Remote Site Using Local Internet Access

Technology Design Guide

August 2014 Series

CISCO VALIDATED DESIGN

Table of Contents

Preface

Cisco Validated Designs (CVDs) present systems that are based on common use cases or engineering priorities. CVDs incorporate a broad set of technologies, features, and applications that address customer needs. Cisco engineers have comprehensively tested and documented each design in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested design details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate existing CVDs but also include product features and functionality across Cisco products and sometimes include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems.

CVD Foundation Series

This CVD Foundation guide is a part of the *August 2014 Series*. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization's problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit the CVD Foundation web site.

Comments and Questions

If you would like to comment on a guide or ask questions, please use the feedback form.

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the scope or breadth of the technology covered the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- **Secure Site-to-Site WAN Communications Using Internet Services**—This guide helps organizations connect remote sites over public cloud Internet services and secure communications between sites.
- **Local Internet Access from Remote Sites**—Remote-site users access cloud-based applications and the web from an Internet connection at the remote site, removing the need to route traffic to the primary site.

For more information, see the "Use Cases" section in this guide.

Scope

This guide covers the following areas of technology and products:

- Design and configuration of remote-site WAN routing and of IOS-based security technologies, to include dynamic multi-point VPN (DMVPN), network address translation (NAT), and Zone-Based Firewall (ZBFW).

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNP Routing and Switching**—3 to 5 years planning, implementing, verifying, and troubleshooting local and wide-area networks
- **CCNP Security**—3 to 5 years testing, deploying, configuring, maintaining security appliances and other devices that establish the security posture of the network

Related CVD Guides

MPLS WAN Technology Design Guide

VPN WAN Technology Design Guide

Layer 2 WAN Technology Design Guide

To view the related CVD guides, click the titles or visit the CVD Foundation web site.

Introduction

The *Remote Sites Using Local Internet Access Technology Design Guide* describes how to enable remote-site users to access the Internet directly and securely, without having to route their traffic to the primary site. Additionally, this guide helps organizations connect remote sites over public cloud Internet services and secure communications between sites.

Related Reading

The MPLS WAN Technology Design Guide provides flexible guidance and configuration for Multiprotocol Label Switching (MPLS) transport.

The Layer 2 WAN Technology Design Guide provides guidance and configuration for a VPLS or Metro Ethernet transport.

The VPN WAN Technology Design Guide provides guidance and configuration for broadband or Internet transport in a both a primary or backup role.

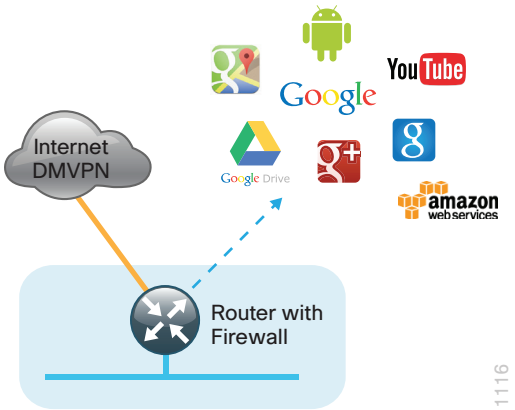
The GET VPN Technology Design Guide provides guidance and configuration for encryption services over private cloud MPLS transport.

Technology Use Cases

For remote-site users to effectively support the business, organizations require that the WAN provide sufficient performance and reliability.

Although many of the applications and services that the remote-site worker uses are centrally located, there are benefits in providing local Internet access at each remote site location. Offloading Internet browsing and providing direct access to public cloud service providers can greatly reduce traffic on the private WAN, saving costs and improving overall survivability. Leveraging the cloud in the remote office can greatly increase performance and the overall cloud experience.

Figure 1 - Remote site with local Internet access



Use Case: Secure Site-to-Site WAN Communications Using Internet Services

This guide helps organizations connect remote sites over public cloud Internet services and secure communications between sites.

This design guide enables the following network capabilities:

- Secure, encrypted communications for Internet-based WAN solutions for up to 500 locations by using a hub-and-spoke tunnel overlay configuration
- Deployment as a secondary connectivity solution for resiliency, providing backup to private MPLS WAN service by using single or dual routers in remote locations
- Support for IP Multicast, replication performed on core, and hub-site routers
- Compatibility with public cloud solutions where Network Address Translation (NAT) is implemented
- Best-effort quality of service for WAN traffic such as voice over IP (VOIP) and business applications

Use Case: Local Internet Access from Remote Site

Remote-site users directly access the Internet for cloud-based applications and user web access without having to route their traffic to the primary site.

This design guide enables the following network capabilities:

- Offload Internet traffic from primary MPLS WAN or Layer 2 WAN link
- More efficient use of Internet link by using it for user web traffic as well as for DMVPN backup
- Deployment of Cisco IOS security services for remote user and applications leveraging Zone-Based Firewall (ZBFW), NAT, and other network security features
- Resilient routing of user Internet traffic that uses local Internet and can reroute to access the Internet through the primary site during local Internet failure conditions
- Quality of service (QoS) for WAN traffic such as VoIP and business critical applications

Design Overview

This guide provides a design that enables highly available, secure, and optimized connectivity for multiple remote-site LANs.

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

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

- VPN WAN connectivity for up to 500 remote sites
- Primary and secondary links to provide redundant topology options for resiliency
- Secure local Internet access from remote sites
- Data privacy via encryption
- Wired LAN access at all remote sites

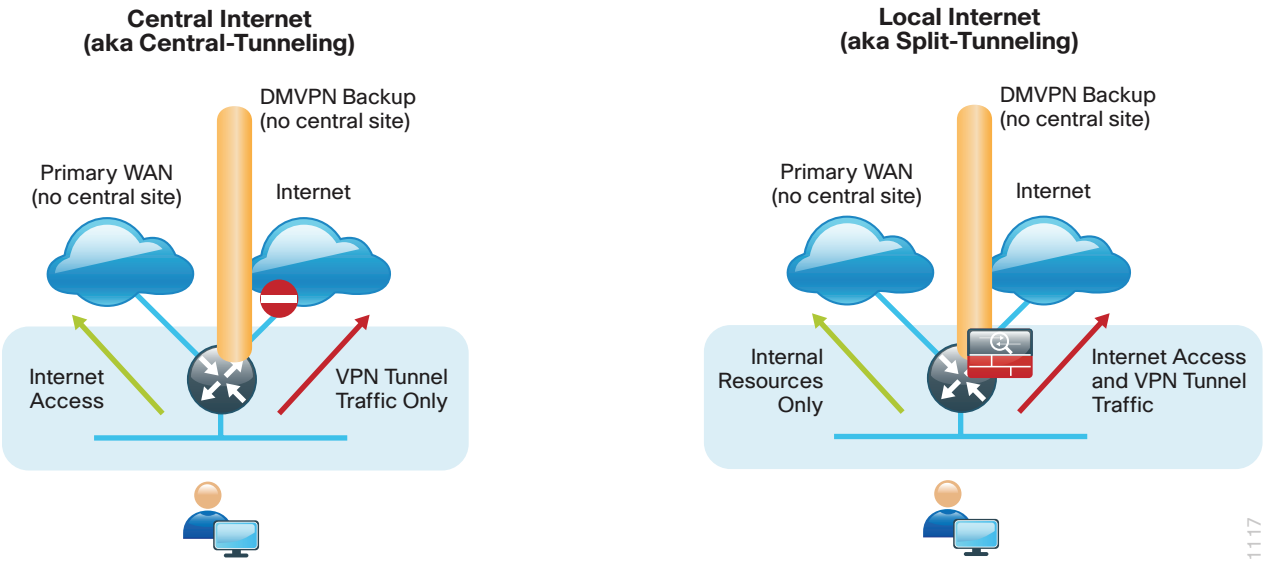
While the Internet is quickly becoming a more stable platform with better price to performance and improved reliability, it still falls short of meeting standards for many businesses. With Cisco WAN services, IT has the security and application services to deliver the highest levels of resiliency and reliability.

VPN WAN is an essential component of the Cisco Intelligent WAN (IWAN). Cisco IWAN delivers an uncompromised user experience over any connection, allowing an organization to right-size their network with operational simplicity and lower costs.

Remote-Site Design

The remote-site design provides the remote office with local Internet access solutions for web browsing and cloud services. This is referred to as the *local Internet model*. With the local Internet model, user web traffic and hosted cloud services traffic are permitted to use the local Internet link in a split-tunneling manner. In this model, a default route is generated locally connecting each remote site directly to the Internet provider. Private WAN connections using DMVPN over Internet, MPLS, or Layer 2 (L2) WAN provide internal routes to the data center and campus. In some configurations, backup Internet routing is provided over the private WAN connections.

Figure 2 - Central Internet and local Internet comparison



This guide documents secure local Internet-enabled WAN remote-site designs based upon various combinations of IP WAN transports mapped to site-specific requirements around service levels and resiliency.

The primary focus of the design is to allow usage of the following commonly deployed remote-site WAN configurations with local Internet access:

- Single router remote site with Internet and DMVPN WAN connectivity
- Single or dual router remote site with MPLS WAN and local Internet using DMVPN for backup
- Single or dual router remote site with both L2 WAN and local Internet using DMVPN for backup
- Single or dual router remote site with dual-Internet DMVPN for primary and backup connectivity

Reader Tip

The choice to use local Internet is locally significant to the remote site. No changes are required to the primary site.

The remote-site designs documented in this guide can be deployed in parallel with other remote-site designs that use centralized Internet access.

This guide does not address the primary aggregation site design and configuration details. This solution is tested and evaluated to work with the design models and WAN-aggregation site configurations as outlined in the MPLS WAN Technology Design Guide, Layer 2 WAN Technology Design Guide, and VPN WAN Technology Design Guide.

