NAT ALG Support

Feature Summary and Revision History

Revision History

Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
First introduced	Pre 21.24

Feature Description

Note This feature is not fully qualified in this release.

NAT performs translation service on any Transmission Control Protocol/User Datagram Protocol (TCP/UDP) traffic that doesn't carry source and/or destination IP addresses in application data stream. These protocols include:

- HTTP

- Trivial File Transfer Protocol (TFTP)
- Telnet
- Archie
- Finger
- Network Time Protocol (NTP)
- Network File System (NFS)
- Remote login (rlogin)
- Remote shell protocol (RSH)
- Remote copy protocol (RCP)

The following specific protocols have the IP address information within the payload. These protocols require the support of an Application Level Gateway (ALG) for translation services.

- FTP
- H323
- Session Initiation Protocol (SIP)
- Session Description Protocol (SDP)
- TFTP
- RTSP
- Point-to-Point Tunneling Protocol (PPTP)

Limitations

NAT64 to v4 translation for H323 is not supported.

Components of Session Initiation Protocol ALG

The following block diagram shows all the components that support SIP ALG for NAT or Firewall. The ALG-CORE and SIP APP are the new components. The other components are existing one which requires enhancements.

Note This example is specific to the SIP ALG, similar component is applicable for all other protocols in the document.

Figure 1: Components of Session Initiation Protocol (SIP) ALG

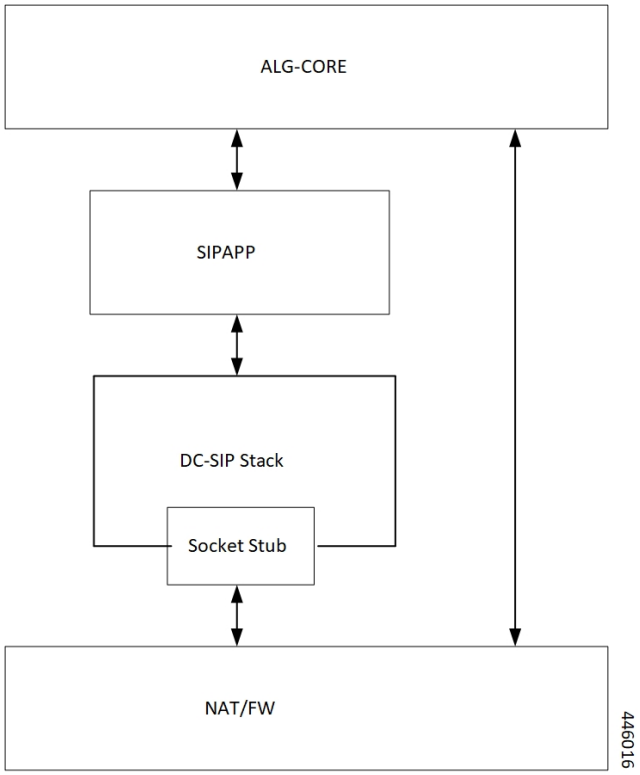

Table 1: Component and Functionality

Component	Function
ALG-CORE	• Interacts with the NAT/FW to create/modify/clear the pinholes. • ALG-CORE has the logic to store the pinhole information inside HA CLP. (defines a new pointer to structure called sip_alg_info). • ALG-CORE processes messages from SIPAPP based on the state and event it received.

Component	Function
SIP APP	• New functionality logic in each per request/response callback. • New data structures to maintain call/session related information's (based on stacks callCb/TransactionCb data structures). • Defines some generic UMM structures for sip/H.323, to interact with the ALG-CORE. • Do the encoding of the SIP message, that is private IP to public IP ...from the information returned by the ALG-CORE.
DC-SIP	DC-SIP is a full-blown sip stack, which parses the sip messages, maintains the transactions and call states. For SIP-ALG functionality the DC-SIP acts as B2BUA. Following are the functionalities DC-SIP stack provides: • Message parsing • Transaction management • Call management • Message encoding • Call back per request/response type.

The Socket Stub is the component that receives/sends packet from/to NAT/FW.

NAT/FW sends/receives the SIP packets to socket stub and it also provides the generic APIs to interact with ALG-CORE.

