

Troubleshooting VPLS

SmartEdge OS Software

FAULT TRACING DIRECT.

Copyright

© Ericsson AB 2010–2011. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

SmartEdge is a registered trademark of Telefonaktiebolaget LM Ericsson.



Contents

| | | |
|----------|--|-----------|
| 1 | Overview | 1 |
| 2 | Step 1: Verify IP Connectivity | 2 |
| 2.1 | Verify IP Connectivity from Local CE to Remote CE | 2 |
| 2.2 | Verify That the Interfaces Are Up | 3 |
| 2.3 | Verify That Routes Were Learned Correctly | 3 |
| 2.4 | Verify That Neighbors Are Known to Each Other | 3 |
| 2.5 | Verify That Ports Are Bound to the Correct Interfaces | 4 |
| 3 | Step 2: Check the MPLS Layer | 4 |
| 3.1 | Verify MPLS PW Traffic Is Flowing | 4 |
| 3.2 | Verify That the MPLS Layer Is Functioning | 5 |
| 4 | Step 3: Verify VPLS Configuration | 5 |
| 4.1 | Verify Targeted LDP Between PE Peers | 6 |
| 4.2 | Verify the VPLS Profile | 6 |
| 4.3 | Verify the VPLS-Enabled Bridges | 6 |
| 5 | Step 4: Verify VPLS Signaling | 7 |
| 5.1 | Check the VPLS Neighbors | 8 |
| 5.2 | Verify PW Connectivity | 8 |
| 5.3 | Check LDP Hello Messages | 9 |
| 5.4 | Verify That the PE Routers Have Exchanged Inner Labels | 9 |
| 5.5 | Verify That Packets Are Flowing | 10 |
| 5.6 | Verify PW Characteristics | 10 |
| 5.7 | Verify Connectivity from the Local to Remote CE Routers | 11 |
| 5.8 | Verify That the MAC Address of the Remote CE Was Learned Through the PW | 11 |
| 5.9 | Verify That the MAC Addresses Were Learned by the Bridge | 11 |
| 6 | Alternative Procedure: Following a Ping Packet from a Local to a Remote CE Router | 12 |
| 6.1 | Ping the Source CE Router | 12 |
| 6.2 | Is the Source CE Directly Connected? | 13 |



| | | |
|----------|--|-----------|
| 6.3 | Is the Route to the Remote CE in the Local CE Router ARP Cache? | 13 |
| 6.4 | Does the Bridge on the Local PE Router Know the Destination MAC Address? | 13 |
| 6.5 | What Is the MPLS Inner Label? | 14 |
| 6.6 | What Is the MPLS Outer Label? | 14 |
| 6.7 | Check the P Router Label Mapping | 15 |
| 6.8 | To Which Bridge Is the VPLS Instance Bound? | 15 |
| 6.9 | Verify that the Packet Is Forwarded Correctly | 15 |
| 6.10 | Does the Destination CE Know the Local CE's MAC Address | 16 |
| 7 | Step 6: Collecting VPLS Debug Information for Customer Support | 16 |

1 Overview

Specific information in this troubleshooting guide assumes a typical Virtual Private LAN Services (VPLS) deployment using SmartEdge® routers, illustrated in Figure 1.