Figure 3 - WAN single router remote-site designs

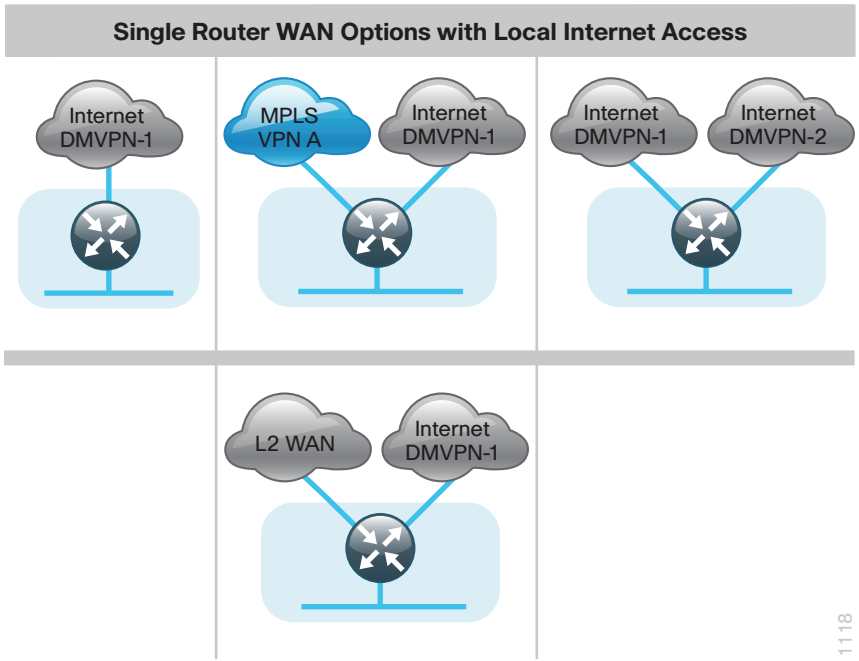
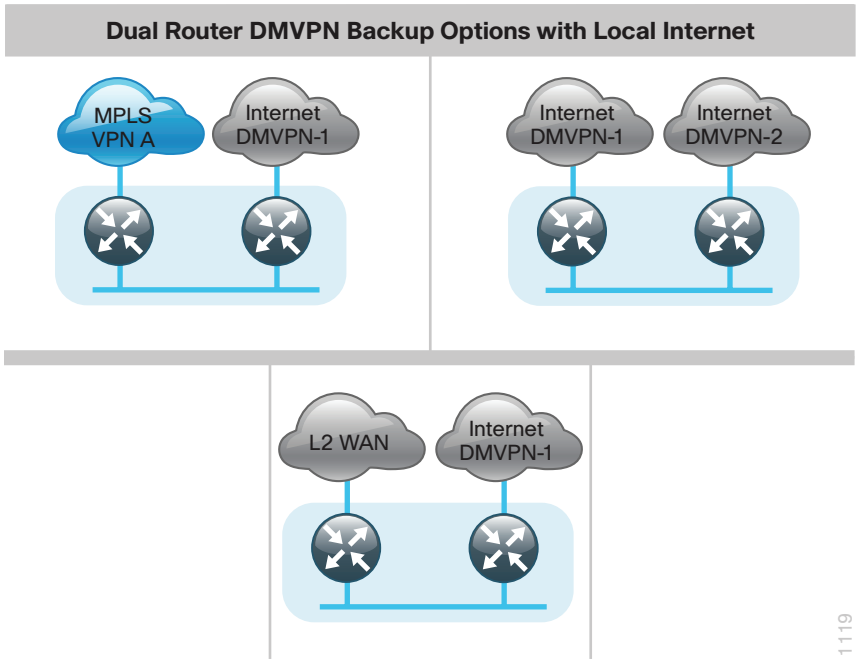


Figure 4 - Dual router remote-site designs



High Availability

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

In many cases, the network must tolerate single failure conditions, including the failure of any single WAN transport link or any single network device at the primary remote site.

- Remote sites classified as single router, dual link must provide Internet failover to the in the event of local Internet link failure. MPLS WAN and L2 WAN configurations will failover to the central Internet model.
- Remote sites classified as dual router, dual link must provide Internet failover in the event of local Internet link or router failure. MPLS WAN and L2 WAN configurations will failover to the central Internet model. Dual Internet configurations will provide redundancy for local Internet connectivity.

Table 1 - WAN remote-site transport options

WAN remote-site routers	WAN transports	Primary transport	Secondary transport
Single	Single	DMVPN-1	–
Single	Dual	MPLS VPN A	DMVPN-1
Single	Dual	DMVPN-1	DMVPN-2
Single	Dual	Layer 2	DMVPN-1
Dual	Dual	MPLS VPN A	DMVPN-1
Dual	Dual	DMVPN-1	DMVPN-2
Dual	Dual	Layer 2	DMVPN-1

The modular nature of the network design enables you to create design elements that you can replicate throughout the network. All of these WAN remote-site designs are standard building blocks in the overall design, providing a consistent deployment method and an easy way to scale the network.

Ethernet WAN

Ethernet has traditionally been a LAN technology primarily due to the distance limitations of the available media and the requirement for dedicated copper or fiber links. 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.

Private MPLS WAN Transport

Cisco IOS Software Multiprotocol Label Switching (MPLS) enables enterprises and service providers to build next-generation, intelligent networks that deliver a wide variety of advanced, value-added services over a single infrastructure. You can integrate this economical solution seamlessly over any existing infrastructure, such as IP, Frame Relay, ATM, or Ethernet.

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

Reader Tip

For more information, see the MPLS WAN Technology Design Guide.

Layer 2 WAN transports are now widely available from service providers and are able to extend various Layer 2 traffic types (Frame Relay, PPP, ATM, or Ethernet) over a WAN. The most common implementations of Layer 2 WAN are used to provide Ethernet over the WAN using either a point-to-point or point-to-multipoint service.

Service providers implement these Ethernet services by using a variety of methods. MPLS networks support both Ethernet over MPLS (EoMPLS) and Virtual Private LAN Service (VPLS). You can use other network technologies, such as Ethernet switches in various topologies, to provide Ethernet Layer 2 WAN services.

Reader Tip

For more information, see the Layer 2 WAN Technology Design Guide.

GET VPN

Many organizations require encryption for data traversing private networks, such as an MPLS service. This ensures data is secure in transit through the service provider network. The use of encryption should not limit the performance or availability of a remote-site application, and should be transparent to end users.

GET VPN is a tunnel-less VPN technology based on the IETF standard (RFC 3547). The technology provides end-to-end data encryption for network infrastructure while maintaining any-to-any communication between sites. You can deploy it across various WAN core transports, such as IP or Multiprotocol Label Switching (MPLS) networks. GET VPN leverages the Group Domain of Interpretation (GDOI) protocol in order to create a secure communication domain among network devices.

The benefits of GET VPN include the following:

- Highly scalable VPN technology that provides an any-to-any meshed topology without the need for complex peer-to-peer security associations
- Low latency and jitter communication with direct traffic between sites
- Centralized encryption policy and membership management with the key servers (KSs)
- Simplified network design due to leveraging of native routing infrastructure (no overlay routing protocol needed)
- Efficient bandwidth utilization by supporting multicast-enabled network core
- Network intelligence such as native routing path, network topology, and QoS

Reader Tip

This guide does not cover the in-depth configuration details for GET VPN. For more information about GET VPN, see the GET VPN Technology Design Guide.

Public Internet as WAN Transport

The WAN uses the Internet for VPN site-to-site connections as both a primary WAN transport and as a backup WAN transport (to a primary VPN site-to-site connection).

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 a primary transport when it is not feasible to connect with another transport option. Additional resiliency is provided by using the Internet as an alternate transport option.

Internet connections are typically included in discussions relevant to the Internet edge, specifically for the primary site. Remote site routers commonly have Internet connections that can be used for local web browsing, cloud services, and private WAN transport. For security, Internet access at remote is maintained by using integrated security features such as Cisco IOS Zone-Based Firewall (ZBFW). All remote-site traffic must be encrypted when transported over public IP networks such as the Internet.

Reader Tip

For more information, see the VPN WAN Technology Design Guide.

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 design guide.

DMVPN is used 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 and are configured with Network Address Translation (NAT). It is common for firewalls to be configured between the DMVPN routers and the Internet. In many cases, designs also require NAT configurations in conjunction with DMVPN.

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

> **Reader Tip**
>
> This guide does not cover the configuration details for the DMVPN hub routers. For information about DMVPN, see the VPN WAN Technology Design Guide.

Routing Protocols

EIGRP

Cisco chose Enhanced Interior Gateway Protocol (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.

With the advances in EIGRP, this guide uses EIGRP named mode. The use of EIGRP named mode allows related EIGRP configurations to be centrally located in the configuration. EIGRP named mode includes features such as wide metrics, which support larger multi-gigabit links. For added security, EIGRP neighbor authentication has been implemented in order to prevent unauthorized neighbor associations.

> **Tech Tip**
>
> In the EIGRP named mode configuration, EIGRP wide metric support is on by default and backward compatible with existing routes.

BGP

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

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

IP Multicast

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

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

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

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

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

DNS Considerations

When deploying remote site WAN with local Internet is important to consider Domain Name System (DNS) configuration requirements and impacts to network redundancy and performance. Remote sites are often geographically diverse and many cloud services have localized resources within the regions of remote site locations that are optimal for user and application traffic. Using centralized DNS will result in sub-optimal routing, poor application performance, and failure if private WAN connections are unavailable. For instance, compare a cloud storage application moving data across the country for storage versus resolving to a local cluster. For these reasons, split DNS designs are recommended for optimal routing and application performance.

