CISCO VALIDATED PROFILE

Routing L2VPN Vertical

April 2016

Table of Contents

Profile Introduction

Cisco is transforming the network edge with Cisco ASR 1000 Series Aggregation Services Routers and Cisco 4000 Series Integrated Services Routers (ISRs), new lines of midrange routers that establish a new price-to-performance class offering, benefiting both enterprises and service providers. These routers provide a great opportunity for simplifying the WAN edge and significantly decreasing network operating expenses (OpEx). By efficiently integrating a critical set of WAN edge functions such as WAN aggregation, Internet edge services, firewall services, VPN termination, etc. into a single platform, enterprises can meet their business objectives by facilitating deployment of advanced services in a secure, scalable, and reliable manner while minimizing the total cost of ownership (TCO).

Cisco WAN aggregation solutions distinguish themselves from other solutions by offering multiservice routers with the highest performance, availability, and density for concurrent data, security, voice, and application-acceleration services with maximum headroom for growth. The solutions feature embedded security, performance, and memory enhancements, and high-performance interfaces featuring the latest WAN technologies can help enterprises meet the needs of the most demanding WAN network.

Interworking is a transforming function that is required to interconnect two heterogeneous attachment circuits (ACs). Several types of interworking functions exist. The function that is used would depend on the type of ACs being used, the type of data being carried, and the level of functionality required. The two main Layer 2 Virtual Private Network (L2VPN) interworking functions supported in Cisco software are bridged and routed interworking.

Layer 2 (L2) transport over multiprotocol label switching (MPLS) and IP already exists for like-to-like ACs, such as Ethernet-to-Ethernet or Point-to-Point Protocol (PPP)-to-PPP. L2VPN Interworking builds on this functionality by allowing disparate ACs to be connected. An interworking function facilitates the translation between different L2 encapsulations.

L2VPN Pseudowire Switching allows the user to extend L2VPN pseudowires across an inter-AS boundary or across two separate MPLS networks, as shown in the figures below. L2VPN Pseudowire Switching connects two or more contiguous pseudowire segments to form an end-to-end multihop pseudowire. This end-to-end pseudowire functions as a single point-to-point pseudowire.

L2VPN Pseudowire Switching enables you to keep the IP addresses of the edge PE routers private across inter-AS boundaries. You can use the IP address of the autonomous system boundary routers (ASBRs) and treat them as pseudowire aggregation (PE-agg) routers. The ASBRs join the pseudowires of the two domains.

L2VPN Pseudowire Switching also enables you to keep different administrative or provisioning domains to manage the end-to-end service. At the boundaries of these networks, PE-agg routers delineate the management responsibilities.

Table 1 lists the key areas on which the profile focuses.

Table 1 Profile feature summary

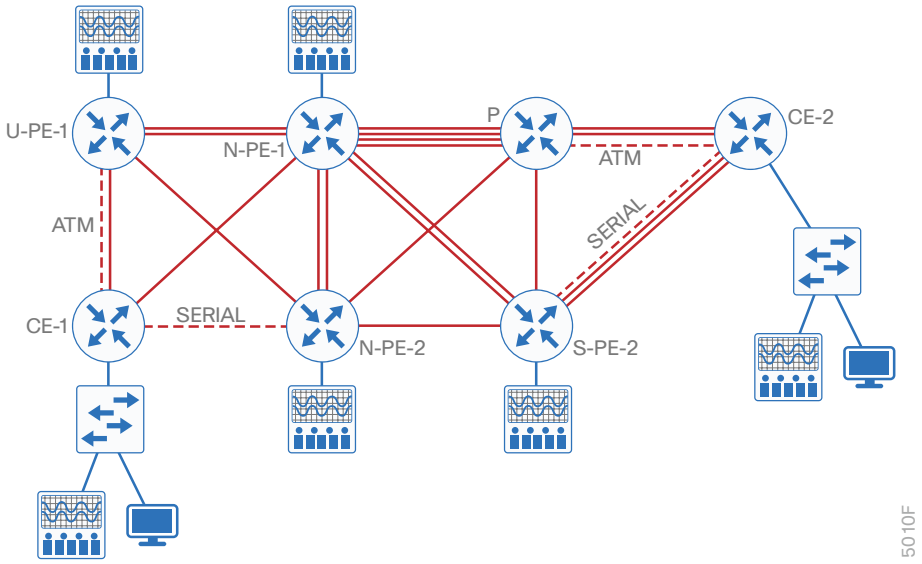
Deployment areas	Features
L2VPN	L2VPN, Layer 2 Tunnel Protocol Version 3 (L2TPv3), Any Transport over MPLS (AToM), Virtual Private LAN Service (VPLS)
Address families	IPv4
Interfaces	Frame-Relay , Asynchronous Transfer Mode Switching (ATM) , Ethernet
Routing	Open Shortest Path First (OSPF)

Network Profile

Based on the research, customer feedback, and configuration samples, the profile is designed with a generic deployment topology that you can easily modify to fit any specific deployment scenario. Refer to the topology for further details.

