



Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to <http://www.cisco.com/go/sba>

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.





SBA

BORDERLESS
NETWORKS

CONFIGURATION
FILES

VPN WAN Configuration Files Guide

● ● ● SMART BUSINESS ARCHITECTURE

August 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2012 are the “August 2012 Series”.

You can find the most recent series of SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100  
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64  
ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the [SBA feedback form](#).

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide	1	RS200-3925-1	51
Introduction	2	RS200-3925-2	54
Using the Deployment Guides	2	RS200-D3750X	58
Using the VPN WAN Configuration Files Guide	3	Remote Site 201: Single-Router, Dual-Link with Access-Layer Stack (MPLS + DMVPN)	64
Graphical Interface Management	3	RS201-2911	64
Appendix A: Product List	5	Remote Site 202: Single-Router, Dual-Link (MPLS + DMVPN)	69
WAN Configuration Files	9	RS202-2911	69
WAN-Aggregation Devices	9	Remote Site 203: Dual-Router, Dual-Link with Access Layer Stack (MPLS + DMVPN)	74
WAN-D3750X	11	RS203-2921-1	74
VPN-ASR1002-1	17	RS203-2921-2	78
VPN-ASR1001-2	21	WAN Remote-Site Devices - DMVPN Backup Dedicated Design Model (Layer 2 WAN)	83
WAN Remote-Site Devices - Dual DMVPN and DMVPN Only Design Models	24	Remote Site 211: Dual-Router, Dual-Link (Layer 2 WAN + DMVPN)	84
Remote Site 230: Single-Router, Single-Link (DMVPN)	25	RS211-2921-1	84
RS230-1941	25	RS211-2921-2	88
Remote Site 231: Single-Router, Dual-Link (DMVPN + DMVPN)	29	Remote site 213: Single-Router, Dual-Link (Layer 2 WAN + DMVPN)	93
RS231-2911	29	RS213-2911	93
Remote Site 232: Dual-Router, Dual-Link with Distribution Layer (DMVPN + DMVPN)	34	WAN-Aggregation Devices – DMVPN Backup Shared Design Model	98
RS232-2911-1	35	CE-ISR3945	99
RS232-2911-2	39	WAN Remote-Site Devices – DMVPN Backup Shared Design Model	103
RS232-D3750X	43	Remote Site 2: Single-Router, Single-Link with Local DHCP (MPLS-B Static)	104
WAN Remote-Site Devices - DMVPN Backup Dedicated Design Model (MPLS)	49	RS2-2921	104
Remote Site 200: Dual-Router, Dual-Link with Distribution Layer (MPLS + DMVPN)	50		

What's In This SBA Guide

Cisco SBA Borderless Networks

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

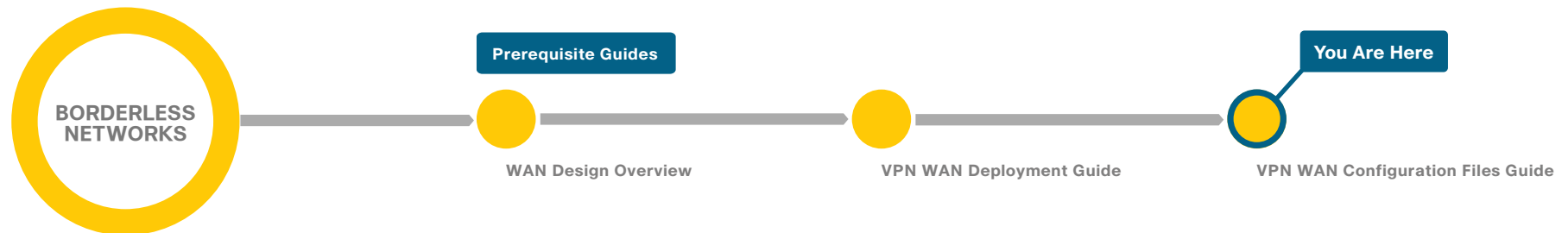
About This Guide

This *configuration files guide* provides, as a comprehensive reference, the complete network device configurations that are implemented in a Cisco SBA deployment guide.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>



Introduction

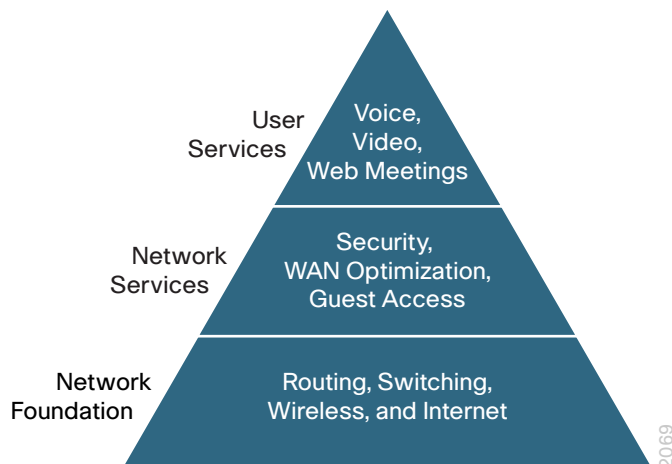
For Cisco partners and customers with up to 10,000 connected users, Cisco has created an “out-of-the-box” deployment that is simple, fast, affordable, scalable, and flexible. It is designed to be easy to configure, deploy, and manage. The simplicity of this deployment, though, belies the depth and breadth of the architecture.

The Cisco Smart Business Architecture (SBA) WAN is documented in a single design guide, and there are deployment guides and configuration files guides for each of the three key WAN technologies: Multiprotocol Label Switching (MPLS) WAN, Layer 2 WAN and VPN WAN.

Cisco SBA is a prescriptive reference design that provides step-by-step instructions for the deployment of the products in the design. It is based on best practice principles. Based on feedback from customers and partners, Cisco has developed a solid network foundation as a flexible platform that does not require reengineering to include additional network or user services.

Some of the base concepts referenced in this guide are covered in the SBA design and deployment guides. Those documents should be reviewed first.

Figure 1 - Smart Business Architecture model



This deployment guide has been architected to make your life a little bit—maybe even a lot—smoother. This architecture:

- Provides a solid foundation.
- Makes deployment fast and easy.
- Accelerates the ability to easily deploy additional services.
- Avoids the need for re-engineering of the core network.

Using the Deployment Guides

To reflect our ease-of-use principle, Cisco SBA has been divided into three sections: LAN, WAN, and Internet edge. Each section has one or more deployment guides and configuration guides. Each guide is organized into modules. You can start at the beginning or jump to any module. Each part of the guide is designed to stand alone, so you can deploy the Cisco technology for that section without having to follow the previous module.

Each deployment guide starts with a Business Problem and Architecture Overview. These sections cover the basics of the deployment guide, the value for you and your customer, and the broad-stroke features and benefits of this compelling design. Each then has different modules depending on the network components being covered.

The *VPN WAN Deployment Guide* has the following sections:

- Deploying a DMVPN WAN
- Deploying a WAN Remote-Site Distribution Layer
- Deploying WAN Quality of Service

Using the VPN WAN Configuration Files Guide

This document provides the available configuration files for the products used in the *VPN WAN Deployment Guide*. It is a companion document to the deployment guide as a reference for engineers who are evaluating or deploying Cisco SBA.

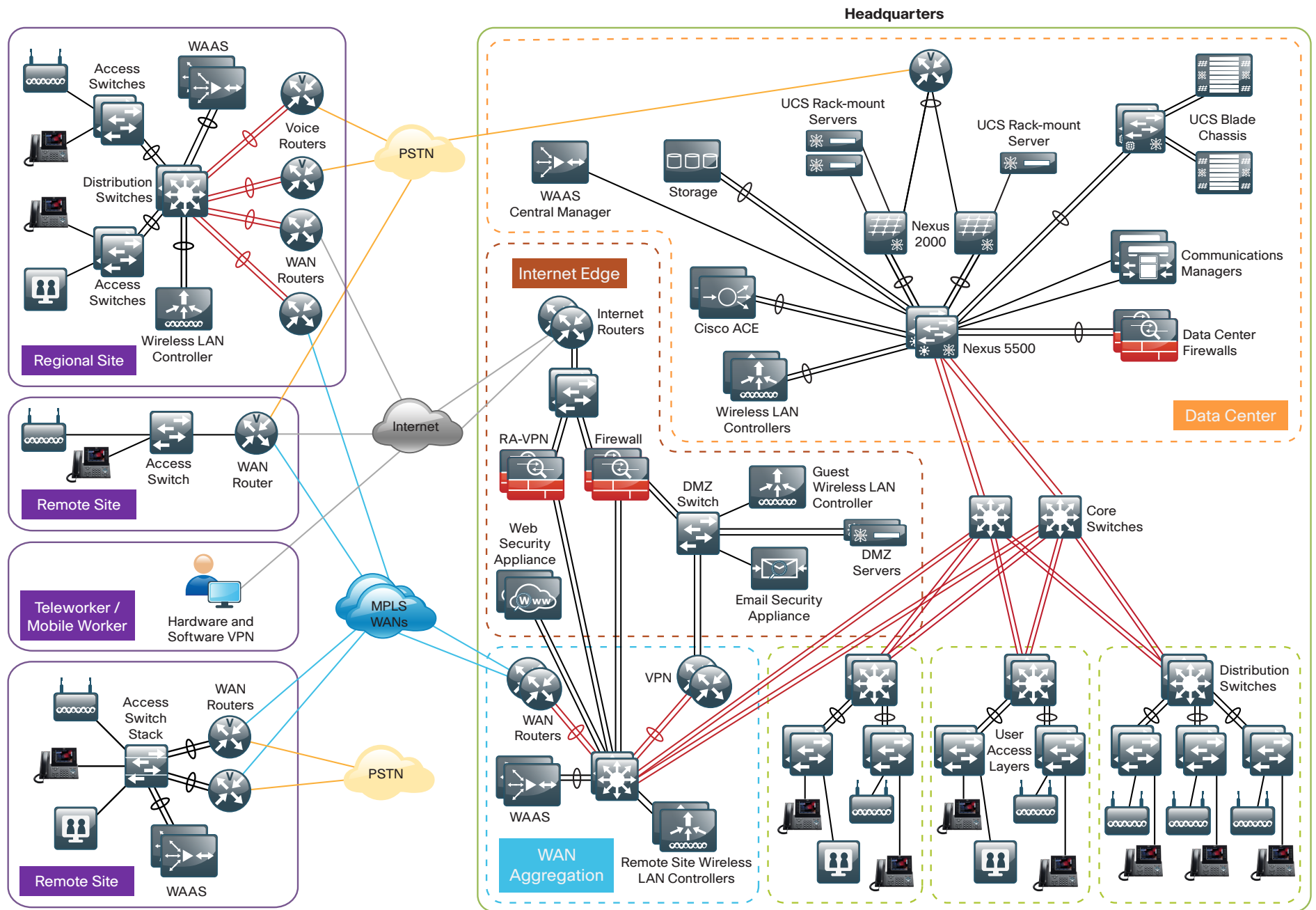
Both the *VPN WAN Deployment Guide* and the *VPN WAN Configuration Files Guide* provide the complete list of products used in the lab testing of this design.

Graphical Interface Management

There are products in this design where we have omitted the configuration file. Those products have browser-based graphical configuration tools. For step-by-step instructions on configuring those products, please refer to the *VPN WAN Deployment Guide* at <http://www.cisco.com/go/sba>.

Notes

Figure 2 - Cisco SBA Overview



Appendix A: Product List

WAN Aggregation

Functional Area	Product Description	Part Numbers	Software
WAN-aggregation Router	Aggregation Services 1002 Router	ASR1002-5G-VPN/K9	IOS-XE 15.2(2)S
	Aggregation Services 1001 Router	ASR1001-2.5G-VPNK9	Advanced Enterprise
WAN-aggregation Router	Cisco 3945 Security Bundle w/SEC license PAK	CISCO3945-SEC/K9	15.1(4)M4
	Cisco 3925 Security Bundle w/SEC license PAK	CISCO3925-SEC/K9	securityk9, datak9
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.1(4)M4
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	securityk9, datak9
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
Modular WAN Remote-site Router	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	15.1(4)M4
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	securityk9, datak9
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9	
Modular WAN Remote-site Router	1941 WAAS Express only Bundle	C1941-WAASX-SEC/K9	15.1(4)M4
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	securityk9, datak9

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 8.6(1)1
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	IPS 7.1(4) E4
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	6.6.114

Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 3750-X Series Stackable 24 10/100/1000 Ethernet ports	WS-C3750X-24T-S	15.0(1)SE2 IP Base

LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG)
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	IP Base
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(1)SE2
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	IP Base
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(1)SE2
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	IP Base
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(1)SE2
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	LAN Base
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.0(1)SY1
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	IP services
	Cisco Catalyst 6500 16-port 10GbE Fiber Module w/DFC4	WS-X6816-10G-2T	
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG)
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	Enterprise Services
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(1)SE2
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	IP Services
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

WAN Configuration Files

WAN-Aggregation Devices

This section includes configuration files corresponding to the Dual DMVPN and DMVPN Only design models as referenced in Figure 3. This section also includes configuration files corresponding to the DMVPN components of both the DMVPN Backup Dedicated design models as referenced in Figure 4 and Figure 5.

Figure 3 - WAN-aggregation design—Dual DMVPN and DMVPN Only

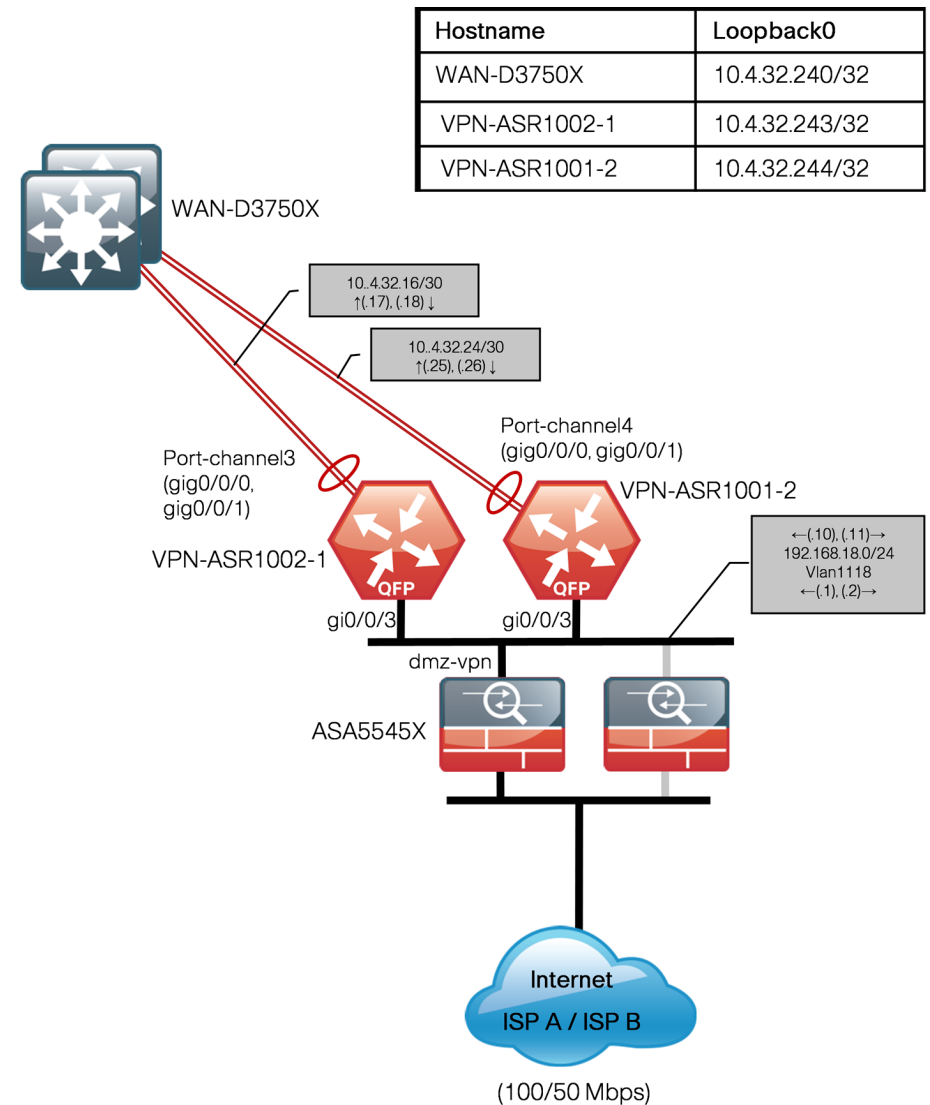


Figure 4 - WAN-aggregation design—DMVPN Backup Dedicated (MPLS WAN)

