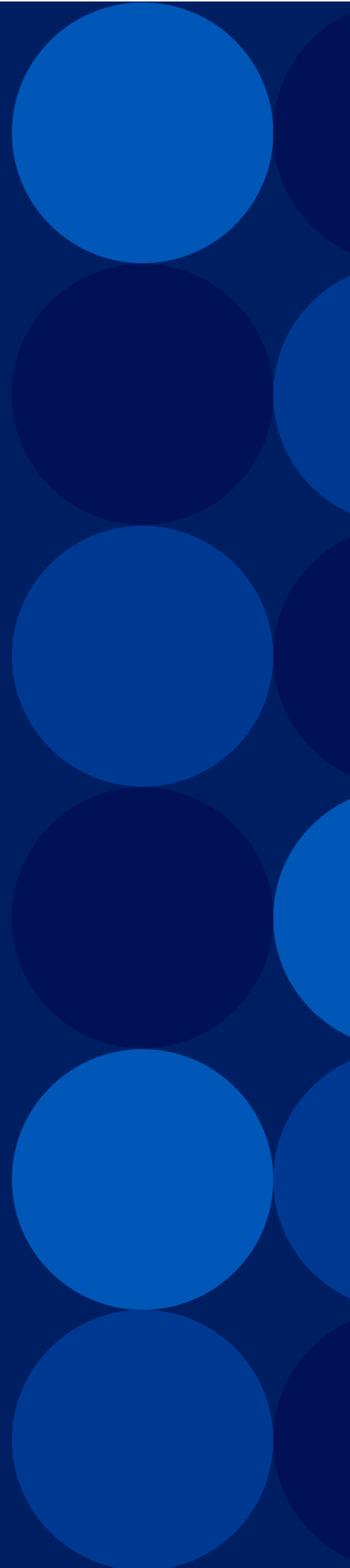


**A10**

**ACOS 7.0.3**  
**Traffic Logging Guide**

May, 2026



© 2026 A10 Networks, Inc. All rights reserved.

Information in this document is subject to change without notice.

## PATENT PROTECTION

A10 Networks, Inc. products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks, Inc. products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at:

[a10-virtual-patent-marking](#).

## TRADEMARKS

A10 Networks, Inc. trademarks are listed at: [a10-trademarks](#)

## CONFIDENTIALITY

This document contains confidential materials proprietary to A10 Networks, Inc.. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc.

## DISCLAIMER

This document does not create any express or implied warranty about A10 Networks, Inc. or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks, Inc. has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks, Inc. assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks, Inc. for current information regarding its products or services. A10 Networks, Inc. products and services are subject to A10 Networks, Inc. standard terms and conditions.

## ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

## FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc. location, which can be found by visiting [www.a10networks.com](http://www.a10networks.com).

# Table of Contents

<b>External Logging Overview</b> .....	<b>14</b>
Logging Overview .....	15
Supported Logging Formats .....	15
Binary Logging Format .....	16
Compact Logging Format .....	16
Custom Logging Format .....	16
RFC 5424 Logging Format .....	16
CEF Logging Format .....	17
IPFIX Logging Format .....	17
Fixed-NAT .....	17
Supported Event Types in Log Messages .....	17
<b>Binary Logging Format</b> .....	<b>19</b>
Configuring Binary Format .....	20
Using the GUI .....	20
Using the CLI .....	20
Wireshark Plugin .....	20
Installing the Wireshark Plug in Files for Binary Logging .....	22
Modifying Plugin Settings .....	23
<b>Compact Logging Format</b> .....	<b>26</b>
Opcodes .....	27
Extensions .....	30
Examples .....	31
Configuration .....	32
Using the GUI .....	32
Using the CLI .....	32
<b>Custom Logging Format</b> .....	<b>33</b>
Overview .....	33

Configuring Custom Log Messages .....	34
Using the GUI .....	35
Using the CLI .....	35
Additional Keywords for Custom Logs .....	36
Configuration Examples .....	38
<b>RFC 5424 Custom Logging Format .....</b>	<b>42</b>
Overview .....	43
Log Message Format .....	43
Header Fields .....	43
Message String Fields .....	45
Message String Customization .....	45
Message String Syntax .....	45
Using the GUI to Customize Message Strings .....	46
Using the CLI to Customize Message Strings .....	47
CLI Example – RFC 5424 Support with Default Message Strings .....	47
CLI Example – RFC 5424 Support with Some Custom Message Strings .....	48
<b>CEF Logging Format .....</b>	<b>51</b>
Overview .....	51
CEF Logs .....	51
Configuring the CEF Logging Format .....	52
<b>NetFlow v9 and v10 (IPFIX) .....</b>	<b>54</b>
NetFlow Overview .....	55
NetFlow Versions Supported .....	55
NetFlow Parameters .....	56
Formatting of NetFlow Records for Long-Lived Sessions .....	58
Predefined NetFlow Templates .....	59
NetFlow Templates .....	59
Templates for A10 Flow Records with NAT Addresses .....	60
Templates for NAT Session Event Records .....	62
Templates for NAT Port Mapping Event Records .....	63

Templates for NAT Port Batching Event Records .....	64
Templates for NAT Port Batching v2 Event Records .....	66
Firewall Event Records Templates .....	67
Supported NetFlow Templates (CGNAT and FW) .....	68
Log Information for Closed Sessions (CGN/FW) .....	81
Configuring Custom Templates .....	81
Examples Reference .....	81
Terminating a Session .....	82
Custom IPFIX Templates .....	83
Overview .....	84
Configuration Details .....	84
Supported Event Types .....	86
Sample Custom Templates .....	87
sesn-event-nat44-creation and sesn-event-nat44-deletion .....	88
sesn-event-nat64-creation, sesn-event-nat64-deletion, sesn-event-dslite-creation, sesn-event-dslite-deletion .....	89
sesn-event-fw4-creation, sesn-event-fw4-deletion .....	90
sesn-event-fw6-creation, sesn-event-fw6-deletion .....	91
port-mapping-nat44-creation, port-mapping-nat44-deletion .....	92
port-mapping-nat64-creation, port-mapping-nat64-deletion, port-mapping-dslite-creation, port-mapping-dslite-deletion .....	93
port-batch-nat44-creation, port-batch-nat44-deletion .....	94
port-batch-nat64-creation, port-batch-nat64-deletion, port-batch-dslite-creation, port-batch-dslite-deletion .....	94
port-batch-v2-nat44-creation, port-batch-v2-nat44-deletion .....	95
port-batch-v2-nat64-creation, port-batch-v2-nat64-deletion, port-batch-v2-dslite-creation, port-batch-v2-dslite-deletion .....	96
cgn-ddos-l3-entry-creation and cgn-ddos-l3-entry-deletion .....	96
cgn-ddos-l4-entry-creation and cgn-ddos-l4-entry-deletion .....	97
fw-ddos-entry-creation and fw-ddos-entry-deletion .....	97
fw-session-limit-exceeded .....	97

deny-reset-event-fw4 .....	98
deny-reset-event-fw6 .....	99
Supported IPFIX Information Elements .....	100
Notes .....	122
NetFlow Logging Over Dedicated Partition .....	123
Configuring NetFlow .....	123
Overview .....	124
Using the GUI to Configure NetFlow .....	124
Using the CLI to Configure NetFlow .....	126
CLI Example: Single Collector .....	126
CLI Example: Multiple Collectors .....	126
CLI Example: Firewall Session Event .....	127
Configuring NetFlow Logging Over a Dedicated Partition .....	128
Disabling CGN Logs based on Destination Protocol and Port Criteria .....	131
Displaying Show Counters .....	131
<b>Configuring External Logging .....</b>	<b>135</b>
External Logging Configuration Overview .....	136
Logging Template Options .....	136
Configuring External Logging .....	140
Using the GUI .....	140
Create Server Configurations for the Traffic Log Servers .....	140
Configure a Service Group and Its Member .....	141
Configure an External Logging Template .....	141
Activate the External Logging Template .....	141
Using the CLI .....	141
Create Server Configurations for the Traffic Log Servers .....	142
Configure a Service Group and Its Member .....	142
Configure an External Logging Template .....	142
Activate the External Logging Template .....	143
Configuration Example: External Logging for LSN Traffic Logs .....	143

Configuration Example: External Logging for DS-Lite Traffic Logs .....	144
Enabling Port Mapping Logs .....	144
Enabling Port Batching .....	145
Enabling Fixed NAT User Port Logging .....	146
Enabling Session Logging .....	146
Viewing Logging Statistics .....	147
Additional Logging Options .....	149
Enable Log Batching .....	149
Enable Session Byte Count in CGN Logging .....	149
Enable Logging for Event Types .....	150
Enable Destination Logging .....	151
Enable Client MAC Address Logging .....	151
Enable Partition Name Logging .....	151
Enable Message Source Address Logging .....	152
Enable Source Port (UDP only) Logging .....	152
Enable Timestamp Granularity Logging .....	152
Enable One-to-One NAT Logging .....	153
Enable Enhanced User Tracking .....	154
Enable Logging for Session Termination Causes .....	156
Logging Statistics .....	157
Merged Session Log .....	157
Configuring Merged Session Logs .....	158
Disabling CGN Logs .....	158
Disabling CGN Logging .....	159
Statistics Counter to Track the Reduction of Logs .....	159
CLI Example .....	159
Enabling CGN Logs .....	160
Suppress Repeated Log Messages .....	161
CLI Configuration .....	161
Configuration and Output Example .....	162

<b>Including Additional Client Information in Logs</b> .....	<b>163</b>
Logging Client HTTP Requests .....	164
Configuration for HTTP Request Logging .....	166
Using the GUI .....	166
Using the CLI .....	166
CLI Example .....	168
Logging HTTP Headers .....	168
Configuring File Extension and Fixed Ordering for Headers in HTTP Logging .....	169
Notes .....	170
Configuration .....	170
Using the CLI .....	171
Custom HTTP Request Syslog Format .....	172
Configuring a Custom HTTP Request Syslog Format .....	172
Logging Client Mobile Numbers .....	173
RADIUS Requirements .....	173
Attributes Required for Client IP Addresses .....	174
Client Mobile Number Accounting .....	174
Notes .....	174
Configuration for Mobile Number Logging .....	175
Enabling Logging of Client Mobile Numbers Using the CLI .....	175
Logging Client MAC Address .....	178
Configuration Using the GUI .....	179
Configuration Using the CLI .....	180
<b>Logging for Fixed NAT</b> .....	<b>181</b>
Configuring Fixed-NAT Logging .....	182
Fixed-NAT Logging Options .....	182
Enabling Logging for Fixed-NAT by Using the GUI .....	182
Enabling Logging for Fixed-NAT by Using the CLI .....	183
Including Port Assignment Lists .....	183
Client IP Addresses in Fixed-NAT Messages .....	184

Examples of Fixed-NAT Messages When a Client Exceeds Their Session Quota .....	184
Examples of Fixed-NAT Messages When No NAT Ports Are Available for a Client .....	185
Example of Message When More Events than the Log Limit Occur .....	186
Periodic Logging of Active Fixed-NAT Sessions .....	186
Configuration Using the GUI .....	187
Configuration Using the CLI .....	188
File Creation with Fixed-NAT Port Mapping and Configuration Removal .....	188
Configuration Using the GUI .....	188
Configuration Using the CLI .....	189
<b>Logging to RADIUS .....</b>	<b>191</b>
Overview of RADIUS Logging .....	192
Event Logging Types .....	192
RADIUS Logging Notes .....	192
VRRP-A Support .....	193
Configure RADIUS Logging .....	193
Configure RADIUS Logging Using the GUI .....	194
Configure RADIUS Logging Using the CLI .....	195
Customize RADIUS Attributes .....	196
Configuring RADIUS Logging Using Custom RADIUS Attributes .....	197
Using the GUI .....	197
Using the CLI .....	197
Attribute Parameters .....	201
Log String Formats .....	202
ASCII (the default format) .....	202
Compact .....	202
RFC 5424 .....	203
Binary .....	203
RADIUS .....	203
Notes for Log String Formats .....	204
RADIUS Interim-Update Message .....	204

Configuring NAT Logging with RADIUS Correlation .....	205
Combined Port Batch Logging and RADIUS Message Configuration Example .....	206
RADIUS Message Handling .....	208
Including Byte Count and Duration .....	211
Handling STOP and START RADIUS Log Entries .....	213
<b>CGN Traffic Logging with L3V Partitions .....</b>	<b>215</b>
Overview of CGN Traffic Logging with L3V Partitions .....	216
Separate Routing for Logging Servers .....	216
Service Group Sharing .....	217
Partition Name Logging .....	218
Configuration Example .....	220
<b>Appendix: Log Message References .....</b>	<b>222</b>
LSN Traffic Logs .....	223
NAT64/DNS64 Traffic Logs .....	225
DS-Lite Traffic Logs .....	227
Merged Session Log Samples .....	230
Additional Client Information Log Samples .....	232
Additional Client Information .....	232
HTTP Headers .....	233
Client MAC .....	236
ASCII .....	236
RFC 5424 .....	236
Compact .....	237
Binary .....	237
RADIUS .....	238
Fixed-NAT Log Samples .....	239
Log Message Enhancements for Fixed-NAT .....	240
ASCII Log Messages .....	240
Compact Log Messages .....	241
RFC 5424 Log Messages .....	241

Binary Log Messages .....	243
Changes for Fixed-NAT Port Allocation .....	243
DDoS Protection Log Samples .....	246
ASCII Log Format .....	246
CEF Log Format .....	247
One-to-One NAT Log Samples .....	247
ASCII Format .....	247
CEF Format .....	248
Default Message Strings for RFC 5424 .....	249
Default Session Creation/Deletion Message Strings .....	250
Event Type – Session created .....	250
Event Type – Session freed .....	250
Default LSN Message Strings .....	251
Event Type – Port allocated .....	251
Event Type – Port freed .....	251
Event Type – Port batch allocated .....	251
Event Type – Port batch freed .....	252
Event Type – Fixed-NAT ports allocated .....	252
Event Type – Fixed-NAT ports freed .....	252
Default HTTP Request Received Message Strings .....	252
Event Type – HTTP request received .....	252
Default DS-Lite Message Strings .....	253
Event Type - Port Allocated .....	253
Event Type – Port freed .....	254
Event Type - Port batch allocated .....	254
Event Type - Port batch freed .....	254
NAT64 Message Strings .....	254
Event Type - Port allocated .....	254
Event Type - Port freed .....	255
Event Type - Port batch allocated .....	255
Event Type - Port batch freed .....	255

Event Type - Fixed-NAT ports allocated .....	256
Event Type - Fixed-NAT ports freed .....	256
6rd-NAT64 Message Strings .....	256
Event Type - Port allocated .....	256
Event Type - Port freed .....	257
Event Type - Port batch allocated .....	257
Event Type - Port batch freed .....	257
Binary Logging Format Reference .....	257
(ACOS 2.8.0 and earlier) .....	257
Packet Header .....	258
Log-message Header .....	258
Session Logs .....	261
Port-mapping Logs .....	266
Port Batching Logs .....	270
Fixed-NAT Logs .....	273
(ACOS 2.8.1 and later) .....	275
Binary Log Packet Examples .....	280
Session Creation/Deletion and Port Mapping .....	280
Port Mapping .....	281
HTTP Request and RADIUS Attribute Logging .....	283
Fixed-NAT .....	285
Traffic Logs in CEF Format .....	285
NAT Session Created .....	286
NAT Session Deleted .....	286
NAT Port Allocated .....	286
NAT Port Freed .....	287
Port Batch Allocated .....	287
Port Batch Freed .....	287
Fixed NAT Port Assigned .....	287
Fixed NAT Port Disabled .....	287
RADIUS Message Formats .....	288

Port Mapping Created Message .....	288
Port Mapping Freed Message .....	289
Port Batch Allocated Message .....	290
Port Batch Freed Message .....	290
Fixed-NAT Port Range Allocated Message .....	291
Automatic Port Assignment (Single Port per Client) .....	291
Automatic Port Assignment (Multiple Ports per Client) .....	292
Manual Port Assignment .....	293
Fixed-NAT Port Range Freed Message .....	294
Session Created Message .....	294
Session Deleted Message .....	295
RADIUS Dictionary File .....	296
Port Batch Log Messages .....	301
Log Examples for Port Batch Allocation .....	301
Message Content .....	302
Port Batch v2 Logging Enhancements .....	302
Configuring Interim-Update Logs for Port Batch v2 .....	307
<b>Glossary .....</b>	<b>312</b>

# External Logging Overview

---

This section provides an overview of the external logging capabilities available for CGNAT and firewall features.

The following topics are covered:

<a href="#">Logging Overview</a> .....	15
<a href="#">Supported Logging Formats</a> .....	15
<a href="#">Supported Event Types in Log Messages</a> .....	17

## Logging Overview

CGNAT and Firewall cannot store traffic log messages locally due to the high volume of logs. Therefore, they are sent to the external syslog servers. External logging server configuration is required for any syslog messages to be sent to an external server.

CGNAT and Firewall do not support event logging mechanism (acos-events) for logging events. They support only external logging.

By default, external logging is not configured. After you configure a logging template and activate it, CGNAT and Firewall captures only the port mapping logs by default. You can enable logging for Session creation and deletion.

ACOS uses Port Batching for reducing the volume of external traffic logs for CGNAT. Normally, each time CGNAT allocates a port mapping for a client, a log message is generated. Port batching reduces logging by allocating a set of multiple ports to the client at the same time, and generating only a single log message for the batch of ports. For more information about Port Batching, see *IPv4-to-IPv6 Transition Solutions Guide*.

Depending on the volume of logging traffic load, 10-Gbps interfaces may be required. If the logging transmission rate is below 1 Gbps, a 1-Gbps interface provides enough bandwidth. If the logging transmission rate is above 1 Gbps, a 10-Gbps interface is recommended.

## Supported Logging Formats

The following logging formats are supported for traffic logging.

The following topics are covered:

<a href="#">Binary Logging Format</a> .....	16
<a href="#">Compact Logging Format</a> .....	16
<a href="#">Custom Logging Format</a> .....	16
<a href="#">RFC 5424 Logging Format</a> .....	16
<a href="#">CEF Logging Format</a> .....	17

<a href="#">IPFIX Logging Format</a> .....	17
<a href="#">Fixed-NAT</a> .....	17

## Binary Logging Format

---

Binary logging format does not use ASCII text. Instead, binary logging uses a unique logging format to represent the log messages.

(For more information, see [Binary Logging Format](#).)

## Compact Logging Format

---

Compact logging format uses ASCII text. It reduces the log size by using operational codes (“opcodes”) for event and protocol names, and by using hexadecimal representation for IPv4 addresses and port numbers.

(For more information, see [Compact Logging Format](#).)

## Custom Logging Format

---

The custom logging feature is an enhancement to the supported RFC custom logs that you can create using the `rfc-custom` command. This format provides the freedom to specify an arbitrary format that is non-compliant with RFC 5424, the syslog standard. It helps to reduce the size of external traffic logs for IPv6 migration traffic. Custom logs also provide the option to include the session start time and session duration in CGN logs.

(For more information, see [Custom Logging Format](#).)

## RFC 5424 Logging Format

---

The ACOS device supports RFC 5424, The Syslog Protocol. When RFC 5424 support is enabled, external log messages use the format described in the RFC. RFC 5424 support is disabled by default. You can configure it in individual logging templates.

(For more information, see [RFC 5424 Custom Logging Format](#).)

## CEF Logging Format

---

Common Event Format (CEF) uses UTF-8 format for encoding log messages. CEF relies on the Syslog message format as a transport channel. CEF log messages contains the Syslog Header, CEF Header and the CEF log message itself.

(For more information, see [CEF Logging Format](#).)

## IPFIX Logging Format

---

The IPFIX protocol uses information elements to record logging messages. ACOS supports fixed NetFlow templates and Custom NetFlow templates. The fixed templates support a list of predefined templates for NAT44, NAT64, DSLite, and so on. The custom template is more agile in sending flow data in a format that meets the needs and requirements of the NetFlow collector and analyzer. You can select the specific information elements (IEs) to be add to different events. There are several new IEs added in the Custom IPFIX Templates.

## Fixed-NAT

---

Fixed-NAT is a log optimization feature that allocates NAT ports for each client from a predetermined (“fixed”) set of ports on the NAT address. Since each client using Fixed-NAT gets a fixed set of ports, a client can be identified without any need for logging. A client can be identified based solely on the NAT IP address and the port numbers within the client’s fixed allocation of ports.

For more information, see the *IPv4-to-IPv6 Transition Solutions Guide*.

## Supported Event Types in Log Messages

By default, ACOS device logs only port mappings. You can enable the CGNAT logging for the following types of events in both Syslog and NetFlow format:

- Session Logs—Logs session creation and deletion, sessions on overloaded ports, and so on.

- Client HTTP requests
- Fixed-NAT (information types listed above are supported)

For a list of sample traffic logs, see [LSN Traffic Logs](#).

# Binary Logging Format

---

Binary logging format is one of the ACOS options that reduces the size of external traffic logs. It uses a unique and efficient A10 binary format to represent log messages.

The following topics are covered:

<a href="#">Configuring Binary Format</a> .....	20
<a href="#">Wireshark Plugin</a> .....	20

## Configuring Binary Format

### Using the GUI

---

To configure binary format using the GUI:

1. Navigate to **CGN > LSN > Templates**.
2. Select **Logging** from the drop-down list.
3. Select an existing template, or click **Create** to create a new template.
4. If creating a new template, enter a name for the template in the Name field.
5. From the drop-down list in the “Format” field, select **Binary**.
6. Click **Update**.

### Using the CLI

---

To enable binary logging format, use the following command at the configuration level of the LSN logging template:

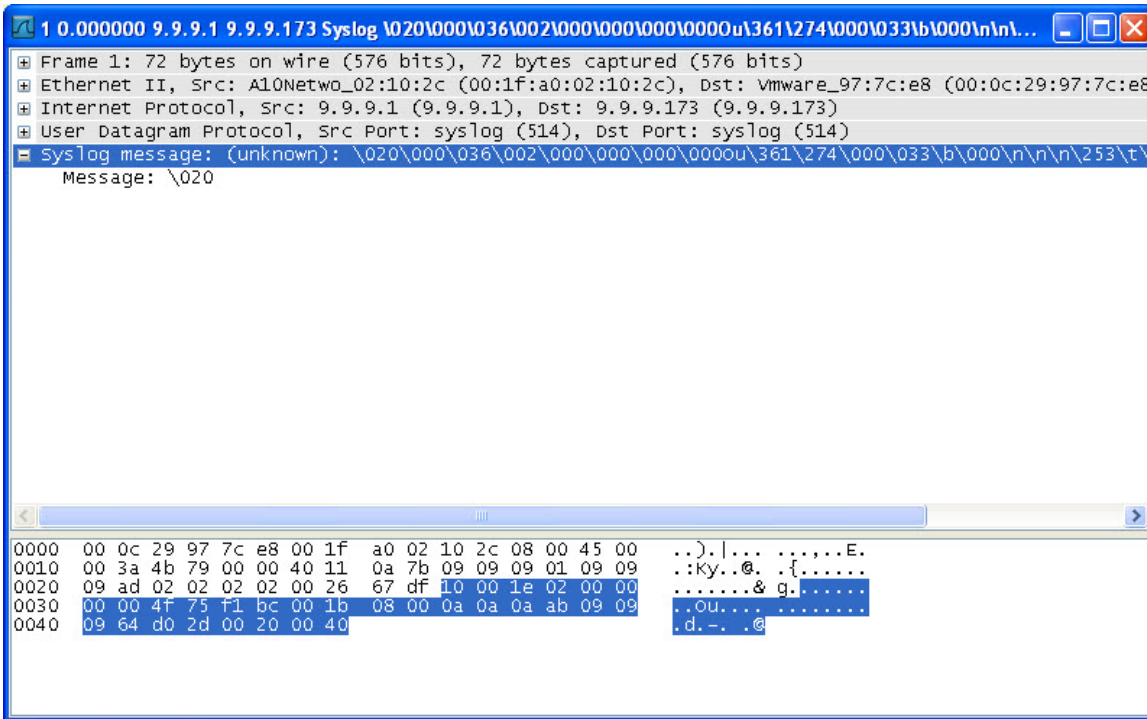
```
ACOS(config)# cgv6 template logging lsn_logging
ACOS(config-logging:lsn_logging)# format binary
```

## Wireshark Plugin

A custom plugin for Wireshark is available from A10 Networks. The plugin converts binary log message data into human-readable format.

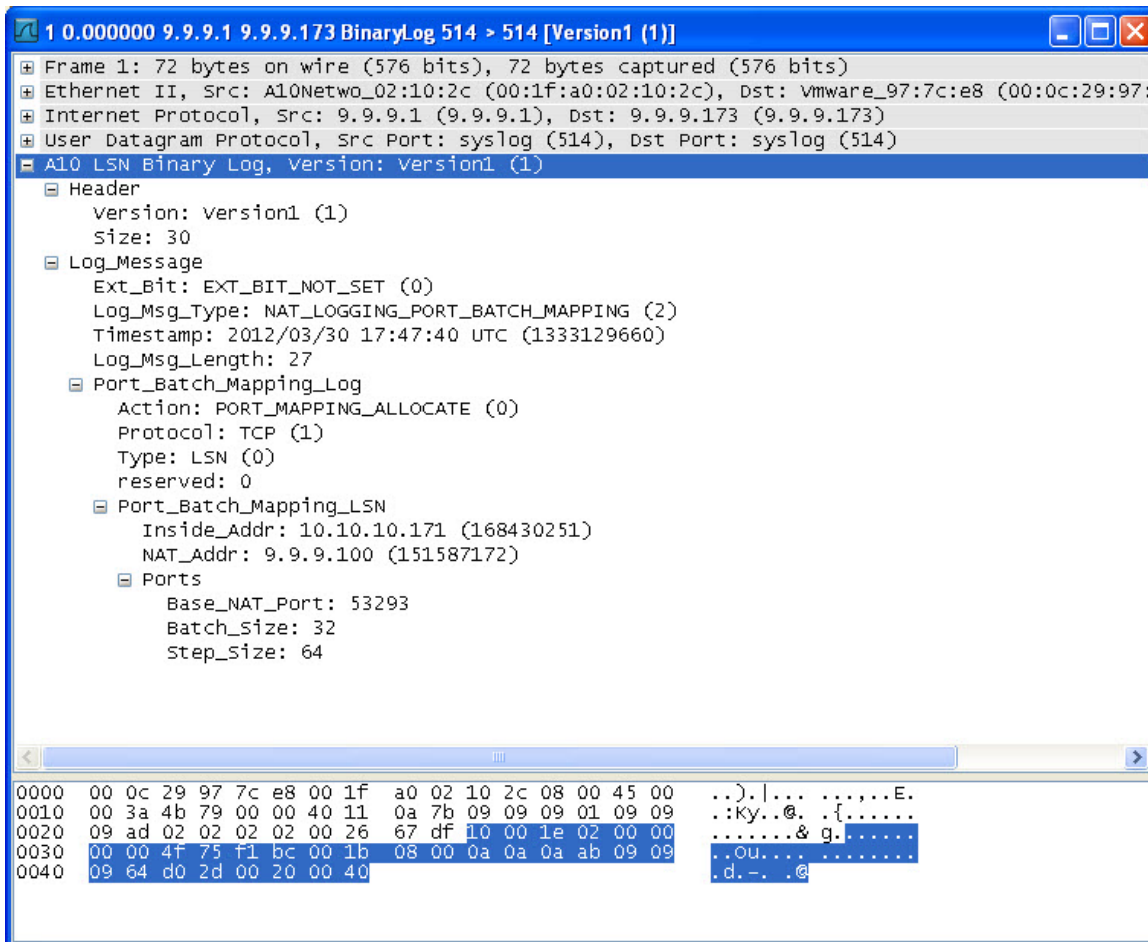
[Figure 1](#) shows an example of how binary log data appears without the A10 Networks plugin.

Figure 1 : Binary Log Viewed in Wireshark (without plugin)



[Figure 2](#) shows an example of how binary log data appears after installation of the A10 Networks plugin.

Figure 2 : Binary Log Viewed in Wireshark (without plugin)



## Installing the Wireshark Plug in Files for Binary Logging

This procedure assumes you already have Wireshark installed. A valid A10 support username and password are required for access to the A10 support site. Contact A10 Networks Technical support for information.

To install the wireshark plug in files for binary logging:

1. Download the Wireshark Generic Dissector DLL from the following URL:

<http://wsgd.free.fr/installation.html>

Install the DLL using the instructions on the web page.

2. Download the zip archive containing the custom plugin files from the A10 Networks support site:
  - a. Navigate to the main page: <http://www.A10networks.com>
  - b. Select SUPPORT PORTAL from the top navigation menu by highlighting SUPPORT and looking under PRODUCT SUPPORT.
  - c. Under the THUNDER & AX SERIES SOFTWARE & DOCUMENTATION tab, expand OTHER UPDATES and TOOLS.
  - d. Download the Wireshark plugin for A10 Binary Logging format.
3. Unzip the archive and copy the files to the plugins folder for Wireshark (ex: C:\Program Files \Wireshark\plugins\1.6.7).
4. The zip archive should contain the following files:
  - `binary_log.fdesc`
  - `binary_log.wsgd`
  - `readme.txt` (includes a copy of these installation instructions)

## Modifying Plugin Settings

---

By default, the Wireshark plugin identifies UDP traffic to destination port 514 as A10 Binary Log Messages.

To use the plugin with TCP logging, modify the following line in the `binary_log.wsgd` file:

```
PARENT_SUBFIELD udp.port
```

to

```
PARENT_SUBFIELD tcp.port
```

To decode A10 Binary Log Messages using a different destination port:

1. Right-click on the packet.
2. Select the “decode as” option and choose “BinaryLog”.

Figure 3 : TCP Logging

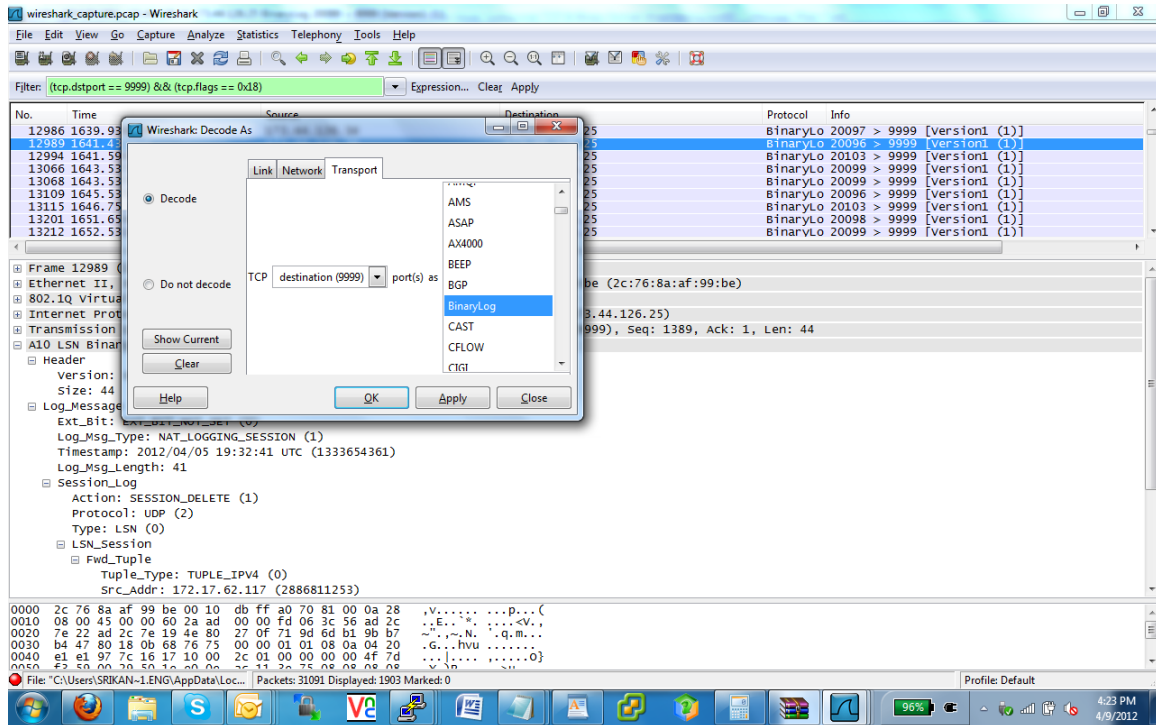
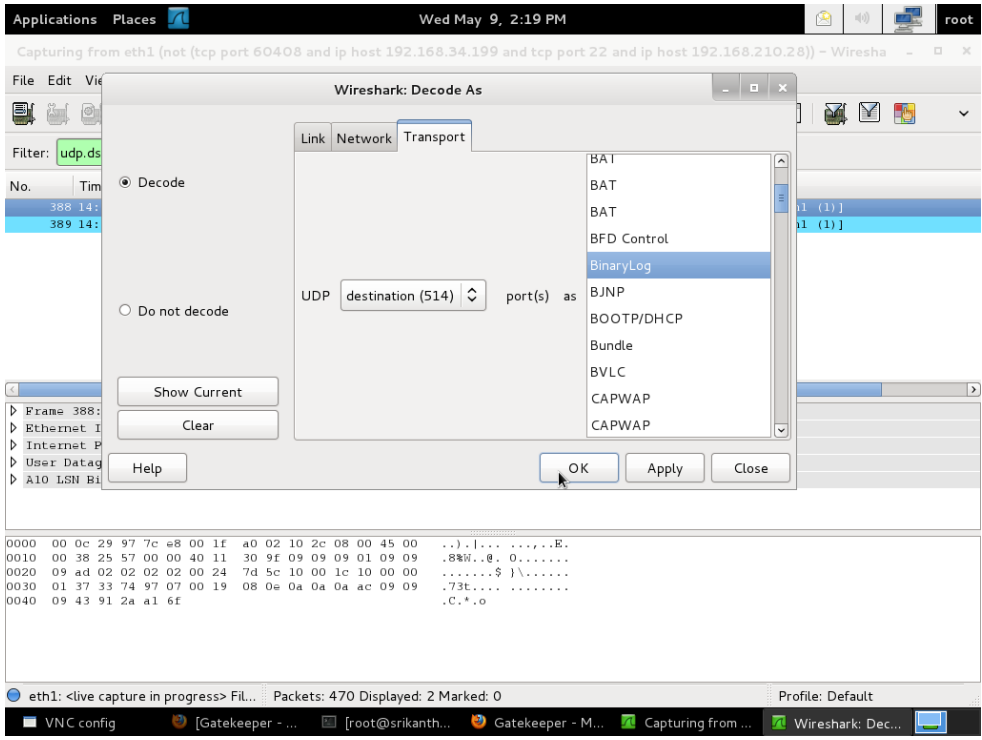


Figure 4 : UDP Logging



# Compact Logging Format

---

Compact logging format is an option to reduce the size of external traffic logs.

Compact logging format reduces log size by using short operational codes (“opcodes”) for the event and protocol names, and hexadecimal format for the IPv4 addresses. IPv6 addresses continue to be shown in their original hexadecimal format.

Compact logging format is disabled by default.

The following topics are covered:

<a href="#">Opcodes</a> .....	27
<a href="#">Extensions</a> .....	30
<a href="#">Examples</a> .....	31
<a href="#">Configuration</a> .....	32

## Opcodes

When compact logging format is enabled, event and protocol names are represented by the opcodes listed in [Table 1](#).

Table 1 : External Logging Opcodes

	Long Form	Opcode
Events	NAT_LOGGING_PORT_ALLOCATED	C
	NAT_LOGGING_PORT_REUSED	E
	NAT_LOGGING_PORT_FREED	F
	NAT_LOGGING_IP_ASSIGNED	A
	NAT_LOGGING_IP_RELEASED	R
	NAT_LOGGING_SESSION_CREATED	N
	NAT_LOGGING_SESSION_DELETED	D
	NAT_LOGGING_PORT_BATCH_ALLOCATED	B
	NAT_LOGGING_PORT_BATCH_FREED	X
	NAT_LOGGING_FIXED_NAT_PORT_ASSIGNED	P
	NAT_LOGGING_FIXED_NAT_PORT_DISABLED	O

Table 1 : External Logging Opcodes

	Long Form	Opcode
	HTTP <sup>1</sup> (HTTP request)	H
	NAT_LOGGING_POOL_ PORT_BATCH_ALLOCATED	T
	NAT_LOGGING_POOL_ PORT_BATCH_FREED	Y
	NAT_LOGGING_POOL_ PORT_BATCH_INTERIM_ UPDATE	I
	NAT_LOGGING_FIXED_ NAT_INTERIM_UPDATE	U
	NAT_LOGGING_DHCPV6_ MAP_PREFIX_ASSIGNED	L
	NAT_LOGGING_DHCPV6_ MAP_PREFIX_RELEASED	S
	NAT_LOGGING_DHCPV6_ MAP_PREFIX_RENEWED	K
	NAT_LOGGING_TRACK_ USER	M
	NAT_LOGGING_IDDOS_ BLACKHOLE_L3_ENTRY_ CREATE	A
	NAT_LOGGING_IDDOS_ BLACKHOLE_L3_ENTRY_ DELETE	D
	NAT_LOGGING_IDDOS_ BLACKHOLE_L4_ENTRY_ CREATE	A
	NAT_LOGGING_IDDOS_ BLACKHOLE_L4_ENTRY_ DELETE	D

---

<sup>1</sup>Logs an HTTP request sent by an inside client.

Table 1 : External Logging Opcodes

	Long Form	Opcode
	BLACKHOLE_L4_ENTRY_DELETE	
Protocol		
ICMP/ ICMPv6	ICM	I
UDP	UDP	U
TCP	TCP	T
IP	IPP	N
ESP	ESP	E
GRE	GRE	G
RTSP	RTP	R
OTHER	OTR	O
RADIUS Attributes (Client Mobile Number Logging)	MSISDN	M
	IMEI	E
	IMSI	S
	Custom attribute 1	R1
	Custom attribute 2	R2
	Custom attribute 3	R3
	Custom attribute 4	R4
	Custom attribute 5	R5
Custom attribute 6	R6	

Table 1 : External Logging Opcodes

	Long Form	Opcode
HTTP Request Logging	Host	H
	URL	U
	RM <sup>1</sup>	R
	File Extension	Ex
	Cookie	C
	Referer	F
	User-Agent	T
	Custom header 1	H1
	Custom header 2	H2
	Custom header 3	H3

H1, H2, and H3 are for the custom header values that you can configure using the information provided later in this section.

Example:

```
Syslog LOCAL0.DEBUG: Nov 8 00:35:57 AX2600-1/shared H: Q=1
U=http://1.0.4.147/\037 C=test_cookie\037 T=CURL\037 F=http://
www.163.com\037 H1=aaaaaa\037 H2=bbbbbb\037 H3=cccc\037\r\n
```

## Extensions

Extensions in Compact format appear in the following order. These extensions apply to ASCII format also:

- Destination IP address
- MSISDN
- IMEI
- IMSI

---

<sup>1</sup>Indicates the HTTP method used in the request; for example: POST or GET.

- RADIUS-Custom1
- RADIUS-Custom2
- RADIUS-Custom3
- RADIUS-Custom4
- RADIUS-Custom5
- RADIUS-Custom6
- Inside MAC address
- Request size
- Response size
- HTTP request number
- Then, in no specific order, the following appear: HTTP Host, HTTP URL, HTTP File-Extension, HTTP Cookie, HTTP Referer, HTTP User-Agent, custom HTTP headers 1-3.

If only some extensions are enabled, the enabled options appear in the same order, but without the disabled options.

## Examples

The following examples show log messages in long format and in reduced format. In these examples, compact logging format is used for log reduction.

### Example 1 – Original Format:

```
[timestamp] [hostname] NAT-UDP-C: 100.100.100.100:10000 ->
150.150.150.150: 10000
```

### Example 1 – Compact Format:

```
[timestamp] [hostname] UC: 64646464:2710->96969696:2710
```

### Example 2 – Original Format:

```
[timestamp] [hostname] NAT-TCP-C: [2001:abcd::1]:54040 -> 150.150.150.150:
54040
```

### Example 2 – Compact Format:

```
[timestamp] [hostname] TC: [2001:abcd::1]:D318->96969696:D318
```

## Configuration

To configure compact logging, use either of the following methods.

### Using the GUI

---

1. Navigate to **CGN > LSN > Templates**.
2. Select **Logging** from the drop-down list.
3. Select an existing template, or click **Create** to create a new template.
4. If creating a new template, enter a name for the template in the Name field.
5. From the drop-down list in the “Format” field, select **Compact**.
6. Click **Update**.

### Using the CLI

---

To enable compact logging format, use the following command at the configuration level of the LSN logging template:

```
ACOS(config)# cgnv6 template logging lsn_logging  
ACOS(config-logging:lsn_logging)# format compact
```

# Custom Logging Format

---

The following topics are covered:

<a href="#">Overview</a> .....	33
<a href="#">Configuring Custom Log Messages</a> .....	34

## Overview

ACOS provides the capability to create a custom CGN log format. This allows the freedom to specify an arbitrary format that is non-compliant with RFC 5424, the syslog standard. Custom logs also provide the option to include the session start time and session duration in CGN logs.

Custom logs provide the following flexibility:

- They do not enforce any mandatory formats. In essence, they provide flexibility to indicate keywords followed by a string or include just a text string without any keywords.
- They do not require a set order in the presentation of information in the log. The `custom` command allows you the freedom to specify an arbitrary format. For instance, the log can start with an IP address and port followed by the date and time, or start with the date and time, followed by the IP address and the port information.
- They do not contain default keywords for any event. Explicitly configure any event that should be logged. If an event is not configured, it will not appear in the resulting log.
- They do not require that keywords be enclosed in square brackets.

The custom logging feature is an enhancement to the supported RFC custom logs that you can create using the `rfc-custom` command. For details on RFC 5424 custom log formats, [RFC 5424 Custom Logging Format](#).

The advantage of custom logging is apparent when compared to RFC custom logs:

Table 2 : Differences between RFC Custom Logs and Custom Logs

RFC Custom Logs	Custom Logs
<p>Logs must conform to the formatting guidelines outlined in RFC 5424, "The Syslog Protocol." For example, when you issue the <code>rfc-custom session-create</code> command, it must be followed by a message ID within quotes, followed by keywords specified inside square brackets to build an RFC-complaint custom log. For example, "MsgId [\$keyword1\$\$keyword2\$]".</p>	<p>Logs can have an arbitrary format. When you issue the <code>custom session-create</code> command, indicate keywords in any random order, without specifying the message ID, such as "\$keyword1\$\$keyword2\$". You may use keywords to build any log. For example, indicate the "<code>\$fwd-src-ip\$  \$fwd-src-port\$</code>" keywords followed by any message.</p>
<p>You can configure a log to display the session duration using the "<code>\$sesn-dur\$</code>" keyword.</p>	<p>You can configure the session duration and the session start time in the log. You may include a text string such as "<code>the session start time is \$sesn-start-time\$</code>". In this case, the keyword will be replaced by an actual value. The log maybe may appear as follows: 80.1.1.124 1234 session start time is 20141231015456.</p>
<p>If you configure RFC custom logs without specifying values for every event, logs will be sent using the default values for those events.</p>	<p>Custom logs do not contain default values, therefore, unless you configure an event explicitly, no messages will be logged.</p>

## Configuring Custom Log Messages

To configure custom logs, follow the procedures documented in this section.

## Using the GUI

---

To configure the custom logging feature, do the following:

1. Navigate to **CGN > LSN > Templates**.
2. Select **Logging** from the drop-down list.
3. Select an existing template, or click **Create** to create a new template.
4. If creating a new template, enter a name for the template in the Name field.
5. From the drop-down list in the “Format” field, select **Custom**.
6. Expand the Custom section further down the page, and enter the custom strings and keywords in the message configuration fields.
7. Click on **Update**.

## Using the CLI

---

To enable custom logging capabilities, issue the following commands:

1. When in the NAT logging configuration mode, use the new custom keyword to begin the arbitrary custom log creation process.
2. Specify the following custom logging sub-options to configure the headers, messages, or time-stamp formats. You may configure these sub options one after another.
3. To configure the syslog-header as the custom header, use the following command:

```
ACOS(config)# cgnv6 template logging syslog
ACOS(config-logging:syslog)# log http-requests host
ACOS(config-logging:syslog)# log sessions
ACOS(config-logging:syslog)# include-destination
ACOS(config-logging:syslog)# include-session-byte-count
ACOS(config-logging:syslog)# rule http-requests dest-port 80 include-
byte-count
ACOS(config-logging:syslog)# batched-logging-disable
ACOS(config-logging:syslog)# service-group sg_log
ACOS(config-logging:syslog)# custom header use-syslog-header
```

- a. To configure the format of the logging message, use the following command:

```
ACOS(config-logging:syslog)# custom message session-deleted "$fwd-src-
ip$|$fwd-src-port$|$rev-dst-ip$|$rev-dst-port$|$sesn-start-
time$|$rev-src-ip$|$rev-src-port$|$sesn-start-time-epoch$|$sesn-
end-time$|$sesn-end-time-epoch$"
```

- b. To configure the default format of the time stamp displayed in the log message, use the following command:

```
ACOS(config-logging:syslog)# custom time-stamp-format "%Y%m%d%H%M%S"
```

The default session time stamp format is as follows: "%Y%m%d%H%M%S"

- c. To configure the custom format of the time stamp to display three-letter month in alphabets in the log message, use the following command:

```
ACOS(config-logging:syslog)# custom time-stamp-format "<%Y> <%o>
<%d> <%H:%M:%S>"
```

where <%o> displays the month in the three-letter alphabet automatically.

---

**NOTE:** For details on the custom keywords, use the `show cgnv6 logging keywords` command to see the list of keywords associated to the session.

---

## Additional Keywords for Custom Logs

The following keyword has been added to both the “custom messages” and the “rfc-custom messages.” The remaining keywords are supported as in previous releases:

- `$rule-name$`– This keyword specifies the rule that is matched by traffic. This keyword is applicable to session-created and session-deleted custom logs.
- `$sesn-dur$`– This keyword specifies the session duration and it is applicable only for the session-delete event.

---

**NOTE:** When you include this keyword, it will reduce the number of sessions. By default, this keyword will not be included. It must be explicitly configured.

---

The following keyword has been added only to “custom messages:”

- `$sesn-start-time$`—This keyword specifies the time a session was created and is for session-create and session-delete events. This format can be configured using the `custom time-stamp-format format-string` CLI command.

---

**NOTE:** When you include this keyword, it will reduce the number of sessions. By default, this keyword will not be included. This format can be customized unlike when using “format rfc5424.” You can access this time information from the event timestamp displayed in the Syslog header.

---

- `$sesn-fwd-byte$` – This keyword specifies the byte count for forward traffic session.
- `$sesn-rev-byte$` – This keyword specifies the byte count for reverse traffic session.

---

**NOTE:** Even if these keywords `$sesn-fwd-byte$` and `$sesn-rev-byte$` are specified in the custom log format, you must have the `include-session-byte-count` option configured in the logging template in order to view the fields. These fields are already included in HTTP logging messages.

---

- `$sesn-start-time-epoch$` – This keyword specifies the start time in epoch millisecond instead of plain text.
- `$sesn-end-time$` – This keyword specifies the session deletion time.
- `$sesn-end-time-epoch$` – This keyword specifies the end time in epoch millisecond instead of plain text.

The following keywords are added for HTTP header logging:

- `$http-file-extension$` – This keyword specifies the URI file extension.
- `$http-hdr-cookie$` – This keyword specifies the Cookie header.
- `$http-hdr-referrer$` – This keyword specifies the Referrer header.
- `$http-hdr-user-agent$` – This keyword specifies the User-Agent header.
- `$http-hdr-custom1$` – This keyword specifies the Custom header.
- `$http-hdr-custom2$` – This keyword specifies the Custom header.

- `$http-hdr-custom3$`— This keyword specifies the Custom header.
- `$http-hdr-custom4$`— This keyword specifies the Custom header.
- `$http-hdr-custom5$`— This keyword specifies the Custom header.
- `$http-hdr-custom6$`— This keyword specifies the Custom header.

To support new interim-update logs for Port Batch version 2, new Custom Logging Format configurable entries and keywords were added in the CLI.

Under the custom logging template in the CLI, new configurable entries were added for the RADIUS interim updates. Keywords for existing Port Batch version 2 and Fixed NAT entries were also added.

Use the `show cgnv6 logging keywords {feature} {event}` command to see all valid keywords specific to the event.

---

**NOTE:** The keywords for Port Batch version 2 freed (port-batch-v2-freed) are the same as the keywords for Port Batch version 2 interim update (port-batch-v2-interim-update, with the addition of the `$ct-msg$` keyword to log connection termination).

