ExtremeManagement™

ExtremeAnalytics® PV-A-305 Installation Guide

9035117-02

Published April 2018

Copyright © 2018 Extreme Networks All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks

Software Licensing

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:
www.extremenetworks.com/support/policies/software-licensing

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: http://www.extremenetworks.com/support/contact/

For product documentation online, visit: https://www.extremenetworks.com/documentation/

Table of Contents

About This Guide

This document describes the installation and initial configuration of the Extreme Application Analytics PV-A-305 hardware engine.

This document is intended for experienced network administrators who are responsible for implementing and maintaining communications networks.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
New!	New Content	Displayed next to new content. This is searchable text within the PDF.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words **enter** and **type**	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
[Key] names	Key names are written with brackets, such as **[Return]** or **[Esc]**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **[Ctrl]**+**[Alt]**+**[Del]**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Related Publications

Extreme Management Center™ Documentation

Extreme Management Center documentation, including release notes, are available at: http://documentation.extremenetworks.com.

Extreme Management Center online help is available by clicking the **?** icon in all Extreme Management Center pages. The online help provides detailed explanations of how to configure and manage your network using Extreme Management Center.

For complete regulatory compliance and safety information, refer to the document *Intel® Server Products Product Safety and Regulatory Compliance*.

ExtremeAnalytics PV-A-305 Installation Guide

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- GTAC (Global Technical Assistance Center) for Immediate Support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- Extreme Portal — Search the GTAC knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
- The Hub — A forum for Extreme customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.

- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at internalinfodev@extremenetworks.com.

1 Engine Overview and Setup

This chapter lists the components shipped with the PV-A-305 engine, describes the front and back panels, and provides information on engine specifications.

For complete regulatory compliance and safety information, refer to the document *Intel® Server Products Product Safety and Regulatory Compliance*, available at the following links:

http://download.intel.com/support/motherboards/server/sb/g23122003_safetyregulatory.pdf
http://www.extremenetworks.com/support/documentation/

Kit Contents

The PV-A-305 engine ships with the following components:

- Extreme Networks URL card
- Front bezel label
- A rack mounting kit
- Two rack handles and appropriate screws
- Two AC power cables
- AC power cord bracket and cable clamp kit
- One USB flash drive

Specifications

The physical specifications for the engine are listed in Table 3. The environmental requirements are listed in Table 4 on page 8.

Table 3: PV-A-305 Physical Specifications

Processor	
Processor type	PV-A-305 - Intel® Xeon® E5-2620 v4 processor
Processor speed	2.1 GHz
CPU Cores	8
Memory	

Table 3: PV-A-305 Physical Specifications (continued)

Architecture	2400 MHz Dual Ranked Registered (RDIMM) ECC DDR4
Memory module capacities	4 GB DIMMs
Minimum RAM (included)	64 GB (sixteen 4 GB DIMMs)
Maximum RAM	128 GB (thirty-two 4 GB RDIMMs)
RAID Configuration	RAID 1 with BBU
Drives	
Hard drives	One 960 GB SSD hard drive
Connectors	
Back	
NIC	Four RJ-45
Serial	9-pin, DTE, 16550-compatible
USB	Three 4-pin, USB 2.0-compliant
Video	15-pin VGA
Networking	Two 1 GB Ethernet
Front	
USB	Two 4-pin, USB 2.0-compliant
Video	15-pin VGA
Power	
AC power supply (per power supply)	Redundant power supply
Wattage	750 watts
Input voltage	• 90 – 132 V at 47/63 Hz 8.2 A • 180 – 264 V at 47/63 Hz 4.4 A
Output voltage	• 62.0A at 12 V • 2.1A at 12 VSB
Physical	
Height	4.45 cm (1.72 in.)
Width	43.0 cm (16.93 in.)
Depth	70.99 cm (27.95 in.)
Weight (maximum configuration)	13.15 kg (29 lb.)

Table 4: PV-A-305 Environmental Specifications

Parameter	Limits
Operating temperature	+10°C (+50°F) to +35°C (+95°F) with the maximum rate of change not to exceed 10°C (+50°F) per hour
Storage temperature	-40°C (-40°F) to +70°C (+158°F)

Table 4: PV-A-305 Environmental Specifications (continued)

Parameter	Limits
Storage humidity	50% to 90%, non-condensing at 28°C (82°F)
Vibration, unpackaged	5 Hz to 500 Hz, 2.20 g RMS random
Shock, operating	Half sine, 2 g-force peak, 11 milliseconds
Shock, unpackaged	Trapezoidal, 25 g, velocity change 136 inches/second (40 lb to < 80 lb)
Shock, packaged	Non-palletized free fall in height 24 inches (40 lb to < 80 lb)
ESD	±12 KV except I/O port ±8 KV per Intel® Environmental test specification
Estimated thermal dissipation	1550 BTU/Hr

Front Panel Features

The following figure shows the PV-A-305 engine front panel features. Figure 2 on page 9 shows the front control panel.