Remote-Site LAN

The focus of the remote-site LAN configurations in this guide is Layer 2 access. WAN remote sites that do not require additional distribution layer routing devices are considered to be flat or, from a LAN perspective, they are considered unrouted Layer 2 sites. All Layer 3 services are provided by the attached WAN routers.

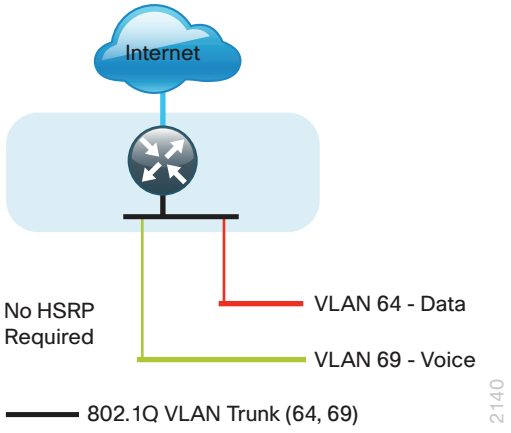
Access switches, through the use of multiple VLANs, can support services such as data and voice. The design shown in the following figure illustrates the standardized VLAN assignment scheme. The benefits of this design are clear: all of the access switches can be configured identically, regardless of the number of sites in this configuration.

Reader Tip

Access switches and their configuration are not included in this guide. For information about the various access switching platforms, see the Campus Wired LAN Technology Design Guide.

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.

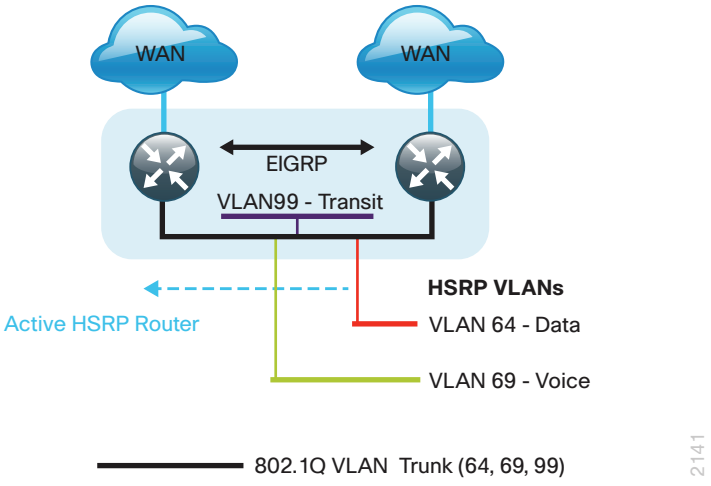
Figure 5 - Single router WAN remote site–L2 LAN



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. You need to configure EIGRP between the routers. For consistency with the primary site LAN, use the EIGRP LAN process (AS 100).

Because there are now two routers per subnet, a First Hop Redundancy Protocol (FHRP) must be implemented. For this design, Cisco selected Hot Standby Router Protocol (HSRP) as the FHRP. HSRP is designed to allow for transparent failover of the first-hop IP router. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts configured with a default gateway IP address.

Figure 6 - Dual router WAN remote site - L2 LAN

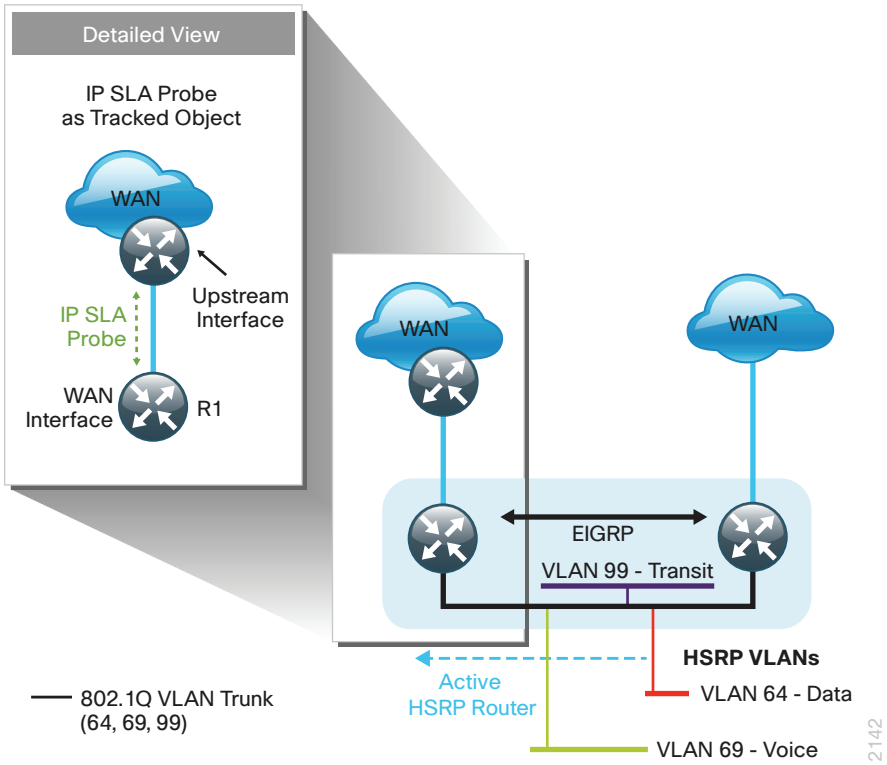


Enhanced Object Tracking (EOT) provides a consistent methodology for various router and switching features to conditionally modify their operation based on information objects available within other processes. The objects that can be tracked include interface line protocol, IP route reachability, and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

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

To improve convergence times after a primary 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, thus providing additional network resiliency.

Figure 7 - WAN remote site–IP SLA probe to verify upstream device reachability



You configure 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 remote-site primary WAN router to the upstream neighbor (MPLS PE, Layer 2 WAN CE, or DMVPN hub) 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 dual DMVPN remote site communicating with a DMVPN2-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 hairpinning.

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

Quality of Service

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

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 QoS to help ensure optimal use of network resources. This functionality allows for the differentiation of applications, ensuring that each has the appropriate share of the network resources to protect the user experience and ensure the consistent operations of business critical applications.

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

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

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

Table 2 - QoS service class mappings

Service class	Per-hop behavior (PHB)	Differentiated services code point (DSCP)	IP precedence (IPP)	Class of service (CoS)
Network layer	Layer 3	Layer 3	Layer 3	Layer 2
Network control	CS6	48	6	6
Telephony	EF	46	5	5
Signaling	CS3	24	3	3
Multimedia conferencing	AF41, 42, 43	34, 36, 38	4	4
Real-time interactive	CS4	32	4	4
Multimedia streaming	AF31, 32, 33	26, 28, 30	3	3
Broadcast video	CS5	40	4	4
Low-latency data	AF21, 22, 23	18, 20, 22	2	2
Operation, administration, and maintenance (OAM)	CS2	16	2	2
Bulk data	AF11, 12, 13	10, 12, 14	1	1
Scavenger	CS1	8	1	1
Default "best effort"	DF	0	0	0

With Internet-based WAN services, QoS preservation across the public Internet is not guaranteed. For best effort in this use case, egress traffic classification prioritizes traffic as it leaves the remote-site router, paying special attention to the priority of DMVPN Internet Security Association and Key Management Protocol (ISAKMP) traffic.

Per-Tunnel QoS for DMVPN

The Per-Tunnel QoS for DMVPN feature allows the configuration of a QoS policy on a DMVPN hub on a per-tunnel (spoke) basis. With Per-Tunnel QoS, a policy is applied outbound for DMVPN hub-to-spoke tunnels, which increases per-tunnel performance for IPsec interfaces.

This feature allows you to apply a QoS policy on a DMVPN hub on a tunnel instance (per-endpoint or per-spoke basis) in the egress direction for DMVPN hub-to-spoke tunnels. It allows you to shape the tunnel traffic to individual spokes (parent policy) and to differentiate individual data flows going through the tunnel for policing (child policy).

Traffic is regulated from the central site (hub) routers to the remote-site (spoke) routers on a per-tunnel basis. With simplified configurations, the hub site is prevented from sending more traffic than any single remote site can handle. This ensures high-bandwidth remote sites do not overrun remote sites with lower bandwidth allocations.

Securing Local Internet Access

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

To help organizations address concerns with cloud security, this guide addresses the implementation of several key integrated security features. As organizations leverage local Internet in the remote site, considerations for securing access at each remote location is necessary. This guide provides general recommendations and guidelines for implementing stateful firewalling, network address translation, and basic router security and hardening.

Network Address Translation

With the growing adoption of distributed cloud applications, NAT plays an integral role in enabling organizations to deploy and secure public and private cloud services.

Network address translation (NAT) enables private IP networks that use unregistered IP addresses (as specified in RFC 1918) to connect to the Internet. NAT is used to translate the private addresses defined on internal networks into legal routable addresses because Internet Service Providers (ISPs) cannot route RFC 1918 addresses.

Primarily designed for IP address conservation and network design simplification, NAT can also serve as a security mechanism by hiding a host's IP address and application ports.

NAT operates on firewall and routers connecting two network segments and translating the internal private addresses to a public address on the external network. It can be configured to show to the outside world only one IP address. This provides additional security by effectively hiding the entire internal network behind a single IP address. This capability is called Port Address Translation (PAT), also referred to as *NAT overload*.

NAT provides the following benefits:

- Security, providing an added layer of defense from external attackers by hiding IP addresses and application ports
- Scalability through the reuse of IP addresses, and by using IP address overloading capabilities
- Simplified provisioning and troubleshooting by enforcing consistent network design across network locations

NAT is typically implemented at the edge of the network wherever an organization connects to the Internet. Today, this may be in central or large aggregation sites or in remote sites providing localized Internet services.

