



# Monitor Protocol and Subscriber

- [Feature Summary and Revision History, on page 1](#)
- [Feature Description, on page 1](#)
- [Configuring Monitor Subscriber and Protocol, on page 2](#)

## Feature Summary and Revision History

### Summary Data

*Table 1: Summary Data*

Applicable Product(s) or Functional Area	cnBNG
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Documentation	<i>Cloud Native BNG Control Plane Command Reference Guide</i>

### Revision History

*Table 2: Revision History*

Revision Details	Release
First introduced.	2021.03.0

## Feature Description

The Monitor Subscriber and Protocol feature supports the debugging functionality.

### Monitor Subscriber

The Monitor Subscriber feature captures all the transactional logs for a given subscriber over a specified period of time across all the Kubernetes pods. It also supports the simultaneous monitoring of multiple subscribers on a given cluster. This information allows to track all the events that had occurred for a given subscriber when the subscriber was coming up or going down.

### Monitor Protocol

The Monitor Protocol feature replicates the packets from different protocol endpoints of cnBNG and sends it to the OAM pod. There two levels of packet replication that occur:

- First replication dumps only the basic packet information
- Second replication dumps the full packet with details like headers, keys of subscriber, and so on.

This feature captures all ingress and egress packets on the cnBNG protocol pods.

## Configuring Monitor Subscriber and Protocol

This section describes how to configure subscriber and protocol monitoring.

Configuring the Monitor Subscriber and Protocol feature involves the following procedures:

- Configuring Monitor Subscriber
- Configuring Monitor Protocol
- Copying Log Files
- Viewing Log Files

## Configuring Monitor Subscriber

Use the following commands to enable the monitoring of a subscriber.

```
monitor subscriber supi subscriber_id capture-duration duration_in_seconds
```

### NOTES:

- **supi** *subscriber\_id*: Enables monitoring of subscribers based on the subscriber identifier (supi). For example: 0000.4096.3e4a.

The subscriber-id format supported is as follows:

<mac-address>@<upf>: This specifies a particular subscriber with the given MAC address from a specific User Plane function (UPF).

Wildcard subscriber-id is also supported. For example:

- \*@<upf>: This specifies all subscribers from a specific UPF.
- <mac>@\*: This specifies all subscribers having the given MAC and from any UPF.
- \*: This specifies all subscribers from all UPFs.

- **capture-duration** : Specifies the duration in seconds during which the monitor subscriber is enabled. The *duration\_in\_seconds* can range from 1 to 2147483647 seconds. The default is 300.
- Other sub-options that are present in the CLI command are not supported

### Example

```

bng# monitor subscriber supi aabb.0000.0001@automation-userplane
supi: aabb.0000.0001@automation-userplane
captureDuration: 300
enableInternalMsg: false
enableTxnLog: false
namespace(deprecated. Use nf-service instead.): none
nf-service: none
gr-instance: 0
  % Total      % Received % Xferd  Average Speed   Time    Time       Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  337  100   119  100   218  10818  19818  --:--:--  --:--:--  --:--:-- 30636
Command: --header Content-type:application/json --request POST --data
('{"name":"mon_sub","params":{"supi":"aabb.0000.0001@automation-userplane","data":{"id":"aabb.0000.0001@automation-userplane","enableInternalMsg":false,"enableTxnLog":false,"nf-service":"none","gr-instance":0}}
http://oam-pod:8879/commands
Result start mon_sub, fileName
->logs/monsublogs/none.aabb.0000.0001@automation-userplane_TS_2021-06-09T12:17:33.838574118.txt
Starting to tail the monsub messages from file:
logs/monsublogs/none.aabb.0000.0001@automation-userplane_TS_2021-06-09T12:17:33.838574118.txt
Defaulting container name to oam-pod.
Use 'kubectl describe pod/oam-pod-0 -n bng' to see all of the containers in this pod.
Subscriber Id: aabb.0000.0001@automation-userplane
Timestamp: 2021/06/09 12:19:30.194843
Message: BNGN4UdpProxyMessage
Description: Received Packet IPOE, IPC Message from udp-proxy
Source: bng.udp-proxy.DC.Local.0
Destination: bng.bng-n4-protocol.DC.Local.0
PAYLOAD:
  BNGN4UdpProxyMessage:
    BNGN4UdpProxyMessage:
      Type: 6
      L2Data:
        SrcMac: aabb.0000.0001
        DstMac: ffff.ffff.ffff
        Outervlan: 100
        Innervlan: 200
        OuterCos: 0
        InnerCos: 0
      IpAddr:
        AfType: 1
        SrcIpv4:
        SrcIpv6:
        DstIPv4: 8.8.8.8
        DstIPv6:
        LinkLocal:
        Port: 8000
      UpData:
        AccessInterface: GigabitEthernet0/0/0/1
        CpSubscriberId: 0
        UpSubscriberId: 0
        UPSubInterfaceId: 0
        RouterName: automation-userplane
        AccessVrf: access-vrf-1
        NASID: NAS-ID-1
      NasInfo:
        Port: 4