---

## Configuration Examples

The following example displays a sample log resulting from a custom configuration:

```
10.58.126.66|8638|5.47.254.85|21920|20130930134646|15000 |188.41.253.11|53
10.56.98.20|58692|5.47.226.23|7463|20130930134649|12000|188.41.253.11|53
```

The following table provides an explanation for the fields that are displayed in the log. In this case, each field is separated by a vertical bar (|).

The table describes the different fields that are displayed in the log file for the example output shown above. Note that it reflects the output based on the custom configuration on the ACOS device. If configured differently, the output will reflect the actual configuration. If your input in your custom logging commands contains a text string with spaces in between the text you provide, be sure to enclose the text within quotation marks:

Table 3 : Custom Logging Field Explanations

Log Message Field	Explanation
10.58.126.66 8638	Indicates the subscriber IP address and source port.
5.47.254.85 21920	Public IP address used for the Network Address Translation (NAT) and the associated port. Typically, this field displays the source port, but it can be configured to display the destination port instead.
20130930134646	Information on when the session was started followed by the hour, minute, and seconds (using the "%Y%m%d%H%M%S" format).
15000	Indicates the session duration in milliseconds.
188.41.253.11 53	Reflects the destination IP address and destination port.

**NOTE:** The external logging servers will be able to read and interpret the keywords specified in the RFC custom logging templates. Since the custom logging templates do not have to use the keywords, the messages presented in the configuration statements will be passed on verbatim and will appear in the logs.

### Example of a Custom Message Format

In the example, use the following commands and keywords to configure the desired log message when a session is deleted:

```
ACOS(config-logging:lsn_logging)# custom message session-deleted "$fwd-
src-ip$|$fwd-src-port$|$rev-dst-ip$|$rev-dst-port$|$sesn-start-time$|$rev-
src-ip$|$rev-src-port$|$sesn-start-time-epoch$|$sesn-end-time$|$sesn-end-
time-epoch$"
```

The above command will display the log message as follows:

```
10.56.98.20|58692|5.47.226.23|7463|20130930134649|188.41.253.11|53|1380548
809000|20130930134749|1380548869000
```

## Example of a Custom Header

In the example, use the following commands and keywords to configure the desired header format in the event of a deleted session:

```
ACOS(config-logging:lsn_logging)# custom header use-syslog-header
ACOS(config-logging:lsn_logging)# custom message session-deleted "$fwd-
src-ip$|$fwd-src-port$|$rev-dst-ip$|$rev-dst-port$|$sesn-start-
time$|$sesn-dur$|$rev-src-ip$|$rev-src-port$"
```

The above command will display the log with the following Syslog header:

```
LOCAL7.DEBUG: 1 2013-11-18T12:26:16+09:00 192.168.105.195 AX5100 shared
10.58.126.66|8638|5.47.254.85|21920|20130930134646|15000 |188.41.253.11|53
```

## Custom Log Generated for a Deleted Session

You may specify the new log string format:

```
ACOS(config-logging:lsn_logging)# custom message session-deleted "Notice:
Deleting session which started at $sesn-start-time$: client IP=$fwd-src-
ip$, session duration=$sesn-dur$."
```

The above command will display the log with the following message in the event of a deleted session:

```
Notice: Deleting session which started at 20131114020334: client
IP=80.1.1.172, session duration=30123.
```

## Example of a Custom Message with File Extension of HTTP URI

In the example, use the following commands and keywords to configure the file extension of HTTP URI:

```
ACOS(config)# cgnv6 template logging log1
ACOS(config-logging:log1)# log http-requests url
ACOS(config-logging:log1)# include-http referer
ACOS(config-logging:log1)# include-http cookie
ACOS(config-logging:log1)# include-http user-agent
ACOS(config-logging:log1)# include-http header1 TestHdr1
ACOS(config-logging:log1)# include-http header2 TestHdr2
ACOS(config-logging:log1)# include-http header3 TestHdr3
ACOS(config-logging:log1)# include-http method
```

```
ACOS (config-logging:log1) # include-http request-number
ACOS (config-logging:log1) # include-http file-extension
ACOS (config-logging:log1) # rule http-requests dest-port 80
ACOS (config-logging:log1) # format custom
ACOS (config-logging:log1) # service-group syslog
ACOS (config-logging:log1) # custom message http-request-got http:[${http-
req-num$|${http-method$|${http-host-or-url$|${http-file-extension$|${http-hdr-
cookie$|${http-hdr-referer$|${http-hdr-user-agent$|${http-hdr-custom1$|${http-
hdr-custom2$|${http-hdr-custom3$|${http-hdr-custom4$|${http-hdr-
custom5$|${http-hdr-custom6$}]
```

To illustrate the custom message configured the following sample HTTP request is used:

```
GET /index.html HTTP/1.1
User-Agent: Wget/1.15 (linux-gnu)
Accept: /
Host: http2.test60:88
Connection: Keep-Alive
Cookie: id=123456
TestHdr1: Customr hdr1
Referer: Ref
TestHdr3: Customr hdr3
```

The above command will display the log with the following message:

```
http:[1|GET|http://http2.test60/index.html|html|id=123456|Ref|Wget/1.15
(linux-gnu)|Customr hdr1|-|Customr hdr3]
```

**NOTE:** The order of HTTP headers in logging packet is predefined, user cannot change it. Custom headers are configurable, but the order is fixed as URL, File-Extension, Cookie, Referer, User-Agent, custom header 1, custom header 2, and custom header 3]. For custom formats, the sequence can be configured differently.

# RFC 5424 Custom Logging Format

---

This section describes support for RFC 5424, the Syslog Protocol, and how to configure it.

The following topics are covered:

<a href="#">Overview</a> .....	43
<a href="#">Message String Customization</a> .....	45

## Overview

The ACOS device supports RFC 5424, the Syslog Protocol. When RFC 5424 support is enabled, external log messages use the format described in the RFC.

RFC 5424 support is disabled by default. You can configure it in an individual logging templates. When RFC 5424 support is enabled, the message strings shown in [Default Message Strings for RFC 5424](#) are used by default. You can customize the strings for individual message types.

## Log Message Format

When RFC 5424 support is enabled, external log messages have the following format:

*header message-string*

Here is an example:

```
<135>1 2012-04-19T05:54:14-07:00 192.168.147.167 AX2600 -
SessionCreated:TCP
[- 3.3.3.50 26548 6.6.6.50 80 - 6.6.6.50 80 6.6.6.200 12218 - -]
```

The portion of the message shown in *Italic type* is the message header. The portion shown in **bold type** is the message string. The “ - ” portions indicate empty or inapplicable fields. In this example, the missing fields are the PROCID in the header (see below), and a couple of data fields. The data fields are described in [CLI Example – RFC 5424 Support with Some Custom Message Strings](#).

## Header Fields

RFC 5424 log message headers contain the following fields:

```
<PRI>VERSION TIMESTAMP HOSTNAME APP-NAME PROCID
```

The header fields provide the following information:

- <PRI> – Integer that specifies the log facility and severity. This value is calculated as follows:

```
facility * 8 + severity
```

The facility number is multiplied by 8. The severity number is then added. For example, value 135 means facility 16 and severity 7.

---

**NOTE:** You can change the severity and facility in the logging template.

---

- VERSION – Version of the Syslog protocol (always 1).
- TIMESTAMP – ACOS system time when the message was generated. Depending on the configuration, the timestamp has one of the following formats:

*YYYY-MM-DDTHH:MM:SSZZZ:ZZ*

*YYYY-MM-DDTHH:MM:SS.SSZZZ:ZZ*

Where:

- YYYY – The year.
  - MM – The month (01-12).
  - DDTHH – The day (1-31) and hour (00-23).
  - MM:SS (or MM:SS.SS) – The minutes and seconds. If 10-ms timestamp resolution is enabled, the “.SS” portion at the end indicates the number of milliseconds. If 10-ms timestamp resolution is disabled, the “.SS” portion does not appear.
  - ZZZ:ZZ – Timezone offset from UTC. The first “Z” indicates the offset from UTC (“+” or “-”).
- HOSTNAME – Management IP address of the ACOS device that generated the message.
  - APP-NAME – Hostname of the ACOS device that generated the message.
  - PROCID – Not used in the current release. This field always appears as a dash with a blank space on each side: “ - ”

---

**NOTE:** Optionally, you can change the TIMESTAMP field’s format to the following:

*YYYY MMM DD HH:MM:SS*

Example: 1990 Jan 15 12:30:30

---

## Message String Fields

Each message string contains, at a minimum, some text. Generally, a message string also contains data fields.

You also can customize individual message strings. (See [Default Message Strings for RFC 5424](#).)

## Message String Customization

You can customize any of the message strings. For example, you can add, move, or delete fields. You also can add, modify, or delete text. For example, LSN port allocation messages use the following message strings by default:

```
LSN:PortAllocation:$proto-name$ [$src-ip$ $src-port$ $nat-ip$ $nat-port$]
```

Here is a message generated using this format:

```
<135>1 2012-04-19T05:54:14-07:00 192.168.147.167 AX2600 -
LSN:PortAllocation:TCP [3.3.3.50 26548 6.6.6.200 12218]
```

Suppose you customize the LSN port allocation message string, to add some text:

```
LSN:PortAllocation:$proto-name$ [Inside=$src-ip$ $src-port$
Global=$nat-ip$ $nat-port$ -]
```

In this case, a port allocation message appears as follows:

```
<135>1 2012-04-19T05:54:14-07:00 192.168.147.167 AX2600 -
LSN:PortAllocation:TCP [Inside=3.3.3.50 26548 Global=6.6.6.200 12218]
```

## Message String Syntax

The syntax for message strings follows RFC 5424. The main syntax rules also are described here.

For text, all characters except \$ and % are supported.

For data fields, you must use structured data format: [*structured-data*]

The structured data can consist of data fields, strings, or both. For example, the following is a sample set of structured data contains some data fields and some text:

```
LSN:PortAllocation:$proto-name$ [$src-ip$ $src-port$ $nat-ip$ $nat-port$]
```

The data fields are shown in italics. When you specify a custom message string, you must spell the data field names exactly as shown, including the “\$” on each end. The brackets ([ and ]) are the delimiters for the structured data set. The “LSN:PortAllocation:” portion is text.

The brackets are included in the actual message. For example:

```
<135>1 2012-04-19T05:54:14-07:00 192.168.147.167 AX2600 -
LSN:PortAllocation:TCP [3.3.3.50 26548 6.6.6.200 12218]
```

No blank spaces are allowed between the left bracket and the following field or text. Likewise, no blank space is allowed immediately before the right bracket.

### Valid

```
NAT64:FixedNATDisabled:$proto-name$ [$src-ip$ $nat-ip$]
```

### Invalid

```
NAT64:FixedNATDisabled:$proto-name$ [ $src-ip$ $nat-ip$]
NAT64:FixedNATDisabled:$proto-name$ [$src-ip$ $nat-ip$ ]
NAT64:FixedNATDisabled:$proto-name$ [ some text first $src-ip$ $nat-ip$]
```

If you use more than one set of structured data, do not use any blank spaces between data sets.

### Valid

```
[structured-data] [structured-data]
```

### Invalid

```
[structured-data] [structured-data]
```

## Using the GUI to Customize Message Strings

To customize message strings using the GUI:

1. Navigate to **CGN > LSN > Templates**.
2. Select **Logging** from the drop-down list.
3. Select an existing template, or click **Create** to create a new template.

4. Expand the RFC Custom section and configure the options.
5. Click **Update**.

## Using the CLI to Customize Message Strings

This section contains the following examples:

- [CLI Example – RFC 5424 Support with Default Message Strings](#)
- [CLI Example – RFC 5424 Support with Some Custom Message Strings](#)

### CLI Example – RFC 5424 Support with Default Message Strings

The following commands configure external logging with RFC 5424 support. (In this example, logging over TCP is configured.)

First, the following commands add the log server configuration:

```
ACOS(config)# cgnv6 server syslog1 203.0.113.1
ACOS(config-real server)# port 514 tcp
ACOS(config-real server-node-port)# exit

ACOS(config)# cgnv6 server syslog2 203.0.113.2
ACOS(config-real server)# port 514 tcp
ACOS(config-real server-node-port)# exit
```

The following commands add the log servers to a service group:

```
ACOS(config)# cgnv6 service-group syslog tcp
ACOS(config-cgnv6 svc group)# member syslog1 514
ACOS(config-cgnv6 svc group)# member syslog2 514
ACOS(config-cgnv6 svc group)# exit
```

The following commands configure the logging template:

```
ACOS(config)# cgnv6 template logging lsn_logging
ACOS(config-logging:lsn_logging)# format rfc5424
ACOS(config-logging:lsn_logging)# service-group syslog
ACOS(config-logging:lsn_logging)# exit
```

The following command activates the logging template:

```
ACOS(config)# cgnv6 lsn logging default-template lsn_logging
```

## Sample Messages:

This configuration can generate log messages such as the following:

```

<135>1 2012-04-19T05:54:14-07:00 192.168.147.167 AX2600 -
SessionCreated:TCP [IPV4 - 3.3.3.50 26548 6.6.6.50 80 - 6.6.6.50 80
6.6.6.200 12218 - -]
<135>1 2012-04-19T05:54:14-07:00 192.168.147.167 AX2600 -
LSN:PortAllocation:TCP [3.3.3.50 26548 6.6.6.200 12218 - -]
<135>1 2012-04-19T05:54:17-07:00 192.168.147.167 AX2600 -
SessionDeleted:TCP [IPV4 - 3.3.3.50 26548 6.6.6.50 80 - 6.6.6.50 80
6.6.6.200 12218 - -]
<135>1 2012-04-19T05:54:17-07:00 192.168.147.167 AX2600 -
LSN:PortFreed:TCP [3.3.3.50 26548 6.6.6.200 12218 - -]

```

## CLI Example – RFC 5424 Support with Some Custom Message Strings

The commands in this example enable RFC 5424 support, and customize the log message strings for session creation and deletion messages.

The following commands add the log server configuration:

```

ACOS(config)# cgmv6 server syslog1 203.0.113.1
ACOS(config-real server)# port 514 tcp
ACOS(config-real server-node-port)# exit

ACOS(config)# cgmv6 server syslog2 203.0.113.2
ACOS(config-real server)# port 514 tcp
ACOS(config-real server-node-port)# exit

```

The following commands add the log servers to a service group:

```

ACOS(config)# cgmv6 service-group syslog tcp
ACOS(config-cgmv6 svc group)# member syslog1 514
ACOS(config-cgmv6 svc group)# member syslog2 514
ACOS(config-cgmv6 svc group)# exit

```

The following commands begin configuration of the logging template:

```

ACOS(config)# cgmv6 template logging lsn_logging
ACOS(config-logging:lsn_logging)# format rfc5424
ACOS(config-logging:lsn_logging)# service-group syslog

```

The following commands list the data field names you can use in log message strings for session creation and deletion:

```
ACOS (config-logging:lsn_logging)# show cgnv6 logging keywords session-
created
$proto-name$           Protocol name
$proto-num$            Protocol number
...

ACOS (config-logging:lsn_logging)# show cgnv6 logging keywords session-
deleted
$proto-name$           Protocol name
$proto-num$            Protocol number
$fwd-tuple-tuple$     Forward tuple type
...
```

The following commands customize the message strings for session creation and deletion:

```
ACOS (config-logging:lsn_logging)# rfc-custom message session-created
"SessionC
[$proto-num$ $fwd-src-ip$ - $rev-dst-ip$ $fwd-src-port$ $rev-dst-port$ -]"
ACOS (config-logging:lsn_logging)# rfc-custom message session-deleted
"SessionD
[$proto-num$ $fwd-src-ip$ - $rev-dst-ip$ $fwd-src-port$ $rev-dst-port$ -]"
```

The hyphens are text. They will appear in the messages but in this case do not indicate missing fields.

### Sample Messages:

This configuration can generate log messages such as the following:

```
<135>1 2012-04-19T05:59:13-07:00 192.168.147.167 AX2600 - SessionC [6
3.3.3.50 - 6.6.6.200 49927 14132 -]
<135>1 2012-04-19T05:59:16-07:00 192.168.147.167 AX2600 - SessionD [6
3.3.3.50 - 6.6.6.200 49927 14132 -]
```

### Data Fields

- The `$fwd-tuple-type$` and `$rev-tuple-type$` data fields specify the IP version (IPv4 or IPv6). For descriptions of the other data fields, see [Message String Fields](#).

- The \$fwd-tunnel\$, \$rev-tunnel\$, \$fwd-dst-tunnel\$, \$rev-dst-tunnel\$, and \$tunnel-ip\$ data fields apply only to DS-Lite and 6rd-NAT64.
- If more than one of the RADIUS attribute keywords is used, the values appear in the following order: MSIDSN, IMEI, and IMSI.
- To use the \$proto-name\$, \$proto-num\$, \$fwd-tuple-type\$, \$fwd-tunnel\$, \$fwd-src-ip\$, \$fwd-src-port\$, \$fwd-dst-tunnel\$, \$fwd-dst-ip\$, \$fwd-dst-port\$, \$rev-tuple-type\$, \$rev-tunnel\$, \$rev-src-ip\$, \$rev-src-port\$, \$rev-dst-tunnel\$, \$rev-dst-ip\$, and \$rev-dst-port\$ keywords, make sure to enable the option to include Layer 4 session information.

For a list of default message strings, see [Default Message Strings for RFC 5424](#).

# CEF Logging Format

---

The following topics are covered:

<a href="#">Overview</a> .....	51
<a href="#">Configuring the CEF Logging Format</a> .....	52

## Overview

The Common Event Format (CEF) uses UTF-8 format for encoding log messages. CEF relies on the Syslog message format as a transport channel. CEF log messages contain the Syslog Header, CEF Header, and the CEF log message itself. The log message is a stream of key-value pairs. The CEF format defines predefined key names, length, and data type. It also specifies custom keys that can be used for information which does not fit into the list of predefined key names.

The support of CEF format is implemented for various log message types supported by CGN traffic logging. The following CGN Traffic log messages are supported with :

- NAT44/NAT64 with LSN and Fixed NAT: session-creation, session deletion, nat port assignment, nat port free
- NAT44/NAT64 with Fixed NAT: fixed nat port usage, fixed-nat port disable
- NAT44/NAT64 with LSN port batching v1: port batch allocation, port batch free
- NAT44/NAT64 with LSN port batching v2: port batch free, port pool batch allocation/free

## CEF Logs

---

The following is a list of CGN logs supporting CEF format:

- CEF\_LOGGING\_NAT\_PORT\_ALLOCATED is the CGN NAT port allocated log supporting CEF.
- CEF\_LOGGING\_NAT\_PORT\_FREED is the CGN NAT port freed log supporting CEF.

- CEF\_LOGGING\_NAT\_SESSION\_CREATED is the CGN NAT session created log supporting CEF.
- CEF\_LOGGING\_NAT\_SESSION\_DELETED is the CGN NAT session deleted log supporting CEF.
- CEF\_LOGGING\_NAT\_PORT\_BATCH\_ALLOCATED is the CGN NAT port batch allocated log supported CEF.
- CEF\_LOGGING\_NAT\_PORT\_BATCH\_FREED is the CGN NAT port batch freed log supporting CEF.
- CEF\_LOGGING\_NAT\_POOL\_PORT\_BATCH\_ALLOCATED is the CGN NAT pool port batch allocated log supporting CEF.
- CEF\_LOGGING\_NAT\_POOL\_PORT\_BATCH\_FREED is the CGN NAT pool port batch freed log supporting CEF.
- CEF\_LOGGING\_FIXED\_NAT\_PORT\_ASSIGNED is the CGN Fixed NAT port assigned log supporting CEF.
- CEF\_LOGGING\_FIXED\_NAT\_PORT\_DISABLED is the CGN Fixed NAT port disabled log supporting CEF.

### Limitation

- CEF format logs support all the options under cgnv6 logging template, except include-http and include-radius-attribute and http logging.
- Batch logging is not supported for CGN CEF log messages.
- Merge style logging for CEF is not supported.
- Fixed Nat Interim update is not supported with CEF logs.

## Configuring the CEF Logging Format

To configure the CEF format using GUI, do the following:

1. Navigate to **CGN > LSN > Templates**.
2. Select **Logging** from the drop-down list.
3. Select an existing template, or click **Create** to create a new template.
4. If creating a new template, enter a name for the template in the Name field.

5. From the drop-down list in the “Format” field, select **CEF**.
6. Expand the Custom section further down the page, and enter the custom strings and keywords in the message configuration fields.
7. Click on **Update**.

To configure CEF format using CLI, use the following commands:

```
ACOS(config)# cgmv6 server syslog1 203.0.118.1  
ACOS(config-real server)# port 514 udp  
ACOS(config-real server)# exit  
ACOS(config)# cgmv6 service-group syslog udp  
ACOS(config-cgmv6 svc group)# member syslog1 514  
ACOS(config-cgmv6 svc group)# exit  
ACOS(config)# cgmv6 template logginglog1  
ACOS(config-logging:log1)# format cef
```

# NetFlow v9 and v10 (IPFIX)

---

This section describes how to configure NetFlow on your ACOS device.

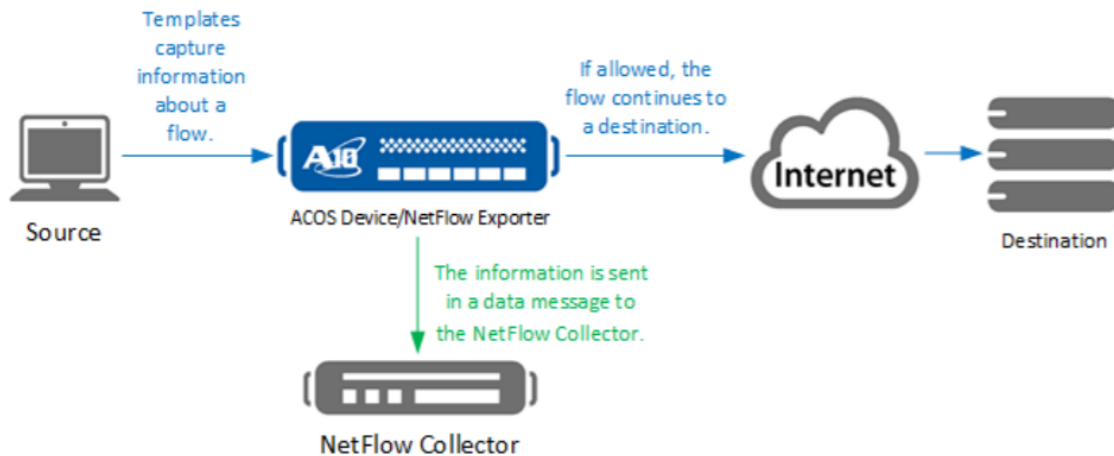
The following topics are covered:

<a href="#">NetFlow Overview</a> .....	55
<a href="#">NetFlow Versions Supported</a> .....	55
<a href="#">NetFlow Parameters</a> .....	56
<a href="#">Formatting of NetFlow Records for Long-Lived Sessions</a> .....	58
<a href="#">Predefined NetFlow Templates</a> .....	59
<a href="#">Custom IPFIX Templates</a> .....	83
<a href="#">NetFlow Logging Over Dedicated Partition</a> .....	123
<a href="#">Configuring NetFlow</a> .....	123
<a href="#">Displaying Show Counters</a> .....	131

## NetFlow Overview

An ACOS device can act as a NetFlow exporter. The NetFlow exporter (ACOS device) monitors traffic and sends the data to one or more NetFlow collectors, where the information can be stored and analyzed by a network administrator.

Figure 5 : NetFlow Architecture with an ACOS device as Exporter



**CAUTION:**

NetFlow is a heavy user of system resources and requires additional memory, which is equivalent to half the size of a session for each data session. When NetFlow is enabled, the session table capacity is reduced by one-third (1/3) of its original amount. For example, a system with a maximum of 100 sessions can only have 66 sessions.

## NetFlow Versions Supported

Both NetFlow version 9 and NetFlow version 10 (IPFIX) are supported.

- NetFlow version 9 is described in RFC 3954, Cisco Systems NetFlow Services Export Version 9.
- NetFlow version 10 (IPFIX) is compliant with RFC 5101 and 5102.

**NOTE:** The terms “NetFlow v10” and “IPFIX” are used interchangeably in this document and in the CLI, even though they are not the same thing. This anomaly exists for backwards compatibility.

---

## NetFlow Parameters

On an ACOS device, you can configure up to 128 NetFlow monitors. This is a global system maximum. If the device has multiple partitions, this maximum applies in aggregate to all the partitions, including the shared partition.

A NetFlow monitor consists of the following protocol parameters, which can be used to configure the ACOS device to export data in the format of NetFlow v9 or NetFlow v10 (IPFIX). The default protocol is NetFlow v9.

- Export destination – External devices to export the collected data. You can specify the IP address of a single NetFlow collector, or configure a service group that comprises multiple collectors.
  - To achieve load balancing of NetFlow traffic among two or more collectors, they must be placed within the same service group.
  - If two or more NetFlow collectors are configured using only IP addresses and are not included in a service group, and if they are configured with the same NetFlow properties (record types), then NetFlow traffic will be duplicated to both places and the NetFlow traffic will not be load-balanced.

**NOTE:** NetFlow information is sent from the ACOS device through a data port that is dynamically selected and is based upon information in the routing table.

---

- Record type – Types of data to export. NetFlow exporters use the following types of messages to send collected data to a collector server:
  - Templates – A NetFlow template defines the set of data to be collected, and the order in which that information will appear in the data messages.
  - Data – NetFlow data messages contain the collected data, such as flow information. Packets for data messages can contain data for more than one

flow.

Each NetFlow monitor can use one or more NetFlow templates. This release includes some predefined NetFlow templates. (See [Predefined NetFlow Templates](#).)

Alternatively, instead of using a predefined NetFlow template, you may wish to create your own custom event template for IPFIX. (See [Custom IPFIX Templates](#).)

- Monitoring filters – Specific type of resources to monitor. You can specify monitoring of the following resource:
  - Ethernet data ports – Specify the list of ports to monitor. Flow information for the monitored interfaces is sent to the NetFlow collector(s). By default, no filters are in effect. Traffic is monitored on all interfaces and Virtual Ethernet (VE) interfaces.
- Flow timeout – This is the interval for sending flow records for long-lived sessions. (For short-lived sessions, any flow records are sent upon termination of the session.) For long-lived sessions, the flow timeout default value is 10 minutes. After this amount of time has elapsed, the ACOS device will send any flow records to the NetFlow collector, even if the flow is still active. The flow timeout can be set to 0-1440 minutes. If this is set to 0, this essentially disables the flow timeout feature. Regardless of how long-lived a flow might be, the ACOS device waits until the flow has ended and the session is deleted before it sends any flow records for it.

---

**NOTE:** This document uses the terms “flow” and “session” interchangeably, while acknowledging that there are subtle differences in their meaning.

---

- Template transmission options – The ACOS device periodically resends the NetFlow templates to the collector(s). The following counters control when the templates are resent:
  - Number of data records sent – This is a running counter of the total number of data messages that have been sent to the NetFlow collector. After the specified number of data records are sent, the ACOS device resends the template that describes the data (as a way to refresh the template). The default is 1000 records. You can configure the set template interval to 0-1000000 records. To disable, set this number to 0.

- Number of seconds since the last time the template was sent – After the specified number of seconds has passed, the ACOS device resends the template to perform a refresh of the template on the collector. The default is 1800 seconds. You can set it to 0-86400 seconds. After the template is resent, this counter is set back to 0 second. To disable, set this number to 0.
- Management interface – Uses the IP of the ACOS management interface, instead of the IP of the data interfaces when sending traffic to the NetFlow collectors. By default, the ACOS device sends NetFlow traffic out to the data interface. When the Management Interface option is enabled, the NetFlow information is still sent via a data interface that is dynamically (and automatically) selected based upon the routing table, but the source IP of the packets will be the IP of the management port.
- Monitor state – Enabled or disabled. By default, a NetFlow monitor is enabled.

## Formatting of NetFlow Records for Long-Lived Sessions

This section discusses the formatting of the “start time” and “duration” fields in NetFlow records for long-lived sessions (typically defined as those lasting more than 10 minutes).

For each new NetFlow record created for a session on the ACOS device, the NetFlow record will show the time that the session began as the start time. Therefore, NetFlow records sent out for different sessions will have different start times.

However, for long-lived sessions (for example, 15 minutes), if the flow-timeout period is set to 5 minutes, then ACOS will produce three flow records for one 15-minute session. The three flow records will each have the same start time, because the records are reporting on the same session.

The following example illustrates the sample NetFlow records:

**Duration: 318.000000000 seconds**

**StartTime: Feb 2, 2015 12:35:52.341000000 Russia TZ 2 Standard Time**

**Duration: 674.964000000 seconds**

**StartTime: Feb 2, 2015 12:35:52.341000000 Russia TZ 2 Standard Time**

**Duration: 1031.924000000 seconds**

**StartTime: Feb 2, 2015 12:35:52.341000000 Russia TZ 2 Standard Time**

---

**NOTE:** The start time is the same for all three records for this one session. In addition, the duration is not reset to zero. Instead, it is incrementally larger for each record since more time has elapsed since the first, second, and third records were sent.

---

The benefit of this method of formatting the session “start time” and “duration” fields in the NetFlow records is that the records are joined into a single session that can be easily stored and searched in a database. The following types of NetFlow records are described in the following sections:

- dslite – DS-Lite Flow Record Template
- nat44 – NAT44 Flow Record Template
- nat64 – NAT64 Flow Record Template
- netflow-v5 – NetFlow V5 Flow Record Template
- netflow-v5-ext – Extended NetFlow V5 Flow Record Template, supports ipv6

## Predefined NetFlow Templates

ACOS device includes the following pre-defined NetFlow templates.

The following topics are covered:

<a href="#">NetFlow Templates</a> .....	59
<a href="#">Firewall Event Records Templates</a> .....	67
<a href="#">Supported NetFlow Templates (CGNAT and FW)</a> .....	68
<a href="#">Log Information for Closed Sessions (CGN/FW)</a> .....	81

## NetFlow Templates

---

The following templates can be used to monitor CGN configurations.

The following topics are covered:

<a href="#">Templates for A10 Flow Records with NAT Addresses</a> .....	60
<a href="#">Templates for NAT Session Event Records</a> .....	62
<a href="#">Templates for NAT Port Mapping Event Records</a> .....	63

[Templates for NAT Port Batching Event Records](#) ..... 64

[Templates for NAT Port Batching v2 Event Records](#) ..... 66

## Templates for A10 Flow Records with NAT Addresses

These templates are bi-directional. One session results in one flow record.

- NAT44 (**nat44**)
- NAT64 (**nat64**)
- DS-Lite (**dslite**)

The following [Table 4](#) includes details about these templates.

Table 4 : ACOS NetFlow Templates for A10 Flow Records with NAT Addresses

Template Name	Key Fields	Non-Key Fields
nat44	<ul style="list-style-type: none"> <li>• IP Protocol</li> <li>• Forward tuple partition ID</li> <li>• IPv4 Source Address</li> <li>• IPv4 Destination Address</li> <li>• Source Port</li> <li>• Destination Port</li> <li>• Flow Direction (inbound, outbound, or hairpin)</li> </ul>	<ul style="list-style-type: none"> <li>• Reverse tuple partition ID</li> <li>• IPv4 NAT source address</li> <li>• IPv4 NAT dest address</li> <li>• NAT source port</li> <li>• NAT dest port</li> <li>• Interface Input</li> <li>• Interface Output</li> <li>• Fwd Bytes</li> <li>• Fwd Packets</li> <li>• Rev Bytes</li> <li>• Rev Packets</li> <li>• Start time (msec)</li> <li>• Duration (msec)</li> </ul>
<b>nat64</b>	<ul style="list-style-type: none"> <li>• IP Protocol</li> <li>• Forward tuple type</li> <li>• Forward tuple partition ID</li> <li>• IPv6 Source Address</li> </ul>	<ul style="list-style-type: none"> <li>• Reverse tuple type</li> <li>• Reverse tuple partition ID</li> <li>• IPv6 NAT source address (hairpin)</li> </ul>

Table 4 : ACOS NetFlow Templates for A10 Flow Records with NAT Addresses

Template Name	Key Fields	Non-Key Fields
	<ul style="list-style-type: none"> <li>• IPv4 Destination Address (IPv6 in IPv4)</li> <li>• IPv6 Destination Address</li> <li>• IPv4 Destination Address</li> <li>• Source Port</li> <li>• Destination Port</li> <li>• Flow Direction (inbound, outbound, or hairpin)</li> </ul>	<ul style="list-style-type: none"> <li>• IPv4 NAT source address</li> <li>• IPv6 NAT dest address</li> <li>• IPv4 NAT dest address</li> <li>• NAT source port</li> <li>• NAT dest port</li> <li>• Interface Input</li> <li>• Interface Output</li> <li>• Fwd Bytes</li> <li>• Fwd Packets</li> <li>• Rev Bytes</li> <li>• Rev Packets</li> <li>• Start time (msec)</li> <li>• Duration (msec)</li> </ul>
<b>dslite</b>	<ul style="list-style-type: none"> <li>• IP Protocol</li> <li>• Forward tuple type</li> <li>• Forward tuple partition ID</li> <li>• IPv6 Source Address</li> <li>• IPv4 Source Address</li> <li>• IPv6 Destination Address</li> <li>• IPv4 Destination Address</li> <li>• Source Port</li> <li>• Destination Port</li> <li>• Flow Direction (inbound, outbound, or hairpin)</li> </ul>	<ul style="list-style-type: none"> <li>• Reverse tuple type</li> <li>• Reverse tuple partition ID</li> <li>• IPv6 NAT source address (hairpin)</li> <li>• IPv4 NAT source address</li> <li>• IPv6 NAT dest address</li> <li>• IPv4 NAT dest address</li> <li>• NAT source port</li> <li>• NAT dest port</li> <li>• Interface Input</li> <li>• Interface Output</li> <li>• Fwd Bytes</li> <li>• Fwd Packets</li> </ul>

Table 4 : ACOS NetFlow Templates for A10 Flow Records with NAT Addresses

Template Name	Key Fields	Non-Key Fields
		<ul style="list-style-type: none"> <li>• Rev Bytes</li> <li>• Rev Packets</li> <li>• Start time (msec)</li> <li>• Duration (msec)</li> </ul>

## Templates for NAT Session Event Records

NAT44 Session Events (**sesn-event-nat44**)

NAT64 Session Events (**sesn-event-nat64**)

DS-List Session Events (**sesn-event-dslite**)

The following [Table 5](#) includes details about these templates.

Table 5 : ACOS NetFlow Template Types for NAT Event Records

Template Name	Key Fields	Non-Key Fields
<b>sesn-event-nat44</b>	<ul style="list-style-type: none"> <li>• IP Protocol</li> <li>• Forward tuple partition ID</li> <li>• IPv4 Source Address</li> <li>• IPv4 Destination Address</li> <li>• Source Port</li> <li>• Destination Port</li> <li>• Flow Direction (inbound, outbound, or hairpin)</li> </ul>	<ul style="list-style-type: none"> <li>• Reverse tuple partition ID</li> <li>• IPv4 NAT source address</li> <li>• IPv4 NAT dest address</li> <li>• NAT source port</li> <li>• NAT dest port</li> <li>• Start time (msec)</li> <li>• sesnEvent (Create, Delete)</li> </ul>
<b>sesn-event-nat64</b>	<ul style="list-style-type: none"> <li>• IP Protocol</li> <li>• Forward tuple type</li> <li>• Forward tuple partition ID</li> <li>• IPv6 Source Address</li> <li>• IPv4 Source Address</li> <li>• IPv6 Destination Address</li> </ul>	<ul style="list-style-type: none"> <li>• Reverse tuple type</li> <li>• Reverse tuple partition ID</li> <li>• IPv6 NAT source address</li> <li>• IPv4 NAT source address</li> <li>• IPv6 NAT dest address</li> <li>• IPv4 NAT dest address</li> </ul>

Table 5 : ACOS NetFlow Template Types for NAT Event Records

Template Name	Key Fields	Non-Key Fields
	<ul style="list-style-type: none"> <li>IPv4 Destination Address</li> <li>Source Port</li> <li>Destination Port</li> <li>Flow Direction (inbound, outbound, or hairpin)</li> </ul>	<ul style="list-style-type: none"> <li>NAT source port</li> <li>NAT dest port</li> <li>Interface Input</li> <li>Interface Output</li> <li>Start time (msec)</li> <li>sesnEvent (Create, Delete)</li> </ul>
<b>sesn-event-dslite</b>	<ul style="list-style-type: none"> <li>IP Protocol</li> <li>Forward tuple type</li> <li>Forward tuple partition ID</li> <li>IPv6 Source Address</li> <li>IPv4 Source Address</li> <li>IPv6 Destination Address</li> <li>IPv4 Destination Address</li> <li>Source Port</li> <li>Destination Port</li> <li>Flow Direction (inbound, outbound, or hairpin)</li> </ul>	<ul style="list-style-type: none"> <li>Reverse tuple type</li> <li>Reverse tuple partition ID</li> <li>IPv6 NAT source address</li> <li>IPv4 NAT source address</li> <li>IPv6 NAT dest address</li> <li>IPv4 NAT dest address</li> <li>NAT source port</li> <li>NAT dest port</li> <li>Start time (msec)</li> <li>sesnEvent (Create, Delete)</li> </ul>

### Templates for NAT Port Mapping Event Records

- NAT44 Port Mapping (**port-mapping-nat44**)
- NAT64 Port Mapping (**port-mapping-nat64**)
- DS-Lite Port Mapping (**port-mapping-dslite**)

The following [Table 6](#) includes details about NetFlow templates for port mapping event records.

Table 6 : ACOS NetFlow Template Types for NAT Port Mapping Event Records

Template Name	Data Fields
<b>port-mapping-nat44</b>	<ul style="list-style-type: none"> <li>IP Protocol</li> </ul>

Table 6 : ACOS NetFlow Template Types for NAT Port Mapping Event Records

Template Name	Data Fields
	<ul style="list-style-type: none"> <li>• IPv4 Source Address</li> <li>• Source Port</li> <li>• IPv4 NAT source address</li> <li>• NAT source port</li> <li>• timestamp (msec)</li> <li>• natEvent (Create, Delete)</li> </ul>
<b>port-mapping-nat64</b>	<ul style="list-style-type: none"> <li>• IP Protocol</li> <li>• IPv6 Source Address</li> <li>• IPv4 Source Address</li> <li>• Source Port</li> <li>• IPv4 NAT source address</li> <li>• NAT source port</li> <li>• timestamp (msec)</li> <li>• natEvent (Create, Delete)</li> </ul>
<b>port-mapping-dslite</b>	<ul style="list-style-type: none"> <li>• IP Protocol</li> <li>• IPv6 Source Address</li> <li>• IPv4 Source Address</li> <li>• Source Port</li> <li>• IPv4 NAT source address</li> <li>• NAT source port</li> <li>• timestamp (msec)</li> <li>• natEvent (Create, Delete)</li> </ul>

### Templates for NAT Port Batching Event Records

- NAT44 Port Batching (**port-batch-nat44**)
- NAT64 Port Batching (**port-batch-nat64**)

- DS-Lite Port Batching (**port-batch-dslite**)

The following [Table 7](#) includes details about NetFlow templates for port batching event records.

Table 7 : ACOS NetFlow Template Types for NAT Port Batching Event Records

Template Name	Data Fields
<b>port-batch-nat44</b>	<ul style="list-style-type: none"> <li>• natEvent (Create, Delete)</li> <li>• IP Protocol</li> <li>• IPv4 Source Address</li> <li>• Post NAT IPv4 Source Address</li> <li>• Flow Start Milliseconds</li> <li>• Flow End Milliseconds</li> <li>• Port Range Start</li> <li>• Port Range End</li> <li>• Port Range Step Size</li> <li>• Port Range Num Ports</li> </ul>
<b>port-batch-nat64</b>	<ul style="list-style-type: none"> <li>• natEvent (Create, Delete)</li> <li>• IP Protocol</li> <li>• IPv6 Source Address</li> <li>• IPv4 Source Address</li> <li>• Post NAT IPv4 Source Address</li> <li>• Flow Start Milliseconds</li> <li>• Flow End Milliseconds</li> <li>• Port Range Start</li> <li>• Port Range End</li> <li>• Port Range Step Size</li> <li>• Port Range Num Ports</li> </ul>
<b>port-batch-dslite</b>	<ul style="list-style-type: none"> <li>• natEvent (Create, Delete)</li> <li>• IP Protocol</li> </ul>

Table 7 : ACOS NetFlow Template Types for NAT Port Batching Event Records

Template Name	Data Fields
	<ul style="list-style-type: none"> <li>• IPv6 Source Address</li> <li>• IPv4 Source Address</li> <li>• Post NAT IPv4 Source Address</li> <li>• Flow Start Milliseconds</li> <li>• Flow End Milliseconds</li> <li>• Port Range Start</li> <li>• Port Range End</li> <li>• Port Range Step Size</li> <li>• Port Range Num Ports</li> </ul>

## Templates for NAT Port Batching v2 Event Records

- NAT44 Port Batching (**port-batch-v2-nat44**)
- NAT64 Port Batching (**port-batch-v2-nat64**)
- DS-Lite Port Batching (**port-batch-v2-dslite**)

The following [Table 8](#) includes details about NetFlow templates for port batching event records.

Table 8 : ACOS NetFlow Template Types for NAT Port Batching Event Records

Template Name	Data Fields
<b>port-batch-v2-nat44</b>	<ul style="list-style-type: none"> <li>• natEvent (Create, Delete)</li> <li>• IP Protocol</li> <li>• IPv4 Source Address</li> <li>• Post NAT IPv4 Source Address</li> <li>• Flow Start Milliseconds</li> <li>• Flow End Milliseconds</li> <li>• Port Range Start</li> <li>• Port Range End</li> </ul>

Table 8 : ACOS NetFlow Template Types for NAT Port Batching Event Records

Template Name	Data Fields
<b>port-batch-v2-nat64</b>	<ul style="list-style-type: none"> <li>• natEvent (Create, Delete)</li> <li>• IP Protocol</li> <li>• IPv6 Source Address</li> <li>• IPv4 Source Address</li> <li>• Post NAT IPv4 Source Address</li> <li>• Flow Start Milliseconds</li> <li>• Flow End Milliseconds</li> <li>• Port Range Start</li> <li>• Port Range End</li> </ul>
<b>port-batch-v2-dslite</b>	<ul style="list-style-type: none"> <li>• natEvent (Create, Delete)</li> <li>• IP Protocol</li> <li>• IPv6 Source Address</li> <li>• IPv4 Source Address</li> <li>• Post NAT IPv4 Source Address</li> <li>• Flow Start Milliseconds</li> <li>• Flow End Milliseconds</li> <li>• Port Range Start</li> <li>• Port Range End</li> </ul>

## Firewall Event Records Templates

---

- IPv4 Firewall Session (**sesn-event-fw4**)
- IPv6 Firewall Session (**sesn-event-fw6**)

The following [Table 9](#) includes details about NetFlow templates for IPv4 and IPv6 firewall sessions.

Table 9 : ACOS NetFlow Template Types for IPv4 and IPv6 Firewall Sessions Event Records

Template Name	Data Fields
<b>sesn-event-fw4</b>	<ul style="list-style-type: none"> <li>• sesnEvent (Create, Delete, Both)</li> <li>• IP Protocol</li> <li>• IPv4 Source Address</li> <li>• IPv4 Destination Address</li> <li>• Source Port</li> <li>• Destination Port</li> <li>• Timestamp (msec)</li> </ul>
<b>sesn-event-fw6</b>	<ul style="list-style-type: none"> <li>• sesnEvent (Create, Delete, Both)</li> <li>• IP Protocol</li> <li>• IPv6 Source Address</li> <li>• IPv6 Destination Address</li> <li>• Source Port</li> <li>• Destination Port</li> <li>• Timestamp (msec)</li> </ul>

## Supported NetFlow Templates (CGNAT and FW)

The IPFIX protocol uses Information Elements (IEs) to record logging messages. These messages are sent to one or more NetFlow collectors, where the information is stored and analyzed. Each IE corresponds to a field and has its own length. The field lengths can be non-standard field lengths or RFC-defined field lengths.

You can configure the `system rfc-ipfix-ie-spec <enable | disable>` command to switch between the non-standard field length and RFC-defined field lengths. If it is enabled, the field length of the IE identifier uses the RFC-defined lengths. If it is disabled, the field length of the IE identifier uses non-standard lengths. These field lengths are recognized by the collectors to collect and analyze the IPFIX packets that are sent by ACOS devices.

In the Fixed templates, the predefined fields use non-standard field lengths and template IDs. There are two options for the fixed templates:

- Use the old template IDs
- Use the new template IDs to use the RFC-defined field length

The template IDs are changed for the following:

Original Fixed Template ID	New Fixed Template ID	Fixed Template Name
1001	1201	nat44-old
1101	1301	nat44
1102	1302	nat64
1103	1303	dslite
1010	1210	netflow-v5
1011	1211	netflow-v5-ext

The following templates can be used to monitor configurations for ADC, CGN, and FW.

The following [Table 10](#) includes details about the A10-supported NetFlow templates.

