



TREND
M I C R O™

TippingPoint™

NX-Platform Hardware Installation and Safety

5998-1403
October 2016

Legal and notice information

© Copyright 2016 Trend Micro Incorporated. All rights reserved.

Trend Micro Incorporated makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Trend Micro Incorporated shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Trend Micro Incorporated. The information is provided “as is” without warranty of any kind and is subject to change without notice. The only warranties for Trend Micro Incorporated products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Trend Micro Incorporated shall not be liable for technical or editorial errors or omissions contained herein.

TippingPoint, the TippingPoint logo, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their respective owners. This document contains confidential information, trade secrets or both, which are the property of Trend Micro Incorporated. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Trend Micro Incorporated or one of its subsidiaries.

All other company and product names may be trademarks of their respective holders.

TippingPoint NX-Platform Hardware Installation and Safety
Publication Part Number: 5998-1403

Contents

- About this guide..... 1**
 - Target audience..... 1
 - Related documentation..... 1
 - Conventions..... 1
 - Contacting support..... 3
- System overview..... 4**
 - TippingPoint architecture..... 4
 - Security Management System (SMS)..... 5
 - SMS server..... 6
 - SMS client..... 6
 - Intrusion Prevention System devices..... 7
 - IPS local clients..... 8
 - Core Controller..... 8
 - High availability..... 9
 - Threat Suppression Engine..... 9
 - Threat Management Center..... 10
- Hardware safety and compliance..... 12**
 - Safety and compliance requirements..... 12
 - Safety guidelines and warnings..... 12
 - Cautions..... 13
 - Warnings..... 13
 - Installation warnings..... 13
 - Parts warnings..... 14

Rack and clearance requirements.....	15
Ventilation and location.....	16
Environmental requirements.....	16
Reliable earthing.....	17
ESD requirements.....	17
Hot swapping guidelines.....	17
Unpack the product.....	18
TippingPoint NX-Platform device overview.....	20
Chassis overview.....	20
Chassis features.....	23
Power button.....	23
Fans and power supplies.....	24
External storage card.....	24
Ports.....	24
Chassis LEDs.....	25
I/O modules.....	26
Bypass I/O modules.....	29
BIOM connectors and speeds.....	30
Notable BIOM behavior.....	30
Link transitions.....	31
Optical insertion loss.....	31
Default I/O module configuration settings.....	32
Hot-swapping I/O modules.....	32
I/O module hot-swapping guidelines.....	33
Module LEDs.....	34
Model requirements.....	35
Power requirements.....	35
Cabling requirements.....	36

Technical specifications.....	36
Hardware and interface specifications.....	36
Software specifications.....	37
Hardware installation and configuration.....	38
TippingPoint NX-Platform IPS chassis.....	38
Determine total rack space.....	38
Attach the device to the rack.....	39
Rack-mounting options.....	39
Power supply and I/O module connections.....	41
Add I/O modules.....	42
Attach cables.....	43
To attach the Console port connection.....	44
To attach the Management Processor connection.....	44
To attach network connections.....	44
Check LEDs.....	44
Setup wizard.....	45
Power supply and fan modules.....	46
NX-Platform AC power supply.....	46
NX-Platform DC power supply.....	47
NX-Platform fans.....	49
Installing the power cord retention bracket.....	51
Power cord retention bracket.....	51
Installing and using the bracket.....	51
Installing the bracket.....	52
Using the power cord retention bracket.....	52
Removing the bracket.....	53
Using the external storage card.....	54

About the external storage card.....	54
External storage card commands.....	54
Connector and pinout specifications.....	56
RJ-45 (COM) console.....	56
RJ-45 Ethernet connectors.....	57
Pluggable transceivers.....	58

About this guide

Welcome to the *NX-Platform Hardware Installation and Safety Guide*.

This section covers the following topics:

- [Target audience](#) on page 1
- [Related documentation](#) on page 1
- [Conventions](#) on page 1
- [Contacting support](#) on page 3

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 (SMTP)
- Simple Network management Protocol (SNMP)

Related documentation

A complete set of product documentation for the TippingPoint Intrusion Prevention Systems is available online. The product document set generally includes conceptual and deployment information, installation and user guides, CLI command references, safety and compliance information, and release notes.

For information about how to access the online product documentation, refer to the *Read Me First* document in your product shipment.

Conventions

This information uses the following conventions.

Typefaces


TypingPoint uses the following typographic conventions for structuring information:

Convention	Element
Bold font	<ul style="list-style-type: none">• Key names• Text typed into a GUI element, such as into a box• GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes. Example: Click OK to accept.
<i>Italics font</i>	Text emphasis, important terms, variables, and publication titles
Monospace font	<ul style="list-style-type: none">• File and directory names• System output• Code• Text typed at the command-line
<i>Monospace, italic font</i>	<ul style="list-style-type: none">• Code variables• Command-line variables
Monospace, bold font	Emphasis of file and directory names, system output, code, and text typed at the command line

Messages

Messages are special text that is emphasized by font, format, and icons.

 **Warning!** Alerts you to potential danger of bodily harm or other potential harmful consequences.

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

Note: Provides additional information to explain a concept or complete a task.

Important: Provides significant information or specific instructions.

Tip: Provides helpful hints and shortcuts, such as suggestions about how to perform a task more easily or more efficiently.

Contacting support

Contact the TippingPoint Technical Assistance Center (TAC) by using any of the following options.

Email support

tippingpoint.support@trendmicro.com

Phone support

North America: +1 866 681 8324

International: See <https://tmc.tippingpoint.com>

System 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 topic includes the following information:

- [TippingPoint architecture](#) on page 4
- [Security Management System \(SMS\)](#) on page 5
- [Intrusion Prevention System devices](#) on page 7
- [Core Controller](#) on page 8
- [High availability](#) on page 9
- [Threat Suppression Engine](#) on page 9
- [Threat Management Center](#) on page 10

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:

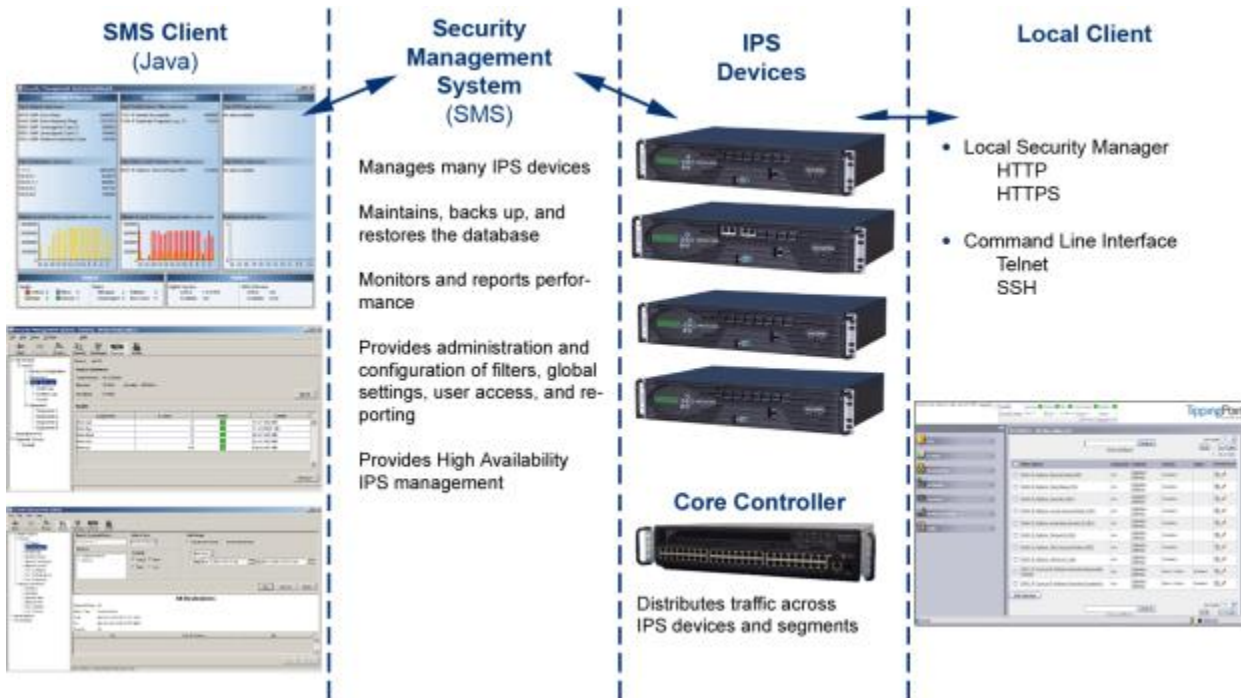


Figure 1. TippingPoint architecture

Security Management System (SMS)

Describes the core components of the 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 OS X
- 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, and 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 of the active system 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.

