



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

ENTERPRISE

BORDERLESS
NETWORKS

WAN Deployment Guide

● ● ● SMART BUSINESS ARCHITECTURE

February 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 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.

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 2011 are the “August 2011 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 forum at the bottom of one of the following sites:

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

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

An RSS feed is available if you would like to be notified when new comments are posted.

Table of Contents

What's In This SBA Guide.....	1	
About SBA	1	
About This Guide	1	
Introduction.....	2	
Related Reading	2	
Design Goals	4	
Architecture Overview.....	5	
WAN Design	5	
Quality of Service.....	12	
WAN Optimization	13	
Deploying the WAN.....	14	
Overall WAN Architecture Design Goals	14	
Deploying an MPLS WAN.....	16	
Business Overview.....	16	
Technology Overview.....	16	
		Deployment Details
		20
		MPLS CE Router Configuration
		20
		Remote-Site MPLS CE Router Configuration.....
		27
		Adding Secondary MPLS Link on Existing MPLS CE Router.....
		35
		Remote-Site Router Configuration (Dual-Router - Router 2).....
		38
		Deploying a DMVPN WAN
		47
		Business Overview.....
		47
		Technology Overview.....
		47
		Deployment Details
		53
		DMVPN Hub Router Configuration
		53
		Firewall and DMZ Switch Configuration
		61
		Enabling DMVPN Backup on Existing MPLS CE Router
		67
		Remote-Site DMVPN Spoke Router Configuration
		73
		Deploying a WAN Remote-Site Distribution Layer
		82
		Remote-Site MPLS CE Router Distribution Layer
		82
		Remote-Site Second Router Distribution Layer
		84
		Remote-Site WAN Distribution Layer Switch Configuration
		86

Deploying WAN Quality of Service	89
Configuring QoS.....	89
Deploying Application Optimization with WAAS.....	93
Business Overview.....	93
Technology Overview.....	93
WAAS/WAE Configuration	96

Appendix A:	
Enterprise Organizations WAN Deployment Product List.....	113
Appendix B: Technical Feature Supplement.....	115
Front Door vREF (FVRF) for DMVPN.....	115
Appendix C: Changes	117

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 NONINFRINGEMENT 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.

What's In This SBA Guide

About SBA

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.

For more information, see the *How to Get Started with Cisco SBA* document:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

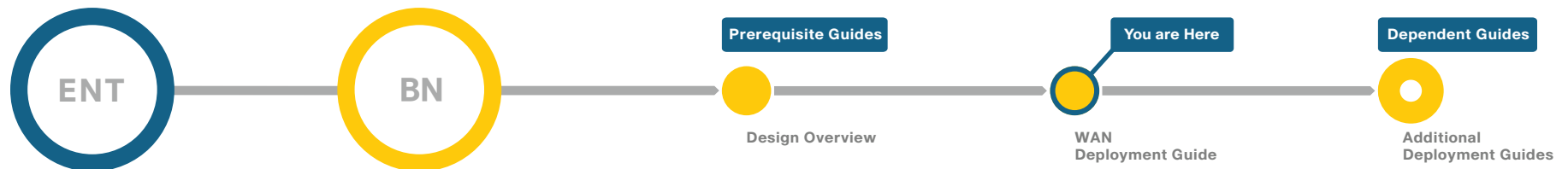
About This Guide

This *foundation deployment guide* is organized in sections, which each include the following parts:

- **Business Overview**—The challenge your organization faces. Business decision makers can use this part to understand the relevance of the solution to their organizations' operations.
- **Technology Overview**—How Cisco solves the challenge. Technical decision makers can use this part to understand how the solution works.
- **Deployment Details**—Step-by-step instructions for implementing the solution. Systems engineers can use this part to get the solution up and running quickly and reliably.

To learn what changed in this guide between the previous series and the current series, see [Appendix C: Changes](#).

This guide presumes that you have read the prerequisite foundation design overview, as shown on the Route to Success below.



Route to Success

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: <http://www.cisco.com/go/sba>
For partner access: <http://www.cisco.com/go/sbachannel>

Introduction

Cisco SBA for Enterprise Organizations—Borderless Networks is a solid network foundation designed to provide networks with 2,000 to 10,000 connected users the flexibility to support new users or network services without re-engineering the network. We created a prescriptive, out-of-the-box deployment guide that is based on best-practice design principles and that delivers flexibility and scalability.

The foundation architecture is described in a single *Design Guide*, as well as several deployment and configuration guides for each of the three parts of the foundation: LAN, WAN, and Internet Edge.

To help focus on specific elements of the architecture, there are three WAN deployment guides:

- This *WAN Deployment Guide* provides flexible guidance and configuration for Multiprotocol Label Switching (MPLS) transport as well as broadband or Internet transport in a backup role.
- *Layer 2 WAN Deployment Guide* provides guidance and configuration for a VPLS or Metro Ethernet transport as well as a broadband or Internet transport in a backup role.
- *VPN Remote Site Deployment Guide* provides guidance and configuration for broadband or Internet transport in a both a primary or backup role

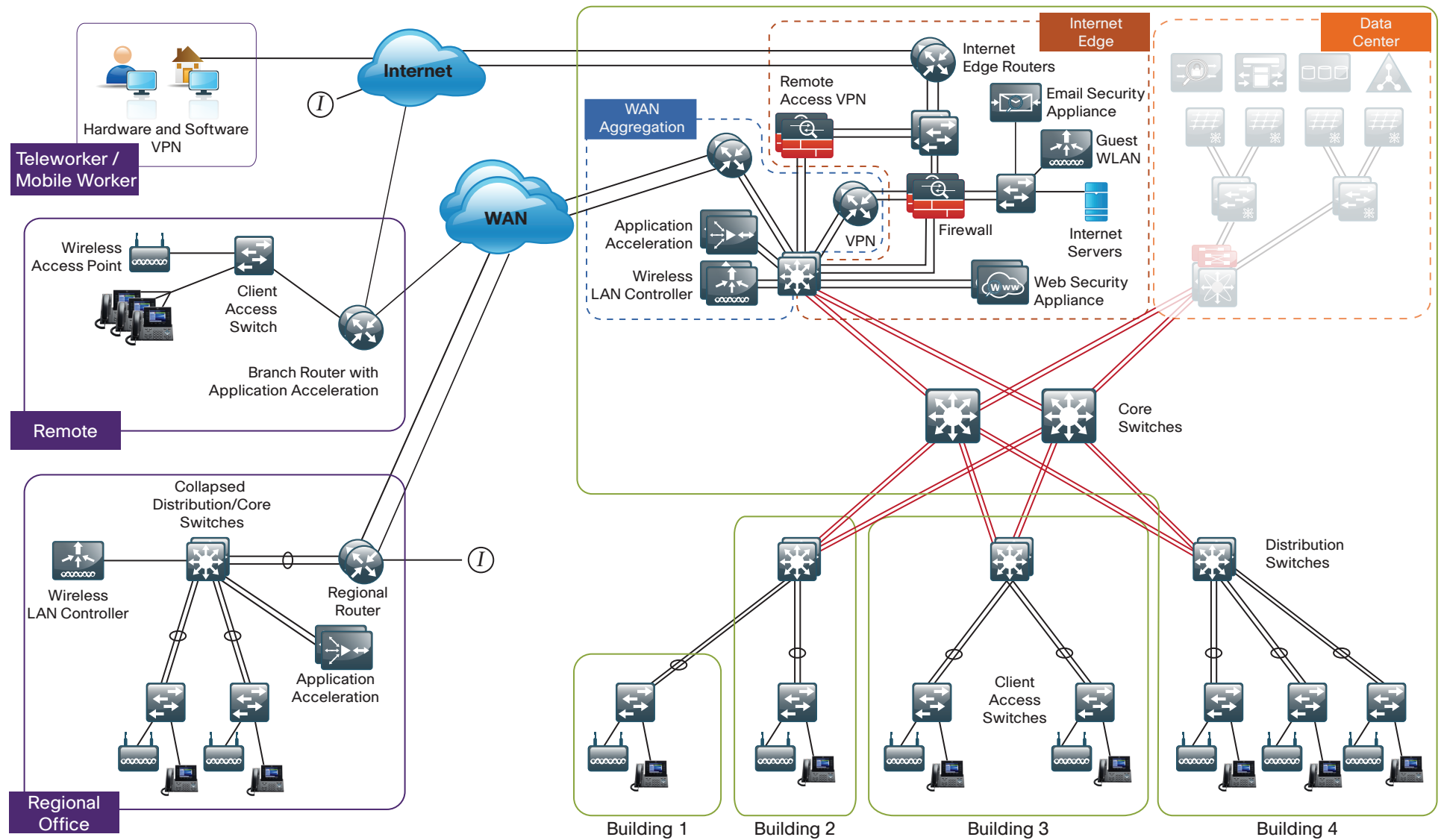
Related Reading

The *Design Guide* orients you to the overall Cisco SBA design and explains the requirements that were considered when selecting specific products.

The *Local Area Network Deployment Guide* describes wired and wireless network access with ubiquitous capabilities for both the larger campus-size LAN as well as the smaller remote-site LAN. Resiliency, security, and scalability are included to provide a robust communications environment. Quality of service (QoS) is integrated to ensure that the base architecture can support a multitude of applications including low latency, drop-sensitive multimedia applications coexisting with data applications on a single network. The guide also provides a guest and partner access solution that is secured from accessing internal confidential information while using the same wireless infrastructure that employees use.

The *Internet Edge Deployment Guide* focuses on security services, such as firewalls and intrusion prevention systems, that protect your organization's gateway to the Internet. Internet service-provider connectivity and routing options, combined with server load balancing, provide resiliency to the design. This guide's "E-Mail Security" section covers protecting email from spam and malware. The "Web Security" section provides acceptable-use control and monitoring as well as guidance on managing the increasing risk associated with clients browsing the Internet. The Remote Access VPN design supports the teleworker and mobile user with secure remote access. All of these elements are covered in separate sections, yet are designed to work together to provide a secure Internet Edge solution.

Figure 1 - Borderless Networks for Enterprise Organizations Overview



Design Goals

This architecture is based on requirements gathered from customers, partners, and Cisco field personnel for organizations with 2000 to 10,000 connected users. When designing the architecture, we considered the gathered requirements and the following design goals.

Ease of Deployment, Flexibility, and Scalability

Organizations with 2000 to 10,000 users are often spread out among different geographical locations, making flexibility and scalability a critical requirement of the network. This design uses several methods to create and maintain a scalable network:

- By keeping a small number of standard designs for common portions of the network, support staff is able to design services for, implement, and support the network more effectively.
- Our modular design approach enhances scalability. Beginning with a set of standard, global building blocks, we can assemble a scalable network to meet requirements.
- Many of the plug-in modules look identical for several service areas; this common look provides consistency and scalability in that the same support methods can be used to maintain multiple areas of the network. These modules follow standard core-distribution-access network design models and use layer separation to ensure that interfaces between the plug-ins are well defined.

Resiliency and Security

One of the keys to maintaining a highly available network is building appropriate redundancy to guard against failure in the network. The redundancy in our architecture is carefully balanced with the complexity inherent in redundant systems.

With the addition of a significant amount of delay-sensitive and drop-sensitive traffic such as voice and video conferencing, we also place a strong emphasis on recovery times. Choosing designs that reduce the time between failure detection and recovery is important for ensuring that the network stays available even in the face of a minor component failure.

Network security is also a strong component of the architecture. In a large network, there are many entry points and we ensure that they are as secure as possible without making the network too difficult to use. Securing the network not only helps keep the network safe from attacks but is also a key component to network-wide resiliency.

Ease of Management

While this guide focuses on the deployment of the network foundation, the design takes next phase management and operation into consideration. The configurations in the deployment guides are designed to allow the devices to be managed via normal device management connections, such as SSH and HTTPS, as well as via NMS. The configuration of the NMS is not covered in this guide.

Advanced Technology-Ready

Flexibility, scalability, resiliency, and security all are characteristics of an advanced technology-ready network. The modular design of the architecture means that technologies can be added when the organization is ready to deploy them. However, the deployment of advanced technologies, such as collaboration, is eased because the architecture includes products and configurations that are ready to support collaboration from day one. For example:

- Access switches provide Power over Ethernet (PoE) for phone deployments without the need for a local power outlet
- The entire network is preconfigured with QoS to support high-quality voice.
- Multicast is configured in the network to support efficient voice and broadcast-video delivery.
- The wireless network is preconfigured for devices that send voice over the wireless LAN, providing IP telephony over 802.11 Wi-Fi (referred to as mobility) at all locations.

The Internet Edge is ready to provide soft phones via VPN, as well as traditional hard or desk phones.

Architecture Overview

The *Cisco SBA for Enterprise Organizations—Borderless Networks WAN Deployment Guide* provides a design that enables highly available, secure, and optimized connectivity for multiple remote-site LANs.

The WAN is the networking infrastructure that provides an IP-based inter-connection between remote sites that are separated by large geographic distances.

This document shows you how to deploy the network foundation and services to enable the following:

- WAN connectivity for 25 to 500 remote sites
- Primary and secondary links to provide redundant topology options for resiliency
- Data privacy via encryption
- WAN optimization and application acceleration
- Wired and wireless LAN access at all remote sites

WAN Design

The primary focus of the design is to allow usage of the following commonly deployed WAN transports:

- Multiprotocol Label Switching (MPLS) Layer 3 VPN
- Internet VPN

At a high level, the WAN is an IP network, and these transports can be easily integrated to the design. The chosen architecture designates a primary WAN-aggregation site that is analogous to the hub site in a traditional hub-and-spoke design. This site has direct connections to both WAN transports and high-speed connections to the selected service providers. In addition, the site uses network equipment scaled for high performance and redundancy. The primary WAN-aggregation site is coresident with the data center and usually the primary Campus or LAN as well.

MPLS WAN Transport

Cisco IOS Software Multiprotocol Label Switching (MPLS) enables enterprises and service providers to build next-generation intelligent networks

that deliver a wide variety of advanced, value-added services over a single infrastructure. You can integrate this economical solution seamlessly over any existing infrastructure, such as IP, Frame Relay, ATM, or Ethernet.

MPLS Layer 3 VPNs use a peer-to-peer VPN Model that leverages the Border Gateway Protocol (BGP) to distribute VPN-related information. This peer-to-peer model allows enterprise subscribers to outsource routing information to service providers, which can result in significant cost savings and a reduction in operational complexity for enterprises.

Subscribers who need to transport IP multicast traffic can enable Multicast VPNs (MVPNs).

The WAN leverages MPLS VPN as a primary WAN transport or as a backup WAN transport (to an alternate MPLS VPN primary).

Internet as WAN Transport

The Internet is essentially a large-scale public WAN composed of multiple interconnected service providers. The Internet can provide reliable high-performance connectivity between various locations, although it lacks any explicit guarantees for these connections. Despite its “best effort” nature, the Internet is a sensible choice for an alternate WAN transport, or for a primary transport when it is not feasible to connect with another transport option.

Internet connections are typically included in discussions relevant to the Internet edge, specifically for the primary site. Remote-site routers also commonly have Internet connections, but do not provide the same breadth of services using the Internet. For security and other reasons, Internet access at remote sites is often routed through the primary site.

The WAN uses the Internet for VPN site-to-site connections as a backup WAN transport (to MPLS VPN).

Dynamic Multipoint VPN

Dynamic Multipoint VPN (DMVPN) is a solution for building scalable site-to-site VPNs that support a variety of applications. DMVPN is widely used for encrypted site-to-site connectivity over public or private IP networks and can be implemented on all WAN routers used in this deployment guide.

DMVPN was selected for the encryption solution for the Internet transport because it supports on-demand full mesh connectivity with a simple hub-and-spoke configuration and a zero-touch hub deployment model for adding remote sites. DMVPN also supports spoke routers that have dynamically assigned IP addresses.

DMVPN makes use of multipoint generic routing encapsulation (mGRE) tunnels to interconnect the hub to all of the spoke routers. These mGRE tunnels are also sometimes referred to as DMVPN clouds in this context. This technology combination supports unicast, multicast, and broadcast IP, including the ability to run routing protocols within the tunnels.

Ethernet WAN

Both of the WAN transports mentioned previously use Ethernet as a standard media type. Ethernet is becoming a dominant carrier handoff in many markets and it is relevant to include Ethernet as the primary media in the tested architectures. Much of the discussion in this guide can also be applied to non-Ethernet media (such as T1/E1, DS-3, OC-3, and so on), but they are not explicitly discussed.

WAN-Aggregation Designs

The WAN-aggregation (hub) designs include two or more WAN edge routers. When WAN edge routers are referred to in the context of the connection to a carrier or service provider, they are typically known as *customer edge (CE) routers*. WAN edge routers that terminate VPN traffic are referred to as VPN hub routers. All of the WAN edge routers connect into a distribution layer.

The WAN transport options include MPLS VPN and traditional Internet access. Both transport types connect to either a CE router or a VPN hub router, respectively. Interfacing with each of these transports requires a different connection method and configuration.

There are two WAN-aggregation designs that are documented in this deployment guide: WAN100 and WAN500. The primary difference between the WAN100 and WAN500 designs is the overall scale of the architecture and the capabilities of the various platforms chosen to support the design.

In both WAN-aggregation designs, tasks such as IP route summarization are performed at the distribution layer. There are other various devices supporting WAN edge services, and these devices should also connect into the distribution layer.

Each MPLS carrier terminates to a dedicated WAN router with a primary goal of eliminating any single points of failure. A single VPN hub router is used across both designs. The various design models are contrasted in the following table.

Table 1 - WAN-aggregation designs

Model	WAN links	Edge routers	Transport 1	Transport 2	Transport 3
WAN100	Dual	Dual	MPLS VPN A	Internet VPN	—
WAN500	Multiple	Multiple	MPLS VPN A	MPLS VPN B	Internet VPN

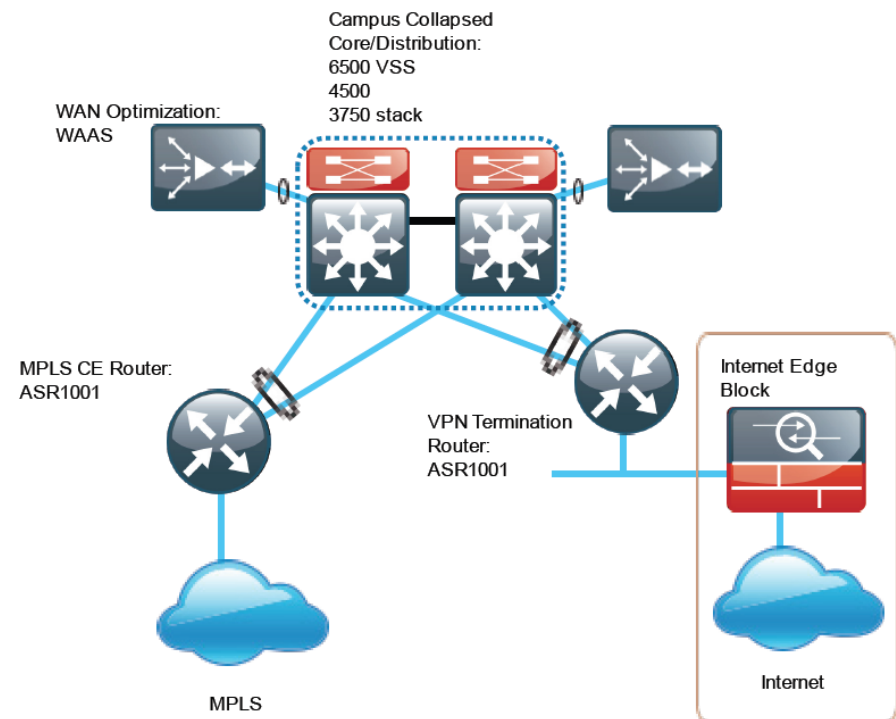
The characteristics of each design are as follows:

WAN100 Design

- Has up to 100 Mbps aggregate bandwidth
- Supports up to 100 remote sites
- Has a single MPLS VPN carrier
- Uses a single Internet link

The WAN100 Design is shown in the following figure.

Figure 2 - WAN100 design

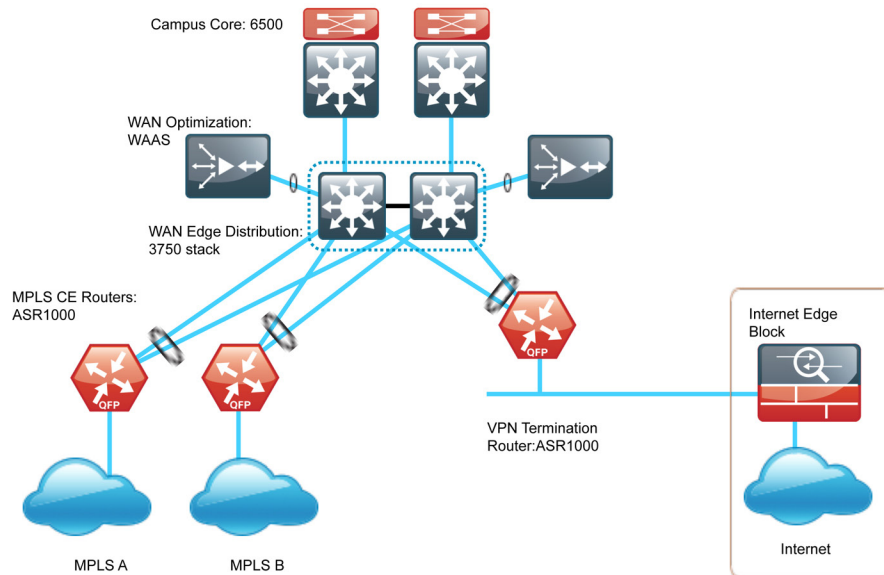


WAN500 Design

- Has up to 1 Gbps aggregate bandwidth
- Supports up to 500 remote sites
- Has multiple MPLS VPN carriers
- Uses a single Internet link

The WAN500 Design is shown in the following figure.

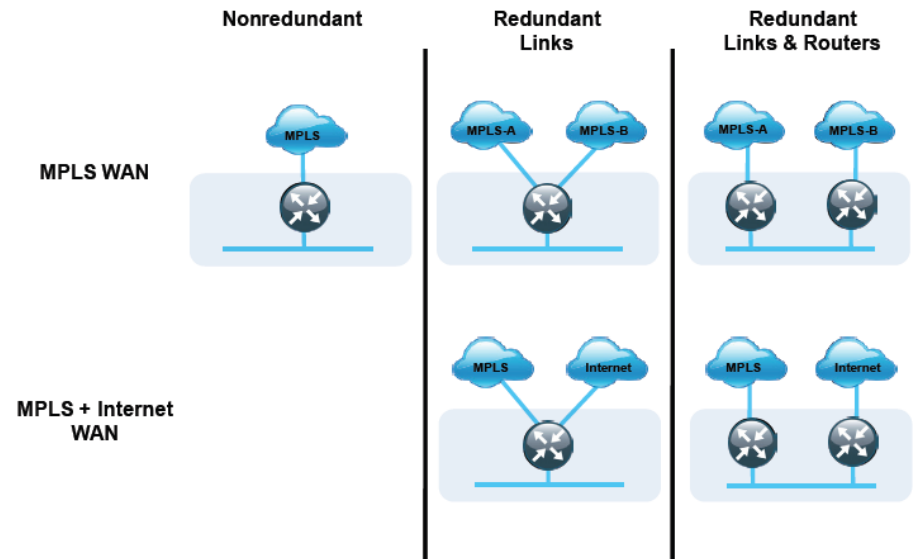
Figure 3 - WAN500 design



WAN Remote-Site Designs

This guide documents multiple WAN remote-site designs, and they are based on various combinations of WAN transports mapped to the site specific requirements for service levels and redundancy.

Figure 4 - WAN Remote-Site Designs



The remote-site designs include single or dual WAN edge routers. These can be either a CE router or a VPN spoke router. In some cases, a single WAN edge router can perform the role of both a CE router and VPN-spoke router.

Most remote sites are designed with a single router WAN edge; however, certain remote-site types require a dual router WAN edge. Dual router candidate sites include regional office or remote campus locations with large user populations, or sites with business critical needs that justify additional redundancy to remove single points of failure.

The overall WAN design methodology is based on a primary WAN-aggregation site design that can accommodate all of the remote-site types that map to the various link combinations listed in the following table.

Table 2 - WAN remote-site transport options

WAN remote-site routers	WAN transports	Primary transport	Secondary transport
Single	Single	MPLS VPN A	-
Single	Dual	MPLS VPN A	MPLS VPN B
Single	Dual	MPLS VPN A	Internet
Single	Dual	MPLS VPN B	Internet
Dual	Dual	MPLS VPN A	MPLS VPN B
Dual	Dual	MPLS VPN A	Internet
Dual	Dual	MPLS VPN B	Internet

The modular nature of the network design enables you to create design elements that you can replicate throughout the network.

Both WAN-aggregation designs and all of the WAN remote-site designs are standard building blocks in the overall design. Replication of the individual building blocks provides an easy way to scale the network and allows for a consistent deployment method.

WAN/LAN Interconnection

The primary role of the WAN is to interconnect primary site and remote-site LANs. The LAN discussion within this guide is limited to how the WAN-aggregation site LAN connects to the WAN-aggregation devices and how the remote-site LANs connect to the remote-site WAN devices. Specific details regarding the LAN components of the design are covered in the *Cisco SBA for Enterprise Organizations—Borderless Networks LAN Deployment Guide*.

At remote sites, the LAN topology depends on the number of connected users and physical geography of the site. Large sites may require the use of a distribution layer to support multiple access layer switches. Other sites may only require an access layer switch directly connected to the WAN remote-site routers. The variants that are tested and documented in this guide are shown in the following table.

Table 3 - WAN remote-site LAN options

WAN remote-site routers	WAN transports	LAN topology
Single	Single	Access only Distribution/access
Single	Dual	Access only Distribution/access
Dual	Dual	Access only Distribution/access

WAN Remotes Sites—LAN Topology

For consistency and modularity, all WAN remote sites use the same VLAN assignment scheme, which is shown in the following table. This deployment guide uses a convention that is relevant to any location that has a single access switch and this model can also be easily scaled to additional access closets through the addition of a distribution layer.

Table 4 - WAN remote-sites—VLAN assignment

VLAN	Usage	Layer 2 access	Layer 3 distribution/access
VLAN 100	Data (primary)	Unused	Yes
VLAN 65	Wireless data	Yes	Yes
VLAN 70	Wireless voice	Yes	Yes
VLAN 64	Data 1	Yes	Yes
VLAN 69	Voice 1	Yes	Yes
Unassigned	Data 2	Unused	Yes
Unassigned	Voice 2	Unused	Yes
VLAN99	Transit	Yes (dual router only)	Yes (dual router only)
VLAN50	Router link (1)	Unused	Yes
VLAN54	Router link (2)	Unused	Yes (dual router only)

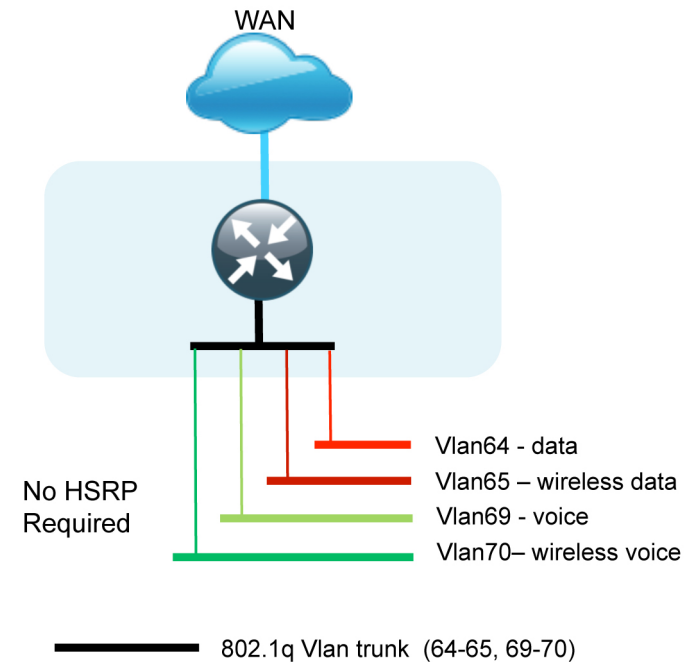
Layer 2 Access

WAN remote sites that do not require additional distribution layer routing devices are considered to be flat or from a LAN perspective they are considered unrouted Layer 2 sites. All Layer 3 services are provided by the attached WAN routers. The access switches, through the use of multiple VLANs, can support services such as data (wired and wireless) and voice (wired and wireless). The design shown in the following figure illustrates the standardized VLAN assignment scheme. The benefits of this design are clear: all of the access switches can be configured identically, regardless of the number of sites in this configuration.

Access switches and their configuration are not included in this guide. The *Cisco SBA for Enterprise Organizations—Borderless Networks LAN Deployment Guide* provides configuration details on the various access switching platforms.

IP subnets are assigned on a per-VLAN basis. This design only allocates subnets with a 255.255.255.0 netmask for the access layer, even if less than 254 IP addresses are required. (This model can be adjusted as necessary to other IP address schemes.) The connection between the router and the access switch must be configured for 802.1Q VLAN trunking with subinterfaces on the router that map to the respective VLANs on the switch. The various router subinterfaces act as the IP default gateways for each of the IP subnet and VLAN combinations.

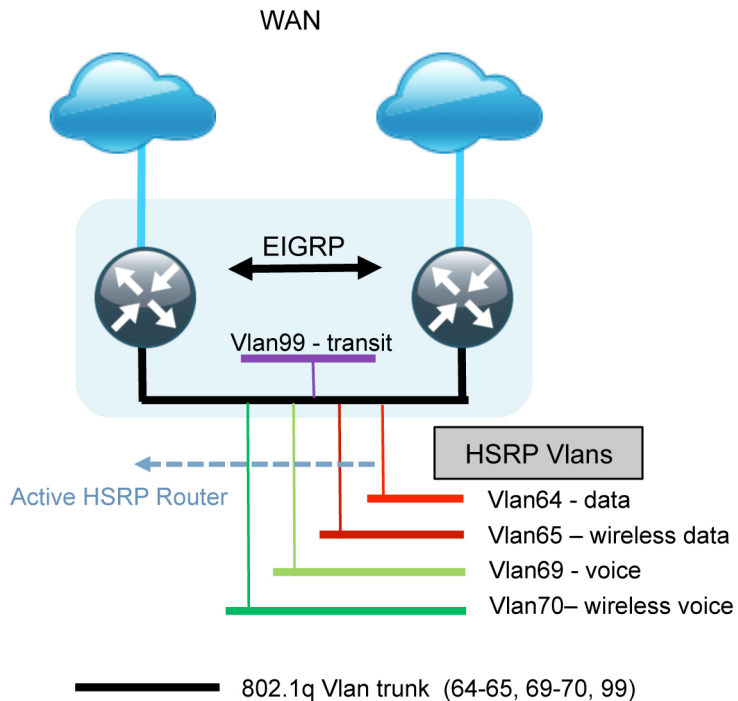
Figure 5 - WAN remote-site—Flat Layer 2 LAN (single router)



A similar LAN design can be extended to a dual-router edge as shown in the following figure. This design change introduces some additional complexity. The first requirement is to run a routing protocol. You need to configure Enhanced Interior Gateway Routing Profile (EIGRP) between the routers. For consistency with the primary site LAN, use EIGRP process 100.

Because there are now two routers per subnet, a First Hop Redundancy Protocol (FHRP) must be implemented. For this design, Cisco selected Hot Standby Router Protocol (HSRP) as the FHRP. HSRP is designed to allow for transparent failover of the first-hop IP router. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts configured with a default gateway IP address. HSRP is used in a group of routers for selecting an active router and a standby router. When there are multiple routers on a LAN, the active router is the router of choice for routing packets; the standby router is the router that takes over when the active router fails or when preset conditions are met.

Figure 6 - WAN remote site—Flat Layer 2 LAN (dual router)



Enhanced Object Tracking (EOT) provides a consistent methodology for various router and switching features to conditionally modify their operation based on information objects available within other processes. The objects that can be tracked include interface line protocol, IP route reachability, and IP service-level agreement (SLA) reachability as well as several others.

The IP SLA feature provides a capability for a router to generate synthetic network traffic that can be sent to a remote responder. The responder can be a generic IP endpoint that can respond to an Internet Control Message Protocol (ICMP) echo (ping) request, or can be a Cisco router running an IP SLA responder process, that can respond to more complex traffic such as jitter probes. The use of IP SLA allows the router to determine end-to-end reachability to a destination and also the roundtrip delay. More complex probe types can also permit the calculation of loss and jitter along the path. IP SLA is used in tandem with EOT within this design.

To improve convergence times after a MPLS WAN failure, HSRP has the capability to monitor the reachability of a next-hop IP neighbor through the use of EOT and IP SLA. This combination allows for a router to give up its HSRP Active role if its upstream neighbor becomes unresponsive and that provides additional network resiliency.

HSRP is configured to be active on the router with the highest priority WAN transport. EOT of IP SLA probes is implemented in conjunction with HSRP so that in the case of WAN transport failure, the standby HSRP router associated with the lower priority (alternate) WAN transport becomes the active HSRP router. The IP SLA probes are sent from the MPLS CE router to the MPLS PE router to ensure reachability of the next hop router. This is more effective than simply monitoring the status of the WAN interface.

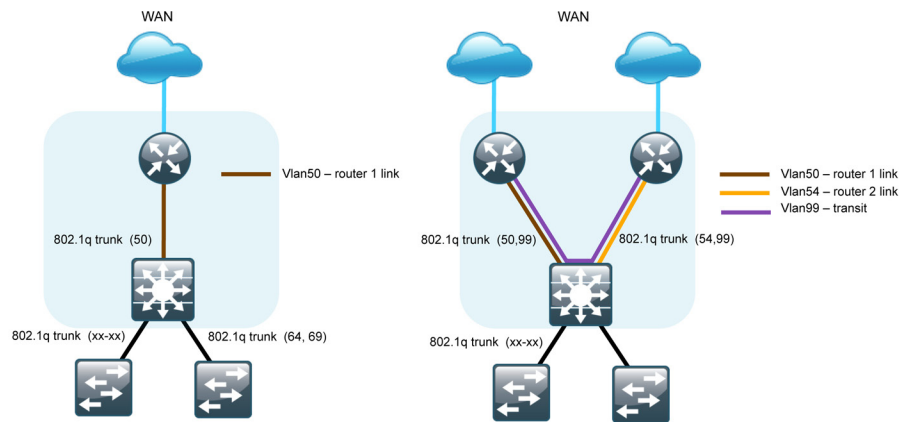
The dual router designs also warrant an additional component that is required for proper routing in certain scenarios. In these cases, a traffic flow from a remote-site host might be sent to a destination reachable via the alternate WAN transport (for example, an MPLS + DMVPN remote site communicating with a DMVPN-only remote site). The primary WAN transport router then forwards the traffic out the same data interface to send it to the alternate WAN transport router, which then forwards the traffic to the proper destination. This is referred to as hair-pinning.

The appropriate method to avoid sending the traffic out the same interface is to introduce an additional link between the routers and designate the link as a transit network (Vlan 99). There are no hosts connected to the transit network, and it is only used for router-router communication. The routing protocol runs between router subinterfaces assigned to the transit network. No additional router interfaces are required with this design modification because the 802.1Q VLAN trunk configuration can easily accommodate an additional subinterface.

Distribution and Access Layer

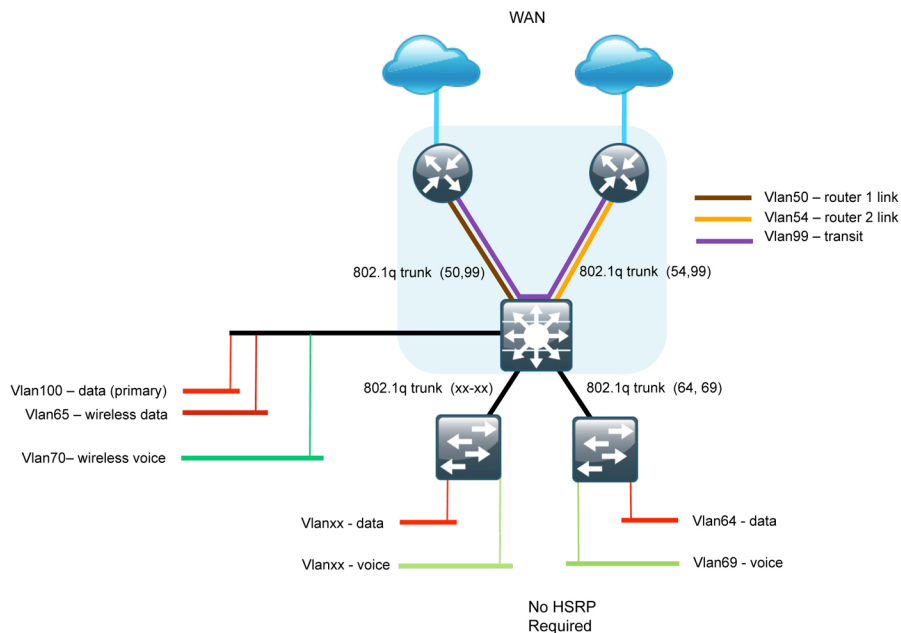
Large remote sites may require a LAN environment similar to that of a small campus LAN that includes a distribution layer and access layer. This topology works well with either a single or dual router WAN edge. To implement this design, the routers should connect via EtherChannel links to the distribution switch. These EtherChannel links are configured as 802.1Q VLAN trunks, to support both a routed point-to-point link to allow EIGRP routing with the distribution switch, and in the dual router design, to provide a transit network for direct communication between the WAN routers.

Figure 7 - WAN remote site—Connection to distribution layer



The distribution switch handles all access layer routing, with VLANs trunked to access switches. No HSRP is required when the design includes a distribution layer. A full distribution and access layer design is shown in the following figure.

Figure 8 - WAN remote site—Distribution and access layer (dual router)



IP Multicast

IP Multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. IP Multicast is much more efficient than multiple individual unicast streams or a broadcast stream that would propagate everywhere. IP telephony Music On Hold (MOH) and IP video broadcast streaming are two examples of IP Multicast applications.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an Internet Group Management Protocol (IGMP) message to their local multicast router. In a traditional IP Multicast design, the local router consults another router in the network that is acting as a rendezvous point (RP) to map the receivers to active sources so that they can join their streams.

The RP is a control-plane operation that should be placed in the core of the network or close to the IP Multicast sources on a pair of Layer 3 switches or routers. IP Multicast routing begins at the distribution layer if the access layer is Layer 2 and provides connectivity to the IP Multicast RP. In designs without a core layer, the distribution layer performs the RP function.

This design is fully enabled for a single global scope deployment of IP Multicast. The design uses an Anycast RP implementation strategy. This strategy provides load sharing and redundancy in Protocol Independent Multicast sparse mode (PIM SM) networks. Two RPs share the load for source registration and the ability to act as hot backup routers for each other.

The benefit of this strategy from the WAN perspective is that all IP routing devices within the WAN use an identical configuration referencing the Anycast RPs. IP PIM SM is enabled on all interfaces including loopbacks, VLANs, and subinterfaces.

Quality of Service

Most users perceive the network as just a transport utility mechanism to shift data from point A to point B as fast as it can. Many sum this up as just “speeds and feeds.” While it is true that IP networks forward traffic on a best-effort basis by default, this type of routing only works well for applications that adapt gracefully to variations in latency, jitter, and loss. However networks are multiservice by design and support real-time voice and video as well as data traffic. The difference is that real-time applications require packets to be delivered within specified loss, delay, and jitter parameters.

In reality, the network affects all traffic flows and must be aware of end-user requirements and services being offered. Even with unlimited bandwidth, time-sensitive applications are affected by jitter, delay, and packet loss. Quality of service (QoS) enables a multitude of user services and applications to coexist on the same network.