Table 10 : \_A10 Supported NetFlow Templates

Template Name (ID)	Fields ID	Field Name	Key Fields?
<b>nat44 (1101) - Old</b>	• 4	• ipprotocolIdentifier (ipProto)	• Yes
	• 33028	• fwdVNPID	• Yes
<b>nat44 (1301) - New</b>	• 8	• sourceIPv4Address	• Yes
	• 12	• destinationIPv4Address	• Yes
	• 7	• sourceTransportPort	• Yes
	• 11	• destinationTransportPort	• Yes
	• 61	• flowDirection	• Yes
	• 33029	• revVNPID	
	• 225	• postNATSourceIPv4Address	
	• 226	• postNATDestinationIPv4Address	

Table 10 : \_A10 Supported NetFlow Templates

Template Name (ID)	Fields ID	Field Name	Key Fields?
	<ul style="list-style-type: none"> <li>• 227</li> <li>• 228</li> <li>• 10</li> <li>• 14</li> <li>• 1</li> <li>• 2</li> <li>• 32769</li> <li>• 32770</li> <li>• 6</li> <li>• 152</li> <li>• 153</li> <li>• 161</li> </ul>	<ul style="list-style-type: none"> <li>• postNAPTsourceTransportPort</li> <li>• postNAPTdestinationTransportPort</li> <li>• ingressInterface</li> <li>• egressInterface</li> <li>• octetDeltaCount (fwdBytes)</li> <li>• packetDeltaCount(fwdPackets)</li> <li>• octetDeltaCount (RevBytes)</li> <li>• RevPackets</li> <li>• tcpControlBits</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• flowDurationMilliseconds</li> </ul>	
<b>nat64 (1102)-Old</b>  <b>nat64 (1302) - New</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 33028</li> <li>• 27</li> <li>• 8</li> <li>• 28</li> <li>• 12</li> <li>• 7</li> <li>• 11</li> <li>• 61</li> <li>• 33025</li> <li>• 33029</li> </ul>	<ul style="list-style-type: none"> <li>• ipprotocolIdentifier (ipProto)</li> <li>• fwdVNPID</li> <li>• sourceIPv6Address</li> <li>• sourceIPv4Address</li> <li>• destinationIPv6Address</li> <li>• destinationIPv4Address</li> <li>• sourceTransportPort</li> <li>• destinationTransportPort</li> <li>• flowDirection</li> <li>• revTupleType</li> <li>• revVNPID</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>

Table 10 : \_A10 Supported NetFlow Templates

Template Name (ID)	Fields ID	Field Name	Key Fields?
	<ul style="list-style-type: none"> <li>• 281</li> <li>• 225</li> <li>• 282</li> <li>• 226</li> <li>• 227</li> <li>• 228</li> <li>• 10</li> <li>• 14</li> <li>• 1</li> <li>• 2</li> <li>• 32769</li> <li>• 32770</li> <li>• 6</li> <li>• 152</li> <li>• 153</li> <li>• 161</li> </ul>	<ul style="list-style-type: none"> <li>• postNATSourceIPv6Address</li> <li>• postNATSourceIPv4Address</li> <li>• postNATDestinationIPv6Address</li> <li>• postNATDestinationIPv4Address</li> <li>• postNAPTsourceTransportPort</li> <li>• postNAPTdestinationTransportPort</li> <li>• ingressInterface</li> <li>• egressInterface</li> <li>• octetDeltaCount (fwdBytes)</li> <li>• packetDeltaCount(fwdPackets)</li> <li>• octetDeltaCount (RevBytes)</li> <li>• RevPackets</li> <li>• tcpControlBits</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• flowDurationMilliseconds</li> </ul>	
<b>dslite (1103)-Old</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 33024</li> <li>• 33028</li> </ul>	<ul style="list-style-type: none"> <li>• ipProtocolIdentifier (ipProto)</li> <li>• fwdTupleType</li> <li>• fwdVNPID</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>
<b>dslite (1303) - New</b>	<ul style="list-style-type: none"> <li>• 27</li> <li>• 8</li> <li>• 28</li> <li>• 12</li> </ul>	<ul style="list-style-type: none"> <li>• sourceIPv6Address</li> <li>• sourceIPv4Address</li> <li>• destinationIPv6Address</li> <li>• destinationIPv4Address</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>

Table 10 : \_A10 Supported NetFlow Templates

Template Name (ID)	Fields ID	Field Name	Key Fields?
	<ul style="list-style-type: none"> <li>• 7</li> <li>• 11</li> <li>• 61</li> <li>• 33025</li> <li>• 33029</li> <li>• 281</li> <li>• 225</li> <li>• 282</li> <li>• 226</li> <li>• 227</li> <li>• 228</li> <li>• 10</li> <li>• 14</li> <li>• 1</li> <li>• 2</li> <li>• 32769</li> <li>• 32770</li> <li>• 6</li> <li>• 152</li> <li>• 153</li> <li>• 161</li> </ul>	<ul style="list-style-type: none"> <li>• sourceTransportPort</li> <li>• destinationTransportPort</li> <li>• flowDirection</li> <li>• revTupleType</li> <li>• revVNPID</li> <li>• postNATSourceIPv6Address</li> <li>• postNATSourceIPv4Address</li> <li>• postNATDestinationIPv6Address</li> <li>• postNATDestinationIPv4Address</li> <li>• postNAPTsourceTransportPort</li> <li>• postNAPTdestinationTransportPort</li> <li>• ingressInterface</li> <li>• egressInterface</li> <li>• octetDeltaCount (fwdBytes)</li> <li>• packetDeltaCount(fwdPackets)</li> <li>• octetDeltaCount (RevBytes)</li> <li>• RevPackets</li> <li>• tcpControlBits</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• flowDurationMilliseconds</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>
<b>sess-event-fw4</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 8</li> </ul>	<ul style="list-style-type: none"> <li>• protocolIdentifier (ipProto)</li> <li>• sourceIPv4Address</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> </ul>

Table 10 : \_A10 Supported NetFlow Templates

Template Name (ID)	Fields ID	Field Name	Key Fields?
<b>(1014)</b>	<ul style="list-style-type: none"> <li>• 12</li> <li>• 7</li> <li>• 11</li> <li>• 152</li> <li>• 153</li> <li>• 233</li> </ul>	<ul style="list-style-type: none"> <li>• destinationIPv4Address</li> <li>• sourceTransportPort</li> <li>• destinationTransportPort</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• firewallEvent</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>
<b>sess-event-fw6 (1015)</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 27</li> <li>• 28</li> <li>• 7</li> <li>• 11</li> <li>• 152</li> <li>• 153</li> <li>• 233</li> </ul>	<ul style="list-style-type: none"> <li>• protocolIdentifier (ipProto)</li> <li>• sourceIPv6Address</li> <li>• destinationIPv6Address</li> <li>• sourceTransportPort</li> <li>• destinationTransportPort</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• firewallEvent</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>
<b>sesn-event-nat44 (1104)</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 33028</li> <li>• 8</li> <li>• 12</li> <li>• 7</li> <li>• 11</li> <li>• 61</li> <li>• 33029</li> <li>• 225</li> <li>• 226</li> </ul>	<ul style="list-style-type: none"> <li>• protocolIdentifier (ipProto)</li> <li>• fwdVNPID</li> <li>• sourceIPv4Address</li> <li>• destinationIPv4Address</li> <li>• sourceTransportPort</li> <li>• destinationTransportPort</li> <li>• flowDirection</li> <li>• revVNPID</li> <li>• postNATSourceIPv4Address</li> <li>• postNATDestinationIPv4Address</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>

Table 10 : \_A10 Supported NetFlow Templates

Template Name (ID)	Fields ID	Field Name	Key Fields?
	<ul style="list-style-type: none"> <li>• 227</li> <li>• 228</li> <li>• 152</li> <li>• 153</li> <li>• 230</li> </ul>	<ul style="list-style-type: none"> <li>• postNAPTsourceTransportPort</li> <li>• postNAPTdestinationTransportPort</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• natEvent</li> </ul>	
<b>sesn-event-nat64 (1105)</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 33024</li> <li>• 33028</li> <li>• 27</li> <li>• 8</li> <li>• 28</li> <li>• 12</li> <li>• 7</li> <li>• 11</li> <li>• 61</li> <li>• 33025</li> <li>• 33029</li> <li>• 281</li> <li>• 225</li> <li>• 282</li> <li>• 226</li> <li>• 227</li> <li>• 228</li> </ul>	<ul style="list-style-type: none"> <li>• protocolIdentifier (ipProto)</li> <li>• fwdTupleType</li> <li>• fwdVNPID</li> <li>• sourceIPv6Address</li> <li>• sourceIPv4Address</li> <li>• destinationIPv6Address</li> <li>• destinationIPv4Address</li> <li>• sourceTransportPort</li> <li>• destinationTransportPort</li> <li>• flowDirection</li> <li>• revTupleType</li> <li>• revVNPID</li> <li>• postNATSourceIPv6Address</li> <li>• postNATSourceIPv4Address</li> <li>• postNATDestinationIPv6Address</li> <li>• postNATDestinationIPv4Address</li> <li>• postNAPTsourceTransportPort</li> <li>• postNAPTdestinationTransportPort</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• yes</li> <li>• Yes</li> <li>• yes</li> <li>• Yes</li> <li>• yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>

Table 10 : \_A10 Supported NetFlow Templates

Template Name (ID)	Fields ID	Field Name	Key Fields?
	<ul style="list-style-type: none"> <li>• 152</li> <li>• 153</li> <li>• 230</li> </ul>	<ul style="list-style-type: none"> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• natEvent</li> </ul>	
<b>sesn-event-dslite (1106)</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 33024</li> <li>• 33028</li> <li>• 27</li> <li>• 8</li> <li>• 28</li> <li>• 12</li> <li>• 7</li> <li>• 11</li> <li>• 61</li> <li>• 33025</li> <li>• 33029</li> <li>• 281</li> <li>• 225</li> <li>• 282</li> <li>• 226</li> <li>• 227</li> <li>• 228</li> <li>• 152</li> <li>• 153</li> <li>• 230</li> </ul>	<ul style="list-style-type: none"> <li>• protocolIdentifier (ipProto)</li> <li>• fwdTupleType</li> <li>• fwdVNPID</li> <li>• sourceIPv6Address</li> <li>• sourceIPv4Address</li> <li>• destinationIPv6Address</li> <li>• destinationIPv4Address</li> <li>• sourceTransportPort</li> <li>• destinationTransportPort</li> <li>• flowDirection</li> <li>• revTupleType</li> <li>• revVNPID</li> <li>• postNATSourceIPv6Address</li> <li>• postNATSourceIPv4Address</li> <li>• postNATDestinationIPv6Address</li> <li>• postNATDestinationIPv4Address</li> <li>• postNAPTsourceTransportPort</li> <li>• postNAPTdestinationTransportPort</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>

Table 10 : \_A10 Supported NetFlow Templates

Template Name (ID)	Fields ID	Field Name	Key Fields?
		<ul style="list-style-type: none"> <li>• natEvent</li> </ul>	
<b>port-map-nat44 (1007)</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 8</li> <li>• 7</li> <li>• 225</li> <li>• 227</li> <li>• 152</li> <li>• 153</li> <li>• 230</li> </ul>	<ul style="list-style-type: none"> <li>• protocolIdentifier (ipProto)</li> <li>• sourceIPv4Address</li> <li>• sourceTransportPort</li> <li>• postNATSourceIPv4Address</li> <li>• postNAPTsourceTransportPort</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• natEvent</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>
<b>port-map-nat64 (1008)</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 27</li> <li>• 8</li> <li>• 7</li> <li>• 225</li> <li>• 227</li> <li>• 152</li> <li>• 153</li> <li>• 230</li> </ul>	<ul style="list-style-type: none"> <li>• protocolIdentifier (ipProto)</li> <li>• sourceIPv6Address</li> <li>• sourceIPv4Address</li> <li>• sourceTransportPort</li> <li>• postNATSourceIPv4Address</li> <li>• postNAPTsourceTransportPort</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• natEvent</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>
<b>port-map-dslite (1009)</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 27</li> <li>• 8</li> <li>• 7</li> <li>• 225</li> <li>• 227</li> </ul>	<ul style="list-style-type: none"> <li>• protocolIdentifier (ipProto)</li> <li>• sourceIPv6Address</li> <li>• sourceIPv4Address</li> <li>• sourceTransportPort</li> <li>• postNATSourceIPv4Address</li> <li>• postNAPTsourceTransportPort</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>

Table 10 : \_A10 Supported NetFlow Templates

Template Name (ID)	Fields ID	Field Name	Key Fields?
	<ul style="list-style-type: none"> <li>• 152</li> <li>• 153</li> <li>• 230</li> </ul>	<ul style="list-style-type: none"> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• natEvent</li> </ul>	
<b>netflow-v5(1010)-Old</b>  <b>netflow-v5 (1210) - New</b>	<ul style="list-style-type: none"> <li>• 8</li> <li>• 12</li> <li>• 15</li> <li>• 10</li> <li>• 14</li> <li>• 2</li> <li>• 1</li> <li>• 22</li> <li>• 21</li> <li>• 7</li> <li>• 11</li> <li>• 6</li> <li>• 4</li> <li>• 5</li> <li>• 16</li> <li>• 17</li> <li>• 9</li> <li>• 13</li> </ul>	<ul style="list-style-type: none"> <li>• sourceIPv4Address</li> <li>• destinationIPv4Address</li> <li>• ipNextHopIPv4Address</li> <li>• ingressInterface</li> <li>• egressInterface</li> <li>• packetDeltaCount(fwdPackets)</li> <li>• octetDeltaCount (fwdBytes)</li> <li>• flowStartSysUpTime</li> <li>• flowEndSysUpTime</li> <li>• sourceTransportPort</li> <li>• destinationTransportPort</li> <li>• tcpControlBits</li> <li>• protocolIdentifier (ipProto)</li> <li>• IpClassOfService</li> <li>• bgpSourceAsNumber</li> <li>• bgpDestinationAsNumber</li> <li>• sourceIPv4PrefixLength</li> <li>• destinationIPv4PrefixLength</li> </ul>	
<b>netflow-v5-ext (1011)-Old</b>	<ul style="list-style-type: none"> <li>• 27</li> <li>• 28</li> <li>• 62</li> </ul>	<ul style="list-style-type: none"> <li>• sourceIPv6Address</li> <li>• destinationIPv6Address</li> <li>• ipNextHopIPv6Address</li> </ul>	

Table 10 : \_A10 Supported NetFlow Templates

Template Name (ID)	Fields ID	Field Name	Key Fields?
<b>netflow-v5-ext (1211) - New</b>	<ul style="list-style-type: none"> <li>• 10</li> <li>• 14</li> <li>• 2</li> <li>• 1</li> <li>• 22</li> <li>• 21</li> <li>• 7</li> <li>• 11</li> <li>• 6</li> <li>• 4</li> <li>• 5</li> <li>• 16</li> <li>• 17</li> <li>• 29</li> <li>• 30</li> </ul>	<ul style="list-style-type: none"> <li>• ingressInterface</li> <li>• egressInterface</li> <li>• packetDeltaCount(fwdPackets)</li> <li>• octetDeltaCount (fwdBytes)</li> <li>• flowStartSysUpTime</li> <li>• flowEndSysUpTime</li> <li>• sourceTransportPort</li> <li>• destinationTransportPort</li> <li>• tcpControlBits</li> <li>• protocolIdentifier (ipProto)</li> <li>• IpClassOfService</li> <li>• bgpSourceAsNumber</li> <li>• bgpDestinationAsNumber</li> <li>• sourceIPv6PrefixLength</li> <li>• destinationIPv6PrefixLength</li> </ul>	
<b>port-batch-nat44 (1020)</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 8</li> <li>• 225</li> <li>• 152</li> <li>• 153</li> <li>• 230</li> <li>• 361</li> <li>• 362</li> <li>• 363</li> </ul>	<ul style="list-style-type: none"> <li>• protocolIdentifier (ipProto)</li> <li>• sourceIPv4Address</li> <li>• postNATSourceIPv4Address</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• natEvent</li> <li>• portRangeStart</li> <li>• portRangeEnd</li> <li>• portRangeStepSize</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> </ul>

Table 10 : \_A10 Supported NetFlow Templates

Template Name (ID)	Fields ID	Field Name	Key Fields?
	<ul style="list-style-type: none"> <li>• 364</li> </ul>	<ul style="list-style-type: none"> <li>• portRangeNumPorts</li> </ul>	
<b>port- batch- nat64 (1021)</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 27</li> <li>• 8</li> <li>• 225</li> <li>• 152</li> <li>• 153</li> <li>• 230</li> <li>• 361</li> <li>• 362</li> <li>• 363</li> <li>• 364</li> </ul>	<ul style="list-style-type: none"> <li>• protocolIdentifier (ipProto)</li> <li>• sourceIPv6Address</li> <li>• sourceIPv4Address</li> <li>• postNATSourceIPv4Address</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• natEvent</li> <li>• portRangeStart</li> <li>• portRangeEnd</li> <li>• portRangeStepSize</li> <li>• portRangeNumPorts</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>
<b>port- batch- dslite (1022)</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 27</li> <li>• 8</li> <li>• 225</li> <li>• 152</li> <li>• 153</li> <li>• 230</li> <li>• 361</li> <li>• 362</li> <li>• 363</li> <li>• 364</li> </ul>	<ul style="list-style-type: none"> <li>• protocolIdentifier (ipProto)</li> <li>• sourceIPv6Address</li> <li>• sourceIPv4Address</li> <li>• postNATSourceIPv4Address</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• natEvent</li> <li>• portRangeStart</li> <li>• portRangeEnd</li> <li>• portRangeStepSize</li> <li>• portRangeNumPorts</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>
<b>port-</b>	<ul style="list-style-type: none"> <li>• 4</li> </ul>	<ul style="list-style-type: none"> <li>• protocolIdentifier (ipProto)</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> </ul>

Table 10 : \_A10 Supported NetFlow Templates

Template Name (ID)	Fields ID	Field Name	Key Fields?
<b>batch-v2-nat44 (1023)</b>	<ul style="list-style-type: none"> <li>• 8</li> <li>• 225</li> <li>• 152</li> <li>• 153</li> <li>• 230</li> <li>• 361</li> <li>• 362</li> </ul>	<ul style="list-style-type: none"> <li>• sourceIPv4Address</li> <li>• postNATSourceIPv4Address</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• natEvent</li> <li>• portRangeStart</li> <li>• portRangeEnd</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> </ul>
<b>port-batch-v2-nat64 (1024)</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 27</li> <li>• 8</li> <li>• 225</li> <li>• 152</li> <li>• 153</li> <li>• 230</li> <li>• 361</li> <li>• 362</li> </ul>	<ul style="list-style-type: none"> <li>• protocolIdentifier (ipProto)</li> <li>• sourceIPv6Address</li> <li>• sourceIPv4Address</li> <li>• postNATSourceIPv4Address</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• natEvent</li> <li>• portRangeStart</li> <li>• portRangeEnd</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>
<b>port-batch-v2-dslite (1025)</b>	<ul style="list-style-type: none"> <li>• 4</li> <li>• 27</li> <li>• 8</li> <li>• 225</li> <li>• 152</li> <li>• 153</li> <li>• 230</li> <li>• 361</li> </ul>	<ul style="list-style-type: none"> <li>• protocolIdentifier (ipProto)</li> <li>• sourceIPv6Address</li> <li>• sourceIPv4Address</li> <li>• postNATSourceIPv4Address</li> <li>• flowStartMilliseconds</li> <li>• flowEndMilliseconds</li> <li>• natEvent</li> <li>• portRangeStart</li> </ul>	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Yes</li> <li>• Yes</li> </ul>

Table 10 : \_A10 Supported NetFlow Templates

Template Name (ID)	Fields ID	Field Name	Key Fields?
	• 362	• portRangeEnd	

## Log Information for Closed Sessions (CGN/FW)

The following topics are covered:

<a href="#">Configuring Custom Templates</a> .....	81
<a href="#">Examples Reference</a> .....	81
<a href="#">Terminating a Session</a> .....	82

### Configuring Custom Templates

You can configure custom templates to provide increased visibility into the cause for session closure for CGN and FW. The following command option configures `flow-end-reason` for session logs:

```
ACOS (config)#netflow template nat44
ACOS (config-template:nat44)#information-element flow-end-reason
```

### Examples Reference

To see examples of this configuration in a template, see the following custom templates under [Sample Custom Templates](#):

- [sesn-event-nat44-creation and sesn-event-nat44-deletion](#)
- [sesn-event-nat64-creation, sesn-event-nat64-deletion, sesn-event-dslite-creation, sesn-event-dslite-deletion](#)
- [port-mapping-nat64-creation, port-mapping-nat64-deletion, port-mapping-dslite-creation, port-mapping-dslite-deletion](#)
- [port-batch-nat44-creation, port-batch-nat44-deletion](#)
- [port-batch-nat64-creation, port-batch-nat64-deletion, port-batch-dslite-creation, port-batch-dslite-deletion](#)

- [port-batch-v2-nat44-creation, port-batch-v2-nat44-deletion](#)
- [port-batch-v2-nat64-creation, port-batch-v2-nat64-deletion, port-batch-v2-dslite-creation, port-batch-v2-dslite-deletion](#)

## Terminating a Session

A session can terminate for a number of reasons as shown in the following table:

End Reason Code	Description
0x01	Indicates that the uplink subscriber session is closed on receiving a FIN.
0x02	Indicates that the DNS Session is closed on receiving a DNS Response.
0x03	Indicates that the session is closed on receiving a RADIUS Stop message for a subscriber.
0x04	Indicates that the downlink subscriber session is closed on receiving a FIN.
0x05	Indicates that the uplink subscriber session is closed on receiving an RST.
0x06	Indicates that the downlink subscriber session is closed on receiving an RST.
0x07	Indicates that the session is closed due to ACOS sending a TCP RST.
0x11	Indicates that the session is closed due to idle timeout.
0x12	Indicates that the session is closed by ACOS while recovering session memory.
0x13	Indicates an active timeout for long-lived sessions.
0x21	Indicates that the session termination is triggered by an explicit action, such as clear sessions, by the system administrator.
0x22	Indicates that the session is closed to accommodate a configuration change such as the removal of Fixed NAT LID or the LSN NAT IP being obsolete.
0x31	Indicates that the session closed is triggered by the configured DDoS

End Reason Code	Description
	features.
0x32	Indicates that the session is not closed normally.
0x41	Indicates that the GTP session is closed when Delete Session Request, Delete Bearer Request, or Delete PDP Context Request is received for the deletion of GTP-C or GTP-U sessions.
0x42	Indicates that the handover request caused the termination of the existing GTP session.
0x43	Indicates that the GTP session is closed as a result of detecting a network element failure.
0x44	Indicates that the GTP-U session is deleted due to the deletion of GTP-C session.
0x45	Indicates that the GTP-C connection is deleted on receiving a retransmitted Create Session Request.

## Custom IPFIX Templates

Beginning with ACOS 4.1.4-P3, you can create custom event templates for IPFIX logging for GiFW. This is an additional configuration option, that is in addition to the pre-defined NetFlow templates.

The following topics are covered:

<a href="#">Overview</a> .....	84
<a href="#">Configuration Details</a> .....	84
<a href="#">Supported Event Types</a> .....	86
<a href="#">Sample Custom Templates</a> .....	87
<a href="#">Supported IPFIX Information Elements</a> .....	100

## Overview

---

ACOS supports creation of custom IPFIX templates, so users can select specific Information Elements (IEs) to record.

The IPFIX protocol is used to export CGN and firewall logging information using custom templates. IPFIX (or IP Flow Information Export) is similar to NetFlow and was derived from NetFlow v9. The protocol is used to perform traffic analysis on traffic flows based on logs exported from the ACOS device and sent to a collector.

In prior releases, ACOS support for NetFlow/IPFIX consisted of a list of predefined templates for NAT44, NAT64, DSLite, firewall, and so on. These predefined (or “fixed”) templates did not support the ability to transmit information about RADIUS attributes, such as IMSI, MSISDN, and ruleset information, like rule name, rule-set name, zone information, interface information, application, and so on.

Now, users can create custom templates, allowing them to be more agile with sending flow data in a format that meets the needs and requirements of their NetFlow collector and analyzer. Users can select the specific IEs for their custom template. The release adds several new IEs, which are available in the custom templates only and not in the fixed templates.

In addition, in previous releases, Firewall Netflow records were only sent for “permit” action. This release extends support such that NetFlow logs will also be sent for the following actions: “fw deny”, and “fw reset” events.

This release supports the ability to create custom IPFIX templates, so you can configure the exact “Field Types” to be logged. The supported field types are documented in NetFlow v10/IPFIX (RFC-5101: <https://tools.ietf.org/html/rfc5101>).

For more information, see the “netflow monitor” and “netflow template” commands in the *Command Line Reference Guide*.

## Configuration Details

---

Keep in mind the following configuration details when configuring a custom template:

- The custom template can be bound under “netflow monitor” with the supported event types. For a list, see [Supported Event Types](#).
- Firewall logs will only be sent if the “log” keyword is configured under the rule in the active ruleset.
- The config under the template cannot be modified until the template is bound. If any change is needed in the template, you must configure a new template and bind it, or you can 1) unbind the template from the Netflow monitor, and 2) then modify the template and the template id, and 3) bind it again.
- Once a template is modified and bound to a NetFlow monitor again, the new definition will be sent out to the NetFlow collector.
- The template IDs need to be unique across different templates. An error message is seen if two templates with the same template IDs are bound to any NetFlow monitor.
- Also, template IDs should not be reused for 3 times the retransmission delay. An error message is seen when a template with such template ID is bound to a NetFlow monitor. [RFC: Template IDs MAY be reused by Exporting Processes by exporting a new Template for the Template ID after waiting at least 3 times the retransmission delay.]
- The criteria upon which Netflow records are differentiated:
  1. Source IP/port
  2. Observation domain (CPU id)
  3. Template ID
- ACOS does not currently have a way to identify which partition is used to send out the NetFlow records, and will not be able to do so unless different IPs are used to send out logs in different partitions. This is not a concern with fixed template, since the template IDs are fixed, so there is no confusion at the collector. However, for custom templates, users must configure a unique source IP for each monitor if they want to be able to differentiate between monitors in different partitions.
- Some of the new IEs have variable-length fields. For variable-length fields, the NetFlow records will include both the length and the value, whereas the template definition will have the length as 65535, as mentioned in the RFC.
- If configuring an IE that is not relevant to the event type it is bound to, then the field will be filled with an invalid value or 0. (IE 33028 and 33029 that correspond to

forward and reverse Partition ids will be set to FFFF if they are not relevant to the event type. The other IEs will be set to 0 if they are not relevant to the event type.)

- For all deletion event records, intermediate logs are sent every 10 minutes for long-lived sessions. "flow-timeout" can be set to 0 under the "netflow monitor" command to disable this.

## Supported Event Types

---

- nat44-session-creation
- nat44-session-deletion
- nat64-session-creation
- nat64-session-deletion
- dslite-session-creation
- dslite-session-deletion
- fw4-session-creation
- fw4-session-deletion
- fw6-session-creation
- fw6-session-deletion
- fw4-deny-reset
- fw4-deny-reset
- fw6-deny-reset
- fw6-deny-reset
- port-mapping-nat44-creation
- port-mapping-nat44-deletion
- port-mapping-nat64-creation
- port-mapping-nat64-deletion
- port-mapping-dslite-creation
- port-mapping-dslite-deletion
- port-batch-nat44-creation

- port-batch-nat44-deletion
- port-batch-nat64-creation
- port-batch-nat64-deletion
- port-batch-dslite-creation
- port-batch-dslite-deletion
- port-batch-v2-nat44-creation
- port-batch-v2-nat44-deletion
- port-batch-v2-nat64-creation
- port-batch-v2-nat64-deletion
- port-batch-v2-dslite-creation
- port-batch-v2-dslite-deletion

## Sample Custom Templates

---

As a guideline for configuring custom templates, examples of template definitions are provided below for several different event types.

The following topics are covered:

<a href="#">sesn-event-nat44-creation and sesn-event-nat44-deletion</a> .....	88
<a href="#">sesn-event-nat64-creation, sesn-event-nat64-deletion, sesn-event-dslite-creation, sesn-event-dslite-deletion</a> .....	89
<a href="#">sesn-event-fw4-creation, sesn-event-fw4-deletion</a> .....	90
<a href="#">sesn-event-fw6-creation, sesn-event-fw6-deletion</a> .....	91
<a href="#">port-mapping-nat44-creation, port-mapping-nat44-deletion</a> .....	92
<a href="#">port-mapping-nat64-creation, port-mapping-nat64-deletion, port-mapping-dslite-creation, port-mapping-dslite-deletion</a> .....	93
<a href="#">port-batch-nat44-creation, port-batch-nat44-deletion</a> .....	94
<a href="#">port-batch-nat64-creation, port-batch-nat64-deletion, port-batch-dslite-creation, port-batch-dslite-deletion</a> .....	94
<a href="#">port-batch-v2-nat44-creation, port-batch-v2-nat44-deletion</a> .....	95
<a href="#">port-batch-v2-nat64-creation, port-batch-v2-nat64-deletion, port-batch-v2-dslite-creation, port-batch-v2-dslite-deletion</a> .....	96
<a href="#">cgnddos-l3-entry-creation and cgnddos-l3-entry-deletion</a> .....	96

<a href="#">cgnddos-l4-entry-creation and cgnddos-l4-entry-deletion</a>	97
<a href="#">fw-ddos-entry-creation and fw-ddos-entry-deletion</a>	97
<a href="#">fw-session-limit-exceeded</a>	97
<a href="#">deny-reset-event-fw4</a>	98
<a href="#">deny-reset-event-fw6</a>	99

## sesn-event-nat44-creation and sesn-event-nat44-deletion

Use the following config:

```
netflow template nat44
  information-element ip-protocol
  information-element fwd-tuple-vnp-id
  information-element rev-tuple-vnp-id
  information-element dest-ipv4-address
  information-element source-ipv4-address
  information-element source-port
  information-element dest-port
  information-element cgn-flow-direction
  information-element post-nat-source-ipv4-address
  information-element post-nat-dest-ipv4-address
  information-element post-nat-source-port
  information-element post-nat-dest-port
  information-element fwd-bytes
  information-element fwd-packets
  information-element rev-bytes
  information-element rev-packets
  information-element in-port
  information-element out-port
  information-element in-interface
  information-element out-interface
  information-element application-id
  information-element rule-name
  information-element rule-set-name
  information-element fw-source-zone
  information-element fw-dest-zone
  information-element radius-imsi
  information-element radius-msisdn
  information-element radius-imei
  information-element radius-custom1
```

```
information-element radius-custom2
information-element radius-custom3
information-element radius-custom4
information-element radius-custom5
information-element radius-custom6
information-element flow-start-msec
information-element flow-end-msec
information-element nat-event
information-element flow-duration-msec-64
information-element tcp-control-bits
information-element flow-end-reason
information-element rfc-flow-end-reason
template-id 2001
```

!

[sesn-event-nat64-creation](#), [sesn-event-nat64-deletion](#), [sesn-event-dslite-creation](#), [sesn-event-dslite-deletion](#)

Use the following config:

```
netflow template nat64
  information-element ip-PROTO
  information-element fwd-tuple-vnp-id
  information-element rev-tuple-vnp-id
  information-element dest-ipv4-address
  information-element source-ipv4-address
  information-element source-port
  information-element dest-port
  information-element cgn-flow-direction
  information-element post-nat-source-ipv4-address
  information-element post-nat-dest-ipv4-address
  information-element post-nat-source-port
  information-element post-nat-dest-port
  information-element fwd-bytes
  information-element fwd-packets
  information-element rev-bytes
  information-element rev-packets
  information-element in-port
  information-element out-port
  information-element in-interface
  information-element out-interface
```

```
information-element application-id
information-element rule-name
information-element rule-set-name
information-element fw-source-zone
information-element fw-dest-zone
information-element radius-imsi
information-element radius-msisdn
information-element radius-imei
information-element radius-custom1
information-element radius-custom2
information-element radius-custom3
information-element radius-custom4
information-element radius-custom5
information-element radius-custom6
information-element flow-start-msec
information-element flow-end-msec
information-element nat-event
information-element flow-duration-msec-64
information-element tcp-control-bits
information-element fwd-tuple-type
information-element rev-tuple-type
information-element post-nat-source-ipv6-address
information-element post-nat-dest-ipv6-address
information-element source-ipv6-address
information-element dest-ipv6-address
information-element flow-end-reason
information-element rfc-flow-end-reason
template-id 2002
```

!

## sesn-event-fw4-creation, sesn-event-fw4-deletion

Use the following config:

```
netflow template fw4
information-element ip-PROTO
information-element fwd-tuple-vnp-id
information-element dest-ipv4-address
information-element source-ipv4-address
information-element source-port
information-element dest-port
```

```
information-element in-port
information-element out-port
information-element in-interface
information-element out-interface
information-element application-id
information-element rule-name
information-element rule-set-name
information-element fw-source-zone
information-element fw-dest-zone
information-element radius-imsi
information-element radius-msisdn
information-element radius-imei
information-element radius-custom1
information-element radius-custom2
information-element radius-custom3
information-element radius-custom4
information-element radius-custom5
information-element radius-custom6
information-element flow-start-msec
information-element flow-end-msec
information-element flow-duration-msec-64
information-element fwd-bytes
information-element fwd-packets
information-element rev-bytes
information-element rev-packets
information-element fw-event
template-id 2003
!
```

## sesn-event-fw6-creation, sesn-event-fw6-deletion

Use the following config:

```
netflow template fw6
  information-element ip-PROTO
  information-element fwd-tuple-vnp-id
  information-element source-port
  information-element dest-port
  information-element in-port
  information-element out-port
  information-element in-interface
```

```
information-element out-interface
information-element application-id
information-element rule-name
information-element rule-set-name
information-element fw-source-zone
information-element fw-dest-zone
information-element radius-imsi
information-element radius-msisdn
information-element radius-imei
information-element radius-custom1
information-element radius-custom2
information-element radius-custom3
information-element radius-custom4
information-element radius-custom5
information-element radius-custom6
information-element flow-start-msec
information-element flow-end-msec
information-element flow-duration-msec-64
information-element fwd-bytes
information-element fwd-packets
information-element rev-bytes
information-element rev-packets
information-element source-ipv6-address
information-element dest-ipv6-address
information-element fw-event
template-id 2004
!
```

## port-mapping-nat44-creation, port-mapping-nat44-deletion

Use the following config:

```
netflow template port_map44
information-element ip-PROTO
information-element source-ipv4-address
information-element source-port
information-element post-nat-source-port
information-element post-nat-source-ipv4-address
information-element flow-start-msec
information-element flow-end-msec
information-element nat-event
```

```
information-element radius-imsi
information-element radius-msisdn
information-element radius-imei
information-element radius-custom1
information-element radius-custom2
information-element radius-custom3
information-element radius-custom4
information-element radius-custom5
information-element radius-custom6
template-id 2005
!
```

### port-mapping-nat64-creation, port-mapping-nat64-deletion, port-mapping-dslite-creation, port-mapping-dslite-deletion

Use the following config:

```
netflow template port_map64
information-element ip-PROTO
information-element source-ipv4-address
information-element source-port
information-element post-nat-source-port
information-element post-nat-source-ipv4-address
information-element flow-start-msec
information-element flow-end-msec
information-element nat-event
information-element source-ipv6-address
information-element radius-imsi
information-element radius-msisdn
information-element radius-imei
information-element radius-custom1
information-element radius-custom2
information-element radius-custom3
information-element radius-custom4
information-element radius-custom5
information-element radius-custom6
information-element flow-end-reason
information-element rfc-flow-end-reason
template-id 2006
!
```

## port-batch-nat44-creation, port-batch-nat44-deletion

Use the following config:

```
netflow template port_batch44
  information-element ip-PROTO
  information-element source-ipv4-address
  information-element post-nat-source-ipv4-address
  information-element nat-event
  information-element radius-imsi
  information-element radius-msisdN
  information-element radius-imei
  information-element radius-custom1
  information-element radius-custom2
  information-element radius-custom3
  information-element radius-custom4
  information-element radius-custom5
  information-element radius-custom6
  information-element flow-start-msec
  information-element flow-end-msec
  information-element port-range-start
  information-element port-range-end
  information-element port-range-step-size
  information-element port-range-num-ports
  information-element flow-end-reason
  information-element rfc-flow-end-reason
  template-id 2007
!
```

## port-batch-nat64-creation, port-batch-nat64-deletion, port-batch-dslite-creation, port-batch-dslite-deletion

Use the following config:

```
netflow template port_batch64
  information-element ip-PROTO
  information-element source-ipv4-address
  information-element post-nat-source-ipv4-address
  information-element nat-event
  information-element radius-imsi
  information-element radius-msisdN
  information-element radius-imei
```

```
information-element radius-custom1
information-element radius-custom2
information-element radius-custom3
information-element radius-custom4
information-element radius-custom5
information-element radius-custom6
information-element flow-start-msec
information-element flow-end-msec
information-element port-range-start
information-element port-range-end
information-element port-range-step-size
information-element port-range-num-ports
information-element source-ipv6-address
information-element flow-end-reason
information-element rfc-flow-end-reason
template-id 2008
!
```

## port-batch-v2-nat44-creation, port-batch-v2-nat44-deletion

Use the following config:

```
netflow template pool_port_batch44
information-element ip-PROTO
information-element source-ipv4-address
information-element post-nat-source-ipv4-address
information-element nat-event
information-element radius-imsi
information-element radius-msisdN
information-element radius-imei
information-element radius-custom1
information-element radius-custom2
information-element radius-custom3
information-element radius-custom4
information-element radius-custom5
information-element radius-custom6
information-element flow-start-msec
information-element flow-end-msec
information-element port-range-start
information-element port-range-end
information-element flow-end-reason
```

```
information-element rfc-flow-end-reason
template-id 2009
!
```

## port-batch-v2-nat64-creation, port-batch-v2-nat64-deletion, port-batch-v2-dslite-creation, port-batch-v2-dslite-deletion

Use the following config:

```
netflow template pool_port_batch64
information-element ip-proto
information-element source-ipv4-address
information-element post-nat-source-ipv4-address
information-element nat-event
information-element radius-imsi
information-element radius-msisdn
information-element radius-imei
information-element radius-custom1
information-element radius-custom2
information-element radius-custom3
information-element radius-custom4
information-element radius-custom5
information-element radius-custom6
information-element flow-start-msec
information-element flow-end-msec
information-element port-range-start
information-element port-range-end
information-element source-ipv6-address
template-id 2010
!
```

## cg-n-ddos-l3-entry-creation and cg-n-ddos-l3-entry-deletion

Use the following config:

```
netflow template cg_n_ddos_l3
information-element rev-tuple-vnp-id
information-element dest-ipv4-address
information-element security-event-type
```

## cg-n-d-dos-l4-entry-creation and cg-n-d-dos-l4-entry-deletion

Use the following config:

```
netflow template cg_n_ddos_l4
  information-element rev-tuple-vnp-id
  information-element dest-ipv4-address
  information-element security-event-type
  information-element dest-port
  information-element ip-PROTO
```

## fw-ddos-entry-creation and fw-ddos-entry-deletion

Use the following config:

```
netflow template fw_ddos_entry
  information-element rev-tuple-vnp-id
  information-element dest-ipv4-address
  information-element dest-ipv4-prefix-len
  information-element dest-ipv6-prefix-len
  information-element security-event-type
  information-element dest-ipv6-address
  information-element radius-custom1
  information-element radius-custom2
  information-element radius-custom3
  information-element radius-custom4
  information-element radius-custom5
  information-element radius-custom6
  information-element rule-name
```

---

**NOTE:** In case of both CGN and Firewall DDoS entries, the IP address under attack will be displayed as the destination IPv4 address.

---

## fw-session-limit-exceeded

Use the following config:

```
netflow template fw_sessn_limit
  information-element rev-tuple-vnp-id
  information-element security-event-type
  information-element source-ipv4-prefix-len
  information-element source-ipv6-prefix-len
```

```
information-element radius-custom1
information-element radius-custom2
information-element radius-custom3
information-element radius-custom4
information-element radius-custom5
information-element radius-custom6
information-element rule-name
information-element limit-exceeded-count
```

## deny-reset-event-fw4

Use the following config:

```
netflow template fw4_deny
  information-element ip-proto
  information-element dest-ipv4-address
  information-element source-ipv4-address
  information-element source-port
  information-element dest-port
  information-element in-port
  information-element out-port
  information-element in-interface
  information-element out-interface
  information-element application-id
  information-element rule-name
  information-element rule-set-name
  information-element fw-source-zone
  information-element fw-dest-zone
  information-element radius-imsi
  information-element radius-msisdn
  information-element radius-imei
  information-element radius-custom1
  information-element radius-custom2
  information-element radius-custom3
  information-element radius-custom4
  information-element radius-custom5
  information-element radius-custom6
  information-element flow-start-msec
  information-element flow-end-msec
  information-element fw-deny-reset-event
  template-id 2011
```

!

## deny-reset-event-fw6

Use the following config:

```
netflow template fw6_deny
  information-element ip-proto
  information-element source-port
  information-element dest-port
  information-element in-port
  information-element out-port
  information-element in-interface
  information-element out-interface
  information-element application-id
  information-element rule-name
  information-element rule-set-name
  information-element fw-source-zone
  information-element fw-dest-zone
  information-element radius-imsi
  information-element radius-msisdn
  information-element radius-imei
  information-element radius-custom1
  information-element radius-custom2
  information-element radius-custom3
information-element radius-custom4
  information-element radius-custom5
  information-element radius-custom6
  information-element flow-start-msec
  information-element flow-end-msec
  information-element fw-deny-reset-event
  information-element dest-ipv6-address
  information-element source-ipv6-address
template-id 2012
!
```

## Supported IPFIX Information Elements

A10 supports the following IP Flow Information Export (IPFIX) information elements. RFC5102 describes the Information Elements used in IPFIX, and it offers details on Information Element naming, numbers, and data type. Information elements are the smallest units or pieces of information in IPFIX log messages.

The [Table 11](#) lists the A10-supported information elements and [Table 12](#) lists the customized information elements.

**NOTE:** Two new RFC-defined IEs: Application Category Name and Application Subcategory Name are added. These IEs can be exported as NetFlow fields and are used to determine the application category for application visibility and category-based policing.

Table 11 : A10 Supported Information Elements

ID	As per RFC5102	Supported by A10	Size	Data Type Semantics	Description
1	octetDeltaCount (fwdBytes)	fwd-bytes	8 bytes/ 4 bytes in A10* unsigned64 * The standard IE size is 8 bytes, but A10's is 4 bytes. Please adjust on the collector side.	deltaCounter	The number of octets since the previous report (if any) in incoming packets for this Flow at the Observation Point. The number of octets includes IP header(s) and IP payload.
2	packetDeltaCount (fwdPackets)	fwd-packets	8 bytes/ 4 bytes in A10* unsigned64	deltaCounter	The number of incoming packets since the previous report (if any) for this flow at the Observation Point.

Table 11 : A10 Supported Information Elements

ID	As per RFC5102	Supported by A10	Size	Data Type Semantics	Description
			* The standard IE size is 8 bytes, but A10's is 4 bytes. Please adjust on the collector side.		
4	protocolIdentifier (ipProto)	ip-proto	1 byte unsigned8	identifier	<p>The value of the protocol number in the IP packet header. The protocol number identifies the IP packet payload type. Protocol numbers are defined in the IANA Protocol Numbers registry.</p> <p>In Internet Protocol version 4 (IPv4), this is carried in the Protocol field. In Internet Protocol version 6 (IPv6), this is carried in the Next Header field in the last extension header of the packet.</p>
6	tcpControlBits	tcp-control-bits	2 bytes unsigned16	flags	<p>TCP control bits observed for the packets of this flow. This information is encoded as a bit field; for each TCP control bit, there is a bit in this set. The bit is set to 1 if any observed packet of this flow has the corresponding TCP control bit set to 1. The bit is cleared to 0 otherwise.</p>

Table 11 : A10 Supported Information Elements

ID	As per RFC5102	Supported by A10	Size	Data Type Semantics	Description
					<p>The values of each bit are shown below, per the definition of the bits in the TCP header [RFC793] [RFC3168][RFC3540]:</p> <p>MSb LSB</p> <p>0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15</p> <pre> +---+---+---+---+---+---+---+---+---+---+ +---+---+   N   C   E   U   A   P   R   S   F     Zero   Future   S   W   C   R   C   S   S   Y   I     (Data Offset)   Use     R   E   G   K   H   T   N   N   +---+---+---+---+---+---+---+---+ +---+---+---+---+---+ bit flag value name description -----+-----+----- ----- </pre>
					<p>0x8000 Zero (see tcpHeaderLength)  0x4000 Zero (see tcpHeaderLength)  0x2000 Zero (see tcpHeaderLength)  0x1000 Zero (see tcpHeaderLength)  0x0800 Future Use  0x0400 Future Use  0x0200 Future Use  0x0100 NS ECN Nonce Sum  0x0080 CWR Congestion Window</p>

Table 11 : A10 Supported Information Elements

ID	As per RFC5102	Supported by A10	Size	Data Type Semantics	Description
					<p>Reduced</p> <p>0x0040 ECE ECN Echo</p> <p>0x0020 URG Urgent Pointer field significant</p> <p>0x0010 ACK Acknowledgment field significant</p> <p>0x0008 PSH Push Function</p> <p>0x0004 RST Reset the connection</p> <p>0x0002 SYN Synchronize sequence numbers</p> <p>0x0001 FIN No more data from sender</p> <p>As the most significant 4 bits of octets 12 and 13 (counting from zero) of the TCP header [RFC793] are used to encode the TCP data offset (header length), the corresponding bits in this Information Element MUST be exported as zero and MUST be ignored by the collector. Use the tcpHeaderLength Information Element to encode this value. (truncated)</p>
7	sourceTransportPort	source-port	2 bytes unsigned16	identifier	The source port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the source port number given in the respective header. This field MAY also be used for future

Table 11 : A10 Supported Information Elements

ID	As per RFC5102	Supported by A10	Size	Data Type Semantics	Description
					transport protocols that have 16-bit source port identifiers.
8	sourceIPv4Address	source-ipv4-address	4 bytes ipv4Address	default	The IPv4 source address in the IP packet header.
9	sourceIPv4PrefixLength	source-ipv4-prefix-len	1 byte unsigned8	--	The number of contiguous bits that are relevant in the sourceIPv4Prefix Information Element.
10	ingressInterface	in-port	4 bytes/ 2 bytes in A10* unsigned32 * The standard IE size is 4 bytes, but A10's is 2 bytes. Please adjust on the collector side.	identifier	The index of the IP interface where packets of this Flow are being received. The value matches the value of managed object 'ifIndex' as defined in [RFC2863]. Note that ifIndex values are not assigned statically to an interface and that the interfaces may be renumbered every time the device's management system is re-initialized, as specified in [RFC2863].
11	destinationTransportPort	dest-port	2 bytes unsigned16	identifier	The destination port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header. This field MAY also be used for future transport protocols that have 16-bit destination port identifiers.

Table 11 : A10 Supported Information Elements

ID	As per RFC5102	Supported by A10	Size	Data Type Semantics	Description
12	destinationIPv4Address	dest-ipv4-address	4 bytes ipv4Address	default	The IPv4 destination address in the IP packet header.
13	destinationIPv4PrefixLength	dest-ipv4-prefix-len	1 byte unsigned8	--	The number of contiguous bits that are relevant in the destinationIPv4Prefix Information Element.
14	egressInterface	out-port	4 bytes/ 2 bytes in A10* unsigned32  * The standard IE size is 4 bytes, but A10's is 2 bytes. Please adjust on the collector side.	identifier	The index of the IP interface where packets of this flow are being sent. The value matches the value of managed object 'ifIndex' as defined in [RFC2863]. Note that ifIndex values are not assigned statically to an interface and that the interfaces may be renumbered every time the device's management system is re-initialized, as specified in [RFC2863].
17	sourceIPv6Address	source-ipv6-address	16 bytes ipv6Address	default	The IPv6 source address in the IP packet header.
18	destinationIPv6Address	dest-ipv6-address	16 bytes ipv6Address	default	The IPv6 destination address in the IP packet header.
19	sourceIPv6PrefixLength	source-ipv6-prefix-len	1 byte unsigned8	--	The number of contiguous bits that are relevant in the destinationIPv6Prefix Information Element.

Table 11 : A10 Supported Information Elements

ID	As per RFC5102	Supported by A10	Size	Data Type Semantics	Description
30	destinationIPv6PrefixLength	dest-ipv6-prefix-len	1 byte unsigned8	--	The number of contiguous bits that are relevant in the destinationIPv6Prefix Information Element.
61	flowDirection	flow-direction	1 byte unsigned8	identifier	The direction of the flow observed at the Observation Point. There are only two values defined.
82	interfaceName (source)	in-interface	16 bytes string	default	A short name uniquely describing an interface, e.g., "ethernet1"
95	applicationId	application-id	3 bytes octetArray	default	The first byte identifies that the selector ID id QOSMOS defined (21). The next two bytes are for the QOSMOS defined ID for the application.
96	applicationName	application-name	Variable (64 bytes max)	default	Indicates the application name.
136	flowEndReason	rfc-flow-end-reason	unsigned8	identifier	The reason for flow termination.
152	flowStartMilliseconds	flow-start-msec	8 bytes dateTimeMilliseconds	default	The absolute timestamp of the first packet of this flow.
153	flowEndMilliseconds	flow-end-msec	8 bytes dateTimeMilliseconds	default	The absolute timestamp of the last packet of this flow.
161	flowDurationMilliseconds	flow-duration-	4 bytes unsigned32	--	The difference in time between the first observed packet of this flow and the last observed packet of this

Table 11 : A10 Supported Information Elements

ID	As per RFC5102	Supported by A10	Size	Data Type Semantics	Description
		msec			flow.
225	postNATSourceIPv4Address	post-nat-source-ipv4-address	4 bytes ipv4Address	default	The definition of this Information Element is identical to the definition of Information Element 'sourceIPv4Address', except that it reports a modified value caused by a NAT middlebox function after the packet passed the Observation Point.
226	postNATDestinationIPv4Address	post-nat-dest-ipv4-address	4 bytes ipv4Address	default	The definition of this Information Element is identical to the definition of Information Element 'destinationIPv4Address', except that it reports a modified value caused by a NAT middlebox function after the packet passed the Observation Point.
227	postNAPTsourceTransportPort	post-nat-source-port	2 bytes unsigned16	identifier	The definition of this Information Element is identical to the definition of Information Element 'sourceTransportPort', except that it reports a modified value caused by a Network Address Port Translation (NAPT) middlebox function after the packet passed the Observation Point.
228	postNAPTdestinationTransportPort	post-nat-dest-port	2 bytes unsigned16	identifier	The definition of this Information Element is identical to the definition of Information Element 'destinationTransportPort', except that it reports a modified value

Table 11 : A10 Supported Information Elements

ID	As per RFC5102	Supported by A10	Size	Data Type Semantics	Description
					caused by a Network Address Port Translation (NAPT) middlebox function after the packet passed the Observation Point.
230	natEvent	nat-event	1 byte unsigned8	identifier	<p>This Information Element identifies a NAT event. This IE identifies the type of a NAT event. Examples of NAT events include, but are not limited to, NAT translation create, NAT translation delete, Threshold Reached, or Threshold Exceeded, etc.</p> <p>Values for this Information Element are listed in the “NAT Event Type” registry, see [<a href="http://www.iana.org/assignments/ipfix/ipfix.xml#ipfix-nat-event-type">http://www.iana.org/assignments/ipfix/ipfix.xml#ipfix-nat-event-type</a>].</p> <p>New assignments of values will be administered by IANA and are subject to Expert Review [RFC8126]. Experts need to check definitions of new values for completeness, accuracy, and redundancy.</p>
233	firewallEvent	fw-event	1 byte unsigned8	--	<p>Indicates a firewall event. The allowed values are:</p> <p>0 - Ignore (invalid)</p> <p>1 - Flow Created</p>

Table 11 : A10 Supported Information Elements

ID	As per RFC5102	Supported by A10	Size	Data Type Semantics	Description
					<p>2 - Flow Deleted</p> <p>3 - Flow Denied</p> <p>4 - Flow Alert</p> <p>5 - Flow Update</p>
281	postNATSourceIPv6Address	post-nat-source-ipv6-address	16 bytes ipv6Address	default	<p>The definition of this Information Element is identical to the definition of Information Element 'sourceIPv6Address', except that it reports a modified value caused by a NAT64 middlebox function after the packet passed the Observation Point.</p> <p>See [RFC8200] for the definition of the Source Address field in the IPv6 header. See [RFC3234] for the definition of middleboxes. See [RFC6146] for nat64 specification.</p>
282	postNATDestinationIPv6Address	post-nat-dest-ipv6-address	16 bytes ipv6Address	default	<p>The definition of this Information Element is identical to the definition of Information Element 'destinationIPv6Address', except that it reports a modified value caused by a NAT64 middlebox function after the packet passed the Observation Point.</p> <p>See [RFC8200] for the definition of the Destination Address field in the IPv6 header. See [RFC3234] for the</p>

Table 11 : A10 Supported Information Elements

ID	As per RFC5102	Supported by A10	Size	Data Type Semantics	Description
					definition of middleboxes. See [RFC6146] for nat64 specification.
3-2-3	observationTimeMilliseconds	event-time-msec	4 bytes unsigned32	--	The absolute time in milliseconds of an event observation
361	portRangeStart	port-range-start	2 bytes unsigned16	identifier	The port number identifying the start of a range of ports. A value of zero indicates that the range start is not specified, ie the range is defined in some other way.
362	portRangeEnd	port-range-end	2 bytes unsigned16	identifier	The port number identifying the end of a range of ports. A value of zero indicates that the range end is not specified, i.e., the range is defined in some other way.  Additional information on defined TCP port numbers can be found at [IANA registry service-names-port-numbers].
363	portRangeStepSize	port-range-step-size	2 bytes unsigned16	identifier	The step size in a port range. The default step size is 1, which indicates contiguous ports. A value of zero indicates that the step size is not specified, i.e., the range is defined in some other way.
364	portRangeNumPorts	port-range-num-ports	2 bytes unsigned16	identifier	The number of ports in a port range. A value of zero indicates that the number of ports is not specified, i.e., the range is defined in some other way.