TSE features include:

- 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 website. 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 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 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:
 - 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.

Hardware safety and compliance

This topic describes TippingPoint product regulatory compliance and provides safety requirements and warnings.

Before installing your TippingPoint product, you must read through all preparation instructions and safety requirements.

- [Safety and compliance requirements](#) on page 12
- [Rack and clearance requirements](#) on page 15
- [Ventilation and location](#) on page 16
- [Environmental requirements](#) on page 16
- [Reliable earthing](#) on page 17
- [ESD requirements](#) on page 17
- [Hot swapping guidelines](#) on page 17
- [Unpack the product](#) on page 18

Safety and compliance requirements

Provides the location of hardware safety and compliance information.

For detailed regulatory compliance information, refer to the *TippingPoint Hardware Safety and Compliance Guide*, available on the TMC and included with your product.

Safety guidelines and warnings

Provides important information and safety warnings.

Before you start the installation procedures, read this entire section for important information and safety warnings. The warnings in this section have been localized to 28 languages in the *TippingPoint Safety Warning Notices* document available at the Threat Management Center (TMC) web site at <https://tmc.tippingpoint.com>.

If not properly installed and maintained, electrical circuitry equipment can pose dangers to both personnel and equipment. To prevent accidents, adhere to the following guidelines to ensure general safety:

- Remove any dust from the area and keep the area around the product clear and dust-free during and after installation.
- Wear safety glasses if you are working under conditions that might be hazardous to your eyes.

- This product has serviceable modules and hot-swappable power supplies. It has no other serviceable parts inside.

Cautions

Cautions tell you how to avoid a serious loss that stops short of physical damage such as the loss of data, time, or security.

Cautions tell you what you should or should not do to avoid such losses, and the consequences of not heeding the caution.

⚠Caution: Do not power up the equipment while you install and connect the system. If you connect the power improperly and then apply power, the cards and chassis could be damaged. You are responsible for installing an AC power disconnect for the entire rack unit. This main disconnect must be readily accessible, and it must be labeled as controlling power to the entire unit, not just to the server.

⚠Caution: The equipment rack must be anchored to an unmovable support to prevent it from falling over when one or more servers are extended in front of it on slide assemblies. The equipment rack must be installed according to the manufacturer's instructions. You must also consider the weight of any other device installed in the rack. Make sure that the chassis cooling fans run continuously while the system is powered.

⚠Caution: Make sure all cards are completely connected to the backplane. Improper connections can disrupt system operation.

⚠Caution: When using a DC power supply, be sure to replace the plastic cover on the on the terminal block input after connecting the power. Failure to do so exposes you to a risk of severe injury from electric shock.

Warnings

Warnings tell you 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 means anything requiring repair. Warnings tell you what you should or should not do, and the consequences of not heeding the warning.

Installation warnings

Provides installation warnings to consider.

⚠Warning! Only trained and qualified personnel should install, replace, or service this equipment. Disconnect the power and network cables before servicing.

⚠Warning! Read all of the installation instructions before you connect the system to its power source.

⚠ Warning! When installing the product, always make the ground connection before applying power to the unit. This equipment needs to be grounded to an external ground connection. Use a green and yellow 12 AWG ground wire to connect the host to earth ground during normal use. Disconnect the ground connection only when the unit is completely powered down.

⚠ Warning! While handling the product during this procedure, wear grounding wrist straps to avoid ESD damage to cards and modules. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

⚠ Warning! To prevent personal injury or damage to the chassis, lift the chassis from underneath its lower edge.

⚠ Warning! This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 60950-1 Service Personnel.

⚠ Warning! The Installation of this product must comply with local and national electrical codes. The electrical rating is labeled on the product.

⚠ Warning! This unit is intended for installation in restricted access areas only.

⚠ Warning! This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.

⚠ Warning! Do not work on the system or connect or disconnect cables during periods of lightning activity.

⚠ Warning! To prevent the unit from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 104° F (40° C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.

⚠ Warning! Enclosed racks may have higher ambient temperatures than open racks. Ensure enclosed racks ambient temperatures do not exceed maximum recommended ambient temperature of 104 °F (40 °C).

⚠ Warning! The final disposal of this product must be done according to all national laws and regulations.

Parts warnings

Provides parts warnings to consider.

⚠ Warning! Do not operate the system unless all cards and top cover is in place.

⚠ Warning! On the product, do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that could disrupt other equipment; and they direct the

flow of cooling air through the chassis. To prevent electric shock, do not open the enclosure of the product.

⚠ Warning! To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.

⚠ Warning! Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

⚠ Warning! When connecting equipment to IT power distributions, Phase to phase voltage must not exceed 240 V. Always use the power adaptor and power cord shipped with the product to the correct voltage.

⚠ Warning! The ports on the front of the product are Safety Extra-Low Voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits.

⚠ Warning! This product might have more than one power supply source. All power sources must be removed to de-energize the unit.

⚠ Warning! Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.

⚠ Warning! Do not expose the product to strong magnets or magnetic fields.

⚠ Warning! Keep all liquids and dust away from the product.

⚠ Warning! All optical interfaces and sources connected to this product and its modules must only use Class 1 lasers. Using any other Laser Class source can create hazardous conditions to the user.

⚠ Warning! This product can contain Class 1 lasers. Do not stare into the laser beam or view it directly with optical instruments. Install covers for the laser connectors when they are not in use.

⚠ Warning! Use caution when touching exposed metallic surfaces, which can become hot during normal operation.

⚠ Warning! The cards and modules can get hot during operation. When removing a card or module, hold it by the faceplate and bottom edge. Allow the card or module to cool before touching any other part of it or before placing it in an antistatic bag.

⚠ Warning! The product uses double pole/neutral fusing. Use caution when servicing this product.

⚠ Warning! The user must install only Optical Transceiver Modules that comply with the appropriate standard and/or regulation - UL 60950-1, FDA/CDRH 21 CFR 1040 Class 1, or (IEC/CENELEC) EN 60825 Class 1.

Rack and clearance requirements

Tipping Point recommends that you mount the product in a standard 19-or 23-inch rack.

The vertical hole spacing on the rack rails must meet standard EIA-310-C requirements, which call for a one inch (2.54 cm) spacing. Ensure that you have a minimum of three inches clearance at the side of the ventilation slots.

Note: Some devices have different rack and clearance requirements, or may have other mounting and installation options. Refer to the appropriate chapter in this guide for more information.

Ventilation and location

Ventilation and proper location are essential to the proper operation of the product.

Follow these guidelines to ensure that the product receives adequate ventilation.

- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- Ensure that the unit is positioned properly on the rack.
- There should be three inches clearance at the ventilation openings.
- When mounting this unit in an enclosed or multi-rack assembly, the operating ambient temperature of the rack may be greater than the room ambient temperature. Ensure that the maximum ambient temperature of 104° F (40° C) is not exceeded.

Environmental requirements

For the product to run properly, your environment must meet the proper criteria.

The following table details the recommendations for temperature, humidity, and altitude settings for the Service Provider (SP) environment.

Environmental specifications	Description
Temperature	0 to 40° C (32 to 104° F) — Operating -20 to 80° C (-4 to 176° F) — Storage
Humidity	5 to 95% (non-condensing)
Altitude	No degradation up to 10,000 feet above sea level

Reliable earthing

Ensure that an external grounding connection is available for the product.

Follow these guidelines:

- For AC-powered products, use only the AC power cords that have been provided with the product. Using other cords could be hazardous to your safety.
- For DC-powered products, ensure that the product is grounded to the ground termination connector labeled with the IEC 60417-5019 symbol:



Always make the ground connection first when you install the product, ensuring that it is in place before turning on the power or connecting any network cables. When disconnecting the product, remove the ground connection last, only after the power has been completely turned off and all cables have been disconnected. When the installation is done in a rack, the rack must be grounded to provide an adequate ground location for the ground wire that is attached to the chassis.