How it Works

Some of network applications exchanges the IP/Port information of server/client as part of payload. The server or client uses that exchanged IP/Port information to create new flows. As part of NAT ALGs, the server or client extracts that IP/Port info and allow those flows dynamically through pinholes.

In case of NAT, the server or client does the IP and transport level translations. The NAT IP and NAT Port replace the private source IP and source Port and conversely. But the sending application may not be aware of these translations since these translations are transparent.

For example, FTP NAT ALG function interprets the 'PORT' and 'PASV reply' messages. NAT translates the same in the payload so that the FTP happens transparently through the NAT.

NAT layer supports NAT 44 translation and NAT 64 translation. The NAT also supports 1:1 On demand NAT translation and Many:1 NAT translation.

Following are supported for each of the ALGs:

- NAT 44 1:1 On demand NAT translation
- NAT 44 Many:1 NAT translation
- NAT 64 1:1 On demand NAT translation
- NAT 64 Many:1 NAT translation

FTP

FTP is a TCP-based protocol and uses two flows one is for control messages another one for data/file transfer. FTP uses PORT and PASSIVE reply commands to exchange data flow parameters. These commands carry IP and Port information as part of the pay load.

RTSP

RTSP is a TC-based real time streaming protocol having different methods to control real-time media transfer. The control messages are having Port information embed, which is to transfer the media.

PPTP

Point-to-Point Tunneling Protocol (PPTP) allows the tunneling for Point to Point Protocol (PPP) through an IP network. PPTP uses an enhanced GRE (Generic Routing Encapsulation) to carry PPP packets. PPTP exchanges IP or port-specific information over its control connection and that information is to transfer the data over tunnel.

SIP

SIP is an application-layer control protocol. SIP can establish, modify, and terminate multimedia sessions (conferences) such as Internet telephony calls. SIP is based on a request/response transaction model. Each transaction consists of a request that invokes a method, or function, on the server and at least one response. These requests and responses have client and server IP and port information. The SDP message bodies for describing multimedia sessions (that maybe present in SIP requests and responses) also has the IP and port information embedded in them.

For the transmission of media streams (voice, video) the SDP payload carried in SIP messages typically employs the Real-time Transport Protocol (RTP). The SIP ALG intercepts all the SIP communication and translates the private IP and port in the payload to NAT IP and Port.

TFTP

Trivial File Transfer Protocol (TFTP) is an application layer protocol for File Transfers. Due to its simple mechanism, many Embedded Systems uses this protocol to download images or files from the server. It’s a UDP-based protocol. TFTP L7 payload doesn’t contain IP or Port information but requires the pinholes to allow the Downlink initiated data flow.

H323

H323 is a set of protocol specifications that can establish, modify, and terminate multimedia sessions such as Internet telephony calls. Protocols involved in successful multimedia session are RAS, H225, H245, and media protocols (RTP, RTCP). RAS protocol is for communication between H323 Gatekeeper and the terminal. This communication helps to locate the other terminal to which it wants to communicate. H225 and H245 communicates between the terminals for session establishment, capability exchange, and media parameters exchange. The H245 messages have the details of the media channel in which the multimedia communication is going to take place. IP and Port information is present in the RAS, H225 and H245 messages. H323 ALG intercepts all the H323 communication and translates the private IP and port in the payload to NAT IP and Port.

NAT FW Processing

After receiving the key for processing the packets, the ECS framework creates flows with 5-tuple:

- Source IP
- Source port
- Protocol
- Destination IP
- Destination port

If it's the first packet with a given 5-tuple, then a NAT/FW rule match applies to check if the packet is acceptable or not. If packet is acceptable, then leads to a flow is creation.

Configuration of the NAT realm (NAT IP) is part of the rules. The NAT realm applicable for a flow is from the rule-definition that matches the packet

Rule configuration happens are based on well-known server addresses/port numbers. For example, the FTP service with port 21, SIP service with port 5060.

So, any FTP control session or SIP control session to well-known servers/port numbers finds a matching firewall rule. However, it may not be possible to configure rules for media flows (child flows) that are dynamically based on the control signaling.

In case of FTP data or SIP media packet, the NAT/FW rule definition match fails and drops the packets.

