Newer Cisco SBA for Government Guides Available

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

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.

WAN Deployment Guide

SBA FOR GOVERNMENT

Revision: H2CY10

The Purpose of this Document

This guide is a reference on deploying a WAN to connect a primary site to up to 500 remote sites using MPLS and Internet.

It includes an overview of the operational problems that can be solved by MPLS and Internet VPN and also a discussion of the agency relevance of application optimization technology. The guide includes details of various topology designs with increasing levels of scale and resiliency. It also provides step-by-step configuration instructions for the routers, switches and WAN optimization devices that make up the WAN and remote site solution.

Who Should Read This Guide

- Has in total 2000–10,000 connected employees
- Has up to 500 remote sites
- Uses MPLS Layer 3 VPN as a WAN transport
- Uses the Internet as a secure WAN transport
- Requires a resilient WAN
- Requires an application optimization solution to improve WAN performance
- Has IT workers with a CCNA® certification or equivalent experience
- Wants to deploy their network infrastructure efficiently
- Wants the assurance of a tested solution
- Requires a migration path for growth

Related Documents

Related Reading

Design Overview

LAN Deployment Guide

Internet Edge Deployment Guide

Optional

Midsize BN Foundation Design Overview

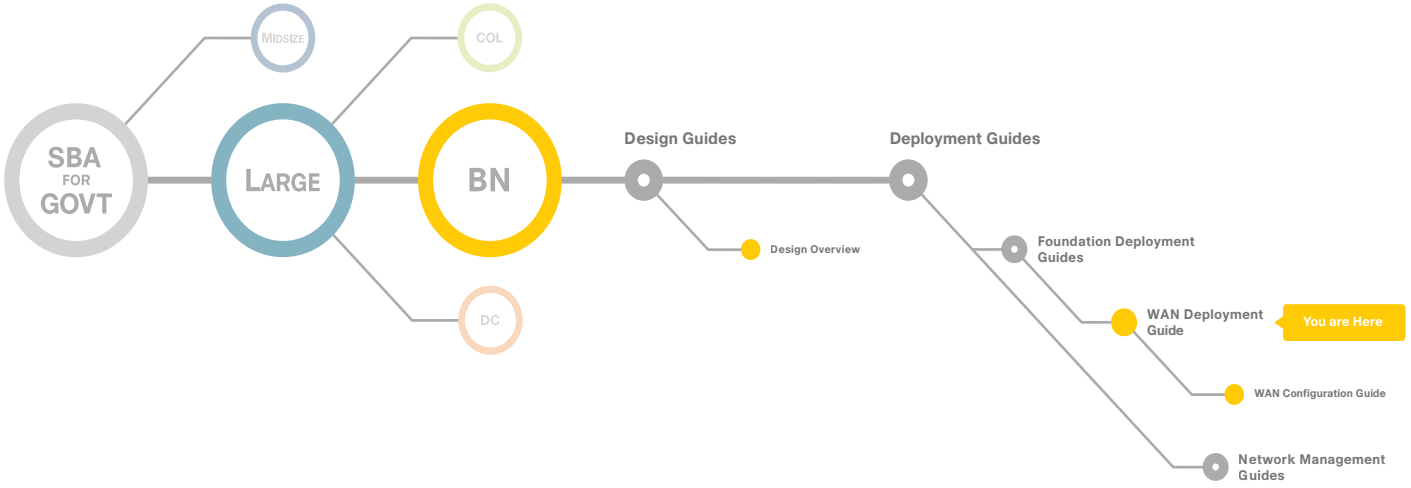


Table of Contents

Introduction

The Cisco Smart Business Architecture (SBA) for Government Large Agencies—Borderless Networks is designed for networks that have 2000 to 10,000 connected users. 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 deployment guides are designed to make the Borderless Network for Large Agencies easy—easy to configure, easy to deploy, and easy to manage.

The goal of any network implementation is to support the applications that benefit the users and the agency that it is built for. As they guide you through the depth and breadth of the architecture, the SBA deployment guides are intended to simplify navigating among and learning the various networking technologies that we used to build the architecture. Cisco SBA is a solid network foundation that provides the flexibility to support new user or network services without re-engineering the network.

Using the Deployment Guides

The Large Agency architecture was designed, built, and validated as an end-to-end system.

To focus on specific elements of the architecture, there are three primary deployment guides, one each for Local Area Network (LAN), Wide Area Network (WAN), and Internet Edge. To enhance the Large Agency architecture, there are a number of supplemental guides that address specific functions, technologies, or features that may be important to solving your operational problems. Within each of these deployment guides, you will find a modular approach that allows you to start at the beginning and work your way through or to jump to a specific module. Each deployment guide and the modules within are designed to stand alone, so that you can deploy the specific Cisco technology in a module without completing each previous module. Each deployment guide includes a complete list of the products and the software revisions tested, and a companion supplemental guide contains all configuration files used.

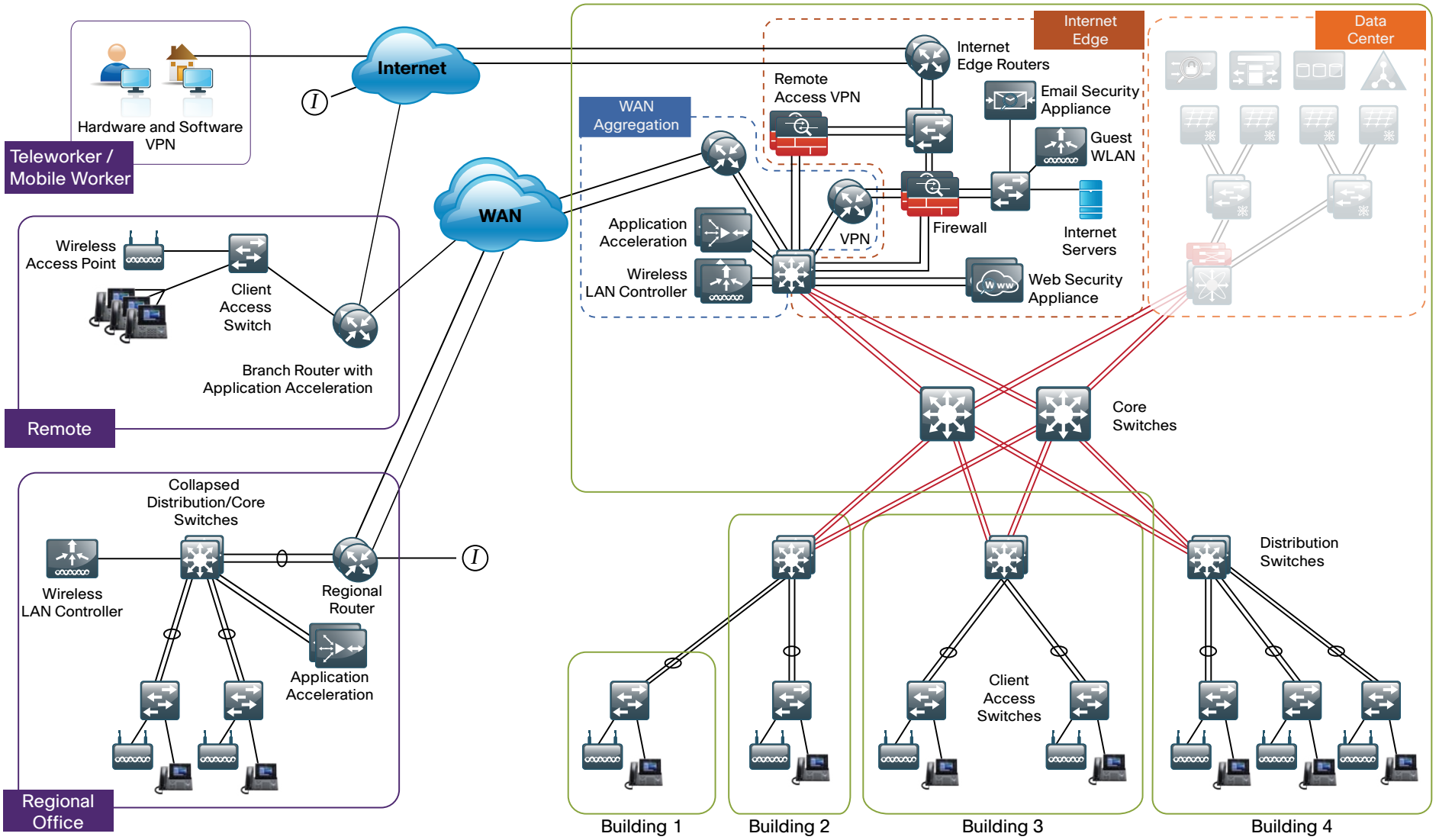
The deployment guides begin with an agency overview of the common operational problems addressed, followed by an architecture overview to assist you with matching the value of a technology solution to your operational problems.

The *Local Area Network Deployment Guide* covers 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 is 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 *Wide Area Network Deployment Guide* includes the primary site aggregation design as well as multiple remote-site designs to accommodate varying scale and service-level requirements in a common approach. The flexibility in the WAN deployment guide provides guidance and configuration for Multiprotocol Label Switching (MPLS) transport as well as broadband or Internet transport in a primary or backup role. QoS is integrated to ensure that the base architecture can support a multitude of applications on a single transport. The design integrates application optimization and the deployment guide provides details on optimizing WAN traffic to ensure economical use of bandwidth while providing
a good user experience.

The *Internet Edge Deployment Guide* focuses on security services such as firewalls and intrusion prevention systems to protect your agency's gateway to the Internet. Internet service provider connectivity and routing options, combined with server load balancing, provide resiliency to the design. The Email Security module covers protecting email from spam and malware. The Web Security module provides acceptable-use control and monitoring as well as managing the increasing risk associated with clients browsing the Internet. The Virtual Private Network (VPN) design supports the teleworker and mobile user with secure remote access. All of these elements are covered in separate modules and yet are designed to work together to provide a secure Internet Edge solution.

Figure 1. SBA for Large Agencies—Borderless Networks Overview



Design Goals

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

- **Ease of Deployment:** Agencies can deploy the design consistently across all products included in the architecture. The configurations used in the deployment represent a best-practice methodology to enable a fast and resilient deployment.
- **Flexibility and Scalability:** The architecture can grow with the agency without being redesigned.
- **Resiliency and Security:** The architecture keeps the network operating even during unplanned outages and attacks.
- **Easy to Manage:** The deployment guidance includes configuring devices to be managed by a network management system (NMS) or as unique elements of the network.
- **Advanced Technology Ready:** Implementing advanced technologies like collaboration is easy because the network foundation is already configured with the required baseline network services.

Ease of Deployment, Flexibility and Scalability

Agencies of 2000 to 10,000 users are often are spread out among different geographical locations. The locations might have labels like remote site, regional site, or headquarters. This architecture addresses how to build a network for all these locations, irrespective of the label.

In this design, several methods are used to create and maintain a scalable network. Defining a common framework with a convergence of design standards drives global consistency and optimizes the design process, which ultimately results in lower cost and complexity. Standardization is the key to scalability; by keeping a small number of standard designs for common portions of the network, support staff are able to design services for, implement, and support these network areas more effectively.

To enhance scalability, we take a modular design approach; beginning with a set of standard, global building blocks, we can assemble a scalable network to meet requirements. For instance, to build a campus network, we might start with a LAN module, connect an Internet edge module, and then add a WAN module.

Many of these plug-in modules look identical for several different service areas; this provides consistency and scalability in that the same support methods can be used in multiple areas of the network to maintain 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 the appropriate redundancy to guard against failure in the network, whether it is link, port, card, or chassis failure. But systems can be engineered to be too redundant, exhibiting failures of overly complex redundancy features, which results in complete communications failure. The redundancy in our architecture is carefully balanced with the complexity inherent in redundant systems.

Building production network services without any form of redundancy is unacceptable to most agencies. When building in the necessary redundancy, care must also be taken to prevent large dependency chains that result in greater risk of system failure. For example, chains of devices that do not have cross-connections may create a dependency on both chains being completely available.

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.

Security of the network is also a very 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 networkwide resiliency.

Easy to Manage

While this guide focuses on the deployment of the network foundation, the next phase management and operation are considered. The configurations in the deployment guides are designed to allow the devices to be managed both via normal device management connections, such as SSH and HTTPS, but also 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 agency 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.

Beyond the wired network, the wireless network is also 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 also ready to provide soft phones via VPN, as well as traditional hard or desk phones.

Notes

Architecture Overview

The *Cisco SBA for Large Agencies—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 Internet Protocol (IP)-based interconnection 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 leverages 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 MPLS enables large agencies and service providers to build next-generation intelligent networks that deliver a wide variety of advanced, value-added services over a single infrastructure. This economical solution can be integrated 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 large-agency subscribers to outsource routing information to service providers, which can result in significant cost savings and a reduction in operational complexity for agencies.

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

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 leverages the Internet for VPN site-to-site connections as either a backup WAN transport (to MPLS VPN) or as a primary WAN transport.

DMVPN

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 Route Encapsulation tunnels

(mGRE) 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 referred to in the context of the connection to a carrier or service provider, the WAN edge routers 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 Table 1.

Table 1. WAN-Aggregation Designs

Model	WAN Links	Edge Router(s)	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

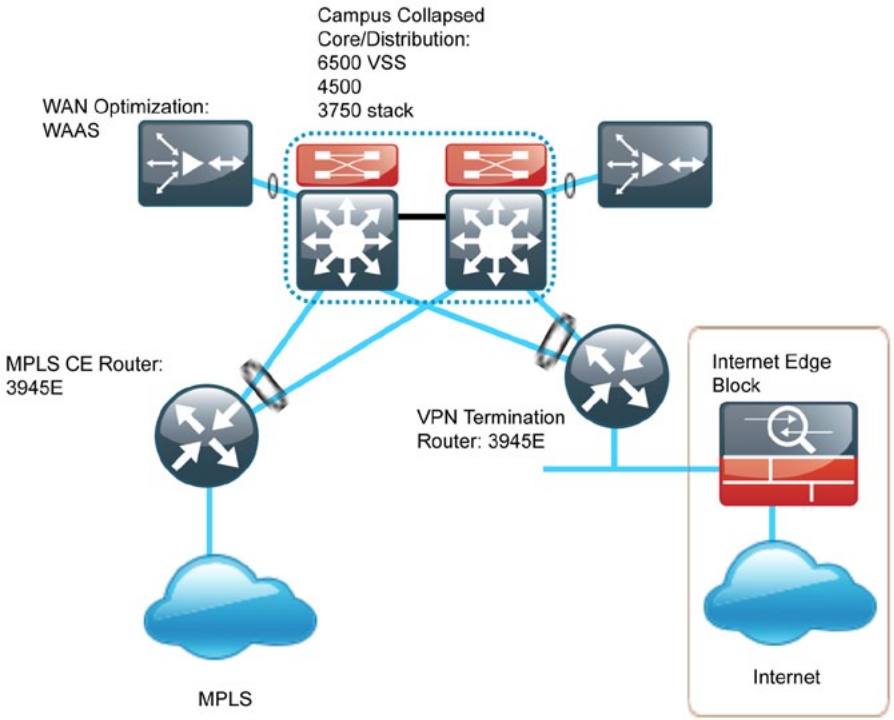
The characteristics of each design are as follows:

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 Figure 2.

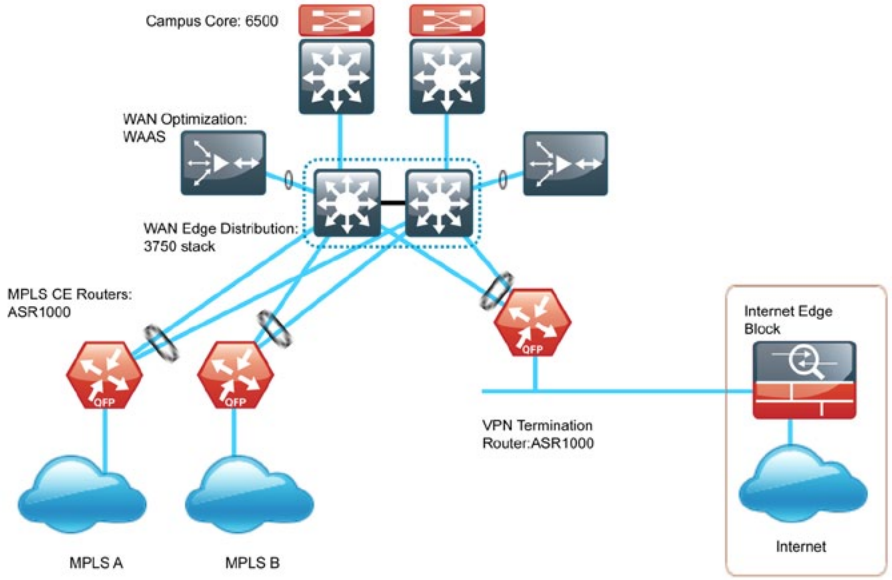
Figure 2. WAN100 Design



- 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 Figure 3.

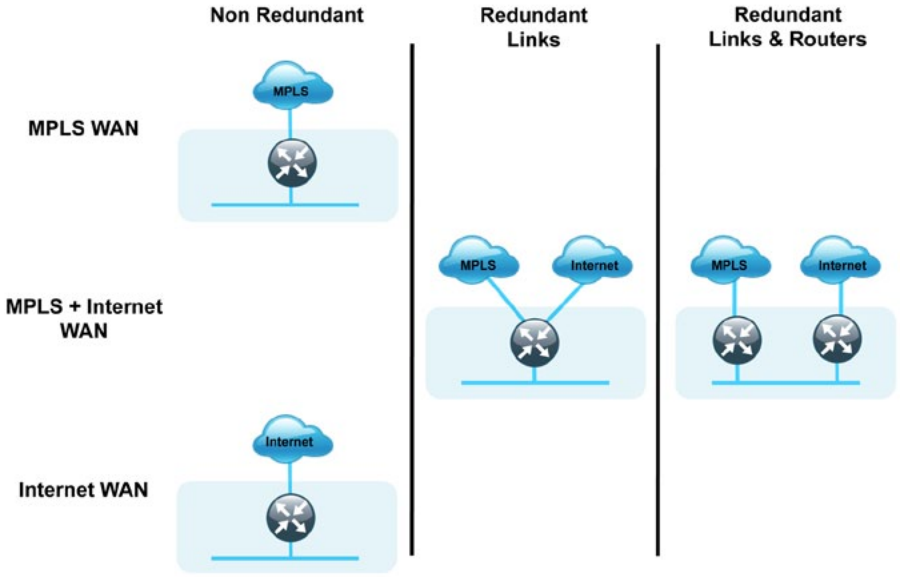
Figure 3. WAN500 Design



WAN Remote-Site Designs

This guide documents multiple remote-site WAN designs, and they are based on various combinations of WAN transports mapped to the site specific requirements for service levels and redundancy. These design variants are shown in Figure 4.

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 mission-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 Table 2.

Table 2. WAN Remote-Site Transport Options

WAN Remote-Site Router(s)	WAN Transports	Primary Transport	Secondary Transport
Single	Single	MPLS VPN A	
		Internet	
Single	Dual	MPLS VPN A	Internet
		MPLS VPN B	Internet
Dual	Dual	MPLS VPN A	Internet
		MPLS VPN B	Internet

Modularity in network design allows you to create design elements that can be replicated 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 Interconnect

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 Large Agencies—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 router(s). The variants that are tested and documented in this guide are shown in Table 3.

Table 3. WAN Remote-Site LAN Options

WAN Remote-Site Router(s)	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 shown in Table 4. 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	L2 Access	L3 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)

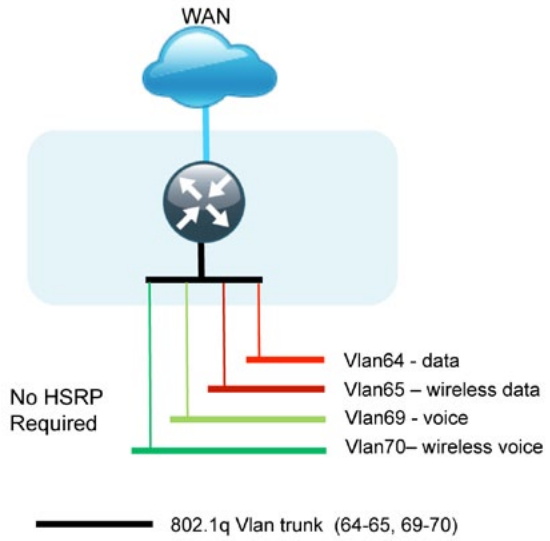
Layer 2 Access

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 router(s). The access switch(es), through the use of multiple VLANs, can support services such as data (wired and wireless) and voice (wired and wireless). The design shown in Figure 5 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 Large Agencies—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.

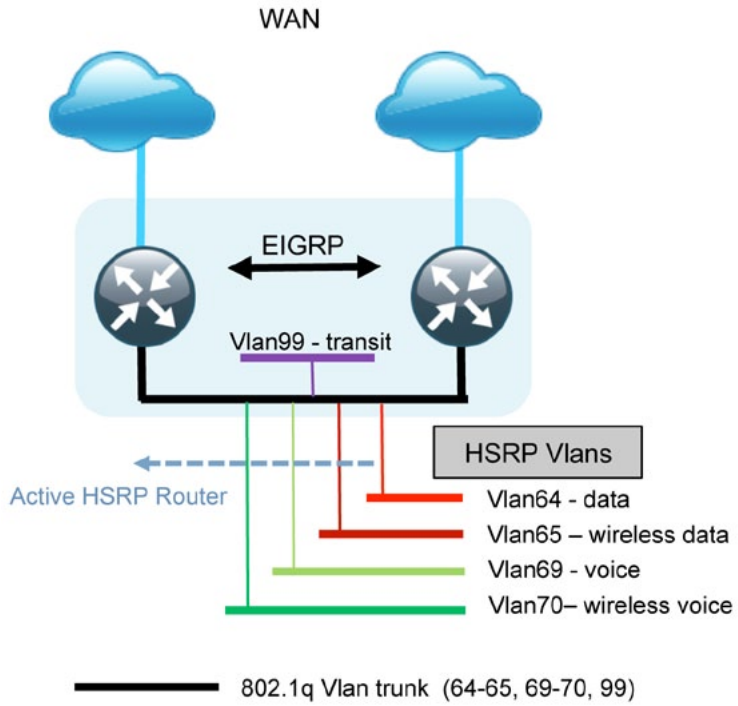
Figure 5. WAN Remote Site—Flat Layer 2 LAN (Single Router)



A similar LAN design can be extended to a dual-router edge as shown in Figure 6. This design change introduces some additional complexity. The first requirement is to run a routing protocol: Enhanced Interior Gateway Protocol (EIGRP) should be configured 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. We selected Hot Standby Router Protocol (HSRP) as the FHRP for this design. 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 sla reachability** as well as several others.

The IP service-level agreement (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 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.

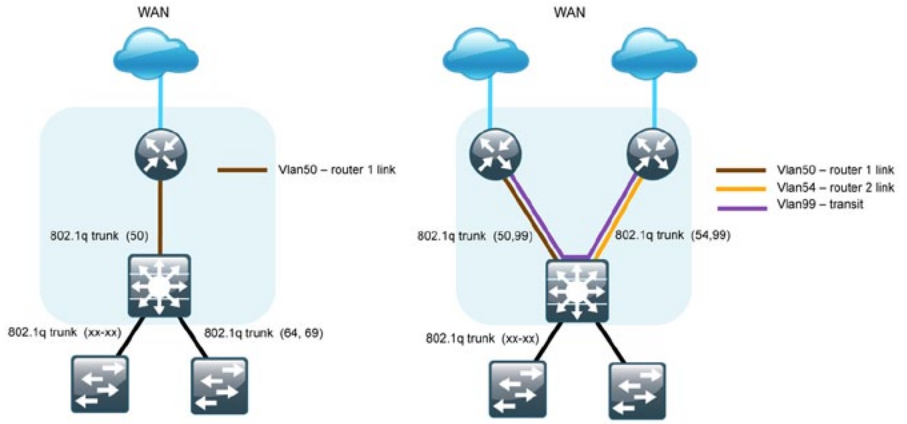
The dual router designs also warrant an additional component that is required for proper routing in certain scenarios. In these cases, a traffic flow from a remote-site host might be sent to a destination reachable via the alternate WAN transport (for example: a MPLS + DMVPN remote site communicating 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 as the 802.1Q VLAN trunk configuration can easily accommodate an additional subinterface.