ESD requirements

Damage from Electromagnetic Static Discharge (ESD) can occur when electronic components are improperly handled.

Its results can be complete or intermittent system failures. Proper ESD protection is required whenever you handle equipment. It is not necessary to open the product chassis to add or remove any components. The following general grounding guidelines apply in the event that a power supply module or ZPHA module must be replaced.

- Always use an ESD wrist strap when adding or removing components from the chassis.
- Avoid touching the circuit boards or connectors on all cards and modules.
- Avoid contact between the printed circuit boards and clothing. The wrist strap only protects components from ESD voltages on the body. ESD voltages on clothing can still cause damage.
- Place a removed component board-side-up on an antistatic surface or in a static-shielding container that is also grounded to the same point as the IPS. If you plan to return the component to the factory, immediately place it in a static-shielding container.

Hot swapping guidelines

Hot swapping allows you to remove and replace cards without disconnecting power to the system.

Some TippingPoint devices allow you to hot swap cards or modules. The TippingPoint has a comprehensive detection system that senses automatically when you add or remove a card or module. It then runs diagnostic and discovery routines and acknowledges the presence or absence of the card.

If you remove a card or module and replace it with the same type of card or module, the system resumes operation without any operator intervention.

- Do not force the card or module into its slot. This can damage the pins on the backplane if they are not aligned properly with the card or module.
- Ensure that the card or module is straight and not at an angle when you install it in the slot, which can damage the equipment. Use the guide rails to install the card or module correctly.
- Fully depress the ejector tabs to ensure that the card connector mates with the backplane correctly. Firmly seat the card in the slot by locking the card with the black levers.

Unpack the product

Describes how to unpack the product.

Each chassis is securely packaged in a shipping box.

△Caution: ESD can damage the product if you do not take necessary precautions. Installation and maintenance personnel should be properly grounded using ground straps to eliminate the risk of ESD damage to the equipment. All cards and modules are subject to ESD damage whenever they are removed from the chassis.

Use caution when opening the product boxes.

To unpack the product, complete the following steps:

1. Inspect the packing container.

If you see any damage or other signs of mishandling, inform both the local freight provider and TippingPoint before unpacking. Your freight provider can provide you with the procedures necessary to file a claim for damages.

2. Carefully open the box.
3. Remove all packing material.
4. Verify the contents in the shipping package.

Compare the packing list to your shipment and to your order. Are all items included? If items are missing, contact your TippingPoint sales or field representative.

5. Remove the chassis from the box.
6. Open the accessory kit.

It contains the cables, documentation, and management software.

7. Inspect all the equipment inside for damage.

If you think any equipment might be damaged, contact your freight provider for how to lodge a damage claim. Also, contact your TippingPoint sales or field representative for instructions.

Note:



The shipping materials are recyclable. Please save for later use or dispose of them appropriately.

TippingPoint NX-Platform device overview

This topic describes the components, chassis, requirements, and installation of the TippingPoint S2600 NX/S5200 NX/S6200 NX/S7100 NX/S7500 NX devices and their components.

These devices are associated with the following part numbers:

Model	HPE part number	Trend Micro part number
TippingPoint S2600 NX	JC874A	TPNN0026
TippingPoint S5200 NX	JC824A	TPNN0029
TippingPoint S6200 NX	JC873A	TPNN0031
TippingPoint S7100 NX	JC644A	TPNN0034
TippingPoint S7500 NX	JC872A	TPNN0037

Prior to installation, you should also obtain the *IPS Command Line Interface Reference*. After installing the components, complete the TippingPoint Setup Wizard as part of the installation and configuration procedures.

This topic includes the following information:

- [Chassis overview](#) on page 20
- [I/O modules](#) on page 26
- [Model requirements](#) on page 35
- [Technical specifications](#) on page 36
- [Hardware installation and configuration](#) on page 38

Chassis overview

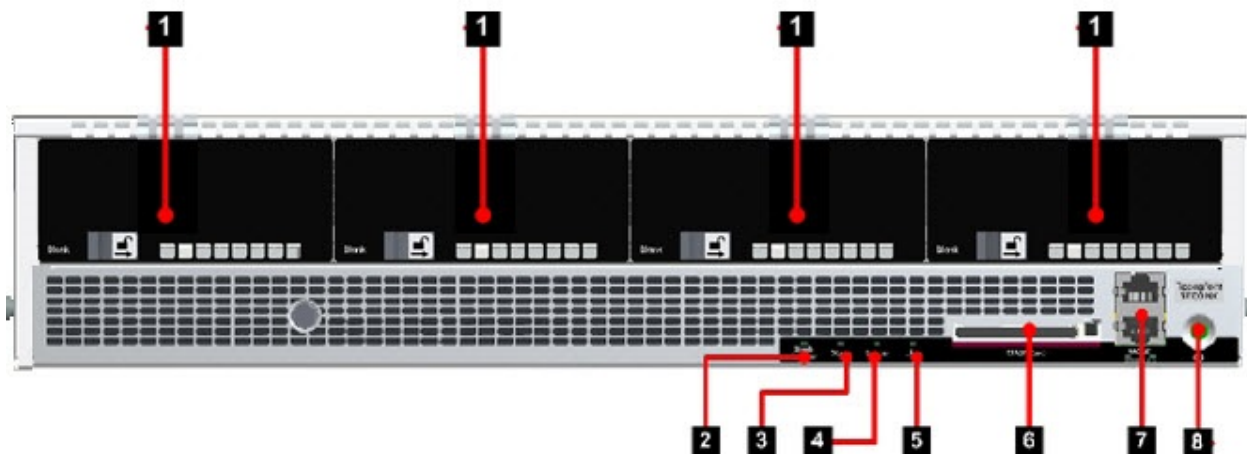
Provides images and an overview of the NX-Platform IPS devices.

The TippingPoint NX-Platform is rack-mountable on a 19- or 23-inch rack and accommodates up to four I/O modules, enabling the user to customize the device to suit the needs of the network. See [I/O modules](#) on page 26 for more information about the available module types.

The following traffic throughputs are supported across multiple copper and fiber segments for each model:

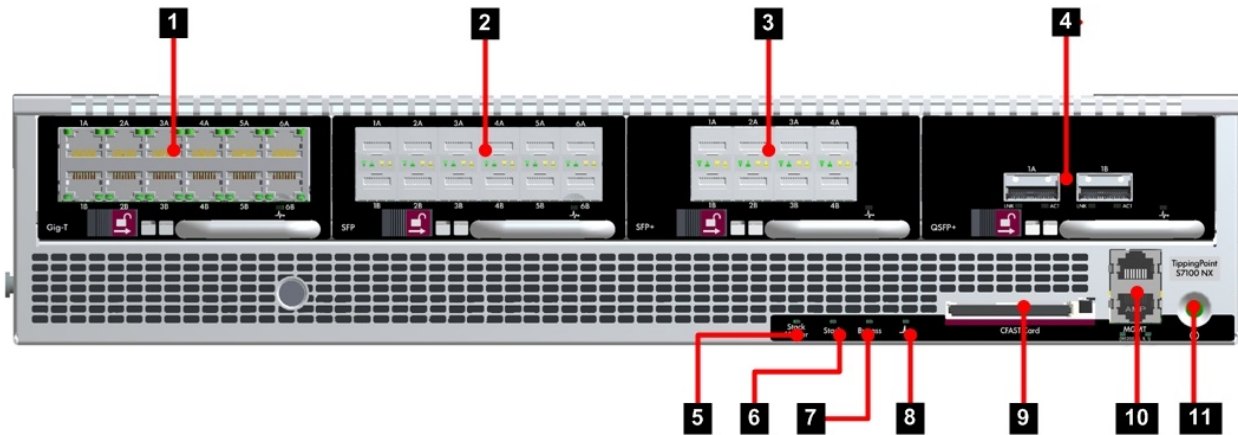
Model	Supported throughput
TippingPoint S2600 NX	Up to 3Gbps
TippingPoint S5200 NX	Up to 5Gbps
TippingPoint S6200 NX	Up to 10Gbps
TippingPoint S7100 NX	Up to 15Gbps
TippingPoint S7500 NX	Up to 20Gbps