Cisco IOS Zone-Based Firewall

With the adoption of remote-site local Internet for user web browsing and cloud services, the deployment of firewall services at the remote office Internet edge is critical to maintaining an organization's security posture.

Cisco Zone-Based Firewall (ZBFW), also called *Zone Policy Firewall*, is a Cisco IOS-integrated stateful firewall implemented on the Cisco Integrated Services Routers (ISR) and Cisco Aggregation Services Routers (ASR) routing platforms.

Firewall zone policies are configured by using the Cisco Common Classification Policy Language (CPL or C3PL), which employs a hierarchical structure to define inspection for network protocols and the groups to which the inspection will be applied. Users familiar with the Cisco IOS Modular QoS CLI (MQC) will recognize the use of class maps to specify which traffic will be affected by the action applied in a policy map.

Within this model, router interfaces are assigned to security zones, which establish the security borders of your network. A security zone defines a boundary where traffic is subjected to policy restrictions; this policy is called a *zone policy*. Zone policies define what traffic is allowed to flow between security zones. Zone policies are unidirectional firewall policies applied between two security zones, called a *zone pair*. A zone pair is defined as two security zones between which a zone policy is applied.

Router interfaces assigned to configured security zones are subject to the default policies and rules:

- An interface can only be a member of a single security zone.
- When an interface is placed into a security zone, traffic is implicitly allowed to flow between other interfaces assigned to the same security zone.
- Traffic flow to interfaces in different security zones is denied with an implicit deny all zone policy.
- Traffic cannot flow between an interface that is a member of security zone and any interface that is not a member of a security zone.
- To allow traffic to flow between different security zones, policies must be configured between any two security zones.
- Pass, inspect, and drop actions can only be applied between two zones.
- By default, traffic to and from the router itself (routing protocols, etc.) is permitted. The router itself (as a source and destination) is defined as the self-zone by the Cisco IOS firewall. Traffic to and from the self-zone on any interface is allowed until traffic is explicitly denied by a user defined zone security policy.

Design Overview

Remote Sites–Router Selection

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

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

Table 3 - WAN remote-site Cisco Integrated Services Router options

Option	2911	2921	2951	3925	3945
Ethernet WAN with services[1]	35 Mbps	50 Mbps	75 Mbps	100 Mbps	150 Mbps
On-board FE ports	0	0	0	0	0
On-board GE ports[2]	3	3	3	3	3
Service module slots	1	1	2	2	4
Redundant power supply option	No	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. A single-router, dual-link remote site requires four router interfaces when using a port-channel to connect to an access or distribution layer. Add the EHWIC-1GE-SFP-CU to the Cisco 2900 and 3900 Series Integrated Services Routers in order to provide the additional WAN-facing interface.

Remote-Site Design Details

This guide focuses on seven remote-site designs with local Internet access. These designs provide configurations and guidance for enabling secure local Internet access in remote office locations. Designs providing local Internet access and internal network communications are deployed by using existing MPLS WAN, L2 WAN, and VPN WAN design models.

The local Internet designs are:

- Single router, single-link VPN WAN
- Single router, dual-link MPLS WAN primary with VPN WAN backup
- Single router, dual-link L2 WAN primary with VPN WAN backup
- Single router, dual-link dual VPN WAN
- Dual-router MPLS WAN primary with VPN WAN backup
- Dual-router L2 WAN primary with VPN WAN backup
- Dual-router dual VPN WAN

Figure 8 - Single router remote site with local Internet design options

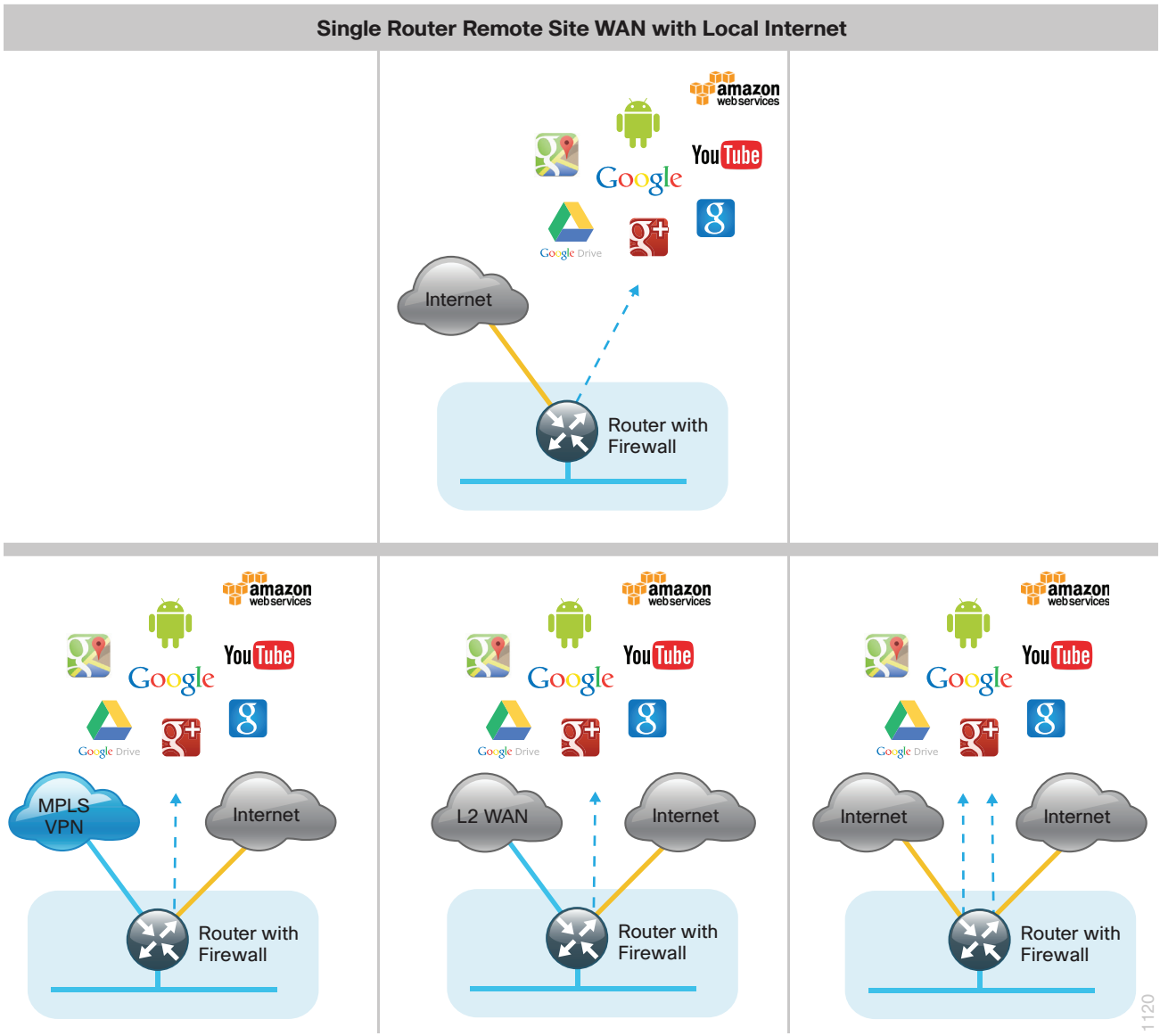
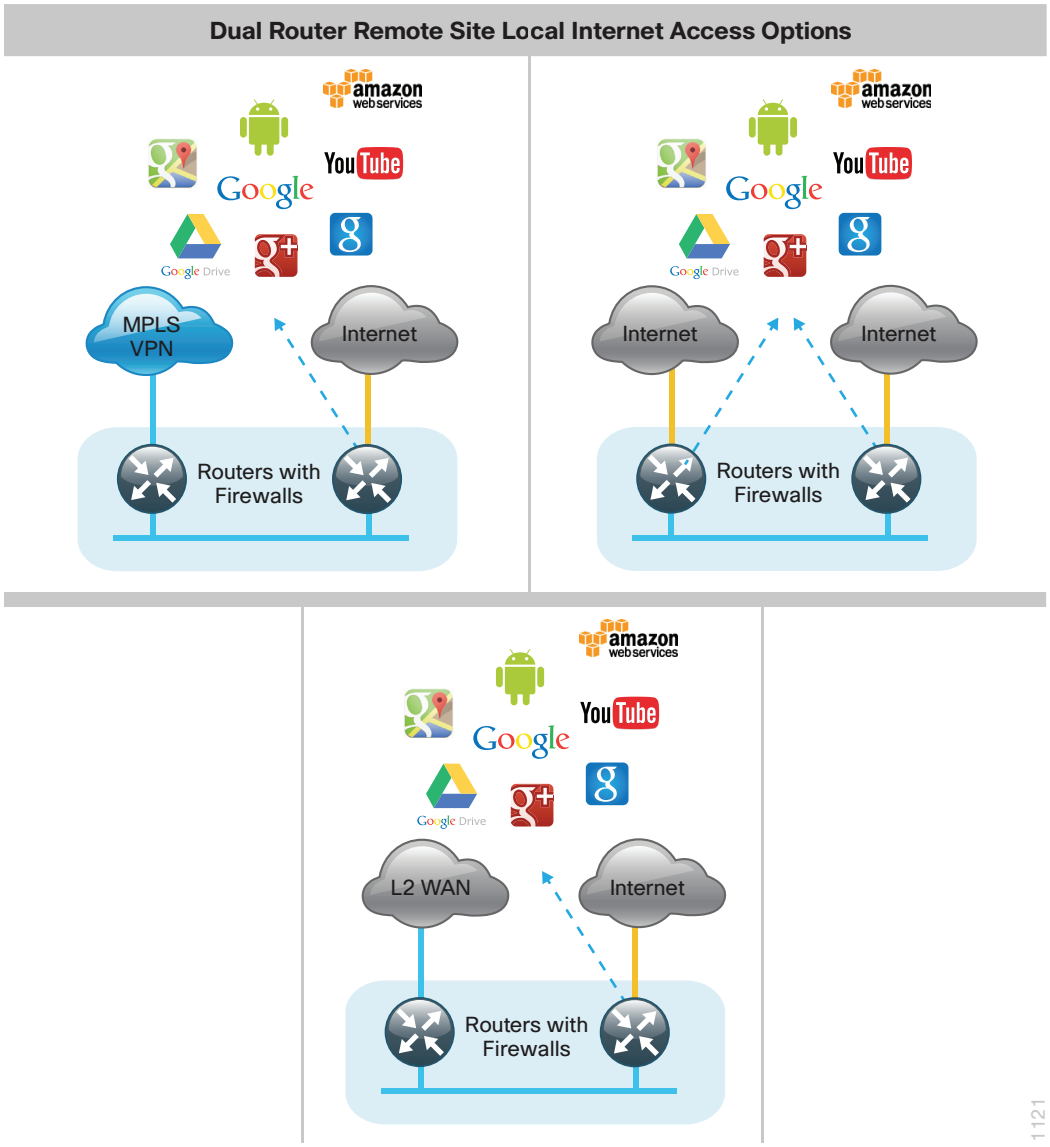