```

```

        Slot: 2
        Adapter: 5
        Subslot: 3
        Chassis: 1
        InterfaceType: 1
    L2TPData:
        PuntPoliceRate: 0
        L2TPTos: 0
        TunnelID: 0
    Packet:
        Payload:
            BaseLayer:
            Operation: 1
            HardwareType: 1
            HardwareLen: 6
            HardwareOpts: 0
            Xid: 1
            Secs: 0
            Flags: 32768
            ClientIP: 0.0.0.0
            YourClientIP: 0.0.0.0
            NextServerIP: 0.0.0.0
            RelayAgentIP: 0.0.0.0
            ClientHWAddr: aa:bb:00:00:00:01
            ServerName:
            File:
            Options: {
    Option(MessageType:Discover)
    Option(ClientID:[1 170 187 0 0 0 1])
}

```

```

-----
Subscriber Id: aabb.0000.0001@automation-userplane
Timestamp: 2021/06/09 12:19:30.205174
Message: RadiusUdpProxyMsg
Description: Send Auth/Acct Request Message to UDP-Proxy
Source: bng.radius-ep.DC.Local.0
Destination: bng.udp-proxy.DC.Local.0
PAYLOAD:
    RadiusUdpProxyMsg:
        RadiusUdpProxyMsg:
            SrcIp: 10.105.254.113
            SrcPort: 16384
            DestIp: 10.105.254.114
            DestPort: 1812
            Payload:
Code = AccessRequest
Id = 2
Authenticator = [148 88 241 197 50 83 83 156 105 245 107 167 117 131 237 165]
User-Name = "cnbng"
User-Password = 0x30b19d11f96401290b6410e8a1b324eb
NAS-IP-Address = 10.105.254.113
NAS-Port = 16384
Service-Type = 5
Called-Station-Id = "1"
Calling-Station-Id = "1"
Nas-Identifier = "bng"
Acct-Session-Id = "Local_DC_16777218"
Event-Timestamp = 1623241161
NAS-Port-Type = 41
NAS-Port-Id = "124536"
NAS-IPv6-Address = ::/0
Cisco-Vsa_cisco-nas-port = "124536"

```

```

Cisco-Vsa_cisco-dhcp-client-id = 0x01aabb00000001
Cisco-Vsa_Cisco AVpair = "client-mac-address=aabb.0000.0001"
Cisco-Vsa_Cisco AVpair = 0x646863702d636c69656e742d69643d01aabb00000001
    PayloadLen: 231
    SubscriberID: aabb.0000.0001@automation-userplane