Figure 2. TippingPoint NX-Platform IPS - front panel, no modules installed



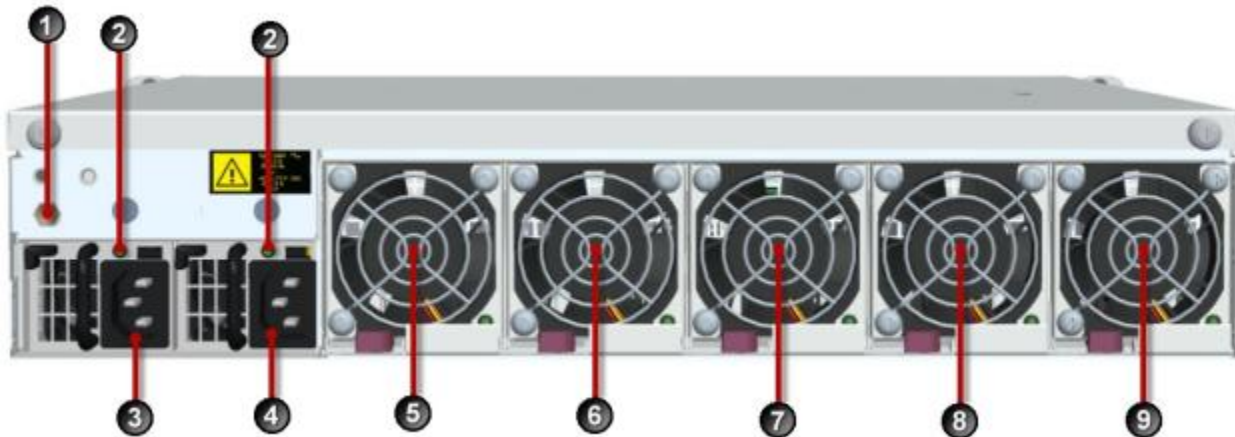
1. Blank module
2. Stack Master LED
3. Stack LED
4. Bypass LED
5. System Health LED
6. CFast Card
7. Console Port (top) and Management Port (bottom)
8. Power Button

Figure 3. TippingPoint NX-Platform IPS - front panel, modules installed



1. 6-Segment Gig-T NX module
2. 6-Segment GbE SFP NX module
3. 4-Segment 10GbE SFP+ NX module
4. 1-Segment 40GbE QSFP+ NX module
5. Stack Master LED
6. Stack LED
7. Bypass LED
8. System Health LED
9. CFAST Card
10. Console Port (top) and Management Port (bottom)
11. Power Button

Figure 4. TippingPoint NX-Platform IPS - back panel



1. Ground strap mounting
2. Power supply health LED
3. Power supply module 1
4. Power supply module 2
5. Fan module 1
6. Fan module 2
7. Fan module 3
8. Fan module 4
9. Fan module 5

Chassis features

Provides links to the various NX-Platform chassis features.

- [Power button](#) on page 23
- [Fans and power supplies](#) on page 24
- [External storage card](#) on page 24
- [Ports](#) on page 24

Power button

The power button is located on the front panel.

The power button light indicates its current status:

- **No light** — Device is powered off.

- **Green** — Device is powered on.

Fans and power supplies

The TippingPoint NX-Platform IPS includes two power supplies and five cooling fans.

See [Power supply and fan modules](#) on page 46.

External storage card

The TippingPoint NX-Platform IPS includes a CFast card slot.

The external storage card is used to store system logs, snapshots, and other system data. The user can remove and insert the card while the device is running; however, the user must be sure to issue the appropriate mounting and preparation commands in the command line interface (CLI).

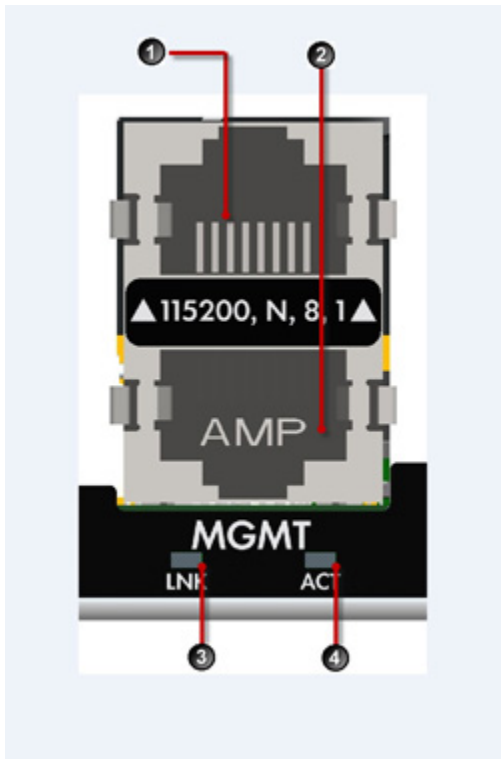
Refer to [Using the external storage card](#) on page 54 for more information.

Ports

Describes the ports of the NX-Platform IPS.

The TippingPoint NX-Platform IPS front panel includes the following ports.

Figure 5. Management and console ports



1. RJ-45 serial console port
2. 1GbE copper management port
3. Link LED
4. Activity LED


The management port LEDs indicate link and activity state:

LED type	Color	Description
Link	Green	Link is active at 1000 Mbps.
	Off	Link is inactive, or is active at 10 Mbps or 100 Mbps.
Activity	Blinking amber	Data traffic is passing.
	Off	No traffic is passing.

Chassis LEDs

The following table describes states of each chassis LED.

Port type	Color	Description
Stack Master	Off	Unit is not stack master or not member of a stack.
	Green	Unit is stack master.
	Yellow	Unit is secondary to master.
	Blinking yellow	Stack election is in progress.
Stack	Off	Unit is not a member of a stack.
	Green	Unit has successfully joined a stack.

Port type	Color	Description
	Yellow	Unit failed to join a stack.
	Blinking yellow	Unit is in process of joining a stack.
	Blinking green	Blink pattern indicates stack ID.
Bypass	Off	The system is not in Layer-2 Fallback (L2FB).
	Red	The system is in L2FB.
System Health 	Solid green	The system health is OK.
	Blinking green	The system is booting up and is not yet ready to inspect traffic.
	Red	The system has a critical error. This could be caused by a number of factors, including temperature or voltage spikes, or fan and power module failures.

I/O modules

Describes the standard and bypass I/O modules.

The TippingPoint NX-Platform IPS supports both standard I/O modules and bypass I/O modules (see the following tables) for fiber and copper components.

Note: Only optical transceiver modules (including SFP, SFP+, and QSFP+) available from TippingPoint have been validated to achieve optimal performance with TippingPoint products. Other vendor devices are not supported. Using other vendor devices could be detrimental to proper operation of the TippingPoint system.




Bypass I/O modules are zero-power high-availability (ZPHA) modules that permit network traffic and services while bypassing the IPS entirely when the IPS loses power. All four standard I/O modules and all five bypass I/O modules are hot-swappable on devices running TOS v3.6.0 or higher.


Important: Hot-swapping a 40GbE I/O module with another 40GbE I/O module is fully supported. However, a full reboot is required under the following conditions:

- If you insert a 40GbE module into a slot which previously did not have a 40GbE module
- If you remove a 40GbE module from a slot and then insert a different module type that is not another 40GbE module

For a list of transceivers supported on NX-Platform device modules, refer to the *TippingPoint Operating System (TOS) Release Notes Version 3.9.0*.