Within the architecture, there are wired and wireless connectivity options that provide advanced classification, prioritizing, queuing and congestion mechanisms as part of the integrated QoS to help ensure optimal use of network resources. This functionality allows for the differentiation of applications, ensuring that each has the appropriate share of the network resources to protect the user experience and ensure the consistent operations of business critical applications.

QoS is an essential function of the network infrastructure devices used throughout this architecture. QoS enables a multitude of user services and applications, including real-time voice, high-quality video, and delay-sensitive data to coexist on the same network. In order for the network to provide predictable, measurable, and sometimes guaranteed services, it must manage bandwidth, delay, jitter, and loss parameters. Even if you do not require QoS for your current applications, you can use QoS for management and network protocols to protect the network functionality and manageability under normal and congested traffic conditions.

The goal of this design is to provide sufficient classes of service to allow you to add voice, interactive video, critical data applications, and management traffic to the network, either during the initial deployment or later with minimum system impact and engineering effort.

The QoS classifications in the following table are applied throughout this design. This table is included as a reference.

Table 5 - QoS service class mappings

Service class	Per-hop behavior (PHB)	Differentiated services code point (DSCP)	IP precedence (IPP)	Class of service (CoS)
Network layer	Layer 3	Layer 3	Layer 3	Layer 2
Network control	CS6	48	6	6
Telephony	EF	46	5	5
Signaling	CS3	24	3	3
Multimedia conferencing	AF41, 42, 43	34, 36, 38	4	4
Real-time interactive	CS4	32	4	4
Multimedia streaming	AF31, 32, 34	26, 28, 30	3	3
Broadcast video	CS5	40	4	4
Low-latency data	AF21, 22, 23	18, 20, 22	2	2
Operation, administration, and maintenance (OAM)	CS2	16	2	2
Bulk data	AF11, 12, 13	10, 12, 14	1	1
Scavenger	CS1	8	1	1
Default “best effort”	DF	0	0	0

WAN Optimization

Cisco Wide Area Application Services (WAAS) is a comprehensive WAN optimization solution that accelerates applications over the WAN, delivers video to a remote office, and provides local hosting of remote-site IT services. Cisco WAAS allows applications to be centralized and to use storage in the data center while maintaining LAN-like application performance.

WAAS accelerates applications and data over the WAN, optimizes bandwidth, empowers cloud computing, and provides local hosting of remote-site IT services, all with industry-leading network integration. Cisco WAAS allows IT organizations to centralize applications and storage while maintaining productivity for remote-site and mobile users.

WAAS is centrally managed and requires one or more Cisco WAAS Central Manager devices that are physically located within the data center but are accessible via a web interface.

The design for optimizing WAN traffic requires the deployment of Cisco Wide Area Application Engine (WAE) appliances or modules at both the WAN-aggregation site and at the WAN remote sites. The WAEs run WAAS software that provides the WAN optimization services. The design requires one or more WAE devices at every location, with multiple devices located at a site to provide resiliency. The Cisco WAAS solution operates as a TCP proxy that integrates transparently with other services in the network and provides WAN optimization benefits to the end users, without creating optimization tunnels across the WAN.

Low bandwidth remote sites can use the embedded WAAS Express (WAASx) capabilities within Cisco IOS software on Cisco routers. WAASx includes several of the base capabilities of WAAS, but not the Application Optimizers such as CIFS and HTTP.

The WAN optimization solution is tightly integrated with the WAN routers, with the routers controlling the interception and redirection of traffic to be optimized with WAAS. The design places the WAE appliances on existing network segments, which removes the need for significant network modifications.

A successful WAAS implementation requires the following:

- A method for intercepting chosen traffic to or from the WAN
- The ability to direct the chosen traffic to the WAE devices for proper optimization
- The ability for the WAE to reinject optimized traffic into the network after optimization

Web Cache Communication Protocol (WCCP) is used on the routers to intercept traffic entering the router from the LAN (sourced from the client or the data center) or entering the router from the WAN (from a remote WAE). As part of the WCCP redirection, traffic is forwarded to a chosen WAE via a generic routing encapsulation (GRE) tunnel.

Multiple WAE devices at one location can operate as a cluster. The routers performing the WCCP redirection are responsible for load sharing across the various WAE devices within a cluster. WAAS high availability uses what is referred to as an N+1 model. This name means that if N equivalent devices are required to support the required performance, one additional device is required to provide redundancy.

Traffic to be reinjected into the network uses a negotiated return WCCP GRE tunnel egress method back to the originating router. This method is preferred because it allows the WAE appliances to be located one or more routed hops away from the WCCP router. There are several benefits associated with this method, which are covered in more detail in the following sections.

A successful WAAS Express implementation requires the following:

- A router that meets the proper hardware requirements, particularly an upgrade to maximum DRAM
- The appropriate feature license to enable WAAS Express

The WAAS Express router does not require any traffic redirection or reinjection so WCCP is not required. This feature does not currently support multiple active links so it is only used in this design for remote sites with a single WAN transport.

Deploying the WAN

Overall WAN Architecture Design Goals

IP Routing

The design has the following IP routing goals:

- Provide optimal routing connectivity from primary WAN-aggregation sites to all remote locations
- Isolate WAN routing topology changes from other portions of the network
- Ensure active/standby symmetric routing when multiple paths exist, for ease of troubleshooting and to prevent oversubscription of IP telephony Call Admission Control (CAC) limits
- Provide site-site remote routing via the primary WAN-aggregation site (hub-and-spoke model)
- Permit optimal direct site-site remote routing when carrier services allow (spoke-to-spoke model)
- Support IP Multicast sourced from the primary WAN-aggregation site

At the WAN remote sites, there is no local Internet access for web browsing or cloud services. This model is referred to as a centralized Internet model. It is worth noting that sites with Internet/DMVPN for backup transport could potentially provide local Internet capability; however, for this design, only encrypted traffic to other DMVPN sites is permitted to use the Internet link. In the centralized Internet model, a default route is advertised to the WAN remote sites in addition to the internal routes from the data center and campus.

LAN Access

All remote sites are to support both wired and wireless LAN access.

High Availability

The network must tolerate single failure conditions including the failure of any single WAN transport link or any single network device at the primary WAN-aggregation site.

- Remote sites classified as single-router, dual-link must be able to tolerate the loss of either WAN transport.
- Remote sites classified as dual-router, dual-link must be able to tolerate the loss of either an edge router or a WAN transport.

Path Selection Preferences

There are many potential traffic flows based on which WAN transports are in use and whether or not a remote site is using a dual WAN transport.

The single WAN transport routing functions as follows:

MPLS VPN-connected site:

- Connects to a site on the same MPLS VPN; the optimal route is direct within the MPLS VPN (traffic is not sent to the primary site).
- Connects to any other site; the route is through the primary site.

The use of the dual WAN transports is specifically tuned to behave in an active/standby manner. This type of configuration provides symmetric routing, with traffic flowing along the same path in both directions. Symmetric routing simplifies troubleshooting because bidirectional traffic flows always traverse the same links.

The design assumes that one of the MPLS VPN WAN transports is designated as the primary transport, which is the preferred path in most conditions.

MPLS VPN primary + MPLS VPN secondary dual-connected site:

- Connects to a site on the same MPLS VPN; the optimal route is direct within the MPLS VPN (traffic is not sent to the primary site).
- Connects to any other site; the route is through the primary site.

MPLS VPN + DMVPN dual-connected site:

- Connects to a site on the same MPLS VPN; the optimal route is direct within the MPLS VPN (traffic is not sent to the primary site).
- Connects to any DMVPN single-connected site; the optimal route is direct within the DMVPN (only initial traffic is sent to the DMVPN hub, and then is cut through via spoke-spoke tunnel).
- Connects to any other site; the route is through the primary site.

Data Privacy (Encryption)

All remote-site traffic must be encrypted when transported over public IP networks such as the Internet.

The use of encryption should not limit the performance or availability of a remote-site application, and should be transparent to end users.

Quality of Service (QoS)

The network must ensure that business applications perform across the WAN during times of network congestion. Traffic must be classified and queued and the WAN connection must be shaped to operate within the capabilities of the connection. When the WAN design uses a service provider offering with QoS, the WAN edge QoS classification and treatment must align to the service provider offering to ensure consistent end-to-end QoS treatment of traffic.

Application Optimization

Most business application traffic from the WAN-aggregation site to any remote site, or any traffic from a remote site to any other remote site, should be optimized.

The use of application optimization should be transparent to end users. The application optimization design should include high-availability components to complement other high-availability components of the WAN design.

Design Parameters

This deployment guide uses certain standard design parameters and references various network infrastructure services that are not located within the WAN. These parameters are listed in the following table.

Table 6 - Universal design parameters

Network service	IP address
Domain name	cisco.local
Active Directory, DNS server, DHCP server	10.4.48.10
Access Control System (ACS)	10.4.48.15
Network Time Protocol (NTP) server	10.4.48.17

Notes

Deploying an MPLS WAN

Business Overview

For remote-site users to effectively support the business, organizations require that the WAN provide sufficient performance and reliability. Although most of the applications and services that the remote-site worker uses are centrally located, the WAN design must provide a common resource access experience to the workforce regardless of location.

To control operational costs, the WAN must support the convergence of voice, video, and data transport onto a single, centrally managed infrastructure. As organizations move into multinational or global business markets, they require a flexible network design that allows for country-specific access requirements and controls complexity. The ubiquity of carrier-provided MPLS networks makes it a required consideration for an organization building a WAN.

To reduce the time needed to deploy new technologies that support emerging business applications and communications, the WAN architecture requires a flexible design. The ability to easily scale bandwidth or to add additional sites or resilient links makes MPLS an effective WAN transport for growing organizations.

Technology Overview

WAN 500 Design

The WAN 500 design is intended to support up to 500 remote sites with a combined aggregate WAN bandwidth of up to 1.0 Gbps. The most critical devices are the WAN routers that are responsible for reliable IP forwarding and QoS. This design uses the Cisco ASR1002 Aggregation Services Router configured with an Embedded Service Processor 5 (ESP5) for the MPLS CE router.

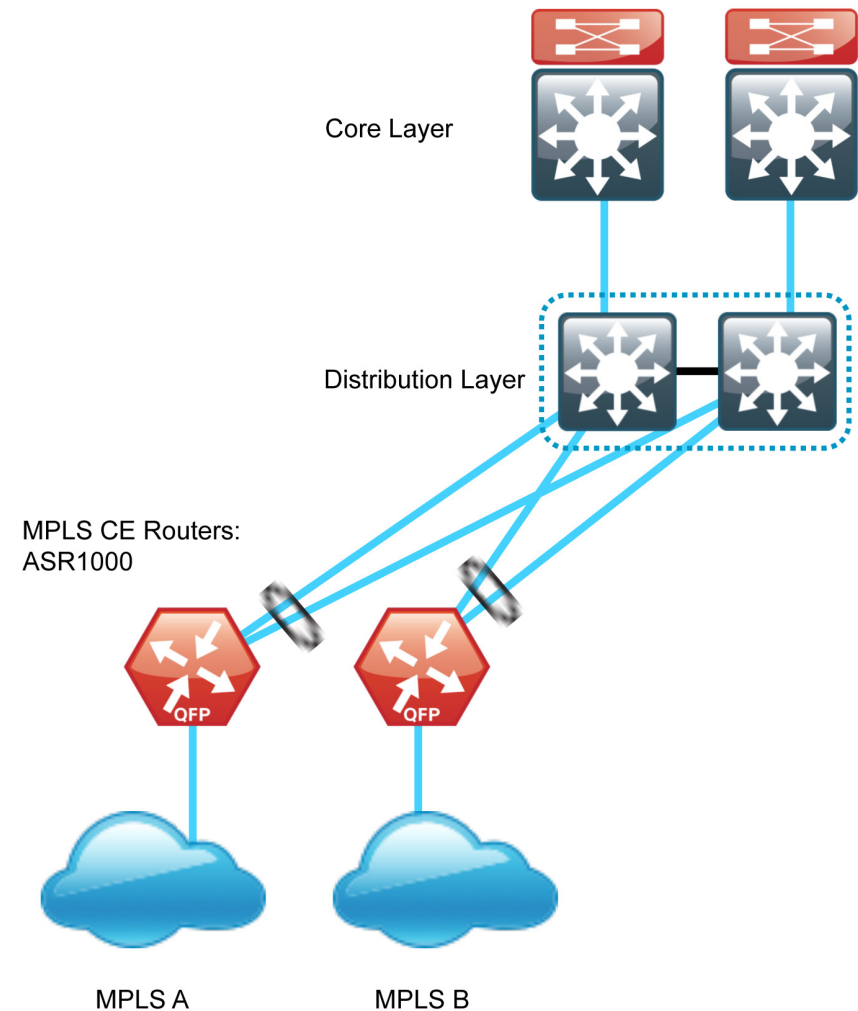
The WAN 500 design uses dual MPLS carriers and dual MPLS CE routers.

The Cisco ASR 1000 Series Aggregation Services Routers represent the next-generation, modular, services-integrated Cisco routing platform. They are specifically designed for WAN aggregation, with the flexibility to support

a wide range of 3- to 16-mpps packet-forwarding capabilities, 2.5- to 40-Gbps system bandwidth performance, and scaling.

The Cisco ASR 1000 Series is fully modular from both hardware and software perspectives, and the routers have all the elements of a true carrier-class routing product that serves both enterprise and service provider networks.

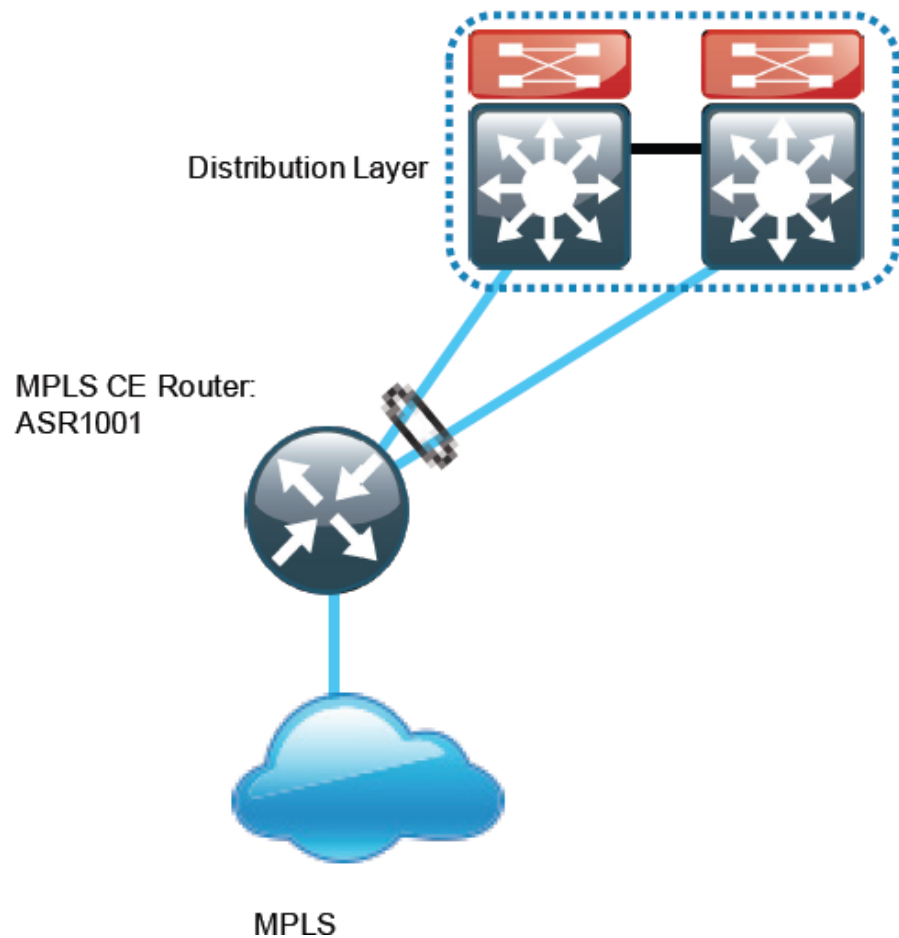
Figure 9 - WAN 500 design—MPLS Connections



WAN 100 Design

The WAN 100 design is intended to support up to 100 remote sites with a combined aggregate WAN bandwidth of up to 100 Mbps. The WAN 100 design is essentially a smaller version of the WAN 500 design. This variant is included to provide a limited scale option. If further growth in bandwidth or an increase in the number of sites is expected, then the WAN 500 design should be used. Using the larger design can prevent unnecessary downtime associated with device upgrades. This design uses the Cisco ASR 1001 for the MPLS CE router. The WAN 100 design uses a single MPLS carrier and a single MPLS CE router.

Figure 10 - WAN 100 design—MPLS connection



Remote Sites—MPLS CE Router Selection

The actual WAN remote-site routing platforms remain unspecified because the specification is tied closely to the bandwidth required for a location and the potential requirement for the use of service module slots. The ability to implement this solution with a variety of potential router choices is one of the benefits of a modular design approach.

There are many factors to consider in the selection of the WAN remote-site routers. Among those, and key to the initial deployment, is the ability to process the expected amount and type of traffic. You also need to make sure that you have enough interfaces, enough module slots, and a properly licensed Cisco IOS Software image that supports the set of features that is required by the topology. Cisco tested five integrated service router models as MPLS CE routers and the expected performance is shown in the following table.

Table 7 - WAN remote-site integrated service router options

Option	1941 ¹	2911	2921	3925	3945
Ethernet WAN with services ²	25 Mbps	35 Mbps	50 Mbps	100 Mbps	150 Mbps
On-board GE ports	2	3	3	3	3
Service module slots ³	0	1	1	2	4
Redundant power supply option	No	No	No	Yes	Yes

Notes:

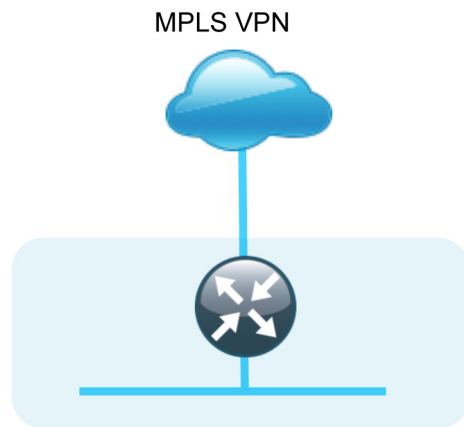
1. The 1941 is recommended for use at single-router, single-link remote sites.
2. The performance numbers are conservative numbers obtained when the router is passing IMIX traffic with heavy services configured and the CPU utilization is under 75 percent.
3. Some service modules are double-wide.

The MPLS CE routers at the WAN remote sites connect in the same manner as the MPLS CE routers at the WAN-aggregation site. The single link MPLS WAN remote site is the most basic of building blocks for any remote location. This design can be used with the CE router connected directly to the access layer, or can support a more complex LAN topology by connecting the CE router directly to a distribution layer.

The IP routing is straightforward and can be handled entirely by using static routes at the WAN-aggregation site and static default routes at the remote site. However, there is significant value to configuring this type of site with dynamic routing.

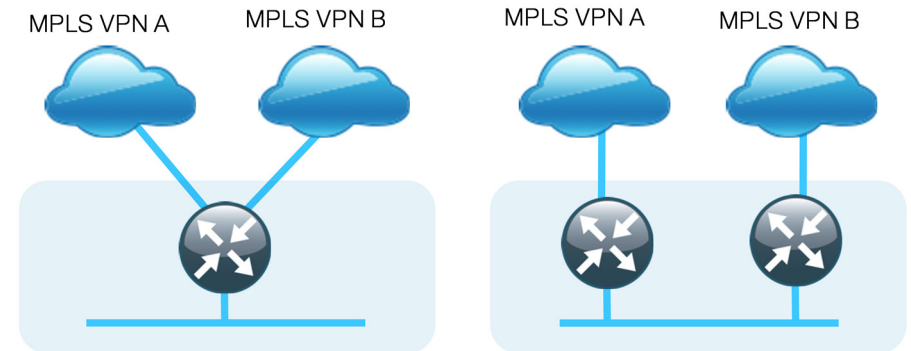
Dynamic routing makes it easy to add or modify IP networks at the remote site because any changes are immediately propagated to the rest of the network. MPLS VPN-connected sites require static routing to be handled by the carrier, and any changes or modifications require a change request to the carrier.

Figure 11 - MPLS WAN remote site (single-router, single-link)



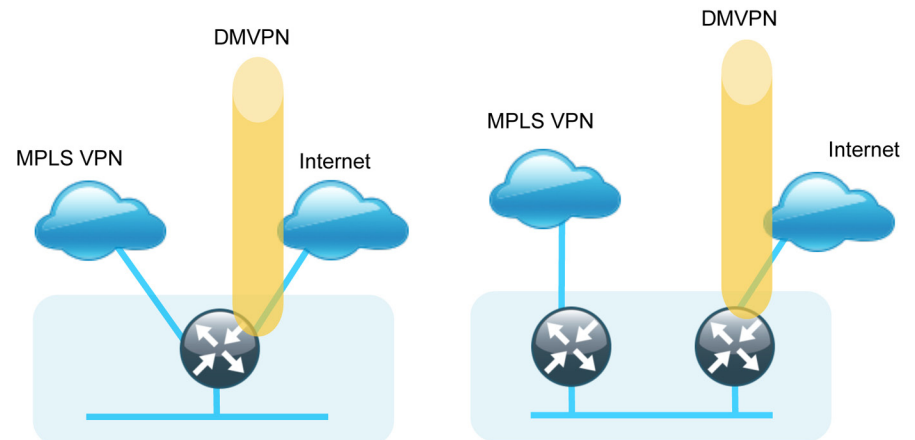
You can augment the basic single-link design by adding an alternate WAN transport that uses a secondary MPLS carrier or DMVPN over Internet and either connects on the same router or on an additional router. By adding an additional link, you provide the first level of high availability for the remote site. The router can automatically detect failure of the primary link and reroute traffic to the secondary path. It is mandatory to run dynamic routing when there are multiple paths. The routing protocols are tuned to ensure that the desired traffic flows.

Figure 12 - MPLS WAN dual-carrier remote site (dual-link options)



The dual-router, dual-link design continues to improve upon the level of high availability for the site. This design can tolerate the loss of the primary router because the secondary router reroutes traffic via the alternate path.

Figure 13 - MPLS WAN + DMVPN remote site (dual-link options)



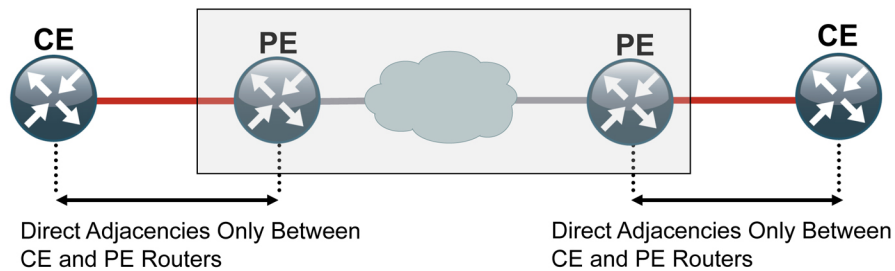
Design Details

All WAN-aggregation MPLS CE routers connect to the same resilient switching device in the distribution layer. All devices use EtherChannel connections consisting of two port bundles. This design provides both resiliency and additional forwarding performance. You can accomplish additional forwarding performance by increasing the number of physical links within an EtherChannel.

WAN transport via Ethernet is the only media type tested and included in the configuration section. Other media types are commonly used (such as T1/E1), and these technologies are reliable and well understood. Due to the multiplicity of potential choices for transport, media type, and interface type, we decided to limit the focus of this deployment guide. Documentation of additional variants is available in other guides.

MPLS VPNs require a link between a provider edge (PE) router and a CE router. The PE and CE routers are considered IP neighbors across this link. CE routers are only able to communicate with other CE routers across the WAN via intermediate PE routers.

Figure 14 - MPLS VPN (PE-CE connections)



Both the PE and CE routers are required to have sufficient IP-routing information to provide end-to-end reachability. Maintaining this routing information typically requires a routing protocol, and BGP is most commonly used for this purpose. The various CE routers advertise their routes to the PE routers. The PE routers propagate the routing information within the carrier network and in turn re-advertise the routes back to other CE routers. This propagation of routing information is known as *dynamic PE-CE routing* and it is essential when any sites have multiple WAN transports (often referred to as dual-homed or multi-homed).

!

Tech Tip

EIGRP and Open Shortest Path First (OSPF) Protocol are also effective as PE-CE routing protocols, but may not be universally available across all MPLS VPN carriers.

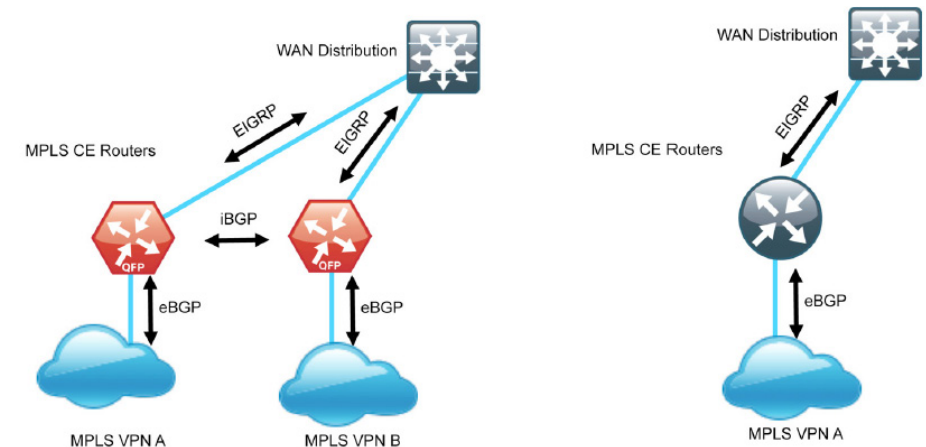
Sites with only a single WAN transport (a single-homed site) do not require dynamic PE-CE routing, and can rely on static routing because there is only a single path to any destination. This design only includes dynamic PE-CE routing to provide consistency with configurations across both single-homed and dual-homed sites. This also allows for easy transition from a single-homed to a dual-homed remote-site design by adding an additional link to an existing remote site.

Cisco did not test the PE routers and their configurations are not included in this guide.

For an MPLS VPN WAN deployment, you need to install and configure MPLS CE routers at every location, including the WAN-aggregation site, and at every MPLS WAN-connected remote site.

At the WAN-aggregation site, an MPLS CE router must be connected both to the distribution layer and to its respective MPLS carrier. Multiple routing protocols (EIGRP and BGP) are used to exchange routing information, and the routing protocol configurations are tuned from their default settings to influence traffic flows to their desired behavior. The IP routing details for the single and dual MPLS carrier WAN-aggregation topology are shown in the following figure.

Figure 15 - WAN500/WAN100 Designs—MPLS CE Routing Detail



EIGRP

Cisco chose EIGRP as the primary routing protocol because it is easy to configure, does not require a large amount of planning, has flexible summarization and filtering, and can scale to large networks. As networks grow, the number of IP prefixes or routes in the routing tables grows as well. You should program IP summarization on links where logical boundaries exist, such as distribution layer links to the wide area or to a core. By performing IP summarization, you can reduce the amount of bandwidth, processor, and memory necessary to carry large route tables, and reduce convergence time associated with a link failure.

In this design, EIGRP process 100 is the primary EIGRP process and is referred to as EIGRP-100.

EIGRP-100 is used at the WAN-aggregation site to connect to the primary site LAN distribution layer and at WAN remote sites with dual WAN routers or with distribution-layer LAN topologies.

BGP

Cisco chose BGP as the routing protocol for PE and CE routers to connect to the MPLS VPNs because it is consistently supported across virtually all MPLS carriers. In this role, BGP is straightforward to configure and requires little or no maintenance. BGP scales well and you can use it to advertise IP aggregate addresses for remote sites.

To use BGP, you must select an Autonomous System Number (ASN). In this design, we use a private ASN (65511) as designated by the Internet Assigned Numbers Authority (IANA). The private ASN range is 64512 to 65534.

A dual-carrier MPLS design requires an iBGP connection between the CE routers to properly retain routing information for the remote sites.

Deployment Details

The procedures in this section provide examples for some settings. The actual settings and values that you use are determined by your current network configuration.

Table 8 - Common Network Services Used in the Deployment Examples

Service	Address
Hostname:	CE-ASR1002-1
Router Loopback IP address:	10.4.32.241/32
Router Port channel IP Address:	10.4.32.2/30

Process

MPLS CE Router Configuration

1. Configure the Distribution Switch
2. Configure the WAN Aggregation Platform
3. Configure Connectivity to the LAN
4. Connect to MPLS PE Router
5. Configure EIGRP
6. Configure BGP

Procedure 1

Configure the Distribution Switch



Reader Tip

This process assumes that the distribution switch has already been configured following the guidance in the *Cisco SBA for Enterprise Organizations—Borderless Networks LAN Deployment Guide*. Only the procedures required to support the integration of the WAN-aggregation router into the deployment are included.

The LAN distribution switch is the path to the organization's main campus and data center. A Layer 3 port-channel interface connects to the distribution switch to the WAN-aggregation router and the internal routing protocol peers across this interface.



Tech Tip

As a best practice, use the same channel numbering on both sides of the link where possible.

Step 1: Configure the Layer 3 port-channel interface and assign the IP address.

```

interface Port-channel1
  description 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
  no shutdown

```

Step 2: Configure EtherChannel member interfaces.

Configure the physical interfaces to tie to the logical port-channel using the **channel-group** command. The number for the port-channel and channel-group must match.

Also, apply the egress QoS macro that was defined in the platform configuration procedure to ensure traffic is prioritized appropriately.

```

interface GigabitEthernet1/0/1
  description CE-ASR1002-1 Gig0/0/0
  !
interface GigabitEthernet2/0/1
  description CE-ASR1002-1 Gig0/0/1
  !
interface range GigabitEthernet1/0/1, GigabitEthernet2/0/1
  no switchport
  macro apply EgressQoS
  carrier-delay msec 0
  channel-protocol lacp
  channel-group 1 mode active
  logging event link-status

```

```

logging event trunk-status
logging event bundle-status
no shutdown

```

Step 3: Configure the interfaces that are connected to the LAN core to summarize the WAN network range.

```

interface range TenGigabitEthernet1/1/1,
TenGigabitEthernet2/1/1
  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

```

Step 4: Allow the routing protocol to form neighbor relationships across the port channel interface.

```

router eigrp 100
  no passive-interface Port-channel1

```

Procedure 2

Configure the WAN Aggregation Platform

Within this design, there are features and services that are common across all WAN aggregation routers. These are system settings that simplify and secure the management of the solution.

Step 1: Configure the device host name.

Configure the device hostname to make it easy to identify the device.

```

hostname CE-ASR1002-1

```

Step 2: Configure device management protocols.

Secure HTTP (HTTPS) and Secure Shell (SSH) are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Secure management of the LAN device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
    transport input ssh
```

Enable Simple Network Management Protocol (SNMP) to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured both for a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Step 3: Configure secure user authentication.

Enable authentication, authorization and accounting (AAA) for access control. AAA controls all management access to the network infrastructure devices (SSH and HTTPS).



Reader Tip

The AAA server used in this architecture is the Cisco ACS. For more information about ACS configuration, see the *Cisco SBA for Enterprise Organizations—Borderless Networks Network Device Authentication and Authorization Deployment Guide*

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
enable secret c1sco123
service password-encryption
!
username admin password c1sco123
aaa new-model
!
tacacs server TACACS-SERVER-1
    address ipv4 10.4.48.15
    key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
    server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

Step 4: Configure a synchronized clock.

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organizations network.

You should program network devices to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. By configuring console messages, logs, and debug output to provide time stamps on output, you can cross-reference events in a network.

```
ntp server 10.4.48.17
!  
clock timezone PST -8  
clock summer-time PDT recurring  
!  
service timestamps debug datetime msec localtime  
service timestamps log datetime msec localtime
```

When synchronous logging of unsolicited messages and debug output is turned on, console log messages are displayed on the console after interactive CLI output is displayed or printed. With this command, you can continue typing at the device console when debugging is enabled.

```
line con 0  
logging synchronous
```

Step 5: Configure an in-band management interface

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer 3 process and features are also bound to the loopback interface to ensure process resiliency.

The loopback address is commonly a host address with a 32-bit address mask. Allocate the loopback address from the IP address block that the distribution switch summarizes to the rest of the network.

```
interface loopback 0  
ip address 10.4.32.241 255.255.255.255  
ip pim sparse-mode
```

The **ip pim sparse-mode** command will be explained further in step 3.

Bind the SNMP and SSH processes to the loopback interface address for optimal resiliency:

```
snmp-server trap-source Loopback0  
ip ssh source-interface Loopback0  
ip pim register-source Loopback0  
ip tacacs source-interface Loopback0  
ntp source Loopback0
```

Step 6: Configure IP unicast routing.

EIGRP is configured facing the LAN distribution or core layer. In this design, the port-channel interface and the loopback must be EIGRP interfaces. The loopback may remain a passive interface. The network range must include both interface IP addresses, either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address.

```
router eigrp 100  
network 10.4.0.0 0.1.255.255  
no auto-summary  
passive-interface default  
eigrp router-id 10.4.32.241
```

Step 7: Configure IP Multicast routing.

IP Multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than multiple individual unicast streams or a Broadcast stream that would propagate everywhere. IP Telephony MOH and IP Video Broadcast Streaming are two examples of IP Multicast applications.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an IGMP message to their local multicast router. In a traditional IP Multicast design, the local router consults another router in the network that is acting as an RP to map the receivers to active sources so they can join their streams.

In this design, which is based on sparse mode multicast operation, Auto RP is used to provide a simple yet scalable way to provide a highly resilient RP environment.

Enable IP Multicast routing on the platforms in the global configuration mode.

```
ip multicast-routing distributed
```

Every Layer 3 switch and router must be configured to discover the IP Multicast RP with autorp. Use the **ip pim autorp listener** command to allow for discovery across sparse mode links. This configuration provides for future scaling and control of the IP Multicast environment and can change based on network needs and design.

```
ip pim autorp listener
```

All Layer 3 interfaces in the network must be enabled for sparse mode multicast operation.

```
ip pim sparse-mode
```

Procedure 3 Configure Connectivity to the LAN

Any links to adjacent distribution layers should be Layer 3 links or Layer 3 EtherChannels.

Step 1: Configure Layer 3 interface.

```
interface Port-channel1
 ip address 10.4.32.2 255.255.255.252
 ip pim sparse-mode
 no shutdown
```

Step 2: Configure EtherChannel member interfaces.

Configure the physical interfaces to tie to the logical port-channel using the channel-group command. The number for the port-channel and channel-group must match.

```
interface GigabitEthernet0/0/0
 description WAN-D3750X Gig1/0/1
!
interface GigabitEthernet0/0/1
 description WAN-D3750X Gig2/0/1
!
interface range GigabitEthernet0/0/0, GigabitEthernet0/0/1
 no ip address
 channel-group 1 mode active
 no shutdown
```

Step 3: Configure the EIGRP interface.

Allow EIGRP to form neighbor relationships across the interface to establish peering adjacencies and exchange route tables.

```
router eigrp 100
 no passive-interface Port-channel 1
```

Procedure 4 Connect to MPLS PE Router

Step 1: Assign the interface bandwidth.

The bandwidth value should correspond to the actual interface speed, or if you are using a substrate service, use the policed rate from the carrier.

The example shows a Gigabit interface (1000 Mbps) with a sub-rate of 300 Mbps.

```
interface GigabitEthernet0/0/3
 bandwidth 300000
```



Reader Tip

Command reference:

bandwidth *kbps*

(300 Mbps = 300000 kbps)

Step 2: Assign the IP address and netmask of the WAN interface.

The IP addressing used between CE and PE routers must be negotiated with your MPLS carrier. Typically a point-to-point netmask of 255.255.255.252 is used.

```
interface GigabitEthernet0/0/3
 ip address 192.168.3.1 255.255.255.252
```

Step 3: Administratively enable the interface and disable CDP.

We do not recommend the use of CDP on external interfaces.

```
interface GigabitEthernet0/0/3
 no cdp enable
 no shutdown
```

Procedure 5 Configure EIGRP

Step 1: Redistribute BGP into EIGRP.

The BGP routes are redistributed into EIGRP with a default metric. By default, only the bandwidth and delay values are used for metric calculation.

```
router eigrp [as number]
 default-metric [bandwidth] [delay] 255 1 1500
 redistribute bgp [BGP ASN]
```



Reader Tip

Command Reference:

default-metric *bandwidth delay reliability loading mtu*

bandwidth—Minimum bandwidth of the route in kilobytes per second

delay—Route delay in tens of microseconds.

Step 2: Configure route-map and inbound distribute-list for EIGRP.

This design uses mutual route redistribution; BGP routes are distributed into EIGRP and EIGRP routes are distributed into BGP (covered in Procedure 5). It is important to tightly control how routing information is shared between different routing protocols when you use this configuration; otherwise, you might experience route flapping, where certain routes are repeatedly installed and with-drawn from the device routing tables. Proper route control ensures the stability of the routing table.

An inbound distribute-list, you use a route-map to limit which routes are accepted for installation into the route table. The WAN-aggregation MPLS CE routers are configured to only accept routes that do not originate from the MPLS or DMVPN WAN sources. To accomplish this task, you must create a route-map that matches any routes originating from the WAN indicated by a specific route tag. This method allows for dynamic identification of the various WAN routes. BGP-learned routes are implicitly tagged with their respective source AS and other WAN routes are explicitly tagged by their WAN-aggregation router (documented in a separate procedure). The specific route tags in use are shown below.

Table 9 - Route tag information for WAN-aggregation MPLS CE routers

Tag	Route source	Tag method	action
65401	MPLS VPN A	implicit	block
65402	MPLS VPN B	implicit	block
300	Layer 2 WAN	explicit	accept
65512	DMVPN hub routers	explicit	block

This example includes all WAN route sources in the reference design. Depending on the actual design of your network, you may need to block more tags.

It is important when creating the route-map that you to include a **permit** statement at the end to permit the installation of routes with non-matching tags.



Tech Tip

If you configure mutual route redistribution without proper matching, tagging, and filtering, route-flapping may occur, which can cause instability.

```
route-map BLOCK-TAGGED-ROUTES deny 10
 match tag 65401 65402 65512
!
route-map BLOCK-TAGGED-ROUTES permit 20
!
router eigrp 100
 distribute-list route-map BLOCK-TAGGED-ROUTES in
 default-metric 100000 100 255 1 1500
 redistribute bgp 65511
```

Step 1: Enable BGP.

To complete this step, you must use a BGP ASN. You can consult with your MPLS carrier on the requirements for the ASN, but you may be permitted to use a private ASN as designated by IANA. The private ASN range is 64512 to 65534.

The CE router only advertises network routes to the PE via BGP when:

- The route is specified in network statements and is present in the local routing table
- The route is redistributed into BGP

```
router bgp 65511
  no synchronization
  bgp router-id 10.4.32.241
  bgp log-neighbor-changes
  no auto-summary
```

Step 2: Configure eBGP.

You must configure BGP with the MPLS carrier PE device. The MPLS carrier must provide their ASN (the ASN in Step 1 is the ASN identifying your site). Because the carrier PE router uses a different ASN, this configuration is considered an external BGP (eBGP) connection.

It is desirable to advertise a route for the PE-CE link, so you should include this network in a network statement. You can use this to determine router reachability for troubleshooting.

```
router bgp 65511
  network 192.168.3.0 mask 255.255.255.252
  neighbor 192.168.3.2 remote-as 65401
```

Step 3: Redistribute EIGRP into BGP.

All EIGRP routes learned by the CE router, including routes from the core and for other WAN sites, should be advertised into the WAN. It is most efficient if you summarize these routes before they are advertised to the CE router.

Because BGP does not propagate a default route via redistribution, you must explicitly specify 0.0.0.0 in a network statement.

```
router bgp 65511
  network 0.0.0.0
  redistribute eigrp 100
```

Step 4: Configure iBGP (Optional).

With dual MPLS carriers, a BGP link is configured between the CE routers.

Since the CE routers are using the same ASN, this configuration is considered an internal BGP (iBGP) connection. This design uses iBGP peering using device loopback addresses, which requires the update-source and next-hop-self-configuration options.