Distribution and Access Layer

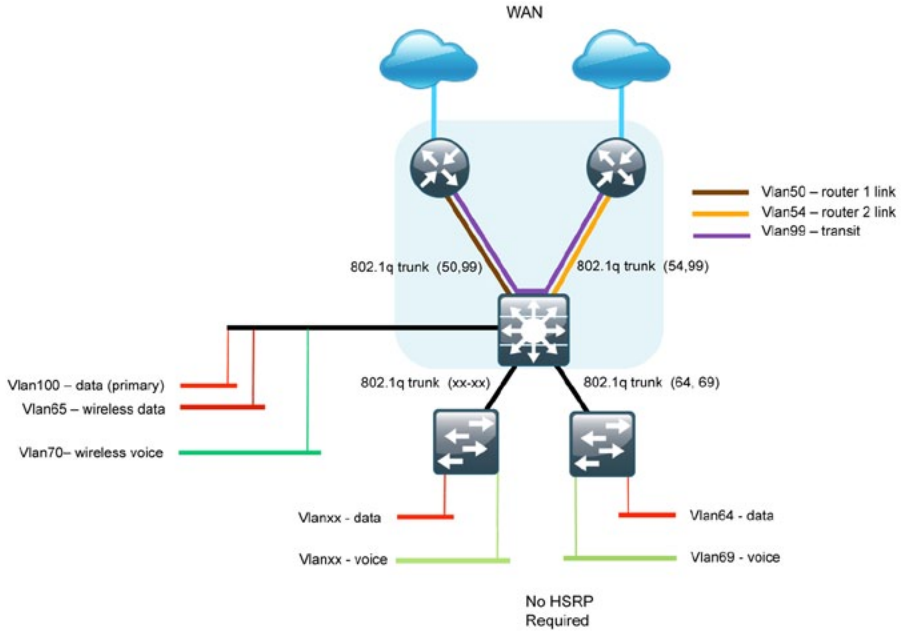
Large remote sites may require a LAN environment similar to that of a small campus LAN that includes a distribution layer and access layer. This topology works well with either a single or dual router WAN edge as shown in Figure 7. To implement this design, the routers should connect via EtherChannel 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 Figure 8.

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 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 Membership 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 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 rendezvous points (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 sparse-mode 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. 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 quality of service (QoS) to help ensure optimal use of network resources. This functionality allows for the differentiation of applications that ensures each has the appropriate share of the network resources to protect the user experience and ensure the operations of mission-critical applications.

Quality of service (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, the use of QoS for management and network protocols protects 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 voice, interactive video, critical data applications, and management traffic to be added to the network, either from the initial deployment or later with minimum system impact and engineering effort.

The QoS classifications in Table 5 are applied throughout this design. This table is included as a reference.

Table 5. QoS Service Class Mappings

	Layer 3			Layer 2
Service Class	**PHB**	**DSCP**	**IPP**	**COS**
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
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.

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 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, then 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 as 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.

Notes

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 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 either a primary or 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 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

DMVPN-connected 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 a spoke-spoke tunnel)
- 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 as bidirectional traffic flows always traverse the same links.

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 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 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 Table 6.

Table 6. Universal Design Parameters

Network Service	IP Address
Domain Name	cisco.local
Active Directory, DNS Server, DHCP Server	10.4.200.10
Authentication Control System (ACS)	10.4.200.15
Network Time Protocol (NTP) Server	10.4.200.17
IP Multicast Rendezvous Point (Anycast RP)	10.4.60.252

Deploying an MPLS WAN

MPLS WAN Agency Overview

Agencies require the WAN to provide sufficient performance and reliability for the remote-site users to be effective in supporting the agency. 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. Many government agencies 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 agency building a WAN.

To reduce the time needed to deploy new technologies that support emerging 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 agencies.

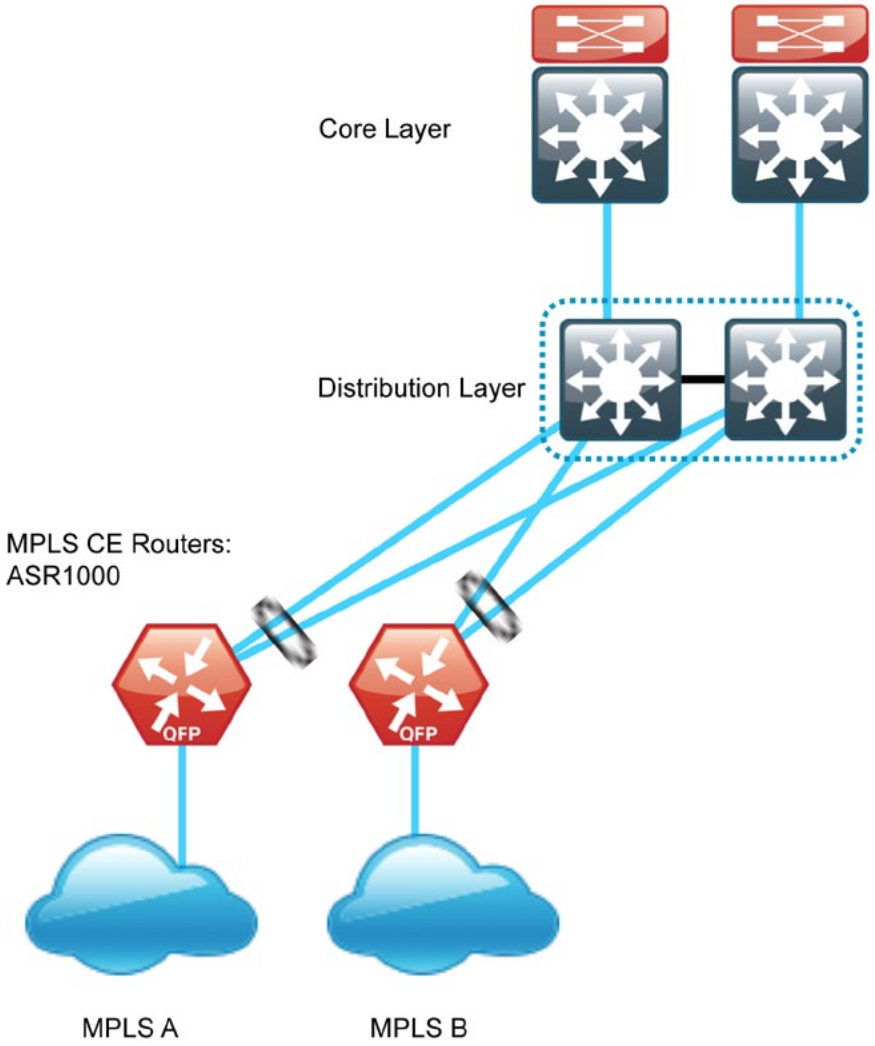
MPLS WAN Technical Overview

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 for the MPLS CE router.

The WAN 500 design uses dual MPLS carriers and dual MPLS CE routers as shown in Figure 9.

Figure 9. WAN 500 Design—MPLS Connections

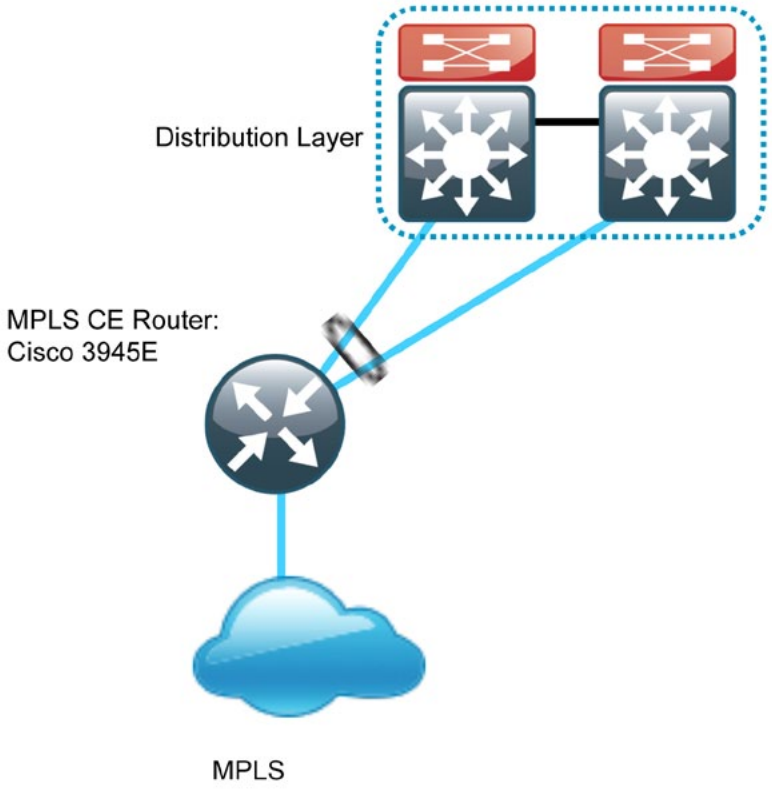


The Cisco ASR 1000 Series Aggregation Services Routers represent the next-generation, modular, services-integrated Cisco routing platform. They are specifically designed for WAN aggregation, with the flexibility to support a wide range of 4- to 16-Mpps packet-forwarding capabilities, 2.5- to 20-Gbps 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 large-agency 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 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 3945E Integrated Services Router for the MPLS CE router. The WAN 100 design uses a single MPLS carrier and a single MPLS CE router as shown in Figure 10.

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. We also need to be concerned with having enough interfaces, enough module slots, and a properly licensed Cisco IOS® image that supports the set of features that is required by the topology. We tested four integrated service router models as MPLS CE routers and the expected performance is shown in Table 7.

Table 7. WAN Remote-Site Integrated Service Router Options

	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	2	2	4
Redundant Power Supply Option	No	No	Yes	Yes

NOTES:
1. 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.
2. 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 shown in Figure 11 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)

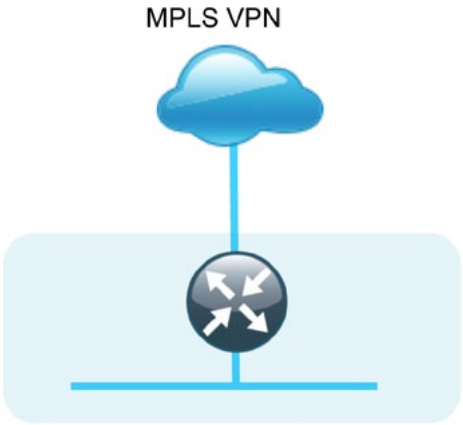
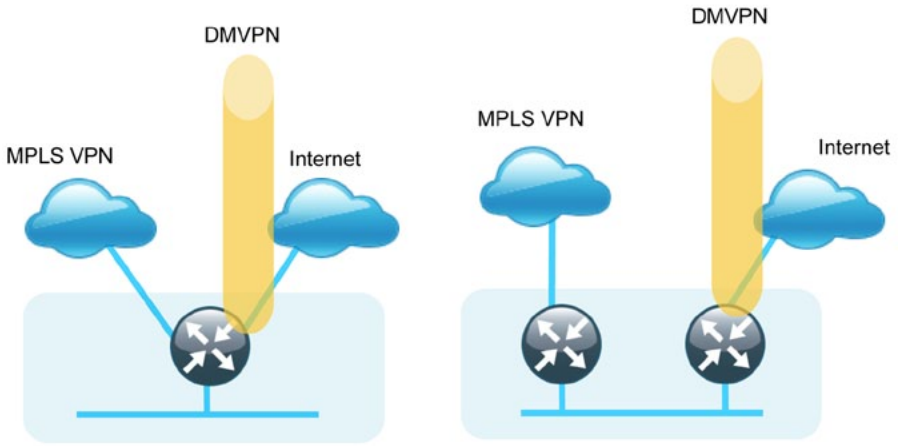


Figure 12. MPLS WAN + DMVPN Remote Site (Dual-Link Options)



The basic single-link design can be augmented through the addition of an alternate WAN transport that uses DMVPN over Internet and either connects on the same router or on an additional router. These alternate designs are shown in Figure 12. Adding an additional link provides 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 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 because the secondary router reroutes traffic via the alternate path.

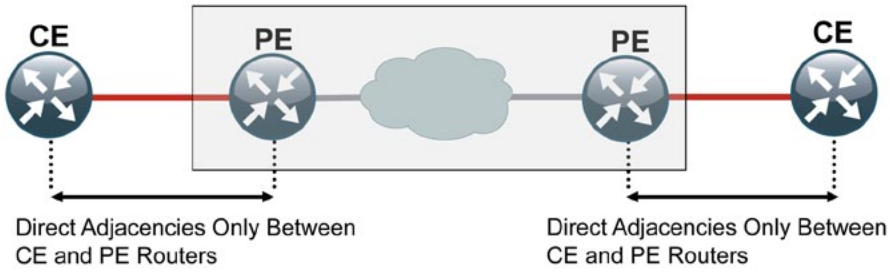
Design Details

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. Additional forwarding performance can be accomplished 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 as shown in Figure 13.

Figure 13. 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 OSPF are also effective as PE-CE routing protocols, but may not be universally available across all MPLS VPN carriers.

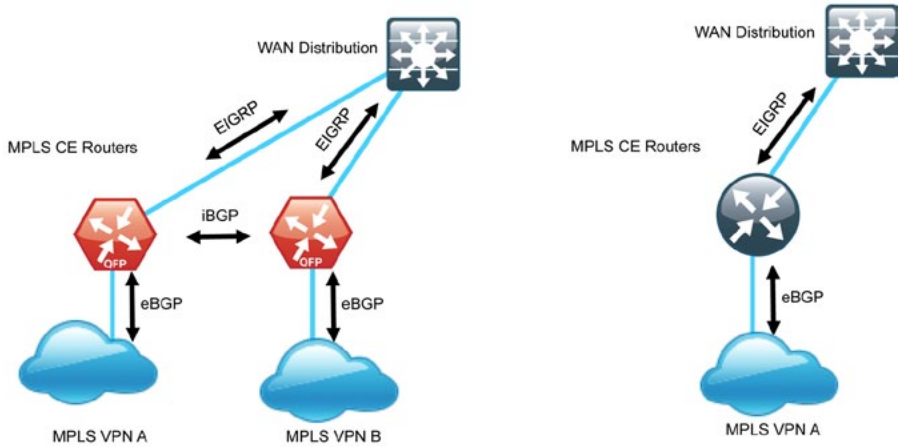
Sites with only a single WAN transport (a single-homed site) do not require dynamic PE-CE routing, and can rely on static routing because there is only a single path to any destination. This design only includes dynamic PE-CE routing to provide consistency with configurations across both single-homed 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.

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

An MPLS VPN WAN deployment requires the installation and configuration of 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 Figure 14.

Figure 14. WAN500/WAN100 Designs—MPLS CE Routing Detail



EIGRP

We 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

We have chosen BGP as the routing protocol for use between the PE and CE routers for connection 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 can be used to advertise IP aggregate addresses for remote sites.

BGP requires the selection of an Autonomous System Number (ASN). In this design, we use a private ASN (65511) as designated by the Internet Assigned Number 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.

Process

WAN-Aggregation MPLS CE Router Configuration

1. Complete the WAN Router Universal Configuration
2. Connect to Distribution Switch
3. Connect to MPLS PE Router
4. Configure EIGRP
5. Configure BGP
6. Configure IP Multicast Routing

Procedure 1 Finish the WAN Router Universal Config

Procedure Steps:

1. Configure the device hostname.
2. Configure in-band management.
3. Configure device-management protocols.
4. Configure secure user authentication.
5. Configure a synchronized clock.

Step 1: Configure the device hostname.

```
hostname [hostname]
```

Step 2: Configure in-band management interface.

All devices leverage a loopback address. A loopback is a virtual interface that is consistently reachable when multiple paths exist to the device. Various other features may use the loopback.

```
interface Loopback0
 ip address [IP address] 255.255.255.255
```

Step 3: Configure device-management protocols.

Secure Shell (SSH) is an application and a protocol that provides a secure replacement to RSH and Telnet.

Secure management access is enabled through the use of the SSH and/or HTTPS protocols.

Secure HTTP (HTTPS) provides the capability to connect a HTTP server securely. It uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, have been disabled.

```
ip domain-name cisco.local
no ip http server
```

Enabling SSH requires that a public/private keypair be generated for the device:

```
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh source-interface Loopback0
```

Various levels of device management may be available through a web interface. For secure access to this interface, you must enable the secure server (the following command also generates a public/private keypair as shown previously):

```
ip http secure-server
```

Allow only SSH access to the device:

```
line vty 0 15
 transport input ssh
```

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. This command is also useful for allowing you to continue typing at the device console when debugging is enabled.

```
line con 0
 logging synchronous
```

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
snmp-server trap-source Loopback0
```

Step 4: Configure secure user authentication.

Authentication, authorization and accounting (AAA) is enabled for access control. All management access to the network infrastructure devices (SSH, Telnet, HTTP, and HTTPS) is controlled with AAA.

A local AAA user database is defined on the network infrastructure devices to provide the ability to manage them in case the centralized RADIUS server is unavailable, or if you do not have a RADIUS server in your agency.

We highly recommend the use of a centralized authentication database.

```
enable secret c1sco123
service password-encryption
!
username admin password c1sco123
aaa new-model
aaa authentication login default group radius local
ip radius source-interface Loopback0
radius-server host 10.4.200.15 key SecretKey
```

Step 5: Configure a synchronized clock.

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 network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

Network devices should be programmed 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. Configuring console messages, logs, and debug output on switches, routers, and other devices in the network to provide timestamps on output allows cross-referencing of events in the network.

```
ntp server 10.4.200.17
ntp source Loopback0
ntp update-calendar      ! this command not for use on ASR1000
Series
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Procedure 2 Connect to Distribution Switch

A Layer 3 port-channel interface connects to the WAN distribution switch. The following configuration creates an EtherChannel link between the router and switch, with two channel-group members.

Procedure Steps:

1. Configure the port-channel interface and assign an IP address.
2. Administratively enable the port-channel group members and assign the appropriate channel group.

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

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

```
interface Port-channel [number]
 ip address [IP address] [netmask]
```

Step 2: Enable the port-channel group members and assign the appropriate channel group.

Not all router platforms can support Link Aggregation Control Protocol (LACP) to negotiate with the switch, so EtherChannel is configured statically.

```
interface [interface type] [number]
 no ip address
 channel-group [number]
 no shutdown
```

Procedure 2 Example

```
interface Port-channel1
 ip address 10.4.128.2 255.255.255.252
!
interface GigabitEthernet0/0/0
 no ip address
 channel-group 1
 no shutdown
!
interface GigabitEthernet0/0/1
 no ip address
 channel-group 1
 no shutdown
```

Procedure 3 Connect to MPLS PE Router

Procedure Steps:

1. Assign the interface bandwidth.
2. Assign the IP address and netmask of the WAN interface.
3. Administratively enable the interface and disable CDP.

Step 1: Assign the interface bandwidth.

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

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

Command Reference:

bandwidth *kbps*

NOTE: 300 Mbps = 300000 kbps

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

Procedure 3 Example

```
interface GigabitEthernet0/0/4
 bandwidth 300000
 ip address 10.4.142.1 255.255.255.252
 no cdp enable
 no shutdown
```

Procedure 4 Configure EIGRP

Procedure Steps:

1. Enable EIGRP.
2. Redistribute BGP into EIGRP.
3. Configure inbound distribute-list for EIGRP.

Step 1: Enable EIGRP.

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 [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: 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.

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.

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

Step 3: Configure 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 this configuration 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 to limit which routes are accepted for installation into the route table. The WAN-aggregation MPLS CE routers are configured to only accept routes which do not originate from the WAN. In order to accomplish this task requires the creation of an access-list that matches any routes originating from the WAN. This design allows for a straightforward summarization of the various WAN routes, which simplifies the creation of the access-list. The specific IP addresses in use are shown in Table 8.

Table 8. WAN IP Address Ranges

IP Address Range	Usage	ACL Entry
10.5.0.0/16	Remote-Site LAN	10.5.0 0 0.0.255.255
10.4.142.0/24	MPLS A PE-CE Links	10.4.142.0 0.0.0.255
10.4.143.0/24	MPLS B PE-CE Links	10.4.143.0 0.0.0.255

This example includes all IP prefixes in use on the WAN remote-site LANs and for the MPLS PE-CE links. Depending on the IP assignment in your network, more IP prefixes may need to be blocked.

It is important when creating the access-list to include a **permit any** statement at the end to permit the installation of non-matching routes.

Tech Tip

Because of the explicit permit entry at the end of the ACL, to add deny entries you must insert new ACL entries with a specific sequence number.

```
ip access-list standard [ACL name]
 deny [network 1] [network 1 inverse mask]
 deny [network 2] [network 2 inverse mask]
      <additional lines as necessary>
 deny [network N] [network N inverse mask]
 permit any

router eigrp [as number]
 distribute-list [ACL name] in
```

Procedure 4 Example

```
ip access-list standard BLOCK-DIST-ROUTES-CE
 remark Block WAN specific routes from WAN distribution layer
 deny   10.5.0.0 0.0.255.255
 deny   10.4.142.0 0.0.0.255
 deny   10.4.143.0 0.0.0.255
 permit any

router eigrp 100
 distribute-list BLOCK-DIST-ROUTES-CE in
 default-metric 100000 100 255 1 1500
 network 10.4.0.0 0.0.255.255
 redistribute bgp 65511
 passive-interface default
 no passive-interface Port-channel1
 eigrp router-id 10.4.128.241
 no auto-summary
```

Procedure 5 Configure BGP

Procedure Steps:

1. Enable BGP.
2. Configure eBGP.
3. Redistribute EIGRP into BGP.
4. Configure iBGP (optional).

Step 1: Enable BGP.

A BGP ASN is required to complete this step. 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 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 (covered in Step 3)

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

Step 2: Configure eBGP.

BGP must be configured 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 this network should be included in a network statement. This is useful to determine router reachability for troubleshooting.

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

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 these routes have been summarized before being 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 [ASN]
 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 [ASN]
 neighbor [iBGP neighbor Loopback0] remote-as [ASN]
 neighbor [iBGP neighbor Loopback0] update-source Loopback0
 neighbor [iBGP neighbor Loopback0] next-hop-self
```

Procedure 5 Example

```
router bgp 65511
 no synchronization
 bgp router-id 10.4.128.241
 bgp log-neighbor-changes
 network 0.0.0.0
 network 10.4.142.0 mask 255.255.255.252
 redistribute eigrp 100
 neighbor 10.4.128.242 remote-as 65511    ! Optional - dual
MPLS only
 neighbor 10.4.128.242 update-source
Loopback0                                 ! Optional - dual
MPLS only
 neighbor 10.4.128.242 next-hop-self      ! Optional - dual
MPLS only
 neighbor 10.4.142.2 remote-as 65401
 no auto-summary
```

Procedure 6 Configure IP Multicast Routing

This procedure applies to all WAN routers.

Procedure Steps:

1. Enable IP multicast routing.
2. Configure PIM, RP and scoping

Step 1: Enable IP multicast routing.

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

```
ip multicast-routing
```

The Cisco ASR1000 Series router requires the **distributed** keyword

```
ip multicast-routing distributed
```

Step 2: Configure PIM, RP and scoping.

Every Layer 3 switch and router must be configured with the address of the IP multicast RP. Use the **rp-address** command in conjunction with an access-list to limit the network size that the RP is responsible for. This configuration provides for future scaling and control of the IP multicast environment and can change based on network needs and design. The PIM source is configured to be the device loopback for resiliency at sites with multiple WAN transports.

