HP TippingPoint

Command Line Interface Reference

TOS Version 3.6

Abstract

This document describes the command line interface (CLI) for the TippingPoint Operating System, the use of the CLI for device setup, and the commands that can be used to configure and manage the device.

5998-1404

Part number: 5998-1404
Edition: October 2013

Legal and notice information

Printed in the US.

Command Line Interface Reference TOS Version 3.6

Contents

About This Guide

Explains intended audience, where related information is located, and how to obtain customer support.

Overview

Welcome to the Command Line Interface Reference.

This section includes the following items:

Target Audience

The intended audience includes technicians and maintenance personnel responsible for installing, configuring, and maintaining TippingPoint security systems and associated devices. Users should be familiar with networking concepts and the following standards and protocols:

- TCP/IP
- UDP
- ICMP
- Ethernet
- Simple Network Time Protocol (SNTP)
- Simple Mail Transport Protocol (SNMP)
- Simple Network management Protocol (SNMP)

Conventions

The TippingPoint documentation uses the following conventions for structuring information.

Headings

Each main section starts with a brief description of the information you can find in that section, which correlates with the major headings in that section. Each major heading corresponds to a task or concept that is important for you to understand. Headings are of a different size and type to make them easy to skim, whether you are viewing an online or print copy of this document.

Typeface

This document uses the following typeface conventions:

Bold — Used for the names of screen elements like buttons, drop-down lists, or fields. For example, when you are done with a dialog, you would click the **OK** button.

`Code` — Used for text a user must type to use the product.

Italic — Used for book titles, variables, and important terms.

Hyperlink — Used for Website and cross reference links.

Cross References

When a topic is covered in depth elsewhere in this document, or in another document in this series, a cross reference to the other information is provided as follows:

Messages

Messages are emphasized by font, format, and icons. There are four types of messages in this document:

- **Warnings** — Indicate how to avoid physical injury to people or equipment. For people, injury includes anything from temporary conditions, such as pain, to irreversible conditions such as death. For equipment, injury includes anything requiring repair. Warnings indicate what you should or should not do and the consequences of not heeding the warning.
- **Cautions** — Indicate how to avoid a serious loss that stops short of physical damage, such as the loss of data, time, or security. Cautions indicate what you should or should not do to avoid such losses and the consequences of not heeding the caution.
- **Notes** —Notes indicate information that might not be obvious or that does not relate directly to the current topic, but that may affect relevant behavior.
- **Tips** — Tips are suggestions about how to perform a task more easily or more efficiently.

WARNING! Warning notes alert you to potential danger of bodily harm or other potential harmful consequences.

CAUTION: Caution notes provide information to help minimize risk, for example, when a failure to follow directions could result in damage to equipment or loss of data.

NOTE: Notes provide additional information to explain a concept or complete a task. Notes of specific importance in clarifying information or instructions are denoted as such.

IMPORTANT: Another type of note that provides clarifying information or specific instructions.

TIP: Tips provide helpful hints and shortcuts, such as suggestions about how you can perform a task more easily or more efficiently.

Product Documentation

TippingPoint Systems have a full set of documentation. For the most current documentation, check the Threat Management Center (TMC) website at https://tmc.tippingpoint.com.

Customer Support

TippingPoint is committed to providing quality customer support to all of its customers. Each customer is provided with a customized support agreement that provides detailed customer and support contact information.

For the most efficient resolution of your problem, take a moment to gather some basic information from your records and from your system before contacting customer support, including your customer number.

Have the following information available:

Information	Location
Your customer number	You can find this number on your Customer Support Agreement and on the shipping invoice that came with your TippingPoint system.
Your device serial number	You can find this information on the bottom of the server chassis. Also, from the TippingPoint CLI, you can run the `show version` command.
Your device version number	From the TippingPoint CLI, you can run the `show version` command.

Contact Information

For additional information or assistance, contact the HP TippingPoint Technical Assistance Center (TAC):

Telephone

North America: +1 866 681 8324
International: +1 512 681 8324

For a list of international toll-free contact numbers, consult the following web page:

https://tmc.tippingpoint.com/TMC/Content/support/Support_Contacts

Online Support Request

1. Log on to the TippingPoint Threat Management Center (TMC) with your HP Passport credentials.

NOTE: If you don't have HP Passport (HPP) credentials, access the TMC and on the Login page, select the **New User Registration** option to register for login credentials. If you are an existing registered TMC user and you have not updated your TMC account to an HPP account, you must log on using your email address registered on the TMC and reset your password. To reset your password, access the TMC and on the Login page, select **Forgot Password** and set a new password.

---

2. In the menu bar click **Support > Support Request**.
3. Complete the information required in the Support Request form and submit the form.

E-mail

tippingpoint.support@hp.com

1 System Overview

Overview

The TippingPoint™ system is a high-speed, comprehensive security system that includes the Intrusion Prevention System (IPS), ™ Local Security Manager (LSM), Digital Vaccine™, the Security Management System Appliance™, and the Core Controller.

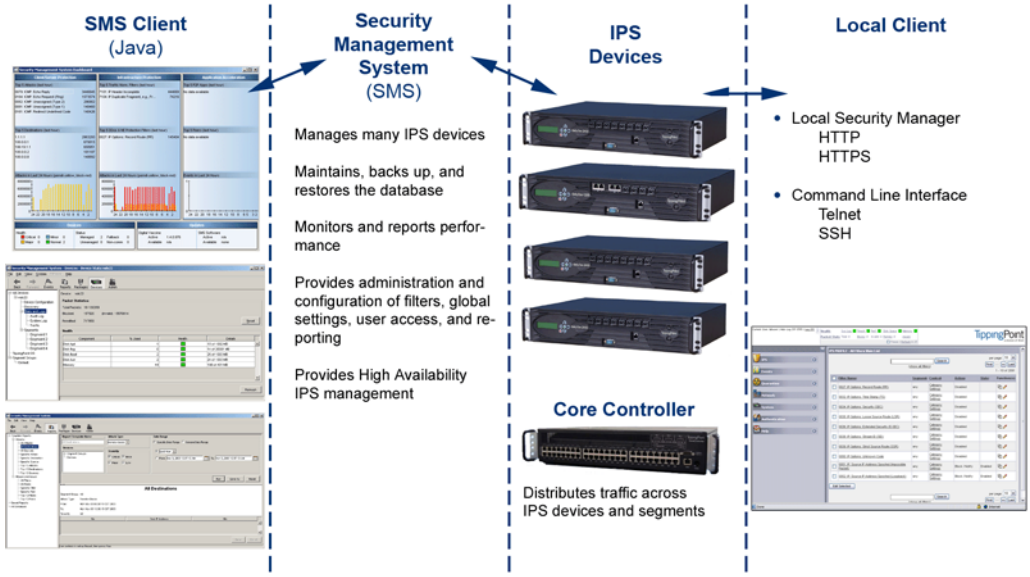
Enterprise security schemes once consisted of a conglomeration of disparate, static devices from multiple vendors. Today, TippingPoint's security system provides the advantages of a single, integrated, highly adaptive security system that includes powerful hardware and an intuitive management interface.

This section includes the following topics:

TippingPoint Architecture

The TippingPoint System uses a flexible architecture that consists of a Java-based SMS Client, SMS Management Server, IPS device(s), and Local Clients including the Local Security Manager (LSM) and Command Line Interface (CLI). The system may also include the Core Controller, a hardware appliance that balances traffic loads for one or more IPSes. The following diagram provides an overview of the architecture:

Figure 1-1 TippingPoint Architecture



Security Management System (SMS)

The SMS core components include:

- **SMS Secure Server** —hardware appliance for managing multiple devices
- SMS Home Page — web-based interface with links to current Client software, documentation, and the Threat Management Center
- **SMS Management Client** — Java-based application for Windows or Linux workstations used to manage your TippingPoint system
- Graphical User Interface (GUI)
- Dashboard
- Command Line Interface (CLI)

The SMS communicates with managed devices that are installed in your network.

The SMS architecture also includes the following components:

- **Threat Management Center** (TMC) — Centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation.
- **Digital Vaccine** (DV) — Update service that includes up-to-date filter packages for protecting your network.
- **Managed Devices** — TippingPoint IPS or Core Controller devices that are installed in your network.

SMS Server

The SMS Server is an enterprise-class management platform that provides centralized administration, configuration, monitoring and reporting for well over a hundred TippingPoint IPS devices. The SMS provides the following functionality:

- **Enterprise-wide device status and behavior monitoring** — Stores logs and device status information, manages updates, and monitors filter, device, software, and network status.
- **IPS networking and configuration** — Stores device information and configures devices according to the settings that are modified, imported, or distributed by clients. These settings affect the flow and detection of traffic according to device, segment, or segment group.
- **Filter customization** — Stores filter customizations in profiles as maintained by the SMS client. These settings are distributed and imported to devices, which can be reviewed and modified by local clients. If a device is managed by the SMS Server, the local clients cannot modify settings.
- **Filter and software distribution** — Monitors and maintains the distribution and import of filters, Digital Vaccine packages, and software for the TippingPoint Operating System and SMS Client. The SMS client and Central Management Server can distribute these packages according to segment group settings. The Central Management Server maintains a link to the Threat Management Center (TMC) for downloading and installing package updates.

SMS Client

The TippingPoint Security Management System (SMS) client provides services and functions to monitor, manage, and configure the entire TippingPoint system. This client is a Java-based application installed and accessed on a computer running the appropriate operating system. Each user receives a specific user level with enhanced security measures to protect access and configuration of the system.

You can monitor the entire TippingPoint system through the SMS client on a computer with the following requirements:

- One of the following operating systems:
  - Windows 98, 2nd edition
  - Windows NT, Service Pack 5 or later
  - Windows 2000, Service Pack 3 or later
  - Windows XP
  - Windows 7

    - Apple
    - Red Hat Linux
- One of the following browsers:
    - Microsoft Internet Explorer, version 6.0 or higher
    - Firefox
    - Safari

The SMS features a policy-based operational model for scalable and uniform enterprise management. It enables behavior and performance analysis with trending reports, correlation and real-time graphs. Reporting includes all, specific, and top attacks and their sources and destinations, as well as all, specific, and top peers and filters for misuse and abuse (peer-to-peer piracy) attacks. You can create, save, and schedule reports using report templates. All reports are run against system and audit logs stored for each device managed by the system. These logs detail triggered filters. You can modify, update, and control distribution of these filters according to segment groups for refined intrusion prevention.

The SMS dashboard provides at-a-glance monitors with launch capabilities into the targeted management applications that provide global command and control of TippingPoint. Included in the SMS dashboard display are the following items:

- Entries for the top five filters triggered over the past hour in various categories
- A graph of triggered filters over the past 24 hours
- The health status of devices
- Update versions for software of the system

Through the Dashboard, you gain an overview of the current performance of your system, including notifications of updates and possible issues with devices monitored by the SMS.

Intrusion Prevention System Devices

Intrusion Prevention System (IPS) devices protect your network with the Threat Suppression Engine (TSE) by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings maintained on each device by a client.

Each device provides intrusion prevention for your network according to the number of network connections and hardware capabilities. IPS devices also have built-in intrinsic high-availability features, guaranteeing that the network keeps running in the event of system failure.

TippingPoint Intrusion Prevention Systems are optimized to provide high resiliency, high-availability security for remote branch offices, small-to-medium and large enterprises and collocation facilities. Each IPS can protect network segments from both external and internal attacks.

Multiple TippingPoint devices can be deployed to extend this unsurpassed protection to hundreds of enterprise zones. You can monitor and manage the devices by using the local client available on each device, or by using the SMS client to monitor and manage well over a hundred devices. The TippingPoint N-Platform and NX-Platform devices support IPv6, tunneling (including GRE and multi-layer tunnels), and inspection bypass rules for trusted traffic.

IPS Local Clients

The TippingPoint System provides various points of interaction, management, and configuration of the IPS. The clients include graphical user interfaces (GUI) and command line interfaces (CLI). These clients include the following:

- **Local Security Manager (LSM)** — Web-based GUI for managing one IPS device. The LSM provides HTTP and HTTPS (secure management) access. This access requires access from a supported web browser (Internet Explorer, Mozilla Firefox, and Netscape). Using the LSM, you have a graphical display for reviewing, searching, and modifying settings. The GUI interface also provides reports to monitor the device traffic, triggered filters, and packet statistics.
- **Command Line Interface (CLI)** — Command line interface for reviewing and modifying settings on the device. The CLI is accessible through Telnet and SSH (secure access).
- **LCD Panel** — Several IPS TippingPoint devices provide an LCD panel to view, configure, and modify some device settings.

Core Controller

The TippingPoint Core Controller is a hardware-based device that enables inspection of up to 20Gbps of traffic by sending the traffic to as many as 24 IPS device segments. The Core Controller can control traffic across its three 10GbE network segment pairs and across multiple TippingPoint E-Series IPS devices. IPS devices are connected by 1GbE uplinks, and each packet that is received on a 10GbE Core Controller interface passes through a load balancer that then determines the IPS connection to use for transmitting the packet.

The Core Controller provides:

- 10GbE bidirectional traffic inspection and policy enforcement
- High Availability with an optional Smart ZPHA module
- Central management through the SMS

NOTE: The Core Controller can be used with the 2400E and 5000E IPS devices, and with all N-Platform and NX-Platform devices.

High Availability

TippingPoint devices are designed to guarantee that your network traffic always flows at wire speeds in the event of internal device failure. The TippingPoint System provides Network High Availability settings for Intrinsic Network HA (INHA) and Transparent Network HA (TNHA). These options enact manually or automatically, according to settings you enter using the clients (LSM and SMS) or LCD panel for IPS devices. Zero-Power High Availability (ZPHA) is available for the IPS as an external modular device, as optional bypass I/O modules on NX-Platform devices, and for the Core Controller as an optional Smart ZPHA module.

The IPS uses INHA for individual device deployment and TNHA for devices deployed in redundant configurations in which one device takes over for another in the event of system failure. With INHA, a failure puts the device into Layer-2 Fallback mode and permits or blocks traffic on each segment. In TNHA, multiple IPS devices are synchronized so that when one device experiences a system failure, traffic is routed to the other device with no interruption in intrusion prevention services.

SMS high availability provides continuous administration through an active-passive SMS system configuration. A passive SMS is configured, synchronized with the active system, and waits in standby mode and monitors the health of the active system. If the health or communications check fails, the passive SMS will be activated.

The ZPHA modular device can be attached to an IPS to route traffic in the event of power loss. Smart ZPHA modules, which are wired into the device, and bypass I/O modules, which are installed directly into NX-Platform devices, perform the same function.

Threat Suppression Engine

The Threat Suppression Engine (TSE) is a line-speed hardware engine that contains all the functions needed for Intrusion Prevention, including:

- IP defragmentation
- TCP flow reassembly
- Statistical analysis
- Traffic shaping
- Flow blocking
- Flow state tracking
- Application-layer parsing of over 170 network protocols

The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. As each new packet of the traffic flow arrives, the engine re-evaluates the traffic for malicious content. The instant the engine detects malicious traffic, it blocks all current and all subsequent packets pertaining to the traffic flow. The blocking of the traffic and packets ensures that the attack never reaches its destination.

The combination of high-speed network processors and custom chips provides the basis for IPS technology. These highly specialized traffic classification engines enable the IPS to filter with extreme accuracy at gigabit speeds and microsecond latencies. Unlike software-based systems whose performance is affected by the number of filters installed, the highly-scalable capacity of the hardware engine allows thousands of filters to run simultaneously with no impact on performance or accuracy.

Threat Management Center

The Threat Management Center (TMC) is a centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation.

The TMC collects threat information and creates Digital Vaccine packages that are made available on the TMC web site. The packages include filters that block malicious traffic and attacks on your network. The filters provide the following protections:

- **Application Protection** — Defend against known and unknown exploits that target applications and operating systems:
  - Attack Protection filters — Detect and block traffic known to be malicious, suspicious, and to have known security implications. These filters include the following: Vulnerabilities and Exploits filters.
  - Security Policy filters — Detect and block traffic that might or might not be malicious. This traffic might be different in its format or content from standard business practice, aimed at specific software or operating systems, or contrary to your company's security policies.
  - Reconnaissance filters — Detect and block scans, sweeps, and probes for vulnerabilities and information about your network. These filters include the following: Probes and Sweeps/Scans filters.
  - Informational filters — Detect and block classic Intrusion Detection System (IDS) infiltration.
- **Infrastructure Protection** — Protect network bandwidth and network infrastructure elements, such as routers and firewalls, from attack using a combination of filter types:
  - Advanced DDoS filters — Available on the 2400E and 5000E. Detect and block denial of service and flood requests, such as SYN Requests, that can overwhelm a system.
  - Network Equipment Protection filters — Protect networked equipment from attacks.
  - Traffic Normalization filters — Detect and block abnormal or malicious traffic.

- **Performance Protection** — Allow key applications to have a prioritized bandwidth-access setting that ensures mission-critical applications have adequate performance during times of high congestion:
  - Misuse and Abuse filters — Protect the resources and usage of file sharing across networks and personal computers. These filters protect peer-to-peer services.
  - Traffic Management filters — Protect the network by shielding against IP addresses or permitting only a set of IP addresses.

2 Initial Configuration

Describes the procedures for initial TippingPoint IPS configuration.

Overview

The TippingPoint IPS Out of Box Experience (OBE) setup wizard provides a convenient method for entering configuration data when installing, moving, or reconfiguring a TippingPoint IPS device. The wizard runs automatically on the console that is connected to the device via the console port or on the LCD keypad. You can also initialize the setup wizard at any time by entering the `setup` command in the CLI.

This chapter is a guide for the CLI and LCD keypad versions of the OBE wizards and includes the following topics:

CLI Setup

Before you begin, ensure that a console is connected to the TippingPoint IPS device via the console port, and that the console is powered on and ready. When you turn on the IPS, you will see several status messages before the OBE setup wizard initializes.

When the OBE setup wizard runs, the following screen appears:

```
Welcome to the TippingPoint Technologies Initial Setup wizard.
Press any key to begin the Initial Setup Wizard or use LCD panel.
```

Press any key to begin the OBE setup wizard. The following message appears:

```
You will be presented with some questions along with default values in brackets[].
Please update any empty fields or modify them to match your requirements. You may
press the ENTER key to keep the current default value. After each group of
entries, you will have a chance to confirm your settings, so don't worry if you
make a mistake.
```

Continue to the following section for instructions on account security.

Account Security Level

The Security Level dialog sets the security level that restricts user names and passwords. The default security level is Level 2, but you have the option to select one of three available levels:

```
There are three security levels for specifying user names and passwords:
 Level 0: User names and passwords are unrestricted.
 Level 1: Names must be at least 6 characters long; passwords
 at least 8.
 Level 2: In addition to level 1 restrictions, passwords must
 contain:
  - at least 2 alpha characters
  - at least 1 numeric character
  - at least 1 non-alphanumeric character
Please specify a security level to be used for initial super-user name and
password creation. As super-user, you can modify the security level later on via
Command Line Interface (CLI) or Local Security Manager (LSM).
Security level [2]:
```

NOTE: For maximum security, TippingPoint recommends setting the account security level to 2.

Super-User Data

The Super-User Data dialog sets the super-user login name and password. The login name and password cannot contain spaces and must meet the restrictions of the security level that you set in the Security Level dialog. The following tables list examples of valid login names and passwords.

Table 2-1 Login and Password Name Examples

Security Level	Valid Login Names	Valid Passwords
Level 0	`fredj`	`mypass`
Level 1	`fjohnson`	`mypassword`

Level 2	`fjohnson`
	`fredj123`
	`fredj-123`
	`fredj-*123`
		`my-pa55word`
		`my-b1rthday`
		`myd*g'snam3`

In this example, the password is presented in italics. In the actual dialog, the password would not be visible.

```
Please enter a user name that we will use to create your super-user account.
Spaces are not allowed.
Name: superuser
Do you wish to accept [superuser] <Y,[N]>:Y
Please enter your super-user account password: root--00
Verify password: root--00
Saving information...Done
Your super-user account has been created.
You may continue initial configuration by logging into your device.
After logging in, you will be asked for additional information.
```

After logging in at the prompt, you can continue with the OBE setup wizard.

Host Management Port Options

The Host Management port is the Ethernet port located on the host processor module. Use the IP address of the Host Management port to connect to the TippingPoint IPS when you use the Command Line Interface and the LSM.

In this example, the host IP address is `10.252.0.71`, the host name is `device71`, and the location is `Lab`. The network mask is the default setting.

```
The host management port is used to configure and monitor this device via a
network connection (e.g., a web browser).
Enter Management IPv4 Address [none]: 10.252.0.71
Enter Network IPv4 Mask [255.255.255.0]:
Enable IPv6 [No]: y
Enable IPv6 Address Autoconfig [No]: y
Enter Host Name [myhostname]: device71
Enter Host Location [room/rack]: Lab

   Host IPv4: 10.252.0.71/24
IPv6 Enabled: Yes
 Host Link-Local IPv6: fe80::207:99ff:fe66:6999/64
   Host IPv6: Auto
   Host Name: device71
        Host Location: Lab
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a
```

Management IPv4 Address

The Host IP address is the IP address through which you access the TippingPoint IPS. The Host IP address must meet the following criteria:

- Must be standard IPv4 address format.
- Must be contained within the local network, but must **not** be contained within any subnets that pass traffic through the Multi-Zone Defense Module. If you assign the management port an IP address that is within a subnet connected through the Multi-Zone Defense Module interface card, the interfaces will not perform reliably.
- Must be accessible from the workstation from which you will manage the device.

