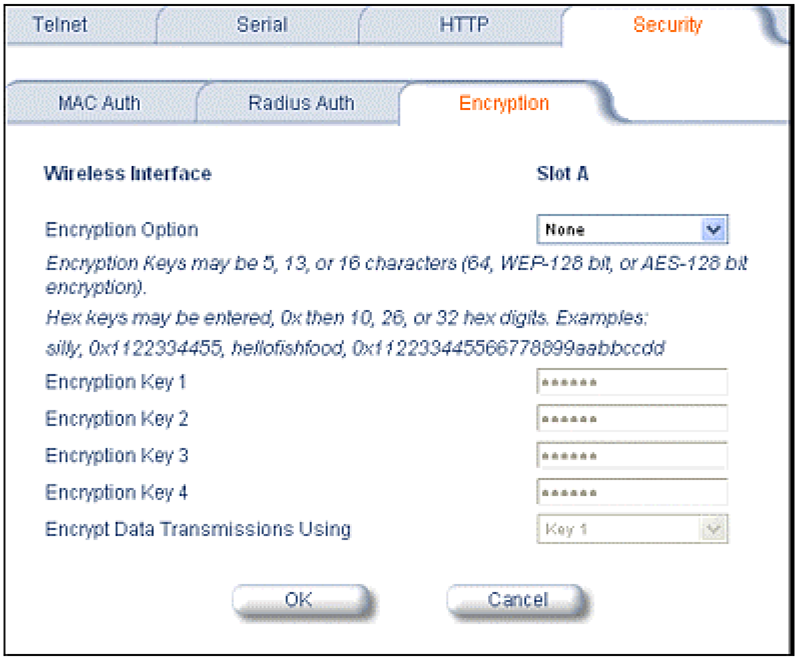
RADIUS Server	Primary	Backup
Server Status	Disable	Disable
Shared Secret	******	******
Confirm Shared Secret	******	******
IP Address	0.0.0.0	0.0.0.0
Destination Port	1812	1812
Response Time (sec)	3	3
Maximum Retransmissions	3	3

In large networks with multiple MP.11/a devices, you can maintain a list of MAC addresses on a centralized location using a RADIUS authentication server that grants or denies access. If you use this kind of authentication, you must specify at least the primary RADIUS server. The backup RADIUS server is optional.

Encryption

You can protect the wireless data link by using encryption. Encryption keys can be 5 (64-bit), 13 (WEP 128-bit), or 16 (AES 128-bit) characters in length. Both ends of the wireless data link must use the same parameter values. *Advanced Encryption Standard (AES) encryption is supported on the MP.11a only.*

Click the **Configure** button, the **Security** tab, and the **Encryption** sub-tab to set encryption keys for the data transmitted and received by the MP.11/a. Note that all devices in one network must use the same encryption parameters to communicate to each other.



Wireless Interface Slot A

Encryption Option: None

Encryption Keys may be 5, 13, or 16 characters (64, WEP-128 bit, or AES-128 bit encryption).

Hex keys may be entered, 0x then 10, 26, or 32 hex digits. Examples:

silly, 0x1122334455, hellofishfood, 0x112233445566778899aabbccdd

Encryption Key 1: ******

Encryption Key 2: ******

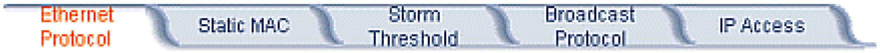
Encryption Key 3: ******

Encryption Key 4: ******

Encrypt Data Transmissions Using: Key 1

10) Filtering

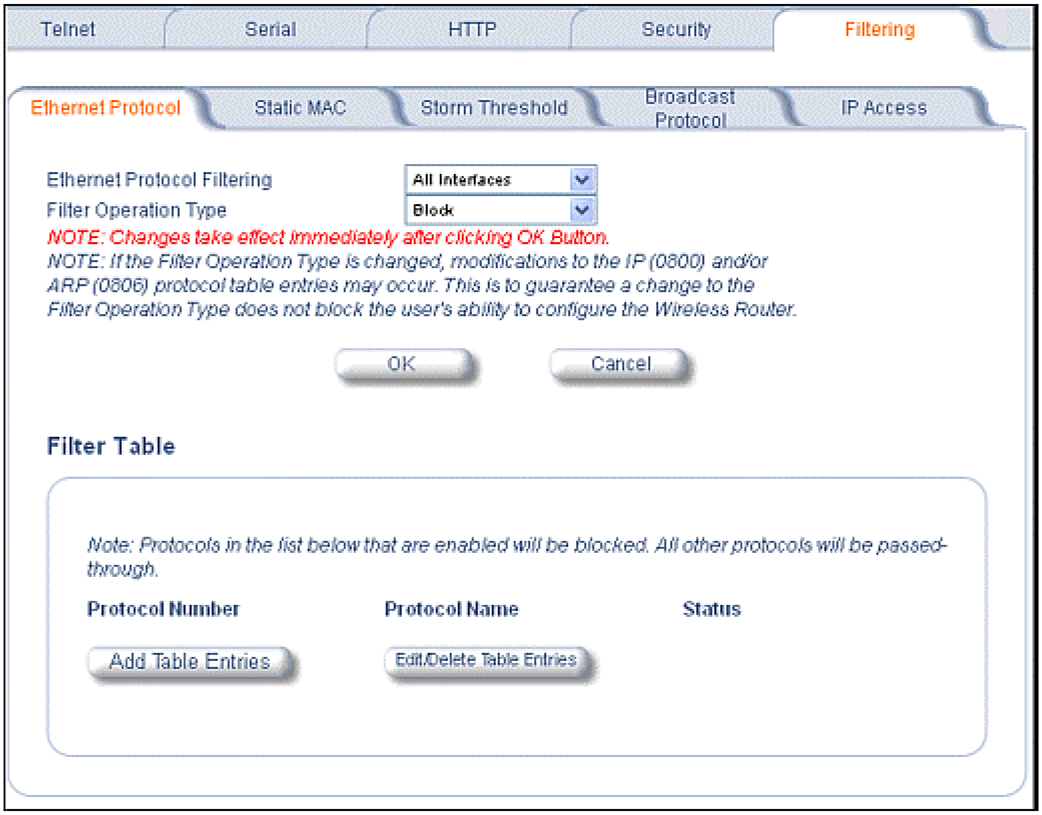
Click the **Configure** button and the **Filtering** tab to configure packet filtering. Packet filtering can be used to control and optimize network performance. Filtering sub-tabs are as follows:



Ethernet Protocol

The Ethernet Protocol Filter blocks or forwards packets based upon the Ethernet protocols they support. Click the **Configure** button, the **Filtering** tab, and the **Ethernet Protocol Filter** sub-tab to enable or disable certain protocols in the table. Entries can be selected from a drop-down box.

- To add an entry to the table, click **Add Table Entries**, select the protocol name from the drop-down box and click the **Add** button.
- To edit or delete table entries, click **Edit/Delete Table Entries**, make your changes or deletions, and click **OK**.



Ethernet Protocol Filtering: All Interfaces

Filter Operation Type: Block

NOTE: Changes take effect immediately after clicking OK Button.

NOTE: If the Filter Operation Type is changed, modifications to the IP (0800) and/or ARP (0806) protocol table entries may occur. This is to guarantee a change to the Filter Operation Type does not block the user's ability to configure the Wireless Router.

Filter Table

Note: Protocols in the list below that are enabled will be blocked. All other protocols will be passed-through.

Protocol Number	Protocol Name	Status

Ethernet Protocol Filtering

Blocks or forwards packets based upon the Ethernet protocols they support:

Ethernet: Packets are examined at the Ethernet interface.

Wireless: Packets are examined at the Wireless interface.

All Interfaces: Packets are examined at both interfaces.

Disabled: The filter is not used.

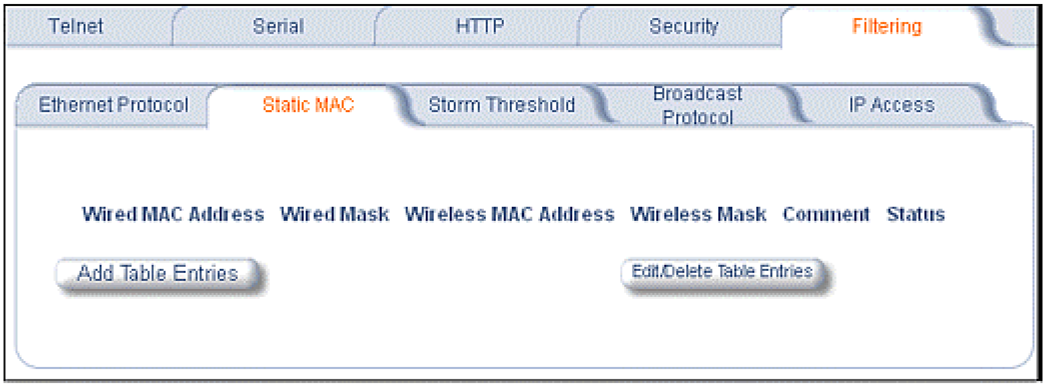
Filter Operation Type

Passthru: Only the enabled Ethernet Protocols listed in the Filter Table pass through the bridge.

Block: the Bridge blocks enabled Ethernet Protocols listed in the Filter Table.

Static MAC Pair Filtering

The Static MAC Address Filter optimizes the performance of a wireless (and wired) network. Click the **Configure** button, the **Filtering** tab, and the **Static MAC Pair Filtering** sub-tab to access the Static MAC Address Filter.



The filter is an advanced feature that lets you limit the data traffic between two specific devices (or between groups of devices based upon MAC addresses) through the wireless interface of the MP.11/a. For example, if you have a server on your network with which you do not want wireless clients to communicate, you can set up a **Static MAC Filter** to block traffic between these devices. However, note that this is an advanced filter and it may be easier to control wireless traffic through other filter options, such as **Protocol Filtering**.

The entry is enabled automatically when saved. To edit an entry, click **Edit**. To disable or remove an entry, click **Edit** and change the **Status** field from **Enable** to **Disable** or **Delete**.

Wired MAC Address

Enter the MAC address of the device on the Ethernet network that you want to prevent from communicating with a device on the wireless network.

Wired Mask

Enter the appropriate bit mask to specify the range of MAC addresses to which this filter is to apply. To specify only the single MAC address you entered in the Wired MAC Address filter, enter FF:FF:FF:FF:FF:FF (all zeroes).

Wireless MAC Address

Enter the MAC address of the wireless device that you want to prevent from communicating with a device on the wired network.

Wireless Mask

Enter the appropriate bit mask to specify the range of MAC addresses to which this filter is to apply. To specify only the single MAC address you entered in the Wireless MAC Address file, enter FF:FF:FF:FF:FF:FF (all zeroes).

Comment

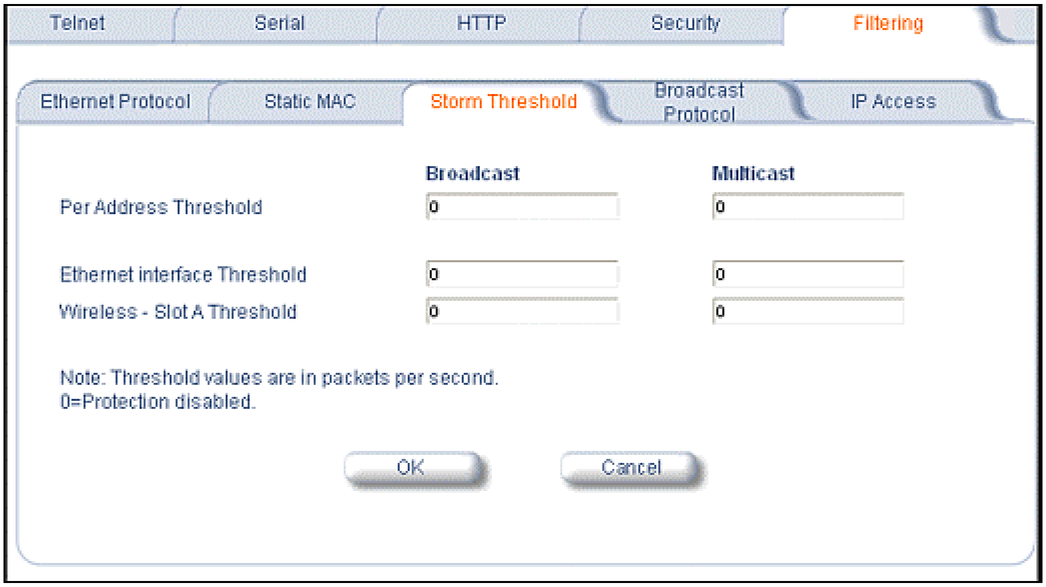
Enter related information.

Status

The Status field can show **Enable**, **Disable**, or **Delete**.

Storm Threshold

Click the **Configure** button, the **Filtering** tab, and the **Storm Threshold** sub-tab to prevent broadcast/multicast overload.



	Broadcast	Multicast
Per Address Threshold	0	0
Ethernet interface Threshold	0	0
Wireless - Slot A Threshold	0	0

Note: Threshold values are in packets per second.
0=Protection disabled.