```
ip pim rp-address [IP address of RP] [ACL number]
ip pim register-source Loopback0
access-list [ACL number] permit [multicast group scope] [inverse mask]
```

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

```
interface [interface type] [number]
 ip pim sparse-mode
```

Procedure 6 Example

```
ip multicast-routing distributed
!
interface Loopback0
 ip pim sparse-mode
!
interface Port-Channel1
 ip pim sparse-mode
!
interface GigabitEthernet0/0/4
 ip pim sparse-mode
!
ip pim rp-address 10.4.60.252 10
ip pim register-source Loopback0
access-list 10 permit 239.1.0.0 0.0.255.255
```

Process

WAN Distribution Switch Configuration

1. Finish Switch Universal Configuration
2. Connect to MPLS CE router
3. Connect to Core
4. Configure EIGRP
5. Configure IP Multicast Routing

Procedure 1 Finish Switch Universal Configuration

This guide assumes that the WAN distribution switch has already been configured. Only the procedures required to complete the connections of the MPLS CE router and core devices are included. Full details on distribution layer switch configuration are included in the *Cisco SBA for Large Agencies—Borderless Networks LAN Deployment Guide*.

Procedure 2 Connect to MPLS CE Router

The port-channel interface connects to a MPLS VPN router and this connection is a Layer 3 port channel. The following configuration creates an EtherChannel link between the switch and router, with two channel-group members.

Procedure Steps:

1. Configure the port-channel interface and assign the IP address.
2. Administratively enable the port-channel group members and assign the appropriate channel group.

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

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

```
interface Port-channel [number]
 no switchport
 ip address [IP address] [netmask]
```

Step 2: 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 switchport
 no ip address
 channel-group [number] mode on
 no shutdown
```

Procedure 2 Example

```
interface Port-channel1
 description bn-ce-1 EtherChannel
 no switchport
 ip address 10.4.128.1 255.255.255.252
 ip summary-address eigrp 100 10.5.0.0 255.255.0.0
!
interface GigabitEthernet1/0/3
 description bn-ce-1 port 1
 no switchport
 no ip address
 channel-group 1 mode on
 no shutdown
!
interface GigabitEthernet2/0/3
 description bn-ce-1 port 2
 no switchport
 no ip address
 channel-group 1 mode on
 no shutdown
```

Procedure 3 Connect to Core

This procedure is only required when the WAN deployment uses a separate dedicated WAN distribution switch. High-performance 10-Gbps interfaces are used. The core consists of two devices. The single link to each core device provides sufficient resiliency such that EtherChannel links are not required. The interfaces are configured as Layer 3 links.

The WAN switch generates IP route summaries for the WAN-aggregation block and for the remote sites. After the summaries have been configured, EIGRP suppresses the advertisement of more specific routes within the summaries.

```
interface [interface type] [number]
 no switchport
 ip address [IP address] [netmask]
 ip summary-address eigrp [as number] [summary network] [summary mask]
 ip summary-address eigrp [as number] [summary network] [summary mask]
```

Procedure 3 Example

```
interface TenGigabitEthernet1/0/1
 description Link to core (1)
 no switchport
 ip address 10.4.60.42 255.255.255.252
 ip summary-address eigrp 100 10.4.128.0 255.255.192.0
 ip summary-address eigrp 100 10.5.0.0 255.255.0.0
```

Procedure 4 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 auto summarization 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 sub-second 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 sub-second 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.

The distribution layer switch must be configured to enable Nonstop Forwarding 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
```

Procedure 4 Example

```
router eigrp 100
 network 10.4.0.0 0.0.255.255
 passive-interface default
 no passive-interface TenGigabitEthernet1/0/1
 no passive-interface TenGigabitEthernet2/0/1
 no passive-interface Port-channel1
 eigrp router-id 10.4.128.240
 no auto-summary
 nsf
```

Procedure 5 Configure IP Multicast Routing

This procedure applies to all WAN routers and distribution layer LAN switches.

Procedure Steps:

1. Enable IP multicast routing.
2. Configure PIM, RP and scoping.

Step 1: Enable IP multicast routing.

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

```
ip multicast-routing
```

The Cisco Catalyst 3750 Series Switch requires the **distributed** keyword

```
ip multicast-routing distributed
```

Step 2: Configure PIM, RP and scoping.

Every Layer 3 switch and router must be configured with the address of the IP multicast RP. Use the `rp-address` command in conjunction with an access-list to limit the network size that the RP is responsible for. This configuration provides for future scaling and control of the IP multicast environment and can change based on network needs and design. The PIM source is configured to be the device loopback for resiliency at sites with multiple WAN transports.

```
ip pim rp-address [IP address of RP] [ACL number]
ip pim register-source Loopback0
access-list [ACL number] permit [multicast group scope] [inverse mask]
```

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

```
interface [interface type] [number]
 ip pim sparse-mode
```

Procedure 5 Example

```
ip multicast-routing distributed
!
interface Loopback0
 ip pim sparse-mode
!
interface Port-Channel3
 ip pim sparse-mode
!
interface TenGigabitEthernet1/0/1
 ip pim sparse-mode
!
ip pim rp-address 10.4.60.252 10
ip pim register-source Loopback0
access-list 10 permit 239.1.0.0 0.0.255.255
```

Notes

Process

Remote-Site MPLS CE Router Configuration

This section includes all required procedures for the configuration of a MPLS CE router for a MPLS WAN remote site (single router, single link).

This set of procedures should also be used for a 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.

These procedures should also be used when configuring the first router of the dual-router, dual-link design.

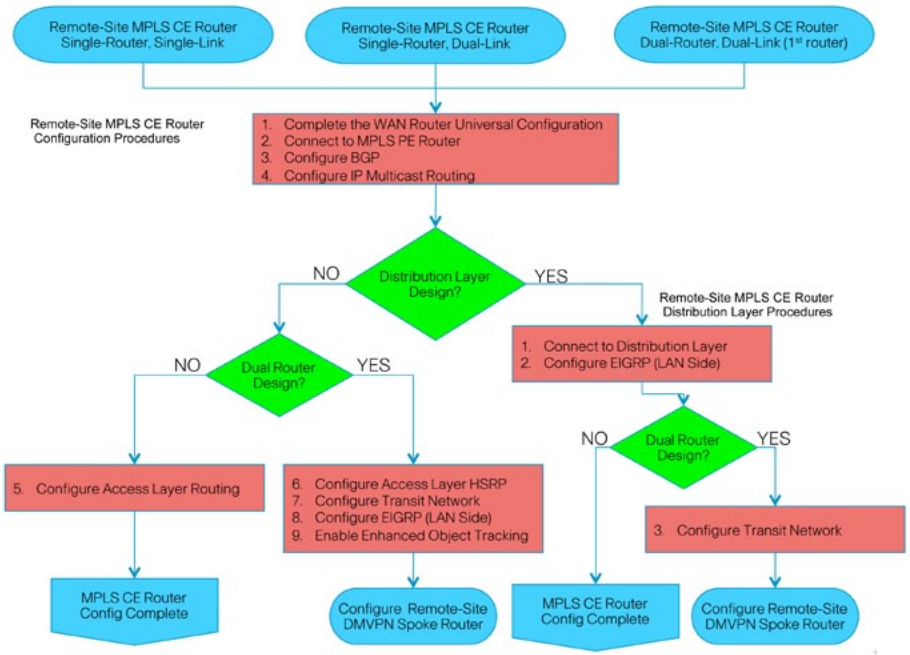
The flowchart in Figure 15 provides details on how to complete the configuration of a remote-site MPLS CE router.

1. Complete the WAN Router Universal Configuration
2. Connect to the MPLS PE Router
3. Configure BGP
4. Configure IP Multicast Routing
5. Configure Access Layer Routing

The following procedures are only relevant for the dual router design:

6. Configure Access Layer HSRP
7. Configure Transit Network
8. Configure EIGRP (LAN side)
9. Enable Enhanced Object Tracking (EOT)

Figure 15. Remote-Site MPLS CE Router Configuration Flowchart



Procedure 1 Finish WAN Router Universal Configuration

Procedure Steps:

1. Configure the device hostname.
2. Configure in-band management.
3. Configure device-management protocols.
4. Configure secure user authentication.
5. Configure a synchronized clock.

Step 1: Configure the device hostname.

```
hostname [hostname]
```

Step 2: Configure in-band management interface.

All devices leverage a loopback address. A loopback is a virtual interface that is consistently reachable when multiple paths exist to the device. Various other features may use the loopback.

```
interface Loopback0
 ip address [IP address] 255.255.255.255
```

Step 3: Configure device-management protocols.

SSH is an application and a protocol that provides a secure replacement to RSH and Telnet. Secure management access is enabled through the use of the SSH and/or HTTPS protocols. HTTPS provides the capability to connect a HTTP server securely. It uses SSL and TLS to provide device authentication and data encryption. Both protocols are encrypted for privacy and the non-secure protocols, Telnet and HTTP, have been disabled.

```
ip domain-name cisco.local
no ip http server
```

Enabling SSH requires that a public/private keypair be generated for the device:

```
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh source-interface Loopback0
```

Various levels of device management may be available through a web interface. For secure access to this interface, you must enable the secure server (the following command also generates a public/private keypair as shown previously):

```
ip http secure-server
```

Allow only SSH access to the device:

```
line vty 0 15
 transport input ssh
```

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. This command is also useful for allowing you to continue typing at the device console when debugging is enabled.

```
line con 0
 logging synchronous
```

SNMP is enabled to allow the network infrastructure devices to be managed by a 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
snmp-server trap-source Loopback0
```

Step 4: Configure secure user authentication.

AAA is enabled for access control. All management access to the network infrastructure devices (SSH, Telnet, HTTP, and HTTPS) is controlled with AAA. A local AAA user database is defined on the network infrastructure devices to provide the ability to manage them in case the centralized RADIUS server is unavailable, or if you do not have a RADIUS server in your agency. We highly recommend the use of a centralized authentication database.

```
enable secret c1sco123
service password-encryption
!
username admin password c1sco123
aaa new-model
aaa authentication login default group radius local
ip radius source-interface Loopback0
radius-server host 10.4.200.15 key SecretKey
```

Step 5: Configure a synchronized clock.

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 network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

Network devices should be programmed 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. Configuring console messages, logs, and debug output on switches, routers, and other devices in the network to provide timestamps on output allows cross-referencing of events in a network.

```
ntp server 10.4.200.17
ntp source Loopback0
```

```
ntp update-calendar      ! this command not for use on ASR1000
Series
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Procedure 2 Connect to MPLS PE Router

Procedure Steps:

1. Assign the interface bandwidth.
2. Assign the IP address and netmask of the WAN interface.
3. Administratively enable the interface and disable CDP.

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.

Command Reference:

bandwidth *kbps*

NOTE: 10 Mbps = 10000 kbps

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

Procedure 2 Example

```
interface GigabitEthernet0/0
 bandwidth 10000
 ip address 10.4.142.153 255.255.255.252
 no cdp enable
 no shutdown
```

Procedure 3 Configure BGP

Procedure Steps:

1. Enable BGP.
2. Configure eBGP.

Step 1: Enable BGP.

A BGP ASN is required to complete this step. It may be possible 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 [ASN]
 no synchronization
 bgp router-id [IP address of Loopback0]
 bgp log-neighbor-changes
 no auto-summary
```

Step 2: Configure eBGP.

BGP must be configured 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 this network should be included in a network statement. This is useful 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 can not be summarized, then each must be listed individually.

```
router bgp [ASN]
 network [PE-CE link network] mask [PE-CE link netmask]
 network [LAN network 1] mask [LAN network 1 netmask]
 network [LAN network 2] mask [LAN network 2 netmask]
 aggregate-address [summary IP address] [summary netmask]
summary-only
 neighbor [IP address of PE] remote-as [carrier ASN]
```

Procedure 3 Example

```
router bgp 65511
 no synchronization
 bgp router-id 10.5.48.254
 bgp log-neighbor-changes
 network 10.4.142.152 mask 255.255.255.252
 network 10.5.52.0 mask 255.255.255.0
 network 10.5.53.0 mask 255.255.255.0
 aggregate-address 10.5.48.0 255.255.248.0 summary-only
 neighbor 10.4.142.154 remote-as 65401
 no auto-summary
```

Procedure 4 Configure IP Multicast Routing

This procedure applies to all WAN routers.

Procedure Steps:

1. Enable IP multicast routing.
2. Configure PIM, RP and scoping.

Step 1: Enable IP multicast routing.

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

```
ip multicast-routing
```

Step 2: Configure PIM, RP and scoping.

Every Layer 3 switch and router must be configured with the address of the IP multicast RP. Use the `rp-address` command in conjunction with an access-list to limit the network size that the RP is responsible for. This configuration provides for future scaling and control of the IP multicast environment and can change based on network needs and design. The PIM source is configured to be the device loopback for resiliency at sites with multiple WAN transports.

```
ip pim rp-address [IP address of RP] [ACL number]
ip pim register-source Loopback0
access-list [ACL number] permit [multicast group scope] [inverse
mask]
```

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

```
interface [interface type] [number]
 ip pim sparse-mode
```

Procedure 4 Example

```
ip multicast-routing
!
interface Loopback0
 ip pim sparse-mode
!
interface GigabitEthernet0/0
 ip pim sparse-mode
!
interface GigabitEthernet0/2.64
 ip pim sparse-mode
!
ip pim rp-address 10.4.60.252 10
ip pim register-source Loopback0
access-list 10 permit 239.1.0.0 0.0.255.255
```

Procedure 5 Configure Access Layer Routing

Procedure Steps:

1. Enable the physical interface.
2. Create subinterfaces and assign VLAN tags.
3. Configure IP settings for each subinterface.

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 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 [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.

If the remote-site MPLS CE 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. For the modified procedure, you should skip to Procedure 6 after completing Steps 1 and 2.

```
interface [interface type] [number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [LAN network 1] LAN network 1 [netmask]
 ip helper-address [IP address of DHCP server]
```

Procedure 5 Example

```
interface GigabitEthernet0/2
 no ip address
 no shutdown
 !
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.52.1 255.255.255.0
 ip helper-address 10.4.200.10
 ip pim sparse-mode
!
interface GigabitEthernet0/2.65
 description WirelessData
 encapsulation dot1Q 65
 ip address 10.5.50.1 255.255.255.0
 ip helper-address 10.4.200.10
 ip pim sparse-mode
!
interface GigabitEthernet0/2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.53.1 255.255.255.0
 ip helper-address 10.4.200.10
 ip pim sparse-mode
!
interface GigabitEthernet0/2.70
 description WirelessVoice
 encapsulation dot1Q 70
 ip address 10.5.51.1 255.255.255.0
 ip helper-address 10.4.200.10
 ip pim sparse-mode
```

The following procedures (6–9) are only relevant for the dual-router design

Procedure 6 Configure Access Layer HSRP

[Dual-Router Design Only]

HSRP is configured to enable the use of a Virtual IP (VIP) to be used as a default gateway that is shared between two routers. The HSRP active router is the MPLS CE router and the HSRP standby router is the DMVPN spoke router. Configure the MPLS CE router with a standby priority that is higher than the DMVPN spoke 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 Table 9.

Table 9. WAN Remote-Site HSRP Parameters (Dual Router)

Router	HSRP Role	Virtual IP Address (VIP)	Real IP Address	HSRP Priority	PIM DR Priority
MPLS CE	Active	.1	.2	110	110
DMVPN Spoke	Standby	.1	.3	105	105

The assigned IP addresses override those configured with the previous procedure 5, 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 Table 9 to be the same value; however there is no requirement that these values must be identical.

This procedure should be repeated 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 [IP address of DHCP server]
 ip pim sparse-mode
 ip pim dr-priority [PIM DR priority]
 standby [number] ip [LAN network 1 gateway address] [LAN
network 1 netmask]
 standby [number] priority [priority]
 standby [number] preempt
```

Procedure 6 Example—MPLS CE Router

```
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.52.2 255.255.255.0
 ip helper-address 10.4.200.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby 1 ip 10.5.52.1
 standby 1 priority 110
 standby 1 preempt
```

Procedure 7 Configure Transit Network

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

Procedure 7 Example—MPLS CE Router

```
interface GigabitEthernet0/2.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.48.1 255.255.255.252
```

Procedure 8 Configure EIGRP (LAN Side)

[Dual-Router Design Only]

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.

Procedure Steps:

1. Enable EIGRP-100.
2. Redistribute BGP into EIGRP-100.

Step 1: Enable EIGRP-100.

EIGRP-100 is configured 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 [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: 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.

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.

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

Procedure 8 Example

```
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 GigabitEthernet0/2.99
 eigrp router-id 10.5.48.254
 no auto-summary
```

Procedure 9 Enable Enhanced Object Tracking

[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 MPLS VPN transport were to fail, the HSRP active router would learn an alternate path through the transit network to the DMVPN router and begin to forward traffic across the alternate path. This is sub-optimal routing, and can be addressed through the use of EOT.

The HSRP active router (MPLS CE) can use the IP SLA feature to send echo probes to the 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).

Procedure Steps:

1. Enable the IP SLA probe.
2. Configure EOT.
3. Link HSRP with the tracked object.

Step 1: Enable the IP SLA probe.

Standard ICMP echo (ping) probes are used, and are sent 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 2.

```
ip sla [probe number]
 icmp-echo [probe destination IP address] source-interface
[WAN interface]
 timeout 1000
 threshold 1000
 frequency 15
ip sla schedule [probe number] 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 [tracked object number] ip sla [probe number]
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]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [LAN network 1 address] [LAN network 1 netmask]
 standby [number] ip [LAN network 1 gateway address] [LAN
network 1 netmask]
 standby [number] priority [priority]
 standby [number] preempt
 standby [number] track [tracked object number] decrement
[priority]
```

Procedure 9 Example

