EDR Format Configuration Mode Commands

The EDR Format Configuration Mode enables configuring Event Data Record (EDR) formats.

Command Modes

Exec > ACS Configuration > EDR Format Configuration

active-charging service *service_name* **> edr-format** *format_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edr)#
```

Important

The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

attribute

This command allows you to specify the fields and their order in EDRs.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > EDR Format Configuration

active-charging service *service_name* **> edr-format** *format_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edr)#
```

Syntax Description

```
attribute attribute { [ format { MM/DD/YY-HH:MM:SS | MM/DD/YY-HH:MM:SS:sss
 | MM/DD/YYYY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS:sss | YYYY/MM/DD-HH:MM:SS |
 MM/DD/YYYY-HH:MM:SS:sss | YYYYMMDDHHMMSS | YYYYMMDDHHMMSSsss | seconds
} ] [ localtime ] | [ { ip | tcp } { bytes | pkts } { downlink | uplink
} ] priority priority }
no attribute attribute [ { ip | tcp } { bytes | pkts } { downlink | uplink
 } ] [ priority priority ]
```

no

If added previously, removes the specified attribute from the EDR format.

attribute

Specifies the attribute.

attribute must be one of the following:

Attributes	Description
bandwidth-policy	This attribute reports the bandwidth policy name of subscriber. Bandwidth policy can be configured or applied to subscriber by — • binding with APN (static) • binding with Rulebase (static) • receiving from AAA server (dynamic) **Important** This attribute field is customer specific. For more information, contact your Cisco account representative.
radius-called-station-id	This attribute reports the Called Station ID of the mobile handling the flow.
radius-calling-station-id	This attribute reports the Calling Station ID of the mobile handling the flow.
radius-fa-nas-identifier	This attribute reports the RADIUS NAS identifier of Foreign Agent (FA).
radius-fa-nas-ip-address	This attribute reports the RADIUS IP address of Foreign Agent (FA).
radius-nas-identifier	This attribute reports the RADIUS NAS identifier.
radius-nas-ip-address	This attribute reports the RADIUS NAS IP address. Note that this attribute is interchangeable with **sn-st16-ip-addr** for the user.
radius-user-name	This attribute reports the user name associated with the flow.

Attributes	Description
sn-3gpp2-always-on	This option has been deprecated. To configure this attribute see the rule-variable, on page 17 command.
sn-3gpp2-bsid	This option has been deprecated. To configure this attribute see the rule-variable, on page 17 command.
sn-3gpp2-esn	This option has been deprecated. To configure this attribute see the rule-variable, on page 17 command.
sn-3gpp2-ip-qos	This option has been deprecated. To configure this attribute see the rule-variable, on page 17 command.
sn-3gpp2-ip-technology	This option has been deprecated. To configure this attribute see the rule-variable, on page 17 command.
sn-3gpp2-release-indicator	This option has been deprecated. To configure this attribute see the rule-variable, on page 17 command.
sn-3gpp2-service-option	This option has been deprecated. To configure this attribute see the rule-variable, on page 17 command.
sn-3gpp2-session-begin	This option has been deprecated. To configure this attribute see the rule-variable, on page 17 command.
sn-3gpp2-session-continue	This option has been deprecated. To configure this attribute see the rule-variable, on page 17 command.
sn-acct-session-id	This attribute reports the unique session identifier for accounting.

Attributes	Description
sn-app-protocol	

Attributes	Description
	This attribute reports the application protocol for the flow. A value indicating the protocol, such as one of the following: • ACS_PROTO_UNKNOWN = 0 • ACS_PROTO_GTP = 1 • ACS_PROTO_IP = 2 • ACS_PROTO_TCP = 3 • ACS_PROTO_UDP = 4 • ACS_PROTO_HTTP = 5 • ACS_PROTO_HTTPS = 6 • ACS_PROTO_FTP = 7 • ACS_PROTO_FTP_CONTROL = 8 • ACS_PROTO_FTP_DATA = 9 • ACS_PROTO_WTP = 10 • ACS_PROTO_WSP = 11 • ACS_PROTO_WTP_WSP_CONNECTION_ORIENTED = 12 • ACS_PROTO_WSP_CONNECTION_LESS = 13 • ACS_PROTO_DNS = 14 • ACS_PROTO_ICMP = 15 • ACS_PROTO_POP3 = 16 • ACS_PROTO_SIP = 17 • ACS_PROTO_SDP = 18 • ACS_PROTO_SMTP = 19 • ACS_PROTO_EMAIL = 20 • ACS_PROTO_MMS = 21 • ACS_PROTO_FILE_TRANSFER = 22 • ACS_PROTO_WWW = 23 • ACS_PROTO_RTP = 24 • ACS_PROTO_RTSP = 25 • ACS_PROTO_IMAP = 26

