Automatic Signature Extraction

First Published: July 19, 2007

The Automatic Signature Extraction (ASE) feature helps shorten the response time for identifying malware by dynamically extracting signatures of unknown viruses and worms traversing the network without the need for human intervention.

Before Cisco IOS Release 12.4(15)T, network protection from malware such as botnets, viruses, and worms was accomplished by deploying solutions that rely on manual signatures to identify the malware. Normally, security professionals require approximately 8 to 12 hours to generate a signature for a new piece of malware. This time interval had been acceptable for thwarting malware, but is no longer acceptable nor scalable due to the exponential increase in malware that is seen on networks.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Automatic Signature Extraction" section on page 24.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

Prerequisites for Automatic Signature Extraction

The following prerequisites apply for the ASE collector.

See the "Automatic Signature Extraction Collector Operation" section on page 4 for more information on the ASE collector.

- The ASE collector runs on an x86-based Linux PC and must have IP connectivity to the network and ASE sensors. Threat Information Distribution Protocol (TIDP) is the communication protocol used between the Linux-based ASE collector and Cisco IOS-based ASE sensors.
- It is recommended that the ASE collector software image run on RedHat Enterprise Linux AS Release 3 or a later release.

Note Contact your Cisco representative for more information about installing the ASE collector functionality on your network.

Restrictions for Automatic Signature Extraction

Contact your Cisco representative for any restrictions concerning the ASE collector or ASE sensor implementation.

Information About Automatic Signature Extraction

The following sections describe how the ASE feature works and how ASE is implemented on a WAN:

- Automatic Signature Extraction Overview, page 3
- Automatic Signature Extraction Sensor Operation, page 3
- Automatic Signature Extraction Collector Operation, page 4
- Automatic Signature Extraction Implementation on a Network, page 5

Automatic Signature Extraction Overview

The Automatic Signature Extraction feature is used to identify and define potential worms and viruses found in network traffic based on the following characteristics:

- Content invariance identifies that all worms have some code that remains unchanged through the infection.
- Content prevalence identifies if packet payloads were observed frequently in the network. Because worms are designed to spread, the unchanged portion of a worm's content appears frequently on a network as it spreads or attempts to spread.
- Address dispersion identifies whether the same payload is sent to and from a large number of source and destination IP address pairs.

Note The ASE feature can detect e-mail viruses but is disabled by default. This feature can be enabled on the ASE collector. Contact your Cisco representative for more information.

When the ASE sensor extracts a malware signature, the ASE sensor sends the signature to the collector using the TIDP Threat Mitigation Service (TMS) to contain and mitigate the malware outbreak among TMS consumers spread across the network. The TMS framework rapidly and efficiently distributes threat information to devices on the network and generates actions to TMS consumers to either drop or redirect the packets containing the malware signature.

Note See the "Automatic Signature Extraction Sensor Operation" section on page 3 for more information on this feature.

See *TIDP Based Mitigation Services* for more information on TMS operation.

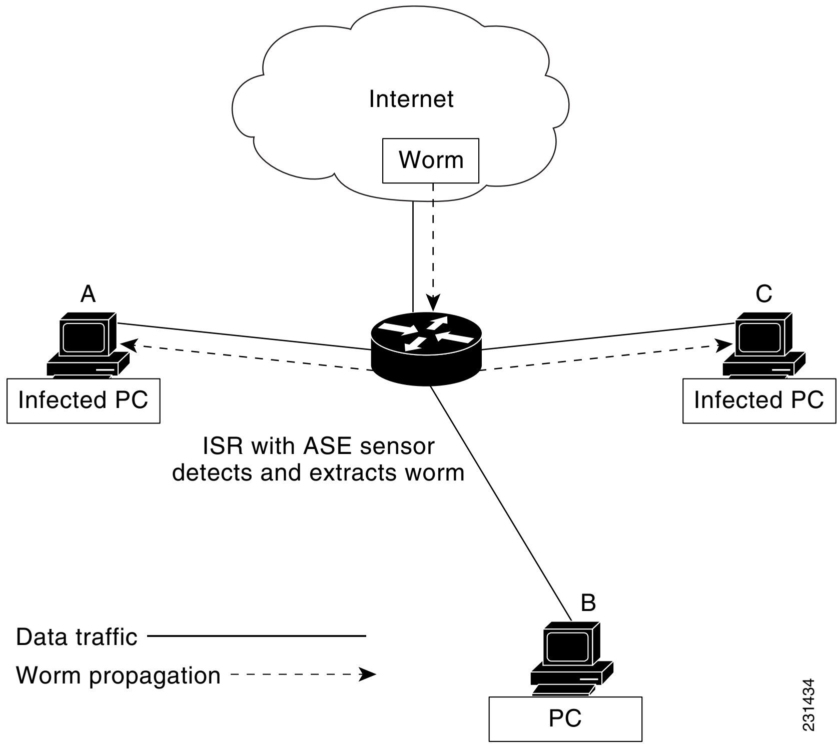
Automatic Signature Extraction Sensor Operation