Network IPv4 Mask

The network mask for the subnet on which the TippingPoint IPS is located.

Enable IPv6/Enable IPv6 Address Autoconfig

Select Y for both of these options to enable IPv6 on the device and to automatically configure the IPv6 address.

Host Name

The host name of the TippingPoint IPS. Use the name that the IPS will be known as on your network.

Host Location

The host location is the physical location of the TippingPoint IPS. It is for informational purposes only.

Default Gateway Options

The Default Gateway options configure the routing information that the TippingPoint IPS needs to communicate with other networks.

NOTE: If the TippingPoint IPS Host Management Port and the workstation from which you will manage the IPS are on different subnets, you must define a default gateway or an additional route to enable network-based management of your IPS. See "Management Port Routing Options" on page 13.

In this example, the default gateway address is `10.252.0.254`.

```
The default gateway is a router that enables this device to communicate with other
devices on the management network outside of the local subnet.
Do you require a default gateway? <Y, [N]>: y
Enter IPv4 Gateway Address (a value of 0.0.0.0 removes the default gateway)
[0.0.0.0]: 10.252.0.254
IPv4 Gateway Address: 10.252.0.254
IPv6 Gateway Address: Auto
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: A
```

Default Gateway

The default gateway is the IP address through which communications with other subnets are routed. If the TippingPoint IPS sends a message to an IP address outside of its subnet, the message and the reply go through the default gateway.

You can specify both an IPv4 and an IPv6 address.

TIP: Using additional routes instead of a default gateway helps assure that your Management Port only communicates with explicitly authorized network segments. See "Management Port Routing Options" on page 13.

DNS Configuration

The DNS configuration options define the DNS servers that the TippingPoint IPS will use to resolve host names.

```
The DNS server resolves hostnames to IP addresses.
Would you like to configure a DNS server? <Y,[N]>:y
Enter the Primary DNS server IP Address: [none]: 152.67.140.3
Would you like to configure a secondary DNS server (currently not configured)?
<Y,[N]>:
Enter the DNS Domain Name []: tippingpoint.com
DNS Primary Server: 152.67.140.3
DNS SecondaryServer:
Domain Name: tippingpoint.com
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a
```

Timekeeping Options

The TippingPoint IPS can keep time using its internal CMOS clock or it can use an Internet Simple Network Time Protocol (SNTP) server. If you decide to use SNTP for timekeeping, the TippingPoint IPS comes with the following SNTP servers defined as the default primary and secondary SNTP servers:

- National Institute of Standards and Technology (192.43.244.18)
- US Naval Observatory (192.5.41.40)

NOTE: If you use the CLI `show sntp` command, the TippingPoint IPS displays the current settings for Primary Addr and Secondary Addr. If SNTP timekeeping is turned off (CONF T NO SNTP), the last SNTP servers defined (or default if never defined) are shown.

CAUTION: Using external SNTP servers could make your TippingPoint IPS susceptible to a man-in-the-middle attack. It is more secure to use an SNTP server on a local, protected network.

The Timekeeping Options dialog follows:

```
Timekeeping options allow you to set the time zone, enable or disable daylight
saving time, and configure or disable SNTP.
Would you like to modify timekeeping options? <Y,[N]>: y
Enter time zone or '?' for complete list [GMT]: CST
Automatically adjust clock for daylight saving changes? [Yes]: Y
Do you want to enable the SNTP client? [No]: Y
Enter Primary SNTP Server address [192.43.244.18]:
Enter Secondary SNTP Server address [192.5.41.40]:
TimeZone: CST
DST enabled: Yes
SNTP enabled: Yes
SNTP Primary Server: 192.43.244.18
SNTP Secondary Server: 192.5.41.40
Enter [A]ccept, [C]hange, or [E]xit without saving [C]:
```

Time Zone

Sets the local time zone on the device. System logs are kept in Universal Time (UTC), but the TippingPoint IPS calculates local time for display purposes.

Daylight Saving Time

Enables or disables the option to calculate time based on the time of year.

Primary Time Server

The IP address of the SNTP server that your TippingPoint IPS uses to keep time.

Secondary Time Server

The IP address of the SNTP server that your TippingPoint IPS uses to keep time if the primary server is unavailable.

After the Setup Wizard

After you have completed the initial setup wizard, if you have changed from the HTTPS or SNMP server settings, you must reboot. Use the `reboot` command in the CLI. After the IPS reboots, you can use the Local Security Manager GUI to perform monitoring and configuration tasks or use the `setup` command in the CLI to perform additional configuration tasks. See "Additional Configuration" on page 11.

Additional Configuration

After you have completed the initial setup wizard through the Command Line Interface or on the LCD screen, you can further configure your TippingPoint IPS. These subsequent setup options include the following:

Web, CLI, and SNMP Server Options

The Web, CLI, and SNMP Server Options dialog enables and disables TippingPoint IPS servers. Always use the secure Web and CLI servers (HTTPS and SSH) when conducting normal operations. Use the non-secure servers (HTTP and telnet) only for troubleshooting if the secure servers are unusable.

NOTE: You do not need to run any servers if you want to control your TippingPoint IPS through the serial port only. However, you cannot manage filters or perform network discovery scans without servers. You can turn off all servers by using the CONF T SERVER commands. For changes to HTTP or HTTPS to take effect, reboot the device.

```
Server options allow you to enable or disable each of the following servers: SSH,
Telnet, HTTPS, HTTP, and SNMP.
Would you like to modify the server options? <Y, [N]>: y
Enable the SSH server? [Yes]:y
Enable the Telnet server? [No]:n
Enable the HTTPS server ('No' disables SMS access)? [Yes]:y
Enable the HTTP server? [No]:n
Enable the SNMP agent ('No' disables SMS and NMS access)? [Yes]:y
SSH: Yes
Telnet: No
HTTPS: Yes
HTTP: No
SNMP: Yes
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: e
```

SSH Server

Enables encrypted terminal communications. The SSH server must be enabled to establish a secure CLI session over your network. This option is enabled by default.

Telnet Server

Enables telnet connections to the IPS. The telnet server can be enabled to run non-secure CLI sessions over your network. This option is disabled by default.

△ **CAUTION:** Telnet is not a secure service. If you enable telnet, you endanger the security of your TippingPoint device. Use SSH instead of telnet when you are conducting normal operations.

HTTPS Server

Enables secure web access and encrypted file transfers over the network. The HTTPS server must be enabled to use SMS management. You can also run the LSM using the HTTPS server. This option is enabled by default.

HTTP Server

Enables non-secure web access. You can enable the HTTP server to run non-secure LSM session on your network. This option is disabled by default.

△ **CAUTION:** HTTP is not a secure service. If you enable HTTP, you endanger the security of your TippingPoint device. Use HTTPS instead of HTTP for normal operations.

SNMP Server

The SNMP Server provides access to interface counters and other statistics, configuration data, and general system information via the Simple Network Management Protocol (SNMP). The SNMP server must be enabled to use SMS management or to allow NMS access. This option is enabled by default.

Restricted SMS Access

The Restricted SMS Access dialog enables you to guard against unauthorized management of the device by a Security Management System (SMS). Using this option, the device accepts management only from an SMS at a specified IP address. When you execute the `setup sms` command, you are prompted to enter the IP address or CIDR of the SMS device that you want to manage the device. The system displays this address as an Allowed SMS, and you are then prompted to save your changes.

```
Enter Security Management System IP Address or CIDR [none]: 123.45.67.890
        Allowed SMS: 123.45.67.890
Enter [A]ccept, [C]hange, or [E]xit without saving [C]:
```

Ethernet Port Settings

The Ethernet Port settings dialog enable and disable ports, and also set port speed, duplex, and negotiation settings. You can only access the Ethernet Port Setup by using the `setup ethernet-port` command in the CLI.

TIP: You can configure Ethernet ports individually using the `conf t interface ethernet` command.

△ **CAUTION:** When you configure an Ethernet port using the command line interface, the port will be shut down. Use the `conf t int ethernet <segment> <port> no shutdown` command to restart the port.

The Ethernet Port Options dialog configures individual port values for the IPS Ethernet interfaces.

```
Would you like to modify the Ethernet ports <Y,[N]>:y
We will now configure your Ethernet ports.
Configure port 1A (Ethernet Port)? <Y,[N]>:y
This port is currently enabled, would you like to disable it? <Y,[N]>:n
Please enter values for the following options
Line speed [1000]:
Duplex setting [Full]:
Auto negotiation [On]:
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a
Configure Port 2 (Ethernet Port)? <Y,[N]>:
```

Line Speed

The line speed setting for a port. You can set a port to 10, 100, or 1000 Kbps.

Duplex Setting

The duplex setting for the port. Copper can be set to FULL or HALF. Fiber ports can be set to FULL.

Auto Negotiation

The auto negotiation setting determines whether the port negotiates its speed based on the connection it can make.

Management Port Routing Options

The Management Port Routing options dialog configures management port routes. You can access the Management Port Routing options only by using the SETUP HOST command in the CLI.

These options enable the TippingPoint IPS device to be managed from a different network than the one to which the management port is connected. You can define up to 12 routes that your Management Port can use to communicate with other subnets.

△ **CAUTION:** Define additional routes with care. The broader the definition of additional routes you use, the greater the chance that an unauthorized user can reach your IPS.

```
Would you like to modify management port routes? <Y,[N]>:y
 Currently, the additional routes are as follows:
  #  Destination        Gateway
  1 any4       10.252.0.254
  2 none       none
  3 none       none
  4 none       none
  5 none       none
  6 none       none
  7 none       none
  8 none       none
  9 none       none
 10 none       none
 11 none       none
 12 none       none
 Enter [A]ccept, [C]hange, [R]emove or [E]xit without saving [C]: c
```

The new route is added to the list. The following example shows an example of a routing table that has had both IPv4 and IPv6 addresses added to it:

```
Currently, the additional routes are as follows:
 #  Destination     Gateway
 1 any4    10.252.0.254
 2 1.2.3.0/24       10.252.0.123
 3 fc01:afc::102:300/120     fe80::205:9bff:fe86:1234
 4 none    none
 5 none    none
 6 none    none
 7 none    none
 8 none    none
 9 none    none
10 none    none
11 none    none
12 none    none
```

NOTE: Whether or not static route entries are included in routing tables depends on several topology factors. These include network specificity, metrics, and whether the next hop IP is on the associated interface. Other routing types, redistributions, and firewall rules also impact static route entries in the routing tables.

Destination Network

The IP network address of the subnet with which you want the IPS to communicate.

Gateway

The IP address on the IPS subnet that can communicate with the destination network.

Default Alert Information

The Default Alert options dialog defines the default sender and recipient for filter alert emails. You can only access the Default Alert options by using the SETUP EMAIL-DEFAULT command in the CLI.

```
Enter TO: email address (128 max. characters)
Must be a full email address (e.g., recipient@company.com) []:
employee@company.com
Enter FROM: email address (128 max. characters)
Must be a full email address (e.g., sender@company.com) []: tpt3@company.com
Enter FROM: Domain Name (128 max. characters, e.g., company.com) []: company.com
Enter email server IP address []: 1.2.3.4
Enter period (in minutes) that email should be sent (1 - 10080) [1]: 5
To: employee@company.com
From: tpt3@company.com
Domain: company.com
Email Server: 1.2.3.4
Period (minutes): 5
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a
```

TO email address

The email address to which alert notifications will be sent. The address must be:

- less than 129 characters long
- a valid email address. For example: johndoe@mycompany.com

FROM email address

The address that alert notifications will contain in the from field. The address must be:

- less than 129 characters long
- a valid email account name on the SMTP server
- a valid email address on the SMTP server

Domain

The domain name of the SMTP server.

Email Server IP address

The address where the SMTP server is located. The address must be a valid IP address for an SMTP server.

Period

The aggregation period for email alerts. The first time a filter that calls for email notification is triggered, the system sends an email notification to the target named in the filter. At the same time, the aggregation timer starts. The TippingPoint device counts additional filter triggers, but does not email another notification until it sends a count of all filter triggers that occurred during that period. The timer continues to count and send notifications at the end of each period. The period must be an integer between 1 and 10,080 representing minutes between notifications.

3 Navigation

Overview

The Command Line Interface (CLI) is a standard embedded system command line interface that provides access to hardware and embedded software configuration. This chapter describes logging in and issuing commands with the CLI.

Accessing the CLI

Log in to the CLI using an SSH session or through a terminal connected to the device through the console port. To log in via SSH, you must have:

- an SSH client
- a valid username and password on the device. If you do not have a username and password, a user with super-user access must create them for you.

To Log in to the CLI

1. If you are using SSH to connect to the CLI, start an SSH session using the IP address of the management port. If you are using the console, ensure that the console and device are powered on and ready.
2. Enter your username at the **Login** prompt.
3. Enter your password at the **Password** prompt.

Navigation

The TippingPoint Command Line Interface offers the following features:

The following sections describe each of these features.

Command Types

The CLI has two types of commands.

- **Global commands**: Available from within any menu level in the CLI. Global commands do not report on or change configuration items. These commands are listed by the command `help commands`.
- **Hierarchical commands**: Configure, manage, and display TippingPoint IPS configuration. Some IPS commands are hierarchical and are available only within a menu or submenu.

Using Hierarchical Commands

The CLI divides the hierarchical commands into functional areas. There are several commands that lead to submenus, including `configure terminal` and `show`.

Context Sensitive Prompt

The CLI prompt helps indicate what menu level you are currently using. The top-level menu prompt is:

```
hostname#
```

When you enter a submenu, the prompt changes to indicate the current menu level. For example, changing to the **show** submenu will change the CLI prompt from:

```
hostname# show
```

to

```
hostname(show)#
```

Exiting Submenus

The `exit` command steps back to the previous menu, or up one submenu. The `exit all` command returns you to the **hostname#** menu level.

Command Hints

On each command level, you can view the hierarchical commands available at that level by typing a question mark (`?`).

Command Completion

The CLI attempts to match partially typed commands with valid commands. For example, if you type:

```
reb?
```

The CLI interprets this command as if you typed the following:

```
reboot
```

You can also use the Tab key for command completion.

Command Line Editing

The following commands can be used to edit your command line entries:

Table 3-1 CLI Edit commands

Key Combination	Edit Function
`Ctrl-d`	Delete current character
`Ctrl-u`	Delete text up to cursor
`Ctrl-k`	Delete from cursor to end of line
`Ctrl-a`	Move to beginning of line
`Ctrl-e`	Move to end of line
`Ctrl-p`	Get prior command from history
`Ctrl-n`	Get next command from history
`Ctrl-b`	Move cursor left
`Ctrl-f`	Move cursor right
`Esc-b`	Move back one word
`Esc-f`	Move forward one word
`Esc-c`	Convert rest of word to uppercase
`Esc-l`	Convert rest of word to lowercase
`Esc-d`	Delete remainder of word
`Ctrl-w`	Delete word up to cursor

Table 3-1 CLI Edit commands

Key Combination	Edit Function
`Ctrl-t`	Transpose current and previous character
`Ctrl-z`	Enter command and return to root prompt
`Ctrl-l`	Refresh input line
`up arrow`	Put last command on the command line
`!! <cr>`	Execute last command

Session Settings

The CLI contains commands to configure how your terminal session behaves. The following table lists the default terminal settings and the CLI commands that you can use to change the settings.

Table 3-2 Default Console Settings

Setting	Description	Default Value	Command to Change Setting
`columns`	Sets the width of the session window in number of columns.	80	`conf t session col <number of columns>`
`rows`	Sets the height of the session window in number of columns.	25	`conf t session row <number of rows>`
`more`	When enabled, displays large amounts of information in page-by-page format.	SSH: Off Console: on	`conf t session more` `conf t session no more`
`wraparound`	When enabled, wraps lines of text.	on	`conf t session no wrap`
`timeout`	Sets the period of inactivity after which a user will be logged off.	20 minutes	`conf t session timeout <number of minutes>`

See the command "conf t session" on page 56 for more information.

NOTE: The timeout persists only if the `-persist` option is used when configuring the terminal session timeout. The `-persist` option requires super-user privileges.

TIP: For best viewing, set your terminal software's row and column settings to match your CLI session's row and column settings.

4 TippingPoint IPS Commands

This chapter provides a reference for the Command Line Interface (CLI) for the TippingPoint IPS.

Overview

This chapter contains reference information for each command and includes the following sections:

Conventions

This chapter is divided into sections by top-level commands. Some top-level commands, such as `configure terminal`, have been split up for easier reference. Each command section includes the following information:

- Description
- Required privileges
- Subcommands and/or options
- Examples of usage

Variables are enclosed in angle brackets. For example, a snapshot name variable is represented as `<snapshot name>`. Optional flags and variables are enclosed in square brackets. For example, an optional profile name is represented as `[-profile <profile name>]`.

△ **CAUTION:** The square brackets are included in usage examples for clarification purposes only. Do not type these brackets when entering a command.

Global Commands

The commands in this section manage your CLI session. The settings and results do not persist across multiple sessions. These commands are available to all users and user roles.

alias

Creates aliases for commands or command strings. You can define an alias to represent all of or a portion of a command line including:

- a command
- a command option
- a command flag or option
- a combination of command, options, and flags

Usage

```
alias <alias> "<command_string>"
```

The following table lists examples of user-created command aliases.

Table 4-1 Alias Definition Examples

define alias	before alias	after alias
`alias s1A "show conf int eth 1A"`	`show conf int eth 1A`	`s1A`
`alias 1A "int eth 1A"`	`show conf int eth 1A`	`show conf 1A`
	`conf t int eth 1A shutdown`	`conf t 1A shut`
`alias eth "int eth"`	`show conf int eth 1A`	`show conf eth 1A`
	`show conf int eth 1A`	`show conf eth 1A`
`alias sc "show conf"`	`show conf int eth 1A`	`sc int eth 1A`
	`show conf clock`	`sc clock`

clear

Resets logs or hardware interfaces.

Required Privilege

Admin, Super-User

NOTE: Users with Admin privileges cannot clear the audit log or execute the `clear configuration` command.

Subcommands

The `clear` command uses the following subcommands:

Table 4-2 clear subcommands

Subcommand	Description	Usage
`adaptive-filter`	Re-enables a filter that has been disabled because of adaptive-filter configuration.	`clear adaptive-filter <number>`
`configuration`	Resets the device configuration settings to the factory defaults. Use the `-echo` option to echo the command when it is executed.	`clear configuration`
`connection-table`	Use the `blocks` option to clear all connection table block entries. Use the `trusts` option to clear all trust table entries.	`clear connection-table blocks` `clear connection-table trusts`

Table 4-2 clear subcommands

Subcommand	Description	Usage
`counter interface`	Clears interface counters.	`clear counter interface`
`counter policy`	Clears policy counters.	`clear counter policy`
`interface`	Clears the interface. When used without options, it resets all interfaces.	`clear interface` `clear interface ethernet <port>`

`log`	Clears log files. When used without options, it erases all entries in all logs.	`clear log`
		`clear log alert`
		`clear log audit`
		`clear log block`
		`clear log packet-trace`
		`clear log quarantine`
		`clear log system`

`np`	Clears np statistical information.
	• `mcfilt-rule-stats` clears microfilter rules and flow statistics
	• `rule-stats` clears rule statistics
	• `softlinx` clears Softlinx-related statistics
	• `tier-stats` clears tier statistics
		`clear np mcfilt-rule-stats`
		`clear np rule-stats`
		`clear np softlinx`
		`clear np tier-stats`

`ramdisk stats`	Clears RAM disk statistics.	`clear ramdisk stats`
`rate-limit`	Clears rate-limited streams from the data table.	`clear rate-limit streams`
`slot`	Sets the module slot and module type to Empty.	`clear slot <slot number>`

NOTE: `clear counter interface`, `clear interface`, and `clear log` are disabled when the device is managed by an SMS.

cls

Clears the terminal screen.

Usage

```
cls
```

exit

Backs you out of one or more command levels. For detailed information about command hierarchy, see "Using Hierarchical Commands" on page 17.

Usage

```
exit
exit all
```

help

Displays documentation about the specified command. At the CLI prompt, you can access the help topics for commands. You can also specify help for commands and edit keys.

Usage

```
help
help commands
help edit
```

history

Displays a list of commands that have been executed during the current CLI session.

Usage

```
history
```

logout

Logs you out of the TippingPoint IPS.

Usage

```
logout
```

quit

Logs you out of the TippingPoint IPS.

Usage

```
quit
```

tree

Displays the full command tree.

Usage

```
tree
```

who

Shows the usernames, connection methods, IP addresses, and login times of all the users who are currently logged in to IPS. By default, the login time is shown in the time zone that you set during setup or with the `conf t clock` command. Use the `-utc` option to view the login times in Universal Time.

Required Privilege

Admin, Super-User

Usage

```
who
who -utc
```

whoami

Displays the username, role, and path of the currently logged-in user.

Usage

```
whoami
```

Tipping Point Operating System Commands

The commands in this section configure, manage, and display information about the Tipping Point Operating System and its users.

boot

Manages boot images on the device.

