

TrinityAE Release 2.6

Administrator's Reference Guide

Sales Office: **+1 (301) 975-1000**
Technical Support: **+1 (301) 975-1007**
E-mail: **support@patton.com**
WWW: **www.patton.com**

Patton Electronics Company, Inc.

7622 Rickenbacker Drive
Gaithersburg, MD 20879 USA
tel: +1 (301) 975-1000
fax: +1 (301) 869-9293
support: +1 (301) 975-1007
web: www.patton.com
e-mail: support@patton.com

Copyright

Copyright © 2012, Patton Electronics Company. All rights reserved.

Notice

The information in this document is subject to change without notice. Patton Electronics assumes no liability for errors that may appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license.

Supported Models

2884	2888	T7900
6081RC	3224	T7714
3034	3038	T7712

Software Versions 2.6 and earlier

Summary Table of Contents

1	Introduction	16
2	Tools	18
3	Authentication.....	26
4	Logging Management.....	33
5	SNMP Configuration	39
6	Interface Status.....	45
7	Network Time Protocol (NTP)	50
8	IP Address Configuration.....	55
9	VLAN Configuration.....	62
10	Bridge Group Configuration.....	68
11	Generic Routing Encapsulation (GRE)	78
12	PPP Configuration.....	82
13	PPTP Client Configuration.....	96
14	PPTP Server Configuration.....	102
15	ARP Table Management.....	110
16	DHCP Server Configuration.....	115
17	NAT and Port Forwarding	121
18	Route Configuration	133
19	RIP Configuration	139
20	Quality of Service (QoS)	148
21	Ingress Traffic Management (ACL)	156
22	Contacting Patton for assistance	165

Table of Contents

Audience.....	15
Structure.....	15
1 Introduction	16
Software Overview.....	17
Getting Started with the WMI	17
Logging in	17
Menu Structure	17
2 Tools	18
Overview.....	19
Web Management Interface (WMI)	20
Configuration Import/Export	20
Software Upgrade	20
Command Line Interface (CLI).....	22
Import/Export Commands	22
Show Commands	22
Copy Command	22
System Boot	22
Software Upgrade Commands	23
Software Upgrade Command	23
Show System Image Command	23
System Image Command	24
CLI Tools	25
Ping	25
Traceroute	25
Reload	25
3 Authentication.....	26
Overview.....	27
Configuration Overview	27
Web Management Interface (WMI)	28
Adding New Users	28
Deleting Users	29
Changing Passwords	29
Command Line Interface (CLI).....	30
Root Mode	30
Configuration Mode	31
Debugging Information	32
4 Logging Management.....	33
Overview.....	34
Web Management Interface (WMI)	35

Remote Log Configuration	35
Local Log Configuration	36
Log Definition Table	36
Local Log Viewer	37
Command Line Interface (CLI).....	38
Logging Configuration Commands	38
5 SNMP Configuration	39
Overview	40
Configuration Overview	40
Web Management Interface (WMI)	41
Configuring the Server	42
Managing SNMP Communities (SNMPv1 and SNMPv2)	42
Adding SNMP Communities	42
Deleting SNMP Communities	42
Managing SNMP Users (SNMPv3)	43
Adding SNMP Users	43
Deleting SNMP Users	43
Managing System Variables	43
Command Line Interface (CLI).....	44
SNMP commands	44
6 Interface Status	45
Overview	46
Web Management Interface (WMI)	47
Viewing Errors	47
Editing Interfaces	47
Command Line Interface (CLI).....	48
Root Mode	48
Configuration Mode	49
7 Network Time Protocol (NTP)	50
Overview	51
Web Management Interface (WMI)	52
Configuring modes	52
Adding an NTP server	52
Command Line Interface (CLI).....	53
Root Mode	53
Configuration Mode	53
Debugging Information	54
8 IP Address Configuration.....	55
Overview	56
Configuration Overview	56
Terms used with IP Interfaces	56
Web Management Interface (WMI).....	58

Adding an IP Interface	59
IP Configuration	59
Adding a DHCP Client	60
DHCP Configuration	60
Command Line Interface (CLI).....	61
IP Interface Commands	61
DHCP Client Commands	61
9 VLAN Configuration.....	62
Overview	63
Configuration Overview	63
Web Management Interface (WMI)	64
Create VLAN	64
Manage VLAN Interfaces	64
Command Line Interface (CLI).....	65
VLAN Configuration Commands	65
VLAN Configuration Example	65
Show VLAN Information	66
10 Bridge Group Configuration.....	68
Overview	69
Configuration Overview	69
Web Management Interface (WMI)	71
Bridge Group Configuration	72
Add/Configure Bridge Groups	72
Delete Bridge Groups	72
Manage Interfaces	72
STP Configuration	73
Set STP Parameters	73
Set STP Forwarding	73
Show STP Status Information	73
Manage MAC Addresses	74
Display MAC Address Information	74
Add MAC Filter Rules	74
Display/Delete MAC Filter Rules	74
Command Line Interface (CLI).....	75
Bridge Group Commands	75
11 Generic Routing Encapsulation (GRE)	78
Overview	79
Configuration Overview	79
Web Management Interface (WMI)	80
Creating GRE Interfaces	80
Deleting GRE Interfaces	80
Command Line Interface (CLI).....	81

12 PPP Configuration	82
Overview	83
Configuration Overview	83
Web Management Interface (WMI)	85
Configure PPP Authentication	85
Add PPP Interfaces	86
Status of PPP Interfaces	86
Delete PPP Interfaces	86
Configure PPP Interfaces	87
Command Line Interface (CLI).....	89
PPP Authentication Commands	89
PPP Configuration Commands	89
Creating the interface	90
Configuring PPP negotiation	90
Enabling PPP on HDLC interfaces	91
Configuring LCP	92
Configuring IPCP	93
Configuring BCP	94
Showing Configuration and Status	95
Debugging Commands	95
13 PPTP Client Configuration	96
Overview	97
Configuration Overview	98
Web Management Interface (WMI)	99
Creating PPTP Client Interfaces	99
Deleting PPTP Client Interfaces	100
Configuring PPTP Client Interfaces	100
Command Line Interface (CLI).....	101
14 PPTP Server Configuration	102
Overview	103
Configuration Overview	104
Web Management Interface (WMI)	106
Configuring the PPTP Server	106
Adding Users to the PPTP Server	107
Viewing Connections to the PPTP Server	107
Command Line Interface (CLI).....	108
15 ARP Table Management	110
Overview	111
Configuration Overview	111
About ARP Entries	111
Web Management Interface (WMI)	112
Adding ARP Entries	112
Deleting ARP Entries	112

Command Line Interface (CLI).....	113
Adding ARP Entries	113
Deleting ARP Entries	113
Displaying ARP Entries	113
16 DHCP Server Configuration.....	115
Overview	116
Configuration Overview	116
Web Management Interface	117
Configuring the DHCP Server	117
Add/Delete Routers	118
Add/Delete DNSs	118
Add/Delete Static Leases	118
Command Line Interface (CLI).....	119
DHCP Server Configuration Commands	119
DHCP Debugging Commands	120
17 NAT and Port Forwarding	121
Overview	122
Configuration Overview	122
About NAT	122
About Port Forwarding	122
Web Management Interface (WMI)	123
NAPT	123
Creating NAPT Profiles	123
Deleting NAPT Profiles	123
Editing NAPT Profiles	124
Port Forwarding	125
Creating Port Forwarding Profiles	125
Deleting Port Forwarding Profiles	125
Editing Port Forwarding Profiles	125
Connection Tracking	126
Command Line Interface (CLI).....	127
NAPT	127
NAPT Configuration Commands	127
NAPT Profile Configuration Commands	127
NAPT CLI Examples	128
Port Forwarding	130
Port Forwarding Configuration Commands	130
Port Forwarding Profile Configuration Commands	130
Port Forwarding CLI Examples	131
Connection Tracking	132
Connection Tracking Configuration Commands	132
Connection Tracking CLI Examples	132
18 Route Configuration	133

Overview	134
Configuration Overview	134
About Flags	134
Web Management Interface (WMI)	136
Adding a route	136
Deleting a route	136
Command Line Interface (CLI).....	137
Adding a route	137
Deleting a route	137
Displaying Routes	138
19 RIP Configuration	139
Overview	140
Configuration Overview	140
About RIP Features	140
Web Management Interface (WMI)	142
Manage RIP	143
Route Redistribution	143
Networks	143
Neighbors	143
Timers	144
Passive Interfaces	144
Configure Interface	144
Command Line Interface (CLI).....	145
Root Mode	145
Configuration Mode	145
RIP Configuration Mode	146
Interface Configuration Mode	147
20 Quality of Service (QoS)	148
Overview	149
Configuration Overview	149
About QoS classes	149
Web Management Interface (WMI)	151
QoS Profiles	151
Adding QoS Profiles	151
Deleting QoS Profiles	151
Cloning QoS Profiles	152
QoS Classes	152
Adding QoS Classes	152
Displaying/Deleting QoS Classes	153
Manage Interfaces	153
Command Line Interface (CLI).....	154
QoS Configuration Commands	154
Show traffic classes of a profile	155

Show QoS configuration	155
21 Ingress Traffic Management (ACL)	156
Overview	157
Configuration Overview	157
About packet actions	157
About packet matches	158
Web Management Interface (WMI)	159
Access Control Profiles	160
Adding Access Control Profile	160
Cloning Access Control Profiles	160
Deleting Access Control Profiles	160
Adding Policing Rules	160
Manage Policing Rules	161
Access Control Rules	161
Adding Access Control Rules	161
Displaying and Deleting Access Control Rules	162
Manage Interfaces	162
Command Line Interface (CLI).....	163
ACL Configuration Commands	163
Show access control rules of a profile	164
Show ACL configuration	164
22 Contacting Patton for assistance	165
Introduction	166
Contact information.....	166
Warranty Service and Returned Merchandise Authorizations (RMAs).....	166
Warranty coverage	166
Out-of-warranty service	166
Returns for credit	166
Return for credit policy	167
RMA numbers	167
Shipping instructions	167

List of Figures

1	WMI Menu Structure	17
2	Configuration	20
3	Software Upgrade	20
4	Authentication main page	28
5	Add a new user	28
6	Deleting a user	29
7	Change Passwords	29
8	Authentication - CLI	32
9	Logging Management main page	35
10	Local Log Definition	36
11	Local Log Viewer	37
12	SNMP main page	41
13	SNMP Communities	42
14	SNMP Users	43
15	System Variables	43
16	Interface Status main page	47
17	Editing an Ethernet interface from the status page	47
18	NTP main page	52
19	Configuring modes	52
20	Adding an NTP server	52
21	IP Address Configuration main page	58
22	Adding an IP interface	59
23	IP Configuration	59
24	Adding a DHCP client	60
25	DHCP configuration	60
26	VLAN Configuration main page	64
27	Create VLAN	64
28	VLAN Interfaces	64
29	Bridge Group Configuration main page	71
30	Managing interfaces	72
31	STP Configuration	73
32	Displaying MAC address information	74
33	Configuring MAC filter rules	74
34	Show MAC address forwarding database	76
35	Show STP configuration	76
36	Configure and show MAC filter information	77
37	Show interface configuration	77
38	GRE Interface Configuration	80
39	Creating a GRE interface	80
40	Deleting a GRE interface	80
41	PPP Authentication Configuration	85
42	Add/Delete PPP Interfaces	86
43	Configuring a PPP interface	87
44	PPTP Work-from-home application	97
45	PPTP remote application	98
46	PPTP Client main page	99
47	Create PPTP Client Interfaces	99

48	Delete PPTP Client Interfaces	100
49	Configure existing PPTP Client interfaces	100
50	PPTP Work-from-home application	103
51	PPTP remote application	104
52	PPTP Server main page	106
53	Configuring and updating the PPTP Server	106
54	Adding users to the PPTP Server	107
55	Viewing connections to the PPTP Server	107
56	ARP main page	112
57	Deleting an ARP entry from the ARP table	112
58	Command Line Interface "show arp" command	114
59	DHCP Server Configuraion Main Screen	117
60	NAT Configuraion	123
61	NAT Profile Configuration	124
62	Main Port Forwarding Configuration	125
63	Port Forwarding Profile Configuration	125
64	Connection Tracking Configuration	126
65	Route Configuration main page	136
66	Route Configuration Flags	136
67	Command Line Interface "show route" command	138
68	RIP Configuration	142
69	Configure Interface	144
70	QoS main page	151
71	QoS Classes	152
72	Manage Interfaces	153
73	Show traffic classes of a profile	155
74	Show QoS configuration	155
75	Ingress Traffic Management main page	159
76	Managing Access Control Profiles	160
77	Managing ACL rules	161
78	Managing interfaces	162
79	Show access control rules of a profile	164
80	Show ACL configuration	164

List of Tables

1	Show Import/Export - CLI Commands	22
2	Copy Import/Export - CLI Commands	22
3	Software Upgrade - CLI Command	23
4	Show System Image - CLI Command	23
5	System Image - CLI Command	24
6	Ping - CLI Command	25
7	Traceroute - CLI Command	25
8	Reload - CLI Command	25
9	Authentication Root Mode - CLI Commands	30
10	Authentication Configuration Mode - CLI Commands	31
11	Logging - CLI Commands	38
12	SNMP - CLI Commands	44
13	Interface Root Mode - CLI Commands	48
14	Interface Configuration Mode - CLI Commands	49
15	NTP Root Mode - CLI Commands	53
16	NTP Configuration Mode - CLI Commands	53
17	NTP Debugging - CLI	54
18	IP Interface - CLI Commands	61
19	DHCP client - CLI Commands	61
20	VLAN - CLI Commands	65
21	Show VLAN Information - CLI Commands	66
22	Bridge Group Configuration - CLI Commands	75
23	GRE Interfaces - CLI Commands	81
24	Steps for Configuring PPP Authentication - CLI	89
25	Steps for Creating a PPP Interface - CLI	90
26	Steps for Configuring PPP Negotiation - CLI	90
27	Steps for Enabling PPP on HDLC interfaces - CLI	91
28	Steps for Configuring LCP - CLI	92
29	Steps for Configuring IPCP - CLI	93
30	Steps for Configuring BCP - CLI	94
31	Showing PPP Configuration and Status	95
32	PPP Debugging Commands - CLI	95
33	PPTP Client Commands - CLI	101
34	PPTP Server Commands - CLI	108
35	ARP - CLI	113
36	Adding ARP Entries - CLI	113
37	Deleting ARP Entries - CLI	113
38	Showing ARP Entries - CLI	113
39	DHCP Server - CLI Commands	119
40	DHCP Debugging - CLI	120
41	NAT Configuration - CLI Commands	127
42	NAT Profile Configuration - CLI Commands	127
43	Port Forwarding Configuration - CLI Commands	130

44	Port Forwarding Profile Configuration - CLI Commands	130
45	Connection Tracking Configuration - CLI Commands	132
46	Route Configuration - CLI Commands	137
47	Showing Routes - CLI	138
48	RIP Root Mode - CLI Command	145
49	RIP Configuration Mode - CLI Command	145
50	RIP Configuration Mode - CLI Commands	146
51	RIP Interface Configuration Mode - CLI Commands	147
52	Match values for QoS	150
53	QoS - CLI Commands	154
54	ACL - CLI Commands	163

About this guide

This *TrinityAE Administrator's Reference Guide* describes how to configure components through both the Web Management Interface (WMI) and the Command Line Interface (CLI) of Patton's Trinity system.

For detailed hardware or set-up information, refer to the product's *User Manual*, available online at www.patton.com/manuals.

Audience

This guide is intended for the following users:

- Operators
- Installers
- Maintenance technicians

Structure

This guide contains the following chapters and appendices:

- [Chapter 1](#) on page 16 provides an overview about the software
- [Chapter 2](#) on page 18 provides information on import/export, software upgrade, and special CLI features
- [Chapter 3](#) on page 26 provides information on managing the authentication of users and privileges
- [Chapter 4](#) on page 33 provides information on syslog functions
- [Chapter 5](#) on page 39 provides information about configuring SNMP
- [Chapter 6](#) on page 45 provides information on the status of interfaces
- [Chapter 7](#) on page 50 provides information about configuring NTP
- [Chapter 8](#) on page 55 provides information on IP commands
- [Chapter 9](#) on page 62 provides information on managing VLANs
- [Chapter 10](#) on page 68 provides information on configuring bridge groups
- [Chapter 11](#) on page 78 provides information on configuring Generic Routing Encapsulation (GRE)
- [Chapter 12](#) on page 82 provides information on configuring PPP
- [Chapter 13](#) on page 96 provides information on configuring the PPTP client
- [Chapter 14](#) on page 102 provides information on configuring the PPTP server
- [Chapter 15](#) on page 110 provides information on the ARP Table Management component
- [Chapter 16](#) on page 115 provides information on configuring the DHCP server
- [Chapter 17](#) on page 121 provides information on NAT and Port Forwarding
- [Chapter 18](#) on page 133 provides information on configuring the route table
- [Chapter 19](#) on page 139 provides information on configuring RIP
- [Chapter 20](#) on page 148 provides information on managing egress (QoS) traffic
- [Chapter 21](#) on page 156 provides information on managing ingress (ACL) traffic
- [Chapter 22](#) on page 165 provides information on contacting Patton for service and support

Chapter 1 **Introduction**

Chapter contents

Software Overview	17
Getting Started with the WMI	17
Logging in	17
Menu Structure	17

Software Overview

This *TrinityAE Administrator's Reference Guide* provides information about configuring the software for your Trinity model. For information about setting up the unit, or for hardware specifications, refer to the model's *User Manual*, available online at www.patton.com/manuals.

Note Some Trinity features only apply to specific models. The configuration information for these features are located in separate appendices related to the *TrinityAE Administrator's Reference Guide*. You can find relevant Trinity appendices online at www.patton.com/manuals.

Getting Started with the WMI

Logging in

To get started with the Web Management Interface (WMI), log into the unit using:

Username: admin

Password: <Leave blank.>

To add users, delete users, or set user privileges, see Chapter 3, “Authentication” on page 26.

Menu Structure

The main menu has the following options (figure 1) The main menu for your model may vary.

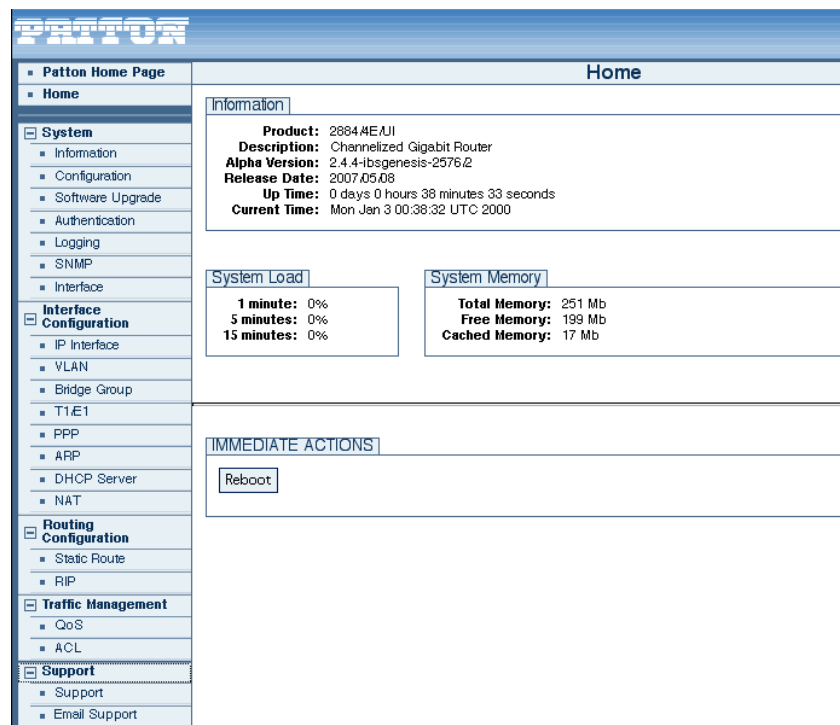


Figure 1. WMI Menu Structure

Chapter 2 **Tools**

Chapter contents

Overview	19
Web Management Interface (WMI)	20
Configuration Import/Export	20
Software Upgrade	20
Command Line Interface (CLI).....	22
Import/Export Commands	22
Show Commands	22
Copy Command	22
System Boot	22
Software Upgrade Commands	23
Software Upgrade Command	23
Show System Image Command	23
System Image Command	24
CLI Tools	25
Ping	25
Traceroute	25
Reload	25

Overview

This chapter describes the web management and configuration commands for importing/exporting configurations, upgrading the software, and other CLI tools, such as ping, traceroute, and reload.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

To import or export a configuration using the WMI, see “[Configuration Import/Export](#)” on page 20.

To import or export a configuration using the CLI, see “[Import/Export Commands](#)” on page 22.

To upgrade the software using the WMI, see “[Software Upgrade](#)” on page 20.

To upgrade the software using the CLI, see “[Software Upgrade Commands](#)” on page 23.

To ping an IP address, see “[Ping](#)” on page 25.

To trace the path of a route, see “[Traceroute](#)” on page 25.

To force the system to reboot, see “[Reload](#)” on page 25.

Web Management Interface (WMI)

Configuration Import/Export

To access the Configuration page, click on **System > Configuration** from the main menu.

Configuration File Name	Source	Dest.	Erase	Download	Preview
test-config			<input type="checkbox"/>	Download	Preview
minimal-config				Download	Preview
shipping-config				Download	Preview
newmultilink-config			<input checked="" type="checkbox"/>	Download	Preview
pppbcp-config			<input type="checkbox"/>	Download	Preview
multilink-config			<input checked="" type="checkbox"/>	Download	Preview
fulllink-config			<input type="checkbox"/>	Download	Preview
ipcp-config			<input checked="" type="checkbox"/>	Download	Preview
running-config			<input type="checkbox"/>	Download	Preview
startup-config			<input checked="" type="checkbox"/>	Download	Preview

Figure 2. Configuration

To import a configuration, click **Browse** to find the configuration file to import, then click **Upload**.

To export a configuration, click the **Download** link next to the configuration file under **File Management**.

Software Upgrade

A unit's software image may be upgraded to a newer software version. New software versions are posted on the Patton Electronics website as features are added and bugs are fixed. Both the web management interface and the command line interface provide the functionality to upgrade the software.

To access the Software Upgrade page, click on **System > Software Upgrade** from the main menu on the left of the screen.

Figure 3. Software Upgrade

During the upgrade, the box will be unresponsive; the web server and telnet server will be shut down. When the upgrade completes, the unit will automatically reboot into the new software and become operational again.

To upgrade the software, click the **Browse** button to select the software image file, then click **Submit** to start the upgrade.

Note The software upgrade uses the *.tar file. Do not extract the contents of this file.

Command Line Interface (CLI)

Import/Export Commands

The following commands describe how to print and copy configuration files using the CLI.

Show Commands

Table 1. Show Import/Export - CLI Commands

Command	Explanation
Trinity# show shipping-config	Prints the shipping configuration (static file).
Trinity# show running-config	Prints the current system config (dynamically generated).
Trinity# show startup-config	Prints the startup configuration (user-updated file).
Trinity# show minimal-config	Prints the minimal configuration (static file).

Copy Command

Table 2. Copy Import/Export - CLI Commands

Command	Explanation
Trinity# copy {running-config shipping-config minimal-config} startup-config	Copies the contents of the minimal-config file or running configuration to the startup configuration file. The startup configuration file will be read at the next boot.

System Boot

During the boot sequence, the contents of the startup configuration file will be applied to the system. Any errors found in the configuration file will be reported, as shown in the example below:

```
Attempting to restore config from /flash/config/startup-config ...
Error Importing Line(12): Invalid Command!
[[ no enable test-server ]]
```


Image Overview

Number of Images: 2
 Current Image: 1
 Next Image: 1

Image #1

Image State: active
 Load Date: Sun Feb 10 07:41:32 2030
 Release Date: Thu May 10 14:53:03 2007
 Image Name: hornet5261_full_image
 Patton Version: 2.4.4

Image #2

Image State: inactive
 Load Date: Tue Jan 22 11:25:29 2030
 Release Date: Thu May 31 16:58:32 2007
 Image Name: hornet5261_full_image
 Patton Version: 2.4

System Image Command

Table 5. System Image - CLI Command

Command	Explanation
Trinity[config]# system image {1 2}	To begin using the software that was just installed, select the system image that is currently inactive, and then reboot.

Note

- Only one software upgrade may be performed at a time. Otherwise, the flash could be corrupted. Both the web interface and command line interface will prevent concurrent upgrades.
- Some models may shut down several services during the upgrade and cannot be counted on to function properly until after the software upgrade completes.
- The config partition is not affected by the software upgrade unless specified by the user.

CLI Tools

Ping

Table 6. Ping - CLI Command

Command	Explanation
Trinity# ping <ip address> [<count> continuous]	Sends ICMP Echo requests to an ip address (broadcast address accepted). The user can optionally specify a number of echo requests to send, or send requests continuously. (CTRL-C will cancel the command in progress.)

```
Trinity# ping 10.11.2.2
PING 10.11.2.2 (10.11.2.2): 56 data bytes
64 bytes from 10.11.2.2: icmp_seq=0 ttl=128 time=17.3 ms
64 bytes from 10.11.2.2: icmp_seq=1 ttl=128 time=3.1 ms
64 bytes from 10.11.2.2: icmp_seq=2 ttl=128 time=2.5 ms
64 bytes from 10.11.2.2: icmp_seq=3 ttl=128 time=3.3 ms
64 bytes from 10.11.2.2: icmp_seq=4 ttl=128 time=4.0 ms

--- 10.11.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.5/6.0/17.3 ms
```

Traceroute

Table 7. Traceroute - CLI Command

Command	Explanation
Trinity# traceroute <ip address>	Traces the hops from the device to an Internet address. (CTRL-C will cancel the command in progress.)

```
Trinity# traceroute 10.10.1.1
 1 192.168.85.2 (192.168.85.2) 11.963 ms 1.024 ms 0.769 ms
 2 10.11.2.1 (10.11.2.1) 3.01 ms 2.725 ms 2.434 ms
 3 10.11.1.1 (10.11.1.1) 3.935 ms 1.585 ms 1.709 ms
 4 10.10.1.1 (10.10.1.1) 3.528 ms * 5.536 ms
```

Reload

Table 8. Reload - CLI Command

Command	Explanation
Trinity# reload [in <seconds> cancel]	Forces the system to reboot. The user can optionally delay the reboot by a number of seconds or cancel a pending reboot.

