CHAPTER 17

Source OIDs of Alarms Generated by Cisco ANA

These topics describe the possible source object identifiers (OIDs) of alarms generated by Cisco ANA. A description of each source OID and OID structure is given, with examples of OIDs and service alarms that use those OIDs as their source.

Note The source OID must be unique in the alarm type context. For example, it is not possible to generate multiple different alarms with the same type from the same component using the component OID as the source. An additional differentiator should be added to the base component OID. See the LSE OID (ILseOid), page 17-7, for an example.

The following source OIDs are described:

Managed Element OID (IManagedElementOid)

Managed Element represents the root component of the VNE. Any alarm related to the top-level component of the VNE will have the Managed Element OID as the source.

Alarms which have Managed Element OID as their source are:

- Device Unreachable
- Device Unsupported
- CPU Overutilized
- Module Unsupported (Investigation State)
- Adaptive Polling
- Cloud Problem (for cloud VNEs)

The structure of the Managed Element OID is:

{[ManagedElement(Key=*deviceName*)]}

Example

```
{[ManagedElement(Key=PE4-NY-7200)]}
```

Topological Link OID (ITopologicalLinkOid)

The Topological Link OID is the source OID for any Link Down alarm. It has the following structure:

{[TopologicalLink(AEndPoint=*AEndOid*)(TunnelID=*tunnelId*)(ZEndPoint=*ZEndOid*)]}

- AEndOid, ZEndOid—The OIDs of the link endpoint components.
- TunnelID—Where multiple links can exist between two components, the TunnelID value is used to distinguish between the links.

Supported Alarms with Topological Link OID Source

Currently the alarms supported in Cisco ANA which have Topological Link OID source are:

- Link Down—Link down between physical ports, the endpoint OIDs of the physical layer. In this case, the TunnelId is not used and is set to -1. See Link Down Endpoint OID Structure, page 17-3.

  Note There are various alarm subtypes of link down (for example, Link Down to Admin Down, and Link Down on Unreachable). They all have the same source OID.

- Link Utilization—The source OID is the same as for link down.
- Tx/Rx Utilization—The source OID is the same as for link down where the physical layer component is adjacent.
- GRE Tunnel Down—The endpoint OIDs are the GRE tunnel endpoints. In this case, the TunnelID is not used and is set to -1. See GRE Tunnel Endpoint OID Structure, page 17-3.

- Layer 2 Tunnel Down—The endpoint OIDs are the Layer 2 MPLS tunnel endpoints. In this case, the TunnelID is not used, nor is it initialized. See Layer2 MPLS Tunnel Endpoint OID Structure, page 17-4.
- BGP Link Down—The endpoint OIDs are the MpBGP. In this case, the TunnelID is not used, nor is it initialized. See BGP Link Down Endpoint OID Structure, page 17-4.

Link Down Endpoint OID Structure

The structure of the Link Down Endpoint OID is:

{[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Shelf(ShelfNum=*shelfNum*)][Slot(SlotNum=*slotNum*)][Module][Slot(SlotNum=*subSlotNum*)][Module][Port(PortNumber=*portNum*)][PhysicalLayer]}

Optional parts of the Link Down Endpoint OID are:

- Shelf
- Second-level slot
- Module representing a submodule

PortNum can also be the port name (see the following examples).

Examples

Source of link down where the physical ports are on a module:

```
{[TopologicalLink(AEndPoint={[ManagedElement(Key=PE3-NY-7300)][PhysicalRoot][Chassis][Slot
(SlotNum=1)][Module][Port(PortNumber=FastEthernet1/1)][PhysicalLayer]})(TunnelID=-1)(ZEndP
oint={[ManagedElement(Key=PE1-NY-GSR)][PhysicalRoot][Chassis][Slot(SlotNum=1)][Module][Slo
t(SlotNum=1)][Module][Port(PortNumber=GigabitEthernet1/1/2)][PhysicalLayer]})]}
```

Source of link down where the physical port of AendPoint is on submodule:

```
{[TopologicalLink(AEndPoint={[ManagedElement(Key=PE1-NY-GSR)][PhysicalRoot][Chassis][Slot(
SlotNum=1)][Module][Slot(SlotNum=1)][Module][Port(PortNumber=GigabitEthernet1/1/1)][Physic
alLayer]})(TunnelID=-1)(ZEndPoint={[ManagedElement(Key=NPE1-NY-7600)][PhysicalRoot][Chassi
s][Slot(SlotNum=4)][Module][Port(PortNumber=FastEthernet4/48)][PhysicalLayer]})]}
```