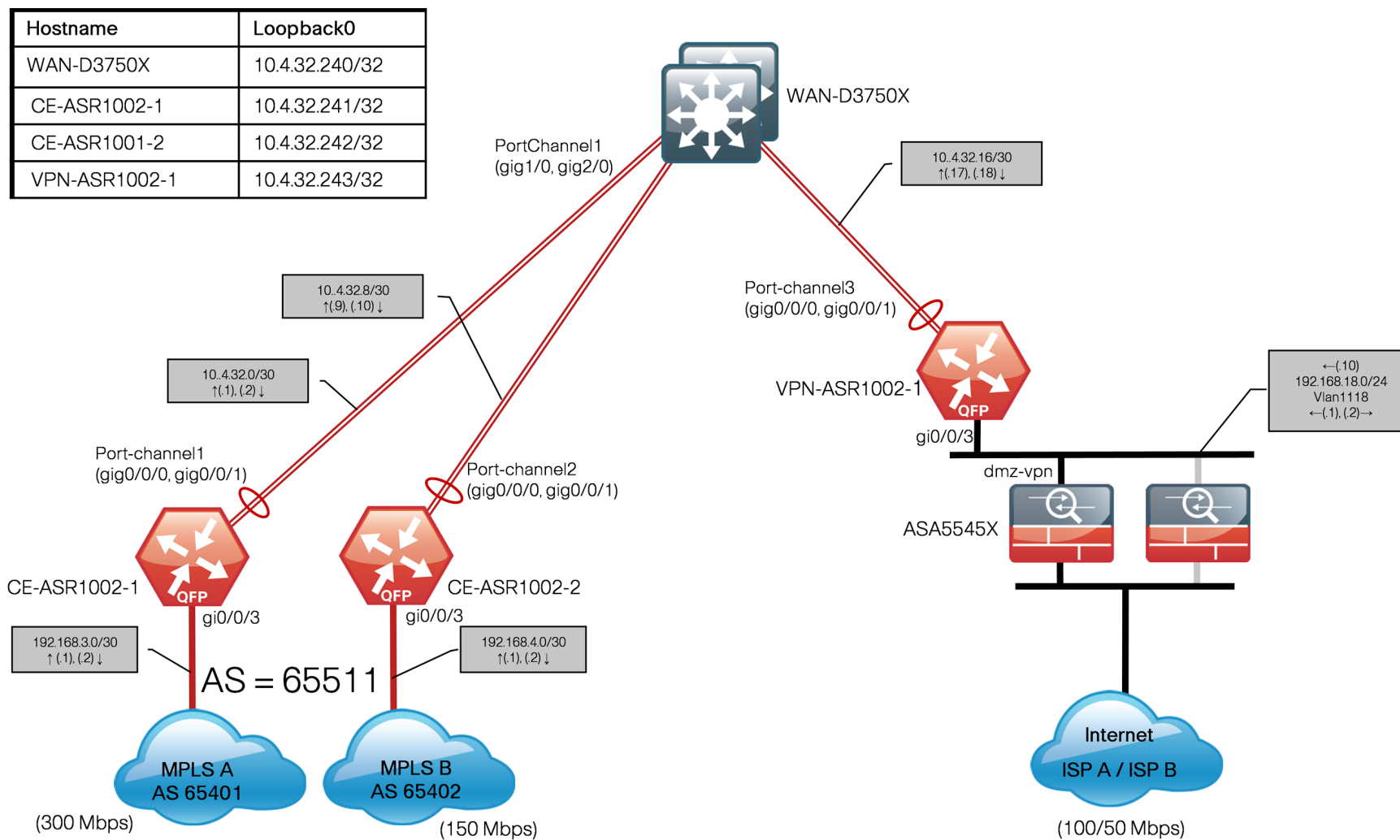


Figure 5 - WAN-aggregation design—DMVPN Backup Dedicated (Layer 2 WAN)

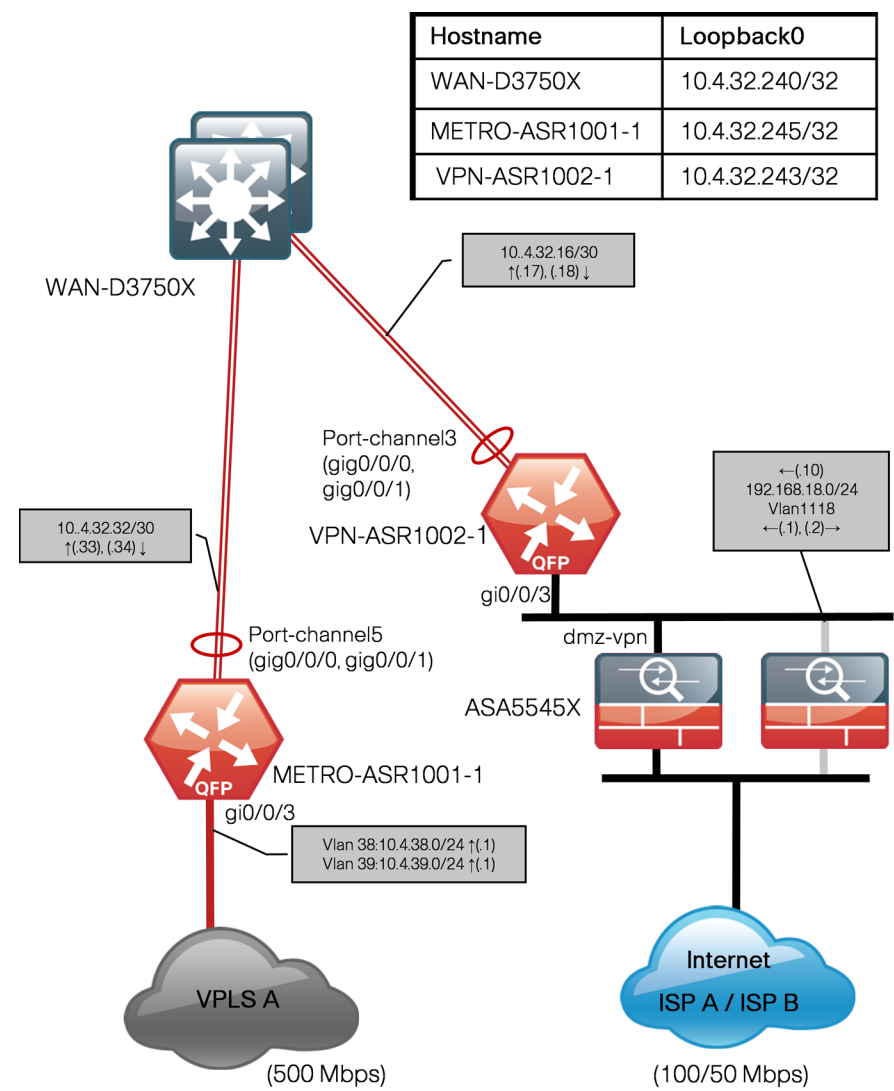


Table 1 provides a summary of the various distribution layer switch device interconnections to other WAN-aggregation components.

Table 1 - Dual DMVPN distribution layer switch port channel information

Port-Channel	Member interfaces	Layer3/Layer2	Connected device
3	gig1/0/3 gig2/0/3	Layer 3	VPN-ASR1002-1
4	gig1/0/4 gig2/0/4	Layer 3	VPN-ASR1001-2

WAN-D3750X

```
version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname WAN-D3750X
!
boot-start-marker
boot-end-marker
!
!
logging buffered 1000000
enable secret 5 $1$ssq/$J5zW2nln0tp6NsQDx48yK1
!
username admin password 7 121A540411045D5679
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
```

```

!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
switch 1 provision ws-c3750x-24
switch 2 provision ws-c3750x-24
stack-mac persistent timer 0
system mtu routing 1500
!
ip routing
!
!
!
ip domain-name cisco.local
ip name-server 10.4.48.10
ip multicast-routing distributed
vtp mode transparent
udld enable

!
mls qos map policed-dscp 0 10 18 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 51
52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58 59
60 61 62 63

```

```

mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19
20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29
30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51
52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59
60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!

license boot level ipservices
license boot level ipservices switch 2

```

```

!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1-4094 priority 24576
!
!
!
port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
!
macro name EgressQoS
  mls qos trust dscp
  queue-set 2
  srr-queue bandwidth share 1 30 35 5
  priority-queue out
@
!
!
interface Loopback0
  ip address 10.4.32.240 255.255.255.255
  ip pim sparse-mode
!
interface Port-channel1
  description connection to CE-ASR1002-1
  no switchport
  ip address 10.4.32.1 255.255.255.252
  ip pim sparse-mode

```

```

  logging event link-status
  carrier-delay msec 0
!
interface Port-channel2
  description connection to CE-ASR1001-2
  no switchport
  ip address 10.4.32.9 255.255.255.252
  ip pim sparse-mode
  logging event link-status
  carrier-delay msec 0
!
interface Port-channel3
  description VPN-ASR1002-1
  no switchport
  ip address 10.4.32.17 255.255.255.252
  ip pim sparse-mode
  logging event link-status
  carrier-delay msec 0
!
interface Port-channel4
  description VPN-ASR1002-1
  no switchport
  ip address 10.4.32.21 255.255.255.252
  ip pim sparse-mode
  logging event link-status
  carrier-delay msec 0
!
interface Port-channel5
  description METRO-ASR1000-1
  no switchport
  ip address 10.4.32.33 255.255.255.252
  ip pim sparse-mode
  logging event link-status
  carrier-delay msec 0
!
interface FastEthernet0
  no ip address

```

```

no ip route-cache
shutdown
!
interface GigabitEthernet1/0/1
description CE-ASR1002-1
no switchport
no ip address
logging event link-status
logging event trunk-status
logging event bundle-status
carrier-delay msec 0
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 1 mode active
!
interface GigabitEthernet1/0/2
description CE-ASR1001-2
no switchport
no ip address
logging event link-status
logging event trunk-status
logging event bundle-status
carrier-delay msec 0
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 2 mode active
!
interface GigabitEthernet1/0/3
description VPN-ASR1002-1 Gig0/0/0

```

```

no switchport
no ip address
logging event link-status
logging event trunk-status
logging event bundle-status
carrier-delay msec 0
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 3 mode active
!
interface GigabitEthernet1/0/4
description VPN-ASR1002-2 Gig0/0/0
no switchport
no ip address
logging event link-status
logging event trunk-status
logging event bundle-status
carrier-delay msec 0
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 4 mode active
!
interface GigabitEthernet1/0/6
description METRO-ASR1000-1 Gig0/0/1
no switchport
no ip address
logging event link-status
logging event trunk-status
logging event bundle-status

```

```

carrier-delay msec 0
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 5 mode on
!
interface TenGigabitEthernet1/1/1
description connection to C6509-2 Te4/6
no switchport
ip address 10.4.40.46 255.255.255.252
ip pim sparse-mode
ip summary-address eigrp 100 10.4.32.0 255.255.248.0
ip summary-address eigrp 100 10.5.0.0 255.255.0.0
logging event link-status
carrier-delay msec 0
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
!
interface GigabitEthernet2/0/1
description CE-ASR1002-1
no switchport
no ip address
logging event link-status
logging event trunk-status
logging event bundle-status
carrier-delay msec 0
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp

```

```

channel-group 1 mode active
!
interface GigabitEthernet2/0/2
description CE-ASR1001-2
no switchport
no ip address
logging event link-status
logging event trunk-status
logging event bundle-status
carrier-delay msec 0
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 2 mode active
!
interface GigabitEthernet2/0/3
description VPN-ASR1002-1 Gig0/0/1
no switchport
no ip address
logging event link-status
logging event trunk-status
logging event bundle-status
carrier-delay msec 0
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 3 mode active
!
interface GigabitEthernet2/0/4
description VPN-ASR1002-2 Gig0/0/1
no switchport

```

```

no ip address
logging event link-status
logging event trunk-status
logging event bundle-status
carrier-delay msec 0
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 4 mode active
!
interface GigabitEthernet2/0/6
description METRO-ASR1000-1 Gig0/0/0
no switchport
no ip address
logging event link-status
logging event trunk-status
logging event bundle-status
carrier-delay msec 0
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 5 mode on
!
interface TenGigabitEthernet2/1/1
description connection to C6509-1 Te4/6
no switchport
ip address 10.4.40.42 255.255.255.252
ip pim sparse-mode
ip summary-address eigrp 100 10.4.32.0 255.255.248.0
ip summary-address eigrp 100 10.5.0.0 255.255.0.0
logging event link-status
carrier-delay msec 0

srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
!
interface Vlan1
no ip address
shutdown
!
!
router eigrp 100
network 10.4.0.0 0.1.255.255
passive-interface default
no passive-interface TenGigabitEthernet2/1/1
no passive-interface TenGigabitEthernet1/1/1
no passive-interface Port-channel1
no passive-interface Port-channel2
no passive-interface Port-channel3
no passive-interface Port-channel4
no passive-interface Port-channel5
nsf
!
!
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip pim autorp listener
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
!
!
logging esm config
logging trap errors
logging 10.4.48.35

```

```

logging 10.4.48.36
access-list 55 permit 10.4.48.0 0.0.0.255
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
    address ipv4 10.4.48.15
    key 7 03375E08140A35674B10
!
!
!
line con 0
line vty 0 4
    exec-timeout 0 0
    transport preferred none
    transport input ssh
line vty 5 15
    exec-timeout 0 0
    transport preferred none
    transport input ssh
!
!
ntp source Loopback0
ntp server 10.4.48.17
end

```

VPN-ASR1002-1

```

version 15.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
no platform punt-keepalive disable-kernel-core
!
hostname VPN-ASR1002-1
!
!

```

```

vrf definition Mgmt-intf
!
    address-family ipv4
    exit-address-family
!
    address-family ipv6
    exit-address-family
!
enable secret 4 /DtCCr53Q4B18jSImlUEqu7cNVZTOhxTZyUnZdsSrs
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
    server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
!
ip vrf INET-PUBLIC
    rd 65512:1
!
!
!
ip domain name cisco.local
ip multicast-routing distributed
!

```

```

!
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
username admin password 7 110A4816141D5A5E57
!
redundancy
 mode none
!
!
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
 match dscp af21
 match ip dscp af21
class-map match-any INTERACTIVE-VIDEO
 match dscp cs4 af41
class-map match-any CRITICAL-DATA
 match dscp cs3 af31
class-map match-any VOICE
 match dscp ef
class-map match-any SCAVENGER
 match dscp cs1 af11
 match ip dscp cs1 af11
class-map match-any NETWORK-CRITICAL

```

```

 match dscp cs2 cs6
 match ip dscp cs2 cs6
 match access-group name ISAKMP
!
policy-map WAN
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-INTERFACE-G0/0/3
 class class-default
  shape average 50000000
  service-policy WAN
!
!
!
crypto keyring DMVPN-KEYRING vrf INET-PUBLIC
 pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC

```

```

keyring DMVPN-KEYRING
match identity address 0.0.0.0 INET-PUBLIC
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
mode transport
!
crypto ipsec profile DMVPN-PROFILE
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile FVRF-ISAKMP-INET-PUBLIC
!
!
!
!
!
!
interface Loopback0
ip address 10.4.32.243 255.255.255.255
ip pim sparse-mode
!
interface Port-channel3
ip address 10.4.32.18 255.255.255.252
ip pim sparse-mode
no negotiation auto
!
interface Tunnel10
bandwidth 10000
ip address 10.4.34.1 255.255.254.0
no ip redirects
ip mtu 1400
ip hello-interval eigrp 200 20
ip hold-time eigrp 200 60
no ip split-horizon eigrp 200
ip pim nbma-mode
ip pim sparse-mode

```

```

ip nhrp authentication cisco123
ip nhrp map multicast dynamic
ip nhrp network-id 101
ip nhrp holdtime 600
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel source GigabitEthernet0/0/3
tunnel mode gre multipoint
tunnel vrf INET-PUBLIC
tunnel protection ipsec profile DMVPN-PROFILE
!
interface GigabitEthernet0/0/0
description WAN-D3750X Gig1/0/3
no ip address
negotiation auto
cdp enable
channel-group 3 mode active
!
interface GigabitEthernet0/0/1
description WAN-D3750X Gig2/0/3
no ip address
negotiation auto
cdp enable
channel-group 3 mode active
!
interface GigabitEthernet0/0/2
no ip address
negotiation auto
!
interface GigabitEthernet0/0/3
ip vrf forwarding INET-PUBLIC
ip address 192.168.18.10 255.255.255.0
negotiation auto
service-policy output WAN-INTERFACE-G0/0/3
!
interface GigabitEthernet0
vrf forwarding Mgmt-intf

```

```

no ip address
shutdown
negotiation auto
!
!
router eigrp 100
network 10.4.0.0 0.1.255.255
redistribute eigrp 200 route-map SET-ROUTE-TAG-DMVPN
passive-interface default
no passive-interface Port-channel3
eigrp router-id 10.4.32.243
!
!
router eigrp 200
network 10.4.34.0 0.0.1.255
redistribute eigrp 100
passive-interface default
no passive-interface Tunnel10
eigrp router-id 10.4.32.243
!
ip forward-protocol nd
!
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip pim autorp listener
ip pim register-source Loopback0
ip route vrf INET-PUBLIC 0.0.0.0 0.0.0.0 192.168.18.1
ip tacacs source-interface Loopback0
!
ip access-list extended ISAKMP
 permit udp any eq isakmp any eq isakmp
!
logging 10.4.48.35
!
route-map SET-ROUTE-TAG-DMVPN permit 10

```

```

match interface Tunnel10
set tag 65512
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
!
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 107D0C1A17120620091D
!
!
control-plane
!
!
!
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
ntp source Loopback0
ntp server 10.4.48.17
!
end