Table 11 : A10 Supported Information Elements

<b>ID</b>	<b>As per RFC5102</b>	<b>Supported by A10</b>	<b>Size</b>	<b>Data Type Semantics</b>	<b>Description</b>
3-7-2	applicationCategoryName	application-category-name	Variable (64 bytes max)	default	An attribute that provides a first level categorization for each Application ID.
3-7-3	applicationSubCategoryName	application-subcategory-name	Variable (64 bytes max)	default	An attribute that provides a second level categorization for each Application ID.
455	mobileIMSI	imsi radius-imsi (Deprecated)	Variable (max 15 bytes) string	default	One of the RADIUS attributes: The International Mobile Subscription Identity (IMSI). The IMSI is a decimal digit string with up to a maximum of 15 ASCII/UTF-8 encoded digits (0x30 - 0x39).
456	mobileMSISDN	msisdn radius-msisdn (Deprecated)	variable (max 15 bytes) string	default	One of the RADIUS attributes: The Mobile Station International Subscriber Directory Number (MSISDN). The MSISDN is a decimal digit string with up to a maximum of 15 ASCII/UTF-8 encoded digits (0x30 - 0x39).

Table 12 : A10 Supported Customized Information Elements

ID	Information Element as per RFC5102	Customized Information Elements supported by A10	Size	Data Type Semantics	Description
32769 (PEN:29305)	octetDeltaCount (RevBytes)	rev-bytes	4 bytes unsigned 64	deltaCounter	This is the same as octetDeltaCount, but in reverse direction.
32770 (PEN:29305)	RevPackets	rev-packets	4 bytes unsigned 64	deltaCounter	This is the same as packetDeltaCount, but in reverse direction.
32850 (PEN:29305)	interfaceName (dest)	out-interface	16 bytes string	default	A short name uniquely describing an interface, e.g., "ethernet1"
33024 (PEN:40842)	fwdTupleType	fwd-tuple-type	1 byte unsigned 8	identifier	The forward A10 tuple type. 1: ipv4 2: ipv6 3: ipv6 in ipv4 4: ipv4 in ipv6

Table 12 : A10 Supported Customized Information Elements

ID	Information Element as per RFC5102	Customized Information Elements supported by A10	Size	Data Type Semantics	Description
33025 (PEN:40842)	revTupleType	rev-tuple-type	1 byte unsigned 8	identifier	Same as fwdTupleType, in reverse direction
33028 (PEN:40842)	fwdVNPID	fwd-tuple-vnp-id	2 bytes unsigned 16	identifier	L3v Partition id for forward tuple
33029 (PEN:40842)	revVNPID	rev-tuple-vnp-id	2 bytes unsigned 16	identifier	L3v partition id for reverse tuple
33030 (PEN:40842)	mobileIMEI	imei radius-imei (Deprecated)	Variable (max 16 bytes) string	default	One of the RADIUS attributes: The International Mobile Equipment Identity is a unique 15 digit code.
33031 (PEN:40842)	Custom1	radius-custom1	Variable (max 63 bytes) string	default	One of the Custom RADIUS attributes (part of the radius

Table 12 : A10 Supported Customized Information Elements

ID	Information Element as per RFC5102	Customized Information Elements supported by A10	Size	Data Type Semantics	Description
					configuration)
33032 (PEN:40842)	Custom2	radius-custom2	Variable (max 63 bytes) string	default	One of the Custom RADIUS attributes (part of the radius configuration)
33033 (PEN:40842)	Custom3	radius-custom3	Variable (max 63 bytes) string	default	One of the Custom RADIUS attributes (part of the radius configuration)
33034 (PEN:40842)	RuleName	rule-name	Variable (max 64 bytes) string	default	Name of the Firewall Rule that the packet hit
33035 (PEN:40842)	RuleSetName	rule-set-name	Variable (max 64 bytes) string	default	Name of the Firewall Ruleset that the packet hit
33036	SourceZone	fw-	Variable	default	Source Zone

Table 12 : A10 Supported Customized Information Elements

ID	Information Element as per RFC5102	Customized Information Elements supported by A10	Size	Data Type Semantics	Description
(PEN:40842)		source-zone	e (max 128 bytes) String		Name
33037 (PEN:40842)	DestZone	fw-dest-zone	Variable (max 128 bytes) String	default	Destination Zone Name
33038 (PEN:40842)	fwDenyReset	fw-deny-reset-event	1 byte unsigned8	default	Indicates a firewall deny/reset event. The allowed values are: <ul style="list-style-type: none"> <li>• 0 - Deny</li> <li>• 1 - Reset</li> </ul>
33039 (PEN:40842)	flowDurationMilliseconds64	flow-duration-msec-64	8 bytes	default	The difference in time between the first observed packet of this Flow and the

Table 12 : A10 Supported Customized Information Elements

ID	Information Element as per RFC5102	Customized Information Elements supported by A10	Size	Data Type Semantics	Description
					last observed packet of this Flow. This has been to accommodate for values more than ff ff ff ff (4294967295 in milliseconds and 49.71026961806 in days)
33040 (PEN:40842)	cgn-flow-direction	cgn-flow-direction	1 byte unsigned8	identifier	Flow direction: 0:inbound(To an outside interface)/1:outbound(To an inside interface)/2:hairpin(From an inside interface to an inside interface) (ID: 33040)
33041	fw-dest-fqdn	fw-dest-	Variabl	default	Firewall

Table 12 : A10 Supported Customized Information Elements

ID	Information Element as per RFC5102	Customized Information Elements supported by A10	Size	Data Type Semantics	Description
		fqdn	e (Max 128 bytes)		Destination FQDN string address
33042	flow-end-reason	flow-end-reason	1 byte	identifier	For detailed information about the A10 flow end reasons and its description, see <a href="#">Terminating a Session</a> .
33043	gtp-deny-reason	gtp-deny-reason	Variable (Max 128 bytes)	default	Indicates the reason in the event of packet drop due to GTP policy violation.
33044	gtp-apn	gtp-apn	Variable (Max 128 bytes)	default	Indicates the GTP Access Point Name
33045	gtp-steid	gtp-steid	4 bytes	default	Indicates the GTP Source

Table 12 : A10 Supported Customized Information Elements

ID	Information Element as per RFC5102	Customized Information Elements supported by A10	Size	Data Type Semantics	Description
					TEID
33046	gtp-dteid	gtp-dteid	4 bytes	default	Indicates the GTP Destination TEID
33047	gtp-selection-mode	gtp-selection-mode	Variable (Max 128 bytes)	default	Indicates the GTP Selection Mode
33048	gtp-mcc	gtp-mcc	3 bytes	default	Indicates the GTP Mobile Country Code
33049	gtp-mnc	gtp-mnc	3 bytes	default	Indicates the GTP Mobile Network Code
33050	gtp-rat-type	gtp-rat-type	6 bytes	default	Indicates the GTP RAT Type
33051	gtp-pdn-pdp-type	gtp-pdn-pdp-type	6 bytes	default	Indicates the GTP PDN/PDP Type
33052	gtp-uli	gtp-uli	Variable (max 128)	default	Indicates the GTP User Location

Table 12 : A10 Supported Customized Information Elements

ID	Information Element as per RFC5102	Customized Information Elements supported by A10	Size	Data Type Semantics	Description
			bytes)		Information
33053	gtp-enduser-v4-addr	gtp-enduser-v4-addr	4 bytes	default	Indicates the GTP PAA IPv4 Address
33054	gtp-enduser-v6-addr	gtp-enduser-v6-addr	16 bytes	default	Indicates the GTP PAA IPv6 Address
33055	gtp-bearer-id-or-nsapi	gtp-bearer-id-or-nsapi	1 byte	default	Indicates the EPS Bearer ID or NSAPI in GTP-C Packet
33056	gtp-qci	gtp-qci	1 byte	default	Indicates the GTP QoS or Traffic Class
33057	gtp-info-event-ind	gtp-info-event-ind	1 byte	identifier	Indicates the GTP INFO event 1 - upon S5 Node restart
33058	gtp-restarted-node-ipv4	gtp-restarted-node-ipv4	4 bytes	default	Indicates the Ipv4 Address of S5 Node restarted
33059	gtp-restarted-node-	gtp-	16	default	Indicates the

Table 12 : A10 Supported Customized Information Elements

ID	Information Element as per RFC5102	Customized Information Elements supported by A10	Size	Data Type Semantics	Description
	ipv6	restarte d-node- ipv6	bytes		Ipv6 Address of S5 Node restarted
33060	gtp-c-tunnels-removed-with-node-restart	gtp-c-tunnels-removed-with-node-restart	4 bytes	totalCounter	Number of GTP-C tunnels deleted with Node restart
33062	limit-exceeded-count	limit-exceeded-count	4 bytes	default	Indicates the limit exceeded count for fire-wall concurrent session
33063	security-event-type	security-event-type	2 bytes	default	Indicates the type of security event
33064 (PEN:40-842)	rate-limit-key	rate-limit-key	Variable (max 128 bytes)	default	Indicates the APN name or the network element
33065 (PEN:40-	rate-limit-type	rate-limit-	Variable	default	Indicates the message type

Table 12 : A10 Supported Customized Information Elements

ID	Information Element as per RFC5102	Customized Information Elements supported by A10	Size	Data Type Semantics	Description
842)		type	(max 128 bytes)		that is causing the packet drop
33066 (PEN:40-842)	rate-limit-drop-count	rate-limit-drop-count	4 bytes	default	Indicates the number of packets dropped due to rate limiting
33067 (PEN:40842)	Custom4	radius-custom4	Variable (max 63 bytes) string	default	One of the Custom RADIUS attributes (part of the radius configuration)
33068 (PEN:40-842)	Custom5	radius-custom5	Variable (max 63 bytes) string	default	One of the Custom RADIUS attributes (part of the radius configuration)
33069 (PEN:40-842)	Custom6	radius-custom6	Variable (max 63 bytes)	default	One of the Custom RADIUS attributes (part

Table 12 : A10 Supported Customized Information Elements

ID	Information Element as per RFC5102	Customized Information Elements supported by A10	Size	Data Type Semantics	Description
			string		of the radius configuration)

## Notes

1. Fields with PEN (Private Enterprise Number) is not documented in NetFlow V9, however we support those fields in V9 packets.
2. The PEN 40842 is for A10 Networks Inc. The fields with this PEN are A10 specific private defined.
3. The PEN 29305 is public defined for bidirectional flow information model (RFC 5103).
4. The PEN 33040 (cgn-flow-direction) is an A10 specified IE that is recommended to be used for CGN flows to distinguish between inbound, outbound and hairpin traffic. The flow-direction (ID 61) is an IANA specified IE that only has two values: inbound and outbound.
5. The PEN 161 (flowDurationMillisecondsNetflow) is an IANA specified IE that records the time a particular session is open. This field is 4 bytes and shows value in milliseconds. Hence, maximum value would be ff ff ff ff. This value corresponds to 4294967295 in milliseconds and 49.71026961806 in days. A new A10 specified IE is added that is 8 bytes in size (flow-duration-msec-64 (ID: 33039)). Select the 32-bit IANA specified IE or the new A10 defined IE based on the use case. Duration is calculated as curr - start. If a user has the below config selected, then the 32 bit IE is good enough, because then the start time is reset each time a NetFlow record

is sent out for the session.

```
ACOS(config)#netflow common ?
reset-time-on-flow-record
Reset session start time to current time on each flow timeout export
for long-lasting session (default: disabled)
```

6. For more information about other fields, see:  
<https://www.iana.org/assignments/ipfix/ipfix.xhtml>.

## NetFlow Logging Over Dedicated Partition

The NetFlow logs can be sent over a dedicated partition to one or more NetFlow collectors. You can also allow other partitions to send the logs through the dedicated partition. This feature helps to meet the requirements of lawful interception that runs on a separate network and uses an overlapping IP range with the subscriber for NetFlow collectors.

The NetFlow logs can be sent over a dedicated partition by configuring `netflow use-partition` during the NetFlow configuration.

You cannot configure `netflow use-partition` on the current partition if NetFlow Monitor is already configured (and vice versa).

To configure NetFlow logging over a dedicated partition, see [Configuring NetFlow Logging Over a Dedicated Partition](#).

## Configuring NetFlow

The following topics are covered:

<a href="#">Overview</a> .....	124
<a href="#">Using the GUI to Configure NetFlow</a> .....	124
<a href="#">Using the CLI to Configure NetFlow</a> .....	126
<a href="#">Disabling CGN Logs based on Destination Protocol and Port Criteria</a> .....	131

## Overview

---

The following is an overview of the steps needed to configure NetFlow:

1. For configuring multiple NetFlow collectors:
  - a. Create a server configuration for each collector.
  - b. Configure a service group and add the log servers to the group.  
Make sure to disable the Layer 4 health check on the UDP port.
2. Configure a NetFlow monitor. Within the monitor, specify the following:

- The destination, which can be one of the following:
  - Host address, if using a single NetFlow collector
  - Service-group name, if using multiple NetFlow collectors
- The record types to export. (Specify them by NetFlow template type.)
- (Optional) The Ethernet interfaces from which to collect NetFlow information. By default, information is collected for all interfaces.
- (Optional) Adjust the flow timeout.
- (Optional) Adjust the template resend counters.
- (Optional) Adjust the maximum packet queue time.

---

**NOTE:** If you plan to use only a single NetFlow collector, you do not need to perform step 1 (as mentioned above). You can specify the NetFlow collector's IP address when configuring the NetFlow monitor (as in step 2).

---

## Using the GUI to Configure NetFlow

---

To configure NetFlow using the GUI:

1. Hover over **System** in the navigation bar, and select **Monitoring**.
2. Click **NetFlow** on the menu bar.
3. Choose one of the following:

- **Monitors** to create a monitor from one of the Predefined Templates. Then choose:
  - **Create Netflow v9**, OR
  - **Create IPFix**
- **Custom Templates** to create a monitor from a Custom Event Templates, and click **Create**.

The Create NetFlow Monitor page appears.

4. Enter a name for the NetFlow monitor in the Name field.
5. Configure the following fields and options:
  - The Destination, which can be one of the following:
    - Host address, if using a single NetFlow collector
    - Service-group name, if using multiple NetFlow collectors
  - (Optional) Adjust the flow timeout. Default is 10 minutes.
  - (Optional) Adjust the amount of records after which to resend template in the Resend Template Records field. The default is 1000 records, after which the template will be re-sent to the collector and the counter will be reset to 0.
  - (Optional) Adjust the timeout for resending template in the Resend Template Timeout field. The default is 1800 seconds, after which the template is re-sent to the collector.
  - (Optional) Set Source IP Use Management to Enable to use the IP address of the management port of the ACOS device as the source IP of the NetFlow packets, even when packets are sent out the data interface.
  - Select the Protocol version. The default is NetFlow Version 9, but you can also select NetFlow Version 10.
  - Select the record types to export. (Specify them by NetFlow template type. See [Predefined NetFlow Templates](#) for details.)
6. When finished, click **Save** to save your changes.ni.

## Using the CLI to Configure NetFlow

This section provides the following CLI examples for configuring NetFlow.

The following topics are covered:

<a href="#">CLI Example: Single Collector</a> .....	126
<a href="#">CLI Example: Multiple Collectors</a> .....	126
<a href="#">CLI Example: Firewall Session Event</a> .....	127
<a href="#">Configuring NetFlow Logging Over a Dedicated Partition</a> .....	128

### CLI Example: Single Collector

The following commands configure NetFlow in a partition. This example uses a single NetFlow collector.

```

ACOS(config)# netflow monitor test
ACOS(config-netflow-monitor)# record netflow-v5
ACOS(config-netflow-monitor)# record netflow-v5-ext
ACOS(config-netflow-monitor)# destination 10.10.3.2
ACOS(config-netflow-monitor)# show netflow monitor
Netflow Monitor test
  Protocol                Netflow v9
  Status:                  Enable
  Filter:                  Global
  Destination:            10.10.3.2:9996
  Source IP Use MGMT:     No
  Flow Timeout:           60 Minutes
  Resend Template Per Records: 1000
  Resend Template Timeout: 1800 Seconds
  Sent:                    45 (Pkts) / 8360 (Bytes)
  Records:
    netflow-v5:            86 (records) / 0 (fails)
    netflow-v5-ext:       0 (records) / 0 (fails)

```

### CLI Example: Multiple Collectors

The following commands configure export of NetFlow records to multiple collectors for a CGN partition.

```
ACOS(config)# cgmv6 server s1 80.1.1.108
ACOS(config-real server)# port 9996 udp
ACOS(config-real server-node port)# health-check-disable
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# cgmv6 server s2 80.1.1.109
ACOS(config-real server)# port 9996 udp
ACOS(config-real server-node port)# health-check-disable
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# cgmv6 service-group sg1 udp
ACOS(config-cgmv6 svc group)# member s1 9996
ACOS(config-cgmv6 svc group)# member s2 9996
ACOS(config-cgmv6 svc group)# exit
ACOS(config)# netflow monitor nf1
ACOS(config-netflow-monitor)# destination service-group sg1
ACOS(config-netflow-monitor)# record nat44
ACOS(config-netflow-monitor)# record dslite
ACOS(config-netflow-monitor)# record sesn-event-nat64 both
ACOS(config-netflow-monitor)# custom-record sesn-event-nat44-creation
template nat44
ACOS(config-netflow-monitor)# end
ACOS#
```

## CLI Example: Firewall Session Event

The following commands configure export of NetFlow records for firewall session events to multiple collectors.

**NOTE:** In the following example, the “service-group netflow-collector” is configured prior to configuring NetFlow.

```
ACOS(config)# netflow monitor netflow_monitor1
ACOS(config-netflow-monitor)# record sesn-event-fw4 both
ACOS(config-netflow-monitor)# destination service-group netflow-collector
ACOS(config-netflow-monitor)# resend-template records 0
ACOS(config-netflow-monitor)# resend-template timeout 1200
ACOS(config-netflow-monitor)# end
ACOS#
```

---

**NOTE:** Use the `both` option to export both creation and deletion events. Use the `creation` option to export only creation events and the `deletion` option to export only deletion events. Use the `sesn-event-fw4` option to configure an IPv4 firewall session, the `sesn-event-fw6` option to configure an IPv6 firewall session.

---

Netflow monitor can be configured for a specific rule. In that case, you must use `scope firewall-rule` command while configuring the template. Note that the default scope is global. The following example shows how to configure NetFlow monitor only for a specific rule.

```
ACOS(config)# netflow monitor netflow_monitor1
ACOS(config-netflow-monitor)# scope firewall-rule
ACOS(config-netflow-monitor)# record sesn-event-fw4 both
ACOS(config-netflow-monitor)# destination service-group netflow-collector
ACOS(config-netflow-monitor)# resend-template records 0
ACOS(config-netflow-monitor)# resend-template timeout 1200
ACOS(config-netflow-monitor)# end
ACOS(config)# rule-set set1
ACOS(config-rule set:set1)# rule 2
ACOS(config-rule set: set1:2)# action-group
ACOS(config-rule set: set1:2-acti...)# permit log netflow-monitor netflow_
monitor1
```

## Configuring NetFlow Logging Over a Dedicated Partition

You can configure NetFlow to send the logs over a dedicated partition to a NetFlow collector. You can also allow other partitions to send the logs over the dedicated partition.

Use the following command to configure a dedicated partition to send the NetFlow logs:

```
ACOS(config)# netflow use-partition <dedicated_partition_name>
```





































































# Including Additional Client Information in Logs

---

In addition to information normally provided in traffic logs, the following types of information can be configured in logging.

The following topics are covered:

<a href="#">Logging Client HTTP Requests</a> .....	164
<a href="#">Logging Client Mobile Numbers</a> .....	173
<a href="#">Logging Client MAC Address</a> .....	178



Table 15 : Maximum URL Characters Logged

Logging Option	Maximum URL Characters Logged
Logging to RADIUS	247

Additional characters are truncated from the right side of the URL string.

The default maximum URL length is 100 characters. You can set the maximum to 100-1000 characters. The limits listed in [Table 15](#) still are applicable.

## Additional Notes

- If you plan to log HTTP requests, you must specify the destination protocol port. You can specify up to 5 destination protocol ports within a given logging template. The supported HTTP methods are GET, HEAD, PUT, POST, OPTIONS, DELETE, TRACE, and CONNECT.
- If an HTTP request is received in multiple packets, the ACOS device examines only the first packet for logging purposes.
- If URL logging is enabled, the maximum number of URL characters that can be logged depends on the log format settings. (See [Configurable Rules for HTTP Request Logging](#).)
- This feature applies to NAT44, NAT64, 6rd-NAT64, DS-Lite, and Fixed-NAT. This feature does not apply to 6rd or Static NAT.
- HTTP request logging does not apply to sessions that already exist when the logging configuration is activated.
- If you use the option to log requested hostnames, and an HTTP request does not contain a hostname, the server IP address in the client-server session is logged instead. For example, the server IP address would appear in logs for HTTP version 1.0 requests.
- Request/response byte counts include all session requests and response packets received by ACOS, including any retransmissions and any non-HTTP traffic on the session.
- HTTP logging is supported for SLB-L7 sessions that use CGN NAT pool.

## Configuration for HTTP Request Logging

---

To configure logging of HTTP request information, use either of the following methods.

### Using the GUI

1. Navigate to **CGN > Templates > Logging**.
2. Click **Create** to create a new template or click on the name of an existing template.
3. If the template is new, enter a name in the Name field.
4. From HTTP Request drop-down list, select one of the following options:
  - **Host** – Includes the requested hostname in logs.
  - **URL** – Includes the requested URL in logs.
5. In the Rules for HTTP Requests section, enter the destination protocol port number in the Dest Port field and click Add.
6. Click the **Add** button.
7. Click **Create**.

### Using the CLI

#### HTTP Request Logging Rules

- To configure rules for HTTP request logging and specify the destination protocol port for which to log requests, use the following commands:

```
ACOS(config-logging:lsn_logging)# rule http-requests dest-port 80
```
- To log every HTTP request in a client session, use the following command. Without this option, only the first request in the session is logged.

```
ACOS(config-logging:lsn_logging)# rule http-requests log-every-http-request
```
- To specify the maximum number of characters logged for each URL string, use the following command. You can specify 100-1000 characters.















































For examples of log messages generated by an ACOS device on which the logging option (Fixed-NAT user ports) is enabled, see [Fixed-NAT Log Samples](#).





- The Acct-Session-Id type is octets for all ACOS-generated CGN traffic logging event when log-receiver is set to RADIUS.
- To enable parsing A10 CGN logging RADIUS attributes in Wireshark, the following steps are required:
  - Copy the dictionary file from the section above or from the System Configuration and Administration Guide and save it to a text file named “dictionary.a10networks”.
  - Place the “dictionary.a10networks” file in the Wireshark RADIUS folder. The default path in Windows is “C:\Program Files\Wireshark\radius”.
  - Edit the file “dictionary” in the Wireshark RADIUS folder, to add the following line:

```
$INCLUDE dictionary.a10networks
```

## VRRP-A Support

---

ACOS stores the RADIUS attributes learned from other RADIUS servers in a table. In a VRRP-A deployment, you enable synchronization of the RADIUS attribute table from the active to the standby device(s). To do so, assign the RADIUS server profile used by CGN to a VRRP-A VRID.

For synchronization of the RADIUS attribute table to work, session synchronization must be enabled and working properly. (For VRRP-A configuration information, see the *Configuring VRRP-A High Availability* guide.)

## Configure RADIUS Logging

To configure logging of IPv6 activity to RADIUS:

1. Create a server configuration for each RADIUS server.
2. Configure a service group (server pool) and add the log servers to the group.
3. Configure a logging template. Within the template, specify the service group and the types of events to log. Also enable logging to RADIUS, and specify the shared secret required for access to the RADIUS server.
4. Activate the template.

---

**NOTE:** In the server configuration, make sure to specify the protocol port number for RADIUS accounting, not the port for authentication.

---

The following topics are covered:

[Configure RADIUS Logging Using the GUI](#) .....194

[Configure RADIUS Logging Using the CLI](#) ..... 195

---

## Configure RADIUS Logging Using the GUI

This example shows how to create a new logging template called "lsm\_logging" and enable RADIUS logging using the GUI:

1. Navigate to **CGN > LSN > Templates**.
2. Select **Logging** from the drop-down list.
3. Click **Create** to create a new logging template.
4. Enter `lsm_logging` as the name for the template in the Name field.
5. Further down the screen, expand the Log Receiver section.
6. Select the checkbox in the Log Receiver RADIUS field.
7. Enter the shared secret in the Secret String field.



### Create Template Logging

General Fields

Name \*

Include Destination

Include Inside User MAC

Include Partition Name

Include Radius Attribute

Attribute	Attribute Event
HTTP Request	

Batched Logging Disable

Source IP

Source IPv6

Service Group

Resolution  Seconds  10 Milliseconds

Format

Any

Source Port Number

Include HTTP

Log Receiver

Log Receiver RADIUS

Secret String

Facility

Severity Type  String  Value

Severity String

8. Click **Create**.

## Configure RADIUS Logging Using the CLI

The commands in this example configure external logging to RADIUS. RADIUS logging packets (syslog packets) cannot be sent via the management interface.

The following commands add the configuration information for the RADIUS servers:

1. Add the RADIUS server configuration:

```
ACOS(config)# cgnv6 server radius1 192.168.1.118
ACOS(config-real server)# port 1813 udp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# cgnv6 server radius2 10.10.10.119
ACOS(config-real server)# port 1813 udp
```

```
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# cgnv6 service-group radiusgp udp
ACOS(config-cgnv6 svc group)# member radius1 1813
ACOS(config-cgnv6 svc group)# member radius2 1813
ACOS(config-cgnv6 svc group)# exit
```

2. The following commands configure the logging template:

```
ACOS(config)# cgnv6 template logging lsn_logging
ACOS(config-logging:lsn_logging)# service-group radiusgp
ACOS(config-logging:lsn_logging)# log-receiver radius secret a10rad
ACOS(config-logging:lsn_logging)# exit
```

3. The following command enables logging using the template:

```
ACOS(config)#cgnv6 lsn logging default-template lsn_logging
```

## Customize RADIUS Attributes

With extended CGN support for RADIUS, configure custom attributes to get additional client information from RADIUS. Depending on the CGN configuration, ACOS can insert the additional client information into CGN log messages, or use the attributes to assign clients to NAT profiles (LSN LIDs).

To obtain client information from RADIUS, the ACOS device acts as a RADIUS server. An external RADIUS client (e.g. NAS, PGW/GGSN) sends a RADIUS accounting request packet containing an Acct-Status-Type attribute with the value “start” to ACOS. The RADIUS server sends an accounting-response message that includes the attribute values assigned to the client. ACOS then stores the attributes in a table. ACOS adds entries to the attribute tables based on RADIUS Accounting Start messages, and removes them based on Accounting Stop messages.

If your deployment uses VRRP-A, you can enable synchronization of this table to the standby device(s).

The following topics are covered:

<a href="#">Configuring RADIUS Logging Using Custom RADIUS Attributes</a> .....	197
<a href="#">Attribute Parameters</a> .....	201
<a href="#">Log String Formats</a> .....	202

## Configuring RADIUS Logging Using Custom RADIUS Attributes

---

To use custom RADIUS attributes with CGN traffic logging over RADIUS logging:

1. Define the attributes in the CGN RADIUS server configuration.
2. In the logging template, enable insertion of the attribute values.
3. (Optional) Assign the RADIUS server profile to an HA group or VRRP-A VRID. (The current release supports configuration of this option only in the CLI.)

### NOTE:

- These steps configure use of custom attributes for logging. You also can use custom attributes to assign clients to LSN LIDs.
  - These steps also assume that external traffic logging is already configured. This includes configuration of a service group containing the log servers, and a logging template that uses the servers.
- 

### Using the GUI

To define attributes in the RADIUS server configuration:

1. Navigate to **CGN > LSN > Global**.
2. Expand the RADIUS Server section, then click the checkboxes next to the custom attributes you plan to use. The options are Custom1 to Custom6.
3. Configure the parameters for each custom attribute. (See [Attribute Parameters](#).)
4. Configure other parameters as applicable. (See [Logging HTTP Headers](#).)
5. Click **Update**.

### Using the CLI

1. The following commands configure the IP list that specifies the external RADIUS client addresses. These servers will send AAA information to the ACOS device.

```
ACOS(config)# ip-list RADIUS_IP_LIST
ACOS(config-ip list)# 9.9.9.9 to 9.9.9.10
ACOS(config-ip list)# exit
```

2. The following commands configure the RADIUS server on the ACOS device. The

attribute commands configure the custom attributes.

```
ACOS(config)# system radius server
ACOS(config-lsn radius)# remote ip-list RADIUS_IP_LIST
ACOS(config-lsn radius)# listen-port 1813
ACOS(config-lsn radius)# attribute inside-ip number 8
ACOS(config-lsn radius)# secret a10
ACOS(config-radius-server)# attribute inside-ip number 8
ACOS(config-radius-server)# attribute msisdn number 31
ACOS(config-radius-server)# attribute imei vendor 10415 number 20
ACOS(config-radius-server)# attribute imsi vendor 10415 number 1
ACOS(config-radius-server)# attribute custom1 NAS-IP-Address value
hexadecimal number 4
ACOS(config-radius-server)# attribute custom2 Connection_PVC vendor
22610 number 43
ACOS(config-radius-server)# attribute custom3 xDSL_number vendor 22610
number 44
ACOS(config-radius-server)# attribute custom4 cus4 vendor 22610 number
81
ACOS(config-radius-server)# attribute custom5 cus5 vendor 22610 number
82
ACOS(config-radius-server)# attribute custom6 cus6 vendor 22610 number
83
ACOS(config-radius-server)# attribute inside-ipv6-prefix prefix-length
64 number 97
ACOS(config-radius-server)# attribute inside-ipv6 vendor 22610 number
29
ACOS(config-radius-server)# accounting start replace-entry
ACOS(config-radius-server)# accounting stop delete-entry-and-sessions
ACOS(config-radius-server)# accounting interim-update replace-entry
ACOS(config-radius-server)# exit
```

### 3. The following commands configure the logging template.

```
ACOS(config)# cgnv6 template logging log
ACOS(config-logging:log)# log http-requests url
ACOS(config-logging:log)# log sessions
ACOS(config-logging:log)# include-radius-attribute msisdn sessions
ACOS(config-logging:log)# include-radius-attribute imei sessions
ACOS(config-logging:log)# include-radius-attribute imsi sessions
```

```

ACOS(config-logging:log)# include-radius-attribute custom1 port-
mappings
ACOS(config-logging:log)# include-radius-attribute custom2 port-
mappings
ACOS(config-logging:log)# include-radius-attribute custom3 port-
mappings
ACOS(config-logging:log)# include-radius-attribute custom4 port-
mappings
ACOS(config-logging:log)# include-radius-attribute custom5 port-
mappings
ACOS(config-logging:log)# include-radius-attribute custom6 port-
mappings
ACOS(config-logging:log)# include-radius-attribute framed-ipv6-prefix
prefix-length 64
ACOS(config-logging:log)# include-port-block-account
ACOS(config-logging:log)# include-http referer
ACOS(config-logging:log)# include-http user-agent
ACOS(config-logging:log)# include-http header1 GET
ACOS(config-logging:log)# include-http l4-session-info
ACOS(config-logging:log)# include-http method
ACOS(config-logging:log)# include-http request-number
ACOS(config-logging:log)# include-http file-extension
ACOS(config-logging:log)# rule http-requests dest-port 80
ACOS(config-logging:log)# rule http-requests log-every-http-request
ACOS(config-logging:log)# rule http-requests max-url-len 200
ACOS(config-logging:log)# rule http-requests include-all-headers
ACOS(config-logging:log)# rule http-requests disable-sequence-check
ACOS(config-logging:log)# batched-logging-disable
ACOS(config-logging:log)# service-group cgn-log-group
ACOS(config-logging:log)# exit

```

4. The following command displays the table of RADIUS attributes stored on the ACOS device:

```

ACOS(config)# show system radius table
LSN RADIUS Table Statistics:
-----
Record Created          3
Record Deleted          0
Key Attribute           MSISDN           IMEI           IMSI

```

```

Charging-Gateway-Address
                                SGSN-Address
                                GGSN-Address
                                RAT-Type
                                User-
Location
                                user1_test1

wurenxiaode222

nihuoniaiwo333
-----
---
5.5.5.100                861015811129572    3732333435363731
31323334353632

10.210.211.42

86.108.150.81

86.108.159.162

                                02

8282f610224482f6100016b020

                                user1
                                yahoo
                                ATENkk

3.3.3.30                861015811129575    3732333435363734
31323334353633
2001:db8::/64

10.210.211.42

86.108.150.81

86.108.159.162

                                02

```

```

8282f610224482f6100016b020
                                ipv6
                                "google "
                                ATEN

2001:db8::5:100                861015811129575    3732333435363734
31323334353633

10.210.211.42

86.108.150.81

86.108.159.162
                                02

8282f610224482f6100016b020
                                ipv6
                                "google "
                                ATEN

Total RADIUS Records Shown: 3

```

The attribute names are listed, followed by the values received by the ACOS RADIUS server for these attributes for individual clients.

## Attribute Parameters

You can configure one or more of the following parameters in the profile for each custom attribute:

- Attribute name – The name assigned to the attribute. You will need to specify this value when you add the attribute to the logging template or ACOS RADIUS server configuration.
- Data type of the attribute value:
  - String – ACOS interprets the value as hexadecimal string data. The following ASCII printable characters are allowed (ASCII 32~126), except for (ASCII 34). This is the default.
  - Hexadecimal – ACOS interprets the value as raw hexadecimal data.

- Vendor ID – RADIUS vendor ID, 1-65535. By default, this value is not set.
- Attribute number – RADIUS attribute number, 1-255. This is the attribute ID used in the dictionary file on the RADIUS server. The default attribute numbers are as follows:
  - 42 – Attribute definition 1 on the ACOS device
  - 43 – Attribute definition 2 on the ACOS device
  - 44 – Attribute definition 3 on the ACOS device

## Log String Formats

This section shows how the custom RADIUS attribute values appear in log messages generated for each of the supported formats. These values come from the RADIUS server used by the client to authenticate.

The following topics are covered:

<a href="#">ASCII (the default format)</a> .....	202
<a href="#">Compact</a> .....	202
<a href="#">RFC 5424</a> .....	203
<a href="#">Binary</a> .....	203
<a href="#">RADIUS</a> .....	203
<a href="#">Notes for Log String Formats</a> .....	204

### ASCII (the default format)

In this example, the username and user ID for a client are included in a message that logs the creation of a UDP port mapping for a client.

```
AX NAT-UDP-C: 192.168.1.1:20001<--> 203.0.210.1:80, 203.0.210.1:80<-->
>203.0.113.1:20001 User_Name="A10 Networks" User_ID="12345"
```

### Compact

Here is a similar message containing the same extra client information as the example in [ASCII \(the default format\)](#), but in Compact format.

```
AX UC: 64646464:2710->96969696:2710 R1="A10 Networks" R2="12345"
```

## RFC 5424

This message shows the same information as [ASCII \(the default format\)](#) and [Compact](#), but in a log expressed in RFC 5424 format.

```
1 2012-04-19T05:54:14-07:00 192.168.147.167 AX2600 - SessionCreated:TCP [-  
3.3.3.50 26548 6.6.6.50 80 - 6.6.6.50 80 6.6.6.200 12218 "A10 Networks"  
"12345"]
```

## Binary

The values retrieved from the client's RADIUS server for the custom RADIUS attributes are encoded in the Type field of the extension header. The following values are used:

- 7 – Value retrieved for custom attribute 1
- 8 – Value retrieved for custom attribute 2
- 9 – Value retrieved for custom attribute 3

## RADIUS

To include the values from the client's RADIUS server in traffic logs sent to a RADIUS server used for CGN traffic logging, use the following attribute values in the accounting-request messages sent to the traffic logging server:

ATTRIBUTE	A10-CGN-RADIUS-Custom-1	42	string
ATTRIBUTE	A10-CGN-RADIUS-Custom-2	43	string
ATTRIBUTE	A10-CGN-RADIUS-Custom-3	44	string

The value for attribute definition 1 in ACOS is sent to the RADIUS server used for CGN logging as the value for attribute 42. This is because the dictionary file on the RADIUS server used for logging includes the definitions listed above. The definition IDs (1-3) for the attributes in ACOS are not the same as the attribute numbers used for those attributes on the CGN RADIUS server.

---

**NOTE:** In the custom attribute definitions (1-3) in ACOS, the configurable attribute numbers are those used by the client's RADIUS server. For example, if the RADIUS server sends the client's username to ACOS as attribute 42, attribute profile 1 in ACOS should be configured to use attribute number 42 for the data. ACOS then sends the data as the value for attribute 42, in the accounting-request message sent to the RADIUS server used for CGN traffic logging.

---

## Notes for Log String Formats

Take note of the following:

- If only some extensions are enabled, the enabled options appear in the same order, but without the disabled options.
- If the value for a custom attribute has not been retrieved yet by ACOS and stored in the attribute table, the attribute is omitted from log strings.
- In L3V partition deployments that support inter-partition traffic, the information for inclusion in CGN logging is provided by the CGN RADIUS server configuration in the L3V partition. The same attribute names must be configured in the CGN RADIUS server configuration in the shared partition.
- Any blank spaces at the beginning of a string value returned for a custom attribute are removed from the string value before the value is added to the attribute table. Likewise, the string values inserted into traffic log messages do not contain the omitted leading blanks.
- If you change the definition of a custom attribute, ACOS does not delete attribute data that was already placed in the table based on the attribute's previous definition.

## RADIUS Interim-Update Message

Whenever a RADIUS INTERIM or RADIUS START message is received for an existing mapping for a private IP, the old mapping is cleared, and a new mapping is created. This should happen whenever a new subscriber uses an IP address previously assigned to a different subscriber. In most cases, a RADIUS STOP message is sent first, and existing sessions related to the username or private IP in the message

should be cleared. In both cases, the sessions are cleared to avoid duplicated IP use or incorrect associations of internal IPs with the logged RADIUS attributes.

## Configuring NAT Logging with RADIUS Correlation

At the LSN RADIUS server configuration level, the following CLI commands specify the action that ACOS takes upon receiving RADIUS messages:

```
ACOS(config)# system radius server
ACOS(config-radius-server)# accounting on ignore
```

Use the following show command to check if a session is being cleared. While a session is being cleared, the user quota session Flag entry will be set to “U”.

```
ACOS(config)# show cgnv6 lsn user-quota-sessions
User-Quota Session Statistics
-----
LSN User-Quota Created                1
LSN User-Quota Freed                  0
LSN User-Quota Creation Failed        0
LSN TCP User-Quota Exceeded           0
LSN UDP User-Quota Exceeded           0
LSN ICMP User-Quota Exceeded          0
LSN Extended User-Quota Matched       0
LSN Extended User-Quota Exceeded      0
LSN Data Session User-Quota Exceeded  0
LSN Conn Rate User-Quota Exceeded     0

LSN User-Quota Sessions:
Inside Address      NAT Address      ICMP   UDP   TCP   Session
Pool               LID   Flag
-----
30.30.30.4         40.40.40.112    0     64   0     1
pbv22              2     U
Total User-Quota Sessions Shown: 1
```

To check if a Fixed NAT user is currently unusable, enter the show command below. A message will be generated in the CLI saying that the user is unavailable.

```
ACOS(config)# show cgnv6 fixed-nat inside-user 40.40.40.205 port-mapping
====Inside-User Marked Unusable (will be usable again once all ports used
by this inside-user are freed)====
NAT IP Address: 40.40.40.205
TCP: 1024 to 65535
UDP: 1024 to 65535
ICMP: 1024 to 65535
```

## Combined Port Batch Logging and RADIUS Message Configuration Example

The following example configures Port Batching version 2 and specifies the external servers which will send RADIUS messages to ACOS. The RADIUS server on the ACOS device is configured to read in RADIUS START, INTERIM, and STOP messages. To generate the logging messages, a CGN Custom logging template is configured to read the RADIUS attributes, and the template is enabled.

```
ACOS(config)# class-list PB_LIST
ACOS(config-class list)# 10.0.0.0/8 lsn-lid 1
ACOS(config-class list)# ip-list RADIUS_IP_LIST
ACOS(config-ip-list)# 40.40.40.1 to 40.40.40.2
ACOS(config-ip-list)# cgnv6 server syslog1 203.0.118.1
ACOS(config-real server)# port 514 udp
ACOS(config-real server-node port)# cgnv6 service-group syslog udp
ACOS(config-cgnv6 svc group)# member syslog1 514
ACOS(config-cgnv6 svc group-member:514)# cgnv6 template logging lsn_
logging
ACOS(config-logging:lsn_logging)# include-radius-attribute custom1 port-
mappings
ACOS(config-logging:lsn_logging)# include-radius-attribute custom2 port-
mappings
ACOS(config-logging:lsn_logging)# include-radius-attribute custom3 port-
mappings
ACOS(config-logging:lsn_logging)# include-radius-attribute custom4 port-
mappings
ACOS(config-logging:lsn_logging)# include-radius-attribute custom5 port-
mappings
```

```
ACOS(config-logging:lsn_logging)# include-radius-attribute custom6 port-
mappings
ACOS(config-logging:lsn_logging)# include-port-block-account
ACOS(config-logging:lsn_logging)# rule port-mappings interim-update 60
ACOS(config-logging:lsn_logging)# format custom
ACOS(config-logging:lsn_logging)# service-group syslog
ACOS(config-logging:lsn_logging)# custom message port-batch-v2-allocated
"$radius-ctm1$|$src-ip$|$nat-ip$|$nat-port-start$|$nat-port-end$|$sesn-
start-time$|$curr-time$|$ul-byte$|$dl-byte$|-|session_start|$radius-
ctm2$|$radius-ctm3$|$radius-ctm4$|$radius-ctm5$|$radius-ctm6$|$sesn-id$"
ACOS(config-logging:lsn_logging)# custom message port-batch-v2-freed
"$radius-ctm1$|$src-ip$|$nat-ip$|$nat-port-start$|$nat-port-end$|$sesn-
start-time$|$curr-time$|$ul-byte$|$dl-byte$|$ct-msg$|session_stop|$radius-
ctm2$|$radius-ctm3$|$radius-ctm4$|$radius-ctm5$|$radius-ctm6$|$sesn-id$"
ACOS(config-logging:lsn_logging)# custom message port-batch-v2-interim-
update "$radius-ctm1$|$src-ip$|$nat-ip$|$nat-port-start$|$nat-port-
end$|$sesn-start-time$|$curr-time$|$ul-byte$|$dl-byte$|-|session_
update|$radius-ctm2$|$radius-ctm3$|$radius-ctm4$|$radius-ctm5$|$radius-
ctm6$|$sesn-id$"
ACOS(config-logging:lsn_logging)# cgnv6 lsn inside source class-list PB_
LIST
ACOS(config)# system radius server
ACOS(config-radius-server)# remote ip-list RADIUS_IP_LIST
ACOS(config-radius-server)# secret a10rad
ACOS(config-radius-server)# attribute inside-ip number 8
ACOS(config-radius-server)# attribute custom1 Username vendor 22610 number
42
ACOS(config-radius-server)# attribute custom2 Connection_PVC vendor 22610
number 43
ACOS(config-radius-server)# attribute custom3 xDSL_number vendor 22610
number 44
ACOS(config-radius-server)# attribute custom4 cus4 vendor 22610 number 81
ACOS(config-radius-server)# attribute custom5 cus5 vendor 22610 number 82
ACOS(config-radius-server)# attribute custom6 cus6 vendor 22610 number 83
ACOS(config-radius-server)# accounting start replace-entry
ACOS(config-radius-server)# accounting interim-update replace-entry
ACOS(config-radius-server)# cgnv6 nat pool PB_POOL 1.1.1.2 1.1.1.3 netmask
/24 port-batch-v2-size 128
ACOS(config)# cgnv6 lsn logging pool PB_POOL template lsn_logging
ACOS(config)# cgnv6 lsn-lid 1
```

```
ACOS (config-lsn-lid) #source-nat-pool PB_POOL
```

For samples of RADIUS logging message in different formats, see [RADIUS Message Formats](#).

## RADIUS Message Handling

RADIUS is primarily configuration driven and consists of a “message type” and an “action” that is taken based on the message type. The actions are controlled via user configuration.

With the use of RADIUS messaging, it helps to maintain the user IP or prefix along with the other subscriber information such as MSISDN, IMEI, IMSI etc. Such information is used for logging to provide usage visibility and ensure government compliance. RADIUS messages comprises of a “message type” and an associated “action” to be taken. If the device is configured as a dual-stack deployment, then an IPv4 or an IPv6 address can be assigned and associated with the RADIUS attributes.

The following RADIUS message types are supported:

- START
- STOP
- INTERIM-UPDATE
- ON

The corresponding actions are:

- Append RADIUS attributes
- Replace RADIUS entry
- Delete RADIUS entry
- Delete RADIUS entry and the corresponding data sessions
- Delete RADIUS entries that match the attribute received in the packet or
- Ignore the message

The status is obtained from the packet after parsing, and the action is specified in the configuration.

The following list summarizes a mapping of RADIUS message types to possible actions:

- **START** - Append RADIUS attributes (default), Replace entry, or Ignore.
  - The default action for the START message is Append Entry. When ACOS receives a START message for an inside user with some attributes, followed by another START for the same inside user, new attributes will be appended, and existing attributes will be overwritten. If there is no existing RADIUS entry, a new entry will be created.

For example:

```
ACOS(config)#system radius server
ACOS(config-radius-server)#accounting start append-entry
```

- Replace Entry must be explicitly configured. When ACOS receives a START message, with an existing entry for the same inside user is found, the old entry will be deleted, and a new entry is created with the attributes received.

---

**NOTE:** Any existing session will not be deleted. If there is no existing RADIUS entry, a new one will be created.

---

For example:

```
ACOS(config)#system radius server
ACOS(config-radius-server)#accounting start replace-entry
```

- If Ignore is configured, ACOS will not process the packet with a START message. The RADIUS request will be dropped.

For example:

```
ACOS(config)#system radius server
ACOS(config-radius-server)#accounting start ignore
```

- **STOP** - Delete RADIUS entry (default), Delete entry and with sessions or Ignore.
  - The default action for STOP message is Delete Entry. When ACOS receives a STOP message with an IPv4 or an IPv6 address, the RADIUS entry is removed. The data sessions for the corresponding user will still reside on ACOS.

---

**NOTE:** If the RADIUS entry is deleted before the user data sessions end, this might cause RADIUS attributes missing in CGN logs. To prevent this, configure “Delete radius attributes and corresponding data sessions”.

---

For example:

```
ACOS(config)#system radius server
ACOS(config-radius-server)#accounting stop delete-entry
```

- To remove the RADIUS entry and the data sessions associated with the inside user, configure Delete radius attributes and corresponding data sessions.

For example:

```
ACOS(config)#system radius server
ACOS(config-radius-server)#accounting stop delete-entry-and-sessions
```

When ACOS receives a STOP message with an IPv4 or an IPv6 address, the RADIUS entry will be removed and any session for the inside user is scheduled to be deleted. The deletion is done via a background task. Considering the number of associated sessions, it can take up to 2 minutes for all the matching sessions to be deleted.