Chapter 3 **Authentication**

Chapter contents

Overview	27
Configuration Overview	27
Web Management Interface (WMI)	28
Adding New Users	28
Deleting Users	29
Changing Passwords	29
Command Line Interface (CLI).....	30
Root Mode	30
Configuration Mode	31
Debugging Information	32

Overview

This chapter describes how to specify the configuration settings for creating/deleting system users, setting user privilege levels, and displaying existing users.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

Configuration Overview

A new user can be added to the system through configuration of one or a combination of the following parameters:

- **Username** (required): The unique identifier for the user. It must be an alphanumeric string from the set of characters [0-9a-zA-Z] with no spaces. The maximum allowed length is 32 characters.
- **Password** (optional): User password associated with the user account. It must be an alphanumeric string from the set of characters [0-9a-zA-Z] with no spaces. The maximum allowed length is 32 characters. It is possible to allow an empty password field by choosing the no password option from the Web GUI. In this case, no password would be required for login.
- **Privilege** (required): The access group/level associated with the user account. Two user access groups are provided:
 - **Superuser access group**: Allows for read/write access to the system.
 - **Monitor access group**: Allows for read-only access to the system.
- **Description** (optional): A short description for the user account. This option is currently available through the WMI only. The alphanumeric string can have a maximum length of 32 characters.

Users can be deleted from the system by specifying the username. Add/Delete user operations require superuser or engineer access level. The show feature displays a list of the existing system users, their privilege level, and the description field.

To configure Authentication through the WMI, see the section "[Web Management Interface \(WMI\)](#)" on page 28.

To configure Authentication through the CLI, see the section "[Command Line Interface \(CLI\)](#)" on page 30.

Web Management Interface (WMI)

To access the Authentication main page, click on **System > Authentication** from the main menu.

The screenshot shows the Patton WMI Authentication page. The left sidebar contains a navigation menu with the following items: Patton Home Page, Home, System (Information, Configuration, Software Upgrade, Authentication, Logging, SNMP, Interface), Interface Configuration, Routing Configuration, Traffic Management, Support (Support, Email Support), and footer information for Patton Electronics Co. © 2005-2007.

The main content area is titled "Authentication" and contains three sections:

- Create New User:** A form with fields for Username, Password, Privilege (set to superuser), and Description. There is a "No Password" checkbox and an "Add" button.
- Change Password:** A form with fields for Username, Old Password, and New Password. There is a "No Password" checkbox and a "Submit" button.
- Currently Defined Users:** A table listing existing users with columns for Username, Privilege, Description, and Delete. Below the table is a "Delete" button.

Username	Privilege	Description	Delete
admin	superuser	system user	<input type="checkbox"/>
monitor	monitor	system user	<input type="checkbox"/>

Figure 4. Authentication main page

Adding New Users

To add a new user:

1. Type the name of the user into the **Username** field.
2. If desired, enter a password for the user. If no password is desired, select the **No Password** checkbox.
3. Select an access group for the user from the **Privilege** drop-down menu.
4. Enter a description of the user account (optional).
5. Click the **Add** button.

This is a close-up of the "Create New User" form. It includes the following fields and controls:

- Username:** A text input field.
- Password:** A text input field.
- No Password:** A checkbox.
- Privilege:** A drop-down menu currently showing "superuser".
- Description:** A text input field.
- Add:** A button to submit the form.

Figure 5. Add a new user

Deleting Users

To delete a user:

1. Select the **Delete** checkbox of the user from the Currently Defined Users table.
2. Click the **Delete** button.

Currently Defined Users			
Username	Privilege	Description	Delete
admin	superuser	system user	<input type="checkbox"/>
monitor	monitor	system user	<input checked="" type="checkbox"/>

Figure 6. Deleting a user

Changing Passwords

To change a password:

1. Enter the username in the **Username** field.
2. Enter the old password of the user in the **Old Password** field.
3. Enter the new password in the **New Password** field, or check **No Password**.
4. Click **Submit**.

Change Password	
Username:	<input type="text"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
No Password:	<input type="checkbox"/>
<input type="button" value="Submit"/>	

Figure 7. Change Passwords

Command Line Interface (CLI)

The CLI configuration is slightly different from the WMI when configuring authentication features. When adding a new user from the CLI, the command line does not allow for a "description" field to be entered for new users. All users are added to the system with the description *system user*.

The CLI provides an extra option to allow passwords to be submitted in MD5 encrypted form. This feature is not meant to be used for creating new users, but for administrators exporting/importing previously saved configurations to the system.

Root Mode

Table 9. Authentication Root Mode - CLI Commands

Command	Explanation
Trinity# configure	Enter the Configuration Mode.
Trinity# show	Enter the Show Mode.
Trinity# show users	Display currently defined system users.

Configuration Mode

Table 10. Authentication Configuration Mode - CLI Commands

Command	Explanation
Trinity[config]# username <name> nopassword privilege <level>	Add a new user with username <name> and privilege level <level>. Available privilege levels are superuser and monitor. No password would be required for login with this command.
Trinity[config]# username <name> password <plain-text> privilege <level>	Add a new user with username <name>, password <plain-text>, and privilege level <level>. Available privilege levels are superuser and monitor. User password is accepted as plain-text, but will be stored as MD5-hash.
Trinity[config]# username <name> password <encryption-type> <encrypted-password> privilege <level>	Add a new user with username <name>, an encrypted password <encrypted-password>, and privilege level <level>. Available privilege levels are superuser and monitor. Currently, the only available encryption type is MD5. The submitted password must be the MD5-hash form of the plain-text password.
Trinity[config]# username <name> changepassword <old password-plain-text> <new password-plain-text>	Change the password of the user with username <name> from <old-plain-text> to <new-plain-text>.
Trinity[config]# username <name> changepassword <old password-plain-text> nopassword	Change the password of the user with username <name> from <old-plain-text> to empty field.
Trinity[config]# no username <name>	Remove a user with username <name> from the system.

```
Trinity#
Trinity#
Trinity# configure
Trinity[config]# username customer
changepassword    Change password for this username.
nopassword        No password is required for login.
password          Specify a password for this username.
Trinity[config]# username customer nopassword
privilege         Specify user access privilege.
Trinity[config]# username customer nopassword privilege
superuser         Privilege level for this username.
monitor           Privilege level for this username.
Trinity[config]# username customer nopassword privilege monitor
<cr>
Trinity[config]# username customer nopassword privilege monitor
Trinity[config]# show users
System Users
      Username      Privilege      Description
      admin         superuser      system user
      monitor        monitor        system user
      customer       monitor        system user
Trinity[config]# █
```

Figure 8. Authentication - CLI

Debugging Information

The Authentication Manager reports the following debugging information:

- All system level failures are reported as LOG_ERR level SYSLOG messages.
- All failures in authentication and authorization –failing to authenticate, validate, renew, or get session keys– are reported as LOG_WARNING level SYSLOG messages. These are not messages indicating an error in the operation of the framework but rather warnings for possible attempts to breach system security or invalid user/component behavior that requires attention.
- All other messages are DEBUG/INFO level messages. They are meant to provide information on the flow of events through the system.

Chapter 4 **Logging Management**

Chapter contents

Overview	34
Web Management Interface (WMI)	35
Remote Log Configuration	35
Local Log Configuration	36
Log Definition Table	36
Local Log Viewer	37
Command Line Interface (CLI).....	38
Logging Configuration Commands	38

Overview

This chapter describes logging functions.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

To manage logging through the WMI, see the section “[Web Management Interface \(WMI\)](#)” on page 35.

To manage logging through the CLI, see the section “[Command Line Interface \(CLI\)](#)” on page 38.

Web Management Interface (WMI)

To access the Logging Management main page, click on **System > Logging** from the main menu.

The screenshot shows the Patton Logging Management interface. The left sidebar contains a navigation menu with the following items: Patton Home Page, Home, System (Information, Configuration, Software Upgrade, Authentication, Logging, SNMP, Interface), Interface Configuration, Routing Configuration, Traffic Management, Support (Support, Email Support), and footer information for Patton Electronics Co. © 2005-2007 Terms & Conditions.

The main content area is titled "Logging Management" and has three tabs: "Remote Log Definition" (selected), "Local Log Definition", and "Local Log Viewer".

Under the "Remote Log Definition" tab, there is a "Filter Definition" form with the following fields:

- Destination IP: [Text Input]
- Protocol: tcp (dropdown)
- Port: 514 (Text Input)
- Priority: err (dropdown)
- [Add] button

Below the form is a "Log Definition Table":

Destination IP/Local Log File Name	Protocol	Port/Line Count	Priority	Delete
syslog	file	200	warn	<input type="checkbox"/>

[Delete] button

Figure 9. Logging Management main page

Remote Log Configuration

To configure the remote log, fill in the following:

- **Destination IP:** IP address of the remote syslog server (in dotted quad format)
- **Protocol:** IP protocol that the remote server is listening on (tcp or udp)
- **Port:** IP port that the remote server is listening on (1-65535)
- **Priority:** The minimum syslog priority of messages to send (emerg, alert, crit, err, warn, notice, info, debug)

Click the **Add** button to save the configuration.

Local Log Configuration

Use the Local Log Definition tab to save syslog messages as a local log file.

Note Only the syslog file is currently supported.

Remote Log Definition **Local Log Definition** Local Log Viewer

Filter Definition

Destination File: syslog

Protocol: file

Line Count: 20

Priority: err

Add

Log Definition Table

Destination IP/Local Log File Name	Protocol	Port/Line Count	Priority	Delete
syslog	file	200	warn	<input type="checkbox"/>

Delete

Figure 10. Local Log Definition

To configure the local log, fill in the following:

- **Destination File:** Name of the log file (Currently limited to *syslog*)
- **Protocol:** The file protocol (file)
- **Line Count:** The minimum number of lines in a log file before the system rotates it to backup. One backup log will be kept at all times. (20-200)
- **Priority:** The minimum syslog priority of messages to save (emerg, alert, crit, err, warn, notice, info, debug)

Click the **Add** button to save the configuration.

Log Definition Table

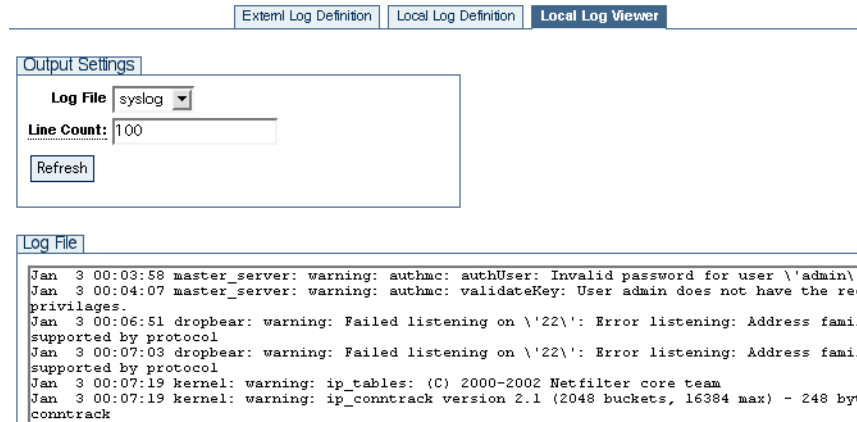
The Log Definition Table shows a list of currently configured logs and is shown on both the Remote and Local tabs. This table displays both log types simultaneously, and provides a Delete checkbox for each log file.

To delete a log file, select the **Delete** checkbox for that file, then click the **Delete** button.

Local Log Viewer

Use the Local Log Viewer tab to view the contents of a local log file. The system will automatically include the contents of the backup file (up to the total line count specified in the Line Count field).

Note Only the syslog file is currently supported.



The screenshot displays the 'Local Log Viewer' tab in a web interface. At the top, there are three tabs: 'External Log Definition', 'Local Log Definition', and 'Local Log Viewer'. Below the tabs is a section titled 'Output Settings' containing a 'Log File' dropdown menu set to 'syslog' and a 'Line Count' input field with the value '100'. A 'Refresh' button is located below these fields. Below the 'Output Settings' section is a 'Log File' section displaying a list of log entries in a monospaced font. The entries include timestamps, source identifiers, and warning messages from various system components like master_server, dropbear, and kernel.

```
Jan 3 00:03:58 master_server: warning: authmc: authUser: Invalid password for user \'admin\'.
Jan 3 00:04:07 master_server: warning: authmc: validateKey: User admin does not have the req
privileges.
Jan 3 00:06:51 dropbear: warning: Failed listening on \'22\': Error listening: Address famil
supported by protocol
Jan 3 00:07:03 dropbear: warning: Failed listening on \'22\': Error listening: Address famil
supported by protocol
Jan 3 00:07:19 kernel: warning: ip_tables: (C) 2000-2002 Netfilter core team
Jan 3 00:07:19 kernel: warning: ip_conntrack version 2.1 (2048 buckets, 16384 max) - 248 byt
conntrack
```

Figure 11. Local Log Viewer

Command Line Interface (CLI)

Logging Configuration Commands

Table 11. Logging - CLI Commands

Command	Explanation
Trinity[config]# [no] logging remote <ip address> [port <20-200>] [priority {<0-7> emerg alert crit err warn notice info debug}]	Adds a rule which sends syslog messages to a remote syslog file. Note: Currently this only supports the persistent files syslog.
Trinity[config]# [no] logging local {syslog} [lines <port number>] [priority {<0-7> emerg alert crit err warn notice info debug}] [protocol {tcp udp}]	Adds a rule that sends syslog messages to a local syslog server.
Trinity# show logging	Shows the list of defined local and remote logs.
Trinity# show logging local {syslog} [lines <2-20>]	Shows the contents of a local log file.

- Example - Trinity# show logging:

Destination IP/File	Protocol	Port/LnCnt	Priority
syslog	file	20	err
111.22.33.44	tcp	514	err
111.55.66.77	tcp	514	emerg

- Example - Trinity# show logging local:

```
Sep 11 19:12:28 kernel: err: VFS: Can't find ext3 filesystem on dev sda.
Sep 11 19:13:02 kernel: err: VFS: Can't find ext3 filesystem on dev sda.
Sep 11 19:13:08 kernel: err: VFS: Can't find ext3 filesystem on dev sda.
Sep 11 19:15:32 kernel: err: sda: assuming drive cache: write through
Sep 11 19:15:32 kernel: err: sda: assuming drive cache: write through
Sep 11 19:35:08 kernel: err: VFS: Can't find ext3 filesystem on dev sda.
Sep 11 19:35:57 kernel: err: VFS: Can't find ext3 filesystem on dev sda.
Sep 11 19:54:56 kernel: err: VFS: Can't find ext3 filesystem on dev sda.
```

Chapter 5 **SNMP Configuration**

Chapter contents

Overview	40
Configuration Overview	40
Web Management Interface (WMI)	41
Configuring the Server	42
Managing SNMP Communities (SNMPv1 and SNMPv2)	42
Adding SNMP Communities	42
Deleting SNMP Communities	42
Managing SNMP Users (SNMPv3)	43
Adding SNMP Users	43
Deleting SNMP Users	43
Managing System Variables	43
Command Line Interface (CLI).....	44
SNMP commands	44

Overview

This chapter describes how to configure Simple Network Management Protocol (SNMP) on the Trinity platform. SNMP allows for the exchange of management information between network devices.

Trinity supports the following SNMP MIBs:

- Standard MIB 2
- RFC 1406 - DS1 (T1/E1)

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

Configuration Overview

To monitor the device using SNMP:

1. Add the SNMPv1/2c communities and/or SNMPv3 users that may access the device.
2. Set the system variables: sysDescription, sysLocation, etc. (optional).
3. Enable the agent.

SNMPv1/2c communities may optionally be limited to certain IP addresses. By default, the IP address and netmask are set to 0.0.0.0, and requests from the community will be accepted regardless from where they originate. However, if the IP address and netmask are set, the request must originate from the designated address.

Once the steps above have been performed, an SNMP management entity may begin to monitor the device.

To configure SNMP through the WMI, see the section “[Web Management Interface \(WMI\)](#)” on page 41.

To configure SNMP through the CLI, see the section “[To update system variables, enter information for the following fields:](#)” on page 43.

Web Management Interface (WMI)

To access the SNMP main page, click on **System > SNMP** from the main menu.

Patton Home Page

- Home
- System**
 - Information
 - Configuration
 - Software Upgrade
 - Authentication
 - Logging
 - SNMP
 - Interface
- Interface Configuration**
- Routing Configuration**
- Traffic Management**
- Support**
 - Support
 - Email Support

Patton Electronics Co.
© 2005-2007
Terms & Conditions

SNMP Configuration

Server Configuration

State: Disabled

Communities (SNMPv1 and SNMPv2)

Delete	Community String	Access	Source IP	Source Netmask
<input type="button" value="Add"/>	<input type="text"/>	Read-only <input type="button" value="v"/>	0.0.0.0 <input type="text"/>	/0 <input type="text"/>
<input type="button" value="Delete"/>				

Users (SNMPv3)

Delete	Username	Password	Access
<input type="button" value="Add"/>	<input type="text"/>	<input type="text"/>	Read-only <input type="button" value="v"/>
<input type="button" value="Delete"/>			

System Variables

sysDescription:

sysLocation:

sysContact:

sysName:

sysServices: 0

sysObjectId:

Figure 12. SNMP main page

Configuring the Server

To enable/disable the server:

1. In the **Server Configuration** section, select **Enabled** or **Disabled** from the **State** drop-down menu.
2. Click **Update**.

Managing SNMP Communities (SNMPv1 and SNMPv2)

Communities (SNMPv1 and SNMPv2)				
Delete	Community String	Access	Source IP	Source Netmask
<input type="checkbox"/>	public	Read-only	0.0.0.0	/0
<input type="button" value="Add"/>	<input type="text"/>	Read-only ▾	<input type="text" value="0.0.0.0"/>	<input type="text" value="/0"/>
<input type="button" value="Delete"/>				

Figure 13. SNMP Communities

Adding SNMP Communities

To add an SNMP community:

1. In the **Communities** section, enter a unique name in the **Community String** text box.
2. **Read-only** is the only available **Access** option.
3. Enter an IP address (in standard dotted quad format) in the **Source IP** field.
4. Enter a netmask address (in /xx format) in the **Source Netmask** field.
5. Click **Add**.

Deleting SNMP Communities

To delete an SNMP community:

1. Select the **Delete** checkbox for the community in the **Communities** table.
2. Click **Delete**.

Managing SNMP Users (SNMPv3)

Users (SNMPv3)			
Delete	Username	Password	Access
<input type="button" value="Add"/>	<input type="text"/>	<input type="text"/>	Read-only ▾
<input type="button" value="Delete"/>			

Figure 14. SNMP Users

Adding SNMP Users

To add an SNMP user:

1. In the Users section, enter a unique name in the **Username** text box.
2. Enter a unique password in the **Password** text box. The password must be at least 8 characters.
3. **Read-only** is the only available **Access** option.
4. Click **Add**.

Deleting SNMP Users

To delete an SNMP user:

1. Select the Delete checkbox for the user in the **Users** table.
2. Click **Delete**.

Managing System Variables

System Variables	
sysDescription:	<input type="text" value="My Description"/>
sysLocation:	<input type="text" value="My Location"/>
sysContact:	<input type="text" value="my@contact.com"/>
sysName:	<input type="text" value="My Name"/>
sysServices:	<input type="text" value="6"/>
sysObjectId:	<input type="text"/>
<input type="button" value="Update"/>	

Figure 15. System Variables

To update system variables, enter information for the following fields:

- **sysDescription** – A description of the system
- **sysLocation** – The location of the system
- **sysContact** – The email address of the administrator for the system
- **sysName** – The name of the system
- **sysServices** – SNMP services for the system
- **sysObjectId** – The object ID for the system

Click **Update** to save the changes.

Command Line Interface (CLI)

The following commands are used to configure SNMP:

SNMP commands

Table 12. SNMP - CLI Commands

Command	Explanation
Trinity# configure snmp	Enter the SNMP configuration mode.
Trinity[snmp]# [no] shutdown	Start/stop the SNMP agent.
Trinity[snmp]# [no] community <community-string> read-only [source <ip> <net-mask>]	Add/remove an SNMPv1/2c community.
Trinity[snmp]# [no] user <username> password <password> read-only	Add/remove an SNMPv3 user.
Trinity[snmp]# sysdescription <string>	Enter a description of the system.
Trinity[snmp]# syslocation <string>	Enter the location of the system.
Trinity[snmp]# syscontact <string>	Enter the email address of the system administrator.
Trinity[snmp]# sysname <string>	Enter the name of the system.
Trinity[snmp]# sysservices <0-127>	Enter an integer for system services. (The integer correlates with layer functionality, i.e. physical, datalink, internet, application, ect...).
Trinity[snmp]# sysobjectid <oid>	Set a unique object identifier for the system.
Trinity[snmp]# show	Enters show mode for SNMP.
Trinity# show snmp	Show the SNMP configuration.

The following is an example of the **show snmp** command:

```

agent is enabled
community      access      source
-----
public         read-only  0.0.0.0/0
limited        read-only  192.168.200.1/32

username      access
-----
user1         read-only

sysDescription: My Description
sysLocation:   My Location
sysContact:    my@contact.com
sysName:       My Name
sysServices:   6
sysObjectId:  <unset>

```

Chapter 6 **Interface Status**

Chapter contents

Overview	46
Web Management Interface (WMI)	47
Viewing Errors	47
Editing Interfaces	47
Command Line Interface (CLI).....	48
Root Mode	48
Configuration Mode	49
Overview	46
Web Management Interface (WMI)	47
Viewing Errors	47
Editing Interfaces	47
Command Line Interface (CLI).....	48
Root Mode	48
Configuration Mode	49

Overview

This chapter describes the interface configuration options for Ethernet interfaces, bridge groups, and VLANs.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

The interface properties that can be configured are:

- **Enable:** Enable or disable administration of an interface.
- **ARP:** Enable or disable transmission and reception of ARP packets.
- **Multicast:** Enable or disable transmission and reception of multicast packets.
- **MTU:** Set the size of the maximum transmission unit (MTU).
- **Speed/Duplex (*Ethernet interfaces only*):** Set the Ethernet speed to 10 Mbps, 100 Mbps, or auto. Set duplex to half, full, or auto.

To configure interfaces through the WMI, see the section “[Web Management Interface \(WMI\)](#)” on page 47.

To configure interfaces through the CLI, see the section “[Command Line Interface \(CLI\)](#)” on page 48.

Web Management Interface (WMI)

To access the Interface Status main page, click on **System > Interface** from the main menu on the left of the screen.

Interface	Status		Rx				Tx		
	Admin	Link	Bytes	Packets	Multicast	Errors	Bytes	Packets	Errors
eth0	Up	Up (100/Full)	1367279	17363	0	0	167142	329	0
eth1	Down	Down	0	0	0	0	0	0	0

[Expand Errors](#)

Figure 16. Interface Status main page

Viewing Errors

To view detailed errors in the status table, click the **Expand Errors** button.

To hide error details, click the **Collapse Errors** button.

Editing Interfaces

To update configuration details of interfaces from the status table, click on the hyperlink of the interface in the **Interface** column. The link will display configuration details for the specific interface. Click **Update** to save changes.

Configure eth0

Enable:

ARP:

Multicast:

MTU:

Speed/Duplex:

Figure 17. Editing an Ethernet interface from the status page

Note The **Speed/Duplex** option is only available for Ethernet interfaces.

Command Line Interface (CLI)

Root Mode

Table 13. Interface Root Mode - CLI Commands

Command	Explanation
Trinity# configure interface <interface-type> <interface-name>	Enter the interface configuration mode for <interface-name>.
Trinity# show interface <interface-type> <interface-name>	Show the current configuration and status of <interface-name>.

The following is example output of the **show interface** command (The ethernet interface *eth0* is used in this example):

```
eth0 is up, line protocol is up
  Hardware is static, address is 00:a0:ba:00:9d:ea
  Speed is administratively auto, operationally 100full
  Internet address 192.168.200.98/24 192.168.200.255
  Internet address 192.168.200.10/24 192.168.200.255secondary
  MTU 1524
  ARP enabled
  Multicast enabled
  Rx Statistics
    0 bytes in 0 packets
    0 errors 0 drops, 0 overruns
    0 multicast packets
  Tx Statistics
    398 bytes in 5 packets
    0 errors 0 drops, 0 collisions 0 carrier errors
```


Configuration Mode

Table 14. Interface Configuration Mode - CLI Commands

Command	Explanation
Trinity# [no] shutdown	Administratively disable this interface. A physical link may still be established, but no packets will be transmitted and any packets received will be ignored. The no shutdown command administratively enables this interface.
Trinity# [no] mtu <mtu>	Set the maximum transmission unit (MTU) for this interface. The no mtu <mtu> command returns the MTU back to its default value (1524 for Ethernet interfaces).
Trinity# [no] enable arp	Allow this interface to transmit ARP requests and respond with ARP replies. The no enable arp command causes the interface to not transmit ARP requests and to ignore any received ARP requests.
Trinity# [no] enable multi-cast	Allow this interface to transmit and receive multicast datagrams. The no enable multicast command causes the interface to not transmit multicast datagrams and to ignore any that are received.
Trinity# show	Show the current configuration and status of the interface. This command performs the same function as show interface <interface-type> <interface-name> available in the root mode.

Chapter 7 **Network Time Protocol (NTP)**

Chapter contents

Overview	51
Web Management Interface (WMI)	52
Configuring modes	52
Adding an NTP server	52
Command Line Interface (CLI).....	53
Root Mode	53
Configuration Mode	53
Debugging Information	54

Overview

This chapter describes the Network Time Protocol (NTP), which provides a client for synchronizing the system time of network devices.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

To configure interfaces through the WMI, see the section “[Web Management Interface \(WMI\)](#)” on page 52.