Attributes	Description
	• ACS_PROTO_FLOW = 27 • ACS_PROTO_CCA = 28 • ACS_PROTO_P2P = 29 • ACS_PROTO_RTCP = 30 • ACS_PROTO_ICMPV6 = 31 • ACS_PROTO_TFTP = 32 • ACS_PROTO_PPTP = 33
	• ACS_PROTO_GREv1 = 34 • ACS_PROTO_PPTP_GRE = 35 • ACS_PROTO_SIP_ADV = 36 • ACS_PROTO_SIP_BASIC_ADV = 37 • ACS_PROTO_H323 = 38 • ACS_PROTO_ESP = 39 • ACS_PROTO_AH = 40 • ACS_PROTO_RTSPSTREAM = 41
sn-cf-category-classification-used	For Category-based Content Filtering, this attribute reports the last classification used by system for the flow, or blank if classification was never successfully performed. For URL Blacklisting, specifies category of the blacklisted URL in the Blacklist database.

Attributes	Description
sn-cf-category-flow-action	For Category-based Content Filtering, this attribute reports the last action taken for the flow, or blank if content filtering was never performed. The following are the possible values: • allow • content-insert • discard • redirect-url • terminate-flow For URL Blacklisting, this attribute reports the last action taken for the flow, or blank if Blacklist matching was never performed. The following are the possible values: • discard • terminate-flow • redirect-url • www-reply-code-terminate-flow
sn-cf-category-policy	For Category-based Content Filtering, this attribute reports the category policy identifier that was used for the flow, or blank if content filtering was never attempted for the flow.
sn-cf-category-rating-type	For Category-based Content Filtering, this attribute reports the type, either "static" or "dynamic" that was last successfully performed for the flow, or blank if content filtering was never successful for the flow. For URL Blacklisting, specifies "blacklisting".
sn-cf-category-unknown-url	This attribute reports the identifier for unknown URL under content filtering action. It holds either "1" for unknown URLs or "0" for the URLs having static rating in its database.
sn-charge-volume	This attribute reports the total charge volume excluding bytes/packets dropped/retransmitted by ECS. This behavior can be changed by configuring to allow dropped/retransmitted bytes/packets to be included in the net volume. See the **edr sn-charge-volume** command in the *ACS Rulebase Configuration Mode Commands* chapter.

Attributes	Description
sn-charging-action	This attribute reports the name of last charging action matched against flow. **Important** This attribute configuration currently supports only static and predefined rules and ruledefs. It will NOT be supported for dynamic rules installed by PCRF.
sn-closure-reason	This attribute reports the reason for termination of the flow/EDR: • 0: Normal end of flow • 1: End of flow by handoff processing • 2: Subscriber session terminated • 3: Inter-chassis Session Recovery switchover • 12: Completion of transaction • 13: End of VoIP call event This is supported only in release 12.2. • 14: End of VoIP call event This is supported in 14.0 and later releases. • 16: ACS_EDR_OCS_REACHABLE • 17: ACS_EDR_OCS_UNREACHABLE • 18: ACS_EDR_INTERIM_VOLUME_EXHAUST • 19: ACS_EDR_INTERIM_TIME_EXHAUST • 20: ACS_EDR_OCS_STATUS_UNKNOWN • 21: ACS_EDR_TETHERING_SIGNATURE_CHANGE
sn-correlation-id	This attribute reports the RADIUS correlation identifier.
sn-direction	This attribute reports the direction of the first packet for the flow. It has following values: • **toMobile**: This value appears when direction of first packet is towards mobile node. • **fromMobile**: This value appears when direction of first packet is towards mobile node. • **unknown**: This value appears when the original originator of a flow can not be determined (for example, a flow that is interrupted due to a Inter-chassis Session Recovery switchover).