When ACOS receives a STOP message with either IPv4 or IPv6 address (but not both), with the START message (or a subsequent INTER-UPDATE message) received having both IPv4 and IPv6 address, sessions matching either of the IP addresses will be deleted.

- If Ignore is configured, ACOS will ignore and drop the packets with a STOP message.

For example:

```
ACOS(config)#system radius server
ACOS(config-radius-server)#accounting stop ignore
```

- INTERIM-UPDATE - Ignore (default), Append or Replace RADIUS attributes.
  - The default action for INTERIM-UPDATE is Ignore, ACOS ignores the packets with an INTERIM-UPDATE message. No processing is done, the RADIUS message is

ignored and dropped.

For example:

```
ACOS(config)#system radius server
ACOS(config-radius-server)#accounting interim-update ignore
```

- Alternatively, Append Entry can be configured to update the attributes in the entry. If an entry is not present, ACOS creates an entry with the insider user IP received in the packet.

For example:

```
ACOS(config)#system radius server
ACOS(config-radius-server)#accounting interim-update append-entry
```

- Replace entry is configured to remove the existing entry and create a new entry with the attributes received. If no corresponding entry is present, ACOS creates a new entry.

```
ACOS(config)#system radius server
ACOS(config-radius-server)#accounting interim-update replace-entry
```

- ON - Ignore (default), delete RADIUS entries that match attribute received.
  - The default action for ON is Ignore. No processing is done, and ACOS ignores and drops the RADIUS message.

```
ACOS(config)#system radius server
ACOS(config-radius-server)#accounting on ignore
```

- Alternatively, delete entries using matching received attribute can be configured to remove all the entries that match an attribute sent in the packet.

```
ACOS(config)#system radius server
ACOS(config-radius-server)#accounting on delete-entries-using-attribute
```

## Including Byte Count and Duration

For the Port Batch version 2, when a new port batch is allocated and when the port batch is freed, you can choose to receive interim log messages.

The log messages for interim update is the same as the Port Batch Allocated log message. In addition to the Port Batch Allocated log messages, you can include the uploaded bytes, downloaded bytes, and the duration for which the port batch is allocated to the subscriber. These attributes can be included for default, custom, compact, binary, and radius formats.

By default, the byte counts and the duration of port allocation are not included in the logging messages. To include the port batch upload bytes, download bytes, and the duration, use the `include-port-block-account` at the configuration level for the LSN or Fixed NAT logging template.

```
ACOS(config)# cgnv6 template logging log
ACOS(config-logging:log)# log sessions
ACOS(config-logging:log)# include-port-block-account
ACOS(config-logging:log)# rule port-mappings interim-update 15
ACOS(config-logging:log)# log-receiver radius secret 123456
ACOS(config-logging:log)# service-group sg_udp
```

To include the upload and download byte count in the Port Batch V2 Interim Update logs with a custom format (i.e. rfc-custom and custom), the keywords “`$ul-byte$`” and “`$dl-byte$`” must be included in the custom message.

```
ACOS(config)# cgnv6 template logging log
ACOS(config-logging:log)# log sessions
ACOS(config-logging:log)# include-port-block-account
ACOS(config-logging:log)# rule port-mappings interim-update 15
ACOS(config-logging:log)# log-receiver radius secret 123456
ACOS(config-logging:log)# service-group sg_udp
ACOS(config-logging:log)# format custom
ACOS(config-logging:log)# custom message port-batch-v2-allocated "BATCH-C
$proto-name$ $src-ip$ $nat-ip$ $nat-port-start$ $nat-port-end$"
ACOS(config-logging:log)# custom message port-batch-v2-freed "BATCH-F
$proto-name$ $src-ip$ $nat-ip$ $nat-port-start$ $nat-port-end$"
ACOS(config-logging:log)# custom message port-batch-v2-interim-update
"INTERIM $proto-name$ $src-ip$ $nat-ip$ $nat-port-start$ $nat-port-end$
$ul-byte$ $dl-byte$"
```

The port batch upload and download bytes are displayed in the Port Batch v2 Allocated and Freed messages. The duration of port batch allocated is displayed in the Port Batch v2 Interim-Update and Port Batch Freed messages.

For log message examples, see [Appendix: Log Message References](#).

## Handling STOP and START RADIUS Log Entries

If ACOS is configured with accounting STOP delete-entry-and-session, the following occurs:

1. ACOS receives a STOP message from GGSN.
2. ACOS marks the existing user quota session as unusable and blocks creating new sessions from that NAT IP.
3. Based on the RADIUS values (that is, Framed IP address – Inside IP), ACOS deletes the RADIUS attribute entry and all active sessions from session table for this Inside IP.
4. ACOS then generates the Delete Session Log containing RADIUS attributes for all sessions.

Sometimes, while clearing the active sessions, another new START message can be sent to the same private IP. To distinguish old sessions from new data sessions, ACOS uses a different NAT IP for the new subscriber requests.

When a new START message is received, ACOS creates a new user quota session with a different NAT IP and starts processing the traffic for the new subscriber. In parallel, ACOS continues to clear the data sessions for the old subscriber.

The following is an example of how the logs are handled for RADIUS STOP and START messages:

- ACOS receives a RADIUS START message for an inside user IPv4-100.64.0.1 (can be IPv6) at 00:50:00:10 (Hr:min:sec:msec) and creates an entry in the RADIUS table with MSISDN +919898989898.
- ACOS creates data sessions with NAT IP 12.12.12.1 for IPv4-100.64.0.1, and logs session create/delete with MSISDN +919898989898.
- ACOS receives RADIUS STOP message from GGSN at 01.01.01.01 for the same Inside IPv4 100.64.0.1 with MSISDN +919898989898 for an existing entry. ACOS blocks new sessions for IPv4 100.64.0.1 and starts clearing all data sessions which has NAT IP 12.12.12.1. ACOS also logs session delete event with MSISDN +919898989898.

- ACOS receives RADIUS START message at 01.01.01.02.105 for the same IPv4 100.64.0.1 for different MSISDN +918989898989. ACOS unblocks new sessions for IPv4 100.64.0.1 and continues clearing old data sessions which has NAT IP 12.12.12.1.
- ACOS creates data sessions with the new NAT IP 12.12.12.2 for IPv4-100.64.0.1 and continues clearing old data sessions which has NAT IP 12.12.12.1.
- ACOS uses MSISDN +919898989898 for sessions with NAT IP 12.12.12.1 and MSISDN +918989898989 for sessions with NAT IP 12.12.12.2.
- All data sessions with NAT IP 12.12.12.1 are cleared. ACOS frees the old RADIUS entry from the system.

## Limitations

- A maximum number of 10 NAT IPs can be reused in a short time for new subscribers using the same private IP. Also, the reuse is limited by the number of NAT IPs in the NAT pool. For example, if a NAT pool has two NAT IPs, the private IP can be reused twice in a short time.
- This feature is supported for LSN only. It is not support for fixed NAT.
- If the same private IP is reused before deleting all old data sessions, the new user's packet may match old user's session. In this case, the packet that is still using the old session is forwarded to the new subscriber. Simultaneously, the old session is cleared soon and a new session is created.
- If the new user's traffic flow matches a full-cone session created by the old user, the traffic is dropped immediately. Only when the old full-cone session is deleted, a new user can create a new full-cone session or data session.

# CGN Traffic Logging with L3V Partitions

---

The following topics are covered:

<a href="#">Overview of CGN Traffic Logging with L3V Partitions</a> .....	216
<a href="#">Separate Routing for Logging Servers</a> .....	216
<a href="#">Service Group Sharing</a> .....	217
<a href="#">Partition Name Logging</a> .....	218
<a href="#">Configuration Example</a> .....	220

## Overview of CGN Traffic Logging with L3V Partitions

ACOS includes support for CGN logging in L3V multi-tenancy deployments. Each L3V partition can have its own CGN logging templates. Partitions also can have their own service groups of log servers or use a service group configured in the shared partition.

The same configuration commands supported in the shared partition for CGN logging also are supported in L3V partitions.

The following deployment scenarios are supported.

- Multiple partitions without inter-partition routing:
  - Service group of logging servers and the CGN logging template both are configured in the L3V partition, for logging traffic for CGN clients attached to the partition.
  - Service group of logging servers is configured in the shared partition, and shared with specific L3V partitions. Within each of those L3V partitions, a logging template is configured. Each of those logging templates uses the service group in the shared partition.
- Multiple partitions with inter-partition routing: logging template and service group for inter-partition traffic both are in the shared partition.

## Separate Routing for Logging Servers

In order to utilize separate routing tables for CGN log servers, ACOS uses a separate VRF/L3V instance for the CGN logging servers. This also enables system logs to be routed from different partitions. Shared or L3V partition can refer to the CGN log servers/system log servers from other partitions. The any-to-any mapping capability allows any given partition to be mapped to the CGN log servers from any other partition.

From a L3V partition, any other partition can also be referenced. From a shared partition, only allowed L3V partition can be referenced.

### CLI Example

To configure separate routing for CGN LSN logging partition, enter the following command:

```
ACOS (config) # cgnv6 lsn logging partition p1
```

To configure for a host partition, enter the following command:

```
ACOS (config) # logging host partition p1
```

### Configuration Notes

- When configuring a syslog server to which to send event messages, use the `logging host partition shared` option to use the server configured in the shared partition as the preferred syslog server.
- When configuring a syslog server to which to send event messages, use the `logging host partition p1` option to use the server configured in the “p1” partition as the preferred syslog server.
- When logging CGN traffic under a L3V partition and to enable CGN logs to be routed from the shared partition, use the `cgnv6 lsn logging partition p1` command.
- When assigning a separate L3V instance for the CGN logging servers and to enable CGN logs to be routed from the “p1” partition, use the `cgnv6 lsn logging partition p1` option.
- If `cgnv6 logging partition` is configured, do not configure `cgnv6 default logging template`, vice versa.

## Service Group Sharing

For deployments without inter-partition routing, L3V partitions can use a service group of logging servers configured in the shared partition. In this case, some additional configuration options are required:

- Service-group configuration – The service group is configured in the shared partition. In the configuration of the shared service group, you must explicitly enable sharing of the group, and specify the partition group or individual partition allowed to use the group.

- Logging template configuration – The logging templates are configured in the L3V partitions. Each partition configured to perform CGN for its clients has its own logging template, which refers to the service group in the shared partition.

Configuration examples for each deployment option are provided later in this section.

## Partition Name Logging

By default, L3V partition names are not included in log messages. To include the partition names, use the `include-partition-name` command at the configuration level for the logging template. For example:

```
ACOS(config)# cgnv6 template logging lsn_logging  
ACOS(config-logging:lsn_logging)# include-partition-name
```

You can enable ACOS to insert the L3V partition name in CGN traffic log messages. Partition-name insertion is supported for all the following log formats:

- ASCII
- RFC 5424
- Compact
- Binary
- CEF
- RADIUS

Partition-name insertion is disabled by default. You can enable it at the configuration level for individual logging templates. After you enable partition-name insertion, the partition name appears as described below.

### ASCII Format:

The partition name is inserted into the Syslog header. For example:

```
AX/partition-name NAT-UDP-C: 192.168.1.1:20001<--> 203.0.210.1:80,  
203.0.210.1:80<-->203.0.113.1:20001
```

### RFC 5424 Format:

The partition name is inserted into the spare PROCID field in the syslog header. For example:

```
1 2012-04-19T05:54:14-07:00 192.168.147.167 AX2600 partition-name  
SessionCreated:TCP [- 3.3.3.50 26548 6.6.6.50 80 - 6.6.6.50 80 6.6.6.200  
12218]
```

### Compact Format:

The partition name is inserted in the Syslog header. For example:

```
AX/partition-name UC: 64646464:2710->96969696:2710
```

### Binary Format:

The partition name is carried in a logging extension:

Type: 6, Length: 8 bits; Value: partition-name string

Extension headers in binary messages appear in the following order.

1. Destination IP address
2. MSISDN
3. IMEI
4. IMSI
5. Inside MAC address
6. Partition name

If only some extensions are enabled, the enabled options appear in the same order, but without the disabled options.

### RADIUS Format:

The partition name is carried as a value for the following attribute:

```
A10-Admin-Partition
```

## Configuration Example

The following commands configure a service group of logging servers in the shared partition, then configure logging templates in some L3V partitions (“pp1” and “pp2” in this example) to use the service group in the shared partition.

### Partition group configuration (optional)

This example assumes the L3V partitions and admin accounts for them already are configured. However, to share a service group with more than one partition, a partition group is needed.

The following commands are entered in the shared partition, to create a partition group. All the partitions that will need to share the service group configured in the shared partition are added to the group.

```
ACOS (config) # partition pp1 id 1  
ACOS (config-partition:pp1) # exit  
ACOS (config) # partition pp2 id 2  
ACOS (config-partition:pp2) # exit  
ACOS (config) # partition-group pp-cgn  
ACOS (config-partition-group:pp-cgn) # member pp1  
ACOS (config-partition-group:pp-cgn) # member pp2  
ACOS (config-partition-group) # exit
```

### Service group configuration:

The following commands are entered in the shared partition, to configure the logging servers and service group:

```
ACOS (config) # cgnv6 server syslog1 203.0.118.1  
ACOS (config-real server) # port 514 udp  
ACOS (config-real server-node port) # cgnv6 service-group cgn-syslog udp  
ACOS (config-cgnv6 svc group) # member syslog1 514  
ACOS (config-cgnv6 svc group) # shared group pp-cgn  
ACOS (config-cgnv6 svc group) # end
```

The **shared** command enables sharing of the service group with other partitions.

## CGN logging template configuration in L3V partition “pp1”

The following commands change the CLI to partition “pp1”, access the global configuration level, and configure a CGN logging template:

```
ACOS# active-partition pp1
Currently active partition: pp1
ACOS[pp1]# configure
ACOS[pp1] (config)# cgnv6 template logging cgn-logging-tmplt
ACOS[pp1] (config-logging:cgn-logging-tmplt)# service-group cgn-syslog
shared
ACOS[pp1] (config-logging:cgn-logging-tmplt)# include-partition-name
```

The **service-group** command specifies the service-group name. The **partition shared** option indicates that the service group is configured in the shared partition.

## CGN logging template configuration in L3V partition “pp2”:

The following commands change the CLI to partition “pp2”, access the global configuration level, and configure a CGN logging template:

```
ACOS[pp1] (config-logging:cgn-logging-tmplt)# end
ACOS[pp1]# active-partition shared
Currently active partition: shared
ACOS# active-partition pp2
Currently active partition: pp2
ACOS[pp2]# configure
ACOS[pp2] (config)# cgnv6 template logging cgn-logging-tmplt
ACOS[pp2] (config-logging:cgn-logging-tmplt)# service-group cgn-syslog
partition shared
ACOS[pp2] (config-logging:cgn-logging-tmplt)# include-partition-name
```

# Appendix: Log Message References

---

This section describes how to configure logs.

The following topics are covered:

<a href="#">LSN Traffic Logs</a> .....	223
<a href="#">Additional Client Information Log Samples</a> .....	232
<a href="#">Fixed-NAT Log Samples</a> .....	239
<a href="#">DDoS Protection Log Samples</a> .....	246
<a href="#">One-to-One NAT Log Samples</a> .....	247
<a href="#">Default Message Strings for RFC 5424</a> .....	249
<a href="#">Binary Logging Format Reference</a> .....	257
<a href="#">Traffic Logs in CEF Format</a> .....	285
<a href="#">RADIUS Message Formats</a> .....	288
<a href="#">Port Batch Log Messages</a> .....	301

## LSN Traffic Logs

For information on logging overview and logging formats, see [External Logging Overview](#).

[Table 16](#) lists the LSN traffic logs that can be generated.

Table 16 : LSN Traffic Logs

Event	Message String Format
<b>LSN Session Logs</b>	
ICMP data session created	<i>ACOS_hostname NAT-ICMP-N: fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
TCP data session created	<i>ACOS_hostname NAT-TCP-N: fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
UDP data session created	<i>ACOS_hostname NAT-UDP-N: fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
RTSP data session created	<i>ACOS_hostname NAT-RTP-C: fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
ICMP data session deleted	<i>ACOS_hostname NAT-ICMP-D: fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
TCP data session deleted	<i>ACOS_hostname NAT-TCP-D: fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
UDP data session deleted	<i>ACOS_hostname NAT-UDP-D: fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
RTSP data session deleted	<i>ACOS_hostname NAT-RTP-D: fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>

Table 16 : LSN Traffic Logs

Event	Message String Format
<b>LSN Port Mapping Logs</b>	
LSN port mapping created for ICMP	<p><i>ACOS_hostname NAT-ICMP-C: inside_ip:inside_port&lt;--&gt;nat_ip:nat_port</i>  <i>to dest_ip:dest_port</i></p> <p><b>Note:</b> In this message and the other port mapping creation messages, the destination (<i>to dest_ip:dest_port</i>) is not included in the message by default. You can enable the destination to be included when you configure LSN external logging.</p>
LSN port mapping created for TCP	<p><i>ACOS_hostname NAT-TCP-C: inside_ip:inside_port&lt;--&gt;nat_ip:nat_port</i>  <i>to dest_ip:dest_port</i></p>
LSN port mapping created for UDP	<p><i>ACOS_hostname NAT-UDP-C: inside_ip:inside_port&lt;--&gt;nat_ip:nat_port</i>  <i>to dest_ip:dest_port</i></p>
LSN port mapping created for RTSP	<p><i>ACOS_hostname NAT-RTP-C: inside_ip:inside_port&lt;--&gt;nat_ip:nat_port</i>  <i>to dest_ip:dest_port</i></p>
LSN port mapping for ICMP freed	<p><i>ACOS_hostname NAT-ICMP-F: inside_ip:inside_port&lt;--&gt;nat_ip:nat_port</i></p>
LSN port mapping for TCP freed	<p><i>ACOS_hostname NAT-TCP-F: inside_ip:inside_port&lt;--&gt;nat_ip:nat_port</i></p>
LSN port mapping for UDP freed	<p><i>ACOS_hostname NAT-UDP-F: inside_ip:inside_port&lt;--&gt;nat_ip:nat_port</i></p>
LSN port mapping for RTSP freed	<p><i>ACOS_hostname NAT-RTP-F: inside_ip:inside_port&lt;--&gt;nat_ip:nat_port to dest_ip:dest_port</i></p>
DDoS Entry Created and Deleted	

## NAT Traffic Examples

The following logs indicate the creation and deletion of a UDP session.

```
ACOS NAT-UDP-N: 192.168.1.1:20001<-->203.0.210.1:80, 203.0.210.1:80<-->
203.0.113.1:20001
ACOS NAT-UDP-D: 192.168.1.1:20001<-->203.0.210.1:80, 203.0.210.1:80<-->
203.0.113.1:20001
```

The following logs indicate the creation and freeing of an LSN port mapping for UDP.

```
ACOS NAT-UDP-C: 192.168.1.1:20001 -> 203.0.113.1:20001 to 203.0.210.1:80
ACOS NAT-UDP-F: 192.168.1.1:20001 -> 203.0.113.1:20001
```

Here is an example of the full string for a log:

```
196 LOCAL0.DEBUG: Nov 8 02:15:00 ACOS NAT-TCP-C: 61.1.1.107:54503 ->
60.1.11.167:54503 to 60.1.1.109:22\r\n
```

## NAT64/DNS64 Traffic Logs

[Table 17](#) lists the NAT64/DNS64 traffic logs that can be generated.

Table 17 : NAT64/DNS64 Traffic Logs

Event	Message String Format
NAT64/DNS64 Session Logs	
TCP data session created	<i>NAT-TCP-N: [client_ipv6_addr]:fwd_src_port -&gt; [fwd_dest_ipv6]:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
UDP data session created	<i>ACOS_hostname NAT-UDP-N: [client_ipv6_addr] fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
RTSP data session created	<i>ACOS_hostname NAT-RTP-C: [client_ipv6_addr] fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
ICMP data session deleted	<i>ACOS_hostname NAT-ICMP-D: [client_ipv6_addr] fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>

Table 17 : NAT64/DNS64 Traffic Logs

Event	Message String Format
TCP data session deleted	<i>ACOS_hostname NAT-TCP-D: [client_ipv6_addr] fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
UDP data session deleted	<i>ACOS_hostname NAT-UDP-D: [client_ipv6_addr] fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
RTSP data session deleted	<i>ACOS_hostname NAT-RTP-D: [client_ipv6_addr] fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
<b>NAT64/DNS64 Port Mapping Logs</b>	
LSN port mapping created for ICMP	<i>ACOS_hostname NAT-ICMP-C: [client_ipv6_addr]:inside_port &lt;--&gt;nat_ip:nat_port to [dest_ipv6:]dest_port</i>  <b>Note: In this message and the other port mapping creation messages, the destination (to <i>dest_ip:dest_port</i>) is not included in the message by default. You can enable the destination to be included when you configure LSN external logging.</b>
LSN port mapping created for TCP	<i>NAT-TCP-C: [client_ipv6_addr]:inside_port &lt;--&gt;nat_ip:nat_port to [dest_ipv6:]dest_port</i>
LSN port mapping created for UDP	<i>ACOS_hostname NAT-UDP-C: [client_ipv6_addr]:inside_port &lt;--&gt;nat_ip:nat_port to [dest_ipv6:]dest_port</i>
LSN port mapping created for RTSP	<i>ACOS_hostname NAT-RTP-C: [client_ipv6_addr]:inside_port &lt;--&gt;nat_ip:nat_port to [dest_ipv6:]dest_port</i>
LSN port mapping for ICMP freed	<i>ACOS_hostname NAT-ICMP-F: [client_ipv6_addr]:inside_port &lt;--&gt;nat_ip:nat_port</i>
LSN port mapping for TCP freed	<i>ACOS_hostname NAT-TCP-F: [client_ipv6_addr]:inside_port &lt;--&gt;nat_ip:nat_port</i>
LSN port mapping for UDP freed	<i>ACOS_hostname NAT-UDP-F: [client_ipv6_addr]:inside_port &lt;--&gt;nat_ip:nat_port</i>
LSN port mapping for RTSP freed	<i>ACOS_hostname NAT-RTP-F: [client_ipv6_addr]:inside_port &lt;--&gt;nat_ip:nat_port</i>

## NAT64/DNS64 Examples

The following logs indicate the creation and freeing of a port mapping for TCP. In this example, the client IPv6 address is 2001:abcd::1. The NAT IP address is 1.1.1.1.

```
ACOS NAT-TCP-C: [2001:abcd::1]:54040 -> 1.1.1.1:54040 to
[64:ff9b::ac10:1010]:80
ACOS NAT-TCP-F: [2001:abcd::1]:54040 -> 1.1.1.1:54040
```

## DS-Lite Traffic Logs

[Table 18](#) lists the DS-Lite traffic logs that can be generated.

Table 18 : DS-Lite Traffic Logs

Event	Message String Format
<b>DS-Lite Session Logs</b>	
TCP data session created	<i>ACOS_hostname NAT-TCP-N: [client_ipv6_addr] fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
UDP data session created	<i>ACOS_hostname NAT-UDP-N: [client_ipv6_addr] fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
RTSP data session created	<i>ACOS_hostname NAT-RTP-C: [client_ipv6_addr] fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
ICMP data session deleted	<i>ACOS_hostname NAT-ICMP-D: [client_ipv6_addr] fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
TCP data session deleted	<i>ACOS_hostname NAT-TCP-D: [client_ipv6_addr] fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
UDP data session deleted	<i>ACOS_hostname NAT-UDP-D: [client_ipv6_addr] fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port, rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
RTSP data session deleted	<i>ACOS_hostname NAT-RTP-D: [client_ipv6_addr] fwd_src_ip:fwd_src_port&lt;--&gt;fwd_dest_ip:fwd_dest_port,</i>

Table 18 : DS-Lite Traffic Logs

Event	Message String Format
	<i>rev_src_ip:rev_src_port&lt;--&gt;rev_dest_ip:rev_dest_port</i>
<b>DS-Lite Port Mapping Logs</b>	
Port mapping created for ICMP	<p><i>ACOS_hostname NAT-ICMP-C: [client_ipv6_addr] inside_ip:inside_port&lt;--&gt;nat_ip:nat_port to dest_ip:dest_port</i></p> <p><b>Note:</b> In this message and the other port mapping creation messages, the destination (<i>to dest_ip:dest_port</i>) is not included in the message by default. You can enable the destination to be included when you configure LSN external logging.</p>
Port mapping created for TCP	<i>ACOS_hostname NAT-TCP-C: [client_ipv6_addr] inside_ip:inside_port&lt;--&gt;nat_ip:nat_port to dest_ip:dest_port</i>
Port mapping created for UDP	<i>ACOS_hostname NAT-UDP-C: [client_ipv6_addr] inside_ip:inside_port&lt;--&gt;nat_ip:nat_port to dest_ip:dest_port</i>
Port mapping created for RTSP	<i>ACOS_hostname NAT-RTP-C: [client_ipv6_addr] inside_ip:inside_port&lt;--&gt;nat_ip:nat_port to dest_ip:dest_port</i>
Port mapping for ICMP freed	<i>ACOS_hostname NAT-ICMP-F: [client_ipv6_addr] inside_ip:inside_port&lt;--&gt;nat_ip:nat_port</i>
Port mapping for TCP freed	<i>ACOS_hostname NAT-TCP-F: [client_ipv6_addr] inside_ip:inside_port&lt;--&gt;nat_ip:nat_port</i>
Port mapping for UDP freed	<i>ACOS_hostname NAT-UDP-F: [client_ipv6_addr] inside_ip:inside_port&lt;--&gt;nat_ip:nat_port</i>
Port mapping for RTSP freed	<i>ACOS_hostname NAT-RTP-F: [client_ipv6_addr] inside_ip:inside_port&lt;--&gt;nat_ip:nat_port</i>

## DS-Lite Examples

The following logs indicate the creation and deletion of a UDP session.

```
ACOS NAT-UDP-N: [2001:10::100]192.168.1.1:20001<-->203.0.210.1:80,
203.0.210.1:80<--> 203.0.113.1:20001
ACOS NAT-UDP-D: [2001:10::100]192.168.1.1:20001<-->203.0.210.1:80,
203.0.210.1:80<--> 203.0.113.1:20001
```

The following logs indicate the creation and freeing of a port mapping for UDP.

```
ACOS NAT-UDP-C: [2001:10::100]192.168.1.1:20001 -> 203.0.113.1:20001 to
203.0.210.1:80
ACOS NAT-UDP-F: [2001:10::100]192.168.1.1:20001 -> 203.0.113.1:20001
```

## NAT64 Examples

The following logs are ICMP messages indicating the creation and deletion of a NAT session.

```
ACOS NAT-ICM-N: [2222:2222:2222:2222::3]:8989<-->[3333::1111:1165]:0,
17.17.17.101:0
<-->17.17.17.205:8989
ACOS NAT-ICM-D: [2222:2222:2222:2222::3]:8989<-->[3333::1111:1165]:0,
17.17.17.101:0
<-->17.17.17.205:8989
```

The following logs are ICMP messages indicating the creation and freeing of a NAT session.

```
ACOS NAT-ICM-C: [2222:2222:2222:2222::3]:8989 -> 17.17.17.205:8989 to
[3333::1111:1165]:0
ACOS NAT-ICM-F: [2222:2222:2222:2222::3]:8989 -> 17.17.17.205:8989
```

Here are some messages for UDP without Port Batching:

```
ACOS NAT-UDP-C: [2222:2222:2222:2222::3]:4427 -> 17.17.17.205:4427 to
[3333::1111:1165]:5353#
ACOS NAT-UDP-N: [2222:2222:2222:2222::3]:4427<-->[3333::1111:1165]:5353,
17.17.17.101:5353<-->17.17.17.205:4427
ACOS NAT-UDP-D: [2222:2222:2222:2222::3]:4427<-->[3333::1111:1165]:5353,
17.17.17.101:5353<-->17.17.17.205:4427
ACOS NAT-UDP-F: [2222:2222:2222:2222::3]:4427 -> 17.17.17.205:4427
```

Here are some messages for TCP with Port Batching:

```
ACOS NAT-TCP-B: [2222:2222:2222:2222::3] -> 17.17.17.205:1041,1024,21
ACOS NAT-TCP-N: [2222:2222:2222:2222::3]:52722<-->[3333::1111:1165]:80,
17.17.17.101:80<-->17.17.17.205:1041
ACOS NAT-TCP-D: [2222:2222:2222:2222::3]:52722<-->[3333::1111:1165]:80,
17.17.17.101:80<-->17.17.17.205:1041
ACOS NAT-TCP-X: [2222:2222:2222:2222::3] -> 17.17.17.205:1041,1024,21
```

## Merged Session Log Samples

For details on how to configure merged session log, see [Merged Session Log](#).

Below are some sample outputs of merged session logs:

### Compact Logging

A sample compact log message with a merged session creation and session deletion is shown below:

```
LOCAL0.DEBUG: Sep 18 14:25:18.68 Sep 18 14:25:22.68 AX3030 I:  
5101016b:37d6-5001016e:0, 5001016e:0-5001011f:37d6
```

### Default Logging

A sample default log message with a merged session creation and session deletion is shown below:

```
LOCAL0.DEBUG: Sep 18 14:25:36.67 Sep 18 14:25:40.66 AX3030 NAT-ICM:  
81.1.1.107:14296<-->80.1.1.110:0, 80.1.1.110:0<-->80.1.1.31:14296
```

### RFC5424 Logging

A sample RFC5424 log message with a merged session creation and session deletion is shown below:

```
LOCAL0.DEBUG: 1 2014-09-18T14:25:45.22+01:00 2014-09-18T14:25:51.22+01:00  
192.168.105.132 AX3030 - SessionDeleted:ICMP [- 81.1.1.107 14297 -  
80.1.1.110 0 - 80.1.1.110 0 - 80.1.1.31 14297]
```

### Custom Logging

A sample custom log message, using the NAT logging template custom header for syslog messages, with a merged session creation and session deletion is shown below:

```
LOCAL0.DEBUG: 1 2014-09-18T14:25:27.83+01:00 2014-09-18T14:25:31.83+01:00  
192.168.105.132 AX3030 - Session:ICMP 81.1.1.107:14295 80.1.1.110:0
```

## Binary Logging

For Binary log messages, the session creation timestamp is added to a session deletion log as an extension.

[Figure 6](#) is an example of a binary log message:

**Figure 6 : Binary Log Messages:**

```
Log_Message
  Ext_Bit: EXT_BIT_SET (1)
  Log_Msg_Type: NAT_LOGGING_SESSION (1)
  Timestamp: 2014/09/18 13:24:55.036 UTC (1411046695360)
  Log_Msg_Length: 52
  Session_Log
    Action: SESSION_DELETE (1)
    Protocol: ICMP (3)
    Type: LSN (0)
    Length: 30
    LSN_Session
      Fwd_Tuple
        Tuple_Type: TUPLE_IPV4 (0)
        Src_Addr: 81.1.1.107 (1359020395)
        Dest_Addr: 80.1.1.110 (1342243182)
        Src_Port: 14293
        Dest_Port: 0
      Rev_Tuple
        Tuple_Type: TUPLE_IPV4 (0)
        Src_Addr: 80.1.1.110 (1342243182)
        Dest_Addr: 80.1.1.31 (1342243103)
        Src_Port: 0
        Dest_Port: 14293
  Extensions
    Type: NAT_LOG_EXT_TYPE_SESSION_CREATED_TIME (21)
    Length: 11
    Timestamp: 2014/09/18 13:24:51.036 UTC (1411046691364)
```

## Radius Logging

For Radius log messages, the session creation timestamp is added after the session information in the Radius request.

[Figure 7](#) is an example of Radius logging messages.

**Figure 7 : Radius Log Messages**

```

RADIUS Protocol
Code: Accounting-Request (4)
Packet identifier: 0x7d (125)
Length: 140
Authenticator: 0aa0a689aa37f2ad0e3ee09095c2af4b
Attribute Value Pairs
  AVP: l=6 t=Acct-Status-Type(40): Stop(2)
    Acct-Status-Type: Stop (2)
  AVP: l=18 t=Acct-Session-Id(44): :\317\001\250\213\315\036\222(F\ag+F\ag
  AVP: l=26 t=NAS-Identifier(32): AX3030-C@192.168.105.131
  AVP: l=70 t=Vendor-Specific(26) v=Raksha Networks Inc.(22610)
    VSA: l=6 t=A10-CGN-Timestamp(6): Mar 30, 2017 04:51:08.000000000
    VSA: l=6 t=A10-CGN-Protocol(7): ICMP(3)
    VSA: l=6 t=A10-CGN-Action(20): Session-Deleted(4)
    VSA: l=6 t=A10-CGN-Inside-Addr(10): 111.2.1.10
    VSA: l=4 t=A10-CGN-Inside-Port(11): 18788
    VSA: l=6 t=A10-CGN-Dest-Addr(14): 188.2.1.89
    VSA: l=4 t=A10-CGN-Dest-Port(15): 0
    VSA: l=6 t=A10-CGN-NAT-Addr(12): 177.88.66.1
    VSA: l=4 t=A10-CGN-NAT-Port(13): 18788
    VSA: l=6 t=A10-CGN-NAT-Dest-Addr(16): 188.2.1.89
    VSA: l=4 t=A10-CGN-NAT-Dest-Port(17): 0
  AVP: l=6 t=A10-CGN-Session-Created-Timestamp(57): Mar 30, 2017 04:51:05.000000000
    A10-CGN-Session-Created-Timestamp: Mar 30, 2017 04:51:05.000000000

```

## Additional Client Information Log Samples

For information on how to configure client information in logs, see [Including Additional Client Information in Logs](#).

## Additional Client Information

Here are some examples of traffic log messages that include the client mobile number and, in the last example, HTTP request information.

### Creation of UDP Port Mapping

The following message indicates creation of a UDP port mapping for the mobile client with number “0123456789”:

```

Mar 8 15:13:35 ACOS1 NAT-UDP-C: [2001:10::100]192.168.1.1:20001 ->
203.0.113.1:20001 to 203.0.210.1:80 MSISDN=0123456789\r\n

```

## Client MSISDN Number Included in Log

The following message indicates that a TCP data session was created for a client whose mobile number is 012-345-6789:

```
Mar 8 15:13:35 ACOS1 NAT-TCP-N: 30.30.30.237:44750<-->40.40.40.5:80,  
40.40.40.5:80<-->40.40.40.106:15900 MSISDN=0123456789\r\n
```

## Client HTTP Request Information Included in Log

The following message indicates that the client with mobile number 012-345-6789 sent an HTTP request to “www.a10.networks.com”:

```
Mar 8 15:13:35 ACOS1 HTTP: MSISDN=0123456789 RM=GET  
URL=http://www.a10networks.com/about/index.php\r\n
```

## HTTP Headers

---

### ASCII (the default format)

The following example shows an HTTP request, and a log message that includes information from the request.

HTTP request from client:

```
GET / HTTP/1.1  
Host: www.a10networks.com  
User-Agent: Mozilla/5.0 Gecko/20100101 Firefox/22.0  
Cookie: A=123; B=456  
Connection: keep-alive
```

Message sent to log server:

Here is the message CGN sends to the log server, to log the request. In this example, ACOS is configured to log the User-Agent and Cookie headers.

```
Aug 16 04:28:51 AX3000 HTTP: 10.225.3.2:38695<-->40.0.0.1:80,  
40.0.0.1:80<-->1.1.3.182:38695 URL=http://www.a10networks.com/^_ User-  
Agent=Mozilla/5.0 Gecko/20100101 Firefox/22.0^_ Cookie=A=123; B=456
```

The HTTP headers are highlighted in blue in this example. The delimiter used by ACOS in ASCII log strings is “ ^\_ ” (an ASCII 31 character and a space), highlighted by green in the example.

If all the information about an HTTP request does not fit in one log message, ACOS sends the information in multiple messages. To allow easy identification of all the separate messages for a request, you can enable tagging of each message with an HTTP request ID. This is a number that ACOS adds to each message related to a given HTTP request.

The following example shows multiple log message for the same request shown above. Each message includes a request ID.

Messages sent to log server:

```
Aug 16 04:28:51 AX3000 HTTP: 10.225.3.2:38695<-->40.0.0.1:80,  
40.0.0.1:80<-->1.1.3.182:38695 Q=1 URL=http://www.a10networks.com/^_ $User-  
Agent=Mozilla/5.0 Gecko/20100101 Firefox/22.0^_  
Aug 16 04:28:51 AX3000 HTTP: 10.225.3.2:38695<-->40.0.0.1:80,  
40.0.0.1:80<-->1.1.3.182:38695 Q=1 Cookie=A=123; B=456^_
```

In ASCII log messages, the request ID is listed by the “Q=” field. In this example, the request ID for each log message is 1. Each of these messages is about the same HTTP request.

Use of HTTP request IDs is optional and is disabled by default.

## Compact

Here is are some message in Compact format, that report the same HTTP request information shown in the ASCII example above.

```
Aug 16 04:28:51 AX3000 H: 1e1e1e0a:be75-28282801:50, 28282801:50-  
2828286b:be75 Q=1 U=http://www.a10networks.com/^_ T=Mozilla/5.0  
Gecko/20100101 Firefox/22.0^_  
Aug 16 04:28:51 AX3000 H: 1e1e1e0a:be75-28282801:50, 28282801:50-  
2828286b:be75 Q=1 C=A=123; B=456^_
```

For the Opcodes for HTTP headers, see [Table 1](#).

## RFC 5424

**NOTE:** The current release does not support HTTP header logging using RFC 5424 format.

## Binary

See [\(ACOS 2.8.0 and earlier\)](#) and [\(ACOS 2.8.1 and later\)](#).

## Custom

For details on Custom logging format, see [Custom Logging Format](#).

## CEF

For details on CEF, see [CEF Logging Format](#).

## RADIUS

To include HTTP request information in traffic logs sent to a RADIUS server used for CGN traffic logging, use the following attribute values in the accounting-request messages sent to the traffic logging server:

ATTRIBUTE	A10-CGN-Request-Size	45	integer
ATTRIBUTE	A10-CGN-Response-Size	46	integer
ATTRIBUTE	A10-CGN-HTTP-Request-Number	47	integer
ATTRIBUTE	A10-CGN-HTTP-Cookie	48	string
ATTRIBUTE	A10-CGN-HTTP-Referer	49	string
ATTRIBUTE	A10-CGN-HTTP-User-Agent	50	string
ATTRIBUTE	A10-CGN-HTTP-Header1	51	string
ATTRIBUTE	A10-CGN-HTTP-Header2	52	string
ATTRIBUTE	A10-CGN-HTTP-Header3	53	string

Attributes 51, 52, and 53 are for the custom header values that you can configure using the information provided later in this section.

## Client MAC

The following sections describe and show examples of how client MAC information appears in each logging format.

### ASCII

ASCII format is the default IPv6 Migration logging format. If client MAC insertion is enabled, the MAC address is appended to the end of the message.

Example:

```
0000 00 0c 29 73 1c 47 00 1f a0 04 ba 4c 08 00 45 00 ..)s.G.. ...L..E.
0010 00 7d 86 ac 00 00 40 11 d3 ab 08 08 08 01 08 08 .)....@. ....
0020 08 08 02 02 02 02 00 69 55 21 3c 31 33 35 3e 20 .....i U|<135>
0030 4d 61 79 20 33 30 20 30 38 3a 34 34 3a 31 38 20 May 30 0 8:44:18
0040 41 58 32 35 30 30 20 4e 41 54 2d 49 43 4d 2d 43 AX2500 N AT-ICM-C
0050 3a 20 33 2e 33 2e 33 2e 32 35 3a 35 37 30 31 20 : 3.3.3. 25:5701
0060 2d 3e 20 31 35 2e 31 35 2e 31 35 2e 35 30 3a 35 -> 15.15.15.50:5
0070 37 30 31 20 4d 41 43 3a 30 30 3a 35 30 3a 35 36 701 MAC: 00:50:56
0080 3a 30 64 3a 30 30 3a 35 32 0d 0a :0d:00:5 2..
```

### RFC 5424

If the default message strings are used, and client MAC insertion is enabled, the MAC address is appended to the end of the message.

Custom messages also can include the inside client MAC option. If the MAC option is not configured in the logging template, the MAC address appears as a blank in the custom string.

Example:

```

0000 00 0c 29 73 1c 47 00 1f a0 04 ba 4c 08 00 45 00 ..)s.G...L..E.
0010 00 9e 8e 92 00 00 40 11 cb a4 08 08 08 01 08 08 .....@. ....
0020 08 08 02 02 02 02 00 8a 2d 08 3c 31 33 35 3e 31 .....<135>1
0030 20 32 30 31 33 2d 30 35 2d 33 30 54 30 38 3a 35 2013-05 -30T08:5
0040 30 3a 32 35 2b 30 31 3a 30 30 20 31 39 32 2e 31 0:25+01: 00 192.1
0050 36 38 2e 32 31 30 2e 38 35 20 41 58 32 35 30 30 68.210.8 5 AX2500
0060 20 2d 20 4c 53 4e 3a 50 6f 72 74 41 6c 6c 6f 63 - LSN:P ortAlloc
0070 61 74 65 64 3a 49 43 4d 50 20 5b 33 2e 33 2e 33 ated:ICM P [3.3.3
0080 2e 32 35 20 33 32 36 20 31 35 2e 31 35 2e 31 35 .25 326 15.15.15
0090 2e 35 30 20 33 30 37 38 31 20 30 30 3a 35 30 3a .50 3078 1 00:50:
00a0 35 36 3a 30 64 3a 30 30 3a 35 32 5d 56:0d:00 :52]

```

## Compact

If client MAC insertion is enabled, the MAC address is appended to the end of the message.

Example:

```

0000 00 0c 29 73 1c 47 00 1f a0 04 ba 4c 08 00 45 00 ..)s.G...L..E.
0010 00 6a 8a 1f 00 00 40 11 d0 4b 08 08 08 01 08 08 .j....@. .K.....
0020 08 08 02 02 02 02 00 56 98 5c 3c 31 33 35 3e 20 .....V .\<135>
0030 4d 61 79 20 33 30 20 30 38 3a 34 38 3a 30 34 20 May 30 0 8:48:04
0040 41 58 32 35 30 30 20 49 43 3a 20 30 33 30 33 30 AX2500 I C: 03030
0050 33 31 39 3a 62 30 34 35 2d 3e 30 66 30 66 30 66 319:b045 ->0f0f0f
0060 33 32 3a 62 30 34 35 20 41 3a 30 30 35 30 35 36 32:b045 A:005056
0070 30 64 30 30 35 32 0d 0a 0d0052..

```

## Binary

If client MAC insertion is enabled, the MAC address is added as an Extension to the log message.

Example:

```

▼ A10 LSN Binary Log, Version: Version1 (1)
  ▼ Header
    Version: Version1 (1)
    Size: 36
  ▼ Log_Message
    Ext_Bit: EXT_BIT_SET (1)
    Log_Msg_Type: NAT_LOGGING_PORT_MAPPING (0)
    Timestamp: 2013/05/30 07:26:27 UTC (1369898787)
    Log_Msg_Length: 33
  ▼ Port_Mapping_Log
    Action: PORT_MAPPING_ALLOCATE (0)
    Protocol: ICMP (3)
    Type: LSN (0)
    Length: 14
  ▼ LSN_Port_Mapping
    Inside_Addr: 3.3.3.25 (50529049)
    NAT_Addr: 15.15.15.50 (252645170)
    Inside_Port: 29250
    NAT_Port: 29250
  ▼ Extensions
    Type: NAT_LOG_EXT_TYPE_INSIDE_MAC_INFO (5)
    Length: 8
    ▼ Inside_User_MAC
      MAC: 0050:560d:0052

```

## RADIUS

To enable your RADIUS server to support client MAC insertion, add the following attribute entry to your A10 :

ATTRIBUTE	A10-CGN-XXXXX	41	ether
-----------	---------------	----	-------

The data type is “ether” (used for Ethernet MAC addresses).

Example:

```

RADIUS Protocol
  Code: Accounting-Request (4)
  Packet identifier: 0x4d (77)
  Length: 119
  Authenticator: e0f978af60ab8ce35e2a448f2e18dc89
  Attribute Value Pairs
    AVP: 1=6 t=Acct-Status-Type(40): Start(1)
    AVP: 1=18 t=Acct-Session-Id(44): \001\247\223\235\222W\237k\000\000\000\000\003\000\000\000
    AVP: 1=23 t=NAS-Identifier(32): AX2500@192.168.210.85
    AVP: 1=52 t=Vendor-Specific(26) v=A10-Networks(22610)
      VSA: 1=6 t=A10-CGN-Timestamp(6): May 30, 2013 01:14:33.000000000 PDT
      VSA: 1=6 t=A10-CGN-Protocol(7): ICMP(3)
      VSA: 1=6 t=A10-CGN-Action(20): Port-Allocated(1)
      VSA: 1=6 t=A10-CGN-Inside-Addr(10): 3.3.3.25
      VSA: 1=4 t=A10-CGN-Inside-Port(11): 43593
      VSA: 1=6 t=A10-CGN-NAT-Addr(12): 15.15.15.50
      VSA: 1=4 t=A10-CGN-NAT-Port(13): 43593
      VSA: 1=8 t=A10-CGN-Include-Inside-User-MAC(41): 00:50:56:0d:00:52
      A10-CGN-Include-Inside-User-MAC: 0050560d0052

```

## Fixed-NAT Log Samples

For information on how to configure Fixed-NAT log messages, see [Logging for Fixed NAT](#).

Here are some examples of log messages generated by an ACOS device on which the logging option (Fixed-NAT user ports) is enabled.

The log output differs slightly depending on the configured port assignment method.

### Automatic Port Assignment (single port per client):

```
FIXED-NAT-PORTS 3001::172->192.168.9.173:1027
```

Compact Format:

```
P: 3001::172->c0a809ad:403
```

### Automatic Port Assignment (multiple ports per client):

```
FIXED-NAT-PORTS 10.10.10.172->192.168.9.173:3000-4000
```

Compact Format:

```
P: 0a0a0aac->c0a809ad:bb8-fa0
```

## Manual Port Assignment (using older syntax with manual port allocation)

```
FIXED-NAT-PORTS 3001::172->192.168.9.173:TCP 3000-4000;UDP 3000-4000;  
ICMP 10000-11000
```

Compact Format:

```
P: 3001::172->c0a809ad:T bb8-fa0;U bb8-fa0;I 2710-2af8
```

## Log Output If the Fixed-NAT LID Is Disabled or the Simplified Fixed-NAT Configuration Is Deleted

```
FIXED-NAT-DISABLE 10.10.10.172->192.168.9.173
```

Compact Format:

```
O: 0a0a0aac->c0a809ad
```

## Log Message Enhancements for Fixed-NAT

Specific to Fixed-NAT, the following enhancements apply for various logging formats:

### ASCII Log Messages

ASCII log messages for Fixed-NAT port allocation have the following new keywords:

- **USE-ALL-IPS** – Indicates this port allocation method is in use. If Use Least NAT IPs (the default) is used instead, no keyword is added to the log message.
- **OFFSET num** – If the offset is not 0, this keyword indicates the offset value. This value controls which inside client IP address will be mapped to a particular NAT IP address of your choice.
- **FIXED** – Indicates that the offset was configured by an admin rather than assigned by random.
- **RANDM** – Indicates that the offset was chosen randomly by ACOS. This value allows ACOS to automatically assign an offset for the inside client IP address. At the time of configuration, a random offset values will be assigned. If the ACOS device reboots, a different value may be chosen the next time.

## Compact Log Messages

For Fixed-NAT, the following keywords are added:

- UA – Indicates that the Use All NAT IPs method for fixed mapping allocation is used.
- O – Indicates that the offset option is enabled.
- num – Indicates the offset value.
- F – Indicates the offset was specified by an admin in the configuration, and is not a random offset calculated by ACOS.
- R – Indicates the offset was a random value calculated by ACOS.

## RFC 5424 Log Messages

The default message string for Fixed-NAT port block allocation messages is changed to the following:

```
LSN:FixedNATAAllocated [$src-ip$ $nat-ip$ $nat-port-start$ $nat-port-end$  
$method$ $offset$]
```

[Table 19](#) lists the default message string and keywords used for Fixed-NAT port allocation messages in RFC 5424 format. This change supports the new Fixed-NAT port allocation options.