To configure interfaces through the CLI, see the section “[Command Line Interface \(CLI\)](#)” on page 53.

Web Management Interface (WMI)

To access the NTP main page, click on **System > NTP** from the main menu on the left of the screen.

Figure 18. NTP main page

Configuring modes

To enable NTP, select **enabled** from the **State** drop-down menu in the **Mode Configuration** section.

To enable the broadcast client, select **enabled** from the **Broadcast Client** drop-down menu in the **Mode Configuration** section. Click **Change** to save your selections.

Figure 19. Configuring modes

Adding an NTP server

To add an NTP server:

1. Enter a host address in the **Host Name/IP Address** field in the **Add NTP Server** section.
2. Select a type (unicast or multicast) from the **Server Type** drop-down menu.
3. Click **Add**.

Figure 20. Adding an NTP server

Command Line Interface (CLI)

Root Mode

Table 15. NTP Root Mode - CLI Commands

Command	Explanation
Trinity# configure ntp	Enter the NTP configuration mode.

Configuration Mode

Table 16. NTP Configuration Mode - CLI Commands

Command	Explanation
Trinity[ntp]# [no] broadcast client	Enable or disable broadcast client capability. The broadcast client may be enabled regardless of whether unicast or multicast servers have been added.
Trinity[ntp]# [no] shutdown	Enable or disables NTP.
Trinity[ntp]# [no] server [ip address hostname]	Add or remove unicast servers via IP or host-name.
Trinity[ntp]# [no] multicast [ipaddr]	Add or remove multicast addresses. A multicast address must be either 224.0.1.1 , in the range 233.0.0.0 to 233.255.255.255 , or in the range 239.0.0.0 to 239.255.255.255 .
Trinity[ntp]# [no] show	Display the configuration and status of NTP. <ul style="list-style-type: none"> • Flags: Provides details about the type of server and whether that server's time is the currently selected time and whether it is in list of candidates for selection. • Offset: The difference in seconds between the current system time and the time of the corresponding server. • Delay: The round trip delay between the system and the corresponding server. • Dispersion: The maximum error of the current system time relative to the corresponding server. • Jitter: Describes variation in the current system time relative to the corresponding server.

Example– Trinity[ntp]# [no] show:

State: Enabled

Broadcast Client: Enabled

Multicast Addresses:

Flags: S - Selected, A - cAndidate, U - Unicast, B - Broadcast

```

+-----+-----+-----+-----+-----+-----+
|  Server  | Flags | Offset | Delay | Dispersion | Jitter |
+-----+-----+-----+-----+-----+-----+
| 10.11.2.238 | B    | 0.000 | 0.000 | 16000.000 | 0.015 |
+-----+-----+-----+-----+-----+

```

Debugging Information

Table 17. NTP Debugging - CLI

Command	Explanation
Trinity# debug ntp	Display NTP debug information.
Trinity# debug ntp [priority {emerg alert crit err warn notice info debug}]	Show all NTP debug messages of the specified priority. If no priority is specified, then err is used.
Trinity# no debug all	Turn off all debugging.

Chapter 8 **IP Address Configuration**

Chapter contents

Overview	56
Configuration Overview	56
Terms used with IP Interfaces	56
Web Management Interface (WMI)	58
Adding an IP Interface	59
IP Configuration	59
Adding a DHCP Client	60
DHCP Configuration	60
Command Line Interface (CLI).....	61
IP Interface Commands	61
DHCP Client Commands	61

Overview

This chapter describes how to add or remove IP addresses from Ethernet-like interfaces.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

Configuration Overview

The user can add or remove IP addresses to and from Ethernet interfaces from both the CLI and the WMI.

The following parameters are configurable when adding an IP address to an Ethernet interface:

- **IP address:** Standard dotted quad. format (Required)
- **Network mask:** Standard dotted quad format or slash notation (Defaults to /32)
- **Broadcast** in the following ways:
 - "+": auto calculates the high-bit broadcast (Default)
 - "-": auto calculates the low-bit broadcast
 - **Dotted quad** (dotted quad format) – (**Note:** The broadcast will not be verified to be correct when using the dotted quad format).

The following information is available when adding DHCP addresses:

- **Accept Routes** forces routes supplied to by the DHCP server to be added to the routing table
- **Accept DNS** forces DNS server supplied by the DHCP server to be added to the DNS pool
- **Accept Hostname** forces the hostname supplied by the DHCP server to be applied

For DHCP addresses, the user is also able to:

- Release
- Renew

Terms used with IP Interfaces

- **Dotted quad (standard dotted quad format):** 32-bit IP address split into 4 8-bit integers (0-255) separated by a '.'. (i.e., 0.0.0.0 to 255.255.255.255)
- **Ethernet-like:** Interfaces capable of sending L2 ethernet style headers (i.e., Physical ethernet, VLANs, Bridge Groups, BCP)
- **High-bit broadcast:** Broadcast address calculated by replacing the masked out bits with 1 (i.e., 192.168.252.100/24 -> 192.168.252.255)
- **Low-bit broadcast:** Broadcast address calculated by replacing masked out bits with 0 (i.e., 192.168.252.100/24 -> 192.168.252.0)
- **Net-block:** A set of IP addresses logically grouped by a network mask.

- **Secondary IP address:** For any given net-block, there can be only one primary IP address. That primary IP is used as a source address for communication initiated by the device. Any additional IP addresses within the same net-block are considered as secondary addresses and are internally linked to the primary IP address in that net-block. A Trinity device will respond to secondary IP addresses. If a primary IP is removed, then all secondaries linked to it are removed as well.
- **Slash notation:** A special network mask notation allowing a user to specify only the masked bits. (i.e., /0 through /32)

To configure IP interfaces through the WMI, see the section “[Web Management Interface \(WMI\)](#)” on page 58.

To configure IP interfaces through the CLI, see the section “[Command Line Interface \(CLI\)](#)” on page 61.

Web Management Interface (WMI)

To access the IP Interface Management main page, click on **Interface Configuration > IP Interface** from the main menu on the left of the screen.

The screenshot shows the 'IP Address Configuration' page. On the left is a navigation sidebar with the following menu items: Patton Home Page, Home, System, Interface Configuration (expanded), IP Interface (selected), VLAN, Bridge Group, T1/E1, PPP, ARP, DHCP Server, NAT, Routing Configuration, Traffic Management, Support, Support, and Email Support. At the bottom of the sidebar is the text: 'Patton Electronics Co. © 2005-2007 Terms & Conditions'.

The main content area is titled 'IP Address Configuration' and contains the following sections:

- Add IP Address:** A form with fields for Interface (dropdown menu showing 'eth0'), IP, Netmask, and Broadcast, and an 'Add' button.
- Add DHCP Client:** A form with fields for Interface (dropdown menu showing 'eth0'), Accept Routes, Accept DNS, and Accept Hostname (all checkboxes), and an 'Add' button.
- IP Configuration:** A table with columns: Interface, IP, Netmask, Broadcast, Flag(s), and Delete. It contains one entry for 'eth0' with IP 10.10.3.31, Netmask 255.255.0.0, and Broadcast 10.10.255.255. A 'Delete' button is located below the table.
- DHCP Configuration:** A table with columns: Interface, Accepting Routes, Accepting DNS, Accepting Hostname, and Disable. It is currently empty. A 'Disable' button is located below the table.

Figure 21. IP Address Configuration main page

Adding an IP Interface

To add an IP interface:

1. Choose a valid interface from the **Interface** drop-down menu.
2. Enter the **IP** address, **Netmask**, and **Broadcast** address.
3. Click the **Add** button to save the IP interface.

Figure 22. Adding an IP interface

IP Configuration

The **IP Configuration** table shows the current IP configuration for the device:

- **Interface:** Interface that is configured for the IP address
- **IP:** IP address in dotted quad format
- **Netmask:** Network mask in dotted quad format
- **Broadcast:** Broadcast address
- **Flags:**
 - *Secondary:* Indicates an IP address as secondary
 - *DHCP:* Indicates an IP was DHCP-assigned and cannot be removed
- **Delete:** Select the checkbox of the interface to delete, then click the **Delete** button.

Interface	IP	Netmask	Broadcast	Flag(s)	Delete
eth0	10.10.3.31	255.255.0.0	10.10.255.255		<input type="checkbox"/>

Figure 23. IP Configuration

Adding a DHCP Client

To add a DHCP client:

1. Choose a valid interface from the **Interface** drop-down menu.
2. Select to **accept routes**, **accept DNS**, and/or **accept hostname** (these are *optional* features).
3. Click **Add**.

The screenshot shows a dialog box titled "Add DHCP Client". Inside the dialog, there is a label "Interface:" followed by a dropdown menu showing "eth0". Below this are three labels with checkboxes: "Accept Routes:" (unchecked), "Accept DNS:" (unchecked), and "Accept Hostname:" (unchecked). At the bottom center of the dialog is a button labeled "Add".

Figure 24. Adding a DHCP client

DHCP Configuration

The DHCP Configuration table shows the current DHCP configurations for the device:

- **Interface:** Interface that has DHCP enabled
- **Accepting Routes:** Indicates that routes given by the DHCP server are added to the routing table
- **Accepting DNS:** Indicates that DNS servers returned by the DHCP server are accepted
- **Accepting Hostname:** Indicates that the hostname supplied by the DHCP server is accepted
- **Disable:** To disable a DHCP configuration, click the **Disable** button in the row of the interface.

Note A DHCP lease cannot be released or renewed through the WMI.
See “[DHCP Client Commands](#)” on page 61.

The screenshot shows a table titled "DHCP Configuration". The table has five columns: "Interface", "Accepting Routes", "Accepting DNS", "Accepting Hostname", and "Disable". The "Disable" column contains a button labeled "Disable".

Interface	Accepting Routes	Accepting DNS	Accepting Hostname	Disable
				Disable

Figure 25. DHCP configuration

Command Line Interface (CLI)

IP Interface Commands

All IP interface commands are accessed by entering `configure interface <interface type> <interface name>`.

Table 18. IP Interface - CLI Commands

Command	Explanation
Trinity# no ip address <IP>	Removes the specified IP.
Trinity# ip address <IP> [netmask <mask> [broadcast <broadcast>]]	Adds a new IP address with the configured options.

DHCP Client Commands

All commands are accessed by entering `configure interface <interface type> <interface name>`. Only the subset of commands that deal with DHCP client configuration are shown in [table 19](#).

Table 19. DHCP client - CLI Commands

Command	Explanation
Trinity# ip address dhcp [release renew request <ip> [ignore <ign options>]] ignore <ign options>	<ul style="list-style-type: none"> • release - release the current DHCP lease on an interface, and will fail if DHCP is not enabled • renew - renews the current DHCP lease on an interface, and will fail if DHCP is not enabled • request - requests an initial IP address from the DHCP (it is only a request and the server might refuse and assign a different IP address) • ignore - specifies the DHCP options that will be ignored (options explained below) <p>Ignored items can be specified in any order but can only exist on the line once.</p>
[ignore route]	<ul style="list-style-type: none"> • route - ignore any supplied default route from the server on this interface
[ignore hostname]	<ul style="list-style-type: none"> • hostname - ignore any supplied hostname from the server on this interface
[ignore dns]	<ul style="list-style-type: none"> • dns - ignore any supplied DNS servers from the server on this interface
Trinity# no ip address dhcp	Disable DHCP client on this interface.

Chapter 9 **VLAN Configuration**

Chapter contents

Overview	63
Configuration Overview	63
Web Management Interface (WMI)	64
Create VLAN	64
Manage VLAN Interfaces	64
Command Line Interface (CLI).....	65
VLAN Configuration Commands	65
VLAN Configuration Example	65
Show VLAN Information	66

Overview

This chapter describes how to configure VLANs on the Trinity platform.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

Configuration Overview

The bulk of the configuration of a VLAN works exactly like a regular Ethernet interface. For those operations, e.g. setting an IP address, see Chapter 8, “[IP Address Configuration](#)” on page 55.

This chapter explains how to create and delete VLANs on a physical interface.

To configure VLANs through the WMI, see the section “[Web Management Interface \(WMI\)](#)” on page 64.

To configure VLANs through the CLI, see the section “[Command Line Interface \(CLI\)](#)” on page 65.

Web Management Interface (WMI)

To access the VLAN Configuration main page, click on **Interface Configuration > VLAN** from the main menu on the left of the screen.



Figure 26. VLAN Configuration main page

Create VLAN

To create a new VLAN:

1. Choose an **Interface** from the drop-down menu. Note that interfaces that have been shutdown cannot have a VLAN created on them. If an interface is not listed, make sure that it has not been shutdown.
2. Type the VLAN ID (**VID**) (a number between 1 and 4094) into the text field.
3. Click **Create**. The VLAN configuration details will be displayed.

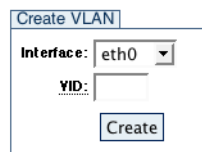


Figure 27. Create VLAN

Manage VLAN Interfaces

The **VLAN Interfaces** table lists the existing VLANs.

To view a VLAN's details, click on the name of the VLAN device.

To delete a VLAN interface, select the Delete checkbox for that profile, then click the **Delete** button.

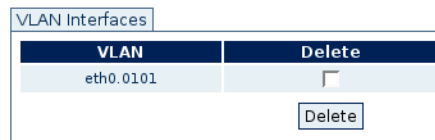


Figure 28. VLAN Interfaces

Command Line Interface (CLI)

VLAN Configuration Commands

Table 20. VLAN - CLI Commands

Command	Explanation
Trinity# [no] interface vlan <interface> <vlan-id>	<p><interface> specifies the interface to create the VLAN on.</p> <p>The <vlan-id> is an integer between 1 and 4094.</p> <p>The no interface command deletes the specified VLAN from the interface, if it exists.</p>

VLAN Configuration Example

VLANs are created on interfaces as shown in the following example:

```
Trinity# configure
Trinity[config]# interface vlan eth0 23
Trinity[vlan(eth0.0023)]#
```

Interface specific properties of A VLAN can be configured with standard interface configuration commands, as documented for ethernet interfaces.

```
Trinity#
Trinity# configure
Trinity[config]# interface vlan
eth0      Interface device name
eth1      Interface device name
Trinity[config]# interface vlan eth0
<1-4094>  New VLAN Id
Trinity[config]# interface vlan eth0 23
Trinity[vlan-eth0.0023]# show
eth0.0023 is down, line protocol is down
  Hardware is static, address is 00:19:db:58:2d:49
  Speed is administratively unknown
  MTU 1500
  ARP enabled
  Multicast enabled
  Rx Statistics
    0 bytes in 0 packets
    0 errors 0 drops, 0 overruns
    0 multicast packets
  Tx Statistics
    0 bytes in 0 packets
    0 errors 0 drops, 0 collisions 0 carrier errors
  VLAN:
    VID: 23
    Interface: eth0
    Reorder Headers: On
    Traffic Statistics:
      Total Headroom Inc: 0
      Total Encap On Xmit: 0
Trinity[vlan-eth0.0023]#
Trinity[vlan-eth0.0023]#
Trinity[vlan-eth0.0023]# █
```

Show VLAN Information

The **show** command is used to display information about VLANs. It can be used from the root mode, configure mode, or configure mode of a specific VLAN.

Table 21. Show VLAN Information - CLI Commands

Command	Explanation
Trinity# show interface vlan	Displays all VLAN information.
Trinity[config]# show interface vlan	Displays all VLAN information.
Trinity# show interface vlan eth0	Displays VLANs on eth0
Trinity# show interface vlan eth0 23	Displays VLAN eth0.0023
Trinity[vlan-eth0.0023]# show	Displays VLAN eth0.0023
Trinity# show interface vlan [interface [vlan-id]]	<p>The show interface vlan mode displays one of the following options at a time:</p> <ul style="list-style-type: none"> • Interface: If a regular interface is given, only VLANs on that interface will be listed. • Vlan-ID: If a Vlan-ID is given, only VLANs using that Vlan-ID will be listed. • Vlan-interface: If a VLAN interface is given (the interface followed by a dot followed by the zero-padded Vlan-ID, for example, <i>eth00.0023</i>), only that VLAN will be listed. <p>Displays VLANs on a specific interface. Displays VLAN information for a specific VLAN ID.</p>

From configure mode for a specific VLAN, the show command displays information for that interface only. The information displayed is a combination of the standard information for an ethernet interface, combined with some VLAN specific information.

For example:

```

eth0.0023 is up , line protocol is up
  Hardware is static, address is
  Speed is Auto
  Internet address 10.1.1.1/24 10.1.1.255
  MTU 2128606600
  ARP enabled
  Multicast enabled
  Rx Statistics
    0 bytes in 0 packets
    0 errors, 0 drops, 0 overruns
    0 multicast packets
  Tx Statistics
    0 bytes in 0 packets
    0 errors, 0 drops, 0 collisions, 0 carrier errors

```

VLAN:

```
VID: 23
Interface: eth0
Reorder Headers: On
Traffic Statistics:
    Total Headroom Inc: 0
    Total Encap On Xmit: 0
```

Chapter 10 **Bridge Group Configuration**

Chapter contents

Overview	69
Configuration Overview	69
Web Management Interface (WMI)	71
Bridge Group Configuration	72
Add/Configure Bridge Groups	72
Delete Bridge Groups	72
Manage Interfaces	72
STP Configuration	73
Set STP Parameters	73
Set STP Forwarding	73
Show STP Status Information	73
Manage MAC Addresses	74
Display MAC Address Information	74
Add MAC Filter Rules	74
Display/Delete MAC Filter Rules	74
Command Line Interface (CLI).....	75
Bridge Group Commands	75

Overview

This chapter describes how to configure bridge groups and manage bridge group interfaces.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

Configuration Overview

The bridge group configuration on the system can be divided into six groups:

1. Managing a bridge group:

- Adding and deleting a bridge group
- Setting the ageing time value (in seconds, default 300) for the bridge group:
Ageing time is the number in seconds a MAC address will be kept in the forwarding database of the bridge group after having received a packet from this address.
- Enabling and disabling Spanning Tree Protocol (STP) for the bridge group. STP manages links in the bridge group and prevents loops from occurring in a network.

2. Managing interfaces:

- Attaching and removing an interface to/from a bridge group
- Setting the path cost for an interface:
(The cost of sending/receiving a packet from this interface; also referred to as the port priority).
The faster interfaces should have lower path costs. These values are used in the computation of the minimal spanning tree.

3. Configuring STP:

- Setting the priority of the bridge group (integer between 0-65525, default=32768):
The bridge with the lowest priority is selected as the root bridge in the spanning tree.
- Setting the forwarding delay (in seconds, default=15):
Forwarding delay is the number in seconds spent in each of the listening and learning states, before the forwarding state is entered.
- Setting the hello interval (in seconds, default=2):
The *hello interval* is the time a hello packet is sent out of the root bridge. Hello packets are used to communicate topology information throughout the entire bridged local area network.
- Setting the maximum message age (in seconds, default=20):
If the last seen hello packet is older than this number of seconds, the bridge in question will start the procedure to take over as the root bridge in the spanning tree.
- Forward/Drop STP packets on a per interfaces basis:
Configures which interfaces of the bridge group will participate in dissemination of spanning tree information (default all interfaces forward STP packets).

4. Configuring the bridge group interface:

- Enable and disable the bridge group interface
- Set MTU size (in bytes)
- Add an IP address to the bridge group interface
- Toggle ARP and MULTICAST flags

5. Monitoring status:

- Displaying current forwarding database
- Displaying current STP configuration
- Displaying bridge group interface configuration
- Displaying existing bridge groups, interfaces enslaved in them, and STP status

6. MAC address filtering:

- Permit and deny packets based on the source MAC address, packet destination MAC address, interface, egress or ingress direction

All six configuration groups can be accessed via the command line interface (CLI). However, the bridge group configuration page of the Web Management Interface (WMI) allows access to bridge-group-only configuration. Therefore, IP and other ethernet-like configuration (enable/disable, MTU, etc.) is only possible through IP and Ethernet WMI pages.

To configure the Bridge Group Management component through the WMI, see the section “[Web Management Interface \(WMI\)](#)” on page 71.

To configure the Bridge Group Management component through the CLI, see the section “[Command Line Interface \(CLI\)](#)” on page 75.

Web Management Interface (WMI)

To access the Bridge Group Configuration main page, click on **Interface Configuration > Bridge Group** from the main menu on the left of the screen.

The screenshot shows the 'Bridge Group Configuration' page. The left sidebar contains a navigation menu with the following items:

- Patton Home Page
- Home
- System
 - Interface Configuration
 - IP Interface
 - VLAN
 - Bridge Group
 - T1/E1
 - PPP
 - APP
 - DHCP Server
 - NAT
- Routing Configuration
- Traffic Management
- Support
 - Support
 - Email Support

The main content area is titled 'Bridge Group Configuration' and has three tabs: 'Bridge Group Configuration' (selected), 'STP Configuration', and 'Manage MAC Addresses'.

The 'Manage Bridge Groups' section contains the following form:

Manage Bridge Groups

Bridge Group:

Add

Bridge Group:

Ageing Value:

STP Status:

Submit

The 'Manage Interfaces' section contains the following table:

Manage Interfaces

Interface	Name	Cost	STP	Attach/Remove
eth0	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
eth1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

Submit

The 'Bridge Groups' section contains the following table:

Bridge Groups

Bridge Group	STP	Interfaces	Delete
			<input type="button" value="Delete"/>

Patton Electronics Co.
© 2005-2007
Terms & Conditions

Figure 29. Bridge Group Configuration main page

The Bridge Group Configuration page consists of three tabs:

- “Bridge Group Configuration” on page 72
- “STP Configuration” on page 73
- “Manage MAC Addresses” on page 74

Bridge Group Configuration

Add/Configure Bridge Groups

To add a bridge group:

1. Enter the name of the bridge group in **br<number>** format, then click **Add**.

To configure a bridge group:

1. Select the group from the **Bridge Group** drop-down menu.
2. Enter the **Ageing Value** in seconds, and select enable or disable from the **STP Status** drop-down menu.
3. Click **Submit**.

Delete Bridge Groups

To delete a bridge group:

1. Select the **Delete** checkbox for the bridge group in the **Bridge Groups** table, then click **Delete**.

Manage Interfaces

Interfaces can be attached and configured using the *Manage Interfaces* table:

- **Attached To:** To attach an interface to a bridge group, select a bridge group from the **Attached To** drop-down menu. If the interface is not attached to any bridge groups, the keyword **None** is displayed.
- **Cost (optional):** If the interface is not attached to any bridge group, the user may enter a cost value in the **Cost** field. If the interface is already attached to a bridge group, the **Cost** field displays either the value set by the user or keyword "default" if no cost value was specified.
- **STP (read only):** The **STP** column displays whether the attached interface is sending STP information (default = *forward*).
- **Force (optional):** Select the **Force** checkbox to remove IP address information from the interface before attaching it to the bridge group. It is usually recommended to remove any IP addresses from attached interfaces in order for the bridge group to operate correctly.

Interface	Attached To	Cost	STP	Force
eth0	None		forward	<input type="checkbox"/>
eth1	br0	100	forward	<input checked="" type="checkbox"/>

Figure 30. Managing interfaces

To attach an interface to a bridge group, select the bridge group from the drop-down menu and click **Submit**. To remove an interface from a bridge group, select **None** from the **Attached To** drop-down menu and click **Submit**.

STP Configuration

Set STP Parameters

Enter information for the following fields in the **Set STP Parameters** section to configure STP:

1. Select a bridge group from the **Bridge Group** drop-down menu.
2. Enter a number in the range (0-65535) in the **Bridge Priority** field.
3. Enter seconds in the range (0-65533) in the **Forwarding Delay** field.
4. Enter seconds in the range (0-65533) in the **Hello Interval** field.
5. Enter seconds in the range (0-65533) in the **Maximum Age** field.
6. Click **Submit**.

Figure 31. STP Configuration

Set STP Forwarding

STP Forwarding prevents loops in a network by allowing a bridge group to forward traffic on a designated interface. To set up STP forwarding for a bridge group:

1. In the **Set STP Forwarding** section, select a bridge group from the **Bridge Group** drop-down menu.
2. Select an interface from the **Interface** drop-down menu.
3. Select **forward** from the **Action** drop-down menu.
4. Click **Submit**.

(To *turn off* STP forwarding, select **drop** from the **Action** drop-down menu).

Show STP Status Information

To show the full STP status for a bridge group:

1. In the **Show Status Information** section, select a bridge group from the **Bridge Group** drop-down menu.
2. Click **Submit**.

Manage MAC Addresses

Display MAC Address Information

The **MAC Address Information** table displays the contents of the bridge group forwarding database for the selected bridge group. The rows display the name of the local port where this MAC address is observed, the MAC address, whether it is local, and the remaining time in seconds until this entry ages out and is removed from the table. Local entries have 0.0 seconds for their ageing value but are never removed from the table.

The screenshot shows a web form titled "MAC Address Information". At the top, there is a "Bridge Group:" label followed by a dropdown menu showing "br0". Below this is a table with four columns: "Local Port", "MAC Address", "Local", and "Ageing Timer". The table contains one row with the following data: "eth1", "00:19:db:58:2e:98", "yes", and "0.00". At the bottom left of the form is a "Submit" button.

Local Port	MAC Address	Local	Ageing Timer
eth1	00:19:db:58:2e:98	yes	0.00

Figure 32. Displaying MAC address information

Add MAC Filter Rules

Use the **Filter Configuration** table to add MAC filter rules for a selected bridge group. Five MAC addresses can be submitted at a time. The following settings may be configured:

- **Port:** Select *egress* to apply the new filter rule to outgoing packets, or select *ingress* to apply the rule to incoming packets.
- **Source MAC address:** Enter a source MAC address that the filter rule will try to match, or leave this field as 00:00:00:00:00:00 to match **all** source MAC addresses.
- **Destination MAC address:** Enter a destination MAC address that the filter rule will try to match, or leave this field as 00:00:00:00:00:00 to match **all** destination MAC addresses.
- **Interface:** Select an interface for the filter rule.
- **Filter:** Select **permit** or **deny** for packets matching the filter rule criteria.