GRE Tunnel Endpoint OID Structure

The structure of the GRE Tunnel Endpoint OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][Context(ContextName=*contextName*)][TunnelContainer(TunnelType=*4*)][TunnelGre(TunnelName=*tunnelName*)]}

Examples

Source of GRE Tunnel Down alarm:

```
{[TopologicalLink(AEndPoint={[ManagedElement(Key=PE-East-IOU-158)][LogicalRoot][Context(Co
ntextName=Default
context)][TunnelContainer(TunnelType=4)][TunnelGre(TunnelName=Tunnel1)]})(TunnelID=-1)(ZEn
dPoint={[ManagedElement(Key=PE-South-IOU-158)][LogicalRoot][Context(ContextName=Default
context)][TunnelContainer(TunnelType=4)][TunnelGre(TunnelName=Tunnel1)]})]}
```

Layer 2 Tunnel Down—The endpoint OIDs are the Layer 2 MPLS tunnel endpoints. In this case, the TunnelID is not used and is not initialized.

Layer2 MPLS Tunnel Endpoint OID Structure

The structure of the s Layer 2 MPLS Tunnel Endpoint OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][Context(ContextName=*contextName*)][TunnelContainer(TunnelType=*1*)][PTPLayer2MplsTunnel(PeerRouterIp=*peerRouterIP*)(TunnelId=*tunnelId*)]}

Example

Source of Layer 2 Tunnel Down:

```
{[TopologicalLink(AEndPoint={[ManagedElement(Key=NPE1-NY-7600)][LogicalRoot][Context(Conte
xtName=Default
context)][TunnelContainer(TunnelType=1)][PTPLayer2MplsTunnel(PeerRouterIp=172.255.1.5)(Tun
nelId=100)]})(TunnelID=)(ZEndPoint={[ManagedElement(Key=PE4-NY-7200)][LogicalRoot][Context
(ContextName=Default
context)][TunnelContainer(TunnelType=1)][PTPLayer2MplsTunnel(PeerRouterIp=172.255.1.3)(Tun
nelId=100)]})]}
```

BGP Link Down Endpoint OID Structure

The structure of the MpBGP Link Down Endpoint OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=7)][TunnelId=*tunnelId*)]}

Example

Source of BGP link down:

```
{[TopologicalLink(AEndPoint={[ManagedElement(Key=PE-East-IOU-159)][LogicalRoot][FWComponen
tContainer(Type=7)][MpBgp]})(TunnelID=-1)(ZEndPoint={[ManagedElement(Key=RR2-IOU-159)][Log
icalRoot][FWComponentContainer(Type=7)][MpBgp]})]}
```

Physical Layer OID (IPhysicalLayerOid)

The Physical Layer OID is the source OID for any alarm related to the physical layer of a port.

Alarms which have Physical Layer OID as their source are:

- Port Down
- Tx/Rx Utilization (no adjacent)
- Tx/Rx Dormant
- Dropped/Discarded Packets
- All IP Interfaces Down

The structure of the Physical Layer OID is:

{[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Shelf(ShelfNum=*shelfNum*)][Slot(SlotNum=*slotNum*)][Module][Slot(SlotNum=*subSlotNum*)][Module][Port(PortNumber=*portNum*)][PhysicalLayer]}

Optional parts of the OID are:

- Shelf
- Second-level slot
- Module representing submodule

PortNum can also be the port name (seethe following examples).

Examples

Source of port down where the port is on a submodule:

```
{[ManagedElement(Key=CRS-1)][PhysicalRoot][Chassis][Shelf(ShelfNum=0)][Slot(SlotNum=4
-Back)][Module][Slot(SlotNum=4)][Module][Port(PortNumber=GigabitEthernet0/4/4/1)][Physical
Layer]}
```

Module OID (IModuleOid)

The Module OID is the source OID for any alarms related to a card/module.

Alarms which have Module OID as their source are:

- Card Out
- Card Down

Possible structures of the Module OIDs are:

- Module under chassis:

  {[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Shelf(ShelfNum=*shelfNum*)][Slot(SlotNum=*slotNum*)][Module]}

- Module under other module (submodule):

  {[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Shelf(ShelfNum=*shelfNum*)][Slot(SlotNum=*slotNum*)][Module][Slot(SlotNum=*subSlotNum*)][Module]}

Shelf is an optional part of the OID.

Example

```
{[ManagedElement(Key=CRS-1)][PhysicalRoot][Chassis][Shelf(ShelfNum=0)][Slot(SlotNum=4
-Back)][Module][Slot(SlotNum=10)][Module]}
```

Shelf OID (IShelfOid)

The Shelf OID is the source OID for any alarms related to shelf.