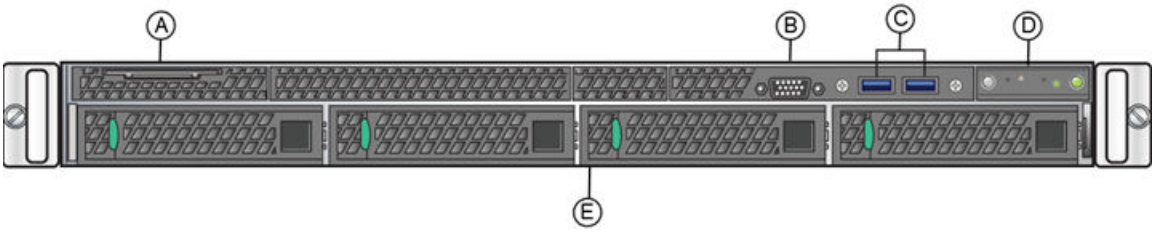


Figure 1: PV-A-305 Front Panel Features

A	System label pull-out	D	Front control panel (see Figure 2 on page 9)
B	Video Connector	E	Hard disk drive bays
C	USB 3.0 Ports		

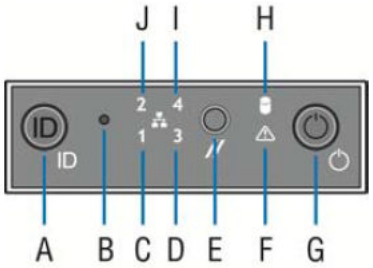


Figure 2: Front Control Panel

A	System ID button w/integrated LED	F	System status LED
B	NMI button (recessed, tool required for use)	G	Power button w/integrated LED

C	Mgmt port activity LED	H	Hard drive activity LED
D	Not used	I	Not used
E	System cold reset button	J	Not used

Hard Drive LED Indicator Patterns

The hard drive has two LED indicators visible from the front of the system: one is a green LED for disk activity, and the other is amber and indicates hard drive status. The LEDs have the following states, as described in Table 5.

Table 5: Hard Drive Activity LED Indicator Patterns

Hard Drive Condition	Activity LED Patterns
Power on and drive spinning up or spinning down	Off
Power on with drive activity	Blinking green

Table 6: Hard Drive Status LED Indicator Patterns

Hard Drive Condition	Status LED Patterns
No access or no fault	Off
Hard drive fault has occurred	Solid amber

Back Panel Features

Figure 3 shows the PV-A-305 engine back panel.

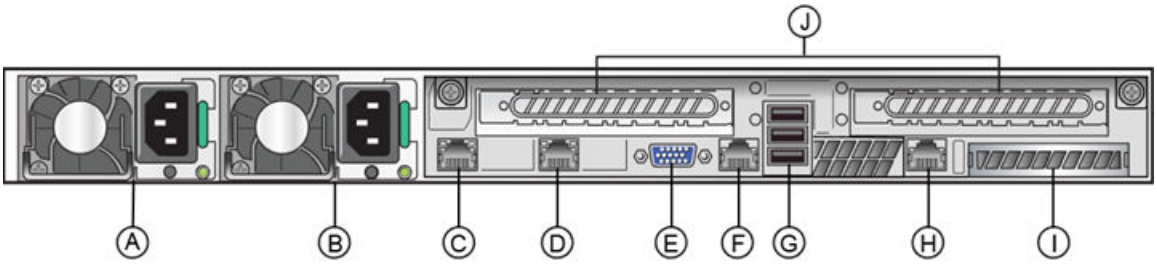


Figure 3: PV-A-305 Back Panel

A	Power supply module #1	F	Serial port
B	Power supply module #2	G	USB 2.0 ports
C	eth0	H	Mgmt port, out of band
D	eth1	I	I/O Module Bay
E	Video connector	J	Riser cards

Table 7 describes the LEDs for the RJ45 management port.

Table 7: RJ45 Port LEDs (Management Port)

LED Type	LED Pattern	Status Indication
Network speed (right)	Off	10 Mbps
	Amber	100 Mbps
	Green	1000 Mbps
Link activity (left)	Off	No link
	Solid Green	Active link
	Blinking Green	Data traffic activity

Power Supply Status Indicator Patterns

The engine has two power supplies, supplying hot-pluggable power redundancy. The system distributes the power load across both power supplies to maximize efficiency.

Each power supply has a single bi-color LED to indicate power supply status, as described in Table 8.

Table 8: Power Supply Status LED Indicator Patterns

LED Pattern	Power Supply Condition
Green	Output on and OK
Off	No AC power to all power supplies
1Hz blinking green	AC present / Only 12VSB on (PS off) or PS in cold redundant state
Amber	AC power cord unplugged or AC power lost. With a 2nd PS in parallel still with AC input power
1Hz blinking amber	Power supply warning events where PS continues to operate — high temp, high power, high current, slow fan
Amber	Power supply critical event causing a shutdown, failure, OCP, OVP, fan fail
2Hz blinking green	Power supply firmware updating

Removing and Installing the Front Bezel

The PV-A-305 engine comes with an optional front panel bezel that can be attached to the front of the chassis by snapping the bezel onto the chassis handles. A key lock allows you to lock the bezel in place so that front panel controls cannot be used. You can still monitor system status indicators with the bezel in place.

Removing the Front Bezel

To remove the front bezel:

1 Unlock the bezel if it is locked.

2 Remove the left end of the front bezel from rack handle.

3 Rotate the front bezel counterclockwise to release the latches on the right end from the rack handle.

Installing the Front Bezel

Note
Before installing the bezel, you must install the rack handles. See Installing the Engine into a Rack on page 12.

To install the front bezel:

1 Lock the right end of the front bezel to the rack handle.
2 Rotate the front bezel clockwise till the left end clicks into place.
3 Lock the bezel, if needed.

Installing the Engine into a Rack

A rack mounting kit and installation guide are included with the PV-A-305 engine. The rack mounting kit allows you to install the engine into a four-post rack cabinet. Refer to the installation guide for complete installation instructions.

If you are table mounting the engine, ensure at least 6 cm of clearance on all sides of the engine for proper ventilation.

If you are installing the engine in a rack:

1 Install the rack handles by aligning a rack handle with the two holes on each side of the engine and attaching each handle to the engine with two screws as shown in Figure 4.

