6AOSCG0029-29E
March 2016

ADTRAN

Configuration Guide

Configuring Packet Capture in AOS

This configuration guide outlines the use and configuration of the packet capture feature for ADTRAN Operating System (AOS) products. The guide includes an overview of the packet capture process, the steps necessary to configure the feature using the command line interface (CLI), how to export packet captures, and troubleshooting information.

This guide consists of the following sections:

Packet Capture Feature Overview

The AOS packet capture feature is used with network monitoring to effectively capture data packets as they traverse the network. As data packets pass through an interface on which the packet capture feature is enabled, a packet-capture monitors the traffic and captures the header and payload of specified packets as they pass through. The captured packets are then exported and stored in either flash memory or CompactFlash® storage, and can then be reviewed to determine the cause of network problems, identify security threats, and to maintain efficient data transmission over the network.

In AOS, packet capturing can be attached to one or more interfaces on the device, and can capture Internet Protocol version 4 (IPv4) packets on Layer 3 of the network open systems interconnection (OSI) model. Packet-captures capture both ingress and egress packets on the interface, and can export the captured packets to a Trivial File Transfer Protocol (TFTP) server, flash memory, or CompactFlash memory in libpcap format with a .pcap file extension. Each packet-capture can be limited to only capturing a specified type of traffic by using an access control list (ACL) to specify what type of traffic the packet-capture should capture. The packet-capture works on user-configured size and time limits, which determine when the Pcap file is exported and another capture is initiated. When the size or time limit for a packet-capture expires, the Pcap file is exported. At this point, the limits reset and a new Pcap file is created for subsequently captured packets. There are two types of packet-captures available in AOS products: a standard packet-capture, and a Session Initiation Protocol (SIP) packet-capture.

Standard Packet-Captures

Standard packet-captures capture packets from all interfaces on which a packet-capture is attached, and archive these captures into a single Pcap file that is exported at regular intervals (based on the packet-capture's size and time limit configuration). The packets captured by standard packet-captures include all ingress and egress IPv4 packets allowed by the ACL associated with the packet-capture, for every interface on which the packet-capture is attached. You can create separate Pcap files on a per-interface basis by creating multiple standard packet-captures and attaching one to each interface of interest.

SIP Packet-Captures

SIP packet-captures differ from standard packet-captures in that they focus on capturing SIP packets, rather than all allowed IPv4 packets. These packet-captures capture all ingress or egress User Datagram Protocol (UDP) packets that are related to SIP messages (including those related to back-to-back user agent (B2BUA) calls, proxy calls, and messages not related to any call) on every interface on which the packet-capture is attached.

SIP packet-captures group captured SIP packets on a per-call basis, resulting in one Pcap file per call which is exported immediately after the call is terminated. The captured packets are not typically grouped by interface, however, you can group captured SIP packets this way by creating multiple SIP packet-captures and attaching them to different interfaces. In addition, non-call related SIP signaling packets can be captured and placed into a separate Pcap file, which is exported at regular intervals (based on the packet-capture's size and time limit configuration).

The AOS device must be using SIP proxy or B2BUA in order for the SIP call related signaling to be grouped into individual packet captures. Otherwise, the SIP messaging will only be captured into the non-call related signaling Pcaps.

SIP packet-captures do not support SIP over Transmission Control Protocol (TCP) or Transport Layer Security (TLS), and SIP packets are ignored by the packet-capture unless the transport protocol and source port (for transmitted packets) or the transport protocol and destination port (for received packets) matches any configured SIP port on the AOS unit.

Pcap Export

Pcap files can be exported by the packet-capture to a TFTP server, or the AOS unit's flash or CompactFlash, or an attached Universal Serial Bus (USB) drive. Using a TFTP server is the recommended method due to the limitations of flash and CompactFlash memory and the shortened file names required by these storage devices. Using TFTP allows the delivery of a Pcap file to an arbitrary TFTP server, and the packet-capture is designed to handle unexpected TFTP transfer failures (such as a server timeout).

HTTP(S) Export

In addition, Pcap files can be exported to and stored on a Hypertext Transfer Protocol (HTTP) or HTTP secure (HTTPS) server. The packet capture archival server HTTP(S), or PCASH server, is a server that receives captured packets and metadata sent from AOS devices for long-term storage, and for use with other applications. The published application programming interface (API), **AOS to PCASH API**, defines the format of the Multipurpose Internet Mail Extensions (MIME) encoded in an HTTP POST request.

HTTP POST requests are used to transfer the Pcap files, with additional metadata, to form capture records stored in the PCASH. The created POST requests include the metadata information outlined in *Table 1* below and *Table 2 on page 4*.