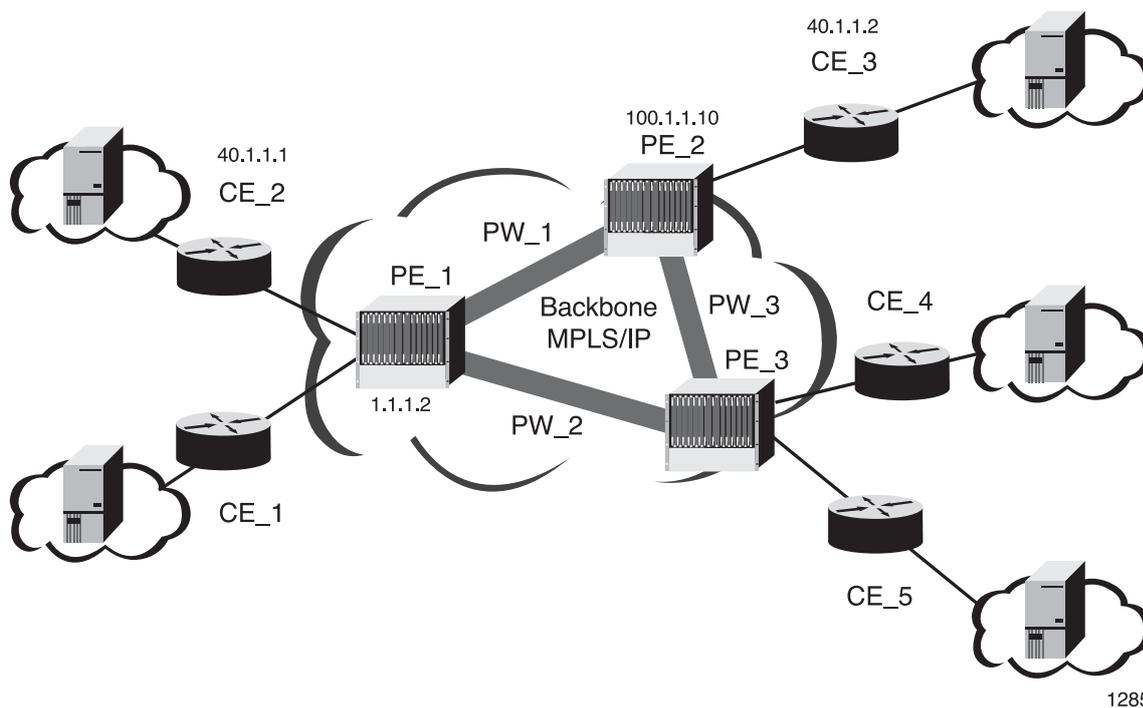


Figure 1 Typical VPLS Deployment

Customer edge (CE) routers, which are on the edge of geographically separate customer networks, are connected by Ethernet to provider edge (PE) routers on an MPLS provider network. A pseudowire (PW) is established for each pair of CE routers to be connected to a virtual private LAN. In the illustration, the PW_1 PW is used to connect the CE_2 and CE_3 routers. The CE_4, and CE_5 routers connect with the CE_1 router over the VPLS network, but not necessarily to each other.

Note: The examples in this document illustrate the procedure to troubleshoot a problem with the connections between the CE routers connected to PE_1 and PE_2 .

Note: The examples assume that the Interior Gateway Protocol (IGP) used to distribute routes is Open Shortest Path First (OSPF) and the label distribution protocol is LDP.



2 Step 1: Verify IP Connectivity

When end-user packets do not reach their destination, you can verify the connectivity of the bridge associated with the target by checking whether traffic is flowing. If traffic is not flowing, verify that the interfaces are up, that routes were learned through IGP, and that the neighbors are up. Use the steps in Table 1 to check and troubleshoot connectivity.

Table 1 Verify IP Connectivity

| Task | Root Command | Notes | Checked? |
|---|---|-------|----------|
| Verify IP Connectivity from Local CE to Remote CE | <code>ping target-ip-addr source ip-addr</code> <code>tracert</code> | | |
| Verify That the Interfaces Are Up | <code>show ip interface brief</code> | | |
| Verify Routes Were Learned Correctly | <code>show ip route</code> | | |
| Verify Neighbors Are Known to Each Other | <code>show ospf neighbor</code> | | |
| Verify Ports Are Bound to the Correct Interfaces | <code>show bindings</code> | | |

2.1 Verify IP Connectivity from Local CE to Remote CE

On the local CE router, enter the `ping target-ip-addr source ip-addr` command, targeting the remote CE:

```
[CE]PE_1#ping 40.1.1.2 source 40.1.1.1
PING 40.1.1.2 (40.1.1.2): source 40.1.1.1, 36 data bytes,
timeout is 1 second !!!!!

----40.1.1.2 PING Statistics----
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.882/2.119/2.740/0.359 ms
```

You can also use the `tracert` command (targeting the loopback address for the egress PE router) to identify the problem or the path:

```
[local]PE_1#tracert 100.1.1.10
se_tracert to 100.1.1.10 (100.1.1.10), 30 hops max, 40 byte packets
 1  1.1.1.2 (1.1.1.2)    4.439 ms  3.763 ms  2.838 ms ----> PE_1 router
 2  10.1.2.2 (10.1.2.2)  2.320 ms  2.802 ms  2.256 ms ----> PE_2 router
 3  100.1.1.10 (100.1.1.10)  4.034 ms  2.921 ms  2.885 ms --> Egress PE
```



If the **ping** and **tracert** commands were not successful, then continue with the following steps.

2.2 Verify That the Interfaces Are Up

If the ping does not return a response, or the **tracert** command does not work, verify that the interfaces are up on this router and its neighboring routers with the **show ip interface brief** command:

```
[local]PE_1#show ip interface brief
Mon Feb  8 16:41:05 2010
Name                Address                MTU   State   Bindings
PE-loop             100.1.1.1/32          1500  Up      (Loopback)
.
.
backbone1           1.1.1.1/30            1500  Up      ethernet 2/1
mgmt                 10.21.1.131/24        1500  Up      ethernet 1/12
```

The example displays the relevant interfaces and indicates that they are up.