Figure 9 - Dual router remote site with local Internet design options



Local Internet Access

Each of the remote-site design options supports local Internet access and internal network communications with the central site. All designs except the single-router, single-link design support resilient routing.

Local Internet traffic is forwarded directly to the Internet by using the default route. This default route is directed at the next-hop router in the Internet Service Provider's (ISP) network. Because RFC-1918 addresses are used for internal networks, all Internet-bound traffic is translated to a public address by using PAT on the ISP-connected interface. The ZBFW is enabled to provide stateful inspection and to enforce a policy that only allows return traffic for sessions initiated by internal users and for DMVPN tunnel traffic between the remote-site router and the DMVPN hub router.

This local Internet model does not use F-VRF (Front Door VRF) with DMVPN to segment the routing table, thus allowing two defaults to exist on the same router. With F-VRF, the default route from the ISP is contained within the Internet VRF and is only used for DMVPN tunnel formation.

In this model, a default route over Internet-based VPN tunnels cannot be allowed because route flapping can occur. In this case, because backup Internet routing is not possible over these VPN tunnels, the recommended best practice is to filter the central-site default route. Ensuring the Dynamic Host Configuration Protocol (DHCP)-derived default route to the local ISP is preferred over the central-site default route also helps to avoid issues if the default route is not filtered due to misconfigurations. Central Internet fallback is possible with MPLS-based WAN services.

The detailed designs for each of the remote-site types listed in Table 4 and Table 5 are discussed in the following section.

Table 4 - Single-router remote site options

Remote site type	Link 1 usage	Link 2 usage
DMVPN (single-router, single link)	DMVPN tunnel Local Internet	-
MPLS + DMVPN (single-router, dual link)	MPLS Central Internet fallback	DMVPN tunnel Local Internet
Layer 2 WAN + DMVPN (single-router, dual link)	Layer 2 WAN Central Internet fallback	DMVPN tunnel Local Internet
DMVPN + DMVPN (single-router, dual link)	DMVPN tunnel Local Internet (backup)	DMVPN tunnel Local Internet

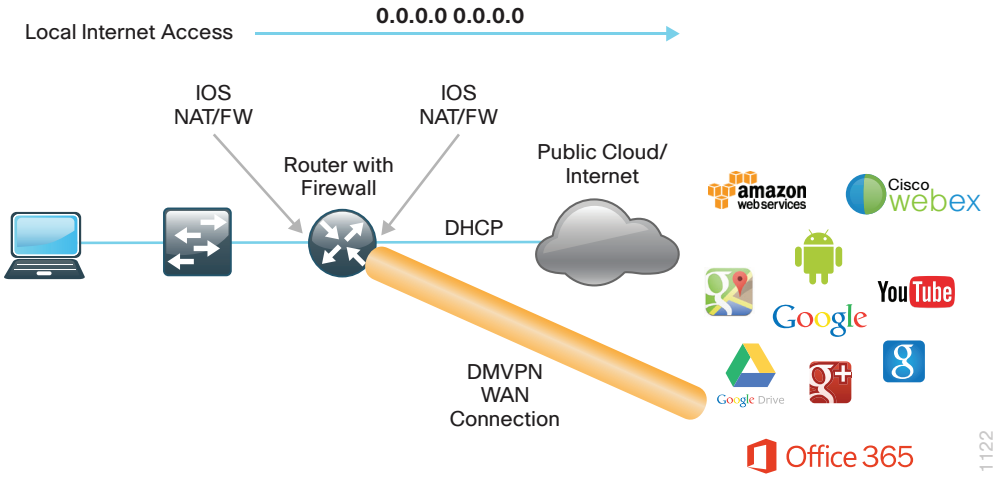
Table 5 - Dual-router remote site options

Remote site type	Router 1 link usage	Router 2 link usage
MPLS + DMVPN (dual-router, dual link)	MPLS Central Internet fallback	DMVPN tunnel Local Internet
Layer 2 WAN + DMVPN (dual-router, dual link)	Layer 2 WAN Central Internet fallback	DMVPN tunnel Local Internet
DMVPN + DMVPN (dual-router, dual link)	DMVPN tunnel Local Internet (backup)	DMVPN tunnel Local Internet

DMVPN Remote Site (Single Router, Single Link)

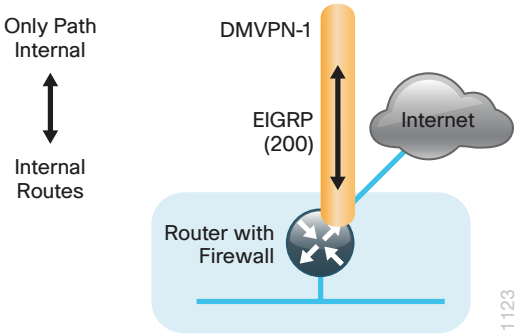
In this design, the remote site is configured with a single router and a single connection to the Internet. This is the most basic of all designs, and is a common building block that other designs are derived from. In this design, the remote site uses a single router and connects to a single Internet connection. This connection will be shared for a combination of internal traffic and local Internet access.

Figure 10 - Single router DMVPN with WAN with local Internet service



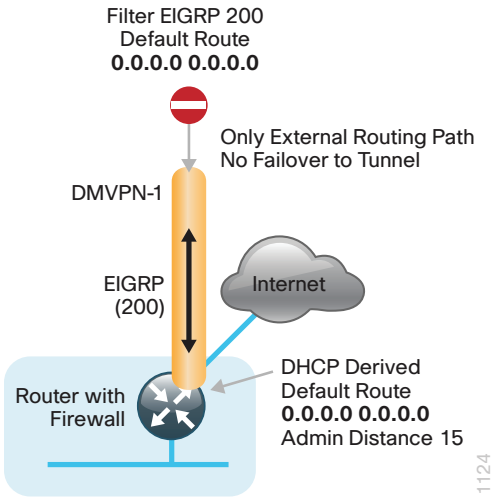
Internal traffic or traffic that says within the organization will be routed over an encrypted tunnel path to the central site by using DMVPN. Internal networks are advertised using EIGRP over the tunnel.

Figure 11 - Single router Internet with WAN internal routing



In this example, the Internet-facing interface on the router obtains an IP address from the ISP by using DHCP. The router also receives a DHCP-assigned default route with a default administrative distance (AD) value of 254. In this case, the default route to the local ISP should be preferred, so the AD value of the DHCP-learned default route is adjusted to 15.

Figure 12 - Single router Internet with WAN default routing

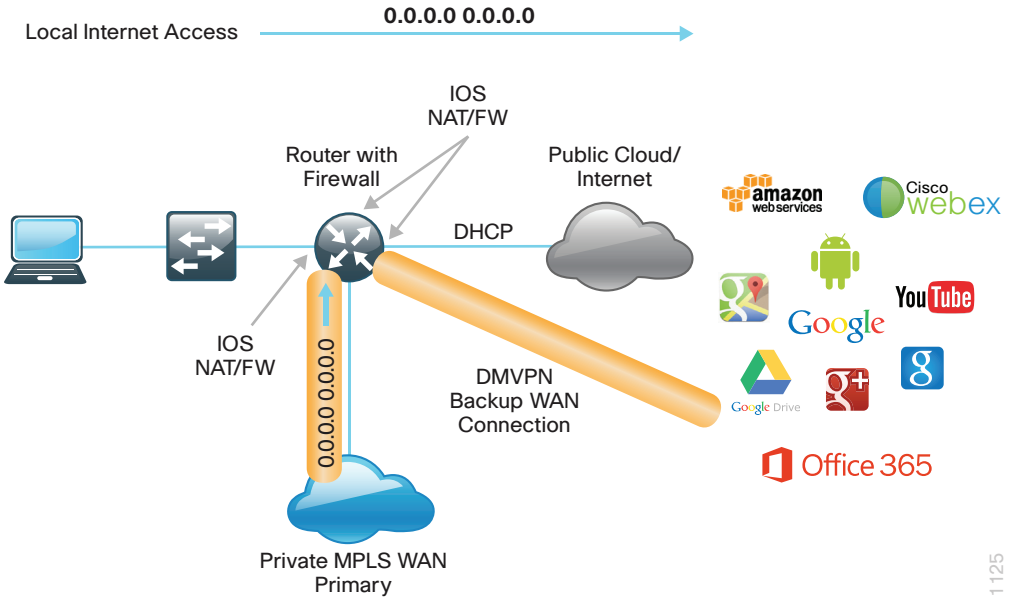


Once the VPN connection has been negotiated, the remote-site router will form an EIGRP adjacency with the DMVPN hub router and exchange routing information. The primary site advertises its default route toward the remote site. With a remote-site local Internet configuration, the default route received over the DMVPN tunnel from the primary site must be filtered from the remote-site routing table.