Table 1. Included Fields in All HTTP(S) POST Requests

Field Name	Field Value	Field Type
version	AOS to PCASH API version (1.0)	Content-Type: text/plain
sniffer_name	The name of the packet-capture that generated this capture.	Content-Type: text/plain
type	The type of capture being exported. Possible types include: **standard** (indicates nothing is known about the type of traffic captured, and has only standard metadata), **sip** (indicates capture is of SIP traffic, and has only standard metadata), and **sip-call** (indicates capture is of an individual SIP call, and has additional metadata not included in other types).	Content-Type: text/plain
device_serial	The serial number of the AOS device.	Content-Type: text/plain
capture_id	The numeric capture ID that is unique per AOS device.	Content-Type: text/plain
start_ts	A UNIX timestamp generated when the capture is initiated.	Content-Type: text/plain
end_ts	A UNIX timestamp generated when the capture is terminated.	Content-Type: text/plain

Table 1. Included Fields in All HTTP(S) POST Requests *(Continued)*

Field Name	Field Value	Field Type
pcap_data	The binary contents of the Pcap file.	Content-Type: application/octet-stream Content-Transfer-Enconding: binary
pcap_size	The size of the Pcap file in bytes.	Content-Type: text/plain
pcap_filename	The filename of the Pcap file.	Content-Type: text/plain

Table 2. Additional Fields for sip-call Type POST Requests

Field Name	Field Value
sip_call_ids	The call ID of every SIP dialog associated with the call, delimited by commas.
call_id	A unique numerical switchboard call identifier (CCMID) used internally by AOS.
call_to	The called user.
call_from	The calling user.

Pcap files can also be exported using HTTP or HTTPS to an n-Command® MSP server that has been selected by auto-link. Auto-link redundancy, a feature introduced in AOS firmware release R10.7.0, allows the configuration of multiple n-Command MSP servers. When multiple MSP servers are configured, ADTRAN units can roll over to the next MSP server for management if the current MSP server fails. Packet captures can be configured to use the auto-link MSP server as the capture export location. When a failover event occurs, packet captures that are configured to export using auto-link automatically roll over to the new server for export.

Considerations for Configuring and Using the Packet Capture Feature

There are some considerations necessary for the configuration and use of packet capturing on an AOS unit. These considerations are outlined in the following sections.

Time and Size Limits

A time or size limit must be configured on each packet-capture. These limits apply to all Pcap files that the packet-capture generates (except SIP call Pcap files). Expiration of the time limit triggers exportation of the Pcap file, so you should consider carefully how often you want to export Pcap files when configuring the time limit for each packet-capture. Both the size and time values can be set to 0 to disable them. If both limits are disabled, an error is displayed.

Memory Usage

Each packet-capture has a user-configured maximum memory usage threshold for its captured packets. When the packet-capture reaches this threshold, it enters memory usage critical (MUC) mode. Once it enters this mode, the packet-capture ceases capturing packets while it completes any ongoing exports. In addition, it closes any open packet captures and begins exporting those as well. The packet-capture remains in MUC mode until the memory usage has decreased to 75 percent of the configured maximum memory usage threshold. Once the memory usage reaches this level, the packet-capture returns to normal operation.

Export Type

Even though exporting Pcap files to flash or CompactFlash is not recommended, you can configure multiple exports to these storage devices as long as the destination path is unique. You can also configure multiple TFTP and HTTP(S) exports as long as the destination address and port are unique. Up to five export types can be configured on each packet-capture, for example, you can export a single Pcap file to two HTTP servers, an HTTPS server, a TFTP server, and a USB drive.

If you are using the PCASH server, and exporting using HTTP(S), you can optionally have the AOS client authenticate with the PCASH server using basic access authentication. Be aware, however, that basic authentication has the disadvantage that credentials can be intercepted if HTTPS is not being used. Whether or not you use basic authentication, you must ensure that the server is configured correctly. Files that are exported to the PCASH server are sent to the following URI on the server by default: **/adtran/pcash/aos/receiveCapture/**.

In addition, when using a TFTP server, you can run a script on the server that polls for new Pcap files. This script must ensure that the Pcap file transfer is complete before attempting to use or copy the file(s). Although this guide does not discuss how to create a script on a TFTP server, you might find these parameters helpful in determining how to view and analyze the captured packets from your network.

PCAP Filenames

PCAP filenames are limited by the export mechanism used. For example, when exporting files to a TFTP server, filenames can be up to **98** characters (a full-length filename), but when exporting to flash, filenames can only be **31** characters in length (a short filename). This number includes the file extension (.pcap). Pcap filenames are comprised of the AOS device serial number, the packet-capture ID, the packet-capture name, the start date/time, and a switchboard call ID (only applies to calls when using a SIP packet-capture).