2.3 Verify That Routes Were Learned Correctly

To verify that the routes for all the routers was learned correctly, use the **show ip route** command, which displays output similar to the following:

```
[local]PE_1#show ip route
Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGp,
I B - IBGP, O - OSPF, O3 - OSPFv3, IA - OSPF(v3) inter-area,
N1 - OSPF(v3) NSSA external type 1, N2 - OSPF(v3) NSSA external type 2
E1 - OSPF(v3) external type 1, E2 - OSPF(v3) external type 2
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, N - NAT
IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
MIP F - Mobile-IP Foreign Agent, MIP H - Mobile-IP Home Agent
A - Derived Default, MH - Media Nexthop
> - Active Route, * - LSP

Type    Network                Next Hop            Dist  Metric  UpTime  Interface
> C     1.1.1.0/30              0                   0      0      6d23h  backbone1
> O     10.1.2.0/30             1.1.1.2             110    2      00:45:11 backbone1
> O     10.1.2.4/30             1.1.1.2             110    3      00:45:11 backbone1
> C     10.21.1.0/24            0                   0      0      15w6d  mgmt
> C     100.1.1.1/32            0                   0      0      3d21h  PE-loop
> O     100.1.1.2/32            1.1.1.2             110    2      00:45:11 backbone1
> O     100.1.1.3/32            1.1.1.2             110    3      00:45:11 backbone1
> O     100.1.1.10/32           1.1.1.2             110    4      00:45:11 backbone1
> S     155.53.0.0/16           10.21.1.254         1      0      15w6d  mgmt
> S     172.31.0.0/16           10.21.1.254         1      0      15w6d  mgmt
> C     192.168.210.48/30      0                   0      0      1w4d   ge-2/2
```

2.4 Verify That Neighbors Are Known to Each Other

If the expected routes are not in the **show ip route** output, enter the **show ospf neighbor** command, which displays output similar to the following. Verify that neighbors are known to each other:

```
[local]PE_1#show ospf neighbor
--- OSPF Neighbors for Instance 1/Router ID 100.1.1.1 ---
NeighborID  NeighborAddress  Pri  State  DR-State  IntfAddress  TimeLeft
100.1.1.2   1.1.1.2          1    Full   BDR       1.1.1.1      30
```



2.5 Verify That Ports Are Bound to the Correct Interfaces

Before continuing, verify that the ports are bound to the correct interfaces in the context. Use the `show bindings` command to verify the bindings.

3 Step 2: Check the MPLS Layer

Check that the Multiprotocol Label Switching (MPLS) layer is functioning, using the tasks in Table 2. For more tasks to troubleshoot MPLS, see *Troubleshooting MPLS*.

Table 2 Verify that the MPLS Layer is Functioning

| Task | Root Command | Notes | Checked? |
|---|--|---|----------|
| Verify MPLS PW Traffic Is Flowing | <code>ping mpls pw pw-id</code> | Enter the commands on the ingress PE router. | |
| Verify That the MPLS Layer Is Functioning | <code>ping mpls ldp ip-addr/netmask number of pings</code> | You can use the <code>show mpls lsp</code> command to identify the Top Label. | |

3.1 Verify MPLS PW Traffic Is Flowing

On the ingress PE router, enter the `ping mpls pw pw-id` command, identifying the egress PE router:

```
[local]PE 1#ping mpls pw pw-id 100 peer 100.1.1.10
PING 100.1.1.10 (100.1.1.10): source 100.1.1.1, 36 data bytes,
timeout is 1 second
!!!!
```

You can look up the PW ID (also called VC ID) in the output for the `show xc l2vpn` or `show vpls peer` commands (see Section 5.2 on page 8) or the `show ldp l2vpn fec` command (see Section 5.4 on page 9).

If there is packet loss in the output of the `ping` command and the PW failure is on a SmartEdge router in the middle of a PW, the SmartEdge router responds to the ping indicating that it is not the egress point for the PW.



Note: If a router at the remote end of the ping is running a version of the SmartEdge OS earlier than Release 6.1.3, you must include the `send-mode` and `control-plane` keywords in the `ping mpls pw pw-id` command on the local router to ensure that the ping is sent over the control plane. In releases prior to 6.1.3, the router could send pings only over the control plane.