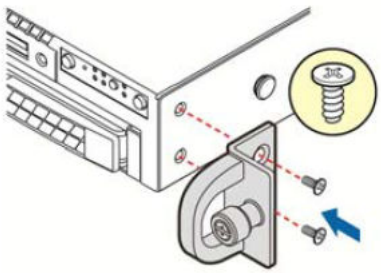


Figure 4: Installing the Rack Handles

2 Read the installation guide included with the rack mounting kit.
3 Install the rails and mount the controller in the rack as instructed.

Torque Values

Table 9 describes the recommended torque values to use when installing the engine using standard threaded fastener machine screws and bolts.

Table 9: Recommended Torque Values by Screw Size

Screw Size		Torque in Pounds			Bit Size
English	Metric	-%5	Nominal	+%5	
N/A	N/A	1.42	1.5	1.57	0
2 – 56	1.5	2.85	3.0	3.15	0
4 – 40	2.5	4.75	5.0	5.25	0/1
6 – 32	3.5	8.55	9.0	9.45	1
8 – 32	4.5	17.10	18.0	18.90	2
10 – 32	5	30.40	32.0	33.60	2
1/4 – 20	6.5	63.65	67.0	70.35	3

2 Configuration

Once the PV-A-305 engine is physically installed into a rack, you need to connect a monitor and a USB keyboard, connect the power cord and network cable, and power it on (see Figure 1 on page 9 and Figure 3 on page 10).

After the engine boots and the engine installation is complete, you must go through the initial configuration process described in this chapter.

This chapter also includes information on how to change your engine settings following your initial configuration and how to upgrade the Extreme Management Center application software. For information on reinstalling the Extreme Management Center engine software, see Reinstalling Engine Software on page 26.

Pre-Configuration Tasks

Ensure that you have the following information prior to executing the configuration steps in the next section:

- Engine hostname, IP address, and netmask
- Default gateway IP address
- Name server IP address and domain name
- NIS (Network Information Services) server IP address
- Network Time Protocol (NTP) server IP address

In addition, you need to obtain the appropriate Extreme Management Center software license prior to launching the Extreme Management Center applications. You will be prompted to enter a license when you launch the application. (When you purchased Extreme Management Center, you received a Licensed Product Entitlement ID. This Entitlement ID allows you to generate a product license. Refer to the instructions included with the Entitlement ID that was sent to you.)

Configuring the Application Analytics Engine

After the initial engine installation is complete, use the following steps to configure the virtual engine to run the Application Analytics application:

1 Login as root with no password, and press **[Enter]**.

The following screen appears:

```
================================================================

Extreme Networks - Application Analytics Engine -

Welcome to the Application Analytics Engine Setup

================================================================

Please enter the information as it is requested to continue with the configuration.
Typically a default value is displayed in brackets. Pressing the [enter] key without
entering a new value will use the bracketed value and proceed to the next item.
If a default value cannot be provided, the prompt will indicate that the item is either
(Required) or (Optional). The [enter] key may be pressed without entering data for
(Optional) items. A value must be entered for (Required) items.
At the end of the setup process, the existing settings will be displayed and
opportunity will be provided to correct any errors.

================================================================

Press [enter] to begin setup or CTRL-C to exit:
```

2 Press **[Enter]** to begin the setup. The Root Password Configuration screen appears:

```
================================================================

Root Password Configuration
================================================================

There is currently no password set in the system administrator
account (root). It is recommended that you set one that is
active the first time the machine is rebooted.
================================================================

Would you like to set a root password (y/n) [y]?
```

Note

You must set a new root password. This new root password will be used by the initial user when logging in to the Application Analytics application.

3 Enter y to set the new root password.

4 Press **[Enter]** and enter the new password as prompted.

```
Enter new UNIX password:

Retype new UNIX password:

Password updated successfully.
```

The Application Analytics Engine Deployment screen appears.

5 Select the deployment mode that matches your network environment.

The default deployment mode is 3.

```
================================================================================
Application Analytics Engine Deployment Modes
================================================================================
This engine supports multiple deployment modes to suit different network environments
and connectivity characteristics. Please select a deployment mode below that best fits
your requirements.

0. Single Interface
     A single interface is used for both management and monitoring traffic.
     Suitable for feeds from XOS/VOSS/SLX switches.
```

```
1. Single Interface With Tunnel
     A single interface is used for both management and monitoring traffic.
     A GRE Tunnel will be configured for traffic monitoring.
     Suitable for feeds from Coreflow switches.

2. Interface Mirrored
     Separate interfaces are configured for management and monitoring traffic.
     The monitoring interface will put into tap mode for traffic monitoring.
     Suitable for feeds from XOS/VOSS/SLX switches.

3. Interface Tunnel Mirrored
     Separate interfaces are configured for management and monitoring traffic.
     The monitoring interface will get its own IP Address and GRE Tunnels will be
configured for traffic monitoring.
     Suitable for feeds from Coreflow switches.

4. Manual Mode
     The interface and tunneling configurations will not be modified by this script,
leaving them to be manually edited by the user instead.

Please select a deployment mode [2]:
```

Note

If you select deployment mode 4, refer to the Extreme Application Analytics Deployment Guide for information on how to configure your deployment manually.

6 If you selected deployment mode 0, 1, 2, or 3 the Application Analytics Engine Network Configuration for eth0 screen appears. For each line, type the requested configuration information and press **[Enter]**.

