Cisco Validated Profile (CVP)

Cisco ASR 9000 Series Web OTT Profile

May 2017

Table of Contents

Profile Introduction

The Cisco® ASR 9000 Series is a true carrier-class solution. It features the modular, microkernel-based Cisco IOS® XR Software operating system, comprehensive system redundancy, and a full complement of network resiliency schemes. Cisco ASR 9000 Series Routers also offer the services and application-level intelligence you need for optimized content delivery (audio, video, and data). The ASR9000 intelligently blends with the following technology/deployment solutions:

- Cable/MSO
- Carrier Ethernet
- Mobile backhaul
- Web OTT
- Multiservice edge
- DCI gateway
- Broadband gateway
- Large enterprise WAN

This document is intended as a reference for ASR9K web OTT deployment profiles with a focus on LER and LSR features and scale requirements. Over the top (OTT) refers to delivery of audio, video, and other media services provided over the Internet rather than via a service provider's own dedicated, managed IPTV network. OTT is delivered directly from provider to viewer using an open Internet/broadband connection, independently of the viewer's ISP, without the need for carrier negotiations and any special infrastructure investment on the part of the provider. It is a best effort, unmanaged method of content delivery via the Internet that suits providers that are primarily broadcasters rather than ISPs. As part of this profile analysis, this document provides a representative feature mix most commonly used in such a deployment role, the associated scale of these features, and an analysis of router health and performance.

Table 1 summarizes the key areas on which this profile focuses.

Table 1. ASR9K Web OTT Profile Feature Summary

Deployment Areas	Features
Edge	BGP, BGP add path, LACP, BFD, QoS, and ACL
Core	Segment routing, RSVP traffic engineering, ether bundles, BFD, QoS, ACL
Network monitoring and troubleshooting	Smart License, Netflow, PAM, SPAN
Network management	SNMP, telemetry, NetConf-Yang, XML, Telnet, SSH, CSM

Network Profile

Topology Diagrams

Figure 1 shows the basic topology used in web OTT profile.

Figure 2 shows the link protection topology used in web OTT profile.

Figure 3 shows the node protection topology used in web OTT profile.