```
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.52.2 255.255.255.0
 ip helper-address 10.4.200.10
 standby 1 ip 10.5.52.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 track 50 decrement 10
!
track 50 ip sla 100 reachability
!
ip sla 100
 icmp-echo 10.4.142.154 source-interface GigabitEthernet0/0
 timeout 1000
 threshold 1000
 frequency 15
ip sla schedule 100 life forever start-time now
```

Deploying a DMVPN WAN

DMVPN WAN Agency Overview

Agencies require the WAN to provide sufficient performance and reliability for the remote-site users to be effective in supporting the agency. 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.

Carrier-based MPLS service is not always available or cost-effective for an agency to use for WAN transport to support remote-site connectivity. Internet-based IP VPNs provide an optional transport that can be used 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 agency 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 agency. Secure data transport over public networks like the Internet requires adequate encryption to protect agency information.

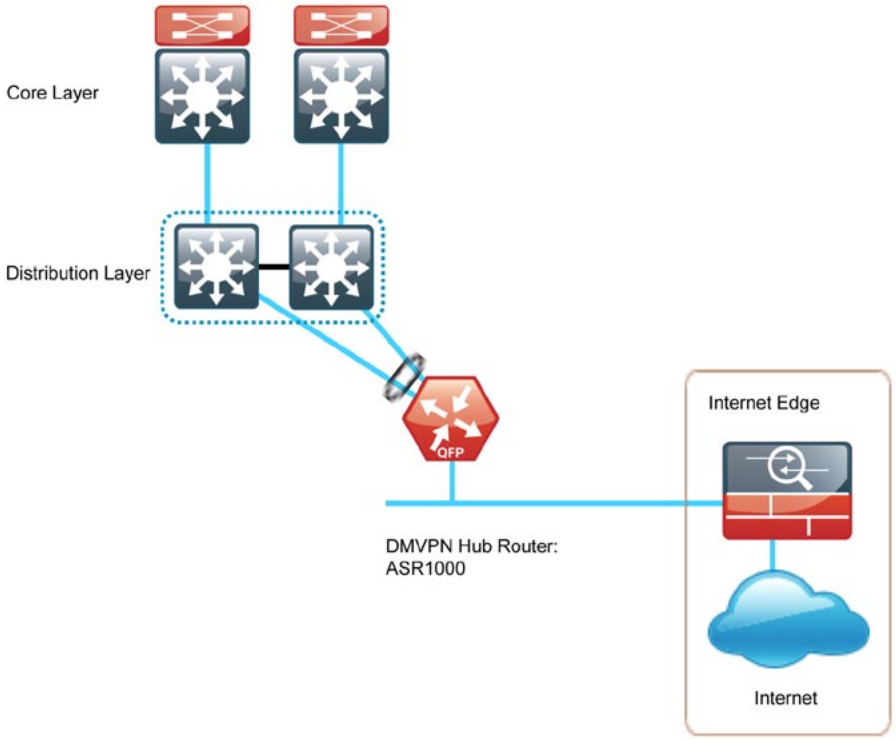
DMVPN WAN Technical Overview

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 for the DMVPN hub router. The WAN 500 design uses a single Internet service provider and a single DMVPN hub router as shown in Figure 16.

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 Large Agencies—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 16. WAN 500 Design—DMVPN Connection

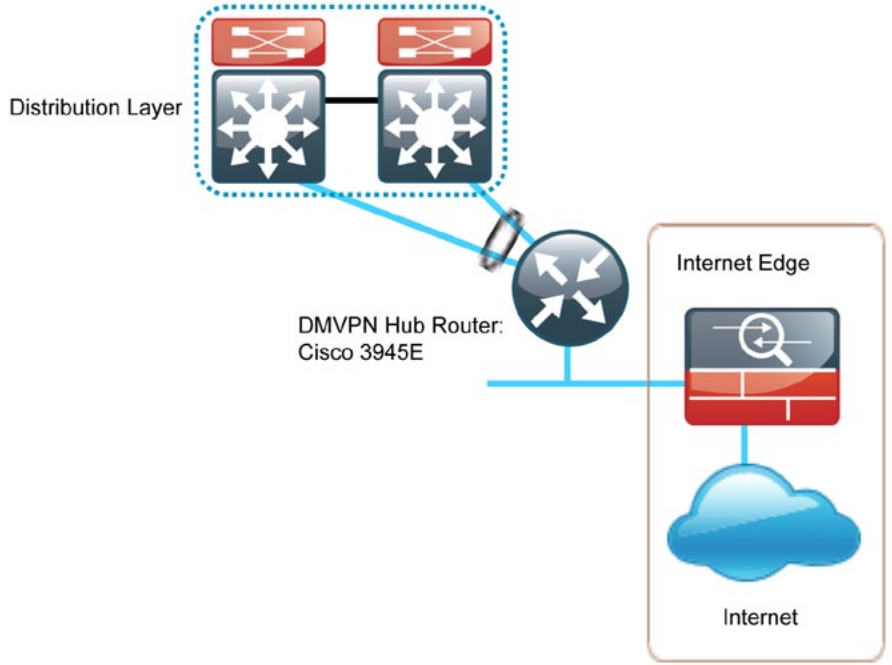


The Cisco ASR1000 Series Aggregation Services Routers represent the next-generation, modular, services-integrated Cisco routing platform. They are specifically designed for WAN aggregation, with the flexibility to support a wide range of 4- to 16-Mpps packet-forwarding capabilities, 2.5- to 20-Gbps system 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 large-agency 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 further growth in bandwidth or an increase in the number of sites is expected, then proceed with the WAN 500 design. Using the larger design can prevent unnecessary downtime associated with device upgrades. This design uses 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 as shown in Figure 17.

Figure 17. WAN 100 Design—DMVPN Connection



Remote Sites—DMVPN Spoke 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. Also we need to be concerned with having enough interfaces, enough module slots, and a properly licensed Cisco IOS image that supports the set of features that is required by the topology. We tested four integrated service router models as DMVPN spoke routers and the expected performance is shown in Table 10.

Table 10. WAN Remote-Site Router Options

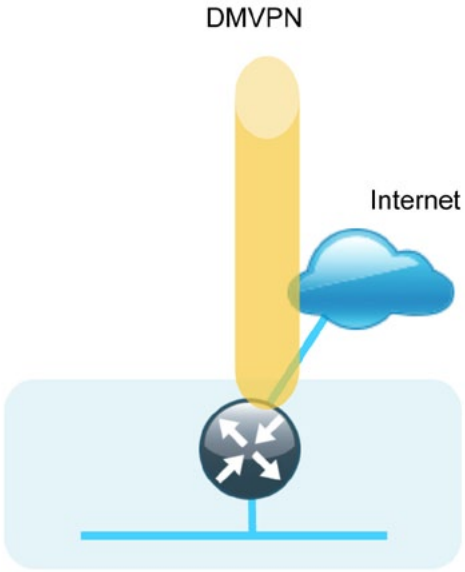
	2911	2921	3925	3945
Ethernet WAN with Services[1]	35 Mbps	50 Mbps	100 Mbps	150 Mbps
On-board GE ports	3	3	3	3
Service Module Slots[2]	1	2	2	4
Redundant Power Supply Option	No	No	Yes	Yes

Notes:
1. 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.
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 shown in Figure 18 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 it 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 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 using dynamic routing because any changes are immediately propagated to the rest of the network.

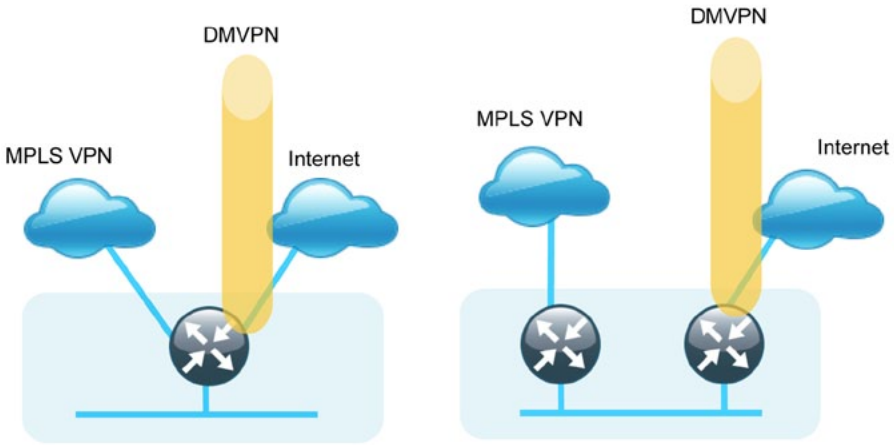
Figure 18. DMVPN Remote Site (Single Link—Single Router)



The DMVPN connection can be the primary WAN transport, or can also be the alternate to an MPLS WAN transport. The DMVPN single-link design can be added to an existing MPLS WAN design to provide additional resiliency either connecting on the same router or on an additional router. These alternate designs are shown in Figure 19. 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 to 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 19. MPLS WAN + DMVPN Remote Site (Dual Link Options)



VRFs and Front Door VRF

Virtual Routing and 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, the same or overlapping IP Addresses can be used without conflicting with each other. Often in a MPLS context, VRF is also defined as VPN Routing and Forwarding.

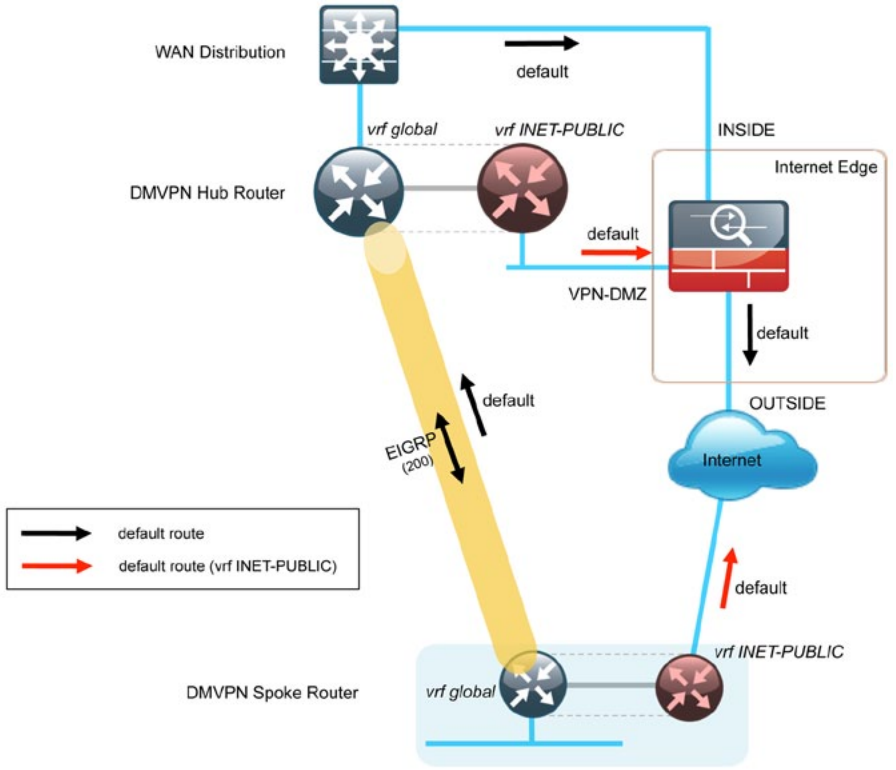
VRF may be implemented in a network device by having distinct routing tables, also known as forwarding information bases (FIBs), one per VRF. Alternatively, a network device may have the ability to configure different virtual routers, where each one has its own FIB that is not accessible to any other 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 (F-VRF), because the VRF faces the Internet and the router internal interfaces and the mGRE tunnel all remain in the global VRF. See Figure 20 for the architecture details. More technical details regarding Front Door VRF can be found in the Technical Feature Supplement appendix.

Figure 20. Front Door VRF



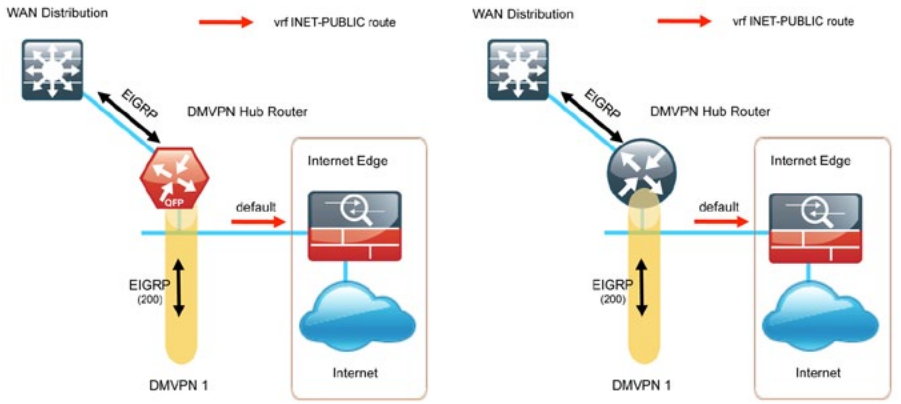
Design Details

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 are required to have sufficient IP-routing information to provide end-to-end reachability. Maintaining this routing information typically requires a routing protocol, and 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, the DMVPN router must be connected to the distribution layer and to the DMZ-VPN that provides Internet connectivity. The DMVPN hub routers use Front Door VRF and have a static default route with the INET-PUBLIC VRF pointing to the firewall DMZ interface. The IP routing details for the DMVPN WAN-aggregation topology are shown in Figure 21.

Figure 21. WAN500/100 Designs—DMVPN Routing Detail



EIGRP

We 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, 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.

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. EIGRP-200 is used for the DMVPN tunnels.

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. Table 11 highlights the packet overhead associated with encryption based on the additional headers required for various combinations of IPsec and GRE.

Table 11. 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 Transfer 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 undesired 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, we recommend that tunnel interfaces are configured 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. This `ip tcp adjust mss 1360` command is implemented on all WAN facing router interfaces in this solution.

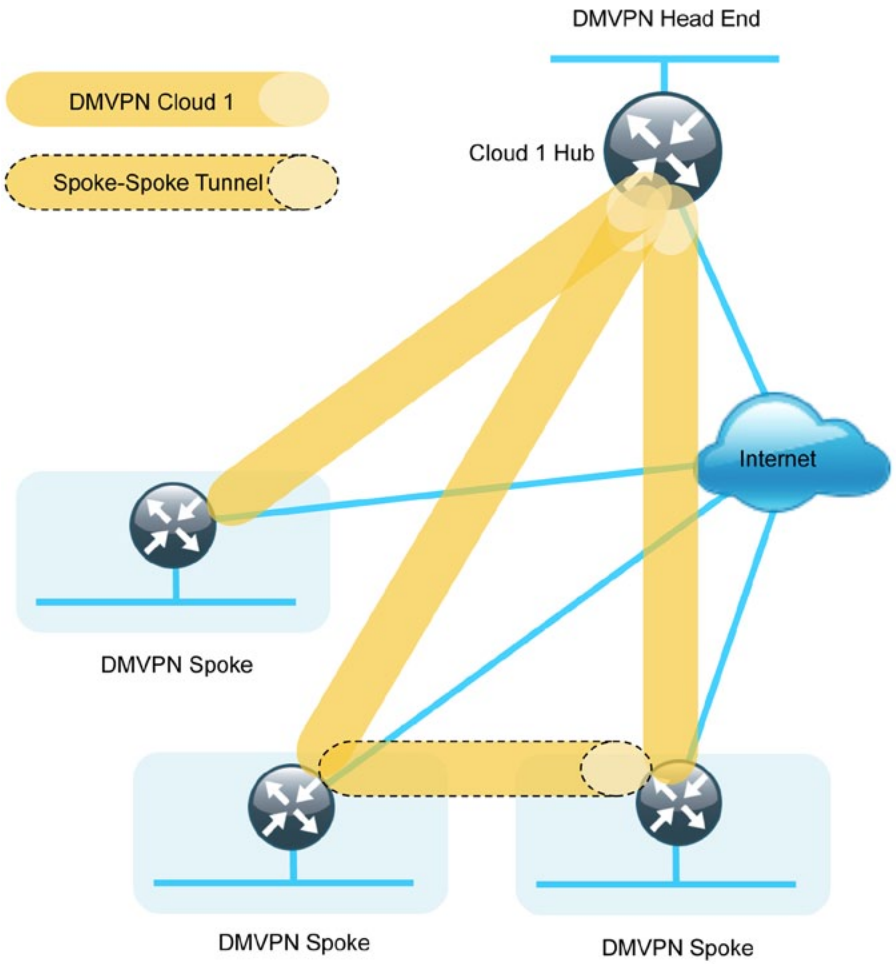
DMVPN

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 Dynamic Multipoint VPN.

Most use cases in this design guide use Internet/DMVPN as a secondary WAN transport that requires a DMVPN single-cloud, single-hub design as shown in Figure 22. 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.

Figure 22. 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.

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) keepalives 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 leverage an Internet default route for reachability to the hub routers and also other spoke addresses.

Process

DMVPN Hub Router Configuration

1. Complete the WAN Router Universal Configuration
2. Connect to the Distribution Switch
3. Configure VRF Lite
4. Connect to the Internet DMZ
5. Configure ISAKMP and IPSec
6. Configure the mGRE Tunnel
7. Configure EIGRP
8. Configure IP Multicast Routing

Procedure 1 Finish WAN Router Universal Configuration

Procedure Steps:

1. Configure the device hostname.
2. Configure in-band management.
3. Configure device-management protocols.
4. Configure secure user authentication.
5. Configure a synchronized clock.

Step 1: Configure the device hostname.

```
hostname [hostname]
```

Step 2: Configure in-band management interface.

All devices leverage a loopback address. A loopback is a virtual interface that is consistently reachable when multiple paths exist to the device. Various other features may use the loopback.

```
interface Loopback0
 ip address [IP address] 255.255.255.255
```

Step 3: Configure device-management protocols.

SSH is an application and a protocol that provides a secure replacement to RSH and Telnet. Secure management access is enabled through the use of the SSH and/or HTTPS protocols. HTTPS provides the capability to connect a HTTP server securely. It uses SSL and TLS to provide device authentication and data encryption. Both protocols are encrypted for privacy and the non-secure protocols, Telnet and HTTP, have been disabled.

```
ip domain-name cisco.local
no ip http server
```

Enabling SSH requires that a public/private keypair be generated for the device:

```
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh source-interface Loopback0
```

Various levels of device management may be available through a web interface. For secure access to this interface you must enable the secure server (the following command also generates a public/private keypair as shown previously):

```
ip http secure-server
```

Allow only SSH access to the device:

```
line vty 0 15
 transport input ssh
```

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. This command is also useful for allowing you to continue typing at the device console when debugging is enabled.

```
line con 0
 logging synchronous
```

SNMP is enabled to allow the network infrastructure devices to be managed by a 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
snmp-server trap-source Loopback0
```

Step 4: Configure secure user authentication.

AAA is enabled for access control. All management access to the network infrastructure devices (SSH, Telnet, HTTP, and HTTPS) is controlled with AAA. A local AAA user database is defined on the network infrastructure devices to provide the ability to manage them in case the centralized RADIUS server is unavailable, or if you do not have a RADIUS server in your agency. We highly recommend the use of a centralized authentication database.

```
enable secret c1sco123
service password-encryption
!
username admin password c1sco123
aaa new-model
aaa authentication login default group radius local
ip radius source-interface Loopback0
radius-server host 10.4.200.15 key SecretKey
```

Step 5: Configure a synchronized clock.

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 network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

Network devices should be programmed 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. Configuring console messages, logs, and debug output on switches, routers, and other devices in the network to provide timestamps on output allows cross-referencing of events in a network.

```
ntp server 10.4.200.17
ntp source Loopback0
ntp update-calendar    ! this command not for use on ASR1000
Series
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Procedure 2 Connect to Distribution Switch

A Layer 3 port-channel interface connects to the WAN distribution switch. The following configuration creates an EtherChannel link between the router and switch, with two channel-group members.

Procedure Steps:

1. Configure the port-channel interface and assign an IP address.
2. Administratively enable the port-channel group members and assign the appropriate channel group.

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

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

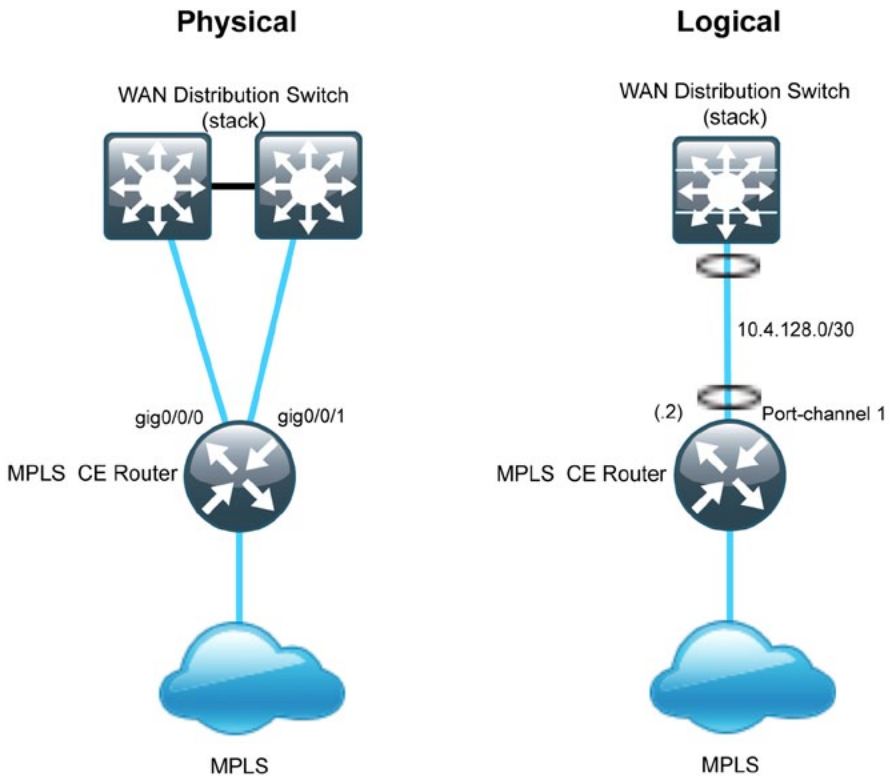
```
interface Port-channel [number]
 ip address [IP address] [netmask]
```

Step 2: 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
```

Procedure 2 Example




```
interface Port-channel3
 ip address 10.4.128.18 255.255.255.252
!
interface GigabitEthernet0/0/0
 no ip address
 channel-group 3
 no shutdown
!
interface GigabitEthernet0/0/1
 no ip address
 channel-group 3
 no shutdown
```

Procedure 3 Configure VRF Lite

An Internet-facing VRF is created to support Front Door VRF for DMVPN. The VRF name is arbitrary but it is useful to select a name that describes the VRF. An associated route distinguisher (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.

Command Reference:

An RD is either of the following:

- ASN-related—Composed of an ASN and an arbitrary number.
- 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.

```
ip vrf [vrf-name]
 rd [ASN:number]
```

Procedure 3 Example

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

Procedure 4 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.

Procedure Steps:

1. Administratively enable the interface, select the VRF, and assign the IP address.
2. Configure the VRF-specific default routing.

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

The IP address used 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 Front Door VRF, so this interface must be placed into the VRF configured in the previous procedure.

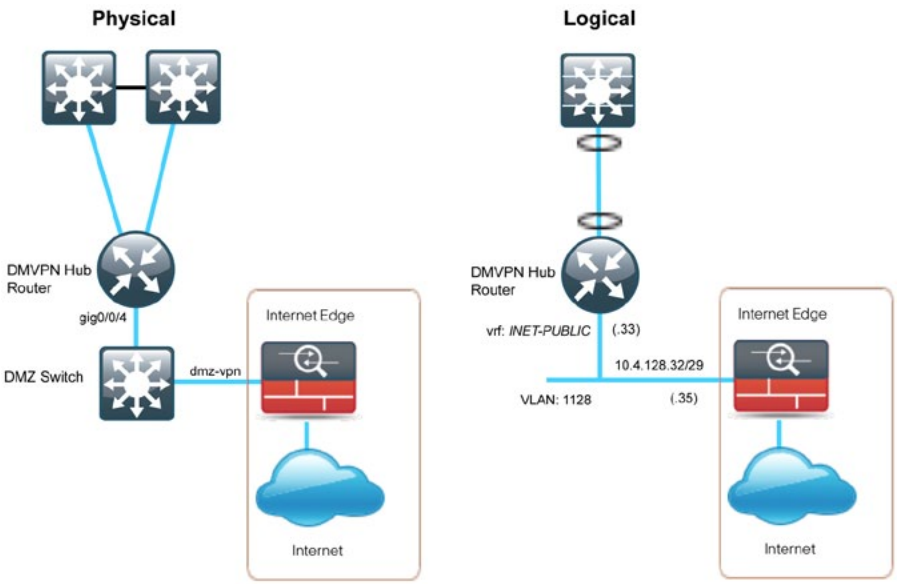
```
interface [interface type] [number]
 ip vrf forwarding [vrf name]
 ip address [IP address] [netmask]
 no shutdown
```

Step 2: Configure the VRF specific default routing.

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

```
ip route vrf [vrf name] 0.0.0.0 0.0.0.0 [ASA5500 DMZ interface
IP address]
```

Procedure 4 Example




```
interface GigabitEthernet0/0/4
 ip vrf forwarding INET-PUBLIC
 ip address 10.4.128.33 255.255.255.248
 no shutdown
 !
ip route vrf INET-PUBLIC 0.0.0.0 0.0.0.0 10.4.128.35
```

Procedure 5 Configure ISAKMP and IPSec

Procedure Steps:

1. Configure the crypto keyring.
2. Configure the ISAKMP policy.
3. Create the ISAKMP profile.
4. Define the IPSec transform set.
5. Create the IPSec profile.

Step 1: Configure the crypto keyring.

The crypto keyring defines a pre-shared key (or password) valid for IP sources reachable within a particular VRF. This key is a wildcard pre-shared key 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 [keyring name] vrf [vrf name]
  pre-shared-key address 0.0.0.0 0.0.0.0 key [pre-shared key]
```

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 pre-shared key
- 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 [ISAKMP profile name]
   keyring [keyring name]
   match identity address 0.0.0.0 [vrf name]
```

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 [IPSec transform-set name] 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 [IPSec profile name]
 set transform-set [IPSec transform-set name]
 set isakmp-profile [ISAKMP profile name]
```

Procedure 5 Example

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

crypto isakmp policy 10
 encr aes 256
 hash sha
 authentication pre-share
 group 2

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

crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC
```

Procedure 6 Configure the mGRE Tunnel

Procedure Steps:

1. Configure basic interface settings.
2. Configure the tunnel.
3. Configure NHRP.
4. Configure EIGRP.

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.

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 Tunnel [number]
 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 Procedure 6 to connect to the Internet. The `tunnel vrf` command should be set to the VRF defined previously for Front Door VRF.

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

```
interface Tunnel [number]
 tunnel source [source interface]
 tunnel mode gre multipoint
 tunnel vrf [vrf name]
 tunnel protection ipsec profile [IPSec profile name]
```

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 Tunnel [number]
 ip nhrp authentication [password]
 ip nhrp map multicast dynamic
 ip nhrp network-id [network id]
 ip nhrp holdtime 600
 ip nhrp redirect
```

Step 4: Configure EIGRP.

EIGRP is configured in the following Procedure 9, but has some specific requirements for the mGRE tunnel interface.

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 hold time is increased to 35 seconds to accommodate up to 500 remote sites on a single DMVPN cloud.

```
interface Tunnel [number]
ip hold-time eigrp [as number – eigrp dmvpn] 35
no ip split-horizon eigrp 200
```

Procedure 6 Example

```
interface Tunnel10
 bandwidth 10000
 ip address 10.4.132.1 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip hold-time eigrp 200 35
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp redirect
 ip tcp adjust-mss 1360
 no ip split-horizon eigrp 200
 tunnel source GigabitEthernet0/0/3
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC
 tunnel protection ipsec profile DMVPN-PROFILE
```

Procedure 7 Configure EIGRP

Two EIGRP processes are used 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 only a single process was used, 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.

Procedure Steps:

1. Enable EIGRP-100 for internal routing.
2. Enable an additional EIGRP-200 process for DMVPN.

Step 1: Enable EIGRP-100 for internal routing.

EIGRP-100 is configured facing the LAN distribution/core. Routes from the other EIGRP process are redistributed. Because the routing protocol is the same, no default metric is required.

In this design, the port-channel interface and the loopback are 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. The tunnel interface address should not be included in the network range. It may be helpful to explicitly list all of the relevant networks rather than include them in a single statement.

```
router eigrp [as number]
 network [port-channel network] [inverse mask]
 network [loopback network] 0.0.0.0
 redistribute eigrp [as number (DMVPN)]
 passive-interface default
 no passive-interface [port-channel interface]
 eigrp router-id [IP address of Loopback0]
 no auto-summary
```

Step 2: Enable an additional EIGRP-200 process for DMVPN.

EIGRP-200 is configured 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 its network range should be explicitly listed.