```

VPN-ASR1001-2

```
version 15.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
no platform punt-keepalive disable-kernel-core
!
hostname VPN-ASR1001-2
!
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
enable secret 4 /DtCCr53Q4B18jSImlUEqu7cNVZTOhXTZyUnZdsSrsW
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
```

```
!
!
ip vrf INET-PUBLIC
rd 65512:2
!
!
!
no ip domain lookup
ip domain name cisco.local
ip multicast-routing distributed
!
!
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
license boot level advanenterprise
!
!
!
!
!
!
username admin password 7 03070A180500701E1D
!
redundancy
mode none
!
!
!
!
```

```

!
ip ssh source-interface Loopback0
ip ssh version 2
!
!
crypto keyring DMVPN-KEYRING vrf INET-PUBLIC
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 2
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC
  keyring DMVPN-KEYRING
  match identity address 0.0.0.0 INET-PUBLIC
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
  mode transport
!
crypto ipsec profile DMVPN-PROFILE
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC
!
!
!
!
!
!
interface Loopback0
  ip address 10.4.32.244 255.255.255.255
  ip pim sparse-mode
!
interface Port-channel4
  ip address 10.4.32.22 255.255.255.252

```

```

ip pim sparse-mode
no negotiation auto
!
interface Tunnel10
  bandwidth 10000
  ip address 10.4.36.1 255.255.254.0
  no ip redirects
  ip mtu 1400
  ip hello-interval eigrp 201 20
  ip hold-time eigrp 201 60
  no ip split-horizon eigrp 201
  ip pim nbma-mode
  ip pim sparse-mode
  ip nhrp authentication cisco123
  ip nhrp map multicast dynamic
  ip nhrp network-id 102
  ip nhrp holdtime 600
  ip nhrp redirect
  ip tcp adjust-mss 1360
  tunnel source GigabitEthernet0/0/3
  tunnel mode gre multipoint
  tunnel vrf INET-PUBLIC
  tunnel protection ipsec profile DMVPN-PROFILE
!
interface GigabitEthernet0/0/0
  description WAN-D3750X Gig1/0/4
  no ip address
  negotiation auto
  cdp enable
  channel-group 4 mode active
!
interface GigabitEthernet0/0/1
  description WAN-D3750X Gig2/0/4
  no ip address
  negotiation auto
  cdp enable
  channel-group 4 mode active

```

```

!
interface GigabitEthernet0/0/2
  no ip address
  negotiation auto
!
interface GigabitEthernet0/0/3
  ip vrf forwarding INET-PUBLIC
  ip address 192.168.18.11 255.255.255.0
  negotiation auto
!
interface GigabitEthernet0
  vrf forwarding Mgmt-intf
  no ip address
  shutdown
  negotiation auto
!
!
router eigrp 100
  network 10.4.0.0 0.1.255.255
  redistribute eigrp 201 route-map SET-ROUTE-TAG-DMVPN
  passive-interface default
  no passive-interface Port-channel4
  eigrp router-id 10.4.32.244
!
!
router eigrp 201
  network 10.4.36.0 0.0.1.255
  redistribute eigrp 100
  passive-interface default
  no passive-interface Tunnel10
  eigrp router-id 10.4.32.244
!
ip forward-protocol nd
!
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip pim autorp listener

```

```

ip pim register-source Loopback0
ip route vrf INET-PUBLIC 0.0.0.0 0.0.0.0 192.168.18.1
ip tacacs source-interface Loopback0
!
!
route-map SET-ROUTE-TAG-DMVPN permit 10
  match interface Tunnel10
  set tag 65512
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
!
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key 7 03375E08140A35674B10
!
!
control-plane
!
!
!
!
line con 0
  logging synchronous
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  transport preferred none
  transport input ssh
line vty 5 15
  transport preferred none
  transport input ssh
!
ntp source Loopback0
ntp server 10.4.48.17
!
end

```

WAN Remote-Site Devices - Dual DMVPN and DMVPN Only Design Models

This section includes configuration files corresponding to the WAN remote-site design topologies as referenced in Figure 6. Each remote-site type has its respective devices grouped together along with any other relevant configuration information.

Table 2 lists the specific details for the DMVPN WAN connections at each site.

Figure 6 - WAN remote-site designs - Dual DMVPN and DMVPN only

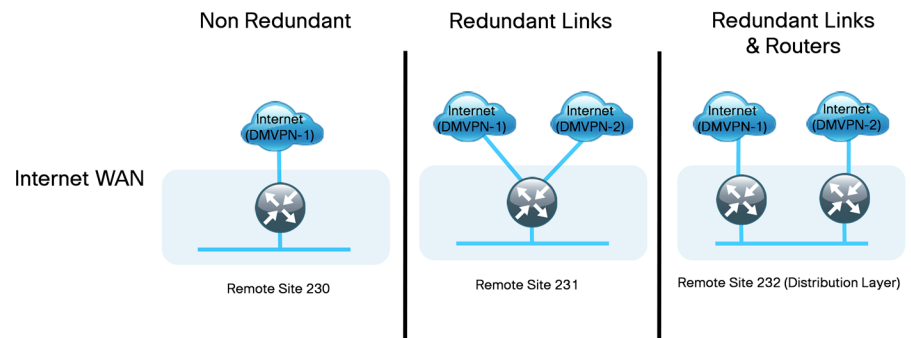


Table 2 - Remote-site WAN connection details

Remote-Site information		DMVPN	LAN interfaces	Loopbacks
Location	Net Block			
Remote site 230 (Single-router, single-link)	10.5.192.0/21	(gi0/0) DHCP	(gi0/1)	10.255.253.230 (r)
Remote site 231 (Single-router, dual-link)	10.5.200.0/21	(gi0/0) DHCP (gi0/1) DHCP	(gi0/2)	10.255.253.231 (r)
Remote site 232 (Dual-router, dual-link with distribution layer)	10.5.208.0/21	(gi0/0) DHCP (gi0/0) DHCP	(gi0/2) (gi0/2)	10.255.253.232 (r1) 10.255.254.232 (r2)

Table 3 lists the link speeds for the remote-site quality-of-service (QoS) traffic shaping policies.

Table 3 - Remote-site link speeds

Remote-Site information		Link speeds (policed rates)	
Location	Net Block	DMVPN-1	DMVPN-2
Remote site 230	10.5.192.0/21	2 Mbps	
Remote site 230 (dual-link)	10.5.200.0/21	10 Mbps	5 Mbps
Remote site 232 (dual-link)	10.5.208.0/21	10 Mbps	5 Mbps

Remote Site 230: Single-Router, Single-Link (DMVPN)

Table 4 shows the IP address information for remote site 230.

Table 4 - Remote site 230—IP address information

Remote-Site information		Wired subnets		Operational IP assignments
Location	Net Block	Data (Vlan 64)	Voice (Vlan 69)	Loopbacks and switches
Remote site 230	10.5.192.0/21	10.5.196.0/24	10.5.197.0/24	10.255.253.205 (router) 10.5.196.5 (access switch)

RS230-1941

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS230-1941
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZT0hxTZyUnZdsSrs
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
```

```
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ipv6 spd queue min-threshold 62
ipv6 spd queue max-threshold 63
ip source-route
ip cef
!
!
!
ip vrf INET-PUBLIC1
rd 65512:1
!
ip multicast-routing
!
!
ip domain name cisco.local
!
multilink bundle-name authenticated
!
license udi pid CISC01941/K9 sn FTX140980GX
license boot module c1900 technology-package datak9
!
```

```

!
username admin password 7 011057175804575D72
!
redundancy
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
  match dscp af21
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
class-map match-any CRITICAL-DATA
  match dscp cs3 af31
class-map match-any VOICE
  match dscp ef
class-map match-any SCAVENGER
  match dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match dscp cs2 cs6
  match access-group name ISAKMP
!
!
policy-map WAN
  class VOICE
    priority percent 10
  class INTERACTIVE-VIDEO
    priority percent 23
  class CRITICAL-DATA
    bandwidth percent 15
    random-detect dscp-based
  class DATA
    bandwidth percent 19
    random-detect dscp-based

```

```

class SCAVENGER
  bandwidth percent 5
class NETWORK-CRITICAL
  bandwidth percent 3
class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 2000000
    service-policy WAN
!
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 2
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
  keyring DMVPN-KEYRING1
  match identity address 0.0.0.0 INET-PUBLIC1
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
  mode transport
!
crypto ipsec profile DMVPN-PROFILE1
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
!
!
!
!
!

```

```

!
interface Loopback0
 ip address 10.255.253.230 255.255.255.255
 ip pim sparse-mode
!
interface Tunnel10
 bandwidth 2000
 ip address 10.4.34.230 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim dr-priority 0
 ip pim nbma-mode
 ip pim sparse-mode
 ip hello-interval eigrp 200 20
 ip hold-time eigrp 200 60
 ip nhrp authentication cisco123
 ip nhrp map multicast 172.16.130.1
 ip nhrp map 10.4.34.1 172.16.130.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.34.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
 ip virtual-reassembly in
 ip virtual-reassembly out
 ip tcp adjust-mss 1360
 ip summary-address eigrp 200 10.5.192.0 255.255.248.0
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC1
 tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Port-channel1
 no ip address
 hold-queue 300 in
!
interface GigabitEthernet0/0
 bandwidth 2000

```

```

 ip vrf forwarding INET-PUBLIC1
 ip address dhcp
 ip access-group ACL-INET-PUBLIC in
 duplex auto
 speed auto
 no cdp enable
 service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
 description RS230-A3560X Gig0/48
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.64
 description Wired Data
 encapsulation dot1Q 64
 ip address 10.5.196.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface GigabitEthernet0/1.69
 description Wired Voice
 encapsulation dot1Q 69
 ip address 10.5.197.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
!
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.255.253.230
 eigrp stub connected summary
!
 ip forward-protocol nd

```

```

!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
ip access-list extended ACL-INET-PUBLIC
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit esp any any
 permit udp any any eq bootpc
 permit icmp any any echo
 permit icmp any any echo-reply
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any gt 1023 ttl eq 1
ip access-list extended ISAKMP
 permit udp any eq isakmp any eq isakmp
!
logging 10.4.48.35
!
!
!
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 00371605165E1F2D0A38
!
!
!
control-plane

```

```

!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
!
end

```

Remote Site 231: Single-Router, Dual-Link (DMVPN + DMVPN)

Table 5 shows the IP address information for remote site 231.

Table 5 - Remote site 231—IP address information

Remote-Site information		Wired subnets		Operational IP assignments
Location	Net Block	Data (Vlan 64)	Voice (Vlan 69)	Loopbacks and switches
Remote site 231	10.5.200.0/21	10.5.204.0/24	10.5.205.0/24	10.255.253.231 (router) 10.5.204.5 (access switch)

RS231-2911

```
version 15.1
service config
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS231-2911
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZT0hxtZyUnZdsSrs
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
```

```
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ip source-route
ip cef
!
!
!
ip vrf INET-PUBLIC1
rd 65512:1
!
ip vrf INET-PUBLIC2
rd 65512:2
!
ip multicast-routing
ip dhcp remember
!
!
ip domain name cisco.local
!
```

```

multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!
!
!
!
license udi pid CISCO2911/K9 sn FTX1411ALG3
hw-module sm 1
!
!
!
username admin password 7 0007421507545A545C
!
redundancy
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
  match dscp af21
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
class-map match-any CRITICAL-DATA
  match dscp cs3 af31
class-map match-any VOICE
  match dscp ef

```

```

class-map match-any SCAVENGER
  match dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match dscp cs2 cs6
  match access-group name ISAKMP
!
!
policy-map WAN
  class VOICE
    priority percent 10
  class INTERACTIVE-VIDEO
    priority percent 23
  class CRITICAL-DATA
    bandwidth percent 15
    random-detect dscp-based
  class DATA
    bandwidth percent 19
    random-detect dscp-based
  class SCAVENGER
    bandwidth percent 5
  class NETWORK-CRITICAL
    bandwidth percent 3
  class class-default
    bandwidth percent 25
    random-detect
policy-map WAN-INTERFACE-G0/1
  class class-default
    shape average 5000000
    service-policy WAN
policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 10000000
    service-policy WAN
!
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123

```

```

crypto keyring DMVPN-KEYRING2 vrf INET-PUBLIC2
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 2
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
  keyring DMVPN-KEYRING1
  match identity address 0.0.0.0 INET-PUBLIC1
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC2
  keyring DMVPN-KEYRING2
  match identity address 0.0.0.0 INET-PUBLIC2
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
  mode transport
!
crypto ipsec profile DMVPN-PROFILE1
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
!
crypto ipsec profile DMVPN-PROFILE2
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC2
!
!
!
!
!
!
!
interface Loopback0
  ip address 10.255.253.231 255.255.255.255
  ip pim sparse-mode

```

```

!
interface Tunnel10
  bandwidth 10000
  ip address 10.4.34.231 255.255.254.0
  no ip redirects
  ip mtu 1400
  ip pim dr-priority 0
  ip pim nbma-mode
  ip pim sparse-mode
  ip hello-interval eigrp 200 20
  ip hold-time eigrp 200 60
  ip nhrp authentication cisco123
  ip nhrp map multicast 172.16.130.1
  ip nhrp map 10.4.34.1 172.16.130.1
  ip nhrp network-id 101
  ip nhrp holdtime 600
  ip nhrp nhs 10.4.34.1
  ip nhrp registration no-unique
  ip nhrp shortcut
  ip nhrp redirect
  ip tcp adjust-mss 1360
  ip summary-address eigrp 200 10.5.200.0 255.255.248.0
  tunnel source GigabitEthernet0/0
  tunnel mode gre multipoint
  tunnel vrf INET-PUBLIC1
  tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Tunnel11
  bandwidth 5000
  ip address 10.4.36.231 255.255.254.0
  no ip redirects
  ip mtu 1400
  ip pim dr-priority 0
  ip pim nbma-mode
  ip pim sparse-mode
  ip hello-interval eigrp 201 20
  ip hold-time eigrp 201 60

```

```

ip nhrp authentication cisco123
ip nhrp map multicast 172.17.130.1
ip nhrp map 10.4.36.1 172.17.130.1
ip nhrp network-id 102
ip nhrp holdtime 600
ip nhrp nhs 10.4.36.1
ip nhrp registration no-unique
ip nhrp shortcut
ip nhrp redirect
ip tcp adjust-mss 1360
ip summary-address eigrp 201 10.5.200.0 255.255.248.0
tunnel source GigabitEthernet0/1
tunnel mode gre multipoint
tunnel vrf INET-PUBLIC2
tunnel protection ipsec profile DMVPN-PROFILE2
!
interface GigabitEthernet0/0
bandwidth 10000
ip vrf forwarding INET-PUBLIC1
ip address dhcp
ip access-group ACL-INET-PUBLIC in
duplex auto
speed auto
no cdp enable
service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
bandwidth 5000
ip vrf forwarding INET-PUBLIC2
ip address dhcp
ip access-group ACL-INET-PUBLIC in
duplex auto
speed auto
no cdp enable
service-policy output WAN-INTERFACE-G0/1
!
interface GigabitEthernet0/2

```

```

description RS231-A2960S Gig1/0/24
duplex auto
speed auto
!
interface GigabitEthernet0/2.64
description Wired Data
encapsulation dot1Q 64
ip address 10.5.204.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
!
interface GigabitEthernet0/2.69
description Wired Voice
encapsulation dot1Q 69
ip address 10.5.205.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
!
interface Vlan1
no ip address
!
!
router eigrp 200
network 10.4.34.0 0.0.1.255
network 10.5.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel10
eigrp router-id 10.255.253.231
eigrp stub connected summary
!
!
router eigrp 201
network 10.4.36.0 0.0.1.255
network 10.5.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
passive-interface default

```

```

no passive-interface Tunnel11
eigrp router-id 10.255.253.231
eigrp stub connected summary
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
ip access-list extended ACL-INET-PUBLIC
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit esp any any
 permit udp any any eq bootpc
 permit icmp any any echo
 permit icmp any any echo-reply
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any gt 1023 ttl eq 1
class-map match-any NETWORK-CRITICAL
 match access-group name ISAKMP
!
logging 10.4.48.35
!
!
!
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15

```