Required Privilege

Super-user, Admin

Subcommands

The `boot` command uses the following subcommands:

Table 4-3 boot subcommands

Subcommand	Description	Usage
`list-image`	Shows a list of all available boot images.	`boot list-image`
`remove-image`	Removes a boot image from the device's hard disk. The image is identified by version number. △ **CAUTION:** Removing a boot image permanently erases it.	`boot remove-image <version>`
`rollback`	Rolls the boot image back to the next most recent valid boot image. This command can be used to revert the operating system to a previous version.	`boot rollback`

NOTE: `boot remove-image` and `boot rollback` are disabled when the device is managed by an SMS.

bugreport

Polls the IPS for statistics and other relevant information and sends the information as a clear-text email message to the specified TippingPoint Technologies email address. Execute this command only when requested by TippingPoint support personnel.

The command can take up to a minute to execute. The default email options must be configured with the "setup" command for the email transfer to succeed.

Required Privilege

Admin, Super-User, Operator

Usage

```
bugreport <email address> "<description>"
```

compact-flash

Controls the external storage card on the TippingPoint IPS devices. The external storage card is used to store logs, snapshots, and other system data.

NOTE: The `conf t compact-flash` command is not supported on the TippingPoint 10/110/330 models.

Required Privilege

Admin, Super-User, Operator

Subcommands

The `compact-flash` command uses the following subcommands:

Table 4-4 compact-flash subcommands

Subcommand	Description	Usage
`format`	Formats the external storage card.	`compact-flash format`
`mount`	Manually mounts the inserted external storage card.	`compact-flash mount`
`unmount`	Unmounts the external storage card so that the user can remove it.	`compact-flash unmount`

configure terminal

The `configure terminal` commands configure IPS settings. The command can be abbreviated as `conf t`. The following configure terminal commands are available:

conf t action-set

Configures new or existing action sets. The subcommands specify the actions taken.

Required Privilege

Admin, Super-User

Subcommands

The `conf t action-set` command uses the following subcommands.

△ **CAUTION:** The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

Table 4-5 conf t action-set subcommands

Subcommand	Description	Usage
`allowed-dest`	Adds or removes a quarantine allowed destination.	`conf t action-set <action set name> allowed-dest <destination address> add` `conf t action-set <action set name> allowed-dest <destination address> remove`
`apply-only`	Adds or removes a CIDR from the quarantine apply-only list.	`conf t action-set <action set name> apply-only <CIDR> add` `conf t action-set <action set name> apply-only <CIDR> remove`

`block`	Creates or modifies an action set that blocks traffic. The following secondary actions can be added:
	• `quarantine`: host IP address is placed into quarantine. Use `no quarantine` to remove the address from quarantine.
	• `reset-both`: TCP reset on the source and destination.
	• `reset-destination`: TCP reset on the destination.
	• `reset-source`: TCP reset on the source.
	• `reset-none`: no TCP reset.
		`conf t action-set <action set name> quarantine`
		`conf t action-set <action set name> no quarantine`
		`conf t action-set <action set name> block reset-both`
		`conf t action-set <action set name> block reset-destination`
		`conf t action-set <action set name> block reset-none`
		`conf t action-set <action set name> block rest-source`

`delete`	Deletes the named action set.	`conf t action-set <action set name> delete`
`http-block`	Blocks http requests from quarantined hosts.	`conf t action-set <action set name> http-block`
`http-page`	Creates a web page to display when a quarantined host makes a web request.	`conf t action-set <action set name> http-page [-show-name <name of page>] [-show-desc <description of page>] [-custom-text <content of page>]`
`http-redirect`	Redirects http requests from a quarantined host to a specified URL.	`conf t action-set <action set name> http-redirect <url>`

Table 4-5 conf t action-set subcommands

Subcommand	Description	Usage
non-http-block	Blocks non-http requests from quarantined hosts. Permits non-http requests with no non-http-block.	conf t action-set <action set name> non-http-block
notify-contact	Adds or removes a notification contact from an action set.	conf t action-set <action set name> notify-contact add <contact name> conf t action-set <action set name> notify-contact remove <contact name>
packet-trace	Enables and sets packet trace settings. Set a priority (high, medium, or low) with the -priority option and the number of bytes to capture (64-1600) with the -capture-size option. Use no packet-trace to disable packet tracing.	conf t action-set <action set name> packet-trace [-priority <priority>] [-capture-size <bytes>] conf t action-set <action set name> no packet-trace
permit	Creates or modifies an action set that permits traffic. Use the quarantine command to quarantine permitted traffic and no quarantine to stop quarantining permitted traffic.	conf t action-set <action set name> permit conf t action-set <action set name> permit quarantine conf t action-set <action set name> permit no quarantine
rate-limit	Creates or modifies an action set that rate-limits traffic. Enter the desired threshold in Kbps.	conf t action-set <action set name> rate-limit <threshold>
rename	Renames the action set.	conf t action-set <action set name> rename <new action set name>
threshold	Sets the quarantine threshold in seconds (1-10000).	conf t action-set threshold <seconds>
threshold-period	Sets the quarantine threshold period in minutes (1-60).	conf t action-set threshold-period <minutes>
trust	Creates or modifies a trust action set.	conf t action-set <action set name> trust
whitelist	Creates a whitelist of trusted IP addresses by using the add or remove subcommands.	conf t action-set <action set name> whitelist add <IP address> conf t action-set <action set name> whitelist remove <IP address>

conf t autodv

Enables and disables the automatic download service for Digital Vaccine (DV) updates. This command requires a day of week and time of day for the download. If required, use the -period option to set the number of days between checks.

Required Privilege

Admin, Super-User

Usage

```
conf t autodv day <day of week> time <time of day> -period <number of days>
conf t no autodv
```

conf t authentication remote

Manages remote authentication. Remote authentication enables an SMS-managed device to use the SMS as an authentication proxy. When a user logs in, the device sends the login information to the SMS, which then authenticates the account against one or more account repositories.

NOTE: Remote authentication will only function when network TCP port 10043 is open and not blocked by a firewall.

Required Privilege

Admin, Super-User

Subcommands

The `conf t authentication remote` command uses the following subcommands:

Table 4-6 conf t authentication remote subcommands

Subcommand	Description	Usage
`enable`	Enables remote authentication.	`conf t authentication remote enable`
`disable`	Disables remote authentication.	`conf t authentication remote disable`
`timeout`	Sets the remote authentication server timeout. The value should be greater than the timeout configured on the SMS.	`conf t authentication remote timeout <seconds>`

conf t category-settings

Enables and disables filter categories. The command also enables you to assign a specific action set to each category. The following filter categories can be configured:

- exploits
- identity-theft
- im
- network-equipment
- p2p
- reconnaissance
- security-policy
- spyware
- streaming-media
- traffic-normal
- virus
- vulnerabilities

Required Privilege

Admin, Super-User

Subcommands

The `conf t category-settings` command uses the following subcommands.

△ **CAUTION:** The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

Table 4-7 conf t category-settings subcommands

Subcommand	Description	Usage
`enable`	Enables a filter category and assigns the named action set to the category. Enable the filter category for a specific profile with the `-profile` option.	`conf t category-settings [-profile <profile name>] <filter category> enable -action-set <action set>`
`disable`	Disables the filter category.	`conf t category-settings [-profile <profile name>] <filter category> disable`

conf t clock

Sets the software clock on the IPS device. Clock changes are synchronized with the appropriate clock driver, and the change is entered in the audit log.

Required Privilege

Admin, Super-User

Subcommands

The `conf t clock` command uses the following subcommands:

Table 4-8 conf t clock subcommands

Subcommand	Description	Usage
`date`	Sets the date.	`conf t clock date <YYYY-MM-DD>`
`dst`	Enables or disables Daylight Savings Time.	`conf t clock dst` `conf t clock no dst`
`time`	Sets the time according to the 24-hour clock. For example, to set the clock to 3:30 PM, enter 15:30.	`conf t clock time <HH:MM:SS>`
`timezone`	Sets the time zone. For a list of available time zones, use the command `show timezones`.	`conf t clock timezone <time zone>`

conf t compact-flash

Configures the mounting options for the external storage card. By default, the device is set to automatically mount external storage cards when inserted.

NOTE: The `conf t compact-flash` command is not supported on the TippingPoint 10/110/330 models.

Required Privilege

Admin, Super-User

Subcommands

The `conf t compact-flash` command uses the following subcommands:

Table 4-9 conf t compact-flash subcommands

Subcommand	Description	Usage
`operation-mode authenticate`	Sets the device to require authentication when an external storage card is inserted.	`conf t compact-flash operation-mode authenticate`
`operation-mode auto-mount`	Sets the device to automatically mount external storage cards when inserted.	`conf t compact-flash operation-mode auto-mount`

conf t cpu-utilization

Configures the period over which average CPU utilization is calculated. The period is specified in seconds. To view processes and utilization, see "debug information" on page 68.

Required Privilege

Admin, Super-User

Usage

```
conf t cpu-utilization <period in seconds>
```

conf t default-alert-sink

Defines the default email recipient of traffic-triggered alerts.

NOTE: The email notification server must be an SMTP server that the IPS device can reach through its host management port. You might have to add an additional route to your host management port using the `conf t interface mgmtEthernet` command to enable this communication. See "conf t interface mgmtEthernet" on page 41.

Required Privilege

Admin, Super-User

Subcommands

The `conf t default-alert-sink` command uses the following options:

Table 4-10 conf t default-alert-sink options

Subcommand	Description	Usage
`domain`	Defines the domain name of the email notification server.	`conf t default-alert-sink domain <domain name>`
`from`	Defines the email address for the IPS device. This must be a valid email user name on the notification server.	`conf t default-alert-sink from <email address>`
`no`	Removes the default email destination.	`conf t no default-alert-sink`
`period`	Defines the default period of time in which the TippingPoint device accumulates notifications before sending an aggregate notification email.	`conf t default-alert-sink period <minutes>`
`server`	Defines the IP address of the email notification server.	`conf t default-alert-sink server <IP address>`
`to`	Defines the email address of the alert recipient. This must be a valid email address.	`conf t default-alert-sink to <email address>`

conf t default-gateway

Defines a default gateway IP address for your IPS. This gateway is used by the management port to communicate with devices located on other network segments. Use the `conf t no default-gateway` command to disable the default gateway IP address.

Required Privilege

Admin, Super-User

Usage

```
conf t default-gateway <IP address>
conf t no default-gateway
```

conf t email-rate-limit

Configures the maximum number of email notifications that the system will send every minute. The minimum is 1, and the maximum is 35.

Required Privilege

Admin, Super-User

Usage

```
conf t email-rate-limit <number>
```

conf t filter

Configures a filter's state and action set category and enables or disables the filter. Filters are identified with unique numbers. When you configure, enable, or disable a filter, enter the number for the filter. Only the `reset` subcommand supports `all` as an option.

Required Privilege

Admin, Super-User

Subcommands

The `conf t filter` command uses the following subcommands:

△ **CAUTION:** The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

Table 4-11 conf t filter subcommands

Subcommand	Description	Usage
`adaptive-config`	Enables or disables adaptive filtering. Apply the change to a specific security profile with the `-profile` option.	`conf t filter <filter number> [-profile <profile name>] adaptive-config` `conf t filter <filter number> no adaptive-config`
`add-exception`	Creates and adds an exception to a filter, identified by source or destination IP address. Apply the change to a specific security profile with the `-profile` option.	`conf t filter <filter number> [-profile <profile name>] add-exception <source IP address> <destination IP address>`
`delete-copy`	Deletes a copy of the filter. Apply the change to a specific security profile with the `-profile` option.	`conf t filter <filter number> [-profile <profile name>] delete-copy`

Table 4-11 conf t filter subcommands

Subcommand	Description	Usage
`disable`	Disables a filter. Apply the change to a specific security profile with the `-profile` option.	`conf t filter <filter number> [-profile <profile name>] disable`
`enable`	Enables a filter. Apply the change to a specific security profile with `-profile` option. Apply the change to a specific action set with the `-action-set` option.	`conf t filter <filter number> [-profile <profile name>] -action-set <action set name> enable`
`remove-exception`	Removes an exception from a filter. Apply the change to a specific profile with the `-profile` option.	`conf t filter <filter number> [-profile <profile name>] remove-exception`
`reset`	Resets filters to the default values.	`conf t filter <filter number> reset` `conf t filter all reset`
`threshold`	Sets the port scan and host sweep filter threshold.	`conf t filter threshold`
`timeout`	Sets the port scan and host sweep filter timeout.	`conf t filter timeout`
`use-category`	Sets a filter to use the default action set of its category and removes any previous overrides. Apply the change to a specific profile with the `-profile` option.	`conf t filter <filter number> [-profile <profile name>] use-category`

conf t high-availability

Enables and disables transparent network high availability (transparent HA) and configures the partner device's IP address. Transparent HA updates data tables between two devices to quickly and efficiently transfer network traffic from one device to the other without the need to rebuild data tables.

Required Privilege

Admin, Super-User

Subcommands

The `conf t high-availability` command uses the following subcommands:

Table 4-12 conf t high-availability subcommands

Subcommand	Description	Usage
`disable`	Disables transparent HA.	`conf t high-availability disable`
`enable`	Enables transparent HA.	`conf t high-availability enable`
`partner`	Sets the IP address and serial number of the partner device. Use `no partner` to clear the address.	`conf t high-availability partner <IP address> <serial number>` `conf t high-availability no partner`
`l2fb`	For 10/110/330 IPS devices only, sets the means by which the device goes in and out of Layer-2 Fallback (L2FB). You can configure L2FB using a link transition via hardware relays, or you can change the L2FB behavior to be software instantiated. • `hardware`: The hardware ZPHA relays are used for L2FB. When the device enters and exits L2FB, a brief link transition occurs. This is the default option. Hardware L2FB is recommended, unless link transitions will cause network failover issues. • `software`: No link transition occurs when the device enters and exits L2FB.	`conf t high-availability l2fb hardware` `conf t high-availability l2fb software`

conf t host

Configures the host management port's name and location strings. TippingPoint recommends using this command to limit access to the management port.

NOTE: The IPS must not be under SMS control when changing management port settings.

Required Privilege

Admin, Super-User. `conf t host fips-mode` requires Super-User.

Subcommands

The `conf t host` command uses the following subcommands.

CAUTION: The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

Table 4-13 conf t host subcommands

Subcommand	Description	Usage
`dns`	Sets the DNS server. The secondary server is optional.	`conf t host dns <domain name> <primary server> [<secondary server>]`
`fips-mode`	Enables FIPS mode. • `crypto`: Only FIPS-approved cryptographic algorithms are allowed, but some FIPS 140-2 requirements are not enforced. Once enabled, this mode can be disabled. • `full`: Only FIPS-approved cryptographic algorithms are allowed, and all FIPS 140-2 requirements are enforced. Once enabled, this mode *cannot* be disabled. Only a factory reset can take the device out of this mode. A warning message prompts you to confirm the setting. A reboot is required to complete the configuration. For more information about FIPS, see "fips" on page 73.	`conf t host fips-mode crypto` `conf t host fips-mode full`
`ip-filter`	Permits or denies communications with the management port from specified IP addresses. Management port IP setting defaults to "permit any IP". Use this subcommand to limit management port access to designated IP addresses.	`conf t host ip-filter deny <IP address>` `conf t host ip-filter permit <IP address>`

Table 4-13 conf t host subcommands

Subcommand	Description	Usage
`location`	Sets a text string that identifies the location of the device. The string is restricted to 63 characters.	`conf t host location <location>`
`name`	Sets a text string that identifies the name of the device. The string is restricted to 63 characters.	`conf t host name <name>`

conf t inspection-bypass

Enables, disables, or removes inspection bypass rules. Inspection bypass rules direct traffic through the IPS without inspection. The rules are identified by an ID number that is generated by the IPS when the rule is created with the `conf t inspection-bypass add` command. You can view a list of current inspection bypass rules with the `show inspection-bypass` command.

NOTE: Inspection bypass rules are available only on the TippingPoint 2500N, TippingPoint 5100N, TippingPoint 6100N, and NX-Platform devices.

Required privilege

Admin

Options

The `conf t inspection-bypass` command uses the following options:

Table 4-14 conf t inspection-bypass options

Subcommand	Description	Usage
`add`	Adds an inspection bypass rule. See "conf t inspection-bypass add" on page 38.	`conf t inspection-bypass add`
`clear-stats`	Clears statistics associated with an inspection bypass rule.	`conf t inspection-bypass clear-stats <rule_ID>`
`enable`	Enables an inspection bypass rule.	`conf t inspection-bypass enable <rule_ID>`
`disable`	Disables an inspection bypass rule.	`conf t inspection-bypass disable <rule_ID>`
`remove`	Removes an inspection bypass rule.	`conf t inspection-bypass remove <rule_ID>`

conf t inspection-bypass add

Creates and defines an inspection bypass rule. When you define an inspection bypass rule, using an option without a specified value defaults to a value of "any".

Required privilege

Admin

Options

The `conf t inspection-bypass add` command uses the following options:

Table 4-15 conf t inspection-bypass add options

Option	Description	Usage
`-eth`	EthType. You can also use the strings `ip` or `!ip`.	`conf t inspection-bypass add -eth <EthType>`
`-ports`	The port or ports to which the rule is applied. For more information, see "ports" on page 39.	`conf t inspection-bypass add -ports <value> -<option>`
`-gre`	Specifies GRE tunneling traffic. Default value is `any`. You can also specify `present` or `absent`.	`conf t inspection-bypass add -gre <value>`
`-mipv4`	Specifies mobile IPv4 tunneling traffic. Default value is `any`. You can also specify `present` or `absent`.	`conf t inspection-bypass add -mipv4 <value>`
`-ipv6in4`	Specifies IPv6 6-in-4 tunneling traffic. Default value is `any`. You can also specify `present` or `absent`.	`conf t inspection-bypass add -ipv6in4 <value>`
`-vlan`	Numeric value or range specifying the permitted VLAN IDs.	`conf t inspection-bypass add -vlan <value>`
`-mpls`	Numeric value or range specifying the permitted MPLS IDs.	`conf t inspection-bypass add -mpls <value>`
`-ip-proto`	IP protocol value. For more information, see "ip-proto" on page 40.	`conf t inspection-bypass add -ip-proto <value>`
`-ip-saddr`	Source CIDR specification. Enter in the form *xxx.xxx.xxx.xxx/xx*.	`conf t inspection-bypass add -ip-saddr <CIDR range>`
`-ip-daddr`	Destination CIDR specification. Enter in the form *xxx.xxx.xxx.xxx/xx*.	`conf t inspection-bypass add -ip-daddr <CIDR range>`
`-upd-sport`	UPD source port.	`conf t inspection-bypass add -upd-sport <value>`
`-upd-dport`	UPD destination port.	`conf t inspection-bypass add -upd-dport <value>`
`-tcp-sport`	TCP source port.	`conf t inspection-bypass add -tcp-sport`
`-tcp-dport`	TCP destination port.	`conf t inspection-bypass add -tcp-dport`

ports

The -ports option can be one or more comma-delimited 1GbE ports (1A, 1B, 2A, 2B, 3A, 3B). If you do not specify a port or define the `-ports` option as `ANY`, the inspection bypass rule is applied to all ports on all segments.

A single inspection bypass rule can apply to all segments, to both ports on one segment, or to one port on one segment. You cannot apply a single inspection bypass rule to ports on two different segments. Instead, you must create a separate inspection bypass rule for each segment.

Example: Rules Applied to a Single Segment

If you want to permit traffic that uses the IP Mobility protocol (MOBILE) on both ports of Segment 1, you would define the inspection bypass rule with the following command:

```
hostname# conf t inspection-bypass add -ports 1A,1B -ip-proto MOBILE
```

Example: Rules Applied Across Multiple Segments

If you want to permit traffic that uses the IP Mobility protocol (MOBILE) on both ports of Segment 1 and Segment 2, you would need to define two inspection bypass rules with the following commands:

```
hostname# conf t inspection-bypass add -ports 1A,1B -ip-proto MOBILE
hostname# conf t inspection-bypass add -ports 2A,2B -ip-proto MOBILE
```

However, if you want to permit that traffic across all ports on all segments, you can define a single inspection bypass rule with the following command:

```
hostname# conf t inspection-bypass add -ip-proto MOBILE
```

When no segment is specified, the command defaults apply the inspection bypass rule to all ports on all segments.

ip-proto

A full list of IP protocol values can be found at the Internet Assigned Numbers Authority website at http://www.iana.org/assignments/protocol-numbers.

conf t interface ethernet

Configures IPS interfaces. Refer to physical interfaces by their segment and port numbers.

On NX-Platform devices, ports are presented in the format *Slot-SegmentPort*. For example, port 4A on slot 3 would be specified as "3-4A".

Required Privilege

Admin, Super-User

Subcommands

The `conf t interface ethernet` command uses the following subcommands:

Table 4-16 conf t interface ethernet subcommands

Subcommand	Description	Usage
`duplex`	Sets the duplex speed to half or full.	`conf t interface ethernet <port> duplex half` `conf t interface ethernet <port> duplex full`
`linespeed`	Sets the line speed. You can set the speed to 10, 100, 1000, or 10000.	`conf t interface ethernet <port> linespeed <speed>`
`negotiate`	Enables or disables auto-negotiate.	`conf t interface ethernet <port> negotiate` `conf t interface ethernet <port> no negotiate`
`shutdown`	Shuts down the port. Use `no shutdown` to reactivate the port after a shutdown command or after configuration has changed.	`conf t interface ethernet <port> shutdown` `conf t interface ethernet <port> no shutdown`

NOTE: When the auto-negotiate feature is on, the IPS device automatically negotiates the highest common speed and duplex that the IPS and the link partner both support. When the auto-negotiate feature is turned off, users can configure all fiber ports (SFP, SFP+, QSFP+) only to their default settings using the `linespeed` subcommand even though the hardware might list other optional values. The 12 fixed RJ-45 copper ports, however, can be configured to 10 Mbps, 100 Mbps, or 1 Gbps using the `linespeed` subcommand.

conf t interface mgmtEthernet

Configures the management port. TippingPoint recommends configuring the management port on the IPS to use a non-routed IP address from the RFC 1918 Private Address space. This helps to prevent direct attack on the management port from the Internet. For more management port configuration settings, see "conf t host" on page 37.