The packet-capture name for full-length filenames has a maximum of 32 characters. The packet-capture name for short filenames are truncated if the name is longer than 8 characters. If the packet-capture name is truncated, 7 characters of the packet-capture name are displayed, followed by a ~ (tilde). To avoid confusion when naming your packet-captures, make sure that the first seven letters of each packet-capture name are unique.

The capture ID, whether used in the full-length or short filename, uniquely identifies the capture. This filename element is exactly 6 decimal digits for a short filename and 8 decimal digits for a full-length filename, padded with zeros if necessary.

The start date and time for full-length filenames indicates the date and time when the capture was initiated. This time is expressed in the following format: yyyy.MM.dd_HH.mm.ss. The start time for the shortened filename is a timestamp, expressed in seconds since the UNIX epoch. This element is represented as 10 hexadecimal digits, padded with zeros if needed.

The switchboard call ID (CCMID) is used for packet captures for SIP calls. The CCMID uniquely identifies the call in a filename component that is exactly 8 decimal digits, padded with zeros if necessary.

When using packet capture for standard packets (packets not associated with a SIP call), by default the full-length format is used. This format has a maximum length of 98 characters, and is used by all export formats except flash. The following is the filename breakdown for the full-length format of the Pcap filename:

LBADTN07AF221_00000001_MySipPcap_2010.10.06_18.50.25.pcap
Device Serial # Capture ID Packet-Capture Name Start Date and Time.pcap

When exporting to the local flash filesystem (not recommended), a shortened form of the file name is used. The shorter form has a maximum character length of 31 characters. The packet-capture name for short filenames are truncated if the name is longer than 8 characters. If the packet-capture name is truncated, 7 characters of the packet-capture name are displayed, followed by a ~ (tilde). The following is the filename breakdown for the short format of the PCAP filename:

000001_MySip~_1362781729.pcap
Capture ID Packet-Capture Start Time.pcap

When using packet capture for SIP calls, the full-length format is used for the Pcap filename. In addition to the device serial number, capture ID, packet-capture name, and start date and time, the filename also includes the switchboard call ID (CCMID) if the capture is of a call through the B2BUA. The following is the filename breakdown for the full-length format of call Pcap filenames:

LBADTN07AF221_00000001_MySippacket-capture_2010.10.06_18.50.25_00000001.pcap
Device Serial # Capture ID Packet-Capture Name Start Date and Time CCMID.pcap

The shortened filename format is used when exporting call captures to flash. The shortened form appears exactly as it does for standard packet-captures, and does not include the CCMID.

Packet-Capture Feedback

When configuring packet-captures, you must take precautions to ensure that no packet-capture captures its own export traffic, or that of any other packet-capture. Preventing packet-capture feedback is crucial because any feedback results in an infinite loop, as packet-captures will capture every packet they send, and will send every packet they capture.

If you are exporting Pcap files to flash or CompactFlash, feedback is not an issue. Feedback loops are also eliminated if no packet-captures are attached to the interface on which captures are exported. The potential for feedback does not exist with SIP packet-captures because the only type of traffic they capture is SIP traffic. In addition, ACLs can be used to limit capture to a specific type of traffic, and export traffic can be excluded.

If feedback is a potential issue, you can configure an ACL that excludes from the capture all IPv4 traffic between the device and server(s) used for capture export. If only TFTP export is used, then only UDP traffic needs to be excluded. Blocking only traffic on UDP port 69 is not sufficient to prevent TFTP feedback.

Hardware and Software Requirements and Limitations

The packet capture feature is available on AOS products running AOS firmware release R10.1.0 or later, as outlined in the *AOS Feature Matrix*, available online at https://supportforums.adtran.com.

For best performance, Rapid Route should be enabled on all interfaces (using the **ip ffe** command), even if packet-captures are not attached to all interfaces.

It is possible to capture RTP streams, both ingress and egress, regardless of whether the firewall and RTP quality monitoring are enabled.

Packet Capture and Auto-link

As of AOS release R10.7.0, packet captures can be exported to the same n-Command MSP server that auto-link is currently using. In addition, if auto-link should fail over to another MSP server, packet capture reporting will also fail over to the new MSP server and send reports to that server. AOS devices running AOS firmware R10.7.0 or later support this feature, as do n-Command MSP servers running firmware version 6.1 or later.

As of AOS release R11.12.0, when packet capture is configured to use auto-link, the capture is sent using the virtual routing and forwarding (VRF) instance specified in the auto-link configuration.

For more information about the auto-link feature and its configuration, refer to the configuration guide *Configuring Auto-Link for AOS and n-Command MSP*, available online at https://supportforums.adtran.com.

Configuring a Packet-Capture

To configure packet capturing on an interface, you must create a standard or SIP packet-capture. In addition, you will need to specify the export mode for the Pcap files, specify the ACL for a standard packet-capture, and you must enable the capture. Additional configuration options include limiting the number of packet bytes captured, limiting the duration of the capture, setting the maximum memory usage allowed for the capture, and limiting the size of all of a packet-capture's open captures.