```
router eigrp [as number (DMVPN)]
 network [mGRE tunnel network] [inverse mask]
 redistribute eigrp [as number]
 passive-interface default
 no passive-interface [mGRE tunnel interface]
 eigrp router-id [IP address of Loopback0]
 no auto-summary
```

Procedure 7 Example

```
router eigrp 100
 network 10.4.128.16 0.0.0.3
 network 10.4.128.243 0.0.0.0
 redistribute eigrp 200
 passive-interface default
 no passive-interface Port-channel3
 no auto-summary

router eigrp 200
 network 10.4.132.0 0.0.1.255
 redistribute eigrp 100
 passive-interface default
 no passive-interface Tunnel10
 no auto-summary
```

Procedure 8 Configure IP Multicast Routing

This procedure applies to all DMVPN Hub routers.

Procedure Steps:

1. Enable IP multicast routing.
2. Configure PIM, RP and scoping.
3. Enable PIM non-broadcast multiple access (NBMA) mode for the DMVPN tunnel

Step 1: Enable IP multicast routing.

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

```
ip multicast-routing
```

The Cisco ASR1000 Series router requires the **distributed** keyword

```
ip multicast-routing distributed
```

Step 2: Configure PIM, RP and scoping.

Every Layer 3 switch and router must be configured with the address of the IP multicast RP. Use the **rp-address** command in conjunction with an access-list to limit the network size that the RP is responsible for. This configuration provides for future scaling and control of the IP multicast environment and can change based on network needs and design. The PIM source is configured to be the device loopback for resiliency at sites with multiple WAN transports.

```
ip pim rp-address [IP address of RP] [ACL number]
ip pim register-source Loopback0
access-list [ACL number] permit [multicast group scope] [inverse mask]
```

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

NOTE: Do not enable PIM on the Internet DMZ interface, as no multicast traffic should be requested from this interface.

```
interface [interface type] [number]
 ip pim sparse-mode
```

Step 3: 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.

```
interface Tunnel [number]
 ip pim nbma-mode
```

Procedure 8 Example

```
ip multicast-routing distributed
!
interface Loopback0
 ip pim sparse-mode
!
interface Port-Channel3
 ip pim sparse-mode
!
interface Tunnel10
 ip pim nbma-mode
 ip pim sparse-mode
!
ip pim rp-address 10.4.60.252 10
ip pim register-source Loopback0
access-list 10 permit 239.1.0.0 0.0.255.255
```

Process

WAN Distribution Switch Configuration

1. Finish Switch Universal Configuration
2. Connect to DMVPN Hub Router
3. Connect to Core
4. Configure EIGRP
5. Configure IP Multicast Routing

Procedure 1 Finish Switch Universal Configuration

This guide assumes that the WAN distribution switch has already been configured. Only the procedures required to complete the connections of the DMVPN hub router and core devices are included. Full details on distribution layer switch configuration are included in the *Cisco SBA for Large Agencies—Borderless Networks LAN Deployment Guide*.

Procedure 2 Connect to DMVPN Hub Router

The port-channel interface connects to a DMVPN hub router. This connection is a Layer 3 port-channel. The following configuration creates an EtherChannel link between the switch and router, with two channel-group members.

Procedure Steps:

1. Configure the port-channel interface and assign the IP address.
2. Administratively enable the port-channel group members and assign the appropriate channel group.

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

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

```
interface Port-channel [number]
 no switchport
 ip address [IP address] [netmask]
```

Step 2: 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 switchport
 no ip address
 channel-group [number] mode on
 no shutdown
```

Procedure 2 Example

```
interface Port-channel3
 description bn-dmvpn-1 EtherChannel
 no switchport
 ip address 10.4.128.17 255.255.255.252
 ip summary-address eigrp 100 10.5.0.0 255.255.0.0
!
interface GigabitEthernet1/0/29
 description bn-dmvpn-1 port 1
 no switchport
 no ip address
 channel-group 3 mode on
 no shutdown
!
interface GigabitEthernet2/0/29
 description bn-dmvpn-1 port 2
 no switchport
 no ip address
 channel-group 3 mode on
 no shutdown
```

Procedure 3 Connect to Core

This procedure is only required when the WAN deployment uses a separate dedicated WAN distribution switch. High-performance 10-Gbps interfaces are used. The core consists of two devices. The single link to each core device provides sufficient resiliency such that EtherChannel links are not required. The interfaces are configured as Layer 3 links.

The WAN switch generates IP route summaries for the WAN-aggregation block and for the remote sites. After the summaries have been configured, EIGRP suppresses the advertisement of more specific routes within the summary ranges.

```
interface [interface type] [number]
 no switchport
 ip address [IP address] [netmask]
 ip summary-address eigrp [as number] [summary network] [summary
mask]
 ip summary-address eigrp [as number] [summary network] [summary
mask]
```

Procedure 3 Example

```
interface TenGigabitEthernet1/0/1
 description Link to core (1)
 no switchport
 ip address 10.4.60.42 255.255.255.252
 ip summary-address eigrp 100 10.4.128.0 255.255.192.0
 ip summary-address eigrp 100 10.5.0.0 255.255.0.0
```

Procedure 4 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 auto summarization 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 sub-second 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 sub-second 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.

The distribution layer switch must be configured to enable Nonstop Forwarding 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
```

Procedure 4 Example

```
router eigrp 100
 network 10.4.0.0 0.0.255.255
 passive-interface default
 no passive-interface TenGigabitEthernet1/0/1
 no passive-interface TenGigabitEthernet2/0/1
 no passive-interface Port-channel3
 eigrp router-id 10.4.128.240
 no auto-summary
 nsf
```

Procedure 5 Configure IP Multicast Routing

This procedure applies to all WAN routers and distribution-layer LAN switches.

Procedure Steps:

1. Enable IP multicast routing.
2. Configure PIM, RP and scoping.

Step 1: Enable IP multicast routing.

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

```
ip multicast-routing
```

The Cisco Catalyst 3750 Series Switch requires the **distributed** keyword

```
ip multicast-routing distributed
```

Step 2: Configure PIM, RP and scoping.

Every Layer 3 switch and router must be configured with the address of the IP multicast RP. Use the `rp-address` command in conjunction with an access-list to limit the network size that the RP is responsible for. This configuration provides for future scaling and control of the IP multicast environment and can change based on network needs and design. The PIM source is configured to be the device loopback for resiliency at sites with multiple WAN transports.

```
ip pim rp-address [IP address of RP] [ACL number]
ip pim register-source Loopback0
access-list [ACL number] permit [multicast group scope] [inverse
mask]
```

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

```
interface [interface type] [number]
 ip pim sparse-mode
```

Procedure 5 Example

```
ip multicast-routing distributed
!
interface Loopback0
 ip pim sparse-mode
!
interface Port-Channel1
 ip pim sparse-mode
!
interface Port-Channel2
 ip pim sparse-mode
```

```
!
interface TenGigabitEthernet1/0/1
 ip pim sparse-mode
!
ip pim rp-address 10.4.60.252 10
ip pim register-source Loopback0
access-list 10 permit 239.1.0.0 0.0.255.255
```

Process

Firewall and DMZ Switch Configuration

1. Configure Firewall DMZ
2. Configure Firewall Address Translation
3. Configure Firewall Policy for DMVPN Hub

Procedure 1 Configure Firewall DMZ

The firewall's DMZ is a portion of the network where, typically, traffic to and from other parts of the network is tightly restricted. Agencies place network services in a DMZ for exposure to the Internet; these servers are typically not allowed to initiate connections to the internal network, except for specific circumstances.

The various DMZ networks are connected using a VLAN trunk to the Gigabit Ethernet interface of the Cisco ASA 5500. The DMVPN hub router connects to the DMZ switch using a single interface; the VPN-DMZ VLAN interface on the firewall is assigned an IP address, which is the default gateway for the VPN-DMZ network. The VLAN interface of the DMZ switch does not have an IP address assigned for the VPN-DMZ VLAN.

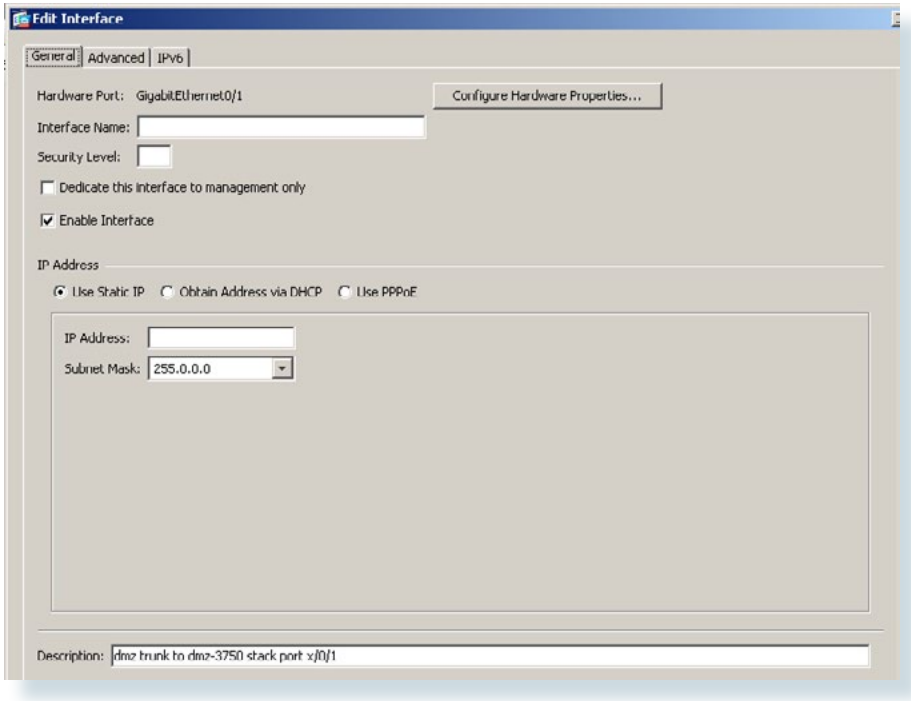
Procedure Steps:

1. Configure the Cisco ASA5500 physical interface.
2. Configure the subinterface for the DMZ-VPN.
3. On the DMZ switch, define the switch ports that connect to the firewall as trunk ports and add the appropriate VLAN.
4. On the DMZ switch, configure the interface and assign the access port VLAN.

Step 1: Configure the Cisco ASA 5500 physical interface.

Configure the interface that carries the VLAN trunk for the various DMZs. Values are not assigned for the interface name, security level, or IP address on trunk interfaces. Configuration details are shown in Figure 23.

Figure 23. Define DMZ Trunk Interface




```
interface GigabitEthernet0/1
 description dmz trunk to dmz-3750 stack port x/0/1
 no nameif
 no security-level
 no ip address
```

Step 2: Configure the subinterface for the DMZ-VPN.

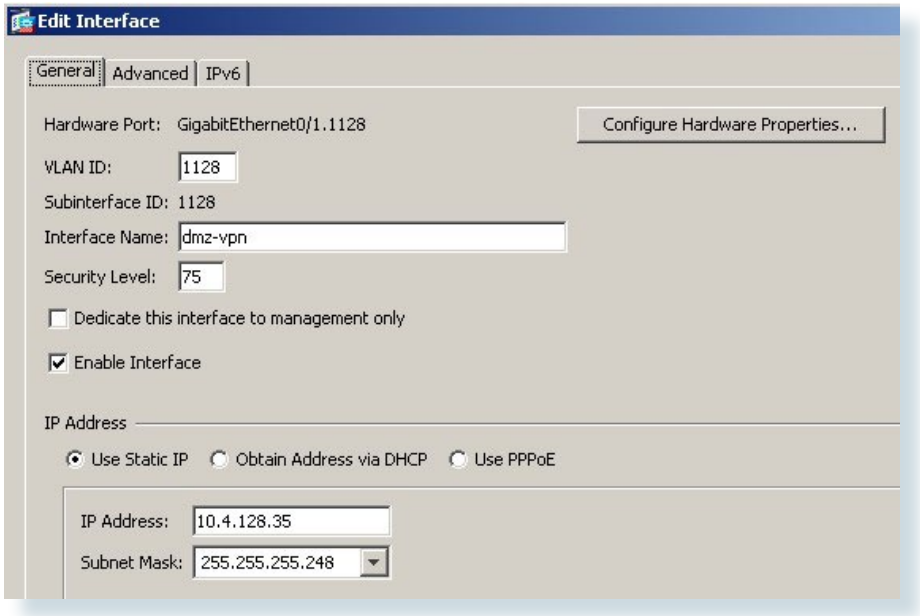
The DMZ VLAN interface must be configured with an appropriate IP address for the attached network, as well as an intuitive interface name to be used for NAT and security policy configuration. The tested design uses the values

shown in Table 12. The configuration for a VLAN interface is illustrated in

Table 12. VPN-DMZ Configuration Parameters

Interface Label	IP Address & Netmask	VLAN	Security Level	Name
GigabitEthernet 0/1.1128	10.4.128.35 255.255.255.248	1128	75	dmz-vpn

Figure 24. DMZ Subinterface Configuration




```
interface GigabitEthernet0/1.1128
 VLAN 1128
 nameif dmz-vpn
 security-level 75
 ip address 10.4.128.35 255.255.255.248
```

Step 3: On the DMZ switch, define the switch ports that connect to the firewall as trunk ports and add the appropriate VLAN.

If this is the first VLAN to be added to the trunk from the DMZ switch, then use the following set of commands:

```
interface GigabitEthernet1/0/1
 description ASA5540-1 DMZ uplink
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 1128
 switchport mode trunk
 spanning-tree link-type point-to-point
```

If this is an additional VLAN being added to an existing trunk from the DMZ switch, then use the following set of commands:

```
interface GigabitEthernet1/0/1
 switchport trunk allowed VLAN add 1128
```

Step 4: On the DMZ switch, configure the interface and assign the access port VLAN.

```
interface [interface type] [number]
 switchport access VLAN [VLAN number]
 no shutdown
```

Procedure 2 Configure Firewall Address Translation

Prior to this procedure, the DMZ-VPN network would have connectivity to the Cisco ASA 5500 interface, but there would be no access from the DMZ-VPN network to the Internet, or from the Internet to the DMZ-VPN. A last step is required to allow Internet connectivity for the DMZ; the DMZ network uses private network (RFC 1918) addressing that is not Internet routable, so the firewall must translate the DMZ address to an outside public address. For this configuration, we are going to translate the DMZ-VPN address of the DMVPN hub router to a public IP address that can be routed on the Internet as shown in Table 13.

Table 13. DMVPN Hub IP Address Translation Information

DMVPN Hub Public Address (actual)	DMVPN Hub Public Address (externally routable after NAT)
10.4.128.133	172.16.130.1

NOTE: As you apply the address translation configuration described in this portion of the document, the security appliance applies its default access rule set that permits traffic from higher-security interfaces to lower-security interfaces. Review your expected traffic carefully; if you cannot allow some or all traffic that is allowed by the default rules, you should shut down the various device interfaces until you have completely configured your firewall rule set.

Procedure Steps:

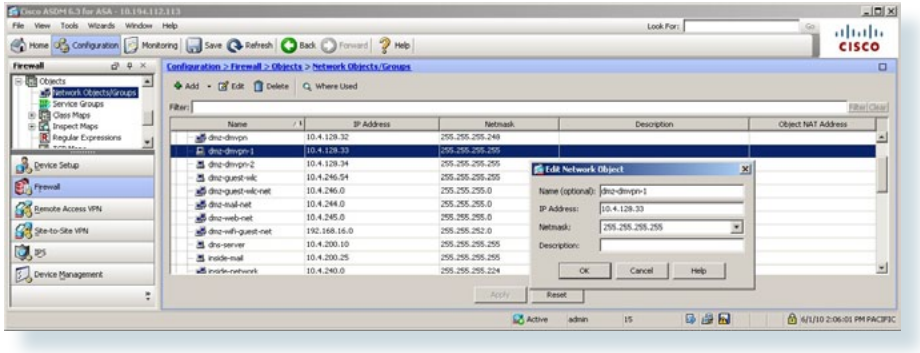
1. Configure name-to-address mappings for DMZ-VPN network and the DMVPN hub router.
2. Define static translation policy for traffic passing between the Internet and the DMVPN hub router in the DMZ-VPN.

Step 1: Configure name-to-address mappings for DMZ-VPN network and the DMVPN hub router.

These names are used for NAT configuration, as well as access-rule definition. Be sure the names that you apply are applicable for all parts of the configuration. Using address-family names and object-groups improves command-line and Cisco Adaptive Security Device Manager (ASDM) usability for the Cisco ASA 5500, as the various IP networks and hosts within your agency are represented as names instead of IP addresses. This step is shown in Figure 25.

Go to **Configuration > Firewall > Objects > Network Objects/Groups**

Figure 25. Configure Network Object Names

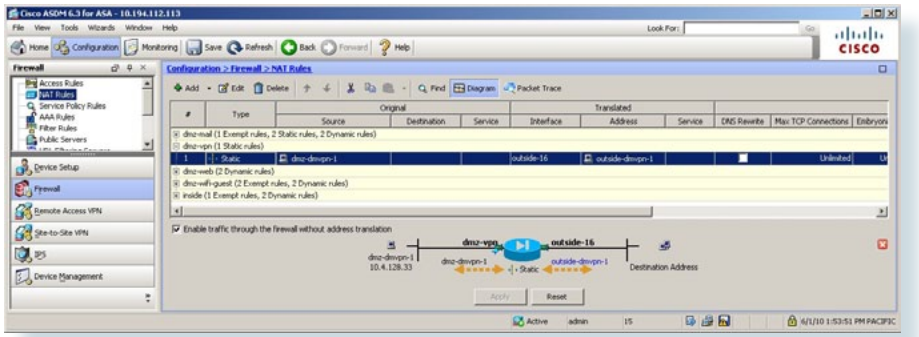


```
names
name 172.16.130.1 outside-dmvpn-1
name 10.4.128.32 dmz-dmvpn
name 10.4.128.33 dmz-dmvpn-1
```

Step 2: Define static translation policy for traffic passing between the Internet and the DMVPN hub router in the DMZ-VPN.

All devices that must be exposed to the Internet require a static translation. The DMVPN hub router translation is shown in Figure 26.

Figure 26. Define Firewall Static Translations for DMVPN Hub Router



```
static (dmz-vpn,outside) 172.16.130.1 10.4.128.33 netmask
255.255.255.255
```

Procedure 3 Configure Firewall Policy for DMVPN Hub

Security policy configuration is fairly arbitrary to suit the policy and management requirements of an agency. Thus, examples here should be used as a basis for your network-security requirements.

The Site-to-Site VPN DMZ provides an additional layer of protection to lower the likelihood of certain types of misconfiguration of the VPN routers exposing the agency network to the Internet. A filter allows only VPN traffic as well as some diagnostic traffic to reach the VPN routers, to facilitate troubleshooting for reachability to the VPN hubs from remote sites.

Table 14. Required DMVPN Protocols (Hub Router)

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

Table 15. Optional Protocols—DMVPN Hub 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

Procedure Steps:

1. Define access-control entries to allow VPN traffic to the DMVPN routers in the DMZ-VPN.
2. Define additional access-control entries to allow diagnostic traffic to the DMVPN routers in the DMZ-VPN.

Step 1: Define access-control entries to allow VPN and diagnostic traffic to the DMVPN routers in the DMZ-VPN.

This policy is applied on the outside-interface Access Rule, and builds on existing policies:

```
access-list OUT-ACCESS-IN extended permit udp any host outside-dmvpn-1 eq 4500
access-list OUT-ACCESS-IN extended permit udp any host outside-dmvpn-1 eq isakmp
access-list OUT-ACCESS-IN extended permit esp any host outside-dmvpn-1
access-group OUT-ACCESS-IN in interface outside-16
```

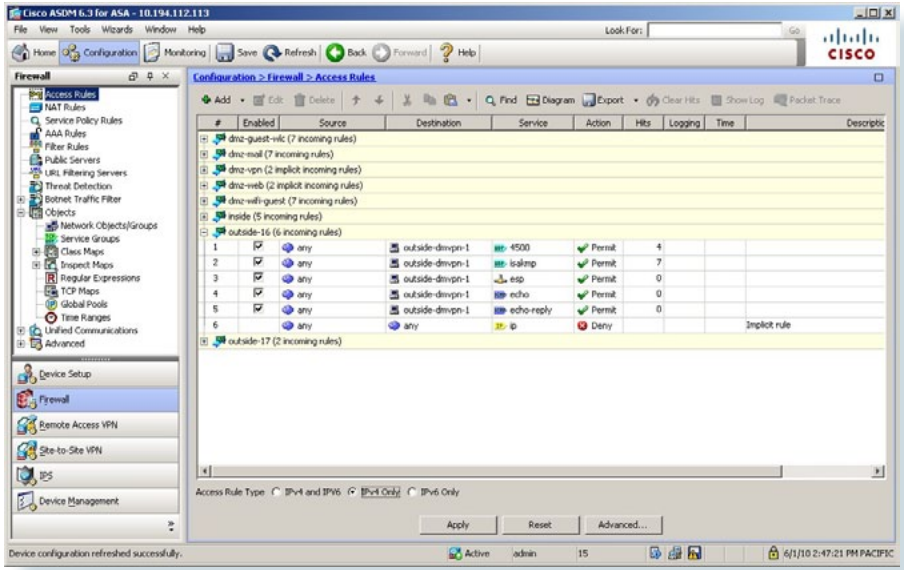
Step 2: This step is optional. Define additional access-control entries to allow diagnostic traffic to the DMVPN routers in the DMZ-VPN.

This policy is applied on the outside-interface access rule, and builds on existing policies:

```
access-list OUT-ACCESS-IN extended permit icmp any host outside-dmvpn-1 echo
access-list OUT-ACCESS-IN extended permit icmp any host outside-dmvpn-1 echo-reply
access-group OUT-ACCESS-IN in interface outside-16
```

The combined policy as implemented in Step 1 and Step 2 is illustrated in Figure 27.

Figure 27. Define Internet to DMZ-VPN Inbound Policy



Process

Enabling DMVPN Backup on Existing MPLS CE Router Configuration

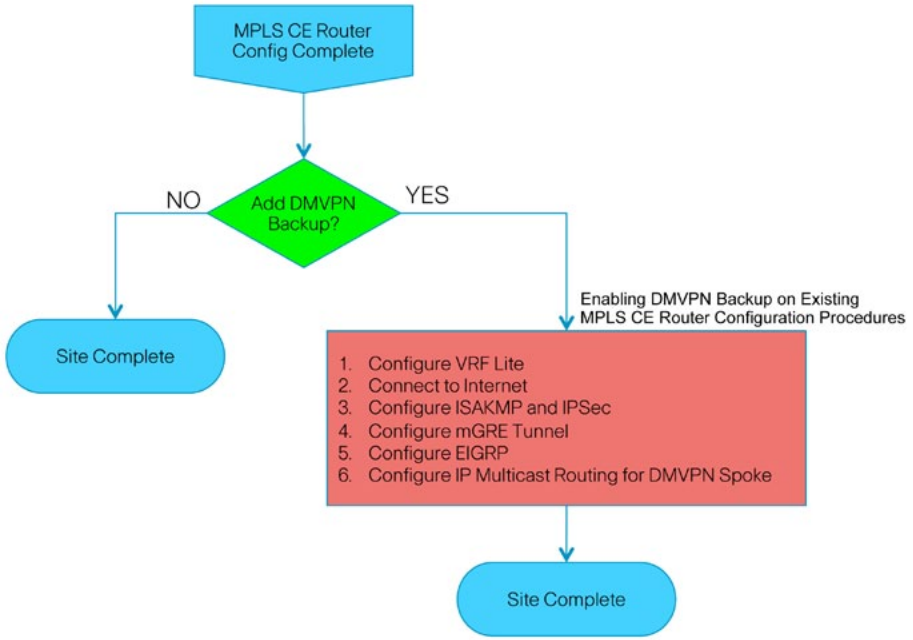
1. Configure VRF Lite
2. Connect to the Internet
3. Configure ISAKMP and IPSec
4. Configure the mGRE Tunnel
5. Configure EIGRP
6. Configure IP Multicast Routing

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 flowchart in Figure 28 provides details on 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 Front Door VRF for DMVPN. The VRF name is arbitrary, but it is useful to select a name that describes the VRF. An associated route distinguisher (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.

Command Reference:

An RD is either of the following:

- ASN-related—Composed of an ASN and an arbitrary number.
- 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.