Required Privilege

Admin, Super-User

Subcommands

The `conf t interface mgmtEthernet` command uses the following subcommands:

Table 4-17 conf t interface mgmtEthernet subcommands

Subcommand	Description	Usage
`duplex`	Sets the duplex speed to half for full.	`conf t interface mgmtEthernet duplex half` `conf t interface mgmtEthernet full`
`ip`	Sets the IP address for the management Ethernet port. The address can be IPv4 or IPv6. Use CIDR notation to set the subnet mask. The default mask is used when the user specifies a non-CIDR IP address.	`conf t interface mgmtEthernet ip <IP address>`
`ipv6`	Enables or disables IPv6 support on the management port.	`conf t interface mgmtEthernet ipv6`
`ipv6auto`	Enables or disables automatic IPv6 configuration, which allows the device to get an IPv6 address automatically from the subnet router.	`conf t interface mgmtEthernet ipv6auto`
`linespeed`	Sets the line speed. You can set the speed to 10, 100, or 1000.	`conf t interface mgmtEthernet linespeed <speed>`
`negotiate`	Enables or disables auto-negotiate.	`conf t interface mgmtEthernet negotiate` `conf t interface mgmtEthernet no negotiate`
`physical-port`	Specifies the physical port.	`conf t interface mgmtEthernet physical-port <port>`

Table 4-17 conf t interface mgmtEthernet subcommands

Subcommand	Description	Usage
`route`	Sets or removes the default route for the management Ethernet port.	`conf t interface mgmtEthernet route <destination> <gateway IP address or CIDR>` `conf t interface mgmtEthernet no route <destination>`
`vlan`	Specifies the VLAN ID.	`conf t interface mgmtEthernet vlan <vlan ID>`

NOTE: When the auto-negotiate feature is on, the IPS device automatically negotiates the highest common speed and duplex that the IPS and the link partner both support. When the auto-negotiate feature is turned off, users can configure all fiber ports (SFP, SFP+, QSFP+) only to their default settings using the `linespeed` subcommand even though the hardware might list other optional values. The 12 fixed RJ-45 copper ports, however, can be configured to 10 Mbps, 100 Mbps, or 1 Gbps using the `linespeed` subcommand.

conf t interface settings

Enables or disables Medium Dependence Interface (MDI) detection when auto-negotiation is off. These settings do not affect the management port.

NOTE: Changes to the MDI settings do not go into effect until the link is shut down. These settings affect all ports and are not configurable on a port-by-port basis.

Required Privilege

Admin, Super-User

Subcommands

The `conf t interface settings` command uses the following subcommands:

Table 4-18 conf t interface subcommands

Subcommand	Description	Usage
`detect-mdi`	Enables or disables MDI detection.	`conf t interface settings detect-mdi enable` `conf t interface settings detect-mdi disable`
`mdi-mode`	Sets the MDI mode to `mdi` or `mdix`. The default setting is `mdix`. The `mdi` setting has no effect if auto-negotiation is enabled, detect-mdix is enabled, or the port media is fiber.	`conf t interface settings mdi-mode mdi` `conf t interface settings mdi-mode mdix`

conf t lcd-keypad

Enables or disables the keypad and buttons for the LCD keypad.

Required Privilege

Admin, Super-User

Subcommands

The `conf t lcd-keypad` command uses the following subcommands:

Table 4-19 conf t lcd-keypad subcommands

Subcommand	Description	Usage
`backlight`	Sets the intensity of the backlighting in a range from 1 (dimmest) to 100 (brightest).	`conf t lcd-keypad backlight <number>`
`contrast`	Sets the contrast in a range from 1 to 50.	`conf t lcd-keypad contrast <number>`
`disable`	Disables the LCD keypad.	`conf t lcd-keypad disable`
`enable`	Enables the LCD keypad.	`conf t lcd-keypad enable`

conf t log audit

Configures the audit log and the actions that are documented in the log.

Required Privilege

Admin, Super-User

Usage

```
conf t log audit select <activity>
conf t log audit select no <activity>
```

The following activities can be documented in the audit log:

- boot
- compact-flash
- configuration
- conn-table
- device
- general
- high-availability
- host
- host-communications
- ip-filter
- login
- logout
- monitor
- policy
- report
- segment
- server
- slot
- sms
- time
- tse
- update
- user

conf t log snmp-add-event-info

Configures whether the SNMP traps receive additional information, such as the client IP address.

Required Privilege

Admin, Super-User

Usage

```
configure terminal log snmp-add-event-info enable
configure terminal log snmp-add-event-info disable
```

conf t monitor

Enables or disables power supply monitoring and sets hardware monitoring thresholds for IPS disk usage, memory, and temperature values.

Required Privilege

Admin, Super-User

Subcommands

The `conf t monitor` command uses the following subcommands:

Table 4-20 conf t monitor subcommands

Subcommand	Description	Usage
`disable power-supply`	Disables power supply monitoring.	`conf t monitor disable power-supply`
`enable power-supply`	Enables power supply monitoring. If any power supplies experience an interruption, the system logs a critical message in the system log and sends a notification to the SMS if the device is under SMS management.	`conf t monitor enable power-supply`

`threshold`	Sets threshold values for disk usage, memory, and temperature values. Disk and memory thresholds are expressed in percentages, and temperature thresholds are expressed in degrees Celsius.
	• The major threshold value must be set at a value less than the critical threshold value and that allows time to react before a problem occurs.
	• The critical threshold value should generate a warning before a problem causes damage.
		`conf t monitor threshold disk -major <60-100> -critical <60-100>`
		`conf t monitor threshold memory -major <60-100> -critical <60-100>`
		`conf t monitor threshold temperature -major <40-80> -critical <40-80>`

conf t named-ip

Enables you to assign names to IPv4 and IPv6 addresses. A name acts as an alias for the named IPv4 or IPv6 network. In any list where the IP address would normally appear, the network name appears instead. You can also enter the network name in any IP address field.

NOTE: Network names are presentation-only. Any configuration settings are associated with the IP address, and changing the network name does not change the configuration. For example, if the name of IP address `100.23.45.123` is changed from `Corporate` to `Corporate-A`, all configuration settings associated with IP address `100.23.45.123` are retained.

Required Privilege

Admin, Super-User

Subcommands

The `conf t named-ip` command uses the following subcommands:

Table 4-21 conf t named-ip subcommands

Subcommand	Description	Usage
`add`	Adds a new named IP address to the system.	`conf t named-ip add <IP address> <name>`
`delete`	Removes a name.	`conf t named-ip remove <name>`
`modify`	Modifies a name.	`conf t named-ip modify <name>`
`rename`	Renames a named IP address.	`conf t named-ip rename <old name> <new name>`

conf t nms

Configures information for a network management system (NMS). The NMS community string is separate from the string used by SMS. Use `conf t no nms` to disable NMS options.

Required Privilege

Admin, Super-User

Subcommands

The `conf t nms` command uses the following subcommands:

Table 4-22 conf t nms subcommands

Subcommand	Description	Usage
`community`	Sets the NMS community string. The string is limited to 31 characters.	`conf t nms community <string>`

`trap-destination`	Adds or removes an NMS trap IP address. You can also specify a port number with the `-port` option.
	For SNMPv3, the following options are also available:
	• `-user`
	• `-password`
	• `-engine`
	• `-des`
		`conf t nms trap-destination add <IP address> -port <port number>`
		`conf t nms trap-destination remove <IP address>`
		`conf t nms trap destination add <IP address> port <port number> -user <user ID> -password <password> -engine <engine> -des <destination>`

conf t notify-contact

Sets the aggregation period for notification contacts. You must enter the name of an existing notification contact and an aggregation period in minutes.

△ **CAUTION:** Short aggregation periods can significantly affect system performance. The shorter the aggregation period, the heavier the load on the system. In the event of a flood attack, a short aggregation period can lead to system performance problems.

Required Privilege

Admin, Super-User

Usage

```
conf t notify-contact <contact name> <aggregation period>
```

conf t port

Configures the protocols that are permitted on the IPS ports. This command enables the user to specify non-standard TCP/UDP ports to help check for signature matches. The available options include:

- auth
- nstcp
- dnsudp
- finger
- ftp
- http
- imac
- ircu
- ms-sql
- nntp
- pop2
- pop3
- portmappertcp
- portmapperudp
- rlogin
- rsh
- smb
- smtp
- snmptcp
- snmpudp
- ssh
- telnet

Required Privilege

Admin, Super-User

Subcommands

The `conf t port` command uses the following subcommands:

Table 4-23 conf t port subcommands

Subcommand	Description	Usage
`add`	Adds a protocol to a port.	`conf t port <protocol> add <segment><port>`
`delete`	Removes a protocol from a port.	`conf t port <protocol> remove <segment><port>`

conf t profile

Creates, modifies, or deletes security or traffic management profiles.

Required Privilege

Admin, Super-User

Subcommands

The `conf t profile` command uses the following subcommands:

Table 4-24 conf t profile subcommands

Subcommand	Description	Usage
`add-pair`	Adds a port pairing to a profile.	`conf t profile <profile name> add-pair <port pair>`
`client-ip`	Enables or disables a client IP address on a profile.	`conf t profile client-ip enable` `conf t profile client-ip disable`
`delete`	Deletes an existing profile.	`conf t profile <profile name> delete`
`description`	Enters a description string for the profile.	`conf t profile <profile name> description "<description>"`

`deployment`	Sets the deployment mode. Deployment modes offer increased flexibility for filter settings. TippingPoint provides recommended settings customized for different deployment types, including Core, Edge, or Perimeter. Use `show deployment-choices` to see your options.	`conf t profile deployment core`
		`conf t profile deployment edge`
		`conf t profile deployment perimeter`
		`conf t profile deployment default`

`remove-pair`	Removes a port pairing from a profile.	`conf t profile <profile name> remove-pair <port pair>`
`rename`	Renames a profile.	`conf t profile <profile name> rename <new profile name>`
`security`	Creates a security profile. You can add a description string with the `-description` option.	`conf t profile <profile name> security` `conf t profile <profile name> security -description "<description>"`
`traffic-mgmt`	Creates a traffic management profile. You can add a description string with the `-description` option.	`conf t profile <profile name> traffic-mgmt` `conf t profile <profile name> traffic-mgmt -description "<description>"`

conf t protection-settings

Creates global exceptions and apply-only restrictions for Application Protection, Infrastructure Protection, and Performance Protection filters. You must specify the profile to which the settings apply.

Required Privilege

Admin, Super-User

Subcommands

The `conf t protection-settings` command uses the following subcommands:

Table 4-25 conf t protection-settings subcommands

Subcommand	Description	Usage
`app-except`	Adds or removes a global exception for Application Protection and Infrastructure Protection filters.	`conf t protection-settings app-except add <source IP address> <destination IP address> -profile <profile name>` `conf t protection-settings app-except remove <source IP address> <destination IP address> -profile <profile name>`
`app-limit`	Adds or removes an apply-only restriction for Application Protection and Infrastructure Protection filters.	`conf t protection-settings app-limit add <source IP address> <destination IP address> -profile <profile name>` `conf t protection-settings app-limit remove <source IP address> <destination IP address> -profile <profile name>`
`dns-except`	Adds or removes a DNS exception for Application Protection and Infrastructure Protection filters.	`conf t protection-settings dns-except add <DNS> -profile <profile name>` `conf t protection-settings dns-except remove <DNS> -profile <profile name>`
`ip-except`	Adds or removes an IP address exception for Application Protection and Infrastructure Protection filters. This exception applies to source and destination IP addresses.	`conf t protection-settings ip-except add <IP address> -profile <profile name>` `conf t protection-settings ip-except remove <IP address> -profile <profile name>`
`perf-limit`	Adds or removes an apply-only restriction for Performance Protection filters.	`conf t protection-settings perf-limit add <source IP address> <destination IP address> -profile <profile name>` `conf t protection-settings perf-limit remove <source IP address> <destination IP address> -profile <profile name>`

conf t ramdisk

Configures log file synchronization between the RAM disk and the hard disk.

Required Privilege

Admin, Super-User

Options

The `conf t ramdisk` command uses the following options:

Table 4-26 conf t ramdisk subcommands

Option	Description	Usage
`force-sync`	Immediately synchronizes the RAM disk with the hard disk. You can synchronize all files, or specify `alert`, `audit`, `block`, or `sys`.	`conf t ramdisk force-sync all` `conf t ramdisk force-sync <file>`
`sync-interval`	Sets the synchronization interval in seconds. With a value of 0 (zero), all writes are immediately written to the hard disk. With a value of -1, the file is written to the hard disk when a `conf t ramdisk force-sync` command is executed, the device is rebooted or halted, or when the device enters high availability fallback mode. You must specify `alert`, `audit`, `block`, or `sys`.	`conf t ramdisk sync-interval <file>`

conf t remote-syslog

Configures a remote recipient of IPS attack and block messages in syslog format. Many operating systems provide the ability to receive remote syslog messages, and third-party remove syslog packages are also available.

NOTE: Designating a remote syslog server does not automatically send attack and block notifications to that server. You must also select the Remote System Log contact by going to the Filters/Vulnerability filters/Action Sets area in the LSM and either creating or editing an action set. After you apply these changes, active filters that are associated with this action set will send remote messages to the designated server.

CAUTION: Use remote syslog only on a secure, trusted network. Remote syslog, in adherence to RFC 3164, sends clear text log messages using the UDP protocol. It does not offer any additional security protections. You should not use remote syslog unless you can be sure that syslog messages will not be intercepted, altered, or spoofed by a third party.

Required Privilege

Admin, Super-User

Subcommands

The `conf t remote-syslog` command uses the following subcommands:

Table 4-27 conf t remote-syslog subcommands

Subcommand	Description	Usage
`add-event-info`	Enables or disables additional information, including client IP address, on the remote syslog.	`conf t remote-syslog add-event-info enable` `conf t remote-syslog add-event-info disable`
`audit`	Enables or disables remote syslog for the Audit log.	`conf t remote-syslog audit <IP address> -port <port>` `conf t remote-syslog no audit`
`delete`	Deletes a remote syslog collector.	`conf t remote-syslog delete <IP address> -port <port>`
`rfc-format`	Enables or disables RFC format on the remote syslog.	`conf t remote-syslog rfc-format enable` `conf t remote-syslog rfc-format disable`
`quarantine`	Enables or disables remote syslog for the Quarantine log.	`conf t remote-syslog quarantine enable` `conf t remote-syslog quarantine disable`

Table 4-27 conf t remote-syslog subcommands

Subcommand	Description	Usage
`system`	Enables or disables remote syslog for the System log.	`conf t remote-syslog system <IP address> -port <port>` `conf t remote-syslog no system`

`update`	Creates or updates a remote syslog collector. A collector is specified by IP address and port. You also have the option to include a delimiter and facility numbers for alert messages, block messages, and misuse/abuse messages. Facility numbers can be any number from 0-31 inclusive. Delimiter options include `tab`, `comma`, `semicolon`, and `bar`.	`conf t remote-syslog update <IP address> -port <port> -alert-facility <number>`
		`conf t remote-syslog update <IP address> -port <port> -block-facility <number>`
		`conf t remote-syslog update <IP address> -port <port> -misuse-facility <number>`
		`conf t remote-syslog update <IP address> -port <port> -delimiter <character>`

conf t reputation

Configures the behavior of IP Reputation filters. Reputation filters enable you to apply block, permit, or notify actions across an entire reputation group. For specific information about configuring reputation groups, see "conf t reputation group" on page 52.

When an IP address or DNS name is added to a reputation group, it is added to the device's reputation database. Incoming traffic is checked against the database, and the appropriate reputation filters are then applied. While the address or name is being looked up, you can choose to have packets from a suspect address dropped or permitted. The TippingPoint SMS offers additional reputation features; refer to the *Tipping Point Security Management System User Guide* for more information.

If you do not specify a security profile in which to configure the filter, the filter is applied to the Default security profile.

TippingPoint ReputationDV

The TippingPoint ReputationDV is a licensed service that identifies and delivers suspect IPv4, IPv6, and DNS addresses to subscribers. The addresses are tagged with reputation, geographic, and other identifiers for ready and easy security policy creation and management. The service provides the addresses and tags multiple times a day like Digital Vaccines do.

NOTE: While any user can manually create reputation groups and filters, the ReputationDV is available only to users who have licensed the service from TippingPoint. For more information about this service, ask your TippingPoint representative.

Required Privilege

Admin, Super-User

Subcommands

The `conf t reputation` command uses the following subcommands:

Table 4-28 conf t reputation subcommands

Subcommand	Description	Usage
`action-when-pending`	The action that the IPS takes on traffic coming from the specified IP address while the IP reputation filter is caching the address. The default action is `permit`.	`conf t reputation action-when-pending [-profile <security profile name>] permit` `conf t reputation action-when-pending drop [-profile <security profile name>] permit`
`check-dest-address`	Enables or disables action on the traffic destination IP address.	`conf t reputation check-dest-address [-profile <security profile name>] enable` `conf t reputation check-dest-address [-profile <security profile name>] disable`
`check-source-address`	Enables or disables action on the traffic source IP address.	`conf t reputation check-source-address [-profile <security profile name>] enable` `conf t reputation check-source-address [-profile <security profile name>] disable`

`filter`	Configures reputation filters and maps a security profile to a reputation group.
	• `delete-copy`: Deletes a filter.
	• `disable`: Disables a filter without deleting it.
	• `enable`: Enables a filter and maps it to a reputation group.
	The `-threshold` option sets a reputation filter threshold based on the IP reputation information maintained by the TippingPoint TMC. Entries that exceed the TMC-set threshold are acted upon by the IPS.
		`conf t reputation filter <group name> [-profile <security profile name>] delete-copy`
		`conf t reputation filter <group name> [-profile <security profile name>] disable`
		`conf t reputation filter <reputation group name> [-profile <security profile name>] enable [-threshold <number>] -action-set <action set name>`

conf t reputation group

Creates and configures groups of IPv4, IPv6, and DNS addresses and define an action set to apply to all of those addresses. After a group is configured, security profiles can be configured to apply reputation filters to the group.

Required Privilege

Admin, Super-User

Subcommands

The `conf t reputation group` command uses the following subcommands:

Table 4-29 conf t reputation group subcommands

Subcommand	Description	Usage
`add-domain`	Adds a domain to a reputation group.	`conf t reputation group add-domain <name> <domain>`
`add-ip`	Adds an IP address to a reputation group.	`conf t reputation group add-ip <name> <domain>`
`create`	Creates an IP reputation group.	`conf t reputation group create <name> [-description "description of option"]`
`delete`	Deletes an IP reputation group.	`conf t reputation group delete <name>`
`remove-domain`	Removes a domain from a reputation group.	`conf t reputation group remove-domain <name> <domain>`
`remove-ip`	Removes an IP address from a reputation group.	`conf t reputation group remove-ip <name> <domain>`
`rename`	Renames an IP reputation group.	`conf t reputation group rename <old name> <new name>`

conf t segment

Configures and names segments, and also configures the intrinsic network high availability (INHA) action for segments.

On NX-Platform devices, ports are presented in the format *Slot-Segment*. For example, segment 4 on slot 3 would be specified as "3-4".

Privilege

Admin, Super-User

Subcommands

The `conf t segment` command uses the following subcommands:

Table 4-30 conf t segment subcommands

Subcommand	Description	Usage
`high-availability`	Sets the intrinsic network high availability (fallback) option for the segment. If the segment is set to `block`, all traffic through that segment is denied in the fallback state. If the segment is set to `permit`, then all traffic is permitted in the fallback state.	`conf t segment <segment name> high-availability block` `conf t segment <segment name> high-availability permit`

`link-down`	Configures the Link-Down Synchronization mode and timeout length. The following modes are available:
	• `hub`: Ensures the partner port is unaffected when the link goes down.
	• `breaker`: Requires both the port and its partner to be manually restarted when the link goes down.
	• `wire`: Automatically restarts the partner port when the link comes back up.
	Valid range of timeout is 0 to 240 seconds.
		`conf t segment <segment name> link-down hub`
		`conf t segment <segment name> link-down breaker -timeout <seconds>`
		`conf t segment <segment name> link-down wire -timeout <seconds>`

`name`	Defines a name for the segment with a maximum of 32 characters. Set the name to `""` to remove the name from the segment. Names must conform to the following rules: • Can only contain letters A-Z and a-z, digits 0-9, single spaces, periods (.), underscores (_), and dashes (-). • Must include at least one non-digit character. • Cannot begin or end with spaces.	`conf t segment <segment name> name "<segment name>"`
`physical-ports`	Specifies the physical ports.	`conf t interface mgmtEthernet physical-port <port a> <port b>`

Table 4-30 conf t segment subcommands

Subcommand	Description	Usage
`restart`	Restarts a segment.	`conf t segment <segment number> restart`
`sflow`	On NX-Platform devices only, enables or disables sFlow sampling on the specified segment. Specify a sampling rate for <number>.	`conf t segment <segment name> sflow enable <number>` `conf t segment <segment name> sflow disable`

conf t server

Activates and deactivates communications services on your IPS device.

