



CHAPTER 2

Observations

This chapter provides details of all observations reported by the Cisco MPLS Diagnostics Expert (MDE) 2.1.3 application for the Cisco IP Solution Center (ISC) Release 5.1.

For more information, e-mail: mpls-diagnostics-expert@cisco.com

2.1 Observations

Observations are conditions that could lead to connectivity problems. Since MDE cannot categorically conclude the cause of the connectivity problem, these conditions are reported as observations.

ACL Configured on PE

There is an access control list (ACL) configured on the provider edge (PE) router. It might be causing failure of the VPN routing/forwarding instance (VRF) ping from this PE to the remote PE, however we have not analyzed the ACL to confirm its usage. This is not causing the connectivity failure from the PE to the local customer edge (CE) router, or customer device.

BGP Neighbor Session Problem

Possible border gateway protocol (BGP) neighbor session problem detected. Displays table with columns BGP Neighbor (Neighbor IP Address) and BGP State (BGP Neighbor State).

BGP Router ID is Not a Loopback Interface

The local BGP router ID on the PE is not assigned to a loopback interface. It is recommended that the router ID is taken from a loopback interface to both reduce the chance of duplication and enhance stability.

Connected Routes Not Redistributed into MP-BGP

Directly connected routes might not be redistributed into MP-BGP.

Core Troubleshooting Could Not be Performed. The VPN Route is External.

Core troubleshooting could not be performed. MDE is unable to determine the label-switched path (LSP) to test, because the PE <PE Name> has no valid VPN route to the remote prefix <IP address> within the VRF <VRF name>. The route is not learned through an internal Border Gateway Protocol (BGP) vpv4 neighbor. It is known through the <Routing Protocol Name>. The next-hop for this external route is <IP address>. Traffic does not flow through the MPLS core, as expected. This might be an intentional back door link, however, it is often a symptom of PE - CE misrouting. To test LSP connectivity, you might want to run a PE to PE Core test that allows you to specify the LSP endpoints manually.

Core Troubleshooting Could Not be Performed. The VPN Route is External and the Next-Hop Is Inaccessible.

Core troubleshooting could not be performed. MDE is unable to determine the LSP to test, because the PE <PE Name> has no valid virtual private network (VPN) route to the remote prefix <IP address> within the VRF <IP address>. The route is not learned through an internal BGP vpnv4 neighbor. It is known through the <Routing Protocol Name>. The next-hop for this external route is inaccessible. This might be an intentional back door link, however, it is often a symptom of PE - CE misrouting. To test LSP connectivity, you might want to run a PE to PE Core test that allows you to specify the LSP endpoints manually.

Core Troubleshooting Could Note be Performed. The VPN Route Next-Hop is Inaccessible.

Core troubleshooting could not be performed. MDE is unable to determine the LSP to test, because the PE <PE Name> has no valid VPN route to the remote prefix <IP address> within the VRF <VRF name>. The next-hop is inaccessible. This might be due to a problem within the Core Interior Gateway Protocol (IGP) or IP connectivity failure. To test LSP connectivity, you might want to run a PE to PE Core test that allows you to specify the LSP endpoints manually.

Duplicate BGP Router ID

BGP Router Identifier on the PE is found to be duplicated on one or more interfaces of the listed devices.

eBGP Maximum Prefixes

The exterior border gateway protocol (eBGP) session between the PE and an eBGP neighbor has a maximum prefix count configured on the PE. There are currently X prefixes in the VRF from this neighbor.

eBGP Neighbor Not Established

It appears that you are running eBGP as your PE-CE routing protocol. The PE and CE interfaces are on different subnets and there is no route to the CE on the PE. Until there is a route to the CE, this eBGP session is not established.

eBGP Neighbors Not Established

eBGP neighbors have been specified in a VRF but are not established and are unreachable.

EIGRP Peer Relationship Not Established

The PE interface is configured with IP unnumbered. The CE interface must either also be using IP unnumbered or be on the same subnet in order for the enhanced interior gateway routing protocol (EIGRP) to establish a peer relationship.

Full-Mesh VPN Topology

These routers appear to be connected via a fully meshed VPN configuration. If this is not correct, there is an issue with the route target configuration.

Hub and Spoke VPN Topology

These routers appear to be connected via a hub and spoke VPN configuration. If this is not correct, there is an issue with the route target configuration.