The ASE feature has two main components: a sensor and collector. The ASE sensor sifts through the contents of network traffic to reduce the number of different source and destination addresses seen in packets. To minimize the impact on the device, sensing can be enabled or disabled on a per-interface basis and traffic designated as ASE traffic can be specified. The ASE sensor observes the same traffic as the router can observe after an access list is applied.

Note The sensor is unable to extract signatures from within encrypted traffic passing through a router.

Figure 1, Cisco IOS Signature Extraction, shows that devices A and C are infected with the same worm. As traffic crosses the Cisco IOS router running the ASE sensor, the router extracts the worm's signature based on its address dispersion and content prevalence. Then the router sends this information to the ASE collector for further processing.

Figure 1 Cisco IOS Signature Extraction



Automatic Signature Extraction Collector Operation

The ASE collector, which runs on a Linux-based PC, performs the following functions:

- Processes signatures it receives from the ASE sensor.
- Initiates the mitigation of signatures.
- Coordinates detection between multiple ASE sensors.
- Manages and distributes entry information and files on the network.
- Collects signatures and packets sent by the sensor.
- Analyzes extracted signatures to determine what the best signature is for a malicious packet to correctly identify a threat.
- Performs post processing of signatures to reduce false alarms.
- Maintains a signature database.
- Reduces false positives in signatures through classification.
- Manages sensor configuration such as thresholds, scanning criteria, and other parameters.
- Generates a report or reports on collected signatures.

Note Contact your Cisco representative for more information about installing the ASE collector functionality on your network.