Another requirement is the control signaling and the corresponding media connection to use the same NAT realm. Same NAT IP address applies for control and media.

Even if the child flow (media connection) finds a matching NAT/FW rule. The child flow uses the NAT realm configuration for that rule, which isn't correct. The media flows should be using the same NAT realm that is applicable for the control connection.

So, the child flows even if there's no matching rule uses the same NAT realm that was for the control connection. In order to achieve the flow, create the pinholes based on the signaling messages. A pinhole contains subset of 5-tuple information.

Pinholes are to allow the traffic without doing any rule match (bypass rule match). The NAT realm is associated with the pinholes. Allows any traffic matching the pinholes and the NAT realm specified in the pinhole applies for noting the packets.

In case of many-to-one NAT, the NAT allows the downlink packets only if there's an active NAT binding. There are many services (SIP for example) where the remote end wants to initiate connections (incoming call). Under such conditions, to allow downlink packets the ALG needs to create required NAT bindings and associate with the pinholes by parsing signaling messages.

Following explains the uplink and downlink packet processing:

Uplink Packet Processing

Refer to the following points for the uplink packet processing.

- On receiving any uplink packet, comparison takes place against existing 5-tuple flows.
- If a matching flow exists (5-tuple match), the NAT binding that is associated with the flow applies on the packet.
- If no flow exists, then a pinhole lookup happens to check if there are any pinholes opened for this flow.
- If pinhole exists, then the NAT binding associated with the pinhole applies on the packet.
- If no pinhole exists, then rule match determines the NAT information for that flow. If no matching rule exists, the packet drops.

In case of outgoing SIP requests, the SIP message associates with the destination port as 5060. So, configure a rule with destination port as 5060 for identifying SIP traffic. The corresponding NAT realm configured for the rule gets applied on the SIP request.

Any pin holes based on the requests should have NAT bindings associated with them. This NAT bindings allocation is from the NAT realm that was for processing the request.

Downlink Packet Processing

Refer to the following points for the uplink packet processing.

- The downlink packets pass only if an active NAT binding exists. If the binding-look up fails, then the packet drops.
- If the binding lookup succeeds, the packet undergoes initial flow match processing same as an uplink packet processing.
- However, in case of downlink packets, no rule match happens for a packet from on a many-to-one NAT IP. The packet passes only if there's matching flow or a matching pinhole otherwise it drops. If a pinhole exists, then the NAT binding with the pinhole applies on that flow.
- In case of one-to-one NAT, even if there's no pinhole, rule match happens, and packet passes if a matching rule is there. The NAT realm that receives the packet applies for that downlink flow.

Configuring NAT ALG

Following are the commands to configure the NAT ALG.

```
configure
  active-charging service acs_service_name
```

```
    firewall nat-alg { default | no } { ftp | pptp | rtsp | sip | h323
}
    end
```

NOTES:

- **default**: Configures this command with the default setting for the specified parameter.
- **no**: Disables all/ or the specified NAT ALG configuration. When disabled, the ALG(s) will not do any payload translation for NAT calls.
- **ftp**: Enables/disables File Transfer Protocol (FTP) NAT ALG.
- **pptp**: Enables/disables Point-to-Point Tunneling Protocol (PPTP) NAT ALG.
- **rstp**: Enables/disables Real Time Streaming Protocol (RTSP) ALG.
- **sip**: Enables/disables Session Initiation Protocol (SIP) NAT ALG.
- **h323**: Enables/disables H323 NAT ALG.

Configuration for Many to One and One to Many

Many to one configuration on the User Plane.

```
ip pool NAT44_PUBLIC4 209.165.200.225 255.255.255.224 napt-users-per-ip-address 4 group-name
 NAT44_GRP2 on-demand max-chunks-per-user 4 port-chunk-size 32256
```

One to One configuration on the User Plane.

```
ip pool NAT44_PUBLIC4 209.165.200.225 255.255.255.224 nat-one-to-one on-demand group-name
NAT44_GRP1
```