```
ip vrf [vrf-name]
 rd [ASN:number]
```

Procedure 1 Example

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

Procedure 2 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. Since 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.

Procedure Steps:

1. Administratively enable the interface, select VRF and enable DHCP.
2. Configure and apply the access list.

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

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

```
interface [interface type] [number]
 ip vrf forwarding [vrf name]
 ip address dhcp
 no shutdown
```

Step 2: Configure and apply the access list.

The IP access list must permit the protocols specified in Table 16. The access list is applied inbound on the WAN interface, so filtering is done on traffic destined to the router.

Table 16. 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 [interface type] [number]
 ip access-group [ACL name] in
ip access-list extended [ACL name]
 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 Table 17 may assist in troubleshooting, but are not explicitly required to allow DMVPN to function properly.

Table 17. 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 2 Example

```
interface GigabitEthernet0/1
 ip vrf forwarding INET-PUBLIC
 ip address dhcp
 ip access-group ACL-INET-PUBLIC in
 no shutdown

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 icmp any any echo
 permit icmp any any echo-reply
 permit udp any any eq bootpc
```

Procedure 3 Configure ISAKMP and IPsec

Procedure Steps:

1. Configure the crypto keyring.
2. Configure the ISAKMP policy and dead peer detection.
3. Create the ISAKMP profile.
4. Define the IPsec transform set.
5. Create the IPsec profile.

Step 1: Configure the crypto keyring.

The crypto keyring defines a pre-shared key (or password) valid for IP sources reachable within a particular VRF. This key is a wildcard pre-shared key 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 [keyring name] vrf [vrf name]
  pre-shared-key address 0.0.0.0 0.0.0.0 key [pre-shared key]
```

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 pre-shared key
- Diffie-Hellman group: 2

DPD is enabled with keepalives 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 [ISAKMP profile name]
   keyring [keyring name]
   match identity address 0.0.0.0 [vrf name]
```

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, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set [IPSec transform-set name] 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 [IPSec profile name]
 set transform-set [IPSec transform-set name]
 set isakmp-profile [ISAKMP profile name]
```

Procedure 3 Example

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

crypto isakmp policy 10
 encr aes 256
 hash sha
 authentication pre-share
 group 2

crypto isakmp keepalive 30 5

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

crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC
```

Procedure 4 Configure the mGRE Tunnel

Procedure Steps:

1. Configure basic interface settings.
2. Configure the tunnel.
3. Configure NHRP.
4. Configure EIGRP.

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.

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 Tunnel [number]
 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 Procedure 2 to connect to the Internet. The tunnel vrf command should be set to the VRF defined previously for Front Door VRF.

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

```
interface Tunnel [number]
 tunnel source [source interface]
 tunnel mode gre multipoint
 tunnel vrf [vrf name]
 tunnel protection ipsec profile [IPSec profile name]
```

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 used 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 Table 18.

Table 18. DMVPN Hub IP Address Information

DMVPN Hub Public Address (actual)	DMVPN Hub Public Address (externally routable after NAT)	NHS (DMVPN Hub mGRE Tunnel Address)
10.4.128.133	172.16.130.1	10.4.132.1

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 allow existing cache entries to be overwritten. 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 Tunnel [number]
 ip nhrp authentication [password]
 ip nhrp map [NHS IP address] [DMVPN hub outside IP address]
 ip nhrp map multicast [DMVPN hub outside IP address]
 ip nhrp network-id [network id]
 ip nhrp holdtime 600
 ip nhrp nhs [NHS IP address]
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
```

Step 4: Configure EIGRP.

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 can not be summarized, then EIGRP continues to advertise the specific routes.

```
interface Tunnel [number]
 ip summary-address eigrp [as number (dmvpn)] [summary
network] [summary mask]
```

Procedure 4 Example

```
interface Tunnel10
 bandwidth 1500
 ip address 10.4.132.205 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco123
 ip nhrp map 10.4.132.1 172.16.130.1
 ip nhrp map multicast 172.16.130.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.132.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 ip summary-address eigrp 200 10.5.192.0 255.255.248.0
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC
 tunnel protection ipsec profile DMVPN-PROFILE
```

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.

```
router eigrp [as number (dmvpn)]
 network [mGRE tunnel network] [inverse mask]
 network [WAN remote range] [inverse mask]
 passive-interface default
 no passive-interface [mGRE tunnel interface]
 eigrp router-id [IP address of Loopback0]
 no auto-summary
```

Procedure 5 Example

```
router eigrp 200
 network 10.4.132.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.5.192.254
 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.

Procedure Steps:

1. Configure PIM on the DMVPN tunnel interface.
2. Enable PIM non-broadcast multiple access mode for the DMVPN tunnel.
3. Configure the DR priority for the DMVPN spoke router.

Step 1: Configure PIM on the DMVPN tunnel interface.

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

NOTE: Do not enable PIM on the Internet interface, as no multicast traffic should be requested from this interface.

```
interface [interface type] [number]
 ip pim sparse-mode
```

Step 2: Enable PIM non-broadcast multiple access 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.

Resolving the NBMA 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.

```
interface Tunnel [number]
 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 Tunnel [number]
 ip pim dr-priority 0
```

Procedure 6 Example

```
interface Tunnel10
 ip pim dr-priority 0
 ip pim nbma-mode
 ip pim sparse-mode
```

Process

Remote-Site DMVPN Spoke Router Configuration

This set of procedures is for the configuration of a DMVPN spoke router for a DMVPN remote site (single-router, single-link) and includes all required procedures.

This set of procedures should also be used when configuring a MPLS WAN + DMVPN remote site. Use these procedures when configuring the second router of the dual-router, dual-link design.

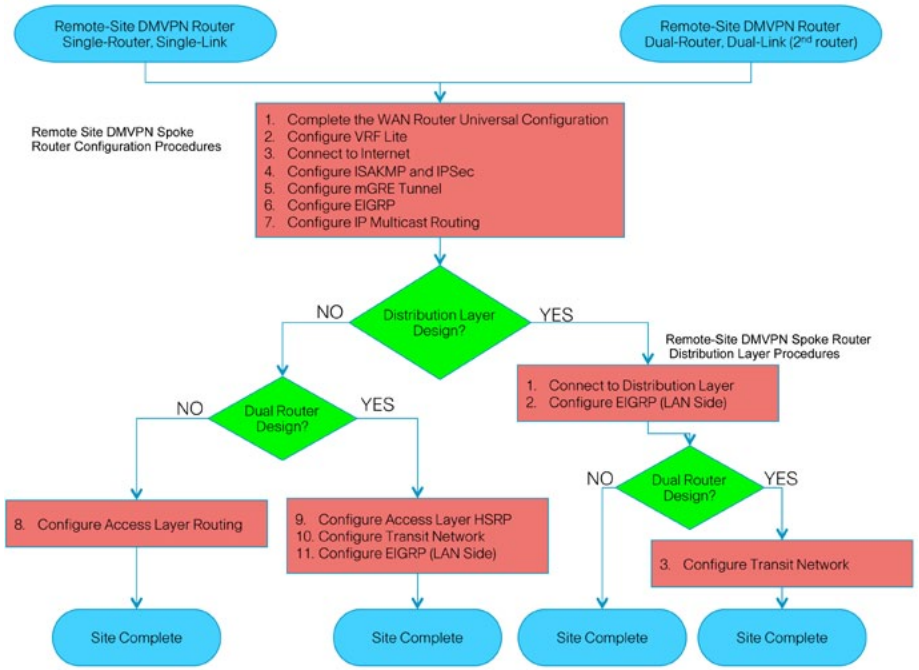
The flowchart in Figure 29 provides details on how to complete the configuration of a remote-site DMVPN spoke router.

1. Complete the 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 Routing

The following procedures are only relevant for the dual-router design:

9. Configure Access Layer HSRP
10. Configure the Transit Network
11. Configure EIGRP (LAN Side)

Figure 29. Remote-Site DMVPN Spoke Router Configuration Flowchart



Procedure 1 Finish WAN Router Universal Configuration

Procedure Steps:

1. Configure the device hostname.
2. Configure in-band management.
3. Configure device-management protocols.
4. Configure secure user authentication.
5. Configure a synchronized clock

Step 1: Configure the device hostname.

```
hostname [hostname]
```

Step 2: Configure in-band management interface.

All devices leverage a loopback address. A loopback is a virtual interface that is consistently reachable when multiple paths exist to the device. Various other features may use the loopback.

```
interface Loopback0
 ip address [IP address] 255.255.255.255
```

Step 3: Configure device-management protocols.

SSH is an application and a protocol that provides a secure replacement to RSH and Telnet. Secure management access is enabled through the use of the SSH and/or HTTPS protocols. HTTPS provides the capability to connect a HTTP server securely. It uses SSL and TLS to provide device authentication and data encryption. Both protocols are encrypted for privacy and the non-secure protocols, Telnet and HTTP, have been disabled.

```
ip domain-name cisco.local
no ip http server
```

Enabling SSH requires that a public/private keypair be generated for the device:

```
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh source-interface Loopback0
```

Various levels of device management may be available through a web interface. For secure access to this interface you must enable the secure server (the following command also generates a public/private keypair as shown previously):

```
ip http secure-server
```

Allow only SSH access to the device:

```
line vty 0 15
 transport input ssh
```

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. This command is also useful for allowing you to continue typing at the device console when debugging is enabled.

```
line con 0
 logging synchronous
```

SNMP is enabled to allow the network infrastructure devices to be managed by a 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
snmp-server trap-source Loopback0
```

Step 4: Configure secure user authentication.

AAA is enabled for access control. All management access to the network infrastructure devices (SSH, Telnet, HTTP, and HTTPS) is controlled with AAA. A local AAA user database is defined on the network infrastructure devices to provide the ability to manage them in case the centralized RADIUS server is unavailable, or if you do not have a RADIUS server in your agency. We highly recommend the use of a centralized authentication database.

```
enable secret c1sco123
service password-encryption
!
username admin password c1sco123
aaa new-model
aaa authentication login default group radius local
ip radius source-interface Loopback0
radius-server host 10.4.200.15 key SecretKey
```

Step 5: Configure a synchronized clock.

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 network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

Network devices should be programmed 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. Configuring console messages, logs, and debug output on switches, routers, and other devices in the network to provide timestamps on output allows cross-referencing of events in a network.

```
ntp server 10.4.200.17
ntp source Loopback0
ntp update-calendar    ! this command not for use on ASR1000
Series
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Procedure 2 Configure VRF Lite

An Internet-facing VRF is created to support Front Door VRF for DMVPN. The VRF name is arbitrary, but it is useful to select a name that describes the VRF. An associated route distinguisher (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.

Command Reference:

An RD is either of the following:

- ASN-related—Composed of an ASN and an arbitrary number.
- 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.

```
ip vrf [vrf-name]
 rd [ASN:number]
```

Procedure 2 Example

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

Procedure 3 Connect to the Internet

The remote sites using DMVPN can use either static or dynamically assigned IP addresses. The design has been tested 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. Since 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.

Procedure Steps:

1. Administratively enable the interface, select VRF, and enable DHCP.
2. Configure and apply the access list.

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

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

```
interface [interface type] [number]
 ip vrf forwarding [vrf name]
 ip address dhcp
 no shutdown
```

Step 2: Configure and apply the access list.

The IP access list must permit the protocols specified in Table 19. The access list is applied inbound on the WAN interface, so filtering is done on traffic
destined to the router.

Table 19. 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 [interface type] [number]
 ip access-group [ACL name] in
ip access-list extended [ACL name]
 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 Table 20 may assist in troubleshooting, but are not explicitly required to allow DMVPN to function properly.

Table 20. 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 3 Example

```
interface GigabitEthernet0/0
 ip vrf forwarding INET-PUBLIC
 ip address dhcp
 ip access-group ACL-INET-PUBLIC in
 no shutdown

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 icmp any any echo
 permit icmp any any echo-reply
 permit udp any any eq bootpc
```

Procedure 4 Configure ISAKMP and IPsec

Procedure Steps:

1. Configure the crypto keyring.
2. Configure the ISAKMP policy and dead peer detection.
3. Create the ISAKMP profile.
4. Define the IPsec transform set.
5. Create the IPsec profile.

Step 1: Configure the crypto keyring.

The crypto keyring defines a pre-shared key (or password) valid for IP sources reachable within a particular VRF. This key is a wildcard pre-shared key 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 [keyring name] vrf [vrf name]
  pre-shared-key address 0.0.0.0 0.0.0.0 key [pre-shared key]
```

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 pre-shared key
- Diffie-Hellman group: 2

DPD is enabled with keepalives 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 [ISAKMP profile name]
   keyring [keyring name]
   match identity address 0.0.0.0 [vrf name]
```

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, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set [IPSec transform-set name] 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 [IPSec profile name]
 set transform-set [IPSec transform-set name]
 set isakmp-profile [ISAKMP profile name]
```

Procedure 4 Example

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

crypto isakmp policy 10
 encr aes 256
 hash sha
 authentication pre-share
 group 2

crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC
   keyring DMVPN-KEYRING
   match identity address 0.0.0.0 INET-PUBLIC

crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC
```

Procedure 5 Configure the mGRE Tunnel

Procedure Steps:

1. Configure basic interface settings.
2. Configure the tunnel.
3. Configure NHRP.
4. Configure EIGRP.

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.

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 Tunnel [number]
 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 Procedure 3 to connect to the Internet. The tunnel vrf command should be set to the VRF defined previously for Front Door VRF.

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

```
interface Tunnel [number]
 tunnel source [source interface]
 tunnel mode gre multipoint
 tunnel vrf [vrf name]
 tunnel protection ipsec profile [IPSec profile name]
```

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 6) relies on a multicast transport. Spoke routers require the NHRP static multicast mapping.

The value used 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 Table 21.

Table 21. DMVPN Hub IP Address Information

DMVPN Hub Public Address (actual)	DMVPN Hub Public Address (externally routable after NAT)	NHS (DMVPN Hub mGRE Tunnel Address)
10.4.128.133	172.16.130.1	10.4.132.1

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 existing cache entries to be overwritten. 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 Tunnel [number]
 ip nhrp authentication [password]
 ip nhrp map [NHS IP address] [DMVPN hub outside IP address]
 ip nhrp map multicast [DMVPN hub outside IP address]
 ip nhrp network-id [network id]
 ip nhrp holdtime 600
 ip nhrp nhs [NHS IP address]
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
```

Step 4: Configure EIGRP.

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 can not be summarized, then EIGRP continues to advertise the specific routes

```
interface Tunnel [number]
 ip summary-address eigrp [as number (dmvpn)] [summary
network] [summary mask]
```

Procedure 5 Example

```
interface Tunnel10
 bandwidth 1500
 ip address 10.4.132.203 255.255.254.0
```

```
no ip redirects
ip mtu 1400
ip nhrp authentication cisco123
ip nhrp map 10.4.132.1 172.16.130.1
ip nhrp map multicast 172.16.130.1
ip nhrp network-id 101
ip nhrp holdtime 600
ip nhrp nhs 10.4.132.1
ip nhrp registration no-unique
ip nhrp shortcut
ip tcp adjust-mss 1360
ip summary-address eigrp 200 10.5.48.0 255.255.248.0
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel vrf INET-PUBLIC
tunnel protection ipsec profile DMVPN-PROFILE
```

Procedure 6 Configure EIGRP

A single EIGRP process is run 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.

```
router eigrp [as number (dmvpn)]
 network [mGRE tunnel network] [inverse mask]
 network [WAN remote range] [inverse mask]
 passive-interface default
 no passive-interface [mGRE tunnel interface]
 eigrp router-id [IP address of Loopback0]
 no auto-summary
```

Procedure 6 Example

```
router eigrp 200
 network 10.4.132.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.5.48.253
 no auto-summary
```

Procedure 7 Configure IP Multicast Routing

This procedure applies to all DMVPN spoke routers.

Procedure Steps:

1. Enable IP multicast routing.
2. Configure PIM, RP and scoping.
3. Enable PIM non-broadcast multiple access mode for DMVPN tunnel.
4. Configure the DR priority for the DMVPN spoke router.

Step 1: Enable IP multicast routing.

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

```
ip multicast-routing
```

Step 2: Configure PIM, RP and scoping.

Every Layer 3 switch and router must be configured with the address of the IP multicast RP. Use the `rp-address` command in conjunction with an access-list to limit the network size that the RP is responsible for. This configuration provides for future scaling and control of the IP multicast environment and can change based on network needs and design. The PIM source is configured to be the device loopback for resiliency at sites with multiple WAN transports.

```
ip pim rp-address [IP address of RP] [ACL number]
ip pim register-source Loopback0
access-list [ACL number] permit [multicast group scope] [inverse mask]
```

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

NOTE: Do not enable PIM on the Internet interface, as no multicast traffic should be requested from this interface.

```
interface [interface type] [number]
 ip pim sparse-mode
```

Step 3: Enable PIM non-broadcast multiple access 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.

Resolving the NBMA 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.

```
interface Tunnel [number]
 ip pim nbma-mode
```

Step 4: 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. This can be prevented by setting the DR priority to 0 for the spokes.

```
interface Tunnel [number]
 ip pim dr-priority 0
```

Procedure 7 Example

```
ip multicast-routing
!
interface Loopback0
 ip pim sparse-mode
!
interface GigabitEthernet0/2.64
 ip pim sparse-mode
!
interface Tunnel10
 ip pim dr-priority 0
 ip pim nbma-mode
 ip pim sparse-mode
!
ip pim rp-address 10.4.60.252 10
ip pim register-source Loopback0
access-list 10 permit 239.1.0.0 0.0.255.255
```

Procedure 8 Configure Access Layer Routing

Procedure Steps:

1. Enable the physical interface.
2. Create subinterfaces and assign VLAN tags.
3. Configure IP settings for each subinterface.

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 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 [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.

If the Remote-site DMVPN spoke router is the second router of a dual-router design, then HSRP is configured at the access layer. This requires a modified IP configuration on each subinterface. For the modified procedure, you should skip to Procedure 9 after completing Steps 1 and 2.

```
interface [interface type] [number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [LAN network 1] LAN network 1 netmask]
```

```
ip helper-address [IP address of DHCP server]
```

Procedure 8 Example

```
interface GigabitEthernet0/2
 no ip address
 no shutdown
 !
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.52.1 255.255.255.0
 ip helper-address 10.4.200.10
 ip pim sparse-mode
!
interface GigabitEthernet0/2.65
 description WirelessData
 encapsulation dot1Q 65
 ip address 10.5.50.1 255.255.255.0
 ip helper-address 10.4.200.10
 ip pim sparse-mode
!
interface GigabitEthernet0/2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.53.1 255.255.255.0
 ip helper-address 10.4.200.10
 ip pim sparse-mode
!
interface GigabitEthernet0/2.70
 description WirelessVoice
 encapsulation dot1Q 70
 ip address 10.5.51.1 255.255.255.0
 ip helper-address 10.4.200.10
 ip pim sparse-mode
```

The following procedures (9–11) are only relevant for the dual-router design.

Procedure 9 Configure Access Layer HSRP

[Dual-Router Design Only]

HSRP is configured to enable the use of a VIP to be used as a default gateway that is shared between two routers. The HSRP active router is the MPLS CE router and the HSRP standby router is the DMVPN spoke router. Configure the DMVPN spoke router with a standby priority that is less than the MPLS CE 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 router, 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 Table 22.

Table 22. WAN Remote-Site HSRP Parameters (Dual Router)

Router	HSRP Role	Virtual IP Address (VIP)	Real IP Address	HSRP Priority	PIM DR Priority
MPLS CE	Active	.1	.2	110	110
DMVPN Spoke	Standby	.1	.3	105	105

The IP addresses assigned override those configured with the previous Procedure 8, so that 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 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.

Note that the HSRP priority and PIM DR priority are shown in Table 22 to be the same value; however, there is no requirement that these values must be identical.

This procedure should be repeated 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 [IP address of DHCP server]
 ip pim sparse-mode
 ip pim dr-priority [PIM DR priority]
 standby [number] ip [LAN network 1 gateway address] [LAN
network 1 netmask]
 standby [number] priority [priority]
 standby [number] preempt
```

Procedure 9 Example—DMVPN Spoke Router

```
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.52.3 255.255.255.0
 ip helper-address 10.4.200.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby 1 ip 10.5.52.1
 standby 1 priority 105
 standby 1 preempt
```

Procedure 10 Configure Transit Network

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

Procedure 10 Example—DMVPN Spoke Router

```
interface GigabitEthernet0/2.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.48.2 255.255.255.252
```

Procedure 11 Configure EIGRP (LAN Side)

[Dual-Router Design Only]

A routing protocol must be configured between the two routers to ensure that the HSRP active router has full reachability information for all WAN remote sites.

Procedure Steps:

1. Enable EIGRP-100.
2. Redistribute EIGRP-200 (DMVPN) into EIGRP-100.

Step 1: Enable EIGRP-100.

EIGRP-100 is configured 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 mGRE tunnel interface as an EIGRP interface for this EIGRP process.

```
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: 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 [as number]
 redistribute eigrp [as number (DMVPN)]
```

Procedure 11 Example—DMVPN Spoke Router

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 redistribute eigrp 200
 passive-interface default
 no passive-interface GigabitEthernet0/1.99
 eigrp router-id 10.5.48.253
 no auto-summary
```

Deploying a WAN Remote-Site Distribution Layer

This set of procedures is for the configuration of a MPLS CE router for a MPLS WAN remote site (single-router, single-link) and includes all required procedures to connect to a distribution layer.

This set of procedures should also be used for a 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. These procedures should also be used when 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 the MPLS CE Router to the Distribution Layer
2. Configure EIGRP (LAN side)

The following procedure is only relevant for the dual-router design

3. Configure the Transit Network

Procedure 1 Connect MPLS CE Router to Distribution Layer

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.

Procedure Steps:

1. Configure the port-channel interface.
2. Configure the port-channel subinterfaces and assign IP addresses.
3. Administratively enable the port channel group members and assign the appropriate channel group.

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 the physical interface has been enabled, then the appropriate subinterfaces can be mapped 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 EtherChannel is configured statically .

```
interface [interface type] [number]
 no ip address
 channel-group [number]
 no shutdown
```

Procedure 1 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)

A routing protocol must be configured between the router and distribution layer.

Procedure Steps:

1. Enable EIGRP-100.
2. Redistribute BGP into EIGRP-100.

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: Redistribute BGP into EIGRP-100.

This step should only be completed on a MPLS CE router

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

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.

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

Procedure 2 Example—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-channel1.50
 eigrp router-id 10.5.48.254
 no auto-summary
```

Procedure 3 Configure the Transit Network

[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 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]
```

Procedure 3 Example—MPLS CE Router

```
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 DMVPN Spoke Router Distribution Layer

1. Connect the DMVPN Spoke Router to the Distribution Layer
2. Configure EIGRP (LAN side)

The following procedure is only relevant for the dual-router design

3. Configure the Transit Network

This set of procedures is for the configuration of a DMVPN spoke router for a DMVPN remote site (single-router, single-link) and includes all required procedures to connect to a distribution layer.

This set of procedures should also be used for 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 to Distribution Layer

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.

Procedure Steps:

1. Configure the port-channel interface.
2. Configure the port-channel subinterfaces and assign IP addresses.
3. Administratively enable the port-channel group members and assign the appropriate channel group.

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.

Once the physical interface has been enabled, then the appropriate subinterfaces can be mapped 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
```

Procedure 1 Example

```
interface Port-channel2
 no ip address

interface Port-channel2.54
 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)

A routing protocol must be configured between the router and distribution layer.

Procedure Steps:

1. Enable EIGRP-100.
2. Redistribute EIGRP-200 (DMVPN) into EIGRP-100.

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: 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. Because the routing protocol is the same, no default metric is required.