Storm Threshold is an advanced **Bridge** setup option that you can use to protect the network against data overload by specifying:

- A maximum number of frames per second as received from a single network device (identified by its MAC address).
- An absolute maximum number of messages per port.

The **Storm Threshold** parameters let you specify a set of thresholds for each port of the MP.11/a, identifying separate values for the number of broadcast messages per second and multicast messages per second.

When the number of frames for a port or identified station exceeds the maximum value per second, the MP.11/a ignores all subsequent messages issued by the particular network device, or ignores all messages of that type.

Per Address Threshold

Enter the maximum allowed number of packets per second.

Ethernet Threshold

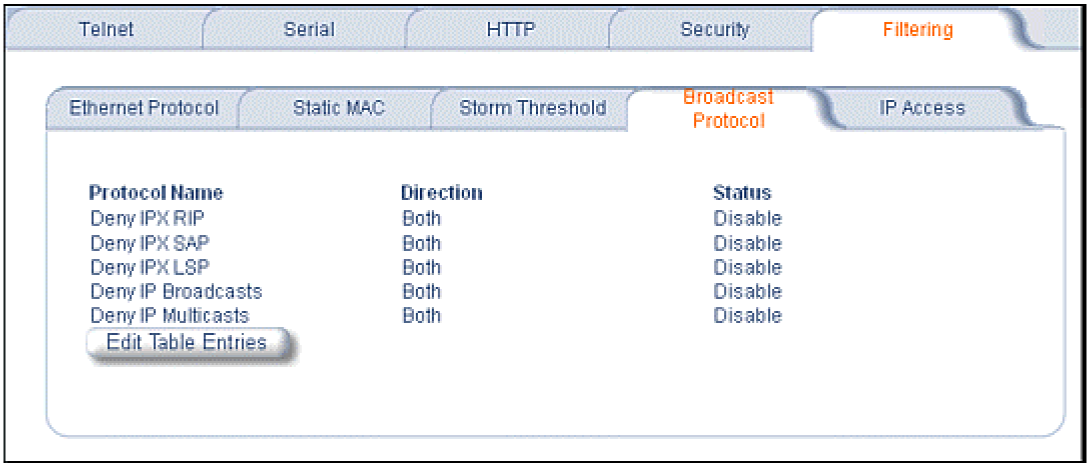
Enter the maximum allowed number of packets per second.

Wireless Threshold

Enter the maximum allowed number of packets per second.

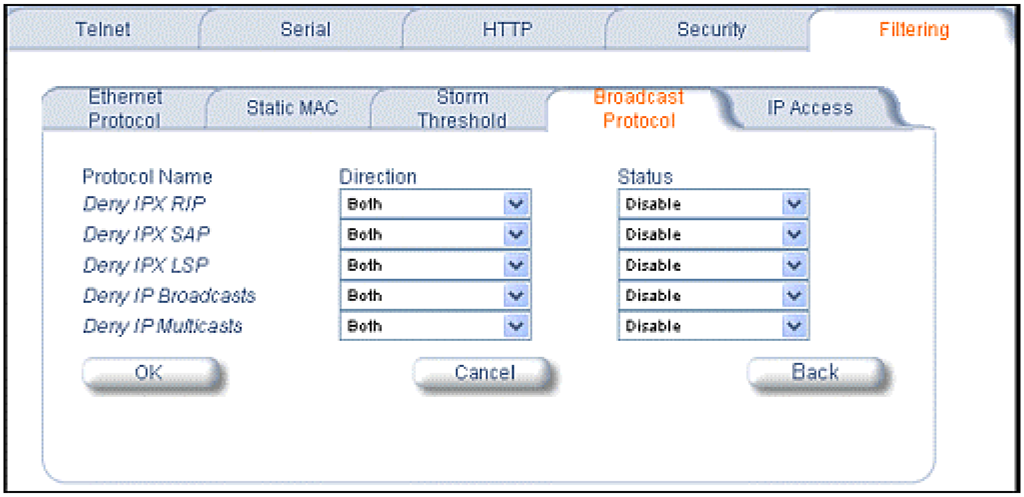
Broadcast Protocol Filtering

Click the **Configure** button, the **Filtering** tab, and the **Broadcast Protocol Filtering** sub-tab to deny specific IP broadcast, IPX broadcast, and multicast traffic.



Protocol Name	Direction	Status
Deny IPX RIP	Both	Disable
Deny IPX SAP	Both	Disable
Deny IPX LSP	Both	Disable
Deny IP Broadcasts	Both	Disable
Deny IP Multicasts	Both	Disable

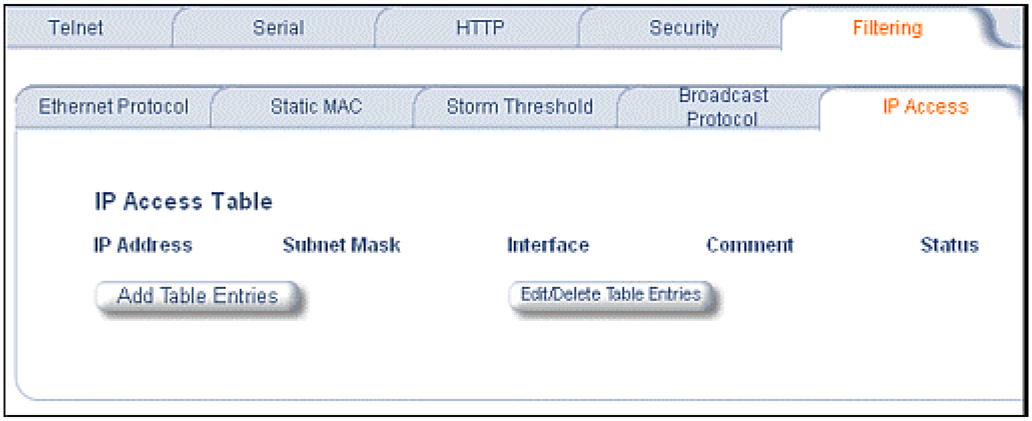
Click the **Edit Table Entries** button to display and editable window such as the following. You can configure whether this traffic must be blocked for Ethernet to wireless, wireless to Ethernet, or both.



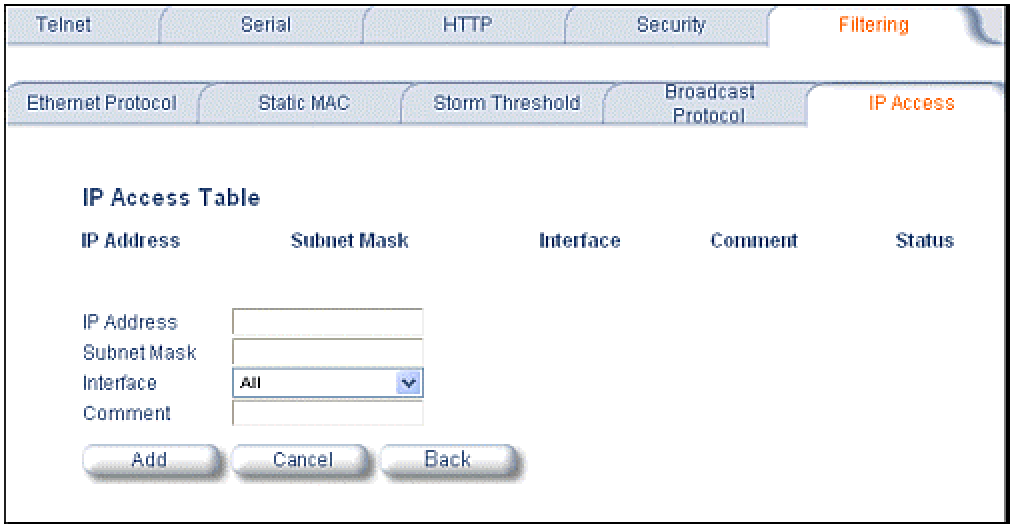
Protocol Name	Direction	Status
Deny IPX RIP	Both	Disable
Deny IPX SAP	Both	Disable
Deny IPX LSP	Both	Disable
Deny IP Broadcasts	Both	Disable
Deny IP Multicasts	Both	Disable

IP Access Table

Entries in this table show which wireless stations are allowed to use SNMP, HTTP, and telnet management interfaces.



To add an entry, click the **Add Table Entries** button, specify the IP address and mask of the wireless stations to which you want to grant access, and click **Add**.



Interface All

For example, **172.17.23.0/255.255.255.0** allows access from all wireless stations with an IP address in the 172.17.23.xxx range.

Ensure that the wireless station you use is the first entry in the table.

ADDITIONAL INTERFACE INFORMATION

Dynamic Frequency Selection (Tsunami MP.11a only)

With Tsunami MP.11a units, Dynamic Frequency Selection (DFS) is enabled automatically based upon the country you select. You can tell DFS is in use because the frequency selection drop-down box on the **Interfaces** page is grayed out (click the **Configure** button and the **Interfaces** tab); it displays only the DFS-selected frequency. You cannot select a preferred frequency or band in which to operate. DFS scans all available frequencies in all available bands to select the operating frequency automatically.

To comply with your country's regulations, change the DFS selection to specify your country. You can do this by logging into the unit, clicking the **Configure** button and selecting the **System** tab. There is a drop-down box labeled "Country" with all available countries from which to select. Choose your country, configure the unit as required, and reboot for the settings to take effect.

Note: Because DFS must scan for radar and interference on multiple channels, you must allow a sufficient amount of time for the units to start up. This is considerably longer than when the unit is not using DFS. Startup time is usually within two to three minutes if no radar is detected. If radar is detected, the unit may reboot multiple times before it becomes fully operational and can take much longer to start. This is expected behavior.

DFS Requirement

Dynamic Frequency Selection (DFS) is required in ETSI countries and is enabled automatically when you select a country with a regulatory domain that requires DFS. DFS is required in ETSI countries for two purposes.

1. *Radar avoidance both at startup and while operational*. To meet these requirements, the Tsunami MP.11a BSU scans available frequencies at startup for the presence of a radar signal on all available frequencies; it does not use any frequency in which radar signals are detected. Once fully operational on a frequency, the BSU actively monitors the occupied frequency for radar interference. If radar interference is detected, the BSU logs a message and reboots to find a new frequency free of interference.

   Understand that radar detection is performed only by the BSU and not by the SU. When an SU is set to a country in which DFS is used, it scans all available channels upon startup looking for a BSU that best matches its connection criteria (such as **Base Station System Name**, **Network Name**, and **Shared Secret**). The SU connects to the BSU automatically on whatever frequency the BSU has selected. Because of this procedure, it is best to set up the BSU and have it fully operational before installing the SU, although this is not required. If a BSU reboots because of radar interference, the SU loses its WORP link and reboots to rescan available frequencies for an active BSU.

2. *Guarantee the efficient use of available frequencies by all devices in a certain area*. To meet this requirement, the BSU scans each available frequency upon startup and selects a frequency based upon the least amount of noise and interference detected. This lets multiple devices operate in the same area with limited interference. This procedure is done only at startup; if another non-radar device comes up on the same frequency, the BSU does not detect this or reboot because of it. It is expected that other devices using these frequencies also are in compliance with country regulations, so this should not happen.

Wireless Outdoor Router Protocol

The Wireless Outdoor Router Protocol (WORP) is a polling algorithm designed for wireless outdoor networks. WORP takes care of the performance degradation incurred by the so-called “hidden-node” problem, which can occur when standards-based 802.11b wireless LAN technology is used for outdoor building-to-building connectivity. In this situation, when multiple radios send an RTS, if another radio is transmitting, it corrupts all data being sent, degrading overall performance. The WORP polling algorithm ensures that these collisions cannot occur, which increases the performance of the overall network significantly.

WORP dynamically adapts to the number of satellites that are active on the network and the amount of data they have queued to send.

Satellite Density

The **Satellite Density** setting is a valuable feature for achieving maximum bandwidth in a wireless network. It influences the receive sensitivity of the radio interface. This feature improves operation in environments with a high noise level. Reducing the sensitivity of the radio enables unwanted “noise” to be filtered out. (It disappears under the threshold.)

You can configure the **Satellite Density** to be **Large**, **Medium**, **Small**, **Mini**, or **Micro**. The default value for this setting is **Large**. The smaller settings are appropriate for high noise environments; a setting of **Large** would be for a low noise environment.

A long distance link may have difficulty maintaining a connection with a small density setting because the wanted signal can disappear under the threshold. Consider both noise level and distance between the peers in a link when configuring this setting. The threshold should be chosen higher than the noise level, but sufficiently below the signal level. A safe value is 10 dB below the present signal strength.

If the Signal-to-Noise Ratio (SNR) is not sufficient, a lower data rate selection may be necessary, or use of antennas with higher gain to increase the margin between wanted and unwanted signals. In a point-to-multipoint configuration, the Base should have a density setting suitable for all of its registered Satellites, especially the ones with the lowest signal levels (longest links).

Take care when configuring a remote interface; check the available signal level first, using Remote Link Test.

Warning!

When the remote interface accidentally is set at too small a value and communication is lost, it cannot be reconfigured remotely and a local action is required to bring the communication back. Therefore, the best place to experiment with the level is at the unit that can be managed without going through the link; if the link is lost, the setting can be adjusted to the correct level to bring the link back.