The screenshot shows a web form titled "Filter Configuration". At the top, there is a "Bridge Group:" label followed by a dropdown menu. Below this is a table with five columns: "Port", "Source MAC", "Destination MAC", "Interface", and "Filter". The table contains five rows, each with the following data: "egress", "00:00:00:00:00:00", "00:00:00:00:00:00", and two empty dropdown menus. At the bottom left of the form is a "Submit" button.

Port	Source MAC	Destination MAC	Interface	Filter
egress	00:00:00:00:00:00	00:00:00:00:00:00		
egress	00:00:00:00:00:00	00:00:00:00:00:00		
egress	00:00:00:00:00:00	00:00:00:00:00:00		
egress	00:00:00:00:00:00	00:00:00:00:00:00		
egress	00:00:00:00:00:00	00:00:00:00:00:00		

Figure 33. Configuring MAC filter rules

Display/Delete MAC Filter Rules

Use the **Filter Display** table to show the existing MAC filter rules for a selected bridge group. Entries can be deleted by selecting the corresponding **Delete** checkbox and clicking the **Submit** button.

Command Line Interface (CLI)

Bridge Group Commands

Table 22. Bridge Group Configuration - CLI Commands

Command	Explanation
Trinity# configure [no] interface bridge {<id> br<id>}	Enter bridge configuration mode
Trinity[bridge(br0)]#	
Trinity[bridge(br0)]# [no] attach <dev> [pathcost <value>] [force]	Manage interfaces
Trinity[bridge(br0)]# ageing <value>	Set ageing value
Trinity[bridge(br0)]# [no] enable {arp multicast stp }	Enable/disable STP
Trinity[bridge(br0)]# stp {bridgeprio hello maxage fwdelay} <value>	Configure STP settings
Trinity[bridge(br0)]# [no] filter mac {ingress egress} {permit deny} [source <srcmac>] [destination <dstmac>] [interface <dev>]	Configure filter rules for MAC addresses
Trinity[bridge(br0)]# filter stp <dev>	Configure filter rules for STP packets
Trinity[bridge(br0)]# mtu <value>	Set MTU value
Trinity[bridge(br0)]# [no] ip {.....}	Add an IP address to the bridge interface
Trinity[bridge(br0)]# show {macs stp filter}	Display details
Trinity[bridge(br0)]# [no] shutdown	Disable the bridge group

Detailed explanations for [table 22](#):

- **Bridge:** The **bridge** command under the interface mode moves the CLI into the bridge group context, creating a new bridge group if the given bridge group id does not exist in the system. The <id> is a unique positive integer number representing the bridge group. The CLI accepts both <id> and br<id> as valid input. The **no bridge** command removes the bridge group from the system.
- **Ageing:** Under the bridge group context, the **ageing** command sets the value of the ageing time, where <value> is in seconds.
- **Enable:** The **enable** command enables spanning tree protocol (STP), and also the ARP or Multicast support on the bridge group interface. Entering **[no]** in front of the command disables STP, ARP or Multicast support on the interface.
- **STP:** The **stp** command sets the values of STP parameters, where <value> is a positive integer for the **bridgeprio** parameter, and is *in seconds* for the **hello**, **maxage**, and **fwdelay** parameters.
- **MTU:** The **mtu** command sets the maximum transmission unit size for the packets transmitted through the bridged interfaces, where <value> is in bytes.
- **IP:** The **ip** command adds an IP address to the bridge group interface. When a bridge group has an IP address, it can act as a routeable network node. Therefore, it becomes possible to send/recv packets (e.g. ping) to the bridge group. The **no ip** command removes the IP address from the bridge group.

- **Filter:** The **filter** command has two options, **mac** and **stp**:
 - The **filter mac** command adds a new MAC address-based filter rule to either permit or deny packets based on the direction (*ingress (incoming)* or *egress (outgoing)*), source MAC address specified in *<srcmac>*, destination MAC address specified in *<dstmac>*, and the interface name *<dev>*. The **no filter mac** command removes the MAC address filter rule from the bridge group.
 - The **filter stp** command adds a filter to stop forwarding of STP information on the interface *<dev>*. The **no filter stp** command enables forwarding of STP information on the interface.
- **Shutdown:** The **shutdown** command disables the bridge group. The bridge group configuration is retained, but no traffic can be forwarded through the bridged interfaces when disabled. The **no shutdown** command enables the bridge group.
- **Show:** The **show** command under the bridge group context can display MAC address forwarding database, the STP status, and the MAC address based filter rules. (See [figure 34](#) on page 76 through [figure 36](#) on page 77).

```
Trinity#
Trinity# configure interface bridge
<id>      Bridge group ID
br0      Existing Bridge group ID
Trinity# configure interface bridge br0
Trinity[bridge(br0)]# show mac
MAC Address Information
+-----+-----+-----+-----+
| Local Port | MAC Address | Local | Timer (secs) |
+-----+-----+-----+-----+
| eth1      | 00:19:db:58:2e:98 | yes  | 0.00         |
+-----+-----+-----+-----+
Trinity[bridge(br0)]# █
```

Figure 34. Show MAC address forwarding database

```
Trinity[bridge(br0)]#
Trinity[bridge(br0)]# show stp
br0
bridge id          8000.0019db582e98
designated root    8000.0019db582e98
root port         0
max age           19.99
hello time        1.99
forward delay     150.00
ageing time       299.95
hello timer       0.03
topology change timer 0.00
flags

eth1 (1)
port id           8001
designated root    8000.0019db582e98
designated bridge  8000.0019db582e98
designated port    8001
designated cost    0
flags
state             disabled
path cost         100
message age timer 0.00
forward delay timer 0.00
hold timer        0.00
Trinity[bridge(br0)]# █
```

Figure 35. Show STP configuration

```

Trinity[bridge(br0)]#
Trinity[bridge(br0)]# filter
mac      Configure MAC address filter
stp      Configure STP packet filter
Trinity[bridge(br0)]# filter mac
ingress  Apply filter to incoming packets
egress   Apply filter to outgoing packets
Trinity[bridge(br0)]# filter mac egress
deny     Deny access
permit   Permit access
destination  Enter destination MAC address
interface Specify an interface
source   Enter source MAC address
<r mac egress source 00:E0:81:25:B6:2C interface eth1 deny
Trinity[bridge(br0)]# show filter
MAC Address Filter Information
+-----+-----+-----+-----+-----+
| Port | Source MAC | Destination MAC | Interface | Filter |
+-----+-----+-----+-----+-----+
| ingress | 00:00:00:00:00:00 | 00:e0:81:25:b6:b6 | | deny |
+-----+-----+-----+-----+-----+
| egress | 00:e0:81:25:b6:2c | 00:00:00:00:00:00 | eth1 | deny |
+-----+-----+-----+-----+-----+
Trinity[bridge(br0)]# █

```

Figure 36. Configure and show MAC filter information

The **show** command under the configure mode can additionally display "ethernet-like" and IP configuration information on the bridge group:

```

Trinity#
Trinity# configure interface bridge br0 show
br0 is up, line protocol is up
  MTU 1500
  ARP enabled
  Multicast enabled
  Rx Statistics
    0 bytes in 0 packets
    0 errors 0 drops, 0 overruns
    0 multicast packets
  Tx Statistics
    0 bytes in 0 packets
    0 errors 0 drops, 0 collisions 0 carrier errors
  STP disabled
  Attached Interfaces:
    eth1
Trinity# █

```

Figure 37. Show interface configuration

Chapter 11 **Generic Routing Encapsulation (GRE)**

Chapter contents

Overview	79
Configuration Overview	79
Web Management Interface (WMI)	80
Creating GRE Interfaces	80
Deleting GRE Interfaces	80
Command Line Interface (CLI).....	81

Overview

This chapter describes how to configure generic routing encapsulation (GRE). GRE is a method of encapsulating one protocol within another protocol. This implementation only supports encapsulating IPv4 in IPv4. It can be used to create a virtual private network (VPN). However, it is important to note that the data is not encrypted, so it should not be sent across the Internet.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

Configuration Overview

The following parameters must be configured in order to establish a GRE tunnel:

- **Destination:** This is the public IP address of the router that will terminate the other end of the GRE tunnel.
- **IP Address:** This is the IP address of the tunnel interface. This IP address is not publicly accessible. Only the other end of the tunnel can access it. It can be used to route the appropriate traffic through the tunnel.
- **MTU (optional):** The maximum transmission unit of the tunnel.

When you have configured the GRE interface, you must then enable it in order to pass traffic through it.

To configure GRE settings through the WMI, see the section “[Web Management Interface \(WMI\)](#)” on page 80.

To configure GRE settings through the CLI, see the section “[Command Line Interface \(CLI\)](#)” on page 81.

Web Management Interface (WMI)

To access the GRE main page, click on **Interface Configuration > GRE** from the menu on the left of the screen.

Figure 38. GRE Interface Configuration

The **GRE Interface Configuration** main page displays the list of created GRE interfaces and configuration options.

Creating GRE Interfaces

To create a GRE interface:

1. In the **Create GRE Interface** section on the GRE main page, enter a name for the new GRE interface in the **Name** field.
2. Enter the IP address of the tunnel endpoint in the **Destination** field.

Figure 39. Creating a GRE interface

3. Click **Create**. The new interface will show up in the **GRE Interfaces** list.

Deleting GRE Interfaces

Interface	Destination	Delete
gre1	192.168.1.1	<input type="checkbox"/>

Figure 40. Deleting a GRE interface

To delete a GRE interface, select the checkbox for the interface in the **GRE Interfaces** table and click **Update**.

Command Line Interface (CLI)

The following commands are used to configure GRE interfaces:

Table 23. GRE Interfaces - CLI Commands

Step	Explanation
configure [no] interface gre <greX>	Enter/create the configuration mode for a specified GRE interface. Entering the no version of the command will delete the specified interface.
[no] shutdown	Enable/disable the interface.
[no] destination <A.B.C.D>	Set the tunnel endpoint.
[no] ip address <A.B.C.D> [netmask <A.B.C.D> [broadcast <A.B.C.D>] secondary]	Add/delete an IP address to/from this interface.
[no] mtu <bytes>	Specify the MTU. Entering the no version of the command will set the MTU to the default setting.
show	Show the interface configuration.
show interface gre <greX>	Show the interface configuration.

Example – show command:

```

Destination: 10.0.0.1
gre1 is up, line protocol is up
  Internet address 192.168.1.1/24 192.168.1.255
  MTU 1476
  ARP disabled
  Multicast disabled
  Rx Statistics
    0 bytes in 0 packets
    0 errors 0 drops, 0 overruns
    0 multicast packets
  Tx Statistics
    0 bytes in 0 packets
    0 errors 0 drops, 0 collisions 0 carrier errors

```

Chapter 12 **PPP Configuration**

Chapter contents

Overview	83
Configuration Overview	83
Web Management Interface (WMI)	84
Configure PPP Authentication	84
Add PPP Interfaces	85
Status of PPP Interfaces	85
Delete PPP Interfaces	85
Configure PPP Interfaces	86
Command Line Interface (CLI).....	88
PPP Authentication Commands	88
PPP Configuration Commands	88
Creating the interface	89
Configuring PPP negotiation	89
Enabling PPP on HDLC interfaces	90
Configuring LCP	91
Configuring IPCP	92
Configuring BCP	93
Showing Configuration and Status	94
Debugging Commands	94

Overview

This chapter describes how to configure PPP on the Trinity platform.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

Configuration Overview

Trinity supports PPP over HDLC. Before a PPP interface can be used, there must be an HDLC channel to which it can bind. On some models, the HDLC channels are preconfigured, whereas on others, the user must explicitly create them.

PPP interfaces can be bridged or routed. When a PPP interface operates in bridged mode, data arriving on the HDLC channel from a remote device is forwarded to the assigned interface (Ethernet or another bridged PPP). When a PPP interface is operating in routed mode, data arriving on the HDLC channel is routed to the corresponding interface based on the destination IP address of the arriving packet.

To create a PPP connection, follow these steps:

1. Configure PPP Authentication (Optional)

- PPP allows one peer to demand the other to authenticate itself. The unit supports two authentication protocols: Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP).
- The unit supports dial-in authentication, but not dial-out. The unit can require peers to authenticate, but it will not authenticate itself to peers.
- PPP Authentication is performed via RADIUS. The unit passes the authentication information received from the peer to a RADIUS server and either accepts or rejects the peer based on the RADIUS response.
- PPP authentication configuration applies to all PPP interfaces on the unit. There is no way to configure PPP authentication on a per-interface basis.

2. Create the PPP Interface

3. Configure the PPP Interface

- Select the NCP: either IPCP or BCP.
 - For BCP, configure the MAC address (optional).
 - For IPCP, configure the local and peer IP addresses.
- Bind one or more HDLC interfaces for the PPP interface to run on top of. If more than one HDLC interface is bound, then Multilink Protocol (MLPPP) must be used.
- Enable the PPP interface.

To configure PPP through the WMI, see the section “[Web Management Interface \(WMI\)](#)” on page 85.

To configure PPP through the CLI, see the section “[Command Line Interface \(CLI\)](#)” on page 89.

Web Management Interface (WMI)

To access the PPP main page, click on **Interface Configuration > PPP** from the main menu on the left of the screen.

Configure PPP Authentication

To configure PPP authentication:

1. Click on the **PPP Authentication Configuration** tab on the main PPP page.
2. Choose **None**, **CHAP**, or **PAP** from the **Authentication** drop-down menu.
3. Click **Update**.

Note When the type of authentication is changed, all PPP links that may be up will be terminated and renegotiated with the selected authentication protocol.

The port for the RADIUS server is optional. If left blank, the default port will be used (1812 for authentication and 1813 for accounting).

The screenshot displays the Patton WMI interface for PPP Authentication Configuration. On the left is a navigation tree with categories: System, Interface Configuration (IP Interface, VLAN, Bridge Group, T1/E1, PPP, ARP, DHCP Server, NAT), Routing Configuration, Traffic Management, and Support. The main area is titled 'PPP Authentication' and has two tabs: 'PPP Interface Configuration' and 'PPP Authentication Configuration'. The 'Authentication' section includes a dropdown menu for 'Authentication' (set to 'None') and a text input for 'NAS ID' (set to 'NASID'), with an 'Update' button below. The 'RADIUS Servers' section contains a table with columns for 'Select', 'IP', 'Port', 'Secret', and 'Type'. The 'Type' column has a dropdown menu set to 'Authentication'. There are 'Add' and 'Delete' buttons below the table.

Figure 41. PPP Authentication Configuration

Add PPP Interfaces

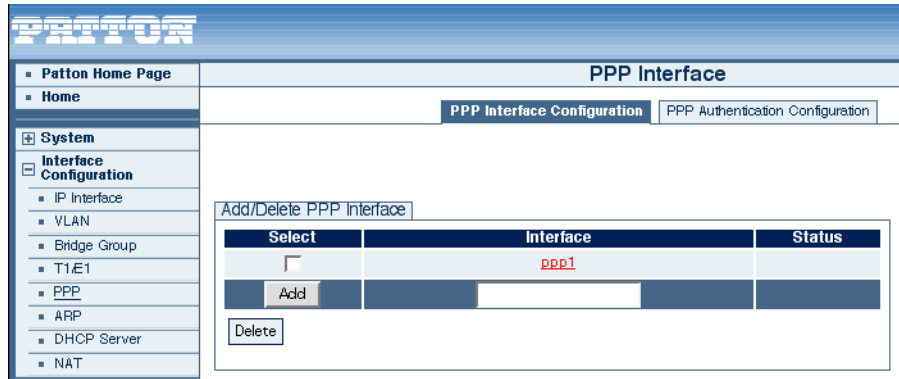


Figure 42. Add/Delete PPP Interfaces

To add a PPP interface:

1. On the PPP Interface Configuration page, enter the name of the interface in the **Interface** field. The name for the PPP interface can be **ppp<number>** or just **<number>**.
2. Click **Add**.

Status of PPP Interfaces

The Status for existing PPP interfaces can be:

- **<blank>**: The PPP interface is not enabled.
- **Down**: The PPP interface is enabled, but has not completed NCP negotiation.
- **Up**: The PPP interface is enabled, has completed NCP negotiation, and is ready to pass traffic.
- **Multilink Partially Up**: The PPP interface is enabled and is ready to pass traffic on at least one, but not all, HDLC interfaces.
- **Multilink Up**: The PPP interface is enabled and is ready to pass traffic on all HDLC interfaces.

Delete PPP Interfaces

To delete a PPP interface:

1. On the PPP Interface Configuration page, click the **Select** checkbox for the interface in the **Add/Delete PPP Interface** table.
2. Click **Delete**.

Configure PPP Interfaces

To configure a PPP interface:

1. Click on the link of the interface you want to configure in the **Add/Delete PPP Interfaces** table on the main PPP page.

PPP Interface - ppp1

PPP Interface Configuration
PPP Authentication Configuration

Select Devices
Update

Enabled
 Multilink (MLPPP)

Bind	Device	Encapsulation	Phase
[icon]	hdlc1	ppp1	Establish
[icon]	hdlc2	ppp2	Establish

LCP

MTU:

MRU:

BCP

MAC:

Management-Inline:

IPCP

Local IP: Accept

Peer IP: Accept

Proxy ARP:

Figure 43. Configuring a PPP interface

2. The **Select Devices** table shows a list of all HDLC devices, but only the devices that are not bound to another PPP interface can be selected. The Phase of HDLC devices can be:
 - **<blank>**: The HDLC device is not bound to a PPP interface or the PPP interface to which it is bound is not enabled.
 - **Holdoff**: Either negotiation failed or the link dropped causing the interface to wait for a period of time before restarting negotiation.
 - **Network**: LCP negotiation has completed, and either IPCP or BCP negotiation is in progress.
 - **Authenticate**: Either CHAP or PAP negotiation is in progress.
 - **Running**: Either IPCP or BCP negotiation has completed, and the PPP is ready to pass data over the HDLC interface.
 - **Multilink Master**: The HDLC interface is the multilink bundle master and is ready to pass data.
 - **Multilink Slave**: The HDLC interface is a multilink bundle slave and is ready to pass data.

Select Devices

Enabled
 Multilink (MLPPP)

Bind	Device	Encapsulation	Phase
[icon]	hdlc1	ppp1	Establish
[icon]	hdlc2	ppp2	Establish

3. For **BCP** configuration, the **Management-Inline** checkbox specifies whether or not to attempt to negotiate the **BCP Management-Inline** option. Some older PPP implementations do not respond correctly to this option causing negotiation to fail.
4. For **IPCP** configuration, both local and peer IP addresses may be configured as:
 - *IP address specified, Accept unchecked*
This causes PPP to attempt to negotiate the specified address and if the peer rejects it, then negotiation fails.
 - *IP address left blank, Accept checked*
This causes PPP to expect the peer to provide the IP address and if the peer does not, then negotiation fails.
 - *IP address specified, Accept checked*
This causes PPP to attempt to negotiate the specified address and if the peer rejects it, to accept the address the peer provides.

Command Line Interface (CLI)

PPP Authentication Commands

Table 24. Steps for Configuring PPP Authentication - CLI

	Command	Explanation
1.	Trinity# configure	Enter the Configuration Mode.
2.	Trinity[config]# pppauth	Enter the PPP Authentication Configuration Mode.
3.	Trinity[pppauth]# authentication {none chap pap}	Start or stop PPP authentication. If the authentication protocol changes, all PPP links that are up will terminate and renegotiate, demanding the selected authentication protocol.
4.	Trinity[pppauth]# nas-id <string>	Set the NAS Identifier.
5.	Trinity[pppauth]# [no] radius-server {auth acct} <A.B.C.D> [port <port>] secret <string>	Add a RADIUS server to the list. If there is a failure accessing a server, the list is tried in round-robin fashion. If <port> is not specified, the default will be used (1812 for authorization and 1813 for accounting).
6.	Trinity[pppauth]# show	Shows the PPP authentication configuration.

- Example - Trinity[pppauth]# show:

```

authentication: chap
nas identifier: MyIdentifier

Server          Password      Type
-----
192.168.200.2:1645  Secret      auth
10.11.2.37       AnotherSecret acct
192.168.200.2     MySecret     auth

```

PPP Configuration Commands

There are different options when creating or configuring PPP interfaces:

- “Creating the interface” on page 90
- “Configuring PPP negotiation” on page 90
- “Enabling PPP on HDLC interfaces” on page 91
- “Configuring LCP” on page 92
- “Configuring IPCP” on page 93
- “Configuring BCP” on page 94
- “Showing Configuration and Status” on page 95

Creating the interface

The following commands create a PPP interface:

Table 25. Steps for Creating a PPP Interface - CLI

	Command	Explanation
1.	Trinity# configure	Enter the Configuration Mode.
2.	Trinity[config]# [no] interface ppp <id>	<id> can be either ppp<number> or just <number>. This creates interface ppp<number> and enters the PPP Configuration Mode. no ppp <id> deletes an interface.

Configuring PPP negotiation

The following commands determine when PPP will attempt to negotiate:

Table 26. Steps for Configuring PPP Negotiation - CLI

	Command	Explanation
1.	Trinity[ppp-ppp2] [no] passive	Setting passive negotiation causes the interface to wait for the peer to start negotiation. The no passive command sets the interface to normal operation, meaning it attempts to negotiate with the peer whether or not the peer has started negotiation.
2.	Trinity[ppp-ppp2] holdoff <seconds>	During the holdoff period, no negotiation will take place. After negotiation fails or LCP determines that the link needs to drop (either by receiving a termination request from the peer or by not receiving replies to echo requests), the interface enters a holdoff period in which it will neither send packets to nor receive packets from the peer.

Enabling PPP on HDLC interfaces

The following commands specify whether the interface is enabled, and if so, over which HDLC interfaces it will run:

Table 27. Steps for Enabling PPP on HDLC interfaces - CLI

	Command	Explanation
1.	Trinity[ppp-ppp2] [no] shutdown	Disables the PPP interface. This causes the PPP interface to attempt to gracefully terminate the session with the peer. no shutdown enables the PPP interface. If the interface was already enabled, it will terminate and then restart using the latest configuration. Note: Any configuration changes made to the PPP interface while it is enabled will not take effect until the no shutdown command is executed.
2.	Trinity[ppp-ppp2] [no] multilink	Enables MLPPP on the interface. This allows the PPP interface to bind to more than one HDLC device.
3.	Trinity[ppp-ppp2] multilink min-frag-size <size>	Configure the minimum fragment size of the first multilink fragment.
4.	Trinity[ppp-ppp2] no multilink min-frag-size	Disable a the minimum fragment size for the first multilink fragment.
5.	Trinity[ppp-ppp2] [no] bind <dev>	Binds a device to an interface. <dev> must be an existing HDLC device. Unless MLPPP is enabled, all HDLC devices bound to this interface must be unbound before binding another HDLC device. If MLPPP is enabled and the PPP link is up, then HDLC devices may be added while the link is running and they will start negotiation immediately.

Configuring LCP

The following commands describe how to configure LCP:

Table 28. Steps for Configuring LCP - CLI

	Command	Explanation
1.	Trinity[ppp-ppp2] lcp	Enter the LCP Configuration Mode.
2.	Trinity[ppp-ppp2-lcp] echo-failure <times>	Sets the number of unanswered LCP Echo-Requests before the PPP interface assumes the link is down and restarts negotiation. PPP sends out LCP Echo-Requests and expects the peer to send LCP Echo-Replies to determine if the link is still up.
3.	Trinity[ppp-ppp2-lcp] echo-interval <seconds>	Sets the time between sending LCP Echo-Requests.
4.	Trinity[ppp-ppp2-lcp] max-configure <times>	Sets the number of LCP Configure-Requests that the peer does not acknowledge before restarting negotiation.
5.	Trinity[ppp-ppp2-lcp] max-failure <times>	Sets the number of LCP Configure-NAKs to send before sending LCP Configure-Rejects instead.
6.	Trinity[ppp-ppp2-lcp] max-terminate <times>	Sets the maximum number of LCP Terminate-Requests to send before terminating.
7.	Trinity[ppp-ppp2-lcp] restart <seconds>	Sets the LCP retransmission timeout.
8.	Trinity[ppp-ppp2-lcp] mru <mru>	Requests the peer to send packets no larger than <mru>.
9.	Trinity[ppp-ppp2-lcp] mtu <mtu>	Requests peer to accept packets at least as large as <mtu>.

Configuring IPCP

The following commands describe how to configure IPCP:

Table 29. Steps for Configuring IPCP - CLI

	Command	Explanation
1.	Trinity[ppp-ppp2] ncp ipcp	Sets PPP to negotiate IPCP as the NCP.
2.	Trinity[ppp-ppp2] ipcp	Enter the IPCP configuration mode.
3.	Trinity[ppp-ppp2-ipcp] {local peer} ip address {accept <A.B.C.D>}	Determines how the IP address will be assigned to the local or peer interface. If an IP address is specified and accept is not, then the PPP interface will attempt to negotiate the address and if the peer rejects, it will terminate. If an IP address is not specified and accept is, then the PPP interface expects the peer to provide the address during negotiation and if the peer does not, it will terminate. If both the IP address and accept are specified, then the PPP interface will attempt to negotiate the address, but if the peer rejects, it will take the address offered by the peer.
4.	Trinity[ppp-ppp2-ipcp] [no] proxy-arp	Enables responding to ARP requests for the peer.
5.	Trinity[ppp-ppp2-ipcp] max-configure <times>	Sets the number of IPCP Configure-Requests that the peer does not acknowledge before restarting negotiation.
6.	Trinity[ppp-ppp2-ipcp] max-failure <times>	Sets the number of IPCP Configure-NAKs to send before sending IPCP Configure-Rejects instead.
7.	Trinity[ppp-ppp2-ipcp] max-terminate <times>	Sets the maximum number of IPCP Terminate-Requests to send before terminating.
8.	Trinity[ppp-ppp2-ipcp] restart <seconds>	Sets the IPCP retransmission timeout.