Table 19 : Default RFC 5424 Message String and Keywords for Fixed-NAT Port Allocation Messages

Event Type	Default Message String
Fixed-NAT ports allocated	<pre>LSN:FixedNATAAllocated [\$src-ip\$ \$nat-ip\$ \$nat-port-start\$ \$nat-port-end\$ \$method\$ \$offset\$]</pre> <p>Keywords:</p> <ul style="list-style-type: none"><li>• \$src-ip\$ – Source IP address of the inside client.</li><li>• \$nat-ip\$ – Public (NAT) IP address assigned to the client.</li><li>• \$nat-port-start\$ – Beginning NAT port number.</li><li>• \$nat-port-end\$ – Ending NAT port number.</li><li>• \$method\$ – Fixed NAT port block allocation method.</li></ul>

Table 19 : Default RFC 5424 Message String and Keywords for Fixed-NAT Port Allocation Messages

Event Type	Default Message String
	<ul style="list-style-type: none"> <li>• \$offset\$ – Starting NAT IP offset.</li> <li>• \$radius-msisdn\$ – RADIUS attribute: MSISDN</li> <li>• \$radius-imei\$ – RADIUS attribute: IMEI</li> <li>• \$radius-imsi\$ – RADIUS attribute: IMSI</li> </ul> <p>Example:</p> <pre>LSN:FixedNATAllocated [166.1.1.22 188.1.1.103 1024 22527 USE-ALL-IPS OFFSET 2 FIXED -]</pre> <p>Notes:</p> <ul style="list-style-type: none"> <li>• The \$method\$ field appears only if the default port allocation method is not used.</li> <li>• The \$offset\$ field appears only if the offset is set to a value higher than 0.</li> </ul>

The following keywords are new in ACOS 2.8.1:

- \$nat-port-start\$ – Beginning NAT port number.
- \$nat-port-end\$ – Ending NAT port number.
- \$method\$ – Fixed NAT port block allocation method.
- \$offset\$ – Starting NAT IP offset.

The following keywords are deprecated in ACOS 2.8.1:

- \$tcp-port-start\$ – Beginning port number in the TCP port batch.
- \$tcp-port-end\$ – Ending port number in the TCP port batch.
- \$udp-port-start\$ – Beginning port number in the UDP port batch.
- \$udp-port-end\$ – Ending port number in the UDP port batch.
- \$icmp-port-start\$ – Beginning port number in the ICMP port batch.
- \$icmp-port-end\$ – Ending port number in the ICMP port batch.

**NOTE:** 

---

The fields are still supported for backwards compatibility.

---

## Binary Log Messages

Binary log messages in ACOS 2.8.2 and later use the Binary logging format for version 2, which affect Fixed-NAT Port Allocation in log messages.

### Changes for Fixed-NAT Port Allocation

If the default port allocation is used (Use Least NAT IPs with no offset), the Fixed-NAT header is unchanged.

If an offset is specified, or if the Use All NAT IPs method is used with or without an offset, the header for Fixed-NAT user-port log messages has the following format. These changes support the new Fixed-NAT allocation methods.

- Spare field reduced from 3 bits to 2 bits. This make room for the following new field.
- AE field (1 bit) to indicate whether an extension for the Fixed-NAT port allocation method is included:
  - Yes – 1
  - No – 0

The Length field is still 8 bits long, and indicates the total length of the header and the NAT mapping and allocation information.

[Figure 8](#) shows the format in ACOS 2.8.0. The new format is shown in [Figure 9](#).

Figure 8 : Binary Logging Format - Fixed-NAT header (ACOS 2.8.0)

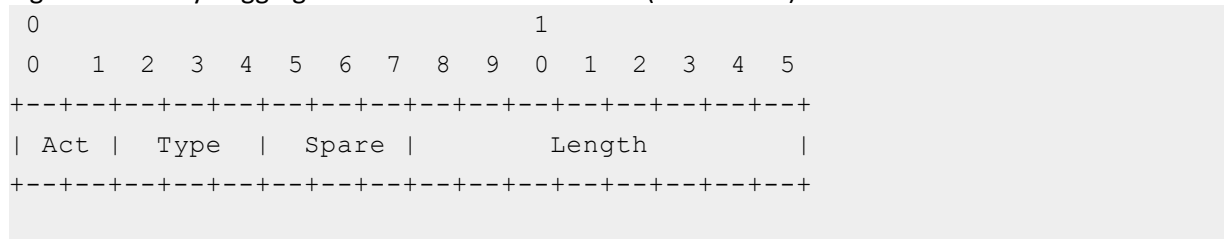
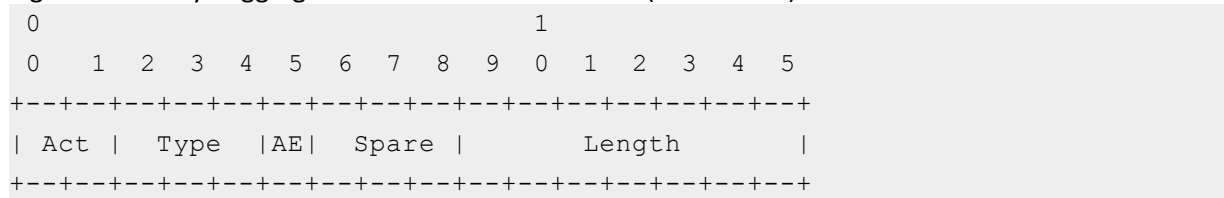


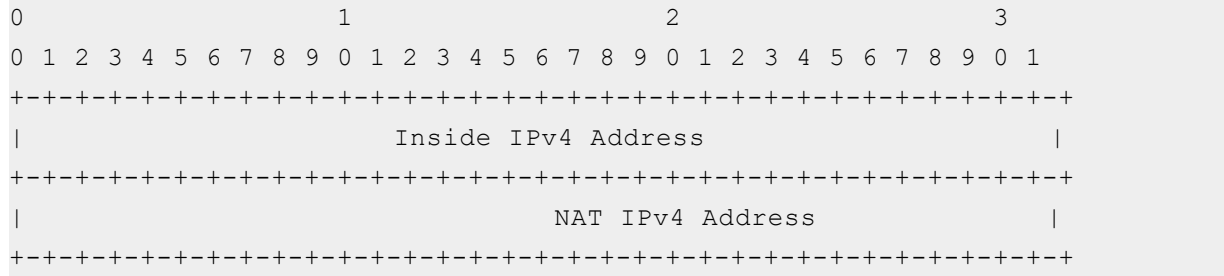
Figure 9 : Binary Logging Format - Fixed-NAT header (ACOS 2.8.2)



The header is followed by the NAT mapping which consists of the Inside User IP address, the NAT address and the port range information.

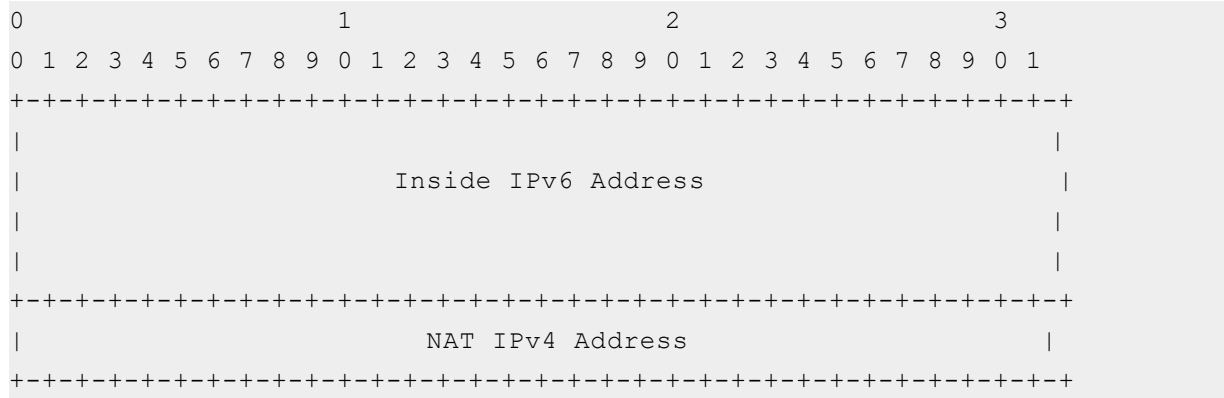
### NAT44

Figure 10 : Binary Logging Format - Fixed-NAT (NAT44)



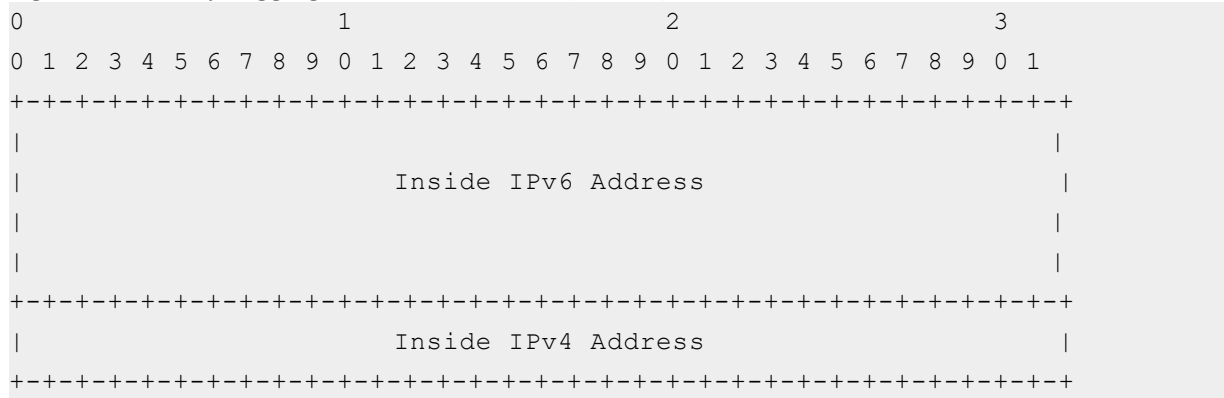
### NAT64

Figure 11 : Binary Logging Format - Fixed-NAT (NAT64)



### DS-Lite

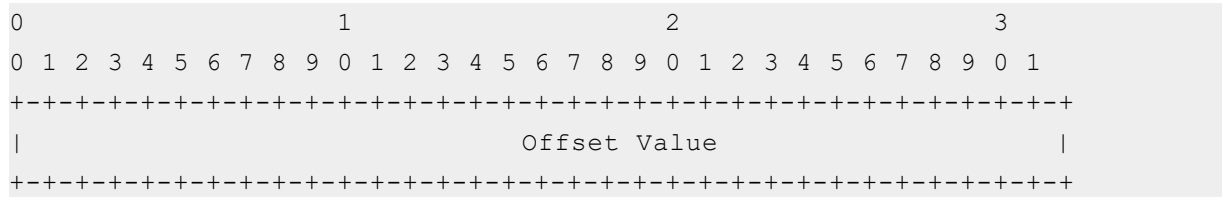
Figure 12 : Binary Logging Format - Fixed-NAT (DS-Lite)





## Information for Non-Default Offset

If an offset type other than the default (no offset) is used, an additional 4 bytes provide the offset value:



## DDoS Protection Log Samples

The logging format supported for DDoS Protection logs are ASCII, CEF, and Netflow. For Netflow information, see [NetFlow v9 and v10 \(IPFIX\)](#).

## ASCII Log Format

The following are the log samples:

### L3 Entry Created

```
Syslog message: LOCAL0.INFO: Nov 12 07:19:15 TH3040-A/shared NAT-DDOS-L3-
A: IP=150.100.1.10
```

### L3 Entry Deleted

```
Syslog message: LOCAL0.INFO: Nov 12 07:20:10 TH3040-A/shared NAT-DDOS-L3-
D: IP=150.100.1.10
```

### L4 Entry Created

```
Syslog message: LOCAL0.INFO: Nov 12 07:12:46 TH3040-A/shared NAT-DDOS-L4-
UDP-A: IP=150.100.1.10 PORT=8000
```

### L4 Entry Deleted

```
Syslog message: LOCAL0.INFO: Nov 12 07:13:19 TH3040-A/shared NAT-DDOS-L4-
UDP-D: IP=150.100.1.10 PORT=8000
```

## CEF Log Format

---

The following are the log samples:

### L3 Entry Creation

```
Syslog message: LOCAL0.INFO: Nov 12 07:17:00 TH3040-A/shared  
CEF:0|A10|CFW|5.2.1-d|CGN 121|iDDoS L3 entry create|5| dst=150.100.1.10
```

### L3 Entry Deletion

```
Syslog message: LOCAL0.INFO: Nov 12 07:17:50 TH3040-A/shared  
CEF:0|A10|CFW|5.2.1-d|CGN 122|iDDoS L3 entry delete|5| dst=150.100.1.10
```

### L4 Entry Creation

```
Syslog message: LOCAL0.INFO: Nov 12 07:15:13 TH3040-A/shared  
CEF:0|A10|CFW|5.2.1-d|CGN 123|iDDoS L4 entry create|5|proto=UDP  
dst=150.100.1.10 dpt=8000
```

### L4 Entry Deletion

```
Syslog message: LOCAL0.INFO: Nov 12 07:15:49 TH3040-A/shared  
CEF:0|A10|CFW|5.2.1-d|CGN 124|iDDoS L4 entry delete|5|proto=UDP  
dst=150.100.1.10 dpt=8000
```

## One-to-One NAT Log Samples

The logging format supported for One-to-One NAT44 and NAT64 logs are ASCII and CEF.

## ASCII Format

---

The following are the log samples for NAT44 logs:

### Session Creation

```
vThunder-1 NAT-UDP-N: 20.20.20.2:18004<-->30.30.30.2:16000,  
30.30.30.2:16000<-->10.0.20.11:18004\r\n
```

### Session Deletion

```
vThunder-1 NAT-UDP-D: 20.20.20.2:18004<-->30.30.30.2:16000,
30.30.30.2:16000<-->10.0.20.11:18004\r\n
```

The following are the log samples for NAT64 logs:

### Session Creation

```
vThunder NAT-TCP-N: [2001:db8:c21a:1::1]:38836<-->[3333::c8c8:c8c9]:80,
200.200.200.201:80<-->10.0.10.24:38836 imei=12343252342 imei=1235455657643
msisdn=4652309482735
```

### Session Deletion

```
vThunder NAT-TCP-D: [2001:db8:c21a:1::1]:38834<-->[3333::c8c8:c8c9]:80,
200.200.200.201:80<-->10.0.10.34:38834 imei=12343252342 imei=1235455657643
msisdn=4652309482735
```

## CEF Format

The following are the log samples for NAT44 logs:

### Session Creation

```
Oct 18 16:57:53 vThunder-1 CEF:0|A10|CFW|5.2.1-p4|CGN 102|Nat Session
Created|5|proto=UDP src=20.20.20.2 spt=18004 dst=30.30.30.2 dpt=16000
sourceTranslatedAddress=10.0.20.11 sourceTranslatedPort=18004
destinationTranslatedAddress=30.30.30.2 destinationTranslatedPort=16000
```

### Session Deletion

```
Oct 18 16:58:32 vThunder-1 CEF:0|A10|CFW|5.2.1-p4|CGN 103|Nat Session
Freed|5|proto=UDP src=20.20.20.2 spt=18004 dst=30.30.30.2 dpt=16000
sourceTranslatedAddress=10.0.20.11 sourceTranslatedPort=18004
destinationTranslatedAddress=30.30.30.2 destinationTranslatedPort=16000
```

The following are the log samples for NAT64 logs:

### Session Creation

```
vThunder CEF:0|A10|CFW|5.2.1-p1-d|CGN 102|Nat Session Created|5|proto=TCP
c6a2=2001:DB8:C21A:1::1 spt=38840 c6a3=3333::C8C8:C8C9 dpt=80
sourceTranslatedAddress=10.0.10.36 sourceTranslatedPort=38840
destinationTranslatedAddress=200.200.200.201 destinationTranslatedPort=80
c6a2Label=Source IPv6 Address c6a3Label=Dest IPv6 Address imei=12343252342
imei=1235455657643 msisdn=4652309482735
```

### Session Deletion

```
vThunder CEF:0|A10|CFW|5.2.1-p1-d|CGN 103|Nat Session Freed|5|proto=TCP
c6a2=2001:DB8:C21A:1::1 spt=38840 c6a3=3333::C8C8:C8C9 dpt=80
sourceTranslatedAddress=10.0.10.36 sourceTranslatedPort=38840
destinationTranslatedAddress=200.200.200.201 destinationTranslatedPort=80
c6a2Label=Source IPv6 Address c6a3Label=Dest IPv6 Address imei=12343252342
imei=1235455657643 msisdn=4652309482735
```

## Default Message Strings for RFC 5424

This section lists the default message strings used when RFC 5424 support is enabled.

For details on how to configure customized RFC 5424 message strings, see [RFC 5424 Custom Logging Format](#).

Use the following command to view the data field names configured in log message strings for session creation and deletion:

```
ACOS(config-logging:lsn_logging)# show cgnv6 logging keywords
```

**NOTE:** Although the ACOS device has default message strings for Fixed-NAT, by default, there is no logging for Fixed-NAT.

The following topics are covered:

<a href="#">Default Session Creation/Deletion Message Strings</a>	250
<a href="#">Default LSN Message Strings</a>	251
<a href="#">Default HTTP Request Received Message Strings</a>	252
<a href="#">Default DS-Lite Message Strings</a>	253
<a href="#">NAT64 Message Strings</a>	254
<a href="#">6rd-NAT64 Message Strings</a>	256

## Default Session Creation/Deletion Message Strings

The following lists the default message strings used for session creation and deletion when RFC 5424 support is enabled.

**NOTE:** To view the full list of keywords associated with different types of message strings, use the `show cgnv6 logging keywords` command.

### Event Type – Session created

```
SessionCreated:$proto-name$ [$fwd-tunnel$ $fwd-src-ip$ $fwd-src-port$  
$fwd-dst-tunnel$ $fwd-dst-ip$ $fwd-dst-port$ $rev-tunnel$ $rev-src-ip$  
$rev-src-port$ $rev-dst-tunnel$ $rev-dst-ip$ $rev-dst-port$]
```

**NOTE:** In this default string and the following default strings, the “\$radius-” keywords are included only if support for them is enabled. See [Logging Client Mobile Numbers](#). If you enable them, they appear at the end of the default log strings, in the following order: \$radius-msisdN\$ \$radius-imei\$ \$radius-imsi\$

#### Example

```
SessionCreated:TCP [- 3.3.3.50 10000 - 6.6.6.50 80 - 6.6.6.50 80 6.6.6.200  
10000]
```

### Event Type – Session freed

```
SessionFreed:$proto-name$ [$fwd-tunnel$ $fwd-src-ip$ $fwd-src-port$ $fwd-  
dst-tunnel$ $fwd-dst-ip$ $fwd-dst-port$ $rev-tunnel$ $rev-src-ip$ $rev-  
src-port$ $rev-dst-tunnel$ $rev-dst-ip$ $rev-dst-port$]
```

#### Example

```
SessionFreed:TCP [- 3.3.3.50 10000 - 6.6.6.50 80 - 6.6.6.50 80 6.6.6.200  
10000]
```

## Default LSN Message Strings

---

The following lists the default message strings used for LSN when RFC 5424 support is enabled.

### Event Type – Port allocated

```
LSN:PortAllocation:$proto-name$ [$src-ip$ $src-port$ $nat-ip$ $nat-port$]
```

---

#### NOTE:

- If you enable inclusion of the destination address in traffic logs, the `$dst-ip$` and `$dst-port$` keywords are included in the default string. See [Enable Destination Logging](#).
  - In this default string and the following default strings, the “`$radius-`” keywords are included only if support for them is enabled. See [Logging Client Mobile Numbers](#). If you enable them, they appear at the end of the default log strings, in the following order: `$radius-msisdn$ $radius-imei$ $radius-imsi$`
- 

#### Example

```
LSN:PortAllocation:TCP [3.3.3.50 10000 6.6.6.100 20000]
```

### Event Type – Port freed

```
LSN:PortFreed:$proto-name$ [$src-ip$ $src-port$ $nat-ip$ $nat-port$]
```

#### Example

```
LSN:PortFreed:TCP [3.3.3.50 10000 6.6.6.100 20000]
```

### Event Type – Port batch allocated

```
LSN:PortBatchAllocated:$proto-name$ [$src-ip$ $nat-ip$ $nat-port$ $batch-size$ $step-size$]
```

#### Example

```
LSN:PortBatchAllocated:TCP [3.3.3.50 6.6.6.100 20000 8 5]
```

## Event Type – Port batch freed

```
LSN:PortBatchFreed:$proto-name$ [$src-ip$ $nat-ip$ $nat-port$ $batch-size$
$step-size$]
```

### Example

```
LSN:PortBatchFreed:TCP [3.3.3.50 6.6.6.100 20000 8 5]
```

## Event Type – Fixed-NAT ports allocated

```
LSN:FixedNATAAllocated [$src-ip$ $nat-ip$ $tcp-port-start$ $tcp-port-end$
$udp-port-start$ $udp-port-end$ $icmp-port-start$ $icmp-port-end$]
```

### Example

```
LSN:FixedNATAAllocated [3.3.3.50 6.6.6.200 2000 5000 3000 3000 8000 9000]
```

## Event Type – Fixed-NAT ports freed

```
LSN:FixedNATFreed: [$src-ip$ $nat-ip$]
```

### Example

```
LSN:FixedNATFreed [3.3.3.50 6.6.6.200]
```

## Default HTTP Request Received Message Strings

The following lists the default message strings used for received HTTP requests, when RFC 5424 support is enabled.

### Event Type – HTTP request received

The default log string depends on the enabled HTTP request and RADIUS options.

- Default log string when `log http-requests host` or `log http-requests url` is enabled:

```
HTTPRequestGot: [$http-host-or-url$]
```

- Default log string when `log http-requests host` or `log http-requests url` is enabled, with `include-http method` enabled:

```
HTTPRequestGot: [$http-method$ $http-host-or-url$]
```

- Default log string when `log http-requests url` is enabled, with `include-radius-attribute msisdn http-requests` and `include-http method` enabled:

```
HTTPRequestGot: [$http-method$ $host-or-url$ $radius-msisdn$]
```

- Default log string when `log http-requests host` Or `log http-requests url` is enabled, with `include-http method` and `include-http 14-session-info` enabled:

```
HTTPRequestGot: [$fwd-tunnel$ $fwd-src-ip$ $fwd-src-port$
$fwd-dst-tunnel$ $fwd-dst-ip$ $fwd-dst-port$ $rev-tunnel$
$rev-src-ip$ $rev-src-port$ $rev-dst-tunnel$ $rev-dst-ip$
$rev-dst-port$ $http-method$ $host-or-url$]
```

## Default DS-Lite Message Strings

The following lists the default message strings used for DS-Lite when RFC 5424 support is enabled.

### Event Type - Port Allocated

```
DS-Lite:PortAllocation:$proto-name$ [$tunnel-ip$ $src-ip$ $src-port$ $nat-
ip$ $nat-port$]
```

#### NOTE:

- If you enable inclusion of the destination address in traffic logs, the `$dst-ip$` and `$dst-port$` keywords are included in the default string. See [Enable Destination Logging](#).
- In this default string and the following default strings, the “`$radius-`” keywords are included only if support for them is enabled. See [Logging Client Mobile Numbers](#). If you enable them, they appear at the end of the default log strings, in the following order:  
`$radius-msisdn$ $radius-imei$ $radius-imsi$`

#### Example

```
DS-Lite:PortAllocation:TCP [2001::100 3.3.3.50 10000 6.6.6.100 20000]
```

## Event Type – Port freed

```
DS-Lite:PortFreed:$proto-name$ [$tunnel-ip$ $src-ip$ $src-port$ $nat-ip$  
$nat-port$]
```

### Example

```
DS-Lite:PortFreed:TCP [2001::100 3.3.3.50 10000 6.6.6.100 20000]
```

## Event Type - Port batch allocated

```
DS-Lite:PortBatchAllocated:$proto-name$ [$tunnel-ip$ $src-ip$ $nat-ip$  
$nat-port$ $batch-size$ $step-size$]
```

### Example

```
DS-Lite:PortBatchAllocated:TCP [2001::100 3.3.3.50 6.6.6.100 20000 8 5]
```

## Event Type - Port batch freed

```
DS-Lite:PortBatchFreed:$proto-name$ [$tunnel-ip$ $src-ip$ $nat-ip$  
$nat-port$ $batch-size$ $step-size$]
```

### Example

```
DS-Lite:PortBatchFreed:TCP [2001::100 3.3.3.50 6.6.6.100 20000 8 5]
```

## NAT64 Message Strings

---

The following lists the default message strings used for NAT64 when RFC 5424 support is enabled.

## Event Type - Port allocated

```
NAT64:PortAllocation:$proto-name$ [$src-ip$ $src-port$ $nat-ip$ $nat-  
port$]
```

---

**NOTE:**

- If you enable inclusion of the destination address in traffic logs, the `$dst-ip$` and `$dst-port$` keywords are included in the default string. See [Enable Destination Logging](#).
  - In this default string and the following default strings, the “`$radius-`” keywords are included only if support for them is enabled. See [Logging Client Mobile Numbers](#). If you enable them, they appear at the end of the default log strings, in the following order:  
`$radius-msisdn$ $radius-imei$ $radius-imsi$`
- 

**Example**

```
NAT64:PortAllocation:TCP [4001::100 10000 8.8.8.100 20000]
```

### Event Type - Port freed

```
NAT64:PortFreed:$proto-name$ [$src-ip$ $src-port$ $nat-ip$ $nat-port$]
```

**Example**

```
NAT64:PortFreed:TCP [4001::100 10000 8.8.8.100 20000]
```

### Event Type - Port batch allocated

```
NAT64:PortBatchAllocated:$proto-name$ [$src-ip$ $nat-ip$ $nat-port$  
$batch-size$ $step-size$]
```

**Example**

```
NAT64:PortBatchAllocated:TCP [4001::100 8.8.8.100 20000 8 5]
```

### Event Type - Port batch freed

```
NAT64:PortBatchFreed:$proto-name$ [$src-ip$ $nat-ip$ $nat-port$ $batch-  
size$ $step-size$]
```

**Example**

```
NAT64:PortBatchFreed:TCP [4001::100 8.8.8.100 20000 8 5]
```

## Event Type - Fixed-NAT ports allocated

```
NAT64:FixedNATAAllocated [$src-ip$ $nat-ip$ $tcp-port-start$ $tcp-port-end$  
$udp-port-start$ $udp-port-end$ $icmp-port-start$ $icmp-port-end$]
```

### Example

```
NAT64:FixedNATAAllocated [4001::100 8.8.8.200 2000 5000 3000 3000 8000  
9000]
```

## Event Type - Fixed-NAT ports freed

```
NAT64:FixedNATDisabled [$src-ip$ $nat-ip$]
```

### Example

```
NAT64:FixedNATDeleted [4001::100 8.8.8.200]
```

## 6rd-NAT64 Message Strings

The following lists the default message strings used for 6rd-NAT64 when RFC 5424 support is enabled.

## Event Type - Port allocated

```
6rd:PortAllocation:$proto-name$ [$tunnel-ip$ $src-ip$ $src-port$ $nat-ip$  
$nat-port$]
```

### NOTE:

- If you enable inclusion of the destination address in traffic logs, the `$dst-ip$` and `$dst-port$` keywords are included in the default string. See [Enable Destination Logging](#).
- In this default string and the following default strings, the “`$radius-`” keywords are included only if support for them is enabled. See [Logging Client Mobile Numbers](#). If you enable them, they appear at the end of the default log strings, in the following order:  
`$radius-msisdn$ $radius-imei$ $radius-imsi$`

### Example

```
6rd:PortAllocation:TCP [3.3.3.50 6001:0:3232:3305:20c:29ff:fed6:4457 10000  
6.6.6.100 20000]
```

## Event Type - Port freed

```
6rd:PortFreed:$proto-name$ [$tunnel-ip$ $src-ip$ $src-port$ $nat-ip$ $nat-  
port$]
```

### Example

```
6rd:PortFreed:TCP [3.3.3.50 6001:0:3232:3305:20c:29ff:fed6:4457 10000  
6.6.6.100 20000]
```

## Event Type - Port batch allocated

```
6rd:PortBatchAllocated:$proto-name$ [$tunnel-ip$ $src-ip$ $nat-ip$ $nat-  
port$ $batch-size$ $step-size$]
```

### Example

```
6rd:PortBatchAllocated:TCP [3.3.3.50 6001:0:3232:3305:20c:29ff:fed6:4457  
10000 6.6.6.100 128 5]
```

## Event Type - Port batch freed

```
6rd:PortBatchFreed:$proto-name$ [$tunnel-ip$ $src-ip$ $nat-ip$ $nat-port$  
$batch-size$ $step-size$]
```

### Example

```
6rd:PortBatchFreed:TCP [3.3.3.50 6001:0:3232:3305:20c:29ff:fed6:4457 10000  
6.6.6.100 128 5]
```

# Binary Logging Format Reference

## (ACOS 2.8.0 and earlier)

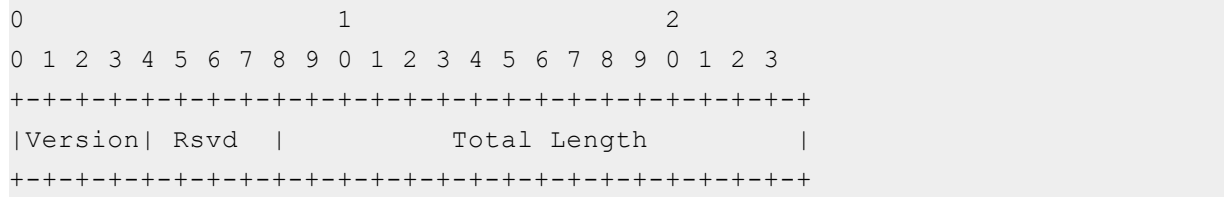
---

This section describes the packet formats used by A10 binary format in v1, used in ACOS 2.8.0 and earlier.

## Packet Header

Each A10 binary logging packet contains only one packet header, regardless of the number of log messages the packet contains.

Figure 15 : Binary Logging Format - packet header



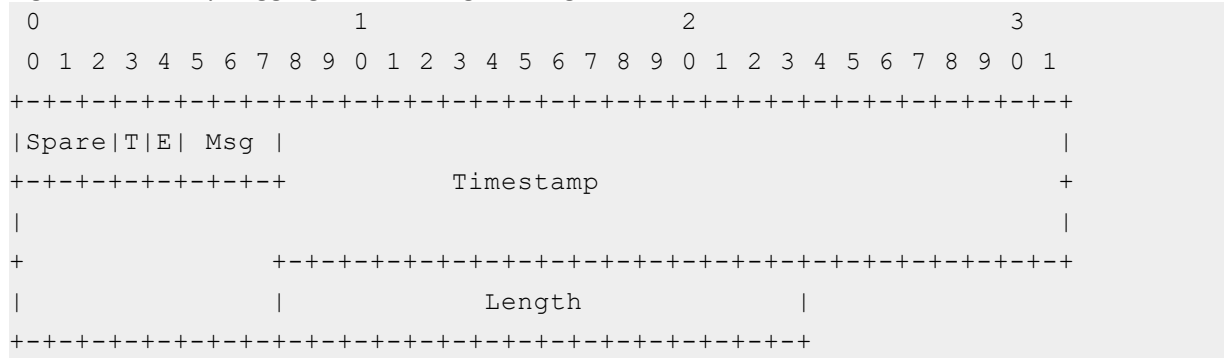
The packet header has the following fields:

- Version (4 bits) – A10 binary logging version (currently 1)
- Reserved (4 bits) – Reserved for future use
- Total Length (16 bits) – Total length of log message (UDP packet payload) in bytes

## Log-message Header

Every A10 binary log message has one log-message header.

Figure 16 : Binary Logging Format - log-message header



The log-message header has the following fields:

- Spare (3 bits) – Unused bits
- T (1 bit) – Timestamp precision:
  - 0 – Precision to within one whole second (default)
  - 1 – Precision to within 10 milliseconds
- E (1 bit) – Extension flag

- Msg (3 bits) – Message type
  - 0 – Port mapping
  - 1 – Session
  - 2 – Port Batching
  - 3 – Fixed-NAT
  - 4 – HTTP request
- Timestamp (64 bits) – Timestamp in UTC
- Length (16 bits) – Log message length (including extensions) in bytes

## Optional Header Extensions

Logging of some types of information is optional and, when enabled, adds extension headers to binary log packets. [Table 20](#) lists the types of binary log messages that may contain extension headers.

Table 20 : Optional extension headers

Type of Binary Log Message	Extension Header			
	Order of Appearance	Description	Default	To Enable...
Session log	1. MSISDN	Mobile Station International ISDN Number (MSISDN) of client.	Disabled (not included)	<a href="#">Logging Client Mobile Numbers</a>
	2. IMEI	International Mobile Equipment Identity (IMEI) of client.	Disabled (not included)	
	3. IMSI	International Mobile Subscriber Identity (IMSI) of	Disabled (not included)	

Table 20 : Optional extension headers

Type of Binary Log Message	Extension Header			
	Order of Appearance	Description	Default	To Enable...
		client.		
Port-mapping log	1. Destination	Destination IP address of port mapping.	Disabled (not included)	<a href="#">Enable Destination Logging</a>
	2. MSISDN	MSISDN of client.	Disabled (not included)	<a href="#">Logging Client Mobile Numbers</a>
	3. IMEI	IMEI of client.	Disabled (not included)	
	4. IMSI	IMSI of client.	Disabled (not included)	
1. MSISDN	MSISDN of client.	Disabled (not included)	<a href="#">Logging Client HTTP Requests</a>	
HTTP request log	2. IMEI	IMEI of client.	Disabled (not included)	
	3. IMSI	IMSI of client.	Disabled (not included)	

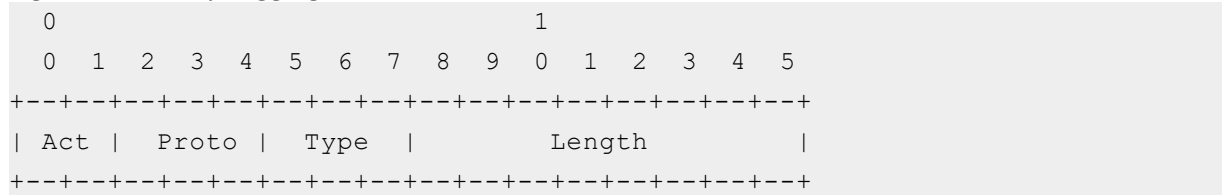
For cases where more than one type of extension header is enabled, the “Order of Appearance” column lists the order in which they appear in log packets. If only some extension headers are enabled, the enabled ones appear in the order shown. The disabled ones do not appear.

## Session Logs

### Session Header

Every session log message begins with the session header.

Figure 17 : Binary Logging Format - session header



The session log header has the following fields:

- Act (2 bits) – Action:
  - Create session – 0
  - Delete session – 1
  - Information for session – 2
- Proto (3 bits) – Session protocol:
  - TCP – 1
  - UDP – 2
  - ICMP – 3
  - RTSP – 6
  - ICMPv6 – 7
- Type (3 bits):
  - LSN – 0
  - NAT64 – 1
  - DS-Lite – 2
  - 6rd or NAT64 – 3
- Length (8 bits) – Length of session message, including session header

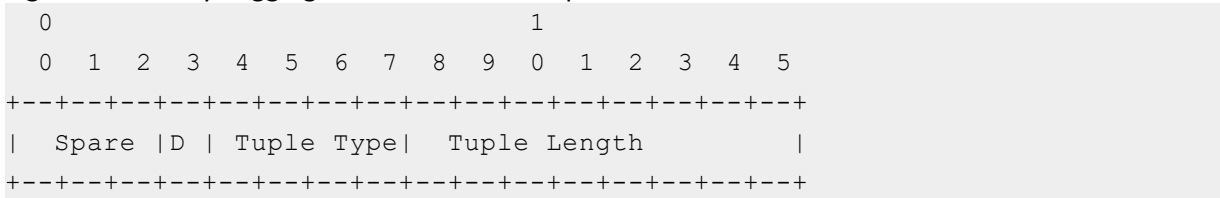
### Session Message

A session creation or deletion log message consists of the following parts:



- Forward tuple header
- Forward tuple
- Reverse tuple header
- Reverse tuple

Figure 18 : Binary Logging Format - forward tuple header



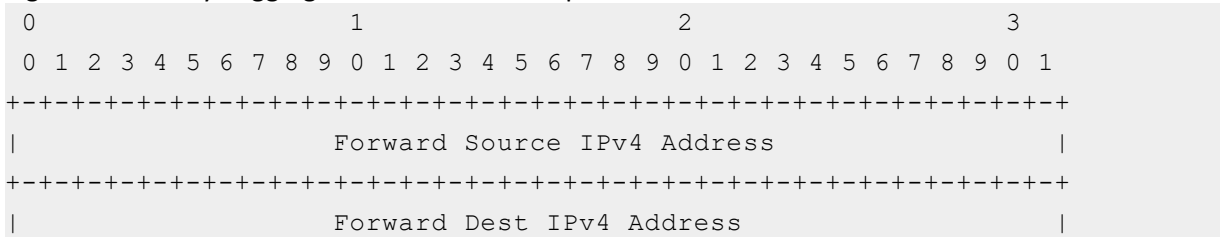
The forward tuple header has the following fields:

- Spare (3 bits) – Unused bits
- D (1 bit) – Direction:
  - Forward – 0
  - Reverse – 1
- Tuple type (4 bits):
  - IPv4 – 0
  - IPv6 – 1
  - IPv4-in-IPv6 – 2
  - IPv6-in-IPv4 – 3
- Tuple Length (8 bits) – Length of the tuple, including tuple header, in bytes

## Forward Tuple

The fields contained in the forward tuple depend on the tuple type in the tuple header.

Figure 19 : Binary Logging Format - forward tuple: IPv4



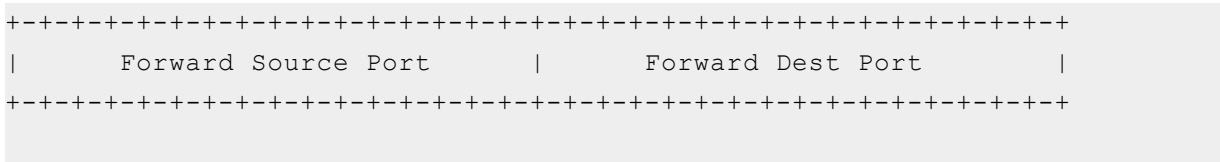
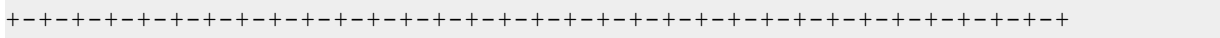


Figure 20 : Binary Logging Format - forward tuple: IPv6



Figure 21 : Binary Logging Format - forward tuple: IPv4 in IPv6





### Reverse Tuple Header

Same as forward tuple header.

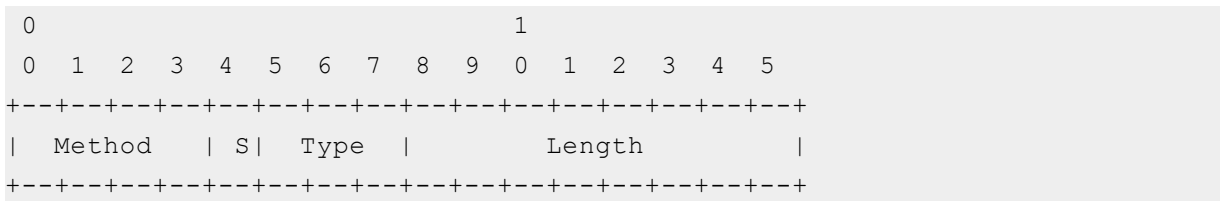
### Reverse Tuple

Same as forward tuple.

### HTTP Request Logging Extensions

If the ACOS device is configured to log client HTTP requests, binary log messages include an extension header that contains information about the request.

### HTTP Request Header



The extension header for HTTP requests has the following fields:

- Method (4 bits) – Method used in the request:
  - Not logged – 0
  - GET – 1
  - HEAD – 2
  - PUT – 3
  - POST – 4
  - OPTIONS – 5
  - DELETE – 6
  - TRACE – 7
  - CONNECT – 8

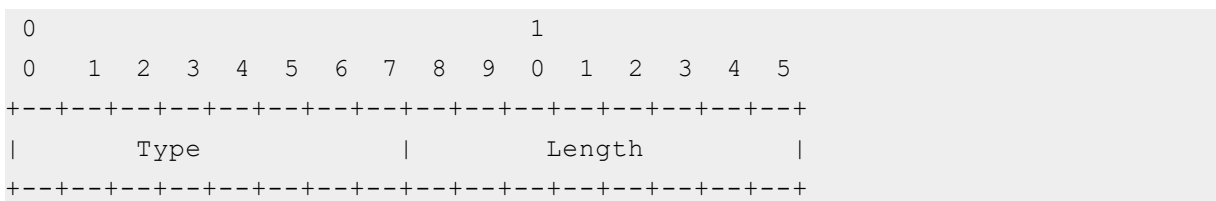


- S (1 bit) – Indicates whether logging of Layer 4 session information is enabled:
  - Disabled – 0
  - Enabled – 1
- Type (3 bits) – Indicates whether host logging or URL logging is enabled:
  - Host – 0
  - URL – 1
- Length (8 bits) – Length of host or URL, including HTTP-REQUESTS header.

## RADIUS Attribute Logging Extensions

If the ACOS device is configured to use RADIUS to obtain and log client information such as mobile numbers, binary log messages include an extension header that contains the Type, Length, and Value (TLV) for the attribute obtained from the RADIUS server.

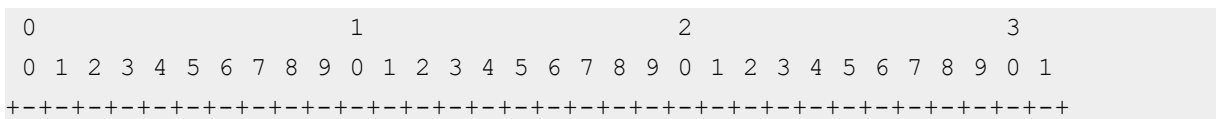
### Extension Header



The extension header for RADIUS has the following fields:

- Type (8 bits) :
  - Mobile Station International ISDN Number (MSISDN) – 2
  - International Mobile Equipment Identity (IMEI) – 3
  - International Mobile Subscriber Identity (IMSI) – 4
- Length (8 bits) – Length of extension message, including extension header

The Type value is always a string of numeric digits in Hexadecimal format. Two digits are packed into one byte. If the length is not even, 0x0f is added as padding.



MSISDN/IMEI/IMSI
.....

## Port-mapping Logs

### Port-mapping Header

Every port-mapping log message begins with the port-mapping header.

Figure 22 : Binary Logging Format - port-mapping header

0										1					
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
Act		Proto			Type			Length							

The port-mapping log header has the following fields:

- Act (2 bits) – Action:
  - Port mapping allocate – 0
  - Port mapping reuse – 1
  - Port mapping free – 2
- Proto (3 bits) – Protocol:
  - TCP – 1
  - UDP – 2
  - ICMP – 3
  - RTSP – 6
  - ICMPv6 – 7
- Type (3 bits) – Port mapping type:
  - LSN – 0
  - NAT64 – 1

- DS-Lite – 2
- 6rd or NAT64 – 3
- Length (8 bits) – Length of port-mapping message, including port mapping header

## Port Mapping Message

There are four possible port-mapping messages, one each for LSN, NAT64, DS-Lite, and 6rd/NAT64.