Sample Configuration for FTP NAT ALG

In order to route the packets to the FTP ALG on Control Plane, Configure the following FTP routing rule.

```
Config
active-charging service acs
    ruledef rt_ftp-control
      tcp either-port = 21
      rule-application routing
      multi-line-or all-lines
    #exit
    ruledef rt_ftp-data
      tcp either-port = 20
      rule-application routing
      multi-line-or all-lines
    #exit
   access-ruledef SFW_HTTP
      ip any-match = TRUE
    #exit
    access-ruledef all
      ip any-match = TRUE
    #exit
    access-ruledef ipv6_nat
      ip server-ipv6-network-prefix = 64:ff98::/96
    #exit
    rulebase prepaid
      route priority 14 ruledef rt_ftp-data analyzer ftp-data
      route priority 15 ruledef rt_ftp-control analyzer ftp-control
```

```
    #exit
    fw-and-nat policy nat_policy1
      access-rule priority 1 access-ruledef ipv6_nat permit nat-realm NAT44_GRP1
      access-rule priority 10 access-ruledef SFW_HTTP permit nat-realm NAT44_GRP1
      access-rule priority 100 access-ruledef all permit nat-realm NAT44_GRP1
      nat policy ipv4-and-ipv6
    #exit
firewall nat-alg ftp ipv4-and-ipv6
  #exit
```

Sample Configuration for RTSP NAT ALG

Following are the sample configuration for RTSP NAT ALG:

```
Config
active-charging service acs
    ruledef rtsp-pkts
      tcp src-port = 554
      rule-application routing
    #exit
    ruledef rtsp-pkts1
      tcp dst-port = 554
      rule-application routing
    #exit
      access-ruledef SFW_HTTP
      ip any-match = TRUE
    #exit
      access-ruledef prefix1
      ip server-ipv6-network-prefix = 64:ff98::/96
    #exit
    rulebase cisco
     tcp 2msl-timeout 20
     tcp mss 1300 limit-if-present
      route priority 105 ruledef rtsp-pkts analyzer rtsp
      route priority 106 ruledef rtsp-pkts1 analyzer rtsp
      rtp dynamic-flow-detection
      fw-and-nat default-policy nat_policy1
#exit
fw-and-nat policy nat_policy1
      access-rule priority 1 access-ruledef prefix1 permit nat-realm NAT44_GRP1
      access-rule priority 10 access-ruledef SFW_HTTP permit nat-realm NAT44_GRP1
      nat policy ipv4-and-ipv6
    #exit
    firewall nat-alg rtsp ipv4-and-ipv6
```

Sample Configuration for PPTP NAT ALG

Following are the sample configuration for PPTP NAT ALG:

```
configure
active-charging service ACS
    ruledef pptp-route
      tcp either-port = 1723
      rule-application routing
      multi-line-or all-lines
     exit
     rulebase cisco
     route priority 1 ruledef pptp-route analyzer pptp
     #exit
#exit
access-ruledef all
```

```
      ip any-match = TRUE
#exit
access-ruledef ipv6_nat
ip server-ipv6-network-prefix = 101:101::/96
#exit
     rulebase cisco
     route priority 1 ruledef pptp-route analyzer pptp
     fw-and-nat default-policy nat_policy1
     #exit
      fw-and-nat policy nat_policy1
      access-rule priority 1 access-ruledef ipv6_nat permit nat-realm NAT44_GRP1
      access-rule priority 100 access-ruledef all permit nat-realm NAT44_GRP1
      nat policy ipv4-and-ipv6
    #exit
firewall nat-alg pptp ipv4-and-ipv6
#exit
```

Sample Configuration for TFTP NAT ALG

Following are the sample configuration for NAT44 on Control Plane:

```
configure
active-charging service ACS
    ruledef rt_tftp
      udp either-port = 69
      rule-application routing
      multi-line-or all-lines
    exit
      rulebase cisco
      route priority 1 ruledef rt_tftp analyzer tftp
   #exit
#exit
```