Configuring BCP

The following commands describe how to configure BCP:

Table 30. Steps for Configuring BCP - CLI

	Command	Explanation
1.	Trinity[ppp-ppp2] ncp bcp	Sets PPP to negotiate BCP as the NCP.
2.	Trinity[ppp-ppp2] bcp	Enter the BCP configuration mode.
3.	Trinity[ppp-ppp2-bcp] mac <XX:XX:XX:XX:XX:XX>	Sets the MAC address for this interface.
4.	Trinity[ppp-ppp2-bcp] [no] management-inline	Negotiates the BCP Management-Inline option. no management-inline does not negotiate the Management-Inline option. Some older PPP implementations do not respond correctly to this option which prevents BCP negotiation from completing.
5.	Trinity[ppp-ppp2-bcp] ieee-802-tagged-frame {allowed required prohibited}	Negotiates whether or not to pass VLAN tagged ethernet frames. The default is to allow, in which case we accept the peer's negotiated value. If the peer does not negotiate tagged frames, then we will not block VLAN tagged frames. The other options are to require the peer to accept tagged frames from us and to prohibit the peer from sending tagged frames to us.
6.	Trinity[ppp-ppp2-bcp] [no] shutdown	Disables the PPP interface when negotiation completes.
7.	Trinity[ppp-ppp2-bcp] [no] ip address <A.B.C.D> [netmask <A.B.C.D> [broadcast <broadcast>]]	Adds an IP address to the PPP interface.
8.	Trinity[ppp-ppp2-bcp] [no] ip address dhcp [ignore {dns hostname route}]	Enables the DHCP client on the interface.

Showing Configuration and Status

Table 31. Showing PPP Configuration and Status

Command	Explanation
Trinity[ppp-ppp2] show	Shows the PPP interface configuration and status.

- **Example - Trinity[ppp-ppp2] show:**

```

No Shutdown
Multilink: Disabled
Device(s):
  hdlc2 (running)
Active
Holdoff:  30 seconds
LCP:
  Echo-Failure: 10  Echo-Interval: 5  Max-Configure: 10  Max-Failure: 10
  Max-Terminate: 3  Restart:        3  MRU:           1500  MTU:           1500
IPCP:
  Local IP: 192.168.254.4
  Peer IP:  192.168.254.5
  Max-Configure: 10  Max-Failure:  10  Max-Terminate: 3  Restart:  3
ppp2 is up
  Internet address 192.168.254.4/0.0.0.0 0 dhcp
  MTU 1500
  ARP disabled
  Multicast enabled
  Rx Statistics
    52 bytes in 4 packets
    0 errors 0 drops, 0 overruns
    0 multicast packets
  Tx Statistics
    46 bytes in 4 packets
    0 errors 0 drops, 0 collisions 0 carrier errors

```

Debugging Commands

Table 32. PPP Debugging Commands - CLI

Command	Explanation
Trinity# debug ppp [<i><id></i>] packet	Shows all PPP packets sent and received on the interface, if one was specified, or else all interfaces.
Trinity# debug ppp [<i><id></i>] [<i>priority {emerg alert crit err warn notice info debug}</i>]	Show all PPP debug messages of at least the priority specified, emerg being the least verbose and debug being the most. If no priority is specified, then err is used.
Trinity# no debug all	Turn off all debugging.

Chapter 13 **PPTP Client Configuration**

Chapter contents

Overview	96
Configuration Overview	97
Web Management Interface (WMI)	98
Creating PPTP Client Interfaces	98
Deleting PPTP Client Interfaces	99
Configuring PPTP Client Interfaces	99
Command Line Interface (CLI).....	100

Overview

This chapter describes how to configure the PPTP Client on the Trinity platform.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

The point-to-point tunneling protocol (PPTP) can be used to create virtual private networks (VPN). It allows remote access to a LAN through the Internet while optionally encrypting the data so that it remains private as it traverses the Internet. It is popular because all Microsoft Windows versions since Windows 95 come with a built-in PPTP client, so no special software needs to be installed.

In a typical application, a PPTP server sits between an office LAN and the Internet. This allows employees to access the office LAN from home, for example to check their email. The setup looks like this:

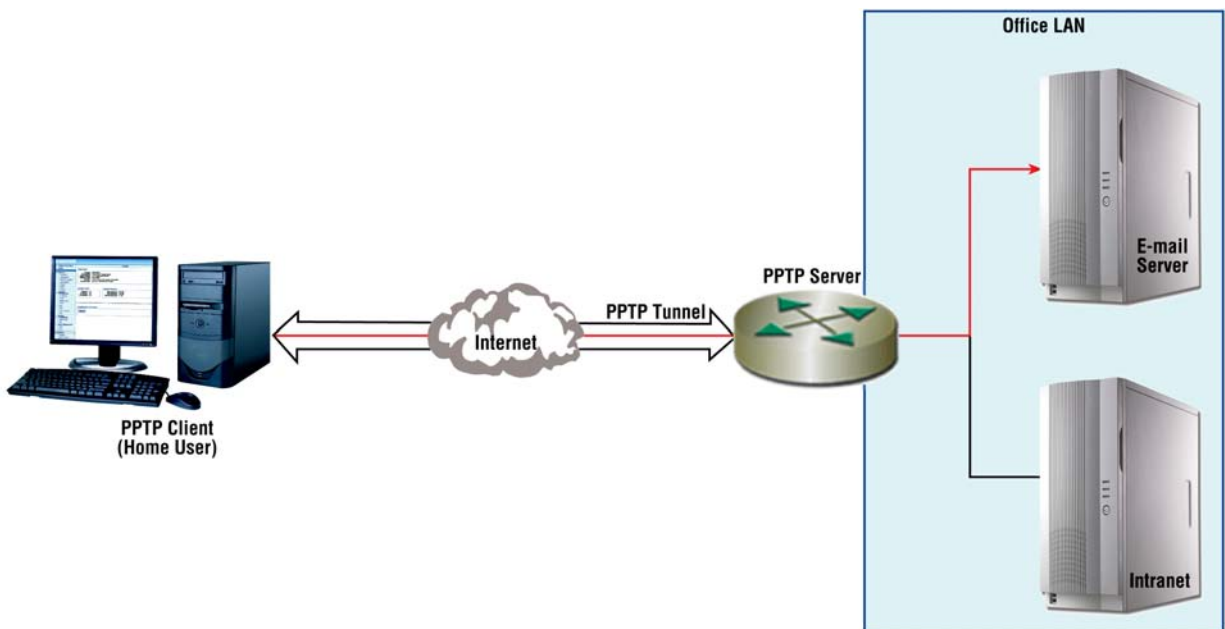


Figure 44. PPTP Work-from-home application

A second common application is used to provide remote offices access to the central office LAN. In this application, as in the first, a PPTP server sits between the central office LAN and the Internet. In addition, each remote office has a router that acts as a PPTP client dialing into the central office. That router then routes all traffic destined for the central office LAN through the PPTP tunnel as show below:

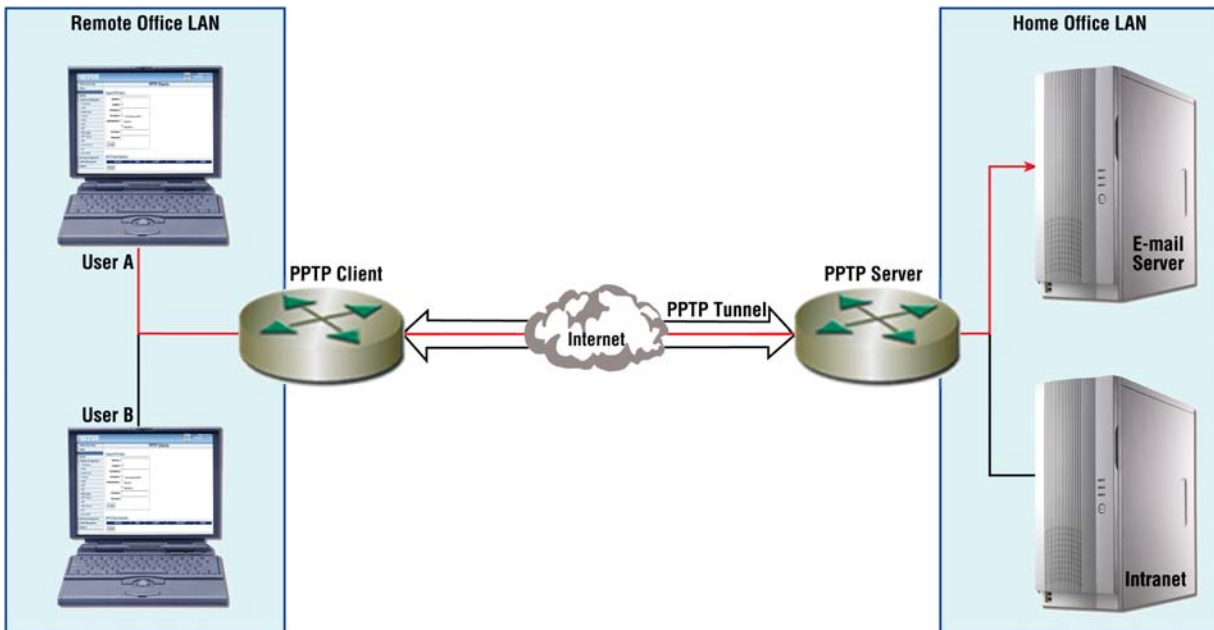


Figure 45. PPTP remote application

Configuration Overview

In order to connect to a PPTP server, you will need to configure the following:

- **Destination:** The PPTP server's hostname or IP address.
- **Username and Password:** These are only required if the server requires authentication. It is far more common that you will need these.

In addition, you may also configure the following optional parameters:

- **Authentication:** Both MSCHAP versions, 1 and 2, are supported. By default, the client will only authenticate to the server using version 2. It will reject requests to authenticate with the less secure version 1.
- **Encryption:** By default, 128 bit MPPE encryption is used, but it may be disabled. This must match the server's setting. Authentication must be enabled for encryption to be used.

When you have configured the interface, enable it to connect to the server.

To configure the PPTP Client through the WMI, see the section "[Web Management Interface \(WMI\)](#)" on page 99.

To configure the PPTP Client through the CLI, see the section "[Command Line Interface \(CLI\)](#)" on page 101.

Web Management Interface (WMI)

To access the PPTP Client main page, click on **Interface Configuration > PPTP Client** from the main menu on the left of the screen.

Figure 46. PPTP Client main page

Creating PPTP Client Interfaces

Figure 47. Create PPTP Client Interfaces

To create a PPTP Client interface, specify the following parameters:

- **Interface:** Enter a name for the new PPTP client interface in the form **<number>** or **pptp<number>**.
- **Enabled:** Check to enable the new PPTP interface.
- **Destination:** Enter a name for the PPTP server to connect to. The server may be specified as either a host-name or an IP address. The destination must be set in order to enable the interface.

- **Encryption:** Check/uncheck the box to enable/disable MPPE encryption. By default, MPPE encryption is enabled, but it can be disabled. The client encryption setting must match the server's encryption setting. Also, authentication must be enabled to use the encryption option.
- **Authentication:** Select the box for MSCHAPv2. By default, the client will only authenticate to the sever using MSCHAP version 2.
- **Username and Password:** Enter a username and password to use to verify access to the server.

Deleting PPTP Client Interfaces

PPTP Client Interfaces				
Interface	State	Local IP	Remote IP	Delete
pptp0	Running	192.168.3.201	192.168.3.200	<input type="checkbox"/>

Delete

Figure 48. Delete PPTP Client Interfaces

To delete a PPTP client interface, select the **Delete checkbox** for the interface you want to delete in the PPTP Client Interfaces table. Then, click **Delete**.

Configuring PPTP Client Interfaces

PPTP Client: pptp0	
<p>Configuration</p> <p>Enabled: <input checked="" type="checkbox"/></p> <p>Destination: 192.168.200.1</p> <p>Encryption: <input checked="" type="checkbox"/> 128 bit stateless MPPE</p> <p>Authentication: <input type="checkbox"/> MSCHAP <input checked="" type="checkbox"/> MSCHAPv2</p> <p>Username: Bob</p> <p>Password: *****</p> <p>Update</p>	<p>Status</p> <p>State: Holdoff</p> <p>Local IP:</p> <p>Remote IP:</p>

Figure 49. Configure existing PPTP Client interfaces

To update an existing PPTP Client interface:

1. From the main PPTP Client page, click on the interface name in the table.
2. The configuration and status page for the interface displays. Make the desired changes, then click **Update**.

Command Line Interface (CLI)

Table 33. PPTP Client Commands - CLI

Command	Explanation
configure interface pptp-client <pptpX>	Enter the configuration mode for an existing PPTP client interface. This command also creates a new PPTP client interface.
configure [no] interface pptp-client <pptpX>	Delete the specified PPTP client interface.
[no] shutdown	Enable/disable the interface.
[no] destination <server>	Set/clear which PPTP server to connect to. The server may be specified as either a hostname or an IP address. The destination must be set in order to enable the interface.
[no] authentication {mschap mschap-v2}	Specify which authentication protocol(s), if any, will be used to authenticate to the server.
[no] encryption mppe	Specify whether or not to use MPPE encryption.
[no] username <username> password <password>	Specify the username and password, if any, to use to authenticate to the server.
show interface pptp-client <pptpX>	Display the PPTP client interface's configuration and status.
[no] debug pptp-client <pptpX> [priority {emerg alert crit err warn notice info debug}]	Debugging a PPTP client interface with a priority of debug will show all PPTP control packets and all PPP packets transmitted and received.

- Example - Router# show interface pptp-client <pptpX>:

```

Destination:      vpn.work.com
Encryption:      128-bit MPPE stateless
Authentication:   MSCHAPv2
Account:         Bob password
State:           Holdoff
Local/Remote IP: <none>/<none>
pptp0 is up, line protocol is down
  MTU 1500
  ARP disabled
  Multicast enabled
  Rx Statistics
    0 bytes in 0 packets
    0 errors 0 drops, 0 overruns
    0 multicast packets
  Tx Statistics
    0 bytes in 0 packets
    0 errors 0 drops, 0 collisions 0 carrier errors

```

Chapter 14 **PPTP Server Configuration**

Chapter contents

Overview	102
Configuration Overview	103
Web Management Interface (WMI)	104
Configuring the PPTP Server	104
Adding Users to the PPTP Server	105
Viewing Connections to the PPTP Server	105
Command Line Interface (CLI).....	106

Overview

This chapter describes how to configure the PPTP Server on the Trinity platform.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

The point-to-point tunneling protocol (PPTP) can be used to create virtual private networks (VPN). It allows remote access to a LAN through the Internet while optionally encrypting the data so that it remains private as it traverses the Internet. It is popular because all Microsoft Windows versions since Windows 95 come with a built-in PPTP client, so no special software needs to be installed.

In a typical application, a PPTP server sits between an office LAN and the Internet. This allows employees to access the office LAN from home, for example to check their email. The setup looks like this:

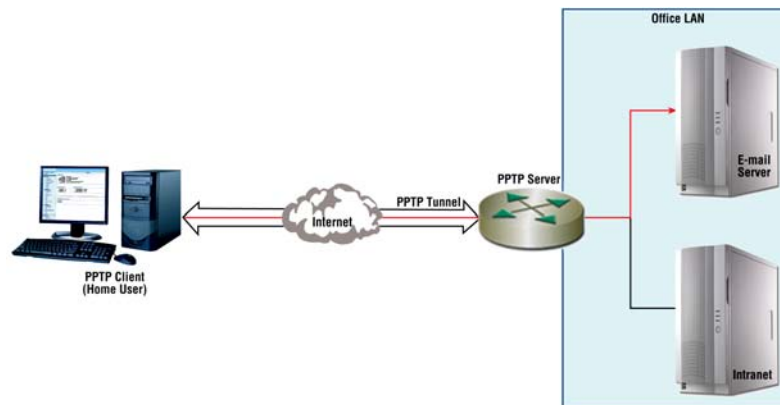


Figure 50. PPTP Work-from-home application

A second common application is used to provide remote offices access to the central office LAN. In this application, as in the first, a PPTP server sits between the central office LAN and the Internet. In addition, each remote office has a router that acts as a PPTP client dialing into the central office. That router then routes all

traffic destined for the central office LAN through the PPTP tunnel as show in Figure 51.

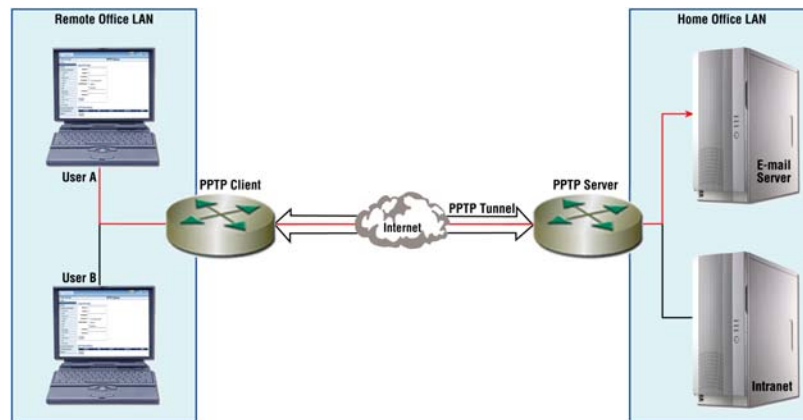


Figure 51. PPTP remote application

Configuration Overview

In order to connect to a PPTP server, you will need to configure the following:

- **Local IP Address**
- **Remote IP Address Pool:** Each client that connects to the PPTP server needs a pair of IP addresses for the tunnel endpoints, one for the server and one for itself. The server endpoint uses the same IP address for each connection and assigns each client endpoint a different IP address from the remote IP address pool. These addresses should be in a subnet different than both the Internet and the private LAN.
- **User Accounts:** If the server requires authentication, as it does by default, then at least one user account must be created.

In addition, you may optionally configure the following:

- **Authentication:** Both MSCHAP version 1 and version 2 are supported. By default, the server requires clients to authenticate themselves using MSCHAP version 2 and refuses the less secure version 1. The configuration is as follows:
 - MSCHAPv1 and MSCHAPv2: The client must authenticate itself, but may choose whether to use version 1 or version 2.
 - MSCHAPv2: The client must authenticate itself using version 2. Version 1 will be rejected.
 - MSCHAPv1: The client must authenticate itself using version 1. Version 2 will be rejected.
 - None: The client does not have to authenticate itself.
- **Encryption:** 128 bit stateless MPPE is supported. By default, the server requires clients to use it. In order to use encryption, authentication must also be required.
- **DNS and WINS Servers:** Windows clients will use the specified DNS and WINS servers. Clients running on most other operating systems ignore these parameters.

Once you have finished configuring the PPTP server, enable it to allow clients to connect.

To configure the PPTP Client through the WMI, see the section “[Web Management Interface \(WMI\)](#)” on page 106.

To configure the PPTP Client through the CLI, see the section “[Command Line Interface \(CLI\)](#)” on page 108.

Web Management Interface (WMI)

To access the PPTP Server main page, click on **Interface Configuration > PPTP Server** from the main menu on the left of the screen.

The screenshot shows the PPTP Server configuration page. The top right corner includes 'Reboot' and 'Save' buttons, along with 'Model: 3038/C/01' and 'Hostname: (none)'. The left sidebar lists various configuration categories. The main area is titled 'PPTP Server' and contains three sections: 'Configuration' with input fields for 'Enabled', 'Local IP', 'Remote IP Pool', 'Encryption' (128 bit stateless MPPE), 'Authentication' (MSCHAP, MSCHAPv2), 'DNS Servers', and 'WINS Servers', plus an 'Update' button; 'Users' with 'Username' and 'Password' fields, an 'Add' button, and a table with 'User' and 'Delete' columns; and 'Connections' with a table header for 'User', 'Public IP', 'Tunnel IP', and 'State'.

Figure 52. PPTP Server main page

Configuring the PPTP Server

To configure the PPTP Server, set the following parameters in the **Configuration** section:

This screenshot shows the 'Configuration' section of the PPTP Server page. The 'Enabled' checkbox is checked. The 'Local IP' field contains '10.0.0.1'. The 'Remote IP Pool' field contains '10.0.0.2' and '10.0.0.5'. The 'Encryption' section has '128 bit stateless MPPE' checked. Under 'Authentication', 'MSCHAPv2' is checked. The 'Update' button is at the bottom left of the configuration box.

Figure 53. Configuring and updating the PPTP Server

- **Enabled:** Check/uncheck the Enabled box to enable/disable the PPTP Server.
- **Local IP:** Enter the local tunnel IP address. This IP address must be set in order to enable the server.

- **Remote IP Pool:** Enter the range of IP addresses to assign client tunnel IP addresses. This range must be set in order to enable the server.
- **Encryption:** Check/uncheck the box to enable/disable MPEE encryption.
- **Authentication:** Select the box for MSCHAPv2.
- **DNS Servers:** Enter the primary and secondary DNS servers for a Windows client to use.
- **WINS Servers:** Enter the primary and secondary WINS servers for a Windows client to use.

Click **Update** to save your settings for the PPTP Server.

Adding Users to the PPTP Server

The screenshot shows the 'Users' section of the PPTP Server configuration. It includes two input fields for 'Username:' and 'Password:', followed by an 'Add' button. Below these is a table with two columns: 'User' and 'Delete'. The table lists four users: Alice, Bob, Cathy, and Donald, each with a corresponding 'Delete' checkbox.

User	Delete
Alice	<input type="checkbox"/>
Bob	<input type="checkbox"/>
Cathy	<input type="checkbox"/>
Donald	<input type="checkbox"/>

Figure 54. Adding users to the PPTP Server

To add a user to the PPTP Server, enter the username and password in the fields in the **Users** section, then click **Add**. The new user will show up in the User list.

Viewing Connections to the PPTP Server

The screenshot shows the 'Connections' table. It has four columns: 'User', 'Public IP', 'Tunnel IP', and 'State'. A single row is visible for user Bob with Public IP 192.168.200.1, Tunnel IP 10.0.0.2, and State Running.

User	Public IP	Tunnel IP	State
Bob	192.168.200.1	10.0.0.2	Running

Figure 55. Viewing connections to the PPTP Server

The **Connections** table on the PPTP Server page displays the IP address and current state of a user's connection to the PPTP Server.

Command Line Interface (CLI)

Table 34. PPTP Server Commands - CLI

Command	Explanation
configure interface pptp-server	Enter the PPTP server configuration mode.
[no] shutdown	Enable/Disable the PPTP server.
[no] ip address <A.B.C.D>	Set/clear the local tunnel IP address. This IP address must be set in order to enable the server.
[no] remote ip pool <A.B.C.D> <A.B.C.D>	Set/clear the range of IP addresses from which to assign client tunnel IP addresses. This range must be set in order to enable the server.
[no] authentication {msc-hap mschapv2}	Specify the method to use to authenticate clients.
[no] encryption mppe	Specify whether or not to use MPPE encryption.
[no] dns-server <A.B.C.D> [<A.B.C.D>]	Specify the primary and secondary DNS servers for a Windows client to use.
[no] wins-server <A.B.C.D> [<A.B.C.D>]	Specify the primary and secondary WINS servers for a Windows client to use.
[no] username <username> password <password>	Create a user account, update an existing user's password, or delete a user account.
show interface pptp-server	Show the PPTP server configuration and the clients currently connected.
[no] debug pptp-server [priority {emerg alert crit err warn notice info debug}]	Enabling PPTP server debugging with a priority of debug will show all PPTP control packets and all PPP packets transmitted and received.

- Example - Router# show interface pptp-server:

```

onfiguration:
  State:          Enabled
  Local IP:       10.0.0.1
  Remote IP Pool: 10.0.0.2-10.0.0.5
  Encryption:     128-bit MPPE stateless
  Authentication: MSCHAPv2
  DNS:
  WINS:

Users:
  Alice
  Bob
  Cathy
  Donald

Connections:

```

Username	Public IP	Tunnel IP	State
-----	-----	-----	-----
Bob	192.168.200.1	10.0.0.2	Running

Chapter 15 **ARP Table Management**

Chapter contents

Overview	109
Configuration Overview	109
About ARP Entries	109
Web Management Interface (WMI)	110
Adding ARP Entries	110
Deleting ARP Entries	110
Command Line Interface (CLI)	111
Adding ARP Entries	111
Deleting ARP Entries	111
Displaying ARP Entries	111

Overview

This chapter describes how to add and delete ARP entries, display the contents of the ARP Table, and flush the ARP Table contents.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

Configuration Overview

An ARP entry can be added to the table by configuring the following:

- IP address
- Interface device name
- Interface device hardware (Ethernet) address
- State

About ARP Entries

The state of an ARP entry designates whether the entry is temporary or permanent. **Temporary entries** are usually the ones added to the table dynamically through address resolution. Temporary entries time-out and are removed from the ARP table automatically. **Permanent entries** are the entries that are added to the table by the user. These entries do not time-out and have to be removed explicitly by the user.

The ARP entries are displayed in a table. The table also displays the type of hardware (e.g. ethernet), a network mask value (if one exists), and a combination of flags:

- **C – Complete** – Represents a valid entry; Entry has been successfully resolved.
- **M – Manual/Permanent** – Permanent entry added by the user.
- **P – Published** – The network device corresponding to the entry is advertising (publishing) its address.
 - This usually happens if the network device is acting as an ARP proxy for other devices. If the device is acting as an ARP proxy to a subnet of devices, the entry might have a netmask value as well.

ARP entries are deleted from the system by selecting them through the Web Management Interface (WMI), or by using the **no arp** command in the Command Line Interface (CLI). The CLI also provides a **flush** command to delete all entries at once. When an entry is submitted for deletion, it is not removed from the ARP table right away. It is marked as a pending deletion and is removed if there are no active connections using it. A temporary entry might be added back to the table immediately if a new connection is established.

To configure ARP through the WMI, see the section “[Web Management Interface \(WMI\)](#)” on page 112.