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

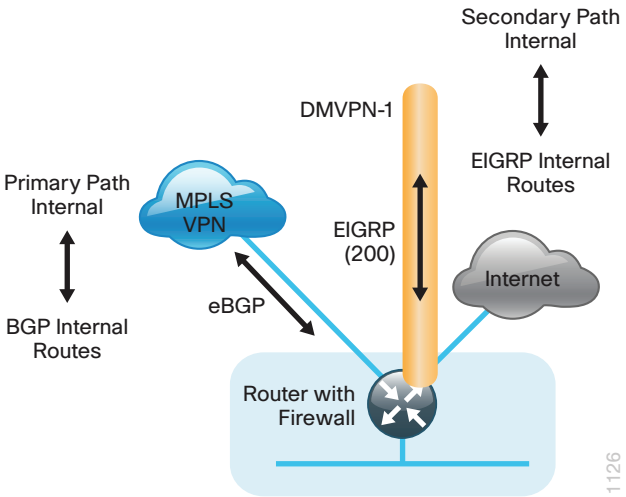
In this design, the remote site is configured with a single router by using MPLS as the primary connectivity for internal traffic. This site is also using an Internet connection on the same router for local Internet access and DMVPN backup for internal traffic.

Figure 13 - Single router MPLS primary with DMVPN backup



Internal traffic or traffic that stays within the organization will be routed primarily over the MPLS WAN connection. In the case of a failure on the MPLS network, internal traffic will then be routed over an encrypted tunnel path to the central site by using DMVPN over the Internet. Internal networks are advertised by using EIGRP over the DMVPN tunnel.

Figure 14 - Single router MPLS primary with DMVPN backup internal routing

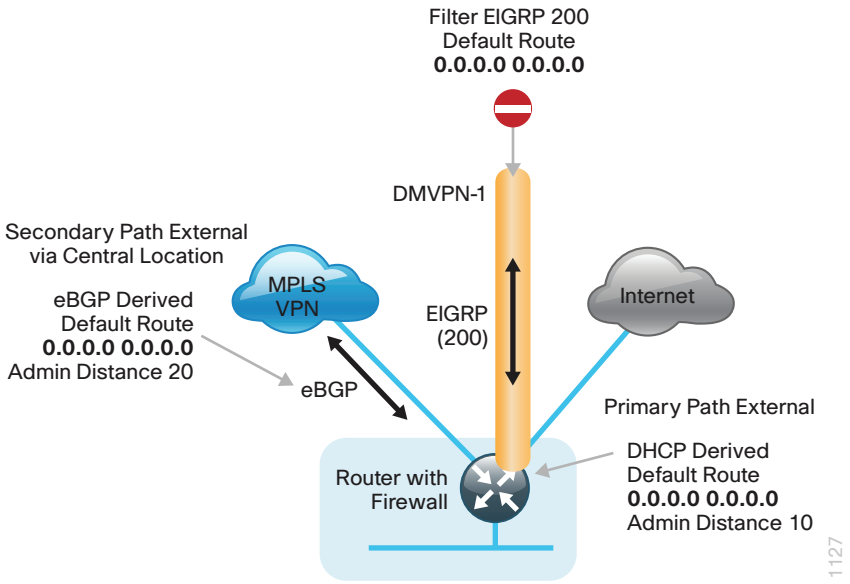


In this example, the Internet-facing Ethernet interface on the router is using DHCP to obtain an IP address from the ISP. The router is also using DHCP to install a default route into the local table. By default, this DHCP-installed static route has an AD value of 254.

In this case, the default route to the local ISP should be preferred so the AD value is changed to 10. This ensures the default route is chosen over other protocols such as EIGRP and BGP.

In this configuration, the MPLS connection will be used as a backup path for Internet if the local Internet connection fails. The central-site default route is advertised over the MPLS network via eBGP with an AD value of 20 and will be used only if the local connection fails.

Figure 15 - Single router MPLS primary with DMVPN backup default routing

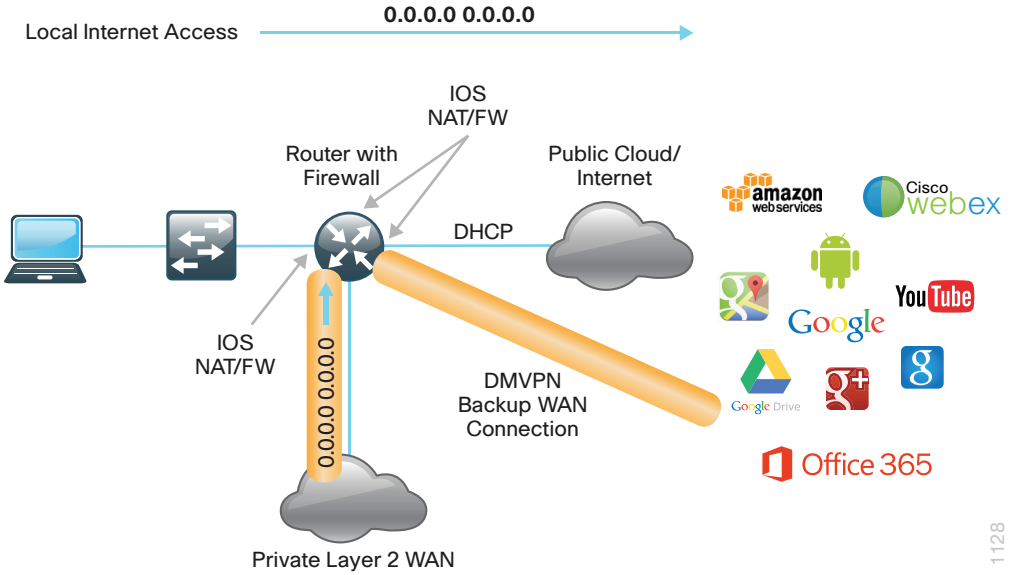


Once the VPN connection has been negotiated, the remote-site router will form an EIGRP adjacency with the DMVPN hub router and exchange routing information. The central site also has a local ISP default route used for central-site Internet access that is advertised by EIGRP. With a remote-site local Internet configuration, the default route received over the DMVPN tunnel from the central site must be filtered from the remote site routing table.

Layer 2 WAN + DMVPN Remote Site (Single Router, Dual Link)

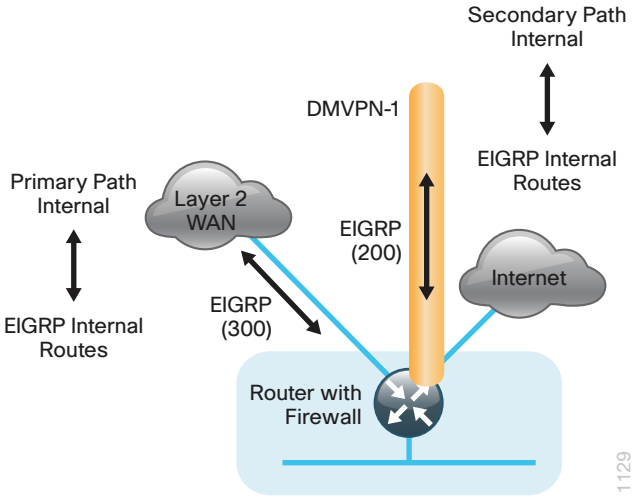
In this design, the remote site is configured with a single router using L2 WAN services such as VPLS as the primary connectivity for internal traffic. This site is also using an Internet connection on the same router for local Internet access and DMVPN backup for internal traffic.

Figure 16 - Single router Layer 2 WAN with DMVPN backup



Internal traffic or traffic that stays within the organization will be routed primarily over the private L2 WAN connection. If the Layer 2 WAN fails, internal traffic will then be routed over an encrypted tunnel path to the central site by using DMVPN over the Internet. Internal networks are advertised using EIGRP over the DMVPN tunnel.

Figure 17 - Single router Layer 2 WAN with DMVPN backup internal routing

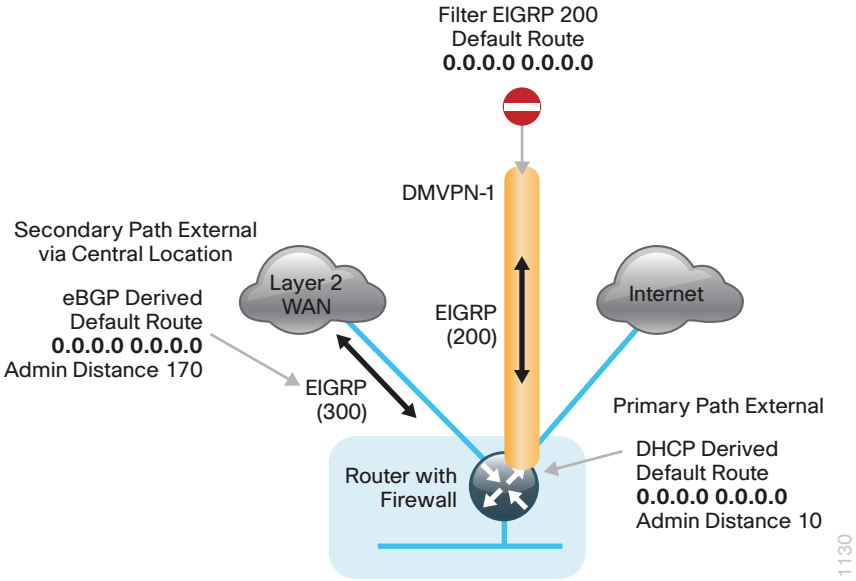


In this example, the Internet-facing Ethernet interface on the router is using DHCP to obtain an IP address from the ISP. The router is also using DHCP to install a default route into the local table. By default, this DHCP-installed static route has an AD value of 254.