Following are the sample configuration for NAT64 on Control Plane:

```
conf
         active-charging service ACS
         ruledef rt_tftp
         udp either-port = 69
         rule-application routing
         multi-line-or all-lines
         exit
         access-ruledef all
         ip any-match = TRUE
         exit
         access-ruledef ipv6_nat
         ip server-ipv6-network-prefix = 64:ff98::/96
         exit
         rulebase cisco
         route priority 1 ruledef rt_tftp analyzer tftp
         fw-and-nat default-policy nat_policy
         #exit
        end
        conf
       context ISP1
       ip pool NAT44_PVT1 209.165.200.225 255.255.255.224 private 0 group-name NAT44_GRP1
       ip pool NAT44_PVT4 209.165.200.226 255.255.255.224 private 0 group-name NAT44_GRP1
      end
      conf
      context ISP1
      apn cisco.com
      ip address pool name NAT44_GRP1
      fw-and-nat policy nat_policy1
```

```
      exit
      end
     configure
     active-charging service ACS
     fw-and-nat policy nat_policy1
     access-rule priority 1 access-ruledef ipv6_nat permit nat-realm NAT44_GRP1
     access-rule priority 10 access-ruledef all permit nat-realm NAT44_GRP1
     nat policy ipv4-and-ipv6
     end
```

Sample Configuration for H323 NAT ALG

Following are the sample configuration for H323 NAT ALG:

```
configure
active-charging service ACS
     ruledef h323
      udp dst-port = 1719
      rule-application routing
    #exit
    ruledef h323_multi
      udp dst-port = 1718
      rule-application routing
    #exit
    ruledef h323_tcp
      tcp dst-port = 1720
      rule-application routing
    #exit
   rulebase cisco
   route priority 6 ruledef h323 analyzer h323
      route priority 7 ruledef h323_tcp analyzer h323
      route priority 8 ruledef h323_multi analyzer h323
      rtp dynamic-flow-detection
 fw-and-nat default-policy nat_policy1
     #exit
      fw-and-nat policy nat_policy1
      access-rule priority 100 access-ruledef all permit nat-realm NAT44_GRP1
      nat policy ipv4-and-ipv6
   #exit
firewall nat-alg h323 ipv4-only
#exit
```

Sample Configuration for SIP NAT ALG

Following are the sample configuration for SIP NAT ALG:

```
conf
active-charging service service_1
    ruledef sipalg
      udp dst-port = 5060
      rule-application routing
    #exit
    ruledef sipalg_tcp
      tcp dst-port = 5060
      rule-application routing
    #exit
   access-ruledef server2
      ip dst-address = 209.165.200.224/27
    #exit
    access-ruledef nat64
      ip server-ipv6-network-prefix = cccc:1111::/96
```

```
    ip any-match = TRUE
  #exit
  #exit
  rulebase base_1
    route priority 1 ruledef sipalg analyzer sip advanced description advanced
    route priority 2 ruledef sipalg_tcp analyzer sip advanced description advanced
    rtp dynamic-flow-detection
    fw-and-nat default-policy fw1
  #exit
  fw-and-nat policy fw1
    access-rule priority 2 access-ruledef server2 permit nat-realm natPool
    access-rule priority 3 access-ruledef nat64 permit nat-realm natPool
    nat policy ipv4-and-ipv6
  #exit
  firewall nat-alg sip ipv4-and-ipv6
  #exit
#exi
```

Monitoring and Troubleshooting

This section provides information on CLI commands that are available for monitoring and troubleshooting for NAT ALG feature in CUPS.

Show Commands and/or Outputs

This section provides information about show CLI commands that are available in support of NAT ALG feature in CUPS.

- **show user-plane-service statistics analyzer name rtsp**: Use this command to view RTSP-related statistics.

```
RTSP Session Stats:
   Total Uplink Bytes:             844   Total Downlink Bytes:          1440
   Total Uplink Pkts:               10   Total Downlink Pkts:              6
   Uplink RTP Bytes:                 8   Downlink RTP Bytes:         2851524
   Uplink RTP Pkts:                  2   Downlink RTP Pkts:             2741
   Uplink Retry Bytes:               0   Downlink Retry Bytes:             0
   Uplink Retry Pkts:                0   Downlink Retry Pkts:              0
   RTSP Sessions:                    1
```

- **show user-plane-service statistics analyzer name rtp**: Use this command to view RTP-related statistics.

```
RTP Session Stats:
   Total Uplink Bytes:               8   Total Downlink Bytes:       2851524
   Total Uplink Pkts:                2   Total Downlink Pkts:           2741

FastPath Statistics :
   Total FP Flows:                   1
   Total Uplink FP Bytes:            0   Total Downlink FP Bytes:    2850497
   Total Uplink FP Pkts:             0   Total Downlink FP Pkts:        2740
```