Figure 23 : Binary Logging Format - port-mapping message: LSN

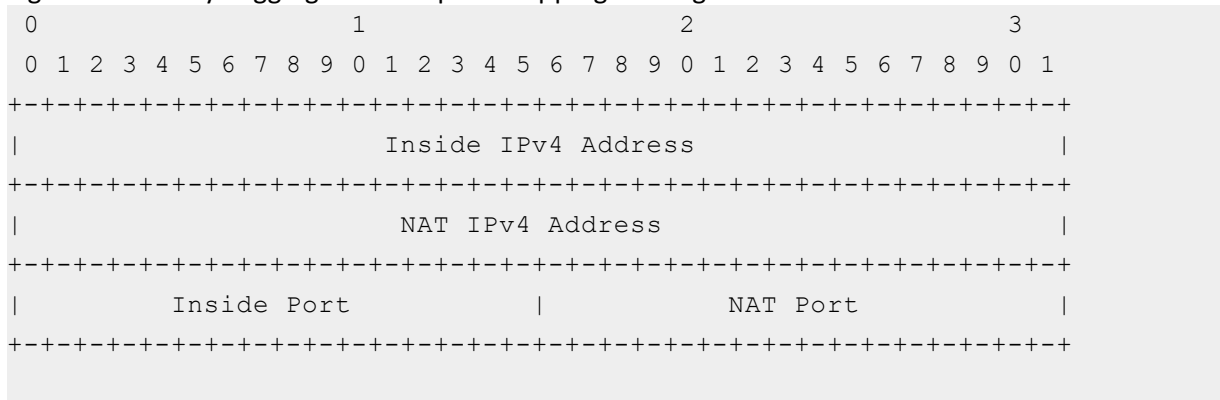


Figure 24 : Binary Logging Format - port-mapping message: NAT64

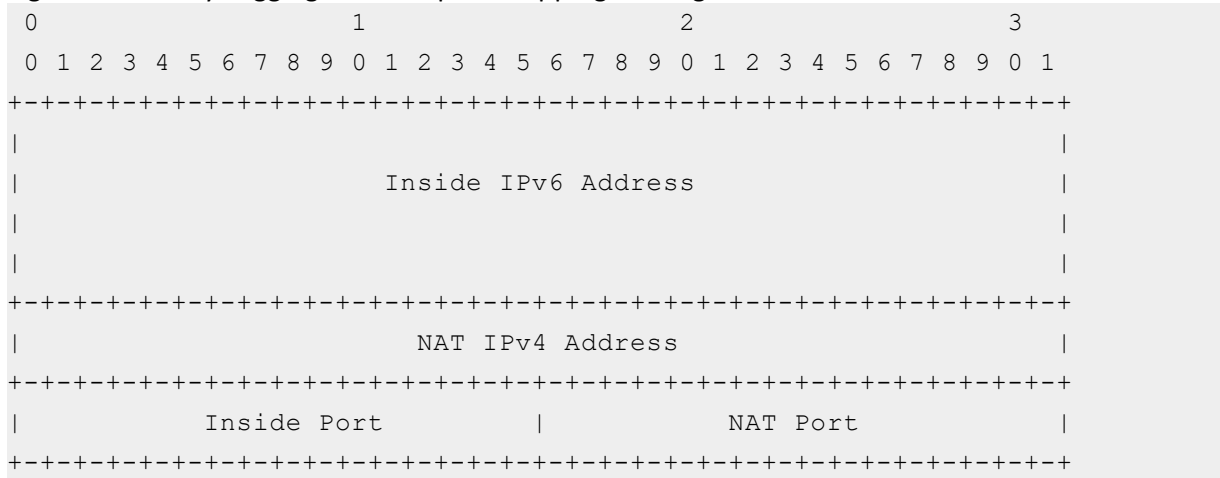
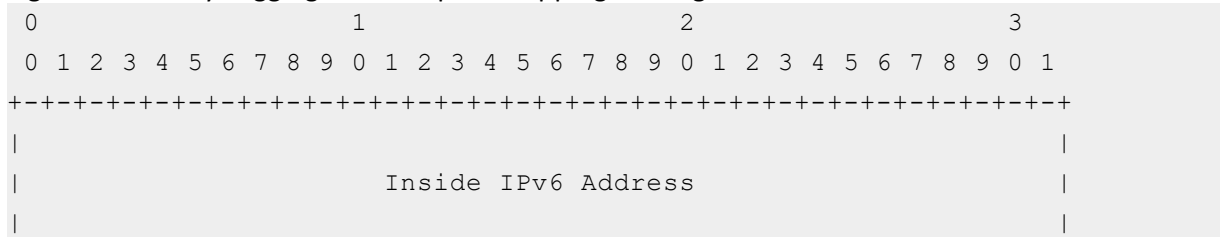


Figure 25 : Binary Logging Format - port-mapping message: DS-Lite



```

|
+-----+
|                               Inside IPv4 Address                               |
+-----+
|                               NAT IPv4 Address                               |
+-----+
|           Inside Port           |           NAT Port           |
+-----+
    
```

Figure 26 : Binary Logging Format - port-mapping message: 6rd/NAT64

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+
|                               Inside IPv4 Address                               |
+-----+
|                               Inside IPv6 Address                               |
|                               |                                               |
|                               |                                               |
+-----+
|                               NAT IPv4 Address                               |
+-----+
|           Inside Port           |           NAT Port           |
+-----+
    
```

### Port Mapping Message Extensions

A port-mapping log message can be configured to include destination information. In this case, an extension is used to hold the destination.

Figure 27 : Binary Logging Format - port-mapping extension header

```

0                               1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-----+
|           Type           |           Length           |
+-----+
    
```

The extension header has the following fields:

- Type (8 bits) – Type of extension:
  - Destination – 1
- Length (8 bits) – Length of extension message, including extension header

**NOTE:** The destination-info extension headers shown in the following figures apply only to port-mapping allocation messages.

Figure 28 : Binary Logging Format - destination-info extension: LSN

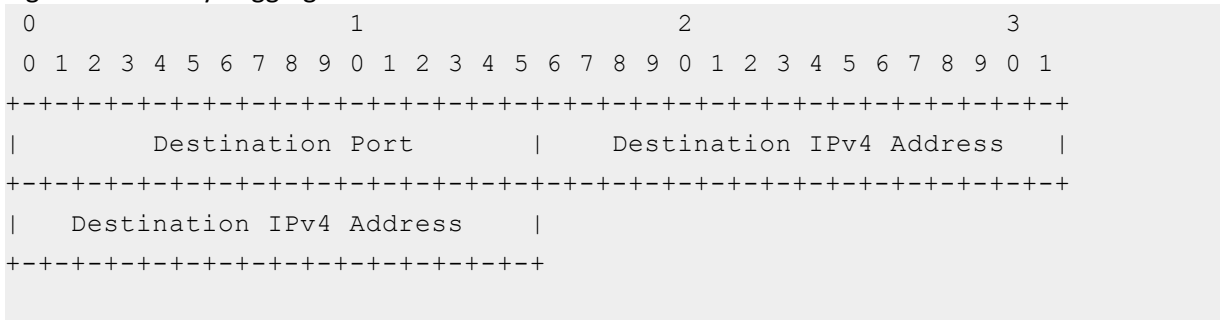


Figure 29 : Binary Logging Format - destination-info extension: NAT64

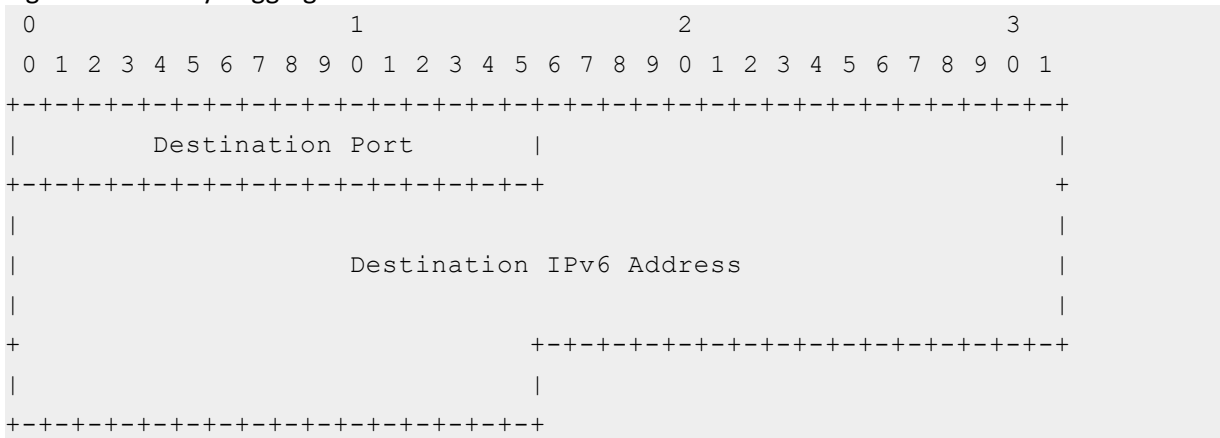
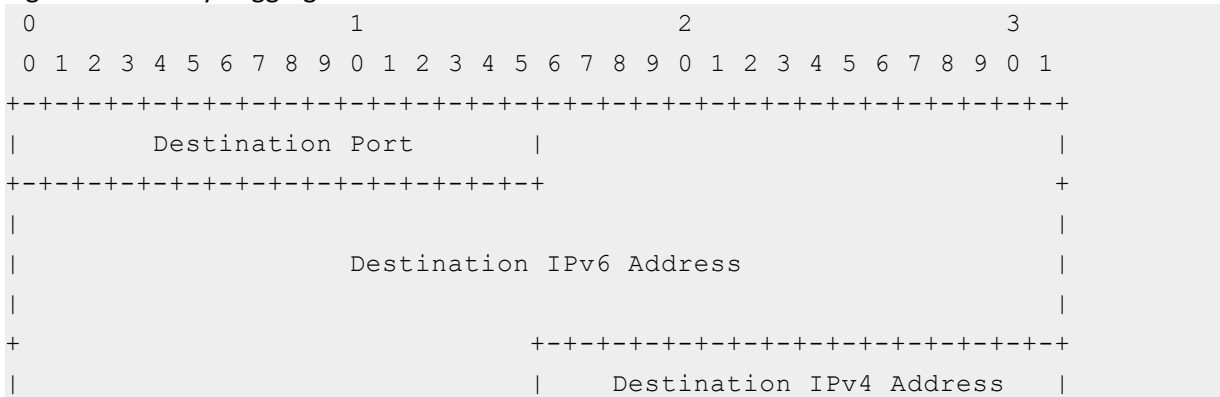


Figure 30 : Binary Logging Format - destination-info extension: DS-Lite



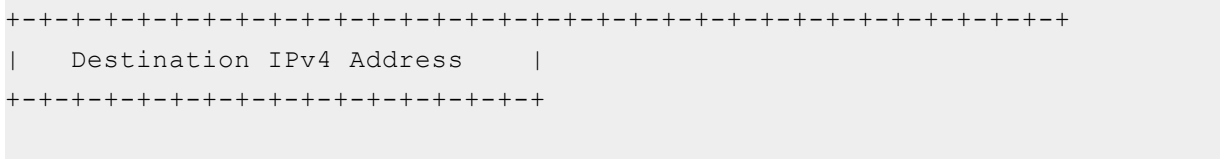
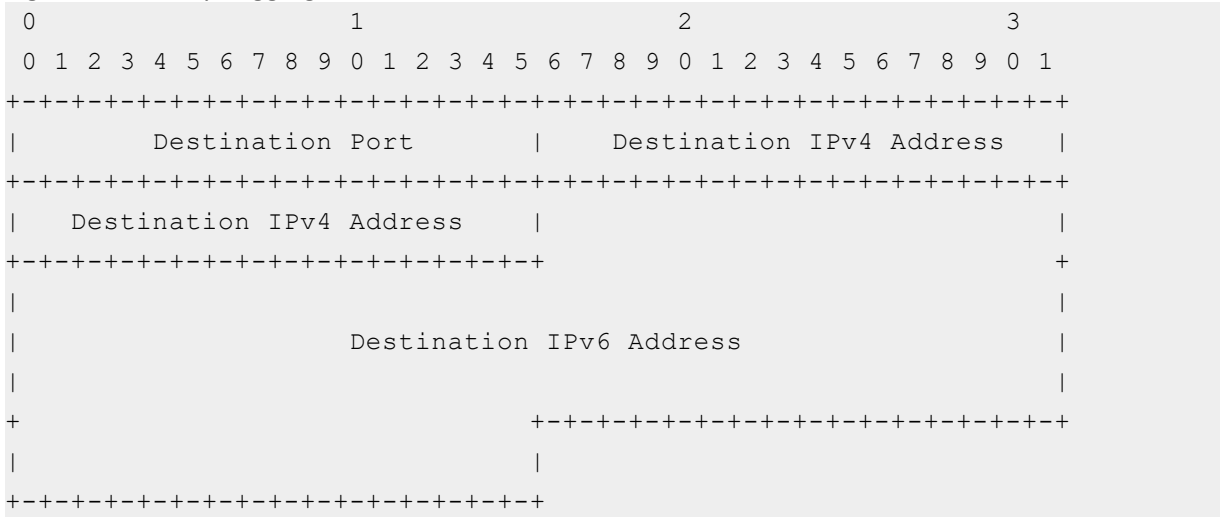


Figure 31 : Binary Logging Format - destination-info extension: 6rd/NAT64

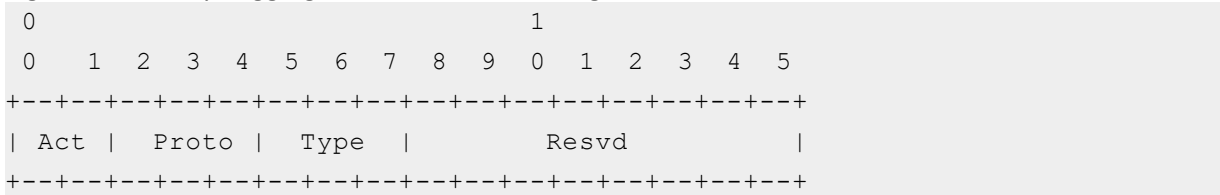


## Port Batching Logs

### Port Batching Header

Every Port Batching log message begins with the Port Batching header.

Figure 32 : Binary Logging Format - Port Batching header



The Port Batching log header has the following fields:

- Act (2 bits) – Action:
  - Port mapping allocate – 0
  - Port mapping free – 2



- Proto (3 bits) – Protocol:
  - TCP – 1
  - UDP – 2
  - ICMP – 3
  - RTSP – 6
  - ICMPv6 – 7
- Type (3 bits) – Session type:
  - LSN – 0
  - NAT64 – 1
  - DS-Lite – 2
  - 6rd or NAT64 – 3

### Port Batching Message

There are four possible Port Batching messages, one each for LSN, NAT64, DS-Lite, and 6rd/NAT64.

Figure 33 : Binary Logging Format - Port Batching message: LSN

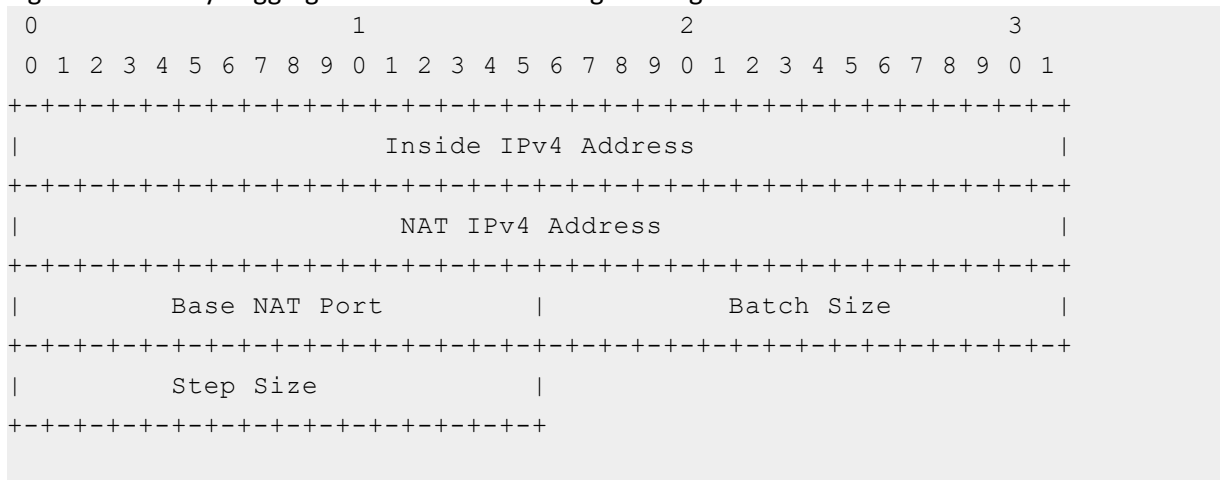
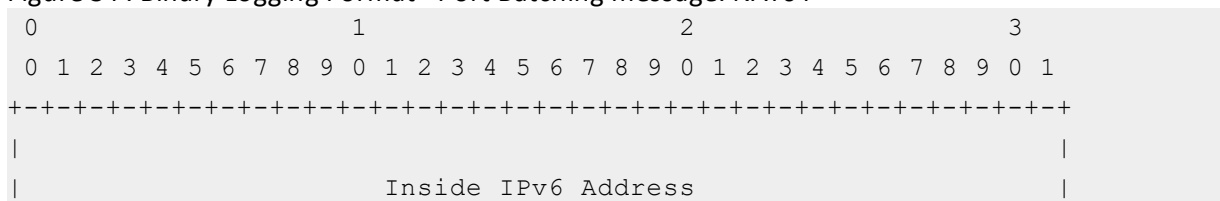


Figure 34 : Binary Logging Format - Port Batching message: NAT64



```

|
|
+-----+
|
|                               NAT IPv4 Address
|
+-----+
|
|   Base NAT Port                |                Batch Size
|
+-----+
|
|   Step Size                    |
|
+-----+
    
```

Figure 35 : Binary Logging Format - Port Batching message: DS-Lite

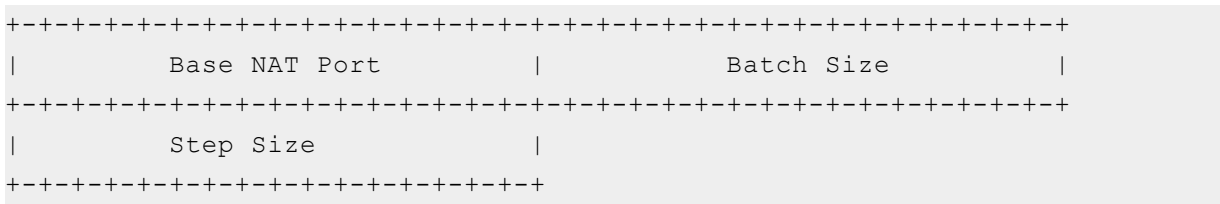
```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+
|
|                               Inside IPv6 Address
|
|
|
+-----+
|
|                               Inside IPv4 Address
|
+-----+
|
|                               NAT IPv4 Address
|
+-----+
|
|   Base NAT Port                |                Batch Size
|
+-----+
|
|   Step Size                    |
|
+-----+
    
```

Figure 36 : Binary Logging Format - Port Batching message: 6rd/NAT64

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+
|
|                               Inside IPv4 Address
|
+-----+
|
|                               Inside IPv6 Address
|
|
|
+-----+
|
|                               NAT IPv4 Address
|
    
```

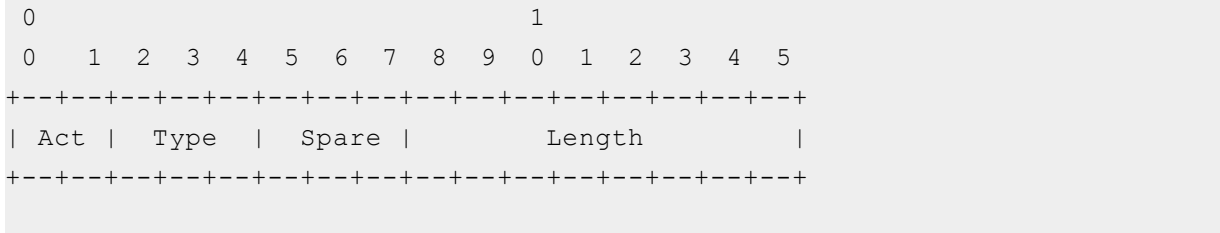


### Fixed-NAT Logs

#### Fixed-NAT Header

Every Fixed-NAT log message begins with the session header.

Figure 37 : Binary Logging Format - Fixed-NAT header



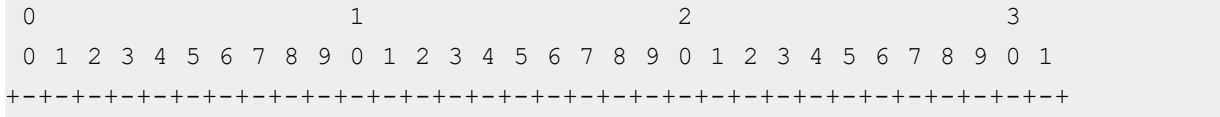
The Fixed-NAT session log header has the following fields:

- Act (2 bits) – Action:
  - Ports assigned – 0
  - Ports disabled – 1
- Type (3 bits) – Session type:
  - NAT44 – 0
  - NAT64 – 1
- Length (8 bits) – Log message length (excluding extensions) in bytes

#### Fixed-NAT Message

Every NAT44 Fixed-NAT message for port assignment or port disable includes the inside IPv4 address and the NAT address.

Figure 38 : Binary Logging Format - NAT44 Fixed-NAT port assignment or deletion (IP address information)



```

|                               Inside IPv4 Address                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               NAT IPv4 Address                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
    
```

Likewise, every NAT64 Fixed-NAT message for port assignment or port disable includes the inside IPv6 address and the NAT address.

Figure 39 : Binary Logging Format - NAT64 Fixed-NAT port assignment or deletion (IP address information)

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               Inside IPv6 Address                               |
|                               |                                               |
|                               |                                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               NAT IPv4 Address                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
    
```

In addition, Fixed-NAT port assignment messages contain the actual range of ports assigned to clients. The message format differs depending on whether the old syntax (2.6.2) or new syntax (2.6.3) is used to configure Fixed-NAT.

Figure 40 : Binary Logging Format - Fixed-NAT port assignment (port ranges) - 2.6.3 syntax

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|  Proto = 0  |                               Start Port                               |  End  |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|  Port      |
+---+---+---+---+---+
    
```

Figure 41 : Binary Logging Format - Fixed-NAT port assignment (port ranges) - 2.6.2 syntax

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|  Proto = 1  |                               Start Port                               |  End  |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|  Port      |  Proto = 2  |                               Start Port                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               End Port                               |  Proto = 3  |  Start  |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
    
```

```

|      Port      |      End Port      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

The Proto field can have the following values:

- 0 – TCP, UDP and ICMP
- 1 – TCP
- 2 – UDP
- 3 – ICMP

## (ACOS 2.8.1 and later)

This section describes the changes in Binary format log messages from v1 to v2, the latter of which is supported in ACOS 2.8.1 and later.

### Increased Data Length in Extension Headers

The Length field for all Binary logging extension headers is increased from 8 to 16 bits. This allows each Binary log packet to contain more than 253 bytes of data in each log packet, which is the maximum in v1.

[Figure 42](#) shows the format in ACOS 2.8.0. The new format in ACOS 2.8.1 is shown in [Figure 43](#).

Figure 42 : Binary Logging - Extension Header (ACOS 2.8.0)

```

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |      Length      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Figure 43 : Binary Logging - Extension Header (ACOS 2.8.1)

```

0                                     1                                     2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |      Length      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

## HTTP Request Header Changes

The format for Binary format log messages with HTTP Request Headers has the following enhancements:

- Length field is increased from 8 to 16 bits (described in [Increased Data Length in Extension Headers.](#))
- Length field is allowed to contain an HTTP-REQUESTS header without any host or URL data immediately after it. In this case, the host or URL data is sent in a subsequent packet with an extension header.
- New Type values for logging extension headers:
  - 10 – Request size
  - 11 – Response size
  - 12 – HTTP request number
  - 13 – HTTP Host
  - 14 – HTTP URL
  - 15 – HTTP Cookie
  - 16 – HTTP Referer
  - 17 – HTTP User-Agent
- 18~20 – For the custom header values that you can configure using the information provided later in this section.

[Figure 42](#) shows the format in ACOS 2.8.0. The new format in ACOS 2.8.1 is shown in [Figure 43](#).

Figure 44 : Binary Logging - HTTP Request Header (ACOS 2.8.0)

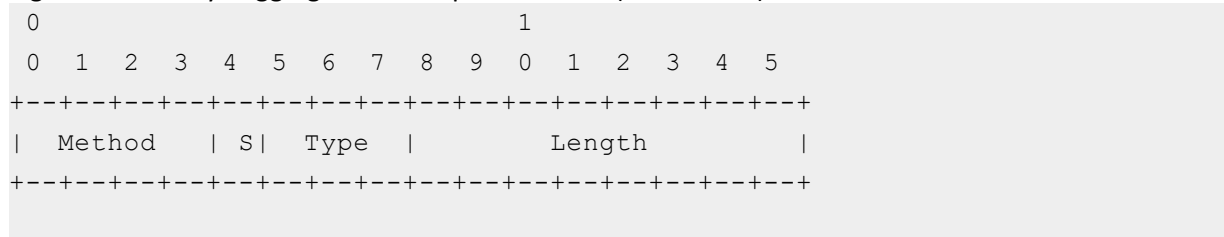
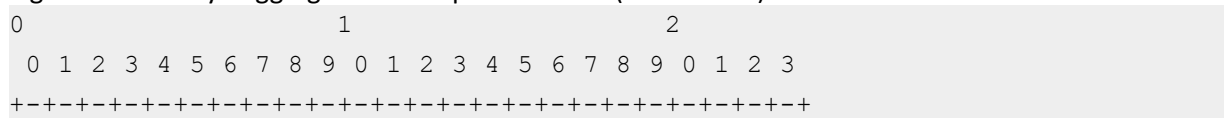


Figure 45 : Binary Logging - HTTP Request Header (ACOS 2.8.1)



Method	S	Type	Length
--------	---	------	--------

### Changes for Fixed-NAT Port Allocation

If the default port allocation is used (Use Least NAT IPs with no offset), the Fixed-NAT header is unchanged.

If an offset is specified, or if the Use All NAT IPs method is used with or without an offset, the header for Fixed-NAT user-port log messages has the following format. These changes support the new Fixed-NAT allocation methods supported in ACOS 2.8.1.

- Spare field reduced from 3 bits to 2 bits. This make room for the following new field.
- AE field (1 bit) to indicate whether an extension for the Fixed-NAT port allocation method is included:
  - Yes – 1
  - No – 0

The Length field is still 8 bits long, and indicates the total length of the header and the NAT mapping and allocation information.

[Figure 46](#) shows the format in ACOS 2.8.0. The new format in ACOS 2.8.2 is shown in [Figure 47](#).

Figure 46 : Binary Logging Format - Fixed-NAT header (ACOS 2.8.0)

0								1							
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+															
Act		Type			Spare			Length							
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+															

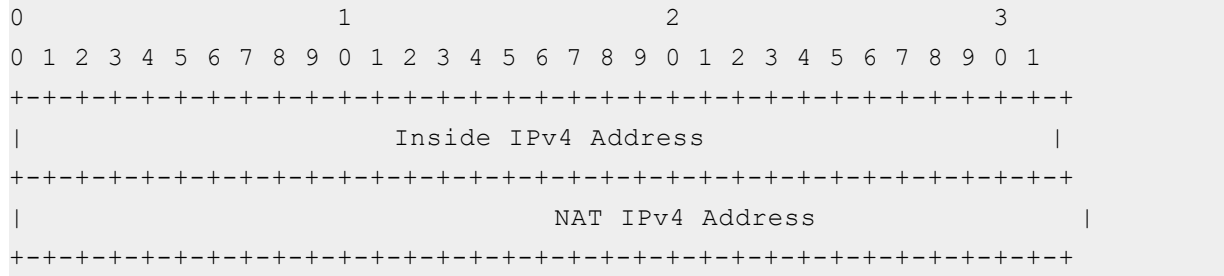
Figure 47 : Binary Logging Format - Fixed-NAT header (ACOS 2.8.2)

0								1								
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+																
Act		Type			AE	Spare			Length							
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+																

The header is followed by the NAT mapping which consists of the Inside User IP address, the NAT address and the port range information.

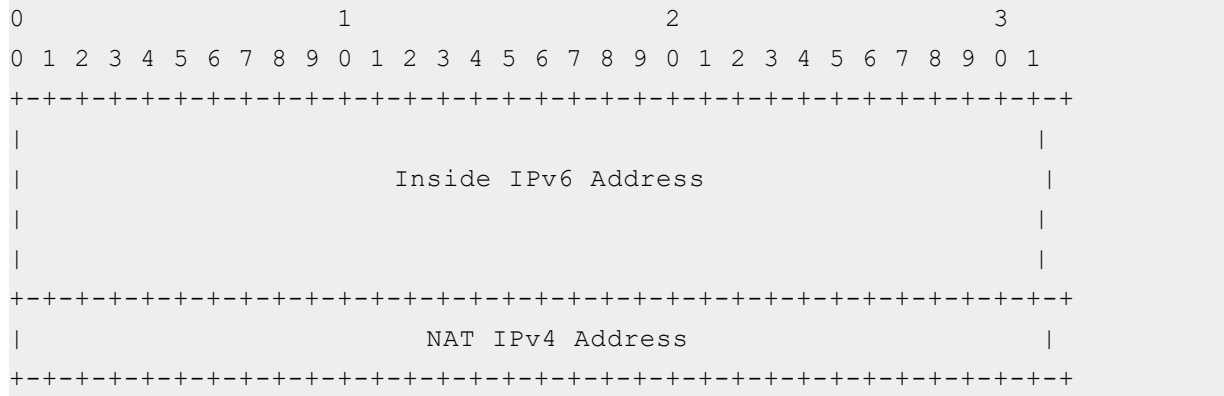
### NAT44

Figure 48 : Binary Logging Format - Fixed-NAT (NAT44)



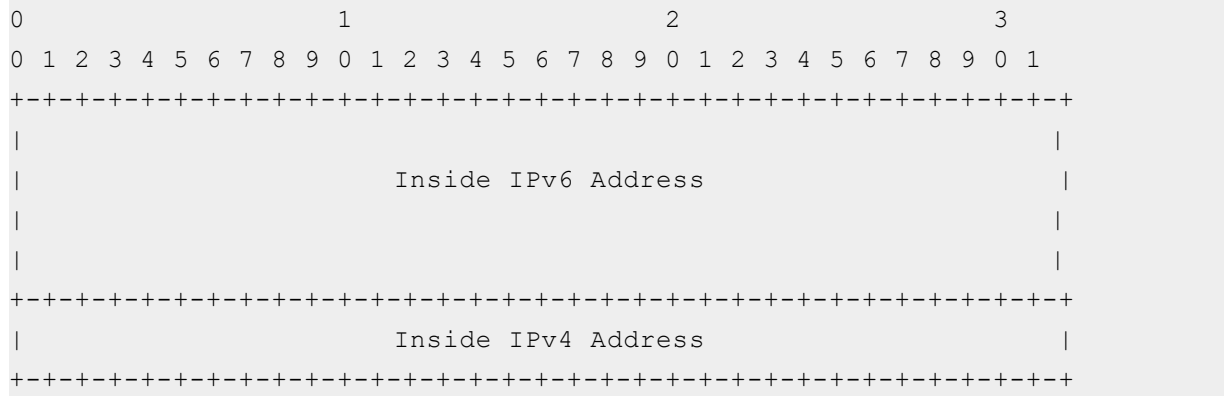
### NAT64

Figure 49 : Binary Logging Format - Fixed-NAT (NAT64)



### DS-Lite

Figure 50 : Binary Logging Format - Fixed-NAT (DS-Lite)



NAT IPv4 Address
------------------

### NAT Port information

Figure 51 : Binary Logging Format - Fixed-NAT (NAT port information)

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
Proto = 0			
Start Port		End	
Port			

### Information for Non-Default Port Allocation Methods

If a port allocation method other than the default (Use Least NAT IPs) is used, the port block allocation information appears next:

Figure 52 : Binary Logging Format - Fixed-NAT header (ACOS 2.8.0)

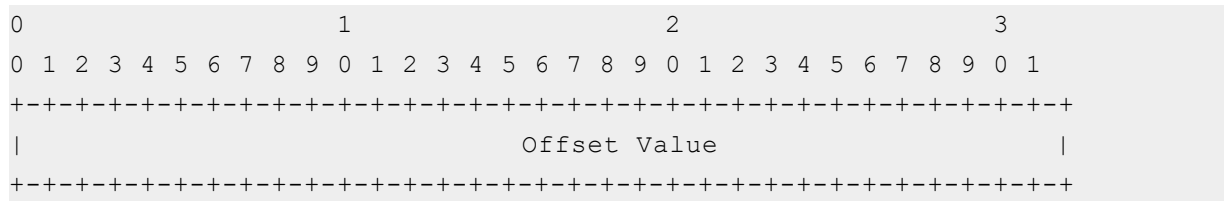
0	1	2	3	4	5	6	7
AM   OT   Spare							

The forward tuple header has the following fields:

- AM (2 bits) – Allocation Method:
  - 0 – Use least NAT IPs
  - 1 – Use all NAT IPs
- OT (2 bits) – Offset Type:
  - 0 – Default (no offset)
  - 1 – Fixed (admin-configured offset)
  - 2 – Random
- Spare (4 bits)

### Information for Non-Default Offset

If an offset type other than the default (no offset) is used, an additional 4 bytes provide the offset value:

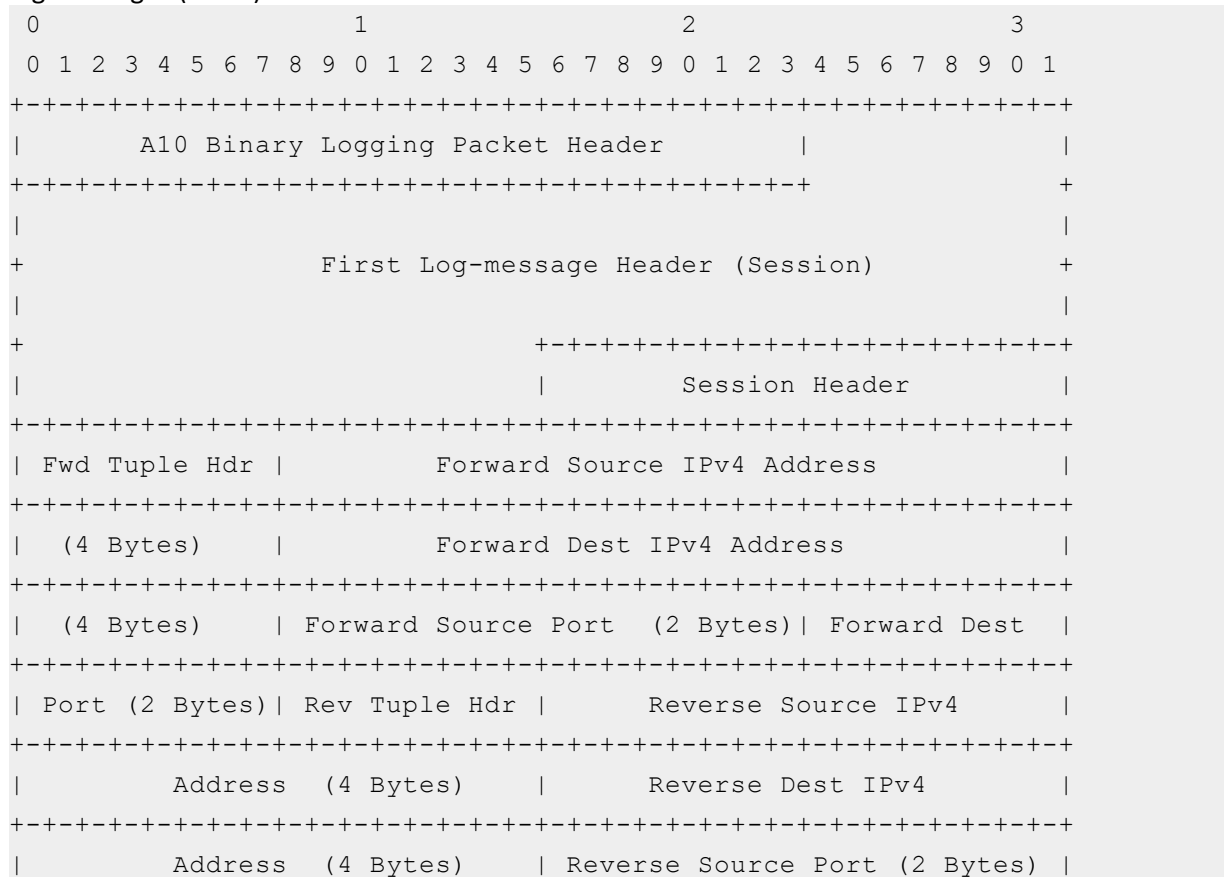


## Binary Log Packet Examples

This section shows examples of external logging packets in A10 binary format.

### Session Creation/Deletion and Port Mapping

Figure 53 : Binary Logging Format - packet containing session and port-mapping (with extensions) log messages (1 of 2)



```

+-----+
| Reverse Dest Port (2 Bytes) |
+-----+
|
|
...
    
```

**Example**

Figure 54 : Binary Logging Format - packet containing session and port-mapping (with extensions) log messages (2 of 2)

```

+-----+
|
+           Second Log-message Header (Port Mapping)
|
+           +-----+
|           | Port Mapping Header | Inside |
+-----+
|           IPv4 Address           | NAT |
+-----+
|           IPv4 Address           | Inside |
+-----+
| Port | NAT Port | Extension |
+-----+
| Header | Destination Port | Destination |
+-----+
|           IPv4 Address           |
+-----+
    
```

**Port Mapping**

Figure 55 : Binary Logging Format - packet containing a single port-mapping (with extensions) log message

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+
| A10 Binary Logging Packet Header |
+-----+
|
+           First Log-message Header
|
+           +-----+
|           | Port Mapping Header |
+-----+
    
```



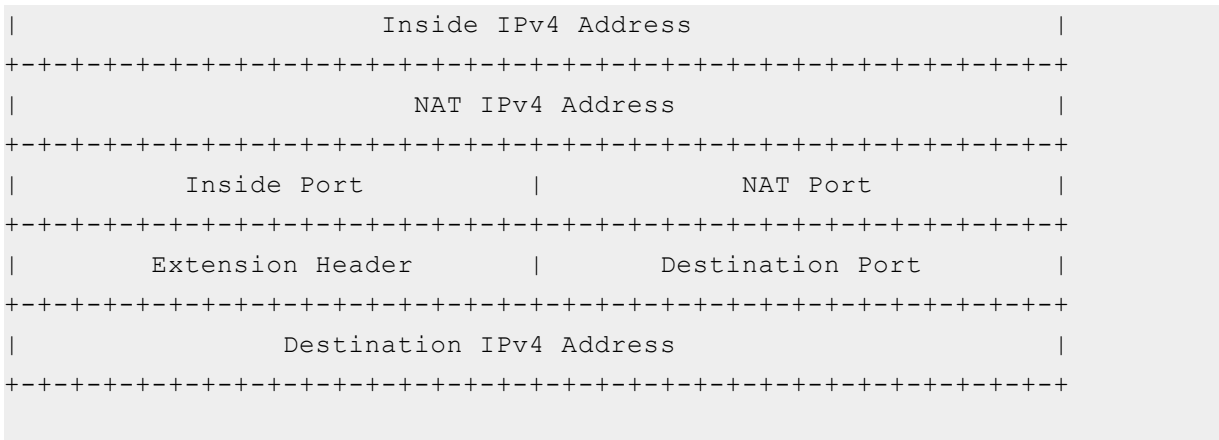
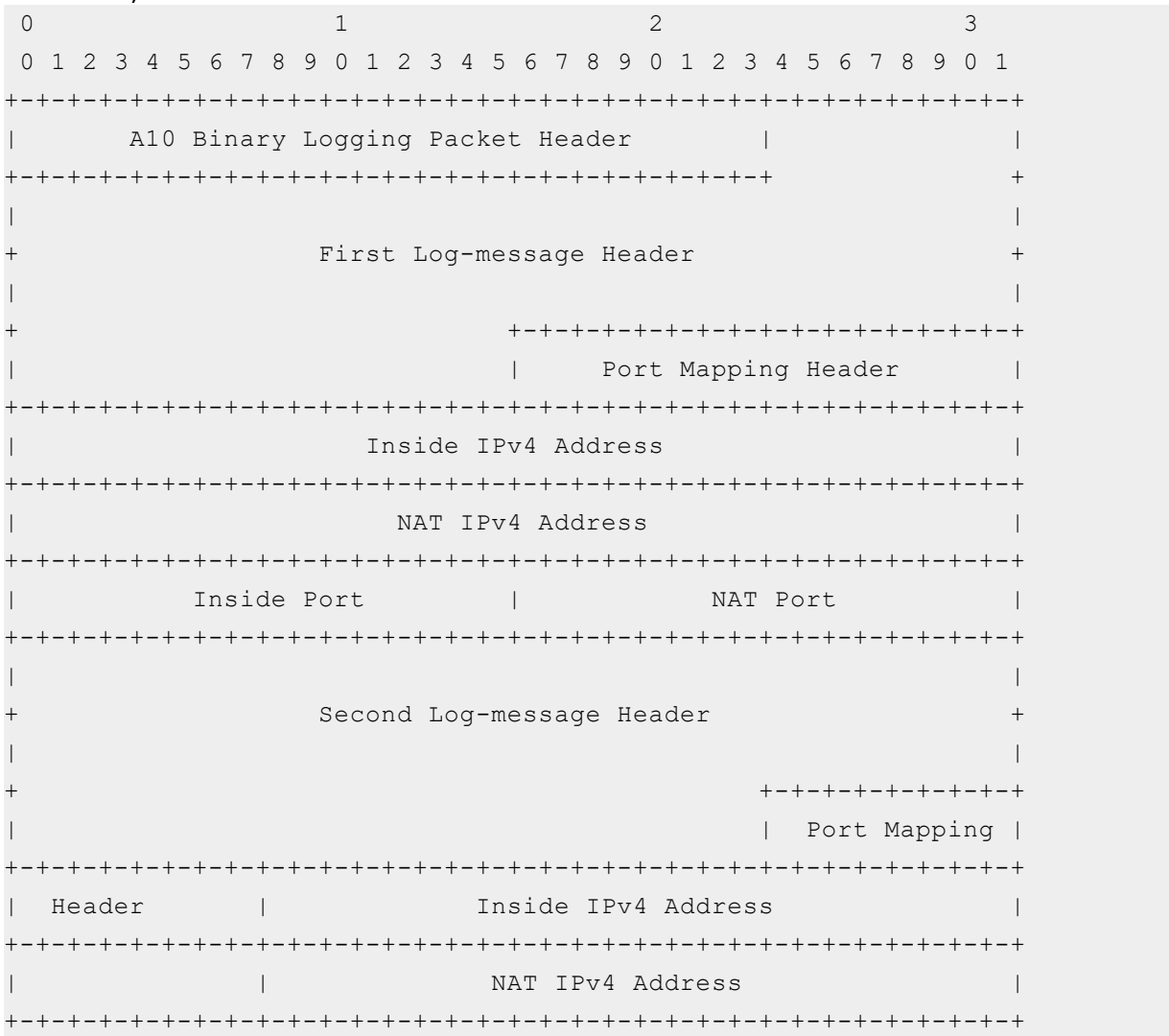


Figure 56 : Binary Logging Format - packet containing two port-mapping log messages (without extensions)



	Inside Port	NAT
Port		

## HTTP Request and RADIUS Attribute Logging

Figure 57 : Binary Logging Format - include client mobile number obtained from RADIUS

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
A10 Binary Logging Packet Header			
Log-message Header (port-mapping)			
Port Mapping Header			
Inside IPv4 Address			
NAT IPv4 Address			
Inside Port		NAT Port	
Extension Header (Dest)		Destination Port	
Destination IPv4 Address			
Extension Header (MSISDN)		MSISDN (Hex)	
MSISDN (Hex)		Extension Header (IMEI)	
IMEI (Hex)			

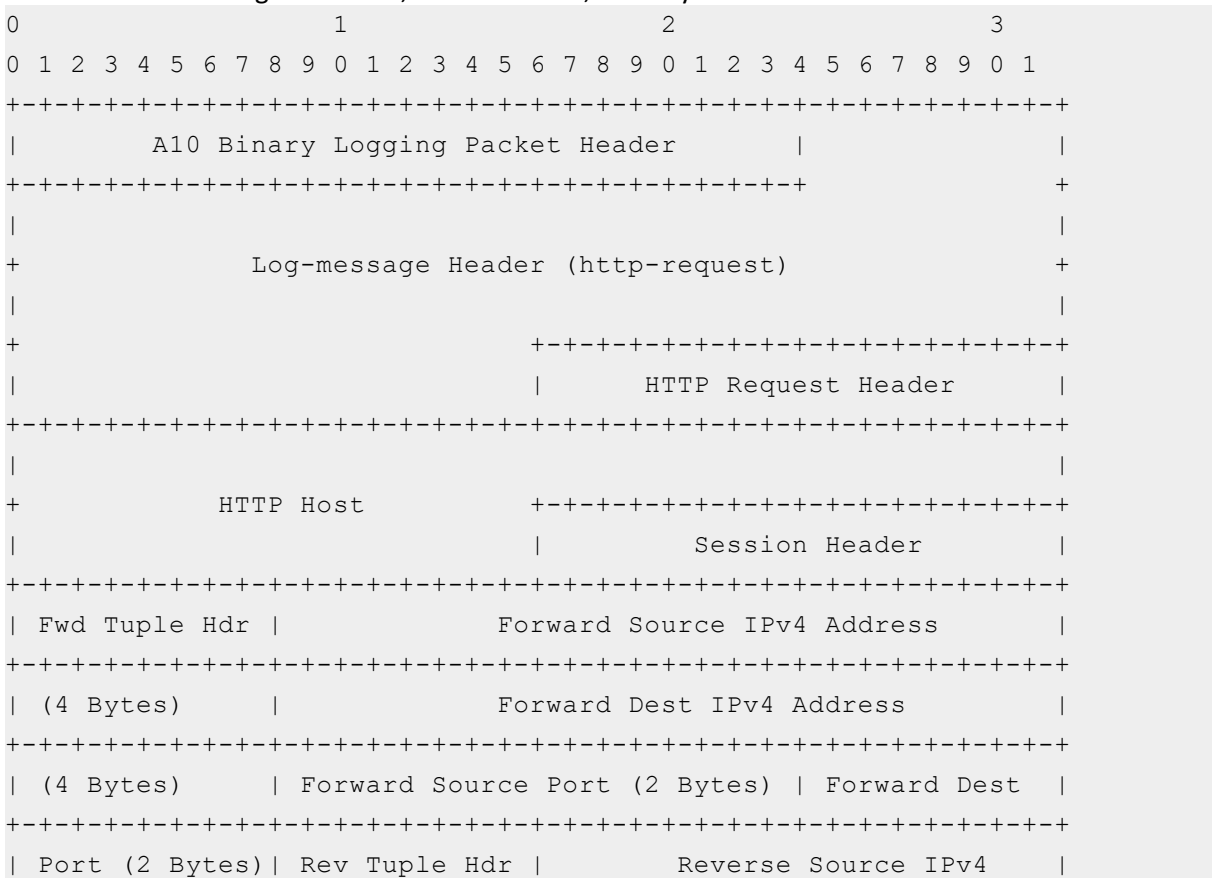
Figure 58 : Binary Logging Format - include client mobile number (MSISDN), HTTP request information including URL, and HTTP method

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			

Appendix: Log Message References



Figure 59 : Binary Logging Format - include client mobile number (MSISDN), HTTP request information including hostname, HTTP method, and Layer 4 session information



```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Address (4 Bytes)          |          Reverse Dest IPv4          |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Address (4 Bytes)          | Reverse Source Port (2 Bytes) |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Reverse Dest Port (2 Bytes) | Extension Header (MSISDN) |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                               MSISDN (Hex)                               |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
    
```

### Fixed-NAT

Figure 60 : Binary Logging Format - Fixed-NAT port assignment

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Fixed-NAT Ports Log Header |          Inside IPv4          |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Address          |          NAT IPv4          |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Address          | Proto = 0 | Port Range |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Start | Port Range End |
+-----+-----+-----+-----+-----+-----+
    
```

Figure 61 : Binary Logging Format - Fixed-NAT port delete

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Fixed-NAT Ports Log Header |          Inside IPv4          |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Address          |          NAT IPv4          |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Address          |
+-----+-----+-----+-----+-----+-----+
    
```

### Traffic Logs in CEF Format

This section provides the CEF log samples.



## NAT Session Created

---

```
May 24 23:06:40 AX2500/shared AX2500 CEF:0|A10 NETWORKS|AX Series Advanced Traffic Manager|4.1|106|Nat Session Created|5|proto=TCP src=3.3.3.89 spt=32038 dst=15.15.15.90 dpt=80 sourceTranslatedAddress=15.15.15.100 sourceTranslatedPort=32038 destinationTranslatedAddress=15.15.15.90 destinationTranslatedPort=80<135> May 24 23:06:40 AX2500/shared AX2500 CEF:0|A10 NETWORKS|AX Series Advanced Traffic Manager|4.1|104|Nat Port Allocated|5|proto=TCP src=3.3.3.89 spt=32038 sourceTranslatedAddress=15.15.15.100 sourceTranslatedPort=32038 dst=15.15.15.90 dpt=80 smac=00:0c:29:c8:17:7d
```

## NAT Session Deleted

---

```
May 24 23:06:44 AX2500/shared AX2500 CEF:0|A10 NETWORKS|AX Series Advanced Traffic Manager|4.1|107|Nat Session Freed|5|proto=TCP src=3.3.3.89 spt=32038 dst=15.15.15.90 dpt=80 sourceTranslatedAddress=15.15.15.100 sourceTranslatedPort=32038 destinationTranslatedAddress=15.15.15.90 destinationTranslatedPort=80<135> May 24 23:06:44 AX2500/shared AX2500 CEF:0|A10 NETWORKS|AX Series Advanced Traffic Manager|4.1|105|Nat Port Freed|5|proto=TCP src=3.3.3.89 spt=32038 sourceTranslatedAddress=15.15.15.100 sourceTranslatedPort=32038
```

## NAT Port Allocated

---

```
May 25 00:19:03 AX2500/shared AX2500 CEF:0|A10 NETWORKS|AX Series Advanced Traffic Manager|4.1|104|Nat Port Allocated|5|proto=UDP src=3.3.3.89 spt=32165 sourceTranslatedAddress=15.15.15.100 sourceTranslatedPort=32165 dst=15.15.15.90 dpt=32165 smac=00:0c:29:c8:17:7d<135> May 25 00:19:03 AX2500/shared AX2500 CEF:0|A10 NETWORKS|AX Series Advanced Traffic Manager|4.1|106|Nat Session Created|5|proto=UDP src=3.3.3.89 spt=32165 dst=15.15.15.90 dpt=32165 sourceTranslatedAddress=15.15.15.100 sourceTranslatedPort=32165 destinationTranslatedAddress=15.15.15.90 destinationTranslatedPort=32165
```

## NAT Port Freed

---

```
May 24 00:19:03 AX2500/shared AX2500 CEF:0|A10 NETWORKS|AX Series Advanced  
Traffic Manager|4.1|105|Nat Port Freed|5|proto=TCP src=3.3.3.89 spt=32252  
sourceTranslatedAddress=15.15.15.150 sourceTranslatedPort=41327
```

## Port Batch Allocated

---

```
May 25 00:19:03 AX2500/shared AX2500 CEF:0|A10 NETWORKS|AX Series Advanced  
Traffic Manager|4.1|108|Nat Port Batch Allocated|5|proto=TCP src=3.3.3.89  
sourceTranslatedAddress=15.15.15.100 sourceTranslatedPort=12980 cn1=16  
cn2=5 smac=00:0c:29:c8:17:7d cn1Label=Number of Ports cn2Label=Port  
Interval<135>
```

## Port Batch Freed

---

```
May 24 00:19:03 AX2500/shared AX2500 CEF:0|A10 NETWORKS|AX Series Advanced  
Traffic Manager|4.1|109|Nat Port Batch Freed|5|proto=TCP src=3.3.3.89  
sourceTranslatedAddress=15.15.15.100 sourceTranslatedPort=12980 cn1=16  
cn2=5 cn1Label=Number of Ports cn2Label=Port Interval<135>
```

## Fixed NAT Port Assigned

---

```
May 25 00:19:03 AX2500/shared AX2500 CEF:0|A10 NETWORKS|AX Series Advanced  
Traffic Manager|4.1|113|Fixed Nat Port Assigned|5| src=3.3.3.89  
sourceTranslatedAddress=15.15.15.130 cn1=1024 cn2=65535 cs1=Use All IPs  
cn3=0 cs2=Offset Random cn1Label=Fixed Nat Port Start cn2Label= Fixed Nat  
Port End cs1Label=Fixed Nat Alloc Type cs2Label=Offset Type
```

## Fixed NAT Port Disabled

---

```
May 24 00:19:03 AX2500/shared AX2500 CEF:0|A10 NETWORKS|AX Series Advanced  
Traffic Manager|4.1|114|Fixed Nat Port Disabled|5| src=3.3.3.89  
sourceTranslatedAddress=15.15.15.130
```

## RADIUS Message Formats

This section provides the several examples for RADIUS message formats. To read the RADIUS messages, use [RADIUS Dictionary](#).

For information on how to configure RADIUS messages, see [Logging to RADIUS](#).

The following topics are covered:

<a href="#">Port Mapping Created Message</a> .....	288
<a href="#">Port Mapping Freed Message</a> .....	289
<a href="#">Port Batch Allocated Message</a> .....	290
<a href="#">Port Batch Freed Message</a> .....	290
<a href="#">Fixed-NAT Port Range Allocated Message</a> .....	291
<a href="#">Fixed-NAT Port Range Freed Message</a> .....	294
<a href="#">Session Created Message</a> .....	294
<a href="#">Session Deleted Message</a> .....	295
<a href="#">RADIUS Dictionary File</a> .....	296

### Port Mapping Created Message

---