```
router bgp 65511
  neighbor 10.4.32.242 remote-as 65511
  neighbor 10.4.32.242 update-source Loopback0
  neighbor 10.4.32.242 next-hop-self
```


Process

Remote-Site MPLS CE Router Configuration

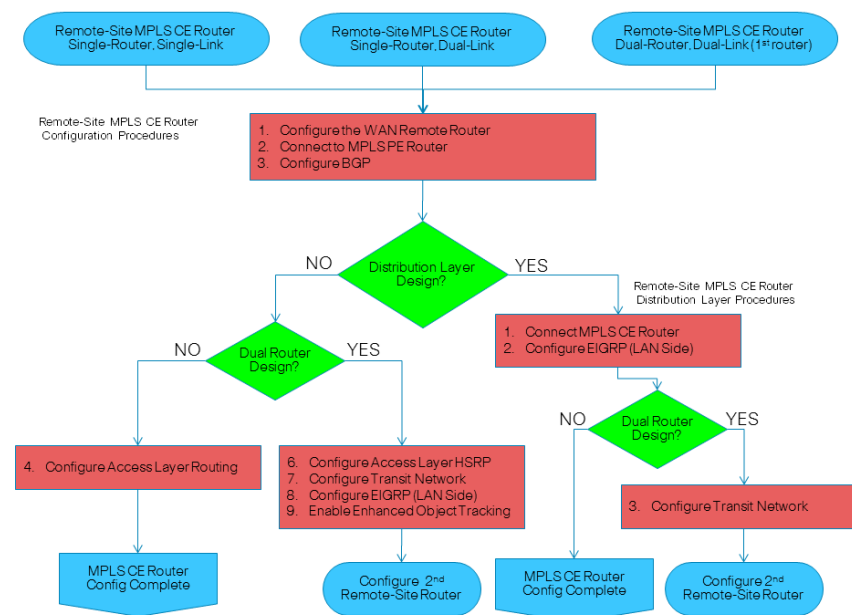
1. Configure the WAN Remote Router
2. Connect to the MPLS PE Router
3. Configure BGP
4. Configure Access Layer Routing
5. Configure Access Layer HSRP
6. Configure Transit Network
7. Configure EIGRP (LAN Side)
8. Enable Enhanced Object Tracking

Use this process for the configuration of any of the following:

- MPLS CE router for a MPLS WAN remote site (single router, single link).
- MPLS WAN Dual Carrier remote site. Use these procedures when performing the initial configuration of a dual-connected MPLS CE in the single-router, dual-link design or for configuring the first router of the dual-router, dual-link design.
- MPLS WAN + DMVPN remote site. Use these procedures when performing the initial configuration of a dual-role MPLS CE and DMVPN spoke router in the single-router, dual-link design.
- The first router of the dual-router, dual-link design.

The following flowchart provides details about the configuration process for a remote-site MPLS CE router.

Figure 16 - Remote-site MPLS CE router configuration flowchart



Procedure 1

Configure the WAN Remote Router

Within this design, there are features and services that are common across all WAN remote site routers. These are system settings that simplify and secure the management of the solution.

Step 1: Configure the device host name to make it easy to identify the device.

```
hostname [hostname]
```

Step 2: Configure device management protocols.

Secure HTTP (HTTPS) and Secure Shell (SSH) are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Secure management of the LAN device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
    transport input ssh
```

Enable Simple Network Management Protocol (SNMP) to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured both for a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Step 3: Configure secure user authentication.

Enable authentication, authorization, and accounting (AAA) for access control. AAA controls all management access to the network infrastructure devices (SSH and HTTPS).



Reader Tip

The AAA server used in this architecture is the Cisco Access Control System. For details about ACS configuration, see the *Cisco SBA for Enterprise Organizations—Borderless Networks Network Device Authentication and Authorization Deployment Guide*.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
enable secret cisco123
service password-encryption
!
username admin password cisco123
aaa new-model
!
tacacs server TACACS-SERVER-1
    address ipv4 10.4.48.15
    key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
    server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

Step 4: Configure a synchronized clock.

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organization's network.

You should program network devices to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. By configuring console messages, logs, and debug output to provide time stamps on output, you can cross-reference events in a network.

```
ntp server 10.4.48.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time  PDT  recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

When synchronous logging of unsolicited messages and debug output is turned on, console log messages are displayed on the console after interactive CLI output is displayed or printed. With this command, you can continue typing at the device console when debugging is enabled.

```
line con 0
logging synchronous
```

Step 5: Configure an in-band management interface.

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer 3 process and features are also bound to the loopback interface to ensure process resiliency.

The loopback address is commonly a host address with a 32-bit address mask. Allocate the remote site router loopback IP address from a unique network range that is not part of any other internal network summary range.

```
interface Loopback0
ip address [ip address] 255.255.255.255
ip pim sparse-mode
```

The **ip pim sparse-mode** command will be explained further in the process.

Bind the SNMP and SSH processes to the loopback interface address for optimal resiliency:

```
snmp-server trap-source Loopback 0
ip ssh source-interface Loopback 0
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
ntp source Loopback0
```

Step 6: Configure IP Multicast routing.

IP Multicast allows a single IP data stream to be replicated by the infrastructure (that is, routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than multiple individual unicast streams or a broadcast stream that would propagate everywhere. IP Telephony MOH and IP Video Broadcast Streaming are two examples of IP Multicast applications.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an IGMP message to their local multicast router. In a traditional IP Multicast design, the local router consults another router in the network that is acting as an RP to map the receivers to active sources so they can join their streams.

In this design, which is based on sparse mode multicast operation, Auto RP is used to provide a simple yet scalable way to provide a highly resilient RP environment.

Enable IP Multicast routing on the platforms in the global configuration mode.

```
ip multicast-routing
```

Every Layer 3 switch and router must be configured to discover the IP Multicast RP with autorp. Use the **ip pim autorp listener** command to allow for discovery across sparse mode links. This configuration provides for future scaling and control of the IP Multicast environment and can change based on network needs and design.

```
ip pim autorp listener
```

All Layer 3 interfaces in the network must be enabled for sparse mode multicast operation.

```
ip pim sparse-mode
```

Procedure 2

Connect to the MPLS PE Router

Step 1: Assign the interface bandwidth.

The bandwidth value should correspond to the actual interface speed, or if a sub-rate service is used, then the policed rate from the carrier should be used.

The example shows a Gigabit interface (1000 Mbps) with a sub-rate of 10 Mbps.

```
interface [interface type] [number]
bandwidth [bandwidth (kbps)]
```



Reader Tip

Command Reference:

bandwidth *kbps*

10 Mbps = 10000 kbps

Step 2: Assign the IP address and netmask of the WAN interface.

The IP addressing used between CE and PE routers must be negotiated with your MPLS carrier. Typically a point-to-point netmask of 255.255.255.252 is used.

```
interface [interface type] [number]
ip address [IP address] [netmask]
```

Step 3: Administratively enable the interface and disable CDP.

We do not recommend the use of CDP on external interfaces.

```
interface [interface type] [number]
no cdp enable
no shutdown
```

Example

```
interface GigabitEthernet0/0
bandwidth 10000
ip address 192.168.3.9 255.255.255.252
no cdp enable
no shutdown
```

Procedure 3

Configure BGP

Step 1: Enable BGP.

To complete this step, a BGP ASN is required. You might be able to reuse the same value used on the MPLS VPN CE from the WAN-aggregation site. Consult with your MPLS carrier on the requirements for the ASN.

The CE router only advertises network routes to the PE via BGP in the following cases:

- The route is specified in network statements and is present in the local routing table
- The route is redistributed into BGP (not applicable in the remote-site use case)

```
router bgp 65511
no synchronization
bgp router-id [IP address of Loopback0]
bgp log-neighbor-changes
no auto-summary
```

Step 2: Configure eBGP.

You must configure BGP with the MPLS carrier PE device. The MPLS carrier must provide their ASN (the ASN in Step 1 is the ASN identifying your site). Since the carrier PE router will use a different ASN, this configuration is considered an external BGP (eBGP) connection.

It is desirable to advertise a route for the PE-CE link, so you should include this network in a network statement. You can use this to determine router reachability for troubleshooting.

You must advertise the remote-site LAN networks. The IP assignment for the remote sites was designed so that all of the networks in use can be summarized within a single aggregate route. The aggregate address as configured below suppresses the more specific routes. If any LAN network is present in the route table, the aggregate is advertised to the MPLS PE, which offers a measure of resiliency. If the various LAN networks cannot be summarized, you must list each individually.

```
router bgp 65511
network [PE-CE link network] mask [PE-CE link netmask]
network [DATA network] mask [netmask]
network [VOICE network] mask [netmask]
network [WLAN DATA network] mask [netmask]
network [WLAN VOICE network] mask [netmask]
aggregate-address [summary IP address] [summary netmask]
summary-only
neighbor [IP address of PE] remote-as [carrier ASN]
```

Example

```
router bgp 65511
  no synchronization
  bgp router-id 10.5.8.254
  bgp log-neighbor-changes
  network 192.168.3.8 mask 255.255.255.252
  network 10.5.10.0 mask 255.255.255.0
  network 10.5.11.0 mask 255.255.255.0
  network 10.5.12.0 mask 255.255.255.0
  network 10.5.13.0 mask 255.255.255.0
  aggregate-address 10.5.8.0 255.255.248.0 summary-only
  neighbor 192.168.3.10 remote-as 65401
  no auto-summary
```

Procedure 4 Configure Access Layer Routing

In the access layer design, the remote sites use collapsed routing, with 802.1Q trunk interfaces to the LAN access layer. The VLAN numbering is locally significant only. The access switches are Layer 2 only.

Step 1: Enable the physical interface.

```
interface GigabitEthernet [number]
  no ip address
  no shutdown
```

Step 2: Create subinterfaces and assign VLAN tags.

After the physical interface has been enabled, then the appropriate data or voice subinterfaces can be mapped to the VLANs on the LAN switch. The subinterface number does not need to equate to the 802.1Q tag, but making them the same simplifies the overall configuration. The subinterface portion of the configuration should be repeated for all data or voice VLANs.

```
interface GigabitEthernet [number].[sub-interface number]
  encapsulation dot1q [dot1q VLAN tag]
```

Step 3: Configure IP settings for each subinterface.

This design uses an IP addressing convention with the default gateway router assigned an IP address and IP mask combination of **N.N.N.1 255.255.255.0** where N.N.N is the IP network and 1 is the IP host.

All router LAN interfaces that use DHCP for end-station IP assignment must use an IP helper to reach a centralized DHCP server in this design.

If the remote-site router is the first router of a dual-router design, then HSRP is configured at the access layer. This requires a modified IP configuration on each subinterface.

```
interface GigabitEthernet [number].[sub-interface number]
  encapsulation dot1q [dot1q VLAN tag]
  ip address [LAN network 1] [LAN network 1 netmask]
  ip helper-address 10.4.48.10
  ip pim sparse-mode
```

Example

```
interface GigabitEthernet0/2
  no ip address
  no shutdown
!
interface GigabitEthernet0/2.64
  description Data
  encapsulation dot1q 64
  ip address 10.5.12.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
!
interface GigabitEthernet0/2.65
  description WirelessData
  encapsulation dot1q 65
  ip address 10.5.10.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
!
interface GigabitEthernet0/2.69
  description Voice
  encapsulation dot1q 69
  ip address 10.5.13.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
!
```

```

interface GigabitEthernet0/2.70
description WirelessVoice
encapsulation dot1Q 70
ip address 10.5.11.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode

```

Step 4: Configure the trunk on the LAN switch.

Use an 802.1Q trunk for the connection to this upstream device, which allows the device to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access switch. DHCP Snooping and Address Resolution Protocol (ARP) inspection are set to trust.

```

interface GigabitEthernet [number]
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 64,65,69,70
switchport mode trunk
macro apply EgressQoS
ip arp inspection trust
ip dhcp snooping trust
logging event link-status
no shutdown

```

The Catalyst 2960-S and 4500 do not require the **switchport trunk encapsulation dot1q** command.

The following procedures (Procedure 11 through Procedure 14) are only relevant for the dual-router design.

The router with the higher standby priority value is elected as the HSRP active router. The preempt option allows a router with a higher priority to become the HSRP active, without waiting for a scenario where there is no router in the HSRP active state. The relevant HSRP parameters for the router configuration are shown in the following table.

Table 10 - WAN remote-site HSRP parameters (dual router)

Router	HSRP role	Virtual IP address (VIP)	Real IP address	HSRP priority	PIM DR priority
MPLS CE (primary)	Active	.1	.2	110	110
MPLS CE (secondary) or DMVPN spoke	Standby	.1	.3	105	105

The assigned IP addresses override those configured in the previous procedure, so the default gateway IP address remains consistent across locations with single or dual routers.

The dual-router access-layer design requires a modification for resilient multicast. The PIM designated router (DR) should be on the HSRP active router. The DR is normally elected based on the highest IP address, and has no awareness of the HSRP configuration. In this design, the HSRP active router has a lower real IP address than the HSRP standby router, which requires a modification to the PIM configuration. The PIM DR election can be influenced by explicitly setting the DR priority on the LAN-facing subinterfaces for the routers.



Tech Tip

The HSRP priority and PIM DR priority are shown in the previous table to be the same value; however, you are not required to use identical values.

Procedure 5 Configure Access Layer HSRP

Applies to Dual-Router Design Only

You need to configure HSRP to enable the use of a Virtual IP (VIP) as a default gateway that is shared between two routers. The HSRP active router is the MPLS CE router connected to the primary MPLS carrier and the HSRP standby router is the router connected to the secondary MPLS carrier or backup link. Configure the HSRP active router with a standby priority that is higher than the HSRP standby router.

This procedure should be repeated for all data or voice subinterfaces.

```
interface GigabitEthernet [number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [LAN network 1 address] [LAN network 1 netmask]
 ip helper-address 10.4.48.10
 ip pim sparse-mode
 ip pim dr-priority 110
 standby 1 ip [LAN network 1 gateway address]
 standby 1 priority 110
 standby 1 preempt
```

Example

```
interface GigabitEthernet0/2
 no ip address
 no shutdown
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.12.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby 1 ip 10.5.12.1
 standby 1 priority 110
 standby 1 preempt
!
interface GigabitEthernet0/2.65
 description WirelessData
 encapsulation dot1Q 65
 ip address 10.5.10.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby 1 ip 10.5.10.1
 standby 1 priority 110
 standby 1 preempt
```

```
!
interface GigabitEthernet0/2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.13.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby 1 ip 10.5.13.1
 standby 1 priority 110
 standby 1 preempt
!
interface GigabitEthernet0/2.70
 description WirelessVoice
 encapsulation dot1Q 70
 ip address 10.5.11.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby 1 ip 10.5.11.1
 standby 1 priority 110
 standby 1 preempt
```

Procedure 6

Configure Transit Network

Applies to Dual-Router Design Only

The transit network is configured between the two routers. This network is used for router-router communication and to avoid hair-pinning. The transit network should use an additional subinterface on the router interface that is already being used for data or voice.

There are no end stations connected to this network, so HSRP and DHCP are not required.

```
interface GigabitEthernet0/2 [number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [transit net address] [transit net netmask]
 ip pim sparse-mode
```

Example—MPLS CE Router (primary)

```
interface GigabitEthernet0/2.99
description Transit Net
encapsulation dot1Q 99
ip address 10.5.8.1 255.255.255.252
ip pim sparse-mode
```

Procedure 7 Configure EIGRP (LAN Side)

Applies to Dual-Router Design Only

You must configure a routing protocol between the two routers. This ensures that the HSRP active router has full reachability information for all WAN remote sites.

Step 1: Enable EIGRP-100.

Configure EIGRP-100 facing the access layer. In this design, all LAN-facing interfaces and the loopback must be EIGRP interfaces. All interfaces except the transit-network subinterface should remain passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address. Do not include the WAN interface (MPLS PE-CE link interface) as an EIGRP interface.

```
router eigrp 100
network [network] [inverse mask]
passive-interface default
no passive-interface [Transit interface]
eigrp router-id [IP address of Loopback0]
no auto-summary
```

Step 2: Redistribute BGP into EIGRP-100.

The BGP routes are redistributed into EIGRP with a default metric. By default, only the bandwidth and delay values are used for metric calculation.

```
router eigrp 100
default-metric [bandwidth] [delay] 255 1 1500
redistribute bgp 65511
```



Reader Tip

Command Reference:

default-metric *bandwidth delay reliability loading mtu*

bandwidth—Minimum bandwidth of the route in kilobytes per second

delay—Route delay in tens of microseconds.

Example

```
router eigrp 100
default-metric 100000 100 255 1 1500
network 10.4.0.0 0.1.255.255
redistribute bgp 65511
passive-interface default
no passive-interface GigabitEthernet0/2.99
eigrp router-id 10.5.48.254
no auto-summary
```

Procedure 8

Enable Enhanced Object Tracking

Applies to Dual-Router Design Only

The HSRP active router remains the active router unless the router is reloaded or fails. Having the HSRP router remain as the active router can lead to undesired behavior. If the primary MPLS VPN transport were to fail, the HSRP active router would learn an alternate path through the transit network to the HSRP standby router and begin to forward traffic across the alternate path. This is sub-optimal routing, and you can address it by using EOT.

The HSRP active router (primary MPLS CE) can use the IP SLA feature to send echo probes to its MPLS PE router and if the PE router becomes unreachable, then the router can lower its HSRP priority, so that the HSRP standby router can preempt and become the HSRP active router.

This procedure is valid only on the router connected to the primary transport (MPLS VPN).

Step 1: Enable the IP SLA probe.

Use standard ICMP echo (ping) probes, and send them at 15 second intervals. Responses must be received before the timeout of 1000 ms expires. If using the MPLS PE router as the probe destination, the destination address is the same as the BGP neighbor address configured in Procedure 3.

```
ip sla 100
  icmp-echo [probe destination IP address] source-interface
  [WAN interface]
  timeout 1000
  threshold 1000
  frequency 15
ip sla schedule 100 life forever start-time now
```

Step 2: Configure EOT.

A tracked object is created based on the IP SLA probe. The object being tracked is the reachability success or failure of the probe. If the probe is successful, the tracked object status is Up; if it fails, the tracked object status is Down.

```
track 50 ip sla 100 reachability
```

Step 3: Link HSRP with the tracked object.

All data or voice subinterfaces should enable HSRP tracking.

HSRP can monitor the tracked object status. If the status is down, the HSRP priority is decremented by the configured priority. If the decrease is large enough, the HSRP standby router preempts.

```
interface [interface type] [number].[sub-interface number]
  standby 1 track 50 decrement 10
```

Example

```
interface range GigabitEthernet0/2.64, GigabitEthernet0/2.65,
GigabitEthernet0/2.69, GigabitEthernet0/2.70
  standby 1 track 50 decrement 10
!
track 50 ip sla 100 reachability
!
ip sla 100
  icmp-echo 192.168.3.10 source-interface GigabitEthernet0/0
  timeout 1000
  threshold 1000
  frequency 15
ip sla schedule 100 life forever start-time now
```

Process

Adding Secondary MPLS Link on Existing MPLS CE Router

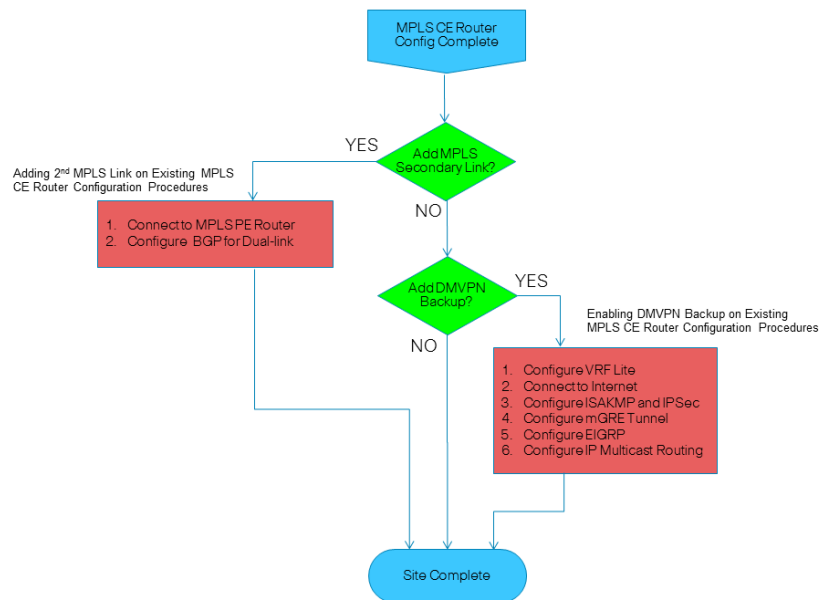
1. Connect to MPLS PE Router
2. Configure BGP for Dual-link

This set of procedures includes the additional steps necessary to complete the configuration of a MPLS CE router for a MPLS WAN dual-carrier remote site (single-router, dual-link).

The following procedures assume that the configuration of a MPLS CE Router for a MPLS WAN remote site (single-router, single-link) has already been completed. Only the additional procedures to add an additional MPLS link to the running MPLS CE router are included here.

The following flowchart provides details on how to add a second MPLS backup link on an existing remote-site MPLS CE router.

Figure 17 - Adding MPLS backup configuration flowchart



Procedure 1 Connect to MPLS PE Router

This procedure applies to the interface used to connect the secondary or additional MPLS carrier.

Step 1: Assign the interface bandwidth.

The bandwidth value should correspond to the actual interface speed, or if you are using a sub-rate service, use the policed rate from the carrier.

The example shows a Gigabit interface (1000 Mbps) with a subrate of 10 Mbps.

```
interface [interface type] [number]
bandwidth [bandwidth (kbps)]
```



Reader Tip

Command Reference:

bandwidth *kbps*

10 Mbps = 10000 kbps

Step 2: Assign the IP address and netmask of the WAN interface.

The IP addressing used between CE and PE routers must be negotiated with your MPLS carrier. Typically, a point-to-point netmask of 255.255.255.252 is used.

```
interface [interface type] [number]
ip address [IP address] [netmask]
```

Step 3: Administratively enable the interface and disable Cisco Discovery Protocol.

Cisco does not recommend that you use the Cisco Discovery Protocol on external interfaces.

```
interface [interface type] [number]
no cdp enable
no shutdown
```

Example

```
interface GigabitEthernet0/1
bandwidth 10000
ip address 192.168.4.13 255.255.255.252
ip pim sparse-mode
no cdp enable
no shutdown
```

Procedure 2

Configure BGP for Dual-link

Step 1: Configure eBGP to add an additional eBGP neighbor and advertise the PE-CE link.

BGP must be configured with the MPLS carrier PE device. The MPLS carrier must provide their ASN (the ASN in this step is the ASN identifying your site). Since the carrier PE router will use a different ASN, this configuration is considered an external BGP (eBGP) connection.

It is desirable to advertise a route for the PE-CE link, so you should include this network in a network statement. You can use it to determine router reachability for troubleshooting.

The remote-site LAN networks are already advertised based on the configuration already completed in the Remote-Site MPLS CE Router Configuration procedures.

```
router bgp 65511
 network [PE-CE link 2 network] mask [PE-CE link 2 netmask]
 neighbor [IP address of PE 2] remote-as [carrier ASN]
```

Step 2: Configure BGP to prevent the remote site from becoming a transit AS.

By default, BGP readvertises all BGP learned routes. In the dual-MPLS design, this means that MPLS-A routes are advertised to MPLS-B and vice-versa. In certain cases, when a link to a MPLS hub has failed, remote sites will advertise themselves as a transit autonomous system providing access between the two carriers. Unless the remote site has been specifically designed for this type of routing behavior, with a high bandwidth connection, it is a best practice to disable the site from becoming a transit site. To do this, you need to use a route-map and an as-path access-list filter. Apply this route-map outbound to the neighbors for both MPLS carriers.

```
router bgp 65511
 neighbor [IP address of PE] route-map NO-TRANSIT-AS out
 neighbor [IP address of PE 2] route-map NO-TRANSIT-AS out
```

The regular expression “^\$” corresponds to routes originated from the remote-site. This type of filter only allows for the locally originated routes to be advertised.

```
ip as-path access-list 10 permit ^$
!
route-map NO-TRANSIT-AS permit 10
 match as-path 10
```

Step 3: Tune BGP routing to prefer the primary MPLS carrier.

BGP uses a well-known ruleset to determine the “best path” when the same IP route prefix is reachable via two different paths. The MPLS dual-carrier design in many cases provides two equal cost paths, and it is likely that the first path selected will remain the active path unless the routing protocol detects a failure. To accomplish the design goal of deterministic routing and primary/secondary routing behavior necessitates tuning BGP. This requires the use of a route-map and an as-path access-list filter.

```
router bgp 65511
 neighbor [IP address of PE] route-map PREFER-MPLS-A in
```

The regular expression “_65401\$” corresponds to routes originated from the AS 65401 (MPLS-A). This allows BGP to selectively modify the routing information for routes originated from this AS. In this example, the BGP local preference is 200 for the primary MPLS carrier. Routes originated from the secondary MPLS carrier will continue to use their default local preference of 100. Apply this route-map inbound to the neighbor for the primary MPLS carrier only.

```
ip as-path access-list 1 permit _65401$
!
route-map PREFER-MPLS-A permit 10
 match as-path 1
 set local-preference 200
!
route-map PREFER-MPLS-A permit 20
```

Example

```
router bgp 65511
 network 192.168.4.12 mask 255.255.255.252
 neighbor 192.168.3.14 route-map PREFER-MPLS-A in
 neighbor 192.168.3.14 route-map NO-TRANSIT-AS out
 neighbor 192.168.4.14 remote-as 65402
 neighbor 192.168.4.14 route-map NO-TRANSIT-AS out
!
ip as-path access-list 1 permit _65401$
ip as-path access-list 10 permit ^$
!
route-map NO-TRANSIT-AS permit 10
 match as-path 10
!
route-map PREFER-MPLS-A permit 10
 match as-path 1
 set local-preference 200
!
route-map PREFER-MPLS-A permit 20
```

Process

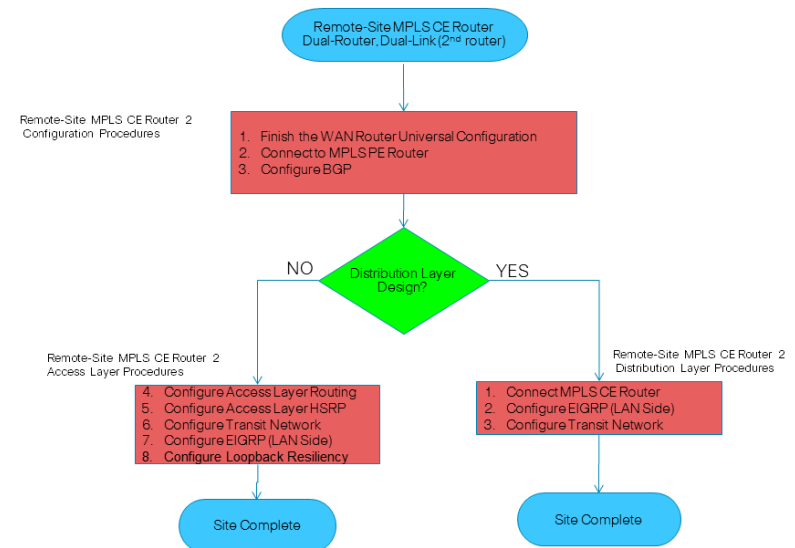
Remote-Site Router Configuration (Dual-Router - Router 2)

1. Finish WAN Router Universal Configuration
2. Connect to the MPLS PE Router
3. Configure BGP
4. Configure Access Layer Routing
5. Configure Access Layer HSRP
6. Configure Transit Network
7. Configure EIGRP (LAN Side)
8. Configure Loopback Resiliency

Use this set of procedures when you configure an MPLS WAN dual-carrier remote-site. Use these procedures when you configure the second MPLS CE router of the dual-router, dual-link design.

The following flowchart provides details about how to configure a remote-site MPLS CE router.

Figure 18 - Remote-site MPLS CE router 2 configuration flowchart



Procedure 1

Finish WAN Router Universal Configuration

Within this design, there are features and services that are common across all WAN remote site routers. These are system settings that simplify and secure the management of the solution.

Step 1: Configure the device host name to make it easy to identify the device.

```
hostname [hostname]
```


Step 2: Configure device management protocols.

Secure HTTP (HTTPS) and Secure Shell (SSH) are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Secure management of the LAN device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
    transport input ssh
```

Simple Network Management Protocol (SNMP) is enabled to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured both for a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Step 3: Configure secure user authentication

Enable authentication, authorization, and accounting (AAA) for access control. AAA controls all management access to the network infrastructure devices (SSH and HTTPS).



Reader Tip

The AAA server used in this architecture is the Cisco Access Control System. For details about configuring ACS, see the *Cisco SBA for Enterprise Organizations—Borderless Networks Network Device Authentication and Authorization Deployment Guide*.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined on each network infrastructure device to provide

a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
enable secret clisco123
service password-encryption
!
username admin password clisco123
aaa new-model
!
tacacs server TACACS-SERVER-1
    address ipv4 10.4.48.15
    key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
    server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

Step 4: Configure a synchronized clock.

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organization's network.

You should program network devices to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. By configuring console messages, logs, and debug output to provide time stamps on output, you can cross-reference events in a network.

```
ntp server 10.4.48.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time  PDT  recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

When synchronous logging of unsolicited messages and debug output is turned on, console log messages are displayed on the console after interactive CLI output is displayed or printed. With this command, you can continue typing at the device console when debugging is enabled.

```
line con 0
logging synchronous
```

Step 5: Configure an in-band management interface.

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer 3 process and features are also bound to the loopback interface to ensure process resiliency.

The loopback address is commonly a host address with a 32-bit address mask. Allocate the remote site router loopback IP address from a unique network range that is not part of any other internal network summary range.

```
interface Loopback0
ip address [ip address] 255.255.255.255
ip pim sparse-mode
```

The **ip pim sparse-mode** command will be explained further in the process.

Bind the SNMP and SSH processes to the loopback interface address for optimal resiliency:

```
snmp-server trap-source Loopback 0
ip ssh source-interface Loopback 0
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
ntp source Loopback0
```

Step 6: Configure IP Multicast routing.

IP Multicast allows a single IP data stream to be replicated by the infrastructure (that is, routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than multiple individual unicast streams or a broadcast stream that would propagate everywhere. IP Telephony MOH and IP Video Broadcast Streaming are two examples of IP Multicast applications.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an IGMP message to their local multicast router. In a traditional IP Multicast design, the local router consults another router in the network that is acting as an RP to map the receivers to active sources so they can join their streams.

In this design, which is based on sparse mode multicast operation, Cisco uses autorp to provide a simple yet scalable way to provide a highly resilient RP environment.

Enable IP Multicast routing on the platforms in the global configuration mode.

```
ip multicast-routing
```

Every Layer 3 switch and router must be configured to discover the IP Multicast RP with autorp. Use the **ip pim autorp listener** command to allow for discovery across sparse mode links. This configuration provides for future scaling and control of the IP Multicast environment and can change based on network needs and design.

```
ip pim autorp listener
```

You must enable all Layer 3 interfaces in the network for sparse mode multicast operation.

```
ip pim sparse-mode
```

Procedure 2

Connect to the MPLS PE Router

Step 1: Assign the interface bandwidth.

The bandwidth value should correspond to the actual interface speed, or if you are using a sub-rate service, use the policed rate from the carrier.

The example shows a Gigabit interface (1000 Mbps) with a sub-rate of 10 Mbps.

```
interface [interface type] [number]
bandwidth [bandwidth (kbps)]
```



Reader Tip

Command Reference:

bandwidth *kbps*

10 Mbps = 10000 kbps

Step 2: Assign the IP address and netmask of the WAN interface.

You must negotiate the IP addressing used between CE and PE routers with your MPLS carrier. Typically, a point-to-point netmask of 255.255.255.252 is used.

```
interface [interface type] [number]
ip address [IP address] [netmask]
```

Step 3: Administratively enable the interface and disable Cisco Discovery Protocol.

Cisco does not recommend that you use Cisco Discovery Protocol on external interfaces.

```
interface [interface type] [number]
no cdp enable
no shutdown
```

Example

```
interface GigabitEthernet0/0
bandwidth 25000
ip address 192.168.4.9 255.255.255.252
no cdp enable
no shutdown
```

Procedure 3 Configure BGP

Step 1: Enable BGP.

To complete this step, you must use a BGP ASN. You might be able to reuse the same value used on the MPLS VPN CE from the WAN-aggregation site.

Consult with your MPLS carrier on the requirements for the ASN.

The CE router only advertises network routes to the PE via BGP in the following cases:

- The route is specified in network statements and is present in the local routing table
- The route is redistributed into BGP (not applicable in the remote-site use case)

```
router bgp 65511
no synchronization
bgp router-id [IP address of Loopback0]
bgp log-neighbor-changes
no auto-summary
```

Step 2: Configure eBGP.

You must configure BGP with the MPLS carrier PE device. The MPLS carrier must provide their ASN (the ASN in Step 1 is the ASN identifying your site). Since the carrier PE router will use a different ASN, this configuration is considered an external BGP (eBGP) connection.

It is desirable to advertise a route for the PE-CE link, so you should include this network in a network statement. You can use this to determine router reachability for troubleshooting.

The remote-site LAN networks must be advertised. The IP assignment for the remote sites was designed so that all of the networks in use can be summarized within a single aggregate route. The aggregate address as configured below suppresses the more specific routes. If any LAN network is present in the route table, the aggregate is advertised to the MPLS PE, which offers a measure of resiliency. If the various LAN networks cannot be summarized, you must list each individually.

```
router bgp 65511
network [PE-CE link network] mask [PE-CE link netmask]
network [DATA network] mask [netmask]
network [VOICE network] mask [netmask]
network [WLAN DATA network] mask [netmask]
network [WLAN VOICE network] mask [netmask]
aggregate-address [summary IP address] [summary netmask]
summary-only
neighbor [IP address of PE] remote-as [carrier ASN]
```

Step 3: Configure iBGP between the remote-site MPLS CE routers.

The dual-carrier MPLS design requires that a BGP link is configured between the CE routers. Since the CE routers are using the same ASN, this configuration is considered an internal BGP (iBGP) connection. This design uses iBGP peering using device loopback addresses, which requires the update-source and next-hop-self configuration options.

You must complete this step on both remote-site MPLS CE routers. Note, the iBGP session will not be established until you complete the transit network and EIGRP (LAN side) steps.

```
router bgp 65511
 neighbor [iBGP neighbor Loopback0] remote-as 65511
 neighbor [iBGP neighbor Loopback0] update-source Loopback0
 neighbor [iBGP neighbor Loopback0] next-hop-self
```

Step 4: Configure BGP to prevent the remote site from becoming a transit AS.

By default, BGP readvertises all BGP learned routes. In the dual-MPLS design, this means that MPLS-A routes will be advertised to MPLS-B and vice-versa. In certain cases, when a link to a MPLS hub has failed, remote sites will advertise themselves as a transit autonomous system providing access between the two carriers. Unless the remote site has been specifically designed for this type of routing behavior, with a high bandwidth connection, it is a best practice to disable the site from becoming a transit site. You must use a route-map and an as-path access-list filter. You need to apply this route-map on both remote-site MPLS CE routers. Each router will apply this outbound to the neighbor for its respective MPLS carrier.

```
router bgp 65511
 neighbor [IP address of PE 2] route-map NO-TRANSIT-AS out
```

The regular expression “^\$” corresponds to routes originated from the remote-site. This type of filter only allows for the locally originated routes to be advertised.

```
ip as-path access-list 10 permit ^$
!
route-map NO-TRANSIT-AS permit 10
 match as-path 10
```

Example - MPLS CE Router (secondary)

```
router bgp 65511
 no synchronization
 bgp router-id 10.5.8.253
 bgp log-neighbor-changes
 network 192.168.4.8 mask 255.255.255.252
 network 10.5.10.0 mask 255.255.255.0
 network 10.5.11.0 mask 255.255.255.0
 network 10.5.12.0 mask 255.255.255.0
 network 10.5.13.0 mask 255.255.255.0
 aggregate-address 10.5.8.0 255.255.248.0 summary-only
 neighbor 10.5.8.254 remote-as 65511
 neighbor 10.5.8.254 update-source Loopback0
 neighbor 10.5.8.254 next-hop-self
 neighbor 192.168.4.10 remote-as 65402
 neighbor 192.168.4.10 route-map NO-TRANSIT-AS out
 no auto-summary
!
ip as-path access-list 10 permit ^$
!
route-map NO-TRANSIT-AS permit 10
 match as-path 10
```

Example - MPLS CE Router (primary)

```
router bgp 65511
 bgp router-id 10.5.8.254
 neighbor 10.5.8.253 remote-as 65511
 neighbor 10.5.8.253 update-source Loopback0
 neighbor 10.5.8.253 next-hop-self
 neighbor 192.168.3.10 route-map NO-TRANSIT-AS out
!
ip as-path access-list 10 permit ^$
!
route-map NO-TRANSIT-AS permit 10
 match as-path 10
```

Procedure 4 **Configure Access Layer Routing**

In the access layer design, the remote-sites use collapsed routing, with 802.1Q trunk interfaces to the LAN access layer. The VLAN numbering is locally significant only. The access switches are Layer 2 only.

Step 1: Enable the physical interface.

```
interface [interface type] [number]
no ip address
no shutdown
```

Step 2: Create subinterfaces and assign VLAN tags.

After you have enabled the physical interface, you can map the appropriate data or voice subinterfaces can be mapped to the VLANs on the LAN switch. The subinterface number does not need to equate to the 802.1Q tag, but making them the same simplifies the overall configuration. The subinterface portion of the configuration should be repeated for all data or voice VLANs.

```
interface [interface type] [number].[sub-interface number]
encapsulation dot1q [dot1q VLAN tag]
```

Step 3: Configure IP settings for each subinterface.

This design uses an IP addressing convention with the default gateway router assigned an IP address and IP mask combination of **N.N.N.1 255.255.255.0** where N.N.N is the IP network and 1 is the IP host.

All router LAN interfaces that use DHCP for end-station IP assignment must use an IP helper to reach a centralized DHCP server in this design.

This remote-site MPLS CE router is the second router of a dual-router design and HSRP is configured at the access layer. The actual interface IP assignments will be configured in the following procedure.

```
interface [interface type] [number].[sub-interface number]
encapsulation dot1q [dot1q VLAN tag]
ip helper-address [IP address of DHCP server]
```

Example

```
interface GigabitEthernet0/2
no ip address
no shutdown
!
!
interface GigabitEthernet0/2.64
description Data
encapsulation dot1q 64
ip helper-address 10.4.48.10
ip pim sparse-mode
!
interface GigabitEthernet0/2.65
description WirelessData
encapsulation dot1q 65
ip helper-address 10.4.48.10
ip pim sparse-mode
!
interface GigabitEthernet0/2.69
description Voice
encapsulation dot1q 69
ip helper-address 10.4.48.10
ip pim sparse-mode
!
interface GigabitEthernet0/2.70
description WirelessVoice
encapsulation dot1q 70
ip helper-address 10.4.48.10
ip pim sparse-mode
```

Procedure 5

Configure Access Layer HSRP

Configure HSRP to use a Virtual IP (VIP) as a default gateway that is shared between two routers. The HSRP active router is the MPLS CE router connected to the primary MPLS carrier and the HSRP standby router is the router connected to the secondary MPLS carrier or backup link. Configure the HSRP active router with a standby priority that is higher than the HSRP standby router.

The router with the higher standby priority value is elected as the HSRP active router. The preempt option allows a router with a higher priority to become the HSRP active, without waiting for a scenario where there is no router in the HSRP active state. The relevant HSRP parameters for the router configuration are shown in the following table.

Table 11 - WAN Remote-Site HSRP Parameters (Dual Router)

Router	HSRP role	Virtual IP address (VIP)	Real IP address	HSRP priority	PIM DR priority
MPLS CE (primary)	Active	.1	.2	110	110
MPLS CE (secondary) or DMVPN Spoke	Standby	.1	.3	105	105

The dual-router access-layer design requires a modification for resilient multicast. The PIM designated router (DR) should be on the HSRP active router. The DR is normally elected based on the highest IP address, and has no awareness of the HSRP configuration. In this design, the HSRP active router has a lower real IP address than the HSRP standby router, which requires a modification to the PIM configuration. The PIM DR election can be influenced by explicitly setting the DR priority on the LAN-facing subinterfaces for the routers.



Tech Tip

The HSRP priority and PIM DR priority are shown in the previous table to be the same value; however, you are not required to use identical values.

Repeat this procedure for all data or voice subinterfaces.