- **show user-plane-service statistics analyzer name rtcp**: Use this command to view RTCP-related statistics.

```
RTCP Session Stats:
      Total Uplink Bytes:          804   Total Downlink Bytes:           728
      Total Uplink Pkts:            16   Total Downlink Pkts:             13
```

- **show user-plane-service statistics analyzer name ftp**: Use this command to view FTP-related statistics.

```
FTP Session Stats:
   Current Control Sessions:         1         Current Data Sessions:         1
   Total Control Sessions:           1         Total Data Sessions:           3
   Uplink Control Bytes:           190         Downlink Control Bytes:      544
   Uplink Control Pkts:             23         Downlink Control Pkts:        15
   Uplink Data Bytes:             6733            Downlink Data Bytes:       12444
   Uplink Data Pkts:              5136         Downlink Data Pkts:           14
   Uplink Error Bytes:               0         Downlink Error Bytes:          0
   Uplink Error Pkts:                0         Downlink Error Pkts:           0
   Request Succeed:                 14         Request Failed:                0
   Unknown Requests:                 0         Unknown Responses:             0
   Uplink Bytes Retrans:             0         Downlink Bytes Retrans:        0
   Uplink Pkts Retrans:              0         Downlink Pkts Retrans:         0
   RETR commands:                    2         STOR commands:                 1
   Unknown packets received:                                                  0
   Data packet received without control connection:                           0
   Invalid packets:                                                           0
   Packets that could not be parsed:                                          0

FastPath Statistics :
   Total FP Control Flows:           0
   Total FP Data Flows:              3
 Uplink :                                  Downlink :
   Total FP Control Pkts :           0      Total FP Control Pkts :           0
   Total FP Control Bytes :          0      Total FP Control Bytes:           0
   Total FP Data Pkts :              0      Total FP Data Pkts :              0
   Total FP Data Bytes :             0      Total FP Data Bytes:              0
```

- **show user-plane-service statistics analyzer name pptp**: Use this command to view PPTP-related statistics.

```
PPTP Session Stats:
  Total Uplink Bytes:               0   Total Downlink Bytes:             0
  Total Uplink Pkts:                0   Total Downlink Pkts:              0
  Total GRE Sessions:               0   Invalid PPTP Pkts:                0
  Unknown PPTP Pkts:                0

  PPTP-GRE Session Stats:
  Total Uplink Bytes:               0   Total Downlink Bytes:             0
  Total Uplink Pkts:                0   Total Downlink Pkts:              0
```

- **show user-plane-service statistics analyzer name h323**: Use this command to view H323-related statistics.

```
H323 Session Stats:
  Total Uplink Bytes              0       Total Downlink Bytes             0
  Total Uplink Packets            0       Total Downlink Packets           0
  Total H323 calls                0
  Total RAS messages              0
  Total Q931 messages             0
  Total H245 messages             0
```

  - **show user-plane-service statistics analyzer name h323 protocol ras**: Use this command to view the h323 protocol ras statistics.

```
  Total RAS messages                  0
    RAS messages                             Uplink
  Downlink
    --------------                     ------------
  ------------
    GatekeeperRequest                          0
     0
    GatekeeperConfirm                          0
     0
    GatekeeperReject                           0
```

```
 0
RegistrationRequest                        0
 0
RegistrationConfirm                        0
 0
RegistrationReject                         0
 0
UnregistrationRequest                      0
 0
UnregistrationConfirm                      0
 0
UnregistrationReject                       0
 0
AdmissionRequest                           0
 0
AdmissionConfirm                           0
 0
AdmissionReject                            0
 0
LocationRequest                            0
 0
LocationConfirm                            0
 0
LocationReject                             0
 0
DisengageRequest                           0
 0
DisengageConfirm                           0
 0
DisengageReject                            0
 0
InfoRequest                                0
 0
InfoRequestResponse                        0
 0
RequestInProgress                          0
 0
Unclassified                               0
 0
```