Attributes	Description
sn-duration	This attribute reports the duration between the last and first packet for the record.
sn-end-time [format *format* **] localtime**	This attribute reports the timestamp for last packet of flow in UTC.
sn-fa-correlation-id	This attribute reports the RADIUS Correlation Identifier of the Foreign Agent (FA).
sn-fa-ip-address	This attribute reports IP address of the Foreign Agent (FA).
sn-filler-blank	This attribute inserts a blank filler field, generates an empty EDR field.
sn-filler-zero	This attribute inserts a "0" in the EDR field.
sn-flow-end-time	This attribute reports the time of flow-end EDR generation—when EDRs are generated at hagr, session-end, timeout, or normal-end-signaling conditions. **sn-start-time** and **sn-end-time** fields of flow end-condition EDRs cannot be used to determine the duration of the flow if intermediate EDRs are generated (rule-match or transaction-complete or any other intermediate EDR). **sn-start-time** field in an EDR gives the time the first packet was received after the last EDR was generated. So, whenever an EDR is generated, this field is reset to the time the EDR gets generated. So the **sn-start-time** field in flow end-condition EDRs may not have the time of the first packet received on that flow. It will have the time at which the last EDR was generated or the first packet time if no EDR was generated for that flow. **sn-end-time** field gives the time at which the last packet on the flow was received. Flow end-condition EDRs may not be generated immediately after receiving the last packet. For example, in case of session-end or timeout EDRs, last packet time and EDR generation time may be different. **sn-flow-start-time** gives the time of the first packet of the flow (irrespective of whether intermediate EDRs were generated), and **sn-flow-end-time** gives the time when EDRs are generated at hagr, session-end, timeout or normal-end-signaling conditions. The values of these fields will be populated in EDRs only for hagr, session-end, timeout and normal-end-signaling EDRs.

Attributes	Description
sn-flow-id	This attribute reports the flow-id assigned internally by the ECS module to each flow.
sn-flow-start-time	This attribute reports the time of the first packet of the flow (irrespective of whether intermediate EDRs were generated). Also see **sn-flow-end-time**.
sn-format-name	This attribute reports the name of the EDR/UDR format used.
sn-group-id	This attribute reports the sequence group ID of the record.
sn-ha-ip-address	This attribute reports IP address of the Home Agent (HA).
sn-ip-pool-name	This attribute reports the IP pool name corresponding to the current flow in EDR.
sn-ip-protocol-name	This attribute reports the IP protocol name for the flow. For IANA registered IP Protocol (Layer 4 Protocol) name, like TCP, UDP, AH, ESP, ICMP, etc.
sn-nat-binding-timer	For Network Address Translation (NAT) in-line service, this attribute reports the port chunk hold timer.
sn-nat-gmt-offset	For NAT in-line service, this attribute reports the GMT offset of the node generating NAT bind record.
sn-nat-ip	For NAT in-line service, this attribute reports the NAT IP address of the port chunk.
sn-nat-last-activity-time-gmt	For NAT in-line service, this attribute reports the time when the last flow in a specific NAT set of flows was seen.
sn-nat-no-port-packet-dropped	For NAT in-line service, this attribute reports the number of packets dropped because of no NAT IP/port.
sn-nat-port-block-end	For NAT in-line service, this attribute reports the last port number of the port chunk.
sn-nat-port-block-start	For NAT in-line service, this attribute reports the starting port number of the port chunk.
sn-nat-port-chunk-alloc-dealloc-flag	For NAT in-line service, this attribute reports whether the port chunk is allocated or released.

Attributes	Description
sn-nat-port-chunk-alloc-time-gmt	For NAT in-line service, this attribute reports when the port chunk was allocated.
sn-nat-port-chunk-dealloc-time-gmt	For NAT in-line service, this attribute reports when the port chunk was released.
sn-nat-realm-name	For NAT in-line service, this attribute reports the name of the NAT realm.
sn-nat-subscribers-per-ip-address	For NAT in-line service, this attribute reports the subscriber(s) per NAT IP address.
sn-nemo-vrf-name	This attribute indicates the VRF name associated with UE behind the Network Mobility Services (NEMO) Mobile Router (MR). **Important** This is a customer-specific attribute, and is available only with NEMO license.
sn-ocs-server-reachable	This attribute indicates the state of the OCS server. This attribute supports the following values: • OCS_SERVER_NOT_APPLICABLE = 0 • OCS_SERVER_UNREACHABLE = 0 + 1 • OCS_SERVER_REACHABLE = 0 + 2
sn-parent-protocol	This attribute reports the parent protocol of the flow. An integer value like in **sn-app-protocol**; for RTCP/RTP flows, the parent protocol may be RTSP or SIP; for GRE flows, the parent protocol will be PPTP, and so on.
sn-port-service-name	This attribute reports the registered name for the server port. For IANA registered/Well Known Transport Port name mapping for the Server Port like SSL, HTTP, DNS, FTP, TELNET, SSH, Diablo, Rainbox six, UnReal_UT etc. This port service name mapping is done based on the Server port, which means if the flow is "FromMobile", the sn-server-port is mapped as the service name port. If the flow is "ToMobile", the sn-subscriber-port is mapped as the service name.
sn-rulebase	This attribute reports the name of the ECS rulebase applied.
sn-ruledef-name	This attribute reports the ruledef name corresponding to the last charging action matched. **Important** This is a customer-specific attribute.