```
interface GigabitEthernet [number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [LAN network 1 address] [LAN network 1 netmask]
 ip helper-address 10.4.48.10
 ip pim sparse-mode
 ip pim dr-priority 110
 standby 1 ip [LAN network 1 gateway address]
 standby 1 priority 110
 standby 1 preempt
```

Example—MPLS CE Router (secondary)

```
interface GigabitEthernet0/2
 no ip address
 no shutdown
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.12.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby 1 ip 10.5.12.1
 standby 1 priority 105
 standby 1 preempt
!
interface GigabitEthernet0/2.65
 description WirelessData
```



```

encapsulation dot1Q 65
ip address 10.5.10.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 105
ip pim sparse-mode
standby 1 ip 10.5.10.1
standby 1 priority 105
standby 1 preempt
!
interface GigabitEthernet0/2.69
description Voice
encapsulation dot1Q 69
ip address 10.5.13.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 105
ip pim sparse-mode
standby 1 ip 10.5.13.1
standby 1 priority 105
standby 1 preempt
!
interface GigabitEthernet0/2.70
description WirelessVoice
encapsulation dot1Q 70
ip address 10.5.11.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 105
ip pim sparse-mode
standby 1 ip 10.5.11.1
standby 1 priority 105
standby 1 preempt

```

Procedure 6 Configure Transit Network

Configure the transit network between the two routers. You use this network for router-router communication and to avoid hairpinning. The transit network should use an additional subinterface on the router interface that is already being used for data or voice.

There are no end stations connected to this network, so HSRP and DHCP are not required.

```

interface [interface type] [number].[sub-interface number]
encapsulation dot1Q [dot1q VLAN tag]
ip address [transit net address] [transit net netmask]

```

Example—MPLS CE Router (secondary)

```

interface GigabitEthernet0/2.99
description Transit Net
encapsulation dot1Q 99
ip address 10.5.8.2 255.255.255.252

```

Procedure 7 Configure EIGRP (LAN Side)

You must configure a routing protocol between the two routers. This ensures that the HSRP active router has full reachability information for all WAN remote sites.

Step 1: Enable EIGRP-100.

Configure EIGRP-100 facing the access layer. In this design, all LAN-facing interfaces and the loopback must be EIGRP interfaces. All interfaces except the transit-network subinterface should remain passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address. Do not include the WAN interface (MPLS PE-CE link interface) as an EIGRP interface.

```

router eigrp 100
network [network] [inverse mask]
passive-interface default
no passive-interface [Transit interface]
eigrp router-id [IP address of Loopback0]
no auto-summary

```

Step 2: Redistribute BGP into EIGRP-100.

The BGP routes are redistributed into EIGRP with a default metric. By default, only the bandwidth and delay values are used for metric calculation.

```
router eigrp 100
  default-metric [bandwidth] [delay] 255 1 1500
  redistribute bgp 65511
```



Reader Tip

Command Reference:

default-metric *bandwidth delay reliability loading mtu*

bandwidth—Minimum bandwidth of the route in kilobytes per second

delay—Route delay in tens of microseconds.

Example

```
router eigrp 100
  default-metric 100000 100 255 1 1500
  network 10.4.0.0 0.1.255.255
  redistribute bgp 65511
  passive-interface default
  no passive-interface GigabitEthernet0/2.99
  eigrp router-id 10.5.48.254
  no auto-summary
```

Procedure 8

Configure Loopback Resiliency

Applies to Dual-Router Design Only

The remote-site routers have in-band management configured via the loopback interface. To ensure reachability of the loopback interface in a dual-router design, redistribute the loopback of the adjacent router into the WAN routing protocol.

If the WAN protocol is EIGRP

Step 1: Configure an access list to limit the redistribution to only the adjacent router's loopback IP address.

```
ip access-list standard R[number]-LOOPBACK
  permit [IP Address of Adjacent Router Loopback]
  !
  route-map LOOPBACK-ONLY permit 10
  match ip address R[number]-LOOPBACK
```

Step 2: Configure EIGRP to redistribute the adjacent router's loopback IP address. The EIGRP stub routing must be adjusted to permit redistributed routes.

```
router eigrp [as]
  redistribute eigrp 100 route-map LOOPBACK-ONLY
  eigrp stub connected summary redistributed
```

If the WAN protocol is BGP

Step 3: Configure BGP to advertise the adjacent router's loopback network

```
router bgp 65511
  network 10.5.12.0 mask 255.255.255.0
  network 10.5.13.0 mask 255.255.255.0
```

Deploying a DMVPN WAN

Business Overview

Organizations require the WAN to provide sufficient performance and reliability for the remote-site users to be effective in supporting the business. Although most of the applications and services that the remote-site worker uses are centrally located, the WAN design must provide the workforce with a common resource-access experience, regardless of location.

Carrier-based MPLS service is not always available or cost-effective for an organization to use for WAN transport to support remote-site connectivity. Internet-based IP VPNs provide an optional transport that you can use as a resilient backup to a primary MPLS network transport or may be adequate to provide the primary network transport for a remote site. Flexible network architecture should include Internet VPN as a transport option without significantly increasing the complexity of the overall design.

While Internet IP VPN networks present an attractive option for effective WAN connectivity, anytime an organization sends data across a public network there is risk that the data will be compromised. Loss or corruption of data can result in a regulatory violation and can present a negative public image, either of which can have significant financial impact on an organization. Secure data transport over public networks like the Internet requires adequate encryption to protect business information.

Technology Overview

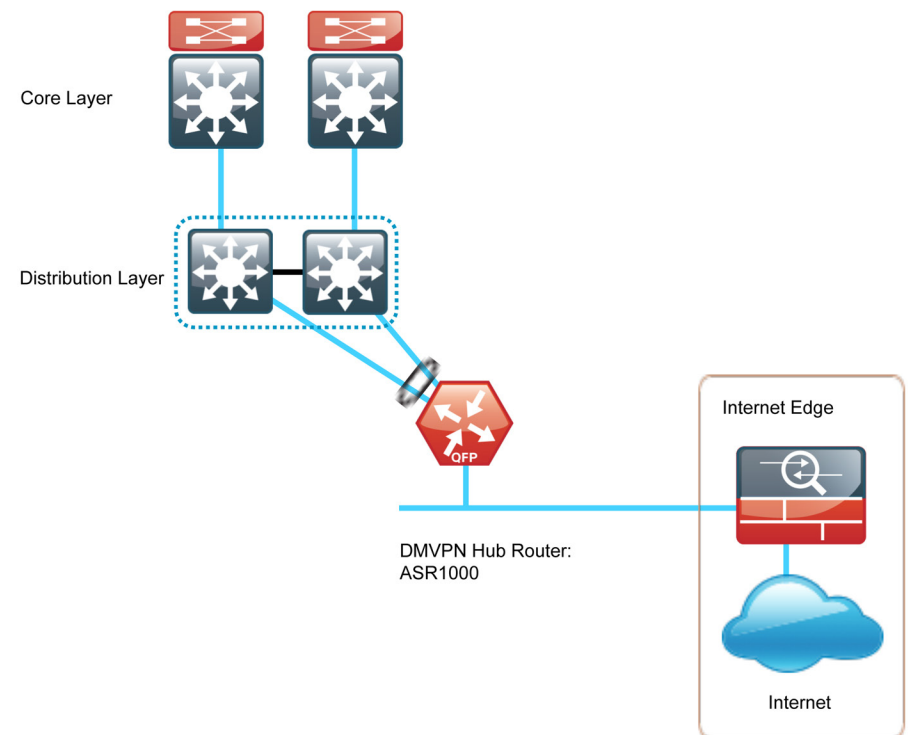
WAN 500 Design

The WAN 500 design is intended to support up to 500 remote sites with a combined aggregate WAN bandwidth of up to 1.0 Gbps. The most critical devices are the WAN routers that are responsible for reliable IP forwarding and QoS. This design uses the Cisco ASR1002 Aggregation Services Router configured with an ESP5 for the Dynamic Multipoint Virtual Private Network (DMVPN) hub router.

The WAN 500 design uses a single Internet service provider and a single DMVPN hub router.

The DMVPN VPN router connects to the Internet indirectly through a firewall demilitarized zone (DMZ) interface contained within the Internet edge. Further details of the primary site Internet connection are referenced in the *Cisco SBA for Enterprise Organizations—Borderless Networks Internet Edge Deployment Guide*. The VPN hub router is connected into the firewall DMZ interface, rather than connected directly with an Internet service provider router.

Figure 19 - WAN 500 design DMVPN connection



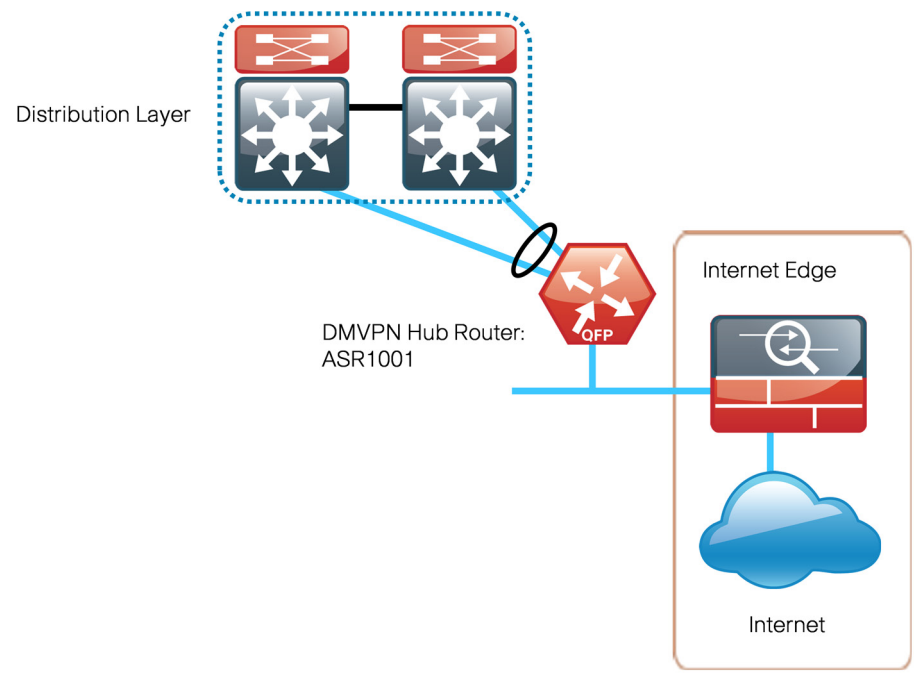
The Cisco ASR1000 Series Aggregation Services Routers represent the next-generation, modular, services-integrated Cisco routing platform. They are specifically designed for WAN aggregation, with the flexibility to support a wide range of 3- to 16-mpps packet-forwarding capabilities, 2.5- to 40-Gbps system bandwidth performance, and scaling.

The Cisco ASR 1000 Series is fully modular, from both hardware and software perspectives, and the routers have all the elements of a true carrier-class routing product that serves both enterprise and service provider networks.

WAN 100 Design

The WAN 100 design is intended to support up to 100 remote sites with a combined aggregate WAN bandwidth of up to 100 Mbps. The WAN 100 design is essentially a smaller scale version of the WAN 500 design. This variant is included to provide a limited scale option. If you expect further growth in bandwidth or an increase in the number of sites, use the WAN 500 design. By using the larger design, you can prevent unnecessary downtime associated with device upgrades. This design uses either the Cisco ASR1001 or the Cisco 3945E Integrated Services Router for the DMVPN hub router. The WAN 100 design uses a single Internet service provider and a single DMVPN hub router.

Figure 20 - WAN 100 design DMVPN connection



DMVPN Spoke Router Selection for Remote Sites

The actual WAN remote-site routing platforms remain unspecified because the specification is tied closely to the bandwidth required for a location and the potential requirement for the use of service module slots. The ability to implement this solution with a variety of potential router choices is one of the benefits of a modular design approach.

There are many factors to consider in the selection of the WAN remote-site routers. Among those, and key to the initial deployment, is the ability to process the expected amount and type of traffic. Also, you need to make sure that you have enough interfaces, enough module slots, and a properly licensed Cisco IOS image that supports the set of features that is required by the topology. Cisco tested four integrated service router models as DMVPN spoke routers and the expected performance is shown in the following table.

Table 12 - WAN remote-site router options

Option	2911	2921	3925	3945
Ethernet WAN with Services ¹	35 Mbps	50 Mbps	100 Mbps	150 Mbps
On-board GE ports	3	3	3	3
Service Module Slots ²	1	1	2	4
Redundant Power Supply Option	No	No	Yes	Yes

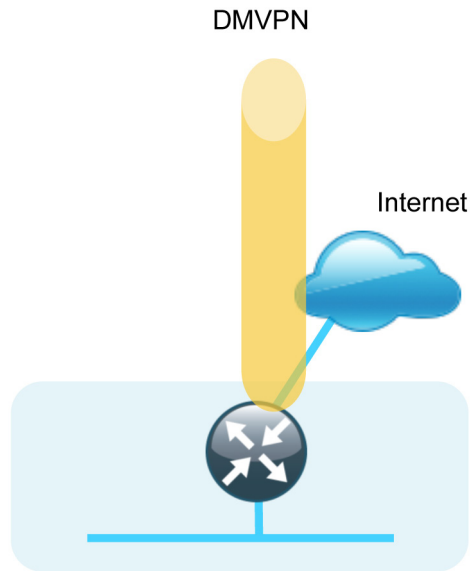
Notes:

1. The performance numbers are conservative numbers obtained when the router is passing Internet mix (IMIX) traffic with heavy services configured and the CPU utilization is under 75 percent.
2. Some service modules are double-wide.

The DMVPN spoke routers at the WAN remote sites connect to the Internet directly through a router interface. More details about the security configuration of the remote-site routers connected to the Internet are discussed later in this guide. The single link DMVPN remote site is the most basic of building blocks for any remote location. You can use this design with the CE router connected directly to the access layer, or you can use it to support a more complex LAN topology by connecting the CE router directly to a distribution layer.

The IP routing is straightforward and can be handled entirely by static routing; using static routes at the WAN-aggregation site and static default routes at the remote site. However, there is significant value to configuring this type of site with dynamic routing. It is easy to add or modify IP networks at the remote site when you use dynamic routing because any changes are immediately propagated to the rest of the network.

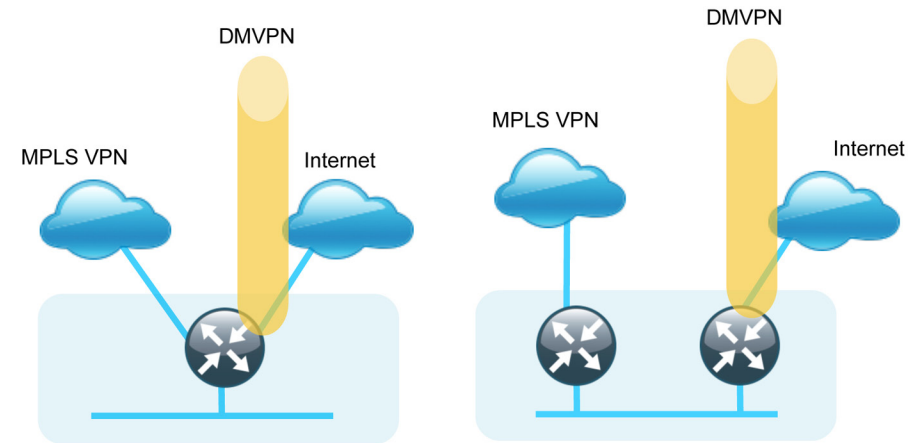
Figure 21 - DMVPN remote site (single link—single router)



The DMVPN connection can be the primary WAN transport, or it can also be the alternate to an MPLS WAN transport. You can add the DMVPN single-link design to an existing MPLS WAN design to provide additional resiliency by either connecting on the same router or on an additional router. Adding an additional link provides the first level of high availability for the remote site. A failure in the primary link can be automatically detected by the router and traffic can be rerouted to the secondary path. It is mandatory that you run dynamic routing when there are multiple paths. The routing protocols are tuned to ensure the desired traffic flows.

The dual-router, dual-link design continues to improve upon the level of high availability for the site. This design can tolerate the loss of the primary router and traffic can be rerouted via the secondary router (through the alternate path).

Figure 22 - MPLS WAN + DMVPN remote site (dual link options)



Virtual Route Forwarding and Front Door Virtual Route Forwarding

Virtual Route Forwarding (VRF) is a technology used in computer networks that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, you can use the same or overlapping IP Addresses without conflicting with each other. Often in a MPLS context, VRF is also defined as VPN Routing and Forwarding.

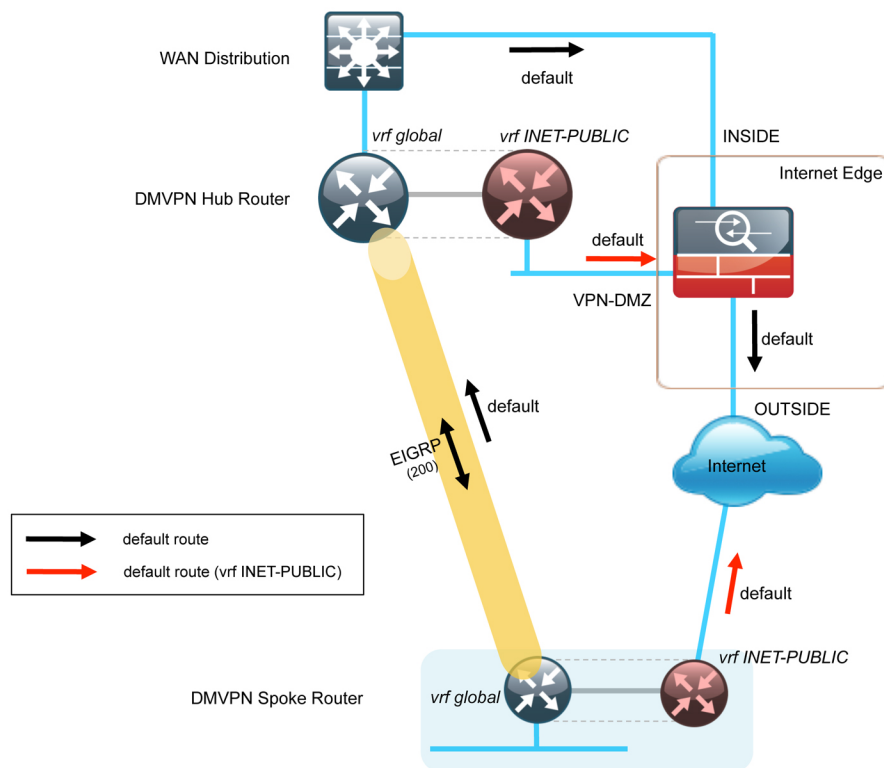
You can implement VRF in a network device by having distinct routing tables, also known as Forwarding Information Bases (FIBs), one per VRF. Alternatively, a network device may have the ability to configure different virtual routers, where each one has its own FIB that is not accessible to any other virtual router instance on the same device.

The simplest form of VRF implementation is VRF Lite. In this implementation, each router within the network participates in the virtual routing environment on a peer-by-peer basis. VRF Lite configurations are only locally significant.

The IP routing policy used in this design for the WAN remote sites does not allow direct Internet access for web browsing or other uses; any remote-site hosts that access the Internet must do so via the Internet edge at the primary site. The end hosts require a default route for all Internet destinations; however, this route must force traffic across the primary or secondary WAN transports (MPLS VPN or DMVPN tunnel). This requirement conflicts with the more general VPN spoke router requirement for an Internet-facing default route to bring up the VPN tunnel.

The multiple default route conundrum is solved through the use of VRFs on the router. A router can have multiple routing tables that are kept logically separate on the device. This separation is similar to a virtual router from the forwarding plane perspective. The global VRF corresponds to the traditional routing table, and additional VRFs are given names and route descriptors (RDs). Certain features on the router are VRF aware, including static routing and routing protocols, interface forwarding and IPsec tunneling. This set of features is used in conjunction with DMVPN to permit the use of multiple default routes for both the DMVPN hub routers and DMVPN spoke routers. This combination of features is referred to as front-door VRF (FVRF), because the VRF faces the Internet and the router internal interfaces and the mGRE tunnel all remain in the global VRF. More technical details regarding FVRF can be found in the Technical Feature Supplement appendix.

Figure 23 - Front-door vREF (FVRF)



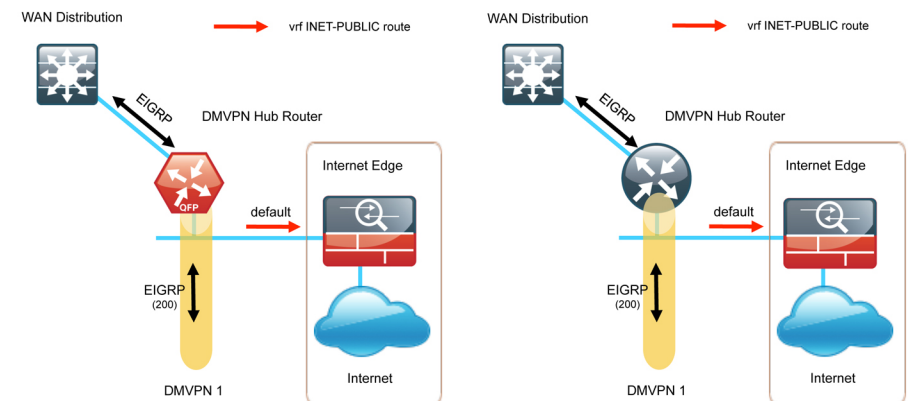
Design Details

The DMVPN hub router connects to a resilient switching device in the distribution layer and in the DMZ. The DMVPN router uses EtherChannel connections consisting of two port bundles. This design provides both resiliency and additional forwarding performance. Additional forwarding performance can be accomplished by increasing the number of physical links within an EtherChannel.

The DMVPN hub routers must have sufficient IP-routing information to provide end-to-end reachability. Maintaining this routing information typically requires a routing protocol, EIGRP is used for this purpose. Two separate EIGRP processes are used, one for internal routing on the LAN (EIGRP-100) and one for the DMVPN (EIGRP-200). The primary reason for the separate EIGRP processes is to simplify the route selection at the WAN-aggregation site when using a MPLS WAN primary path and a DMVPN alternate path. This method ensures that both MPLS learned routes and DMVPN learned routes appear as EIGRP external routes after they are redistributed into the EIGRP-100 process used on the campus LAN.

At the WAN-aggregation site, you must connect the DMVPN router to the distribution layer and to the DMZ-VPN that provides Internet connectivity. The DMVPN hub routers use FVRF and have a static default route with the INET-PUBLIC VRF pointing to the firewall DMZ interface.

Figure 24 - WAN500/100 designs DMVPN routing details



EIGRP

Cisco uses Enhanced IGRP (EIGRP) as the primary routing protocol because it is easy to configure, does not require a large amount of planning, has flexible summarization and filtering, and can scale to large networks. As networks grow, the number of IP prefixes or routes in the routing tables grows as well. You should program IP summarization on links where logical boundaries exist, like distribution layer links to the wide area or to a core. By performing IP summarization, you can reduce the amount of bandwidth, processor, and memory necessary to carry large route tables, and reduce convergence time associated with a link failure.

In this design, EIGRP process 100 is the primary EIGRP process and is referred to as EIGRP-100.

Use EIGRP-100 at the WAN-aggregation site to connect to the primary site LAN distribution layer and at WAN remote sites with dual WAN routers or with distribution-layer LAN topologies. Use EIGRP-200 for the DMVPN tunnels. You should configure EIGRP-200 for stub routing on all remote-site routers to improve network stability and reduce resource utilization.

Encryption

The primary goal of encryption is to provide data confidentiality, integrity, and authenticity by encrypting IP packets as the data travels across a network.

The encrypted payloads are then encapsulated with a new header (or multiple headers) and transmitted across the network. The additional headers introduce a certain amount of overhead to the overall packet length. The following table highlights the packet overhead associated with encryption based on the additional headers required for various combinations of IPsec and GRE.

Table 13 - Overhead associated with IPsec and GRE

Encapsulation	Overhead
GRE only	24 bytes
IPsec (Transport Mode)	36 bytes
IPsec (Tunnel Mode)	52 bytes
IPsec (Transport Mode) + GRE	60 bytes
IPsec (Tunnel Mode) + GRE	76 bytes

There is a maximum transmission unit (MTU) parameter for every link in an IP network and typically the MTU is 1500 bytes. IP packets larger than 1500 bytes must be fragmented when transmitted across these links. Fragmentation is not desirable and can impact network performance. To avoid fragmentation, the original packet size plus overhead must be 1500 bytes or less, which means that the sender must reduce the original packet size. To account for other potential overhead, Cisco recommends that you configure tunnel interfaces with a 1400 byte MTU.

There are dynamic methods for network clients to discover the path MTU, which allow the clients to reduce the size of packets they transmit. However, in many cases, these dynamic methods are unsuccessful, typically because security devices filter the necessary discovery traffic. This failure to discover the path MTU drives the need for a method that can reliably inform network clients of the appropriate packet size. The solution is to implement the **ip tcp adjust mss [size]** command on the WAN routers, which influences the TCP maximum segment size (MSS) value reported by end hosts.

The MSS defines the maximum amount of data that a host is willing to accept in a single TCP/IP datagram. The MSS value is sent as a TCP header option only in TCP SYN segments. Each side of a TCP connection reports its MSS value to the other side. The sending host is required to limit the size of data in a single TCP segment to a value less than or equal to the MSS reported by the receiving host.

The IP and TCP headers combine for 40 bytes of overhead, so the typical MSS value reported by network clients will be 1460. This design includes encrypted tunnels with a 1400 byte MTU, so the MSS used by endpoints should be configured to be 1360 to minimize any impact of fragmentation. In this solution, you implement the **ip tcp adjust mss 1360** on all WAN facing router interfaces.

DMVPN

This solution uses the Internet for WAN transport. For data security and privacy concerns any site-to-site traffic that traverses the Internet must be encrypted. Multiple technologies can provide encryption, but the method that provides the best combination of performance, scale, application support, and ease of deployment is DMVPN.

Most use cases in this design guide use Internet/DMVPN as a secondary WAN transport that requires a DMVPN single-cloud, single-hub design. The DMVPN routers use tunnel interfaces that support IP unicast as well as IP multicast and broadcast traffic, including the use of dynamic routing protocols. After the initial spoke-to-hub tunnel is active, it is possible to create dynamic spoke-to-spoke tunnels when site-to-site IP traffic flows require it.

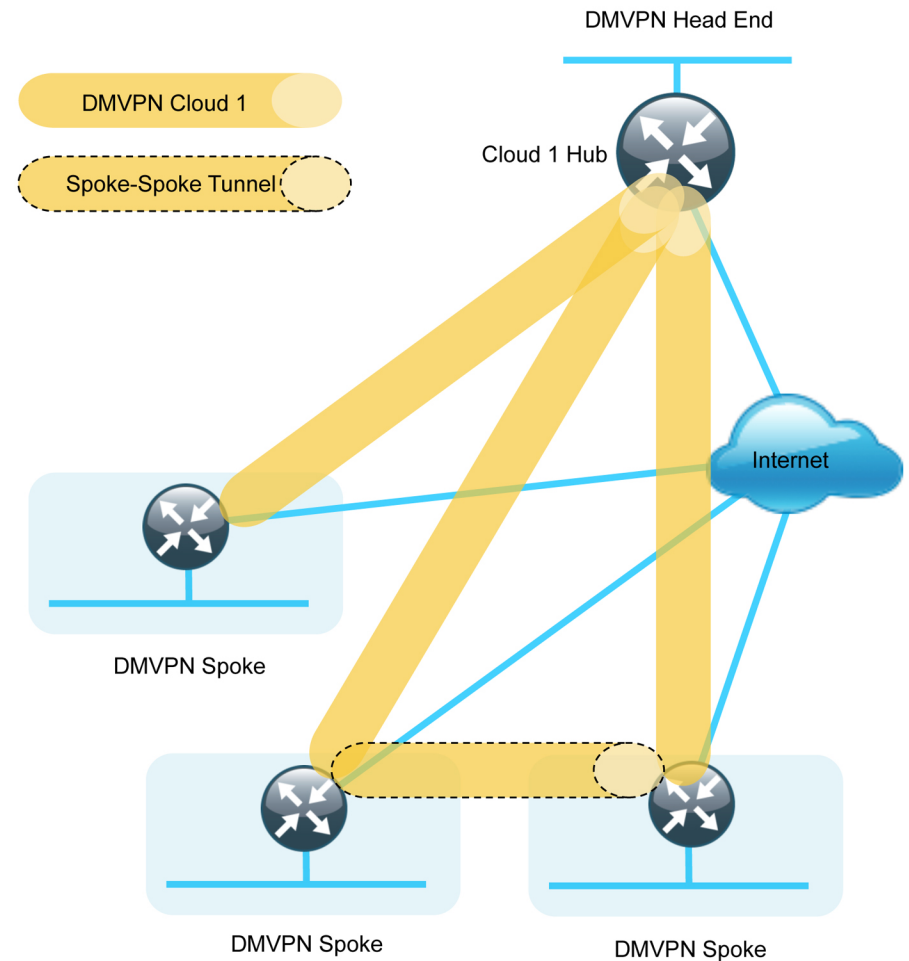
The information required by a spoke to set up dynamic spoke-to-spoke tunnels and properly resolve other spokes is provided through the Next Hop Resolution Protocol (NHRP). Spoke-to-spoke tunnels allow for the optimal routing of traffic between locations without indirect forwarding through the hub. Idle spoke-to-spoke tunnels gracefully time out after a period of inactivity.

It is common for a firewall to be placed between the DMVPN hub router and the Internet. In many cases, the firewall may provide Network Address Translation (NAT) from an internal RFC-1918 IP address (such as 10.4.128.33) to an Internet-routable IP address. The DMVPN solution works well with NAT but requires the use of IPsec transport mode to support a DMVPN hub behind static NAT.

DMVPN requires the use of Internet Security Association and Key Management Protocol (ISAKMP) keepalive intervals for Dead Peer Detection (DPD), which is essential to facilitate fast reconvergence and for spoke registration to function properly in case a DMVPN hub is reloaded. This design enables a spoke to detect that an encryption peer has failed and that the ISAKMP session with that peer is stale, which then allows a new one to be created. Without DPD, the IPsec security association (SA) must time out (the default is 60 minutes) and when the router cannot renegotiate a new SA, a new ISAKMP session is initiated. The maximum wait time is approximately 60 minutes.

One of the key benefits of the DMVPN solution is that the spoke routers can use dynamically assigned addresses, often using DHCP from an Internet provider. The spoke routers can use an Internet default route for reachability to the hub routers and also other spoke addresses.

Figure 25 - DMVPN Single Cloud



The DMVPN hub router has a static IP address assigned to its public-facing interface. This configuration is essential for proper operation as each of the spoke routers has this IP address embedded in their configurations.

Deployment Details

The procedures in this section provide examples for some settings. The actual settings and values that you use are determined by your current network configuration.

Table 14 - Common network services used in the deployment examples

Service	Address
Hostname:	VPN-ASR1002-1
Router Loopback IP address:	10.4.32.243/32
Router Port channel IP Address:	10.4.32.18/30

Process

DMVPN Hub Router Configuration

1. Configure the Distribution Switch
2. Configure the WAN-Aggregation Platform
3. Configure Connectivity to the LAN
4. Configure VRF Lite
5. Connect to Internet DMZ
6. Configure ISAKMP and IPsec
7. Configure the mGRE Tunnel
8. Configure EIGRP

Procedure 1

Configure the Distribution Switch



Reader Tip

This process assumes that the distribution switch has already been configured following the guidance in the *Cisco SBA for Enterprise Organizations—Borderless Networks LAN Deployment Guide*. Only the procedures required to support the integration of the WAN-aggregation router into the deployment are included in this guide.

The LAN distribution switch is the path to the organization's main campus and data center. A Layer 3 port-channel interface connects to the distribution switch to the WAN-aggregation router and the internal routing protocol peers across this interface.



Reader Tip

As a best practice, use the same channel numbering on both sides of the link where possible.

Step 1: Configure the Layer 3 port-channel interface and assign the IP address.

```
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
no shutdown
```

Step 2: Configure EtherChannel member interfaces.

Configure the physical interfaces to tie to the logical port-channel using the **channel-group** command. The number for the port-channel and channel-group must match.

Also, apply the egress QoS macro that was defined in the platform configuration procedure to ensure traffic is prioritized appropriately.

```
interface GigabitEthernet1/0/3
  description VPN-ASR1002-1 Gig0/0/0
!
interface GigabitEthernet2/0/3
  description VPN-ASR1002-1 Gig0/0/1
!
interface range GigabitEthernet1/0/3, GigabitEthernet2/0/3
  no switchport
  macro apply EgressQoS
  carrier-delay msec 0
  channel-protocol lacp
  channel-group 3 mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
```

Step 3: Configure the interfaces that are connected to the LAN core to summarize the WAN network range.

```
interface range TenGigabitEthernet1/1/1,
TenGigabitEthernet2/1/1
  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
```

Step 4: Allow the routing protocol to form neighbor relationships across the port channel interface.

```
router eigrp 100
  no passive-interface Port-channel3
```

Procedure 2

Configure the WAN-Aggregation Platform

Within this design, there are features and services that are common across all WAN-aggregation routers. These are system settings that simplify and secure the management of the solution.

Step 1: Configure the device host name.

```
hostname VPN-ASR1002-1
```

Step 2: Configure device management protocols.

Secure HTTP (HTTPS) and Secure Shell (SSH) are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Secure management of the LAN device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

```
cdp run
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
```

Simple Network Management Protocol (SNMP) is enabled to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured both for a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Step 3: Configure secure user authentication.

Enable authentication, authorization, and accounting (AAA) for access control. All management access to the network infrastructure devices (SSH and HTTPS) is controlled with AAA.



Reader Tip

In this architecture, the AAA server is the Cisco Access Control System (ACS). For more information about configuring ACS, see the *Cisco SBA for Enterprise Organizations—Borderless Networks Network Device Authentication and Authorization Deployment Guide*.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
enable secret c1sco123
service password-encryption
!
username admin password c1sco123
aaa new-model
!
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

Step 4: Configure a synchronized clock.

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organizations network.

You should program your network devices to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. By configuring console messages, logs, and debug output to provide time stamps on output, you can cross-reference events in a network.

```
ntp server 10.4.48.17
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

When synchronous logging of unsolicited messages and debug output is turned on, console log messages appear in the console after interactive CLI output is displayed or printed. This command also allows you to continue typing at the device console when debugging is enabled.

```
line con 0
  logging synchronous
```

Step 5: Configure an in-band management interface.

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer 3 process and features are also bound to the loopback interface to ensure process resiliency.

The loopback address is commonly a host address with a 32-bit address mask. Allocate the loopback address from the IP address block that the distribution switch summarizes to the rest of the network. .

```
interface Loopback 0
  ip address 10.4.32.243 255.255.255.255
  ip pim sparse-mode
```

The ip pim sparse-mode command will be explained further in this procedure.

Bind the SNMP and SSH processes to the loopback interface address for optimal resiliency:

```
snmp-server trap-source Loopback0
ip ssh source-interface Loopback0
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
ntp source Loopback0
```

Step 6: Configure IP unicast routing

Configure EIGRP facing the LAN distribution or core layer. In this design, the port-channel interface and the loopback must be EIGRP interfaces. The loopback may remain a passive interface. The network range must include both interface IP addresses, either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address.

```
router eigrp 100
 network 10.4.0.0 0.1.255.255
 no auto-summary
 passive-interface default
 eigrp router-id 10.4.32.243
```

Step 7: Configure IP Multicast routing

With IP Multicast, you can replicate a single IP data stream by the infrastructure (routers and switches) and send it from a single source to multiple receivers. Using IP multicast is much more efficient than multiple individual unicast streams or a broadcast stream that would propagate everywhere. IP Telephony MOH and IP Video Broadcast Streaming are two examples of IP Multicast applications.

To receive a particular IP multicast data stream, end hosts must join a multicast group by sending an Internet Group Management Protocol (IGMP) message to their local multicast router. In a traditional IP multicast design, the local router consults another router in the network that is acting as an RP to map the receivers to active sources so they can join their streams.

In this design, which is based on sparse mode multicast operation, Auto RP is used to provide a simple yet scalable way to provide a highly resilient RP environment.

Enable IP multicast routing on the platforms in the global configuration mode.

```
ip multicast-routing distributed
```

Every Layer 3 switch and router must be configured to discover the IP multicast RP with autorp. Use the **ip pim autorp listener** command to allow for discovery across sparse mode links. This configuration provides for future scaling and control of the IP multicast environment and can change based on network needs and design.

```
ip pim autorp listener
```

All Layer 3 interfaces in the network must be enabled for sparse mode multicast operation.

```
ip pim sparse-mode
```

Procedure 3

Configure Connectivity to the LAN

Any links to adjacent distribution layers should be Layer 3 links or Layer 3 EtherChannels.

Step 1: Configure Layer 3 interface.

```
interface Port-channel3
 ip address 10.4.32.18 255.255.255.252
 ip pim sparse-mode
 no shutdown
```

Step 2: Configure EtherChannel member interfaces.

Configure the physical interfaces to tie to the logical port channel using the **channel-group** command. The number for the port channel and channel group must match.

```
interface GigabitEthernet0/0/0
 description WAN-D3750X Gig1/0/3
 !
interface GigabitEthernet0/0/1
 description WAN-D3750X Gig2/0/3
 !
interface range GigabitEthernet0/0/0, GigabitEthernet0/0/1
 no ip address
 channel-group 3 mode active
 cdp enable
 no shutdown
```


Step 3: Configure the EIGRP interface.

Allow EIGRP to form neighbor relationships across the interface to establish peering adjacencies and exchange route tables.

```
router eigrp 100
  no passive-interface Port-channel 3
```

Procedure 4 Configure VRF Lite

An Internet-facing VRF is created to support FVRF for DMVPN. The VRF name is arbitrary but it is useful to select a name that describes the VRF. An associated route descriptor (RD) must also be configured to make the VRF functional. The RD configuration also creates the routing and forwarding tables and associates the RD with the VRF instance.

This design uses VRF Lite so that the RD value can be chosen arbitrarily. It is a best practice to use the same VRF/RD combination across multiple devices when using VRFs in a similar manner. However, this convention is not strictly required.

```
ip vrf INET-PUBLIC
  rd 65512:1
```



Reader Tip

Command Reference:

An RD is either ASN-related (composed of an ASN and an arbitrary number) or IP-address-related (composed of an IP address and an arbitrary number).

You can enter an RD in either of these formats:

16-bit autonomous-system-number:your 32-bit number

For example, 65512:1.

32-bit IP address: your 16-bit number

For example, 192.168.122.15:1.

Procedure 5

Connect to Internet DMZ

The DMVPN hub requires a connection to the Internet, and in this design the DMVPN hub is connected through a Cisco ASA5500 Adaptive Security Appliance using a DMZ interface specifically created and configured for a VPN termination router.

Step 1: Enable the interface, select the VRF, and assign the IP address.

The IP address that you use for the Internet-facing interface of the DMVPN hub router must be an Internet routable address. There are two possible methods to accomplish this task:

- Assign a routable IP address directly to the router.
- Assign a non-routable RFC-1918 address directly to the router and use a static NAT on the Cisco ASA5500 to translate the router IP address to a routable IP address.