Figure 1. ASR9k Web OTT Profile: Basic Topology Overview

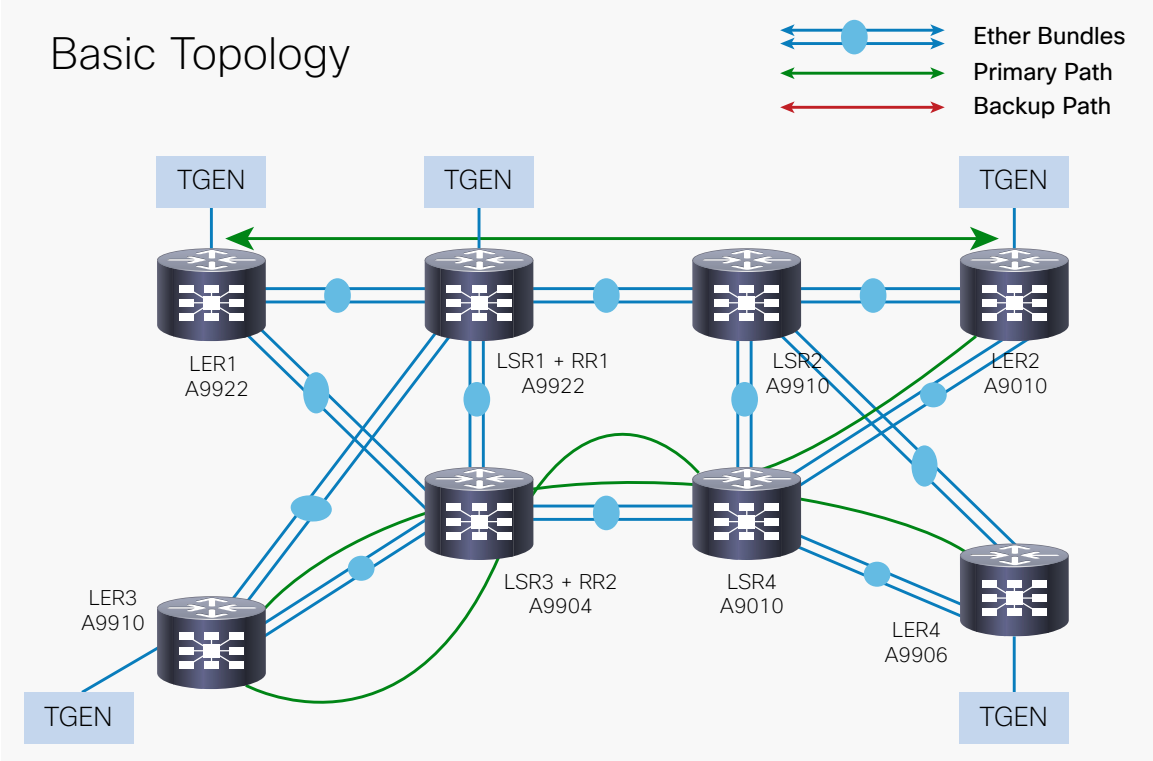


Figure 2. ASR9k Web OTT Profile: Link Protection Topology Overview

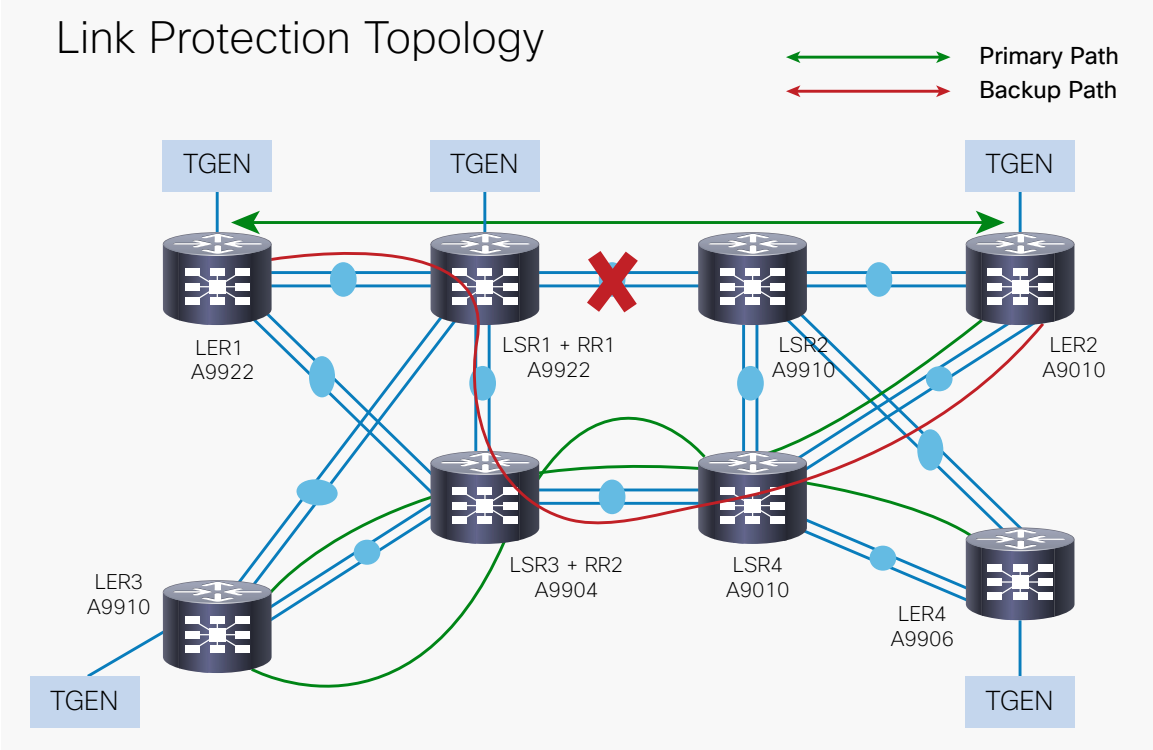
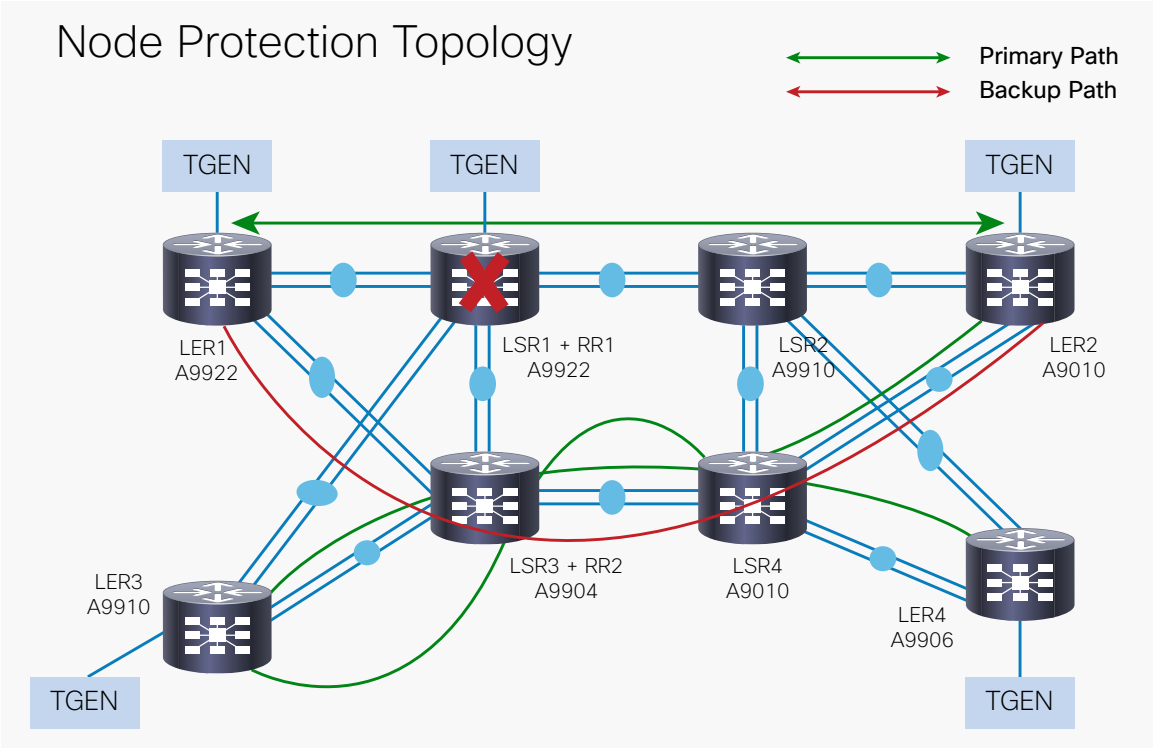