```
router eigrp [as number]
 redistribute eigrp [as number (DMVPN)]
```

Procedure 2 Example—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

[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 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]
```

Procedure 3 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. Complete the Distribution Layer Switch Universal Configuration
2. Connect to the WAN Routers
3. Configure EIGRP
4. Configure the Transit Network VLAN

Procedure 1 Finish Dist. Layer 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. Full details on distribution layer switch configuration are included in the *Cisco SBA for Large Agencies—Borderless Networks LAN Deployment Guide*.

Procedure 2 Connect to the WAN Routers

The port-channel interface(s) 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.

Procedure Steps:

1. Create the VLAN for the router link on the switch, create the VLAN interface and assign the IP address.
2. Configure the port-channel interface and configure for 802.1Q VLAN trunking.
3. Administratively enable the port-channel group members and assign the appropriate channel group. Configure for 802.1 VLAN trunking.

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]
```

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 802.1 VLAN trunking.

Not all router platforms can support LACP to negotiate with the switch, so EtherChannel is configured 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
```

Procedure 2 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
```

Procedure 3 EIGRP Configuration

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 auto summarization 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 sub-second 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 sub-second 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.

The distribution layer switch must be configured to enable Nonstop Forwarding 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
```

Procedure 3 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
```

Procedure 4 Configure Transit Network VLAN

[Dual-Router Design Only]

The transit network is configured between the two routers; however, a physical link between the routers is not required. Instead a transit VLAN is used. 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.

Procedure Steps:

1. Create the transit VLAN on the switch.
2. Add the transit VLAN to the existing port-channel trunk interface and channel group members.

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]
```

Procedure 4 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
```

Process

QoS Configuration

1. Create the WAN QoS Class Maps to Classify Traffic Types
2. Create the Policy Map to Mark BGP Traffic
3. Add DMVPN ISAKMP Traffic to NETWORK-CRITICAL Class of Service
4. Define the Policy Map to Implement the Queuing Policy
5. Configure Physical Interface Shaping and Queuing Policy
6. Apply the WAN QoS Policy to a Physical interface

When configuring the WAN-edge QoS, you are defining how traffic will egress your network. It is critical that the classification, marking, and bandwidth allocations align to the service provider offering in order to ensure consistent QoS treatment end to end.

Procedure 1 Create the QoS Maps to Classify Traffic

This procedure applies to all WAN routers.

Procedure Steps:

1. Create the class maps for DSCP matching.
2. Create a class map for BGP protocol matching.

The `class-map` command is used 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 wish 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. Two forms of the `match` command are used: `match dscp` and `match protocol`.

The following steps are used to configure the required WAN class-maps and matching criteria.

Step 1: Create the class maps for DSCP matching.

This step will be repeated to create a class-map for each of the six WAN classes of service listed in Table 23.

You do not need to explicitly configure the default class.

```
class-map match-any [class-map name]
match ip dscp [dcsp value] [optional additional dscp value(s)]
```

Table 23. QoS Classes of Service

Class of Service	Traffic type	DSCP Value(s)	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. Network Based Application Recognition (NBAR) is used 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]
```

Procedure 1 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 ip dscp af21

class-map match-any SCAVENGER
match ip dscp af11 cs1

class-map match-any NETWORK-CRITICAL
match ip dscp cs6 cs2

class-map match-any BGP
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 is using 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 [policy-map name]
class [class-map name to match]
set dscp [dcsp value]
```

Procedure 2 Example

```
policy-map MARK-BGP
class BGP
set dscp cs6
```

Procedure 3 Add DMVPN ISAKMP Traffic to NETWORK

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.

Procedure steps:

1. Create the access-list.
2. Add the match criteria to the existing NETWORK-CRITICAL class-map.

Step 1: Create the access-list.

```
ip access-list extended [name]
  permit [protocol] [source] eq [port] [destination] eq [port]
```

Step 2: Add the match criteria to the existing NETWORK-CRITICAL class-map.

```
class-map match-any [class-map name]
match access-group name [name]
```

Procedure 3 Example

```
ip access-list extended ISAKMP
 permit udp any eq isakmp any eq isakmp

class-map match-any NETWORK-CRITICAL
match access-group name ISAKMP
```

Procedure 4 Define Policy Map to use the 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.

Tech Tip

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.

Procedure Steps:

1. Create the parent policy map.
2. Apply the previously created class-map.
3. Assign the maximum guaranteed bandwidth for the class (optional).
4. Define the priority queue for the class (optional).
5. Apply the child service policy (optional).
6. Define the congestion mechanism (optional).

Step 1: Create the parent policy map.

```
policy-map [policy-map-name]
```

Steps 2–6 are repeated for each class in Table 23 including class-default.

Step 2: Apply the previously created class-map.

```
class [class-name]
```

Step 3: Assign the maximum guaranteed bandwidth for the class.

This is an optional step.

```
bandwidth percent [percentage]
```

Step 4: Define the priority queue for the class.

This is an optional step.

```
priority percent [percentage]
```

Step 5: 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: Define the congestion mechanism.

This is an optional step.

```
random-detect [type]
```

Procedure 4 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

While 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 agency 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, shaping needs to be configured on the physical interface. This shaping is accomplished with a QoS service policy. A QoS service policy is configured 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 configuring the `shape average` command, ensure the value matches the contracted bandwidth rate from your service provider.

This procedure applies to all WAN routers. This procedure may be repeated multiple times to support devices that have multiple WAN connections attached to different interfaces.

Procedure Steps:

1. Create the parent policy map.
2. Configure the shaper.
3. Apply the child service policy.

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]
```

Procedure 5 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 WAN QoS Policy to a Physical Interface

To invoke shaping and queuing on a physical interface, you must apply the parent policy configured in the previous procedure.

This procedure applies to all WAN routers. This procedure may be repeated multiple times to support devices that have multiple WAN connections attached to different interfaces.

Procedure Steps:

1. Select the WAN interface.
2. Apply the WAN QoS policy.

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]
```

Procedure 6 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

Application Optimization Agency 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 have the number of remote sites 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 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 agency data assets.

Consolidating data centers while growing the remote-site population means that increasing numbers of remote employees access LAN-based agency 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 agency'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.

Application Optimization Technical Overview

WAN Aggregation

The WAN-aggregation site uses a cluster of two or more WAE devices to provide WAAS capabilities as shown in Figure 30. 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 Table 24. The fan-out numbers correspond to the total number of remote-peer WAE devices.

Table 24. WAN-Aggregation WAE Options

Device	Max Optimized TCP Connections	Max Recommended WAN Link [Mbps]	Max Optimized Throughput [Mbps]	Max Core Fan-out [Peers]
WAVE-574-3GB	00750	0008	0100	0035
WAVE-574-6GB	01300	0020	0150	0070
WAE-674-4GB	02000	0045	0250	0100
WAE-674-8GB	06000	0090	0350	0200
WAE-674-8GB-VB	04000	0090	0350	0200
WAE-7341	12000	0310	1000	1400
WAE-7371	50000	1000	2500	2800

A more comprehensive, interactive WAAS sizing tool is available for registered users of cisco.com: 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).

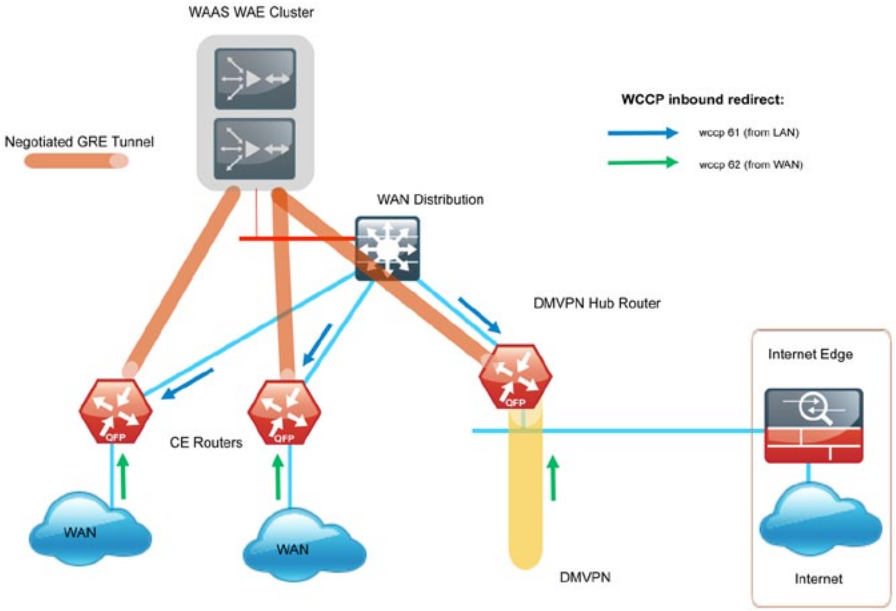
WCCP is enabled on the MPLS CE and DMVPN routers. The WCCP redirect uses service groups 61 and 62 to match traffic for redirection. These service groups must be used in pairs.

- 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.

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 (non-redundant) 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.

There are many factors to consider in the selection of the WAN remote-site WAE devices. 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 Table 25. The optimized throughput numbers correspond to the apparent bandwidth available after successfully optimization by WAAS.

Table 25. WAN Remote-Site WAE Options

Device	Max Optimized TCP Connections	Max Recommended WAN Link [Mbps]	Max Optimized Throughput [Mbps]
NME-WAE-302	250	4	90
NME-WAE-502	400	4	150
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-274	200	2	90
WAVE-474	400	4	90
WAVE-574-3GB	750	8	100
WAVE-574-6GB	1300	20	150
WAE-674-4GB	2000	45	250
WAE-674-8GB	6000	90	350
WAE-674-8GB-VB	4000	90	350
WAE-7341	12000	310	1000
WAE-7371	50000	1000	2500

A more comprehensive, interactive WAAS sizing tool is available for registered users of cisco.com: http://tools.cisco.com/WAAS/sizing

The WAE form factors previously discussed include a router enhanced network module (NME), a router Service 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.

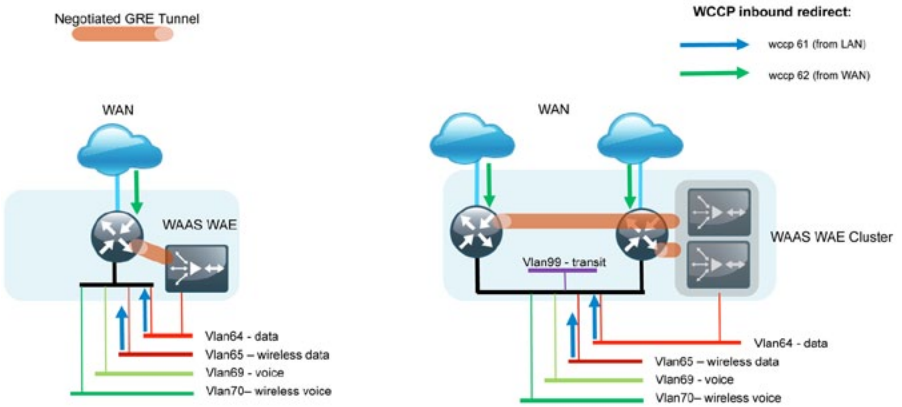
- NME: One internal interface (router connect only), one external interface
- SRE: One internal interface (router connect only), one external interface
- Appliance: Two interfaces (both external)

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, NME, and appliance devices can use an identical design. The internal interfaces of the NME and SRE are not used for this design, except for the initial bootstrapping of the device configurations.

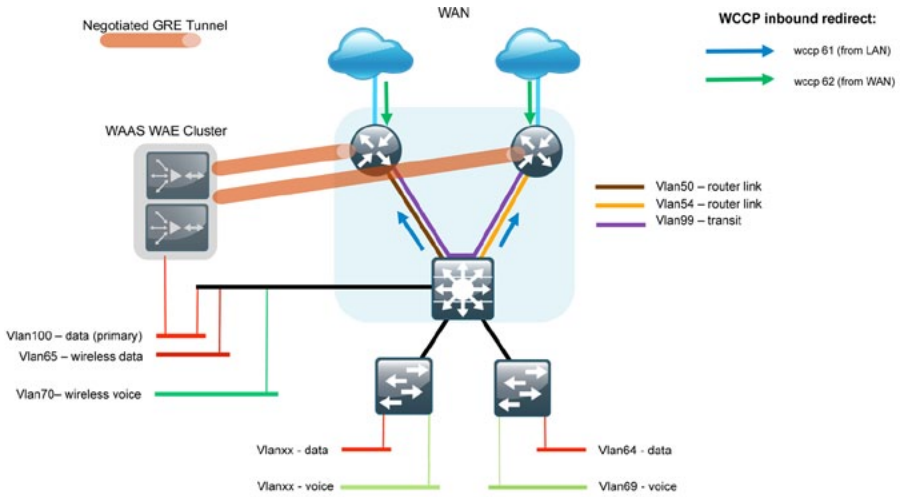
NOTE: You must connect an external Ethernet cable from each NME or SRE module for this solution.

Figure 31. WAN Remote Site—WAAS Topology (Access Layer Connection)



The WAE device(s) should connect to the data VLAN of the access switch in all flat Layer 2 designs as shown in Figure 31. When the deployment uses a distribution-layer design, the WAE device(s) should connect to the primary data VLAN on the distribution switch as shown in Figure 32.

Figure 32. WAN Remote Site—WAAS Topology (Distribution Layer Connection)



The WAE appliance(s) should be connected, where possible, 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.

Process

WAAS/WAE Configuration

The following steps provide an overview of the tasks required to configure a basic WAAS environment.

1. Configure the WAAS Central Manager
2. Configure Switch for WAE Appliances
3. Configure the WAE Appliance Devices
4. Configure the WAE SRE and NME Devices
5. Configure Remote Switch for WAE Devices
6. Configure WCCPv2 on Routers

Procedure 1 Configure the WAAS Central Manager

A Cisco WAVE-574 device is used 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]:
10.4.200.100/24
Enter Default Gateway IP Address [Not configured]: 10.4.200.1
```

Step 5: Configure DNS, host, and NTP settings.

```
Enter Domain Name Server IP Address [Not configured]:
10.4.200.10
Enter Domain Name(s) (Not configured): cisco.local
Enter Host Name (None): bn-waas-wcm-1
Enter NTP Server IP Address [None]: 10.4.200.17
```

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               10.4.200.100
```

```
 7.     IP Network Mask          255.255.255.0
 8.  IP Default Gateway         10.4.200.1
 9.  DNS IP Address             10.4.200.10
10.  Domain Name(s)             cisco.local
11.  Host Name                  bn-waas-wcm-1
12.  NTP Server Address         10.4.200.17
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.

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
```

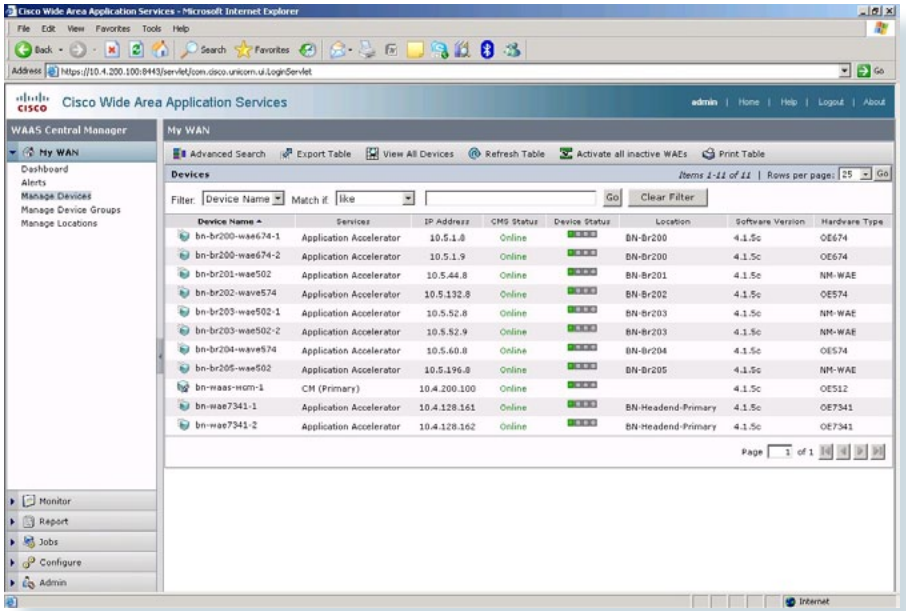
Step 9: Save the configuration.

After making configuration changes through the console, save the configuration.

```
copy running-config startup-config
```

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 hostname if it has been configured in DNS. Specify secure HTTP and the port number 8443 to access the Central Manager, for example https://10.4.200.100:8443. Login using the default username of admin and password of default. Choosing **My WAN -> Manage Devices** from the panel on the left should display a screen showing the Central Manager initially as the only managed device.



Procedure 2 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 Large Agencies—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.

Procedure Steps:

1. On the WAN distribution switch, create the VLAN and SVI.
2. On the WAN distribution switch, configure Layer 2 EtherChannel links for the devices and associate them with the VLAN.

Step 1: Create the VLAN and SVI.

```
vlan [VLAN number]
 name [VLAN name]

interface Vlan [VLAN number]
 ip address [IP address] [netmask]
```

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 GigabitEthernet1/0/2
 switchport access vlan [VLAN number]
 channel-group [number] mode on
 no shutdown
!
```

Procedure 3 Example

```
vlan 350
 name WAN_Service_Net-10.4.128.128

interface Port-channel7
 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 10.4.128.129 255.255.255.192
```

Procedure 3 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. These device are connected directly to the WAN distribution-layer switch, leveraging GRE-negotiated return to communicate with the WCCP routers.

WAE appliances may also be deployed at WAN remote sites, either individually or as part of a WAE cluster. This procedure should be used for configure WAN remote-site WAE appliances.

The same setup utility used in the initial configuration of the WAAS Central Manager is used for the setup of the WAE appliance devices. These devices only require basic setup through their console port to assign initial settings; after you complete this setup, all management of the WAAS network can be performed through the graphical interface of the WAAS Central Manager system.

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 username 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]:
10.4.128.161/29
Enter Default Gateway IP Address [Not configured]: 10.4.128.129
Enter Central Manager IP Address (WARNING: An invalid entry
will cause SETUP to take a long time when applying WAAS
configuration) [None]: 10.4.200.100
```

Step 6: Configure DNS, host, and NTP settings.

```
Enter Domain Name Server IP Address [Not configured]:
10.4.200.10
Enter Domain Name(s) (Not configured): cisco.local
Enter Host Name (None): bn-wae7341-1
Enter NTP Server IP Address [None]: 10.4.200.17
```

Step 7: Configure WCCP router list.

```
Enter WCCP Router (max 4) IP Address list (ip1 ip2 ...) []:
10.4.128.241 10.4.128.242 10.4.128.243
```

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              10.4.128.161
 8.     IP Network Mask         255.255.255.248
 9. IP Default Gateway       10.4.128.129
10. CM IP Address            10.4.200.100
11. DNS IP Address           10.4.200.10
12. Domain Name(s)           cisco.local
13. Host Name                bn-wae7341-1
14. NTP Server Address       10.4.200.17
15. WCCP Router List         10.4.128.241 10.4.128.242
10.4.128.243
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: Configure port-channel connection for WAE to connect to the distribution switch stack.

This is an optional step only required when connecting the WAE using a port channel for a resilient connection.

```
interface GigabitEthernet 1/0
no ip address 10.4.128.161 255.255.255.192
exit
!
primary-interface PortChannel 1
!
interface PortChannel 1
 ip address 10.4.128.161 255.255.255.192
 exit
!
!
interface GigabitEthernet 1/0
 channel-group 1
 exit
interface GigabitEthernet 2/0
 channel-group 1
 exit
```

Step 12: 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 10.4.200.100
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 setting are configured in Steps 13 through 15.

Step 13: Configure GRE negotiated return.

All WAE devices use GRE-negotiated return with their respective WCCP router(s):

```
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:

```
bn-wae-7341-1# show running-config | include wccp router-list
wccp router-list 8 10.4.128.241 10.4.128.242 10.4.128.243
```

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 10.4.128.241 10.4.128.242 10.4.128.243
wccp router-list 1 10.4.128.241 10.4.128.242 10.4.128.243
```

This design uses authentication between the routers and WAE. 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
```

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: Save the configuration.

After making configuration changes through the console, save the configuration.

```
copy running-config startup-config
```

Procedure 4 Configure the WAE SRE and NME Devices

The remote-site WAAS equipment in this design can be a variety of WAE appliances, SRE, or NME-WAE form-factors, depending on the performance requirements. If you are configuring a WAE appliance, use Procedure 3.

The SRE and NME-WAE modules can be inserted directly into a corresponding module slot in the remote-site router and are configured somewhat differently from the appliances. If you are using an appliance, then you can follow the WAN-Aggregation WAE Device set of procedures.

Although the remote-site router can potentially communicate directly with the SRE or NME-WAE using the router backplane, this design leverages the external interfaces on the modules, which allows for a consistent design implementation regardless of the chosen WAE device. The Integrated-Service-Engine 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.

NOTE: 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 or NME IP addresses on the host router.

To permit console access to the SRE or NME modules, you must enter the following commands on the host router (this example shows a SRE service module).

```
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: 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, then you must first authenticate with a valid router login credential before logging into the WAE console session.

```
bn-br203-2921-1# service-module sm 1/0 session
```

Step 3: 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 4: Configure interception method.

```
1. WCCP
2. Other
Select Interception Method [1]: 1
```

Step 5: Configure time zone.

```
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)>
[UTC 0 0]: PST -8 0
```

Step 6: 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
```

NOTE: 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:

Enter Central Manager IP Address (WARNING: An invalid entry
will cause SETUP to take a long time when applying WAAS
configuration) [None]: 10.4.200.100
```

Step 7: Configure DNS, host, and NTP settings.

```
Enter Domain Name Server IP Address [Not configured]:
10.4.200.10
Enter Domain Name(s) (Not configured): cisco.local
Enter Host Name (None): bn-br203-wae-sre-1
Enter NTP Server IP Address [None]: 10.4.200.17
```

Step 8: Configure WCCP router list.

```
Enter WCCP Router (max 4) IP Address list (ip1 ip2 ...) []:
10.5.48.253 10.5.48.254
```

Step 9: 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 10: 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             10.4.200.100
 7. DNS IP Address            10.4.200.10
 8. Domain Name(s)            cisco.local
 9. Host Name                 bn-br203-wae-sre-1
10. NTP Server Address        10.4.200.17
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 ...
```

NOTE: 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.

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**.

Step 11: Configure GRE negotiated return.

All WAE devices use GRE-negotiated return with their respective WCCP router(s):

```
egress-method negotiated-return intercept-method wccp
```

Step 12: 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:

```
bn-br203-wae-sre-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 router-list-num 1 password c1sco123
```

Step 13: Enable SSH.