Once the packet-capture has been configured, it must be applied to an interface. To configure a standard packet-capture, follow these steps:

1. Create the standard packet-capture using the **packet-capture** <*name*> **standard** command from the Global Configuration mode prompt. Create a SIP packet-capture using the **packet-capture** <*name*> **sip** command. These commands create and name the capture, specify it is a standard (**standard**) or SIP (**sip**) packet-capture, and enter the packet-capture's configuration mode. The <*name*> parameter is the name of the packet-capture, which can be **1** to **32** characters in length. Using the **no** form of this command removes the packet-capture from the AOS device configuration. To create a standard packet-capture, enter the command as follows:

   ```
   (config)#packet-capture 1CAPTURE standard
   (config-packet-capture-1CAPTURE)#
   ```

   

   Remember to make the first seven characters of the packet-capture name unique if you exporting the captures to flash.

2. Next, specify the export mode used for the Pcap files. There are four main commands used to specify where the Pcap files should be exported. Use the **export [cflash [**<*path*>**] | flash [**<*path*>**] | usbdrive0 [**<*path*>**]]** command to export the files to the local CompactFlash, flash, or USB file systems. If the optional <*path*> parameter is not specified, the files are exported to the **/PacketCapture** directory by default on the filesystem. If you do not want to use the default directory, you can optionally specify a path. Paths can be between **1** and **255** characters in length. Remember that paths must be specified using **/** as the separating character, they must be unescaped, and if they contain spaces, they must be enclosed in quotation marks. Use the **no** form of this command to remove the export entry. For example, to export the Pcap files of **1CAPTURE** to the default directory on the CompactFlash, enter the command from the packet-capture's configuration mode as follows:

```
(config-packet-capture-1CAPTURE)#export cflash
(config-packet-capture-1CAPTURE)#
```

> NOTE *Exporting packet-captures to the root directory of CFLASH is not recommended due to the FAT16 limit of 256 entries in the root directory of the file system.*

The second **export** commands specifies an HTTP(S) server to which to send the Pcap files. You can specify an HTTP or HTTPS server using the following command: **export [http | https]** <*ipv4 address | hostname*> **[port** <*path*>**] [path** <*path*>**] [username** <*username*> **password [encrypted]** <*password*>**]** from the Packet Capture Configuration mode. The **http** and **https** parameters specify whether you are exporting to an HTTP or HTTPS server. The server is then identified by entering either an IPv4 address (expressed in dotted decimal notation, for example, **X.X.X.X**), or the host name of the server (for example, **hostname.com**). Host names can be between **4** and **255** characters in length. The optional **port** <*port*> parameter specifies specifies the port on the server to which the Pcap file is sent. Valid port range is **1** to **65535**. If no port is specified, the files are sent to the default port of **80** (HTTP) or **443** (HTTPS). Multiple HTTP(S) exports in the same packet-capture can have the same IPv4 address or host name as long as the port is different. The optional **path** <*path*> parameter specifies the directory to which the files are exported. If a path is not specified, the default request path (**/adtran/pcash/aos/receiveCapture/**) is used. Paths can be between **1** and **255** characters in length. Remember that paths must be specified using **/** as the separating character, they must be unescaped, and if they contain spaces, they must be enclosed in quotation marks. The optional **username** <*username*> **password** <*password*> parameters specify that basic authentication credentials are sent with every HTTP(S) POST request. User names and passwords can be between **6** and **32** characters in length. The optional **encrypted** keyword specifies the password is encrypted. User names cannot contain spaces, and if passwords contain spaces, they must be enclosed in quotation marks (for example, **"open sesame"**). Using the **no** form of this command, without specifying additional parameters, removes all export entries of the specified type (HTTP or HTTPS). Using the **no** form of this command with additional parameters specified removes the export entry that is an exact match.

To export Pcap files to the PCASH server at **10.10.2.5** using HTTP with the default directory and port, and without any authentication, enter the command from the packet-capture's configuration mode as follows:

```
(config-packet-capture-1CAPTURE)#export http 10.10.2.5
(config-packet-capture-1CAPTURE)#
```


The third **export** command specifies a TFTP server to which to send the Pcap files. You can specify the TFTP server using the command **export tftp** <*ipv4 address*> **[port** <*port*>**]**. The <*ipv4 address*> parameter specifies the IPv4 address of the TFTP server. IPv4 addresses should be expressed in dotted decimal notation, for example, **X.X.X.X**. The optional **port** <*port*> parameter specifies a nondefault UDP port to use. Valid port range is **1** to **65535**. By default, the files are exported to UDP port **69**. Using the **no** form of this command removes the export configuration from the packet-capture. To specify that the files are exported to a TFTP server with an IPv4 address of **10.10.5.3**, using the default port, enter the command from the packet-capture's configuration mode as follows:

```
(config-packet-capture-1CAPTURE)#export tftp 10.10.5.3
(config-packet-capture-1CAPTURE)#
```