NX-Platform devices support the following standard I/O modules:

Module name	Ports	Port speed	Part number
6-Segment Gig-T NX (Gig-T) 	12 Copper	10/100/1000 Mbps	TPNN0059
6-Segment GbE SFP NX (SFP) 	12 SFP	1Gbps	TPNN0068
4-Segment 10GbE SFP+ NX (SFP+) 	8 Fiber	10Gbps	TPNN0060

Module name	Ports	Port speed	Part number
1-Segment 40GbE QSFP+ NX (QSFP+) 	2 Fiber	40Gbps	TPNN0069

Note: If you insert an SFP into a 10GbE module slot, the port might go down. To use an SFP in a 10GbE module, configure the slot by entering the following command in the command line interface:

```
conf term interface ethernet 1-1A negotiate
```


OR





```
conf term interface ethernet 1-1A no negotiate
conf term interface ethernet 1-1A linespeed 1000
```

You can revert to SFP+ by inserting an SFP+ into the 10GbE module and entering the following command in the command line interface:

```
conf term interface ethernet 1-1A no negotiate
conf term interface ethernet 1-1A linespeed 10000
```

NX-Platform devices support the following bypass I/O modules:

Module name	Ports	Port speed	Part number
NX IPS 4-Segment Gig-T Bypass Module 	8 Copper	10/100/1000 Mbps	TPNN0070

Module name	Ports	Port speed	Part number
NX IPS 2-Segment 1GbE Fiber SR Bypass Module 	4 Multi-Mode Fiber (LC type)	1Gbps	TPNN0071
NX IPS 2-Segment 1GbE Fiber LR Bypass Module 	4 Single-Mode Fiber (LC type)	1Gbps	TPNN0072
NX IPS 2-Segment 10GbE Fiber SR Bypass Module 	4 Multi-Mode Fiber (LC type)	1/10Gbps	TPNN0073
NX IPS 2-Segment 10GbE Fiber LR Bypass Module 	4 Single-Mode Fiber (LC type)	1/10Gbps	TPNN0074

Bypass I/O modules

The NX-Platform IPS supports a range of bypass I/O modules (BIOMs), which combine the IPS segment interfaces with mechanical bypass switches for high-availability purposes.

The BIOMs offered for the NX-Platform support various interface speed and connectivity types, including copper or fiber, 1Gbps or 10Gbps, and long range or short range.

The BIOMs can route traffic within the module when the IPS loses power or when the module is removed from the IPS. Using the LSM, CLI, or SMS, you can also configure the BIOMs to bypass traffic on a per-module basis.

Note: When you hot-insert a BIOM, it remains in bypass mode until an administrator removes it from bypass mode through the CLI, LSM, or SMS. Rebooting the IPS after a hot-insertion also brings the module into normal (non-bypass) mode. After the system has fully rebooted, it is ready for inspection.

BIOM connectors and speeds

The fiber BIOMs are distinguished by speed and type of fiber.

The 10GbE Fiber BIOMs have internal dual-rate SFP+ transceivers that can operate at either 1Gbps (the default) or 10Gbps speeds. For the 10GbE Fiber BIOMs to operate at 10Gbps speeds, the system software determines the module's data rate with the auto-negotiate feature and sets the link speed accordingly.

The BIOM network connections are as follows:

- The NX IPS 4-segment Gig-T Bypass Module (JC877A) can accept network connections for up to four 10/100/1000Mbps copper/RJ45 network segments.
- The NX IPS 2-segment 1Gbps Fiber SR Bypass Module (JC878A) can accept two 1Gbps Short Reach/Multimode (850nm) fiber network segments.
- The NX IPS 2-segment 10Gbps Fiber SR Bypass Module (JC880A) can accept two 10Gbps/1Gbps Short Reach/Multimode (850nm) fiber network segments.
- The NX IPS 2-segment 1Gbps Fiber LR Bypass Module (JC879A) can accept two 1Gbps Long Reach/Single-mode (1310nm) fiber network segments.
- The NX IPS 2-segment 10Gbps Fiber LR Bypass Module (JC881A) can accept two 10Gbps/1Gbps Long Reach/Single-mode (1310nm) fiber network segments.

Notable BIOM behavior

When deploying BIOMs, ensure that traffic passes in the normal inspection mode in addition to when the module is in bypass mode.

BIOMs should continue to pass traffic even while not connected to the NX-Platform device, or while the device is powered off or administratively placed in bypass mode. If the module does not pass traffic under these conditions, ensure that you have the appropriate cable for your network. In many cases, replacing a straight-through cable with a cross-over cable will resolve link issues.

For a list of SFP+ direct access cables currently supported on NX-Platform devices, refer to the *TippingPoint Operating System (TOS) Release Notes Version 3.8.0*.

As long as the network cables are connected, BIOMs can operate in bypass mode even while the module is not inserted into the chassis.

Because the BIOM bypasses passively, a BIOM that is inline and in bypass mode must adhere to the length requirement between a cable's source and destination. For example, if the maximum cable length budget

between equipment A and B is 100 meters, then the cable length between equipment A and BIOM-1A plus equipment B and BIOM-1B cannot exceed 100 meters.

⚠Warning! BIOMs use internal mechanical switches that are highly sensitive. Use care when removing the module from the IPS while the network is still connected to the segment ports. Rough or reckless handling of the BIOM could cause the mechanical switches to break connection, which could result in temporary loss of network connectivity.

Link transitions

Describes how link transitions occur.

When transitioning into or out of bypass mode, a link transition can result. During a link transition, the link goes down briefly and then comes back up. Even though the transition of the bypass happens quickly, some network equipment can take longer to establish a link. To recognize normal patterns for your IPS, take note of the link times required by your network equipment that connects to the bypass module.

Optical insertion loss

Describes how optical insertion loss for BIOM link occurs.

Insertion loss for optical BIOMs is higher than for standard I/O modules. This normal drop in signal power occurs because of the presence of optical switches and the two duplex connections on the module's front panel. Unlike standard I/O modules, insertion loss for a BIOM link happens twice—once when the signal enters the module's duplex connection and once when it exits the connection.

In addition to the duplex adapter loss, the BIOM experiences a drop in signal power between the optical switch and the duplex adaptor as well as between the switch and the SFP+ transceiver. This loss also happens twice—when the signal enters the module and when it exits the module.

The maximum connection lengths to other equipment is limited by the insertion loss during bypass mode. The combined external connection lengths on a bypass port pair must be less than the allowed maximum length for a normal connection adjusted for the bypass module insertion loss.

The following table provides estimates of both nominal and worst-case bypass module optical insertion loss. Note these limitations when configuring your network connections.

	SR multimode		LR multimode	
	Nominal	Worst case	Nominal	Worst case
Each duplex adapter	0.1dB	0.35dB	0.1dB	0.30dB
Each internal fibre	0dB	0.15dB	0dB	0.15dB

	SR multimode		LR multimode	
	Nominal	Worst case	Nominal	Worst case
Switch loss	0.6dB	1.0dB	0.7dB	1.0dB
Total module insertion loss	0.8dB	2.0dB	0.9dB	1.9dB

Default I/O module configuration settings

Describes the default I/O module settings.

Configurations for the I/O modules can be changed after they are set to the defaults values. However, the default settings themselves cannot be changed. These default settings are as follows:

- Module configuration defaults:
 - No action necessary to restart the module
 - No action necessary to delete the slot configuration
- Network port configuration defaults:
 - Auto-negotiation is enabled
 - Line speed set to the maximum for this type of port
 - Duplex set to full
 - Port enabled
- Segment configuration defaults:
 - Segments are named according to Segment `<slotNum >-<segNum >`
 - L2FB action of permit all
 - Link down synch of hub
 - Link down synch wait time of 1 second

Hot-swapping I/O modules

Provides an overview of hot-swapping I/O modules.

I/O modules are hot-swappable. As long as the IPS is running TOS v3.6.0 or higher, I/O modules can be inserted, removed, or replaced while the IPS is operational. I/O modules in other slots are not impacted, and the IPS continues to function and inspect traffic.

Note: Hot-swapping I/O modules during system initialization is not supported.

Important: Hot-swapping a 40GbE I/O module with another 40GbE I/O module is fully supported. However, a full reboot is required under the following conditions:

- If you insert a 40GbE module into a slot which previously did not have a 40GbE module
- If you remove a 40GbE module from a slot and then insert a different module type that is not another 40GbE module

I/O module hot-swapping guidelines

Provides guidelines on hot-swapping I/O modules.

When hot-swapping I/O modules, note the following administrative guidelines:

- If a slot has always been empty, all possible ports and segments on the slot are absent and unavailable.
- If a slot's configuration is erased by the user, configuration of that slot's ports and segments is deleted and all possible ports and segments on the slot become absent and unavailable. However, any policy-related configuration for these ports does not change when the bay configuration is erased and must be manually cleaned up by the user.
- When a module is inserted into a slot or restarted, the system software performs the following evaluation. When the IPS boots up, the evaluation is performed for every module installed in a slot:
 - The module is validated.
 - The status of the module (whether there is a module in the slot, what type of module it is, whether it is being used or is in error) is determined.
 - The physical state (Present or Absent) and availability state (Available or Unavailable) for each possible port and segment on this slot is determined.
 - The configuration is changed and applied as necessary.
 - A syslog message is added (depending on whether the module passed validation and the module status check).
- Removing a module from a slot does not change or reapply the configuration. It also does not change the availability state of ports and segments. It will, however, change the physical state to Absent. An error-level syslog message indicates that the module was removed. In addition, users are shown the physical state when viewing configuration and status related to that slot. These changes also occur when the IPS boots up for every empty slot.