```

```

-----
Subscriber Id: aabb.0000.0001@automation-userplane
Timestamp: 2021/06/09 12:19:30.206778
Message: RadiusUdpProxyMsg
Description: Received Auth/Acct Response Message from UDP-Proxy
Source: bng.udp-proxy.DC.Local.0
Destination: bng.radius-ep.DC.Local.0
PAYLOAD:
  RadiusUdpProxyMsg:
    RadiusUdpProxyMsg:
      SrcIp: 10.105.254.114
      SrcPort: 1812
      DestIp: 10.105.254.113
      DestPort: 16384
      Payload:
Code = AccessAccept
Id = 2
Authenticator = [127 214 195 68 205 142 58 23 126 138 11 70 241 169 153 92]
    PayloadLen: 20

```

```

-----
Subscriber Id: aabb.0000.0001@automation-userplane
Timestamp: 2021/06/09 12:19:30.216130
Message: DHCPPTx
Description: Sending Packet IPOE, IPC Message to udp-proxy
Source: bng.bng-n4-protocol.DC.Local.0
Destination: bng.udp-proxy.DC.Local.0
PAYLOAD:
  DHCPPTx:
    DHCPPTx:
      Type: 6
      L2Data:
        DstMac: ff:ff:ff:ff:ff:ff
        Outervlan: 100
        Innervlan: 200
        OuterCos: 0
        InnerCos: 0
      IpAddr:
        AfType: 1
        SrcIpv4: 33.0.0.1
        SrcIpv6:
        DstIPv4: 255.255.255.255
        DstIPv6:
        LinkLocal:
        Port: 68
      UpData:
        AccessInterface: GigabitEthernet0/0/0/1
        CpSubscriberId: 16777218
        UpSubscriberId: 0
        USubInterfaceId: 0
        RouterName: automation-userplane
        AccessVrf: access-vrf-1
        NASID: NAS-ID-1
    Packet:
      Payload:
        BaseLayer:

```

```

        Operation: 2
        HardwareType: 1
        HardwareLen: 6
        HardwareOpts: 0
        Xid: 1
        Secs: 0
        Flags: 32768
        ClientIP: 0.0.0.0
        YourClientIP: 33.0.0.3
        NextServerIP: 0.0.0.0
        RelayAgentIP: 0.0.0.0
        ClientHWAddr: aa:bb:00:00:00:01
        ServerName:
        File:
        Options: {
Option (MessageType:Offer)
Option (ClientID:[1 170 187 0 0 0 1])
Option (SubnetMask:255.255.224.0)
Option (LeaseTime:90060)
Option (Timer1:45030)
Option (Timer2:78802)
Option (ServerID:33.0.0.1)
}

```

```

-----
Subscriber Id: aabb.0000.0001@automation-userplane
Timestamp: 2021/06/09 12:19:30.293167
Message: BNGN4UdpProxyMessage
Description: Received Packet IPOE, IPC Message from udp-proxy
Source: bng.udp-proxy.DC.Local.0
Destination: bng.bng-n4-protocol.DC.Local.0
PAYLOAD:
  BNGN4UdpProxyMessage:
    BNGN4UdpProxyMessage:
      Type: 6
      L2Data:
        SrcMac: aabb.0000.0001
        DstMac: ffff.ffff.ffff
        Outervlan: 100
        Innervlan: 200
        OuterCos: 0
        InnerCos: 0
      IpAddr:
        AfType: 1
        SrcIpv4:
        SrcIpv6:
        DstIPv4: 8.8.8.8
        DstIPv6:
        LinkLocal:
        Port: 8000
      UpData:
        AccessInterface: GigabitEthernet0/0/0/1
        CpSubscriberId: 0
        UpSubscriberId: 0
        USubInterfaceId: 0
        RouterName: automation-userplane
        AccessVrf: access-vrf-1
        NASID: NAS-ID-1
      NasInfo:
        Port: 4
        Slot: 2
        Adapter: 5
        Subslot: 3