Automatic Signature Extraction Implementation on a Network

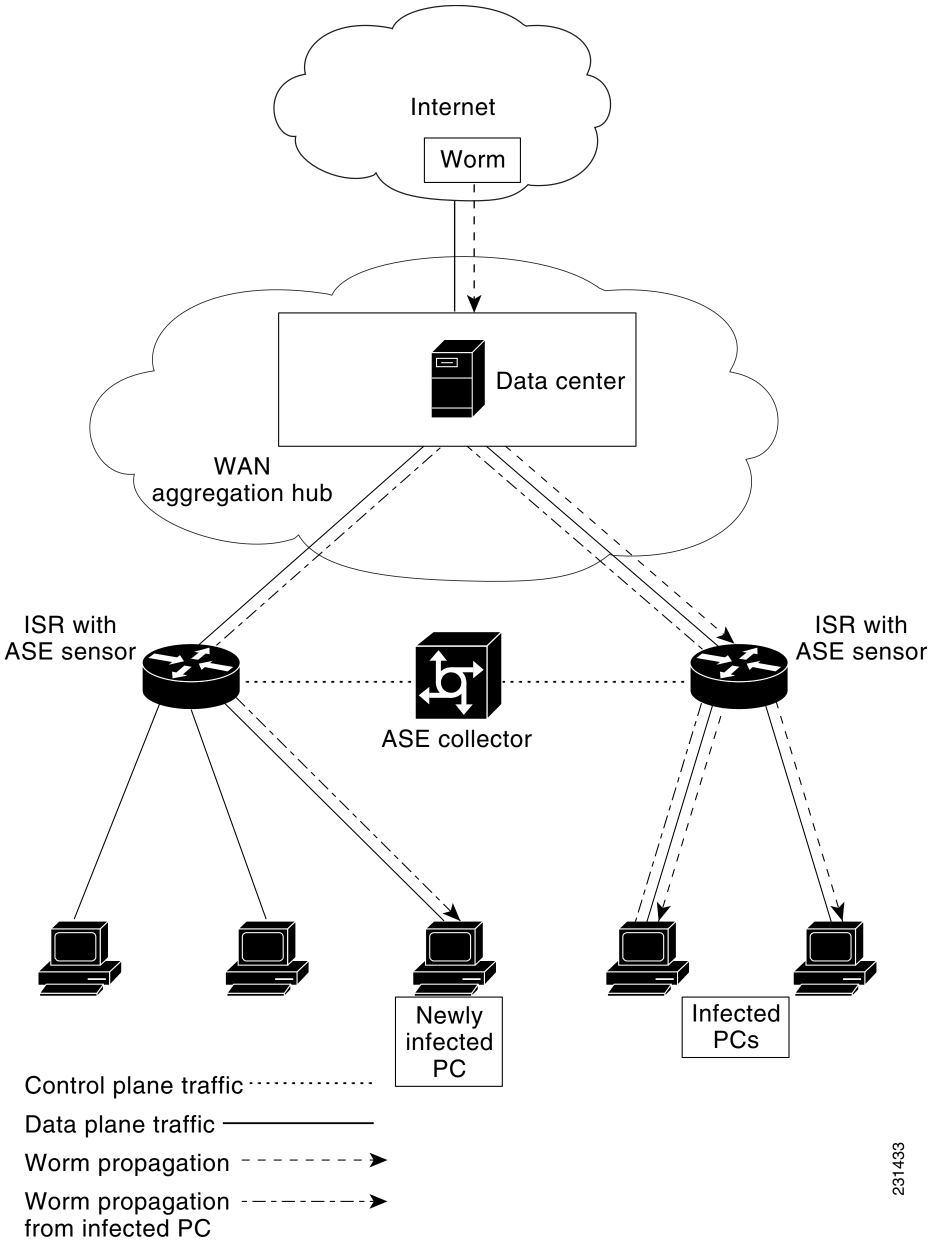
Self-propagating worms continue to grow and affect the security of hosts and networks. These malicious malware attacks often target specific victims or subnets within an enterprise organization. Specifically, a worm can affect and saturate the local network (including all hosts), the branch router, and the local WAN connection or both. The optimal location to detect, contain, and mitigate these worms is on the gateway network connection to prevent the worms from spreading to the entire network, including all connected branches.

Using the WAN Aggregation Model to Contain Malware

The ASE sensor is typically deployed on the Customer Premises Equipment (CPE) WAN so that worms closest to the source can be extracted and prevented from spreading to other areas of the enterprise network.

The WAN aggregation model refers to the traditional deployment scenario in which CPEs are terminated over WAN links to an aggregation HUB. In this model, the CPEs would serve as ASE sensors, and the aggregation HUB would provide ASE Collector functionality. Figure 2, WAN Aggregation Model, shows how worm signatures are extracted at the CPEs and the HUB site with the ASE sensor and shows how the ASE sensor uses this signature information with the ASE collector to contain the outbreak.

Figure 2 WAN Aggregation Model



How to Configure Automatic Signature Extraction

This section contains the following task:

- Configuring Automatic Signature Extraction

Configuring Automatic Signature Extraction

This section describes how to configure the Automatic Signature Extraction sensor feature on an ISR router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ase group** *TIDP-group-number*
4. **ase collector** *ip-address*
5. **ase signature extraction**
6. **interface** *interface-type number*
7. **ase enable**
8. **end**
9. **show ase**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`ase group`** *`TIDP-group-number`*
	Example:
	`Router(config)# ase group 10`
		The group number range is between 1 and 65535, which identifies the TIDP group number used for exchange between the ASE sensor and ASE collector.
		Note See the *Threat Information Distribution Protocol* feature documentation for more information on TIDP groups.

Step 4	**`ase collector`** *`ip-address`*
	Example:
	`Router(config)# ase collector 10.10.10.3`
		Enters the destination IP address of the ASE collector server so that the ASE sensor has IP connectivity to the ASE collector.

Step 5	**`ase signature extraction`**
	Example:
	`Router(config)# ase signature extraction`
		Enables the ASE feature globally on the router.

Step 6	**`interface`** *`interface-type number`*
	Example:
	`Router(config)# interface GigabitEthernet0/1`
		Enters the interface for the ASE feature, and enters interface configuration mode.