To configure ARP through the CLI, see the section “[Command Line Interface \(CLI\)](#)” on page 113.

Web Management Interface (WMI)

To access the ARP main page, click on **Interface Configuration > ARP** from the main menu on the left of the screen.

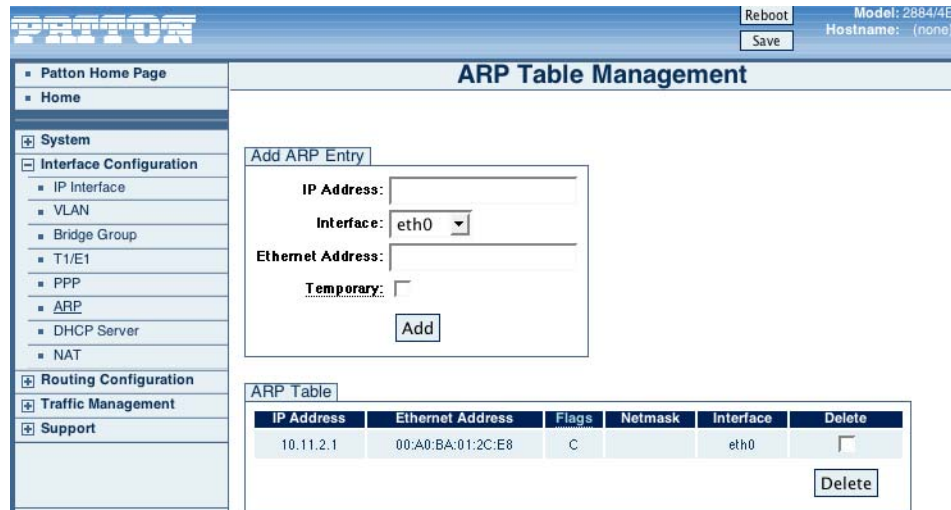


Figure 56. ARP main page

Adding ARP Entries

To add an ARP entry:

1. Enter an IP address (dotted quad) for the entry in the **IP Address** box.
2. Choose an interface from the **Interface** drop-down menu.
3. Enter the **Ethernet (Hardware) Address** (<XX:XX:XX:XX:XX:XX>).
4. Select the **Temporary** checkbox to mark an entry as temporary (optional). The default State is permanent. For more information on the state of an ARP entry, see the section “[About ARP Entries](#)” on page 111.

Deleting ARP Entries

The ARP Table displays all existing entries in the system. To delete an entry:

1. Select the Delete checkbox for the entry in the **ARP Table**.
2. Click **Delete**.

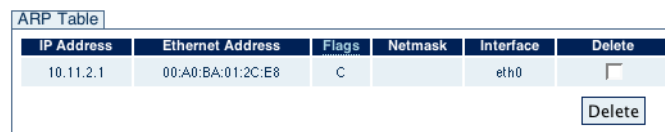


Figure 57. Deleting an ARP entry from the ARP table

Command Line Interface (CLI)

Table 35. ARP - CLI

Command	Explanation
<ipaddr>	Network address; Must be given in standard form (<dotted quad>)
<dev>	Interface device name
<hwaddr>	Hardware address of the interface device (<XX:XX:XX:XX:XX:XX>)
temp	Explicitly marks an entry as temporary

Adding ARP Entries

ARP entries are added using the **arp** command under the configure mode of the CLI:

Table 36. Adding ARP Entries - CLI

Command	Explanation
Trinity# configure	Enter configuration mode.
Trinity [config]# arp <ipaddr> <dev> <hwaddr> [temp]	Add an ARP entry. Example: <i>Trinity [config]# arp 192.168.1.50 eth1 00:a0:ba:00:69:ef</i>

Deleting ARP Entries

ARP entries are deleted using the **no arp** command, or by using the **arp flush** command as shown below:

Table 37. Deleting ARP Entries - CLI

Command	Explanation
Trinity# configure	Enter configuration mode.
Trinity# configure [no] arp <ipaddr> <dev>	Delete an ARP entry. Example: <i>Trinity [config]# no arp 192.168.1.50 eth1</i>
Trinity [config]# arp flush	Deletes all ARP entries at the same time.

Displaying ARP Entries

The ARP table is displayed using the **show arp** command either under the configure mode or at the root:

Table 38. Showing ARP Entries - CLI

Command	Explanation
Trinity# show arp	Show the list of ARP entries at the root.
Trinity# configure	Enter configuration mode.
Trinity[config]# show arp	Show a list of ARP entries in configuration mode.

```
Trinity# show arp
System Arp Table
Flags: C - complete, M - manual/permanent, P - published
-----+-----+-----+-----+-----+-----+
| IP Address | Type | HW Address | Flags | Netmask | Interface |
-----+-----+-----+-----+-----+
| 192.168.1.1 | ether | AA:BB:CC:DD:EE:FF | CM | | eth0 |
-----+-----+-----+-----+-----+
Trinity# configure
Trinity(config)# show arp
System Arp Table
Flags: C - complete, M - manual/permanent, P - published
-----+-----+-----+-----+-----+
| IP Address | Type | HW Address | Flags | Netmask | Interface |
-----+-----+-----+-----+-----+
| 192.168.1.1 | ether | AA:BB:CC:DD:EE:FF | CM | | eth0 |
-----+-----+-----+-----+-----+
Trinity(config)# █
```

Figure 58. Command Line Interface "show arp" command

Chapter 16 **DHCP Server Configuration**

Chapter contents

Overview	114
Configuration Overview	114
Web Management Interface	115
Configuring the DHCP Server	115
Add/Delete Routers	116
Add/Delete DNSs	116
Add/Delete Static Leases	116
Command Line Interface (CLI).....	117
DHCP Server Configuration Commands	117
DHCP Debugging Commands	118

Overview

This chapter describes how to configure the DHCP server. DHCP is a client/server protocol used to provide configuration parameters to hosts on a network.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

Configuration Overview

The DHCP server is configured using the following:

- **IP Range:** This is the range of IP addresses in the IP address pool used for automatic allocation of IP leases. This list is inclusive - both the start and end addresses are included in the range.
- **Lease/Max Lease Time:** This is the maximum time the client may lease an IP address before either requesting it again or relinquishing it.
- **Domain Name:** This is the domain name that the client will use to resolve hostnames. This is optional and may or may not be provided to the client.
- **Routers:** This is the list of routers used to configure the client's routing table. The first item is the default gateway. The others are other routes. This list may be empty.
- **DNS Servers:** This is the list of the DNS servers for the client to use. The order of the list is important. The first item is the preferred DNS server. The others are alternates. This list may be empty.
- **Static Leases:** This is a list of manual allocations. It maps an IP address to a MAC address. The IP addresses in this list may, but do not have to, overlay with the IP range. This list may be empty.

The DHCP server may be configured only when it is not bound to any interface. It may be bound to a single interface at a time. The interface to which this server is bound must have an IP address assigned to it. The IP address should be on the same subnet as the addresses in the IP range.

To configure the DHCP server through the WMI, see the section "[Web Management Interface](#)" on page 117.

To configure the DHCP server through the CLI, see the section "[Command Line Interface \(CLI\)](#)" on page 119.

Web Management Interface

To access the DHCP Server Configuration page, click on **Interface Configuration > DHCP Server** from the main menu on the left of the screen.

Figure 59. DHCP Server Configuration Main Screen

Configuring the DHCP Server

To configure the DHCP server:

1. Select an interface from the **Interface** drop-down menu.
2. Enter the first IP address (dotted quad format) in the pool of IP addresses to lease in the **IP Start** field.
3. Enter the last IP address (dotted quad format) in the pool of IP addresses to lease in the **IP End** field.
4. Enter the address for the netmask (dotted quad or /xx format) in the **Netmask** field.
5. Enter the number of seconds for the max lease time in the **Max Lease** field.
6. Enter a domain name in the **Domain Name** field (optional). If left blank, the server will not supply any domain name to a client.
7. Click **Update**.
8. To configure the DHCP server with new settings, click **Unbind**, then repeat steps 1-7.

Add/Delete Routers

To add a router, enter the router's address in dotted quad format in the text box in the **Routers** section, then click **Add**.

To delete a router, select the router from the list in the **Routers** section, then click **Delete**.

Add/Delete DNSs

To add a DNS server, enter the server's address in dotted quad format in the text box in the **DNSs** section, then click **Add**.

To delete a DNS server, select the server from the list in the **DNSs** section, then click **Delete**.

Add/Delete Static Leases

The **Static Leases** section shows a list of manual bindings. To add a static lease, enter the MAC address in XX:XX:XX:XX:XX:XX format in the **MAC Address** text box. Enter the IP address in dotted quad format in the **IP Address** text box. Then, click **Add**.

To delete a static lease, select the lease from the list in the **Static Leases** section, then click **Delete**.

Command Line Interface (CLI)

DHCP Server Configuration Commands

The DHCP server may be configured from the command line under the **configure dhcpd** mode:

Table 39. DHCP Server - CLI Commands

Command	Explanation
Trinity# iprange <ipstart> <ipend>	Must be in <dotted quad> format.
Trinity# subnet <netmask>	Must be in <dotted quad> or /xx format
Trinity# lease <days> [<hours> [<minutes> [<seconds>]]]	Sets the length of lease to offer. <days> must be an integer, <hours> must be between 0 and 23, and <minutes> and <seconds> must be between 0 and 59.
Trinity# domain-name <domain-name>	May be any arbitrary string.
Trinity# no domain-name	Unsets any domain name that may have been set. The server will not provide any domain name to the client.
Trinity# default-router <router1> [<router2 .. router8>]	Must be in <dotted quad> format. At least one router is required. Up to eight may be specified on one command line.
Trinity# no default-router	Removes all default routers that may have been entered previously.
Trinity# dns-server <server1> [<server2 .. server8>]	Must be in <dotted quad> format. At least one server is required. Up to eight may be specified on one command line.
Trinity# no dns-server	Removes all DNS servers that may have been entered previously.
Trinity# static-lease <mac> <ip>	<mac> must be supplied in XX:XX:XX:XX:XX:XX format, where xx is a hexadecimal octet. <ip> must be supplied in <dotted quad> format.
Trinity# no static-lease	Removes all static leases that may have been entered previously.
Trinity# bind <interface>	Binds the server to the specified interface. <interface> must be an interface that is up and that has at least one IP address bound to it. The server may no longer be configured until it is unbound from the interface.
Trinity# no bind	Unbinds the server from any interface to which it may be bound. The server may now be configured.

The configuration may be viewed from the root mode using the `show dhcpd` command. The following is example output:

```
Configuration:
Interface:    <unbound>
IP Range:    192.168.200.100 - 192.168.200.200
Subnet:      255.255.255.0
Lease:       10d 0h 0m 0s
Domain:      patton.com
Routers:     192.168.200.1
             192.168.200.2
DNS:         192.168.200.2
Static Leases: MAC Address      IP Address
                00:A0:BA:00:01:23 192.168.200.50
                00:A0:BA:00:AB:CD 192.168.200.150

Leases:
MAC Address      IP Address      Expires In
00:C0:49:63:07:84 192.168.200.100 9d 23h 55m 51s
00:13:20:6E:41:58 192.168.200.101 6d 23h 6m 47s
00:A0:BA:00:94:DA 192.168.200.104 9d 23h 55m 51s
00:0F:1F:54:F7:93 192.166.200.106 0d 20h 41m 40s
00:03:B3:0B:D5:81 192.168.200.121 2d 18h 11m 3s
00:A0:BA:00:55:5A 192.168.200.169 9d 18h 56m 39s
```

DHCP Debugging Commands

Table 40. DHCP Debugging - CLI

Command	Explanation
Trinity# debug dhcpd [priority {emerg alert crit err warn notice info debug}]	Specifying the priority is optional. The debugging output shows the packets sent by the DHCP server.

Example output:

```
Nov 1 00:26:17 udhcpd: info: sending OFFER of 192.168.200.100
Nov 1 00:26:17 udhcpd: info: sending ACK to 192.168.200.100
```

Note

- If the message "Could not start DHCP server." is displayed when attempting to bind to an interface, it is most likely because the interface does not have an IP assigned to it.
- This DHCP server will never lease all of the addresses in the IP range at one time. It will always have at least one that is not leased, and possibly more if any static leases have been assigned to a host.

Chapter 17 NAT and Port Forwarding

Chapter contents

Overview	120
Configuration Overview	120
About NAT	120
About Port Forwarding	120
Web Management Interface (WMI)	121
NAPT	121
Creating NAPT Profiles	121
Deleting NAPT Profiles	121
Editing NAPT Profiles	122
Port Forwarding	123
Creating Port Forwarding Profiles	123
Deleting Port Forwarding Profiles	123
Editing Port Forwarding Profiles	123
Connection Tracking	124
Command Line Interface (CLI).....	125
NAPT	125
NAPT Configuration Commands	125
NAPT Profile Configuration Commands	125
Sample Rules.....	126
Sample Bindings.....	126
NAPT CLI Examples	126
Example - Simple NAPT Setup.....	126
Example - Importance of Rule Order	126
Example - Masquerading Rule.....	127
Port Forwarding	128
Port Forwarding Configuration Commands	128
Port Forwarding Profile Configuration Commands	128
Sample Rules.....	129
Sample Bindings.....	129
Port Forwarding CLI Examples	129
Example - Configuring a Port Forwarding Profile	129
Example - Defining Rules for a Port Forwarding Profile.....	129
Connection Tracking	130
Connection Tracking Configuration Commands	130
Connection Tracking CLI Examples	130
Example - Configuring Connection Tracking	130

Overview

This chapter describes how to configure Network Address Port Translation (NAPT) and Port Forwarding.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

Configuration Overview

Both NAT and Port Forwarding follow the same basic approach. First, a profile is created, and the rules defining the address translation behavior are added to the profile. Finally, the profile is bound to an interface. Profiles can be bound to more than one interface, although this may not be very useful. NAT and Port Forwarding differ in what rules are available to them.

About NAT

NAT maps traffic from local addresses behind a gateway device to public addresses. The NAT component can map all local IP addresses, a range of local IP addresses, or a single local IP address. When NAT profiles are bound to the interface, the traffic will be going out. Under the most common use, all the public addresses referred to in the rules need to be assigned to that interface.

However, there are cases where it is desirable to have the public addresses for the NAT be different than the address of the outgoing interface. There may be some security benefit by not having the NAT device's publicly visible address be the same as the value being broadcast to an outside site, or port exhaustion may be mitigated by spreading the NAT over several addresses. In this case, it may be necessary to set up static routes in the upstream routers so that return traffic is correctly forwarded to the NAT device.

For example, if the NAT device is at public address 10.10.1.1, and we are using 10.10.2.2 for NAT traffic, upstream routers will not know how to return traffic to 10.10.2.2 unless we set up static routes indicating that the next hop for 10.10.2.2 is 10.10.1.1.

About Port Forwarding

Port Forwarding maps incoming traffic destined for a public address to a local address. There are three types of Port Forwarding supported: DMZ (where all incoming traffic to a public address is redirected to a local address), by protocol, and by port (for the TCP and UDP protocols).

Trinity provides a basic connection track for TCP and UDP protocols. However, some protocols require special connection tracking handling to work through address translation. Currently, Trinity supports the special handling that FTP requires. Specialized connection tracking for a protocol is turned on on a system wide basis, and can be enabled or disabled as desired.

To configure NAT through the WMI, see the section "[Web Management Interface \(WMI\)](#)" on page 123.

To configure NAT through the CLI, see the section "[Command Line Interface \(CLI\)](#)" on page 127.

Web Management Interface (WMI)

The NAT and Port Forwarding Page is divided into three configuration tabs:

- “NAPT” on page 123
- “Port Forwarding” on page 125
- “Connection Tracking” on page 126

To access the NAT main page, click on **Interface Configuration** > **NAT** from the main menu on the left of the screen.

Figure 60. NAT Configuration

NAPT

Creating NAPT Profiles

To create a NAPT profile:

1. Enter the profile name in the **Name** field in the **Create a NAPT Profile** section. Profile names must be alpha-numeric and no longer than 25 characters.
2. Click **Submit**.
3. The configuration page for that profile will be displayed. If the profile already exists, a warning message and the configuration page for the profile will be displayed.

Deleting NAPT Profiles

The **NAPT Profiles** table lists all the profiles, how many rules each profile has, and how many interfaces it is bound to. To delete a NAPT profile, select the **Delete** checkbox for the profile in the **NAPT Profiles** table and click **Delete Selected**.

Editing NAT Profiles

myprofile - NAT Profile

Rules:

Local IP Start	Local IP End	Public IP Start	Public IP End	Delete
10.10.0.1	10.10.0.50	192.168.1.1	192.168.1.50	<input type="checkbox"/>
10.10.0.127		Masquerade		<input checked="" type="checkbox"/>

Add New Rule:

Local IP Start	Local IP End	Public IP Start	Public IP End	Masquerade
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Interface Bindings:

Interface	Unbind
eth1	<input checked="" type="checkbox"/>

Bind to Interface:

Add Interface binding:

Figure 61. NAT Profile Configuration

To edit a NAT profile, click on the link of the profile name in the **NAPT Profiles** table. The link will lead to the configuration page for that profile.

The following can be set on a profile's configuration page:

- **Rules:** Lists the existing rules.
 - **Add Rule:** To add a rule, fill in information for **Local IP Start**, **Local IP End**, **Public IP Start**, and **Public IP End**, then click **Submit**. **Local IP End** or **Public IP End** field can be omitted if the NAT mapping is *from* a single local IP address or *to* a single public IP, respectively.
 - **Create Masquerading Rule:** To create a masquerading rule, fill in the information for **Local IP Start** and **Local IP End** (optional) fields, and select the **Masquerade** checkbox. In this case, the public IP address to map the local IP addresses will be determined dynamically by the system based on the interface the profile is bound to.
 - **Delete Rule:** To delete a rule, select the **Delete** checkbox for the rule, then click **Submit**.
- **Interface Bindings:** Lists interface bindings.
 - To bind an interface, select an option from the **Add interface binding** drop-down menu, and click **Submit**.
 - To unbind an interface, select the **Unbind** checkbox and click **Submit**.

Port Forwarding

Figure 62. Main Port Forwarding Configuration

Creating Port Forwarding Profiles

To create a Port Forwarding profile:

1. Enter the profile name in the **Name** field in the **Create a Port Forwarding Profile** section. Profile names must be alpha-numeric and no longer than 25 characters.
2. Click **Submit**.
3. The configuration page for that profile will be displayed. If the profile already exists, a warning message and the configuration page for the profile will be displayed.

Deleting Port Forwarding Profiles

The **FWRD Profiles** table lists all the profiles, how many rules each profile has, and how many interfaces it is bound to. To delete a Port Forwarding profile, select the **Delete** checkbox for the profile in the **FWRD Profiles** table and click **Delete Selected**.

Editing Port Forwarding Profiles

Local IP	Local Port	Public IP	Public Port	Protocol	Delete
10.10.1.2	8080	192.168.200.2	80	tcp	<input type="checkbox"/>
10.10.1.2	22	192.168.200.2	22	tcp	<input checked="" type="checkbox"/>

Interface	Unbind
eth0.0023	<input type="checkbox"/>

Figure 63. Port Forwarding Profile Configuration

To edit a Port Forwarding profile, click on the link of the profile name in the **FWRD Profiles** table. The link will lead to the configuration page for that profile.

The following can be set on a profile's configuration page:

- **Rules:** Lists the existing rules.
 - To add a rule, fill in information for **Local IP**, **Local Port**, **Public IP**, **Public Port**, and **Protocol**, then click **Submit**.

Local IP: Local IP address to port forward to in dotted-quad form (<A.B.C.D>)

Local Port: Local port number to use when forwarding traffic; range 0-65535. Local Port is an optional field. However, if a Public Port is specified then Local Port must also be specified.

Public IP: Public IP address to port forward from in dotted-quad form (<A.B.C.D>).

Public Port: Public port number to use when forwarding traffic; range 0-65535. Public Port is an optional field. However, if a Local Port is specified then Public Port must also be specified.

If both Local and Public Port fields are omitted, incoming traffic ports will be forwarded to identical local ports.

Protocol: Protocol to use when port forwarding traffic, protocol number in integer form or keywords {tcp, udp}. Protocol number for different protocols can be found at www.iana.org/assignments/protocol-numbers. Protocol is an optional field. However, if Local and Public Port fields are specified a protocol type is required.

- To delete a rule, select the Delete checkbox for the rule, then click **Submit**.
- **Interface Bindings:** Lists interface bindings.
 - To bind an interface, select an option from the **Add interface binding** drop-down menu, and click **Submit**.
 - To unbind an interface, select the **Unbind** checkbox and click **Submit**.

Connection Tracking

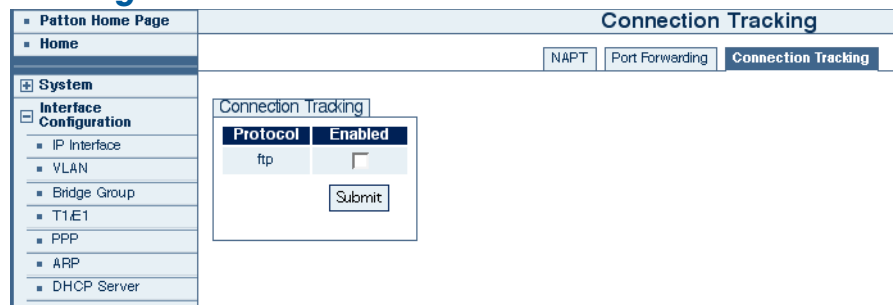


Figure 64. Connection Tracking Configuration

Connection Tracking saves information about network connections on a specific protocol. The Connection Tracking tab lists the protocols available for connection tracking.

To enable a protocol for connection tracking, click the **Enabled** box for the protocol and click **Submit**.

To disable a protocol, uncheck its **Enabled** box, and click **Submit**.

Command Line Interface (CLI)

NAPT

NAPT Configuration Commands

NAT Configuration Mode is entered by typing **configure napt** at the root level.

Table 41. NAT Configuration - CLI Commands

Command	Explanation
configure napt	Enters NAPT configuration mode from the root level.
[no] profile <profile-name>	Creates a new profile named <profile-name> if it doesn't exist, and switches to configuration mode for the profile. no profile will delete the profile. Profiles that are bound to an interface cannot be deleted.
show	Displays a list of existing NAPT profiles.

NAPT Profile Configuration Commands

Table 42. NAT Profile Configuration - CLI Commands

Command	Explanation
[no] rule public <public-ip> [public-ip-end] [local <local-ip> [local-ip-end]]	<p>Adds a rule to the profile. Outgoing packets will be rewritten to use <public-ip> as their source address. If [public-ip-end] is also given, the range of addresses from <public-ip> to [public-ip-end] will be used. By default, all traffic going out via a bound interface is rewritten.</p> <p>The local keyword can be used to limit what traffic is rewritten. If only <local-ip> is provided, only traffic from that ip will be rewritten. If [local-ip-end] is also provided, source addresses must be from <local-ip> to [local-ip-end].</p> <p>Typing [no] in front of the command will delete the first instance of the specified rule from the profile.</p>
[no] rule masquerade [local <local-ip> [local-ip-end]]	<p>Creates a masquerading rule. The outgoing packets will be rewritten to use the public-ip of the interface that the profile is bound to as their source address. This will be dynamically chosen by the system. The local keyword can be used to limit what traffic rewritten. If only local-ip is provided, only traffic from that ip will be rewritten. If local-ip-end is also provided, source addresses must be from local-ip to local-ip-end.</p> <p>Typing [no] in front of the command will delete the first instance of the specified rule from the profile.</p>

Table 42. NAT Profile Configuration - CLI Commands

Command	Explanation
bind <interface>	Binds a profile to an interface. Traffic going out via a bound interface will be processed by the rules, and rewritten if its source address matches a rule's local address range. (Rules without a local address range match all outgoing traffic. If multiple rules would match, the first rule that matches is used.)
show [rules bindings]	Display the rules or bindings of a profile. If not specified, the rules will be shown.

Sample Rules. show rules command:

```

Local IP Start |   Local IP End | Public IP Start |   Public IP End
-----+-----+-----+-----
                |           | 192.168.1.2 |

```

Sample Bindings. show bindings command:

```

Interface
-----
eth0

```

NAPT CLI Examples

Example - Simple NAPT Setup. This example creates a simple NAPT setup. First the profile is created, and a rule added to rewrite all outgoing traffic to have a source address of 1.2.3.4. Finally the profile is bound to eth0. The end result is that all traffic leaving eth0 will be rewritten to have a source address of 1.2.3.4.

```

Trinity# configure napt
Trinity[napt]# profile pf1
Trinity[napt(pf1)]# rule public 1.2.3.4
Trinity[napt(pf1)]# bind eth0

```

Example - Importance of Rule Order. This example illustrates setting restrictions on local address to be translated, and the importance of rule order. The first rule defines a 256 address block in 10-net to use 2.3.4.5 as its outgoing address. The second sets all of 10-net to use 2.3.4.6. However, addresses defined in the first rule will not be handled by the second. Once a rule processes traffic, all processing for that traffic is finished; later rules are ignored.

```

Trinity# configure napt
Trinity[napt]# profile pf2
Trinity[napt(pf2)]# rule public 2.3.4.5 local 10.0.0.0 10.0.0.255
Trinity[napt(pf2)]# rule public 2.3.4.6 local 10.0.0.0 10.255.255.255
Trinity[napt(pf2)]# rule public 2.3.4.6 local 192.168.0.0 192.168.255.255
Trinity[napt(pf2)]# bind eth1

```

If the first two rules had been reversed, such as—


```
Trinity[napt(pf2)]# rule public 2.3.4.6 local 10.0.0.0 10.255.255.255
Trinity[napt(pf2)]# rule public 2.3.4.5 local 10.0.0.0 10.0.0.255
```

The second rule would never be reached because the first would always intercept 10-net traffic.