To set the Satellite Density, click the **Configure** button, then the **Interfaces** tab and the **Wireless** sub-tab. Make your density selection from the drop-down menu. This setting requires a reboot of the unit.

Sensitivity threshold settings related to the density settings are:

Satellite Density	Large	Medium	Small	Mini	Micro
Receive Sensitivity Threshold	-99 dBm	-90 dBm	-85 dBm	-72 dBm	-66 dBm
Defer Threshold	-95 dBm	-85 dBm	-75 dBm	-62 dBm	-56 dBm

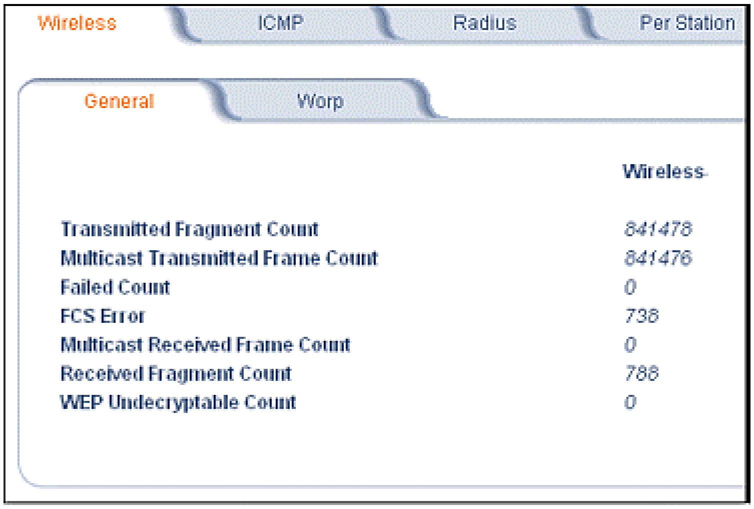
MONITOR

Use this section of the interface to obtain detailed information about the settings and performance of the MP.11/a. There are 10 tabs in the **Monitor** section.

1) Wireless

General

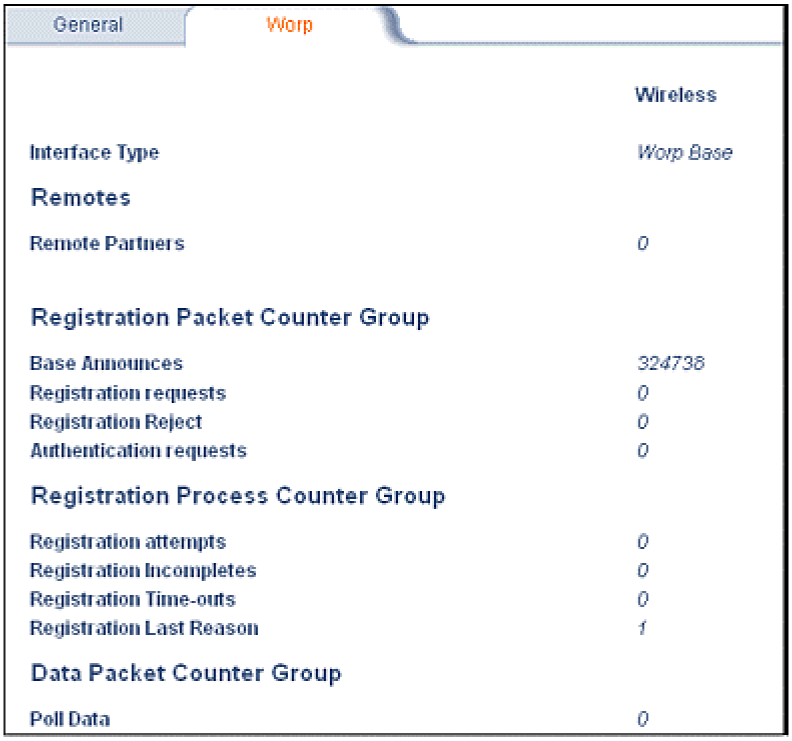
Click the **Monitor** button and the **General** tab to monitor the general performance of the wireless interface.



	Wireless
Transmitted Fragment Count	841478
Multicast Transmitted Frame Count	841476
Failed Count	0
FCS Error	738
Multicast Received Frame Count	0
Received Fragment Count	788
WEP Undecryptable Count	0

WORP

Click the **Monitor** button and the **WORP** tab to monitor the performance of the WORP Base or WORP Satellite interfaces.



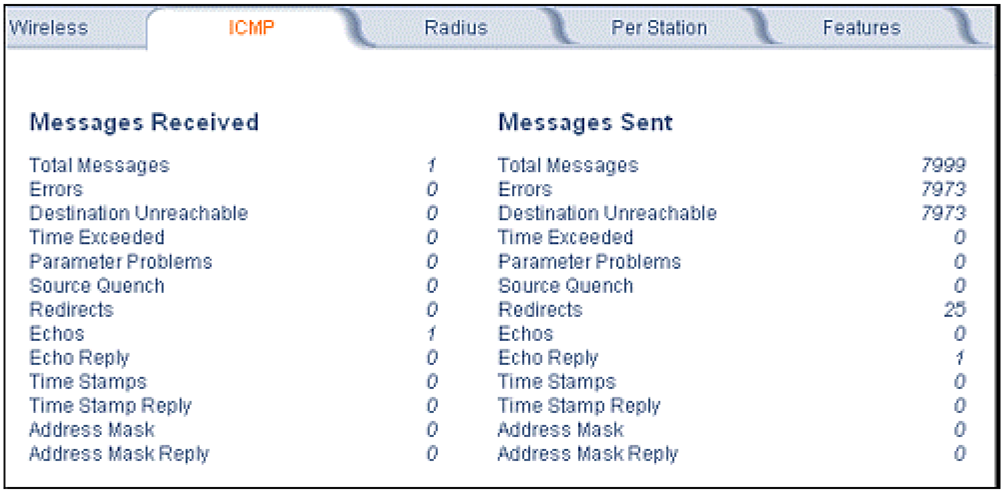
	Wireless
Interface Type	*Worp Base*
Remotes	
Remote Partners	*0*
Registration Packet Counter Group	
Base Announces	*324738*
Registration requests	*0*
Registration Reject	*0*
Authentication requests	*0*
Registration Process Counter Group	
Registration attempts	*0*
Registration Incompletes	*0*
Registration Time-outs	*0*
Registration Last Reason	*1*
Data Packet Counter Group	
Poll Data	*0*

Possible values for the **Registration Last Reason** field are as follows:

1 = Successful registration
2 = Maximum number of satellites reached
3 = Authentication failure
4 = Reserved for future use
5 = No response from satellite within the Registration Timeout Period
6 = Reserved for future use

2) ICMP

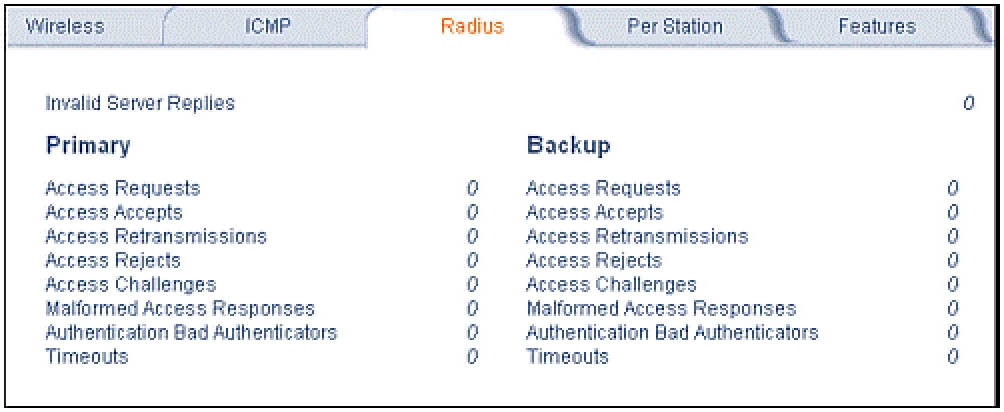
Click the **Monitor** button and the **ICMP** tab to view the number of ICMP messages send and received by the MP.11/a. It includes **ping**, **route**, and **host unreachable** messages.



Messages Received		Messages Sent	
Total Messages	1	Total Messages	7999
Errors	0	Errors	7973
Destination Unreachable	0	Destination Unreachable	7973
Time Exceeded	0	Time Exceeded	0
Parameter Problems	0	Parameter Problems	0
Source Quench	0	Source Quench	0
Redirects	0	Redirects	25
Echos	1	Echos	0
Echo Reply	0	Echo Reply	1
Time Stamps	0	Time Stamps	0
Time Stamp Reply	0	Time Stamp Reply	0
Address Mask	0	Address Mask	0
Address Mask Reply	0	Address Mask Reply	0

3) Radius

Click the **Monitor** button and the **Radius** tab to view information about the traffic exchanged with a RADIUS server.

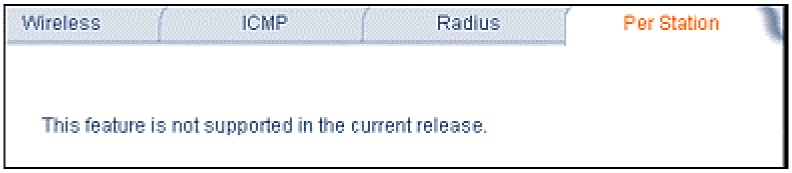


Invalid Server Replies 0

Primary		Backup	
Access Requests	0	Access Requests	0
Access Accepts	0	Access Accepts	0
Access Retransmissions	0	Access Retransmissions	0
Access Rejects	0	Access Rejects	0
Access Challenges	0	Access Challenges	0
Malformed Access Responses	0	Malformed Access Responses	0
Authentication Bad Authenticators	0	Authentication Bad Authenticators	0
Timeouts	0	Timeouts	0

4) Per Station

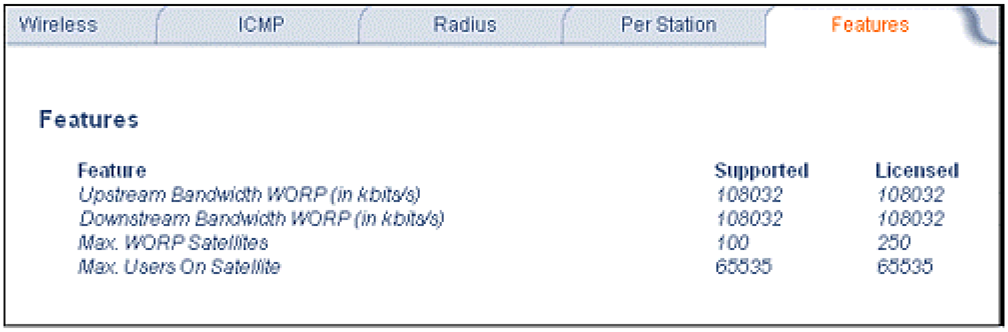
Click the **Monitor** button and the **Per Station** tab to view the following information:



This feature is not supported in the current release.

5) Features

Click the **Monitor** button and the **Features** tab to view the following information:



Features

Feature	Supported	Licensed
Upstream Bandwidth WORP (in kbits/s)	108032	108032
Downstream Bandwidth WORP (in kbits/s)	108032	108032
Max. WORP Satellites	100	250
Max. Users On Satellite	65535	65535

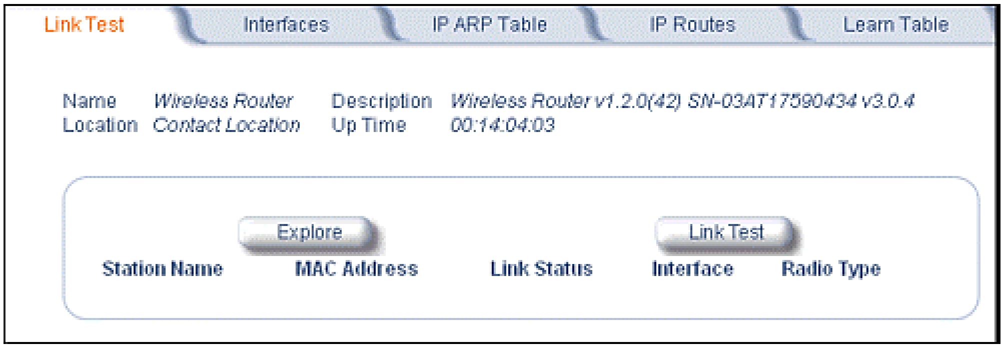
Note: A Base Station shows how many WORP satellites it can support; the Subscriber Unit and Residential Subscriber Unit will show how many Ethernet hosts they support on their Ethernet port as the “Max Users on Satellite” parameter.

6) Link Test

Click the **Monitor** button and the **Link Test** tab to find out which wireless stations are in range and to check their link quality.

Link Test for the MP.11a reports a single Receive Signal Strength Indicator (RSSI) value; the higher the number, the better the signal.