Attributes	Description
sn-rating-group	This attribute reports the rating group corresponding to last charging action matched. **Important** This attribute configuration currently supports only static and predefined rules and ruledefs. It will NOT be supported for dynamic rules installed by PCRF.
sn-sequence-no	This attribute reports the unique sequence number (per **sn-sequence-group** and **radius-nas-ip-address**) of EDR identifier and linearly increasing in EDR file.
sn-server-port	This attribute reports the TCP/UDP port number of the server in a subscriber's data flow.
sn-service-id	This attribute reports the Service ID corresponding to last charging action matched. **Important** This attribute configuration currently supports only static and predefined rules and ruledefs. It will NOT be supported for dynamic rules installed by PCRF.
sn-st16-ip-addr	This attribute reports the IP address of the chassis handling this flow. **Important** Note that this attribute is interchangeable with **radius-nas-ip-address** for other systems.
sn-start-time [format *format* **] localtime**	This attribute reports the timestamp for last packet of flow in UTC.
sn-subscriber-imsi	This attribute reports the IMSI number of the subscriber.
sn-subscriber-nat-flow-ip	For NAT in-line service, this attribute reports the NAT IP address of NAT-enabled subscriber.
sn-subscriber-nat-flow-port	For NAT in-line service, this attribute reports the NAT port number of NAT-enabled subscriber.
sn-subscriber-port	This attribute reports the TCP/UDP port number of the Mobile handling subscriber data flow.
sn-volume-amt { ip | tcp } { bytes | pkts } { uplink | downlink }	This attribute reports IP/TCP protocol-specific volume amount of downlink/uplink bytes/packets during a flow. This includes all the bytes/packets received by ECS, including the bytes/packets dropped and retransmitted by ECS.

Attributes	Description
sn-volume-dropped-amt { ip | tcp } { bytes | packets } { downlink | uplink }	For Stateful Firewall in-line service, this attribute reports IP/TCP protocol-specific volume amount of downlink/uplink bytes/packets dropped by Stateful Firewall during a flow.
sn-volume-ip-with-rtsp-or-rtp bytes { downlink | priority | uplink }	This attribute reports the IP volume amount of downlink/uplink bytes of an RTSP flow and the RTP flows controlled by it, or Comma Separated Value (CSV) position priority of this field. If **uplink** or **downlink** is not specified it shows the total of both.
sn-vrf-name	This attribute indicates the VRF name associated with the base session of NEMO. **Important** This is a customer-specific attribute.
subscriber-ipv4-address	For NAT in-line service, this attribute generates the subscriber IPv4 address in the NBR.
subscriber-ipv6-address	For NAT in-line service, this attribute generates the subscriber IPv6 prefix in the NBR.
transaction-charge-downlink-bytes	This attribute reports the total charge downlink bytes for the transaction. Excludes the dropped/retransmitted bytes from the total transaction downlink bytes.
transaction-charge-downlink-packets	This attribute reports the total charge downlink packets for the transaction. Excludes the dropped/retransmitted packets from the total transaction downlink packets.
transaction-charge-uplink-bytes	This attribute reports the total charge uplink bytes for the transaction. Excludes the dropped/retransmitted bytes from the total transaction uplink bytes.
transaction-charge-uplink-packets	This attribute reports the total charge uplink packets for the transaction. Excludes the dropped/retransmitted packets from the total transaction uplink packets.
transaction-downlink-bytes	This attribute reports the total downlink bytes for the transaction.
transaction-downlink-packets	This attribute reports the total downlink packets for the transaction.
transaction-uplink-bytes	This attribute reports the total uplink bytes for the transaction.
transaction-uplink-packets	This attribute reports the total uplink packets for the transaction.

format { MM/DD/YY-HH:MM:SS | MM/DD/YY-HH:MM:SS:sss | MM/DD/YYYY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS:sss | YYYY/MM/DD-HH:MM:SS | MM/DD/YYYY-HH:MM:SS:sss | YYYYMMDDHHMMSS | YYYYMMDDHHMMSSsss | seconds

Specifies the timestamp format.

In releases prior to 18.0, the current timestamps available in the EDR format configuration allow recording of time information only up to seconds level. In 18.0 and later releases, new timestamp formats are added to allow recording of time information up to milliseconds granularity.

This feature enables to record timestamps of the events at finer granularity. The timestamps will be populated according to the selected timestamp format whenever any of the predefined events/event triggers for generating EDRs is encountered.

localtime

Specifies timestamps with the local time. By default, timestamps are displayed in GMT/UTC.

{ ip | tcp }{ bytes | pkts }{ downlink | uplink }

Specifies bytes/packets sent/received from/by mobile.

priority *priority*

Specifies the position priority of the value within the EDR record. Lower numbered priorities (across all attribute, event-label, and rule-variable) occur first.

priority must be an integer from 1 through 65535. Up to 50 position priorities (across all attribute, event-label, and rule-variable) can be configured.