In this case, the default route to the local ISP should be preferred so the AD value is changed to 10. This ensures it is chosen over other protocols such as EIGRP and BGP.

In this configuration, the L2 WAN connection will be used as a backup path for Internet if the local Internet connection fails. The central-site default route is advertised over the L2 WAN via EIGRP with an AD value of 170 and will be used only if the local connection fails.

Figure 18 - Single router MPLS primary with DMVPN backup default routing

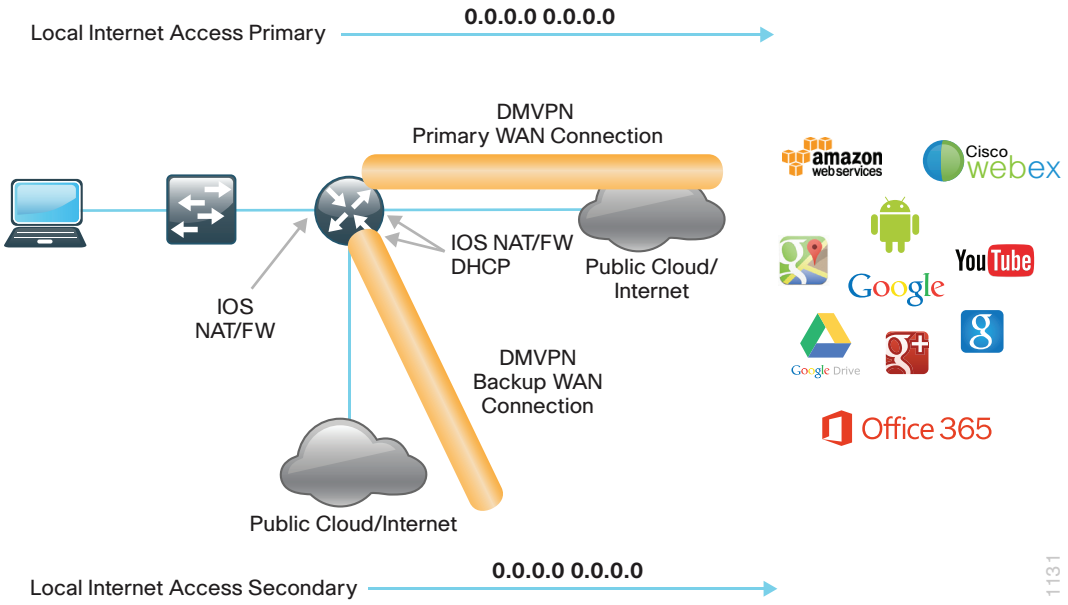


Once the VPN connection has been negotiated, the remote-site router will form an EIGRP adjacency with the DMVPN hub router and exchange routing information. The central site also has a local ISP default route used for central-site Internet access that is advertised by EIGRP. With a remote-site local Internet configuration, the default route received over the DMVPN tunnel from the central site must be filtered from the remote site routing table.

DMVPN + DMVPN Remote Site (Single Router, Dual Link)

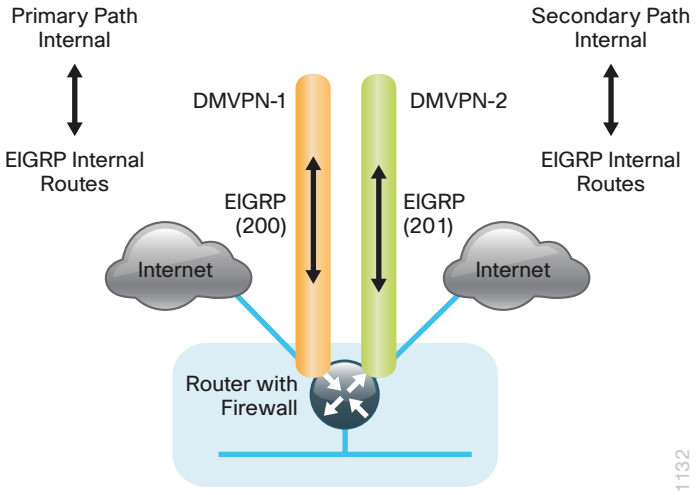
In this design, the remote site is configured with a single router using dual Internet connections with DMVPN for primary and backup connectivity.

Figure 19 - Single router with dual DMVPN site



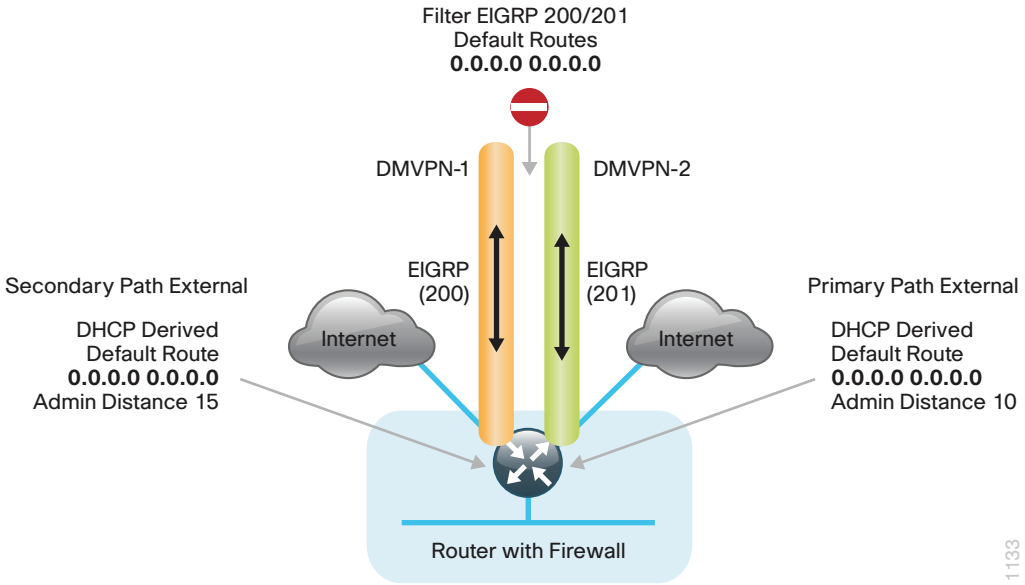
Internal traffic or traffic that says within the organization will be encrypted and routed over the primary Internet (DMVPN-1) connection. In the case of a failure on the primary ISP network, internal traffic will then be encrypted and routed over the secondary DMVPN tunnel (DMVPN-2). Internal networks are advertised using EIGRP over the DMVPN tunnels.

Figure 20 - Single router with dual DMVPN internal routing



In this example, the Internet-facing Ethernet interfaces on the router are using DHCP to obtain an IP address from the ISP. The router is also using DHCP to install a default route into the local table. By default, these DHCP-2i installed static routes have an AD value of 254. With two connections, preference to these routes needs to be ensured.

Figure 21 - Single router with dual DMVPN default routing



In this case, the default route to the secondary link should be preferred, so the AD value is changed to 10. Using the secondary link as the primary path for external traffic provides more usable bandwidth during a normal network operational state. In this configuration, the primary Internet-interface AD value is set to 15. This ensures the local default route is chosen over other protocols such as EIGRP. The primary link will be used as a backup path for Internet traffic should the other local Internet connection fail.

Once the VPN connection has been negotiated, the remote-site router will form an EIGRP adjacency with the DMVPN hub router and exchange routing information. The central site also has a local ISP default route used for central site Internet access that is advertised by EIGRP toward the remote site. With a remote-site local Internet configuration, the default route received over the DMVPN tunnel from the central site must be filtered from the remote site routing table.

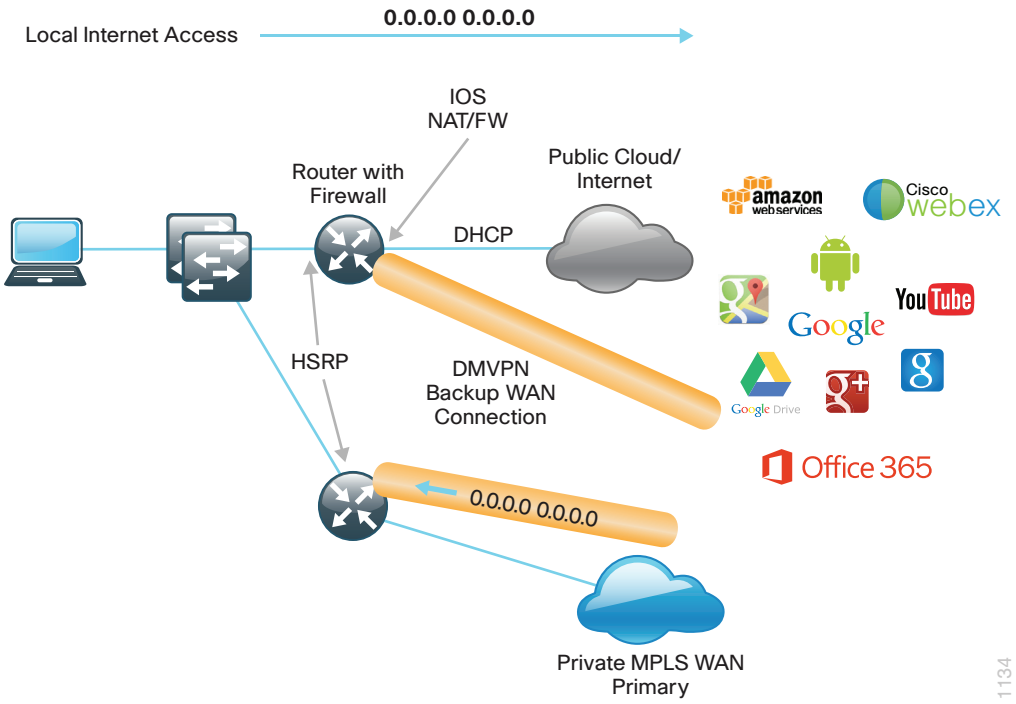
> **Tech Tip**
>
> The DMVPN spoke-to-spoke tunnel setup may not work properly with dual Internet configurations if the service providers implement security measures as outlined in RFC2827 per the guidelines of RFC 3013. These security measures are intended to reduce source address spoofing and denial of service (DoS) attack propagation by using ACLs and unicast Reverse Path Forwarding (RPF) capabilities ingress at the ISP network edge.