```

```

    Chasis: 1
    InterfaceType: 1
L2TPData:
    PuntPoliceRate: 0
    L2TPTos: 0
    TunnelID: 0
Packet:
    Payload:
        BaseLayer:
            Operation: 1
            HardwareType: 1
            HardwareLen: 6
            HardwareOpts: 0
            Xid: 1
            Secs: 0
            Flags: 32768
            ClientIP: 0.0.0.0
            YourClientIP: 0.0.0.0
            NextServerIP: 0.0.0.0
            RelayAgentIP: 0.0.0.0
            ClientHWAddr: aa:bb:00:00:00:01
            ServerName:
            File:
            Options: {
Option(MessageType:Request)
Option(ClientID:[1 170 187 0 0 0 1])
Option(ServerID:33.0.0.1)
Option(RequestIP:33.0.0.3)
}

```

```

-----
Subscriber Id: aabb.0000.0001@automation-userplane
Timestamp: 2021/06/09 12:19:30.301343
Message: BNGN4SessionEstablishmentReq
Description: Sending N4 Session Establishment Request, IPC Message to udp-proxy
Source: bng.bng-n4-protocol.DC.Local.0
Destination: bng.udp-proxy.DC.Local.0
PAYLOAD:
    BNGN4SessionEstablishmentReq:
        BNGN4SessionEstablishmentReq:
            PfcpsessionHeader:
                Version: 1
                SeidSet: true
                MessageType: 50
                MessageLen: 413
                SequenceNumber: 5
                Seid: 0
                Priority: 1
            NodeID:
                Valid: true
                Ip: Afi=v4 Ip=10.105.254.113
            Fseid:
                Valid: true
                Seid: 16777218
                Ipv4: 0.0.0.0
                Ipv6:
            CreatePdrList:
                CreatePdrList[0]:
                    Valid: true
                    PdrId:
                        Valid: true
                        RuleId: 1
                    Precedence:

```

```

        Valid: true
        Val: 1
Pdi:
    Valid: true
    SrcIface:
        Valid: true
        Value: 1
    TrafficEndptId:
        Valid: true
        Val: 1
FarId:
    Valid: true
    Val: 1
OuterHeaderRemoval:
    Valid: false
    Description: 0
UrrId:
    Valid: true
    Val: 1
CreatePdrList[1]:
    Valid: true
    PdrId:
        Valid: true
        RuleId: 2
    Precedence:
        Valid: true
        Val: 1
    Pdi:
        Valid: true
        SrcIface:
            Valid: true
            Value: 2
        TrafficEndptId:
            Valid: false
            Val: 0
    FarId:
        Valid: true
        Val: 2
    OuterHeaderRemoval:
        Valid: false
        Description: 0
    UrrId:
        Valid: false
        Val: 0
CreateFarList:
    CreateFarList[0]:
        Valid: true
        FarId:
            Valid: true
            Val: 1
        ApplyAction:
            Valid: true
            Drop: false
            Forward: true
            Buffer: false
            NotifyCP: false
            Duplicate: false
        ForwParams:
            Valid: true
            DestIface:
                Valid: true
                Value: 2
            OuterHeaderCreation:
                Valid: true