3.2 Verify That the MPLS Layer Is Functioning

If you can't ping the PW, to verify that the MPLS layer is functioning, enter the `ping mpls ldp egress-loopback-address/length num-pings` command. From the ingress PE router, ping the egress PE router with this command.

The (outer) top label in the output is `0x800006`. In decimal numbers, the label value translates to `524294` (which is the label corresponding to `100.1.1.10`).

To verify this, enter the `show mpls lsp` command as in the following example, which reports the Out Label in decimal numbers).

```
[local]PE_1#show mpls lsp
Codes : S - MPLS-Static, R - RSVP, L - LDP, B - BGP
Type Endpoint          Direct Next-hop  Out Label      Adjacency Id
L   10.1.2.8/30         1.1.1.2         3              0x1300011
L   100.1.1.2/32        1.1.1.2         3              0x1300013
L   100.1.1.10/32       1.1.1.2         524294         0x1300015
```

The output of these two commands indicates that MPLS is functioning.

For more procedures to troubleshoot MPLS see *Troubleshooting MPLS*

4 Step 3: Verify VPLS Configuration

If MPLS is functioning but traffic is not flowing, verify that the VPLS configuration is correct using the steps in Table 3.

Table 3 Verify VPLS Configuration

| Task | Root Command | Notes | Checked? |
|-----------------------------------|--|-------|----------|
| Verify Targeted LDP Between Peers | <code>show configuration ldp</code> | | |
| Verify the VPLS Profile | <code>show vpls profile</code> | | |
| Verify the VPLS-Enabled Bridges | <code>show configuration bridge</code> | | |



4.1 Verify Targeted LDP Between PE Peers

Is targeted LDP configured between PE peers? To verify LDP configuration, examine the output from the `show configuration ldp` command:

```
[local]PE_1>show configuration ldp
Building configuration...
```

Current configuration:

```
context local

!
router ldp
  neighbor 100.1.1.10 targeted
  interface PE-loop
  interface backbone1
!
! ** End Context **
!

end
```

In this case, you can see the `neighbor ip-addr targeted` command is part of the router LDP configuration.

4.2 Verify the VPLS Profile

Does the VPLS profile contain the correct IP addresses for remote neighbors? To verify the VPLS profile, enter the `show vpls profile` command as in the following example:

```
[local]PE_1>show vpls profile
VPLS Profile      PE ID      Bridge Profile  Type  Peers(Up)
PE_1              100.1.1.2  Hub             Hub   1 (1)
PE_2              100.1.1.10 Hub            1 (1)
```

The output shows the remote neighbor's IP address configured through targeted LDP.

4.3 Verify the VPLS-Enabled Bridges

Is there a VPLS-enabled bridge for each customer, an interface for each circuit type, and a bridge profile applied to each circuit? To verify VPLS-enabled bridges, interfaces, and bridge profiles, examine the output of the `show configuration bridge` command:



```
[local]PE_1#show configuration bridge
Building configuration...

! Bridge global configuration
bridge br1
 vpls
  profile PE-1 pw-id 10
  trunk

! VPLS global configuration
vpls profile PE_1 pw-id 10
 neighbor 100.1.1.10
 pw-encap ether
```

A bridge facing subscribers is a tributary type bridge and one facing a VPLS neighbor is a trunk type bridge, configured in the bridge profile. For VPLS, it should be trunk type.

5 Step 4: Verify VPLS Signaling

To verify VPLS signaling, perform the steps in Table 4:

Table 4 Verify VPLS Signaling

| Task | Root Command | Notes | Checked? |
|--|--------------------------------------|--|----------|
| Check the VPLS Neighbors | <code>show ldp neighbor</code> | | |
| Verify PW Connectivity | <code>show vpls peer</code> | Also use <code>show xc l2vpn</code> | |
| Check LDP HELLO Messages | <code>debug ldp message hello</code> | You can add the <code>detail</code> keyword for more detailed output or the <code>vc-id vpn-id</code> construct to focus on HELLO messages for a single circuit. | |
| Verify That the PE Routers Have Exchanged Inner Labels | <code>show ldp l2vpn fec</code> | | |
| Verify That Packets Are Flowing | <code>ping mpls pw pw-id</code> | | |



Table 4 Verify VPLS Signaling

| Task | Root Command | Notes | Checked? |
|--|-----------------------------|---|----------|
| Verify Local and Remote PW Type Are the Same | <code>show vpls peer</code> | View more characteristics of the PW. You can also use the <code>show xc l2vpn detail</code> command. | |
| Verify Connectivity from Local CE to Remote CE Routers | <code>ping ip-addr</code> | | |