The fourth **export** command specifies the n-Command MSP server that auto-link is currently using as the server to which to send the Pcap files. Packet capturing can be configured to use the auto-link MSP server as the Pcap file export location. When a failover event occurs, packet captures that are configured using auto-link automatically roll over to the new server for export. You can specify that packet capture is exported to the currently selected auto-link server using the command **export [http | https] auto-link [port** <*path*>**] [path** <*path*>**] [username** <*username*> **password [encrypted]** <*password*>**]** from the Packet Capture Configuration mode. The **http** and **https** parameters specify whether you are exporting to an HTTP or HTTPS auto-link server. The optional **port** <*port*> parameter specifies specifies the port on the server to which the Pcap file is sent. Valid port range is **1** to **65535**. If no port is specified, the files are sent to the default port of **80** (HTTP) or **443** (HTTPS). The optional **path** <*path*> parameter specifies the directory to which the files are exported. If a path is not specified, the default request path (**/adtran/pcash/aos/receiveCapture/**) is used. Paths can be between **1** and **255** characters in length. Remember that paths must be specified using / as the separating character, they must be unescaped, and if they contain spaces, they must be enclosed in quotation marks. The optional **username** <*username*> **password** <*password*> parameters specify that basic authentication credentials are sent with every HTTP(S) POST request. User names and passwords can be between **6** and **32** characters in length. The optional **encrypted** keyword specifies the password is encrypted. User names cannot contain spaces, and if passwords contain spaces, they must be enclosed in quotation marks (for example, **"open sesame"**). Using the **no** form of this command, without specifying additional parameters, removes all export entries of the specified type (HTTP or HTTPS). Using the **no** form of this command with additional parameters specified removes the export entry that is an exact match.

To export Pcap files to the auto-link server using HTTP with the default directory and port, and with authentication, enter the command from the packet-capture's configuration mode as follows:

```
(config-packet-capture-1CAPTURE)#export http auto-link username pcap password secret
(config-packet-capture-1CAPTURE)#
```

*For compatibility with n-Command MSP, the default port and path should be used and the user name and password must match the credentials specified in the n-Command MSP administrative interface (**Settings** > **PCASH Settings**).*

3. After configuring the export mode, use the **match list** <*ipv4 acl name*> command to specify that the packet-capture uses an ACL to limit the type of traffic that is captured. This command can be used to prevent feedback if necessary, or to filter the type of traffic captured for other network management reasons. The <*ipv4 acl name*> parameter specifies the name of the IPv4 ACL you want to use to limit the traffic captured. Using the **no** form of this command removes the IPv4 ACL from the

packet-capture. To apply the previously created IPv4 ACL **PREVENTFEEDBACK** to the packet-capture, enter the command from the packet-capture's configuration mode as follows:

```
(config-packet-capture-1CAPTURE)#match list PREVENTFEEDBACK
(config-packet-capture-1CAPTURE)#
```

> NOTE *For more information about configuring and using IPv4 ACLs, refer to the configuration guide Configuring IP ACLs in AOS, available online at http://supportforums.adtran.com.*

4. After configuring the basics of the packet-capture, you must enable the packet-capture for it to function using the **no shutdown** command from the packet-capture's configuration mode. Enter the command as follows to enable the packet-capture:

```
(config-packet-capture-1CAPTURE)#no shutdown
(config-packet-capture-1CAPTURE)#
```

After configuring these packet-capture parameters, you must apply the packet-capture to the interface to begin capturing packets (refer to *Applying the Packet-Capture to an Interface on page 12*), or you can continue to configure the packet-capture using the optional commands described in the following section.

Optional Packet-Capture Configuration Commands

In addition to the commands previously described, there are several other optional commands you can use to further specify the packet-capture's capturing behavior. These commands are outlined in the following section.