△ **CAUTION:** The `conf t server` command enables you to activate the telnet server and HTTP. Telnet and HTTP are **not** secure services. If you enable telnet and HTTP, you endanger the security of your TippingPoint device. Use SSH instead of telnet and HTTPS instead of HTTP when you are conducting normal operations.

△ **CAUTION:** The SMS requires HTTPS communications. If you turn off the HTTPS server, the SMS cannot manage your TippingPoint device.

Required Privilege

Admin, Super-User

Subcommands

The `conf t server` command uses the following subcommands:

Table 4-31 conf t server subcommands

Subcommand	Description	Usage
`browser-check`	Enables and disables browser checking.	`conf t server browser-check` `conf t server no browser-check`
`http`	Enables and disables HTTP. You must reboot the device after changing HTTP settings.	`conf t server http` `conf t server no http`
`https`	Enables and disables HTTPS. You must reboot the device after changing HTTPS settings.	`conf t server https` `conf t server no https`
`ssh`	Enables and disables SSH.	`conf t server ssh` `conf t server no ssh`
`telnet`	Enables and disables telnet.	`conf t server telnet` `conf t server no telnet`

conf t service-access

Enables and disables a special remote access user login that can be used by a TippingPoint technical support representative to retrieve diagnostic information. This special login functions only if you specifically enable it, and it will be deleted after the technical support representative logs out. If you need technical support again in the future, you must reissue the command.

NOTE: When you issue the configure terminal service-access command, the IPS returns the serial number and a "salt" value. You must retain these numbers for the technical support representative.

To manually disable service access, use the `conf t no service-access` command.

Required Privilege

Super-User

Usage

```
conf t service-access
```

conf t session

Configures the display of the CLI session on your management terminal. Except for the timeout option, configure terminal session commands are not persistent and session changes will be lost when you log out. This command is enabled when the SMS manages the device.

Required Privilege

Admin, Super-User, Super-User only for `timeout`.

Options

The `conf t session` command uses the following options:

Table 4-32 conf t session subcommands

Option	Description	Usage
`columns`	Sets the column width of the terminal session.	`conf t session columns <number of columns>`
`more`	Enables or disables page-by-page output.	`conf t session more` `conf t session no more`
`rows`	Sets the row height of the session.	`conf t session rows <number of rows>`
`timeout`	Sets the inactivity timeout. The `-persist` option applies this value to future sessions for all users as well as the current session.	`conf t session timeout <minutes>` `conf t session timeout <minutes> -persist`
`wraparound`	Enables or disables text-wrapping for long text lines.	`conf t session wraparound` `conf t session no wraparound`

conf t sms

Enables or disables SMS management of the IPS and configures SMS communications.

Required Privilege

Admin, Super-User

Options

The `conf t sms` command uses the following options:

Table 4-33 conf t sms subcommands

Option	Description	Usage
`[no options]`	Enables SMS management.	`conf t sms`
`ip`	Sets the IP address and port of the SMS that will manage the IPS.	`conf t sms ip <IP address> -port <port>`
`must-be-ip`	Enables or disables restriction of SMS management to a specified IP address. Only the SMS with this IP can manage the device.	`conf t sms must-be-ip <IP address or CIDR>` `conf t sms no must-be-ip`
`no`	Disables SMS management.	`conf t no sms`
`v2`	Enables or disables SNMP v2 communication.	`conf t sms v2` `conf t sms no v2`
`v3`	Enables or disables SNMP v3 communication.	`conf t sms v3` `conf t sms no v3`

conf t sntp

Configures SNTP timekeeping options.

△ **CAUTION:** Using external SNTP servers could possibly make your IPS susceptible to a man-in-the-middle attack. It is more secure to use an SNTP server on a local, protected network.

Required Privilege

Admin, Super-User

Options

The `conf t sntp` command uses the following options:

Table 4-34 conf t sntp subcommands

Option	Description	Usage
`[no options]`	Enables SNTP.	`conf t sntp`
`duration`	Sets the interval at which the IPS checks with the time server. A `0` (zero) value causes time to be checked once on boot.	`conf t sntp duration <minutes>`
`no`	Disables SNTP.	`conf t no sntp`

Table 4-34 conf t sntp subcommands

Option	Description	Usage
offset	If the difference between the new time and the current time is equal to or greater than the offset, the new time is accepted by the IPS. A 0 (zero) value forces time to change every time the IPS checks.	conf t sntp offset <seconds>
port	Identifies the port to use for the time server.	conf t sntp port <port>
primary	Sets or removes the IP address of your primary SNTP time server.	conf t sntp primary <IP address> conf t sntp no primary
retries	Sets the number of retries that the device attempts before declaring the SNTP connection is lost.	conf t sntp retries <number>
secondary	Sets or removes the IP address of your secondary SNTP time server.	conf t sntp secondary <IP address> conf t sntp no secondary
timeout	Sets the number of seconds that the device waits before declaring the SNTP connection is lost.	conf t sntp timeout <seconds>

conf t traffic-mgmt

Configures traffic management filters.

Required Privilege

Admin, Super-User

Subcommands

The following subcommands can be used to create or modify an existing traffic management filter. If more than one traffic management profile is defined on the system, you must specify the profile name.

The conf t traffic-mgmt command uses the following subcommands.

△ **CAUTION:** The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

Table 4-35 conf t traffic-mgmt subcommands

Option	Description	Usage
icmp	Creates an ICMP traffic management filter. You can also specify the ICMP type, or use any to apply the filter to all types.	conf t traffic-mgmt icmp [-type <ICMP type>] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]
icmp6	Creates an ICMPv6 traffic management filter. You can also specify the ICMPv6 type, or use any to apply the filter to all types.	conf t traffic-mgmt icmp6 [-type <ICMPv6 type>] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]

Table 4-35 conf t traffic-mgmt subcommands

Option	Description	Usage
`ip`	Creates a IP traffic management filter. You can also specify whether the IP fragments are filtered with the `-ip-frag-only` or `-no-ip-frag-only` options.	`conf t traffic-mgmt ip [-ip-frag-only] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]` `conf t traffic-mgmt ip [-no-ip-frag-only] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]`
`ip6`	Creates an ipv6 traffic management filter. You can also specify whether the IP fragments are filtered with the `-ip-frag-only` or `-no-ip-frag-only` options.	`conf t traffic-mgmt ip6 [-ip-frag-only] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]` `conf t traffic-mgmt ip6 [-no-ip-frag-only] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]`
`tcp`	Creates a TCP traffic management filter. You can also specify the TCP source and destination ports.	`conf t traffic-mgmt tcp [-srcport <TCP port>] [-destport <TCP port>] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]`
`udp`	Creates a UDP traffic management filter. You can also specify the UDP source and destination ports.	`conf t traffic-mgmt udp [-srcport <UDP port>] [-destport <UDP port>] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]`

The following subcommands can be used only to modify an existing traffic management filter. If more than one traffic management profile is defined on the system, you must specify the profile name.

△ **CAUTION:** The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

Table 4-36 conf t traffic-mgmt subcommands

Subcommand	Description	Usage
`allow`	Permits all traffic that fits the named filter.	`conf t traffic-mgmt <filter name> [-profile <profile>] allow`
`block`	Blocks all traffic that fits the named filter.	`conf t traffic-mgmt <filter name> [-profile <profile>] block`
`delete`	Deletes the named filter.	`conf t traffic-mgmt <filter name> [-profile <profile>] delete`

Table 4-36 conf t traffic-mgmt subcommands

Subcommand	Description	Usage
`position`	Changes the priority of the filter.	`conf t traffic-mgmt <filter name> [-profile <profile>] position <number>`
`rate-limit`	Rate-limits and applies the named action set to all traffic that fits the filter.	`conf t traffic-mgmt <filter name> [-profile <profile>] rate-limit <action set name>`
`rename`	Renames the filter.	`conf t traffic-mgmt <filter name> [-profile <profile>] rename`
`trust`	Enables trust of all packets that match the filter.	`conf t traffic-mgmt <filter name> [-profile <profile>] trust`

conf t tse

Configures settings for the Threat Suppression Engine (TSE).

Required Privilege

Admin, Super-User

Subcommands

The `conf t tse` command uses the following subcommands:

Table 4-37 conf t tse subcommands

Subcommand	Description	Usage
`adaptive-filter`	Sets the adaptive filter mode to automatic or manual.	`conf t tse adaptive-filter mode automatic` `conf t tse adaptive-filter mode manual`
`afc-severity`	Sets the severity of messages logged by the Adaptive Filter Configuration (AFC). Options include: • `critical` • `error` • `warning` • `info`	`conf t tse afc-severity <severity>`
`asymmetric-network`	Enables or disables asymmetric mode for the TSE. Use asymmetric mode if your network uses asymmetric routing.	`conf t tse asymmetric-network enable` `conf t tse asymmetric-network disable`
`congestion`	Enables or disables notification when traffic congestion reaches a defined threshold.	`conf t tse congestion notify enable -threshold <threshold>` `conf t tse congestion notify disable`

Table 4-37 conf t tse subcommands

Subcommand	Description	Usage

`connection-table`	Sets the timeout for the connection tables.
	• `non-tcp-timeout`: Defines the timeout for non-TCP connections. The range is 30 to 1800 seconds.
	• `timeout`: Defines the global connection table timeout. The range is 30 to 1800 seconds.
	• `trust-timeout`: Defines the timeout for the trust table. The range is 30 to 1800 seconds.
		`conf t tse connection-table non-tcp-timeout <seconds>`
		`conf t tse connection-table timeout <seconds>`
		`conf t tse connection-table trust-timeout <seconds>`

`gzip-compression`	Enables or disables GZIP decompression.	`conf t tse gzip-compression enable` `conf t tse gzip-compression disable`

`http-encoded-resp`	Specifies inspection of encoded HTTP responses.
	• `accelerated`: Hardware acceleration is used to detect and decode encoded HTTP responses.
	• `inspect`: Enables strict detection and decoding of HTTP responses.
	• `ignore`: The device does not detect or decode HTTP responses.
		`conf t tse http-encoded-resp accelerated`
		`conf t tse http-encoded-resp inspect`
		`conf t tse http-encoded-resp ignore`

`ids-mode`	Enables or disables IDS mode. When enabled, IDS mode configures the device to operate in a manner similar to an Intrusion Detection System (IDS). • Performance protection is disabled. • Adaptive Filtering mode is set to Manual. • Filters currently set to Block are not switched to Permit, and Block filters can be still be set. **NOTE:** IDS mode becomes disabled if you manually enable performance protection or set Adaptive Filtering mode to Automatic.	`conf t tse ids-mode enable` `conf t tse ids-mode disable`

Table 4-37 conf t tse subcommands

Subcommand	Description	Usage
`logging-mode`	Sets the logging mode: • `conditional`: Improves performance by turning off alert/block logging when the device experiences a specified amount of congestion. This feature is enabled by default. The `-threshold` setting defines the percentage of packet loss that turns off logging. The `-period` setting sets the length of time logging remains off. • `unconditional`: The device always logs alerts and blocks, even if traffic is dropped under high load.	`conf t tse logging-mode conditional -threshold <percentage> -period <seconds>` `conf t tse logging-mode unconditional`
`quarantine`	Sets the quarantine duration. The range is 1 to 1440 minutes.	`conf t tse quarantine <minutes>`
`sflow`	On NX-Platform devices only, enables or disables global sFlow.	`conf t tse sflow disable` `conf t tse sflow enable`
`sflow collector`	On NX-Platform devices only, adds or removes collector IP address. You must manually enable the collector IP address that you add. Two collector IP addresses (either IPv4 or IPv6) are supported for TOS V. 3.6.	`conf t tse sflow collector add <IP Address> <optional Port>` `conf t tse sflow collector remove <IP Address> <optional Port>`

conf t user

Manages user accounts. This command is enabled when the device is managed by an SMS. For more information about editing user options, see "conf t user options" on page 65.

Required Privilege

Super-User

NOTE: All users can modify their own passwords. Only the super-user can execute other commands on user accounts.

Subcommands

The `conf t user` command uses the following subcommands.

NOTE: Do not use quotation marks in passwords. Quotation marks are treated differently depending on how you enter them and where you place them within a password and can lead to confusion when attempting to log in to the TippingPoint device.

Table 4-38 conf t user subcommands

Subcommand	Description	Usage
`add`	Adds a user. Requires the following options: • `name`: Login name. Maximum of 31 characters. • `role`: Privilege level. Privileges can be `operator`, `administrator`, or `super-user`. • `password`: Password. Maximum 32 characters. If you do not create a password, you will be asked if you want to do so. • `-tech-support`: Enables the Technical Support Landing Page when the user logs in to the LSM. (TippingPoint 10 only)	`conf t user add <username> -password <password> -role <role>`
`enable`	Enables a user account that has been disabled due to lockout or expiration.	`conf t user enable <username>`

Table 4-38 conf t user subcommands

Subcommand	Description	Usage
`modify`	Modifies the named user. Requires one or more of the following options: • `role`: Privilege level. Privileges can be `operator`, `administrator`, or `super-user`. • `password`: Password. Maximum 32 characters. • `-tech-support`: Enables the Technical Support Landing Page when the user logs in to the LSM. (TippingPoint 10 only)	`conf t user modify <username> -password <password> -role <role>`
`remove`	Removes a user login.	`conf t user remove <username>`

conf t user options

Enables you to view or change the security options for all user accounts on the TippingPoint device. If you use `conf t user options` without any options, it displays the current settings.

Security Levels

Security levels are defined as follows:

- Level 0: User names cannot contain spaces. Passwords are unrestricted.
- Level 1: User names must contain at least 6 characters without spaces. Passwords must contain at least 8 characters without spaces.
- Level 2: Includes Level 1 restrictions and requires the following:
  - 2 alphabetic characters
  - 1 numeric character
  - 1 non-alphanumeric character (special characters such as ! ? and *).

Required Privilege

Super-User

Subcommands

The `conf t user options` command uses the following subcommands:

Table 4-39 conf t user options subcommands

Subcommand	Description	Usage
`attempt-action`	Specifies the action to take when the maximum number of login attempts is reached. • `disable`: Requires a super-user to re-enable the user. • `lockout`: Prevents the user from logging in for the lockout-period. • `notify`: Posts a notification to the audit log.	`conf t user option attempt-action disable` `conf t user option attempt-action lockout`

`expire-action`	Specifies the action to take when a user account expires.
	• `disable`: Disables the account.
	• `expire`: Expires the account.
	• `notify`: Audits the expiration to the audit log.
		`conf t user option expire-action disable`
		`conf t user option expire-action expire`
		`conf t user option expire-action notify`

`expire-period`	Sets the number of days before a password expires. Valid values are 0, 10, 20, 30, 45, 90, 332, and 365. With a value of 0, passwords do not expire.	`conf t user option expire-period <value>`
`lockout-period`	Sets the number of minutes that a user is locked out after the maximum number of unsuccessful login attempts.	`conf t user option lockout-period <value>`

Table 4-39 conf t user options subcommands

Subcommand	Description	Usage
`max-attempts`	Sets the maximum number of login attempts that are permitted before the action specified in `attempt-action` takes place. Valid values are integers between 1 and 10, inclusive.	`conf t user option max-attempts <value>`
`security-level`	Sets the security level for user names and passwords. Valid values are integers between 0 and 2 inclusive. See "Security Levels" on page 65.	`conf t user option security-level <value>`

conf t virtual-port

Configures the network virtual ports.

Required Privilege

Admin, Super-User

Subcommands

The `conf t virtual-port` command uses the following subcommands.

△ **CAUTION:** The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

Table 4-40 conf t virtual-port subcommands

Subcommand	Description	Usage
`add-row`	Configures the physical port, VLAN ID, and CIDR associated with a virtual port. Leaving an option blank sets the value to `any`.	`conf t virtual-port <port name> add-row -port-list <physical port> -vlan-list <VLAN ID> -cidr-list <CIDR address>`
`create`	Creates a virtual port and assigns a name. The maximum number of characters is 32. Spaces are not allowed. Use the `-description` option to add a description.	`conf t virtual-port <name> create [-description "<description>"] <zones>`
`delete`	Deletes a virtual port.	`conf t virtual-port <name> delete`
`description`	Enters a description of the virtual ports.	`conf t virtual-port <name> description "<description>"`
`remove-row`	Removes the physical port, VLAN, and CIDR associated with a virtual port, resetting its values to `any`.	`conf t virtual-port <port name> remove-row`
`rename`	Changes the name of the virtual ports.	`conf t virtual-port <name> rename <new name>`
`zones`	Sets the physical port list and VLAN list for a virtual port.	`conf t virtual-port <name> zones <VLAN range>`

conf t virtual-segment

Configures, updates, or deletes network virtual segments.

Required Privilege

Admin, Super-User

Subcommands

The `conf t virtual-segment` command uses the following subcommands.

△ **CAUTION:** The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

Table 4-41 conf t virtual-segment subcommands

Subcommand	Description	Usage
`delete`	Deletes a virtual segment.	`conf t virtual-segment <incoming virtual port> <outgoing virtual port> delete`
`position`	Sets the precedence of a virtual segment. Assigning a position of 1 gives the segment topmost precedence.	`conf t virtual-segment <incoming virtual port> <outgoing virtual port> [-position <position in list>]`
`update`	Creates, moves, or edits a virtual segment.	`conf t virtual-segment <incoming virtual port> <outgoing virtual port> update`

conf t vlan-translation

Adds or removes a VLAN translation setting. For detailed information about the concepts behind VLAN translation, refer to the *TippingPoint Local Security Manager User's Guide V. 3.6* or to the LSM online Help. Use the `-auto-reverse` flag to automatically create a reverse VLAN translation.

Required Privilege

Admin, Super-User

Usage

```
conf t vlan translation add <incoming VLAN ID> <outgoing VLAN ID>
conf t vlan translation add <incoming VLAN ID> <outgoing VLAN ID>
-auto-reverse
conf t vlan translation remove <incoming VLAN ID> <outgoing VLAN ID>
```

debug

Most debug commands should be used only when you are instructed to do so by TippingPoint technical support. The following commands can be used to improve performance or diagnose network traffic:

debug information

The debug information commands display process and CPU Utilization information. To configure utilization statistics collection, see "conf t cpu-utilization" on page 33.

Required Privilege

Super-User

Subcommands

The `debug information` command uses the following subcommands:

Table 4-42 debug information subcommands

Subcommand	Description	Usage
`dp-ps`	Lists all processes.	`debug information dp-ps`
`ticks`	Lists the number of processes currently running in the control and data planes, the maximum CPU usage, and the average CPU usage. The following options provide more information: • `-details`: Provides a more detailed list of processes and CPU usage. • `-tiers`: Lists processes and CPU usage by tier.	`debug information ticks`

debug np best-effort

Best Effort mode protects latency-sensitive applications on the network by shunting permitted traffic packets. When the latency reaches the user-defined threshold, permitted traffic is shunted until latency falls to the user-defined recovery percentage.

NOTE: Best Effort Mode is not available on the TippingPoint 10, 110, and 330.

Required Privilege

Super-User

Subcommands

The `debug np best-effort` command uses the following subcommands:

Table 4-43 debug best-effort-mode subcommands

Subcommand	Description	Usage
`enable`	Enables Best Effort mode.	`debug np best-effort enable [-queue-latency <microseconds>] [-recover-percent <percent>]`
`disable`	Disables Best Effort mode.	`debug np best-effort disable`

Options

The `debug np best-effort` command uses the following options:

Table 4-44 debug np best-effort options

Subcommand	Description	Usage
`-queue-latency`	Defines the latency threshold at which Best Effort mode is entered. The default is 1000 microseconds.	`debug np best-effort enable -queue-latency <microseconds>`
`-recover-percent`	Defines the recovery percentage at which Best Effort mode is exited. The default is 20%; if the latency threshold is 1000 microseconds, the device exits Best Effort mode when latency drops to 200 microseconds (20% of 1000).	`debug np best-effort enable -recover-percent <percent>`

debug np mcfilt-regex

The debug microfilter commands display or clear microfilter regular expression statistics.

Required Privilege

Super-User

Subcommands

The `debug np mcfilt-regex` command uses the following subcommands:

Table 4-45 debug mcfilt-regex subcommands

Subcommand	Description	Usage
`clear`	Clears microfilter regular expression statistics.	`debug np mcfilt-regex clear`
`show`	Displays microfilter regular expression statistics.	`debug np mcfilt-regex show`

debug reputation

The debug reputation commands are used to manage the IP reputation cache and database. For more information about reputation, see "conf t reputation" on page 51 and "conf t reputation group" on page 52.

Required Privilege

Super-User

Subcommands

The `debug reputation` command uses the following subcommands:

Table 4-46 debug reputation subcommands

Subcommand	Description	Usage
`clear-caches`	Clears the reputation caches.	`debug reputation clear-caches`
`show-cache-stats`	Shows the reputation cache statistics.	`debug reputation show-cache-stats`

debug snmp trap

The SNMP trap feature enables you to test SNMP trap functionality for NMS devices.