5.1 Check the VPLS Neighbors

To verify that VPLS signaling is operational, enter the `show ldp neighbor` command on the ingress PE router, as in the following example:

```
[local]PE_1#show ldp neighbor
PeerFlags: A - LocalActiveOpen, D - Deleted, R - Reseting, E - OpenExtraDelay
           N - OpenNoDelay, P - SetMD5Passwd, T - RetainRoute, F - FlushState
           X - ExplicitNullEnabled, C - ExplicitNullStatusChanging
           G - Graceful Restart Supported, L - Session Life Extended
           V - Reachable Via RSVP-TE LSP
SHld - Session Holdtime Left, HHld - Hello Holdtime Left

NeighborAddr  LDP Identifier      State  Flag SHld HHld Interface
100.1.1.2     100.1.1.2:0        Oper   G   89  13  backbone1
100.1.1.10   100.1.1.10:0       Oper   G   62  39  none - remote
```

In this output, you see the egress PE router, 100.1.1.10, and the ingress PE router, 100.1.1.2. If the neighbor's state is `none`, or if no entry exists for the neighbor, there may be a problem with targeted LDP signaling.

5.2 Verify PW Connectivity

In Section 5.1 on page 8, the example output shows that neighbors are known. If the labels have not been exchanged correctly, you would then verify PW connectivity with the `show vpls peer`.

```
[local]PE_1#show vpls peer
VPLS Bridge      Peer ID      Pseudo-wire ID  Circuit ID  Type  State
br1              100.1.1.10  10              VPLS 4      Hub   Up
```

This output shows that the PW is up. You can also verify the PW state using the `show xc l2vpn` command as in the following example:

```
[local]PE_1#show xc l2vpn
LDP L2VPN Circuits
L2 Circuit      L2 State Peer address  VC Id  L-Label  State
VPLS 0x4000004  Up       100.1.1.10   10     131072  Up
```



5.3 Check LDP Hello Messages

If you do not see the egress PE router in the output for the `show ldp neighbor` command, check the LDP HELLO messages with the `debug ldp message hello` command. The debug output should provide clues to further investigate the problem..

```
[local]FWN-SR_1#Mar 15 16:36:31: %LDP-7-HELLO: rcv HELLO on intf backbone1
from 1.1.1.2, LDP Id
100.1.1.2:0, trans addr 100.1.1.2,
local addr 0.0.0.0 paklen 42, holdtime 15 870986736
Mar 15 16:36:32: %LDP-7-HELLO: send HELLO on interface backbone1
cct 2/1:1023:63/1/1/22, paklen 42
Mar 15 16:36:36: %LDP-7-HELLO: rcv HELLO on intf backbone1 from 1.1.1.2,
LDP Id
100.1.1.2:0, trans addr 100.1.1.2, local addr 0.0.0.0 paklen 42,
holdtime 15 870986736
Mar 15 16:36:36: %LDP-7-HELLO: rcv targeted hello: sender 172.16.10.6
with transport addr 172.16.10.6 and LDP Id
172.16.10.6:0 is not configured as a remote neighbor. Ignored.
```

This debug output displays several problems:

- HELLO messages from a different LDP ID than expected on interface backbone1. Go to that router and investigate the problem.
- The egress PE router is not configured as a remote neighbor. Check the configuration on the remote router. Even though this loopback address was not part of the MPLS or LDP interfaces from the sending router, the system still sent it.

To investigate further, you can collect information with the `debug ldp all` command.

5.4 Verify That the PE Routers Have Exchanged Inner Labels

To check the control plane for VPLS signaling, verify that the PE routers have exchanged inner labels.

```
[local]PE_1#show ldp l2vpn fec
Codes : GID - Group ID, F - Frame Relay, V - VLAN, E - Ether, A - ATM
        L - Local, R - Remote

VC ID  VC  Type  Peer          L-Label  R-Label  L-GID  R-GID  State
10     E           100.1.1.10  131072   131072   0      0      LR
```

This example displays information about the configured PW 10, including the inner local label and the inner remote label (the label received from the remote PE router).