```



```
        CprNSH: false
        TfEndpt: true
        L2tp: false
        Ppp: false
        TunnelID: 0
        SessionID: 0
DuplParams:
    Valid: false
    DestIface:
        Valid: false
        Value: 0
    OuterHeaderCreation:
        Valid: false
        Teid: 0
        Ipv4:
        Ipv6:
        PortNum: 0
    IntrInfo:
        Valid: false
        InterceptId:
            Valid: false
        Dscp:
            Valid: false
            Dscp: 0
CreateFarList[1]:
    Valid: true
    FarId:
        Valid: true
        Val: 2
    ApplyAction:
        Valid: true
        Drop: false
        Forward: true
        Buffer: false
        NotifyCP: false
        Duplicate: false
ForwParams:
    Valid: true
    DestIface:
        Valid: true
        Value: 1
    OuterHeaderCreation:
        Valid: true
        CprNSH: false
        TfEndpt: true
        L2tp: false
        Ppp: false
        TunnelID: 0
        SessionID: 0
DuplParams:
    Valid: false
    DestIface:
        Valid: false
        Value: 0
    OuterHeaderCreation:
        Valid: false
        Teid: 0
        Ipv4:
        Ipv6:
        PortNum: 0
    IntrInfo:
        Valid: false
        InterceptId:
            Valid: false
```

```

        Dscp:
            Valid: false
            Dscp: 0
CreateTrafficEndptList:
CreateTrafficEndptList[0]:
    Valid: true
    Tfid:
        Valid: true
        Val: 1
    AccessPortId:
        Valid: true
        Value: GigabitEthernet0/0/0/1
    UeIPAddr:
        Valid: true
        Flags: 2
        Ipv4Addr: Afi=v4 Ip=33.0.0.3
        Ipv6Addr:
        IPv6PrefixLen: 0
        Ipv6PAddr:
        Ipv6LLAddr:
    UeMacAddress: aa:bb:00:00:00:01
    PppoeSessId:
        Valid: false
        Value: 0
    AddressFamily:
        Valid: true
        Value: 3
    Cvlan:
        Valid: true
        Pcp: 0
        Dei: 0
        VlanId: 200
    Svaln:
        Valid: true
        Pcp: 0
        Dei: 0
        VlanId: 100
    L2tpTunnel:
        Valid: false
        TunnelEndpoint:
            Valid: false
            Choose: false
            LocalID: 0
            RemoteID: 0
        SessionID:
            Valid: false
            SessionID: 0
            RemoteSessionID: 0
        TunnelFeatures:
            Valid: false
            SetTOS: false
            ReflectTOS: false
            SetDF: false
            ReflectDF: false
            TcpMssAdjust: false
            TunnelStatsEnabled: false
            SessStatsEnabled: false
            TSI: false
            SSI: false
            TosVal: 0
            TcpMssVal: 0
            TunnelStatsInterval: 0
            SessStatsInterval: 0
SubParams:

```

```

Valid: true
Stype:
  Valid: true
  Value: 1
SrgIntfId:
  Valid: false
  Value: 0
SrgGrpId:
  Valid: false
  Value: 0
Vrf:
  Valid: true
  Value: automation-vrf
AccessVrf:
  Valid: false
CreateURR:
  CreateURR[0]:
    Valid: true
    UrrID:
      Valid: true
      Val: 1
    MeasurementMethod:
      Valid: true
      Event: false
      Volume: true
      Duration: false
    Trigger:
      Valid: true
      PeriodicReporting: true
      VolumeThreshold: false
      TimeThreshold: false
      QuotaHoldingTime: false
      StartOfTraffic: false
      StopOfTraffic: false
      DroppedDlTrafficThreshold: false
      ImmediateReport: false
      VolumeQuota: false
      TimeQuota: false
      LinkedUsageReporting: false
      TerminationReport: true
      MonitoringTime: false
      EnvelopeClosure: false
      MacAddressReporting: false
      EventThreshold: false
      EventQuota: false
      TerminationByUP: false
    MeasurementPeriod:
      Valid: true
      Val: 1940
Keepalive:
  Valid: false
  Tfid:
    Valid: false
    Val: 0
  Timer:
    Valid: false
    TimeInterval: 0
    RetryCount: 0
  MagicNum:
    Valid: false
    LocalMagicNum: 0
    PeerMagicNum: 0
CreateQspList:
  CreateQspList[0]:

```

```

Valid: true
Service:
  Valid: true
  Length: 0
  Value: automation-feature-template-accounting
QoSIngress:
  Valid: true
  Length: 0
  Name: inpolicy
  Priority: 0
QoSEgress:
  Valid: true
  Length: 0
  Name: outpolicy
  Priority: 0
Stats:
  Valid: true
  Value: true
Spi:
  Valid: false
  Value: 0
PlainQos: false
CreateACL:
  Valid: false
  Ipv4InACL:
    Valid: false
  Ipv4OutACL:
    Valid: false
  Ipv6InACL:
    Valid: false
  Ipv6OutACL:
    Valid: false
CreatePBR:
  Valid: false
  PbrIngress:
    Valid: false
    Length: 0
CreateuRPF:
  Valid: false
  Strictv4: false
  Strictv6: false
  Loosev4: false
  Loosev6: false
CreateICMP:
  Valid: false
  V4: false
  V6: false
RemoveICMP:
  Valid: false
  V4: false
  V6: false
CreateMTU:
  Valid: true
  V4Mtu: 1400
  V6Mtu: 0
  PPPMtu: 0
TransactionIdentifier:
  Valid: true
  Value: 1
-----