```

key 7 0812494D1B1C113C1712
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 exec-timeout 0 0
 transport preferred none
 transport input ssh
line vty 5 15
 exec-timeout 0 0
 transport preferred none
 transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
!
end

```

Remote Site 232: Dual-Router, Dual-Link with Distribution Layer (DMVPN + DMVPN)

Table 6 shows the IP address information for remote site 232.

Table 6 - Remote site 232—IP address information

Remote-Site information		Wired subnets		Operational IP assignments
Location	Net Block	Data	Voice	Loopbacks and switches
Remote site 232	10.5.208.0/21	10.5.209.0/24 (Vlan 100) 10.5.211.0/24 (Vlan 102)	10.5.210.0/24 (Vlan 101) 10.5.212.0/24 (Vlan 103)	10.255.253.232 (router 1) 10.255.254.232 (router 2) 10.5.215.254 (distribution switch) 10.5.215.2 (access switch 1) 10.5.215.3 (access switch 2)

Table 7 and Table 8 provide additional information to connect to the distribution layer.

Table 7 - Remote site 232—router connections to distribution layer

Remote-Site information		Connection to distribution layer switch			Port-Channel subinterface and IP assignments		
Location	Net Block	Router	Port channel	Member interfaces	Subinterface	Vlan	Network
Remote site 232	10.5.208.0/21	RS232-2911-1	1	gi0/1 gi0/2	Port-channel1.50	50	10.5.208.0/30
					Port-channel1.99 (transit network)	99	10.5.208.8/30
		RS232-2911-2	2	gi0/1 gi0/2	Port-channel2.54	54	10.5.208.4/30
					Port-channel2.99 (transit network)	99	10.5.208.8/30

Table 8 - Remote site 232—distribution layer switch connections

Port-Channel	Member interfaces	Layer3/Layer2	Connected device
1	gi1/0/11 gi2/0/11	Trunk (Vlan50, 99)	RS232-2911-1
2	gi1/0/12 gi2/0/12	Trunk (Vlan54, 99)	RS232-2911-2
10	gi1/0/1 gi2/0/1	Layer 2 (Vlan100,101,106)	RS232-A3560X
11	gi1/0/2	Trunk (Vlan102,103,106)	RS232-A3560X-PR2

RS232-2911-1

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS232-2911-1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 /DtCCr53Q4B18jSImlUEqu7cNVZTOhXTZyUnZdsSrsW
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
    server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
!
ip source-route
ip cef
```

```
!
!
!
ip vrf INET-PUBLIC1
    rd 65512:1
!
ip multicast-routing
!
!
ip domain name cisco.local
!
multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!
!
!
!
!
license udi pid CISC02911/K9 sn FTX1420AJLB
license boot module c2900 technology-package securityk9
hw-module pvdm 0/0
!
!
!
username admin password 7 011057175804575D72
!
redundancy
!
!
!
```

```

!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
  match dscp af21
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
class-map match-any CRITICAL-DATA
  match dscp cs3 af31
class-map match-any VOICE
  match dscp ef
class-map match-any SCAVENGER
  match dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match dscp cs2 cs6
  match access-group name ISAKMP
!
!
policy-map WAN
  class VOICE
    priority percent 10
  class INTERACTIVE-VIDEO
    priority percent 23
  class CRITICAL-DATA
    bandwidth percent 15
    random-detect dscp-based
  class DATA
    bandwidth percent 19
    random-detect dscp-based
  class SCAVENGER
    bandwidth percent 5
  class NETWORK-CRITICAL
    bandwidth percent 3
  class class-default
    bandwidth percent 25
    random-detect

```

```

policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 10000000
    service-policy WAN
!
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 2
!
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
  keyring DMVPN-KEYRING1
  match identity address 0.0.0.0 INET-PUBLIC1
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
  mode transport
!
crypto ipsec profile DMVPN-PROFILE1
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
!
!
!
!
!
interface Loopback0
  ip address 10.255.253.232 255.255.255.255
  ip pim sparse-mode
!
interface Tunnel10

```

```

bandwidth 10000
ip address 10.4.34.232 255.255.254.0
no ip redirects
ip mtu 1400
ip pim dr-priority 0
ip pim nbma-mode
ip pim sparse-mode
ip hello-interval eigrp 200 20
ip hold-time eigrp 200 60
ip nhrp authentication cisco123
ip nhrp map multicast 172.16.130.1
ip nhrp map 10.4.34.1 172.16.130.1
ip nhrp network-id 101
ip nhrp holdtime 600
ip nhrp nhs 10.4.34.1
ip nhrp registration no-unique
ip nhrp shortcut
ip nhrp redirect
ip tcp adjust-mss 1360
ip summary-address eigrp 200 10.5.208.0 255.255.248.0
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel vrf INET-PUBLIC1
tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Port-channel1
description EtherChannel link to RS232-D3750X
no ip address
hold-queue 150 in
!
interface Port-channel1.50
description R1 routed link to distribution layer
encapsulation dot1Q 50
ip address 10.5.208.1 255.255.255.252
ip pim sparse-mode
!
interface Port-channel1.99

```

```

description Transit Net
encapsulation dot1Q 99
ip address 10.5.208.9 255.255.255.252
ip pim sparse-mode
!
interface GigabitEthernet0/0
description DMVPN WAN Uplink
ip vrf forwarding INET-PUBLIC1
ip address dhcp
ip access-group ACL-INET-PUBLIC in
duplex auto
speed auto
no cdp enable
service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
description LAN-1 Uplink
no ip address
duplex auto
speed auto
channel-group 1
!
interface GigabitEthernet0/2
description LAN-2 Uplink
no ip address
duplex auto
speed auto
channel-group 1
!
!
router eigrp 200
network 10.4.34.0 0.0.1.255
network 10.5.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
redistribute eigrp 100 route-map LOOPBACK-ONLY
passive-interface default
no passive-interface Tunnel10

```

```

eigrp router-id 10.255.253.232
eigrp stub connected summary redistributed
!
!
router eigrp 100
network 10.5.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
redistribute eigrp 200
passive-interface default
no passive-interface Port-channel1.50
no passive-interface Port-channel1.99
eigrp router-id 10.255.253.232
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
ip access-list standard R2-LOOPBACK
permit 10.255.254.232
!
ip access-list extended ACL-INET-PUBLIC
permit udp any any eq non500-isakmp
permit udp any any eq isakmp
permit esp any any
permit udp any any eq bootpc
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any ttl-exceeded
permit icmp any any port-unreachable
permit udp any any gt 1023 ttl eq 1

```

```

ip access-list extended ISAKMP
permit udp any eq isakmp any eq isakmp
!
logging 10.4.48.35
!
!
!
route-map LOOPBACK-ONLY permit 10
match ip address R2-LOOPBACK
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key 7 13361211190910012E3D
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
gatekeeper
shutdown
!
!
!
line con 0

```

```

logging synchronous
line aux 0
line vty 0 4
    transport preferred none
    transport input ssh
line vty 5 15
    transport preferred none
    transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
!
end

```

RS232-2911-2

```

version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS232-2911-2
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsW
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
    server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console

```

```

aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
!

ip source-route
ip cef
!
!
!
ip vrf INET-PUBLIC2
    rd 65512:2
!
ip multicast-routing
!
!
ip domain name cisco.local
!
multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!

```

```

!
!
!
!
license udi pid CISCO2911/K9 sn FTX1420AJL8
license boot module c2900 technology-package securityk9
hw-module pvdm 0/0
!
!
!
username admin password 7 04585A150C2E1D1C5A
!
redundancy
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
    match dscp af21
class-map match-any INTERACTIVE-VIDEO
    match dscp cs4 af41
class-map match-any CRITICAL-DATA
    match dscp cs3 af31
class-map match-any VOICE
    match dscp ef
class-map match-any SCAVENGER
    match dscp cs1 af11
class-map match-any NETWORK-CRITICAL
    match dscp cs2 cs6
    match access-group name ISAKMP
!
!
policy-map WAN
    class VOICE

```

```

        priority percent 10
    class INTERACTIVE-VIDEO
        priority percent 23
    class CRITICAL-DATA
        bandwidth percent 15
        random-detect dscp-based
    class DATA
        bandwidth percent 19
        random-detect dscp-based
    class SCAVENGER
        bandwidth percent 5
    class NETWORK-CRITICAL
        bandwidth percent 3
        class class-default
        bandwidth percent 25
        random-detect
policy-map WAN-INTERFACE-G0/0
    class class-default
        shape average 5000000
        service-policy WAN
!
!
crypto keyring DMVPN-KEYRING2 vrf INET-PUBLIC2
    pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
    encr aes 256
    authentication pre-share
    group 2
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC2
    keyring DMVPN-KEYRING2
    match identity address 0.0.0.0 INET-PUBLIC2
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-  

sha-hmac

```

```

mode transport
!
crypto ipsec profile DMVPN-PROFILE2
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC2
!
!
!
!
!
interface Loopback0
  ip address 10.255.254.232 255.255.255.255
  ip pim sparse-mode
!
interface Tunnel11
  bandwidth 5000
  ip address 10.4.36.232 255.255.254.0
  no ip redirects
  ip mtu 1400
  ip pim dr-priority 0
  ip pim nbma-mode
  ip pim sparse-mode
  ip hello-interval eigrp 201 20
  ip hold-time eigrp 201 60
  ip nhrp authentication cisco123
  ip nhrp map multicast 172.17.130.1
  ip nhrp map 10.4.36.1 172.17.130.1
  ip nhrp network-id 102
  ip nhrp holdtime 600
  ip nhrp nhs 10.4.36.1
  ip nhrp registration no-unique
  ip nhrp shortcut
  ip nhrp redirect
  ip tcp adjust-mss 1360
  ip summary-address eigrp 201 10.5.208.0 255.255.248.0
  tunnel source GigabitEthernet0/0

```

```

tunnel mode gre multipoint
tunnel vrf INET-PUBLIC2
tunnel protection ipsec profile DMVPN-PROFILE2
!
interface Port-channel2
  description EtherChannel link to RS232-D3750X
  no ip address
  hold-queue 150 in
!
interface Port-channel2.54
  description R2 routed link to distribution layer
  encapsulation dot1Q 54
  ip address 10.5.208.5 255.255.255.252
  ip pim sparse-mode
!
interface Port-channel2.99
  description Transit net
  encapsulation dot1Q 99
  ip address 10.5.208.10 255.255.255.252
  ip pim sparse-mode
!
interface GigabitEthernet0/0
  description DMVPN WAN Uplink
  ip vrf forwarding INET-PUBLIC2
  ip address dhcp
  duplex auto
  speed auto
  service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
  description LAN-1 Uplink
  no ip address
  duplex auto
  speed auto
  channel-group 2
!
interface GigabitEthernet0/2

```

```

description LAN-2 Uplink
no ip address
duplex auto
speed auto
channel-group 2
!
!
router eigrp 201
 network 10.4.36.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 passive-interface default
 no passive-interface Tunnel11
 eigrp router-id 10.255.254.232
 eigrp stub connected summary redistributed
!
!
router eigrp 100
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 201
 passive-interface default
 no passive-interface Port-channel2.54
 no passive-interface Port-channel2.99
 eigrp router-id 10.255.254.232
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0

```

```

!
ip access-list standard R1-LOOPBACK
 permit 10.255.253.232
!
ip access-list extended ACL-INET-PUBLIC
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit esp any any
 permit udp any any eq bootpc
 permit icmp any any echo
 permit icmp any any echo-reply
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any gt 1023 ttl eq 1
ip access-list extended ISAKMP
 permit udp any eq isakmp any eq isakmp
!
logging 10.4.48.35
!
!
!
!
route-map LOOPBACK-ONLY permit 10
 match ip address R1-LOOPBACK
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 107D0C1A17120620091D
!
!
!
control-plane
!

```

```

!
!
mgcp profile default
!
!
!
!
!
gatekeeper
    shutdown
!
!
!
line con 0
    logging synchronous
line aux 0
line vty 0 4
    transport preferred none
    transport input ssh
line vty 5 15
    transport preferred none
    transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
!
end

```

RS232-D3750X

```

version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS232-D3750X
!
boot-start-marker
boot-end-marker
!
!
logging buffered 1000000
enable secret 5 $1$cKuX$kbkjDnW.LpKWshlt9zitp1
!
username admin password 7 04585A150C2E1D1C5A
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
    server name TACACS-SERVER-1
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization exec default group tacacs+ local
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
switch 1 provision ws-c3750x-12s
switch 2 provision ws-c3750x-12s
stack-mac persistent timer 0

```

```

system mtu routing 1500
ip routing
!
!
!
ip domain-name cisco.local
ip name-server 10.4.48.10
ip multicast-routing distributed
vtp mode transparent
udld enable

!
mls qos map policed-dscp 0 10 18 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 51
52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58 59
60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47

```

```

mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19
20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29
30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51
52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59
60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1-4094 priority 24576
!
!
!
port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!

```

```

vlan 50
  name R1-link
!
vlan 54
  name R2-link
!
vlan 99
  name Transit-net
!
vlan 100
  name DataVLAN1
!
vlan 101
  name VoiceVLAN1
!
vlan 102
  name DataVLAN2
!
vlan 103
  name VoiceVLAN2
!
vlan 106
  name Management
!
vlan 999
  name NativeVLAN
!
ip ssh source-interface Loopback0
ip ssh version 2
!
!
!
!
macro name EgressQoS
  mls qos trust dscp
  queue-set 2
  srr-queue bandwidth share 1 30 35 5

```

```

priority-queue out
@
!
!
interface Loopback0
  ip address 10.5.215.254 255.255.255.255
  ip pim sparse-mode
!
interface Port-channel1
  description EtherChannel link to RS232-2911-1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 50,99
  switchport mode trunk
  ip arp inspection trust
  spanning-tree portfast trunk
  ip dhcp snooping trust
!
interface Port-channel2
  description EtherChannel link to RS232-2911-2
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 54,99
  switchport mode trunk
  ip arp inspection trust
  spanning-tree portfast trunk
  ip dhcp snooping trust
!
interface Port-channel10
  description EtherChannel link to RS232-A3560X
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 999
  switchport trunk allowed vlan 100,101,106
  switchport mode trunk
  logging event link-status
!
interface Port-channel11
  description EtherChannel link to RS232-A3560X-PR2
  switchport trunk encapsulation dot1q

```

```

switchport trunk native vlan 999
switchport trunk allowed vlan 102,103,106
switchport mode trunk
logging event link-status
!
interface FastEthernet0
no ip address
no ip route-cache
shutdown
!
interface GigabitEthernet1/0/1
description RS232-A3560X Gig1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 100,101,106
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 10 mode active
!
interface GigabitEthernet1/0/2
description RS232-A3560X-PR2 Gig1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 102,103,106
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5

```

```

queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 11 mode active
!
interface GigabitEthernet1/0/11
description Link to RS232-2911-1 Gig0/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 50,99
switchport mode trunk
ip arp inspection trust
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 1 mode on
ip dhcp snooping trust
!
interface GigabitEthernet1/0/12
description Link to RS232-2911-2 G0/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 54,99
switchport mode trunk
ip arp inspection trust
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp

```

```

macro description EgressQoS
channel-group 2 mode on
ip dhcp snooping trust
!
interface GigabitEthernet2/0/1
description RS232-A3560X Gig1/2
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 100,101,106
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 10 mode active
!
interface GigabitEthernet2/0/2
description RS232-A3560X-PR2 Gig1/3
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 102,103,106
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 11 mode active

```

```

!
interface GigabitEthernet2/0/11
description Link to RS232-2911-1 Gig0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 50,99
switchport mode trunk
ip arp inspection trust
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 1 mode on
ip dhcp snooping trust
!
interface GigabitEthernet2/0/12
description Link to RS232-2911-2 G0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 54,99
switchport mode trunk
ip arp inspection trust
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 2 mode on
ip dhcp snooping trust
!
interface Vlan1
no ip address

```

```

shutdown
!
interface Vlan50
 ip address 10.5.208.2 255.255.255.252
 ip pim sparse-mode
!
interface Vlan54
 ip address 10.5.208.6 255.255.255.252
 ip pim sparse-mode
!
interface Vlan100
 ip address 10.5.209.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface Vlan101
 ip address 10.5.210.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface Vlan102
 ip address 10.5.211.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface Vlan103
 ip address 10.5.212.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface Vlan106
 ip address 10.5.215.1 255.255.255.128
 ip pim sparse-mode
!
!
router eigrp 100
 network 10.4.0.0 0.1.255.255
 passive-interface default
 no passive-interface Vlan50

```

```

no passive-interface Vlan54
eigrp router-id 10.5.215.254
!
!
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip pim autorp listener
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
!
ip sla responder
logging esm config
logging 10.4.48.35
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 06350A225E4B1D32000E
!
!
line con 0
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
ntp source Loopback0
ntp server 10.4.48.17
!
end

```

WAN Remote-Site Devices - DMVPN Backup Dedicated Design Model (MPLS)

This section includes configuration files corresponding to the WAN remote-site design topologies as referenced in Figure 7. Each remote-site type has its respective devices grouped together along with any other relevant configuration information.

Figure 7 - WAN remote-site designs - DMVPN Backup Dedicated (MPLS primary)

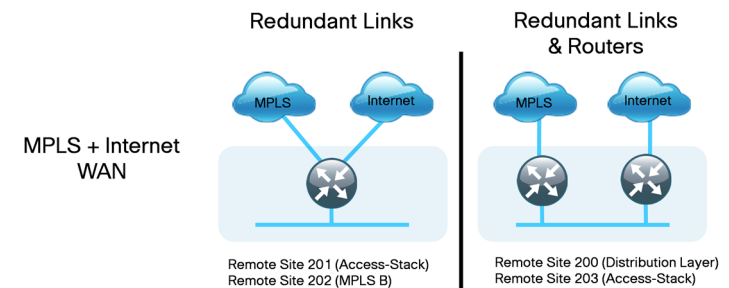


Table 9 lists the specific details for the MPLS and DMVPN WAN connections at each site.

