CISCO VALIDATED PROFILE

Routing
Private WAN Base 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.

This profile is designed in such a way to integrate key requirements in any WAN aggregation router and to validate the feature interoperability in a typical deployment.

WAN optimization and security are the key requirements of any enterprise deployment. This Private WAN Base profile addresses the following key requirements:

- **Security**–Security is one of the main concerns for any enterprise deployment. Special care must be taken to protect data and transactions and even to monitor and authenticate the devices that are being used within any enterprise.
- **WAN optimization**–As the traffic in any enterprise network grows, the need for WAN optimization becomes inevitable. Cisco AppNav virtualization technology provides network-integrated WAN optimization in the data center that allows elastic pooling of resources in a manner that is policy-based and on demand, with the best scalability, performance, and resiliency available. ISR-WAAS on the ISR 4400 series provides an option to deploy WAAS in the container of the router instead of having an external WAAS appliance.
- **Efficient WAAS management and monitoring**–Network administrators should be able to efficiently manage and monitor WAAS devices in their networks. Cisco-provided tools such as WCM could be used to quickly to manage, monitor, and troubleshoot WAAS devices.
- **System and network resiliency**–Any WAN aggregation or branch router would require a robust network with strict system and network-level resiliency. Routers with redundant route processor and forwarding processors help in designing a network that is stable and provides high-availability. With respect to WAAS devices, Cisco provides high availability using the capabilities such as having multiple AppNav controllers in a group and multiple service nodes in a service node group.

Table 1 *Private WAN BASE Profile feature summary*

Deployment areas	Features
Security	MPLSoDMVPN, DMVPN, unified threat defense, ZBFW, ACL
WAN optimization	AppNav, WAAS including Physical WAVE appliance and ISR-WAAS
Network planning & trouble-shooting	AVC, ERSPAN,NBAR, CoPP
Management & monitoring	SNMP, SysLog Server, WAAS Central Manager
System resiliency	SSO, HA, Service node groups, AppNav controller groups
Network services	OSFP, BGP, MPLS

Network Profile

Based on the research, customer feedback, and configuration samples, the Private WAN Base Profile is designed with a generic deployment topology that you can easily modify to fit any specific deployment scenario.

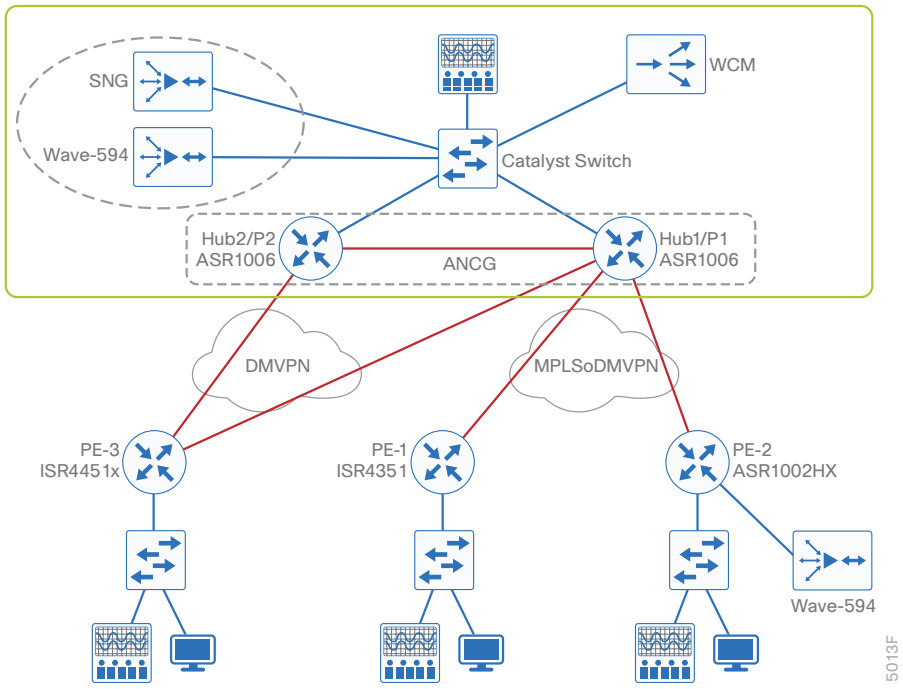
TOPOLOGY DIAGRAM

Figure 1 shows the Private WAN base profile network that is used for the validation of the Private WAN Base Profile.

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.

Figure 1 *Private WAN Base Profile: topology overview*



Scenario 1 (the left-portion of the topology) represents ISR4451 with ISR-WAAS being used as a branch router with two WAN links connecting two P routers using two DMVPN tunnels.

Scenario 2 (the right portion of the topology) represents the MPLSoDMVPN deployment scenario where the two branch routers with MPLS VPNs communicate with each other through P router over DMVPN tunnels. Here, the spoke-to-spoke communication always happens through the P router.

HARDWARE & FEATURE SPECIFICATIONS

This section describes the 3-D feature matrix where the hardware platforms are listed, along with their place-in-network (PIN) and the relevant vertical deployed.

Key Vertical Features

Table 2 defines the 3-D hardware, 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.

Table 2 3-D Feature summary with hardware and PIN

Deployment layer (PIN)	Platforms	Critical vertical features
Hub/P1	ASR1006	MPLSoDMVPN NBAR PerTunnel QoS AppNav BGP OSPF EPC CoPP
Hub/P2	ASR1006	NBAR AppNav BGP OSPF DMVPN
Branch/PE-SPOKE Router	ASR1002-HX ISR4351/K9 ISR4451-X/K9	MPLSoDMVPN AppNav ISR-WAAS SNORT PerTunnelQoS AVC NBAR ZBFW ACL
WAAS	WAVE-594	Application accelerator with AppNav controller as the interception method

Disclaimer

Refer to appropriate CCO documentation for release/feature support across different platforms.