Use the **limit size** <*value*> command to trigger a Pcap file export after the combined size of all the packet-capture's open captures exceeds the specified size. The <*value*> parameter is the maximum combined size of the packet-capture's open captures, and can be expressed in bytes, kilobytes (**k** or **K**), or megabytes (**m** or **M**). For packet-captures, K values are 2^10 and M values are 2^20 bytes. Valid range is **0** to **4095M**. If this value is set to **0**, the size limit feature is disabled. By default, the size limit is set to **1M**. Using the **no** form of this command returns the maximum open capture size limit to the default value. To change the maximum combined open capture size limit, enter the command from the packet-capture's configuration mode as follows:

```
(config-packet-capture-1CAPTURE)#limit size 3M
(config-packet-capture-1CAPTURE)#
```

> NOTE *At least one capture limit, whether size or time, must be configured with a non-zero value before the packet-capture can be enabled.*

Use the **limit time** <*value*> command to specify the time limit for the capture. This command triggers a file export after the given time value is exceeded. The <*value*> parameter of this command is the capture time limit in seconds, with a valid range of **0** to **604800** seconds (one week). By default, Pcap files are set to export after **900** seconds, or 15 minutes. You can set this value to **0** to disable the capture's time limit. Using the **no** form of this command returns the time limit to the default value. To change a capture's time limit, enter the command from the packet-capture's configuration mode as follows:

```
(config-packet-capture-1CAPTURE)#limit time 1800
(config-packet-capture-1CAPTURE)#
```

At least one capture limit, whether size or time, must be configured with a non-zero value before the packet-capture can be enabled. ADTRAN recommends that you do not disable the time and size limits.

Use the **max-memory-usage** <*value*> command to specify the maximum memory the capture is allowed to use. This command specifies a memory usage threshold for the capture. When this threshold is is reached, the packet-capture enters memory usage critical (MUC) mode. When in MUC mode, the capture stops capturing packets, continues any ongoing exports, and closes any open captures to begin exporting them. The packet-capture remains in MUC mode until memory usage decreases to 75 percent of the maximum memory usage threshold. The <*value*> parameter of this command is the memory usage threshold, and can be expressed in bytes, kilobytes, or megabytes. Valid range for the threshold is **0** to **4294967295** bytes, **0** to **4194303** kilobytes (**k** or **K**), or **0** to **4095** megabytes (**m** or **M**). By default, the maximum memory usage threshold is set to **5M**. Using the **no** form of this command returns the threshold to the default value. To configure the maximum memory usage threshold for the packet-capture, enter the command from the packet-capture's configuration mode as follows:

```
(config-packet-capture-1CAPTURE)#max-memory-usage 10M
(config-packet-capture-1CAPTURE)#
```

When configuring the maximum memory usage for packet-captures, take into consideration the amount of RAM installed in your AOS unit.

Use the **truncate-packet** <*value*> command to specify the the maximum number of bytes to be captured from each packet. This command is primarily used for performance reasons. The largest possible packet on a network depends on the maximum transmission unit (MTU) of network packets, and can be as large as **1500** bytes. You might only be interested in capturing packets that are significantly smaller than this, particularly if you are only interested in packet headers. This command allows you to specify that fewer packet bytes are captured. For example, to capture the minimum possible size of an Internet Protocol version 4 (IPv4) header, you can specify that only **28** bytes of a packet are captured, which is enough to capture only the IP and UDP headers of most IPv4 UDP packets (with IP headers of 20 bytes and UDP headers of 8 bytes). The <*value*> parameter of this command is the amount of bytes you want captured from a packet. This value can be expressed in bytes, kilobytes (**k** or **K**), or megabytes (**m** or **M**). By default, the truncated packet size is set to **0**, which indicates that packets should not be truncated. Using the **no** form of this command returns the truncated packet size to the default value. To enable packet truncation, specify the number of packet bytes to be captured by entering the command from the Packet-Capture Configuration mode as follows:

```
(config-packet-capture-1CAPTURE)#truncate-packet 28
(config-packet-capture-1CAPTURE)#
```

Applying the Packet-Capture to an Interface

After configuring and enabling the packet-capture, it must be applied to an interface to begin capturing packets. To apply the packet-capture to an interface, enter the **ip packet-capture** <*name*> command from the interface's configuration mode. For example, to enable IPv4 packet-capture **1CAPTURE** on the Ethernet interface (**eth 0/1**), enter the command as follows:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip packet-capture 1CAPTURE
```

Once you have applied the packet-capture to an interface, the packet-capture configuration is complete.

Packet-Capture Configuration Example

The following example illustrates how to configure packet capturing to capture packets on Ethernet interfaces **eth 0/1** and **eth 0/2**. The interface **eth 0/1** is configured with both a SIP and standard packet-capture, and the interface **eth 0/2** is configured with a standard packet-capture. The standard packet-capture is configured to use the IPv4 ACL **PREVENTFEEDBACK** to prevent feedback.

The configuration parameters entered in this example are sample configurations only, and only pertain to the configuration of packet capturing. This application should be configured in a manner consistent with the needs of your particular network. CLI prompts have been removed from the configuration example to provide a method of copying and pasting configurations directly from this configuration guide into the CLI. This configuration should not be copied without first making the necessary adjustments to ensure they will function properly in your network.