Table 9 - Remote-site WAN connection details - (MPLS + DMVPN remote sites)

Remote-Site		MPLS (Our AS = 65511)			DMVPN	LAN interfaces	Loopbacks
Location	Net Block	MPLS CE	MPLS PE	Carrier AS			
Remote site 200 (Dual-router, dual-link with distribution layer)	10.5.0.0/21	(gi0/0) 192.168.3.17	192.168.3.18	65401 (A)	(gi0/0) DHCP	(gi0/1, gi0/2) (gi0/1, gi0/2)	10.255.251.200 (r1) 10.255.253.200 (r2)
Remote site 201 (Single-router, dual-link with access-layer stack)	10.5.40.0/21	(gi0/0) 192.168.3.21	192.168.3.22	65401 (A)	(gi0/0) DHCP	(gi0/1, gi0/2)	10.255.251.201 (r)
Remote site 202 (Single-router, dual-link)	10.5.64.0/21	(gi0/0) 192.168.4.5	192.168.4.6	65402 (B)	(gi0/1) DHCP	(gi0/2)	10.255.252.202 (r)
Remote site 203 (Dual-router, dual-link with access-layer stack)	10.5.48.0/21	(gi0/0) 192.168.3.25	192.168.3.26	65401 (A)	(gi0/0) DHCP	(gi0/1, gi0/2) (gi0/1, gi0/2)	10.255.251.203 (r1) 10.255.253.203 (r2)

Table 10 lists the link speeds for the remote-site QoS traffic shaping policies.

Table 10 - Remote-site link speeds

Remote-Site information		Link speeds (policed rates)	
Location	Net Block	MPLS	DMVPN
Remote site 200	10.5.0.0/21	50 Mbps	25 Mbps
Remote site 201	10.5.40.0/21	10 Mbps	10 Mbps
Remote site 202	10.5.64.0/21	10 Mbps	10 Mbps
Remote site 203	10.5.48.0/21	20 Mbps	10 Mbps

Remote Site 200: Dual-Router, Dual-Link with Distribution Layer (MPLS + DMVPN)

Table 11 shows the IP address information for remote site 200.

Table 11 - Remote site 200—IP address information

Remote-Site information		Wired subnets		Operational IP assignments
Location	Net Block	Data	Voice	Loopbacks and switches
Remote site 200	10.5.0.0/21	10.5.1.0/24 (Vlan100) 10.5.3.0/24 (Vlan 102)	10.5.2.0/24 (Vlan 101) 10.5.4.0/24 (Vlan 103)	10.255.251.200 (router 1) 10.255.253.200 (router 2) 10.5.7.254 (distribution switch) 10.5.7.2 (access switch 1) 10.5.7.3 (access switch 2)

Table 12 and Table 13 provide additional information to connect to the distribution layer.

Table 12 - Remote site 200—router connections to distribution layer

Remote-Site information		Connection to distribution layer switch			Port-Channel subinterface and IP assignments		
Location	Net Block	Router	Port channel	Member interfaces	Subinterface	Vlan	Network
Remote site 200	10.5.0.0/21	RS200-3925-1	1	gi0/1 gi0/2	Port-channel1.50	50	10.5.0.0/30
					Port-channel1.99 (transit network)	99	10.5.0.8/30
		RS200-3925-2	2	gi0/1 gi0/2	Port-channel2.54	54	10.5.0.4/30
					Port-channel2.99 (transit network)	99	10.5.0.8/30

Table 13 - Remote site 200—distribution layer switch connections

Port-Channel	Member interfaces	Layer3/Layer2 trunk	Connected device
1	gi1/0/11 gi2/0/11	Trunk (Vlan50, 99)	RS200-3925-1
2	gi1/0/12 gi2/0/12	Trunk (Vlan54, 99)	RS200-3925-2
10	gi1/0/1 gi2/0/1	Layer 2 (Vlan100,101,106)	RS200-A3750X
11	gi1/0/2	Layer 2 (Vlan102,103,106)	RS200-A3750X-PR1

RS200-3925-1

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS200-3925-1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 /DtCCr53Q4B18jSImlUEqu7cNVZTOhXTZyUnZdsSrsW
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
    server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ipv6 spd queue min-threshold 62
ipv6 spd queue max-threshold 63
!
```

```
!
ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
ip domain name cisco.local
!
multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!
!
!
!
!
license udi pid C3900-SPE100/K9 sn FOC14415C5Q
hw-module sm 2
!
!
!
username admin password 7 070C705F4D06485744
!
redundancy
!
!
!
!
```

```

ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
  match dscp af21
class-map match-any BGP-ROUTING
  match protocol bgp
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
class-map match-any CRITICAL-DATA
  match dscp cs3 af31
class-map match-any VOICE
  match dscp ef
class-map match-any SCAVENGER
  match dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match dscp cs2 cs6
!
!
policy-map MARK-BGP
  class BGP-ROUTING
    set dscp cs6
policy-map WAN
  class VOICE
    priority percent 10
  class INTERACTIVE-VIDEO
    priority percent 23
  class CRITICAL-DATA
    bandwidth percent 15
    random-detect dscp-based
  class DATA
    bandwidth percent 19
    random-detect dscp-based
  class SCAVENGER
    bandwidth percent 5
  class NETWORK-CRITICAL
    bandwidth percent 3

```

```

  service-policy MARK-BGP
class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 25000000
    service-policy WAN
!
!
!
!
!
interface Loopback0
  ip address 10.255.251.200 255.255.255.255
  ip pim sparse-mode
!
interface Port-channel1
  description EtherChannel link to RS200-D3750X
  no ip address
  hold-queue 150 in
!
interface Port-channel1.50
  description R1 routed link to distribution layer
  encapsulation dot1Q 50
  ip address 10.5.0.1 255.255.255.252
  ip pim sparse-mode
!
interface Port-channel1.99
  description Transit net
  encapsulation dot1Q 99
  ip address 10.5.0.9 255.255.255.252
  ip pim sparse-mode
!
interface GigabitEthernet0/0
  bandwidth 50000
  ip address 192.168.3.17 255.255.255.252

```

```

duplex auto
speed auto
no cdp enable
service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
description RS200-D3750X Gig2/0/23
no ip address
duplex auto
speed auto
channel-group 1
!
interface GigabitEthernet0/2
description RS200-D3750X Gig1/0/23
no ip address
duplex auto
speed auto
channel-group 1
!
interface Vlan1
no ip address
!
!
router eigrp 100
default-metric 25000 100 255 1 1500
network 10.5.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
redistribute bgp 65511
passive-interface default
no passive-interface Port-channel1.50
no passive-interface Port-channel1.99
eigrp router-id 10.255.251.200
!
router bgp 65511
bgp router-id 10.255.251.200
bgp log-neighbor-changes

```

```

network 10.5.1.0 mask 255.255.255.0
network 10.5.3.0 mask 255.255.255.0
network 10.255.251.200 mask 255.255.255.255
network 10.255.253.200 mask 255.255.255.255
network 192.168.3.16 mask 255.255.255.252
aggregate-address 10.5.0.0 255.255.248.0 summary-only
neighbor 192.168.3.18 remote-as 65401
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
!
logging 10.4.48.35
!
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key 7 04680E051D2458650C00
!
!

```

```

!
control-plane
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
  shutdown
!
!
!
line con 0
  logging synchronous
line aux 0
line vty 0 4
  transport preferred none
  transport input ssh
line vty 5 15
  transport preferred none
  transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
end

```

RS200-3925-2

```

version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS200-3925-2
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZT0hxTZyUnZdsSrs
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ipv6 spd queue min-threshold 62
ipv6 spd queue max-threshold 63
!
!

```

```

ip source-route
ip cef
!
!
!
ip vrf INET-PUBLIC1
  rd 65512:1
!
ip multicast-routing
!
!
ip domain name cisco.local
!
multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!
!
!
!
!
license udi pid C3900-SPE100/K9 sn FOC133932KA
!
!
username admin password 7 094F1F1A1A0A464058
!
redundancy
!
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2

```

```

!
class-map match-any DATA
  match dscp af21
class-map match-any BGP-ROUTING
  match protocol bgp
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
class-map match-any CRITICAL-DATA
  match dscp cs3 af31
class-map match-any VOICE
  match dscp ef
class-map match-any SCAVENGER
  match dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match dscp cs2 cs6
  match access-group name ISAKMP
!
!
policy-map WAN
  class VOICE
    priority percent 10
  class INTERACTIVE-VIDEO
    priority percent 23
  class CRITICAL-DATA
    bandwidth percent 15
    random-detect dscp-based
  class DATA
    bandwidth percent 19
    random-detect dscp-based
  class SCAVENGER
    bandwidth percent 5
  class NETWORK-CRITICAL
    bandwidth percent 3
  class class-default
    bandwidth percent 25
    random-detect
policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 25000000

```

```

    service-policy WAN
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
    pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
    encr aes 256
    authentication pre-share
    group 2
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
    keyring DMVPN-KEYRING1
    match identity address 0.0.0.0 INET-PUBLIC1
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
    mode transport
!
crypto ipsec profile DMVPN-PROFILE1
    set transform-set AES256/SHA/TRANSPORT
    set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
!
!
!
!
!
!
interface Loopback0
    ip address 10.255.253.200 255.255.255.255
    ip pim sparse-mode
!
interface Tunnel10
    bandwidth 25000
    ip address 10.4.34.200 255.255.254.0
    no ip redirects
    ip mtu 1400
    ip pim dr-priority 0
    ip pim nbma-mode

```

```

ip pim sparse-mode
ip hello-interval eigrp 200 20
ip hold-time eigrp 200 60
ip nhrp authentication cisco123
ip nhrp map 10.4.34.1 172.16.130.1
ip nhrp map multicast 172.16.130.1
ip nhrp network-id 101
ip nhrp holdtime 600
ip nhrp nhs 10.4.34.1
ip nhrp registration no-unique
ip nhrp shortcut
ip nhrp redirect
ip tcp adjust-mss 1360
ip summary-address eigrp 200 10.5.0.0 255.255.248.0
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel vrf INET-PUBLIC1
tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Port-channel2
    description EtherChannel link to RS200-D3750X
    no ip address
    hold-queue 150 in
!
interface Port-channel2.54
    description R2 routed link to RS200-D3750X
    encapsulation dot1Q 54
    ip address 10.5.0.5 255.255.255.252
    ip pim sparse-mode
!
interface Port-channel2.99
    description Transit net
    encapsulation dot1Q 99
    ip address 10.5.0.10 255.255.255.252
    ip pim sparse-mode
!
interface GigabitEthernet0/0
    ip vrf forwarding INET-PUBLIC1
    ip address dhcp

```

```

ip access-group ACL-INET-PUBLIC in
duplex auto
speed auto
no cdp enable
service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
description RS200-D3750X Gig2/0/24
no ip address
duplex auto
speed auto
channel-group 2
!
interface GigabitEthernet0/2
description RS200-D3750X Gig1/0/24
no ip address
duplex auto
speed auto
channel-group 2
!
!
router eigrp 200
network 10.4.34.0 0.0.1.255
network 10.5.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
redistribute eigrp 100 route-map LOOPBACK-ONLY
passive-interface default
no passive-interface Tunnel10
eigrp router-id 10.255.253.200
eigrp stub connected summary redistributed
!
!
router eigrp 100
network 10.5.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
redistribute eigrp 200
passive-interface default
no passive-interface Port-channel2.54
no passive-interface Port-channel2.99

```

```

eigrp router-id 10.255.253.200
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
ip access-list standard R1-LOOPBACK
permit 10.255.251.200
!
ip access-list extended ACL-INET-PUBLIC
permit udp any any eq non500-isakmp
permit udp any any eq isakmp
permit esp any any
permit udp any any eq bootpc
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any ttl-exceeded
permit icmp any any port-unreachable
permit udp any any gt 1023 ttl eq 1
ip access-list extended ISAKMP
permit udp any eq isakmp any eq isakmp
!
logging 10.4.48.35
!
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
route-map LOOPBACK-ONLY permit 10
match ip address R1-LOOPBACK
!

```

```

!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key 7 0538030C33495A221C1C
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
  shutdown
!
!
!
line con 0
  logging synchronous
line aux 0
line vty 0 4
  transport preferred none
  transport input ssh
line vty 5 15
  transport preferred none
  transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
end

```

RS200-D3750X

```

version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS200-D3750X
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$x0JT$FtmnsQGSNhDjO.siJKuJg0
!
username admin password 7 130646010803557878
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
switch 1 provision ws-c3750x-24s
switch 2 provision ws-c3750x-24s
stack-mac persistent timer 0
system mtu routing 1500
!

```

```

!
ip routing
!
!
!
ip domain-name cisco.local
ip name-server 10.4.48.10
ip multicast-routing distributed
vtp mode transparent
udld enable
!
mls qos map policed-dscp 0 10 18 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 51
52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58 59
60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19
20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29

```

```

30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51
52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59
60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
!
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1-4094 priority 24576
!
!
!
port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!
vlan 50
    name R1-link
!
vlan 54
    name R2-link
!
vlan 99

```

```

name Transit-net
!
vlan 100
  name DataVLAN1
!
vlan 101
  name VoiceVLAN1
!
vlan 102
  name DataVLAN2
!
vlan 103
  name VoiceVLAN2
!
vlan 106
  name Management
!
vlan 999
  name NATIVE
!
ip ssh source-interface Loopback0
ip ssh version 2
!
!
!
!
!
macro name EgressQoS
  mls qos trust dscp
  queue-set 2
  srr-queue bandwidth share 1 30 35 5
  priority-queue out
@
!
!
interface Loopback0
  ip address 10.5.7.254 255.255.255.255
  ip pim sparse-mode
!

```

```

interface Port-channel1
  description EtherChannel link to RS200-3925-1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 50,99
  switchport mode trunk
  ip arp inspection trust
  spanning-tree portfast trunk
  ip dhcp snooping trust
!
interface Port-channel2
  description EtherChannel link to RS200-3925-2
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 54,99
  switchport mode trunk
  ip arp inspection trust
  spanning-tree portfast trunk
  ip dhcp snooping trust
!
interface Port-channel10
  description EtherChannel link to RS200-A3750X
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 999
  switchport trunk allowed vlan 100,101,106
  switchport mode trunk
  logging event link-status
!
interface Port-channel11
  description EtherChannel link to RS200-A3750X-PR1
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 999
  switchport trunk allowed vlan 102,103,106
  switchport mode trunk
  logging event link-status
!
interface FastEthernet0
  no ip address
  no ip route-cache
  shutdown
!

```

```

interface GigabitEthernet1/0/1
description RS200-A3750X Gig2/1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 100,101,106
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 10 mode active
!
interface GigabitEthernet1/0/2
description RS200-A3750X-PR1 Gig1/1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 102,103,106
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 11 mode active
service-policy type performance-monitor input PerfMon-Baseline
!
interface GigabitEthernet1/0/23
description Link to RS200-3925-1 Gig0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 50,99

```

```

switchport mode trunk
ip arp inspection trust
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 1 mode on
ip dhcp snooping trust
!
interface GigabitEthernet1/0/24
description Link to RS200-3925-2 Gig0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 54,99
switchport mode trunk
ip arp inspection trust
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 2 mode on
ip dhcp snooping trust
!
interface GigabitEthernet2/0/1
description RS200-A3750X Gig1/1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 100,101,106
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status

```

```

srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 10 mode active
!
interface GigabitEthernet2/0/2
description **RS200-A3750X-PR1 Gig1/1/2**
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 102,103,106
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 11 mode active
!
interface GigabitEthernet2/0/23
description Link to RS200-3925-1 Gig0/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 50,99
switchport mode trunk
ip arp inspection trust
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS

```

```

channel-group 1 mode on
ip dhcp snooping trust
!
interface GigabitEthernet2/0/24
description Link to RS200-3925-2 Gig0/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 54,99
switchport mode trunk
ip arp inspection trust
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 2 mode on
ip dhcp snooping trust
!
interface Vlan1
no ip address
shutdown
!
interface Vlan50
ip address 10.5.0.2 255.255.255.252
ip pim sparse-mode
!
interface Vlan54
ip address 10.5.0.6 255.255.255.252
ip pim sparse-mode
!
interface Vlan100
description Wired Data 1
ip address 10.5.1.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
!
interface Vlan101

```

```

description Wired Voice 1
ip address 10.5.2.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
!
interface Vlan102
description Wired Data 2
ip address 10.5.3.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
!
interface Vlan103
description Wired Voice 2
ip address 10.5.4.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
!
interface Vlan106
description Management
ip address 10.5.7.1 255.255.255.128
ip pim sparse-mode
!
!
router eigrp 100
network 10.5.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
passive-interface default
no passive-interface Vlan50
no passive-interface Vlan54
eigrp router-id 10.5.7.254
nsf
!
!
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip pim autorp listener

```

```

ip pim register-source Loopback0
ip tacacs source-interface Loopback0
!
ip sla responder
logging esm config
logging 10.4.48.35
access-list 55 permit 10.4.48.0 0.0.0.255
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key 7 06350A225E4B1D32000E
!
!
line con 0
line vty 0 4
transport preferred none
transport input ssh
line vty 5 15
transport preferred none
transport input ssh
!
ntp source Loopback0
ntp server 10.4.48.17
end

```

Remote Site 201: Single-Router, Dual-Link with Access-Layer Stack (MPLS + DMVPN)

Table 14 shows the IP address information for remote site 201.

Table 14 - Remote site 201—IP address information

Remote-Site information		Wired subnets		Operational IP assignments
Location	Net Block	Data (Vlan 64)	Vlan (Vlan 69)	Loopbacks and switches
Remote site 201	10.5.40.0/21	10.5.44.0/24	10.5.45.0/24	10.255.251.201 (router) 10.5.44.5 (access-switch)

RS201-2911

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS201-2911
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$Rmfp$Btut/0xCUYD0mlruhEsPt1
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
```

```
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ipv6 spd queue min-threshold 62
ipv6 spd queue max-threshold 63
!
ip source-route
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
ip cef
!
!
!
ip vrf INET-PUBLIC1
rd 65512:1
!
ip multicast-routing
!
!
ip domain name cisco.local
ip name-server 10.4.48.10
!
```

```

multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!
!
!
!
license udi pid CISCO2911/K9 sn FTX1347A1TN
license boot module c2900 technology-package datak9
hw-module sm 1
!
!
!
!
username admin password 7 04585A150C2E1D1C5A
!
redundancy
!
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
    match dscp af21
class-map match-any BGP-ROUTING
    match protocol bgp
class-map match-any INTERACTIVE-VIDEO
    match dscp cs4 af41
class-map match-any CRITICAL-DATA