5.5 Verify That Packets Are Flowing

If you know that the PW is up, use the `ping mpls pw pw-id` command to verify that packets are flowing through the PW, as in the following example:

```
[local]PE_1#ping mpls pw pw-id 10 peer 100.1.1.10
Sending 5 100-byte MPLS echos to 100.1.1.10 for LDP PWID 10,
source 100.1.1.1,
    timeout is 1 second, send interval is 0 msec: !!!!!
---- MPLS PING Statistics----
5 packets transmitted, 5 packets received no error, 0.0%
packet loss/error
round-trip min/avg/max/stddev = 2.793/7.707/23.469/8.848 ms
```

5.6 Verify PW Characteristics

If the PW is down, check to see if the local and remote PW type are the same and the other PW characteristics are correct using the `show vpls peer` command:

```
[local]PE_1#show vpls peer detail
VPLS peer_(bridge/ip:pwid): br1/1001.1.1:10
Oper State      : Up          Context name      : local
Admin State     : Enable     Circuit id        : VPLS 4
Peer Flags      :
Bridge id       : 0x1        Context id        : 0x40080001
PE peering type : Hub        PE local mode    : PE-rs
Prev state      : Init       Profile name      : PE-1
Prev event      : init       Last error       : no error
Peer up/down cnt : 0        Peer state changes : 1
Peer reset cnt  : 0        Peer config changes : 0
Peer restart cnt : 0        Peer proc restarts : 0
MAC flush sent  : 0        MAC flush received : 0
Circ up/down cnt : 0        Circ cfg changes   : 0
Circ error cnt  : 0        Circ delete cnt    : 0
PW state        : Up, Active
PW up/down cnt  : 0        PW signaling type  : LDP
PW error cnt    : 0        PW restart cnt     : 0
PW In label     : 131072   PW encap type     : Ethernet
PW Out label    : 131072   PW Exp bits       : 0x0
PW local MTU    : 1500    PW remote MTU     : 1500
LSP Configured :
LSP Used       :
PW flags : in-rib, in-lblmap, up, in-ldp, from-ldp, from-cfg peer-up
```

In this output, you can see that the PW state is up.

You can also view PW characteristics in the output for the `show xc l2vpn detail` command:

```
[local]PE_1#show xc l2vpn detail
LDP L2VPN Circuit VPLS 0x4000019 L2 State : Up      Peer : 100.1.1.10
VC ID             : 10          XC state      : Up
Local Label       : 131072     Access Circuit : 255/21:1023:63/0/1/25
Remote Label     : 131072     L2VPN Circuit : 255/21:1023:63/0/1/25
EXP bits         : 0          Local Encap   : ethernet
Remote Group ID  : 0          Remote Encap  :
Local VC Type    : Ethernet    Remote VC Type : Ethernet
Local VC MTU     : 1500       Remote VC MTU : 1500
XC group         :
LSP Configured  :             LSP Used     :
Flags 0x000d11e9: in-rib, in-lblmap, up, in-ldp, from-ldp, from-cfg :
peer-up
```



In this example, the VPLS circuit connects the local PE with the remote PE (Peer) 100.1.1.10. The common PW for this circuit (VC ID) is 10. This must match at the local and remote end of the circuit. For the PW to be up, the L2 state must be up. The local PE and the remote PE (VC) assign a label of 131072 (the labels are only locally significant and do not have to match). However, the labels are used to map traffic to the right bridge. The PW type (VC type) must be the same on both ends.

5.7 Verify Connectivity from the Local to Remote CE Routers

Use the `ping` command to verify connectivity from the local CE router to the remote CE router across the PW:

```
[CE]PE_1#ping 40.1.1.2
PING 40.1.1.2 (40.1.1.2): source 40.1.1.1, 36 data bytes,
timeout is 1 second
!!!!

----40.1.1.2 PING Statistics----
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.803/2.567/3.555/0.775 ms
```

5.8 Verify That the MAC Address of the Remote CE Was Learned Through the PW

Verify that the MAC address of the remote CE was learned through the pseudowire:

```
[CE]PE_1#show arp-cache
Total number of arp entries in cache: 2
Resolved entry : 2
Incomplete entry : 0
Host Hardware address Ttl Type Circuit
40.1.1.1 00:30:88:00:27:6b - ARPA 1/5
40.1.1.2 00:30:88:12:9f:1d 1852 ARPA 1/5
```

5.9 Verify That the MAC Addresses Were Learned by the Bridge

Verify that the MAC addresses were learned by the bridge and you have configured the MAC address associated with the bridge itself:

```
[CE]PE_1#show bridge table VPN1 VPN1
Context Bridge Group MAC Circuit
VPN1 VPN1 00:30:88:01:a8:ea sysMac-All Circuits
Static MAC = 1, Dynamic MAC = 0, Drop MAC = 0, Multicast = 0
```

In the command, the first `VPN1` is the bridge name and the second `VPN1` is the context where the bridge was configured (which is associated with the VPLS profile).