Step 7	**`ase enable`**
	Example:
	`Router(config-if)# ase enable`
		Enables the ASE feature on this interface.

	Command or Action	Purpose

Step 8	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 9	**show ase** **Example:** `Router# show ase`	Displays the ASE run-time status. The four states are: • Not Enabled—(Not displayed) The ASE feature is not enabled in global configuration mode. • Enabled—The ASE feature is enabled in global configuration mode, but the ASE sensor has not connected with the ASE collector. • Connected—The ASE sensor has connected with the ASE collector, but it has not completed initialization. • Online—The ASE is ready for inspecting traffic.

What to Do Next

Start the ASE collector. The ASE collector, which runs on a Linux-based PC, provides the ASE sensor software on the Cisco IOS with entries and analysis on extracted signatures.

Note Contact your Cisco representative for more information about installing the ASE collector on your network.

After the ASE collector is started, the ASE run-time status information can be displayed by using the **show ase** command, as shown below:

Note The ASE collector must be started in order for the ASE run-time status information to be displayed.

```
Router# show ase
ASE Information:

Collector IP: 10.10.10.3
TIDP Group  : 10
Status      : Online

Packets inspected: 1105071
Address Dispersion Threshold: 20
Prevalence Threshold: 10
Sampling set to: 1 in 64
Address Dispersion Inactivity Timer: 3600s
Prevalence Table Refresh Time: 60s
```

Additional References

The following sections provide references related to Automatic Signature Extraction.

Related Documents

Related Topic	Document Title
Threat Information Distribution Protocol (TIDP) Mitigation Service (TMS)	*TIDP Based Mitigation Services*
	Threat Information Distribution Protocol
Security related information	*Cisco IOS Security Configuration Guide*, Release 12.4

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this release.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Command Reference

This section documents only commands that are new or modified.

- ase collector
- ase enable
- ase group
- ase signature extraction
- clear ase signatures
- debug ase
- show ase

ase collector

To enter the destination IP address of the Automatic Signature Extraction (ASE) collector server, use the **ase collector** command in global configuration mode. To remove this IP address, use the **no** form of this command.

ase collector *ip-address*

no ase collector *ip-address*

Syntax Description

ip-address	Provides IP connectivity between the ASE sensor and ASE collector.

Command Default

No ASE collector IP address is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example shows how to configure an ASE collector IP address:

```
Router(config)# ase collector 10.10.10.3
```

Related Commands

Command	Description
ase enable	Enables the ASE feature on a specified interface.
ase group	Identifies the TIDP group number for the ASE feature.
ase signature extraction	Enables the ASE feature globally on the router.
clear ase signature	Clears ASE signatures that were detected on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Shows the ASE run-time status, which includes the TIDP group number.

ase enable

To enable the Automatic Signature Extraction (ASE) feature on a specified interface, use the **ase enable** command in interface configuration mode. To disable the ASE feature on a specified interface, use the **no** form of this command.

ase enable

no ase enable

Syntax Description

This command has no arguments or keywords.

Command Default

The ASE feature is disabled on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example shows how to enable the ASE feature on a specified interface:

```
Router(config-if)# ase enable
```

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase group	Identifies the TIDP group number for the ASE feature.
ase signature extraction	Enables the ASE feature globally on the router.
clear ase signature	Clears ASE signatures that were detected on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Shows the ASE run-time status, which includes the TIDP group number.

ase group

To identify the Threat Information Distribution Protocol (TIDP) group number used for exchange between the Automatic Signature Extraction (ASE) sensor and ASE collector, use the **ase group** command in global configuration mode. To disable this group number, use the **no** form of this command.

ase group *TIDP-group-number*

no ase group *TIDP-group-number*

Syntax Description

TIDP-group-number	TIDP group number for the ASE feature. The range of group numbers is between 1 and 65535.

Command Default

No TIDP group number is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example shows how to configure a TIDP group number for the ASE feature:

```
Router(config)# ase group 10
```

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase enable	Enables the ASE feature on a specified interface.
ase signature extraction	Enables the ASE feature globally on the router.
clear ase signature	Clears ASE signatures that were detected on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Shows the ASE run-time status, which includes the TIDP group number.

ase signature extraction

To enable the Automatic Signature Extraction (ASE) feature globally on the router, use the **ase signature extraction** command in global configuration mode. To disable the ASE feature globally on the router, use the **no** form of this command.

ase signature extraction

no ase signature extraction

Syntax Description

This command has no arguments or keywords.