This design assumes that the Cisco ASA5500 is configured for static NAT for the DMVPN hub router.

The DMVPN design is using FVRF, so this interface must be placed into the VRF configured in the previous procedure.

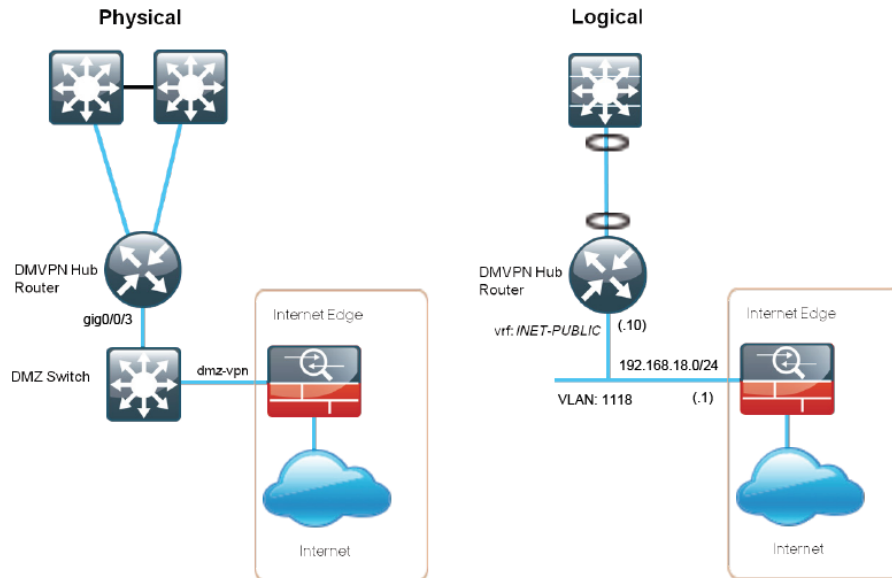
```
interface GigabitEthernet0/0/3
  ip vrf forwarding INET-PUBLIC
  ip address 192.168.18.10 255.255.255.0
  no shutdown
```

Step 2: Configure the VRF specific default routing.

The VRF created for FVRF must have its own default route to the Internet. This default route points to the ASA5500 DMZ interface IP address.

```
ip route vrf INET-PUBLIC 0.0.0.0 0.0.0.0 192.168.18.1
```

Figure 26 - Physical and logical views for DMZ connection



Procedure 6 Configure ISAKMP and IPsec

Step 1: Configure the crypto keyring.

The crypto keyring defines a Pre-Shared Key (PSK) (or password) valid for IP sources that are reachable within a particular VRF. This key is a wildcard PSK if it applies to any IP source. A wildcard key is configured using the 0.0.0.0 0.0.0.0 network/mask combination.

```
crypto keyring DMVPN-KEYRING vrf INET-PUBLIC
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

Step 2: Configure the ISAKMP policy.

The ISAKMP policy for DMVPN uses the following:

- Advanced Encryption Standard (AES) with a 256-bit key
- Secure Hash Standard (SHA)
- Authentication by a PSK
- Diffie-Hellman group: 2

```
crypto isakmp policy 10
```

```
encr aes 256
hash sha
authentication pre-share
group 2
```

Step 3: Create the ISAKMP Profile.

The ISAKMP profile creates an association between an identity address, a VRF, and a crypto keyring. A wildcard address within a VRF is referenced with 0.0.0.0.

```
crypto isakmp profile FVRF-ISA-KMP-INET-PUBLIC
keyring DMVPN-KEYRING
match identity address 0.0.0.0 INET-PUBLIC
```

Step 4: Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for DMVPN uses the following:

- ESP with the 256-bit AES encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Because the DMVPN hub router is behind a NAT device, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256
esp-sha-hmac
mode transport
```

Step 5: Create the IPsec profile.

The IPsec profile creates an association between an ISAKMP profile and an IPsec transform-set.

```
crypto ipsec profile DMVPN-PROFILE
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile FVRF-ISA-KMP-INET-PUBLIC
```

Procedure 7 Configure the mGRE Tunnel

Step 1: Configure basic interface settings.

Tunnel interfaces are created as they are configured. The tunnel number is arbitrary, but it is best to begin tunnel numbering at 10 or above, because other features deployed in this design may also require tunnels and they may select lower numbers by default.

The bandwidth setting should be set to match the Internet bandwidth of the respective primary or secondary carrier.

Configure the IP MTU to 1400 and the ip tcp adjust-mss to 1360. There is a 40 byte difference which corresponds to the combined IP and TCP header length.

```
interface Tunnel10
  bandwidth 10000
  ip address 10.4.34.1 255.255.254.0
  no ip redirects
  ip mtu 1400
  ip tcp adjust-mss 1360
```

Step 2: Configure the tunnel.

DMVPN uses multipoint GRE (mGRE) tunnels. This type of tunnel requires a source interface only. The source interface is the interface that is connected to the Internet. Set the **tunnel vrf** command to the VRF defined previously for FVRF.

Enabling encryption on this interface requires the application of the IPsec profile configured in the previous procedure.

```
interface Tunnel10
  tunnel source GigabitEthernet0/0/3
  tunnel mode gre multipoint
  tunnel vrf INET-PUBLIC
  tunnel protection ipsec profile DMVPN-PROFILE
```

Step 3: Configure NHRP.

The DMVPN hub router acts in the role of NHRP server for all of the spokes. NHRP is used by remote routers to determine the tunnel destinations for peers attached to the mGRE tunnel.

NHRP requires all devices within a DMVPN cloud to use the same network ID and authentication key. The NHRP cache holdtime should be configured to 600 seconds.

EIGRP (configured in the following procedure) relies on a multicast transport and requires NHRP to automatically add routers to the multicast NHRP mappings.

The **ip nhrp redirect** command allows the DMVPN hub to notify spoke routers that a more optimal path may exist to a destination network, which may be required for DMVPN spoke-spoke direct communications.

```
interface Tunnel10
  ip nhrp authentication cisco123
  ip nhrp map multicast dynamic
  ip nhrp network-id 101
  ip nhrp holdtime 600
  ip nhrp redirect
```

Step 4: Enable PIM non-broadcast multiple access (NBMA) mode for the DMVPN tunnel.

Spoke-to-spoke DMVPN networks present a unique challenge because the spokes cannot directly exchange information with one another, even though they are on the same logical network. This inability to directly exchange information can also cause problems when running IP Multicast.

To resolve this issue requires a method where each remote PIM neighbor has its join messages tracked separately. A router in PIM NBMA mode treats each remote PIM neighbor as if it were connected to the router through a point-to-point link.



Tech Tip

Do not enable PIM on the Internet DMZ interface because you shouldn't request any multicast traffic from this interface.

```
interface Tunnel10
  ip pim sparse-mode
  ip pim nbma-mode
```

Step 5: Configure EIGRP.

You configure EIGRP in the following Procedure 8, but there are some specific requirements for the mGRE tunnel interface that you need to configure first.

Spoke-to-spoke DMVPN networks present a unique challenge because the spokes cannot directly exchange information with one another, even though they are on the same logical network. This limitation requires that the DMVPN hub router advertise routes from other spokes on the same network. This advertisement of these routes would normally be prevented by split horizon, and can be overridden by the **no ip split-horizon eigrp** command.

The EIGRP hello interval is increased to 20 seconds and the EIGRP hold time is increased to 60 seconds to accommodate up to 500 remote sites on a single DMVPN cloud.

```
interface Tunnel10
 ip hello-interval eigrp 200 20
 ip hold-time eigrp 200 60
 no ip split-horizon eigrp 200
```

Procedure 8 Configure EIGRP

You use two EIGRP processes on the DMVPN hub routers. The primary reason for the additional process is to ensure that routes learned from the WAN remotes appear as EIGRP external routes on the WAN distribution switch. If you used only a single process, then the remote-site routes would appear as EIGRP internal routes on the WAN distribution switch, which would be preferred to the MPLS VPN learned routes.

Step 1: Enable an additional EIGRP-200 process for DMVPN.

Configure EIGRP-200 for the DMVPN mGRE interface. Routes from the other EIGRP process are redistributed. Because the routing protocol is the same, no default metric is required.

The tunnel interface is the only EIGRP interface, and you need to explicitly list its network range.

```
router eigrp 200
 network 10.4.34.0 0.0.1.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.4.32.243
 no auto-summary
```

Step 2: Tag and redistribute the routes.

This design uses mutual route redistribution. DMVPN Routes from the EIGRP-200 process are redistributed into EIGRP-100 and other learned routes from EIGRP-100 are redistributed into EIGRP-200. Because the routing protocol is the same, no default metric is required.

It is important to tightly control how routing information is shared between different routing protocols when this mutual route redistribution is used; otherwise, it is possible to experience route flapping, where certain routes are repeatedly installed and with-drawn from the device routing tables. Proper route control ensures the stability of the routing table.

An inbound distribute-list is used on the WAN-aggregation MPLS CE routers to limit which routes are accepted for installation into the route table. These routers are configured to only accept routes which do not originate from the MPLS and DMVPN WAN sources. To accomplish this task, the DMVPN learned WAN routes must be explicitly tagged by their DMVPN hub router during the route redistribution process. The specific route tags in use are shown in the following table.

Table 15 - Route tag information for DMVPN hub router

Tag	Route source	Tag method	Action
65401	MPLS A	implicit	accept
65402	MPLS B	implicit	accept
300	Layer 2 WAN	explicit	accept
65512	DMVPN hub routers	explicit	tag

This example includes all WAN route sources in the reference design. Depending on the actual design of your network, you might need to use more tags.

```
router eigrp 100
 redistribute eigrp 200 route-map SET-ROUTE-TAG-DMVPN
!
router eigrp 200
 redistribute eigrp 100
!
route-map SET-ROUTE-TAG-DMVPN permit 10
 match interface Tunnel10
 set tag 65512
```

Process

Firewall and DMZ Switch Configuration

1. Configure the DMZ Switch
2. Configure Demilitarized Zone Interface
3. Configure Network Address Translation
4. Configure Security Policy

Procedure 1 Configure the DMZ Switch



Reader Tip

This procedure assumes that the switch has already been configured following the guidance in the *Cisco SBA for Enterprise Organizations—Borderless Networks LAN Deployment Guide*. Only the procedures required to support the integration of the firewall into the deployment are included in this guide.

Step 1: Set the DMZ switch to be the spanning-tree root for the VLAN that contains the DMVPN-aggregation router.

```
vlan 1118
spanning-tree vlan 1118 root primary
```

Step 2: Configure the interfaces that are connected to the appliances as a trunk.

```
interface GigabitEthernet1/0/24
description IE-ASA5540a Gig0/1
!
interface GigabitEthernet1/0/24
description IE-ASA5540b Gig0/1
```

```
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 1118
switchport mode trunk
macro apply EgressQoS
logging event link-status
logging event trunk-status
no shutdown
```

Step 3: Configure the interfaces that are connected to the DMVPN-aggregation router.

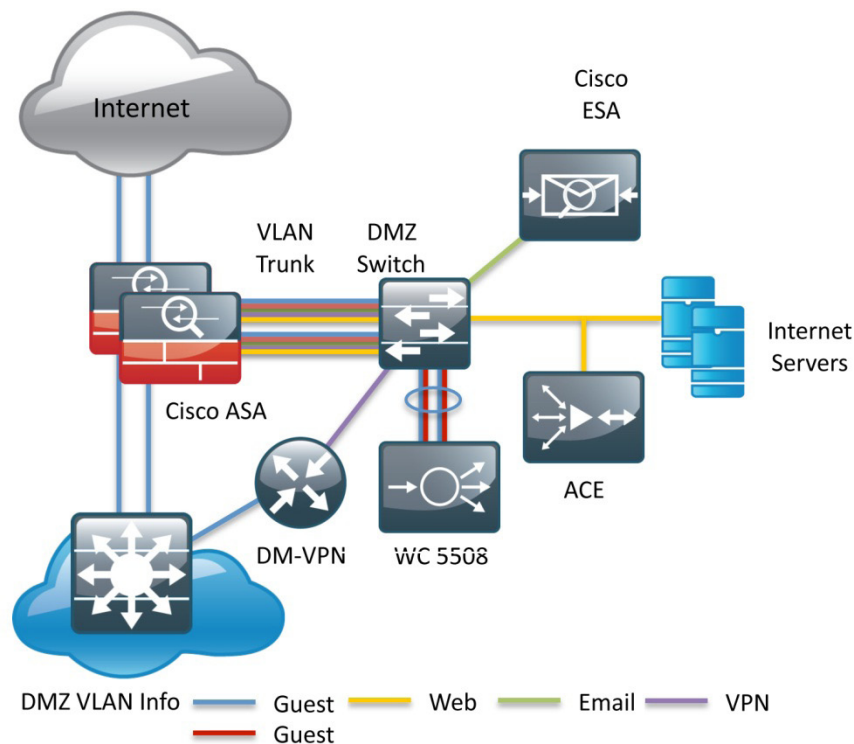
```
interface GigabitEthernet1/0/7
description VPN-ASR1002-1
switchport access vlan 1118
switchport host
macro apply EgressQoS
logging event link-status
no shutdown
```

Procedure 2 Configure Demilitarized Zone Interface

The firewall's demilitarized zone (DMZ) is a portion of the network where, typically, traffic to and from other parts of the network is tightly restricted. Organizations place network services in a DMZ for exposure to the Internet. These servers are typically not allowed to initiate connections to the 'inside' network, except for specific circumstances.

The DMZ network is connected to the appliances on the appliances' GigabitEthernet interface via a VLAN trunk to allow the greatest flexibility if new VLANs must be added to connect additional DMZs. The trunk connects the appliances to a 3750x access-switch stack to provide resiliency. The DMZ VLAN interfaces on the Cisco ASA are each assigned an IP address, which will be the default gateway for each of the VLAN subnets. The DMZ switch only offers Layer 2 switching capability; the DMZ switch's VLAN interfaces do not have an IP address assigned, save for one VLAN interface with an IP address for management of the switch.

Figure 27 - DMZ VLAN topology and services



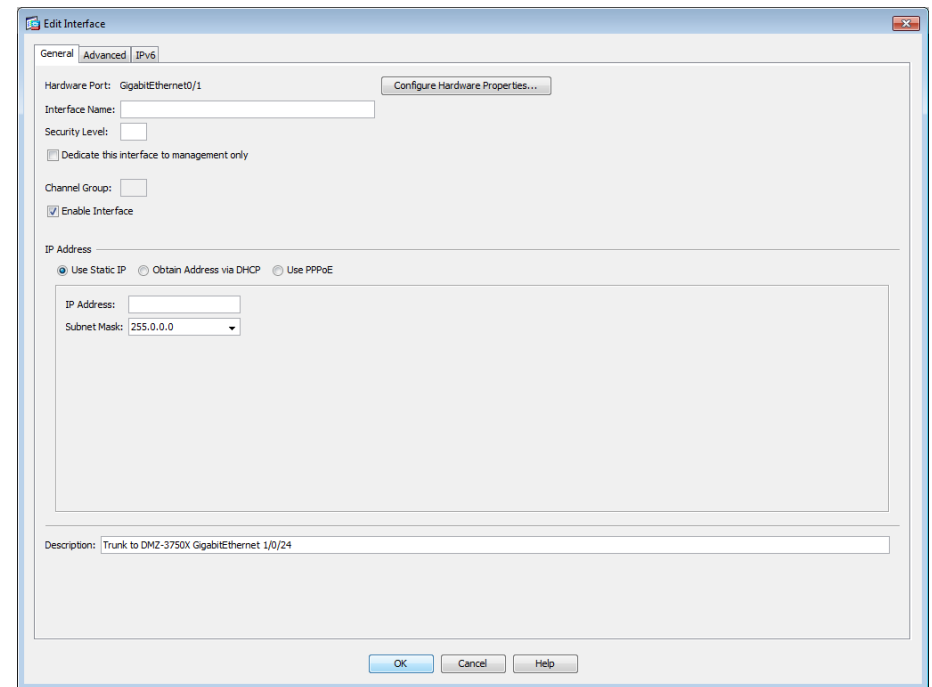
Tech Tip

By setting the DMZ connectivity as a VLAN trunk, you get the greatest flexibility.

Step 1: In **Configuration > Device Setup > Interfaces**, click the interface that is connected to the DMZ switch. (Example: GigabitEthernet0/1)

Step 2: Click **Edit**.

Step 3: Select **Enable Interface**, and then click **OK**.



Step 4: In the **Interface** pane, click **Add > Interface**.

Step 5: In the **Hardware Port** list choose the interface configured in Step 1. (Example: GigabitEthernet0/1)

Step 6: In the **VLAN ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1118)

Step 7: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1118)

Step 8: Enter an **Interface Name**. (Example: dmz-dmvpn)

Step 9: In the **Security Level** box, enter a value of **75**.

Step 10: Enter the interface **IP Address**. (Example: 192.168.18.1)

Step 11: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)

Step 12: Click Apply.

General Advanced IPv6

Hardware Port: GigabitEthernet0/1
VLAN ID: 1118
Subinterface ID: 1118
Interface Name: dmz-dmvpn
Security Level: 75

☐ Dedicate this interface to management only

Channel Group:
☒ Enable Interface

IP Address

☒ Use Static IP ☐ Obtain Address via DHCP ☐ Use PPPoE

IP Address: 192.168.18.1
Subnet Mask: 255.255.255.0

Description: DMVPN aggregation router connections on VLAN 1118

OK Cancel Help

Step 13: In Configuration > Device Management > High Availability > click Failover.

Step 14: On the **Interfaces** tab, for the interface that you created in Step 4, in the **Standby IP address** column enter the IP address of the standby unit. (Example: 192.168.18.2)

Step 15: Select **Monitored**.

Step 16: Click Apply.

Configuration > Device Management > High Availability > Failover

Setup Interfaces Criteria MAC Addresses

Define interface standby IP addresses and monitoring status. Double-click on a standby address or click on a monitoring checkbox to edit it. Press the Tab or Enter key after editing an address.

Interface Name	Name	Active IP Address	Subnet Mask/Prefix Length	Standby IP Address	Monitored
GigabitEthernet0/0	inside	10.4.24.30	255.255.255.224	10.4.24.29	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1116	dmz-web	192.168.16.1	255.255.255.0	192.168.16.2	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1117	dmz-mail	192.168.17.1	255.255.255.0	192.168.17.2	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1118	dmz-dmvpn	192.168.18.1	255.255.255.0	192.168.18.2	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1123	dmz-management	192.168.23.1	255.255.255.0	192.168.23.2	<input checked="" type="checkbox"/>
GigabitEthernet0/3.16	outside-16	172.16.132.124	255.255.255.0	172.16.132.123	<input checked="" type="checkbox"/>
GigabitEthernet0/3.17	outside-17	172.17.132.124	255.255.255.0	172.17.132.123	<input checked="" type="checkbox"/>
Management0/0	management	192.168.1.1	255.255.255.0		<input checked="" type="checkbox"/>

Apply Reset

Procedure 3 Configure Network Address Translation

The DMZ network uses private network (RFC 1918) addressing that is not Internet routable, so the firewall must translate the DMZ address of the DMVPN-aggregation router to an outside public address.

The example DMZ address to public IP address mapping is shown in the following table.

DMVPN-aggregation router DMZ address	DMVPN-aggregation router public address (externally routable after NAT)
192.168.18.10	172.16.130.1 (ISP-A)

Step 1: In Configuration > Firewall > Objects > click Network Objects/Groups.

First, add a network object for the public address of the DMVPN-aggregation router on the primary internet connection.

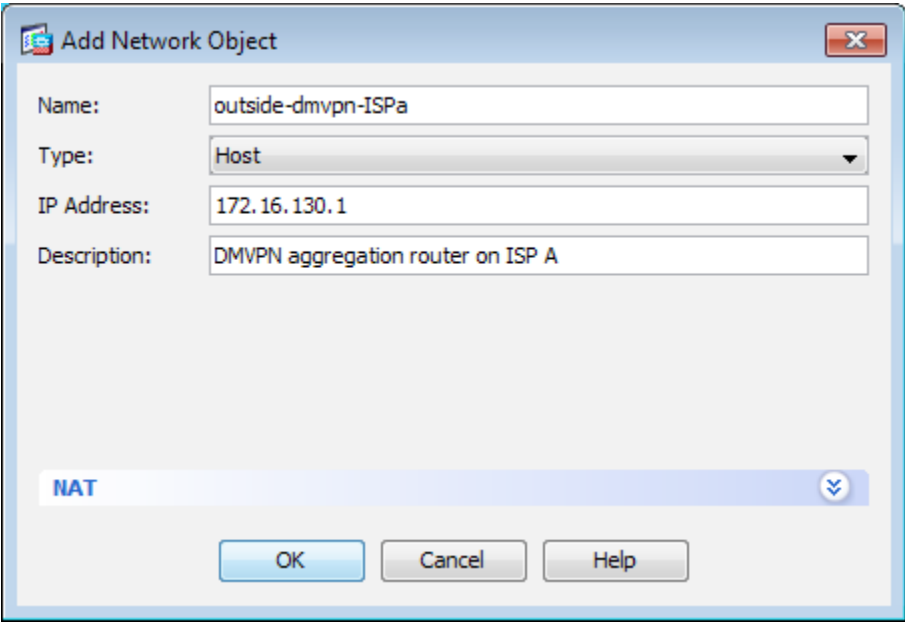
Step 2: Click Add > Network Object.

Step 3: On the Add Network Object dialog box, in the **Name box**, enter a description for the DMVPN-aggregation router's public IP address. (Example: outside-dmvpn-ISPa)

Step 4: In the **Type** list, choose **Host**.

Step 5: In the **IP Address** box, enter the DMVPN-aggregation router's public IP address, and then click **OK**. (Example: 172.16.130.1)

Step 6: Click Apply.



Next, you add a network object for the private DMZ address of the DMVPN-aggregation router.

Step 7: Click Add > Network Object.

Step 8: In the **Add Network Object** dialog box, in the **Name box**, enter a description for the DMVPN-aggregation router's private DMZ IP address. (Example: dmz-dmvpn-1)

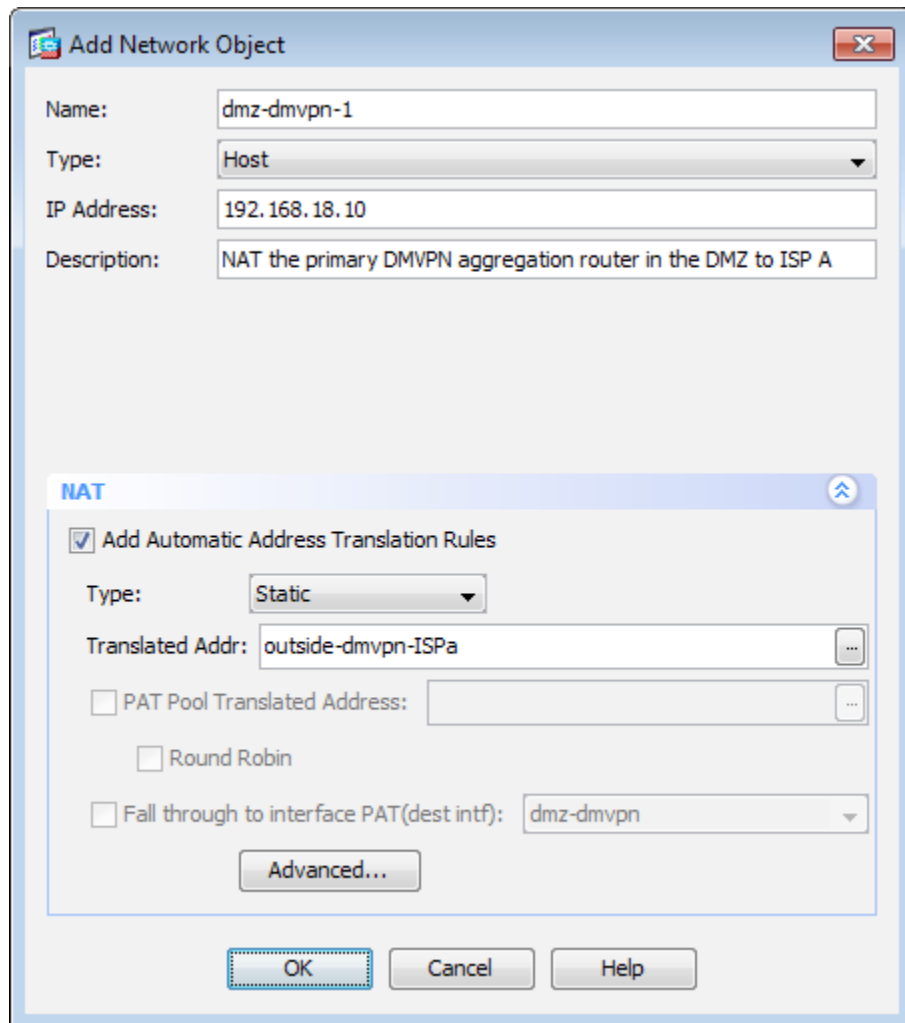
Step 9: In the **Type** list, choose **Host**.

Step 10: In the **IP Address** box, enter the router's private DMZ IP address. (Example: 192.168.18.10)

Step 11: Click the two down arrows. The NAT pane expands.

Step 12: Select **Add Automatic Address Translation Rules**.

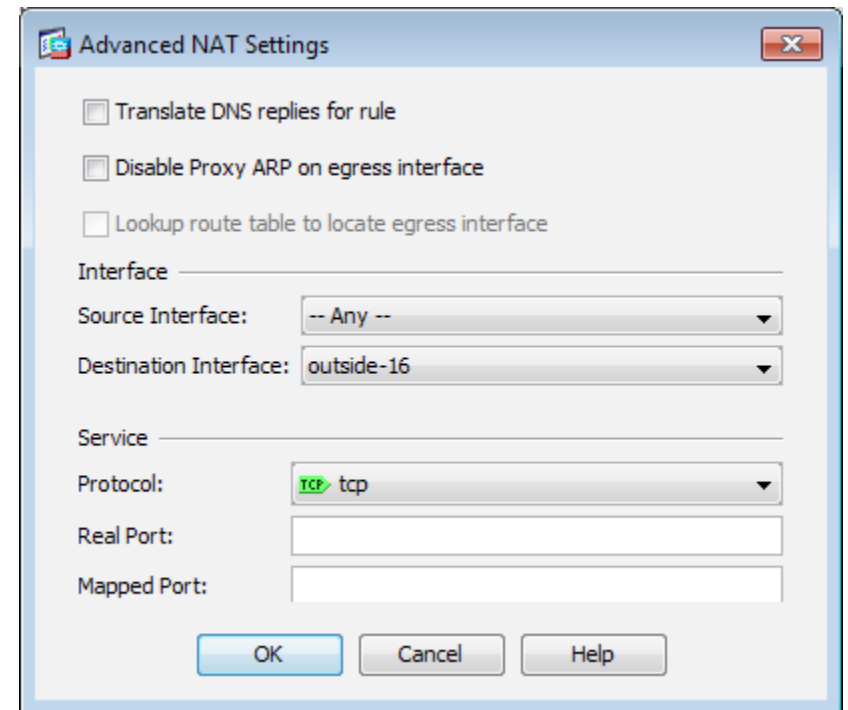
Step 13: In the **Translated Addr** list, choose the network object created in Step 2.



The **Add Network Object** dialog box is shown. The **Name** field contains "dmz-dmvpn-1", **Type** is set to "Host", **IP Address** is "192.168.18.10", and **Description** is "NAT the primary DMVPN aggregation router in the DMZ to ISP A". Below these fields is a **NAT** section with a tab icon. The **NAT** section has a checked checkbox for "Add Automatic Address Translation Rules". The **Type** dropdown is set to "Static". The **Translated Addr** field contains "outside-dmvpn-ISPa" and has a browse button "...". Below this are two unchecked checkboxes: "PAT Pool Translated Address:" and "Round Robin". The "Fall through to interface PAT(dest intf):" checkbox is also unchecked, and its dropdown is set to "dmz-dmvpn". An "Advanced..." button is at the bottom of the NAT section. At the bottom of the main dialog are "OK", "Cancel", and "Help" buttons.

Step 14: Click **Advanced**.

Step 15: In the **Destination Interface** list choose the interface name for the primary internet connection, and then click **OK**. (Example: outside-16)



The **Advanced NAT Settings** dialog box is shown. It has three unchecked checkboxes: "Translate DNS replies for rule", "Disable Proxy ARP on egress interface", and "Lookup route table to locate egress interface". Below these is the **Interface** section with a "Source Interface:" dropdown set to "-- Any --" and a "Destination Interface:" dropdown set to "outside-16". The **Service** section has a "Protocol:" dropdown set to "TCP" (with a green icon) and "tcp" text, and empty fields for "Real Port:" and "Mapped Port:". At the bottom are "OK", "Cancel", and "Help" buttons.

Step 16: Click **OK**.

Step 17: Click **Apply**.

Procedure 4 Configure Security Policy

The DMVPN DMZ provides an additional layer of protection to lower the likelihood of certain types of misconfiguration of the DMVPN routers exposing the business network to the Internet. A filter allows only DMVPN related traffic to reach the DMVPN-aggregation routers.

Table 16 - Required DMVPN protocols (aggregation router)

Name	Protocol	Usage
non500-isakmp	UDP 4500	IPsec via NAT-T
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec

Table 17 - Optional protocols—DMVPN-aggregation router

Name	Protocol	Usage
icmp echo	ICMP Type 0, Code 0	Allow remote pings
icmp echo-reply	ICMP Type 8, Code 0	Allow ping replies (from our requests)
icmp ttl-exceeded	ICMP Type 11, Code 0	Allow traceroute replies (from our requests)
icmp port-unreachable	ICMP Type 3, Code 3	Allow traceroute replies (from our requests)
UDP high ports	UDP > 1023	Allow remote traceroute

Step 1: In **Configuration > Firewall** click **Access Rules**.

Step 2: Click the rule that denies traffic from the DMZ toward other networks.



Next, you must insert a new rule above the rule you selected.

Step 3: Click **Add > Insert**.

You must enable the DMVPN remote routers to communicate with the DMVPN-aggregation routers in the DMZ.

Step 4: In the **Destination** list, choose the network object group created in Procedure 2 Step 16. (Example: dmz-dmvpn-network/24)

Step 5: In the **Service** list box, enter **esp, udp/4500, udp/isakmp**, and then click **OK**.

Next, you must insert a new rule to allow diagnostic traffic to the DMVPN-aggregation routers.

Step 6: Click **Add > Insert**.

You must enable the DMVPN remote routers to communicate with the DMVPN-aggregation routers in the DMZ.

Step 7: In the **Destination** list, choose the automatically created network object for the DMVPN DMZ. (Example: dmz-dmvpn-network/24)

Step 8: In the **Service** list box, enter **icmp/echo, icmp/echo-reply**, and then click **OK**.

Step 9: Click **Apply**.

Process

Enabling DMVPN Backup on Existing MPLS CE Router

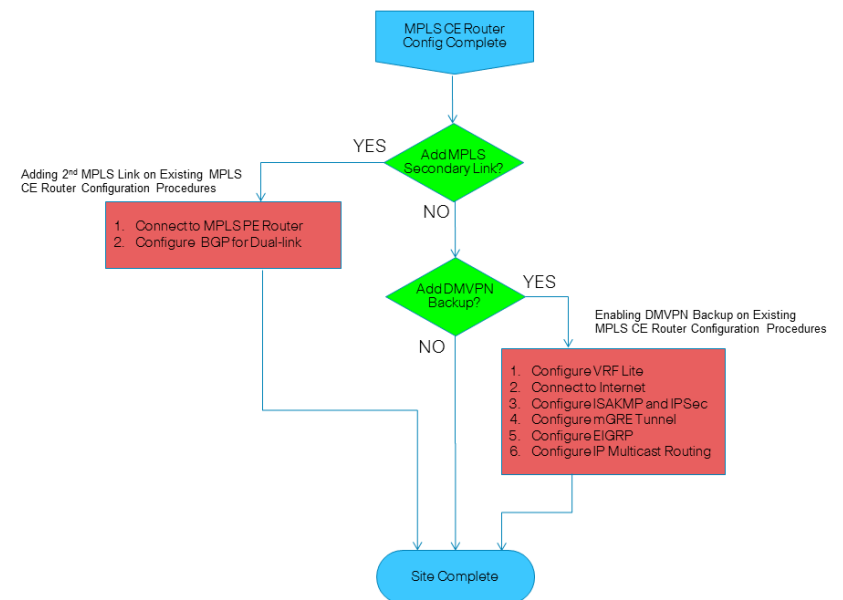
1. Configure VRF Lite
2. Connect to the Internet
3. Configure ISAKMP and IPsec
4. Configure the mGRE Tunnel
5. Configure EIGRP
6. Configure IP Multicast Routing

This set of procedures includes the additional steps necessary to complete the configuration of a dual-role MPLS CE and DMVPN spoke router for a MPLS WAN + DMVPN remote site (single-router, dual-link).

The following procedures assume that the configuration of a MPLS CE Router for a MPLS WAN remote site (single-router, single-link) has already been completed. Only the additional procedures to add the DMVPN backup to the running MPLS CE router are included here.

The following flowchart provides details about how to add DMVPN backup on an existing remote-site MPLS CE router.

Figure 28 - Adding DMVPN backup configuration flowchart



Procedure 1

Configure VRF Lite

An Internet-facing VRF is created to support FVRF for DMVPN. The VRF name is arbitrary, but it is useful to select a name that describes the VRF. An associated RD must also be configured to make the VRF functional. The RD configuration also creates the routing and forwarding tables and associates the RD with the VRF instance.

This design uses VRF Lite so the RD value can be chosen arbitrarily. It is a best practice to use the same VRF/RD combination across multiple devices when using VRFs in a similar manner. However, this convention is not strictly required.

```
ip vrf INET-PUBLIC
rd 65512:1
```



Reader Tip

Command Reference:

An RD is either ASN-related (composed of an ASN and an arbitrary number) or IP-address-related (composed of an IP address and an arbitrary number).

You can enter an RD in either of these formats:

16-bit autonomous-system-number: your 32-bit number

For example, 65512:1

32-bit IP address: your 16-bit number

For example, 192.168.122.15:1.

Procedure 2

Connect to the Internet

The remote sites that are using DMVPN can use either static or dynamically assigned IP addresses. Cisco tested the design with a DHCP assigned external address, which also provides a dynamically configured default route.

The DMVPN spoke router connects directly to the Internet without a separate firewall. This connection is secured in two ways. Because the Internet interface is in a separate VRF, no traffic can access the global VRF except traffic sourced through the DMVPN tunnel. This design provides implicit security. Additionally, an IP access list permits only the traffic required for an encrypted tunnel, as well as DHCP and various ICMP protocols for troubleshooting.

Step 1: Enable the interface, select VRF and enable DHCP.

The DMVPN design uses FVRF, so this interface must be placed into the VRF configured in the previous procedure.

```
interface GigabitEthernet 0/1
ip vrf forwarding INET-PUBLIC
ip address dhcp
no shutdown
```

Step 2: Configure and apply the access list.

The IP access list must permit the protocols specified in the following table. The access list is applied inbound on the WAN interface, so filtering is done on traffic destined to the router.

Table 18 - Required DMVPN protocols

Name	Protocol	Usage
non500-isakmp	UDP 4500	IPsec via NAT-T
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec
bootpc	UDP 68	DHCP

Example access list:

```
interface GigabitEthernet 0/1
ip access-group ACL-INET-PUBLIC in
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
```


The additional protocols listed in the following table may assist in troubleshooting, but are not explicitly required to allow DMVPN to function properly.

Table 19 - Optional protocols for DMVPN spoke router

Name	Protocol	Usage
icmp echo	ICMP Type 0, Code 0	Allow remote pings
icmp echo-reply	ICMP Type 8, Code 0	Allow ping replies (from our requests)
icmp ttl-exceeded	ICMP Type 11, Code 0	Allow traceroute replies (from our requests)
icmp port-unreachable	ICMP Type 3, Code 3	Allow traceroute replies (from our requests)
UDP high ports	UDP > 1023, TTL=1	Allow remote traceroute

The additional optional entries for an access list to support ping are as follows:

```
permit icmp any any echo
permit icmp any any echo-reply
```

The additional optional entries for an access list to support traceroute are as follows:

```
permit icmp any any ttl-exceeded      ! for traceroute
(sourced)
permit icmp any any port-unreachable  ! for traceroute
(sourced)
permit udp any any gt 1023 ttl eq 1    ! for traceroute
(destination)
```

Step 2: Configure the ISAKMP Policy and Dead Peer Detection.

The ISAKMP policy for DMVPN uses the following:

- Advanced Encryption Standard (AES) with a 256-bit key
- Secure Hash Standard (SHA)
- Authentication by PSK
- Diffie-Hellman group: 2

DPD is enabled with keepalive intervals sent at 30-second intervals with a 5-second retry interval, which is considered to be a reasonable setting to detect a failed hub.

```
crypto isakmp policy 10
  encr aes 256
  hash sha
  authentication pre-share
  group 2
!
crypto isakmp keepalive 30 5
```

Step 3: Create the ISAKMP profile.

The ISAKMP profile creates an association between an identity address, a VRF and a crypto keyring. A wildcard address within a VRF is referenced with 0.0.0.0.

```
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC
  keyring DMVPN-KEYRING
  match identity address 0.0.0.0 INET-PUBLIC
```

Step 4: Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for DMVPN uses the following:

- ESP with the 256-bit AES encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Procedure 3 Configure ISAKMP and IPsec

Step 1: Configure the crypto keyring.

The crypto keyring defines a Pre-Shared Key (PSK) (or password) valid for IP sources reachable within a particular VRF. This key is a wildcard PSK if it applies to any IP source. A wildcard key is configured using the 0.0.0.0 0.0.0.0 network/mask combination.

```
crypto keyring DMVPN-KEYRING vrf INET-PUBLIC
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

Since the DMVPN hub router is behind a NAT device, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256  
esp-sha-hmac  
mode transport
```

Step 5: Create the IPsec profile.

The IPsec profile creates an association between an ISAKMP profile and an IPsec transform-set.

```
crypto ipsec profile DMVPN-PROFILE  
set transform-set AES256/SHA/TRANSPORT  
set isakmp-profile FVRF-ISAKMP-INET-PUBLIC
```

Procedure 4 Configure the mGRE Tunnel

Step 1: Configure basic interface settings.

Tunnel interfaces are created as they are configured. The tunnel number is arbitrary, but it is best to begin tunnel numbering at 10 or above, because other features deployed in this design may also require tunnels and they may select lower numbers by default.

The bandwidth setting should be set to match the Internet bandwidth.

Configure the IP MTU to 1400 and the **ip tcp adjust-mss** to 1360. There is a 40 byte difference, which corresponds to the combined IP and TCP header length.

```
interface Tunnel10  
bandwidth [bandwidth (kbps)]  
ip address [IP address] [netmask]  
no ip redirects  
ip mtu 1400  
ip tcp adjust-mss 1360
```

Step 2: Configure the tunnel.

DMVPN uses multipoint GRE (mGRE) tunnels. This type of tunnel requires a source interface only. The source interface should be the same interface used in to connect to the Internet. The **tunnel vrf** command should be set to the VRF defined previously for FVRF.

Enabling encryption on this interface requires the application of the IPsec profile configured in the previous procedure.

```
interface Tunnel10  
tunnel source GigabitEthernet 0/1  
tunnel mode gre multipoint  
tunnel vrf INET-PUBLIC  
tunnel protection ipsec profile DMVPN-PROFILE
```

Step 3: Configure NHRP.

The DMVPN hub router is the NHRP server for all of the spokes. NHRP is used by remote routers to determine the tunnel destinations for peers attached to the mGRE tunnel.

The spoke router requires several additional configuration statements to define the NHRP server (NHS) and NHRP map statements for the DMVPN hub router mGRE tunnel IP address. EIGRP (configured in the following Procedure 5) relies on a multicast transport. Spoke routers require the NHRP static multicast mapping.