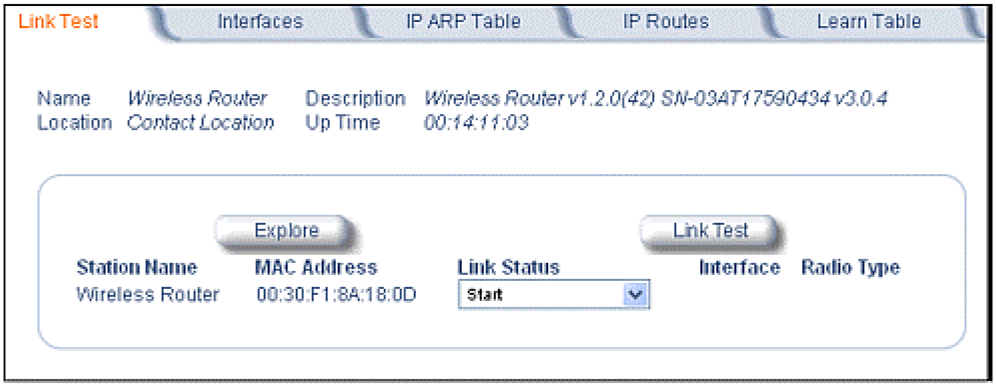
- **Explore** from a BSU displays all its registered SUs.
- **Explore** from an SU or RSU displays only the BSU with which it is registered.



Name Wireless Router
Location Contact Location
Description Wireless Router v1.2.0(42) SN-03AT17590434 v3.0.4
Up Time 00:14:04:03

Station Name	MAC Address	Link Status	Interface	Radio Type

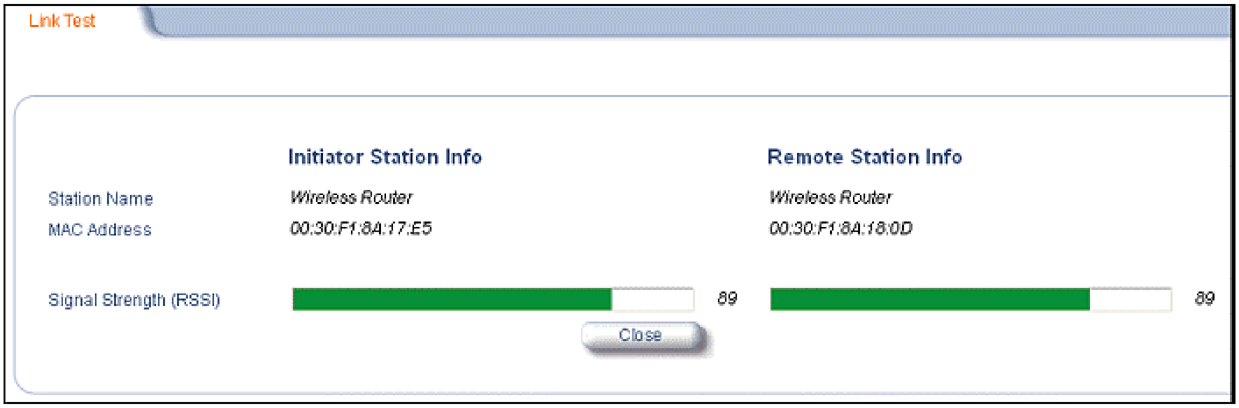
All stations displayed after “Explore” come up “Disabled.” Select a station by changing **Disabled** to **Start** and click the **Link Test** button. You can change multiple stations to **Start**, but only the last station in the list is displayed as the remote partner when you click the **Link Test** button. See the following figure:



Name *Wireless Router* Description *Wireless Router v1.2.0(42) SN-03AT17590434 v3.0.4*
Location *Contact Location* Up Time *00:14:11:03*

Station Name	MAC Address	Link Status	Interface	Radio Type
Wireless Router	00:30:F1:8A:18:0D	Start		

The Link Test provides the following information:



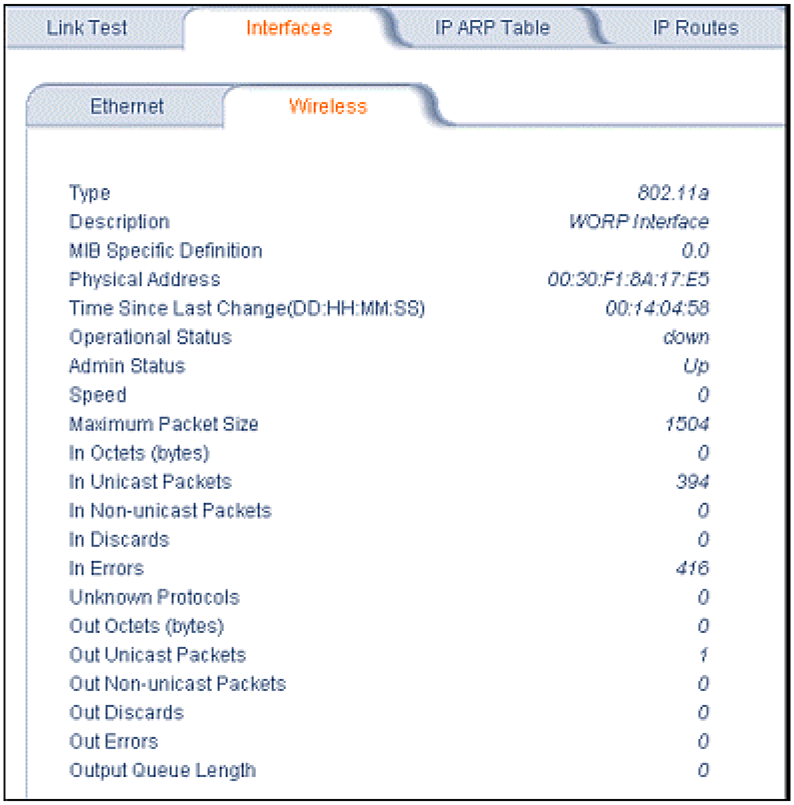
	Initiator Station Info	Remote Station Info
Station Name	*Wireless Router*	*Wireless Router*
MAC Address	*00:30:F1:8A:17:E5*	*00:30:F1:8A:18:0D*
Signal Strength (RSSI)	*89*	*89*

Link Test stops when you close the **Link Test** page.

7) Interfaces

Click the **Monitor** button and the **Interfaces** tab to view detailed information about the IP-layer performance of the MP.11/a interfaces. There are two sub-tabs: **Wireless** and **Ethernet**.

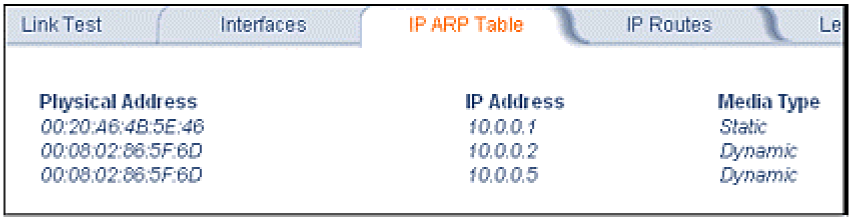
The following figure shows the **Wireless** interface; the same information is provided for the Ethernet interface on the **Ethernet** sub-tab.



Type	802.11a
Description	WORP Interface
MIB Specific Definition	0.0
Physical Address	00:30:F1:8A:17:E5
Time Since Last Change(DD:HH:MM:SS)	00:14:04:58
Operational Status	down
Admin Status	Up
Speed	0
Maximum Packet Size	1504
In Octets (bytes)	0
In Unicast Packets	394
In Non-unicast Packets	0
In Discards	0
In Errors	416
Unknown Protocols	0
Out Octets (bytes)	0
Out Unicast Packets	1
Out Non-unicast Packets	0
Out Discards	0
Out Errors	0
Output Queue Length	0

8) IP ARP Table

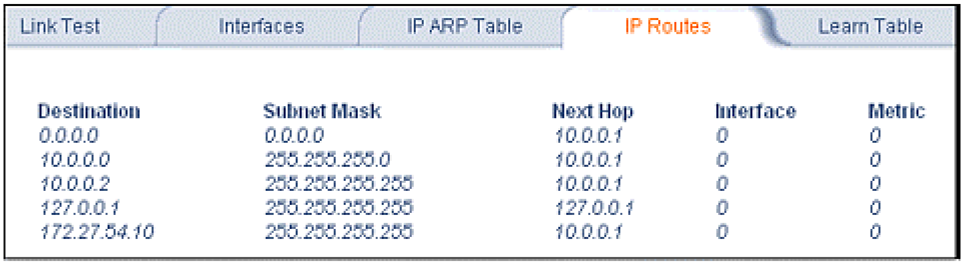
Click the **Monitor** button and the **IP ARP Tabl**e tab to view the mapping of the IP and MAC addresses of all radios registered at the MP.11/a. This information is based upon the Address Resolution Protocol (ARP).



Physical Address	IP Address	Media Type
00:20:A6:4B:5E:46	10.0.0.1	Static
00:08:02:86:5F:6D	10.0.0.2	Dynamic
00:08:02:86:5F:6D	10.0.0.5	Dynamic

9) IP Routes

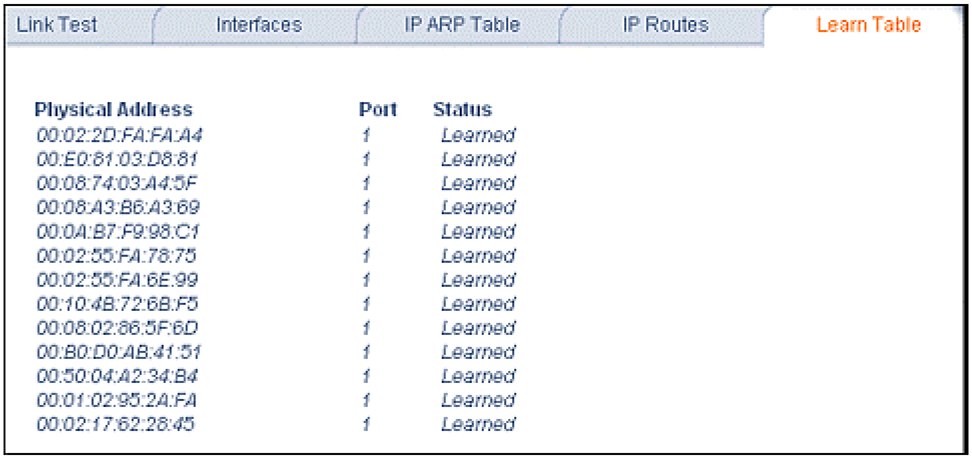
Click the **Monitor** button and the **IP Routes** tab to view all active IP routes of the MP.11/a. These can be either static or dynamic (obtained through RIP). This tab is available only in **Router** mode, and you can add routes only when in **Router** mode.



Destination	Subnet Mask	Next Hop	Interface	Metric
0.0.0.0	0.0.0.0	10.0.0.1	0	0
10.0.0.0	255.255.255.0	10.0.0.1	0	0
10.0.0.2	255.255.255.255	10.0.0.1	0	0
127.0.0.1	255.255.255.255	127.0.0.1	0	0
172.27.54.10	255.255.255.255	10.0.0.1	0	0

10) Learn Table

Click the **Monitor** button and the **Learn Table** tab to view all MAC addresses the MP.11 has detected on an interface. The **Learn Table** displays information relating to network bridging. It reports the MAC address for each node that the device has learned is on the network and the interface on which the node was detected. There can be up to 10,000 entries in the **Learn Table**. This tab is only available in **Bridge** mode.



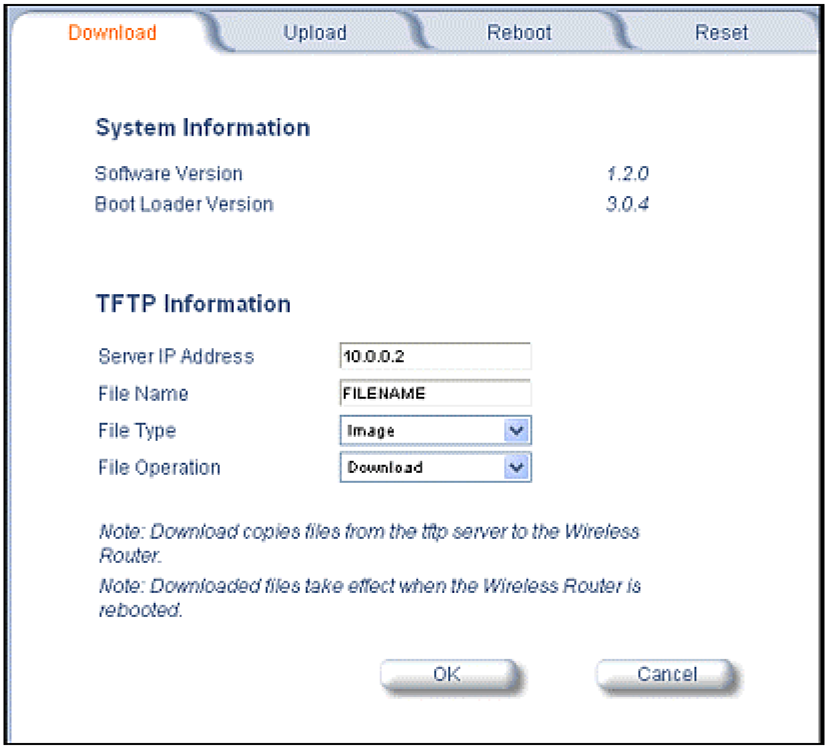
Physical Address	Port	Status
00:02:2D:FA:FA:A4	1	Learned
00:E0:81:03:D8:81	1	Learned
00:08:74:03:A4:5F	1	Learned
00:08:A3:B6:A3:69	1	Learned
00:0A:B7:F9:98:C1	1	Learned
00:02:55:FA:78:75	1	Learned
00:02:55:FA:6E:99	1	Learned
00:10:4B:72:6B:F5	1	Learned
00:08:02:86:5F:6D	1	Learned
00:B0:D0:AB:41:51	1	Learned
00:50:04:A2:34:B4	1	Learned
00:01:02:95:2A:FA	1	Learned
00:02:17:62:28:45	1	Learned

COMMANDS

This section describes the commands that you can perform with the Web Interface. There are five tabs in the Commands section.