Command Default

The ASE feature is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example shows how to enable the ASE feature globally on the router:

```
Router(config)# ase signature extraction
```

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase group	Identifies the TIDP group number for the ASE feature.
ase enable	Enables the ASE feature on a specified interface.
clear ase signature	Clears ASE signatures that were detected on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Displays the ASE run-time status, which includes the TIDP group number.

clear ase signatures

To remove all Automatic Extraction Signatures (ASEs), use the **clear ase signatures** command in privileged EXEC configuration mode.

clear ase signatures

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

This command is used to remove all the generated signatures that are displayed in the **show ase signatures** command output.

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example output demonstrates the result of removing generated signatures:

```
Router# show ase signatures

Automatic Signature Extraction Detected Signatures
==================================================

Signature Hash: 0x1E4A2076AAEA19B1, Offset: 54, Dest Port: TCP 135,
Signature: 05 00 00 03 10 00 00 00 F0 00 10 00 01 00 00 00 B8 00 00 00 00 00 03 00 01 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
Signature Hash: 0x24EC60FB1CF9A800, Offset: 72, Dest Port: TCP 445,
Signature: 00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 00 00 00 00 62 00 02 50 43 20 4E
45 54 57 4F 52 4B 20 50 52 4F 47 52 41 4D
Signature Hash: 0x0B0275535FFF480C, Offset: 54, Dest Port: TCP 445,
Signature: 00 00 00 85 FF 53 4D 42 72 00 00 00 00 18 53 C8 00 00 00 00 00 00 00 00 00 00
00 00 00 00 FF FE 00 00 00 00 00 62 00 02

Router# clear ase signatures

Router# show ase signatures

Automatic Signature Extraction Detected Signatures
==================================================
```

Table 1 describes the significant fields shown in the display.

Table 1 clear ase signatures Field Descriptions

Field	Description
Signature Hash	Hash (total) value of the 40-byte pattern, used as a check number for error control
Offset	Offset within the packet where the pattern begins
Dest Port	Layer 4 destination port for packets that contain this pattern
Signature	40 bytes of packet data used to potentially identify a piece of malware

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase group	Identifies the TIDP group number for the ASE feature.
ase enable	Enables the ASE feature on a specified interface.
ase signature extraction	Enables the ASE feature globally on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Shows the ASE run-time status, which includes the TIDP group number.

debug ase

To gather Automatic Signature Extraction (ASE) error, log, messaging, reporting, status, and timer information, use the **debug ase** command in privileged EXEC mode. To disable error, log, messaging, reporting, status, and timer information, use the **no** form of this command.

debug ase {**errors** | **log** | **messages** | **reports** | **status** | **timing**}

no debug ase {**errors** | **log** | **messages** | **reports** | **status** | **timing**}

Syntax Description

errors	Displays ASE error information.
log	Displays ASE logging information.
messages	Displays ASE messaging information.
reports	Displays ASE reports.
status	Displays ASE status information.
timing	Displays ASE timer information.

Command Default

Disabled

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase enable	Enables the ASE feature on a specified interface.
ase group	Identifies the TIDP group number for the ASE feature.
ase signature extraction	Enables the ASE feature globally on the router.
clear ase signature	Clears ASE signatures that were detected on the router.
show ase	Displays the ASE run-time status, which includes the TIDP group number.

show ase

To display the Automatic Signature Extraction (ASE) run-time status or detected signatures, use the **show ase** command in privileged EXEC mode.

show ase [**signature** **|**]

Syntax Description

signature	(Optional) Displays the detected ASE signatures.
|	(Optional) Use output modifiers to display specific information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

If you specify the **show ase** command with no keywords, then only the run-time status is shown. If the **show ase signature** command is specified, then only detected ASE signatures are displayed.

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example output displays the ASE run-time status.

Note The ASE collector must be started in order for the ASE run-time status information to be displayed.

```
Router# show ase
ASE Information:

Collector IP: 10.10.10.3
TIDP Group  : 10
Status      : Online

Packets inspected: 1105071
Address Dispersion Threshold: 20
Prevalence Threshold: 10
Sampling set to: 1 in 64
Address Dispersion Inactivity Timer: 3600s
Prevalence Table Refresh Time: 60s
```

Table 1 describes the significant fields shown in the display.