```

## Configuring Monitor Protocol

Use the following commands to enable protocol monitoring for a subscriber.

```
monitor protocol interface pcap_interface capture-duration duration_in_seconds
```

### NOTES:

- **interface** *pcap\_interface* : Specifies the packet capture (PCAP) interface. The valid PCAP interfaces are: Packet Forwarding Control Protocol (PFCP), GPRS Tunnelling Protocol User Plane (GTP-U), and Remote Authentication Dial-In User Service (RADIUS).
- **capture-duration** *duration\_in\_seconds* : Specifies the duration in seconds during which the monitor protocol is enabled. The *duration\_in\_seconds* can range from 1 to 2147483647 seconds. The default is 300.
- cnBNG uses a custom GTPU packet format. Therefore, packet decode errors are displayed on the screen because the standard decode plugin does not support the cnBNG format. Capture the packet to PCAP and use the cnBNG specific LUA plugin during Wireshark decode.
- Interface names must be entered manually and must match the name mentioned in the description, else the packet capture may fail.
- Only one physical-interface (NIC) packet capture is supported. For PFCP and GTPU this limitation is not applicable as they always run-on a single interface (VIP). However for RADIUS, certain deployments may use different VIPs for Auth/Acct/COA, leading to different physical NICs. Due to the infrastructure limitation, packet-capture can run on only one of the physical-NICs.

### Example

```
monitor protocol interface pfcfcp
```

```
InterfaceName = N4:10.86.73.161:8805 | InterfaceIP = 10.86.73.161 | Filter = (tcp or udp)
and (port 8805)
<<<<OUTBOUND
from 10.86.73.161:8805 to 10.86.73.162:8805
Protocol: UDP | Sequence Number: 0
Packet Metadata: {Timestamp:2019-10-22 09:22:34.029363 +0000 UTC CaptureLength:72 Length:72
InterfaceIndex:2 AncillaryData:[]}
```

Packet Raw Bytes:

```
0050569c14610050569c85c08004500003a76c5400040111bffa5649a10a5649a226522650026a8262006001a00000004003c0005000a5649a100130010100600004e159480e
```

Packet Dump:

```
-- FULL PACKET DATA (72 bytes) -----
00000000 00 50 56 9c 14 61 00 50 56 9c 8d 5c 08 00 45 00
00000010 00 3a 76 c5 40 00 40 11 1b ff 0a 56 49 a1 0a 56
00000020 49 a2 22 65 22 65 00 26 a8 26 20 06 00 1a 00 00
00000030 00 04 00 3c 00 05 00 0a 56 49 a1 00 13 00 01 01
00000040 00 60 00 04 e1 59 48 0e
--- Layer 1 ---
Ethernet {Contents=[..14..] Payload=[..58..] SrcMAC=00:50:56:9c:8d:5c DstMAC=00:50:56:9c:14:61
EthernetType=IPv4 Length=0}
00000000 00 50 56 9c 14 61 00 50 56 9c 8d 5c 08 00
--- Layer 2 ---
IPv4 {Contents=[..20..] Payload=[..38..] Version=4 IHL=5 TOS=0 Length=58 Id=30405 Flags=DF
FragOffset=0 TTL=64 Protocol=UDP Checksum=7167 SrcIP=10.86.73.161 DstIP=10.86.73.162
Options=[] Padding=[]}
00000000 45 00 00 3a 76 c5 40 00 40 11 1b ff 0a 56 49 a1
```

```

00000010 0a 56 49 a2
--- Layer 3 ---
UDP {Contents=[.8..] Payload=[.30..] SrcPort=8805(pfcp) DstPort=8805(pfcp) Length=38
Checksum=43046}
00000000 22 65 22 65 00 26 a8 26 |"e"e.&.&|
--- Layer 4 ---
Payload 30 byte(s)
00000000 20 06 00 1a 00 00 00 04 00 3c 00 05 00 0a 56 49
00000010 a1 00 13 00 01 01 00 60 00 04 e1 59 48 0e