If you will be using DNS, provide the IP address of the name server. If you are using a name server enter a domain name for the engine. The NIS server is used to authenticate users logging into the engine. If you are using an NIS server, make sure the NIS domain name is valid or users may not be able to log in to the Management Center applications.

```
======================================================================
Application Analytics Engine Network Configuration for eth0
======================================================================
Enter information below to configure eth0

Enter the hostname for the engine (Required):

Enter the IP address for eth0 on 10.54.56.141 [10.54.56.141]:

Enter the IP netmask [255.255.255.0]:

Enter the gateway address [10.54.56.2]:

Enter the IP address of the name server (Optional):

Enter the domain name for 10.54.56.141 (Optional):

Enable NIS (y/n) [n]?
```

7 Continue to the appropriate section:

- For deployment mode 0, proceed to step 9.
- For deployment mode 1, proceed to step 7.
- For deployment mode 2, proceed to step 8.

8 Specify one or more tap ports. If you have an installed the optional PV-A-305-10G-UG I/O module, the ports are eth4 and eth5. For each line, type the requested configuration information and press **[Enter]**.

```
=========================================================================
Application Analytics Engine Network Configuration for Tap Mode
=========================================================================

Enter the interface name for Tap Mode [eth1]:  eth4

Would you like to add another interface for Tap Mode (y/n) [n]? y

Enter the interface name for Tap Mode [eth2]:  eth5

Would you like to add another interface for Tap Mode (y/n) [n]? n
```

Proceed to step 10.

9 Specify one or more GRE tunnel interfaces. If you have an installed the optional PV-A-305-10G-UG I/O module, the ports are eth4 and eth5. For each line, type the requested configuration information and press **[Enter]**.

```
=========================================================================
Application Analytics Engine Network Configuration for Tunnel Interfaces
=========================================================================

Enter the interface name for Tunnel Configuration [eth1]:  eth4

Enter information below to configure eth4

Enter the IP address for eth4 on pv88 [10.54.211.116]:

Enter the IP netmask [255.255.255.0]:

Enter the gateway address [10.54.211.1]:

Would you like to add another interface for Tunnel Configuration (y/n) [n]? y

Enter the interface name for Tunnel Configuration [eth1]:  eth5

Enter information below to configure eth5

Enter the IP address for eth5 on pv88 [10.54.222.117]:

Enter the IP netmask [255.255.255.0]:

Enter the gateway address [10.54.222.1]:

Would you like to add another interface for Tunnel Configuration (y/n) [n]? n
```

10 Enter the IP addresses for one or more GRE tunnels. For each line, type the requested configuration information and press **[Enter]**.

```
=============================================================================
Application Analytics Engine GRE Configuration
=============================================================================
Remote mirroring can be configured in Coreflow Switches using GRE tunnels.
This requires a specific mirroring configuration enabled on the switches.


Enter the SRC IP address for the GRE Tunnel [10.54.211.116]:

Enter the DST IP address for the GRE Tunnel [192.168.1.1]: 10.54.1.116

Add another GRE Tunnel (y/n) [n]? y
```

```
Enter the SRC IP address for the GRE Tunnel [10.54.222.117]:

Enter the DST IP address for the GRE Tunnel [192.168.1.1]: 10.54.2.117

Add another GRE Tunnel (y/n) [n]? n
```

11 A screen appears asking you to confirm your network setting. Enter **0** to accept the settings.

The following example shows the Confirm Network Settings screen for deployment mode 1.

```
=====================================================================
Confirm Network Settings
=====================================================================
These are the settings you have entered. Enter 0 or any key other than a valid
selection to continue. If you need to make a change, enter the appropriate number now
or run the /usr/postinstall/dnetconfig script at a later time.
=====================================================================

0. Accept settings and continue
1. Hostname:                                pv88
2. Deployment Mode:                         Dual Interface Mirrored
3. Management Interface Configuration (eth0):
       Address:                             10.54.184.88
       Netmask:                             255.255.255.0
       Gateway:                             10.54.184.1
       Nameserver:                          10.54.188.120
       Domain name:                         nac2003.com
4. NIS Server/Domain:                       Not Configured
5. Monitor Interface Configuration:
       Tap Mode Interfaces:                 eth4, eth5
```

The following example shows the Confirm Network Settings screen for deployment mode 2.

```
=====================================================================
Confirm Network Settings
=====================================================================
These are the settings you have entered. Enter 0 or any key other than a valid
selection to continue. If you need to make a change, enter the appropriate number now
or run the /usr/postinstall/dnetconfig script at a later time.
=====================================================================

0. Accept settings and continue
1. Hostname:                                pv88
2. Deployment Mode:                         Dual Interface Tunnel Mirrored
3. Management Interface Configuration (eth0):
       Address:                             10.54.184.88
       Netmask:                             255.255.255.0
       Gateway:                             10.54.184.1
       Nameserver:                          10.54.188.120
       Domain name:                         nac2003.com
4. NIS Server/Domain:                       Not Configured
5. Mirror Interface Configuration:
       Name:                                eth4
       Address:                             10.54.211.116
       Netmask:                             255.255.255.0
       Gateway:                             10.54.211.1
       Name:                                eth5
       Address:                             10.54.222.117
       Netmask:                             255.255.255.0
       Gateway:                             10.54.222.1
6. GRE tunnels:                             10.54.211.116/10.54.1.116
                                            10.54.222.117/10.54.2.117
```

12 In the SNMP Configuration screen, type the requested information for each line and press **[Enter]**.

```
=================================================================
SNMP Configuration
```

```
==========================================================================
The following information will be used to configure SNMP management of this device. The
SNMP information entered here must be used to contact this device with remote
management applications such as Extreme Management Center Console.
==========================================================================
Please enter the SNMP user name [snmpuser]:
Please enter the SNMP authentication credential [snmpauthcred]:
Please enter the SNMP privacy credential [snmpprivcred]:
```