The value that you use for the NHS is the mGRE tunnel address for the DMVPN hub router. The map entries must be set to the outside NAT value of the DMVPN hub, as configured on the Cisco ASA5500. This design uses the values shown in the following table.

Table 20 - DMVPN hub IP address information

DMVPN hub DMZ address	DMVPN hub external address	NHS (DMVPN Hub mGRE tunnel address)
192.168.18.10	172.16.130.1	10.4.34.1

NHRP requires all devices within a DMVPN cloud to use the same network ID and authentication key. The NHRP cache holdtime should be configured to 600 seconds.

This design supports DMVPN spoke routers that receive their external IP addresses through DHCP. It is possible for these routers to acquire different IP addresses after a reload. When the router attempts to register with the NHRP server, it may appear as a duplicate to an entry already in the cache and be rejected. The **registration no-unique** option allows you to overwrite existing cache entries. This feature is only required on NHRP clients (DMVPN spoke routers).

The **ip nhrp redirect** command allows the DMVPN hub to notify spoke routers that a more optimal path may exist to a destination network, which may be required for DMVPN spoke-to-spoke direct communications. DMVPN spoke routers also use shortcut switching when building spoke-to-spoke tunnels.

```
interface Tunnel10
 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
```

Step 4: Configure EIGRP.

You configure EIGRP in the following Procedure 5, but you need to configure some specific requirements for the mGRE tunnel interface first.

The EIGRP hello interval is increased to 20 seconds and the EIGRP hold time is increased to 60 seconds to accommodate up to 500 remote sites on a single DMVPN cloud.

```
interface Tunnel10
 ip hello-interval eigrp 200 20
 ip hold-time eigrp 200 60
```

The remote-site LAN networks must be advertised. The IP assignment for the remote sites was designed so that all of the networks in use can be summarized within a single aggregate route. The summary address as configured below suppresses the more specific routes. If any network within the summary is present in the route table, the summary is advertised to the DMVPN hub, which offers a measure of resiliency. If the various LAN networks cannot be summarized, then EIGRP continues to advertise the specific routes.

```
interface Tunnel10
 ip summary-address eigrp 200 [summary network] [summary mask]
```

Procedure 5

Configure EIGRP

A single EIGRP-200 process runs on the DMVPN spoke router. All interfaces on the router are EIGRP interfaces, but only the DMVPN tunnel interface is non-passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address. All DMVPN spoke routers should run EIGRP stub routing to improve network stability and reduce resource utilization.

```
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id [IP address of Loopback0]
 eigrp stub connected summary
 no auto-summary
```

Procedure 6

Configure IP Multicast Routing

This procedure includes additional steps for completing the IP Multicast configuration when adding DMVPN backup capability to a router with IP multicast already enabled.

Step 1: Configure PIM on the DMVPN tunnel interface.

Use sparse-mode for IP multicast interface operation mode and to enable it on all Layer 3 interfaces, including DMVPN tunnel interfaces.



Tech Tip

Do not enable PIM on the Internet DMZ interface because you shouldn't request any multicast traffic from this interface.

```
interface Tunnel10
 ip pim sparse-mode
```

Step 2: Enable PIM NBMA mode for the DMVPN tunnel.

Spoke-to-spoke DMVPN networks present a unique challenge because the spokes cannot directly exchange information with one another, even though they are on the same logical network. This inability to directly exchange information can also cause problems when running IP Multicast.

To resolve the NBMA issue, you need to implement a method where each remote PIM neighbor has its join messages tracked separately. A router in PIM NBMA mode treats each remote PIM neighbor as if it were connected to the router through a point-to-point link.

```
interface Tunnel10
 ip pim nbma-mode
```

Step 3: Configure the DR priority for the DMVPN spoke router.

Proper multicast operation across a DMVPN cloud requires that the hub router assumes the role of PIM Designated Router (DR). Spoke routers should never become the DR. You can prevent that by setting the DR priority to 0 for the spokes.

```
interface Tunnel10
 ip pim dr-priority 0
```

Notes

Process

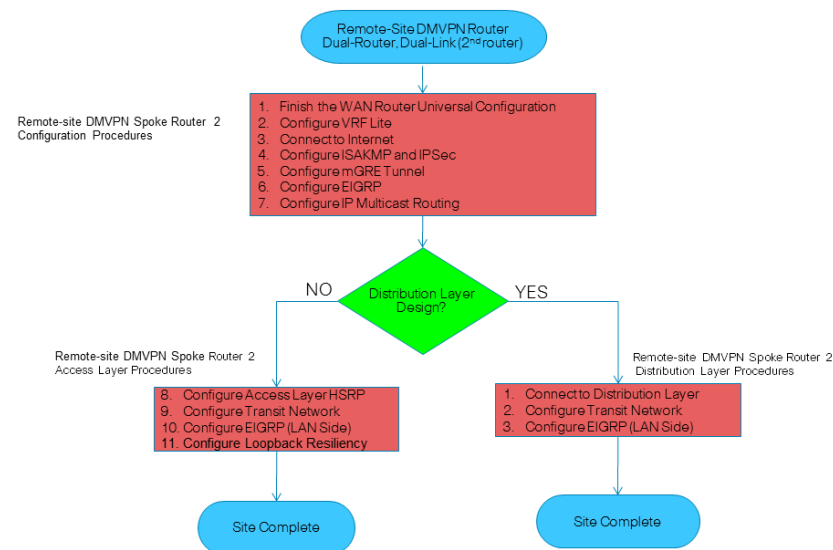
Remote-Site DMVPN Spoke Router Configuration

1. Finish WAN Router Universal Configuration
2. Configure VRF Lite
3. Connect to the Internet
4. Configure ISAKMP and IPsec
5. Configure the mGRE Tunnel
6. Configure EIGRP
7. Configure IP Multicast Routing
8. Configure Access Layer HSRP
9. Configure Transit Network
10. Configure EIGRP (LAN Side)
11. Configure Loopback Resiliency

Use this set of procedures when you configure a MPLS WAN + DMVPN remote site. Use these procedures when you configure the second router of the dual-router, dual-link design.

The following flowchart provides details about how to complete the configuration of a remote-site DMVPN spoke router.

Figure 29 - Remote-Site DMVPN Spoke Router Configuration Flowchart



Procedure 1

Finish WAN Router Universal Configuration

Within this design, there are features and services that are common across all WAN remote-site routers. These are system settings that simplify and secure the management of the solution.

Step 1: Configure the device host name to make it easy to identify the device.

```
hostname [hostname]
```

Step 2: Configure device management protocols.

Secure HTTP (HTTPS) and Secure Shell (SSH) are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

You enable secure management of the LAN device through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
    transport input ssh
```

Simple Network Management Protocol (SNMP) is enabled to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured both for a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Step 3: Configure secure user authentication.

Enable authentication, authorization, and accounting (AAA) for access control. AAA controls all management access to the network infrastructure devices (SSH and HTTPS).



Reader Tip

The AAA server used in this architecture is the Cisco Access Control System. For details about configuring ACS, see the *Cisco SBA for Enterprise Organizations—Borderless Networks Network Device Authentication and Authorization Deployment Guide*.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
enable secret cisco123
service password-encryption
!
```

```
username admin password cisco123
aaa new-model
!
tacacs server TACACS-SERVER-1
    address ipv4 10.4.48.15
    key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
    server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

Step 4: Configure a synchronized clock.

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organization's network.

You should program network devices to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. By configuring console messages, logs, and debug output to provide time stamps on output, you can cross-reference events in a network.

```
ntp server 10.4.48.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

When synchronous logging of unsolicited messages and debug output is turned on, console log messages appear in the console after interactive CLI output is displayed or printed. With this command, you can continue typing at the device console when debugging is enabled.

```
line con 0
    logging synchronous
```


Step 5: Configure an in-band management interface.

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer 3 process and features are also bound to the loopback interface to ensure process resiliency.

The loopback address is commonly a host address with a 32-bit address mask. Allocate the remote site router loopback IP address from a unique network range that is not part of any other internal network summary range.

```
interface Loopback0
 ip address [ip address] 255.255.255.255
 ip pim sparse-mode
```

The **ip pim sparse-mode** command is explained further in this procedure.

Bind the SNMP and SSH processes to the loopback interface address for optimal resiliency:

```
snmp-server trap-source Loopback0
 ip ssh source-interface Loopback0
 ip pim register-source Loopback0
 ip tacacs source-interface Loopback0
 ntp source Loopback0
```

Step 6: Configure IP Multicast routing.

IP Multicast allows a single IP data stream to be replicated by the infrastructure (that is, routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than multiple individual unicast streams or a broadcast stream that would propagate everywhere. IP Telephony MOH and IP Video Broadcast Streaming are two examples of IP Multicast applications.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an Internet Group Management Protocol (IGMP) message to their local multicast router. In a traditional IP Multicast design, the local router consults another router in the network that is acting as an RP to map the receivers to active sources so they can join their streams.

In this design, which is based on sparse mode multicast operation, Cisco uses autorp to provide a simple yet scalable way to provide a highly resilient RP environment.

Enable IP multicast routing on the platforms in the global configuration mode.

```
ip multicast-routing
```

Every Layer 3 switch and router must be configured to discover the IP Multicast RP with autorp. Use the **ip pim autorp listener** command to allow for discovery across sparse mode links. This configuration provides for future scaling and control of the IP Multicast environment and can change based on network needs and design.

```
ip pim autorp listener
```

You must enable all Layer 3 interfaces in the network for sparse mode multicast operation.

```
ip pim sparse-mode
```

Procedure 2

Configure VRF Lite

An Internet-facing VRF is created to support FVRF for DMVPN. The VRF name is arbitrary but it is useful to select a name that describes the VRF. You must also configure an associated RD to make the VRF functional. The RD configuration creates the routing and forwarding tables and associates the RD with the VRF instance.

This design uses VRF Lite so that the RD value can be chosen arbitrarily. It is a best practice to use the same VRF/RD combination across multiple devices when using VRFs in a similar manner. However, this convention is not strictly required.

```
ip vrf INET-PUBLIC
 rd 65512:1
```



Reader Tip

Command Reference:

An RD is either ASN-related (composed of an ASN and an arbitrary number) or IP-address-related (composed of an IP address and an arbitrary number).

You can enter an RD in either of these formats:

16-bit autonomous-system-number:your 32-bit number

For example, 65512:1.

32-bit IP address: your 16-bit number

For example, 192.168.122.15:1.

Procedure 3

Connect to the Internet

The remote sites using DMVPN can use either static or dynamically assigned IP addresses. We tested the design with a DHCP-assigned external address, which also provides a dynamically configured default route.

The DMVPN spoke router connects directly to the Internet without a separate firewall. This connection is secured in two ways. Because the Internet interface is in a separate VRF, no traffic can access the global VRF except traffic sourced through the DMVPN tunnel. This design provides implicit security. Additionally, an IP access list permits only the traffic required for an encrypted tunnel, as well as DHCP and various ICMP protocols for troubleshooting.

Step 1: Enable the interface, select VRF and enable DHCP.

The DMVPN design uses FVRF, so this interface must be placed into the VRF configured in the previous procedure.

```
interface GigabitEthernet0/1
 ip vrf forwarding INET-PUBLIC
 ip address dhcp
 no shutdown
```

Step 2: Configure and apply the access list.

The IP access list must permit the protocols specified in the following table. The access list is applied inbound on the WAN interface, so filtering is done on traffic destined to the router.

Table 21 - Required DMVPN protocols

Name	Protocol	Usage
non500-isakmp	UDP 4500	IPsec via NAT-T
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec
bootpc	UDP 68	DHCP

Example access list:

```
interface GigabitEthernet0/1
 ip access-group ACL-INET-PUBLIC in
 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
```

The additional protocols listed in the following table may assist in troubleshooting, but are not explicitly required to allow DMVPN to function properly.

Table 22 - Optional protocols DMVPN spoke router

Name	Protocol	Usage
icmp echo	ICMP Type 0, Code 0	Allow remote pings
icmp echo-reply	ICMP Type 8, Code 0	Allow ping replies (from our requests)
icmp ttl-exceeded	ICMP Type 11, Code 0	Allow traceroute replies (from our requests)
icmp port-unreachable	ICMP Type 3, Code 3	Allow traceroute replies (from our requests)
UDP high ports	UDP > 1023, TTL=1	Allow remote traceroute

The additional optional entries for an access list to support ping are as follows:

```
permit icmp any any echo
permit icmp any any echo-reply
```

The additional optional entries for an access list to support traceroute are as follows:

```
permit icmp any any ttl-exceeded      ! for traceroute
(sourced)
permit icmp any any port-unreachable  ! for traceroute
(sourced)
permit udp any any gt 1023 ttl eq 1    ! for traceroute
(destination)
```

Procedure 4 Configure ISAKMP and IPsec

Step 1: Configure the crypto keyring.

The crypto keyring defines a PSK (or password) valid for IP sources reachable within a particular VRF. This key is a wildcard PSK if it applies to any IP source. A wildcard key is configured using the 0.0.0.0 0.0.0.0 network/mask combination.

```
crypto keyring DMVPN-KEYRING vrf INET-PUBLIC
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

Step 2: Configure the ISAKMP Policy and Dead Peer Detection (DPD).

The ISAKMP policy for DMVPN uses the following:

- Advanced Encryption Standard (AES) with a 256-bit key
- Secure Hash Standard (SHA)
- Authentication by PSK
- Diffie-Hellman group: 2

DPD is enabled with keepalive intervals sent at 30-second intervals with a 5-second retry interval, which is considered to be a reasonable setting to detect a failed hub.

```
crypto isakmp policy 10
encr aes 256
hash sha
authentication pre-share
group 2
!
crypto isakmp keepalive 30 5
```

Step 3: Create the ISAKMP profile.

The ISAKMP profile creates an association between an identity address, a VRF and a crypto keyring. A wildcard address within a VRF is referenced with 0.0.0.0.

```
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC
keyring DMVPN-KEYRING
match identity address 0.0.0.0 INET-PUBLIC
```

Step 4: Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for DMVPN uses the following:

- ESP with the 256-bit AES encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Since the DMVPN hub router is behind a NAT device, you must configure the IPsec transform for transport mode.

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256
esp-sha-hmac
mode transport
```

Step 5: Create the IPsec profile.

The IPsec profile creates an association between an ISAKMP profile and an IPsec transform-set.

```
crypto ipsec profile DMVPN-PROFILE
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile FVRF-ISAKMP-INET-PUBLIC
```

Procedure 5 Configure the mGRE Tunnel

Step 1: Configure basic interface settings.

You create tunnel interfaces as you configure them. The tunnel number is arbitrary, but it is best to begin tunnel numbering at 10 or above, because other features deployed in this design may also require tunnels and they may select lower numbers by default.

The bandwidth setting should be set to match the Internet bandwidth.

The IP MTU should be configured to 1400 and the **ip tcp adjust-mss** should be configured to 1360. There is a 40 byte difference, which corresponds to the combined IP and TCP header length.

```
interface Tunnel10
  bandwidth [bandwidth (kbps)]
  ip address [IP address] [netmask]
  no ip redirects
  ip mtu 1400
  ip tcp adjust-mss 1360
```

Step 2: Configure the tunnel.

DMVPN uses multipoint GRE (mGRE) tunnels. This type of tunnel requires a source interface only. The source interface should be the same interface you use to connect to the Internet. You should set the **tunnel vrf** command to the VRF defined previously for FVRF.

To enable encryption on this interface, you must apply the IPsec profile that you configured in the previous procedure.

```
interface Tunnel10
  tunnel source GigabitEthernet0/1
  tunnel mode gre multipoint
  tunnel vrf INET-PUBLIC
  tunnel protection ipsec profile DMVPN-PROFILE
```

Step 3: Configure NHRP.

The DMVPN hub router is the NHRP server for all of the spokes. NHRP is used by remote routers to determine the tunnel destinations for peers attached to the mGRE tunnel.

The spoke router requires several additional configuration statements to define the NHRP server (NHS) and NHRP map statements for the DMVPN hub router mGRE tunnel IP address. EIGRP (configured in the following Procedure 5) relies on a multicast transport. Spoke routers require the NHRP static multicast mapping.

For the NHS value, use the mGRE tunnel address for the DMVPN hub router. The map entries must be set to the outside NAT value of the DMVPN hub, as configured on the Cisco ASA5500. This design uses the values shown in the following table.

Table 23 - DMVPN hub IP address information

DMVPN hub DMZ address	DMVPN hubexternal address	NHS (DMVPN hub mGRE tunnel address)
192.168.18.10	172.16.130.1	10.4.34.1

NHRP requires all devices within a DMVPN cloud to use the same network ID and authentication key. You should configure the NHRP cache holdtime to 600 seconds.

This design supports DMVPN spoke routers that receive their external IP addresses through DHCP. It is possible for these routers to acquire different IP addresses after a reload. When the router attempts to register with the NHRP server, it may appear as a duplicate to an entry already in the cache and be rejected. The **registration no-unique** option allows you to overwrite existing cache entries. This feature is only required on NHRP clients (DMVPN spoke routers).

The **ip nhrp redirect** command allows the DMVPN hub to notify spoke routers that a more optimal path may exist to a destination network, which may be required for DMVPN spoke-to-spoke direct communications. DMVPN spoke routers also use shortcut switching when building spoke-to-spoke tunnels.

```
interface Tunnel10
  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
```

Step 4: Configure EIGRP.

You configure EIGRP in the following Procedure 6, but you need to configure some specific requirements for the mGRE tunnel interface first.

Increase the EIGRP hello interval to 20 seconds and the EIGRP hold time to 60 seconds to accommodate up to 500 remote sites on a single DMVPN cloud.

```
interface Tunnel10
 ip hello-interval eigrp 200 20
 ip hold-time eigrp 200 60
```

You must advertise the remote-site LAN networks. The IP assignment for the remote sites was designed so that all of the networks in use can be summarized within a single aggregate route. The summary address as configured below suppresses the more specific routes. If any network within the summary is present in the route table, the summary is advertised to the DMVPN hub, which offers a measure of resiliency. If the various LAN networks cannot be summarized, then EIGRP continues to advertise the specific routes.

```
interface Tunnel10
 ip summary-address eigrp 200 [summary network] [summary mask]
```

Procedure 6 Configure EIGRP

A single EIGRP-200 process runs on the DMVPN spoke router. All interfaces on the router are EIGRP interfaces, but only the DMVPN tunnel interface is non-passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements.

This design uses a best practice of assigning the router ID to a loopback address. All DMVPN spoke routers should run EIGRP stub routing to improve network stability and reduce resource utilization.

```
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id [IP address of Loopback0]
 eigrp stub connected summary
 no auto-summary
```

Procedure 7

Configure IP Multicast Routing

This procedure includes additional steps for completing the IP multicast configuration when adding DMVPN backup capability to a router with IP multicast already enabled.

Step 1: Configure PIM on the DMVPN tunnel interface.

Cisco recommends that you use sparse mode for IP Multicast interface operation mode and to enable it on all Layer 3 interfaces, including DMVPN tunnel interfaces.



Tech Tip

Do not enable PIM on the Internet DMZ interface because you shouldn't request any multicast traffic from this interface.

```
interface Tunnel10
 ip pim sparse-mode
```

Step 2: Enable PIM NBMA mode for the DMVPN tunnel.

Spoke-to-spoke DMVPN networks present a unique challenge because the spokes cannot directly exchange information with one another, even though they are on the same logical network. This inability to directly exchange information can also cause problems when running IP Multicast.

To resolve the NBMA issue, you need to implement a method where each remote PIM neighbor has its join messages tracked separately. A router in PIM NBMA mode treats each remote PIM neighbor as if it were connected to the router through a point-to-point link.

```
interface Tunnel10
 ip pim nbma-mode
```

Step 3: Configure the DR priority for the DMVPN spoke router.

Proper multicast operation across a DMVPN cloud requires that the hub router assumes the role of PIM Designated Router (DR). Spoke routers should never become the DR. You can prevent that by setting the DR priority to 0 for the spokes.

```
interface Tunnel10
 ip pim dr-priority 0
```

Procedure 8

Configure Access Layer HSRP

You configure HSRP to enable a VIP that you use as a default gateway that is shared between two routers. The HSRP active router is the MPLS CE router connected to the primary MPLS carrier and the HSRP standby router is the DMVPN spoke router. Configure the HSRP standby router with a standby priority that is lower than the HSRP active router.

The router with the higher standby priority value is elected as the HSRP active router. The preempt option allows a router with a higher priority to become the HSRP active, without waiting for a scenario where there is no router in the HSRP active state. The relevant HSRP parameters for the router configuration are shown in the following table.

Table 24 - WAN remote-site HSRP parameters (dual router)

Router	HSRP role	Virtual IP address (VIP)	Real IP address	HSRP priority	PIM DR priority
MPLS CE (primary)	Active	.1	.2	110	110
MPLS CE (secondary) or DMVPN Spoke	Standby	.1	.3	105	105

The dual-router access-layer design requires a modification for resilient multicast. The PIM DR should be on the HSRP active router. The DR is normally elected based on the highest IP address and has no awareness of the HSRP configuration. In this design, the HSRP active router has a lower real IP address than the HSRP standby router, which requires a modification to the PIM configuration. The PIM DR election can be influenced by explicitly setting the DR priority on the LAN-facing subinterfaces for the routers.



Tech Tip

The HSRP priority and PIM DR priority are shown in the previous table to be the same value; however there is no requirement that these values must be identical.

Repeat this procedure for all data or voice subinterfaces.

```
interface [interface type] [number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [LAN network 1 address] [LAN network 1 netmask]
 ip helper-address 10.4.48.10
 ip pim sparse-mode
 ip pim dr-priority 105
 standby 1 ip [LAN network 1 gateway address]
 standby 1 priority 105
 standby 1 preempt
```

Example

```
interface GigabitEthernet0/2.64
 description 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
 ip pim sparse-mode
 standby 1 ip 10.5.52.1
 standby 1 priority 105
 standby 1 preempt
!
interface GigabitEthernet0/2.69
 description 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 1 ip 10.5.53.1
 standby 1 priority 105
 standby 1 preempt
```


Procedure 9 Configure Transit Network

The transit network is configured between the two routers. This network is used for router-router communication and to avoid hairpinning. The transit network should use an additional subinterface on the router interface that is already being used for data or voice.

There are no end stations connected to this network, so HSRP and DHCP are not required.

```
interface GigabitEthernet0/2.99
  description Transit Net
  encapsulation dot1Q 99
  ip address 10.5.48.2 255.255.255.252
  ip pim sparse-mode
```

Procedure 10 Configure EIGRP (LAN Side)

A routing protocol must be configured between the two routers. This ensures that the HSRP active router has full reachability information for all WAN remote sites.

Step 1: Enable EIGRP-100.

You configure EIGRP-100 facing the access layer. In this design, all LAN-facing interfaces and the loopback must be EIGRP interfaces. All interfaces except the transit-network subinterface should remain passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address. Do not include the WAN interface (MPLS PE-CE link interface) as an EIGRP interface.

```
router eigrp 100
  network 10.5.0.0 0.0.255.255
  passive-interface default
  no passive-interface GigabitEthernet0/2.99
  eigrp router-id [IP address of Loopback0]
  no auto-summary
```

Step 2: Redistribute EIGRP-200 (DMVPN) into EIGRP-100.

This step should only be completed on the DMVPN spoke router.

EIGRP-200 is already configured for the DMVPN mGRE interface. Routes from this EIGRP process are redistributed. Since the routing protocol is the same, no default metric is required.

```
router eigrp 100
  redistribute eigrp 200
```

Procedure 11 Configure Loopback Resiliency

Applies to Dual-Router Design Only

The remote-site routers have in-band management configured via the loopback interface. To ensure reachability of the loopback interface in a dual-router design, redistribute the loopback of the adjacent router into the WAN routing protocol.

Option 1. The WAN protocol is EIGRP

Step 1: Configure an access list to limit the redistribution to only the adjacent router's loopback IP address.

```
ip access-list standard R[number]-LOOPBACK
permit [IP Address of Adjacent Router Loopback]
!
route-map LOOPBACK-ONLY permit 10
match ip address R[number]-LOOPBACK
```

Step 2: Configure EIGRP to redistribute the adjacent router's loopback IP address. The EIGRP stub routing must be adjusted to permit redistributed routes.

```
router eigrp [as]
  redistribute eigrp 100 route-map LOOPBACK-ONLY
  eigrp stub connected summary redistributed
```

Option 2. The WAN protocol is BGP

Step 1: Configure BGP to advertise the adjacent router's loopback network

```
router bgp 65511
  network 10.5.12.0 mask 255.255.255.0
  network 10.5.13.0 mask 255.255.255.0
```

Deploying a WAN Remote-Site Distribution Layer

Use this set of procedures to configure a MPLS CE router for a MPLS WAN remote site (single-router, single-link). This section includes all required procedures to connect to a distribution layer.

Also, use this set of procedures for a dual-carrier MPLS or MPLS WAN + DMVPN remote site. Use these procedures to connect a distribution layer to a dual-role MPLS CE and DMVPN spoke router in the single-router, dual-link design. Use these procedures when you are connecting a distribution layer to the first router of the dual-router, dual-link design.

Process

Remote-Site MPLS CE Router Distribution Layer

1. Connect MPLS CE Router
2. Configure EIGRP (LAN Side)
3. Configure the Transit Network

Procedure 1

Connect MPLS CE Router

A Layer 2 port-channel interface connects to the WAN distribution switch. This connection allows for multiple VLANs to be included on the EtherChannel if necessary.

The following configuration creates an EtherChannel link between the router and switch, with two channel-group members.

Step 1: Configure the port-channel interface.

Create the port-channel interface. As a best practice, use the same channel numbering on both sides of the link where possible.

```
interface Port-channel [number]
no ip address
```

Step 2: Configure the port channel subinterfaces and assign IP addresses.

After you have enabled the physical interface, map the appropriate subinterfaces to the VLANs on the distribution layer switch. The subinterface number does not need to equate to the 802.1Q tag, but making them the same simplifies the overall configuration.

The subinterface configured on the router corresponds to a VLAN interface on the distribution-layer switch. Traffic is routed between the devices with the VLAN acting as a point-to-point link.

```
interface Port-channel [number].[sub-interface number]
encapsulation dot1Q [dot1q VLAN tag]
ip address [IP address] [netmask]
```

Step 3: Administratively enable the port channel group members and assign the appropriate channel group.

Not all router platforms can support LACP to negotiate with the switch, so you configure EtherChannel statically.

```
interface [interface type] [number]
no ip address
channel-group [number]
no shutdown
```

Example

```
interface Port-channel1
no ip address
!
interface Port-channel1.50
encapsulation dot1Q 50
ip address 10.5.0.1 255.255.255.252
ip pim sparse-mode
!
interface GigabitEthernet0/1
no ip address
```

```

channel-group 1
no shutdown
!
interface GigabitEthernet0/2
no ip address
channel-group 1
no shutdown

```

Procedure 2 Configure EIGRP (LAN Side)

You must configure a routing protocol between the router and distribution layer.

Step 1: Enable EIGRP-100.

Configure EIGRP-100 facing the distribution layer. In this design, all distribution-layer-facing subinterfaces and the loopback must be EIGRP interfaces. All other interfaces should remain passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address.

```

router eigrp 100
network 10.5.0.0 0.0.255.255
passive-interface default
no passive-interface [interface]
eigrp router-id [IP address of Loopback0]
no auto-summary

```

Step 2: Redistribute BGP into EIGRP-100.

Complete this step on a MPLS CE router only.

The BGP routes are redistributed into EIGRP with a default metric. By default, only the bandwidth and delay values are used for metric calculation.

```

router eigrp [as number]
default-metric [bandwidth] [delay] 255 1 1500
redistribute bgp 65511

```



Reader Tip

Command Reference:

default-metric *bandwidth delay reliability loading mtu*

bandwidth—Minimum bandwidth of the route in kilobytes per second

delay—Route delay in tens of microseconds.

Example

```

router eigrp 100
default-metric 100000 100 255 1 1500
network 10.5.0.0 0.0.255.255
passive-interface default
no passive-interface Port-channel1.50
eigrp router-id 10.5.48.254
no auto-summary

```

Procedure 3

Configure the Transit Network

Applies to Dual-Router Design Only

Configure the transit network between the two routers. You use this network for router-router communication and to avoid hairpinning. The transit network should use an additional subinterface on the EtherChannel interface that is already used to connect to the distribution layer.

The transit network must be a non-passive EIGRP interface.

There are no end stations connected to this network so HSRP and DHCP are not required.

```
interface Port-channel1.99
  description Transit Net
  encapsulation dot1Q 99
  ip address 10.5.0.9 255.255.255.252
  ip pim sparse-mode
!
router eigrp 100
  no passive-interface Port-channel1.99
```

Process

Remote-Site Second Router Distribution Layer

1. Connect DMVPN Spoke Router
2. Configure EIGRP (LAN Side)
3. Configure the Transit Network

Use this set of procedures for a dual-carrier MPLS WAN remote site of a MPLS WAN + DMVPN remote site. Use these procedures to connect a distribution layer when configuring the second router of the dual-router, dual-link design.

Procedure 1 Connect DMVPN Spoke Router

A Layer 2 port-channel interface connects to the WAN distribution switch. This connection allows for multiple VLANs to be included on the EtherChannel if necessary.

The following configuration creates an EtherChannel link between the router and switch, with two channel-group members.

Step 1: Configure the port-channel interface.

Create the port-channel interface. As a best practice, use the same channel numbering on both sides of the link where possible.

```
interface Port-channel [number]
  no ip address
```

Step 2: Configure the port-channel subinterfaces and assign IP addresses.

After you have enabled the physical interface, map the appropriate subinterfaces to the VLANs on the distribution-layer switch. The subinterface number does not need to equate to the 802.1Q tag, but making them the same simplifies the overall configuration.

The subinterface configured on the router corresponds to a VLAN interface on the distribution-layer switch. Traffic is routed between the devices with the VLAN acting as a point-to-point link.

```
interface Port-channel [number].[sub-interface number]
  encapsulation dot1Q [dot1q VLAN tag]
  ip address [IP address] [netmask]
```

Step 3: Enable the port-channel group members and assign the appropriate channel group.

Not all router platforms can support LACP to negotiate with the switch, so EtherChannel is configured statically.

```
interface [interface type] [number]
  no ip address
  channel-group [number]
  no shutdown
```

Example

```
interface Port-channel12
  no ip address
!
interface Port-channel12.54
  encapsulation dot1Q 54
  ip address 10.5.0.5 255.255.255.252
  ip pim sparse-mode
!
interface GigabitEthernet0/1
  no ip address
```

```

channel-group 2
no shutdown
!
interface GigabitEthernet0/2
no ip address
channel-group 2
no shutdown

```

Procedure 2 Configure EIGRP (LAN Side)

You must configure a routing protocol between the router and distribution layer. Step 2, Option 1 is relevant for a MPLS CE router. If configuring a DMVPN spoke router, then perform Step 2, Option 2.

Step 1: Enable EIGRP-100.

EIGRP-100 is configured facing the distribution layer. In this design, all distribution-layer-facing subinterfaces and the loopback must be EIGRP interfaces. All other interfaces should remain passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address.

```

router eigrp [as number]
network [network] [inverse mask]
passive-interface default
no passive-interface [interface]
eigrp router-id [IP address of Loopback0]
no auto-summary

```

Step 2: Configure your router.

Option 1. Redistribute BGP into EIGRP-100 (MPLS CE router only)

Complete this step on an MPLS CE router only. The BGP routes are redistributed into EIGRP with a default metric. By default, only the bandwidth and delay values are used for metric calculation.

```

router eigrp [as number]
default-metric [bandwidth] [delay] 255 1 1500
redistribute bgp [BGP ASN]

```



Reader Tip

Command Reference:

default-metric *bandwidth delay reliability loading mtu*

bandwidth—Minimum bandwidth of the route in kilobytes per second

delay—Route delay in tens of microseconds.

Example—Option 1, MPLS CE Router

```

router eigrp 100
default-metric 100000 100 255 1 1500
network 10.5.0.0 0.0.255.255
redistribute bgp 65511
passive-interface default
no passive-interface Port-channel2.54
eigrp router-id 10.5.48.253
no auto-summary

```

Option 2. Redistribute EIGRP-200 (DMVPN) into EIGRP-100 (DMVPN spoke router only).

Complete this step on the DMVPN spoke router only.

EIGRP-200 is already configured for the DMVPN mGRE interface. Routes from this EIGRP process are redistributed. Because the routing protocol is the same, no default metric is required.

```

router eigrp [as number]
redistribute eigrp [as number (DMVPN)]

```

Example—Option 2, DMVPN Spoke Router

```

router eigrp 100
network 10.5.0.0 0.0.255.255
redistribute eigrp 200
passive-interface default
no passive-interface Port-channel2.54
eigrp router-id 10.5.0.253
no auto-summary

```

Procedure 3 Configure the Transit Network

Applies to Dual-Router Design Only

Configure the transit network between the two routers. You use this network for router-router communication and to avoid hairpinning. The transit network should use an additional subinterface on the EtherChannel interface that is already used to connect to the distribution layer.

The transit network must be a non-passive EIGRP interface.

There are no end stations connected to this network so HSRP and DHCP are not required.

```
interface [interface type] [number].[sub-interface number]
 encapsulation dot1q [dot1q VLAN tag]
 ip address [transit net address] [transit net netmask]
```

Example—DMVPN Spoke Router

```
interface Port-channel2.99
 description Transit Net
 encapsulation dot1q 99
 ip address 10.5.0.10 255.255.255.252
 ip pim sparse-mode
 !
router eigrp 100
 no passive-interface Port-channel2.99
```

Process

Remote-Site WAN Distribution Layer Switch Configuration

1. Finish the Dist Switch Universal Config
2. Connect to the WAN Routers
3. Configure EIGRP
4. Configure Transit Network VLAN

Procedure 1 Finish the Dist Switch Universal Config

This guide assumes that the distribution layer switch has already been configured. Only the procedures required to complete the connection of the switch to the WAN edge routers are included. For details about distribution layer switch configuration, see the *Cisco SBA for Enterprise Organizations—Borderless Networks LAN Deployment Guide*.

Procedure 2 Connect to the WAN Routers

The port-channel interfaces connect to either single or dual WAN routers, and these connections are Layer 2 port channels. The following configuration creates an EtherChannel link between the switch and a router, with two channel-group members. This procedure is repeated for an additional WAN router if necessary.

Step 1: Create the VLAN for the router link on the switch, create the VLAN interface and assign the IP address.

Create the point-to-point VLAN for the router link.

```
vlan [VLAN number]
```

Create the VLAN interface and assign the IP address for the point-to-point link.

```
interface Vlan [VLAN number]
 ip address [IP address] [netmask]
 no shutdown
```

Step 2: Configure the port-channel interface and configure for 802.1q VLAN trunking.

As a best practice, use the same channel numbering on both sides of the link where possible.

```
interface Port-channel [number]
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan [VLAN number]
 switchport mode trunk
```

Step 3: Administratively enable the port-channel group members and assign the appropriate channel group. Configure for 802.1q VLAN trunking.

Not all router platforms can support LACP to negotiate with the switch, so you configure EtherChannel statically.

```
interface [interface type] [number]
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan [VLAN number]
  switchport mode trunk
  channel-group [number] mode on
  no shutdown
```

Example

```
vlan 50
!
interface Port-channel1
  description MPLS CE router
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 50
  switchport mode trunk
!
interface GigabitEthernet1/0/1
  description MPLS CE router port 1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 50
  switchport mode trunk
  channel-group 1 mode on
  no shutdown
!
interface GigabitEthernet2/0/1
  description MPLS CE router port 2
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 50
  switchport mode trunk
  channel-group 1 mode on
  no shutdown
!
interface Vlan50
  ip address 10.5.0.2 255.255.255.252
  no shutdown
```

Procedure 3

Configure EIGRP

Enable EIGRP for the IP address space that the network will be using. If needed for your network, you can enter multiple network statements. Disable autosummarization of the IP networks and enable all routed links to be passive by default. The Loopback 0 IP address is used for the EIGRP router ID to ensure maximum resiliency.

The single logical distribution layer design uses stateful switchover and nonstop forwarding to provide subsecond failover in the event of a supervisor data or control plane failure. This ability reduces packet loss in switchover to redundant logic and keeps packets flowing when the data plane is still intact to adjacent nodes. In the stack-based distribution layer approach, a single logical control point still exists and the master control plane in a stack can failover to another member in the stack providing near-second or subsecond resiliency. When the supervisor or master switch of a distribution platform switches over from the Active to the Hot-Standby supervisor, it will continue switching IP data traffic flows in hardware. However, the supervisor requires time to reestablish control plane two-way peering with EIGRP routing neighbors and avoid the peer router from tearing down adjacencies due to missed hellos that would cause a reroute and disruption of traffic. To allow this time for the supervisor to recover, there is a Nonstop Forwarding (NSF) setting for the routing protocol to wait for the dual supervisor peer switch to recover. The neighboring router is said to be NSF aware if it has a release of IOS that recognizes an NSF peer. All of the platforms used in this design are NSF aware for the routing protocols in use.

You must configure the distribution layer switch to enable NSF for the protocol in use so that it can signal a peer when it switches over to a Hot-Standby supervisor for the peering neighbor to allow it time to reestablish EIGRP protocol to that node. No tuning of the default NSF timers is needed in this network. Nothing has to be configured for an NSF-aware peer router.

```
router eigrp [as number]
  network [network] [inverse mask]
  passive-interface default
  no passive-interface [interface]
  eigrp router-id [IP address of Loopback0]
  no auto-summary
  nsf
```

Example

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 passive-interface default
 no passive-interface Vlan50
 eigrp router-id 10.5.0.252
 no auto-summary
 nsf
```

Example

```
vlan 99
!
interface Port-channel1
 switchport trunk allowed vlan add 99
!
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan add 99
!
interface GigabitEthernet2/0/1
 switchport trunk allowed vlan add 99
```

Procedure 4 Configure Transit Network VLAN

Applies to Dual-Router Design Only

You configure the transit network between the two routers; however, a physical link between the routers is not required. Instead, use a transit VLAN. The distribution layer extends the VLAN across the two existing Layer 2 EtherChannels. The distribution layer does not participate in any routing on the transit network so a VLAN interface is not required for the transit VLAN.

Step 1: Create the transit VLAN on the switch.

Create the transit VLAN.

```
vlan [VLAN number]
```

Step 2: Add the transit VLAN to the existing port-channel trunk interface and channel group members.

```
interface Port-channel [number]
 switchport trunk allowed vlan add [VLAN number]
!
interface [interface type] [number]
 switchport trunk allowed vlan add [VLAN number]
```

Deploying WAN Quality of Service

When configuring the WAN-edge QoS, you are defining how traffic egresses your network. It is critical that the classification, marking, and bandwidth allocations align to the service provider offering to ensure consistent QoS treatment end to end.

Process

Configuring QoS

1. Create the QoS Maps to Classify Traffic
2. Create the Policy Map to Mark BGP Traffic
3. Add ISAKMP Traffic to Network-Critical
4. Define Policy Map to use Queuing Policy
5. Configure Physical Interface S&Q Policy
6. Apply QoS Policy to a Physical Interface

Procedure 1 Create the QoS Maps to Classify Traffic

Use the **class-map** command to define a traffic class and identify traffic to associate with the class name. These class names are used when configuring policy maps that define actions you wish to take against the traffic type. The **class-map** command sets the match logic. In this case, the **match-any** keyword indicates that the maps matches any of the specified criteria. This keyword is followed by the name you want to assign to the class of service. After you have configured the **class-map** command, you define specific values, such as DSCP and protocols to match with the **match** command. You

use the following two forms of the **match** command: **match dscp** and **match protocol**.

Use the following steps to configure the required WAN class-maps and matching criteria.

Step 1: Create the class maps for DSCP matching.

Repeat this step to create a class-map for each of the six WAN classes of service listed in the following table.

You do not need to explicitly configure the default class.