- The following conditions are displayed when the corresponding ports and segments are available, and are hidden when they are unavailable:
 - Segment configuration
 - Network port configuration
 - Network port health
 - Network port throughput performance
 - Traffic profile by network port
- A BIOM that is installed with the system powered on remains in bypass mode. This way the network can continue to pass traffic while users configure the number of network ports and their speeds to meet specific requirements. The BIOM must be taken out of bypass mode either administratively (using the CLI or the LSM) or through a reboot.
- BIOMs that are installed with the power off are taken out of bypass mode automatically by the system software.
- To change a BIOM from bypass mode to normal mode administratively:
 - From the CLI, type:




```
high-availability zero-power no bypass-ips [-slot <slot number>]
```
 - From the LSM menu, click **System > High Availability** and select **Normal** in the **Zero-Power HA External** field.

For more information on making I/O module administrative changes through these interfaces, see the *IPS Command Line Interface Reference TOS Version 3.7* and the *Local Security Manager User's Guide TOS Version 3.7*.

Module LEDs

The following table describes the states of each LED on the I/O module.

Feature	LED	Color	Description
Fixed RJ45 copper port	Link	Green	Link is active.
	Activity	Blinking amber	Data traffic passing.
Optical transceiver port	Link	Green	Link is active.

Feature	LED	Color	Description
	Activity	Amber	Data traffic passing.
Module Health 	Status	Green	The module is configured, in service, and in good health.
		Blinking amber	The module has been inserted and powered up, but is not yet recognized by the software.
		Solid amber	The module is experiencing a fault.
		Off	Module is disconnected, still powering up, or rendered out of service by user.
Bypass 	Status	Off	Module in bypass.
		Green	Module in normal mode (not in bypass).

Model requirements

Provides links to topics that describe power and cabling requirements.

The following topics describe power and cabling requirements for the TippingPoint NX-Platform IPS:

- [Power requirements](#) on page 35
- [Cabling requirements](#) on page 36

Power requirements

Describes the power requirements of the NX-Platform devices.

The TippingPoint NX-Platform IPS requires one input of Alternating Current (AC) that must meet the following requirements:

- AC: Voltage 100 – 240; Current 12 – 6; Frequency 50/60 Hz
- DC: Voltage -40 to -60; Current 24 – 16; SELV

The device's maximum power consumption is 750 W.

⚠ Warning! This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.

The TippingPoint NX-Platform IPS power supply modules are hot-swappable. Refer to the installation instructions that shipped with your replacement power supply module for information about hot-swapping modules.

Cabling requirements

Describes the cable requirements of the NX-Platform devices.

The TippingPoint NX-Platform IPS ships with the following cables:

- Two AC power cables, one for each hot-swappable power supply
- Null modem cable for the serial console management port (DB-9 to RJ-45)

For a list of SFP+ direct access cables currently supported on NX-Platform devices, refer to the *TippingPoint Operating System (TOS) Release Notes Version 3.8.0*.

You can also receive a Right Angle IEC Receptacle power cord for the device. You can use this cable for connecting power to the device in cases where you might not have enough room for a straight power connection cable. This cable helps in situations when you need to install a device in a tight rack with a door. The 90 degree bend in the female end of the cable prevents the cord from being pinched between the device and the door.

Technical specifications

Provides links to topics that describe the hardware and software specifications of the NX-Platform devices.

The following topics describe the hardware, interface, and software specifications for the TippingPoint NX-Platform IPS.

- [Hardware and interface specifications](#) on page 36
- [Software specifications](#) on page 37

Hardware and interface specifications

The following table provides technical specifications for all the TippingPoint NX-Platform devices.

Specification	Description
Dimensions	2RU - 3.41 in x 16.84 in x 22 in (8.67 cm x 42.78 cm x 55.88 cm)
Weight	42 lbs (19.05 kg)
Power Requirements	<ul style="list-style-type: none"> AC: Voltage 100 – 240; Current 12 – 6; Frequency 50/60 Hz DC: Voltage -40 to -60; Current 24 – 16; SELV <p>The device's maximum power consumption is 750 W.</p>
Service Provider operating requirements:	
<ul style="list-style-type: none"> Temperature 	32 to 104° F (0-40° C) — Operating -4 to 158° F (-20 to 70° C) — Storage
<ul style="list-style-type: none"> Altitude 	No degradation up to 10,000 feet (3048 m)
<ul style="list-style-type: none"> Humidity 	5% to 95% (non-condensing)
External interfaces	<ul style="list-style-type: none"> 1x1GbE copper management port 1x1 RJ-45 console port 1 external storage card drive <p>Data port interfaces vary depending on the installed I/O modules. See I/O modules on page 26.</p>

Note: The pluggable transceiver ports do not include SFP, SFP+, or QSFP+ transceivers.

Software specifications

Provides software specification considerations.

To connect to and configure the TippingPoint NX-Platform IPS, you must have a network-connected PC that supports Internet Explorer 7 and up, Firefox 1.5+, Mozilla 1.7+, or Netscape 8.1+.

If you want to use the TippingPoint Security Management System (SMS) to manage the IPS, the TippingPoint SMS device must be installed on your network and you must have the TippingPoint SMS client software V. 3.6 installed on an appropriate client computer. Refer to the SMS documentation for more information.

Hardware installation and configuration

Provides an introduction and topic links for installing and configuring your device.

After you have completed preparation procedures and unpacked the TippingPoint NX-Platform IPS, you can install and configure the components. Prior to installation, you should also obtain the *IPS Command Line Interface Reference*. After installation of the components, run through the OBE Setup Wizard as part of the installation and configuration procedures.

This topic includes the following information:

- [TippingPoint NX-Platform IPS chassis](#) on page 38
- [Attach cables](#) on page 43
- [Check LEDs](#) on page 44
- [Setup wizard](#) on page 45

TippingPoint NX-Platform IPS chassis

Provides the task topics that describe how to install the IPS device.

To install the IPS you must do the following:

- [Determine total rack space](#) on page 38
- [Attach the device to the rack](#) on page 39
- [Power supply and I/O module connections](#) on page 41

Note: The TippingPoint NX-Platform IPS weighs 42 pounds (19.05 kilograms), which exceeds the OSHA limit for a single-person lift. TippingPoint recommends that the device should be lifted by two people.

Determine total rack space

Provides rack space information for your IPS device.

Before you install the chassis, determine the total rack space that is required to install your system. The required rack space will increase if you plan to install multiple systems. The TippingPoint NX-Platform IPS fits in either a 19-inch or a 23-inch wide rack.

Attach the device to the rack

Describes how to load the device onto the rack.

The IPS ships with a slide rail kit to mount the device to the rack. Slide rail kits are also separately available for order from TippingPoint. Refer to the instructions in the slide rail kit for information about installing the slide rails.

If you are bolting the IPS to the rack, follow these guidelines.

⚠ Warning! To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable.

- If the rack comes with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.
- If the rack is partially filled, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If you plan to expand your system to include additional TippingPoint systems in the future, allow space in the rack for additions. During the initial installation, keep in mind the weight distribution and stability of the rack.

Rack-mounting options

You can choose from the following configurations to install your chassis into the rack.

- The most typical rack-mounting configuration is the front mount. To install the chassis through a front mount, secure the two rack-mounting ears to the chassis using the flat-head screws (six on each side) that came with the kit, as shown in the following figure. Secure the rack-mounting ears into the holes of the front rack post with screws (six on each side, not included).

Figure 6. Front mounting



- For extra support against seismic vibrations, you can secure an additional bracket to each of the rack-mounting ears. The seismic brackets accommodate two-post racks that are 5 – 6 inches deep. After securing the chassis to the rack with the standard rack-mounting ears, loosely mount the seismic brackets into the holes of the rack-mounting ears with the provided SEMS screws (four on each side, included). Then secure the seismic brackets to the rear rack post with screws (six on each side, not included). Finally, tighten all screws, including the SEMS screws that fasten both pairs of brackets together.