6 Alternative Procedure: Following a Ping Packet from a Local to a Remote CE Router

An alternative method to troubleshoot VPLS is to follow a ping packet from the local CE router to a remote CE router.

In the scenario in this section, the destination address of the packet is 40.1.1.2 and the source address is 40.1.1.1.

To follow the ping packet, perform the steps in Table 5.

Table 5 Following a Ping Packet From a Local to a Remote CE

| Task | Command | Notes | Checked? |
|---|---|-------|----------|
| Ping the Source CE | <code>ping dest-ip source-source-i p</code> | | |
| Is the Source CE Directly Connected? | <code>show ip route</code> | | |
| Is the Remote CE in the Local CE's ARP Cache? | <code>show arp-cach e</code> | | |
| Does the Bridge on the Local PE Know the Destination MAC Address? | <code>show bridge table all show xc l2vpn ldp</code> | | |
| What is the MPLS Inner Label? | <code>show xc l2vpn ldp detail</code> | | |
| What is the MPLS Outer Label? | <code>show mpls lsp</code> | | |
| Check the P Router's Label Mapping | <code>show mpls label-mapping</code> | | |
| To Which Bridge is VPLS Bound? | <code>show bridge binding all</code> | | |
| Verify that the Packet is Forwarded Correctly | <code>show bridge table bridge-g roupcontext</code> | | |
| Verify the Destination CE Knows the Local CE's MAC Address | <code>show arp-cach e</code> | | |

6.1 Ping the Source CE Router

Ping the source CE router, as in the following example:



```
[CE]PE_1#ping 40.1.1.2 source 40.1.1.1
PING 40.1.1.2 (40.1.1.2): source 40.1.1.1, 36 data bytes,
timeout is 1 second !!!!!

----40.1.1.2 PING Statistics----
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.882/2.119/2.740/0.359 ms
```

6.2 Is the Source CE Directly Connected?

When you run the `show ip route` command, the local CE checks its routing table and finds that network `40.1.1.0/30` is directly connected, as shown in the following extraction from the command output:

```
Type   Network      Next Hop   Dist  Metric   UpTime   Interface
C      40.1.1.0/30          0         0      22:14:10   ce
```

6.3 Is the Route to the Remote CE in the Local CE Router ARP Cache?

If the route to the remote CE is up, then the route should be in the remote CE router's ARP cache; to check this, use the `show arp-cache` command, as in the following example:

```
[CE]PE_1#show arp-cache
Total number of arp entries in cache: 2
  Resolved entry   : 2
  Incomplete entry : 0

Host           Hardware address  Ttl   Type  Circuit
40.1.1.1       00:30:88:00:27:6b -     ARPA  1/5
40.1.1.2       00:30:88:12:9f:1d 796   ARPA  1/5
```

6.4 Does the Bridge on the Local PE Router Know the Destination MAC Address?

To verify that the bridge on the local PE knows the destination MAC address, check the bridge table for the remote CE router's MAC address. If it is present, the local CE router has learned the MAC address through the VPLS PW.

```
[CE]PE_1#show bridge table all
Context  Bridge Group  MAC                               Circuit
local    Unbound      00:30:88:01:a8:ea sysMac-All Circuits
VPN1     VPN1         00:30:88:01:a8:ea sysMac-All Circuits
VPN1     VPN1         00:30:88:12:9f:1d VPLS 4
```

To identify the PW, label, and status for a circuit, such as VPLS 4, use the `show xc l2vpn ldp` command, as in the following example:



```
[local]PE_1#show xc l2vpn ldp
      LDP L2VPN Circuits

L2 Circuit      L2 State Peer address   VC Id   L-Label  State
VPLS 0x4000004 Up         100.1.1.10     10      131072   Up
```

The output indicates that VPLS 4 (with PW ID 10) connects the local PE router with remote peer 100.1.1.10. The common PW ID is 10 at the local and remote end; this ID must match. The local PE router assigns a label of 131072.

6.5 What Is the MPLS Inner Label?

The PE recognizes the correct bridge by the MPLS inner label. To determine the inner label, use the `show xc l2vpn ldp detail` command, as in the following example:

```
[local]PE_1#show xc l2vpn ldp detail
LDP L2VPN Circuit VPLS 0x4000004
  L2 State      : Up           Peer           : 100.1.1.10
  VC ID         : 10          XC state       : Up
  Local Label   : 131072     Access Circuit : 255/21:1023:63/0/1/4
  Remote Label  : 131072    L2VPN Circuit : 255/21:1023:63/0/1/4
  EXP bits     : 0          Local Encap    : ethernet
  Remote Group ID : 0       Remote Encap   :
  Local VC Type : Ethernet   Remote VC Type : Ethernet
  Local VC MTU  : 1500      Remote VC MTU  : 1500
  XC group      :           Negotiated cbit : no
  LSP Configured :         LSP Used       :
  XC profile    :
  Flags 0x000d11e9: in-rib, in-lblmap, up, in-ldp, from-ldp, from-cfg
                  : peer-up
```

Note the peer address, 100.1.1.10, and remote label, 131072, which matches the local label. The egress PE router requires label 131072 for packets that are sent over PW with ID 10.