Example - Masquerading Rule. This example illustrates entering a masquerading rule. The outgoing public IP address for packets within the given range will be dynamically determined by the system based on the IP address of the eth2 interface.

```
Trinity# configure napt
Trinity[napt]# profile pf3
Trinity[napt(pf3)]# rule masquerade local 10.0.0.0 10.0.0.255
Trinity[napt(pf3)]# bind eth2
```

Port Forwarding

Port Forwarding Configuration Commands

Port Forwarding Configuration Mode is entered by entering **configure fwd** at the root level.

Table 43. Port Forwarding Configuration - CLI Commands

Command	Explanation
[no] profile <profile-name>	Creates a new profile named <profile-name> if it doesn't exist, and switches to configuration mode for the profile. no profile <profile-name> will delete the profile. Profiles that are bound to an interface cannot be deleted.
show	Displays a list of the existing Port Forwarding profiles.

Port Forwarding Profile Configuration Commands

Table 44. Port Forwarding Profile Configuration - CLI Commands

Command	Explanation
[no] rule local <local-ip>	<p>These are the four forms that Port Forwarding rules can take.</p> <ul style="list-style-type: none"> In the first form, all traffic entering a bound interface will be redirected to <local-ip>. The second form adds the restriction that incoming traffic must be destined for <public-ip>. The third further restricts it to traffic of the given protocol, which must be a protocol number, tcp, or udp. Finally, the last form, valid only for tcp and udp traffic, matches traffic on public-port and redirects it to local-port (along with rewriting ip addresses).
[no] rule local <local-ip> public <public-ip>	
[no] rule local <local-ip> public <public-ip> protocol <protocol>	
[no] rule local <local-ip> <local-port> public <public-ip> <public-port> protocol <udp tcp>	
	If the command is prefixed with no , the first instance of the specified rule will be deleted from the profile.
bind <interface>	Binds the profile to the specified interface. Incoming traffic that matches one of the profile's rules will have its destination address and port rewritten according to the first rule it matches.
show [rules bindings]	Display the rules or bindings of a profile. If not specified, the rules will be shown.

Sample Rules. show rules command:

```
Public IP | Public Port |      Local IP | Local Port | Protocol
-----+-----+-----+-----+-----
      192.168.1.2 |      80 |   10.10.10.10 |      80 |    tcp
              |      0 |   10.1.1.1 |      0 |
```

Sample Bindings. show bindings command:

```
Interface
-----
      eth0
```

Port Forwarding CLI Examples

Example - Configuring a Port Forwarding Profile. This example creates a DMZ. First, a profile is created and a rule is added to redirect all traffic to 10.1.1.1. Finally, the profile is bound to eth0. The end result is that all traffic coming in eth0 will be redirected to 10.1.1.1.

```
Trinity# configure fwd
Trinity[fwd]# profile pf1
Trinity[fwd(pf1)]# rule local 10.1.1.1
Trinity[fwd(pf1)]# bind eth0
```

Example - Defining Rules for a Port Forwarding Profile. This example adds a few more rules. The first rule redirects web traffic (port 80) destined for 1.2.3.4 to port 8080 on 10.1.1.80. The second rule behaves in the same way as the first rule, except that it effects DNS traffic.

Note Be careful with redirecting udp/53, as this may disable DNS for parts of your network.

The third rule redirects icmp (protocol 1) traffic. The final rule redirects all traffic to 1.2.3.4 that wasn't intercepted by the first three rules to 10.1.1.254.

Note Note the importance of the order of the rules. If the fourth rule were first, it would intercept all the traffic to 1.2.3.4, and the other three rules would never be reached.

```
Trinity# configure fwd
Trinity[fwd]# profile pf2
Trinity[fwd(pf2)]# rule local 10.1.1.80 8080 public 1.2.3.4 80 protocol tcp
Trinity[fwd(pf2)]# rule local 10.1.1.10 53 public 1.2.3.4 53 protocol udp
Trinity[fwd(pf2)]# rule local 10.1.1.1 public 1.2.3.4 protocol 1
Trinity[fwd(pf2)]# rule local 10.1.1.254 public 1.2.3.4
Trinity[fwd(pf2)]# bind eth1
```

Connection Tracking

Connection Tracking Configuration Commands

Connection Tracking Configuration Mode is entered by entering **configure conntrack** at the root level.

Table 45. Connection Tracking Configuration - CLI Commands

Command	Explanation
[no] enable <protocol>	Enables special connection tracking for protocol. Prefixing the command with <i>no</i> disables the connection tracking. Currently the only supported protocol is <i>ftp</i> . Most protocols, such as <i>http</i> for web, or <i>IMAP</i> or <i>POP3</i> for mail, do not require specialized connection tracking.

Connection Tracking CLI Examples

Example - Configuring Connection Tracking.

```
Trinity# configure conntrack
Trinity[conntrack]# enable ftp
```

Chapter 18 **Route Configuration**

Chapter contents

Overview	132
Configuration Overview	132
About Flags	132
Web Management Interface (WMI)	134
Adding a route	134
Deleting a route	134
Command Line Interface (CLI)	135
Adding a route	135
Deleting a route	135
Displaying Routes	136

Overview

This chapter describes how to add and delete static routes to the system and monitor the routing table. The Routing Table displays the routes added by the user and the routes configured through other system components, such as those providing dynamic routing support.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

Configuration Overview

The routes are added to the system by configuring the following:

- Destination IP (required)
- Network mask (required)
- Gateway IP address *or* Interface device name (one is required)
- TOS (optional; default=0)
- Local IP address (optional)
- Route metric (optional)

Note A route can be configured either by specifying an interface device name or a gateway IP address, but not both. When setting default routes, '0.0.0.0' is accepted as a valid destination network address and network mask.

The routes are deleted from the system by selecting them through the Web Management Interface (WMI), or by using the **no route command** in the Command Line Interface (CLI).

About Flags

In both WMI and CLI, the routes are displayed in a table. The table also displays a combination of flags:

- **C** – DHCP – Routes configured via DHCP
- **D** – Dynamic – Routes configured via dynamic routing protocols, e.g. RIP
- **G** – Use Gateway – The route uses the specified gateway
- **H** – Target is a Host – The next hop is a host device
- **R** – User – The route is configured by the user
- **U** – Route is Up – The route is configured and is in the system
- **S** – System – The route is added by the system, e.g. interface routes

To configure routes through the WMI, see the section “[Web Management Interface \(WMI\)](#)” on page 136.

To configure routes through the CLI, see the section “[Command Line Interface \(CLI\)](#)” on page 137.

Web Management Interface (WMI)

To access the Route Configuration page, click on **Routing Configuration > Static Route** from the main menu on the left of the screen.

The screenshot shows the WMI interface with a sidebar menu on the left containing: Home, System, Interface Configuration, Routing Configuration (selected), Traffic Management, and Support. Under Routing Configuration, 'Static Route' is selected. The main content area has a title 'Add Static Route' and a form with the following fields:

- Destination IP: 192.169.0.0
- Netmask: 255.255.0.0
- Interface: eth0 (dropdown menu)
- Gateway: (empty)
- TOS: 0
- Local IP: (empty)
- Metric: 0

Below the form is an 'Add' button. Underneath is a 'Routing Table' section containing a table with the following data:

Destination IP	Netmask	Gateway	Flags	Metric	TOS	Interface	Local IP	Delete
192.168.1.0	255.255.255.0	*	US	0	0	eth0	192.168.1.10	<input type="checkbox"/>
192.168.200.0	255.255.255.0	*	US	0	0	eth0	192.168.200.10	<input type="checkbox"/>
192.169.0.0	255.255.0.0	*	UR	0	0	eth0		<input type="checkbox"/>

At the bottom right of the table is a 'Delete' button.

Figure 65. Route Configuration main page

Gateway	Flags	Metric	TOS	Interface
*	US			eth0
0.1.51	UGR			eth0

Legend for flags:

- C - dhCp
- D - Dynamic
- G - use Gateway
- H - target is a Host
- R - useR
- U - route is Up
- S - System

Figure 66. Route Configuration Flags

Note Hovering the mouse over the Flags column will display an explanation of flags used in the Routing Table.

Adding a route

Users can add a static route by specifying either an interface device or a gateway address.

To add a static route:

1. Enter values for the **Destination IP** and **Netmask**.
2. Choose an option from the **Interface** drop-down menu or enter an IP address for **Gateway**.
3. Enter values for **TOS**, **Local IP**, and **Metric** (optional).
4. Click **Add**.

Deleting a route

The **Routing Table** displays all existing routes in the system. To delete a route, select the Delete checkbox in the Routing Table and click **Delete**. Only the static routes added by the user can be deleted using the Routing Table.

Command Line Interface (CLI)

Table 46. Route Configuration - CLI Commands

Command	Explanation
Trinity# <prefix>	Destination network address prefix; Must be given in dotted-quad form (<A.B.C.D>)
Trinity# netmask <netmask>	Network mask; Can be in dotted-quad form (<A.B.C.D>) or in integer form (<0-32>)
Trinity# interface <name>	Device name
Trinity# gateway <ipaddr>	IP address of the gateway; Must be in dotted-quad form (<A.B.C.D>)
Trinity# metric <value>	Route metric value; Optional parameter between <0-15>
Trinity# source <srcaddr>	IP address of the source; Optional parameter, must be in dotted-quad form (<A.B.C.D>)
Trinity# tos <value>	Route tos value, optional parameter between <0-15> or one of the following pre-set values: mincost (tos=1), reliability (tos=2), throughput (tos=4), lowdelay (tos=8).

Adding a route

The static routes are added using the **route command** under the configure mode of the CLI:

```
Trinity# configure
Trinity [config]# route 192.168.1.0 netmask 255.255.255.0 interface eth0 source 192.168.1.10
Trinity [config]# route default gateway 192.168.1.1 metric 1
Trinity [config]# route 192.168.2.0 netmask 24 interface eth1 metric 3
```

The full command line options for adding a route are given below:

```
Trinity# route <prefix> netmask <netmask> {interface <name> | gateway <ipaddr>} [metric <value>]
[source <srcaddr>] [tos <value>]
Trinity# default {interface <name> | gateway <ipaddr>} [metric <value>] [source <srcaddr>] [tos <value>]
```

Deleting a route

The routes are deleted using the **no route command** as shown in the following example:

```
Trinity# configure
Trinity [config]# no route 192.168.1.0 netmask 255.255.255.0 interface eth0
```

The command line for deleting a route has the following form:

```
Trinity# no route <prefix> netmask <netmask> {interface <name> | gateway <ipaddr>} [metric <value>]
[tos <value>]
Trinity# default {interface <name> | gateway <ipaddr>} [metric <value>] [tos <value>]
```

Displaying Routes

The routes are displayed using the **show route** command either under the configure mode or at the root:

Table 47. Showing Routes - CLI

Command	Explanation
Trinity# show route	Show the list of routes at the root.
Trinity# configure	Enter configuration mode.
Trinity[config]# show route	Show a list of routes in configuration mode.

```
Trinity# show route
System Routing Table
Flags: C - dhCp, D - Dynamic, G - use Gateway, H - target is a host
       R - useR, U - route is Up, S - System
-----+-----+-----+-----+-----+-----+-----+-----+
| Destination | Gateway | Netmask | Flags | Metric | TOS | Interface | Source |
-----+-----+-----+-----+-----+-----+-----+-----+
| 192.168.1.0 | *       | 255.255.255.0 | US | 0 | 0 | eth0 | 192.168.1.10 |
| 192.168.201.0 | 192.168.200.1 | 255.255.255.0 | UGR | 3 | 0 | eth0 | 192.168.200.10 |
| 192.168.200.0 | *       | 255.255.255.0 | US | 0 | 0 | eth0 | 192.168.200.10 |
| 192.169.0.0 | *       | 255.255.0.0 | UR | 0 | 0 | eth0 | 192.169.0.0 |
| 192.168.2.0 | *       | 255.255.255.0 | R | 3 | 0 | eth1 | 192.168.2.0 |
-----+-----+-----+-----+-----+-----+-----+
Trinity# configure
Trinity[config]# show route
System Routing Table
Flags: C - dhCp, D - Dynamic, G - use Gateway, H - target is a host
       R - useR, U - route is Up, S - System
-----+-----+-----+-----+-----+-----+-----+-----+
| Destination | Gateway | Netmask | Flags | Metric | TOS | Interface | Source |
-----+-----+-----+-----+-----+-----+-----+-----+
| 192.168.1.0 | *       | 255.255.255.0 | US | 0 | 0 | eth0 | 192.168.1.10 |
| 192.168.201.0 | 192.168.200.1 | 255.255.255.0 | UGR | 3 | 0 | eth0 | 192.168.200.10 |
| 192.168.200.0 | *       | 255.255.255.0 | US | 0 | 0 | eth0 | 192.168.200.10 |
| 192.169.0.0 | *       | 255.255.0.0 | UR | 0 | 0 | eth0 | 192.169.0.0 |
| 192.168.2.0 | *       | 255.255.255.0 | R | 3 | 0 | eth1 | 192.168.2.0 |
-----+-----+-----+-----+-----+-----+-----+
Trinity[config]# █
```

Figure 67. Command Line Interface "show route" command

Chapter 19 **RIP Configuration**

Chapter contents

Overview	138
Configuration Overview	138
About RIP Features	138
Web Management Interface (WMI)	140
Manage RIP	141
Route Redistribution	141
Networks	141
Neighbors	141
Timers	142
Passive Interfaces	142
Configure Interface	142
Command Line Interface (CLI).....	143
Root Mode	143
Configuration Mode	143
RIP Configuration Mode	144
Interface Configuration Mode	145

Overview

This chapter describes how to configure Routing Information Protocol (RIP).

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

RIP features that can be configured include:

- RIP version (1 or 2) both globally and on a per interface basis
- Passive or active RIP, both globally and on a per interface basis
- Broadcast of RIP routes:
 - To a specific network (e.g. 10.10.0.0/16)
 - To all the networks on a specific interface (e.g. eth0)
 - To a specific neighbor (e.g. 192.168.12.17)
- Whether to redistribute static and/or connected routes
- Timing values such as how often to send updates and how soon routes should time out
- Whether an interface should use split-horizon with or without poisoned-reverse
- Whether an interface should use plain text authentication

Configuration Overview

RIP is suitable only for small and simple networks. Networks with much variation in bandwidth may not produce optimal routes. Also, no two nodes may be more than 15 hops apart or not all nodes will be able to reach one another.

About RIP Features

- **RIP Versions:** Trinity supports both version 1 and version 2 of RIP. Version 1 is limited in how it can support modern classless routing, so version 2 should be used unless it is necessary to inter-operate with old equipment that only supports version 1. The version of RIP used can be set globally and also on a per interface basis. This enables a Trinity device to "bridge" between version 1 and version 2.
- **Enabling RIP:** The simplest RIP configuration involves enabling RIP globally, then enabling RIP on one of more networks and/or interfaces. When RIP is enabled on a network, RIP data is sent and received on all interfaces on that network. When enabled on an interface, RIP data is sent and received on that interface. Additionally, neighbors, which are explicit devices to exchange RIP information with, can be configured.
- **Route Redistribution:** There are a number of ways RIP behavior can be modified. Routes that are redistributed into RIP have the option to be controlled. By default, only routes on the interfaces that have RIP enabled are redistributed (in addition to routes learned via RIP). Optionally, static routes and directly connected routes on non-RIP enabled interfaces can also be distributed into RIP.

- **Passive Interfaces:** Some or all interfaces can be set into passive mode, where they only accept RIP information, but do not broadcast any. Timing information, such as how often RIP information is set out or how quickly a learned route times out, can be set. Plain text authentication can be configured on a per interface basis to restrict what devices may exchange RIP information.
- **Split Horizon:** Split Horizon is a RIP feature that improves the speed at which network changes are propagated. Poisoned-reverse further increases convergence speed, but at the cost of increasing the amount of bandwidth RIP consumes. In general, split horizon should be enabled with poisoned-reverse. However, if bandwidth is limited poisoned-reverse can be turned off. Split horizon should never be disabled except in very unusual circumstances.

To configure RIP through the WMI,
see the section “[Web Management Interface \(WMI\)](#)” on page 142.

To configure RIP through the CLI,
see the section “[Command Line Interface \(CLI\)](#)” on page 145.

Web Management Interface (WMI)

To access the RIP main page, click on **Routing Configuration > RIP** from the menu on the left of the screen.

Manage RIP

RIP Enable:

Default Passive:

Default Version: 2

Route Redistribution

Source	Redistribute	Metric
static	<input type="checkbox"/>	1
connected	<input type="checkbox"/>	1

Networks

Network	Remove
	- Add

Neighbors

Neighbor	Remove
	- Add

Timers

Timer	Time (seconds)
Update	30
Timeout	180
Garbage	120

Passive Interfaces

Interface	Active
	- Add

Configure Interface

Interface:

Configure

Update

Patton Electronics Co.
© 2005-2007
Terms & Conditions

Figure 68. RIP Configuration

The RIP Configuration page has several sections:

- “Manage RIP”
- “Route Redistribution”
- “Networks”
- “Neighbors”
- “Timers”
- “Passive Interfaces”
- “Configure Interface”

Manage RIP

The following are RIP settings:

- **RIP Enable:** Select/deselect the RIP Enable checkbox to enable/disable RIP. If RIP is disabled, all RIP settings will be erased. Then, if RIP is re-enabled, the RIP settings that were previously set will be the default values.
- **Default Passive:** The Default Passive checkbox controls which interfaces are in passive mode by default. If the default mode is changed, all interface assignments will be reset to the default value.
- **Default Version:** The Default Version drop-down menu controls which version of RIP to use by default. The RIP version can also be set on each interface separately.

Route Redistribution

Use the Route Redistribution table to redistribute static and connected routes that are not on an interface running RIP.

- **Redistribute:** Select the checkbox under the Redistribute column to enable or disable distribution of static or connected routes.
- **Metric (optional):** The metric value to use for these routes can be set (valid values 1-15, default=1) in the text box under the metric heading.

Networks

The Networks table determines which networks and interfaces RIP will be enabled on. If a network is given, RIP announcements will be sent and received on all interfaces on that network. Networks are specified in CIDR format (e.g. 1.2.3.4/24). If an interface is given, RIP announcements will be sent and received on that interface. Any number of networks and/or interfaces may be added.

- To add a network entry, type the name in the Network field and click **Update**.
- To remove a network entry, select the checkbox under the Remove heading for the appropriate entry, and click **Update**.

Neighbors

The Neighbors table provides an alternative to the Networks table, which can be used instead of or in conjunction with the Networks table. The Neighbors table shows specific hosts to communicate RIP information with.

- To add a neighbor, enter the IP address of the neighbor into the text field and click **Update**.
- To remove a neighbor, select the checkbox under the Remove heading for the appropriate entry, and click **Update**.

Timers

The Timers table sets three timers that control RIP behavior and route lifetimes. All times entered are in seconds, with a minimum value of 5 seconds.

- **Update timer:** Controls how often RIP announcements are made. The default is 30 seconds.
- **Timeout timer:** Determines how long a route learned via RIP should be regarded as valid without receiving an announcement for it. Once a route has timed out, it will no longer be valid. The Timeout timer defaults to 180 seconds.
- **Garbage timer:** After the Timeout timer has expired, the system will announce the route as invalid. After the garbage period, all information about the route is removed from the system. The garbage timer defaults to 120 seconds.

Passive Interfaces

The Passive Interfaces table will be displayed if the Default Passive box is not checked in the Manage RIP section. The Active Interfaces table will be displayed if the Default Passive box is checked. The checkbox under the Passive (or Active) heading can be used to remove interfaces from the table. All settings are cleared if the Default Passive setting is changed.

- **Passive Interfaces:** Specifies which interfaces should be passive (i.e. receives RIP information but does not announce it).

Configure Interface

To configure an interface per interface RIP options, enter an interface name into the text box and click **Configure**.



The image shows a web form titled "Configure Interface". It contains a label "Interface:" followed by a text input field. Below the input field is a button labeled "Configure".

Figure 69. Configure Interface

Command Line Interface (CLI)

Root Mode

Table 48. RIP Root Mode - CLI Command

Command	Explanation
Trinity# configure	Enter the configuration mode.

Configuration Mode

Table 49. RIP Configuration Mode - CLI Command

Command	Explanation
Trinity[config]# [no] router rip	Enable RIP and enter RIP configuration mode. no router rip disables RIP and deletes all RIP configuration.

RIP Configuration Mode

Table 50. RIP Configuration Mode - CLI Commands

Command	Explanation
Trinity[config-rip]# version {1 2}	Sets the default RIP version to use. This can be overridden on a per interface basis.
Trinity[config-rip]# [no] network {<network> <interface>}	Enables the RIP on the given network or interface. If a network is supplied, all interfaces on that network are enabled. Networks are specified in CIDR format, e.g. 10.10.0.0/16. no network disables RIP on the network or interface.
Trinity[config-rip]# [no] network <ip-address> [netmask <netmask>]	Alternate way to specify a network. If no netmask is provided, assume a /8, /16, or /24 as per the old classful routing.
Trinity[config-rip]# [no] neighbor <ip-address>	Specifies a RIP neighbor for devices that do not understand multicast. no neighbor <ip-address> disables the RIP neighbor.
Trinity[config-rip]# [no] passive-interface {<interface> default}	Sets the given interface to only passively accept RIP announcements, but not send any. no passive-interface sets the behavior to also send RIP announcements. The keyword default sets the default behavior for unspecified interfaces. Note that if the passive default setting is changed, all the other passive settings will be cleared.
Trinity[config-rip]# redistribute {static connected} [metric <0-16>]	Specifies which routes to redistribute through RIP. By default, only routes learned via RIP and routes directly connected to RIP-enabled interfaces are redistributed., and the default metric is one. Static refers to all static routes. Connected redistributes routes directly connected to non-RIP enabled interfaces.
Trinity[config-rip]# no redistribute <static connected>	Stops redistributing static or connected routes.
Trinity[config-rip]# timers basic <update> <timeout> <garbage>	Reconfigures the RIP timers. Defaults are: update = 30 seconds; timeout = 180 seconds; and garbage = 120 seconds. Update determines how often to send out announcements. Timeout determines how long to wait before a route without announcements is considered invalid. Garbage is how long after the timeout before the route is deleted from the routing table. During the garbage period, the route will be announced as invalid.
Trinity[config-rip]# show status	Displays the RIP status.

Table 50. RIP Configuration Mode - CLI Commands

Command	Explanation
Trinity[config-rip]# show routes	Displays routes sent and received by RIP. Similar to <i>show ip protocols</i> at the root mode, but shows only RIP details.

Interface Configuration Mode

Table 51. RIP Interface Configuration Mode - CLI Commands

Command	Explanation
Trinity[iftype-ifname]# ip rip receive version [1] [2]	Sets the RIP version to receive on this interface. The default is to receive both versions, 1 and 2.
Trinity[iftype-ifname]# ip rip send version [1] [2]	Sets the RIP version to send on this interface. The default is to send version 2.
Trinity[iftype-ifname]# [no] ip rip split-horizon	Controls whether to perform split-horizon on this interface.
Trinity[iftype-ifname]# [no] ip rip poison-reverse	Controls whether to use poison-reverse when split-horizon is in effect on this interface. If split-horizon is not in effect, this has no meaning.
Trinity[iftype-ifname]# [no] ip rip authentication mode text	Specifies whether to use plain text authentication on this interface.
Trinity[iftype-ifname]# [no] ip rip authentication string <password>	Specifies the plain text password for this interface

Chapter 20 **Quality of Service (QoS)**

Chapter contents

Overview	147
Configuration Overview	147
About QoS classes	147
Web Management Interface (WMI)	149
QoS Profiles	149
Adding QoS Profiles	149
Deleting QoS Profiles	149
Cloning QoS Profiles	150
QoS Classes	150
Adding QoS Classes	150
Add Custom QoS Class.....	150
Add Pre-Configured QoS Class.....	150
Displaying/Deleting QoS Classes	151
Manage Interfaces	151
Command Line Interface (CLI).....	152
QoS Configuration Commands	152
Show traffic classes of a profile	153
Show QoS configuration	153

Overview

This chapter describes how to create and manage QoS traffic classes. The QoS management component can classify traffic either based on common application types (http, ssh, telnet, etc.) or based on packet fields and markings that were set using the ACL component. This chapter describes the management of QoS classes on a device.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

Note Access Control Lists are discussed in Chapter 21, “Ingress Traffic Management (ACL)” on page 156.

Configuration Overview

QoS classes on a device are managed by *profiles*. A *QoS profile* is a set of traffic QoS classes that can be applied (bound) to an interface on the device. The traffic classes of the profile become effective only when the profile is bound to an interface. A profile can be bound to one or more interfaces at the same time. Several profiles may exist in the system at the same time, but they can be bound to an interface one-at-a-time. New traffic classes can be added to or existing classes can be removed from a profile only when the profile is not bound to any interface.

About QoS classes

A QoS class is configured through a combination of the following parameters:

- **Class Type:** Chosen either from a group of pre-configured application types {default, ftp, http, icmp, imap, pop, smtp, ssh, telnet, voice} or can be based on:
 - TOS field value
 - DSCP (diffServ) field value
 - VLAN Prio field value (applicable only if the interface is a VLAN interface)
 - VLAN ID value (applicable only if the interface is a VLAN interface)
 - Custom packet marking

If a pre-configured application type is selected, the management component creates a queue and adds the required classifiers to send packets matching the application type to this queue. The default type stands for all traffic that is not classified by any of the configured classes.

If a traffic class is created based on the various fields, a packet or a custom marking, then the management component creates a queue and sends all packets with the matching mark or field value to the appropriate queue.

- **Rate Share:** The guaranteed percent share of the traffic class of the total outgoing rate of the interface. However, all traffic classes can grab any excess capacity that is not used by other traffic classes. The Rate Share parameter is given as a percentage of the total capacity (100%) to allow a profile to be bound to interfaces with different capacity.

- **Burst Size:** The amount of buffering available (in KB) for the class if the rate of traffic exceeds the configured rate share.
- **Match Value:** Only available for traffic classes that use various packet fields or packet marking to classify packets. See [table 52](#) for match values.