Hardware Profile

Table 3 defines the set of relevant hardware, servers, test equipment, and endpoints that are used to complete the end-to-end 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 3 *Hardware profile of servers and endpoints*

VM and HW	Software versions	Description
WCM	5.5.5a-b9	For monitoring WAAS statistics
UCS Server	ESXi 5.5.0	To manage and host the Windows virtual machines, WCM, ICA traffic tool, etc.
Ixia	IxLoad	Test tool to generate HTTP, FTP, DNS, and Telnet traffic
Windows VM clients	Windows 7	Endpoints to test end-to-end traffic
WAVE-594	5.5.5a-b9	for wan optimization—used as a service node

Test Environment

This section describes the features and the relevant scales at which the features are deployed across the physical topology. Table 4 lists the scale for each feature.

Disclaimer

The table below captures a sample set of scale values used in one of the use cases. Refer to appropriate CCO documentation/datasheets for comprehensive scale data.

Table 4 *Private WAN Base Profile: feature scale*

Feature	Scale
DMVPN	1000 tunnels 500 towards Hub1-P1 and 500 towards Hub2-P2
Dot1q	500
AppNav	1000 tunnels
SNG	2 service nodes in SNG
AVC	Enabled on 100 DMVPN Tunnels
NBAR	Enabled on 100 DMVPN Tunnels
VRF	500 VRFs
SNORT	Enabled on 1 Tunnel (non-vrf)
ANCG	2 AppNav controllers in ANCG
ISR-WAAS	ISR-WAAS-750 profile on ISR-4351

Use Case Scenarios

TEST METHODOLOGY

The use cases listed in Table 5 are executed using the topology defined in Figure 1, along with the test environment shown in Table 4.

Images are loaded on the devices under test via the tftp server using the Management interface.

To validate a new release, the network topology is upgraded with the new software image with existing configuration composed of the use cases and relevant traffic profiles. Additional use cases acquired from the field or customer deployments are added on top of the existing configuration.

During each use case execution, syslog is monitored closely across the devices for any relevant system events, errors, or alarms. With respect to longevity for this profile setup, CPU and memory use/leaks are monitored during the validation phase. Furthermore, to test the robustness of the software release and platform under test, typical networks events would be triggered during the use case execution process.

USE CASES

Table 5 describes the use cases that were executed on the Private WAN Base Profile. These use cases are divided into buckets of technology areas to see the complete coverage of the deployment scenarios. Use cases continuously evolve based on the feedback from the field.

These technology buckets are composed of WAN optimization, security, network services, monitoring & troubleshooting, simplified management, and system health monitoring, along with system resiliency.

Table 5 *List of use case scenarios*

No.	Focus area	Use cases
Security		
1	DMVPN	DMVPN tunnel is used between the ISR branches to communicate with Hub/DC routers.
2	MPLSoDMVPN	Network admin should be able to extend the MPLS VPN between different branches through the Hub/P router. ▪ This is being achieved using MPLSoDMVPN. ▪ DMVPN tunnels are established between the PE routers to P routers. ▪ MP-BGP is used as the overlay protocol. ▪ PE-PE communication always happens through the P/Hub router.

Table 5 continued

3	UTD	Network administrator should be able to activate UTD on the branch routers to detect and protect the branches from threat traffic/unwanted traffic. ▪ Install and activate SNORT/UTD on the branch router ▪ Enable threat detection and verify that the threat traffic is detected ▪ Enable threat protection and verify that the threat traffic is dropped ▪ Verify that ISR-WAAS and UTD co-exists on the branch router and interaction works properly
WAN optimization		
4	AppNav	Network admin should be able to enable WAAS optimization for end to end WAAS optimization. ▪ Install and activate ISR-WAAS on branch router ▪ Configure AppNav on the hub routers to redirect traffic to WAVE appliances connected ▪ Configure redirection and optimization policies for desired traffic types ▪ Verify that the traffic optimization happens ▪ Verify that the ISR-WAAS and UTD co-exists on the container and interacts properly
Network services		
5	QoS	Network admin needs to enhance user experience by ensuring traffic and application delivery using pertunnelQoS for MPLSoDMVPN tunnels.
6	ZBFW	Network admin to secure the traffic using zone-based firewall ▪ Inspect traffic based on type of traffic or source/destination address
Monitoring & troubleshooting		
7	EPC	Network admin should be able to troubleshoot the network by capturing and analyzing the traffic. ▪ Embedded Packet Capture ▪ Wireshark
8	AVC	Enable IT admins to determine network resource use and capacity planning by monitoring IP traffic flows using Application Visibility and Control. ▪ Traffic types: IPv4, HTTP

Table 5 continued

Simplified management		
9	Monitoring	Simplify WAAS management and monitoring for network admins ▪ Manage and monitor WAAS devices by registering WAAS devices to WCM and monitoring the application stats on WCM dashboard ▪ Exporting and monitoring UTD logs from the syslog server
System health monitoring		
10	System health	Monitor system health for CPU use, memory consumption, and memory leaks during longevity
System & network resiliency, robustness		
11	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
12	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 ▪ WAAS events such as SN shut/unshut, ISR-WAAS deactivate/activate, SN reload, SN remove/add from SNG, AppNav controller remove/add from ANCG ▪ QoS events such as adding/removing QoS policy, modifying the ACL, modifying the class map ▪ UTD events such as disabling/enabling UTD virtual-service, deactivating/activating UTD, removing/adding UTD on tunnel interfaces

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.