The alarm which has Shelf OID as its source is:

- Shelf Out

The structure of the Shelf OID is:

{[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Shelf(ShelfNum=*shelfNum*)]}

Example

```
{[ManagedElement(Key=CRS-1)][PhysicalRoot][Chassis][Shelf(ShelfNum=0)]}
```

IP Interface OID (IPInterfaceOid)

The IP Interface OID is the source OID for any alarms related to the IP interface.

Alarms supported by Cisco ANA with IP Interface source OID are:

- Interface Status
- HSRP Group Status Changed

The structure of the IP Interface OID can be one of the following:

- IP interface under the global routing (RoutingEntity):

  {[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=1)][RoutingEntity][IpInterface(IpInterfaceName=*ifName*)]}

- IP interface under a VRF:

  {[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=*3*)][Vrf(VrfName=*vrfName*)][IpInterface(IpInterfaceName=*ifName*)]}

Examples

IP Interface OID under the RoutingEntity:

```
{[ManagedElement(Key=PE2-TX-GSR)][LogicalRoot][FWComponentContainer(Type=1)][RoutingEntity][IpInterface(IpInterfaceName=POS0/0)]}
```

IP Interface OID under a VRF:

```
{[ManagedElement(Key=PE-South)][LogicalRoot][FWComponentContainer(Type=3)][Vrf(VrfName=vrfA)][IpInterface(IpInterfaceName=Serial2/0.400)]}
```

MpBgp OID (IMpBgpOid)

The MpBgp OID will be the source OID for any alarms related to BGP service.

The alarm supported by Cisco ANA with MpBgp source OID is:

- BGP Process Down

The structure of the MpBgp OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=7)][MpBgp]}

Example

```
{[ManagedElement(Key=Juniper M5)][LogicalRoot][FWComponentContainer(Type=7)][MpBgp]}
```

BGP Neighbor Entry OID (IBgpNeighborEntryOid)

The BGP Neighbor Entry OID is the source OID for any alarms related to BGP neighbors.

The alarm supported by Cisco ANA with BGP Neighbor Entry source OID is:

- BGP Neighbor Loss

The structure of the BGP Neighbor Entry OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=7)][MpBgp][BgpNeighbourEntry(PeerIdentifier=*peerIP*)(VrfName=*vrfName*)]}

The VrfName identifier in the BGP entry part exists if the entry is under VRF.

Example

```
{[ManagedElement(Key=PE3-NY-7300)][LogicalRoot][FWComponentContainer(Type=7)][MpBgp][BgpNe
ighbourEntry(PeerIdentifier=10.0.7.4)(VrfName=Red)]}
```

LSE OID (ILseOid)

The LSE (Label Switching Entity) OID is used as the source for various alarms related to MPLS.

Currently alarms supported by Cisco ANA with LSE OID are:

- MPLS Black Hole Found
- MPLS Interface Removed
- LDP Neighbor Loss

The structure of the LSE OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=4)][Lse]}

Alarm Differentiators

Multiple alarms of the same type cannot have the same source. When this occurs, then the LSE OID is used as a base OID and is augmented with a differentiator. A specific alarm differentiator is used for each type of alarm.

The following examples show how specific alarm differentiators are used in the different types of alarms:

Example 1

MPLS Black Hole Found—[ServiceEvent(DiffObject=*ifName nextHop*)]

Source OIDs of MPLS Black Hole Found:

```
{[ManagedElement(Key=RR1-IOU)][LogicalRoot][FWComponentContainer(Type=4)][Lse][ServiceEven
t(DiffObject=Ethernet0/0 192.168.1.210)]}
```

```
{[ManagedElement(Key=RR1-IOU)][LogicalRoot][FWComponentContainer(Type=4)][Lse][ServiceEven
t(DiffObject=Ethernet0/0 192.168.1.310)]}
```

Example 2

MPLS Interface Removed—[ServiceEvent(DiffObject=*mplsIfDescr*)]

Source OIDs of MPLS Interface Removed:

```
{[ManagedElement(Key=PE4-NY-7200)][LogicalRoot][FWComponentContainer(Type=4)][Lse][Service
Event(DiffObject=MPLS on interface FastEthernet0/1)]}
```

```
{[ManagedElement(Key=PE4-NY-7200)][LogicalRoot][FWComponentContainer(Type=4)][Lse][Service
Event(DiffObject=MPLS on interface FastEthernet0/2)]}
```

Example 3

LDP Neighbor Loss—[ServiceEvent(DiffObject=*peerLdpId*)]

Source OIDs of LDP Neighbor Loss:

```
{[ManagedElement(Key=CORE2-NY-GSR)][LogicalRoot][FWComponentContainer(Type=4)][Lse][Servic
eEvent(DiffObject=172.255.0.1:0)]}

{[ManagedElement(Key=CORE2-NY-GSR)][LogicalRoot][FWComponentContainer(Type=4)][Lse][Servic
eEvent(DiffObject=172.255.0.1:5)]}
```

LSE Entry OID (IMplsEntryOid)

The LSE Entry OID is used as the source OID for any alarms related to LSE entries.