Figure 3. ASR9k Web OTT Profile: Node Protection Topology Overview



Hardware and Feature Specifications

Web OTT customers use ASR9000s as both LER and LSR devices to provide content delivery in their network. The high scale and high processing power of NPU make ASR9000s globally accepted LER and LSR devices in Web OTT customer profiles.

Following are the roles for which the ASR9000 platform was tested and characterized for web OTT profile for release 6.1.3:

- LER 9922 with Tomahawk and Skyhammer line cards
- LSR 9904 and 9922 with Tomahawk and Skyhammer line cards
- RR 9904 with Tomahawk line card

Hardware Profile

Table 2 defines the set of relevant hardware used to complete the end-to-end Carrier Ethernet profile deployment.

Table 2. Hardware Profile of Access and Core Devices

Hardware	Software Versions	Description
ASR9K 9922	XR 06.01.03	For edge and core functionality
ASR9K 9904	XR 06.01.03	For RR functionality

Test Environment

This section contains the description of the features and the relevant scales at which the features are deployed across the physical topology. Table 3 lists out the scale for each respective feature.

Table 3. Carrier Ethernet Profile: Feature Scale Validated in This Profile

Feature	Scale
Ether bundles	64x10G: 1 and 2x100G: 1
MPLS-TE	Headend: 4k, midpoint: 64K, tail end: 4k
Routing ISIS	Adj: 10 v4 and v6, routes: 10k v4 and 4K v6
Routing BGP	eBGP: 200v4 and 100v6, route: 2M v4 with 10M paths 400K v4 with 4M paths
QoS	Class-maps: 12 and policy-maps all interfaces
Netflow	Sampling rate 1 out of 8192. Enabled on all interfaces
SNMP	No. of polling servers: 3; polling frequency: 30 sec, 1 min, and 10 min
SRLG for TE	32 groups per IF
Flex CLI	Bundles, ISIS, MPLS TE, RSVP
Infra	5 SSH sessions
ACL	10 V4 and V6 ACLs

Use Case Scenarios

Test Methodology

The use cases listed in Table 4 will be executed using the topologies defined in Figure 1, Figure 2, and Figure 3 along with the test environment, already explained in this document.

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

Use Cases

Table 4 describes the use cases that were executed on the web OTT profile. These use cases are divided into buckets of technology areas to provide the complete coverage of the deployment scenarios.