1) Download

Click the **Commands** button and the **Download** tab to download image, configuration, and license files to the MP.11/a.



System Information

Software Version 1.2.0

Boot Loader Version 3.0.4

TFTP Information

Server IP Address 10.0.0.2

File Name FILENAME

File Type Image

File Operation Download

Note: Download copies files from the tftp server to the Wireless Router.

Note: Downloaded files take effect when the Wireless Router is rebooted.

Server IP address

Enter the TFTP Server IP address. (Double-click the TFTP server icon on your desktop and locate the IP address assigned to the TFTP server.)

File Name

Enter the name of the file to be downloaded.

File Type

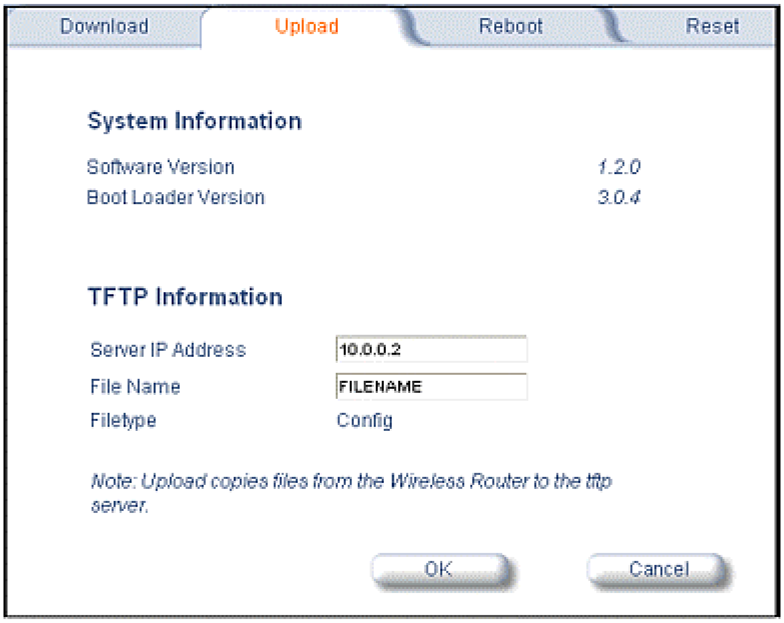
Config, **image**, **bootloader**, or **license**.

File Operation

Download or **Download and Reboot**.

2) Upload

Click the **Commands** button and the **Upload** tab to upload a configuration file from the MP.11/a.



System Information

Software Version 1.2.0

Boot Loader Version 3.0.4

TFTP Information

Server IP Address 10.0.0.2

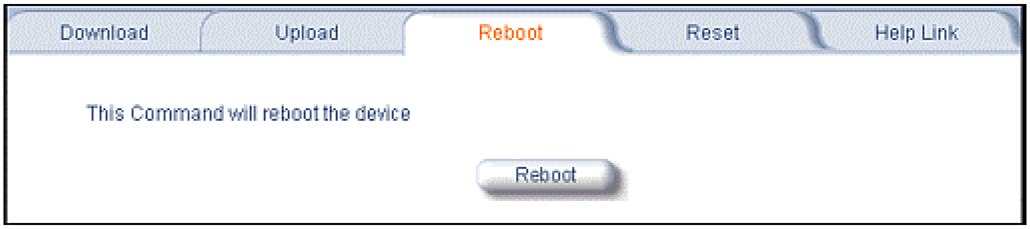
File Name FILENAME

Filetype Config

Note: Upload copies files from the Wireless Router to the tftp server.

3) Reboot

Click the **Commands** button and the **Reboot** tab to restart the embedded software of the MP.11/a. Configuration changes are saved and the MP.11/a is reset.

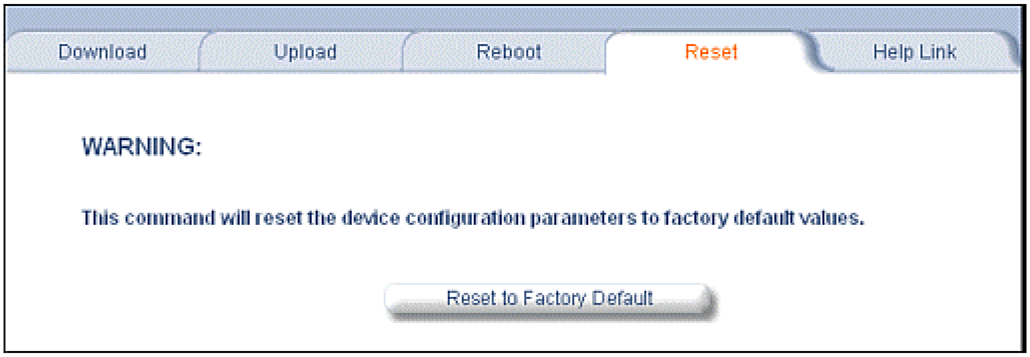


This Command will reboot the device

CAUTION:* *Rebooting the unit causes all users currently connected to lose their connection to the network until the MP.1/a1 has completed the restart process and resumed operation.

4) Reset

Click the **Commands** button and the **Reset** tab to restore the configuration of the MP.11/a to the factory default values.



WARNING:

This command will reset the device configuration parameters to factory default values.

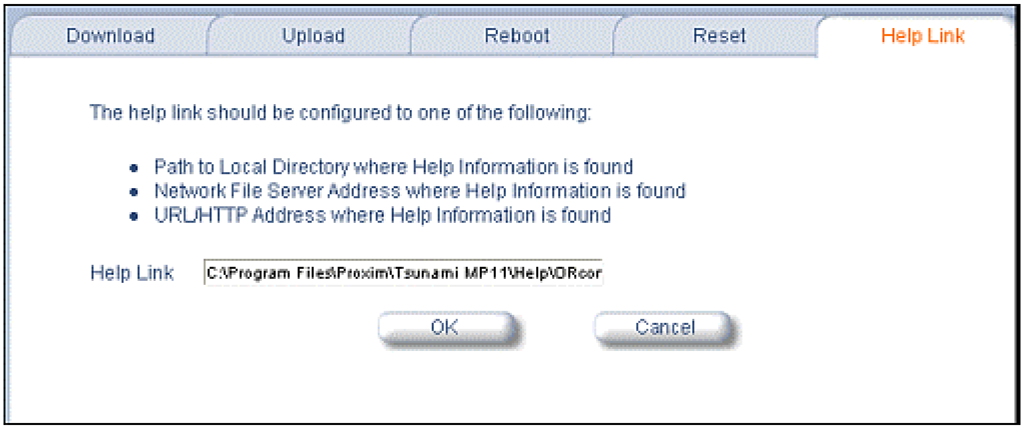
You can also reset the MP.11/a from the RESET button located on the side of the unit. Because this resets the MP.11/a's current IP address, a new IP address must be assigned.

CAUTION: ***Resetting the MP.11/a to its factory default configuration permanently overwrites all changes made to the unit. The MP.11/a reboots automatically after this command has been issued.***

5) Help Link

Click the **Commands** button and the **Help Link** tab to set the location of the help files of the Web Interface. If the help files cannot be found, pressing the **?** button results in an error message. Upon installation, the help files are installed in the **C:\Program Files\Proxim\Tsunami MP.11/a** folder.

If you want to place these files on a shared drive, copy the **Help** folder to the new location and specify the new path in the **Help Link** box.



The help link should be configured to one of the following:

- Path to Local Directory where Help Information is found
- Network File Server Address where Help Information is found
- URL/HTTP Address where Help Information is found

Help Link C:\Program Files\Proxim\Tsunami MP11\Help\ORcor

Chapter 6. Command Line Interface

The Command Line Interface (CLI) provides a text-based interface with which you can configure and manage the MP.11/a using commands. You can enter these commands or submit them in the form of a script to allow batch processing. Accessing the CLI is discussed in “Command Line Interface Overview” in the *Tsunami MP.11/a Installation and Management Guide.*.

Administrators use the CLI to control MP.11/a operation and monitor network statistics. The MP.11/a supports 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.

BOOT LOADER COMMAND LINE INTERFACE

The Boot Loader is started when the MP.11/a is switched on or reset, and is responsible for starting the embedded software. The Boot Loader CLI is available when the MP.11/a embedded software is not running.

The Boot Loader CLI is a minimal subset of the normal CLI used to perform initial configuration of the MP.11/a. This interface is accessible only through the serial interface if the MP.11/a 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. Configuration items include the IP address and other network-specific values. Config files can be downloaded to the MP.11/a or uploaded for backup or troubleshooting.

Download versus Upload

Downloads transfer files to the MP.11/a. Uploads transfer files from the MP.11/a. 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 MP.11/a software executed from RAM. To update an MP.11/a, you typically download a new Image File.

Parameter

A fundamental network value that can be displayed and may be changeable. For example, the MP.11/a 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 dd 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
download	Transfer files from the TFTP server to the MP.11/a
exit (page	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 MP.11a
passwd	Change the password used to access the CLI
quit	Disconnects and closes the current CLI session
reboot	Signal the MP.11/a to reboot after a specified number of seconds
save	Save the current MP.11/a configuration to flash memory
search	Display the parameter entries in a specified table
set	Change parameter values
show	View parameter and statistical values
upload	Transfer files from the MP.11/a to the TFTP server

Also see “Show and Set Parameters” on page 89 and “Table Parameters” on page 98.

? (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 **set** or **show** 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.

Done Command

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

Download Command

The **`download`** command is used to transfer files from the TFTP server to the MP.11/a. 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 MP.11/a:

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

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

`config` - Configuration file, the current settings of the MP.11/a
`image` - Image file, embedded software for the MP.11/a
`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
```

The following represents part of the displayed output:

```
Special keys supported:
Arrow Keys
DEL, BS .... delete previous character
Ctrl-A  .... go to beginning of line
Ctrl-E  .... go to end of line
Ctrl-F  .... go forward one character
Ctrl-B  .... go backward one character
Ctrl-D  .... delete current character
Ctrl-U, X .. delete to beginning of line
Ctrl-K  .... delete to end of line
Ctrl-W ..... delete previous word
Ctrl-T ..... transpose previous character
Ctrl-P  .... go to previous line in history buffer
Ctrl-N  .... go to next line in history buffer
Tab     .... will attempt command completion
?       .... will provide command listing
```

For a description and example of the specified command, enter:

`help <command name>` or **`<command name> 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 MP.11/a.

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 MP.11/a and the CLI cannot be accessed. In this case, the MP.11/a must be reset to factory defaults. The default password for the CLI is **public**.

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 MP.11/a 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 MP.11/a 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 98 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 MP.11/a IP address parameter:

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

Some parameter values change only when the MP.11 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 89 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 89 for a list of parameters that can be used with the show command.

Upload Command

The **upload** command is used to transfer files from the MP.11/a to the TFTP server.

To upload a file from the MP.11/a to the TFTP server:

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

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

config - Configuration file, the current settings of the MP.11/a
image - Image file, embedded software for the MP.11/a
bootloader - Boot software
license - License file

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

There are a few basic configuration parameters that you may want to set up immediately when you receive the MP.11/a. For example:

- Set System Name, Location, and Contact information
- Set IP address for the MP.11/a
- Configure interfaces
- Set WEP Encryption and passwords
- Download an MP.11/a configuration file from your TFTP server
- Backup your MP.11/a configuration file
- Reboot
- Reset to factory defaults

Basic CLI Management Commands

Task	Commands
Set System Name, Location, and Contact information	show system set sysname <name> set sysloc <location> set sysactname <contact name> set sysctemail <contact email> set sysctphone <contact phone>
Set IP address for the MP.11/a	set ipaddrtype <static | dynamic> set ipaddr 1 ipaddress <ip address> set ipaddr 1 ipsubmask <subnet mask> set ipaddr 1 ipgw <gateway IP address> For example: set ipaddr 1 ipaddress <ip address> ipsubmask <subnet mask>
Configure Wireless Interface	set wif 3 channel 10 set wif 3 netname <network name>
Configure Ethernet Interface	show ethernet show ethermacaddr set Ethernet 1 etherspeed <autospeedauto | autospeedhalf | 100auto | 100full | 100 half | 10full | 10half>
Set Encryption for the Wireless interface	show wifsec set wifsec 3 encryptkeytx <1-4> set wifsec 3 encryptkey1 <key 1> set wifsec 3 encryptallowdeny <enable | disable>
Set Telnet Password	show telnet set tellogintout <login timeout> set telport <port number> set telsessions <maximum number of sessions> set telsessiontout <inactivity timeout>
Set Web Interface Password	show http set httppasswd <password> set httpport <port number> set httpstatus <0-15>
Set SNMP Password	show snmp set snmprpasswd <read password> set snmprwpasswd <read/write password> set snmpstatus <0-15>
Download an MP.11/a configuration file from your TFTP server	set tftpfilename <file name> <tftpfiletype config tftpipaddr <IP address of your TFTP server> show tftp (to ensure the entries are correct) download * reboot 0
Backup your MP.11/a configuration file	upload <TFTP Server IP address> <tftpfilename(such as “config.sys”)> config show tftp (to ensure the entries are correct) upload *
Reboot	reboot [<number of seconds>]
Reset to Factory Defaults	set sysresettodefaults 1

SHOW AND SET PARAMETERS

The following table details the non-table parameters available to be viewed and set within the MP.11/a CLI.

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

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]

DHCP RELAY PARAMETERS **Enable or disable dynamic host configuration**		
`dhcprelay`	R	DHCP Relay Group
`dhcprelaystatus`	RW	DHCP Relay Status [1=enable, 2=disable]
`dhcprelaytbl`	RW	DHCP Relay Agent IP Table
`index`	R	Index (maximum of ten table entries)
`dhcprlyipaddr`	RW	DHCP Server IP address
`dhcprlycmt`	RW	Comment
`dhcprlystatus`	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]
`ethermacaddr`	RW	MAC address
`ethrxbwlimit`	RW	Incoming bandwidth limit
`ethtxbwlimit`	RW	Outgoing bandwidth limit

ETHERNET FILTERING PARAMETERS Control network traffic based upon protocol type		
etherflt	R	Ethernet Filtering Group
etherflttbl	RW	Ethernet Filter Table
index	R	Index
proto	RW	Ethernet Filtering Protocol
cmt	RW	Comment {2-31 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 Setup the Graphical Web Browser Interface		
http	R	HTTP Group
httpport	RW	HTTP port
httppasswd	W	HTTP password
httpifbitmask	RW	HTTP interface bitmask
httphelplink	RW	Help link

INVENTORY MANAGEMENT PARAMETERS Hardware, firmware, and software version information		
sysinvmgmt	R	Inventory Management Group
sysinvmgmtcmpiftbl	R	Inventory Interface Table
sysinvmgmtcmptbl	R	Inventory Component Table

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
iparpfltipaddr	RW	IP address
iparpfltstatus	RW	Status [1=enable, 2=disable]
iparpfltsubmask	RW	Subnet mask

LINK INTEGRITY PARAMETERS		
`linkinttbl`	RW	Link Integrity Target IP Address Table
`index`	R	Index
`cmt`	RW	Comment
`ipaddr`	RW	IP address
`status`	RW	Status of table entry [1=enable, 2=disable, 3=delete, 4=create]

MAC ACCESS CONTROL TABLE PARAMETERS **Control wireless access based upon MAC address**		
`macacl`	R	MAC Access Control Group
`macacltbl`	RW	MAC Access Control Table
`index`	R	Index
`macaddr`	RW	MAC address
`cmt`	RW	Comment
`status`	RW	Status of table entry [1=enable, 2=disable]
`macaclstatus`	RW	Status [1=enable, 2=disable]
`macacloptype`	RW	Operation type [1=allow, 2=deny]

MISCELLANEOUS PARAMETERS		
`queries`	R	RIP v2 Global Queries
`routechg`	R	RIP v2 Global Route Changes

NETWORK PARAMETERS **Configure IP and Network Settings**		
`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 (Router mode only)
`ipaddr`	R	IP address
`metric`	RW	Routing metric
`routtype`	RW	Route Type
`ipsubmask`	RW	Subnet Mask
`ipgw`	RW	Gateway IP address
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`		

RADIUS PARAMETERS **Primary and Backup RADIUS Server Table Parameters and** **RADIUS Authentication and Accounting Information**		
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
radmacacctrl	RW	MAC Access Control

RIP INTERFACE PARAMETERS		
ripifcfg	RW	RIP Interface Configuration Table
authtype	RW	Authentication Type [1 = No Authentication,2 = Simple Password]
authkey	RW	Authentication Key
txmode	RW	Transmission Mode [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

SERIAL PARAMETERS **Serial Port Setup**		
serial	R	Serial Group
serbaudrate	RW	Baudrate [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]

SNMP PARAMETERS
Set Read and Read/Write Passwords

`snmp`	R	SNMP Group
`snmpipscccesstbl`	RW	SNMP IP Access Table
`index`	R	Index
`ipaddr`	RW	IP address
`submask`	RW	Subnet mask
`if`	RW	Interface [1=Ethernet, 2=PC Card A, 3=PC Card B]
`cmt`	RW	Comment
`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
`status`	RW	Status of table entry [1=enable, 2=disable, 3=delete]
`snmprpasswd`	W	Read password
`snmprwpasswd`	W	Read/write password

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
```

SECURITY PARAMETERS
MP.11/a Security Settings

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

SPANNING TREE PARAMETERS (Bridge mode only)
Help prevent network loops

`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 PARAMETER Enable and disable specific addresses		
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 [2-31 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
statripgloabl	R	RIP Global Statistics
staticmp	R	ICMP Statistics

STORM THRESHOLD PARAMETERS Set threshold for number of broadcast packets		
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]
mcast	RW	Multicast address threshold [4-250]

SYSTEM PARAMETERS
MP.11/a System Information

`system`	R	System group
`sysname`	RW	Name
`sysmode`	RW	Mode [1=bridge, 2=router]
`sysloc`	RW	Location
`sysctname`	RW	Contact name
`sysctemail`	RW	Contact email
`sysctphone`	RW	Contact phone
`sysdescr`	R	Description
`sysoid`	R	OID
`sysservices`	R	Services
`sysuptime`	R	Up time
`sysflashbckint`	RW	Flash backup interval (seconds)
`sysflashupdate`	RW	Flash update [1=write flash]
`sysresettodefaults`	RW	Resets to factory defaults. [1=reset and immediate reboot] Example: This command sets the MP.11/a to Router mode: `set sysmode 2`

TELNET PARAMETERS
Telnet Port Setup

`telnet`	R	Telnet Group
`telifbitmask`	RW	Telnet interface bitmap
`telsessions`	RW	Telnet sessions [0-5=max number of telnet sessions]
`telport`	RW	Telnet port
`tellogintout`	RW	Telnet login timeout (seconds)
`telsessiontout`	RW	Telnet session timeout (seconds)

Example: This command changes the login timeout and the session timeout.

```
set tellogintout 200 telsessiontout 1800
```

TFTP PARAMETERS
Setup for File Transfers

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

WIRELESS INTERFACE PARAMETER **Configure wireless settings**		
`wif`	RW	Wireless Interface Group
`index`	R	Index [3]
`netname`	RW	Network name
`satden`	RW	Satellite density (1=large, 2= medium, 3=small, 4=mini, 5=micro]
`interrobust`	RW	Interference Robustness [1=enable, 2=disable]
`dtimperiod`	RW	DTIM period
`autochannel`	RW	Auto channel select status [1=enable, 2=disable]
`channel`	RW	Frequency channel
`medres`	RW	RTS/CTS Medium Reservation
`multrate`	RW	Multicast rate (megabits per second) [1=1, 2=2, 3=5.5, 4=11, 5=6, 6=9, 7=12, 8=18, 9=24, 10=36, 11=48, 12=54, 13=72, 14=96, 15=108]
`countrycode`	RW	Country code [see Country Code table]
`dfsstatus`	RW	DFS status [1=enable, 2=disable]
`tpcmode`	RW	TPC mode [1=half, 2=quarter, 3=eighth, 4=min, 5=full]
`closedsys`	RW	Closed system [1=enable, 2=disable]
`ldbalance`	RW	Load balancing [1=enable, 2=disable]
`meddendistrib`	RW	Medium Density Distribution [1=enable, 2=disable]
`macaddr`	R	MAC address
`suppdatarates`	R	Supported data rates
`suppchannels`	R	Supported channels
`phytype`	R	Physical layer type
`regdomain`	R	Regulatory Domain List
`txrate`	RW	Transmit rate [0=auto fallback, 1-255=(<value>/2) megabits per second]
`wifrxbwlimit`	RW	Incoming bandwidth limit
`wiftxbwlimit`	RW	Outgoing bandwidth limit
`turbomode`	RW	Turbo mode [1=enable, 2=disable]
`opermode`	R	Operational mode
`preambletype`	R	Preamble type
`protmech`	R	Protection mechanism status
Example: This command disables closed system and enables 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 [0-3=Keys 1-4, respectively]
Example: This command sets the encryption option to aes, sets a new string for key2, and sets it as the key used for encryption. `set wifsec 3 encryptoption 4 encryptkey2 abcdefghi encryptkeytx 1`		

WORP PARAMETERS		
`worp`	`R`	WORP Group
`worpcfg`	`RW`	WORP Interface Configuration
`index`	`R`	Index
`mode`	`RW`	Mode [1=disabled, 2=ap, 3=base, 4=satellite]
`netname`	`RW`	Network Name
`basename`	`RW`	Base Station Name
`maxsatellites`	`RW`	Maximum number of satellites allowed
`multrate`	`RW`	Multicast rate
`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	

Set the IP address parameter	Syntax:
	`set <parameter name> <parameter value>`
	Example:
	`set ipaddr 10.0.0.12`

Create a table row or entry	Syntax:
	`set <table name> <table index> <element 1> <value 1> … <element n> <value n>`
	Example:
	`set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0`

Modify a table entry or row	Examples:
	`set mgmtipaccesstbl 1 ipaddr 10.0.0.11`
	`set mgmtipaccesstbl 1 ipaddr 10.0.0.12 ipmask 255.255.255.248 cmt “First Row”`

Show the group parameters	Syntax:
	`show <group name>`
	Example:
	`show network`

Show individual and table parameters	Syntax:
	`show <parameter name>   show <table name>`
	Examples:
	`show ipaddr        show mgmtipaccesstbl`

Enable, disable, or delete a table entry or row	Syntax:
	`set <Table> index status <enable, disable, delete>`
	`set <Table> index status <1=enable, 2=disable, 3=delete>`
	Examples:
	`set mgmtipaccesstbl 2 status enable`
	`set mgmtipaccesstbl 2 status disable`
	`set mgmtipaccesstbl 2 status delete`
	`set mgmtipaccesstbl 2 status 2`

Table Parameters

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 MP.11/a CLI and an example of a row entry for that table are listed in the following table.

broadcastflttbl		
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]
dhcprelaytbl		
index	R	Index
dhcprlyipaddr	RW	DHCP Server Address
dhcprlycmt	RW	Comment
dhcprlystatus	RW	Status of table entry [1=enable, 2=disable]
etherflttbl		
index	R	Index
proto	RW	Ethernet filtering protocol
cmt	RW	Comment [2-31 characters]
status	RW	Status of table entry [1=enable, 2=disable]
macacltbl		
index	R	Index
macaddr	RW	MAC Address
cmt	RW	Comment [2-31 characters]
status	RW	Status of table entry [1=enable, 2=disable]
radiustbl		
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
secenckeylentbl		
index	R	Index
enckeylen	RW	Encryption Key Length
snmpipaccesstbl		
index	R	Index
ipaddr	RW	IP address
submask	RW	Subnet mask
if	RW	Interface [1=Ethernet, 2=PC card A, 3=PC card B]
cmt	RW	Comment [2-31 characters]
status	RW	Status of table entry [1=enable, 2=disable]

snmptraphosttbl		
index	R	Index
ipaddr	RW	IP address
passwd	W	Password
cmt	RW	Comment [2-31 characters]
status	RW	Status of table entry [1=enable, 2=disable]
staticmactbl		
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 [2-31 characters]
status	RW	Status of table entry [1=enable, 2=disable]
stmthrestbl		
index	R	Index
bcast	RW	Broadcast address threshold [4-250]
mcast	RW	Multicast address threshold [4-250]
sptbl		
index	R	Index
priority	RW	Priotity
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
```

COUNTRY CODE TABLE

Either the index number or the two-letter abbreviation can be used to set the country code.

Example: Both of these commands set Taiwan as the country:

```
set wif 3 countrycode 158
set wif 3 countrycode tw
```

Country	Index	Code
No Country	0	na
Argentina	32	ar
Armenia	51	am
Australia	36	au
Austria	40	at
Azerbaijan	31	az
Belgium	56	be
Belize	84	bz
Bolivia	68	bo
Brunei Darussalam	96	bn
Bulgaria	100	bg
Canada	124	ca
China	156	cn
Colombia	170	co
Croatia	191	hr
Cyprus	196	cy
Czech Republic	203	cz
Denmark	208	dk
Dominican Republic	214	do
Estonia	233	ee
Finland	246	fi
France	250	fr
Georgia	268	ge
Germany	276	de
Guatemala	320	gt
Hong Kong	344	hk
Hungary	348	hu
Iceland	352	is
Iran	364	ir
Ireland	372	ie
Italy	380	it
Japan	392	jp
Japan2	393	jr
North Korea	408	kp
Korea Republic	410	kr
Korea Republic 2	411	kR
Liechtenstein	438	li
Lithuania	440	lt
Luxembourg	442	lu
Macau	446	mo
Mexico	484	mx
Monacco	492	mc
Netherlands	528	nl
New Zealand	554	nz
Norway	578	no
Panama	591	pa
Philippines	608	ph
Poland	616	pl
Portugal	620	pt
Puerto Rico	630	pr
Singapore	702	sg
Slovak Republic	703	sk
Slovenia	705	si
South Africa	710	za
Sweden	752	se
Switzerland	756	ch
Taiwan	158	tw
Thailand	764	th
Turkey	792	tr
United Kingdom	826	gb
United States	840	us
Uruguay	858	uy
Venezuela	862	ve

Chapter 7. Procedures

This chapter contains a set of procedures, as described in the following table:

Procedure	Description
TFTP Server Setup	Prepares the TFTP server for transferring files to and from the MP.11/a. This procedure is used by the other procedures that transfer files.
Image File Download	Upgrades the embedded software.
Configuration Backup	Saves the configuration of the MP.11.
Configuration Restore	Restores a previous configuration through configuration file download.
Soft Reset to Factory Default	Resets the MP.11/a to the factory default settings through the Web or Command Line Interface.
Hard Reset to Factory Default	In some cases, it may be necessary to revert to the factory default settings (for example, if you cannot access the MP.11/a or you lost the password for the Web Interface.
Force Reload	Completely resets the MP.11 and erases the embedded software. Use this procedure only as a last resort if the MP.11 does not boot and the "Hard Reset to Factory Default" procedure did not help. If you perform a "Forced Reload," you must download a new image file as described in "Image File Download with the Boot Loader."
Image File Download with the Boot Loader	If the MP.11/a does not contain embedded software, or the embedded software is corrupt, you can use this procedure to download a new image file.

TFTP SERVER SETUP

To download or upload a file, you must connect to the computer with the TFTP server through the MP.11/a's Ethernet port. This can be any computer in the network or a computer connected to the MP.11/a with a cross-over Ethernet cable. For information about installing the TFTP server, see "Installing Documentation and Software" on page 15.

Ensure that the upload or download directory is correctly set, the required file is present in the directory, and the TFTP server is running. ***The TFTP server must be running only during file upload and download.*** You can check the connectivity between the MP.11/a and the TFTP server by pinging the MP.11/a from the computer that hosts the TFTP server. The ping program should show replies from the MP.11/a.

WEB INTERFACE IMAGE FILE DOWNLOAD

In some cases, it may be necessary to upgrade the embedded software of the MP.11/a by downloading an image file. To download an image file through the Web Interface:

1. Set up the TFTP server as described in "TFTP Server Setup" on page 104.
2. Access the MP.11/a as described in "Web Interface Overview" on page 22.
3. Click the **Commands** button and the **Download** tab.
4. Fill in the following details:

   Server IP Address <IP address TFTP server>
   File Name <image file name>
   File Type Image
   File Operation Download

5. Click **OK** to start the file transfer.

The MP.11/a downloads the image file. The TFTP server program should show download activity after a few seconds. When the download is complete, the MP.11 is ready to start the embedded software.

CONFIGURATION BACKUP

You can back up the MP.11/a configuration by uploading the configuration file. You can use this file to restore the configuration or to configure another MP.11/a (see "Configuration Restore" on page 106).

To upload a configuration file through the Web Interface:

1. Set up the TFTP server as described in "TFTP Server Setup" on page 104.
2. Access the MP.11 as described in "Web Interface Overview" on page 22.
3. Click the **Commands** button and the **Upload** tab.
4. Fill in the following details:
   Server IP Address <IP address TFTP server>
   File Name <configuration file name>
   File Type Config
   File Operation Upload
5. Click **OK** to start the file transfer.

The MP.11/a uploads the configuration file. The TFTP server program should show upload activity after a few seconds. When the upload is complete, the configuration is backed up.

CONFIGURATION RESTORE

You can restore the configuration of the MP.11/a by downloading a configuration file. The configuration file contains the configuration information of an MP.11/a.

To download a configuration file through the Web Interface:

1. Set up the TFTP server as described in "TFTP Server Setup" on page 104.
2. Access the MP.11/a as described in "Web Interface Overview" on page 22.
3. Click the **Commands** button and the **Download** tab.
4. Fill in the following details:
   Server IP Address <IP address TFTP server>
   File Name <configuration file name>
   File Type Config
   File Operation Download
5. Click **OK** to start the file transfer.

The MP.11/a downloads the configuration file. The TFTP server program should show download activity after a few seconds. When the download is complete and the system rebooted, the configuration is restored.

SOFT RESET TO FACTORY DEFAULT

If necessary, you can reset the MP.11/a to the factory default settings. Resetting to default settings means that you must configure the MP.11/a anew.

To reset to factory default settings using the Web Interface:

1. Click the **Commands** button and the **Reset** tab.
2. Click the **Reset to Factory Default** button.

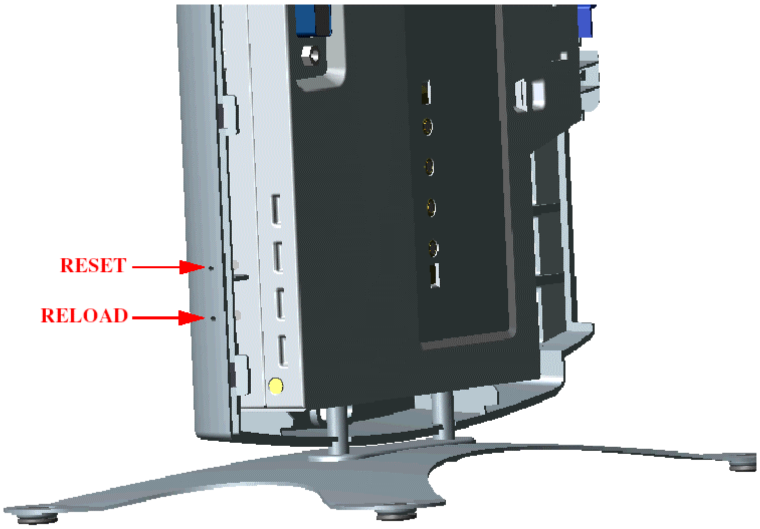
The device configuration parameter values are reset to their factory default values.

If you do not have access to the MP.11/a, you can use the procedure described in "Hard Reset to Factory Default" on page 107 as an alternative.

HARD RESET TO FACTORY DEFAULT

If you cannot access the unit or you have lost its password, you can reset the MP.11/a to the factory default settings. Resetting to default settings means you must configure the MP.11/a anew.

To reset to factory default settings, press and hold the **RELOAD** button on the MP.11/a unit for about 10 seconds. The MP.11/a reboots and restores the factory default settings.



To access the MP.11/a see “Chapter 3. Management Overview” on page 19.

FORCED RELOAD

With Forced Reload, you reset the MP.11/a to the factory default settings and erase the embedded software. Use this procedure only as last resort if the MP.11/a does not boot and the “Reset to Factory Defaults” procedure did not help. If you perform a Forced Reload, you must download a new image file with the Boot Loader (see “Image File Download with the Boot Loader” below).

Caution! ***The following procedure erases the embedded software of the MP.11/a. This software image must be reloaded via an Ethernet connection with a TFTP server. The image filename to be downloaded can be configured with either ScanTool through the Ethernet interface or with the Boot Loader CLI through the serial port to make the MP.11/a functional again.***

To do a forced reload:

1. Press the RESET button on the MP.11/a unit; the MP.11/a resets and the LEDs flash.

2. Immediately press and hold the RELOAD button on the MP.11/a unit for about 20 seconds. Now image and configuration are deleted from the unit.

3. Follow the procedure “Image File Download with the Boot Loader” to download an image file.

IMAGE FILE DOWNLOAD WITH THE BOOTLOADER

The following procedures download an image file to the MP.11/a after the embedded software has been erased with **Forced Reload** or when the embedded software cannot be started by the Boot Loader.

A new image file can be downloaded to the MP.11/a with ScanTool or the Command Line Interface through the MP.11/a serial port. In both cases, the file is transferred through Ethernet with TFTP. Because the CLI serial port option requires a serial RS-232C cable, Proxim recommends the ScanTool option.

Download with ScanTool

To download an image file with the ScanTool:

1. Set up the TFTP server as described in "TFTP Server Setup" on page 104.
2. Run ScanTool on a computer that is connected to the same LAN subnet as the MP.11/a. ScanTool scans the subnet for MP.11/a units and displays the found units in the main window. If in **Forced Reload** state (Power and Ethernet LEDs are amber), ScanTool will not find the device until the MP.11/a bootloader times out, and the Power LED turns RED and the Ethernet LED goes OFF. Click **Rescan** to re-scan the subnet and update the display.
3. Select the MP.11/a to which you want to download an image file and click **Change**.
4. Ensure that **IP Address Type Static** is selected and fill in the following details:
   - **IP Address** and **Subnet Mask** of the MP.11/a.
   - **TFTP Server IP Address** and, if necessary, the **Gateway IP Address** of the TFTP server.
   - **Image File Name** of the file with the new image.
5. Click **OK** to start the file transfer.

   The MP.11/a downloads the image file. The TFTP server program should show download activity after a few seconds. When the download is complete, the LED pattern should return to **Forced Reload** state (Power and Ethernet LEDs are amber). the MP.11/a is ready to start the embedded software.
6. Press and release the **Reset** button. It may take several seconds to cycle through the Forced Reload LED pattern and through the initialization LED sequence.

After a Forced Reload procedure, the MP.11/a returns to factory default settings and must be reconfigured. ScanTool can be used to set the system name and IP address.

To access the MP.11/a see "Chapter 3. Management Overview" on page 19.

Download with CLI

To use the CLI through the serial port of the MP.11/a you need the following items:

- A serial RS-232C cable with a male and a female DB-9 connector.
- An ASCII terminal program such as HyperTerminal.

Proxim recommends you switch off the MP.11 and the computer before connecting or disconnecting the serial RS-232C cable.

To download an image file:

1. Set up the TFTP server as described in "TFTP Server Setup" on page 104.

2. Start the terminal program (such as HyperTerminal), set the following connection properties, and then connect:

COM port	(for example COM1 or COM2, to which the MP.11 serial port is connected)
Bits per second	9600
Data bits	8
Stop bits	1
Flow control	None
Parity	None

3. Press the **RESET** button on the MP.11/a unit; the terminal program displays Power On Self Test (POST) messages.

4. When the **`Sending Traps to SNMP manager periodically`** message is displayed after about 30 seconds, press the **ENTER** key.

5. The command prompt is displayed; enter the following commands:

```
set ipaddr <IP address MP.11>
set ipsubmask <subnet mask>
set ipaddrtype static
set tftpipaddr <IP address TFTP server>
set tftpfilename <image file name>
set ipgw <gateway IP address>
reboot
```

For example:

```
set ipaddr 10.0.0.12
set ipsubmask 255.255.255.0
set ipaddrtype static
set tftpipaddr 10.0.0.20
set tftpfilename image.bin
set ipgw 10.0.0.30
reboot
```

The MP.11/a reboots and downloads the image file. The TFTP server program should show download activity after a few seconds. When the download is complete, the MP.11/a is ready for configuration.

To access the MP.11/a see "Chapter 3. Management Overview" on page 19. Note that the IP configuration in normal operation differs from the IP configuration of the Boot Loader.

Chapter 8. Specifications

This chapter provides Hardware and Radio Specifications.

HARDWARE SPECIFICATIONS

Physical Specifications (without metal base)	
Dimensions (h x w x l)	3.5 x 17 x 21.5 cm (1.5 x 6.75 x 8.5 in.)
Weight	0.68 kg (1.5 lb.)
Electrical Specifications	
Using the Power Adapter	
Voltage (Input)	100 to 240 VAC (50-60 Hz) @ 0.4 A
Voltage (Output)	12 VDC
Power Consumption	10 Watts (maximum)
Using Active Ethernet	
Input Voltage	42 to 60 VDC
Output Current	200mA at 48V
Power Consumption	10 Watts
Environmental Specifications	
Operating Temperature	0º to 55º C ambient temperature (without plastic cabinet)
Operating Humidity	95% maximum (non-condensing)
Storage Temperature	-20º to +75º C ambient temperature
Storage Humidity	95% maximum (non-condensing)
Interfaces	
Ethernet	10/100 Base-TX, RJ-45 female socket
Serial port	Standard RS-232C interface with DB-9, female connector
Active Ethernet	Category 5, foiled, twisted pair cables must be used to ensure compliance with FCC Part 15, subpart B, Class B requirements. Standard 802.3af pin assignments.
Wireless	Mini PC Card

RADIO SPECIFICATIONS

Channel Frequencies

The following table shows MP.11 (802.11b) channel allocations that vary from country to country. Values listed in bold indicate default channels and frequencies.

Channel ID	FCC/World (GHz)	ETSI (GHz)	France (GHz)	Japan (GHz)
1	2.412	2.412	--	2.412
2	2.417	2.417	--	2.417
3 (default in most countries)	**2.422**	**2.422**	**--**	**2.422**
4	2.427	2.427	--	2.427
5	2.432	2.432	--	2.432
6	2.437	2.437	--	2.437
7	2.442	2.442	--	2.442
8	2.447	2.447	--	2.447
9	2.452	2.452	--	2.452
10	2.457	2.457	2.457	2.457
11 (default in France)	2.462	2.462	**2.462**	2.462
12	--	2.467	2.467	2.467
13	--	2.472	2.472	2.472
14				2.484

The following table shows MP.11a (802.11a) channel allocations that vary from country to country. Values listed in bold indicate default channels and frequencies.

Channel ID	FCC	ETSI
56	5.280	—
60	5.300	—
64	5.320	—
100	—	5.500
104	—	5.520
108	—	5.540
112	—	5.560
116	—	5.580
120	—	5.600
124	—	5.620
128	—	5.640
132	—	5.660
136	—	5.680
149	5.745	—
153	5.765	—
157	5.785	—
161	5.805	—
165	5.825	—

Turbo Mode Channels	
Channel ID	FCC
1	5.290*
2	5.300
3	5.760
4	5.800

* Turbo channel ID 1, 5.290 – The MP.11a firmware limits the upper limit of this channel to be below 12.13 dBm for release in the United States and Canada.

Chapter 9. Troubleshooting

This chapter helps you to isolate and solve problems with your MP.11/a. In the event this chapter does not provide a solution, or the solution does not solve your problem, check our website:

http://www.proxim.com/support

Before you start troubleshooting, it is important that you have checked the details in the user's guides and manuals. For details about RADIUS, TFTP, terminal and telnet programs, and Web browsers, please refer to their appropriate documentation.

The following sections can help to solve your problem:

- LED Indicators below
- MP.11/a Connectivity Issues on page 113
- Setup and Configuration Issues on page 115

In some cases, rebooting the MP.11/a clears the problem. If nothing else helps, consider a "Soft Reset to Factory Defaults" (on page 29) or a "Forced Reload" (on page 107). The Forced Reload option requires you to download a new image file to the MP.11/a.

LED INDICATORS

The following table shows the status of the four LEDs when the MP.11/a is operational (the fourth LED is unused).

Power	
OFF	No power is present or malfunctioning.
GREEN	Power is present; the unit is operational.
AMBER	The unit is initializing after reboot (less than two minutes); it cannot get a dynamic IP address or is in Forced Reload state when Ethernet LED also is amber.*
RED	A fatal error in the unit.
Ethernet Link	
OFF	Not connected.
GREEN	Connected at 10 Mbps.
BLINKING GREEN	Data is being sent.
AMBER	Connected at 100 Mbps, in Forced Reload state when Power LED also is amber*, or the unit is initializing after reboot (less than two minutes).
BLINKING AMBER	Data is being sent.
RED	An error in data transfer.
Wireless Link	
OFF	Wireless interface is up properly but no wireless link established.
GREEN	Immediately after connecting a wireless link.
BLINKING GREEN	Data is being sent or the wireless interface is initializing after reboot (less than two minutes).
RED	There is a fatal error on the wireless interface.
* See "Forced Reload" on page 107.	

MP.11 CONNECTIVITY ISSUES

The issues described in this section relate to the connections of the MP.11/a.

MP.11 Does Not Boot

The MP.11 shows no activity (the power LED is off).

1. Ensure that the power supply is properly working and correctly connected.
2. Ensure that all cables are correctly connected.
3. Check the power source.
4. If you are using an Active Ethernet splitter, ensure that the voltage is correct.

Serial Link Does Not Work

The MP.11/a cannot be reached through the serial port.

1. Check the cable connection between the MP.11/a and the computer.

2. Ensure that the correct COM port is used.

3. Start the terminal program; set the following connection properties (also see “HyperTerminal Connection Properties”), and then connect.

COM port	For example, COM1 or COM2, to which the MP.11 serial port is connected
Bits per second	9600
Data bits	0
Stop bits	1
Flow control	None
Parity	None
Line ends	Carriage return with line feed

4. Ensure that the MP.11/a and the computer use the same serial port configuration parameters.

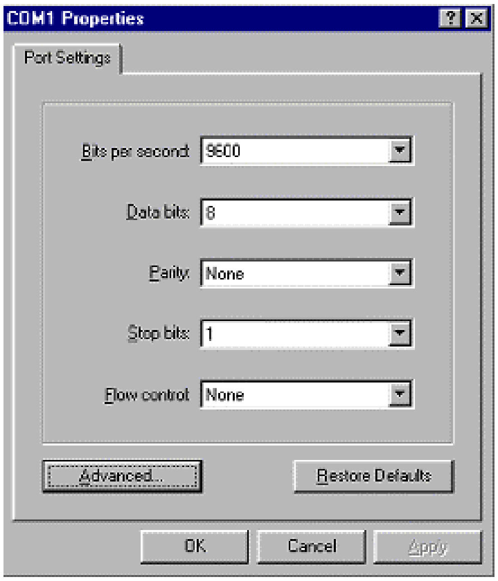
5. Press the RESET button on the MP.11/a unit. The terminal program displays Power On Self Tests (POST) messages and displays the following after approximately 90 seconds:

```
Please enter password:
```

HyperTerminal Connection Problems

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

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



COM1 Properties

Port Settings

Bits per second: 9600

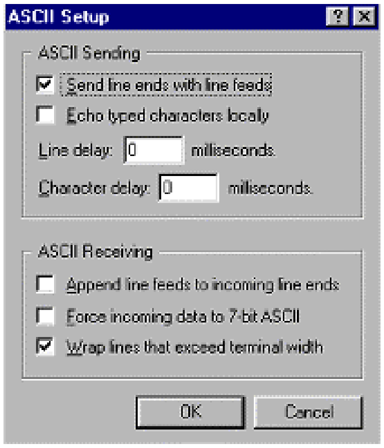
Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

3. Make the necessary changes and click **OK**.
4. Click the **Settings** tab and then **ASCII Setup…**. A window similar to the following is displayed:



ASCII Setup

ASCII Sending

☑ Send line ends with line feeds

☐ Echo typed characters locally

Line delay: 0 milliseconds.

Character delay: 0 milliseconds.

ASCII Receiving

☐ Append line feeds to incoming line ends

☐ Force incoming data to 7-bit ASCII

☑ Wrap lines that exceed terminal width

5. Ensure that **Send line ends with line feeds** is selected and click **OK** twice. HyperTerminal is now correctly configured.

Ethernet Link does not work

First check the Ethernet LED;

- Dim is “no media connected.”
- Green and steady is 10 Base-T
- Amber and steady is 100 Base-T
- Blinking Green or Amber is traffic

Verify pass-through versus cross-over cable.

Cannot use the Web Interface:

1. Open a command prompt window and enter **`ping`** `<ip address MP.11>` (for example **`ping 10.0.0.1`**). If the MP.11/a does not respond, make sure that you have the correct IP address. If the MP.11/a responds, the Ethernet connection is working properly, continue with this procedure.
2. Ensure that you are using one of the following Web browsers:
   - Microsoft Internet Explorer version 5.0 or later (Version 6.0 or later recommended)
   - Netscape version 6.0 or later.
3. Ensure that you are not using a proxy server for the connection with your Web browser.
4. Ensure that you have not exceeded the maximum number of Web Interface or CLI sessions (with the CLI command **show pelsessions**).
5. Double-check the physical network connections. Use a well known unit to ensure the network connection is properly functioning.
6. Perform network infrastructure troubleshooting (check switches, routers, and so on).

SETUP AND CONFIGURATION ISSUES

The following issues relate to setup and configuration problems.

Lost the MP.11/a Password

If you lost your password, you must reset the MP.11/a to the default settings. See “Hard Reset to Factory Default” on page 107. The default password is **public**.

If you record your password, keep it in a safe place.

The MP.11/a Responds Slowly

If the MP.11/a takes a long time to become available, it could mean that:

- No DHCP server is available.
- The IP address of the MP.11/a is already in use.

  Verify that the IP address is assigned only to the MP.11/a. Do this by switching off the MP.11/a and then pinging the IP address. If there is a response to the ping, another device in the network is using the same IP address. If the MP.11/a uses a static IP address, switching to DHCP mode could remedy this problem. Also see "Dynamic IP Address with DHCP" on page 21.
- There is too much network traffic.

Web Interface Does Not Work

If you cannot connect to the MP.11/a Web server through the network:

1. Connect a computer to the serial port of the MP.11/a and check the HTTP status. The HTTP status can restrict HTTP access at different interfaces. For more information, see "Serial Port" on page 25.
2. Open a command prompt window and enter:

   `ping` `<ip address MP.11>` (for example `ping 10.0.0.1`)

   If the MP.11/a does not respond, ensure that you have the correct IP address. If the MP.11/a responds, the Ethernet connection is working properly, continue with this procedure.
3. Ensure that you are using one of the following Web browsers:
   - Microsoft Internet Explorer version 5.0 or later (Version 6.0 or later recommended)
   - Netscape version 6.0 or later
4. Ensure that you are not using a proxy server for the connection with your Web browser (with the CLI command **`show pelsessions`**).
5. Ensure that you have not exceeded the maximum number of Web Interface sessions.

Command Line Interface Does Not Work

If you cannot connect to the MP.11/a through the network:

1. Connect a computer to the serial port of the MP.11/a and check the SNMP table. The SNMP table can restrict telnet or HTTP access. For more information, see “Serial Port” on page 25.
2. Open a command prompt window and enter: **`ping`** `<ip address MP.11>` (for example **`ping 10.0.0.1`**).
   - If the MP.11/a does not respond, ensure that you have the correct IP address.
   - If the MP.11/a responds, the Ethernet connection is working properly; continue with this procedure.
3. Ensure that you have not exceeded the maximum number of CLI sessions.

TFTP Server Does Not Work

With TFTP, you can transfer files to and from the MP.11/a. Also see “TFTP Server Setup” on page 104. If a TFTP server is not properly configured and running, you cannot upload and download files. The TFTP server:

- Can be situated either local or remote
- Must have a valid IP address
- Must be set for send and receive without time-out
- Must be running only during file upload and download

If TFTP server does not upload or download files, it could mean:

- The TFTP server is not running
- The IP address of the TFTP server is invalid
- The upload or download directory is not correctly set
- The file name is not correct

Online Help Is Not Available

Online help does not appear when the **?** (question mark) button is clicked in the Web Interface:

1. Make sure that the Help files are installed on your computer or server. Also see “Installing Documentation and Software”.
2. Verify whether the path of the help files in the Web Interface refers to the correct directory. See “Help” on page 79.

Changes Do Not Take Effect

Changes made in the Web Interface do not take effect:

1. Restart your Web browser. Log into the MP.11/a again and make changes. Reboot the MP.11/a when prompted to do so.

2. Wait until the reboot is completed before accessing the MP.11/a again.

Glossary

ARP

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

Authentication method

The process the MP.11/a 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; WORP only supports shared key because of security constraints.

Authentication server “Shared Secret”

This is a kind of password shared between the MP.11/a and the RADIUS authentication server. This password is used to encrypt important data exchanged between the MP.11/a 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.

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 (WORP), it is either a base or a satellite interface. A base interface controls the communication on the channel and is located in the central part of the network cell. Multiple satellites 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 a pool of IP addresses from which the MP.11/a can assign IP addresses to clients, which perform a DHCP Request.

Configuration Files

A configuration file contains the MP.11/a 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 MP.11/a for restoring the configuration.

DHCP Relay Agent

A feature of the MP.11/a that intercepts DHCP requests from clients and forwards them to a DHCP server. For the client, the DHCP Relay Agent of the MP.11/a 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 will be translated in 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 MP.11/a downloading means transferring a file from a TFTP server to the MP.11/a.

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 will broadcast a request that will be answered by a DHCP Server.

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 send across the network.

Ethernet

Ethernet is the most widely installed Local Area Network (LAN) technology. The MP.11/a 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 logical collection of network parameters. For example, the System Group is composed of several parameters and tables giving system information of the MP.11/a. 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 MP.11/a 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 MP.11/a software. To update the MP.11/a 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 MP.11/a. The MP.11/a 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 MP.11/a to enable these additional features.

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 MP.11/a specific objects. .

Network Mask

See **subnet mask**.

Parameter

A parameter is fundamental value that can be displayed and changed. For example, the MP.11/a 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 MP.11/a is password protected. To access the MP.11/a 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 satellite interface. For a base interface, the number of remotes is the number of satellites registered; for a satellite interface, there will be 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.

Satellite

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

ScanTool

A computer program that can be used to retrieve or set the IP address of a locally connected MP.11/a.

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 MP.11/a 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.

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**.

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 with the Web Interface, command line interface and SNMP.

Topology

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

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 MP.11/a; using the upload and download commands, the MP.11/a can respectively copy a file to or from a TFTP server. TFTP server software is provided on the MP.11/a CD-ROM.

Upload

Uploading a file means copying a file from a network device to a remote server. In case of the MP.11/a uploading means transferring a file from the MP.11/a 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**.

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.