```
class-map match-any [class-map name]
  match dscp [dscp value] [optional additional dscp value(s)]
```

Table 25 - QoS classes of service

Class of service	Traffic type	DSCP values	Bandwidth %	Congestion avoidance
VOICE	Voice traffic	ef	10 (PQ)	-
INTERACTIVE-VIDEO	Interactive video (video conferencing)	cs4, af41	23 (PQ)	-
CRITICAL-DATA	Highly interactive (such as Telnet, Citrix, and Oracle thin clients)	af31, cs3	15	DSCP based
DATA	Data	af21	19	DSCP based
SCAVENGER	Scavenger	af11, cs1	5	-
NETWORK-CRITICAL	Routing protocols. Operations, administration and maintenance (OAM) traffic.	cs6, cs2	3	-
default	Best effort	other	25	random

Step 2: Create a class map for BGP protocol matching.

BGP traffic is not explicitly tagged with a DSCP value. Use NBAR to match BGP by protocol.

This step is only required for a WAN-aggregation MPLS CE router or a WAN

remote-site MPLS CE router that is using BGP.

```
class-map match-any [class-map name]
  match ip protocol [protocol name]
```

Example

```
class-map match-any VOICE
  match dscp ef
!
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
!
class-map match-any CRITICAL-DATA
  match dscp af31 cs3
!
class-map match-any DATA
  match dscp af21
!
class-map match-any SCAVENGER
  match dscp af11 cs1
!
class-map match-any NETWORK-CRITICAL
  match dscp cs6 cs2
!
class-map match-any BGP-ROUTING
  match protocol bgp
```



Tech Tip

You do not need to configure a Best-Effort Class. This is implicitly included within class-default as shown in Procedure 4.

Procedure 2

Create the Policy Map to Mark BGP Traffic

This procedure is only required for a WAN-aggregation MPLS CE router or a WAN remote-site MPLS CE router that uses BGP.

To ensure proper treatment of BGP routing traffic in the WAN, you must assign a DSCP value of cs6. Although the class-map you created in the previous step matches all BGP traffic to the class named BGP, you must configure a policy-map to assign the required DSCP value to all BGP traffic.

```
policy-map MARK-BGP
  class BGP-ROUTING
    set dscp cs6
```

Procedure 3

Add ISAKMP Traffic to Network-Critical

For a WAN connection using DMVPN, you need to ensure proper treatment of ISAKMP traffic in the WAN. To classify this traffic requires the creation of an access-list and the addition of the access-list name to the NETWORK-CRITICAL class-map created in Procedure 1.

This procedure is only required for a WAN-aggregation DMVPN hub router or a WAN remote-site DMVPN spoke router.

Step 1: Create the access-list.

```
ip access-list extended ISAKMP
  permit udp any eq isakmp any eq isakmp
```

Step 2: Add the match criteria to the existing NETWORK-CRITICAL class-map.

```
class-map match-any NETWORK-CRITICAL
  match access-group name ISAKMP
```

Procedure 4 Define Policy Map to use Queuing Policy

This procedure applies to all WAN routers.

The WAN policy map references the class names you created in the previous procedures and defines the queuing behavior along with the maximum guaranteed bandwidth allocated to each class. This specification is accomplished with the use of a policy-map. Then, each class within the policy map invokes an egress queue, assigns a percentage of bandwidth, and associates a specific traffic class to that queue. One additional default class defines the minimum allowed bandwidth available for best effort traffic.

The local router policy maps define seven classes while most service providers offer only six classes of service. The NETWORK-CRITICAL policy map is defined to ensure the correct classification, marking, and queuing of network-critical traffic on egress to the WAN. After the traffic has been transmitted to the service provider, the network-critical traffic is typically remapped by the service provider into the critical data class. Most providers perform this remapping by matching on DSCP values cs6 and cs2.

Step 1: Create the parent policy map.

```
policy-map [policy-map-name]
```

Steps 2–6 are repeated for each class in Table 25 including class-default.

Step 2: Apply the previously created class-map.

```
class [class-name]
```

Step 3: (Optional) Assign the maximum guaranteed bandwidth for the class.

```
bandwidth percent [percentage]
```

Step 4: (Optional) Define the priority queue for the class.

```
priority percent [percentage]
```

Step 5: (Optional) Apply the child service policy.

This is an optional step only for the NETWORK-CRITICAL class of service with the MARK-BGP child service policy.

```
service-policy [policy-map-name]
```

Step 6: (Optional) Define the congestion mechanism.

```
random-detect [type]
```

Example

```
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
```



Tech Tip

Although these bandwidth assignments represent a good baseline, it is important to consider your actual traffic requirements per class and adjust the bandwidth settings accordingly.

Procedure 5 Configure Physical Interface S&Q Policy

With WAN interfaces using Ethernet as an access technology, the demarcation point between the enterprise and service provider may no longer have a physical-interface bandwidth constraint. Instead, a specified amount of access bandwidth is contracted with the service provider. To ensure the offered load to the service provider does not exceed the contracted rate that results in the carrier discarding traffic, you need to configure shaping on the physical interface. This shaping is accomplished with a QoS service policy. You configure a QoS service policy on the outside Ethernet interface, and this parent policy includes a shaper that then references a second or subordinate (child) policy that enables queuing within the shaped rate. This is called a hierarchical Class-Based Weighted Fair Queuing (HCBWFQ) configuration. When you configure the **shape average** command, ensure that the value matches the contracted bandwidth rate from your service provider.

This procedure applies to all WAN routers. You can repeat this procedure multiple times to support devices that have multiple WAN connections attached to different interfaces.

Step 1: Create the parent policy map.

As a best practice, embed the interface name within the name of the parent policy map.

```
policy-map [policy-map-name]
```

Step 2: Configure the shaper.

```
class [class-name]
  shape [average | peak] [bandwidth (kbps)]
```

Step 3: Apply the child service policy.

```
policy-map [policy-map-name]
```

Example

This example shows a router with a 20-Mbps link on interface GigabitEthernet0/0 and a 10-Mbps link on interface GigabitEthernet0/1.

```
policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 20000000
  service-policy WAN
!
policy-map WAN-INTERFACE-G0/1
  class class-default
    shape average 10000000
  service-policy WAN
```

Procedure 6 Apply QoS Policy to a Physical Interface

To invoke shaping and queuing on a physical interface, you must apply the parent policy that you configured in the previous procedure.

This procedure applies to all WAN routers. You can repeat this procedure multiple times to support devices that have multiple WAN connections attached to different interfaces.

Step 1: Select the WAN interface.

```
interface [interface type] [number]
```

Step 2: Apply the WAN QoS policy.

The service policy needs to be applied in the outbound direction.

```
service-policy output [policy-map-name]
```

Example

```
interface GigabitEthernet0/0
  service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
  service-policy output WAN-INTERFACE-G0/1
```


Deploying Application Optimization with WAAS

Business Overview

The number of remote work sites is increasing, so network administrators need tools to help them ensure solid application performance in remote locations. Recent trends show that the number of remote sites is increasing and that a majority of new hires are located at remote sites. These trends are tied to global expansion, employee attraction and retention, mergers and acquisitions, cost savings, and environmental concerns.

In the meantime, remote-site communications requirements are evolving to embrace collaborative applications, video, and Web 2.0 technologies. These developments are also placing greater performance demands on the remote sites and the WAN.

The enterprise trend toward data-center consolidation also continues. The consolidation efforts move most remote-site assets into data centers, largely to comply with regulatory mandates for centralized security and stronger control over corporate data assets.

Consolidating data centers while growing the remote-site population means that increasing numbers of remote employees access LAN-based business applications across comparatively slow WANs. With these applications growing increasingly multimedia-centric and latency-sensitive, IT and networking staffs are further challenged to keep remote-application response times on par with the experiences of users situated locally to the company's application servers in the data center. These local users enjoy multimegabit LAN speeds and are not affected by any distance-induced delay, unlike their counterparts at the other end of a WAN connection.

Application optimization can boost network performance along with enhancing security and improving application delivery. Cisco WAN Optimization is an architectural solution comprising a set of tools and techniques that work together in a strategic systems approach to provide best-in-class WAN optimization performance while minimizing its total cost of ownership.

Technology Overview

WAN Aggregation

The WAN-aggregation site uses a cluster of two or more WAE devices to provide WAAS capabilities. The WAE appliances connect to the distribution-layer switch. The connections use EtherChannel both for increased throughput and for resiliency. The WAEs connect to the WAN services network that is configured on the distribution switch.

The WAN 500 design uses a cluster of WAE-7371 devices. The total number of devices required is a minimum of 2 (for N+1 redundancy). Similarly, the WAN 100 design uses a cluster of WAE-7341 devices and the total number of devices required is a minimum of 2 (for N+1 redundancy). Additional detail on the WAE sizing is provided in the following table. The fan-out numbers correspond to the total number of remote-peer WAE devices.

Table 26 - WAN-aggregation WAE options

Device	Max optimized TCP connections	Max recommended WAN link [Mbps]	Max optimized throughput [Mbps]	Max core fan-out [Peers]
WAVE-594-8GB	750	50	250	50
WAVE-594-12GB	1300	100	300	100
WAE-694-16GB	2500	200	450	150
WAE-694-24GB	6000	200	500	300
WAE-7341	12000	310	1000	1400
WAE-7371	50000	1000	2500	2800
WAVE-7541	18000	500	1000	700
WAVE-7571	60000	1000	2000	1400
WAVE-8541	150000	2000	4000	2800

A more comprehensive, interactive WAAS sizing tool is available for registered users of [cisco.com](http://tools.cisco.com/WAAS/sizing):

<http://tools.cisco.com/WAAS/sizing>

The WCCP is a protocol developed by Cisco. Its purpose is to transparently intercept and redirect traffic from a network device to a WCCP appliance such as a WAE running WAAS (discussed below).

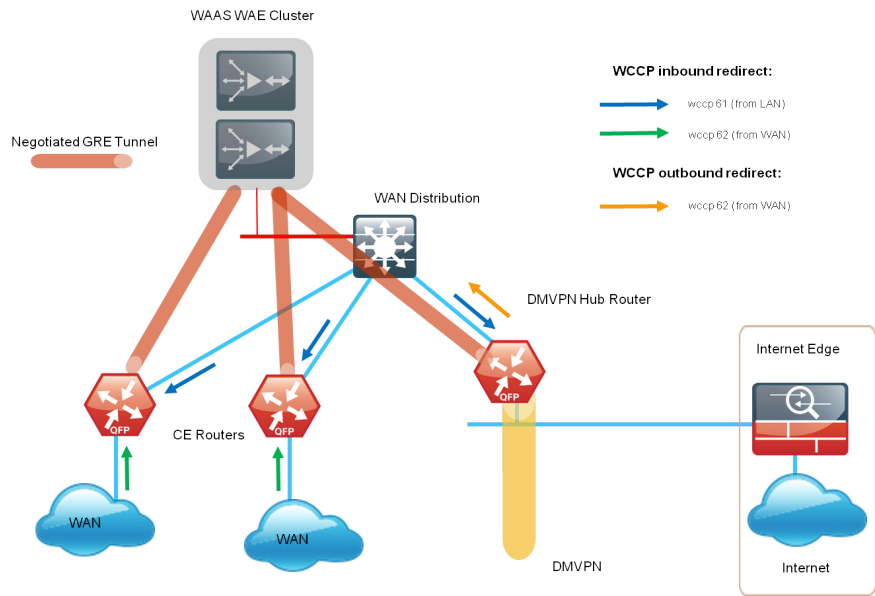
WCCP is enabled on the MPLS CE and DMVPN routers. The WCCP redirect uses service groups 61 and 62 to match traffic for redirection. These service groups must be used in pairs:

- Service group 61 uses the source address to redirect traffic
- Service group 62 uses the destination address to redirect traffic

This design uses WCCP 61 inbound on LAN-facing interfaces to match unoptimized data sourced from the data center that is destined for clients at the WAN remote sites. WCCP 62 is used inbound on WAN-facing interfaces, matching optimized data sourced from the WAN remote sites. WCCP 62 is used outbound on LAN interfaces for DMVPN hub routers.

The connections from the switch to the MPLS CE and DMVPN routers are all routed point-to-point links. This design mandates the use of a negotiated-return GRE tunnel from WAE to router. When a design uses a GRE negotiated return, it is not required to extend the WAN services VLAN to include the MPLS CE and DMVPN routers.

Figure 30 - WAN aggregation—WAAS topology



Remote Sites

The WAN Optimization design for the remote sites can vary somewhat based on site-specific characteristics. Single router sites use a single (nonredundant) WAE. Similarly, all dual-router sites use dual WAEs. The

specifics of the WAE sizing and form-factor primarily depend on the number of end users and bandwidth of the WAN links. Low bandwidth (< 2 Mbps) single-router, single-link sites can also use the embedded WAASx capability of the router.

There are many factors to consider in the selection of the WAN remote-site WAN Optimization platform. The primary parameter of interest is the bandwidth of the WAN link. After the bandwidth requirement has been met, the next item under consideration is the maximum number of concurrent, optimized TCP connections. Additional detail on the WAE sizing is provided in the following table. The optimized throughput numbers correspond to the apparent bandwidth available after successfully optimization by WAAS.

Table 27 - WAN remote-site WAE options

Device	Max optimized TCP connections	Max recommended WAN link [Mbps]	Max optimized throughput [Mbps]
Cisco1941/WAASX ¹	150	4	8
SRE-700-S	200	20	200
SRE-700-M	500	20	200
SRE-900-S	200	50	300
SRE-900-M	500	50	300
SRE-900-L	1000	50	300
WAVE-294-4GB	200	10	100
WAVE-294-8GB	500	20	150
WAVE-594-8GB	750	50	250
WAVE-594-12GB	1300	100	300
WAE-694-16GB	2500	200	450
WAE-694-24GB	6000	200	500
WAE-7341	12000	310	1000
WAE-7371	50000	1000	2500
WAVE-7541	18000	500	1000
WAVE-7571	60000	1000	2000
WAVE-8541	150000	2000	4000

Notes:

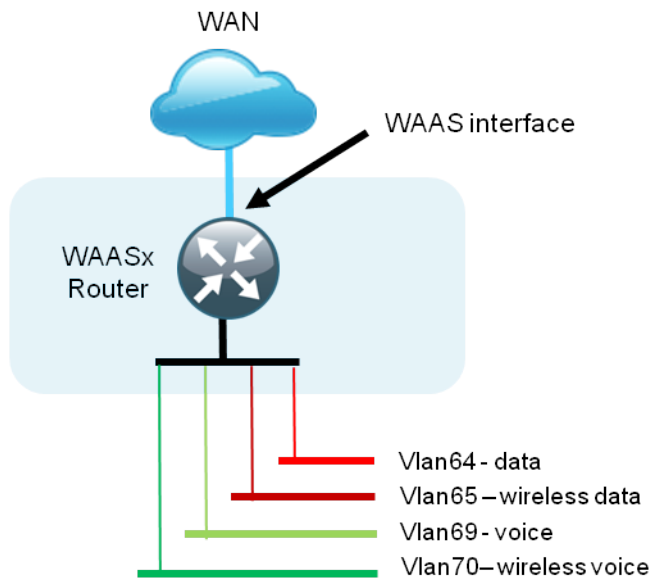
1. Single link design only

A more comprehensive, interactive WAAS sizing tool is available for registered users of cisco.com:

<http://tools.cisco.com/WAAS/sizing>

The embedded router WAASx provides a subset of the full set of WAAS capabilities available on the WAE platforms. The current WAASx software release is compatible with single-link WAN designs, cost-effective, and easy to deploy. No design or architecture changes are required to enable this functionality on the router.

Figure 31 - WAN remote-site - WAASx topology



The WAE form factors previously discussed include a router Services Ready Engine (SRE) and an external appliance. These variants all run the same WAAS software and are functionally equivalent. The primary difference is the method of LAN attachment for these devices:

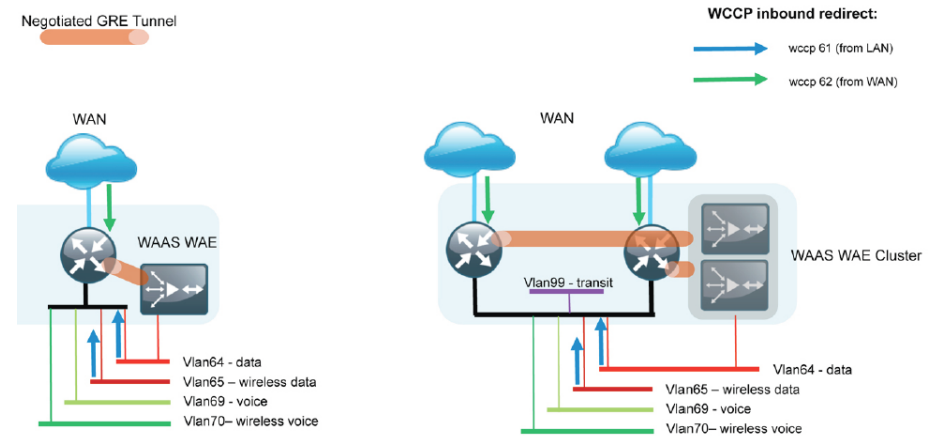
- SRE: One internal interface (router connect only), one external interface
- Appliance: Two interfaces (both external)

The approach for connecting the WAE devices to the LAN is to be consistent regardless of the chosen hardware form-factor. All WAE connections are made using the external interfaces. The benefit of this method is that it is not necessary to create a dedicated network specifically to attach the WAE devices, and the SRE and appliance devices can use an identical design. The internal interface of the SRE is not used for this design, except for the initial bootstrapping of the device configurations.

You must connect an external Ethernet cable from each SRE module for this solution.

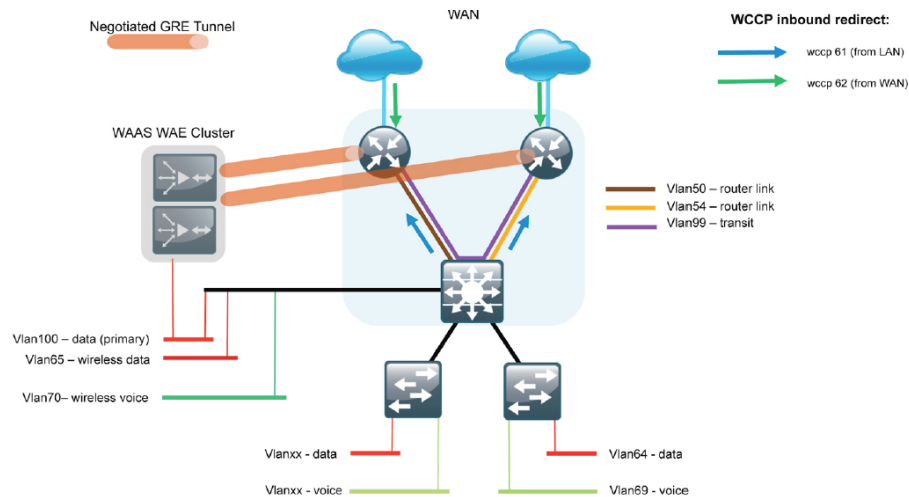
You should connect the WAE devices to the data VLAN of the access switch in all flat Layer 2 designs.

Figure 32 - WAN remote-site—WAAS topology (access layer connection)



When the deployment uses a distribution-layer design, the WAE devices should connect to the primary data VLAN on the distribution switch.

Figure 33 - WAN remote-site—WAAS topology (distribution layer connection)



Where possible, connect the WAE appliances through both interfaces using EtherChannel for performance and resiliency.

WCCP Version 2 is enabled on the WAN routers to redirect traffic to the WAAS appliances.

The WCCP redirect uses service groups 61 and 62 to match traffic for redirection. These services groups must be used in pairs:

- Service group 61 uses the source address to redirect traffic
- Service group 62 uses the destination address to redirect traffic

This design uses WCCP 61 inbound on LAN-facing VLAN subinterfaces to match unoptimized data sourced from the clients destined for the data center (or other remote sites). In all cases, WCCP 62 is used inbound on WAN-facing interfaces to match optimized data sourced from the data center (or other remote sites).

Because the WAE is connected to the data VLAN, this design requires the use of a negotiated-return GRE tunnel from the WAE to the router. When using a GRE-negotiated return, you are not required to create a new network on the routers specifically to attach the WAEs.

The following steps provide an overview of the tasks required to configure a basic WAAS environment.

Process

WAAS/WAE Configuration

1. Install the vWAAS Virtual Machine
2. Configure the WAAS Central Manager
3. Configure Switch for WAE Appliances
4. Configuring the WAE Appliance Devices
5. Configure the WAE SRE Devices
6. Configure Remote Switch for WAE Devices
7. Configure WCCPv2 on Routers
8. Configure the Central Manager for WAASx
9. Configure WAAS Express Routers

Procedure 1

Install the vWAAS Virtual Machine

This procedure is optional and only required if you are using a Virtual WAAS (vWAAS).

vWAAS is provided as an Open Virtual Appliance (OVA). The OVA is pre-packaged with disk, memory, CPU, NICs and other virtual machine related configuration parameters. This is an industry standard and many virtual appliances are available in this format. A different OVA file is provided for each vWAAS model.



Tech Tip

The OVA files are only available in DVD media format and are not available for download on www.cisco.com at this time.

Step 1: Deploy OVF Template with VMWare vSphere client.

You must first install the vWAAS OVA on the VMware ESX/ESXi server using vSphere before configuring vWAAS.

Step 2: Configure the device using the VMware console.

The procedures and steps for configuring the vWAAS Central Manager and vWAAS Application Accelerator devices are identical to those for the WAE appliance and SRE form factors. Select the appropriate following procedure to complete the vWAAS configuration.

Procedure 2 Configure the WAAS Central Manager

Use a Cisco WAVE-574 device for the Central Manager function at the primary location to provide graphical management, configuration, and reporting for the WAAS network. This device resides in the server farm because it is not directly in the forwarding path of the WAN optimization, but provides management and monitoring services. Initial configuration of the Central Manager requires terminal access to the console port for basic configuration options and IP address assignment. For all WAE devices, the factory default username is admin and the factory default password is default.

You can start the initial setup utility from the command line by entering the **setup** command.

Step 1: Run setup.

Parameter	Default Value
1. Device Mode	Application Accelerator
2. Interception Method	WCCP
3. Time Zone	UTC 0 0
4. Management Interface	GigabitEthernet 1/0
5. Autosense	Enabled
6. DHCP	Enabled
ESC Quit ? Help	WAAS Default Configuration

Press 'y' to select above defaults, 'n' to configure all, <1-6> to change specific default [y]: n

Step 2: Configure as Central Manager.

1. Application Accelerator
 2. Central Manager
- Select device mode [1]: 2

Step 3: Configure time zone.

Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)>
[UTC 0 0]: **PST -8 0**

Step 4: Configure management interface, IP address, and default gateway.

No.	Interface Name	IP Address	Network Mask
1.	GigabitEthernet	1/0	dhcp
2.	GigabitEthernet	2/0	dhcp

Select Management Interface [1]: 1
Enable Autosense for Management Interface? (y/n) [y]: **y**
Enable DHCP for Management Interface? (y/n) [y]: **n**
Enter Management Interface IP Address
<a.b.c.d or a.b.c.d/X(optional mask bits)> [Not configured]:
10.4.48.100/24
Enter Default Gateway IP Address [Not configured]: **10.4.48.1**

Step 5: Configure DNS, host, and NTP settings.

Enter Domain Name Server IP Address [Not configured]:
10.4.48.10
Enter Domain Name(s) (Not configured): **cisco.local**
Enter Host Name (None): **WAAS-WCM-1**
Enter NTP Server IP Address [None]: **10.4.48.17**

Step 6: Select appropriate license.

The product supports the following licenses:

1. Enterprise
- Enter the license(s) you purchased [1]: **1**

Step 7: Verify configuration settings and initiate reload.

Parameter	Configured Value
1. Device Mode	Central Manager
2. Time Zone	PST -8 0
3. Management Interface	GigabitEthernet 1/0
4. Autosense	Enabled
5. DHCP	Disabled
6. IP Address	10.4.48.100
7. IP Network Mask	255.255.255.0
8. IP Default Gateway	10.4.48.1
9. DNS IP Address	10.4.48.10
10. Domain Name(s)	cisco.local
11. Host Name	WAAS-WCM-1
12. NTP Server Address	10.4.48.17
13. License	Enterprise

ESC Quit ? Help ! CLI ————— WAAS Final Configuration

Press 'y' to select configuration, 'd' to toggle defaults display, <1-13> to change specific parameter [y]: **y**
 Apply WAAS Configuration: Device Mode changed in SETUP; New configuration takes effect after a reload. If applicable, registration with CM, CM IP address, WAAS WCCP configuration etc, are applied after the reboot. Initiate system reload?
 <y/n> [n] **y**
 Are you sure? <y/n> [n]: **y**

Step 8: After the reboot, login to the WAAS Central Manager and enable SSH.

To enable SSH, you need to generate the RSA key and enable the sshd service.

```
ssh-key-generate key-length 2048
sshd version 2
sshd enable
```

Step 9: Disable telnet.

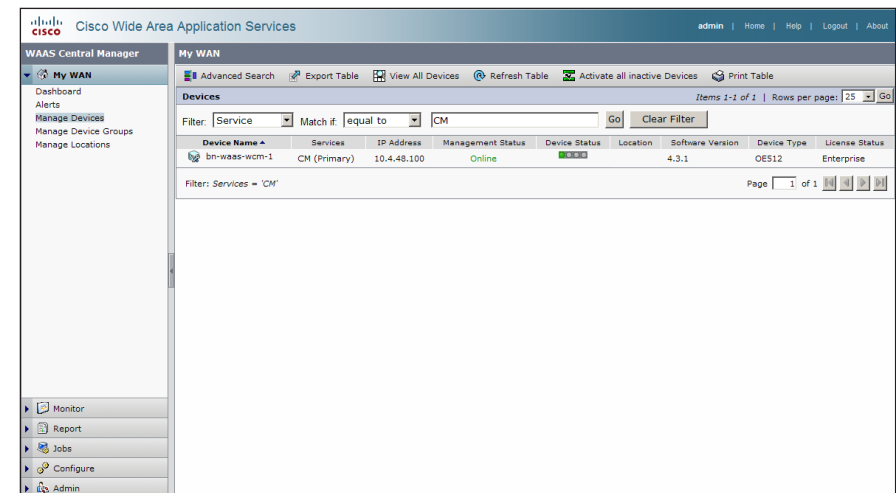
```
no telnet enable
```

Step 10: Access the WAAS Central Manager through the web interface.

The Central Manager device should now be up and running after the reload completes, and be accessible to a web browser at the IP address assigned during Step 6 of the setup utility, or at the associated host name if it has been configured in DNS. Specify secure HTTP and the port number 8443 to access the Central Manager, for example https://10.4.48.100:8443. Login using the default user name of **admin** and password of **default**.

Step 11: Click **My WAN > Manage Devices**. The Central Manager appears in the My WAN window as the only managed device.

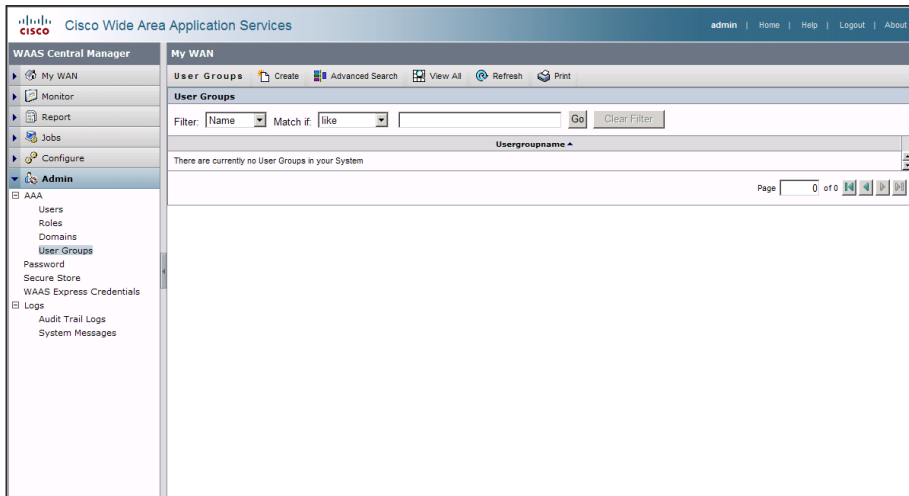
Figure 34 - WAAS Central Manager-Initial Managed device list



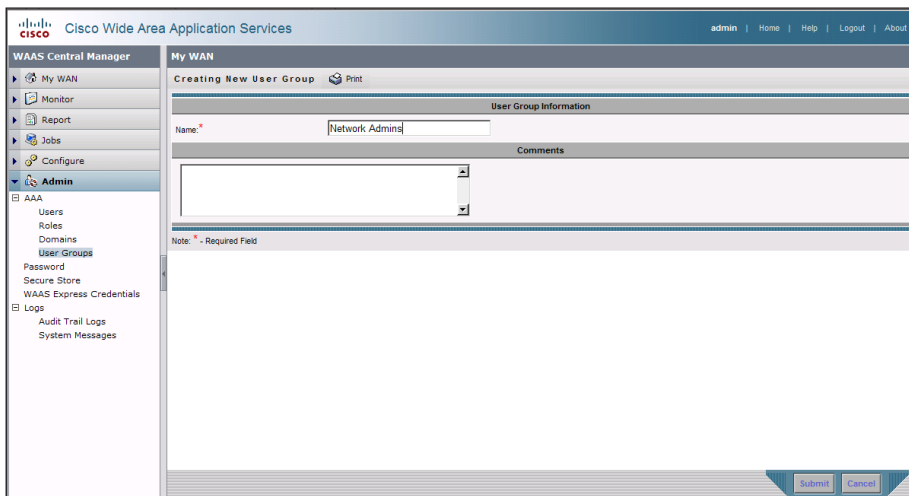
Step 12: Configure Network-Admins user group.

The web interface for the Central Manager requires a user group with the proper role assigned to authorize users from an external AAA database. This step must be completed before enabling AAA in the following step and can only be performed using the web interface.

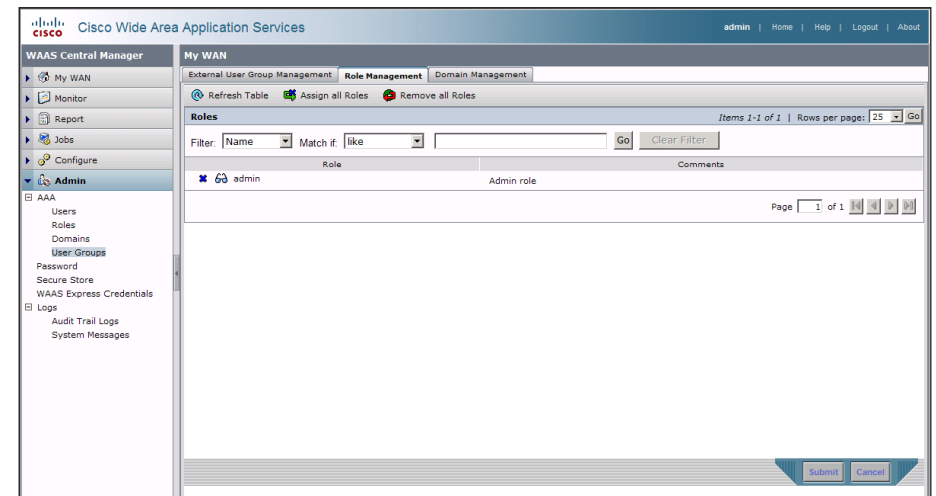
In **Admin > AAA** click **User Groups**.



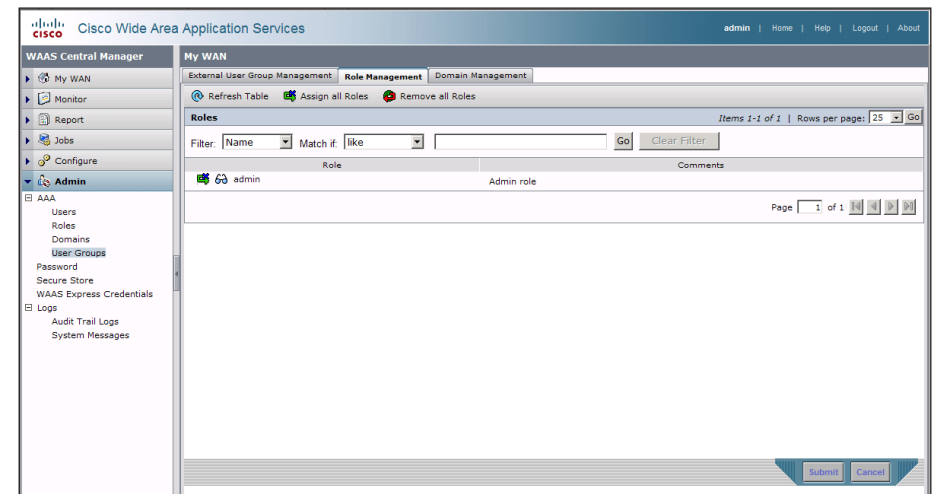
Click **Create** and then in the Name field, type a name. This name must match exactly (case sensitive) the group name used on the AAA server. For example, "Network Admins" in this implementation.



After you create the group, click the **Role Management** tab and then click the **X** to assign the role.



After you properly assign the role, a large green check marks appears next to the icon.



Step 13: Configure secure user authentication

Enable AAA authentication for access control. AAA controls all management access to the WAAS/WAE devices (SSH and HTTPS).

A local admin user was created on the WAAS/WAE during setup. This user account provides the ability to manage the device in case the centralized TACACS+ server is unavailable or in case you do not have a TACACS+ server in your organization.



Tech Tip

The AAA configuration details shown are for the WAAS devices only. Additional configuration is required on the AAA server for successful user authorization. Do not proceed with configuring secure user authentication until you have completed the relevant steps in the *Cisco SBA for Enterprise Organizations—Borderless Networks Network Device Authentication and Authorization Deployment Guide*.

The following configures TACACS+ as the primary method for user authentication (login) and user authorization (configuration).

```
tacacs key SecretKey
tacacs password ascii
tacacs host 10.4.48.15 primary
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
```

Step 14: After you make configuration changes, save the configuration.

```
copy running-config startup-config
```

Procedure 3

Configure Switch for WAE Appliances

The WAN distribution switch is the appropriate location to physically connect devices at the WAN-aggregation site such as WAE appliances that support WAN optimization. This device type requires a resilient connection but does not require a routing protocol. This type of connection can use a Layer 2 EtherChannel link.

This guide assumes that the distribution layer switch has already been configured. Only the procedures required to complete the connection of the switch to the WAE appliances are included. Full details on distribution layer switch configuration are included in the *Cisco SBA for Enterprise Organizations—Borderless Networks LAN Deployment Guide*.

You must create a VLAN and SVI for this and other devices with similar connectivity requirements. This VLAN is referred to as the WAN service network.

Step 1: Create the VLAN and SVI.

```
vlan [VLAN number]
  name [VLAN name]
!
interface Vlan [VLAN number]
  ip address [IP address] [netmask]
  no shutdown
```

Step 2: Configure Layer 2 EtherChannel links for the devices and associate them with the VLAN.

```
interface Port-channel [number]
  switchport access vlan [VLAN number]
!
interface [type] [number]
  switchport access vlan [VLAN number]
  channel-group [number] mode on
  no shutdown
```

Example

```
vlan 350
  name WAN_Service_Net
!
interface Port-channel17
  description bn-wae-1 EtherChannel
  switchport access vlan 350
!
interface GigabitEthernet1/0/2
  description bn-wae-1 port 1
  switchport access vlan 350
  channel-group 7 mode on
  no shutdown
!
interface GigabitEthernet2/0/2
  description bn-wae-1 port 2
  switchport access vlan 350
  channel-group 7 mode on
  no shutdown
!
interface Vlan350
  ip address 10.4.32.129 255.255.255.192
  no shutdown
```

Procedure 4 Configuring the WAE Appliance Devices

A cluster of Cisco WAE-7341 appliances is deployed at the WAN-aggregation site to provide the headend termination for WAAS traffic to and from the remote sites across the WAN. You connect these devices directly to the WAN distribution-layer switch, using GRE-negotiated return to communicate with the WCCP routers.

You can also deploy WAE appliances at WAN remote sites, either individually or as part of a WAE cluster. You should use this procedure to configure WAN remote-site WAE appliances. You use the same setup utility that you used in the initial configuration of the WAAS Central Manager to set up WAE appliance devices. These devices only require basic setup through their console port to assign initial settings. After you complete this setup, you can perform all management of the WAAS network through the WAAS Central Manager console.

Initial configuration of the WAE application accelerators requires terminal access to the console port for basic configuration options and IP address assignment. For all WAE devices, the factory default user name is admin and the factory default password is default.

The setup utility configuration steps for the application accelerator WAEs are similar to the setup of the Central Manager, but the steps begin to differ after you choose application-accelerator as the device mode in Step 2. After you choose this mode, the setup script changes to allow you to register the WAE with the existing Central Manager, and to define the traffic interception method as WCCP.

Step 1: Run setup.

You can start the initial setup utility from the command line by entering the **setup** command.

Parameter	Default Value
1. Device Mode	Application Accelerator
2. Interception Method	WCCP
3. Time Zone	UTC 0 0
4. Management Interface	GigabitEthernet 1/0
5. Autosense	Enabled
6. DHCP	Enabled
ESC Quit ? Help	WAAS Default Configuration

Press 'y' to select above defaults, 'n' to configure all, <1-6> to change specific default [y]: n

Step 2: Configure as application accelerator.

1. Application Accelerator
 2. Central Manager
- Select device mode [1]: **1**

Step 3: Configure interception method.

1. WCCP
 2. Other
- Select Interception Method [1]: **1**

Step 4: Configure time zone.

Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)>
[UTC 0 0]: **PST -8 0**

Step 5: Configure management interface, IP address, and default gateway.

```
No. Interface Name      IP Address      Network Mask
 1. GigabitEthernet    1/0             dhcp
 2. GigabitEthernet    2/0             dhcp

Select Management Interface [1]: 1
Enable Autosense for Management Interface? (y/n) [y]: y
Enable DHCP for Management Interface? (y/n) [y]: n
Enter Management Interface IP Address
<a.b.c.d or a.b.c.d/X(optional mask bits)> [Not configured]:
10.4.32.161/26
Enter Default Gateway IP Address [Not configured]: 10.4.32.129
Enter Central Manager IP Address (WARNING: An invalid entry
will cause SETUP to take a long time when applying WAAS
configuration) [None]: 10.4.48.100
```

Step 6: Configure DNS, host, and NTP settings.

```
Enter Domain Name Server IP Address [Not configured]:
10.4.48.10
Enter Domain Name(s) (Not configured): cisco.local
Enter Host Name (None): WAE7341-1
Enter NTP Server IP Address [None]: 10.4.48.17
```

Step 7: Configure WCCP router list.

```
Enter WCCP Router (max 4) IP Address list (ip1 ip2 ...) []:
10.4.32.241 10.4.32.242 10.4.32.243
```

Step 8: Select appropriate license.

```
The product supports the following licenses:
 1. Transport
 2. Enterprise
 3. Enterprise & Video
 4. Enterprise & Virtual-Blade
 5. Enterprise, Video & Virtual-Blade
Enter the license(s) you purchased [2]: 2
```

Step 9: Verify configuration settings.

Parameter	Configured Value
2. Interception Method	WCCP
3. Time Zone	PST -8 0
4. Management Interface	GigabitEthernet 1/0
5. Autosense	Enabled
6. DHCP	Disabled
7. IP Address	10.4.32.161
8. IP Network Mask	255.255.255.192
9. IP Default Gateway	10.4.32.129
10. CM IP Address	10.4.48.100
11. DNS IP Address	10.4.48.10
12. Domain Name(s)	cisco.local
13. Host Name	WAE7341-1
14. NTP Server Address	10.4.48.17
15. WCCP Router List	10.4.32.241 10.4.32.242 10.4.32.243
16. License	Enterprise

```
ESC Quit ? Help ! CLI _____ WAAS Final Configuration
```

```
Press 'y' to select configuration, <F2> to see all
configuration, 'd' to toggle defaults display, <1-16> to
change specific parameter [y]: y
Applying WAAS configuration on WAE ...
May take a few seconds to complete ...
```

If the switch connection to the WAE is configured as a port-channel, this procedure will fail, because the WAE setup script does not enable the port-channel. If so, the registration with the WAAS Central Manager is completed manually in Step 11.

Step 10: (Optional) Configure port-channel connection for WAE to connect to the distribution switch stack.

This is an optional step that is only required when connecting the WAE using a port channel for a resilient connection.