Hub To Hub, Hub and Spoke VPN Topology

These routers appear to be connected via a hub to hub, hub and spoke VPN configuration. If this is not correct, there is an issue with the route target configuration.

Incomplete CEF Adjacencies

Incomplete Cisco express forwarding (CEF) adjacencies on the access circuit interface.

Incorrect Multilink Virtual-Access Interface Specified

If you are specifying a multilink access circuit interface for the PE ensure that the virtual access interface specified is an active multilink bundle interface and that it has active bundle links.

Interface Not In VLAN

Warning: Ethernet access circuit interface is not associated with a virtual LAN (VLAN).

Intermittent Ping Success

The ping showed only intermittent connectivity.

Inverse ARP Disabled on FR Interface

The Frame Relay interface is dynamically configured but has inverse address resolution protocol (ARP) explicitly disabled.

Inverse ARP Implicitly Disabled on FR Interface

There is a Frame Relay static map on the interface. This interface is configured dynamically but the presence of the static map will, as a side effect, disable inverse ARP.

LMI Disabled on Frame Relay Interface

Warning: Frame Relay permanent virtual circuit (PVC) status cannot be checked on interface because the local management interface (LMI) is disabled.

LSP Endpoint is Not a Loopback Interface

The VPNv4 route is being sent to IBGP neighbor(s). However, the next hop address is one of the directly connected physical interfaces. It is recommended to use loopback interfaces as the next hops for VPNv4 IBGP neighbors. If the address is not available at the correct hop via the IGP, it could break connectivity between VPN sites because no forwarding label information is available.

MPLS OAM Package is not enabled on IOS XR Router

MPLS OAM package is not enabled on the IOS XR router.

MPLS TE Package is not Enabled on IOS XR Router

MPLS TE package is not enabled on the IOS XR router.

Multiple Equal Cost Paths

Equal cost multiple paths (ECMP) were found.

Non-compliant IOS Version on PE Router

Core troubleshooting could not be performed because the provider edge (PE) router is running a non MPLS OAM compliant Cisco IOS version.

No Routes Received from eBGP

It appears that you are running eBGP as your PE-CE routing protocol. However, no routes have been received from the neighbor.

No Route to Remote Prefix Received from eBGP

It appears that you are running eBGP as your PE-CE routing protocol. However, the route to a remote prefix has not been received from the neighbor. Check PE and customer edge (CE) BGP configuration.

No VPN Label in VRF for Prefix

No virtual private network (VPN) label was found for the address in the VPN routing/forwarding (VRF) on the device.

OSPF Peer Relationship Not Established

The PE interface is configured with IP unnumbered. The CE interface must either also be using IP unnumbered or be on the same subnet in order for open shortest path first (OSPF) to establish a peer relationship.

PE-PE Core Only Test Performed and the Optional Loopback IP Address Parameters Have Not Been Supplied

The LSP under test was selected based on the BGP router-id of the remote site PE. If the network has multiple LSPs between the two PEs, the reported result might not accurately reflect the state of the LSP used for customer traffic. To ensure the correct LSP is tested, you can supply the LSP endpoints on the test input window.

Possible Backup Link

The ping from the PE to the destination prefix succeeded, however the route from the PE to the destination prefix has not been learned via the expected PE interface. There might be a backup link in operation, or you might have input the incorrect parameters.

Possible Blocking Route Map

A route map is configured on the PE which might be causing route traffic to be lost. If this is an intranet/extranet VPN configuration, then there might be a route map configuration error.

Possible Core IP Failure

The internet control message protocol (ICMP) ping issued from the local PE to the remote PE failed. There is no route to the remote PE in the Interior Gateway Protocol (IGP) route table of the local PE. Try troubleshooting IP connectivity between these devices.

Possible Ethernet Duplex Mismatch

Warning: Access circuit interface has late collisions. This might be caused by an Ethernet duplex mismatch.

Route Limit Reached

The route count on the device has reached the route limit.

Traceroute Not Transmitted

The MPLS traceroute was not transmitted.

Unrecognized VPN Topology

These routers do not appear to be connected via any VPN configuration. If running a hub and spoke VPN architecture, ensure the test is being run from hub to spoke, not from spoke to spoke.

Unrecognized VPN Topology

These routers do not appear to be connected via any VPN configuration. No reciprocal link can be found.