Required Privilege

Super-User

Subcommands

The `debug snmp trap` command uses the following subcommands:

Table 4-47 debug snmp trap subcommands

Subcommand	Description	Usage
`list-ID`	Lists all the SNMP traps and their object identifiers (OIDs) on a given IPS device.	`debug snmp trap list-ID`
`test`	Sends a test SNMP trap request for the specified OID to an NMS server. **NOTE:** Before using this command, configure the NMS server using the `conf t nms trap-destination add <IP address> -port <port number>` command. Alternatively, configure the NMS server by selecting **System > SMS/NMS** from the LSM menu.	`debug snmp trap test <trap-ID>`

debug traffic-capture

The traffic capture feature enables you to capture a selection of traffic received by the device, including traffic that triggers filters and traffic that does not trigger any filters. You can capture up to 10,000,000 packets, 10 MB (10,000,000 bytes), or 100 files of IPv4 and IPv6 traffic. The traffic capture files are saved on the external storage card.

NOTE: When a traffic capture is close to filling the storage card, the traffic capture will stop and a warning message is recorded in the system log.

Required Privilege

Super-User

Subcommands

The `debug traffic-capture` command uses the following subcommands.

CAUTION: The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

Table 4-48 debug traffic-capture subcommands

Subcommand	Description	Usage
`list`	Returns a list of all traffic captures currently saved on the IPS.	`debug traffic-capture list`
`remove`	Removes a saved traffic capture. Use the `-f` flag to force the removal of the file when a traffic capture is in progress.	`debug traffic-capture remove <traffic capture filename>` `debug traffic-capture remove -f <traffic capture filename>`
`start`	Initiates a traffic capture. This subcommand can be used in conjunction with the options or with an expression.	`debug traffic-capture start [-c <number of packets>] [-C <file size>] [-i <virtual segment>] [-w <file>] <expression>`
`stop`	If only one traffic capture is currently in progress, terminates the traffic capture in progress. If two or more traffic captures are currently in progress, you must specify a filename.	`debug traffic-capture stop` `debug traffic-capture stop <filename>`
`stop-all`	Stops traffic captures currently in progress.	`debug traffic-capture stop-all`

Options

The `debug traffic-capture start` command uses the following options:

Table 4-49 debug traffic-capture start options

Subcommand	Description	Usage
`-c`	Defines the number of packets at which the traffic capture will stop. The default is 100.	`debug traffic-capture start -c <number of packets>`
`-C`	Defines the capture file size at which the traffic capture will stop. The size is defined in bytes. The default is 100000.	`debug traffic-capture start -C <file size>`
`-i`	Sets the virtual segment on which the traffic will be captured. The default is to capture on all segments. The segment should be defined with the syntax `1A-1B`.	`debug traffic-capture start -i <virtual segment> <expression>`
`-w`	Defines a name for the traffic capture file. Do not include an extension; the TOS will automatically append one. The default file name is the date and time at which the traffic capture was initiated, in the format `YYYYMMDD-HHMMSS.pcap`.	`debug traffic-capture start -w <file>`

Expression Usage

Traffic capture expressions are used to narrow down the types of traffic that are captured. This feature supports true tcpdump expressions. For more information about expression usage, refer to "TCPDUMP Expressions" on page 87. The expression must be enclosed in straight quotes (`'`).

Examples

To capture only TCP traffic, enter the following command:

```
debug traffic-capture start 'tcp'
```

To capture all traffic to and from IP address 172.31.255.254, enter:

```
debug traffic-capture start 'host 172.31.255.254'
```

To capture all traffic from that address, enter:

```
debug traffic-capture start 'src 172.31.255.254'
```

To capture all traffic to that address, enter:

```
debug traffic-capture start 'dst 172.31.255.254'
```

To capture all traffic from that address to IP address 10.10.10.10, enter:

```
debug traffic-capture start 'src 172.31.255.254 and dst 10.10.10.10'
```

The following, more complex example captures IPv4 HTTP packets on virtual segment 3A-3B that are transmitting to and from port 80, and only includes packets that contain data. SYN, FIN, and ACK packets are excluded.

```
debug traffic-capture start -i 3A-3B 'tcp port 80 and
(((ip[2:2] - ((ip[0]&0xf)<<2)) - ((tcp[12]&0xf0)>>2)) != 0)'
```

fips

Manages FIPS authentication and key information. For information on enabling FIPS mode, see "conf t host" on page 37.

Required Privilege

Super-User

Subcommands

The `fips` command uses the following subcommands.

△ **CAUTION:** The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

Table 4-50 fips subcommands

Subcommand	Description	Usage
`auth delete`	Reboots the device and wipes out the user database. Use the `-add` and `-password` options to create a new default super user. If you do not specify a username and password, you will be forced to create one via the serial port terminal when the device reboots. • `-add`: Defines the new default super-user name. • `-password`: Creates a password for the user. If you specify an asterisk (`*`) for the password, you will be prompted for the password.	`fips auth delete` `fips auth delete -add <user name> -password <password>`
`keys`	Manages generated keys and SSL keys. You must specify two options for managing SSL keys. The first option specifies what to do with the generated keys: • `keep`: Saves the keys when the box is rebooted. • `generate`: Generates a new key on reboot. • `delete`: Deletes the generated keys on reboot. The second option specifies the action for the authorized SSL key that was originally obtained with the device. This option does not take effect until after a reboot. • `keep`: Saves the key. • `delete`: Deletes the default key. • `restore-default`: Restores the default key.	`fips keys <keep/generate/delete> <keep/delete/restore-default>`
`restore-ssl`	Restores the default SSL key.	`fips restore-ssl`

halt

Shuts down the IPS device. Use the `now` option to shut the device down immediately. You can also enter 1 to 3600 seconds for the IPS to wait before initiating the halt sequence. You will be prompted to confirm that you want to halt the device.

Required Privilege

Admin, Super-User

Usage

```
halt now
halt <seconds>
```

high-availability

Either forces the system into layer-2 fallback (also known as Intrinsic HA), or returns it to normal mode (inspection). Although layer-2 fallback is a system-wide setting, you can configure whether traffic is permitted (default) or blocked on a segment-by-segment basis using the `conf t segment high-availability` command.

This command can also control any bypass modules or zero-power HA devices used by the device.

Required Privilege

Admin, Super-User

Subcommands

The `high-availability` command uses the following subcommands.

△ **CAUTION:** The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

Table 4-51 high-availability subcommands

Subcommand	Description	Usage
`force`	The `fallback` option forces the TippingPoint into fallback or Intrinsic Network High Availability (INHA) mode. The `normal` option causes the TippingPoint to return to normal (non-INHA) operation.	`high-availability force fallback` `high-availability force normal`

`zero-power`	Forces a ZPHA module into one of two modes:
	• `normal`: Traffic passes through the IPS.
	• `bypass`: Traffic bypasses the IPS.
	With no options specified, this command affects the external ZPHA module. Use the `-segment` option to set the mode of a Smart ZPHA module. Use the `-slot` option to set the mode for bypass I/O modules (BIOMs). A ZPHA module can be one of the following:
	• An external module connected to the device through the ZPHA interface.
	• A Smart ZPHA module on the 2500N, 5100N, or 6100N.
	• A BIOM in the NX-platform models.
		`high-availability zero-power bypass-ips [-segment <segment name>]`
		`high-availability zero-power no bypass-ips [-segment <segment name>]`
		`high-availability zero-power bypass-ips [-slot <slot number>]`
		`high-availability zero-power no bypass-ips [-slot <slot number>]`
		`high-availability zero-power bypass-ips [-all]`
		`high-availability zero-power no bypass-ips [-all]`

ping

Tests whether a particular IP address can be reached and how long it takes to receive a reply. You can specify an IP address and a number of packets to send. You can send 1 to 9,999 packets.

Required Privilege

Admin, Super-User

Options

The `ping` command uses the following options:

Table 4-52 ping subcommands

Option	Description	Usage
`-q`	Suppresses statistics	`ping <IP address> <packet count> -q`
`-v`	Returns verbose results.	`ping <IP address> <packet count> -v`
`-4`	IPv4 traffic only.	`ping <IP address> <packet count> -4`
`-6`	IPv6 traffic only.	`ping <IP address> <packet count> -6`

quarantine

Manages the quarantined traffic and IP addresses.

Required Privilege

Admin, Super-User

Subcommands

The `quarantine` command uses the following subcommands:

Table 4-53 quarantine subcommands

Subcommand	Description	Usage
`add`	Adds an IP address to the quarantine list. You can also enter an action set that applies to all traffic from that IP address.	`quarantine add <IP address> <action set name>`
`empty`	Flushes the quarantine list of all IP addresses.	`quarantine empty`
`list`	Displays a list of quarantined IP addresses. You can filter the addresses with the `filter` subcommand and an IP string, and you can use `*` as a wildcard, as in `100.*.*.*`.	`quarantine list` `quarantine list filter <IP address>`
`remove`	Removes an IP address from the quarantine list.	`quarantine remove <IP address>`

reboot

Reboots the device. You can specify a delay before the device reboots or execute the reboot immediately. Specify a full system restart with the `-full` flag.

Required Privilege

Admin, Super-User

Usage

```
reboot
reboot <0-3600>
reboot -full
```

setup

Runs the configuration wizard. For more information about the configuration wizard, refer to "Initial Configuration" on page 7. You can also use this command to run specific sections of the configuration wizard.

Required Privilege

Super-User; Super-User and Administrator for setup email-default

Subcommands

The `setup` command uses the following subcommands:

Table 4-54 setup subcommands

Subcommand	Description	Usage
`email-default`	Configures the default email contact.	`setup email-default`
`ethernet-port`	Configures the ethernet ports.	`setup ethernet-port`
`host`	Configures the management port.	`setup host`
`servers`	Configures Web, CLI, and SNMP servers.	`setup servers`
`sms`	Restricts SMS to a specified IP address.	`setup sms`
`time`	Configures time management.	`setup time`
`vlan-translation`	Configures VLAN translation.	`setup vlan-translation`

show

Displays the current status of hardware and software components. To view the information in the current configuration files, use the `show configuration` command. See "show configuration" on page 81.

Required Privilege

Admin, Operator, Super-User

NOTE: Only users with Super-User role can use the `show log audit` command.

Subcommands

The `show` command uses the following subcommands.

CAUTION: The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

Table 4-55 show subcommands A-M

Subcommand	Description	Usage
`action-sets`	Displays all action sets with their settings and contacts.	`show action-sets`
`arp`	Displays the link level ARP table.	`show arp`
`autodv`	Displays the state of the automatic DV feature.	`show autodv`
`clock`	Displays the time and timezone for the internal clock.	`show clock` `show clock -details`
`compact-flash`	Displays whether the storage card is mounted, and if so, its model number, serial number, revision number, capacity, operation mode, and mount status.	`show compact-flash`

Table 4-55 show subcommands A-M

Subcommand	Description	Usage
`default-alert-sink`	Displays the to and from addresses and SMTP settings for the default alert sink.	`show default-alert-sink`
`default-gateway`	Displays the IP address of the default gateway.	`show default-gateway`
`deployment-choices`	Displays the deployment modes available for the device.	`show deployment-choices`
`dns`	Displays the DNS that the device is using.	`show dns`
`filter`	Displays the filter information. Specify the filter by number.	`show filter <number>`
`fips`	Displays FIPS and key information. Use the `-details` option for more information.	`show fips` `show fips -details`

`health`	Displays the disk space, memory usage, power supply status, temperature, fans, I2C bus timeouts, and voltage of the device.	`show health`
		`show health disk-space`
		`show health fan`
		`show health i2c-bus`
		`show health memory`
		`show health power-supply`
		`show health temperature`
		`show health voltage`

`high-availability`	Displays the current HA status. On NX-platforms, the status of each module slot is displayed as being either `normal` or `IPS bypass`.	`show high-availability`
`host`	Displays the host management port configurable options and the current settings. Use the `-details` option for more information.	`show host` `show host -details`
`inspection-bypass`	Displays the inspection bypass rules.	`show inspection-bypass` `show inspection-bypass -details]`
`interface`	Displays network interface data. Specify one of the following: • `mgmtEthernet`: Management interface. • `ethernet`: Port specifier (1A, 1B, etc.).	`show interface mgmtEthernet` `show interface ethernet`
`license`	Shows the license status for the TOS, Digital Vaccine, and IP Reputation.	`show license`

Table 4-55 show subcommands A-M

Subcommand	Description	Usage

`log`	Displays a log file. Only users with super-user privileges can view the audit log.	`show log alert`
		`show log audit`
		`show log block`
		`show log quarantine`
		`show log summary`
		`show log system`

`mfg-info`	Displays manufacturing information, including the device serial number and MAC address.	`show mfg-info`

Table 4-56 show subcommands N-Z

Subcommand	Description	Usage

`np`	Displays the network processor statistic sets.	`show np engine`
		`show np engine filter`
		`show np engine packet`
		`show np engine parse`
		`show np engine reputation dns`
		`show np engine reputation ip`
		`show np engine rule`
		`show np general`
		`show np general statistics`
		`show np mcfilt-rule-stats`
		`show np protocol-mix`
		`show np reassembly`
		`show np reassembly ip`
		`show np reassembly tcp`
		`show np rule-stats`
		`show np softlinx`
		`show np tier-stats`

`policy counters`	Displays the counters for Total, Invalid, Alert, and Blocked.	`show policy counters`
`profile`	Displays detailed information about a named profile. Enclose the name of the profile in quotes "".	`show profile "<profile name>"`
`protection-settings`	Displays category settings.	`show protection-settings -profile <profile name>`
`ramdisk`	Displays the RAM disk status.	`show ramdisk files` `show ramdisk stats`
`rate-limit-speeds`	Displays all valid rate limit speeds.	`show rate-limit-speeds`

Table 4-56 show subcommands N-Z

Subcommand	Description	Usage

`reputation`	Displays the reputation groups and filters.	`show reputation`
		`show reputation filter <filter name>`
		`show reputation groups`

`reputation lookup`	Looks up an address in the reputation database.	`show reputation lookup <IP address>`
`routes`	Displays the configured routes.	`show routes`
`server`	Displays the servers running on the device.	`show servers`
`service-access`	Displays the status of service access to the device.	`show service-access`
`session`	Displays the current session settings.	`show session`
`slot`	Displays slot configuration, including the module type currently in the slot.	`show slot`
`sms`	Indicates whether an SMS is managing the device and displays information about the SMS.	`show sms`
`sntp`	Displays the current SNTP settings.	`show sntp`
`timezones`	Displays the available time zones.	`show timezones`
`traffic-mgmt`	Displays all traffic management filters defined in a traffic management profile. You must specify the profile by name unless there is only one profile on the device.	`show traffic-mgmt -profile <profile name>`

`tse`	Displays information and settings regarding the Threat Suppression Engine.	`show tse adaptive-filter top-ten`
		`show tse connection-table blocks`
		`show tse connection-table timeout`
		`show tse connection-table trusts`
		`show tse rate-limit streams`

`user`	Displays the user login accounts on the TippingPoint device.	`show user` `show user -details`
`version`	Displays the version of the TOS software running on the IPS device.	`show version`
`virtual-port`	Displays information about a virtual port.	`show virtual-port <port number>`
`virtual-segments`	Displays all of the virtual segments configured on the device.	`show virtual-segments`

show configuration

Shows persistent configuration settings on the IPS. Show configuration commands can be used to feed configuration information back to the console. Without options, the command shows the system's configuration.

TIP: You can use the abbreviation `show conf`. Also, you can define an alias using the `alias` command.

Required Privilege

Admin, Operator, Super-User

Subcommands

The `show configuration` command uses the following subcommands:

Table 4-57 show configuration subcommands

Subcommand	Description	Usage
`action-set`	Lists all action sets that have been defined for this device. You can also view a single action set by specifying the action set name.	`show conf action-set` `show conf action-set <action set name>`
`authentication`	Displays the remote authentication configuration.	`show conf authentication`
`autodv`	Shows configuration settings for the automatic update service for Digital Vaccine packages.	`show conf autodv`
`category-settings`	Shows configuration settings for filter categories. You can also view the settings for a single profile by specifying the profile name.	`show conf category-settings` `show conf category-settings -profile <profile name>`
`clock`	Shows time zone and daylight savings time settings.	`show conf clock`
`compact-flash`	Shows the storage card operation mode.	`show conf compact-flash`
`default-alert-sink`	Shows the default email address to which attack alerts will be directed.	`show conf default-alert-sink`
`default-gateway`	Shows the device default gateway.	`show conf default-gateway`
`email-rate-limit`	Shows the maximum number of email notifications the system sends every minute. The minimum is 1; the maximum is 35.	`show conf email-rate-limit`
`filter`	Shows the filter data for a specific filter, identified by filter number.	`show conf filter <number>`
`high-availability`	Shows high availability configuration settings.	`show conf high-availability`
`host`	Shows the host name and location.	`show conf host`
`inspection-bypass`	Shows the current inspection bypass rule configuration.	`show conf inspection-bypass`

Table 4-57 show configuration subcommands

Subcommand	Description	Usage

`interface`	When used without qualifiers, shows configuration of all ports.
	• `ethernet`: Shows Ethernet port information. Without options, this subcommand shows the status of all Ethernet ports. Use port specifiers (1A, 2A, etc.) to view the status of a single port.
	• `mgmtEthernet`: Shows Management Ethernet port information.
	• `settings`: Shows the persistent configuration settings for MDI-detection.
		`show conf interface`
		`show conf interface ethernet`
		`show conf interface mgmtEthernet`
		`show conf interface settings`

`lcd-keypad`	Shows the configuration setting for the LCD keypad.	`show conf lcd-keypad`

`log`	Shows log configuration.	`show conf log`
		`show conf log audit-log`
		`show conf log snmp-add-event-info`

`monitor`	Shows the persistent configuration of monitor thresholds.	`show conf monitor`
`nms`	Shows the NMS settings.	`show conf nms`
`notify-contacts`	Shows the notification contacts and settings.	`show conf notify-contacts`
`port`	Shows the configuration of all ports on the IPS.	`show conf port`
`profile`	Lists all profiles that have been configured on the device. You can view an individual profile by including the profile name.	`show conf profile` `show conf profile <profile name>`
`protection-settings`	Shows the protection settings. You can also view the settings for a single profile by specifying the profile name.	`show conf protection-settings` `show conf protection-settings -profile <profile name>`
`ramdisk`	Shows the RAM disk configuration.	`show conf ramdisk`
`remote-syslog`	Shows the remote syslog configuration and the IP address of the remote log.	`show conf remote-syslog`

`reputation`	Shows the configuration of reputation filters and groups, and of the IP Reputation feature.	`show conf reputation`
		`show conf reputation group`
		`show conf reputation filter`

`segment`	Shows the segment configuration. You can view an individual segment by including the segment name.	`show conf segment` `show conf segment <segment name>`

Table 4-57 show configuration subcommands

Subcommand	Description	Usage
server	Shows the device server configuration.	show conf server
service-access	Shows whether service access is enabled or disabled.	show conf service-access
session	Shows the session timeout settings. Use show session to view the current session configuration.	show conf session
sms	Shows if SMS is enabled and other SMS configuration settings.	show conf sms
sntp	Shows the SNTP configuration.	show conf sntp
traffic-mgmt	Shows the traffic management configuration.	show conf traffic-mgmt
tse	Shows the TSE information, including connection table timeout, sFlow (NX-platform devices only), asymmetric network setting, adaptive aggregation threshold, adaptive filter mode, and IDS mode.	show conf tse
user	Shows user options. Use the -details option to view additional information.	show conf user show conf user -details
virtual-port	Shows virtual port configuration. To show the configuration of a specific virtual port, specify the virtual port name.	show conf virtual-port show conf virtual-port <virtual port name>
virtual-segments	Shows the configuration of the virtual segments.	show conf virtual-segments
vlan-translation	Shows the VLAN translation configuration	show conf vlan-translation

snapshot

Creates and manages snapshots of the device configuration settings. These snapshots can be applied to other devices, to roll back to previous configurations, and to back up the current configuration.

Required Privilege

Admin, Super-User

Subcommands

The snapshot command uses the following subcommands:

Table 4-58 snapshot subcommands

Subcommand	Description	Usage
create	Creates a snapshot with the given name.	snapshot create <snapshot name>
list	Lists all snapshots saved on the device.	snapshot list

Table 4-58 snapshot subcommands

Subcommand	Description	Usage
`remove`	Deletes the named snapshot.	`snapshot remove <snapshot name>`
`restore`	Replaces the current configuration settings with the settings in the named snapshot. This process can take some time and will require a reboot of the device.	`snapshot restore <snapshot name>`

Options

The `snapshot` command uses the following options:

NOTE: Including Reputation addresses and Reputation DV can generate a very large snapshot file.

Table 4-59 snapshot options

Subcommand	Description	Usage
`-include-reputation`	When this flag is included in the command, the snapshot includes the files from the Reputation DV package in the snapshot.	`snapshot create -include-reputation`
`-include-manual-entries`	When this flag is included in the command, the snapshot includes the user-defined IP and DNS reputation entries in the snapshot.	`snapshot create -include-manual-entries`
`-include-network`	When this flag is included in the command, the snapshot includes management port configuration information.	`snapshot create -include-network`
`-exclude-network`	When this flag is included with the `snapshot restore` command, the snapshot excludes management port configuration information during the restore process.	`snapshot create -exclude-network`

tech-support-report

Polls the IPS for statistics and other relevant information and sends the information as a clear-text email message to the specified TippingPoint Technologies email address. You should execute this command only when requested by TippingPoint support personnel.

Use the `-include-snapshot` option to include a system snapshot in the report.

The command can take up to a minute to execute. The default email options must be configured with the `setup` command for the email transfer to succeed.

NOTE: This command is used only on the TippingPoint 10.