```

## Copying Log Files

Use the following commands to copy the stored log files externally or on the BNG Ops Center.

These files either can be copied outside or dumped on the bng-opscenter using the following CLI command.

```
monitor subscriber-dump filename <file path got from monitor
subscriber-list CLI>
```

### Example:

```

monitor subscriber dump filename
/opt/workspace/logs/monsublogs/none.aabb.0000.0001@automation-userplane_TS_2021-06-09T12:17:33.838574118.txt.sorted
RELEASE_NAMESPACE: 'bng'
Dumping file
'/opt/workspace/logs/monsublogs/none.aabb.0000.0001@automation-userplane_TS_2021-06-09T12:17:33.838574118.txt.sorted'
**** Received 19 messages ****
Subscriber Id: aabb.0000.0001@automation-userplane
Timestamp: 2021/06/09 12:19:30.194843
Message: BNGN4UdpProxyMessage
Description: Received Packet IPOE, IPC Message from udp-proxy
Source: bng.udp-proxy.DC.Local.0
Destination: bng.bng-n4-protocol.DC.Local.0
PAYLOAD:
  BNGN4UdpProxyMessage:
    BNGN4UdpProxyMessage:
      Type: 6
      L2Data:
        SrcMac: aabb.0000.0001
        DstMac: ffff.ffff.ffff
        Outervlan: 100
        Innervlan: 200
        OuterCos: 0
        InnerCos: 0
      IpAddr:
        AfType: 1
        SrcIpv4:
        SrcIpv6:
        DstIPv4: 8.8.8.8
        DstIPv6:
        LinkLocal:
        Port: 8000
      UpData:
        AccessInterface: GigabitEthernet0/0/0/1
        CpSubscriberId: 0
        UpSubscriberId: 0
        USubInterfaceId: 0
        RouterName: automation-userplane
        AccessVrf: access-vrf-1
        NASID: NAS-ID-1
      NasInfo:
        Port: 4
        Slot: 2