Table 4. Use Case Scenario

Number	Focus Area	Use Cases
Bootup and Management		
1	Boot up cXR	Web OTT customers should be able to boot up ASR9K nodes with 32-bit software via TURBOBOOT as well as PIE upgrade to the targeted IOXR images successfully. The following scenarios are validated in this profile: ▪ Turboboot ▪ Pie upgrade (upgrade, downgrade, FPD, config backup/restore) ▪ -SMU activation ▪ NV satellite upgrade
2	Boot up eXR	Web OTT customers should be able to boot up ASR9K with IOS-XR 64-bit software with DHCP option or upgrade router with install upgrade CLI.
3	Boot up eXR with GISO image	GISO is custom-built ISO image. This has option to include mini IOS plus required rpms plus any smus required plus configuration of device. This ISO is built out of the box on any Linux server. After ISO is built, ASR9k can be upgraded to this image or pxe booted even with external USB. All these options are tested and verified with 6.1.3 image.
4	System infra/ management	Validate that syslog, SNMP, SSH, Telnet, NTP are functioning well after node bootup.
5	Smart licensing	Validate that the smart licenses client on the node is registered with the node and the correct number and type of the licenses are being consumed.
Web OTT Solution		
6	Basic MPLS TE	In this scenario, headend is configured with 64 tunnels to 62 different LER devices. BGP traffic is flowing over these tunnels to remote end LERs. This test scenario verifies basic MPLS traffic engineering functionality over 64 ECMP paths: ▪ 64 bundle members with 64 traffic engineering tunnels over this bundle interface. ▪ Traffic is load balanced with 64 ECMP paths.

Number	Focus Area	Use Cases
7	MPLS TE + FRR (link protection)	In this scenario FRR functionality (link protection) is verified with tunnels with 64 ECMP paths. As shown in Figure 2, link is broken between LER and LSR node. This routes traffic through backup path. Traffic loss is measured during this event: ▪ Traffic is correctly routed through backup path with FRR status shown as active. ▪ Traffic loss is < 50ms for local event. ▪ After restoring link, traffic flows over primary link, and traffic loss is less than 20ms.
8	MPLS TE + FRR (node protection)	In this scenario FRR functionality (node protection) is verified with tunnels with 64 ECMP paths. As shown in Figure 3, node is brought down between LER and LSR node. This routes traffic through backup path. Traffic loss is measured during this event: ▪ Traffic is correctly routed through backup path with FRR status shown as active. ▪ Traffic loss is < 50ms. ▪ After restoring node, traffic flows over primary link, and traffic loss is less than 20ms.
9	MPLS TE preemption	In this scenario low-priority LSP is preempted by high-priority LSP. Initially both high-priority and low-priority traffic is sent over bundle links that meet BW requirement. Later, bundle members are shut down so BW requirement is exceeded. In the event of trigger, it's verified that: ▪ No high-priority LSPs are brought down. ▪ Only low-priority LSPs are brought down. No high-priority traffic item loss is seen. Only low-priority traffic item loss is seen.
10	QoS verification	In this scenario QoS functionality is verified on bundle interface with 64 member ECMP paths. As shown in Figure 1, priority Q scheduler with proportional traffic, per class traffic, and bursty traffic tests are verified. Traffic Q starvation tests are also verified.
11	Device drain and undrain by application of ISIS overload bit	In this scenario ISIS overload bit is configured to drain the node during maintenance, if router needs to be drained for LSP path. Configure flex group with ISIS overload bit configuration and apply this configuration to router ISIS configuration. On event of this configuration: ▪ Router where this configuration is applied will be removed from LSP path. ▪ Tunnel LSP will be reoptimized to backup path. ▪ Traffic flows over backup path. ▪ If backup does not exist, then reoptimization is tried for 3 minutes with every 30-second interval.

Number	Focus Area	Use Cases
Convergence, HA, and Network Resiliency		
12	Process start	This profile verifies that during process restart, the web OTT services mentioned in steps 4 through 10 are recovered with minimal system effect.
13	Link flap	This profile verifies that during link flap event (link down and link up), the carrier Ethernet services mentioned in steps 4 through 10 are recovered with minimal system effect.
14	LC OIR	This profile verifies that during LC OIR (soft OIR or physical plug out and plug back in), the carrier Ethernet services mentioned in steps 4 through 10 are recovered with minimal system effect.
15	RSP FO	This profile verifies that during redundant RSP/RP failover, the carrier Ethernet services mentioned in steps 4 through 10 are recovered with minimal system effect.
16	Node failure	This profile verifies that during node failure (soft reload or physical power off and power back on), the carrier Ethernet services mentioned in steps 4 through 10 are recovered with minimal system effect.
System Health Monitoring		
17	System health	Monitor system health for CPU usage, memory consumption, and memory leaks during longevity.

C07-738916-00 08/17