```

```

    match dscp cs3 af31
class-map match-any VOICE
    match dscp ef
class-map match-any SCAVENGER
    match dscp cs1 af11
class-map match-any NETWORK-CRITICAL
    match dscp cs2 cs6
    match access-group name ISAKMP
!
!
policy-map MARK-BGP
    class BGP-ROUTING
        set dscp cs6
policy-map WAN
    class VOICE
        priority percent 10
    class INTERACTIVE-VIDEO
        priority percent 23
    class CRITICAL-DATA
        bandwidth percent 15
        random-detect dscp-based
    class DATA
        bandwidth percent 19
        random-detect dscp-based
    class SCAVENGER
        bandwidth percent 5
    class NETWORK-CRITICAL
        bandwidth percent 3
        service-policy MARK-BGP
    class class-default
        bandwidth percent 25
        random-detect
policy-map WAN-INTERFACE-G0/0/0
    class class-default
        shape average 10000000
    service-policy WAN
policy-map WAN-INTERFACE-G0/0

```

```

class class-default
  shape average 10000000
  service-policy WAN
!
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 2
!
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
  keyring DMVPN-KEYRING1
  match identity address 0.0.0.0 INET-PUBLIC1
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
  mode transport
!
crypto ipsec profile DMVPN-PROFILE1
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
!
!
!
!
interface Loopback0
  ip address 10.255.251.201 255.255.255.255
  ip pim sparse-mode
!
interface Tunnel10
  bandwidth 10000
  ip address 10.4.34.201 255.255.254.0

```

```

no ip redirects
ip mtu 1400
ip pim dr-priority 0
ip pim nbma-mode
ip pim sparse-mode
ip hello-interval eigrp 200 20
ip hold-time eigrp 200 60
ip nhrp authentication cisco123
ip nhrp map multicast 172.16.130.1
ip nhrp map 10.4.34.1 172.16.130.1
ip nhrp network-id 101
ip nhrp holdtime 600
ip nhrp nhs 10.4.34.1
ip nhrp registration no-unique
ip nhrp shortcut
ip nhrp redirect
ip tcp adjust-mss 1360
ip summary-address eigrp 200 10.5.40.0 255.255.248.0
tunnel source GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel vrf INET-PUBLIC1
tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Port-channel1
  description EtherChannel link to RS201-A2960S
  no ip address
  hold-queue 150 in
!
interface Port-channel1.64
  description Wired Data
  encapsulation dot1Q 64
  ip address 10.5.44.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
!
interface Port-channel1.69
  description Wired Voice

```

```

encapsulation dot1Q 69
ip address 10.5.45.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
!
interface GigabitEthernet0/0
bandwidth 10000
ip address 192.168.3.21 255.255.255.252
duplex auto
speed auto
no cdp enable
service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
description RS201-A2960S Gig2/0/24
no ip address
duplex auto
speed auto
channel-group 1
!
interface GigabitEthernet0/2
description RS201-A2960S Gig1/0/24
no ip address
duplex auto
speed auto
channel-group 1
!
interface GigabitEthernet0/0/0
ip vrf forwarding INET-PUBLIC1
ip address dhcp
ip access-group ACL-INET-PUBLIC in
duplex auto
speed auto
no cdp enable
service-policy output WAN-INTERFACE-G0/0/0
!
interface Vlan1

```

```

no ip address
!
!
!
router eigrp 200
network 10.4.34.0 0.0.1.255
network 10.5.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel10
eigrp router-id 10.255.251.201
eigrp stub connected summary
!
router bgp 65511
bgp router-id 10.255.251.201
bgp log-neighbor-changes
network 10.5.44.0 mask 255.255.255.0
network 10.5.45.0 mask 255.255.255.0
network 10.255.251.201 mask 255.255.255.255
network 192.168.3.20 mask 255.255.255.252
aggregate-address 10.5.40.0 255.255.248.0 summary-only
neighbor 192.168.3.22 remote-as 65401
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
ip access-list extended ACL-INET-PUBLIC
permit udp any any eq non500-isakmp
permit udp any any eq isakmp

```

```

permit esp any any
permit udp any any eq bootpc
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any ttl-exceeded
permit icmp any any port-unreachable
permit udp any any gt 1023 ttl eq 1
ip access-list extended ISAKMP
permit udp any eq isakmp any eq isakmpip sla responder
!
logging 10.4.48.35
access-list 55 permit 10.4.48.0 0.0.0.255
!
!
!
!
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key 7 0538030C33495A221C1C
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper

```

```

shutdown
!
!
!
line con 0
logging synchronous
line aux 0
line vty 0 4
access-class 55 in
transport preferred none
transport input ssh
line vty 5 15
access-class 55 in
transport preferred none
transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
!
end

```

Remote Site 202: Single-Router, Dual-Link (MPLS + DMVPN)

Table 15 shows the IP address information for remote site 202.

Table 15 - Remote site 202—IP address information

Remote-Site information		Wired subnets		Operational IP assignments
Location	Net Block	Data (Vlan 64)	Vlan (Vlan 69)	Loopbacks and switches
Remote site 202	10.5.64.0/21	10.5.68.0/24	10.5.69.0/24	10.255.252.202 (r) 10.5.68.5 (sw)

RS202-2911

```
version 15.1
service config
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS202-2911
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsW
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
```

```
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ip source-route
ip cef
!
!
!
ip vrf INET-PUBLIC1
rd 65512:1
!
ip multicast-routing
!
!
ip domain name cisco.local
!
multilink bundle-name authenticated
!
!
!
!
```

```

!
voice-card 0
!
!
!
!
!
!
license udi pid CISCO2911/K9 sn FTX1347A1TC
!
!
username admin password 7 0205554808095E731F
!
redundancy
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
  match dscp af21
class-map match-any BGP-ROUTING
  match protocol bgp
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
class-map match-any CRITICAL-DATA
  match dscp cs3 af31
class-map match-any VOICE
  match dscp ef
class-map match-any SCAVENGER
  match dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match dscp cs2 cs6
  match access-group name ISAKMP

```

```

!
!
policy-map MARK-BGP
  class BGP-ROUTING
    set dscp cs6
policy-map WAN
  class VOICE
    priority percent 10
  class INTERACTIVE-VIDEO
    priority percent 23
  class CRITICAL-DATA
    bandwidth percent 15
    random-detect dscp-based
  class DATA
    bandwidth percent 19
    random-detect dscp-based
  class SCAVENGER
    bandwidth percent 5
  class NETWORK-CRITICAL
    bandwidth percent 3
    service-policy MARK-BGP
  class class-default
    bandwidth percent 25
    random-detect
policy-map WAN-INTERFACE-G0/1
  class class-default
    shape average 10000000
  service-policy WAN
policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 10000000
  service-policy WAN
!
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!

```

```

crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 2
!
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
  keyring DMVPN-KEYRING1
  match identity address 0.0.0.0 INET-PUBLIC1
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
  mode transport
!
crypto ipsec profile DMVPN-PROFILE1
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
!
!
!
!
!
interface Loopback0
  ip address 10.255.252.202 255.255.255.255
  ip pim sparse-mode
!
interface Tunnel10
  bandwidth 10000
  ip address 10.4.34.202 255.255.254.0
  no ip redirects
  ip mtu 1400
  ip pim dr-priority 0
  ip pim nbma-mode
  ip pim sparse-mode
  ip hello-interval eigrp 200 20
  ip hold-time eigrp 200 60

```

```

ip nhrp authentication cisco123
ip nhrp map multicast 172.16.130.1
ip nhrp map 10.4.34.1 172.16.130.1
ip nhrp network-id 101
ip nhrp holdtime 600
ip nhrp nhs 10.4.34.1
ip nhrp registration no-unique
ip nhrp shortcut
ip nhrp redirect
ip tcp adjust-mss 1360
ip summary-address eigrp 200 10.5.64.0 255.255.248.0
tunnel source GigabitEthernet0/1
tunnel mode gre multipoint
tunnel vrf INET-PUBLIC1
tunnel protection ipsec profile DMVPN-PROFILE1
!
interface GigabitEthernet0/0
  bandwidth 10000
  ip address 192.168.4.5 255.255.255.252
  duplex auto
  speed auto
  no cdp enable
  service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
  ip vrf forwarding INET-PUBLIC1
  ip address dhcp
  ip access-group ACL-INET-PUBLIC in
  duplex auto
  speed auto
  no cdp enable
  service-policy output WAN-INTERFACE-G0/1
!
interface GigabitEthernet0/2
  no ip address
  duplex auto
  speed auto

```

```

!
interface GigabitEthernet0/2.64
  description Wired Data
  encapsulation dot1Q 64
  ip address 10.5.68.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
!
interface GigabitEthernet0/2.69
  description Wired Voice
  encapsulation dot1Q 69
  ip address 10.5.69.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
!
!
router eigrp 200
  network 10.4.34.0 0.0.1.255
  network 10.5.0.0 0.0.255.255
  network 10.255.0.0 0.0.255.255
  passive-interface default
  no passive-interface Tunnel10
  eigrp router-id 10.255.252.202
  eigrp stub connected summary
!
router bgp 65511
  bgp router-id 10.255.252.202
  bgp log-neighbor-changes
  network 10.5.68.0 mask 255.255.255.0
  network 10.5.69.0 mask 255.255.255.0
  network 10.255.252.202 mask 255.255.255.255
  network 192.168.4.4 mask 255.255.255.252
  aggregate-address 10.5.64.0 255.255.248.0 summary-only
  neighbor 192.168.4.6 remote-as 65402
!
ip forward-protocol nd
!

```

```

ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
ip access-list extended ACL-INET-PUBLIC
  permit udp any any eq non500-isakmp
  permit udp any any eq isakmp
  permit esp any any
  permit udp any any eq bootpc
  permit icmp any any echo
  permit icmp any any echo-reply
  permit icmp any any ttl-exceeded
  permit icmp any any port-unreachable
  permit udp any any gt 1023 ttl eq 1
ip access-list extended ISAKMP
  permit udp any eq isakmp any eq isakmp
!
logging 10.4.48.35
!
!
!
!
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key 7 122A0014000E182F2F32
!
!
!
!

```

```
control-plane
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
  shutdown
!
!
!
line con 0
  logging synchronous
line aux 0
line vty 0 4
  transport preferred none
  transport input ssh
line vty 5 15
  transport preferred none
  transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
!
End
```

Notes

Remote Site 203: Dual-Router, Dual-Link with Access Layer Stack (MPLS + DMVPN)

Table 16 shows the IP address information for remote site 203.

Table 16 - Remote site 203—IP address information

Remote-Site information		Wired subnets		Operational IP assignments
Location	Net Block	Data (Vlan 64)	Vlan (Vlan 69)	Loopbacks and switches
Remote site 203	10.5.48.0/21	10.5.52.0/24	10.5.53.0/24	10.255.251.203 (router 1) 10.255.253.203 (router 2) 10.5.52.5 (sw)

RS203-2921-1

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS203-2921-1
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$pj0/$nqa8fNoI84ek9xadTFdVw.
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
```

```
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ipv6 spd queue min-threshold 62
ipv6 spd queue max-threshold 63
ip source-route
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
ip cef
!
!
!
ip multicast-routing
!
!
ip domain name cisco.local
!
multilink bundle-name authenticated
!
!
!
```

```

!
voice-card 0
!
!
!
!
!
!
!
license udi pid CISCO2921/K9 sn FTX1446AKCZ
license boot module c2900 technology-package securityk9
hw-module sm 1
!
!
!
username admin password 7 0508571C22431F5B4A
!
redundancy
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
track 50 ip sla 100 reachability
!
class-map match-any DATA
  match dscp af21
class-map match-any BGP-ROUTING
  match protocol bgp
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
class-map match-any CRITICAL-DATA
  match dscp cs3 af31
class-map match-any VOICE
  match dscp ef

```

```

class-map match-any SCAVENGER
  match dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match dscp cs2 cs6
!
!
policy-map MARK-BGP
  class BGP-ROUTING
    set dscp cs6
policy-map WAN
  class VOICE
    priority percent 10
  class INTERACTIVE-VIDEO
    priority percent 23
  class CRITICAL-DATA
    bandwidth percent 15
    random-detect dscp-based
  class DATA
    bandwidth percent 19
    random-detect dscp-based
  class SCAVENGER
    bandwidth percent 5
  class NETWORK-CRITICAL
    bandwidth percent 3
    service-policy MARK-BGP
  class class-default
    bandwidth percent 25
    random-detect
policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 20000000
    service-policy WAN
!
!
!
!
!

```

```

!
interface Loopback0
 ip address 10.255.251.203 255.255.255.255
 ip pim sparse-mode
!
interface Port-channel1
 description EtherChannel link to RS203-A3750X
 no ip address
 hold-queue 150 in
!
interface Port-channel1.64
 description Wired Data
 encapsulation dot1Q 64
 ip address 10.5.52.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.52.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string 7 130646010803557878
 standby 1 track 50 decrement 10
!
interface Port-channel1.69
 description Wired Voice
 encapsulation dot1Q 69
 ip address 10.5.53.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.53.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string 7 141443180F0B7B7977
 standby 1 track 50 decrement 10
!
interface Port-channel1.99

```

```

 encapsulation dot1Q 99
 ip address 10.5.48.1 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet0/0
 bandwidth 20000
 ip address 192.168.3.25 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 no cdp enable
 service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
 description RS203-A3750X Gig1/0/23
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface GigabitEthernet0/2
 description RS203-A3750X Gig2/0/23
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
!
interface Vlan1
 no ip address
!
!
router eigrp 100
 default-metric 20000 100 255 1 1500
 network 10.4.0.0 0.1.255.255
 network 10.255.0.0 0.0.255.255
 redistribute bgp 65511
 passive-interface default
 no passive-interface Port-channel1.99

```

```

eigrp router-id 10.255.251.203
!
router bgp 65511
  bgp router-id 10.255.251.203
  bgp log-neighbor-changes
  network 10.5.52.0 mask 255.255.255.0
  network 10.5.53.0 mask 255.255.255.0
  network 10.255.251.203 mask 255.255.255.255
  network 10.255.253.203 mask 255.255.255.255
  network 192.168.3.24 mask 255.255.255.252
  aggregate-address 10.5.48.0 255.255.248.0 summary-only
  neighbor 192.168.3.26 remote-as 65401
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
!
ip sla 100
  icmp-echo 192.168.3.26 source-interface GigabitEthernet0/0
  threshold 1000
  timeout 1000
  frequency 15
ip sla schedule 100 life forever start-time now
logging 10.4.48.35
!
!
!
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW

```

```

snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key 7 03375E08140A35674B10
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
!
gatekeeper
  shutdown
!
!
!
line con 0
  logging synchronous
line aux 0
line vty 0 4
  transport preferred none
  transport input ssh
line vty 5 15
  transport preferred none
  transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
!
end

```

RS203-2921-2

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS203-2921-2
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 /DtCCr53Q4B18jSImlUEqu7cNVZTOhXTZyUnZdsSrsW
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
    server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ip source-route
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
```

```
ip cef
!
!
!
ip vrf INET-PUBLIC1
    rd 65512:1
!
ip multicast-routing
!
!
ip domain name cisco.local
!
multilink bundle-name authenticated
!
!
!
!
voice-card 0
!
!
!
!
!
!
!
license udi pid CISC02921/K9 sn FTX1348AHMM
hw-module sm 1
!
!
!
username admin password 7 0508571C22431F5B4A
!
redundancy
!
!
!
!
```

```

ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
  match dscp af21
class-map match-any BGP-ROUTING
  match protocol bgp
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
class-map match-any CRITICAL-DATA
  match dscp cs3 af31
class-map match-any VOICE
  match dscp ef
class-map match-any SCAVENGER
  match dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match dscp cs2 cs6
  match access-group name ISAKMP
!
!
policy-map WAN
  class VOICE
    priority percent 10
  class INTERACTIVE-VIDEO
    priority percent 23
  class CRITICAL-DATA
    bandwidth percent 15
    random-detect dscp-based
  class DATA
    bandwidth percent 19
    random-detect dscp-based
  class SCAVENGER
    bandwidth percent 5
  class NETWORK-CRITICAL
    bandwidth percent 3
  class class-default
    bandwidth percent 25

```

```

    random-detect
policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 10000000
    service-policy WAN
!
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 2
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
  keyring DMVPN-KEYRING1
  match identity address 0.0.0.0 INET-PUBLIC1
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
  mode transport
!
crypto ipsec profile DMVPN-PROFILE1
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
!
!
!
!
!
!
interface Loopback0
  ip address 10.255.253.203 255.255.255.255
  ip pim sparse-mode
!