```

```
Adapter: 5
Subslot: 3
Chassis: 1
InterfaceType: 1
L2TPData:
  PuntPoliceRate: 0
  L2TPTos: 0
  TunnelID: 0
Packet:
  Payload:
    BaseLayer:
      Operation: 1
      HardwareType: 1
      HardwareLen: 6
      HardwareOpts: 0
      Xid: 1
      Secs: 0
      Flags: 32768
      ClientIP: 0.0.0.0
      YourClientIP: 0.0.0.0
      NextServerIP: 0.0.0.0
      RelayAgentIP: 0.0.0.0
      ClientHWAddr: aa:bb:00:00:00:01
      ServerName:
      File:
      Options: {
        Option(MessageType:Discover)
        Option(ClientID:[1 170 187 0 0 0 1]).
```

```
-----
Subscriber Id: aabb.0000.0001@automation-userplane
Timestamp: 2021/06/09 12:19:30.205174
Message: RadiusUdpProxyMsg
Description: Send Auth/Acct Request Message to UDP-Proxy
Source: bng.radius-ep.DC.Local.0
Destination: bng.udp-proxy.DC.Local.0
PAYLOAD:
  RadiusUdpProxyMsg:
    RadiusUdpProxyMsg:
      SrcIp: 10.105.254.113
      SrcPort: 16384
      DestIp: 10.105.254.114
      DestPort: 1812
      Payload:
```

```
-----
Subscriber Id: aall.0000.0003@asr9k-1
Timestamp: 2021/06/03 06:26:26.796023
Message: RadiusUdpProxyMsg
Description: Send Auth/Acct Request Message to UDP-Proxy
Source: BNG.radius-ep.DC.Local.0
Destination: BNG.udp-proxy.DC.Local.0
PAYLOAD:
  RadiusUdpProxyMsg:
    RadiusUdpProxyMsg:
      SrcIp: 10.1.4.150
      SrcPort: 16384
      DestIp: 10.1.4.151
```

```

DestPort: 1813
Payload:
  Code = AccountingRequest
  Id = 31
  Authenticator = [88 13 251 114 225 205 9 68 52 194 48 231 234 226
226 184]
  User-Name = "cnbng"
  NAS-IP-Address = 10.1.4.150
  NAS-Port = 16384
  Service-Type = 5
  Framed-IP-Address = 1.0.3.13
  Nas-Identifler = "CISCO-BNG-ACCT"
  Acct-Status-Type = 1
  Acct-Delay-Time = 0
  Acct-Session-Id = "Local_DC_16777230"
  Event-Timestamp = 1622701602
  NAS-Port-Type = 41
  Acct-Interim-Interval = 300
  NAS-Port-Id = "asr9k-1/2/3/4/100.200"
  NAS-IPv6-Address = ::/0
  Cisco-Vsa_cisco-nas-port = "asr9k-1/2/3/4/100.200"
  Cisco-Vsa_cisco-dhcp-client-id = 0x01aa1100000003
  Cisco-Vsa_Cisco AVpair = "client-mac-address=aa11.0000.0003"
  Cisco-Vsa_Cisco AVpair = "dhcp-class=RJIL_DHCPV4_CLASS_2"
  Cisco-Vsa_Cisco AVpair = "dhcp-class=RJIL_DHCPV6_CLASS_1"
  Cisco-Vsa_Cisco AVpair = "accounting-list=aaa-prof1"
  Cisco-Vsa_Cisco AVpair =
0x646863702d636c69656e742d69643d01aa1100000003
  Cisco-Vsa_Cisco AVpair = "vrf=ISP"
  PayloadLen: 396
  SubscriberID: aa11.0000.0003@asr9k-1

```

```

-----
Subscriber Id: aa11.0000.0003@asr9k-1
Timestamp: 2021/06/03 06:26:26.800776
Message: RadiusUdpProxyMsg
Description: Received Auth/Acct Response Message from UDP-Proxy
Source: BNG.udp-proxy.DC.Local.0
Destination: BNG.radius-ep.DC.Local.0
PAYLOAD:

```

```

  RadiusUdpProxyMsg:
    RadiusUdpProxyMsg:
      SrcIp: 10.1.4.151
      SrcPort: 1813
      DestIp: 10.1.4.150
      DestPort: 16384
      Payload:
        Code = AccountingResponse
        Id = 31
        Authenticator = [168 192 147 70 117 31 151 16 237 80 68 105 42 191
215 186]
      PayloadLen: 20

```

```

-----
bng#

```



**Note**

- While receiving CoA or DM packets, the RADIUS pod does not have the subscriber-information, instead the information is available only with the BNG-SM pod. Therefore, the packet related session programming N4-SESS-UPDATE TX and RX is dumped on the screen first followed by the CoA or DM TX and RX dump.
- Packet dumps are not captured for PFCP session report request and response.

## Viewing Log Files

Use the following commands to view the stored log files for a monitor protocol or subscriber.

```
monitor subscriber list
```

```
monitor protocol list
```

The following is a sample output for the **monitor subscriber list**.

**Example:**

```
bng# monitor subscriber list
none.aall.0000.0004*_TS_2021-06-03T06:28:13.564009704.txt.sorted
none.aall.0000.0003@asr9k-1_TS_2021-06-03T06:26:20.627655233.txt.sorted
none.*_TS_2021-06-03T06:25:04.176857711.txt.sorted
bng#
```