Figure 7. Reinforced mounting, front view (top) and rear view (bottom)





- For mid-mounting, reverse the two rack-mounting ears and secure them to the chassis using the flat-head screws (six on each side) that came with the kit, as shown in the following figure. Fasten the rack-mounting ears to the rear rack post with screws (six on each side, not included).

Figure 8. Mid-mounting



Power supply and I/O module connections

After you have bolted the IPS to the rack, attach the power supply AC connections.

Depending on the TOS your device is running, insert your I/O modules as described in the following section before turning the power on. For devices running TOS V. 3.5.x, I/O modules must be added with your device turned off. For devices running TOS V. 3.6.0 or higher, I/O modules can be added with

your device running. Refer to [Hot-swapping I/O modules](#) on page 32 for more information on installing modules with the IPS running.

Note: Hot-swapping I/O modules during system initialization is not supported.

To turn the power on, use the power button located on the front panel of the device.

The TippingPoint NX-Platform IPS comes with a power cord retention bracket and a cable management assembly. For instructions on installing these accessories, refer to [Installing the power cord retention bracket](#) on page 51.

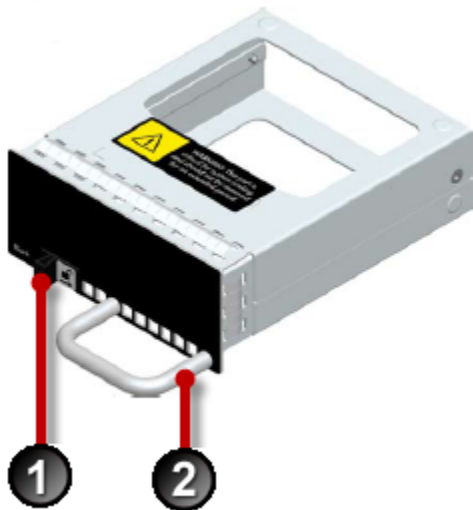
Add I/O modules

Describes how to add I/O modules to your IPS device.

For a complete list of the I/O modules available for the TippingPoint NX-Platform IPS, see [I/O modules](#) on page 26.

The device comes with four blank modules inserted into the module slots.

Figure 9. Blank module



1. Slide latch
2. Handle

To remove the blank module, slide the slide latch to the right and pull the handle.

Figure 10. Removing a blank module



To insert an I/O module, slide the module into the empty module slot. When the module is in the correct position, the slide latch automatically slides into position.

Important: Handle all I/O modules with care. The bypass modules contain mechanical switches that are very sensitive to handling when not installed in the system. Network disruption can occur if handled improperly.

Figure 11. Inserting an I/O module



Attach cables

Describes which connections to use to access the OBE setup wizard.

During setup, use the management processor connection or the console port to access the OBE setup wizard.

To attach the Console port connection

Describes how to attach the console port connection.

1. Connect the RJ-45 null modem cable to the Console port on the unit.
2. Connect the other end of your cable (standard-sized female DB-9 connector) to your VT100-compatible terminal or your computer.

Use the following terminal settings for the Console port:

- Baud rate: 115.2 Kbps
- Character size: 8 bits
- Parity: None
- Stop Bits: One
- Flow Control: None

To attach the Management Processor connection

Describes how to attach the management processor connection.

1. Connect one end of the Category 5 Ethernet cable to the port labeled MGMT located on the front panel.
2. Connect the other end of the Ethernet cable to your network.

This enables remote management.

To attach network connections

Describes how to attach the network connections.

1. Attach the cable for incoming traffic to the A port on the segment.
2. Attach the cable for outgoing traffic to the B port on the segment.
3. Connect the cables to the appropriate ports on your network router.

For more information about TippingPoint NX-Platform IPS configuration and network connections, refer to the *Local Security Manager User Guide*.

Check LEDs

When you connect power to the IPS, the system completes a series of component checks.

It then displays LEDs to show the status of each component. Refer to [Model requirements](#) on page 35 for more information about the LEDs.

Setup wizard

After you have powered on, the TippingPoint Setup wizard is displayed on your COM port terminal.

The wizard prompts you to perform basic configuration tasks and periodically input information. After you run the setup, you can further configure your system using subsequent setup commands through the Command Line Interface (CLI).

See the *IPS Command Line Interface Reference* for detailed instructions.

Power supply and fan modules

This topic provides links to installation instructions for power supply modules and fans.

The following subjects are discussed.

- [NX-Platform AC power supply](#) on page 46
- [NX-Platform DC power supply](#) on page 47
- [NX-Platform fans](#) on page 49

⚠ Warning! This product might have more than one power supply source. All power sources must be removed to de-energize the unit.

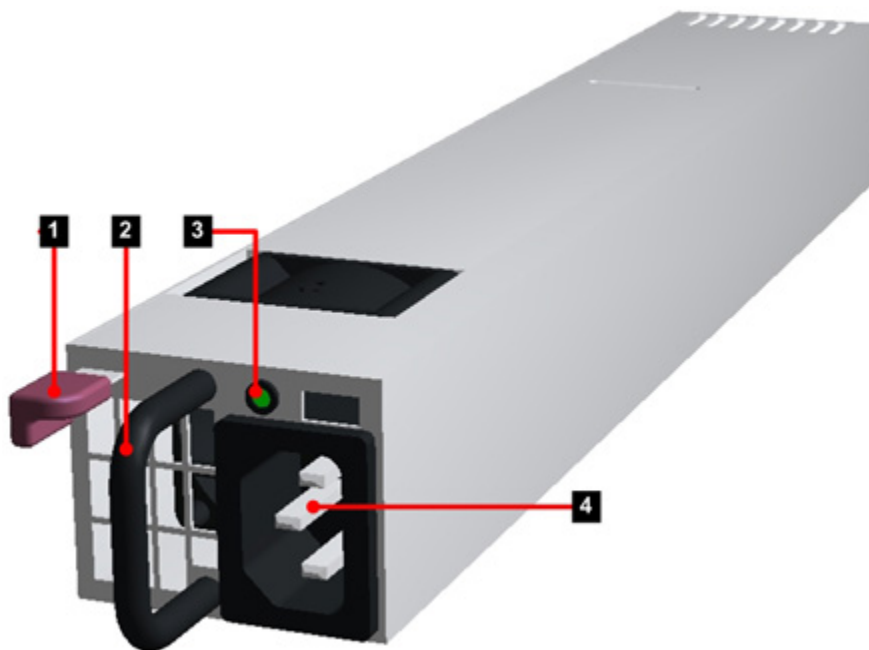
Note: This product has serviceable modules and hot-swappable power supplies. It has no other serviceable parts inside.

NX-Platform AC power supply

Describes how to install the AC power supply.

The NX-Platform device includes two power supply modules. The modules are hot-pluggable, redundant, and current-sharing, and the device can run with one active module.

Figure 12. NX-platform AC power supply



1. Removal latch
2. Handle
3. Status LED
4. AC male power input

The Status LED is green when the module is powered and running normally.

When the AC power supply has been securely placed in the device, use the following procedure to connect power to the AC power supply:

1. Locate the male power input on the back of the chassis.
2. Plug one end of a standard female power plug into the power input.
3. Plug the other end into an AC outlet, power strip, or UPS.

The power should meet the following requirements:

- Voltage: 100 – 240 VAC
 - Current: 12 – 6 Amps
 - Frequency: 50/60 Hz
4. The NX-Platform device returns to its previous power-on state in the event of a power interruption.

If power was on when the interruption occurred, the device automatically powers back on when the power is reconnected; if power was off, the device stays off when the power is reconnected. If necessary, power on the device with the button on the front of the chassis.

NX-Platform DC power supply

Describes how to install the DC power supply.

DC power supplies are available for the TippingPoint N-Platform. Consult your TippingPoint account contact for more information if you require a DC power supply.

The NX-Platform DC power supply is similar to the NX-Platform AC power supply, except that it includes a power input terminal block.

⚠ Warning! When installing the product, always make the ground connection before applying power to the unit. This equipment needs to be grounded to an external ground connection. Use a green and yellow 12 AWG ground wire to connect the host to earth ground during normal use. Disconnect the ground connection only when the unit is completely powered down.