```

```

interface Tunnel10
 bandwidth 10000
 ip address 10.4.34.203 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim dr-priority 0
 ip pim nbma-mode
 ip pim sparse-mode
 ip hello-interval eigrp 200 20
 ip hold-time eigrp 200 60
 ip nhrp authentication cisco123
 ip nhrp map multicast 172.16.130.1
 ip nhrp map 10.4.34.1 172.16.130.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.34.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
 ip tcp adjust-mss 1360
 ip summary-address eigrp 200 10.5.48.0 255.255.248.0
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC1
 tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Port-channel2
 description EtherChannel link to RS203-A3750X
 no ip address
 hold-queue 150 in
!
interface Port-channel2.64
 description Wired Data
 encapsulation dot1Q 64
 ip address 10.5.52.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105

interface Port-channel2.69
 description Wired Voice
 encapsulation dot1Q 69
 ip address 10.5.53.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.52.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string 7 130646010803557878
!
interface Port-channel2.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.48.2 255.255.255.252
!
interface GigabitEthernet0/0
 ip vrf forwarding INET-PUBLIC1
 ip address dhcp
 ip access-group ACL-INET-PUBLIC in
 duplex auto
 speed auto
 no cdp enable
 service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
 description RS203-A3750X Gig2/0/24
 no ip address
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.53.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string 7 130646010803557878
!

```

```

duplex auto
speed auto
channel-group 2
!
interface GigabitEthernet0/2
description RS203-A3750X Gig1/0/24
no ip address
duplex auto
speed auto
channel-group 2
!
!
interface Vlan1
no ip address
!
!
router eigrp 200
network 10.4.34.0 0.0.1.255
network 10.5.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
redistribute eigrp 100 route-map LOOPBACK-ONLY
passive-interface default
no passive-interface Tunnel10
eigrp router-id 10.255.253.203
eigrp stub connected summary redistributed
!
!
router eigrp 100
network 10.4.0.0 0.1.255.255
network 10.255.0.0 0.0.255.255
redistribute eigrp 200
passive-interface default
no passive-interface Port-channel2.99
eigrp router-id 10.255.253.203
!
ip forward-protocol nd
!

```

```

ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
ip access-list standard R1-LOOPBACK
permit 10.255.251.203
!
ip access-list extended ACL-INET-PUBLIC
permit udp any any eq non500-isakmp
permit udp any any eq isakmp
permit esp any any
permit udp any any eq bootpc
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any ttl-exceeded
permit icmp any any port-unreachable
permit udp any any gt 1023 ttl eq 1
ip access-list extended ISAKMP
permit udp any eq isakmp any eq isakmp
!
logging 10.4.48.35
!
!
!
!
route-map LOOPBACK-ONLY permit 10
match ip address R1-LOOPBACK
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0

```

```
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key 7 107D0C1A17120620091D
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
  shutdown
!
!
!
line con 0
  logging synchronous
line aux 0
line vty 0 4
  transport preferred none
  transport input ssh
line vty 5 15
  transport preferred none
  transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
!
end
```

Notes

WAN Remote-Site Devices - DMVPN Backup Dedicated Design Model (Layer 2 WAN)

This section includes configuration files corresponding to the WAN remote-site design topologies as referenced in Figure 8. Each remote-site type has its respective devices grouped together along with any other relevant configuration information.

Figure 8 - WAN remote-site designs - DMVPN Backup Dedicated (Layer 2 Primary)

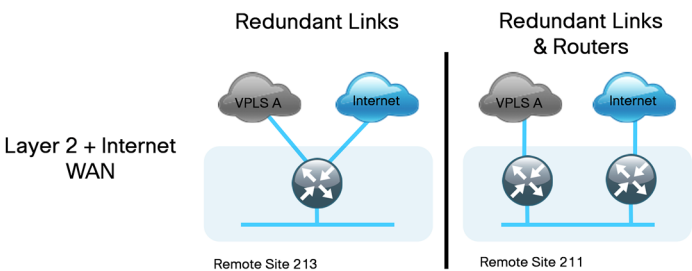


Table 17 lists the specific details for the Layer 2 WAN and DMVPN WAN connections at each site.

Table 17 - Remote-site WAN connection details - (Layer 2 WAN + DMVPN remote sites)

Remote-Site		Layer 2 WAN (EIGRP 300)			DMVPN	LAN interfaces	Loopbacks
Location	Net Block	(WAN interface) address/mask	Vlan	WAN aggregation router			
Remote site 211 (Dual-router, dual-link)	10.5.152.0/21	(gi0/0.38) 10.4.38.211/24	38	10.4.38.1	(gi0/0) DHCP	(gi0/2) (gi0/2)	10.255.255.211 (r1) 10.255.253.211 (r2)
Remote site 213 (Single-router, dual-link)	10.5.176.0/21	(gi0/0.39) 10.4.39.213/24	39	10.4.39.1	(gi0/0) DHCP	(gi0/2)	10.255.255.213 (r)

Table 18 lists the link speeds for the remote-site QoS traffic shaping policies.

Table 18 - Remote-site link speeds

Remote-Site information		Link speeds (policed rates)	
Location	Net Block	Layer 2 WAN	DMVPN
Remote site 211	10.5.152.0/21	10 Mbps	5 Mbps
Remote site 213	10.5.176.0/21	20 Mbps	10 Mbps

Remote Site 211: Dual-Router, Dual-Link (Layer 2 WAN + DMVPN)

Table 19 shows the IP address information for remote site 211.

Table 19 - Remote site 211—IP address information

Remote-Site information		Wired subnets		Operational IP assignments
Location	Net Block	Data (Vlan 64)	Voice (Vlan 69)	Loopbacks and switches
Remote site 211	10.5.152.0/21	10.5.156.0/24	10.5.157.0/24	10.255.255.211 (router 1) 10.255.253.211 (router 2) 10.5.156.5 (access switch)

RS211-2921-1

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS211-2921-1
!
boot-start-marker
boot-end-marker
!
!
card type t1 0 0
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZT0hxtZyUnZdsSrs
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
```

```
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
network-clock-participate wic 0
!
no ipv6 cef
ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
ip domain name cisco.local
!
multilink bundle-name authenticated
!
!
!
!
voice-card 0
```

```

dspfarm
dsp services dspfarm
!
!
!
!
!
license udi pid CISCO2911/K9 sn FTX1418AM08
hw-module pvdm 0/0
!
!
!
username admin password 7 121A540411045D5679
!
redundancy
!
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
track 50 ip sla 100 reachability
!
class-map match-any DATA
  match dscp af21
class-map match-any BGP-ROUTING
  match protocol bgp
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
class-map match-any CRITICAL-DATA
  match dscp cs3 af31
class-map match-any VOICE
  match dscp ef
class-map match-any SCAVENGER
  match dscp cs1 af11

```

```

class-map match-any NETWORK-CRITICAL
  match dscp cs2 cs6
!
!
policy-map WAN
  class VOICE
    priority percent 10
  class INTERACTIVE-VIDEO
    priority percent 23
  class CRITICAL-DATA
    bandwidth percent 15
    random-detect dscp-based
  class DATA
    bandwidth percent 19
    random-detect dscp-based
  class SCAVENGER
    bandwidth percent 5
  class NETWORK-CRITICAL
    bandwidth percent 3
  class class-default
    bandwidth percent 25
    random-detect
policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 10000000
    service-policy WAN
!
!
!
!
!
interface Loopback0
  ip address 10.255.255.211 255.255.255.255
  ip pim sparse-mode
!
interface GigabitEthernet0/0
  bandwidth 20000

```

```

no ip address
duplex auto
speed auto
no cdp enable
service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/0.38
 encapsulation dot1Q 38
 ip address 10.4.38.211 255.255.255.0
 ip pim sparse-mode
 ip summary-address eigrp 300 10.5.152.0 255.255.248.0
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 description RS211-A2960S Gig1/0/24
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/2.64
 description Wired Data
 encapsulation dot1Q 64
 ip address 10.5.156.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.156.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string 7 0007421507545A545C
 standby 1 track 50 decrement 10

```

```

!
interface GigabitEthernet0/2.69
 encapsulation dot1Q 69
 ip address 10.5.157.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.157.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string 7 04585A150C2E1D1C5A
 standby 1 track 50 decrement 10
!
interface GigabitEthernet0/2.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.152.1 255.255.255.252
 ip pim sparse-mode
!
!
router eigrp 300
 network 10.4.38.0 0.0.0.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 passive-interface default
 no passive-interface GigabitEthernet0/0.38
 eigrp router-id 10.255.255.211
 eigrp stub connected summary redistributed
!
!
router eigrp 100
 network 10.4.0.0 0.1.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 300
 passive-interface default

```

```

no passive-interface GigabitEthernet0/2.99
eigrp router-id 10.255.255.211
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
ip access-list standard R2-LOOPBACK
permit 10.255.253.211
!
ip sla 100
icmp-echo 10.4.38.1 source-interface GigabitEthernet0/0.38
threshold 1000
timeout 1000
frequency 15
ip sla schedule 100 life forever start-time now
logging 10.4.48.35
!
!
!
route-map LOOPBACK-ONLY permit 10
match ip address R2-LOOPBACK
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15

```

```

key 7 122A0014000E182F2F32
!
!
!
control-plane
!
!
!
!
!
gatekeeper
shutdown
!
!
!
!
line con 0
logging synchronous
line aux 0
line vty 0 4
transport preferred none
transport input ssh
line vty 5 15
transport preferred none
transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
!
end

```

RS211-2921-2

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS211-2921-2
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 /DtCCr53Q4B18jSImlUEqu7cNVZTOhXTZyUnZdsSrsW
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
    server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ip source-route
ip cef
!
```

```
!
!
ip vrf INET-PUBLIC1
    rd 65512:1
!
!
!
ip domain name cisco.local
!
multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!
!
!
license udi pid CISCO2911/K9 sn FTX1420AJLC
hw-module pvdm 0/0
!
!
!
username admin password 7 141443180F0B7B7977
!
redundancy
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
    match dscp af21
```

```

class-map match-any BGP-ROUTING
  match protocol bgp
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
class-map match-any CRITICAL-DATA
  match dscp cs3 af31
class-map match-any VOICE
  match dscp ef
class-map match-any SCAVENGER
  match dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match dscp cs2 cs6
  match access-group name ISAKMP
!
!
policy-map WAN
  class VOICE
    priority percent 10
  class INTERACTIVE-VIDEO
    priority percent 23
  class CRITICAL-DATA
    bandwidth percent 15
    random-detect dscp-based
  class DATA
    bandwidth percent 19
    random-detect dscp-based
  class SCAVENGER
    bandwidth percent 5
  class NETWORK-CRITICAL
    bandwidth percent 3
  class class-default
    bandwidth percent 25
    random-detect
policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 10000000
    service-policy WAN

```

```

!
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 2
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
  keyring DMVPN-KEYRING1
  match identity address 0.0.0.0 INET-PUBLIC1
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
  mode transport
!
crypto ipsec profile DMVPN-PROFILE1
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
!
!
!
!
!
!
interface Loopback0
  ip address 10.255.253.211 255.255.255.255
  ip pim sparse-mode
!
interface Tunnel10
  bandwidth 10000
  ip address 10.4.34.211 255.255.254.0
  no ip redirects
  ip mtu 1400

```

```

ip pim dr-priority 0
ip pim nbma-mode
ip pim sparse-mode
ip hello-interval eigrp 200 20
ip hold-time eigrp 200 60
ip nhrp authentication cisco123
ip nhrp map 10.4.34.1 172.16.130.1
ip nhrp map multicast 172.16.130.1
ip nhrp network-id 101
ip nhrp holdtime 600
ip nhrp nhs 10.4.34.1
ip nhrp registration no-unique
ip nhrp shortcut
ip nhrp redirect
ip tcp adjust-mss 1360
ip summary-address eigrp 200 10.5.152.0 255.255.248.0
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel vrf INET-PUBLIC1
tunnel protection ipsec profile DMVPN-PROFILE1
!
interface GigabitEthernet0/0
ip vrf forwarding INET-PUBLIC1
ip address dhcp
ip access-group ACL-INET-PUBLIC in
duplex auto
speed auto
no cdp enable
service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/2

```

```

description RS211-A2960S Gig1/0/23
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/2.64
description Wired Data
encapsulation dot1Q 64
ip address 10.5.156.3 255.255.255.0
ip helper-address 10.4.48.10
ip wccp 61 redirect in
ip pim dr-priority 105
ip pim sparse-mode
standby version 2
standby 1 ip 10.5.156.1
standby 1 priority 105
standby 1 preempt
standby 1 authentication md5 key-string 7 104D580A061843595F
!
interface GigabitEthernet0/2.69
description Wired Voice
encapsulation dot1Q 69
ip address 10.5.157.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 105
ip pim sparse-mode
standby version 2
standby 1 ip 10.5.157.1
standby 1 priority 105
standby 1 preempt
standby 1 authentication md5 key-string 7 08221D5D0A16544541
!
interface GigabitEthernet0/2.99
description Transit Net
encapsulation dot1Q 99
ip address 10.5.152.2 255.255.255.252
!

```

```

!
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.255.253.211
 eigrp stub connected summary redistributed
!
!
router eigrp 100
 network 10.4.0.0 0.1.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 200
 passive-interface default
 no passive-interface GigabitEthernet0/2.99
 eigrp router-id 10.255.253.211
!
ip forward-protocol nd
!
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
ip access-list standard R1-LOOPBACK
 permit 10.255.255.211
!
ip access-list extended ACL-INET-PUBLIC
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit esp any any

```

```

 permit udp any any eq bootpc
 permit icmp any any echo
 permit icmp any any echo-reply
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any gt 1023 ttl eq 1
ip access-list extended ISAKMP
 permit udp any eq isakmp any eq isakmp
!
logging 10.4.48.35
!
!
!
!
route-map LOOPBACK-ONLY permit 10
 match ip address R1-LOOPBACK
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 15210E0F162F3F0F2D2A
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
!
gatekeeper
 shutdown

```

```
!  
!  
!  
line con 0  
  logging synchronous  
line aux 0  
line vty 0 4  
  transport preferred none  
  transport input ssh  
line vty 5 15  
  transport preferred none  
  transport input ssh  
!  
scheduler allocate 20000 1000  
ntp source Loopback0  
ntp server 10.4.48.17  
!  
end
```

Notes

Remote site 213: Single-Router, Dual-Link (Layer 2 WAN + DMVPN)

Table 20 shows the IP address information for remote site 213.

Table 20 - Remote site 213—IP address information

Remote-Site information		Wired subnets		Operational IP assignments
Location	Net Block	Data (Vlan 64)	Voice (Vlan 69)	Loopbacks and switches
Remote site 213	10.5.176.0/21	10.5.180.0/24	10.5.181.0/24	10.255.255.213 (router) 10.5.180.5 (access switch)

RS213-2911

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS213-2911
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$EZVQ$SdWFvRIIMCDGtrW5l5P7b1
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
```

```
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
!
!
ip source-route
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
ip cef
!
!
!
ip vrf INET-PUBLIC1
 rd 65512:1
!
ip multicast-routing
ip dhcp remember
!
!
no ip domain lookup
ip domain name cisco.local
!
```

```

multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!
!
!
!
!
license udi pid CISCO2911/K9 sn FTX1420AJL9
license boot module c2900 technology-package securityk9
hw-module pvdm 0/0
!
!
!
username admin password 7 08221D5D0A16544541
!
redundancy
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
    match dscp af21
class-map match-any INTERACTIVE-VIDEO
    match dscp cs4 af41
class-map match-any CRITICAL-DATA
    match dscp cs3 af31
class-map match-any VOICE

```

```

    match dscp ef
class-map match-any SCAVENGER
    match dscp cs1 af11
class-map match-any NETWORK-CRITICAL
    match dscp cs2 cs6
    match access-group name ISAKMP
!
!
policy-map WAN
    class VOICE
        priority percent 10
    class INTERACTIVE-VIDEO
        priority percent 23
    class CRITICAL-DATA
        bandwidth percent 15
        random-detect dscp-based
    class DATA
        bandwidth percent 19
        random-detect dscp-based
    class SCAVENGER
        bandwidth percent 5
    class NETWORK-CRITICAL
        bandwidth percent 3
    class class-default
        bandwidth percent 25
        random-detect
policy-map WAN-INTERFACE-G0/1
    class class-default
        shape average 10000000
    service-policy WAN
policy-map WAN-INTERFACE-G0/0
    class class-default
        shape average 20000000
    service-policy WAN
!
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1

```

```

pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 2
!
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
  keyring DMVPN-KEYRING1
  match identity address 0.0.0.0 INET-PUBLIC1
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
mode transport
!
crypto ipsec profile DMVPN-PROFILE1
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
!
!
!
!
!
interface Loopback0
  ip address 10.255.255.213 255.255.255.255
  ip pim sparse-mode
!
interface Tunnel10
  bandwidth 10000
  ip address 10.4.34.213 255.255.254.0
  no ip redirects
  ip mtu 1400
  ip pim dr-priority 0
  ip pim nbma-mode
  ip pim sparse-mode

```