Table 2 show ase Field Descriptions

Field	Description
Collector IP	The IP address of the ASE collector.
TIDP Group	Threat Information Distribution Protocol (TIDP) group used for exchange between the ASE sensor and ASE collector.
Status	The four states are: • Not Enabled—(Not displayed) The ASE feature is not enabled in global configuration mode. • Enabled—The ASE feature is enabled in global configuration mode, but the ASE sensor has not connected with the ASE collector. • Connected—The ASE sensor has connected with the ASE collector, but it has not completed initialization. • Online—The ASE is ready for inspecting traffic.
Packets inspected	Total number of packets inspected on this ASE collector.
Address Dispersion Threshold	Number of IP address occurrences that are permitted by the ASE sensor before this signature is considered an anomaly. **Note** The Address Dispersion Threshold is configured on the ASE collector. This information is shown on the ASE sensor (this router) for informational purposes.
Prevalence Threshold	The number of signature occurrences that are permitted before this signature is considered an anomaly. The default threshold is 10 seconds.
Sampling set to	A sampling value that sets the chance for which a signature is being inspected. For example, 1 in 64 is less than 1 in 32 chances.
Address Dispersion Inactivity Timer	Number of seconds that a signature does not occur. After this interval elapses, the signature is purged from the Address Dispersion table.
Prevalence Table Refresh Time	Number of seconds that the ASE sensor has before it clears the occurrence table. If a signature does not occur for the Prevalence Threshold during a refresh, then the Prevalence Threshold is not considered.

The following example output displays the detected ASE signatures:

```
Router# show ase signature
Automatic Signature Extraction Detected Signatures
==================================================

Signature Hash: 0x1E4A2076AAEA19B1, Offset: 54, Dest Port: TCP 135,
Signature: 05 00 00 03 10 00 00 00 F0 00 10 00 01 00 00 00 B8 00 00 00 00 00 03 00 01 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
Signature Hash: 0x24EC60FB1CF9A800, Offset: 72, Dest Port: TCP 445,
Signature: 00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 00 00 00 00 62 00 02 50 43 20 4E
45 54 57 4F 52 4B 20 50 52 4F 47 52 41 4D
```

```
Signature Hash: 0x0B0275535FFF480C, Offset: 54, Dest Port: TCP 445,
Signature: 00 00 00 85 FF 53 4D 42 72 00 00 00 00 18 53 C8 00 00 00 00 00 00 00 00 00 00
00 00 00 00 FF FE 00 00 00 00 00 62 00 02
```

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase group	Identifies the TIDP group number for the ASE feature.
ase enable	Enables the ASE feature on a specified interface.
ase signature extraction	Enables the ASE feature globally on the router.
clear ase signature	Clears ASE signatures that were detected on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.

Feature Information for Automatic Signature Extraction

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for Automatic Signature Extraction

Feature Name	Releases	Feature Information
Automatic Signature Extraction	12.4(15)T	The Automatic Signature Extraction feature helps shorten the response time for identifying malware by dynamically extracting signatures for unknown viruses and worms traversing the network without the need for human intervention. This feature was introduced on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Glossary

botnet—Slang term for a collection of software robots, or bots, which run autonomously or to a network of compromised “zombie” computers running distributed programs, which are usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure.

CPE—Customer Premises Equipment. Terminating equipment, such as a router installed at a customer site, and connected to a WAN.

ISR—Integrated Services Router. Router that supports integrated or multimedia services, including traffic management mechanisms.

malware—Detrimental software designed to infiltrate or damage a computer system without the owner's informed consent. Examples of malware include viruses, worms, botnets, spam, adware, etc.

signature—The 40 bytes of packet data that can be used to identify a piece of malware.

TIDP—Threat Information Distribution Protocol. Communication protocol used between the Linux-based Automatic Signature Extraction collector and Cisco IOS-based ASE sensors.

TMS—Threat Mitigation Service. TMS is used with the TIDP protocol to contain and mitigate the malware outbreak among TMS consumers on a network.

Virus—Hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting—that is, inserting a copy of itself into and becoming part of—another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

WAN—wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs.

worm—Computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and can consume computer resources destructively.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.