Usage Guidelines

Use this command to set the attributes and priority for EDR file format.

A particular field in EDR format can be entered multiple times at different priorities. While removing the EDR field using the **no attribute** command either you can remove all occurrences of a particular field by specifying the field name or a single occurrence by additionally specifying the optional **priority** keyword.

In 21.1 and later releases, a maximum of 75 EDR attribute fields can be configured in an EDR record. The limit is expanded from 50 fields up to 75 fields.

Example

The following is an example of this command:

```
attribute radius-user-name priority 12
```

delimiter

This command allows you to configure a comma or a tab as a delimiter character for EDRs.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > EDR Format Configuration

active-charging service *service_name* **> edr-format** *format_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edr)#
```

Syntax Description

```
delimiter { comma | tab }
no delimiter
```

no

This **no** variant reverts back to the default configuration. By default, comma is used as the delimiter for EDRs.

comma

This keyword allows you to specify comma as an EDRdelimiter. Comma is the default configuration.

tab

This keyword allows you to specify tab as an EDR delimiter.

Usage Guidelines

Use this command to configure either comma or tab as the delimiter between EDR fields.

The comma character is currently used as the delimiter between EDR fields. But comma is a valid character for URLs. Thus when a EDR URL contains a comma, the downstream parser encounters issues.

Hence, this feature has been developed to allow TAB as an additional character to be used as the delimiter in the EDR file. For backward compatibility reasons, this CLI configuration is introduced to choose the delimiter character between both comma and TAB.

Example

The following example specifies tab as the delimiter configuration for EDRs:

```
delimiter tab
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
end
```

Usage Guidelines

Use this command to return to the Exec mode.

event-label

This command allows you to specify an optional event label/identifier to be used as an attribute in the EDRs.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > EDR Format Configuration

active-charging service *service_name* **> edr-format** *format_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-acs-edr)#`

Syntax Description

`event-label` *`event_label`* **`priority`** *`priority`*
`no event-label`

no

If previously configured, removes the event label configuration.

event_label

Specifies the event label/identifier to be used as EDR attribute.

event_label must be an alphanumeric string of 1 through 63 characters.

priority *priority*

Specifies the Comma Separated Value (CSV) position of the attribute (label/identifier) in the EDR.

priority must be an integer from 1 through 65535.

Usage Guidelines

Use this command to configure an optional event label/identifier as an attribute in the EDR and its position in the EDR.

Example

The following is an example of this command:

```
event-label radius_csv1 priority 23
```

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description **exit**

Usage Guidelines Use this command to return to the parent configuration mode.

rule-variable

This command allows you to specify fields and their order in EDRs.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > EDR Format Configuration

active-charging service *service_name* **> edr-format** *format_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-acs-edr)#`

Syntax Description

rule-variable *rule_variable* **priority** *priority* **[in-quotes]**
no rule-variable *rule_variable* **[priority** *priority* **]**

no

If previously configured, removes the specified rule variable configuration.

rule_variable

Specifies the rule variable for the EDR format.

rule_variable must be one of the following options:

- **bearer 3gpp**: 3GPP bearer-related fields:
  - **charging-id**: Charging ID of the bearer flow
  - **imei**: IMEI or IMEISV (depending on the case) associated with the bearer flow. Only available in StarOS 8.1 and later releases.
  - **imsi**: Specific Mobile Station Identification number.
  - **pcrf-correlation-id**: PCRF correlation ID of the bearer flow sent by Gx interface.
  - **rat-type**: RAT type associated with the bearer flow. Only available in StarOS 8.1 and later releases.
  - **sgsn-address**: SGSN associated with the bearer flow. Only available in StarOS 8.1 and later releases. For MIPv6 calls, sgsn-address field is populated with HSGW address.
  - **user-location-information**: User location information associated with the bearer flow. Only available in StarOS 8.1 and later releases.
- **bearer 3gpp2**: 3GPP2 bearer-related fields:
  - **always-on**: 3GPP2 always on indicator

- **bsid**: 3GPP2 BSID
- **esn**: 3GPP2 ESN
- **ip-qos**: 3GPP2 IP QoS
- **ip-technology**: 3GPP2 IP technology
- **release-indicator**: 3GPP2 release indicator
- **service-option**: 3GPP2 service option
- **session-begin**: 3GPP2 session begin indicator
- **session-continue**: 3GPP2 session continue indicator

- **bearer ggsn-address**: GGSN IP address field. For MIPv6 calls, ggsn-address field in EDR will be populated with PGW address.
- **bearer qci**: QCI of the bearer corresponding to the flow for which the EDR is getting generated.
- **dns**: Domain Name System (DNS) related fields:
  - **answer-ip-list**: DNS Host IP list. A maximum of 4 IP addresses will be part of an EDR.
  - **answer-name**: DNS answer name. This depends upon query type.
  - **previous-state**: DNS previous state information
  - **query-name**: DNS query name
  - **query-type**: DNS query type. Numeric value as per the DNS specifications.
  - **return-code**: DNS query response code
  - **state**: DNS current state information
  - **tid**: DNS Transaction Identifier
- **file-transfer**: File Transfer related fields:
  - **chunk-number**: Number of chunks
  - **current-chunk-length**: Length of current chunk
  - **declared-chunk-length**: Declared size of the chunk
  - **declared-file-size**: Declared size of the file
  - **filename**: Name of the file being transferred
  - **previous-state**: Previous state of session
  - **state**: Current state of session
  - **transferred-file-size**: Transferred size of the file
- **flow**:Flow related fields:
  - **ip-control-param**: First 8 bytes of IPv6 header is inserted in EDRs.

- **tethered**: Tethering detected on flow. Enables/disables tethering detection result field in EDRs sent to MUR.
- **tethered-application**: Application based tethering detected on flow.
- **tethered-dns**: DNS-based tethering detected on flow. Either 0 or 1.
- **tethered-ip-ttl**: IP-TTL based tethering detected on flow.
- **ttl**: Time To Live/Max hops value received in the first packet of the flow.

- **ftp**: File Transfer Protocol (FTP) related fields:
  - **client-ip-address**:
  - **client-port**
  - **command name**: Command sent
  - **connection-type**
  - **filename**: File name being transferred in any of the FTP-related FTP command
  - **pdu-length**: FTP PDU length
  - **pdu-type**
  - **previous-state**: Previous state of FTP session
  - **reply code**
  - **server-ip-address**
  - **server-port**
  - **session-length**: Total length of FTP session
  - **state**: Current state of FTP session
  - **url**: URL of file
  - **user**: User identifier

- **http**: Hypertext Transport Protocol (HTTP) related fields:
  - **accept**: Content types that are acceptable for the response
  - **attribute-in-data**: Dynamic header field in application payload
  - **attribute-in-url**: Dynamic header field in URL
  - **content disposition**
  - **content length**
  - **content type**
  - **cookie**: HTTP cookie header
  - **domain**
  - **dnt**

- **header-length**: HTTP header length
- **host**
- **payload-length**: Payload length
- **pdu-length**
- **previous-state**: Previous state of session
- **referer**
- **reply code**: HTTP response
- **request method**: HTTP request method
- **session-length**: Total length of HTTP session
- **state**: Current state of session
- **transaction-length**: Total length of HTTP transaction
- **transfer-encoding**: Transfer encoding
- **uri**: Uniform Resource Identifier
- **url**: Uniform Resource Locator
  - **length** *size*: This optional filter allows the user to configure the HTTP URL length from 1 to 4095. The EDR rule-variable "HTPP URL" supports the maximum length of 4095. That is, any URL greater than the maximum length is truncated and then written to EDR.