13 A summary screen appears asking you to accept your SNMP Configuration settings. Enter **0** to accept the settings.

```
==========================================================================
SNMP Configuration
==========================================================================
These are the current SNMP V3 settings. To accept them and complete SNMP configuration,
enter 0 or any key other than the selection choices. If you need to make a change,
enter the appropriate number now or run the /usr/postinstall/snmpconfig script at a
later time.
0. Accept the current settings
1. SNMP User: snmpuser
2. SNMP Authentication: snmpauthcred
3. SNMP Privacy: snmpprivcred
4. Modify all settings
==========================================================================
Enter selection [0]: 0
```

14 In the Configure Date and Time Settings screen, select whether you want to use an external Network Time Protocol (NTP) server. Enter **y** to use NTP, and enter your NTP server IP address(es). Enter **n** to configure the date and time manually and proceed to step 15.

```
==========================================================================
Configure Date And Time Settings
==========================================================================
The engine date and time can be set manually or using an external
 Network Time Protocol (NTP) server. It is strongly recommended that
NTP is used to configure the date and time to ensure accuracy of time
values for SNMP communications and logged events. Up to 5 server IP addresses may be
entered if NTP is used.
==========================================================================
Do you want to use NTP (y/n) [y]? y
Please enter a NTP Server IP Address (Required): 144.131.10.120
Would you like to add another server (y/n) [n]? y
Please enter a NTP Server IP Address (Required): 144.131.10.121
Would you like to add another server (y/n) [n]? n
```

15 In the NTP Servers validate selection screen, enter **0** to accept the current settings and proceed to the Set Time Zone screen at step 17.

```
==========================================================================
NTP Servers
==========================================================================
These are the currently specified NTP servers. Enter 0 or any key other than a valid
selection to complete NTP configuration and continue.
If you need to make a change, enter the appropriate number from the choices listed
below.
144.131.10.120
144.131.10.121
0. Accept the current settings
1. Restart NTP server selection
2. Set date and time manually
==========================================================================
Enter selection [0]: 0
```

16 If you answered "no" to using an NTP server to set date and time, set the date and time in the Set Date and Time screen.

```
==========================================================================
Set Date And Time
```

```
================================================================
The current system date and time is:    Thu Oct 28 09:34:08 2013
Please enter the values for date and time as directed where input is expected in the
following format:
MM   - 2 digit month of year
DD   - 2 digit day of month
YYYY - 4 digit year
hh   - 2 digit hour of day using a 24 hour clock
mm   - 2 digit minute of hour
ss   - 2 digit seconds
================================================================
Please enter the month [08]:
Please enter the day of the month [02]:
Please enter the year [2016]:
Please enter the hour of day [09]:
Please enter the minutes [34]:
Please enter the seconds [08]:
```

17 In the Use UTC screen, select whether you want the system clock to be set to use UTC.

```
================================================================
Use UTC
================================================================
The system clock can be set to use UTC. Specifying no for using UTC,
sets the hardware clock using localtime.
================================================================
Do you want to use UTC (y/n) [n]?
```

18 In the Set Time Zone screen, select the appropriate time zone and press **[Enter]**.

```
================================================================
Set Time Zone
================================================================
You will now be asked to enter the time zone information for this system. Available
time zones are stored in files in the /usr/share/zoneinfo directory. Please select from
one of the following example time zones:
1. US Eastern
2. US Central
3. US Mountain
4. US Pacific
5. Other - Shows a graphical list
================================================================
Enter selection [1]:
```

19 The Modify Settings screen summarizes the settings you have entered and provides an opportunity to modify the settings, if desired. Enter **0** to accept the settings.

```
================================================================
Modify Settings
================================================================
All of the information needed to complete the installation of the Application Analytics
Engine has been entered. Enter 0 or any key other than a valid selection to continue.
If you need to make a change, enter the appropriate number from the choices listed
below.
================================================================
0. Accept settings and continue

1. Set the root user password

2. Set user to run server as

3. Set hostname and network settings

4. Set SNMP settings

5. Set the system time

6. Modify all settings
```

```
Enter selection [0]:
```

The Application Analytics application software is automatically installed. This may take a few minutes. When the installation is complete, you see the following screen.

```
================================================================

Extreme Networks - Application Analytics Engine - Setup Complete

================================================================

Setup of the Application Analytics Engine is now complete. The engine is now operational
and ready to accept remote connections. Details of the installation are located in
the /var/log/install directory.

================================================================
```

Launching the Application Analytics Application

Now that you have configured the Application Analytics engine, you are ready to access the Extreme Management Center Launch Page and run the applications from a remote client machine.

1 Open a browser window on the remote client machine and enter the Extreme Management Center Launch page URL in the following format:

`http://<servername>:8080/`

where *<servername>* is the Extreme Management Center engine IP address or hostname, and 8080 is the required port number. For example,

`http://10.20.30.40:8080/`

The Extreme Management Center Launch Page opens.