Table 52. Match values for QoS

Classification	Integer Range/Value Set
TOS	0 - 15
VLAN prio	0 - 7
VLAN id	0 - 4095
DSCP	BE, EF, AFxx, CSx
Packet marking	0 - 65535

When a profile is bound to an interface, a rate shaping value is given for the interface. The rate shaping value in KB/s is the limit on the total outgoing rate of the interface. All traffic classes calculate their service rates based on this rate value and their percent share.

A default traffic class is created automatically with 10% guaranteed rate-share and zero burst allowance as part of every new profile. A default class must exist to forward traffic that does not match any other configured class. As any other traffic class, the default class would grab any excess capacity not used by other classes. The default class can be deleted, or its rate-share can be changed by the user. However, if no default class exists, any unclassified traffic would bypass QoS configuration.

To configure QoS through the WMI, see the section “[Web Management Interface \(WMI\)](#)” on page 151.

To configure QoS through the CLI, see the section “[Command Line Interface \(CLI\)](#)” on page 154.

Web Management Interface (WMI)

To access the QoS main page, click on **Traffic Management > QoS** from the main menu on the left of the screen.

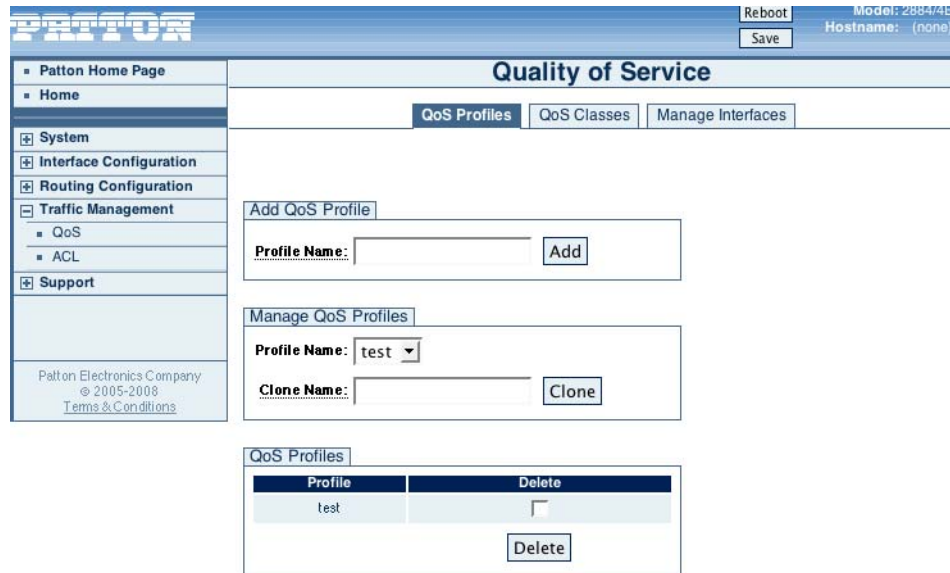


Figure 70. QoS main page

The QoS configuration page is divided into three tabs:

- “QoS Profiles” (See page 151)
- “QoS Classes” (See page 152)
- “Manage Interfaces” (See page 153)

QoS Profiles

The QoS Profiles tab contains the configuration forms for managing QoS profiles (figure 70).

Adding QoS Profiles

To add a QoS profile:

1. Enter a name for the profile in the **Profile Name** field. The profile name can have a maximum length of 16 alpha-numeric characters, and it should be unique among other QoS profiles.
2. Click **Add**.

Deleting QoS Profiles

To delete a QoS profile:

1. Select it from the **Profile Name** drop-down menu.
2. Click **Delete**. A profile can be deleted only if it is not bound to an interface.

Cloning QoS Profiles

To clone an existing profile:

1. Select the profile from the **Profile Name** drop-down menu.
2. Enter a new name for the profile in the **Clone Name** text box.
3. Click **Clone**. A profile can be cloned while it is bound to an interface.

QoS Classes

A profile must not be bound to an interface in order to add or delete a QoS class (figure 71).

The screenshot displays the QoS Classes configuration interface. At the top, there are three tabs: "QoS Profiles", "QoS Classes" (which is active), and "Manage Interfaces". Below the tabs, there are three main sections:

- Add Custom QoS Class:** This section contains a "Profile Name" dropdown menu, a "Class Name" text input field, and a "Classification Type" section with five radio button options: "TOS Field", "Packet MARK", "DSCP field", "VLAN Id", and "VLAN Prio". Below these are "Rate Share (%)" and "Burst Size (KB)" text input fields, and an "Add" button.
- Add Pre-Configured QoS Class:** This section contains a "Profile Name" dropdown menu, a "Class Name" text input field, a "Class Type" dropdown menu, "Rate Share (%)" and "Burst Size (KB)" text input fields, and an "Add" button.
- Display QoS Classes:** This section contains a "Profile Name" dropdown menu, a table with the following columns: "Class Name", "Class Type", "Rate-share (%)", "Burst Size (KB)", and "Delete", and a "Submit" button.

Figure 71. QoS Classes

Adding QoS Classes

Add Custom QoS Class. To add a custom QoS class to an existing profile:

1. Select a profile from the **Profile Name** drop-down menu.
2. Select one **Classification Type** by clicking the corresponding button and filling in the **Value** for your selection. The Classification Type can be based on various packet fields or packet mark values.
3. Fill in the values for **Rate Share (%)** and **Burst Size (KB)**.
4. Click **Add**.

Add Pre-Configured QoS Class. To add a pre-configured QoS class to an existing profile:

1. Select a profile from the **Profile Name** drop-down menu.
2. Choose the application type to match from the **Class Type** drop-down menu.
3. Fill in the values for **Rate Share (%)** and **Burst Size (KB)**.

4. Click Add.

Displaying/Deleting QoS Classes

The Display QoS Classes table shows the existing classes of a profile when a profile is selected from the drop-down menu. To delete a QoS class, select the **Delete** checkbox for that class and click **Submit**. The traffic classes can be displayed at any time but can only be deleted when the profile is not bound to an interface.

Manage Interfaces

The **Manage Interfaces** tab allows users to select an existing profile from a drop-down menu and bind it to a system interface. A rate limit value must be provided in KB/s when binding a profile to an interface. The outgoing rate of the interface is shaped to this rate.

When bound, the **Profile Name** drop-down menu for the interface displays the name of the profile, and the rate-limit field displays the set value.

To unbind a profile from the interface, select the **Bind/Unbind** checkbox of the profile and click **Submit**.

Interface	Profile Name	Rate-limit (KB/s)	Bind/Unbind
eth0	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
eth1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Figure 72. Manage Interfaces

Command Line Interface (CLI)

QoS Configuration Commands

Table 53. QoS - CLI Commands

Command	Explanation
configure [no] qos profile <name>	Create a new QoS profile.
qos profile <name> clone <newname>	Clone a QoS profile.
bind [<dev> all] <rate>	Bind a QoS profile.
[no] bind <dev>	Unbind a QoS profile.
class <classname> TYPE <share> <burst>	Configure a QoS class.
[no] class <classname>	Delete a QoS class.
show	Show QoS profiles.
TYPE := {default ftp http imap icmp pop smtp ssh telnet voice custom {mark tos dscp vlanprio vlanid} <value>}	Available classification types for QoS classes.
configure show qos [<name>]	Configure the display table of QoS classes.

Key for [table 53](#):

- <name> and <newname> – Unique profile name with a maximum length of 16 alpha-numeric characters.
- <rate> – Rate shaping value to be applied on the interface in KB/s.
- <dev> – Interface device name. If all is selected, the profile will be bound to all existing interfaces.
- <classname> – Unique class name in a profile with a maximum length of 16 alpha-numeric characters.
- <share> – Rate share of the traffic class (%).
- <burst> – Burst allowance in KB.
- <value> – Depends on the selected classification type.
If **mark** is selected, the value is an integer between 0-65535.
If **tos** is selected, the value is an integer between 0-15.

Note The order of QoS classes is important. A packet will be classified based on the first class type it matches.

Show traffic classes of a profile

The **show** command under the *qos profile context* and the **show qos <name>** command under the *configure context* allows users to display the existing traffic classes of the given profile (figure 73).

```
Trinity#
Trinity# configure
Trinity[config]# qos profile
<name>                QoS profile name
myprofile              Existing QoS profile name
myprofile2            Existing QoS profile name
Trinity[config]# qos profile my
myprofile
myprofile2
Trinity[config]# qos profile myprofile
Trinity[qos(myprofile)]# show
+-----+-----+-----+-----+
| Class Name | Type | Rate share (%) | Burst (KB) |
+-----+-----+-----+-----+
| default   | default | 10             | 0           |
+-----+-----+-----+-----+
| class1    | ftp    | 20             | 100        |
+-----+-----+-----+-----+
| class2    | http   | 20             | 150        |
+-----+-----+-----+-----+
Trinity[qos(myprofile)]#
```

Figure 73. Show traffic classes of a profile

Show QoS configuration

The **show qos** command (without a profile name) displays the system interfaces, profiles that are bound to them, and rate shaping applied on the interface (figure 74).

```
Trinity# configure show qos
myprofile              Existing QoS profile name
myprofile2            Existing QoS profile name
<cr>
Trinity# configure show qos
QoS Configuration:
+-----+-----+-----+-----+
| Interface | Profile | Rate-limit (KB/s) |
+-----+-----+-----+-----+
| eth0      |         |                    |
+-----+-----+-----+-----+
| eth1      | myprofile | 2000              |
+-----+-----+-----+-----+
| eth2      | myprofile2 | 1000              |
+-----+-----+-----+-----+
| lo        |         |                    |
+-----+-----+-----+-----+
| sit0      |         |                    |
+-----+-----+-----+-----+
Trinity#
```

Figure 74. Show QoS configuration

Chapter 21 **Ingress Traffic Management (ACL)**

Chapter contents

Overview	155
Configuration Overview	155
About packet actions	155
About packet matches	156
Web Management Interface (WMI)	157
Access Control Profiles	158
Adding Access Control Profile	158
Cloning Access Control Profiles	158
Deleting Access Control Profiles	158
Adding Policing Rules	158
Manage Policing Rules	159
Access Control Rules	159
Adding Access Control Rules	159
Displaying and Deleting Access Control Rules	160
Manage Interfaces	160
Command Line Interface (CLI).....	161
ACL Configuration Commands	161
Show access control rules of a profile	162
Show ACL configuration	162

Overview

This chapter describes how to create access control (AC) rules to filter and mark incoming packets. The ACL component is an integral part of the Quality of Service (QoS) suite of the Trinity Software Platform, and the packets marked via the AC rules can be classified into different QoS queues on the egress path.

Note The menu, commands, and features for your model may vary slightly from what is shown in this manual. Some models may not include all of the features mentioned. Refer to the model's *User Manual*, available online at www.patton.com/manuals, to see which features are available.

Note QoS features are discussed in Chapter 20, "Quality of Service (QoS)" on page 148.

Configuration Overview

Access control rules on a device are managed by *profiles*. An *AC profile* is a collection of Access control rules that can be applied (bound) to an interface on the device. The rules of the profile become effective only when the profile is bound to an interface. A profile can be bound to one or more interfaces at the same time. Several profiles may exist in the system at the same time, but they can be bound to an interface individually. New rules can be added or existing rules can be deleted from a profile only when the profile is not bound to any interface. Access control rules consist of match criteria and actions that can be taken on the packets that match the criteria.

About packet actions

The following actions can be taken on a packet:

- **permit:** The packet is permitted to the device without any alteration.
- **deny:** The packet is denied, i.e. it is dropped at the interface before being forwarded to a device.
- **setmark:** The packet is permitted but marked by the system. The **setmark** action is only valid while the packet traverses the device, and the packet remains unaltered when it is sent out of the device. Such marking is used for QoS classification.
- **settos:** The packet is permitted but the TOS bits field is changed to the given **settos** value. The **settos** value remains valid even when the packet leaves the system, and can be used for both QoS classification inside the device and for traffic management across the users' network.
- **setdscp:** The packet is permitted but the DSCP (diffServ) bits field is changed to the given **setdscp** value. The **setdscp** value remains valid even when the packet leaves the system, and can be used both for QoS classification inside the device and for traffic management across the users' network.

About packet matches

The packets can be matched based on the following criteria:

- **Protocol Type:** Match by protocol type of the packets (TCP, UDP, ICMP).
- **Source Address:** Match by the source address of the packets. The match can be based on a single host address, or a range of addresses.
- **Destination Address:** Match by the destination address of the packets. The match can be based on a single host address, or a range of addresses.
- **Source Port:** Match by the source port number of the packets. This match is valid only when used with TCP/UDP protocol match. The match can be based on a single port number or a range of port numbers.
- **Destination Port:** Match by the destination port number of the packets. This match is valid only when used with a TCP/UDP protocol match. The match can be based on a single port number or a range of port numbers.
- **ICMP Message Type:** Match by the icmp message type of the ICMP packets. This match is valid only when used with an ICMP protocol match (echo-request, echo-reply, redirect, destination-unreachable).

In addition to access control rules, a profile can also have a policing rule that is applied to the interface to rate-limit the traffic on the ingress path. The packets are dropped when the rate exceeds the given limit regardless of any access control rules, -- i.e. even when permit rules exist.

To configure the Access Control List through the WMI, see the section "[Web Management Interface \(WMI\)](#)" on page 159.

To configure the Access Control List through the CLI, see the section "[Command Line Interface \(CLI\)](#)" on page 163.

Web Management Interface (WMI)

To access the ACL main page, click on **Traffic Management > ACL** from the main menu on the left of the screen.

Figure 75. Ingress Traffic Management main page

The ACL configuration is accessed via the Ingress Traffic Management page. The configuration page is divided into three tabs:

- “Access Control Profiles” (See page 160)
- “Access Control Rules” (See page 161)
- “Manage Interfaces” (See page 162)

Access Control Profiles

The screenshot displays the 'Access Control Profiles' management interface. It is divided into several sections:

- Add Access Control Profile:** A form with a 'Profile name:' text input field and an 'Add' button.
- Manage Access Control Profiles:** A form with a 'Profile Name:' dropdown menu, a 'Clone Name:' text input field, and a 'Clone' button.
- AC Profiles:** A table with columns for 'Profile' and 'Delete'. A 'Delete' button is located below the table.
- Add Policing Rule:** A form with a 'Profile Name:' dropdown menu, a 'Rate (KB/s):' text input field, a 'Burst (KB):' text input field, and an 'Add' button.
- Manage Policing Rules:** A table with columns for 'Profile Name', 'Rate (KB/s)', 'Burst (KB)', and 'Delete'. A 'Submit' button is located below the table.

Figure 76. Managing Access Control Profiles

Adding Access Control Profile

To add a new ACL profile:

1. Enter a name for the profile in the **Profile Name** field. The profile name can have a maximum length of 16 alpha-numeric characters, and it should be unique.
2. Click **Add**.

Cloning Access Control Profiles

To clone an ACL profile:

1. Select the profile from the **Profile Name** drop-down menu.
2. Enter a new name for the profile in the **Clone Name** text box.
3. Click **Clone**. A profile can be cloned while it is bound to an interface.

Deleting Access Control Profiles

To delete an ACL profile:

1. Click **Delete** next to the profile in the **AC Profiles** table.

Adding Policing Rules

To add a policing rule:

1. Select the profile from the **Profile Name** drop-down menu.
2. Enter the rate and burst values.

- Click **Add**. It accepts a rate-limit value in KB/s and a burst allowance in KB for temporarily buffering the traffic that is in excess of the given limit.

Manage Policing Rules

The **Manage Policing Rules** table displays existing policing rules on profiles. To delete a policing rule, select it using the Delete checkbox, then click **Submit**. Policing operations (Add/Delete) are only possible when the profile is not bound to an interface.

Access Control Rules

Access Control Profiles
Access Control Rules
Manage Interfaces

Add Access Control Rule

Profile Name:

Rule Name:

ACL Action Type:

Deny:

Permit:

Set TOS field:

Set Packet MARK:

Set DSCP field:

ACL Match Rule:

Protocol:

Set ICMP Type:

Source Host Address: any

Destination Host Address: any

From:

To:

Src Port:

Dst Port:

Display Rules

Profile Name:

Name	Type	Protocol	Source Address	Port	Destination Address	Port	Delete

Figure 77. Managing ACL rules

Adding Access Control Rules

To add a new ACL rule:

- Select a profile name from the **Profile Name** drop-down menu.
- Enter a **Rule Name**. It must be unique within a given profile, and can have a maximum length of 16 alphanumeric characters.
- Select an **ACL Action Type** from **one of the following** options:
 - deny, permit, set MARK, set TOS, or set DSCP.
 - **Deny:** The packet is denied, i.e. it is dropped at the interface before being forwarded to device.
 - **Permit:** The packet is permitted to the device without any alteration.

- **Set TOS value:** Can be set to any integer value between 0-15 corresponding to TOS bits.
 - **Set MARK value:** Can be set to any integer value between 0-65535.
 - **SET DSCP value:** Can be chosen from a drop-down menu of available values.
4. Select a protocol from the **Protocol Type** drop-down menu (optional).
 5. Select an option from the **Source Host Address** drop-down menu:
 - If **host** is selected, a source IP address must be entered in the From field.
 - If **range** is selected, IP addresses must be entered in the From and To fields representing the source address range.
 - If **all** is selected, all valid source addresses are matched; no entry is required in either of the From and To fields.
 - If **any** is selected, the rule ignores source addresses; no entry is required in either of the From and To fields.
 6. Select an option from the **Destination Host Address** drop-down menu. This field works similar to the source address matching.
 7. Enter a single port number or a port number range in the **Src Port** field (optional). The source port can be entered in the form <A> or <A:B>. This field can be left blank if no port number matching is required. TCP or UDP protocol *must* be selected when entering **Src Port**.
 8. Enter a port number or range in the **Destination Port** field. This field works similar to source port matching.
 9. If ICMP is selected as the protocol, select an option from the **Set ICMP Type** drop-down menu. This field can be left blank if all ICMP packets will be matched.
10. Click **Add**.

Displaying and Deleting Access Control Rules

The **Display Rules** table shows the existing rules of a profile when a profile is selected from the **Profile Name** drop-down menu. To delete a rule, select the **Delete** checkbox for that rule and click **Submit**. The rules can be displayed at any time but can only be deleted when the profile is not bound to an interface.

Manage Interfaces

The **Manage Interfaces** tab allows users to select an existing profile from the **Profile Name** drop-down menu and bind it to a system interface.

When a profile is bound to an interface, the **Profile Name** column displays the name of the profile.

To unbind a profile from the interface, select the **Bind/Unbind** checkbox of the profile and click **Submit**.

Apply Access Control Profiles		
Interface	Profile Name	Bind/Unbind
eth0	<input type="text"/>	<input type="checkbox"/>
eth1	<input type="text"/>	<input type="checkbox"/>

Figure 78. Managing interfaces

Command Line Interface (CLI)

ACL Configuration Commands

Table 54. ACL - CLI Commands

Command	Explanation
Trinity# configure [no] acl profile <name>	Create a new ACL profile.
Trinity# acl profile <name> clone <newname>	Clone an ACL profile.
 police <rate> <burst>	Add a policing rule.
 [no] police	Add/delete a policing rule.
 [no] bind {<dev> all}	Bind an interface.
rule <rulename> {deny permit setmark <markvalue> settos <tosvalue> setdscp <dscpvalue> } OPTIONS	Configure ACL rule.
 [no] rule <rulename>	Create ACL rule.
 show	Show ACL profiles.
OPTIONS: {<A.B.C.D-W.X.Y.Z> all any} [icmp [<type>] {tcp udp} [sport <svalue> dport	Available protocols for ACL rules.
Trinity# configure show acl [<name>]	Configure the display table of ACL rules.

Key for [table 54](#):

- <name> and <newname> – Unique profile name with a maximum length of 16 alpha-numeric characters.
- <rate> – Rate shaping value to be applied on the interface in KB/s.
- <burst> – Burst allowance in KB.
- <dev> – Interface device name. If all is selected, the profile will be bound to all existing interfaces.
- <rulename> – Unique rule name in a profile with a maximum length of 16 alpha-numeric characters.
- <markvalue> – Integer value between 0-65535.
- <tosvalue> – Integer value between 0-15 corresponding to TOS bits.
- <dscpvalue> – DSCP class value {BE, EF, AFxx, and CSx}.
- <A.B.C.D-W.X.Y.Z> – Source or destination address range. A single IP address can be given for both source and destination if a range match is not required.
- <svalue> – Source port value, given as a single port number (0-65535) N or a range N:M.
- <dvalue> – Destination port value, given as a single port number (0-65535) N or a range N:M.
- <type> – ICMP message type {echo-request, echo-reply, redirect, destination-unreachable}.

Note The order of ACL rules is important. A packet will be filtered or marked based on the first rule type it matches.

Show access control rules of a profile

The **show** command under the *acl profile context* and the **show acl <name>** command under the *configure context* allows users to display the access control rules of a given profile (figure 79).

```
Trinity#
Trinity# configure
Trinity[config]# show acl
myprofile          Existing ACL profile name
<cr>
Trinity[config]# show acl myprofile
+-----+-----+-----+-----+-----+
| Name      | Type  | Protocol | Src Range | Dst Range |
+-----+-----+-----+-----+-----+
| myrule1   | deny  | tcp      | 192.168.200.13 | 10.11.2.35 |
|           |       | sport 22:80 | to         | to         |
|           |       | dport 22:80 | 192.168.200.50 | 10.11.2.50 |
+-----+-----+-----+-----+-----+
| myrule2   | setmark | icmp     | all       | all       |
|           | 2      | echo-request |           |           |
+-----+-----+-----+-----+-----+
Trinity[config]#
```

Figure 79. Show access control rules of a profile

Show ACL configuration

The **show acl** command (without a profile name) displays the system interfaces, profiles that are bound to them and, whether or not any policing exists on the interfaces (figure 80).

```
Trinity[config]#
Trinity[config]# show acl
acl                Shows ACL configuration
Trinity[config]# show acl
ACL Configuration:
+-----+-----+-----+-----+-----+
| Interface | Profile | Policed | Rate (KB/s) | Burst (KB) |
+-----+-----+-----+-----+-----+
| eth0      |         |         |              |             |
+-----+-----+-----+-----+-----+
| eth1      | myprofile1 | No     |              |             |
+-----+-----+-----+-----+-----+
| eth2      | myprofile2 | Yes    | 2000         | 150         |
+-----+-----+-----+-----+-----+
| lo        |         |         |              |             |
+-----+-----+-----+-----+-----+
| sit0      |         |         |              |             |
+-----+-----+-----+-----+-----+
Trinity[config]#
```

Figure 80. Show ACL configuration

Chapter 22 **Contacting Patton for assistance**

Chapter contents

- Introduction.....164
- Contact information.....164
- Warranty Service and Returned Merchandise Authorizations (RMAs).....164
 - Warranty coverage164
 - Out-of-warranty service164
 - Returns for credit164
 - Return for credit policy165
 - RMA numbers165
 - Shipping instructions165

Introduction

This chapter contains the following information:

- “Contact information”—describes how to contact PATTON technical support for assistance.
- “Warranty Service and Returned Merchandise Authorizations (RMAs)” —contains information about the RAS warranty and obtaining a return merchandise authorization (RMA).

Contact information

Patton Electronics offers a wide array of free technical services. If you have questions about any of our other products we recommend you begin your search for answers by using our technical knowledge base. Here, we have gathered together many of the more commonly asked questions and compiled them into a searchable database to help you quickly solve your problems.

- Online support—available at www.patton.com.
- E-mail support—e-mail sent to support@patton.com will be answered within 1 business day
- Telephone support—standard telephone support is available Monday through Friday, from 8:00 A.M. to 5:00 P.M. EST (8:00 to 17:00 UTC-5), Monday through Friday by calling +1 (301) 975-1007

Warranty Service and Returned Merchandise Authorizations (RMAs)

Patton Electronics is an ISO-9001 certified manufacturer and our products are carefully tested before shipment. All of our products are backed by a comprehensive warranty program.

Note If you purchased your equipment from a Patton Electronics reseller, ask your reseller how you should proceed with warranty service. It is often more convenient for you to work with your local reseller to obtain a replacement. Patton services our products no matter how you acquired them.

Warranty coverage

Our products are under warranty to be free from defects, and we will, at our option, repair or replace the product should it fail within one year from the first date of shipment. Our warranty is limited to defects in workmanship or materials, and does not cover customer damage, lightning or power surge damage, abuse, or unauthorized modification.

Out-of-warranty service

Patton services what we sell, no matter how you acquired it, including malfunctioning products that are no longer under warranty. Our products have a flat fee for repairs. Units damaged by lightning or other catastrophes may require replacement.

Returns for credit

Customer satisfaction is important to us, therefore any product may be returned with authorization within 30 days from the shipment date for a full credit of the purchase price. If you have ordered the wrong equipment or you are dissatisfied in any way, please contact us to request an RMA number to accept your return. Patton is not responsible for equipment returned without a Return Authorization.

Return for credit policy

- Less than 30 days: No Charge. Your credit will be issued upon receipt and inspection of the equipment.
- 30 to 60 days: We will add a 20% restocking charge (crediting your account with 80% of the purchase price).
- Over 60 days: Products will be accepted for repairs only.

RMA numbers

RMA numbers are required for all product returns. You can obtain an RMA by doing one of the following:

- Completing a request on the RMA Request page in the *Support* section at www.patton.com
- By calling +1 (301) 975-1000 and speaking to a Technical Support Engineer
- By sending an e-mail to returns@patton.com

All returned units must have the RMA number clearly visible on the outside of the shipping container. Please use the original packing material that the device came in or pack the unit securely to avoid damage during shipping.

Shipping instructions

The RMA number should be clearly visible on the address label. Our shipping address is as follows:

Patton Electronics Company

RMA#: xxxx

7622 Rickenbacker Dr.

Gaithersburg, MD 20879-4773 USA

Patton will ship the equipment back to you in the same manner you ship it to us. Patton will pay the return shipping costs.