6.6 What Is the MPLS Outer Label?

To determine the outer label, use the `show mpls lsp` command, as in the following example:

```
[local]PE_1#show mpls lsp
Codes : S - MPLS-Static, R - RSVP, L - LDP, B - BGP

Type Endpoint      Direct Next-hop  Out Label  Adjacency Id
L   10.1.2.8/30    1.1.1.2        3          0x1300011
L   100.1.1.2/32  1.1.1.2        3          0x1300013
L   100.1.1.10/32 1.1.1.2        524294     0x1300015
```

The system here uses 524294 as the outer label and sends the MPLS packet to the provider (P) router.



6.7 Check the P Router Label Mapping

The P router does not know the MAC address, the inner label, or the IP address. It routes the packet received based on the outer label, shown by issuing the `show mpls label-mapping` command on the P router:

```
[local]PE_1#show mpls label-mapping
Codes : S - MPLS-Static, R - RSVP, L - LDP, B - BGP

Type      In Label  Action      Direct Next hop  Out Label  Adjacency Id
-----
L         524294   php         10.1.2.10        3          0x1300010
L         524296   php         1.1.1.1          3          0x1300012
```

This P router performs penultimate hop popping, removes the outer label, and sends the packet out with a label of 3 to the egress PE router.

6.8 To Which Bridge Is the VPLS Instance Bound?

To determine the bridge to which the VPLS circuit is bound, on the ingress PE router, enter the `show bridge binding all` command. The output maps the bridge group to the context on which the bridge group is configured (the context to which the customer router or switch is attached).

```
[local]PE_1#show bridge binding all
Context      Bridge Group      Circuit
-----
VPN1         VPN1              1/4
VPN1         VPN1              VPLS 4
```

If the deployment has too many bridge circuits to easily determine the mapping from the output, you can use the `grep` command to find the appropriate VPLS circuit.

6.9 Verify that the Packet Is Forwarded Correctly

Next, use the `show bridge table` command to verify that the CE router receives the Ethernet packet, checks the bridge forwarding table, and forwards the packet on the correct circuit to the customer router.

```
[local]PE_1#show bridge table VPN1 VPN1
Context      Bridge Group      MAC              Circuit
-----
VPN1         VPN1              00:30:88:00:27:6b 1/4
VPN1         VPN1              00:30:88:01:a8:ea sysMac-All Circuits

Static MAC = 1, Dynamic MAC = 1, Drop MAC = 0, Multicast = 0
```

The example shows the packet going out slot and port 1/4 to customer premises equipment (CPE) with MAC address 00:30:88:00:27:6b.



6.10 Does the Destination CE Know the Local CE's MAC Address

Now, on the remote CE router, examine the ARP cache to verify the egress CE router has the MAC address of the local CE router (which is why it responds to the original ping from the local CE router in Section 6.1 on page 12).

```
[local]CE_3#show arp-cache
Total number of arp entries in cache: 2
Resolved entry : 2   Incomplete entry : 0
Host           Hardware address  Ttl   Type  Circuit
40.1.1.1       00:30:88:00:27:6b    2910  ARPA  2/1
40.1.1.2       00:30:88:12:9f:1d    -      ARPA  2/1
```

The output verifies that the MAC address for the source CE router is 00:30:88:00:27:6b.

7 Step 6: Collecting VPLS Debug Information for Customer Support

If you have performed the troubleshooting steps in this document and the problem persists, you can use the following commands to collect debug information for analysis by customer support:

- `debug l2vpn all`
- `debug l2vpn config`
- `debug ldp message address detail`
- `debug ldp message label`
- `debug ldp protocol l2vpn detail`
- `debug lm l2vpn`
- `debug lm vpls`
- `debug vpls cct`
- `debug vpls config`
- `debug vpls event`
- `debug vpls peer`
- `debug vpls state.`

For the full syntax for these commands, see *Command List*.



Run these commands for a short time, save the output, and send it to customer support. For more information, see *Data Collection Guideline for the SmartEdge Router*.