Required Privilege

Admin, Super-User, Operator

Usage

```
tech-support-report <email address> "<description>"
tech-support-report <email address> "<description>" -include-snapshot
```

A TCPDUMP Expressions

The debug traffic capture command uses tcpdump expressions to define the traffic captures. The following information is taken from the TCPDUMP man page maintained at http://www.tcpdump.org/. Refer to that site for the most recent version of this documentation.

TCPDUMP

Section: User Commands (1)

Updated: 05 March 2009

Index Return to Main Contents

Name

tcpdump - dump traffic on a network

Synopsis

```
tcpdump [ -AdDefIKlLnNOpqRStuUvxX ] [ -B buffer_size ] [ -c count ]
[ -C file_size ] [ -G rotate_seconds ] [ -F file ]
[ -i interface ] [ -m module ] [ -M secret ]
[ -r file ] [ -s snaplen ] [ -T type ] [ -w file ]
[ -W filecount ]
[ -E spi@ipaddr algo:secret,... ]
[ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
[ expression ]
```

Description

Tcpdump prints out a description of the contents of packets on a network interface that match the boolean *expression*. It can also be run with the `-w` flag, which causes it to save the packet data to a file for later analysis, and/or with the `-r` flag, which causes it to read from a saved packet file rather than to read packets from a network interface. In all cases, only packets that match *expression* will be processed by tcpdump.

Tcpdump will, if not run with the `-c` flag, continue capturing packets until it is interrupted by a SIGINT signal (generated, for example, by typing your interrupt character, typically control-C) or a SIGTERM signal (typically generated with the `kill(1)` command); if run with the `-c` flag, it will capture packets until it is interrupted by a SIGINT or SIGTERM signal or the specified number of packets have been processed.

When *tcpdump* finishes capturing packets, it will report counts of:

- packets ``captured'' (this is the number of packets that *tcpdump* has received and processed);
- packets ``received by filter'' (the meaning of this depends on the OS on which you're running *tcpdump*, and possibly on the way the OS was configured - if a filter was specified on the command line, on some OSes it counts packets regardless of whether they were matched by the filter expression and, even if they were matched by the filter expression, regardless of whether *tcpdump* has read and processed them yet, on other OSes it counts only packets that were matched by the filter expression regardless of whether *tcpdump* has read and processed them yet, and on other OSes it counts only packets that were matched by the filter expression and were processed by *tcpdump*);
- packets ``dropped by kernel'' (this is the number of packets that were dropped, due to a lack of buffer space, by the packet capture mechanism in the OS on which *tcpdump* is running, if the OS reports that information to applications; if not, it will be reported as 0).

On platforms that support the SIGINFO signal, such as most BSDs (including Mac OS X) and Digital/Tru64 UNIX, it will report those counts when it receives a SIGINFO signal (generated, for example, by typing your ``status'' character, typically control-T, although on some platforms, such as Mac OS X, the ``status'' character is not set by default, so you must set it with `stty(1)` in order to use it) and will continue capturing packets.

Reading packets from a network interface may require that you have special privileges; see the `pcap(3PCAP)` man page for details. Reading a saved packet file doesn't require special privileges.

Options

Option	Description
-A	Print each packet (minus its link level header) in ASCII. Handy for capturing web pages.
-B	Set the operating system capture buffer size to *buffer_size*.
-c	Exit after receiving *count* packets.
-C	Before writing a raw packet to a savefile, check whether the file is currently larger than *file_size* and, if so, close the current savefile and open a new one. Savefiles after the first savefile will have the name specified with the `-w` flag, with a number after it, starting at 1 and continuing upward. The units of *file_size* are millions of bytes (1,000,000 bytes, not 1,048,576 bytes).
-d	Dump the compiled packet-matching code in a human readable form to standard output and stop.
-dd	Dump packet-matching code as a C program fragment.
-ddd	Dump packet-matching code as decimal numbers (preceded with a count).
-D	Print the list of the network interfaces available on the system and on which tcpdump can capture packets. For each network interface, a number and an interface name, possibly followed by a text description of the interface, is printed. The interface name or the number can be supplied to the `-i` flag to specify an interface on which to capture. This can be useful on systems that don't have a command to list them (e.g., Windows systems, or UNIX systems lacking `ifconfig -a`); the number can be useful on Windows 2000 and later systems, where the interface name is a somewhat complex string. The `-D` flag will not be supported if *tcpdump* was built with an older version of *libpcap* that lacks the `pcap_findalldevs()` function.
-e	Print the link-level header on each dump line.

Option	Description
-E	Use *spi@ipaddr algo:secret* for decrypting IPsec ESP packets that are addressed to *addr* and contain Security Parameter Index value `spi`. This combination may be repeated with comma or newline seperation. Note that setting the secret for IPv4 ESP packets is supported at this time. Algorithms may be `des-cbc`, `3des-cbc`, `blowfish-cbc`, `rc3-cbc`, `cast128-cbc`, or `none`. The default is `des-cbc`. The ability to decrypt packets is only present if *tcpdump* was compiled with cryptography enabled. *secret* is the ASCII text for ESP secret key. If preceeded by `0x`, then a hex value will be read. The option assumes RFC2406 ESP, not RFC1827 ESP. The option is only for debugging purposes, and the use of this option with a true `secret' key is discouraged. By presenting IPsec secret key onto command line you make it visible to others, via `ps(1)` and other occasions. In addition to the above syntax, the syntax *file name* may be used to have tcpdump read the provided file in. The file is opened upon receiving the first ESP packet, so any special permissions that tcpdump may have been given should already have been given up.
-f	Print `foreign' IPv4 addresses numerically rather than symbolically (this option is intended to get around serious brain damage in Sun's NIS server -- usually it hangs forever translating non-local internet numbers).  The test for `foreign' IPv4 addresses is done using the IPv4 address and netmask of the interface on which capture is being done. If that address or netmask are not available, available, either because the interface on which capture is being done has no address or netmask or because the capture is being done on the Linux "any" interface, which can capture on more than one interface, this option will not work correctly.
-F	Use *file* as input for the filter expression. An additional expression given on the command line is ignored.
-G	If specified, rotates the dump file specified with the `-w` option every *rotate_seconds* seconds. Savefiles will have the name specified by `-w` which should include a time format as defined by `strftime(3)`. If no time format is specified, each new file will overwrite the previous. If used in conjunction with the `-C` option, filenames will take the form of `*file*<count>'.
-i	Listen on *interface*. If unspecified, *tcpdump* searches the system interface list for the lowest numbered, configured up interface (excluding loopback). Ties are broken by choosing the earliest match. On Linux systems with 2.2 or later kernels, an interface argument of ``any'' can be used to capture packets from all interfaces. Note that captures on the ``any'' device will not be done in promiscuous mode. If the `-D` flag is supported, an interface number as printed by that flag can be used as the interface argument.

Option	Description
-I	Put the interface in "monitor mode"; this is supported only on IEEE 802.11 Wi-Fi interfaces, and supported only on some operating systems. Note that in monitor mode the adapter might disassociate from the network with which it's associated, so that you will not be able to use any wireless networks with that adapter. This could prevent accessing files on a network server, or resolving host names or network addresses, if you are capturing in monitor mode and are not connected to another network with another adapter. This flag will affect the output of the `-L` flag. If `-I` isn't specified, only those link-layer types available when not in monitor mode will be shown; if `-I` is specified, only those link-layer types available when in monitor mode will be shown.
-K	Don't attempt to verify IP, TCP, or UDP checksums. This is useful for interfaces that perform some or all of those checksum calculation in hardware; otherwise, all outgoing TCP checksums will be flagged as bad.
-l	Make stdout line buffered. Useful if you want to see the data while capturing it. E.g., `tcpdump -l | tee dat'' or ``tcpdump -l > dat & tail -f dat`
-L	List the known data link types for the interface, in the specified mode, and exit. The list of known data link types may be dependent on the specified mode; for example, on some platforms, a Wi-Fi interface might support one set of data link types when not in monitor mode (for example, it might support only fake Ethernet headers, or might support 802.11 headers but not support 802.11 headers with radio information) and another set of data link types when in monitor mode (for example, it might support 802.11 headers, or 802.11 headers with radio information, only in monitor mode).
-m	Load SMI MIB module definitions from file *module*. This option can be used several times to load several MIB modules into *tcpdump*.
-M	Use secret as a shared *secret* for validating the digests found in TCP segments with the TCP-MD5 option (RFC 2385), if present.
-n	Don't convert addresses (i.e., host addresses, port numbers, etc.) to names.
-N	Don't print domain name qualification of host names. E.g., if you give this flag then *tcpdump* will print ``nic'' instead of ``nic.ddn.mil''.
-O	Do not run the packet-matching code optimizer. This is useful only if you suspect a bug in the optimizer.
-p	Don't put the interface into promiscuous mode. Note that the interface might be in promiscuous mode for some other reason; hence, `-p' cannot be used as an abbreviation for `ether host {local-hw-addr} or ether broadcast'.
-q	Quick (quiet?) output. Print less protocol information so output lines are shorter.
-R	Assume ESP/AH packets to be based on old specification (RFC1825 to RFC1829). If specified, *tcpdump* will not print replay prevention field. Since there is no protocol version field in ESP/AH specification, *tcpdump* cannot deduce the version of ESP/AH protocol.
-r	Read packets from file (which was created with the `-w` option). Standard input is used if *file* is ``-''.
-S	Print absolute, rather than relative, TCP sequence numbers.

Option	Description
-s	Snarf *snaplen* bytes of data from each packet rather than the default of 65535 bytes. Packets truncated because of a limited snapshot are indicated in the output with ``[|*proto*]'', where *proto* is the name of the protocol level at which the truncation has occurred. Note that taking larger snapshots both increases the amount of time it takes to process packets and, effectively, decreases the amount of packet buffering. This may cause packets to be lost. You should limit *snaplen* to the smallest number that will capture the protocol information you're interested in. Setting *snaplen* to 0 sets it to the default of 65535, for backwards compatibility with recent older versions of *tcpdump*.
-T	Force packets selected by "*expression*" to be interpreted the specified *type*. Currently known types are `aodv` (Ad-hoc On-demand Distance Vector protocol), `cnfp` (Cisco NetFlow protocol), `rpc` (Remote Procedure Call), `rtp` (Real-Time Applications protocol), `rtcp` (Real-Time Applications control protocol), `snmp` (Simple Network Management Protocol), `tftp` (Trivial File Transfer Protocol), `vat` (Visual Audio Tool), and `wb` (distributed White Board).
-t	Don't print a timestamp on each dump line.
-tt	Print an unformatted timestamp on each dump line.
-ttt	Print a delta (micro-second resolution) between current and previous line on each dump line.
-tttt	Print a timestamp in default format proceeded by date on each dump line.
-ttttt	Print a delta (micro-second resolution) between current and first line on each dump line.
-u	Print undecoded NFS handles.
-U	Make output saved via the `-w` option ``packet-buffered''; i.e., as each packet is saved, it will be written to the output file, rather than being written only when the output buffer fills. The `-U` flag will not be supported if *tcpdump* was built with an older version of *libpcap* that lacks the `pcap_dump_flush()` function.
-v	When parsing and printing, produce (slightly more) verbose output. For example, the time to live, identification, total length and options in an IP packet are printed. Also enables additional packet integrity checks such as verifying the IP and ICMP header checksum. When writing to a file with the `-w` option, report, every 10 seconds, the number of packets captured.
-vv	Even more verbose output. For example, additional fields are printed from NFS reply packets, and SMB packets are fully decoded.
-vvv	Even more verbose output. For example, telnet `SB ... SE` options are printed in full. With `-X` Telnet options are printed in hex as well.
-w	Write the raw packets to *file* rather than parsing and printing them out. They can later be printed with the `-r` option. Standard output is used if *file* is ``-''. See `pcap-savefile(5)` for a description of the file format.
-W	Used in conjunction with the `-C` option, this will limit the number of files created to the specified number, and begin overwriting files from the beginning, thus creating a 'rotating' buffer. In addition, it will name the files with enough leading 0s to support the maximum number of files, allowing them to sort correctly. Used in conjunction with the `-G` option, this will limit the number of rotated dump files that get created, exiting with status 0 when reaching the limit. If used with `-C` as well, the behavior will result in cyclical files per timeslice.

Option	Description
-x	When parsing and printing, in addition to printing the headers of each packet, print the data of each packet (minus its link level header) in hex. The smaller of the entire packet or snaplen bytes will be printed. Note that this is the entire link-layer packet, so for link layers that pad (e.g. Ethernet), the padding bytes will also be printed when the higher layer packet is shorter than the required padding.
-xx	When parsing and printing, in addition to printing the headers of each packet, print the data of each packet, including its link level header, in hex.
-X	When parsing and printing, in addition to printing the headers of each packet, print the data of each packet (minus its link level header) in hex and ASCII. This is very handy for analysing new protocols.
-XX	When parsing and printing, in addition to printing the headers of each packet, print the data of each packet, including its link level header, in hex and ASCII.
-y	Set the data link type to use while capturing packets to datalinktype.
-z	Used in conjunction with the `-C` or `-G` options, this will make tcpdump run " command file " where file is the savefile being closed after each rotation. For example, specifying `-z gzip` or `-z bzip2` will compress each savefile using gzip or bzip2. Note that tcpdump will run the command in parallel to the capture, using the lowest priority so that this doesn't disturb the capture process. And in case you would like to use a command that itself takes flags or different arguments, you can always write a shell script that will take the savefile name as the only argument, make the flags & arguments arrangements and execute the command that you want.
-Z	Drops privileges (if root) and changes user ID to user and the group ID to the primary group of *user*. This behavior can also be enabled by default at compile time. *expression* selects which packets will be dumped. If no *expression* is given, all packets on the net will be dumped. Otherwise, only packets for which expression is `true' will be dumped. For the expression syntax, see `pcap-filter(7)`. Expression arguments can be passed to *tcpdump* as either a single argument or as multiple arguments, whichever is more convenient. Generally, if the expression contains Shell metacharacters, it is easier to pass it as a single, quoted argument. Multiple arguments are concatenated with spaces before being parsed.

Examples

To print all packets arriving at or departing from sundown:

```
tcpdump host sundown
```

To print traffic between helios and either hot or ace:

```
tcpdump host helios and \( hot or ace \)
```

To print all IP packets between ace and any host except helios:

```
tcpdump ip host ace and not helios
```

To print all traffic between local hosts and hosts at Berkeley:

```
tcpdump net ucb-ether
```

To print all ftp traffic through internet gateway snup: (note that the expression is quoted to prevent the shell from (mis-)interpreting the parentheses):

```
tcpdump 'gateway snup and (port ftp or ftp-data)'
```

To print traffic neither sourced from nor destined for local hosts (if you gateway to one other net, this stuff should never make it onto your local net).

```
tcpdump ip and not net localnet
```

To print the start and end packets (the SYN and FIN packets) of each TCP conversation that involves a non-local host.

```
tcpdump 'tcp[tcpflags] & (tcp-syn|tcp-fin) != 0 and not src and dst net localnet'
```

To print all IPv4 HTTP packets to and from port 80, i.e. print only packets that contain data, not, for example, SYN and FIN packets and ACK-only packets. (IPv6 is left as an exercise for the reader.)

```
tcpdump 'tcp port 80 and (((ip[2:2] - ((ip[0]&0xf)<<2)) - ((tcp[12]&0xf0)>>2)) !=
0)'
```

To print IP packets longer than 576 bytes sent through gateway snup:

```
tcpdump 'gateway snup and ip[2:2] > 576'
```

To print IP broadcast or multicast packets that were not sent via Ethernet broadcast or multicast:

```
tcpdump 'ether[0] & 1 = 0 and ip[16] >= 224'
```

To print all ICMP packets that are not echo requests/replies (i.e., not ping packets):

```
tcpdump 'icmp[icmptype] != icmp-echo and icmp[icmptype] != icmp-echoreply'
```

Output Format

The output of tcpdump is protocol dependent. The following gives a brief description and examples of most of the formats.

Link Level Headers

If the '-e' option is given, the link level header is printed out. On Ethernets, the source and destination addresses, protocol, and packet length are printed.

On FDDI networks, the '-e' option causes tcpdump to print the `frame control' field, the source and destination addresses, and the packet length. (The `frame control' field governs the interpretation of the rest of the packet. Normal packets (such as those containing IP datagrams) are `async' packets, with a priority value between 0 and 7; for example, `async4'. Such packets are assumed to contain an 802.2 Logical Link Control (LLC) packet; the LLC header is printed if it is not an ISO datagram or a so-called SNAP packet.

On Token Ring networks, the '-e' option causes tcpdump to print the `access control' and `frame control' fields, the source and destination addresses, and the packet length. As on FDDI networks, packets are assumed to contain an LLC packet. Regardless of whether the '-e' option is specified or not, the source routing information is printed for source-routed packets.

On 802.11 networks, the '-e' option causes tcpdump to print the `frame control' fields, all of the addresses in the 802.11 header, and the packet length. As on FDDI networks, packets are assumed to contain an LLC packet.

(N.B.: The following description assumes familiarity with the SLIP compression algorithm described in RFC-1144.)

On SLIP links, a direction indicator (``I'' for inbound, ``O'' for outbound), packet type, and compression information are printed out. The packet type is printed first. The three types are ip, utcp, and ctcp. No further link information is printed for ip packets. For TCP packets, the connection identifier is printed following the type. If the packet is compressed, its encoded header is printed out. The special cases are printed out as *S+n and *SA+n, where n is the amount by which the sequence number (or sequence number and ack) has changed. If it is not a special case, zero or more changes are printed. A change is indicated by U (urgent pointer), W (window), A (ack), S (sequence number), and I (packet ID), followed by

a delta (+n or -n), or a new value (=n). Finally, the amount of data in the packet and compressed header length are printed.

For example, the following line shows an outbound compressed TCP packet, with an implicit connection identifier; the ack has changed by 6, the sequence number by 49, and the packet ID by 6; there are 3 bytes of data and 6 bytes of compressed header:

```
O ctcp * A+6 S+49 I+6 3 (6)
```

ARP/RARP Packets

Arp/rarp output shows the type of request and its arguments. The format is intended to be self explanatory. Here is a short sample taken from the start of an `rlogin' from host rtsg to host csam:

```
arp who-has csam tell rtsg
arp reply csam is-at CSAM
```

The first line says that rtsg sent an arp packet asking for the Ethernet address of internet host csam. Csam replies with its Ethernet address (in this example, Ethernet addresses are in caps and internet addresses in lower case).

This would look less redundant if we had done tcpdump -n:

```
arp who-has 128.3.254.6 tell 128.3.254.68
arp reply 128.3.254.6 is-at 02:07:01:00:01:c4
```

If we had done tcpdump -e, the fact that the first packet is broadcast and the second is point-to-point would be visible:

```
RTSG Broadcast 0806  64: arp who-has csam tell rtsg
CSAM RTSG 0806  64: arp reply csam is-at CSAM
```

For the first packet this says the Ethernet source address is RTSG, the destination is the Ethernet broadcast address, the type field contained hex 0806 (type ETHER_ARP) and the total length was 64 bytes.

TCP Packets

(N.B.:The following description assumes familiarity with the TCP protocol described in RFC-793. If you are not familiar with the protocol, neither this description nor tcpdump will be of much use to you.)

The general format of a tcp protocol line is:

```
src > dst: flags data-seqno ack window urgent options
```

Src and dst are the source and destination IP addresses and ports. Flags are some combination of S (SYN), F (FIN), P (PUSH), R (RST), W (ECN CWR) or E (ECN-Echo), or a single `.' (no flags). Data-seqno describes the portion of sequence space covered by the data in this packet (see example below). Ack is sequence number of the next data expected the other direction on this connection. Window is the number of bytes of receive buffer space available the other direction on this connection. Urg indicates there is `urgent' data in the packet. Options are tcp options enclosed in angle brackets (e.g., <mss 1024>).

Src, dst and flags are always present. The other fields depend on the contents of the packet's tcp protocol header and are output only if appropriate.

Here is the opening portion of an rlogin from host rtsg to host csam.

```
rtsg.1023 > csam.login: S 768512:768512(0) win 4096 <mss 1024>
csam.login > rtsg.1023: S 947648:947648(0) ack 768513 win 4096 <mss 1024>
rtsg.1023 > csam.login: . ack 1 win 4096
rtsg.1023 > csam.login: P 1:2(1) ack 1 win 4096
csam.login > rtsg.1023: . ack 2 win 4096
rtsg.1023 > csam.login: P 2:21(19) ack 1 win 4096
csam.login > rtsg.1023: P 1:2(1) ack 21 win 4077
csam.login > rtsg.1023: P 2:3(1) ack 21 win 4077 urg 1
csam.login > rtsg.1023: P 3:4(1) ack 21 win 4077 urg 1
```

The first line says that tcp port 1023 on rtsg sent a packet to port login on csam. The S indicates that the SYN flag was set. The packet sequence number was 768512 and it contained no data. (The notation is

`first:last(nbytes)' which means `sequence numbers first up to but not including last which is nbytes bytes of user data'.) There was no piggy-backed ack, the available receive window was 4096 bytes and there was a max-segment-size option requesting an mss of 1024 bytes.

Csam replies with a similar packet except it includes a piggy-backed ack for rtsg's SYN. Rtsg then acks csam's SYN. The `.' means no flags were set. The packet contained no data so there is no data sequence number. Note that the ack sequence number is a small integer (1). The first time tcpdump sees a tcp `conversation', it prints the sequence number from the packet. On subsequent packets of the conversation, the difference between the current packet's sequence number and this initial sequence number is printed. This means that sequence numbers after the first can be interpreted as relative byte positions in the conversation's data stream (with the first data byte each direction being `1'). `-S' will override this feature, causing the original sequence numbers to be output.