2 Enter your Extreme Management Center username and password and click **Login**.

3 Click the Analytics tab at the top of the window.

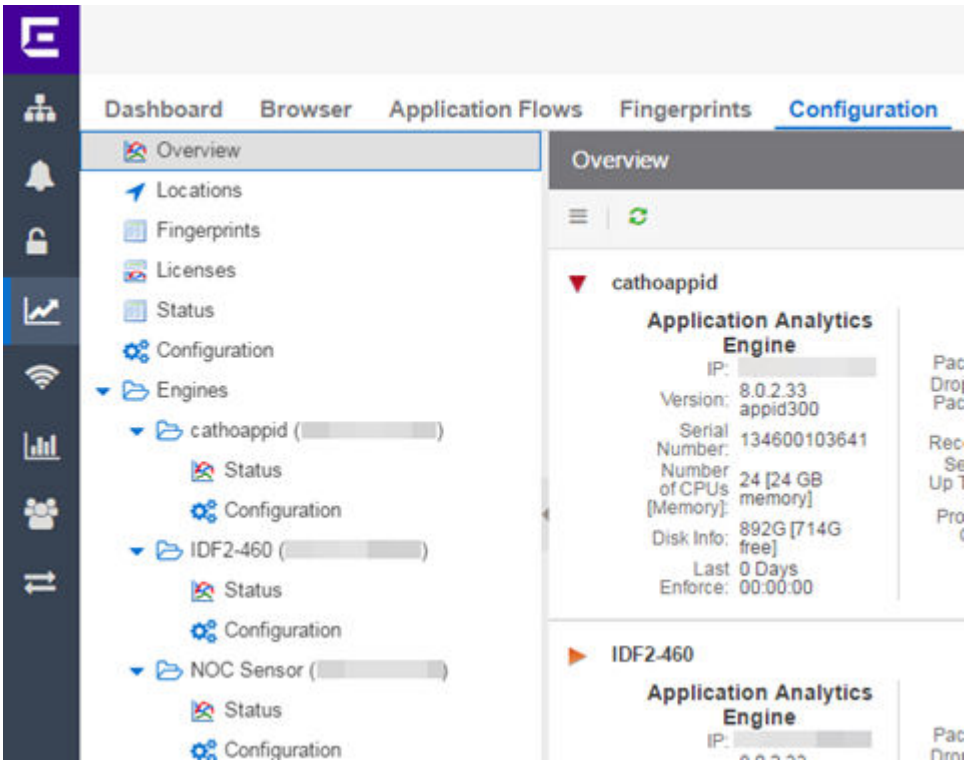
The Analytics tab displays.

For more information on the Extreme Management Center Launch page, access the Online Help by clicking on **?** in top-right corner. In the Online Help Table of Contents, select *Installation Guide* and then read the section titled "Remote Client Launch."

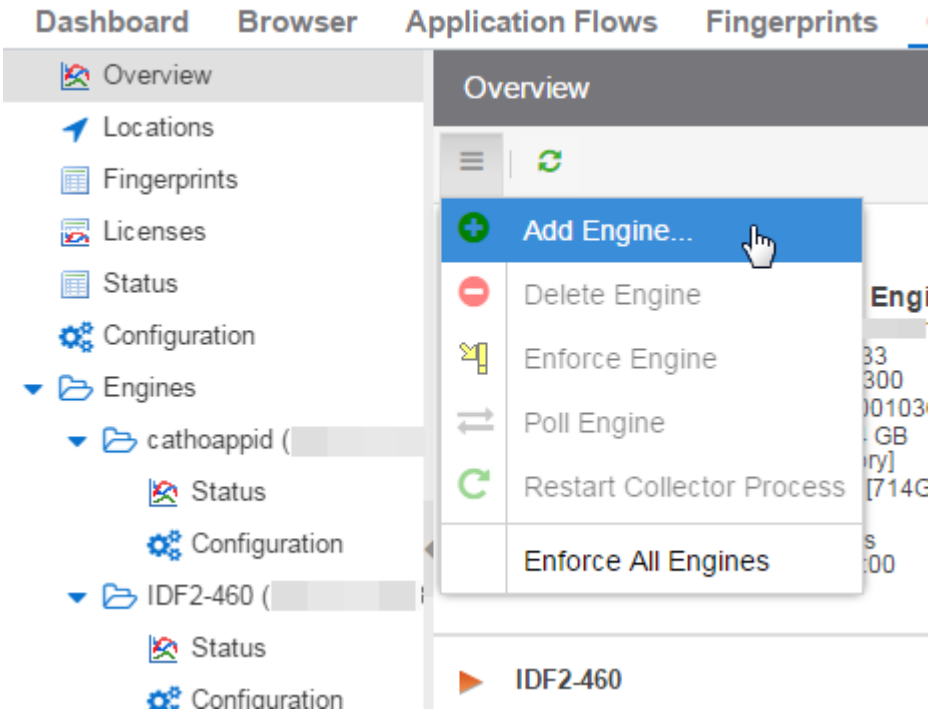
Adding the Application Analytics Engine

To add the Application Analytics engine to the Analytics tab in Extreme Management Center:

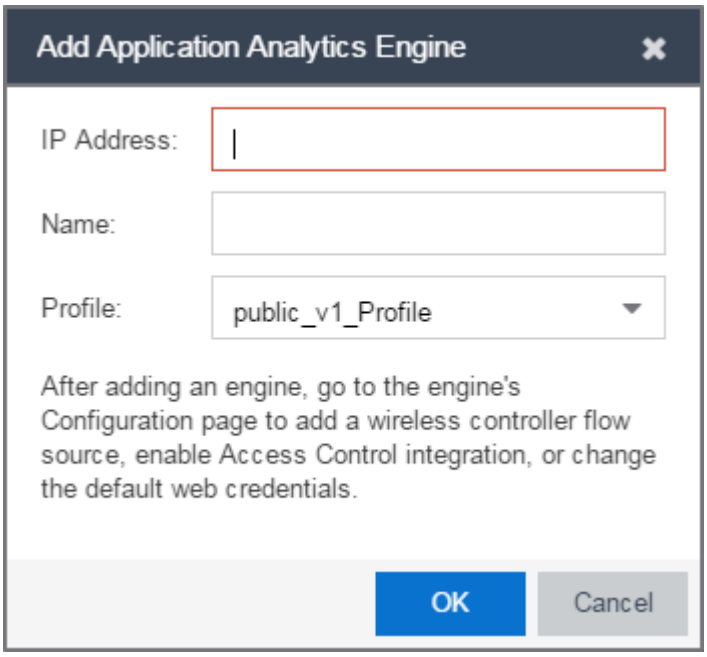
1 Select the Configuration tab in the Analytics tab.