```
!
ip access-list extended PREVENTFEEDBACK
   deny udp host 10.17.127.249 host 10.17.127.251
   deny udp host 10.17.127.251 host 10.17.127.249
   permit ip any any
   exit
!
packet-capture 1CAPTURE sip
   export tftp 10.17.127.251
   export https pcash.example.com
   max-memory-usage 10M
   no shutdown
!
packet-capture 2CAPTURE standard
   match list PREVENTFEEDBACK
   export tftp 10.17.127.251
   no shutdown
!
interface ethernet 0/1
   ip packet-capture 1CAPTURE
   ip packet-capture 2CAPTURE
   ip address 10.17.127.249 255.255.255.0
!
interface ethernet 0/2
   ip packet-capture 2CAPTURE
   ip address 192.168.2.1 255.255.255.0
!
```

Packet Capture Configuration Command Summary

The following table summarizes the commands used to configure packet capturing on an AOS device.

Table 3. Packet Capture Command Summary

Command	Description
(config)#**[no] packet-capture** <*name*> **[sip | standard]**	Creates the packet-capture, specifies that the packet-capture captures SIP or standard traffic, and enters the packet-capture's configuration mode.
(config-packet-capture-1CAPTURE)# **[no] export [cflash [**<*path*>**] | flash [**<*path*>**] | usbdrive0 [**<*path*>**]]**	Specifies that the Pcap files are exported to the either the CompactFlash, flash, or USB drive filesystem. The <*path*> parameter specifies the location within the filesystem to which to export the Pcap files. If no path is specified, the default path of **/PacketCapture** is used.

Table 3. Packet Capture Command Summary *(Continued)*

Command	Description
(config-packet-capture-1CAPTURE)# **[no] export [http | https]** <*ipv4 address* | *hostname*> **[port** <*path*>**] [path** <*path*>**] [username** <*username*> **password [encrypted]** <*password*>**]**	Specifies that the Pcap files are exported to an HTTP(S) server. The optional **port** parameter specifies the port on the server to which the Pcap file is sent. If a port is not specified, port **80** (HTTP) or **443** (HTTPS) is used. The optional **path** parameter specifies the directory to which the files are exported. If no path is specified, the default path **/adtran/pcash/ aos/receiveCapture/** is used. The optional **username** and **password** parameters specify that basic authentication is used. The optional **encrypted** parameter specifies that the password is encrypted.
(config-packet-capture-1CAPTURE)**#[no] export tftp** <*ipv4 address*> **[port** <*port*>**]**	Specifies that the Pcap files are exported to a TFTP server. The optional **port** parameter specifies a nondefault UDP port to use. By default, port **69** is used.
(config-packet-capture-1CAPTURE)# **[no] export [http | https] auto-link [port** <*path*>**] [path** <*path*>**] [username** <*username*> **password [encrypted]** <*password*>**]**	Specifies that Pcap files are exported to an auto-link server. The optional **port** parameter specifies the port on the server to which the Pcap file is sent. If a port is not specified, port **80** (HTTP) or **443** (HTTPS) is used. The optional **path** parameter specifies the directory to which the files are exported. If no path is specified, the default path **/adtran/pcash/ aos/receiveCapture/** is used. The optional **username** and **password** parameters specify that basic authentication is used. The optional **encrypted** parameter specifies that the password is encrypted. For compatibility with n-Command MSP, the default port and path should be used and the user name and password must match the credentials specified in the n-Command MSP administrative interface (**Settings** > **PCASH Settings**).
(config-packet-capture-1CAPTURE)**#[no] limit time** <*value*>	Specifies the time limit for the capture. The <*value*> parameter is the time limit in seconds. By default, the time limit for the capture is set to **900** seconds.
(config-packet-capture-1CAPTURE)**#[no] max-memory-usage** <*value*>	Specifies the maximum memory usage allowed for the capture. The <*value*> parameter can be expressed in bytes, kilobytes (**k** or **K**), or megabytes (**m** or **M**). By default, the maximum memory usage is set to **5M**.
(config-packet-capture-1CAPTURE)**#[no] match-list** <*ipv4 acl name*>	Specifies an IPV4 ACL to apply to the capture to limit the type of traffic that is captured.
(config-packet-capture-1CAPTURE)**#[no] limit size** <*value*>	Specifies the combined size limit for all the packet-capture's open captures. The <*value*> parameter is the maximum allowed size, and can be expressed in bytes, kilobytes (**k** or **K**), or megabytes (**m** or **M**). By default, the maximum size limit is set to **1M**.

Table 3. Packet Capture Command Summary *(Continued)*

Command	Description
(config-packet-capture-1CAPTURE)**#[no] truncate-packet** <*value*>	Specifies the maximum number of bytes to be captured from each packet. The <*value*> parameter specifies the packet size in bytes, kilobytes (**k** or **K**), or megabytes (**m** or **M**). By default, the truncated packet size is set to **0**, which indicates packets should not be truncated.
(config-packet-capture-1CAPTURE)**#[no] shutdown**	Enables or disables the packet-capture.
(config-eth 0/1)**#ip packet-capture** <*name*>	Applies the specified packet-capture to an interface.

Troubleshooting

The following **show** and **debug** commands can be used to verify the packet-capture configuration, view capture statistics, and enable debug messaging for the packet-capture features. Each of these commands is entered from the Enable mode prompt.

Show Commands

The following **show** commands can be used to view capture statistics and verify the packet-capture configuration.

Use the **show packet-capture captures [realtime]** command to display the active captures of every configured packet-capture. The optional **realtime** parameter displays the output in real time. Enter the command from the Enable mode as follows:

```
>enable
#show packet-capture captures
Active Captures:
CapturID     packet-capture     State      Size     Start
331          1CAPTURE           open       24       2011.03.15 23:50:10
332          2CAPTURE           exporting  24       2011.03.15 23:48:27

Export Jobs (ongoing or recently completed):
CaptID  Sent    Destination              Status
332     151K    10.17.127.251:69         In progress
```


Use the **show packet-capture interfaces [realtime]** command to display interfaces with attached packet-captures and any observed Netifs. The optional **realtime** parameter displays the output in real time. Enter the command from the Enable mode as follows:

```
>enable
#show packet-capture interfaces
Interface Attachments:
packet-capture                  Interface
1CAPTURE                        eth 0/1
2CAPTURE                        eth 0/1
2CAPTURE                        eth 0/2

Observed Netifs:
NetifID     Interface           Primary IP
3           eth 0/1             10.17.127.226
```

Use the **show packet-capture sip-calls [realtime]** command to display the active calls of every SIP packet-capture. The optional **realtime** parameter displays the output in real time. Enter the command from the Enable mode as follows:

```
>enable
#show packet-capture sip-calls
Active Calls:
CapturID    packet-capture      CallID      SIP Dialog Call-IDs
325         3CAPTURE            5           1-6596@10.17.127.251
```

Use the **show packet-capture memory-usage [captures [sip-calls] | [interfaces]] [realtime]** command to display packet capturing memory usage statistics. The optional **captures** parameter displays memory usage statistics and all active captures, and the optional **sip-calls** parameter adds to that output all active SIP calls. The optional **interfaces** parameter displays memory usage statistics and all information for all interfaces with an attached packet-capture. The optional **realtime** parameter displays the output in real time. Enter the command from the Enable mode as follows:

```
>enable
#show packet-capture memory-usage
Memory Usage:
packet-capture      Usage       Maximum     Critical
2CAPTURE            232         1M          N
```


Use the **show packet-capture verbose [realtime]** command to display detailed configuration information for all configured packet-captures. The optional **realtime** parameter displays the output in real time. Enter the command from the Enable mode as follows:

```
>enable
#show packet-capture verbose
Memory Usage:
packet-capture          Usage       Maximum     Critical
1CAPTURE                5M          10M         N
2CAPTURE                232         1M          N

Interface Attachments:
packet-capture                      Interface
1CAPTURE                            eth 0/1
2CAPTURE                            eth 0/1
2CAPTURE                            eth 0/2

Observed Netifs:
NetifID     Interface               Primary IP
3           eth 0/1                 10.17.127.226

Active Captures:
CapturID    packet-capture          State       Size    Start
331         1CAPTURE                open        24      2011.03.15 23:50:10
332         2CAPTURE                exporting   24      2011.03.15 23:48:27

Export Jobs (ongoing or recently completed):
CaptID  Sent    Destination             Status
332     151K    10.17.127.251:69        In progress

Active Calls:
CapturID        packet-capture      CallID      SIP Dialog Call-IDs
331             1CAPTURE            5           1-6596@10.17.127.251
```

Use the **show running-config packet-capture [**<*name*>**]** to display the running-configuration of every configured packet-capture, or of a specified packet-capture. This command does not display the interface attachments of the captures. To view the interface attachments of the capture, use the **show running-config interface** command. To view the running-configuration of all configured packet-captures, enter the command from Enable mode as follows:

```
>enable
#show running-config packet-capture
```


Debug Commands

The following **debug** commands can be used to enable debug messaging for packet-captures.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Use the **debug packet-capture** command to enable debug messages for all packet-capture activities. Enter the command from the Enable mode as follows:

```
>enable
#debug packet-capture
```

In addition, it can be helpful when troubleshooting to enable debug messages for any TFTP or HTTP(S) exports you have configured with packet capturing. Enable these debug messages using either the **debug tftp client packets** or the **debug http client** commands. For example, to enable debug messages for TFTP client packets, enter the command from the Enable mode as follows:

```
>enable
#debug tftp client packets
```