- **show user-plane-service statistics analyzer name h323**: Use this command to view H323-related statistics.

```
H323 Session Stats:
  Total Uplink Bytes              0       Total Downlink Bytes             0
  Total Uplink Packets            0       Total Downlink Packets           0
  Total H323 calls                0
  Total RAS messages              0
  Total Q931 messages             0
  Total H245 messages             0
```

  - **show user-plane-service statistics analyzer name h323 protocol h245** : Use this command to view the h323 protocol h245 statistics.

```
Total H245 messages                 0
 H245 messages                     Uplink                              Downlink

 -------------                    ------------
------------
 OpenLogicalChannel                         0
   0
 OpenLogicalChannelAck                      0
   0
 OpenLogicalChannelReject                   0
```

```
    0
   OpenLogicalChannelConfirm                  0
    0
   RequestChannelClose                        0
    0
   CloseLogicalChannel                        0
    0
   CloseLogicalChannelAck                     0
    0
   EndSessionCommand                          0
    0
   Unclassified                               0
    0
```

- **show user-plane-service statistics analyzer name h323 protocol q931** : Use this command to view the h323 protocol q931 statistics.

```
  Total Q931 messages                  0
    Q931 messages                      Uplink                              Downlink

    -------------                     ------------
  -------------
    Alerting                                  0
     0
    CallProceeding                            0
     0
    Setup                                     0
     0
    Connect                                   0
     0
    ReleaseComplete                           0
     0
    Facility                                  0
     0
    Progress                                  0
     0
    Information                               0
     0
    Unclassified                              0
     0
```

- **show user-plane-service statistics analyzer name tftp**: Use this command to view TFTP-related statistics.

```
TFTP Session Stats:
  Total Uplink Bytes:                0   Total Downlink Bytes:                0
  Total Uplink Packets:              0   Total Downlink Packets:              0
  Total Read Sessions:               0   Total Write Sessions:                0
  Total Invalid Control Packets:                                          0
  Total Invalid Data Packets:                                             0
  Total Packets with Unknown Request Type:                                0

  TFTP DATA Session Stats:
  Total Uplink Bytes:                0   Total Downlink Bytes:                0
  Total Uplink Packets:              0   Total Downlink Packets:              0
```

- **show user-plane-service statistics analyzer name sip**: Use this command to view SIP-related statistics.

```
SIP Session Stats:
      Total Uplink Bytes:              0          Total Downlink Bytes:          0
      Total Uplink Pkts:               0          Total Downlink Pkts:           0
      Uplink Valid Pkts:               0          Downlink Valid Pkts:           0
      Uplink Retry Pkts:               0          Downlink Retry Pkts:           0
      Uplink Error Pkts:               0          Downlink Error Pkts:           0
```

```
      Total SIP Calls:                 0
SIP Advanced Session Stats:
  Total Uplink Bytes               0   Total Downlink Bytes              0
  Total Uplink Packets             0   Total Downlink Packets            0

  Total SIP Calls                  0   Current SIP Calls                 0
  Total SIP UDP Calls              0   Current SIP UDP Calls             0
  Total SIP TCP Calls              0   Current SIP TCP Calls             0

  SIP Request                          Total received         Total transmitted
      Retransmitted
  -----------                      --------------------     --------------------
--------------------
  Register                                        0                        0
               0
  Invite                                          0                          0
                 0
  Ack                                             0                          0
                 0
  Bye                                             0                          0
                 0
  Info                                             0                         0
                  0
  Prack                                           0                          0
                 0
  Refer                                           0                          0
                 0
  Cancel                                         0                          0
                0
  Update                                         0                          0
                0
  Message                                        0                         0
               0
  Options                                         0                          0
                0
  Publish                                         0                          0
                 0
  Subscribe                                      0                         0
               0
  Notify                                          0                          0
                 0


  SIP Response                         Total received         Total transmitted
      Retransmitted
  ------------                     --------------------     --------------------
--------------------
  1XX                                             0                          0
                 0
  2XX                                             0                          0
                 0
  3XX                                             0                          0
                 0
  4XX                                             0                          0
                 0
  5XX                                             0                          0
                 0
  6XX                                             0                          0
                 0
```