2 Click the **Menu** icon and select **Add Engine**.



The Add Application Analytics Engine window displays.



3 Enter the **IP Address** of the eth0 interface and the **Name** of the Application Analytics engine.
4 Select the appropriate SNMP Profile from the **Profile** drop-down menu.
5 Click **OK**.
6 Select **Enforce Engine** from the drop-down menu.

The Application Analytics engine is added to Management Center.

Changing Application Analytics Engine Settings

Use these steps if you need to change your Application Analytics engine settings following your initial engine configuration.

Changing Basic Network Configuration

To change basic network configuration settings such as hostname and engine IP address, enter the following command at the engine CLI:

```
/usr/postinstall/dnetconfig
```

This starts the network configuration script and allows you to make the required changes. You must reboot the engine for the new settings to take effect.

Changing SNMP Configuration

To change SNMP configuration settings such as SNMP Trap Community String, SNMP User, SNMP Authentication, and SNMP Privacy credentials, enter the following command at the engine CLI:

```
/usr/postinstall/snmpconfig
```

This starts the SNMP configuration script and allows you to make the required changes.

Changing Date and Time Settings

To enable or disable using NTP to configure the engine date and time, or to manually set the date and time on the engine, enter the following command at the engine CLI:

```
/usr/postinstall/dateconfig
```

This starts the date and time configuration script and allows you to change the settings.

Changing the Management Center Server IP Address

To change the IP address of the Management Center server, enter the following command at the engine CLI:

```
/opt/appid/configMgmtIP <ipaddress>
```

Enter the following command to start using the new Management Center server:

```
service appidserver restart
```

Changing the Web Service Credentials

The Web Service credentials provide access to the Application Analytics Engine Administration web page and the web services interface for the Application Analytics engine. Engines are shipped with a preconfigured default password.

If you have changed the credentials in the Analytics tab and then install a new engine using the default password, you will not be able to monitor or enforce to the new engine until you change the password on the engine using this command. The credentials you enter on the engine must match the credentials specified in **Analytics** > **Configuration**.

To change Web Service credentials:

1. Enter the following command at the login prompt in the Console tab:
   ```
   /opt/appid/configWebCredentials <username> <password>
   ```
2. Restart the engine:
   ```
   service appidserver restart
   ```

Upgrading Application Analytics Engine Software

Upgrades to the Application Analytics engine software will be made available from the Network Management Suite (NMS) Download web page.

1. Download the Extreme Analytics Engine Image 64bit (ZIP) file to your system.

   To download an engine image:

   1. Access the Extreme Portal at: https://extremeportal.force.com/.
   2. After entering your email address and password, you are on the Support page.
   3. Click the **Products** tab and select **ExtremeAnalytics**.
   4. Click **ExtremeAnalytics** in the right-panel.

5 Select a version.

6 Download the following image file and extract the file to a directory on your system:

`Application Analytics Engine Upgrade (BIN)`

2 Use FTP, SCP, or a shared mount point, to copy the upgrade file to the Application Analytics engine.

3 SSH to the engine.

4 Cd to the directory where you downloaded the upgrade file.

For example, enter the following to change to the /Users/jsmith directory: `cd /Users/jsmith`

5 Change the permissions on the upgrade file by entering the following command:

`chmod 755 purview_appliance_upgrade_to_`*`version`*`.bin`

6 Run the install program by entering the following command:

`./purview_appliance_upgrade_to_`*`version`*`.bin`

The upgrade begins automatically.

The Application Analytics engine restarts automatically when the upgrade is complete. Because your Application Analytics engine settings were migrated, you are not required to perform any configuration on the engine following the upgrade.

A Reinstalling Engine Software

In the event a software reinstall becomes necessary, use this procedure. Be aware that this procedure reformats the hard drive and reinstalls all the engine software, the operating system, and all related Linux packages.

Connect a monitor and a USB keyboard to the Application Analytics engine prior to performing these steps.

1 Download the Extreme Analytics Engine Image 64bit (ZIP) file to your system.

To download an engine image:

1 Access the Extreme Portal at: https://extremeportal.force.com/.
2 After entering your email address and password, you are on the Support page.
3 Click the **Products** tab and select **ExtremeAnalytics**.
4 Click **ExtremeAnalytics** in the right-panel.
5 Select a version.
6 Download the following image file and extract the file to a directory on your system:

`Application Analytics Engine Upgrade (BIN)`

2 Insert the USB flash drive that came with the PV-A-305 engine into the USB port on your system and note the drive letter it is assigned.
3 Format the USB flash drive.
4 Open a command prompt window and cd to the directory where you extracted the file.

For example, enter the following to change to the /Users/jsmith directory: `cd /Users/jsmith`

5 Type `make_disk.bat` *`drive letter`*`:`.

Note
Because the reinstall procedure reformats the drive, be sure you have specified the correct drive letter.

6 Press **[Enter]**.

The files are copied to the USB flash drive. When the copy is complete you see the message:
`Successfully installed into <drive letter>: Press any key to continue.`

7 Remove the USB flash drive from your system.
8 Insert the USB flash drive into a USB port on the engine (see Figure 1 on page 9).
9 Press the power button on the PV-A-305 engine.