    In 17.0 and later releases: The length of HTTP URL is from 1 to 4095.

    In 15.0 and 16.0 releases: The length of HTTP URL is from 1 to 255.

    In releases prior to 15.0: The length of HTTP URL is from 1 to 127.
- **user-agent**
  - **length** *size*: This optional filter allows the user to configure the HTTP User-Agent length from 1 to 255. In releases prior to 15.0, the EDR rule-variable "HTPP User-Agent" supports the maximum length of 127. That is, any user-agent greater than 127 is truncated and then written to EDR.
- **version**
- **x-header**: extension header
- **ad-delivered**, **ad-replaced**, **compression-bytes-in**, **compression-bytes-out**, **dns-resolution-locally**, **dns-resolution-remotely**, **tpo-enabled**

Important The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

- **icmp**: Internet Control Message Protocol (ICMP) related fields:

- **code**: ICMP code
- **type**: ICMP type

- **icmpv6**: Internet Control Message Protocol Version 6 (ICMPv6) related fields:
  - **code**: ICMPv6 code
  - **type**: ICMPv6 type

- **imap**: Internet Message Access Protocol (IMAP) related fields:
  - **cc**: IMAP e-mail CC field
  - **command**: IMAP command
  - **content**
  - **date**: IMAP e-mail Date field
  - **final-reply**: IMAP final reply
  - **from**: IMAP e-mail From field
  - **mail-size**: IMAP size of e-mail in RFC822 format
  - **mailbox-size**: IMAP number of e-mails in the mailbox
  - **message-type**: IMAP message type
  - **previous-state**: IMAP session previous state
  - **session-length**: IMAP session length
  - **session-previous-state**: IMAP session previous state
  - **session-state**: IMAP session state
  - **state**: IMAP state
  - **subject**: IMAP e-mail Subject field
  - **to**: IMAP e-mail To field

- **ip**: Internet Protocol (IP) related fields:
  - **dst-address**: destination IP address
  - **protocol**: Protocol being transported by IP packet
  - **server-ip-address**: IP address of server. This field in EDR contains either the IPv4 or IPv6 address of the server for a particular flow (flow level). The maximum length of this field is 48 characters. For an IPv6 address, the maximum length is 45 characters; for an IPv4 address, the maximum length is 15 characters.
  - **src-address**: Source IP address
  - **subscriber-ip-address**: IP address of subscriber. This field in EDR contains either the IPv4 or IPv6 address of the client/subscriber for a particular call (subscriber level). The value of this field does not change for a particular call. The maximum length of this field is 48 characters. For an IPv6

address, the maximum length is 45 characters. For an IPv4 address, the maximum length is 15 characters.

- **total-length**: Total length of packet, including payload
- **version**: IP version

- **mms**: Multimedia Message Service (MMS) related fields:
  - **bcc**
  - **cc**
  - **content location**
  - **content type**
  - **date [format { MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS }]**
  - **from**
  - **message-size**
  - **previous-state**
  - **response status**
  - **state**
  - **subject**
  - **tid**
  - **to**

- **p2p**: Peer-to-peer protocol related fields:
  - **app-identifier { quic-sni | tls-cname | tls-sni }**: P2P application-identifiers - QUIC-SNI, TLS-common name, or TLS-SNI
  - **duration**: P2P protocol duration
  - **protocol**: P2P protocol
  - **protocol-group**: Associated protocol group of the specific P2P protocol/application
  - **ssl-params**: Specifies the SSL flow parameters.
    - **cert-issuer-cname**: Specifies the SSL Certificate Issuer CName.
    - **cert-subject-oname**: Specifies the SSL Certificate Subject Organization Name.
    - **cert-issuer-oname**: Specifies the SSL Certificate Issuer Organization Name.
    - **cert-validity**: Specifies the validity of SSL Certificate.
    - **ssl-decode-failure**: Specifies the reason for SSL Decode failure.

- **pop3**: Post Office Protocol version 3 (POP3) related fields:
  - **command name**: Command of POP3 session

- **mail-size**: Mail size
- **pdu-length**: Length of POP3 PDU
- **pdu-type**: Type of packet
- **previous-state**: Previous state of POP3 session
- **reply status**: Reply for the POP3 command
- **session-length**: Total length of POP3 session
- **state**: Current state of POP3 session
- **user-name**: User of POP3 session

- **rtcp:** RTP Control Protocol (RTCP) related fields:
  - **control-session-flow-id**: Flow ID of the controlling RTSP/SIP session
  - **jitter**: RTCP interarrival jitter
  - **rtsp-id**: RTSP ID of the RTCP flow
  - **uri**: URI of the control protocol related to the RTCP flow
- **rtp**: Real-time Transfer Protocol (RTP) related fields:
  - **control-session-flow-id**: Flow ID of the controlling RTSP/SIP session
  - **pdu-length**: Length of RTP PDU
  - **rtsp-id**: RTSP ID of the flow
  - **session-length**: Total length of RTP session
  - **uri**: URI of the control protocol related to the RTP flow
- **rtsp**: Real Time Streaming Protocol (RTSP) related fields:
  - **command-id**: RTSP command ID
  - **content type**
  - **date**: RTSP Date field
  - **previous-state**: RTSP previous state
  - **reply code**
  - **request method 1**: play method
  - **request method 2**: setup method
  - **request method 3**: pause method
  - **request method 4**: record method
  - **request method 5**: options method
  - **request method 6**: redirect method