TOPOLOGY DIAGRAM

Figure 1 *L2VPN Profile: topology overview*



Disclaimer

The links between the different network layers in the topology are mainly to facilitate this profile validation across different platform combinations, and the actual deployment could vary based on specific requirements.

HARDWARE & FEATURE SPECIFICATIONS

Key Vertical Features

Table 2 defines the hardware, place-in-network (PIN), and the features deployed. The scale of these configured features, the test environment, the list of endpoints, and the hardware/software versions of the network topology are defined later.

The following physical topology is used for L2VPN profile testing. The devices shown were used in the topology.

The following devices simulate the the ISP with which the edge router peers:

- ASR1004 with RP2/ESP40 simulating CE1 and CE2
- ASR1006 with RP2/ESP40 simulating the UPE1 and SPE2 as shown in the diagram above
- ASR1001-X simulating NPE1, P, NPE2

Hardware Profile

Table 2 defines the set of relevant hardware, servers, test equipment, and endpoints that are used to complete the L2VPN Vertical Profile deployment.

This list of hardware, along with the relevant software versions and the role of these devices, complement the actual physical topology shown in Figure 1.

Table 2 Hardware profile of servers and endpoints

VM and HW	Software versions	Description
Ixia	IxExplorer version 6.20	Generate TCP UDP ICMP traffic streams
	IxLoad version 5.20	Generate stateful TCP traffic.

TEST ENVIRONMENT

This section describes the features and the relevant scales at which the features are deployed across the physical topology.

Table 3 *Feature scale validated in this profile*

Feature	Scale
Pseudowire (PW)	13000
Ethernet Flow Points (EFP)	6000
Virtual Forwarding Instance (VFI)	3064
VFI QoS Sessions	500
Multiple Spanning Tree (MST) sessions	64
Ethernet over MPLS (EoMPLS) sessions	3000
Traffic Engineering (TE) tunnels	1500
MAC ACL sessions	100
EFP QoS sessions	100

Use Case Scenarios

TEST METHODOLOGY

The use cases listed in Table 4 are executed using the topology shown in Figure 1, along with the test environment shown in Table 4.

With respect to the longevity for this profile setup, the CPU and memory use are monitored overnight, as well as during the weekends, along with any mem-leak checks. In order to test the robustness, certain negative events are triggered during the use case testing.

USE CASES

Table 4 describes the use cases that were executed on the L2VPN Profile. These use cases are divided into buckets of technology areas to show the complete coverage of the deployment scenarios.

These technology buckets are composed of Bringing Up Setup, feature interaction, events, monitoring and troubleshooting, simplified management, system health monitoring, system & network resiliency, and robustness.

Table 4 *List of use case scenarios*

No.	Focus area	Use cases
Setup Bringup		
1	L2VPN config	Bring up MP-BGP in the core with IGP (OSPF) in between PE and P routers and verify that IGP (OSPF) neighbors are established in core. ▪ Inject 10K ipv4 IGP routes in MP-BGP core and verify routes installation on all PE and P routers in core, MPLS LDP on the core facing interfaces, BFD on the on the MPLS interfaces and verify the sessions are established. ▪ Bring up 100 ibgp sessions in between all PE routers in MP-BGP core and verify ibgp sessions are established in core
2	HVPLS Routed Pseudowire	HVPLS Routed Pseudowire: On H-VPLS setup, configure BDI interface and connect to the same BD. ▪ Send L3 traffic from end-to-end and check if the traffic is received. ▪ Send L2 and L3 multicast traffic and verify they are received. ▪ Send bidirection traffic and check the MAC learning and forwarding w.r.t split-horizon group configuration. H-VPLS setup on NPE1 and NPE3 , eompls on NPE2. ▪ Send bi-direction traffic and check the MAC learning and forwarding w.r.t split-horizon group configuration.

Table 4 continued

Features testing		
3	MAC filtering	MAC ACL filtering: ▪ In HVPLS setup, apply MAC ACLs on service instances ▪ Verify that MAC access-lists are matching and traffic is filtered accordingly
4	Storm control	Configure storm control. ▪ Verify functionality
Events		
5	Virtual Forwarding Instance (VFI) events QoS events L2VPN events	▪ Add /remove VFI , flap VFI. ▪ Remove and add BD,vpn id ,vpls id and route-targets wherever applicable. ▪ Change default values of vpnid and vpls id ▪ Add/remove neighbor commands ▪ Enable and disable QoS. ▪ Add/remove xconnect
Monitoring & troubleshooting		
6	NetFlow	Enable NetFlow and sampler and collect statistics using collector.
System health monitoring		
7	System health	Monitor system health for CPU use, memory consumption, and memory leaks during longevity
System & network resiliency, robustness		
8	System resiliency	Verify system-level resiliency during the following events: ▪ Active RP failure/RP switchover ▪ Active/Standby ESP failure ▪ WAN/LAN interface flaps ▪ SIP/SPA reload/OIR
9	Negative events, triggers	Verify that the system holds well and recovers to working condition after the following negative events are triggered: ▪ Config changes–add/remove config snippets, config replace ▪ Routing protocol Interface flaps ▪ CE/PE router failure scenario

Appendix A

You can find example configurations at the following location:

http://cvddocs.com/fw/cvpconfig-routing

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.