10 Verify the USB flash drive is available as a boot option:

   a Press **F2** to open the BIOS Setup Menu when prompted, as shown in the figure below.

   b Press the right arrow button to select the Boot Options tab.

   c Select **Internal EFI Shell** as **Boot Option #1** in the boot menu.

   d Select **[Enabled]** in the **USB Boot Priority** field.

   e Press `F10` to save the changes.

   A confirmation window displays.

   f Select **Yes** and press **[Enter]**.

   The engine restarts.

11 Type **F6** to open the Boot Menu when prompted, as shown in the figure below.

12 Select **Install** <*version number*> from the menu.

   The installation begins automatically and once complete, the engine shuts off.

13 Remove the USB flash drive.

14 Turn on the engine.

15 Proceed to Configuration on page 14, and follow the instructions for configuring the engine.

Glossary

ad hoc mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an AP.

ARP

Address Resolution Protocol is part of the TCP/IP suite used to dynamically associate a device's physical address (MAC address) with its logical address (IP address). The system broadcasts an ARP request, containing the IP address, and the device with that IP address sends back its MAC address so that traffic can be transmitted.

ATM

Asynchronous Transmission Mode is a start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

BSS

Basic Service Set is a wireless topology consisting of one access point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also *IBSS (Independent Basic Service Set)*.

Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

CHAP

Challenge-Handshake Authentication Protocol is one of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

CLI

Command Line Interface. The CLI provides an environment to issue commands to monitor and manage switches and wireless appliances.

Data Center Connect

DCC, formerly known as DCM (Data Center Manager), is a data center fabric management and automation tool that improves the efficiency of managing a large virtual and physical network. DCC provides an integrated view of the server, storage, and networking operations, removing the need to use multiple tools and management systems. DCC automates VM assignment, allocates appropriate network resources, and applies individual policies to various data objects in the switching fabric (reducing VM sprawl). Learn more about DCC at http://www.extremenetworks.com/product/data-center-connect/.

DoS attack

Denial of Service attacks occur when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable

from normal heavy traffic. ExtremeXOS software has configurable parameters that allow you to defeat DoS attacks.

DSSS

Direct-Sequence Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare with *FHSS (Frequency-Hopping Spread Spectrum)*.)

EAP-TLS/EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.
In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
(See also *PEAP (Protected Extensible Authentication Protocol)*.)

ESRP

Extreme Standby Router Protocol is an Extreme Networks-proprietary protocol that provides redundant Layer 2 and routing services to users.

Extreme Access Control

EAC, formerly NAC™, featuring both physical and virtual appliances, is a pre- and post-connect solution for wired and wireless LAN and VPN users. Using Identity and Access appliances and/or Identity and Access Virtual Appliance with the *Extreme Management Center* software, you can ensure only the right users have access to the right information from the right place at the right time. EAC is tightly integrated with the Intrusion Prevention System (IPS) and Security Information and Event Manager (SIEM) to deliver best-in-class post-connect access control. Learn more about EAC at http://www.extremenetworks.com/product/extreme-access-control/.

Extreme Application Analytics

EAA, formerly Purview™, is a network powered application analytics and optimization solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations, and devices. EAA provides data to show how applications are being used.

This can be used to better understand customer behavior on the network, identify the level of user engagement, and assure business application delivery to optimize the user experience. The software also provides visibility into network and application performance allowing IT to pinpoint and resolve performance issues in the infrastructure whether they are caused by the network, application, or server. Learn more about EAA at http://www.extremenetworks.com/product/extremeanalytics/.

Extreme Management Center

Extreme Management Center (Extreme Management Center), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. Extreme Management Center reaches beyond ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, Extreme Management Center becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about Extreme Management Center at http://www.extremenetworks.com/product/management-center/.

ExtremeCloud

ExtremeCloud is a cloud-based network management Software as a Service (SaaS) tool. ExtremeCloud allows you to manage users, wired and wireless devices, and applications on corporate and guest networks. You can control the user experience with smarter edges – including managing QoS, call admission control, secure access policies, rate limiting, multicast, filtering, and traffic forwarding, all from an intuitive web interface. Learn more about ExtremeCloud at http://www.extremenetworks.com/product/extremecloud/.

ExtremeSwitching

ExtremeSwitching is the family of products comprising different switch types: Modular (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); Stackable (X-series and A, B, C, and 7100 series switches); Standalone (SSA, X430, and D, 200, 800, and ISW series); and Mobile Backhaul (E4G). Learn more about ExtremeSwitching at http://www.extremenetworks.com/products/switching-routing/.

ExtremeWireless

ExtremeWireless products and solutions offer high-density WiFi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at http://www.extremenetworks.com/products/wireless/.

ExtremeXOS

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway, OpenFlow, and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy. Learn more about ExtremeXOS at http://www.extremenetworks.com/product/extremexos-network-operating-system/.

FHSS

Frequency-Hopping Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that 'hops' in a random but predictable sequence from frequency to frequency as a function of time

over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare with *DSSS (Direct-Sequence Spread Spectrum)*.)

IBSS

An IBSS is the 802.11 term for an ad hoc network. See *ad hoc mode*.

MIC

Message Integrity Check (or Code), also called 'Michael', is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte ICV appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.
Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with.

netmask

A netmask is a string of 0s and 1s that mask, or screen out, the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the netmask allows the specific host computer address to be visible.

PEAP

Protected Extensible Authentication Protocol is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (See also *EAP-TLS/EAP-TTLS*.)

SSL

Secure Socket Layer is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the public-and-private key encryption system, which includes the use of a digital certificate. SSL is used for other applications than SSH, for example, OpenFlow.

syslog

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.
syslog uses the UDP as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)

Index

Numerics

A

B

C

D

F

P

R

S

T