Enabling SSH requires the generation of the RSA key and enabling of the sshd service:

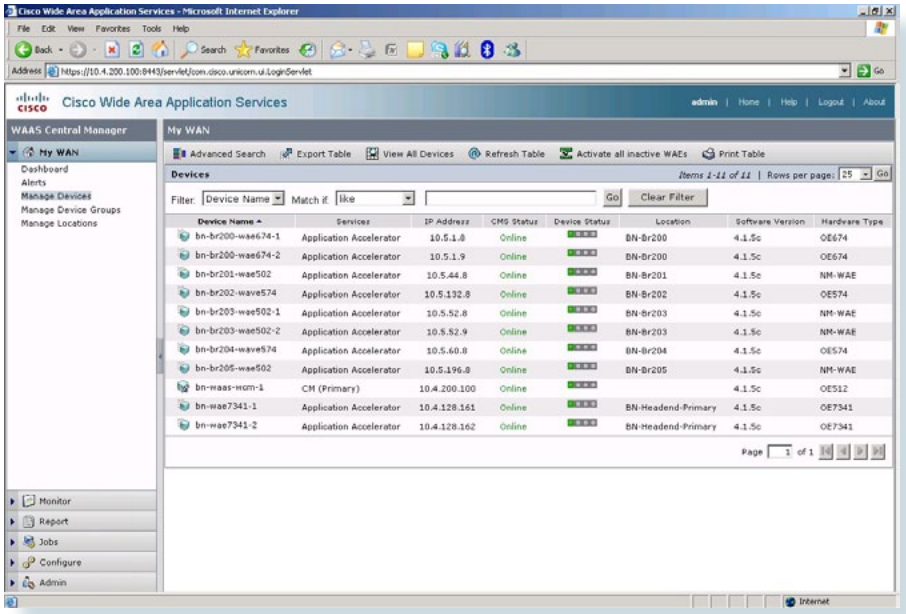
```
ssh-key-generate key-length 2048
sshd version 2
sshd enable
```

Step 14: Save the configuration.

After making configuration changes through the console, 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.



Procedure 5 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 Large Agencies—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.

Procedure Steps:

1. On the WAN distribution switch, create the VLAN and SVI.
2. On the WAN distribution switch, configure Layer 2 EtherChannel links for the devices and associate them with the VLAN.

Step 1: Create the VLAN and SVI (if necessary).

```
vlan [VLAN number]
 name [VLAN name]

interface Vlan [VLAN number]
 ip address [IP address] [netmask]
```

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 GigabitEthernet1/0/2
 switchport access vlan [VLAN number]
 channel-group [number] mode on
 no shutdown
!
interface GigabitEthernet2/0/2
 switchport access vlan [VLAN number]
 channel-group [number] mode on
 no shutdown
```

Procedure 5 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
```

Procedure 6 Configure WCCPv2 on Routers

WCCP is used in this design to divert 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.

Procedure Steps:

1. Configure global WCCP parameters and enable services 61 and 62.
2. Configure WCCP redirect on the LAN and WAN interfaces.

Step 1: Configure global WCCP parameters and enable services 61 and 62.

Services 61 and 62 must be enabled 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 redirect on the LAN and WAN interfaces.

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
```

Procedure 6 Example

```
ip wccp version 2
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list BN-WAE
password c1sco123
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list BN-WAE
password c1sco123
!
interface Port-channel1
 ip wccp 61 redirect in
!
interface GigabitEthernet0/0/4
 ip wccp 62 redirect in

ip access-list standard BN-WAE
 permit 10.4.128.161
 permit 10.4.128.162

ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Mgmt 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
```

Notes

Large Agencies WAN Deployment Product List

Functional Area	Product	Part Numbers	Software Version
WAN 500 Design			
WAN Aggregation: MPLS CE Router	ASR1002 Router	ASR1002 SASR1R1-AISK9-26SR ASR1002-PWR-AC ASR1000-ESP5	IOS XE 3.1.0S asr1000rp1-advipservicesk9.03.01.00.S.150-1.S.bin
WAN Aggregation: DMVPN Hub Router	ASR1002 Router	ASR1002 SASR1R1-AISK9-26SR FLASR1-IPSEC-RTU ASR1002-PWR-AC ASR1000-ESP5	IOS XE 3.1.0S asr1000rp1-advipservicesk9.03.01.00.S.150-1.S.bin
WAN Aggregation: WAAS Central Manager	WAVE-574 WAAS Appliance	WAVE-574-K9 WAAS-ENT-APL	4.2.1 (WAAS-UNIVERSAL-K9) Build b38 oe574-4.2.1.38
WAN Aggregation: WAAS Application Accelerator	WAE-7371-K9 WAAS Appliance	WAE-7371-K9 SF-WAAS-4.2-SAS-K9 WAAS-ENT-APL	4.2.1 (WAAS-UNIVERSAL-K9) Build b38 oe7371-4.2.1.38
WAN 100 Design			
WAN Aggregation: MPLS CE Router	Cisco3945E	CISCO3945E/K9 SL-39-DATA-K9 C3900-SPE250/K9 PWR-3900-AC	15.1(1)T c3900e-universalk9-mz.SPA.151-1.T.bin
WAN Aggregation: DMVPN Hub Router	Cisco3945E	CISCO3945E-SEC/K9 SL-39-DATA-K9 C3900-SPE250/K9 PWR-3900-AC	15.1(1)T c3900e-universalk9-mz.SPA.151-1.T.bin
WAN Aggregation: WAAS Central Manager	WAVE-574 WAAS Appliance	WAVE-574-K9 WAAS-ENT-APL	4.2.1 (WAAS-UNIVERSAL-K9) Build b38 oe574-4.2.1.38

Functional Area	Product	Part Numbers	Software Version
WAN Aggregation: WAAS Application Accelerator	WAE-7341-K9 WAAS Appliance	WAE-7341-K9 SF-WAAS-4.2-SAS-K9 WAAS-ENT-APL	4.2.1 (WAAS-UNIVERSAL-K9) Build b38 oe7341-4.2.1.38
WAN Remote Site Routers			
MPLS CE Router DMVPN Spoke Router	Cisco2911	CISCO2911-VSEC/K9 SL-29-DATA-K9 PWR-2911-AC	15.0(1)M2 c2900-universalk9-mz.SPA.150-1.M2.bin
MPLS CE Router DMVPN Spoke Router	Cisco2921	CISCO2921-VSEC/K9 SL-29-DATA-K9 PWR-2921-AC	15.0(1)M2 c2900-universalk9-mz.SPA.150-1.M2.bin
MPLS CE Router DMVPN Spoke Router	Cisco3925	C3925-VSEC/K9 SL-39-DATA-K9 PWR-3900-AC	15.0(1)M2 c3900-universalk9-mz.SPA.150-1.M2.bin
MPLS CE Router DMVPN Spoke Router	Cisco3945	C3945-VSEC/K9 SL-39-DATA-K9 PWR-3900-AC	15.0(1)M2 c3900-universalk9-mz.SPA.150-1.M2.bin
WAN Remote Site WAAS			
Application Accelerator Network Module for ISR-G2	NME-WAE-502	NME-WAE-502-K9 SM-NM-ADPTR WAAS-ENT-NM	4.2.1 (WAAS-UNIVERSAL-K9) Build b38 nme-wae-502-4.2.1.38
Application Accelerator Service Module for ISR-G2	SM-SRE-700-K9	SM-SRE-700-K9 WAAS-ENT-NM	4.2.1 (WAAS-UNIVERSAL-K9) Build b38 sm-wae-4.2.1.38
Application Accelerator WAVE-574 Appliance	WAVE-574	WAVE-574-K9 WAAS-ENT-APL	4.2.1 (WAAS-UNIVERSAL-K9) Build b38 oe574-4.2.1.38
Application Accelerator WAE-674 Appliance	WAE-674	WAE-674-K9 WAAS-ENT-APL	4.2.1 (WAAS-UNIVERSAL-K9) Build b38 oe674-4.2.1.38

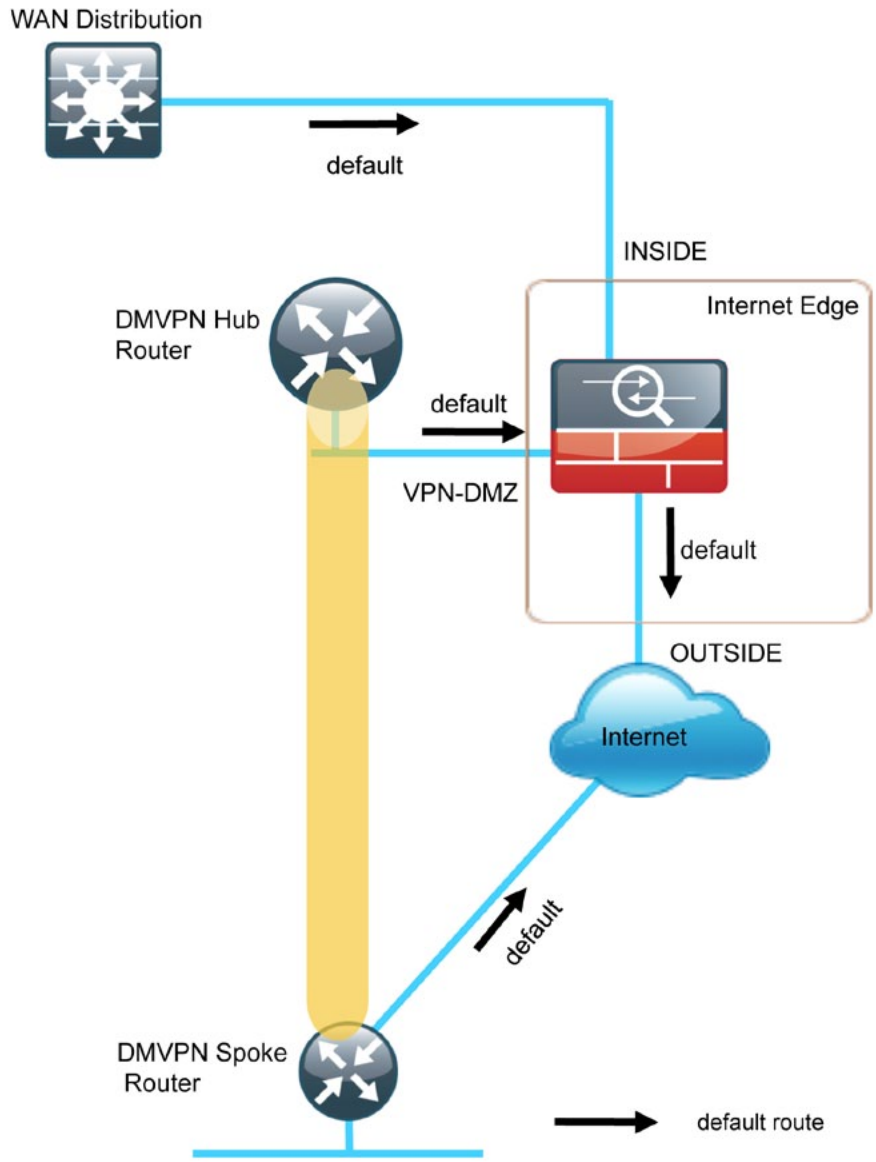
Functional Area	Product	Part Numbers	Software Version
LAN Switching			
Distribution Layer	Catalyst 3750G Stackable 12 Port SFP	WS-C3750G-12S-S Catalyst 3750 12 SFP + IPS Image CAB-STACK-50CM	12.2(53)SE1 c3750e-universalk9-mz.122-53.SE1.bin
Distribution Layer	Catalyst 4507RE Dual Supervisors Dual Power Supplies	WS-C4507R-E Catalyst 4500 E-Series 7-Slot Chassis WS-X45-SUP6-E Catalyst 4500 E-Series Sup 6-E, 2x10GE(X2) with Twin Gig WS-X4624-SFP-E Catalyst 4500 E-Series 24-Port GE (SFP) WS-X4606-X2-E Catalyst 4500 E-Series 6-Port 10GbE (X2)	12.2-53.SG1 cat4500e-entservicesk9-mz.122-53.SG1.bin
Distribution Layer	Catalyst 6500 VSS	WS-C6506-E Catalyst 6500 E-Series 6-Slot Chassis VS-S720-10G-3C Catalyst 6500 VSS Supervisor 720 with 2 ports 10GbE WS-X6724-SFP Catalyst 6500 24-port GigE Mod (SFP) WS-X6716-10G-3C Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3C (X2)	12.2(33) SXI3 with the IP Services Feature Set s72033-ipservicesk9_wan-mz.122-33.SXI3.bin

Appendix A: Technical Feature Supplement

Front Door VRF for DMVPN

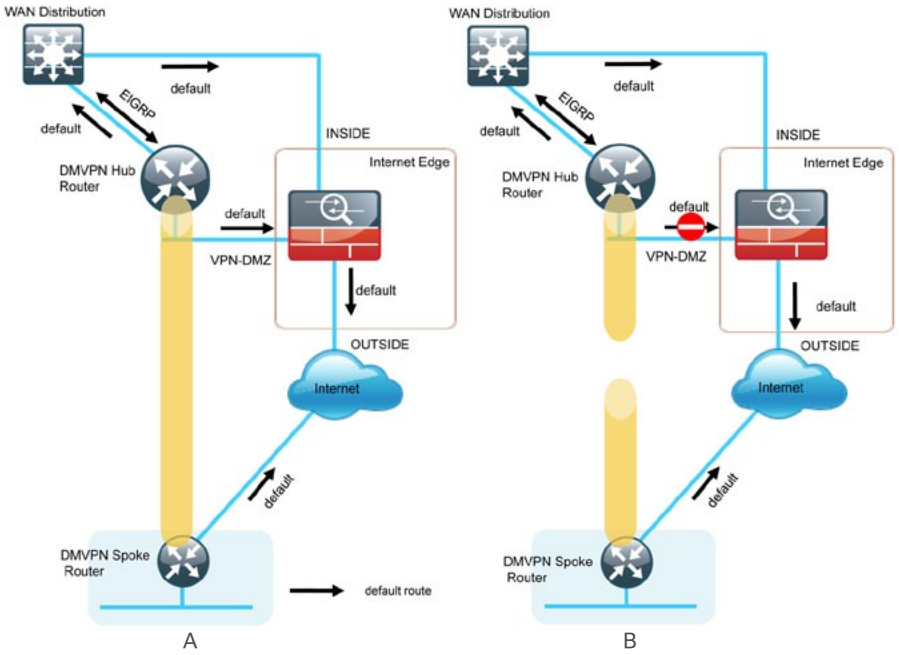
Building an IPsec tunnel requires reachability between the crypto routers. When you use the Internet, routers use a default route to contact their peers as shown in Figure 33.

Figure 33. IPsec Tunnel



If you need to extend the internal network (and the same default routing options that are available to internal users), then a default route must be advertised to the VPN hub router. See Figure 34A.

Figure 34. IPsec Tunnel Before/After Default Route Injection



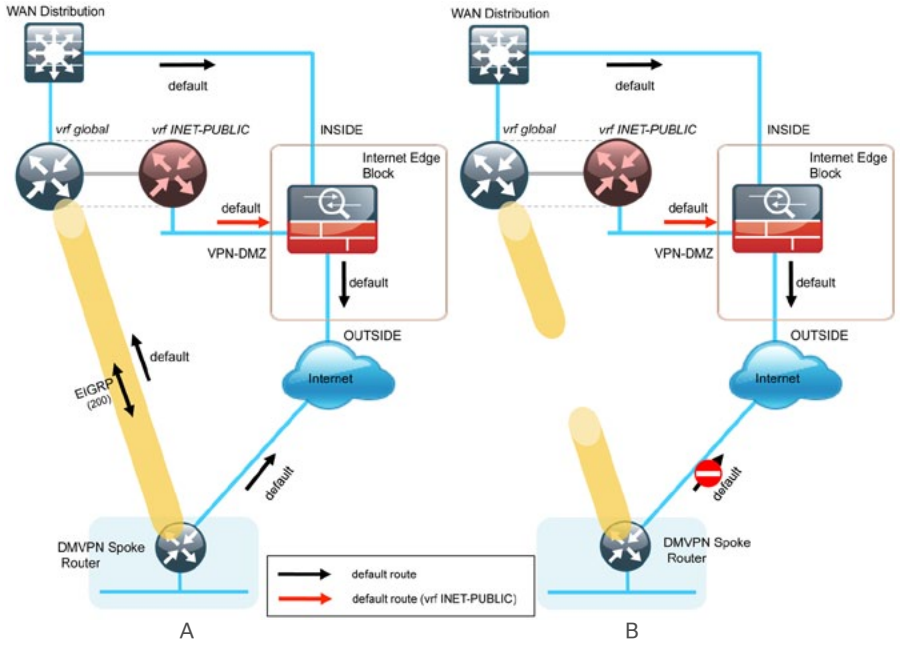
The advertisement of a default route to the hub router (with an existing default route) is problematic. This route requires a better administrative distance to become the active default, which then overrides the default route that is supporting the peer-peer IPsec tunnel connection. This routing advertisement breaks the tunnel as shown in Figure 34B.

Through the introduction of an external VRF INET-PUBLIC (shown in red), the hub router can support multiple default routes. The internal network remains in the global VRF. This is shown in Figure 35A.

Tech Tip

Most additional features on the hub router do not require VRF-awareness.

Figure 35. IPsec Tunnel with F-VRF Aggregation



This configuration is referred to as Front Door VRF (F-VRF), because the Internet is contained in a VRF. The alternative to this design is Inside VRF (I-VRF), 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.

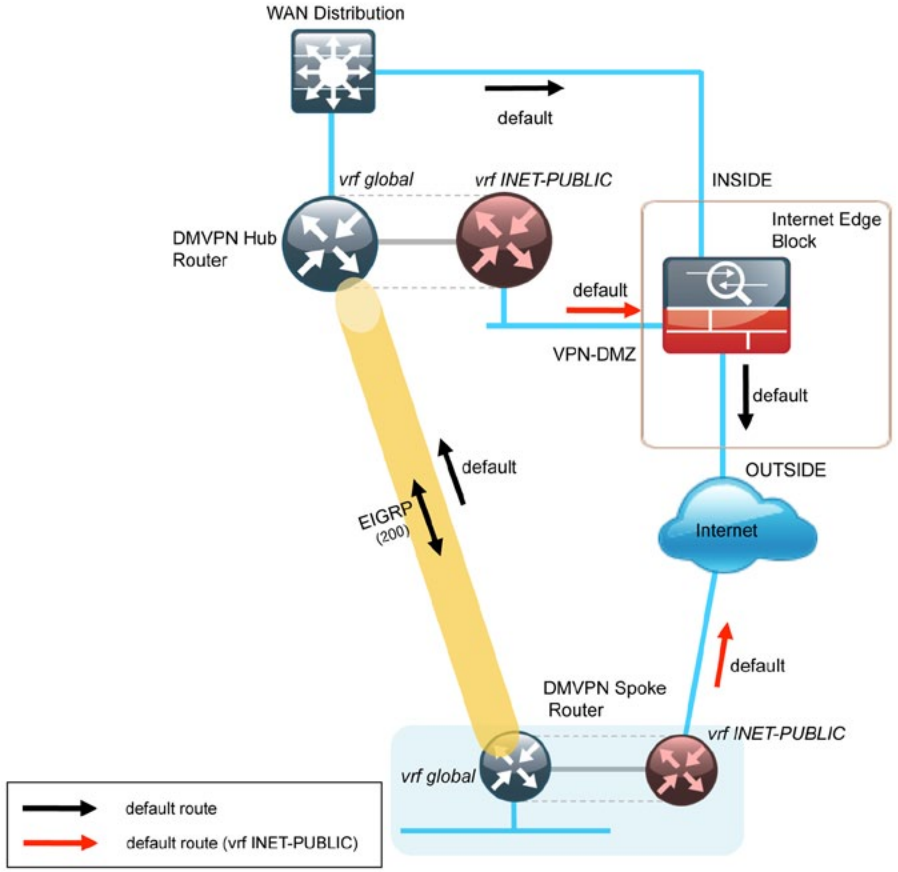
It is now possible to reestablish the IPSec tunnel to the remote peer router. As the remote-site policy requires central Internet access for end users, a default route is advertised through the tunnel. This advertisement causes a similar default routing issue on the remote router; the tunnel default overrides the Internet-pointing default and the tunnel connection breaks as shown in Figure 35B.

This configuration requires using F-VRF on the remote-site router as well. The primary benefits of using this solution are as follows:

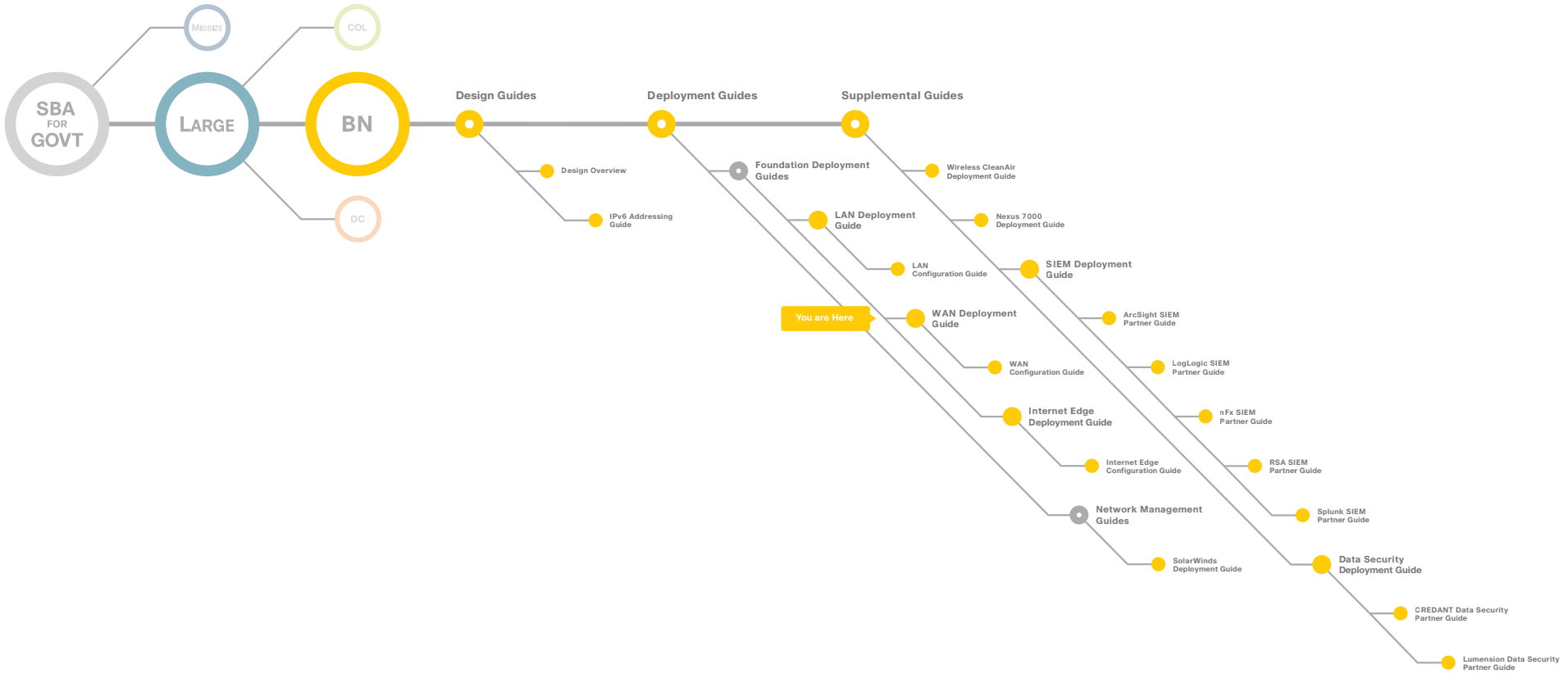
- Simplified default routing and static default routes in the INET-PUBLIC VRFs
- Ability to support default routing for end-users traffic through VPN tunnels
- Ability to leverage dynamic default routing for sites with multiple WAN transports
- Ability to build spoke-to-spoke tunnels with DMVPN with end-user traffic routed by default through VPN tunnels

The final design that uses F-VRF at both the WAN-aggregation site and a WAN remote site is shown in Figure 36.

Figure 36. Front Door VRF—Final Configuration



Appendix B:
SBA for Large Agencies Document System



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.**

C07-641107-00 12/10