```

ip hello-interval eigrp 200 20
ip hold-time eigrp 200 60
ip nhrp authentication cisco123
ip nhrp map multicast 172.16.130.1
ip nhrp map 10.4.34.1 172.16.130.1
ip nhrp network-id 101
ip nhrp holdtime 600
ip nhrp nhs 10.4.34.1
ip nhrp registration no-unique
ip nhrp shortcut
ip nhrp redirect
ip tcp adjust-mss 1360
ip summary-address eigrp 200 10.5.176.0 255.255.248.0
tunnel source GigabitEthernet0/1
tunnel mode gre multipoint
tunnel vrf INET-PUBLIC1
tunnel protection ipsec profile DMVPN-PROFILE1
!
interface GigabitEthernet0/0
  bandwidth 20000
  no ip address
  duplex auto
  speed auto
  no cdp enable
  service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/0.39
  encapsulation dot1Q 39
  ip address 10.4.39.213 255.255.255.0
  ip pim sparse-mode
  ip summary-address eigrp 300 10.5.176.0 255.255.248.0
!
interface GigabitEthernet0/1
  description Internet WAN Uplink
  bandwidth 10000
  ip vrf forwarding INET-PUBLIC1
  ip address dhcp

```

```

ip access-group ACL-INET-PUBLIC in
duplex auto
speed auto
no cdp enable
service-policy output WAN-INTERFACE-G0/1
!
interface GigabitEthernet0/2
description RS213-3560X Gig0/24
ip address 10.5.176.129 255.255.255.248
duplex auto
speed auto
!
interface GigabitEthernet0/2.64
description Wired Data
encapsulation dot1Q 64
ip address 10.5.180.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
!
interface GigabitEthernet0/2.69
description Wired Voice
encapsulation dot1Q 69
ip address 10.5.181.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
!
!
router eigrp 300
network 10.4.39.0 0.0.0.255
network 10.5.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
passive-interface default
no passive-interface GigabitEthernet0/0.39
eigrp router-id 10.255.255.213
eigrp stub connected summary
!
!

```

```

router eigrp 200
network 10.4.34.0 0.0.1.255
network 10.5.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel10
eigrp router-id 10.255.255.213
eigrp stub connected summary
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
!
ip access-list extended ACL-INET-PUBLIC
permit udp any any eq non500-isakmp
permit udp any any eq isakmp
permit esp any any
permit udp any any eq bootpc
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any ttl-exceeded
permit icmp any any port-unreachable
permit udp any any gt 1023 ttl eq 1
ip access-list extended ISAKMP
permit udp any eq isakmp any eq isakmp
!
logging 10.4.48.35
!
!

```

```

!
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
    address ipv4 10.4.48.15
    key 7 15210E0F162F3F0F2D2A
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
    shutdown
!
!
!
line con 0
    logging synchronous
line aux 0
line vty 0 4
    exec-timeout 0 0
    transport preferred none
    transport input ssh
line vty 5 15
    exec-timeout 0 0
    transport preferred none

```

```

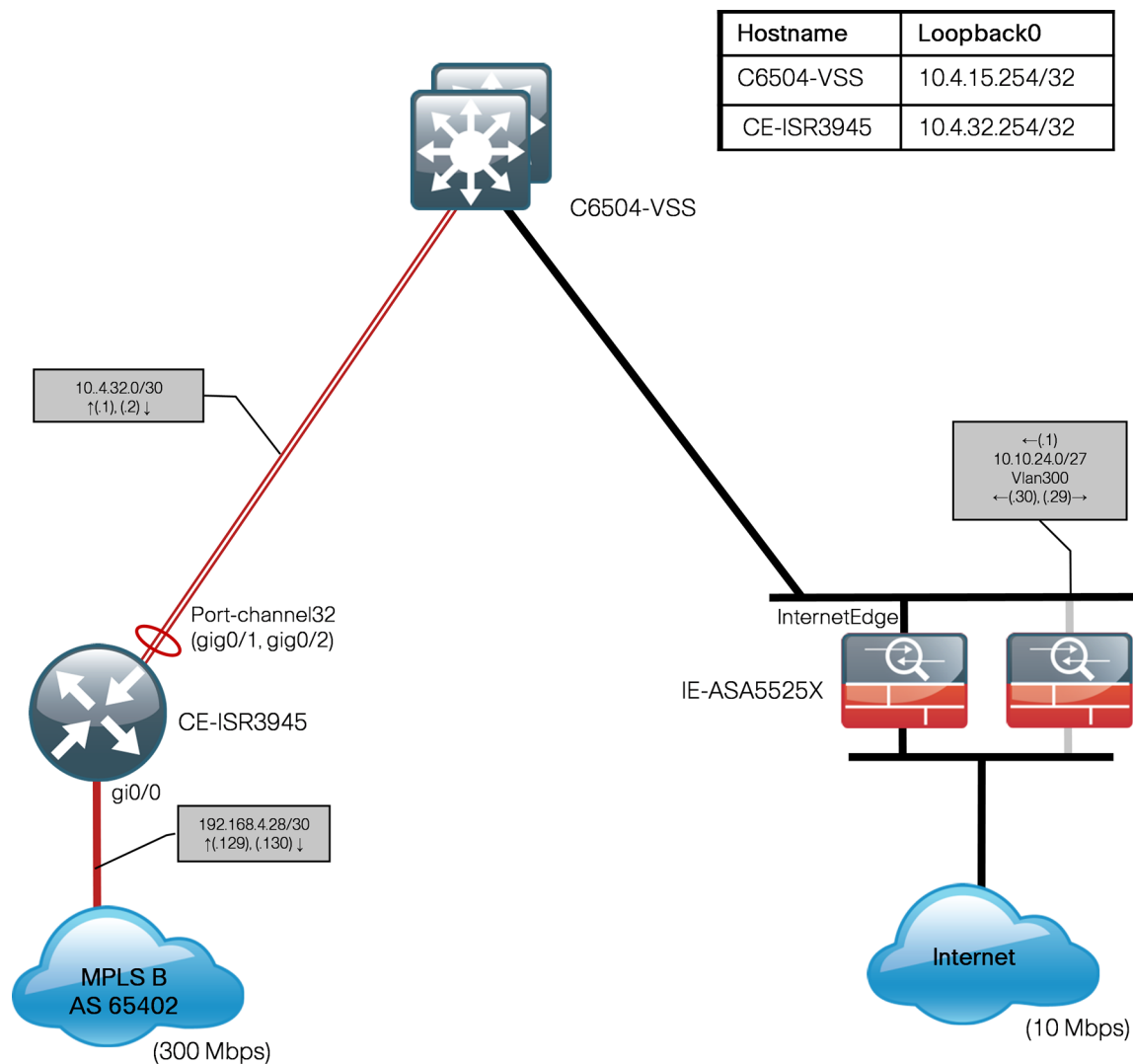
    transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
!
end

```

WAN-Aggregation Devices – DMVPN Backup Shared Design Model

This section includes configuration files corresponding to the DMVPN Backup Shared design model as referenced in Figure 9.

Figure 9 - WAN-aggregation design—DMVPN Backup Shared



CE-ISR3945

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname CE-ISR3945
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$65Nt$Q8DJB/6aNGP5lgpo6CCkA.
!
aaa new-model
!
!
!
!
!
!
!
aaa session-id common
!
!
!
clock timezone PST -8
clock summer-time PDT recurring
!
!
no ipv6 cef
ip source-route
ip cef
!
!
ip multicast-routing
!
!
```

```
ip domain name cisco.local
!
multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!
!
!
!
license udi pid C3900-SPE150/K9 sn FOC133037KH
!
!
!
username admin password 7 04585A150C2E1D1C5A
!
redundancy
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
crypto keyring DMVPN-KEYRING
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 2
crypto isakmp profile ISAKMP-PROFILE
keyring DMVPN-KEYRING
match identity address 0.0.0.0
```

```

!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
mode transport
!
crypto ipsec profile DMVPN-PROFILE
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile ISAKMP-PROFILE
!
!
!
!
!
!
interface Loopback0
ip address 10.4.32.254 255.255.255.255
ip pim sparse-mode
!
!
interface Tunnel10
bandwidth 10000
ip address 10.4.34.1 255.255.255.0
no ip redirects
ip mtu 1400
ip pim nbma-mode
ip pim sparse-mode
ip hello-interval eigrp 200 20
ip hold-time eigrp 200 60
ip nhrp authentication cisco123
ip nhrp map multicast dynamic
ip nhrp network-id 101
ip nhrp holdtime 600
ip nhrp redirect
ip tcp adjust-mss 1360
no ip split-horizon eigrp 200
tunnel source Port-channel32

```

```

tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN-PROFILE
!
!
interface Port-channel32
ip address 10.4.32.2 255.255.255.252
ip pim sparse-mode
!
hold-queue 150 in
!
interface GigabitEthernet0/0
bandwidth 300000
ip address 192.168.4.129 255.255.255.252
duplex auto
speed auto
no cdp enable
!
!
interface GigabitEthernet0/1
description C6504-VSS Gig2/2/23
no ip address
duplex auto
speed auto
channel-group 32
!
!
interface GigabitEthernet0/2
description C6504-VSS Gig1/2/23
no ip address
duplex auto
speed auto
channel-group 32
!
!
interface FastEthernet0/0/0
no ip address
shutdown

```

```

duplex auto
speed auto
!
!
interface FastEthernet0/0/1
no ip address
shutdown
duplex auto
speed auto
!
!
!
router eigrp 100
default-metric 300000 300 255 1 1500
network 10.4.0.0 0.1.255.255
redistribute static
redistribute eigrp 200 route-map SET-ROUTE-TAG-DMVPN
passive-interface default
no passive-interface Port-channel32
eigrp router-id 10.4.32.254
!
!
router eigrp 200
network 10.4.34.0 0.0.0.255
redistribute eigrp 100
passive-interface default
no passive-interface Tunnel10
eigrp router-id 10.4.32.254
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http secure-server
!

```

```

ip route 10.5.0.0 255.255.0.0 192.168.4.130
ip route 10.255.252.2 255.255.255.255 192.168.4.130
ip route 10.255.252.4 255.255.255.255 192.168.4.130
ip route 192.168.4.128 255.255.255.224 192.168.4.130
!
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
route-map SET-ROUTE-TAG-DMVPN permit 10
match interface Tunnel10
set tag 65512
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
!
control-plane
!
!
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
logging synchronous
line aux 0

```

```
line vty 0 4
  transport preferred none
  transport input ssh
line vty 5 15
  transport preferred none
  transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 10.4.48.17
end
```

Notes

WAN Remote-Site Devices – DMVPN Backup Shared Design Model

This section includes configuration files corresponding to the DMVPN Backup Shared design model as referenced in Figure 10. Each remote-site type has its respective devices grouped together along with any other relevant configuration information.

Figure 10 - WAN remote-site designs—DMVPN Backup Shared

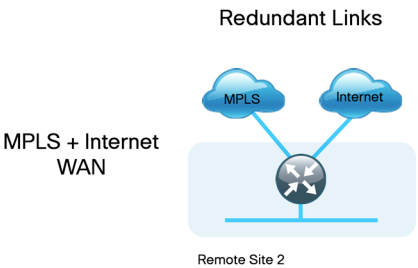


Table 21 lists the specific details for the MPLS WAN and DMVPN WAN connections at each site.

Table 21 - Remote-site WAN connection details

Remote-Site		MPLS (Our AS = 65511)			DMVPN	LAN interfaces	Loopbacks
Location	Net Block	MPLS CE	MPLS PE	Carrier AS			
Remote site 2 (Single-router, single-link with local DHCP)	10.5.8.0/21	(gi0/0) 192.168.4.137	192.168.4.138	Statically routed (B)	(gi0/0) DHCP	(gi0/2)	10.255.252.2 (r)

Table 22 lists the link speeds for the remote-site QoS traffic shaping policies.

Table 22 - Remote-site link speeds

Remote-Site information		Link speeds (policed rates)	
Location	Net Block	Layer 2 WAN	DMVPN
Remote site 2	10.5.8.0/21	10 Mbps	5 Mbps

Remote Site 2: Single-Router, Single-Link with Local DHCP (MPLS-B Static)

Table 23 shows the IP address information for remote site 2.

Table 23 - Remote site 2—IP address information

Remote-Site information		Wired subnets		Operational IP assignments
Location	Net Block	Data (Vlan 64)	Vlan (Vlan 69)	Loopbacks and switches
Remote site 2	10.5.8.0/21	10.5.12.0/24	10.5.13.0/24	10.255.252.2 (router) 10.5.12.5 (access switch)

RS2-2921

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS2-2921
!
boot-start-marker
boot-end-marker
!
!
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZT0hxTZyUnZdsSrs
!
aaa new-model
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
```

```
!
no ipv6 cef
ip source-route
ip cef
!
!
!
ip vrf INET-PUBLIC1
rd 65512:1
!
ip multicast-routing
ip dhcp excluded-address 10.5.12.1 10.5.12.19
ip dhcp excluded-address 10.5.13.1 10.5.13.19
!
ip dhcp pool DHCP-Wired-Data
network 10.5.12.0 255.255.255.0
default-router 10.5.12.1
domain-name cisco.local
dns-server 10.4.48.10
!
ip dhcp pool DHCP-Wired-Voice
network 10.5.13.0 255.255.255.0
default-router 10.5.13.1
domain-name cisco.local
dns-server 10.4.48.10
!
!
```

```

!
ip domain name cisco.local
!
multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!
!
!
!
!
license udi pid CISCO2921/K9 sn FTX1419ALZK
hw-module pvdm 0/0
!
!
!
!
username admin password 7 070C705F4D06485744
!
redundancy
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
track 60 ip sla 200 reachability
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!

```

```

crypto isakmp policy 10
encr aes 256
authentication pre-share
group 2
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
keyring DMVPN-KEYRING1
match identity address 0.0.0.0 INET-PUBLIC1
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
mode transport
!
crypto ipsec profile DMVPN-PROFILE1
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
!
!
!
!
!
interface Loopback0
ip address 10.255.252.2 255.255.255.255
ip pim sparse-mode
!
interface Tunnel10
bandwidth 5000
ip address 10.4.34.102 255.255.255.0
no ip redirects
ip mtu 1400
ip pim dr-priority 0
ip pim nbma-mode
ip pim sparse-mode
ip hello-interval eigrp 200 20
ip hold-time eigrp 200 60
ip nhrp authentication cisco123

```

```

ip nhrp map 10.4.34.1 172.17.30.4
ip nhrp map multicast 172.17.30.4
ip nhrp network-id 101
ip nhrp holdtime 600
ip nhrp nhs 10.4.34.1
ip nhrp registration no-unique
ip nhrp shortcut
ip nhrp redirect
ip tcp adjust-mss 1360
ip summary-address eigrp 200 10.5.8.0 255.255.248.0
shutdown
tunnel source GigabitEthernet0/1
tunnel mode gre multipoint
tunnel vrf INET-PUBLIC1
tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
bandwidth 10000
ip address 192.168.4.137 255.255.255.252
duplex auto
speed auto
no cdp enable
!
interface GigabitEthernet0/1
ip vrf forwarding INET-PUBLIC1
ip address dhcp
ip access-group ACL-INET-PUBLIC in
duplex auto
speed auto
no cdp enable
!
interface GigabitEthernet0/2
description RS2-A3560X Gig0/24

```

```

no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/2.64
description Wired Data
encapsulation dot1Q 64
ip address 10.5.12.1 255.255.255.0
ip pim sparse-mode
!
interface GigabitEthernet0/2.69
description Wired Voice
encapsulation dot1Q 69
ip address 10.5.13.1 255.255.255.0
ip pim sparse-mode
!
!
!
router eigrp 200
network 10.4.34.0 0.0.1.255
network 10.5.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel10
eigrp router-id 10.255.252.2
eigrp stub connected summary
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.4.138
!
ip access-list extended ACL-INET-PUBLIC

```

```

permit udp any any eq non500-isakmp
permit udp any any eq isakmp
permit esp any any
permit udp any any eq bootpc
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any ttl-exceeded
permit icmp any any port-unreachable
permit udp any any gt 1023 ttl eq 1
!
ip sla 200
icmp-echo 192.168.4.129 source-interface GigabitEthernet0/0
threshold 1000
frequency 15
ip sla schedule 200 life forever start-time now
!
!
!
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
!
!
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
shutdown

```

```

!
!
!
line con 0
logging synchronous
line aux 0
line vty 0 4
transport preferred none
transport input ssh
line vty 5 15
transport preferred none
transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 10.4.48.17
event manager applet ACTIVATE-VPN
event track 60 state down
action 1 cli command "enable"
action 2 cli command "configure terminal"
action 3 cli command "interface tunnel10"
action 4 cli command "no shutdown"
action 5 cli command "end"
action 99 syslog msg "Primary Link Down - Activating VPN
interface"
event manager applet DEACTIVATE-VPN
event track 60 state up
action 1 cli command "enable"
action 2 cli command "configure terminal"
action 3 cli command "interface tunnel10"
action 4 cli command "shutdown"
action 5 cli command "end"
action 99 syslog msg "Primary Link Restored - Deactivating VPN
interface"
!
end

```

Feedback

Click [here](#) to provide feedback to Cisco SBA.



SMART BUSINESS ARCHITECTURE

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)