The alarm supported by Cisco ANA with the LSE Entry source OID is:

- Broken LSP Discovered

The structure of the LSE Entry OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=4)][Lse][LSEEntries(InLabel=*inLabel*)][MplsEntry(OutInterface=*outIfOid*)]}

The OutInterface is the IP interface OID of the outgoing interface.

Example

```
{[ManagedElement(Key=PE1-NY-GSR)][LogicalRoot][FWComponentContainer(Type=4)][Lse][LSEEntri
es(InLabel=74)][MplsEntry(OutInterface={[ManagedElement(Key=PE1-NY-GSR)][LogicalRoot][FWCo
mponentContainer(Type=1)][RoutingEntity][IpInterface(IpInterfaceName=POS0/0)]})]}
```

Note The structure of the OutInterface is a separate OID.

MPLS TE Tunnel OID (IMplsTETunnelOid)

The MPLS TE Tunnel OID is the source OID for any alarms related to MPLS TE tunnels.

The alarm supported by Cisco ANA with MPLS TE Tunnel source OID is:

- MPLS TE Tunnel Down

The structure of the MPLS TE Tunnel OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=1)][RoutingEntity][IpInterface(IpInterfaceName=*ifName*)][MplsTETunnel]}

Example

```
{[ManagedElement(Key=CRS1-PE)][LogicalRoot][FWComponentContainer(Type=1)][RoutingEntity][I
pInterface(IpInterfaceName=tunnel-te0)][MplsTETunnel]}
```

Note The structure of the OID will be different when the IP interface is under a VRF (See IP Interface OID (IPInterfaceOid), page 17-6).

Logical Port OID (ILogicalPortOid)

A logical port represents a logical ATM/FrameRelay interface which is configured on top of a physical port. One physical port might have multiple logical ports. In ATM, logical ports are differentiated by VP muxing, that is, each logical port is configured with a range of VPIs. This type of configuration exists in Lucent GX/CBX, which are supported by Cisco ANA.

The Logical Port OID is the source OID for any alarms related to logical ports.

The alarm supported by Cisco ANA with the Logical Port source OID is:

- Logical Port Down

The structure of the Logical Port OID can be one of the following:

- Logical port on a module's physical port:

  {[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Slot(SlotNum=*slotNum*)][Module][Port(PortNumber=*portNum*)][PhysicalLayer][VpMux][LogicalPort(LogicalPortNumber=*logicalPortNum*)]}

- Logical port on a submodule's physical port:

  {[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Slot(SlotNum=*slotNum*)][Module][Slot(SlotNum=*subSlotNum*)][Module][Port(PortNumber=*portNum*)][PhysicalLayer][VpMux][LogicalPort(LogicalPortNumber=*logicalPortNum*)]}

- Logical port of a subport:

  {[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Slot(SlotNum=*slotNum*)][Module][Port(PortNumber=*portNum*)][PhysicalLayer][SubPort(SubPortNumber=*subPortNumber*)][VpMux][LogicalPort(LogicalPortNumber=*logicalPortNum*)]}

L2TP Peer OID (IL2tpPeerOid)

L2TP modeling in Cisco ANA is currently available only for Redback SMS devices. L2TP Peer is a component that is used to model administrative aspect of L2TP tunnels. It is basically an entity responsible for creating L2TP tunnels based on its configuration.

The L2TP Peer OID is the source OID for any alarms related to L2TP Peer components.

Alarms supported by Cisco ANA with L2TP Peer source OID are:

- L2TP Peer Not Established
- L2TP Session Threshold

The structure of the L2TP Peer OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][Context(ContextName=*contextName*)][FWComponentContainer(Type=6)][L2tpPeer(PeerName=*peerName*)]}

Example

```
{[ManagedElement(Key=redback)][LogicalRoot][Context(ContextName=l2tpCtx)][FWComponentContainer(Type=6)][L2TPPeer(PeerName=peer5)]}
```