On the 6th line, rtsg sends csam 19 bytes of data (bytes 2 through 20 in the rtsg -> csam side of the conversation). The PUSH flag is set in the packet. On the 7th line, csam says it's received data sent by rtsg up to but not including byte 21. Most of this data is apparently sitting in the socket buffer since csam's receive window has gotten 19 bytes smaller. Csam also sends one byte of data to rtsg in this packet. On the 8th and 9th lines, csam sends two bytes of urgent, pushed data to rtsg.

If the snapshot was small enough that tcpdump didn't capture the full TCP header, it interprets as much of the header as it can and then reports ``[|tcp]'' to indicate the remainder could not be interpreted. If the header contains a bogus option (one with a length that's either too small or beyond the end of the header), tcpdump reports it as ``[bad opt]'' and does not interpret any further options (since it's impossible to tell where they start). If the header length indicates options are present but the IP datagram length is not long enough for the options to actually be there, tcpdump reports it as ``[bad hdr length]''.

Capturing TCP packets with particular flag combinations (SYN-ACK, URG-ACK, etc.)

There are 8 bits in the control bits section of the TCP header:

```
CWR | ECE | URG | ACK | PSH | RST | SYN | FIN
```

Let's assume that we want to watch packets used in establishing a TCP connection. Recall that TCP uses a 3-way handshake protocol when it initializes a new connection; the connection sequence with regard to the TCP control bits is

1) Caller sends SYN

2) Recipient responds with SYN, ACK

3) Caller sends ACK

Now we're interested in capturing packets that have only the SYN bit set (Step 1). Note that we don't want packets from step 2 (SYN-ACK), just a plain initial SYN. What we need is a correct filter expression for tcpdump.

Recall the structure of a TCP header without options:

```
0                            15                              31
-----------------------------------------------------------------
|          source port          |       destination port        |
-----------------------------------------------------------------
|                        sequence number                        |
-----------------------------------------------------------------
|                     acknowledgment number                     |
-----------------------------------------------------------------
|  HL   | rsvd  |C|E|U|A|P|R|S|F|        window size            |
-----------------------------------------------------------------
|         TCP checksum          |       urgent pointer          |
-----------------------------------------------------------------
```

A TCP header usually holds 20 octets of data, unless options are present. The first line of the graph contains octets 0 - 3, the second line shows octets 4 - 7 etc.

Starting to count with 0, the relevant TCP control bits are contained in octet 13:

```
0             7|             15|             23|             31
---------------|---------------|---------------|---------------
|  HL   | rsvd  |C|E|U|A|P|R|S|F|        window size            |
---------------|---------------|---------------|---------------
|               |  13th octet   |               |               |
```

Let's have a closer look at octet no. 13:

```
|               |
|---------------|
|C|E|U|A|P|R|S|F|
|---------------|
|7   5   3     0|
```

These are the TCP control bits we are interested in. We have numbered the bits in this octet from 0 to 7, right to left, so the PSH bit is bit number 3, while the URG bit is number 5.

Recall that we want to capture packets with only SYN set. Let's see what happens to octet 13 if a TCP datagram arrives with the SYN bit set in its header:

```
|C|E|U|A|P|R|S|F|
|---------------|
|0 0 0 0 0 0 1 0|
|---------------|
|7 6 5 4 3 2 1 0|
```

Looking at the control bits section we see that only bit number 1 (SYN) is set.

Assuming that octet number 13 is an 8-bit unsigned integer in network byte order, the binary value of this octet is

```
00000010
```

and its decimal representation is

```
7     6     5     4     3     2     1     0
0*2 + 0*2 + 0*2 + 0*2 + 0*2 + 0*2 + 1*2 + 0*2  =  2
```

We're almost done, because now we know that if only SYN is set, the value of the 13th octet in the TCP header, when interpreted as a 8-bit unsigned integer in network byte order, must be exactly 2.

This relationship can be expressed as

```
tcp[13] == 2
```

We can use this expression as the filter for tcpdump in order to watch packets which have only SYN set:

```
tcpdump -i xl0 tcp[13] == 2
```

The expression says "let the 13th octet of a TCP datagram have the decimal value 2", which is exactly what we want.

Now, let's assume that we need to capture SYN packets, but we don't care if ACK or any other TCP control bit is set at the same time. Let's see what happens to octet 13 when a TCP datagram with SYN-ACK set arrives:

```
|C|E|U|A|P|R|S|F|
|---------------|
|0 0 0 1 0 0 1 0|
|---------------|
|7 6 5 4 3 2 1 0|
```

Now bits 1 and 4 are set in the 13th octet. The binary value of octet 13 is

```
00010010
```

which translates to decimal

```
7     6     5     4     3     2     1     0
0*2 + 0*2 + 0*2 + 1*2 + 0*2 + 0*2 + 1*2 + 0*2   = 18
```

Now we can't just use 'tcp[13] == 18' in the tcpdump filter expression, because that would select only those packets that have SYN-ACK set, but not those with only SYN set. Remember that we don't care if ACK or any other control bit is set as long as SYN is set.

In order to achieve our goal, we need to logically AND the binary value of octet 13 with some other value to preserve the SYN bit. We know that we want SYN to be set in any case, so we'll logically AND the value in the 13th octet with the binary value of a SYN:

```
      00010010 SYN-ACK 00000010 SYN
AND   00000010 (we want SYN)   AND  00000010 (we want SYN)
      --------                      --------
=     00000010                 =    00000010
```

We see that this AND operation delivers the same result regardless whether ACK or another TCP control bit is set. The decimal representation of the AND value as well as the result of this operation is 2 (binary 00000010), so we know that for packets with SYN set the following relation must hold true:

```
( ( value of octet 13 ) AND ( 2 ) ) == ( 2 )
```

This points us to the tcpdump filter expression

```
tcpdump -i xl0 'tcp[13] & 2 == 2'
```

Note that you should use single quotes or a backslash in the expression to hide the AND ('&') special character from the shell.

UDP Packets

UDP format is illustrated by this rwho packet:

```
actinide.who > broadcast.who: udp 84
```

This says that port who on host actinide sent a udp datagram to port who on host broadcast, the Internet broadcast address. The packet contained 84 bytes of user data.

Some UDP services are recognized (from the source or destination port number) and the higher level protocol information printed. In particular, Domain Name service requests (RFC-1034/1035) and Sun RPC calls (RFC-1050) to NFS.

UDP Name Server Requests

(N.B.:The following description assumes familiarity with the Domain Service protocol described in RFC-1035. If you are not familiar with the protocol, the following description will appear to be written in greek.)

Name server requests are formatted as

```
src > dst: id op? flags qtype qclass name (len)
h2opolo.1538 > helios.domain: 3+ A? ucbvax.berkeley.edu. (37)
```

Host h2opolo asked the domain server on helios for an address record (qtype=A) associated with the name ucbvax.berkeley.edu. The query id was `3'. The `+' indicates the recursion desired flag was set. The query length was 37 bytes, not including the UDP and IP protocol headers. The query operation was the normal one, Query, so the op field was omitted. If the op had been anything else, it would have been printed between the `3' and the `+'. Similarly, the qclass was the normal one, C_IN, and omitted. Any other qclass would have been printed immediately after the `A'.

A few anomalies are checked and may result in extra fields enclosed in square brackets: If a query contains an answer, authority records or additional records section, ancount, nscount, or arcount are printed as `[na]', `[nn]' or `[nau]' where n is the appropriate count. If any of the response bits are set (AA, RA or rcode) or any of the `must be zero' bits are set in bytes two and three, `[b2&3=x]' is printed, where x is the hex value of header bytes two and three.

UDP Name Server Responses

Name server responses are formatted as

```
src > dst:  id op rcode flags a/n/au type class data (len)

helios.domain > h2opolo.1538: 3 3/3/7 A 128.32.137.3 (273)
helios.domain > h2opolo.1537: 2 NXDomain* 0/1/0 (97)
```

In the first example, helios responds to query id 3 from h2opolo with 3 answer records, 3 name server records and 7 additional records. The first answer record is type A (address) and its data is internet address 128.32.137.3. The total size of the response was 273 bytes, excluding UDP and IP headers. The op (Query) and response code (NoError) were omitted, as was the class (C_IN) of the A record.

In the second example, helios responds to query 2 with a response code of non-existent domain (NXDomain) with no answers, one name server and no authority records. The `*' indicates that the authoritative answer bit was set. Since there were no answers, no type, class or data were printed.

Other flag characters that might appear are `-' (recursion available, RA, not set) and `|' (truncated message, TC, set). If the `question' section doesn't contain exactly one entry, `[nq]' is printed.

SMB/CIFS decoding

tcpdump now includes fairly extensive SMB/CIFS/NBT decoding for data on UDP/137, UDP/138 and TCP/139. Some primitive decoding of IPX and NetBEUI SMB data is also done.

By default a fairly minimal decode is done, with a much more detailed decode done if -v is used. Be warned that with -v a single SMB packet may take up a page or more, so only use -v if you really want all the gory details.

For information on SMB packet formats and what all te fields mean see www.cifs.org or the pub/samba/specs/ directory on your favorite samba.org mirror site. The SMB patches were written by Andrew Tridgell (tridge@samba.org).

NFS Requests and Replies

Sun NFS (Network File System) requests and replies are printed as:

```
src.xid > dst.nfs: len op args
src.nfs > dst.xid: reply stat len op results

sushi.6709 > wrl.nfs: 112 readlink fh 21,24/10.73165
wrl.nfs > sushi.6709: reply ok 40 readlink "../var"
sushi.201b > wrl.nfs:
   144 lookup fh 9,74/4096.6878 "xcolors"
wrl.nfs > sushi.201b:
   reply ok 128 lookup fh 9,74/4134.3150
```

In the first line, host sushi sends a transaction with id 6709 to wrl (note that the number following the src host is a transaction id, not the source port). The request was 112 bytes, excluding the UDP and IP headers. The operation was a readlink (read symbolic link) on file handle (fh) 21,24/10.731657119. (If one is lucky, as in this case, the file handle can be interpreted as a major,minor device number pair, followed by the inode number and generation number.) Wrl replies `ok' with the contents of the link.

In the third line, sushi asks wrl to lookup the name `xcolors' in directory file 9,74/4096.6878. Note that the data printed depends on the operation type. The format is intended to be self explanatory if read in conjunction with an NFS protocol spec.

If the -v (verbose) flag is given, additional information is printed. For example:

```
sushi.1372a > wrl.nfs:
   148 read fh 21,11/12.195 8192 bytes @ 24576
wrl.nfs > sushi.1372a:
   reply ok 1472 read REG 100664 ids 417/0 sz 29388
```

(-v also prints the IP header TTL, ID, length, and fragmentation fields, which have been omitted from this example.) In the first line, sushi asks wrl to read 8192 bytes from file 21,11/12.195, at byte offset 24576. Wrl replies `ok'; the packet shown on the second line is the first fragment of the reply, and hence is only 1472 bytes long (the other bytes will follow in subsequent fragments, but these fragments do not have NFS or even UDP headers and so might not be printed, depending on the filter expression used). Because the -v flag is given, some of the file attributes (which are returned in addition to the file data) are printed: the file type (``REG'', for regular file), the file mode (in octal), the uid and gid, and the file size.

If the -v flag is given more than once, even more details are printed.

Note that NFS requests are very large and much of the detail won't be printed unless snaplen is increased. Try using `-s 192' to watch NFS traffic.

NFS reply packets do not explicitly identify the RPC operation. Instead, tcpdump keeps track of ``recent'' requests, and matches them to the replies using the transaction ID. If a reply does not closely follow the corresponding request, it might not be parsable.

AFS Requests and Replies

Transarc AFS (Andrew File System) requests and replies are printed as:

```
src.sport > dst.dport: rx packet-type
src.sport > dst.dport: rx packet-type service call call-name args
src.sport > dst.dport: rx packet-type service reply call-name args\

elvis.7001 > pike.afsfs:
   rx data fs call rename old fid 536876964/1/1 ".newsrc.new"
   new fid 536876964/1/1 ".newsrc"
pike.afsfs > elvis.7001: rx data fs reply rename
```

In the first line, host elvis sends a RX packet to pike. This was a RX data packet to the fs (fileserver) service, and is the start of an RPC call. The RPC call was a rename, with the old directory file id of 536876964/1/1 and an old filename of `.newsrc.new', and a new directory file id of 536876964/1/1 and a new filename of `.newsrc'. The host pike responds with a RPC reply to the rename call (which was successful, because it was a data packet and not an abort packet).

In general, all AFS RPCs are decoded at least by RPC call name. Most AFS RPCs have at least some of the arguments decoded (generally only the `interesting' arguments, for some definition of interesting).

The format is intended to be self-describing, but it will probably not be useful to people who are not familiar with the workings of AFS and RX.

If the -v (verbose) flag is given twice, acknowledgement packets and additional header information is printed, such as the the RX call ID, call number, sequence number, serial number, and the RX packet flags.

If the -v flag is given twice, additional information is printed, such as the the RX call ID, serial number, and the RX packet flags. The MTU negotiation information is also printed from RX ack packets.

If the -v flag is given three times, the security index and service id are printed.

Error codes are printed for abort packets, with the exception of Ubik beacon packets (because abort packets are used to signify a yes vote for the Ubik protocol).

Note that AFS requests are very large and many of the arguments won't be printed unless snaplen is increased. Try using `-s 256' to watch AFS traffic.

AFS reply packets do not explicitly identify the RPC operation. Instead, tcpdump keeps track of ``recent'' requests, and matches them to the replies using the call number and service ID. If a reply does not closely follow the corresponding request, it might not be parsable.

KIP AppleTalk (DDP in UDP)

AppleTalk DDP packets encapsulated in UDP datagrams are de-encapsulated and dumped as DDP packets (i.e., all the UDP header information is discarded). The file /etc/atalk.names is used to translate AppleTalk net and node numbers to names. Lines in this file have the form

```
number  name

1.254  ether
16.1   icsd-net
1.254.110   ace
```

The first two lines give the names of AppleTalk networks. The third line gives the name of a particular host (a host is distinguished from a net by the 3rd octet in the number - a net number must have two octets and a host number must have three octets.) The number and name should be separated by whitespace (blanks or tabs). The /etc/atalk.names file may contain blank lines or comment lines (lines starting with a `#').

AppleTalk addresses are printed in the form

```
net.host.port

144.1.209.2 > icsd-net.112.220
office.2 > icsd-net.112.220
jssmag.149.235 > icsd-net.2
```

(If the /etc/atalk.names doesn't exist or doesn't contain an entry for some AppleTalk host/net number, addresses are printed in numeric form.) In the first example, NBP (DDP port 2) on net 144.1 node 209 is sending to whatever is listening on port 220 of net icsd node 112. The second line is the same except the full name of the source node is known (`office'). The third line is a send from port 235 on net jssmag node 149 to broadcast on the icsd-net NBP port (note that the broadcast address (255) is indicated by a net name with no host number - for this reason it's a good idea to keep node names and net names distinct in /etc/atalk.names).

NBP (name binding protocol) and ATP (AppleTalk transaction protocol) packets have their contents interpreted. Other protocols just dump the protocol name (or number if no name is registered for the protocol) and packet size.

NBP packets are formatted like the following examples:

```
icsd-net.112.220 > jssmag.2: nbp-lkup 190: "=:LaserWriter@*"
jssmag.209.2 > icsd-net.112.220: nbp-reply 190: "RM1140:LaserWriter@*" 250
techpit.2 > icsd-net.112.220: nbp-reply 190: "techpit:LaserWriter@*" 186
```

The first line is a name lookup request for laserwriters sent by net icsd host 112 and broadcast on net jssmag. The nbp id for the lookup is 190. The second line shows a reply for this request (note that it has the same id) from host jssmag.209 saying that it has a laserwriter resource named "RM1140" registered on port 250. The third line is another reply to the same request saying host techpit has laserwriter "techpit" registered on port 186.

ATP packet formatting is demonstrated by the following example:

```
jssmag.209.165 > helios.132: atp-req  12266<0-7> 0xae030001
helios.132 > jssmag.209.165: atp-resp 12266:0 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp 12266:1 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp 12266:2 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp 12266:3 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp 12266:4 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp 12266:5 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp 12266:6 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp*12266:7 (512) 0xae040000
jssmag.209.165 > helios.132: atp-req  12266<3,5> 0xae030001
helios.132 > jssmag.209.165: atp-resp 12266:3 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp 12266:5 (512) 0xae040000
jssmag.209.165 > helios.132: atp-rel  12266<0-7> 0xae030001
jssmag.209.133 > helios.132: atp-req* 12267<0-7> 0xae030002
```

Jssmag.209 initiates transaction id 12266 with host helios by requesting up to 8 packets (the `<0-7>'). The hex number at the end of the line is the value of the `userdata' field in the request.

Helios responds with 8 512-byte packets. The `:digit' following the transaction id gives the packet sequence number in the transaction and the number in parens is the amount of data in the packet, excluding the atp header. The `*' on packet 7 indicates that the EOM bit was set.

Jssmag.209 then requests that packets 3 & 5 be retransmitted. Helios resends them then jssmag.209 releases the transaction. Finally, jssmag.209 initiates the next request. The `*' on the request indicates that XO (`exactly once') was not set.

IP Fragmentation

Fragmented Internet datagrams are printed as

```
(frag id:size@offset+)
(frag id:size@offset)
```

(The first form indicates there are more fragments. The second indicates this is the last fragment.)

Id is the fragment id. Size is the fragment size (in bytes) excluding the IP header. Offset is this fragment's offset (in bytes) in the original datagram.

The fragment information is output for each fragment. The first fragment contains the higher level protocol header and the frag info is printed after the protocol info. Fragments after the first contain no higher level protocol header and the frag info is printed after the source and destination addresses. For example, here is part of an ftp from arizona.edu to lbl-rtsg.arpa over a CSNET connection that doesn't appear to handle 576 byte datagrams:

```
arizona.ftp-data > rtsg.1170: . 1024:1332(308) ack 1 win 4096 (frag 595a:328@0+)
arizona > rtsg: (frag 595a:204@328)
rtsg.1170 > arizona.ftp-data: . ack 1536 win 2560
```

There are a couple of things to note here: First, addresses in the 2nd line don't include port numbers. This is because the TCP protocol information is all in the first fragment and we have no idea what the port or sequence numbers are when we print the later fragments. Second, the tcp sequence information in the first line is printed as if there were 308 bytes of user data when, in fact, there are 512 bytes (308 in the first frag and 204 in the second). If you are looking for holes in the sequence space or trying to match up acks with packets, this can fool you.

A packet with the IP don't fragment flag is marked with a trailing (DF).

Timestamps

By default, all output lines are preceded by a timestamp. The timestamp is the current clock time in the form

```
hh:mm:ss.frac
```

and is as accurate as the kernel's clock. The timestamp reflects the time the kernel first saw the packet. No attempt is made to account for the time lag between when the Ethernet interface removed the packet from the wire and when the kernel serviced the `new packet' interrupt.

See Also

stty(1), pcap(3PCAP), bpf(4), nit(4P), pcap-savefile(5), pcap-filter(7)

Authors

The original authors are:

Van Jacobson, Craig Leres and Steven McCanne, all of the Lawrence Berkeley National Laboratory, University of California, Berkeley, CA.

It is currently being maintained by tcpdump.org.

The current version is available via http:

http://www.tcpdump.org/

The original distribution is available via anonymous ftp:

ftp://ftp.ee.lbl.gov/tcpdump.tar.Z

IPv6/IPsec support is added by WIDE/KAME project. This program uses Eric Young's SSLeay library, under specific configurations.

Bugs

Please send problems, bugs, questions, desirable enhancements, patches etc. to:

tcpdump-workers@lists.tcpdump.org

NIT doesn't let you watch your own outbound traffic, BPF will. We recommend that you use the latter.

On Linux systems with 2.0[.x] kernels:

- packets on the loopback device will be seen twice;
- packet filtering cannot be done in the kernel, so that all packets must be copied from the kernel in order to be filtered in user mode;
- all of a packet, not just the part that's within the snapshot length, will be copied from the kernel (the 2.0[.x] packet capture mechanism, if asked to copy only part of a packet to userland, will not report the true length of the packet; this would cause most IP packets to get an error from tcpdump);
- capturing on some PPP devices won't work correctly.

We recommend that you upgrade to a 2.2 or later kernel.

Some attempt should be made to reassemble IP fragments or, at least to compute the right length for the higher level protocol.

Name server inverse queries are not dumped correctly: the (empty) question section is printed rather than real query in the answer section. Some believe that inverse queries are themselves a bug and prefer to fix the program generating them rather than tcpdump.

A packet trace that crosses a daylight savings time change will give skewed time stamps (the time change is ignored).

Filter expressions on fields other than those in Token Ring headers will not correctly handle source-routed Token Ring packets.

Filter expressions on fields other than those in 802.11 headers will not correctly handle 802.11 data packets with both To DS and From DS set.

ip6 proto should chase header chain, but at this moment it does not. ip6 protochain is supplied for this behavior.

Arithmetic expression against transport layer headers, like tcp[0], does not work against IPv6 packets. It only looks at IPv4 packets.

Index

This document was created by man2html, using the manual pages.
Time: 14:27:56 GMT, November 19, 2009

Index

T

U

V