- **request method 7**: describe method
- **request method 8**: announce method
- **request method 9**: teardown method
- **request method 10**: get-parameter method
- **request method 11**: set-parameter method
- **request packet**
- **rtp-uri**: RTSP RTP-Info stream-uri field
- **session-id**: RTSP session-id field
- **session-length**: Total number of bytes passed through the RTSP data session
- **state**: RTSP state
- **uri**: RTSP uri field
- **uri sub-part**
- **user-agent**: RTSP user-agent field

- **sdp**: Session Description Protocol (SDP) related fields:
  - **connection-ip-address**: IP address in SDP connection field
  - **media-audio-port**: Port used for audio media
  - **media-video-port**: Port used for video media
- **secure-http**: HTTPS related field.
- **sip**: Session Initiation Protocol (SIP) related fields:
  - **call-id**: SIP call-id field
  - **content type**
  - **from**: SIP From field
  - **previous-state**: SIP previous state
  - **reply code**
  - **request method**
  - **request packet**
  - **state**: SIP state
  - **to**: SIP To field
  - **uri**: SIP URI field
  - **uri sub-part**
- **smtp**: Simple Mail Transfer Protocol (SMTP) related fields:

- **command name**: Command of SMTP session
- **mail-size**: Size of given mail
- **pdu-length**: Length of SMTP PDU
- **previous-state**: Previous state of SMTP session
- **recipient**: SMTP e-mail Recipient field
- **reply status**: Response for the SMTP command
- **sender**: SMTP e-mail Sender field
- **session-length**: Total length of SMTP session
- **state**: Current state of SMTP session

- **tcp**: Transmission Control Protocol (TCP) related fields:
  - **dst-port**: TCP destination port
  - **duplicate**: TCP retransmitted/duplicate packet
  - **flag**: Current packet TCP flag
  - **os-signature**: OS signature string for IPv4 TCP flow. Enables/disables OS Signature field in EDRs sent to MUR.
  - **out-of-order**: TCP out of order packet analyzed
  - **payload-length**: TCP payload length
  - **previous-state**: Previous state of MS
  - **sn-tcp-accl**: TCP Acceleration enabled on flow. Either 0 or 1.
  - **sn-tcp-accl-reject-reason**: Reason for not accelerating the TCP flow.
  - **sn-tcp-min-rtt**: Specifies minimum RTT observed for accelerated TCP flow.
  - **sn-tcp-rtt**: Specifies smoothed RTT for accelerated TCP flow.
  - **src-port**: TCP source port
  - **state**: Current state of MS
  - **tpo-enabled**

Important The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

  - **syn-control-params**: 8 bytes following the TCP Acknowledgement in the TCP SYN packet displayed as hexadecimal string of characters.
  - **syn-options**: All TCP options received in the TCP SYN packet displayed as hexadecimal string of characters.

- **syn-seq**: The absolute 4 byte value of the sequence number received in the TCP SYN packet displayed as decimal value.
- **v6-os-signature**: OS signature string for IPv6 TCP flow. Enables/disables OS Signature field in EDRs sent to MUR.

- **tls sni**: TLS/SSL SNI field (SNI rule variable configured for TLS/SSL flows in EDR).
- **traffic-type**: Traffic type of flow (voice or non-voice depending upon flow type).
- **udp**: User Datagram Protocol (UDP) related fields:
  - **dst-port**: UDP destination port
  - **src-port**: UDP source port
- **voip-duration**: Duration of voice call, in seconds. For a flow in which voice call end is detected, output will be a non-zero value. For other flows it will be zero.

  This is no longer supported for P2P in 14.0 and later releases.
- **wsp**: Wireless Session Protocol (WSP) related fields:
  - **content type**
  - **domain**: WSP domain name
  - **host**: WSP host name
  - **pdu-length**: WSP PDU length
  - **pdu-type**: WSP PDU type
  - **reply code**
  - **session-length**: WSP total packet length
  - **tid**: WSP transaction identifier
  - **total-length**: WSP total packet length
  - **url**: WSP URL
  - **user-agent**: WSP user agent
- **wtp**: Wireless Transaction Protocol (WTP) related fields:
  - **gtr**: Group Transmission Flag
  - **pdu-length**: PDU length of the WTP packet
  - **pdu-type**: WTP protocol data unit information
  - **previous-state**: WTP previous state information
  - **state**: WTP current state information
  - **tid**: WTP transaction identifier
  - **transaction class**: WTP transaction class

- **ttr**: WTP Trailer Transmission flag

Important For more information on protocol-based rules, see the *ACS Ruledef Configuration Mode Commands* chapter.

priority *priority*

Specifies the CSV position of the field (protocol rule) in the EDR.

priority must be an integer from 1 through 65535.

in-quotes

Specifies placing double quotes (" ") around the specified field in the EDR.

Important In this release, this keyword is only valid for the MMS protocol **to** and **subject** fields. **rule-variable mms to priority** *priority* **[in-quotes] rule-variable mms subject priority** *priority* **[in-quotes]**

Usage Guidelines

Use this command to specify what field appears in which order in the EDR.

A particular field in an EDR format can be entered multiple times with different priorities. While removing the EDR field using the **no rule-variable** command you can remove all occurrences of a particular field by specifying the field name or a single occurrence by additionally specifying the optional **priority** keyword.

Example

The following is an example of this command:

```
rule-variable tcp dst-port priority 36
```