```
interface GigabitEthernet 1/0
 no ip address 10.4.32.161 255.255.255.192
 exit
!
primary-interface PortChannel 1
```

```

!
interface PortChannel 1
 ip address 10.4.32.161 255.255.255.192
 exit
!
interface GigabitEthernet 1/0
 channel-group 1
 exit
interface GigabitEthernet 2/0
 channel-group 1
 exit

```

Step 11: (Optional) Complete registration with WAAS Central Manager.

After the port-channel has been configured, the WAE can reach the WAAS Central Manager. Run the **cms enable** command to force a manual registration.

This is an optional step only required when connecting the initial attempt to register in Step 9 has failed.

```

cms enable
Registering WAAS Application Engine...
Sending device registration request to Central Manager with
address 10.4.48.100
Please wait, initializing CMS tables
Successfully initialized CMS tables
Registration complete.
Please preserve running configuration using 'copy running-
config startup-config'.
Otherwise management service will not be started on reload and
node will be shown 'offline' in WAAS Central Manager UI.
management services enabled

```

There are several additional non-default settings that are enabled on the WAE devices to complete the configuration. These settings are configured in Steps 13 through 15.

Step 12: Configure GRE negotiated return.

All WAE devices use GRE-negotiated return with their respective WCCP routers.

```
egress-method negotiated-return intercept-method wccp
```

Step 13: Configure WCCP router list.

The setup script generated a router-list based on the information provided. To view the device configuration, enter the following command:

```

WAE-7341-1# show running-config | include wccp router-list
wccp router-list 8 10.4.32.241 10.4.32.242 10.4.32.243

```

Router list 8 is specifically for use with WCCP configured on a default gateway router. This design uses GRE-negotiated return and router loopback addresses so we need to create a new router list and delete router list 8.

All WAE configurations in this design use router list 1.

```

no wccp router-list 8 10.4.32.241 10.4.32.242 10.4.32.243
wccp router-list 1 10.4.32.241 10.4.32.242 10.4.32.243

```

This design uses authentication between the routers and WAE.

NOTE: ASR1000 series routers must use WCCP mask-assign mode for WCCP to operate properly.

If any of the WCCP routers are Cisco ASR1000 Series routers, then change the default setting of hash-source-ip to mask-assign. This change is made on the WAEs, not on the routers.

```

wccp tcp-promiscuous router-list-num 1 password c1sco123 mask-
assign

```

All other router platforms can use the default setting:

```
wccp tcp-promiscuous router-list-num 1 password c1sco123
```

Step 14: Enable SSH.

To enable SSH, you must generate the RSA key and enable the sshd service.

```

ssh-key-generate key-length 2048
sshd version 2
sshd enable

```

Step 15: Disable telnet.

```
no telnet enable
```

Step 16: Configure secure user authentication.

Enable AAA authentication for access control. AAA controls all management access to the WAAS/WAE devices (SSH and HTTPS).

A local admin user was created on the WAAS/WAE during setup. This user account provides the ability to manage the device in case the centralized TACACS+ server is unavailable, or if you do not have a TACACS+ server in your organization.

The following configures TACACS+ as the primary method for user authentication (login) and user authorization (configuration).

```
tacacs key SecretKey
tacacs password ascii
tacacs host 10.4.48.15 primary
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
```

Step 17: Save the configuration.

After you make configuration changes, save the configuration.

```
copy running-config startup-config
```

Procedure 5

Configure the WAE SRE Devices

You can use a variety of WAE appliances or SRE form-factors for the remote-site WAAS equipment in this design, depending on the performance requirements.

You can insert the SRE modules directly into a corresponding module slot in the remote-site router and configure them somewhat differently from the appliances. If you are using an appliance, you can follow the WAN-Aggregation WAE device set of procedures with remote-site addressing parameters.

Although the remote-site router can potentially communicate directly with the SRE by using the router backplane, this design uses the external interfaces on the modules, which allows for a consistent design implementation regardless of the chosen WAE device. The SM interface must be enabled and have an arbitrary (locally significant only) IP address assigned in order to be accessed through a console session from the host router.

You must connect the external interface to the data network on the access or distribution switch for this configuration to work properly.

Step 1: Configure console access and SRE IP addresses on the host router.

To permit console access to the SRE modules, you must enter the following commands on the host router.

```
interface SM1/0
ip address 1.1.1.1 255.255.255.252
service-module external ip address 10.5.52.8 255.255.255.0
service-module ip default-gateway 10.5.52.1
no shutdown
```



Tech Tip

The IP address assigned 1.1.1.1 to SM/0 is arbitrary in this design and only locally significant to the host router.

Step 2: (Optional) Configure a AAA exemption for SRE devices.

If AAA has been enabled on the router, you will be prompted for both a router login and a WAAS login; this can be confusing. Disabling the initial router authentication requires the creation of a AAA method, which then is applied to the specific line configuration on the router associated with the SRE/NME.

Create the AAA login method:

```
aaa authentication login MODULE none
```

Determine which line number is assigned to SRE. The example output below shows line 67.

```
Br203-2921-1# show run | begin line con 0
line con 0
  logging synchronous
line aux 0
line 67
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
```

```

flowcontrol software
line vty 0 4
password 7 04585A150C2E1D1C5A
transport input ssh

```

Restrict access to the SRE/NME console by creating an access-list. The access-list number is arbitrary, but the IP address must match the address assigned to the SM interface in the previous step.

```
access-list 67 permit 1.1.1.1
```

Assign the method to the appropriate line:

```

line 67
login authentication MODULE
access-class 67 in
transport output none

```

Step 3: Connect to the WAE console using a session from the host router.

After the IP address is assigned, and the interface is enabled, it is possible to open a session on the WAE and run the setup script. For all WAE devices, the factory default username is admin and the factory default password is default.

NOTE: If you are using secure user authentication on the router and have not created a AAA exemption, you must first authenticate with a valid router login credential before logging into the WAE console session.

```
Br203-2921-1# service-module sm 1/0 session
```

Step 4: Run setup.

You can start the initial setup utility from the command line by entering the setup command.

```

Parameter                Default Value
Device Mode               Application Accelerator
1. Interception Method    WCCP
2. Time Zone              UTC 0 0
3. Management Interface   GigabitEthernet 1/0      (internal)
                           Autosense              Disabled
                           DHCP                  Disabled
ESC Quit ? Help _____ WAAS Default Configuration

```

Press 'y' to select above defaults, 'n' to configure all, <1-3> to changespecific default [y]: n

Step 5: Configure interception method.

1. WCCP
 2. Other
- Select Interception Method [1]: 1

Step 6: Configure time zone.

```

Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)>
[UTC 0 0]: PST -8 0

```

Step 7: Configure management interface, IP address, and default gateway.

This design uses the external interface as the management interface.

```

No. Interface Name   IP Address   Network Mask
1. GigabitEthernet  1/0          unassigned   unassigned
(internal)
2. GigabitEthernet  2/0          dhcp
(external)
Select Management Interface [1]: 2
Enable Autosense for Management Interface? (y/n) [y]: y
Enable DHCP for Management Interface? (y/n) [y]: n

```



Tech Tip

You may receive the following warning. This warning may be disregarded as the IP address configuration was provided previously.

```

*** You have chosen to disable DHCP! Any network
configuration learnt from DHCPserver will be
unlearnt! SETUP will indicate failure as the
managementinterface cannot be brought up - Please
make sure WAE Management Interface IPaddress and
Default Gateway are configured from the Router;
Press ENTER to continue:

```

Step 8: Configure Central Manager address.

Enter Central Manager IP Address (WARNING: An invalid entry will cause SETUP to take a long time when applying WAAS configuration) [None]: **10.4.48.100**

Step 9: Configure DNS, host, and NTP settings.

Enter Domain Name Server IP Address [Not configured]: **10.4.48.10**

Enter Domain Name(s) (Not configured): **cisco.local**

Enter Host Name (None): **Br203-WAE-SRE700-1**

Enter NTP Server IP Address [None]: **10.4.48.17**

Step 10: Configure WCCP router list.

Enter WCCP Router (max 4) IP Address list (ip1 ip2 ...) []: **10.5.48.253 10.5.48.254**

Step 11: Select appropriate license.

The product supports the following licenses:

1. Transport
2. Enterprise
3. Enterprise & Video

Enter the license(s) you purchased [2]: **2**

Step 12: Verify configuration settings.

Parameter	Configured Value
1. Interception Method	WCCP
2. Time Zone	PST -8 0
3. Management Interface	GigabitEthernet 2/0 (external)
4. Autosense	Enabled
5. DHCP	Disabled
IP Address	10.5.52.8
IP Network Mask	255.255.255.0
IP Default Gateway	10.5.52.1
6. CM IP Address	10.4.48.100
7. DNS IP Address	10.4.48.10
8. Domain Name(s)	cisco.local
9. Host Name	Br203-WAE-SRE700-1
10. NTP Server Address	10.4.48.17
11. WCCP Router List	10.5.48.253 10.5.48.254
12. License	Enterprise
ESC Quit ? Help ! CLI ————— WAAS Final Configuration	

Press 'y' to select configuration, <F2> to see all configuration, 'd' to toggle defaults display, <1-12> to change specific parameter [y]: **y**

Router WCCP configuration

First WCCP router IP in the WCCP router list seems to be an external address; WCCP configuration on external routers is not allowed through SETUP. Please press ENTER to apply WAAS configuration on WAE ...

Applying WAAS configuration on WAE ...

May take a few seconds to complete ...

WAAS configuration applied successfully!!

Saved configuration to memory.

Press ENTER to continue ...

You will be prompted with a recommended router WCCP configuration template. This router configuration is covered in depth in a following procedure, so you do not need to retain this information.

Step 13: Configure GRE negotiated return.

All WAE devices use GRE-negotiated return with their respective WCCP routers:

```
egress-method negotiated-return intercept-method wccp
```

Step 14: Configure WCCP router list.

The setup script generated a router-list based on the information provided. To view the device configuration, enter the following command:

```
Br203-WAE-SRE700-1# show running-config | include wccp router-list
wccp router-list 8 10.5.48.253 10.5.48.254
```

Router list 8 is specifically for use with WCCP configured on a default gateway router. This design uses GRE-negotiated return and router loopback addresses so we need to create a new router list and delete router list 8.

All WAE configurations in this design use router list 1.

```
no wccp router-list 8 10.5.48.253 10.5.48.254
wccp router-list 1 10.5.48.253 10.5.48.254
```

This design uses authentication between the routers and the WAEs.

```
wccp tcp-promiscuous service-pair 61 62 router-list-num 1
password cisco123
```

Step 15: Enable SSH.

Enabling SSH requires the generation of the RSA key and enabling of the sshd service.

```
ssh-key-generate key-length 2048
sshd version 2
sshd enable
```

Step 16: Disable telnet.

```
no telnet enable
```

Step 17: Configure secure user authentication.

Enable AAA authentication for access control. AAA controls all management access to the WAAS/WAE devices (SSH and HTTPS).

A local admin user was created on the WAAS/WAE during setup. This user account provides the ability to manage the device in case the centralized TACACS+ server is unavailable or in case you do not have a TACACS+ server in your organization.

The following configures TACACS+ as the primary method for user authentication (login) and user authorization (configuration).

```
tacacs key SecretKey
tacacs password ascii
tacacs host 10.4.48.15 primary
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
```

Step 18: Save the configuration.

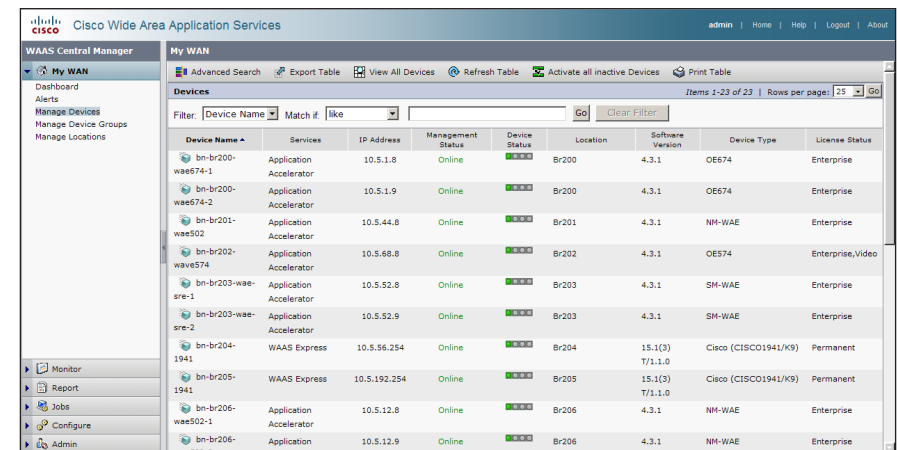
After you make configuration changes, save the configuration.

```
copy running-config startup-config
```

Each WAE registers with the WAAS Central Manager as they become active on the network. You can verify this registration using the **show cms info** command on the respective WAE or via the web interface to the WCM.

When this configuration is complete, you can return the session to the command line of the host router by entering the escape sequence Ctrl-Shift-6 x.

Figure 35 - WAAS Central Manager-Populated managed device list



The screenshot displays the Cisco Wide Area Application Services (WAAS) Central Manager web interface. The main section shows a table of managed devices. The table has columns for Device Name, Services, IP Address, Management Status, Device Status, Location, Software Version, Device Type, and License Status. The devices listed include various accelerators and WAAS Express devices, all showing 'Online' status and 'Enterprise' license status.

Device Name	Services	IP Address	Management Status	Device Status	Location	Software Version	Device Type	License Status
bn-br200-wae674-1	Application Accelerator	10.5.1.8	Online	Online	Br200	4.3.1	OE674	Enterprise
bn-br200-wae674-2	Application Accelerator	10.5.1.9	Online	Online	Br200	4.3.1	OE674	Enterprise
bn-br201-wae502	Application Accelerator	10.5.44.8	Online	Online	Br201	4.3.1	NM-WAE	Enterprise
bn-br202-wae674	Application Accelerator	10.5.68.8	Online	Online	Br202	4.3.1	OE674	Enterprise, Video
bn-br203-wae-sre-1	Application Accelerator	10.5.52.8	Online	Online	Br203	4.3.1	SM-WAE	Enterprise
bn-br203-wae-sre-2	Application Accelerator	10.5.52.9	Online	Online	Br203	4.3.1	SM-WAE	Enterprise
bn-br204-1941	WAAS Express	10.5.56.254	Online	Online	Br204	15.1(3) 7/1.1.0	Cisco (CISCO1941/K9)	Permanent
bn-br205-1941	WAAS Express	10.5.192.254	Online	Online	Br205	15.1(3) 7/1.1.0	Cisco (CISCO1941/K9)	Permanent
bn-br206-wae502-1	Application Accelerator	10.5.12.8	Online	Online	Br206	4.3.1	NM-WAE	Enterprise
bn-br206-wae502-2	Application Accelerator	10.5.12.9	Online	Online	Br206	4.3.1	NM-WAE	Enterprise

Procedure 6 Configure Remote Switch for WAE Devices

If you are using a remote-site distribution-layer design, the distribution switch is the appropriate location to physically connect the WAE devices. This device type requires a resilient connection, but does not require a routing protocol. This type of connection can use a Layer 2 EtherChannel link.

This guide assumes that the distribution layer switch has already been configured. Only the procedures required to complete the connection of the switch to the WAE appliances are included. Full details on distribution layer switch configuration are included in the *Cisco SBA for Enterprise Organizations—Borderless Networks LAN Deployment Guide*.

This design locates the WAE devices on the data (primary) VLAN. It is required to create a VLAN and SVI for this VLAN if it does not already exist.

Step 1: Create the VLAN and SVI (if necessary).

```
vlan [VLAN number]
  name [VLAN name]
!
interface Vlan [VLAN number]
  ip address [IP address] [netmask]
  no shutdown
```

Step 2: Configure Layer 2 EtherChannel links for the devices and associate them with the VLAN.

```
interface Port-channel [number]
  switchport access vlan [VLAN number]
!
interface [type] [number]
  switchport access vlan [VLAN number]
  channel-group [number] mode on
  no shutdown
!
interface [type] [number]
  switchport access vlan [VLAN number]
  channel-group [number] mode on
  no shutdown
```

Example

```
vlan 100
  name Data
!
interface Port-channel7
  description bn-wae-1 EtherChannel
  switchport access vlan 100
!
interface GigabitEthernet1/0/3
  description bn-wae-1 port 1
  switchport access vlan 100
  channel-group 7 mode on
  no shutdown
!
interface GigabitEthernet2/0/3
  description bn-wae-1 port 2
  switchport access vlan 100
  channel-group 7 mode on
  no shutdown
!
interface Vlan100
  ip address 10.5.1.1 255.255.255.0
  no shutdown
```

Procedure 7 Configure WCCPv2 on Routers

In this design, WCCP diverts network traffic destined for the WAN to the WAAS system for optimization. This method provides for a clean deployment with minimal additional cabling, and requires both the WAN-aggregation and remote-site routers to be configured for WCCP.

Step 1: Configure global WCCP parameters and enable services 61 and 62.

You must enable services 61 and 62 for WCCP redirect for WAAS. These services should be using WCCP Version 2. As a best practice, exempt certain critical traffic types from WCCP redirect by using a redirect list.

To prevent unauthorized WAE devices from joining the WAAS cluster, you should configure a group-list and password.

```
ip wccp version 2
ip wccp 61 redirect-list [redirect ACL] group-list [group ACL]
password [password]
ip wccp 62 redirect-list [redirect ACL] group-list [group ACL]
password [password]
!
ip access-list standard [group ACL]
 permit [WAAS cluster member IP]
 permit [WAAS cluster member IP]
!
ip access-list extended [redirect ACL]
 deny tcp [src IP address] [dest IP address] any eq [TCP
port]
 deny tcp [src IP address] [dest IP address] any eq [TCP
port]
! Additional lines as necessary
 deny tcp [src IP address] [dest IP address] any eq [TCP
port]
 permit tcp any any
```

Step 2: Configure WCCP redirection on the LAN and WAN interfaces.

Option 1. All WAAS routers except for DMVPN hub routers

Specific interfaces must be identified where traffic to and from the WAN are intercepted.

Traffic from the LAN is intercepted with service 61 inbound on all LAN interfaces. It is not necessary to configure WCCP interception on voice interfaces and voice VLANs.

```
interface [interface type] [number]
 ip wccp 61 redirect in
```

Traffic from the WAN is intercepted with service 62 inbound on all WAN interfaces, including DMVPN tunnel interfaces (but not their underlying physical interfaces).

```
interface [interface type] [number]
 ip wccp 62 redirect in
```

Example—Option 1

```
ip wccp version 2
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list BN-WAE
password cisco123
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list BN-WAE
password cisco123
!
interface Port-channel1
 ip wccp 61 redirect in
!
interface GigabitEthernet0/0/3
 ip wccp 62 redirect in
!
ip access-list standard BN-WAE
 permit 10.4.32.161
 permit 10.4.32.162
ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect List
 deny tcp any any eq 22
 deny tcp any eq 22 any
 deny tcp any eq telnet any
 deny tcp any any eq telnet
 deny tcp any eq bgp any
 deny tcp any any eq bgp
 deny tcp any any eq 123
 deny tcp any eq 123 any
 permit tcp any any
```

Option 2. DMVPN hub routers

Specific interfaces must be identified where traffic to and from the WAN are intercepted.

Traffic from the LAN is intercepted with service 61 inbound on the LAN interfaces.

```
interface [interface type] [number]
 ip wccp 61 redirect in
```

DMVPN hub routers require WCCP 62 outbound on the LAN interface to support dynamic creation of spoke to spoke tunnels.

Traffic from the WAN is intercepted with service 62 outbound on the LAN interfaces.

```
interface [interface type] [number]
 ip wccp 62 redirect out
```

Example—Option 2

```
ip wccp version 2
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list BN-WAE
password cisco123
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list BN-WAE
password cisco123
!
interface Port-channel3
 ip wccp 61 redirect in
 ip wccp 62 redirect out
!
ip access-list standard BN-WAE
 permit 10.4.32.161
 permit 10.4.32.162
ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect List
 deny tcp any any eq 22
 deny tcp any eq 22 any
 deny tcp any eq telnet any
 deny tcp any any eq telnet
 deny tcp any eq bgp any
 deny tcp any any eq bgp
 deny tcp any any eq 123
 deny tcp any eq 123 any
 permit tcp any any
```

Procedure 8

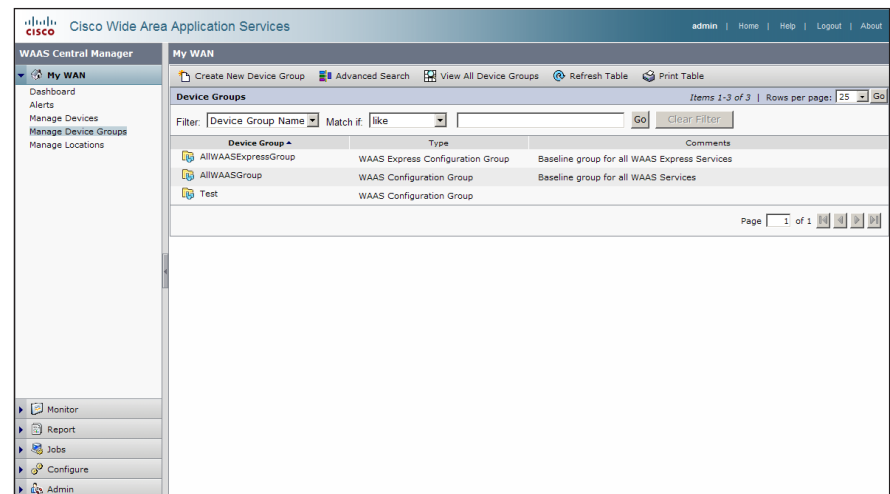
Configure the Central Manager for WAASx

You can use the WAAS Central Manager to centrally manage WAASx routers, similar to a WAE appliance. You must define a user name and password that the WCM will use to access the WAASx routers for monitoring and management. These communications are secured using HTTPS, which requires the use of digital certificates.

Step 1: Set up credentials for WAASx routers.

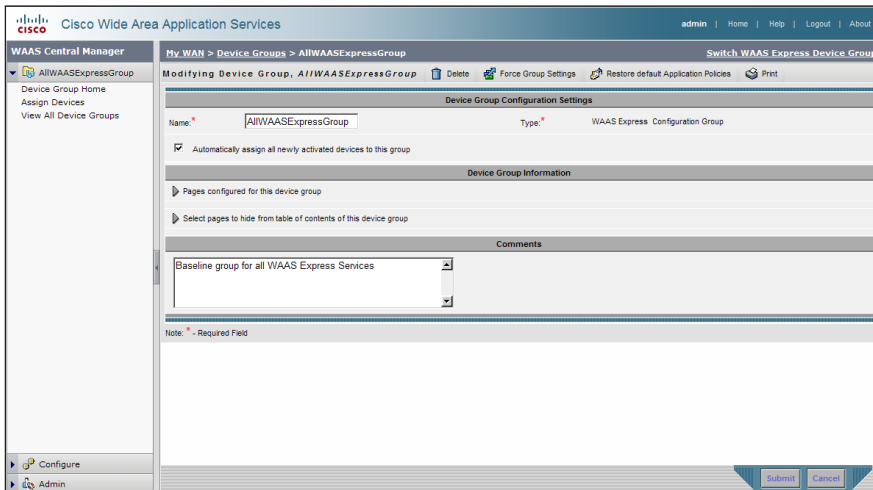
In the WAAS Central Manager web interface (<https://10.4.48.100:8443>), configure login and password credentials for the WAASx router. You can do this by editing the device group **AllWAASExpressGroup**. From the main WAAS Central Manager page, click **My Wan -> Manage Device Groups** on the left.

Figure 36 - WAAS Central Manager-Manage device groups



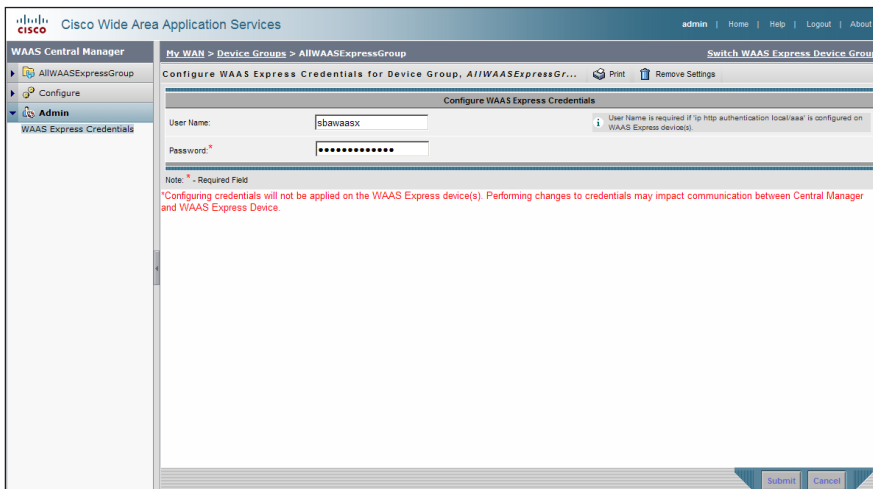
To select the device group, click **AllWAASExpressGroup**, and then click the **Admin** tab (associated with the **AllWAASExpressGroup** device group).

Figure 37 - WAAS Central Manager-AllWAASExpressGroup



Click **WAAS Express Credentials**.

Figure 38 - WAAS Central Manager-WAASx credentials



Enter the appropriate user name and password that you also plan to configure on the WAASx router or on the central AAA server. The example shows user name **sbawaasx** and password **c1sco123**.

Step 2: Export trusted digital certificate from WCM.

To enable secure communications between the WCM and the router requires that you install the digital certificate from the WCM on each of the WAASx routers. The certificate can be exported in Privacy Enhanced Mail (PEM) Base64 format. This command is available through the device command line interface.

```
WAAS-WCM-1#show crypto certificate-detail admin | begin BEGIN
...skipping
-----BEGIN CERTIFICATE-----
<certificate data deleted>
-----END CERTIFICATE-----
```

Because this information will be required for all WAASx routers, copy and paste this certificate, and then save it to a secure file.

Procedure 9

Configure WAAS Express Routers

To turn on the embedded WAN optimization, you must enable WAAS optimization on the router's WAN interface. WAASx can also be centrally managed by the same WAAS Central Manager used with WAE devices. The router must also be properly configured to communicate securely with the WCM.

Note that WAASx is a specially licensed feature. This license must be installed on a router with sufficient DRAM to support the WAASx functionality.

WAASx routers must be configured with maximum DRAM

WCCP redirection is not used for a WAASx implementation. There is no need to redirect traffic to an external device, because all traffic optimization is performed on the router.

Step 1: Enable WAAS on the WAN interface.

WAASx was designed to be enabled with just a single command.

On a remote-site router with WAN interface GigabitEthernet0/0.

```
interface GigabitEthernet0/0
  waas enable
```

Step 2: Configure self-signed trustpoint and generate digital certificate.

On the WAASx router, configure a persistent self-signed trust point and enroll. This step is necessary even if you already have a self-signed trustpoint that is auto-generated from HTTPS that was enabled previously. Be sure to match the host name and domain-name that are already configured on the router for the subject-alt-name field.

```
crypto pki trustpoint SELF-SIGNED-TRUSTPOINT
  enrollment selfsigned
  subject-alt-name Br204-1941.cisco.local
  revocation-check none
  rsakeypair SELF-SIGNED-RSAKEYPAIR 2048
  exit
```

```
crypto pki enroll SELF-SIGNED-TRUSTPOINT
```

The router has already generated a Self Signed Certificate for trustpoint TP-self-signed-xxxxxx.

If you continue the existing trustpoint and Self Signed Certificate will be deleted.

Do you want to continue generating a new Self Signed Certificate? [yes/no]: **yes**

% Include the router serial number in the subject name? [yes/no]: **no**

% Include an IP address in the subject name? [no]: **no**

Generate Self Signed Router Certificate? [yes/no]: **yes**

Router Self Signed Certificate successfully created

Step 3: Configure HTTPS client and server.

Configure the WAASx router to use a loopback interface as the source for any HTTP client communication.

```
ip http client source-interface Loopback0
```

Enable the HTTPS secure server.

```
ip http secure-server
```

```
ip http secure-trustpoint SELF-SIGNED-TRUSTPOINT
```

Step 4: Create a trustpoint and import the WAAS Central Manager certificate.

```
crypto pki trustpoint WAAS-WCM
  revocation-check none
  enrollment terminal pem
  exit
```

```
crypto pki authenticate WAAS-WCM
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

Now, paste the PEM certificate from the WAAS Central Manager that was generated in the previous procedure.

```
-----BEGIN CERTIFICATE-----
```

```
<certificate data deleted>
```

```
-----END CERTIFICATE-----
```

Certificate has the following attributes:

Fingerprint MD5: 2EA6FF8F 38ABC32F 25168396 1A587F17

Fingerprint SHA1: 8DAB6185 7B95FC4C 34FDACDC A8F2B1A4 8074709B

% Do you accept this certificate? [yes/no]: **yes**

Trustpoint CA certificate accepted.

% Certificate successfully imported

Step 5: Register the WAASx router with the WAAS Central Manager.

After you have properly generated and installed the digital certificates, you can register the router with the WCM.

```
waas cm-register https://10.4.48.100:8443/wcm/register
```

The router appears as a Managed Device on the WCM.

Appendix A:

Enterprise Organizations WAN Deployment Product List

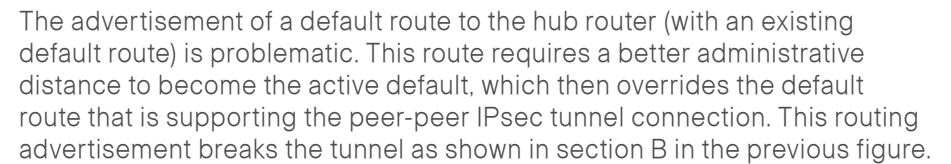
Functional Area	Product	Part Numbers	Software Version
WAN 500 Design			
WAN Aggregation	ASR1002	ASR1002-5G-VPN/K9 ASR1002-PWR-AC	IOS-XE 15.1(3)S0a
WAN Aggregation: WAAS Central Manager	WAVE-594 WAAS Appliance	WAVE-594-K9 WAAS-ENT-APL	4.4.1 (WAAS-UNIVERSAL-K9)
WAN Aggregation: WAAS Application Accelerator	WAE-7571-K9 WAAS Appliance	WAE-7571-K9 WAAS-ENT-APL	4.4.1 (WAAS-UNIVERSAL-K9)
WAN 100 Design			
WAN Aggregation:	ASR1001	ASR1001-2.5G-VPNK9 ASR1001-PWR-AC	IOS-XE 15.1(3)S0a
WAN Aggregation: WAAS Central Manager	WAVE-594 WAAS Appliance	WAVE-594-K9 WAAS-ENT-APL	4.4.1 (WAAS-UNIVERSAL-K9)
WAN Aggregation: WAAS Application Accelerator	WAE-7541-K9 WAAS Appliance	WAE-7541-K9 WAAS-ENT-APL	4.4.1 (WAAS-UNIVERSAL-K9)
WAN Remote Site Routers			
WAN Remote Site Router	Cisco1941	C1941-WAASX-SEC/K9 SL-19-DATA-K9	15.1(4)M2
WAN Remote Site Router	Cisco2911	C2911-VSEC/K9 SL-29-DATA-K9	15.1(4)M2
WAN Remote Site Router	Cisco2921	C2921-VSEC/K9 SL-29-DATA-K9	15.1(4)M2
WAN Remote Site Router	Cisco3925	C3925-VSEC/K9 SL-39-DATA-K9	15.1(4)M2
WAN Remote Site Router	Cisco3945	C3945-VSEC/K9 SL-39-DATA-K9	15.1(4)M2

Functional Area	Product	Part Numbers	Software Version
WAN Remote Site WAAS			
Application Accelerator	SM-SRE-700-K9	SM-SRE-700-K9 WAAS-ENT-SM	4.4.1 (WAAS-UNIVERSAL-K9)
Application Accelerator	SM-SRE-900-K9	SM-SRE-900-K9 WAAS-ENT-SM	4.4.1 (WAAS-UNIVERSAL-K9)
Application Accelerator	WAVE-294	WAVE-294-K9 WAAS-ENT-APL	4.4.1 (WAAS-UNIVERSAL-K9)
Application Accelerator	WAVE-594	WAVE-594-K9 WAAS-ENT-APL	4.4.1 (WAAS-UNIVERSAL-K9)
Application Accelerator	WAVE-694	WAVE-694-K9 WAAS-ENT-APL	4.4.1 (WAAS-UNIVERSAL-K9)

Building an IPsec tunnel requires reachability between the crypto routers. When you use the Internet, routers use a default route to contact their peers.

The diagram illustrates a DMVPN Hub-and-Spoke topology. A WAN Distribution router (represented by a star icon) connects to a DMVPN Hub Router (represented by a circular icon with four arrows) via a 'default' route. The Hub Router connects to multiple DMVPN Spoke Routers (represented by circular icons with four arrows) via a 'VPN-DMZ' interface. The Hub Router also connects to an Internet Edge router (represented by a square icon with a magnifying glass) via an 'INSIDE' interface. The Internet Edge router connects to the Internet (represented by a cloud icon) via an 'OUTSIDE' interface. A 'default' route is shown from the Internet Edge router to the Internet. A 'default' route is also shown from the Internet to the Spoke Routers.

Figure 40 - IPsec tunnel before/after default route injection

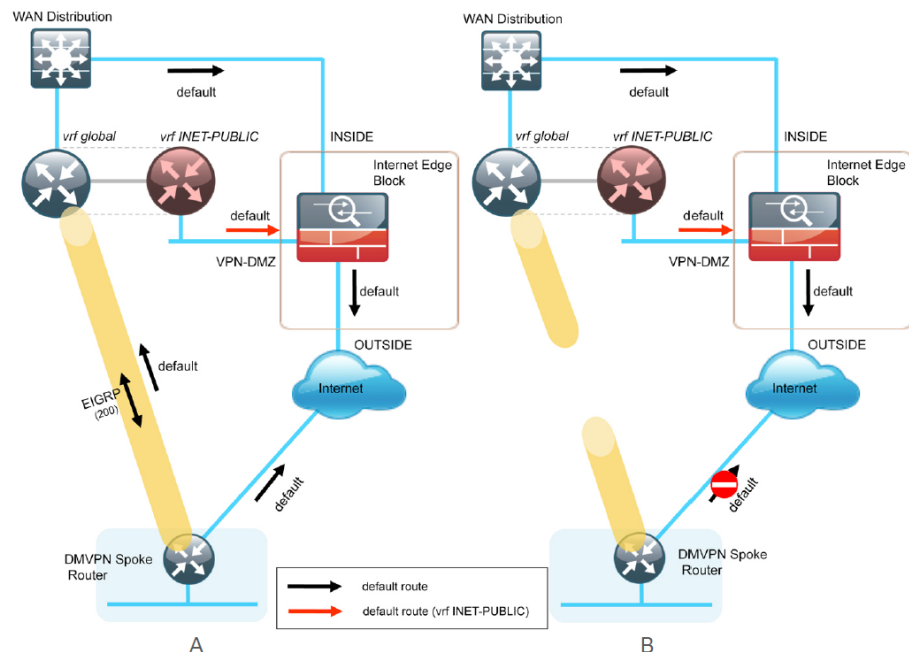




Tech Tip

Most additional features on the hub router do not require VRF-awareness.

Figure 41 - IPsec tunnel with FVRF aggregation



This configuration is referred to as FVRF), because the Internet is contained in a VRF. The alternative to this design is inside VRF (IVRF), where the internal network is in a VRF on the VPN hub and the Internet remains in the global VRF. This method is not documented in this guide.

It is now possible to reestablish the IPsec tunnel to the remote peer router. As the remote-site policy requires central Internet access for end users, a default route is advertised through the tunnel. This advertisement causes a similar default routing issue on the remote router; the tunnel default overrides the Internet-pointing default and the tunnel connection breaks as shown in section B in the previous figure.

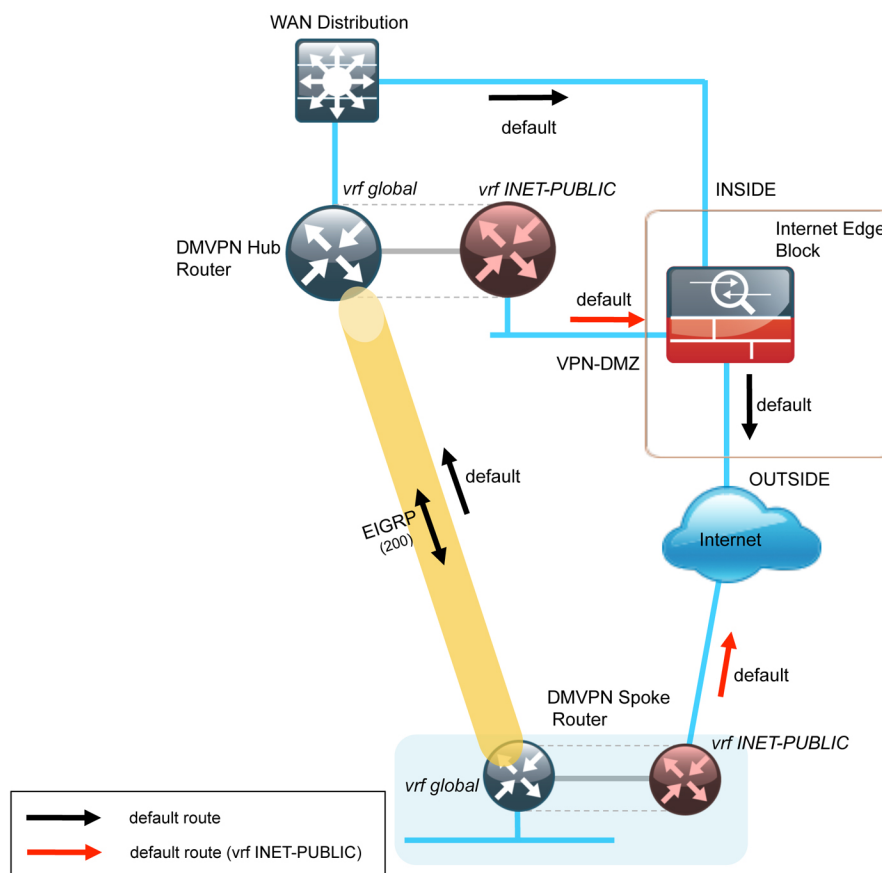
This configuration requires using F-VRF on the remote-site router as well.

The primary benefits of using this solution are as follows:

- Simplified default routing and static default routes in the INET-PUBLIC VRFs
- Ability to support default routing for end-users traffic through VPN tunnels
- Ability to use dynamic default routing for sites with multiple WAN transports
- Ability to build spoke-to-spoke tunnels with DMVPN with end-user traffic routed by default through VPN tunnels

The final design that uses FVRF at both the WAN-aggregation site and a WAN remote-site is shown in the following figure.

Figure 42 - FVRF—Final configuration



Appendix C: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- For IP multicast, we enabled Cisco Auto RP, to simplify deployment.
- For remote site router loopback interfaces, we suggest using an IP address range not in the summary range of any other part of the network.
- For AAA, we updated the commands to a new syntax.
- For the WAN aggregation platform options, we removed the Cisco 3945E Integrated Services Router.
- For the application acceleration platform options, we removed the previous generation appliances.

Notes



SMART BUSINESS ARCHITECTURE



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 of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)