Figure 13. DC grounding screw holes to accept the lug connector attached to ground



△Caution: Do not attach a ground wire to the ground screw on the DC power supply module. Attach the ground wire to the NX-Platform chassis DC grounding screw holes (0.63-inch hole spacing) with #10 screws. The DC grounding screw holes are located in the rear of the NX-Platform chassis. Refer to the preceding image.

The Status LED is green when the module is powered and running normally.

When the DC power supply has been securely placed in the device, use the following procedure to connect power to the DC power supply:

1. Locate the ground screw on the back of the chassis.
2. Attach a 12 AWG ground wire to the chassis ground strap mounting.

The wire should be crimped with a ring lug.

3. Locate the power input terminal block on the back of the module.
4. Attach the 12 AWG DC power wires to the power input terminal block labeled -48V and RTN.

The power wires should be crimped with lug spades to ensure a secure connection.

5. Connect the other side of the power cable to the SELV power source.

The power source should meet the following requirements:

- Voltage: -40 to -60 V
 - 24 – 16 Amps
 - SELV
6. The NX-Platform device returns to its previous power-on state in the event of a power interruption.

If power was on when the interruption occurred, the device automatically powers back on when the power is reconnected; if power was off, the device stays off when the power is reconnected. If necessary, power on the device with the button on the front of the chassis.

NX-Platform fans

Describes how to install NX-Platform fans.

The NX-Platform devices include five cooling fans. The fans are redundant and hot-pluggable, and can be replaced without powering down the device.

The IPS NX-Platform Spare Fan (part number TPNN0084) is a replacement unit and can only be used with TippingPoint NX-Platform devices.

Figure 14. NX Series fan



1. Removal Latch
2. Handle
3. Status LED
 - Green: The fan is running normally.
 - Off: The fan is faulty.

Note: The fan LED will also be off when the system is booting up and when a fan has just been replaced. Ensure that the system is fully booted when checking status.

After you have identified the faulty fan assembly, follow this procedure to replace the fan:

1. Remove the fan assembly by sliding the removal latch to the left and pulling out the fan.
2. Set the faulty fan aside.
3. Remove the new fan assembly from the packaging.

4. Install the new fan assembly by sliding the fan into the open slot.

The latch slides into place automatically.

After you insert the fan module, the fan LED blinks for up to two minutes while the system verifies the fan RPM.

Installing the power cord retention bracket

This topic provides links to topics with installation instructions for the power cord retention bracket.

The following subjects are discussed:

- [Power cord retention bracket](#) on page 51
- [Installing and using the bracket](#) on page 51
- [Removing the bracket](#) on page 53

Power cord retention bracket

Provides a description and image of the power cord retention bracket.

The power cord retention bracket (part number 5066-1202) helps reduce strain on the power cord and power supply outlets.

Figure 15. Power cord retention bracket



Installing and using the bracket

Shows an NX-Platform IPS with the power cord retention bracket installed.

The following figure shows an NX-Platform IPS with the power cord retention bracket installed:

Figure 16. TippingPoint NX-Platform IPS - back panel



1. Ground Strap Mounting
2. Power Cord Bracket

Follow the procedures in this topic to install and use the power cord retention bracket and the cable management bracket.

Installing the bracket

Describes how to install the bracket.

Use the following procedure to install the power cord retention bracket:

1. Orient the bracket against the back surface of the chassis.
2. Slide the bracket over the two shoulder rivets on the back of the chassis.

The spring-loaded plunger in the center of the bracket slides into place.

Using the power cord retention bracket

Describes how to attach the power cord to the retention bracket.

Follow this procedure to attach the power cord to the retention bracket:

1. Fold the power cable and slide it into the slot.
2. Push the folded cable into the slot until the cable loop goes past the sheet metal tabs.
3. Secure the folded cable loop under the sheet metal tabs and attach the power cable to the power supply.

Removing the bracket

If you need to remove one of the brackets, pull the spring-loaded plunger in the middle of the bracket and slide the bracket up and off the shoulder rivets.

Using the external storage card

This topic provides links to topics with external storage card information.

The following subjects are discussed:

- [About the external storage card](#) on page 54
- [External storage card commands](#) on page 54

About the external storage card

The external storage card is used to store system logs, snapshots, and other system data.

The user can remove and insert the card while the device is running; however, the user must be sure to issue the appropriate mounting and preparation commands in the command line interface (CLI).

The device will continue to perform correctly if an external storage card is not available. However, if you attempt to take a system snapshot, the operation fails and an error is recorded in the system log.

All NX-Platform devices come with a pre-formatted 32 GB CFast card.

External storage card commands

Lists the commands used to manage the external storage card.

The following table lists the commands used to manage the external storage card in the CLI. Refer to the *IPS Command Line Interface Reference* for detailed documentation of these commands.

Command	Description
<code>compact-flash format</code>	Formats a new card that has not already been formatted according to TippingPoint guidelines.
<code>compact-flash mount</code>	Manually mounts the inserted card.
<code>compact-flash unmount</code>	Unmounts the card so that the user can remove it.
<code>conf t compact-flash operation-mode authenticate</code>	Sets the device to require authentication when a card is inserted.

Command	Description
<pre>conf t compact-flash operation-mode auto-mount</pre>	Sets the device to automatically mount cards when inserted.
<pre>show compact-flash</pre>	Displays whether the card is mounted, and if so, its model number, serial number, revision number, capacity, operation mode, and mount status.
<pre>show conf compact-flash</pre>	Shows the card's operation mode.

Connector and pinout specifications

This topic provides links to topics with connector and pinout information for the TippingPoint system.

This topic contains the following information:

- [RJ-45 \(COM\) console](#) on page 56
- [RJ-45 Ethernet connectors](#) on page 57
- [Pluggable transceivers](#) on page 58

RJ-45 (COM) console

Describes and provides an image of the RJ-45 connector.

The following figure displays the RJ-45 connector.



Figure 17. RJ-45 connector

The following table shows the RJ-45 console connector pinouts.

Pin number	Signal name
1	Request to Send (RTS)
2	Data Terminal Ready (DTR)
3	Transmit Data (TxD)
4	Ground (GND)
5	Ground (GND)
6	Receive Data (RxD)

Pin number	Signal name
7	Data Set Ready (DSR)
8	Clear to Send (CTS)

RJ-45 Ethernet connectors

Describes how to use the RJ-45 connector under different operating conditions.

Use the following pinout information when your RJ-45 device is operating in 10Mbps/100Mbps mode.

Pin number	Signal name
1	Transmit positive (Tx+)
2	Transmit negative (Tx-)
3	Receive positive (Rx+)
4	Ground (GND)
5	Ground (GND)
6	Receive negative (Rx-)
7	Ground (GND)
8	Ground (GND)

Note: These ports can auto-negotiate their mode and can automatically detect whether they should operate in straight-through or cross-over mode.

Use the following pinout information when your RJ-45 device is operating in 1000Mbps (1GbE) mode.

Pin number	Signal name
1	Twisted Pair 1 positive (TP1+)
2	Twisted Pair 1 negative (TP1-)
3	Twisted Pair 2 positive (TP2+)
4	Twisted Pair 3 positive (TP3+)
5	Twisted Pair 3 negative (TP3-)
6	Twisted Pair 2 negative (TP2-)
7	Twisted Pair 4 positive (TP4+)
8	Twisted Pair 4 negative (TP4-)

Pluggable transceivers

The IPS can also have pluggable transceivers.

Note: Only optical transceiver modules (including SFP, SFP+, and QSFP+) available from TippingPoint have been validated to achieve optimal performance TippingPoint products. Other vendor devices are not supported. Using other vendor devices could be detrimental to proper operation of the TippingPoint system.

For a list of transceivers currently supported on NX-Platform device modules, refer to the *TippingPoint Operating System (TOS) Release Notes Version 3.9.0*.

- TippingPoint NX-platform models that use one or more 4-Segment 10GbE SFP+ NX modules support 10GbE SFP+ (10GbE Enhanced Small Form-Factor Pluggable) transceivers.
- When NX-platform models use one or more 1-Segment 40GbE QSFP+ NX module, the 40GbE QSFP+ (Quad Small Form-Factor Pluggable) transceiver is supported.

The following table details the information for SFP, SFP+, and QSFP transceivers.

Fiber input	Signal
Left side	Transmit
Right side	Receive