```
Accounting Request {
  Header : {
    Packet Code=0x04 (1 octet)
    Id=0x5D (1 octet)
    Length = XXX (2 octets)
    Request Authenticator = 0123456789ABCDEF (16 octets)
  }
  Attributes : {
    Acct-Status-Type : Integer Value = 1 (4 octets)
    Acct-Session-Id : String Value = 000032384DDFB3..26 (16 octets)
    NAS-ID : Address Value = ACOS@10.10.10.110 (MAX 50 octets)
    Vendor-Specific: String Value= {
      A10-CGN-Timestamp : String Value = 1329235583 (8 octets)
      A10-CGN-Protocol : Integer Value = 1 (4 octets)
      A10-CGN-Action: Integer Value = 1 (4 octets)
    }
  }
}
```

```

        A10-CGN-Inside-Addr : String Value = 192.168.150.100 (4
octets)
        A10-CGN-Inside-Port : String Value = 32585 (2 octets)
        A10-CGN-Nat-Addr : String Value = 2.2.2.1 (4 octets)
        A10-CGN-Nat-Port : String Value = 5660 (2 octets)
    }
}
}

```

## Port Mapping Freed Message

```

Accounting Request {
  Header : {
    Packet Code=0x04 (1 octet)
    Id=0x5E (1 octet)
    Length = XXX (2 octets)
    Request Authenticator = 0123456789ABCDEF (16 octets)
  }
  Attributes : {
    Acct-Status-Type : Integer Value = 2 (4 octets)
    Acct-Session-Id : String Value = 000032384DDFB3..26 (16 octets)
    NAS-ID : Address Value = ACOS@10.10.10.110 (MAX 50 octets)
    Vendor-Specific: String Value= {
      A10-CGN-Timestamp : String Value = 1329235583 (8 octets)
      A10-CGN-Protocol : Integer Value = 1 (4 octets)
      A10-CGN-Action: Integer Value = 2 (4 octets)
      A10-CGN-Inside-Addr : String Value = 192.168.150.100 (4
octets)
      A10-CGN-Inside-Port : String Value = 32585 (2 octets)
      A10-CGN-Nat-Addr : String Value = 2.2.2.1 (4 octets)
      A10-CGN-Nat-Port : String Value = 5660 (2 octets)
    }
  }
}
}

```

## Port Batch Allocated Message

```
Accounting Request {
  Header : {
    Packet Code=0x04 (1 octet)
    Id=0x5D (1 octet)
    Length = XXX (2 octets)
    Request Authenticator = 0123456789ABCDEF (16 octets)
  }
  Attributes : {
    Acct-Status-Type : Integer Value = 1 (4 octets)
    Acct-Session-Id : String Value = 000032384DDFB3..26 (16 octets)
    NAS-ID : Address Value = ACOS@10.10.10.110 (MAX 50 octets)
    Vendor-Specific: String Value= {
      A10-CGN-Timestamp : String Value = 1329235583 (8 octets)
      A10-CGN-Protocol : Integer Value = 1 (4 octets)
      A10-CGN-Action: Integer Value = 5 (4 octets)
      A10-CGN-Inside-Addr : String Value = 192.168.150.100 (4
octets)
      A10-CGN-Nat-Addr : String Value = 2.2.2.1 (4 octets)
      A10-CGN-Nat-Port : String Value = 5660 (2 octets)
      A10-CGN-Nat-Port-Batch-Size : String Value = 16 (1 octets)
      A10-CGN-Nat-Port-Batch-Step-Size : String Value = 512 (2
octets)
    }
  }
}
```

## Port Batch Freed Message

```
Accounting Request {
  Header : {
    Packet Code=0x04 (1 octet)
    Id=0x5D (1 octet)
    Length = XXX (2 octets)
    Request Authenticator = 0123456789ABCDEF (16 octets)
  }
  Attributes : {
```

```

Acct-Status-Type : Integer Value = 2 (4 octets)
Acct-Session-Id : String Value = 000032384DDFB3..26 (16 octets)
NAS-ID : Address Value = ACOS@10.10.10.110 (MAX 50 octets)
Vendor-Specific: String Value= {
    A10-CGN-Timestamp : String Value = 1329235583 (8 octets)
    A10-CGN-Protocol : Integer Value = 1 (4 octets)
    A10-CGN-Action: Integer Value = 6 (4 octets)
    A10-CGN-Inside-Addr : String Value = 192.168.150.100 (4
octets)

    A10-CGN-Nat-Addr : String Value = 2.2.2.1 (4 octets)
    A10-CGN-Nat-Port : String Value = 5660 (2 octets)
    A10-CGN-Nat-Port-Batch-Size : String Value = 16 (1 octets)
    A10-CGN-Nat-Port-Batch-Step-Size : String Value = 512 (2
octets)
A10-CGN-Port-Block-Acct-Upload-Bytes : String Value = (79) l=10 val=135779
A10-CGN-Port-Block-Acct-Download-Bytes(80) l=10 val=94326
A10-CGN-PORT_BATCH_DURATION(84) l=6 val=1437
    }
}
}

```

## Fixed-NAT Port Range Allocated Message

The message format for Fixed-NAT port range assignment differs depending on the configured assignment method:

- [Automatic Port Assignment \(Single Port per Client\)](#)
- [Automatic Port Assignment \(Multiple Ports per Client\)](#)
- [Manual Port Assignment](#)

### Automatic Port Assignment (Single Port per Client)

```

Accounting Request {
  Header : {
    Packet Code=0x04 (1 octet)
    Id=0x5D (1 octet)
    Length = XXX (2 octets)
  }
}

```

```

    Request Authenticator = 0123456789ABCDEF (16 octets)
  }
  Attributes : {
    Acct-Status-Type : Integer Value = 1 (4 octets)
    Acct-Session-Id : String Value = 000032384DDFB3..26 (16 octets)
    NAS-ID : Address Value = ACOS@10.10.10.110 (MAX 50 octets)
    Vendor-Specific: String Value= {
      A10-CGN-Timestamp : String Value = 1329235583 (8 octets)
      A10-CGN-Action: Integer Value = 7 (4 octets)
      A10-CGN-Inside-Addr : String Value = 192.168.150.100 (4
octets)
      A10-CGN-Nat-Addr : String Value = 2.2.2.1 (4 octets)
      A10-CGN-Nat-Port : String Value = 5660 (2 octets)
    }
  }
}

```

## Automatic Port Assignment (Multiple Ports per Client)

```

Accounting Request {
  Header : {
    Packet Code=0x04 (1 octet)
    Id=0x5D (1 octet)
    Length = XXX (2 octets)
    Request Authenticator = 0123456789ABCDEF (16 octets)
  }
  Attributes : {
    Acct-Status-Type : Integer Value = 1 (4 octets)
    Acct-Session-Id : String Value = 000032384DDFB3..26 (16 octets)
    NAS-ID : Address Value = ACOS@10.10.10.110 (MAX 50 octets)
    Vendor-Specific: String Value= {
      A10-CGN-Timestamp : String Value = 1329235583 (8 octets)
      A10-CGN-Action: Integer Value = 7 (4 octets)
      A10-CGN-Inside-Addr : String Value = 192.168.150.100 (4
octets)
      A10-CGN-Nat-Addr : String Value = 2.2.2.1 (4 octets)
      A10-CGN-Fixed-Nat-Port-Start : String Value = 5660 (2
octets)
      A10-CGN-Fixed-Nat-Port-End : String Value = 6660 (2 octets)
    }
  }
}

```

```

}
}

```

## Manual Port Assignment

```

Accounting Request {
  Header : {
    Packet Code=0x04 (1 octet)
    Id=0x5D (1 octet)
    Length = XXX (2 octets)
    Request Authenticator = 0123456789ABCDEF (16 octets)
  }
  Attributes : {
    Acct-Status-Type : Integer Value = 1 (4 octets)
    Acct-Session-Id : String Value = 000032384DDFB3..26 (16 octets)
    NAS-ID : Address Value = ACOS@10.10.10.110 (MAX 50 octets)
    Vendor-Specific: String Value= {
      A10-CGN-Timestamp : String Value = 1329235583 (8 octets)
      A10-CGN-Action: Integer Value = 7 (4 octets)
      A10-CGN-Inside-Addr : String Value = 192.168.150.100 (4
octets)
      A10-CGN-Nat-Addr : String Value = 2.2.2.1 (4 octets)
      A10-CGN-Protocol : Integer Value = 1 (4 octets)
      A10-CGN-Fixed-Nat-Port-Start : String Value = 5660 (2
octets)
      A10-CGN-Fixed-Nat-Port-End : String Value = 6660 (2 octets)
      A10-CGN-Protocol : Integer Value = 2 (4 octets)
      A10-CGN-Fixed-Nat-Port-Start : String Value = 5660 (2
octets)
      A10-CGN-Fixed-Nat-Port-End : String Value = 6660 (2 octets)
      A10-CGN-Protocol : Integer Value = 3 (4 octets)
      A10-CGN-Fixed-Nat-Port-Start : String Value = 5660 (2
octets)
      A10-CGN-Fixed-Nat-Port-End : String Value = 6660 (2 octets)
    }
  }
}

```

## Fixed-NAT Port Range Freed Message

```
Accounting Request {
  Header : {
    Packet Code=0x04 (1 octet)
    Id=0x5D (1 octet)
    Length = XXX (2 octets)
    Request Authenticator = 0123456789ABCDEF (16 octets)
  }
  Attributes : {
    Acct-Status-Type : Integer Value = 2 (4 octets)
    Acct-Session-Id : String Value = 000032384DDFB3..26 (16 octets)
    NAS-ID : Address Value = ACOS@10.10.10.110 (MAX 50 octets)
    Vendor-Specific: String Value= {
      A10-CGN-Timestamp : String Value = 1329235583 (8 octets)
      A10-CGN-Action: Integer Value = 8 (4 octets)
      A10-CGN-Inside-Addr : String Value = 192.168.150.100 (4
octets)
      A10-CGN-NAT-Addr : String Value = 2.2.2.1 (4 octets)
    }
  }
}
```

## Session Created Message

```
Accounting Request {
  Header : {
    Packet Code=0x04 (1 octet)
    Id=0x5D (1 octet)
    Length = XXX (2 octets)
    Request Authenticator = 0123456789ABCDEF (16 octets)
  }
  Attributes : {
    Acct-Status-Type : Integer Value = 1 (4 octets)
    Acct-Session-Id : String Value = 000032384DDFB3..26 (16 octets)
    NAS-ID : Address Value = ACOS@10.10.10.110 (MAX 50 octets)
    Vendor-Specific: String Value= {
      A10-CGN-Timestamp : String Value = 1329235583 (8 octets)
      A10-CGN-Protocol : Integer Value = 1 (4 octets)
    }
  }
}
```

```

    A10-CGN-Action: Integer Value = 3 (4 octets)
    A10-CGN-Inside-Addr : String Value = 192.168.150.100 (4
octets)

    A10-CGN-Inside-Port : String Value = 32585 (2 octets)
    A10-CGN-Nat-Addr : String Value = 2.2.2.1 (4 octets)
    A10-CGN-Nat-Port : String Value = 5660 (2 octets)
    A10-CGN-Dest-Addr : String Value = 3.3.3.1 (4 octets)
    A10-CGN-Dest-Port : Integer Value = 8080 (2 octets)
    A10-CGN-Nat-Dest-Addr : String Value = 3.3.3.1 (4 octets)
    A10-CGN-Nat-Dest-Port : Integer Value = 8080 (2 octets)
  }
}
}

```

## Session Deleted Message

```

Accounting Request {
  Header : {
    Packet Code=0x04 (1 octet)
    Id=0x5E (1 octet)
    Length = XXX (2 octets)
    Request Authenticator = 0123456789ABCDEF (16 octets)
  }

  Attributes : {
    Acct-Status-Type : Integer Value = 2 (4 octets)
    Acct-Session-Id : String Value = 000032384DDFB3..26 (16 octets)
    NAS-ID : Address Value = ACOS@10.10.10.110 (MAX 50 octets)
    Vendor-Specific: String Value= {
      A10-CGN-Timestamp : String Value = 1329235583 (8 octets)
      A10-CGN-Protocol : Integer Value = 1 (4 octets)
      A10-CGN-Action: Integer Value = 4 (4 octets)
      A10-CGN-Inside-Addr : String Value = 192.168.150.100 (4
octets)

      A10-CGN-Inside-Port : String Value = 32585 (2 octets)
      A10-CGN-Nat-Addr : String Value = 2.2.2.1 (4 octets)
      A10-CGN-Nat-Port : String Value = 5660 (2 octets)
      A10-CGN-Dest-Addr : String Value = 3.3.3.1 (4 octets)
      A10-CGN-Dest-Port : Integer Value = 8080 (2 octets)
      A10-CGN-Nat-Dest-Addr : String Value = 3.3.3.1 (4 octets)
    }
  }
}

```

```
        A10-CGN-Nat-Dest-Port : Integer Value = 8080 (2 octets)
    }
}
}
```

## RADIUS Dictionary File

---

For reference, this section shows the RADIUS dictionary file supported.

```
# A10 Networks dictionary.
#
VENDOR      A10-Networks      22610
```

```

BEGIN-VENDOR A10-Networks

#
#   Admin
#
ATTRIBUTE   A10-App-Name           1   string
ATTRIBUTE   A10-Admin-Privilege   2   integer
ATTRIBUTE   A10-Admin-Partition   3   string
ATTRIBUTE   A10-Admin-Access-Type 4   string
ATTRIBUTE   A10-Admin-Role        5   string

VALUE       A10-Admin-Privilege   Read-only-Admin      1
VALUE       A10-Admin-Privilege   Read-write-Admin     2
VALUE       A10-Admin-Privilege   System-Admin         3
VALUE       A10-Admin-Privilege   Network-Admin        4
VALUE       A10-Admin-Privilege   Network-Operator     5
VALUE       A10-Admin-Privilege   Slb-Service-Admin    6
VALUE       A10-Admin-Privilege   Slb-Service-Operator 7
VALUE       A10-Admin-Privilege   Partition-Read_write 8
VALUE       A10-Admin-Privilege   Partition-Network-Operator 9
VALUE       A10-Admin-Privilege   Partition-SlbService-Admin 10
VALUE       A10-Admin-Privilege   Partition-SlbService-Operator 11
VALUE       A10-Admin-Privilege   Partition-Read-Only 12

#
#   CGN accounting
#
ATTRIBUTE   A10-CGN-Timestamp      6   date
ATTRIBUTE   A10-CGN-Protocol       7   integer
ATTRIBUTE   A10-CGN-Port-Batch-Size 8   short
ATTRIBUTE   A10-CGN-Port-Batch-Step-Size 9   short
ATTRIBUTE   A10-CGN-Inside-Addr    10  ipaddr
ATTRIBUTE   A10-CGN-Inside-Port    11  short
ATTRIBUTE   A10-CGN-NAT-Addr       12  ipaddr
ATTRIBUTE   A10-CGN-NAT-Port       13  short
ATTRIBUTE   A10-CGN-Dest-Addr      14  ipaddr
ATTRIBUTE   A10-CGN-Dest-Port      15  short
ATTRIBUTE   A10-CGN-NAT-Dest-Addr  16  ipaddr

```

## Appendix: Log Message References

ATTRIBUTE	A10-CGN-NAT-Dest-Port	17	short
ATTRIBUTE	A10-CGN-Fixed-NAT-Port-Start	18	short
ATTRIBUTE	A10-CGN-Fixed-NAT-Port-End	19	short
VALUE	A10-CGN-Protocol	TCP	1
VALUE	A10-CGN-Protocol	UDP	2
VALUE	A10-CGN-Protocol	ICMP	3
VALUE	A10-CGN-Protocol	IP	4
VALUE	A10-CGN-Protocol	GRE	5
VALUE	A10-CGN-Protocol	RTSP	6
VALUE	A10-CGN-Protocol	OTHER	0
ATTRIBUTE	A10-CGN-Action	20	integer
VALUE	A10-CGN-Action	Port-Allocated	1
VALUE	A10-CGN-Action	Port-Freed	2
VALUE	A10-CGN-Action	Session-Created	3
VALUE	A10-CGN-Action	Session-Deleted	4
VALUE	A10-CGN-Action	Port-Batch-Allocated	5
VALUE	A10-CGN-Action	Port-Batch-Freed	6
VALUE	A10-CGN-Action	Fixed-NAT-Port-Range-Allocated	7
VALUE	A10-CGN-Action	Fixed-NAT-Port-Range-Freed	8
VALUE	A10-CGN-Action	MSISDN-Query	9
VALUE	A10-CGN-Action	HTTP-Request-Got	10
VALUE	A10-CGN-Action	Port-Batch-Pool-Allocated	11
VALUE	A10-CGN-Action	Port-Batch-Pool-Freed	12
VALUE	A10-CGN-Action	MAP-DHCPv6-Prefix-Assigned	13
VALUE	A10-CGN-Action	MAP-DHCPv6-Prefix-Renewed	14
VALUE	A10-CGN-Action	MAP-DHCPv6-Prefix-Released	15
VALUE	A10-CGN-Action	Pool-Port-Batch-interim-update	16
ATTRIBUTE	A10-CGN-Response	21	integer
VALUE	A10-CGN-Response	Success	1
VALUE	A10-CGN-Response	Failure	2
ATTRIBUTE	A10-CGN-HTTP-Request-Method	22	integer

## Appendix: Log Message References

VALUE	A10-CGN-HTTP-Request-Method	GET	1
VALUE	A10-CGN-HTTP-Request-Method	HEAD	2
VALUE	A10-CGN-HTTP-Request-Method	PUT	3
VALUE	A10-CGN-HTTP-Request-Method	POST	4
VALUE	A10-CGN-HTTP-Request-Method	OPTIONS	5
VALUE	A10-CGN-HTTP-Request-Method	DELETE	6
VALUE	A10-CGN-HTTP-Request-Method	TRACE	7
VALUE	A10-CGN-HTTP-Request-Method	CONNECT	8
ATTRIBUTE	A10-CGN-HTTP-Host	23	string
ATTRIBUTE	A10-CGN-HTTP-Url	24	string
ATTRIBUTE	A10-CGN-MSISDN	25	string
ATTRIBUTE	A10-CGN-IMEI	26	string
ATTRIBUTE	A10-CGN-IMSI	27	string
ATTRIBUTE	A10-CGN-Timestamp-Millisecond	28	octets
ATTRIBUTE	A10-CGN-Inside-IPv6-Addr	29	ipv6addr
ATTRIBUTE	A10-CGN-NAT-IPv6-Addr	30	ipv6addr
ATTRIBUTE	A10-CGN-Dest-IPv6-Addr	31	ipv6addr
ATTRIBUTE	A10-CGN-NAT-Dest-IPv6-Addr	32	ipv6addr
ATTRIBUTE	A10-CGN-Inside-Tunnel-Addr	33	ipaddr
ATTRIBUTE	A10-CGN-NAT-Tunnel-Addr	34	ipaddr
ATTRIBUTE	A10-CGN-Dest-Tunnel-Addr	35	ipaddr
ATTRIBUTE	A10-CGN-NAT-Dest-Tunnel-Addr	36	ipaddr
ATTRIBUTE	A10-CGN-Inside-Tunnel-IPv6-Addr	37	ipv6addr
ATTRIBUTE	A10-CGN-NAT-Tunnel-IPv6-Addr	38	ipv6addr
ATTRIBUTE	A10-CGN-Dest-Tunnel-IPv6-Addr	39	ipv6addr
ATTRIBUTE	A10-CGN-NAT-Dest-Tunnel-IPv6-Addr	40	ipv6addr
ATTRIBUTE	A10-CGN-Inside-User-MAC	41	ether
ATTRIBUTE	A10-CGN-Radius-Custom-1	42	string
ATTRIBUTE	A10-CGN-Radius-Custom-2	43	string
ATTRIBUTE	A10-CGN-Radius-Custom-3	44	string
ATTRIBUTE	A10-CGN-Request-Size	45	integer
ATTRIBUTE	A10-CGN-Response-Size	46	integer
ATTRIBUTE	A10-CGN-HTTP-Request-Number	47	integer
ATTRIBUTE	A10-CGN-HTTP-Cookie	48	string

## Appendix: Log Message References

ATTRIBUTE	A10-CGN-HTTP-Referer	49	string	
ATTRIBUTE	A10-CGN-HTTP-User-Agent	50	string	
ATTRIBUTE	A10-CGN-HTTP-Header1	51	string	
ATTRIBUTE	A10-CGN-HTTP-Header2	52	string	
ATTRIBUTE	A10-CGN-HTTP-Header3	53	string	
ATTRIBUTE	A10-CGN-Fixed-NAT-Alloc-Method	54	integer	
VALUE	A10-CGN-Fixed-NAT-Alloc-Method	Use-Least-IPs		0
VALUE	A10-CGN-Fixed-NAT-Alloc-Method	Use-All-IPs		1
ATTRIBUTE	A10-CGN-Fixed-NAT-Offset-Type	55	integer	
VALUE	A10-CGN-Fixed-NAT-Offset-Type	Default		0
VALUE	A10-CGN-Fixed-NAT-Offset-Type	Fixed		1
VALUE	A10-CGN-Fixed-NAT-Offset-Type	Random		2
ATTRIBUTE	A10-CGN-Fixed-NAT-Offset-Value	56	integer	
ATTRIBUTE	A10-CGN-Session-Created-Timestamp			57 date
ATTRIBUTE	A10-CGN-Session-Created-Timestamp-Millisecond			58 octets
ATTRIBUTE	A10-CGN-Port-Batch-Pool-Port-Start			59 short
ATTRIBUTE	A10-CGN-Port-Batch-Pool-Port-End			60 short
ATTRIBUTE	A10-CGN-HTTP-File-Extension			61 string
ATTRIBUTE	A10-CGN-Session-Forward-Bytes			62 integer
ATTRIBUTE	A10-CGN-Session-Reverse-Bytes			63 integer
ATTRIBUTE	A10-CGN-MAP-DHCPv6-Type			64 short
ATTRIBUTE	A10-CGN-MAP-DHCPv6-DUID-Type			65 short
ATTRIBUTE	A10-CGN-MAP-DHCPv6-DUID-Time			66 integer
ATTRIBUTE	A10-CGN-MAP-DHCPv6-DUID-Length			67 integer
ATTRIBUTE	A10-CGN-MAP-DHCPv6-DUID-HW-Type			68 integer
ATTRIBUTE	A10-CGN-MAP-DHCPv6-DUID-ENT-NUM			69 integer
ATTRIBUTE	A10-CGN-MAP-DHCPv6-DUID-Data			70 string
ATTRIBUTE	A10-CGN-MAP-DHCPv6-IAID			71 integer
ATTRIBUTE	A10-CGN-MAP-DHCPv6-Prefix			72 ipaddr
ATTRIBUTE	A10-CGN-MAP-DHCPv6-Prefix-Length			73 integer
ATTRIBUTE	A10-CGN-MAP-DHCPv6-Prefix-Type			74 short
ATTRIBUTE	A10-CGN-MAP-DHCPv6-Prefix-PSID			75 integer

ATTRIBUTE	A10-CGN-MAP-DHCPv6-Prefix-PSID-Length	76	short
ATTRIBUTE	A10-CGN-MAP-DHCPv6-Prefix-PSID-Offset	77	short
ATTRIBUTE	A10-CGN-MAP-DHCPv6-Domain-Name	78	string
ATTRIBUTE	A10-CGN-Port-Block-Acct-Upload-Bytes	79	integer
ATTRIBUTE	A10-CGN-Port-Block-Acct-Download-Bytes	80	integer
ATTRIBUTE	A10_CGN_RADIUS_ATTRIBUTE_CUSTOM4	81	integer
ATTRIBUTE	A10_CGN_RADIUS_ATTRIBUTE_CUSTOM5	82	integer
ATTRIBUTE	A10_CGN_RADIUS_ATTRIBUTE_CUSTOM6	83	integer
ATTRIBUTE	A10_CGN_PORT_BATCH_DURATION	84	integer
END-VENDOR	A10-Networks		

## Port Batch Log Messages

### Log Examples for Port Batch Allocation

Here are some examples of log messages that are generated when port batching is enabled.

#### LSN Messages (Batch Size 8)

```
Jan 23 14:33:30 Jan 23 13:27:35 AX5200-11 NAT-UDP-B: 30.30.30.11 ->
162.168.20.220:36448,8,23
Jan 23 14:34:19 Jan 23 13:28:24 AX5200-11 NAT-UDP-X: 30.30.30.11 ->
162.168.20.220:36448,8,23
```

#### DS-Lite Messages (Batch Size 16)

```
Jan 23 14:28:33 Jan 23 13:22:39 AX5200-11 NAT-UDP-B: [5001::2]30.30.30.11
-> 162.168.30.240:43076,16,23
Jan 23 14:29:15 Jan 23 13:23:21 AX5200-11 NAT-UDP-X: [5001::2]30.30.30.11
-> 162.168.30.240:43076,16,23
```

## NAT64 Messages (Batch Size 8)

```
Jan 23 14:37:24 Jan 23 13:31:29 AX5200-11 NAT-UDP-B:  
[5001:0:200:0:20f:1fff:fe65:b615] -> 162.168.20.220:31498,8,23  
Jan 23 14:37:51 Jan 23 13:31:56 AX5200-11 NAT-UDP-X:  
[5001:0:200:0:20f:1fff:fe65:b615] -> 162.168.20.220:31498,8,23
```

## Message Content

Each port-batching log message contains the following information:

```
Timestamp ACOS-hostname NAT-protocol-code: Client-IP-address ->  
NAT-address:starting-port,batch-size,assignment-increment
```

- Timestamp – ACOS system timestamp when the log message was sent.
- ACOS hostname – ACOS device that sent the log.
- NAT-protocol-code – Protocol and activity.

The protocol value can be TCP or UDP. The code can be one of the following:

- B – Batch assigned
- X – Batch freed
- Client IP address
- NAT address
- Protocol port information:
  - starting-port – Beginning port number of the batch.
  - batch-size – Number of ports in the batch.
  - assignment-increment – Number of port numbers between each port added to the batch.

For example, *31498,8,23* indicates that the starting port in the batch is *31498*, the batch size is *8*, and every 23rd port that starts with *31498* is included in the batch.

## Port Batch v2 Logging Enhancements

Use of port batches version 2 create new logs, similar to the existing port batching logs. Here are some examples of log messages that are generated when port batching

v2 is enabled:

## Syslog

Port batching logs can reflect the starting port and ending port for port batches, rather than the batch size and the step size. In the examples below, note the difference in the event identifier (NAT-UDP-B and NAT-UDP-T) that indicate how to interpret the highlighted portion of each log message.

In the following port batch v1 logs, the highlighted numbers indicate the starting point, the port batch size, and the step size:

```
Message: Jan 23 13:27:35 AX5200-11 NAT-UDP-B: 30.30.30.11 ->
162.168.20.220:36448,64,23
Message: Jan 23 13:28:24 AX5200-11 NAT-UDP-X: 30.30.30.11 ->
162.168.20.220:36448,64,23
```

In the following port batching v2 pool logs below, the highlighted numbers indicate the starting port and the ending port. The highlighted letters indicate a different event:

```
Message: Jan 23 13:27:35 AX5200-11 NAT-UDP-T: 30.30.30.11 ->
162.168.20.220:36448,36511
Message: Jan 23 13:28:24 AX5200-11 NAT-UDP-Y: 30.30.30.11 -> 162.168.20.220:36448,
36511
```

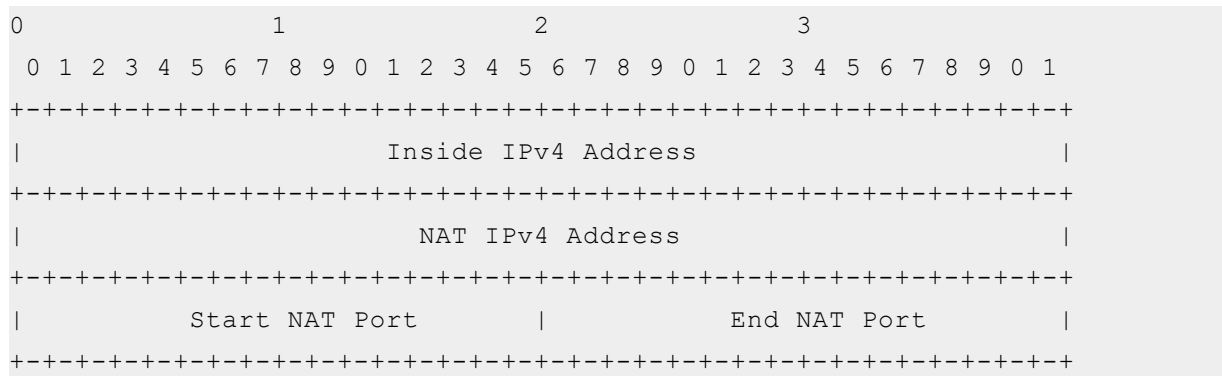
## Binary Log

For binary logging format, the “Proto” field of the port batching log header is changed from 3 bits to 2 bits. A new 1 bit header “V” is added to indicate use of the second version of port batching. If the “V” bit is set, then the new logging format is used. Existing port batching will not have the “V” bit set and will use the legacy logging format.

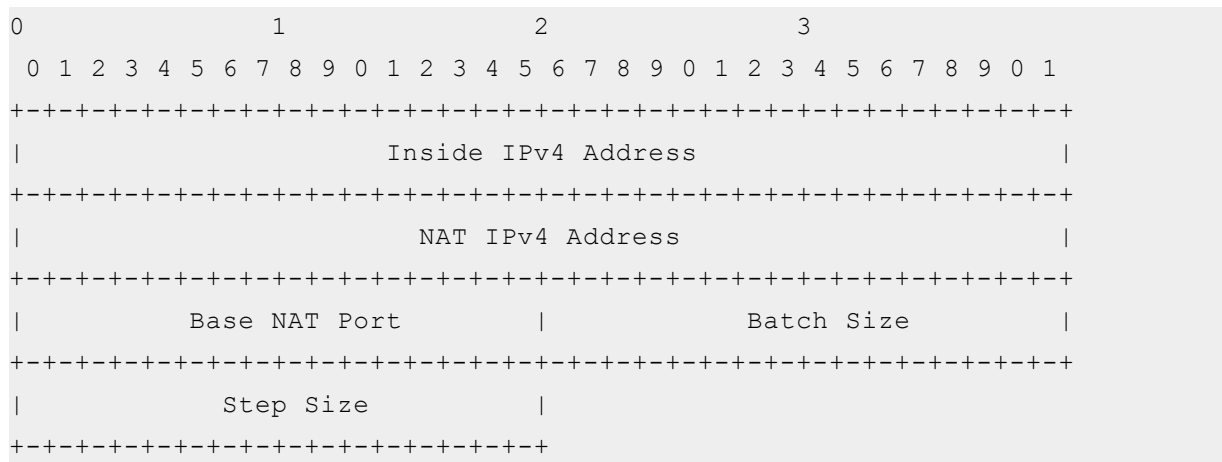
Below is an example of a port batching log header:

```
0                                     1
0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Act | V | Proto | Type |                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---
```

If the “V” bit is set, then the following log format is used:



If the “P” bit is not set, then the legacy log format below is used:



### RADIUS Log

For RADIUS logging, the following new event codes are added:

VALUE	A10-CGN-Action	Port-Batch-V2-Allocated	11
VALUE	A10-CGN-Action	Port-Batch-V2-Freed	12
ATTRIBUTE	A10-CGN-Port-Batch-V2-Port-Start	59	short
ATTRIBUTE	A10-CGN-Port-Batch-V2-Port-End	60	short

## RFC5424 Format and Custom Format:

For RFC5424 logging, there are two new custom keywords for the port batch allocation and port batch freed events.

### **port-batch-v2-allocated**

\$proto-name\$	Protocol name
\$proto-num\$	Protocol number
\$src-ip\$	Source IP
\$nat-ip\$	NAT IP
\$nat-port-start\$	Start port of batch NAT ports
\$nat-port-end\$	End port of batch NAT ports
\$inside-user-mac\$	Inside user MAC
\$radius-msisdn\$	RADIUS attribute: MSISDN
\$radius-imei\$	RADIUS attribute: IMEI
\$radius-imsi\$	RADIUS attribute: IMSI
\$radius-ctm1\$	RADIUS attribute: Custom1
\$radius-ctm2\$	RADIUS attribute: Custom2
\$radius-ctm3\$	RADIUS attribute: Custom3
\$radius-ctm4\$	RADIUS attribute: Custom4
\$radius-ctm5\$	RADIUS attribute: Custom5
\$radius-ctm6\$	RADIUS attribute: Custom6

The default string for “port-batch-v2-allocated” is as follows:

```
LSN:PortBatchV2Allocated:$proto-name$ [$src-ip$ $nat-ip$ $nat-port-start$  
$nat-port-end$]
```

### **port-batch-v2-freed**

\$proto-name\$	Protocol name
\$proto-num\$	Protocol number
\$src-ip\$	Source IP
\$nat-ip\$	NAT IP
\$nat-port-start\$	Start port of batch NAT ports
\$nat-port-end\$	End port of batch NAT ports
\$radius-msisdn\$	RADIUS attribute: MSISDN
\$radius-imei\$	RADIUS attribute: IMEI
\$radius-imsi\$	RADIUS attribute: IMSI
\$radius-ctm1\$	RADIUS attribute: Custom1
\$radius-ctm2\$	RADIUS attribute: Custom2
\$radius-ctm3\$	RADIUS attribute: Custom3

```
$radius-ctm4$          RADIUS attribute: Custom4
$radius-ctm5$          RADIUS attribute: Custom5
$radius-ctm6$          RADIUS attribute: Custom6
```

The default string for “port-batch-v2-freed” is as follows:

```
LSN:PortBatchV2Freed:$proto-name$ [$src-ip$ $nat-ip$ $nat-port-start$
$nat-port-end$]
```

## NetFlow

NetFlow logging can be configured for NAT pool port batching. To do so, enter the following command at the NetFlow configuration level:

```
ACOS(config)# netflow monitor monitor1
ACOS(config-netflow-monitor)# record port-batch-v2-nat44 creation
```

These options configure NetFlow monitor records for NAT pool port batches for NAT44, NAT64, or DSLite. The option of both exports both creation and deletion NetFlow records, whereas the options of `creation` or `deletion` export only those respective NetFlow records.

## TCP/UDP Port Batch Allocation Logging

When simultaneous TCP and UDP port batch allocation is configured, only a single log message is generate. The protocol string for the log message is “Other”.

### Default format:

```
Jun 22 19:00:10 30.30.30.81 NAT-OTR-T: 30.30.30.122 ->
40.40.40.111:2002,2065
Jun 22 19:00:12 30.30.30.81 NAT-OT
```

### Compact format:

```
Jun 22 19:00:23 30.30.30.81 OT: 1e1e1e7a->2828286f:7d2,811
Jun 22 19:00:25 30.30.30.81 OY: 1e1e1e7a->2828286f:7d2,811
```

### RFC5424 format:

```
Jun 22 11:17:46 30.30.30.81 1 2015-06-22T19:01:34-07:00 10.0.17.81 AX2500
- LSN:PortBatchV2Allocated:- [30.30.30.122 40.40.40.111 2002 2065]
Jun 22 11:17:48 30.30.30.81 1 2015-06-22T19:01:36-07:00 10.0.17.81 AX2500
- LSN:PortBatchV2Freed:- [30.30.30.122 40.40.40.111 2002 2065]
```

### Binary format:

```
Log_Msg_Type: NAT_LOGGING_PORT_BATCH_MAPPING (2)
  Port_Batch_Mapping_Log
    Action: PORT_MAPPING_ALLOCATE (0)
    Pool_Based: TRUE (1)
    Protocol: OTHER (0)
    Type: LSN (0)
    Length: 14
  Port_Batch_Mapping_LSN
    Inside_Addr: 111.2.1.10 (1862402314)
    NAT_Addr: 177.81.1.1 (2974875905)
  Ports
    Start_NAT_Port: 46080
    End_NAT_Port: 46143
```

### RADIUS:

```
A10-CGN-Protocol: OTHER (0)
A10-CGN-Action: Port-Batch-Pool-Allocated (11)
A10-CGN-Port-Batch-Pool-Port-Start: 62272
A10-CGN-Port-Batch-Pool-Port-End: 62335
```

## Configuring Interim-Update Logs for Port Batch v2

To support new interim-update logs for Port Batch version 2, new Custom Logging Format configurable entries and keywords were added in the CLI.

### Custom Format Entry and Keywords:

Under the custom logging template in the CLI, new configurable entries were added for the RADIUS interim updates. Keywords for existing Port Batch version 2 and Fixed NAT entries were also added.

For custom logging, there are new keywords for port-batch-v2-allocated and port-batch-v2-freed entries:

**port-batch-v2-allocated**

\$proto-name\$	Protocol name
\$proto-num\$	Protocol number
\$src-ip\$	Source IP
\$nat-ip\$	NAT IP
\$nat-port-start\$	Start port of batch NAT ports
\$nat-port-end\$	End port of batch NAT ports
\$inside-user-mac\$	Inside user MAC
\$ul-byte\$	Upload byte count (only for "format custom")
\$dl-byte\$	Download byte count (only for "format custom")
\$sesn-start-time\$	Session start time (only for "format custom")
\$curr-time\$	Log generated time (only for "format custom")
\$sesn-id\$	Session Identifier (only for "format custom")
\$radius-msisdn\$	RADIUS attribute: MSISDN
\$radius-imei\$	RADIUS attribute: IMEI
\$radius-imsi\$	RADIUS attribute: IMSI
\$radius-ctm1\$	RADIUS attribute: Custom1
\$radius-ctm2\$	RADIUS attribute: Custom2
\$radius-ctm3\$	RADIUS attribute: Custom3
\$radius-ctm4\$	RADIUS attribute: Custom4
\$radius-ctm5\$	RADIUS attribute: Custom5
\$radius-ctm6\$	RADIUS attribute: Custom6

**port-batch-v2-freed**

\$proto-name\$	Protocol name
\$proto-num\$	Protocol number
\$src-ip\$	Source IP
\$nat-ip\$	NAT IP
\$nat-port-start\$	Start port of batch NAT ports
\$nat-port-end\$	End port of batch NAT ports
\$ul-byte\$	Upload byte count (only for "format custom")
\$dl-byte\$	Download byte count (only for "format custom")
\$sesn-start-time\$	Session start time (only for "format custom")
\$curr-time\$	Log generated time (only for "format custom")
\$ct-msg\$	Connection Termination Message (only for "format custom")
\$sesn-id\$	Session Identifier (only for "format custom")
\$radius-msisdn\$	RADIUS attribute: MSISDN
\$radius-imei\$	RADIUS attribute: IMEI
\$radius-imsi\$	RADIUS attribute: IMSI
\$radius-ctm1\$	RADIUS attribute: Custom1
\$radius-ctm2\$	RADIUS attribute: Custom2
\$radius-ctm3\$	RADIUS attribute: Custom3
\$radius-ctm4\$	RADIUS attribute: Custom4
\$radius-ctm5\$	RADIUS attribute: Custom5
\$radius-ctm6\$	RADIUS attribute: Custom6

Two new configuration entries are added to custom logging format for interim logs. There is an new entry for Port Batch version 2 interim updates, and a new entry for Fixed NAT interim updates.

**port-batch-v2-interim-update**

\$proto-name\$	Protocol name
\$proto-num\$	Protocol number
\$src-ip\$	Source IP
\$nat-ip\$	NAT IP
\$nat-port-start\$	Start port of batch NAT ports
\$nat-port-end\$	End port of batch NAT ports
\$ul-byte\$	Upload byte count (only for "format custom")
\$dl-byte\$	Download byte count (only for "format custom")
\$sesn-start-time\$	Session start time (only for "format custom")
\$curr-time\$	Log generated time (only for "format custom")
\$sesn-id\$	Session Identifier (only for "format custom")
\$radius-msisdn\$	RADIUS attribute: MSISDN
\$radius-imei\$	RADIUS attribute: IMEI
\$radius-imsi\$	RADIUS attribute: IMSI
\$radius-ctm1\$	RADIUS attribute: Custom1
\$radius-ctm2\$	RADIUS attribute: Custom2
\$radius-ctm3\$	RADIUS attribute: Custom3
\$radius-ctm4\$	RADIUS attribute: Custom4
\$radius-ctm5\$	RADIUS attribute: Custom5
\$radius-ctm6\$	RADIUS attribute: Custom6

**NOTE:** The keywords for Port Batch version 2 freed (port-batch-v2-freed) are the same as the keywords for Port Batch version 2 interim update (port-batch-v2-interim-update, with the addition of the \$ct-msg\$ keyword to log connection termination).

**fixed-nat-interim-update**

<code>\$src-ip\$</code>	Source IP
<code>\$nat-ip\$</code>	NAT IP
<code>\$nat-port-start\$</code>	First NAT port
<code>\$nat-port-end\$</code>	Last NAT port
<code>\$ul-byte\$</code>	Upload byte count (only for "format custom")
<code>\$dl-byte\$</code>	Download byte count (only for "format custom")
<code>\$sesn-start-time\$</code>	Session start time (only for "format custom")
<code>\$curr-time\$</code>	Log generated time (only for "format custom")
<code>\$sesn-id\$</code>	Session Identifier (only for "format custom")
<code>\$radius-msisdn\$</code>	RADIUS attribute: MSISDN
<code>\$radius-imei\$</code>	RADIUS attribute: IMEI
<code>\$radius-imsi\$</code>	RADIUS attribute: IMSI
<code>\$radius-ctm1\$</code>	RADIUS attribute: Custom1
<code>\$radius-ctm2\$</code>	RADIUS attribute: Custom2
<code>\$radius-ctm3\$</code>	RADIUS attribute: Custom3
<code>\$radius-ctm4\$</code>	RADIUS attribute: Custom4
<code>\$radius-ctm5\$</code>	RADIUS attribute: Custom5
<code>\$radius-ctm6\$</code>	RADIUS attribute: Custom6

# Glossary

## A

---

### ASCII

American Standard Code for Information Interchange (ASCII) is a character encoding standard used for representing text in computers. In ACOS logging, ASCII format is used for human-readable log messages.

## B

---

### Binary Logging

A logging format where records are exported in binary form for efficient processing. In ACOS, binary logging is used for high-performance log export.

## C

---

### CEF Logging

Common Event Format Logging (CEF) is a structured logging format used for

security and event logging. In ACOS, CEF logging enables exporting traffic and NAT logs in CEF format to external logging systems.

### CEF Logging Format

The specific structure of logs when exported using Common Event Format in ACOS.

### Compact Logging

A logging method that reduces log size by eliminating redundant fields and encoding information efficiently. In ACOS, compact logging minimizes bandwidth and storage consumption while exporting NAT and traffic logs.

### CURL

Client URL (CURL) a command-line tool used for transferring data using various protocols. In ACOS

logging context, cURL can be used to test logging endpoints or collectors.

### **Custom Logging**

User-defined logging configuration that allows customization of exported log fields and formats in ACOS.

## **D**

---

### **Default Logging Template**

A predefined logging template provided by ACOS for exporting NAT and traffic logs with standard fields.

## **E**

---

### **Enhanced User Tracking**

A logging feature that includes additional subscriber identification fields. In ACOS, it improves traceability for compliance.

### **External Logging**

The process of exporting log records to an external log server. In ACOS, logs are sent to external collectors such as SYSLOG, IPFIX, or CEF servers.

## **F**

---

### **Fixed-NAT Logging**

Logging for fixed NAT port allocations assigned to subscribers. In ACOS, it records persistent port assignments.

### **Flow Records**

Log entries that contain information about IP traffic flows. In ACOS, flow records are exported for traffic analysis and subscriber tracking.

### **Flow Timeout**

The duration after which an inactive flow is terminated. In ACOS, flow timeout values deter-



ine when traffic log records are generated.

## G

---

### **GGSN**

Gateway GPRS Support Node (GGSN) is a network node that connects the GPRS network to external IP networks. In ACOS, logging supports subscriber traffic associated with GGSN environments.

### **GTP**

GPRS Tunneling Protocol (GTP) is a protocol used for carrying subscriber data within mobile core networks. In ACOS, GTP information can be included in traffic and NAT logs for mobile subscriber tracking.

## I

---

### **IANA**

Internet Assigned Numbers Authority (IANA)

the organization responsible for global IP address and protocol parameter assignments. In ACOS, IANA-defined values may be referenced in logging formats and protocol fields.

### **INTERIM**

Interim Accounting. Periodic accounting updates sent during an active session. In ACOS, interim records are generated to report session usage before session termination.

### **IPFIX Logging**

IP Flow Information Export (IPFIX) Logging is flow-based logging format used to export traffic flow information. In ACOS, IPFIX logging exports NAT and traffic flow records to collectors.

### **IPFIX Templates**

Template definitions used in IPFIX logging to

describe exported fields. In ACOS, templates define the structure of NAT and flow records.

## L

---

### L3 Entry

A logging entry containing Layer 3 information such as IP addresses. In ACOS, L3 entries record IP-level session details.

### L4 Entry

A logging entry containing Layer 4 information such as TCP/UDP ports and protocol. In ACOS, L4 entries record transport-layer session details.

### Lite Flow Record

A simplified flow record containing essential fields. In ACOS, lite flow records reduce logging overhead while maintaining traceability.

### Lived Sessions

Active sessions currently being tracked. In ACOS, logging can report sessions that remain active over time.

### Logging Template

A configuration profile that defines the format and fields included in exported traffic or NAT logs in ACOS.

## M

---

### MAC Address

Media Access Control (MAC) Address is a unique hardware identifier assigned to a network interface. In ACOS logging, MAC address information can be logged for subscriber and device identification.

### Merged Session Log

A logging method that combines multiple session events into a single log record. In ACOS, it

reduces the number of log entries generated for a session.

### **Message String**

The textual portion of a log record containing event information. In ACOS, message strings carry session and NAT event details.

## **N**

---

### **NAT Port Allocation**

The assignment of source ports for translated sessions. In ACOS, NAT port allocation details are logged for session tracking and compliance.

### **NetFlow Exporter**

A feature that exports flow information in NetFlow format. In ACOS, it sends flow records to NetFlow collectors.

## **O**

---

### **One-to-One NAT Logging**

Logging for static one-to-one NAT mappings. In ACOS, it records mappings between private and public IP addresses.

### **Opcodes**

Operation codes that identify the type of log record or event. In ACOS, opcodes differentiate session, reset, or tunnel events.

## **P**

---

### **Periodic Logging**

Logging generated at regular intervals during a session. In ACOS, periodic logs provide ongoing session accounting.

### **PGW**

Packet Gateway (PGW) is a gateway in LTE networks that connects the mobile network to

external IP networks. In ACOS deployments, logging may include PGW-related subscriber traffic information.

### **Port Batch Log**

A log record that groups multiple port allocation events into a single entry. In ACOS, it improves logging efficiency.

### **Port Batch Logging**

A logging method where multiple NAT port allocation events are grouped into a single log record for efficiency in ACOS.

### **Port Mapping File**

A file that contains mappings between private and public IP addresses and ports. In ACOS, this file is used to track NAT port allocations for subscriber traceability.

## **R**

---

### **RADIUS Attributes**

Parameters included in RADIUS accounting messages. In ACOS, RADIUS attributes are logged to provide subscriber and session information.

### **RADIUS Logging**

Logging of subscriber and session information using the RADIUS protocol. In ACOS, RADIUS logging is used for accounting and subscriber activity reporting.

### **Reset Event Records**

Log entries generated when a session is reset. In ACOS, these records capture TCP reset-related events.

### **RFC 5424 Logging**

Logging compliant with RFC 5424 SYSLOG message format. In ACOS, logs are exported in

standardized structured SYSLOG format.

## S

---

### Session Event Records

Log entries generated for session creation and termination events. In ACOS, these records provide session lifecycle information.

### SYSLOG

A standard protocol used to send system log messages to a centralized server. In ACOS, SYSLOG is used to export traffic, NAT, and system logs.

## T

---

### Timestamp Granularity Logging

Logging with configurable timestamp precision. In ACOS, it allows microsecond or millisecond timestamp accuracy.

## TLV

Type-Length-Value (TLV) is a structured data encoding format. In ACOS logging, TLV format is used in IPFIX and other logging templates to define exported fields.

### Tunnel Records

Log entries containing information about tunneled sessions. In ACOS, tunnel records are generated for GTP or other encapsulated traffic sessions

## U

---

## URI

Uniform Resource Identifier (URI) is a string of characters used to identify a resource on the Internet. In ACOS logging context, URI information can be included in traffic logs to identify specific application requests or accessed resources.

**V**

---

**VRF**

Virtual Routing and Forwarding (VRF) is a technology that allows multiple routing tables on the same device. In ACOS, VRF information can be included in traffic logging for multi-tenant environments.

**W**

---

**Wireshark Generic Dissector DLL**

A dynamic library used by Wireshark to decode ACOS binary logging formats for analysis.

**Wireshark Plugin**

A plugin used in Wireshark to decode and analyze ACOS binary log records.



©2026 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, Thunder TPS, A10 Harmony, SSLi and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: [www.a10networks.com/company/legal/trademarks/](http://www.a10networks.com/company/legal/trademarks/).