MPLS + DMVPN Remote Site (Dual Router, Dual Link)

In this design, the remote site is configured with dual routers for added resiliency by using MPLS as the primary transport for internal traffic. In all DMVPN configurations with local Internet access, the default route is filtered and removed from EIGRP over the DMVPN tunnel.

The secondary router in this remote site configuration is connected to the Internet providing local Internet access and DMVPN backup for internal traffic.

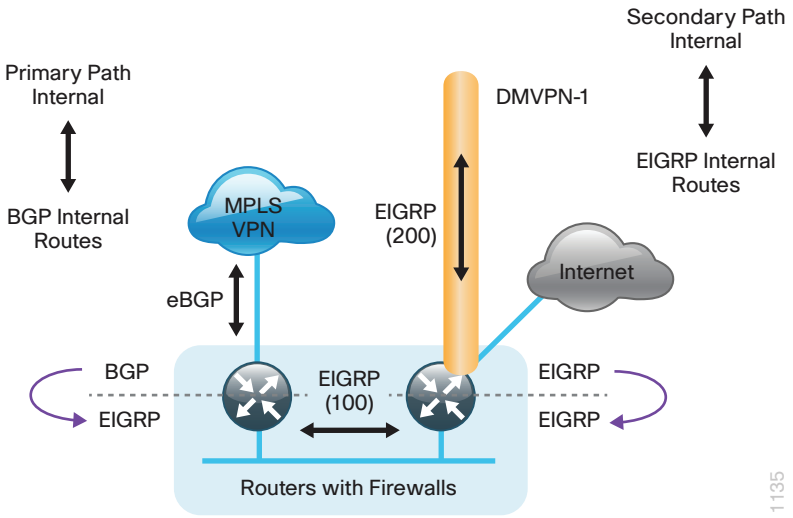
Figure 22 - Dual-router MPLS primary with DMVPN backup internal routing



Internal traffic or traffic that stays within the organization will be routed primarily over the MPLS WAN connection on the primary router. In the case of a failure on the MPLS network, internal traffic will then be routed over an encrypted tunnel path to the central site by using DMVPN over the Internet on the secondary router. Internal networks are advertised using EIGRP over MPLS WAN and the DMVPN tunnel to each router.

Between the remote site routers, this design uses an additional EIGRP LAN process (AS100) over the transit network in order to exchange routing information. The BGP process on the primary router is redistributed into EIGRP AS100. On the secondary router, EIGRP AS200 is redistributed into EIGRP AS100.

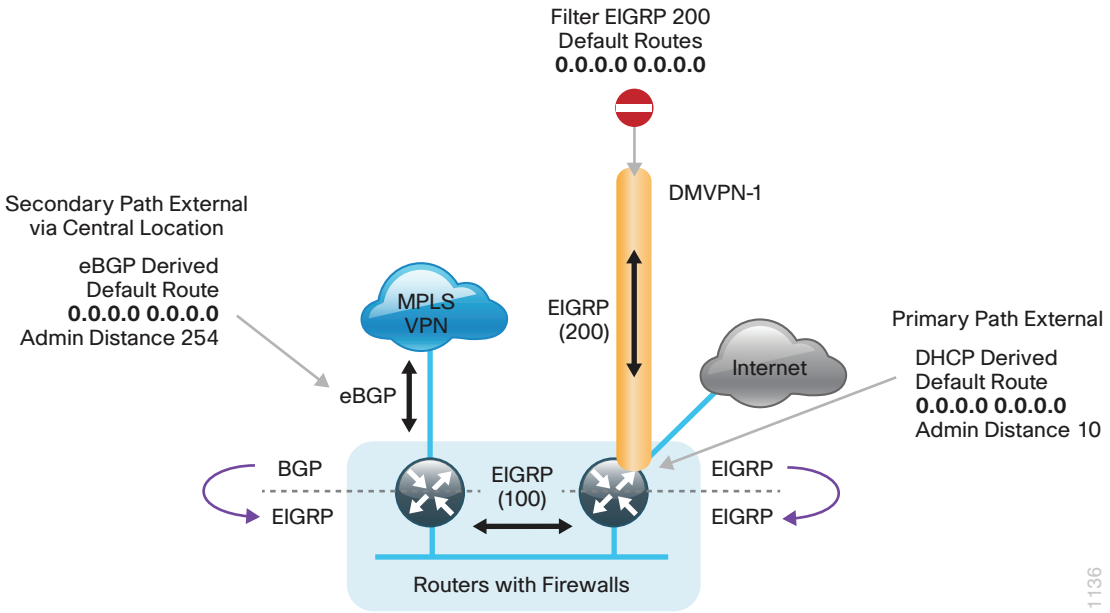
Figure 23 - Dual-router MPLS primary with DMVPN backup internal routing



In this configuration, the Internet-facing Ethernet interface on the secondary router is using DHCP to obtain an IP address from the ISP. This router is also using DHCP to install a default route into the local table. By default, this DHCP-installed static route has an AD value of 254.

In this design model, the default route to the local ISP should be preferred, so the AD value is changed to 10 on the secondary router. This ensures this route is chosen over other protocols such as EIGRP and BGP.

Figure 24 - Dual-router MPLS primary with DMVPN backup default routing



By redistributing the DHCP-derived route into EIGRP AS100 on the secondary router, the default route will be advertised to the primary router with a default AD value of 170 (external EIGRP).

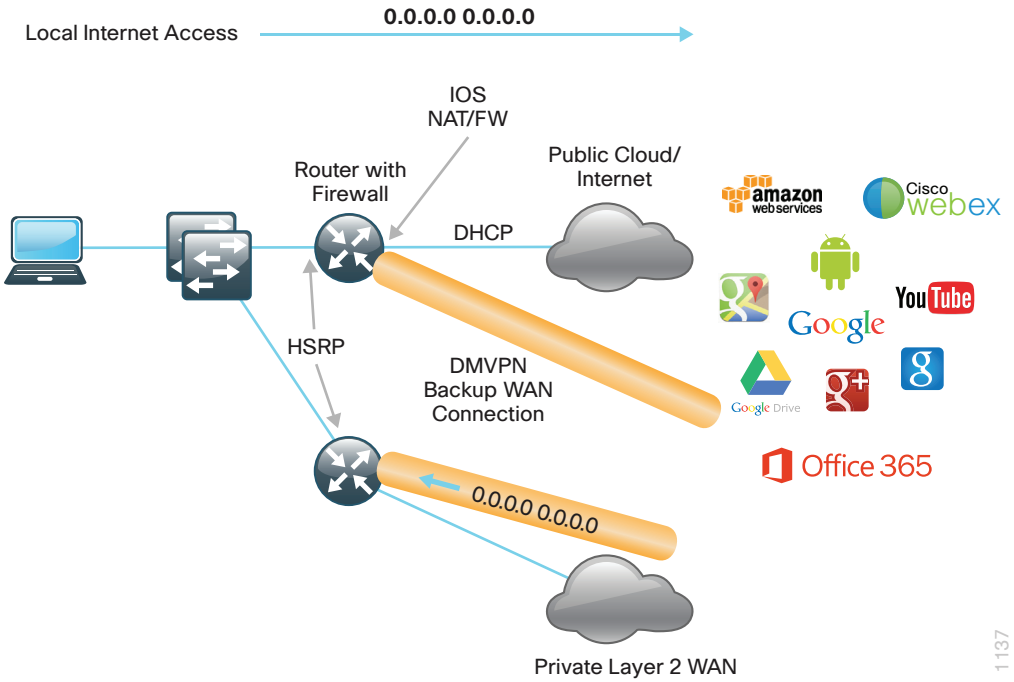
The central site default route is advertised over the MPLS network via eBGP with an AD value of 20 on the primary router. If the BGP default AD value of 20 is left on the primary router, it will be chosen over the EIGRP default received from the secondary router. In this case, the AD for the BGP default route on the primary router is changed to 254 so the local internet path is chosen. The MPLS connection will be used as a backup path for Internet traffic if the local Internet connection on the secondary router fails.

Once the VPN connection has been negotiated, the remote-site router will form an EIGRP adjacency with the DMVPN hub router and exchange routing information. The central site also has a local ISP default route that is advertised by EIGRP and is used for central-site Internet access. With a remote site local Internet configuration, you need to ensure the default route received over the DMVPN tunnel from the central site is filtered from the remote site routing table.

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

In this design, the remote site is configured with dual routers for added resiliency by using a L2 WAN service as the primary transport for internal traffic. The secondary router in this remote site configuration is connected to the Internet, providing local Internet access and DMVPN backup for internal traffic.

Figure 25 - Dual router Layer 2 WAN Primary, DMVPN backup internal routing

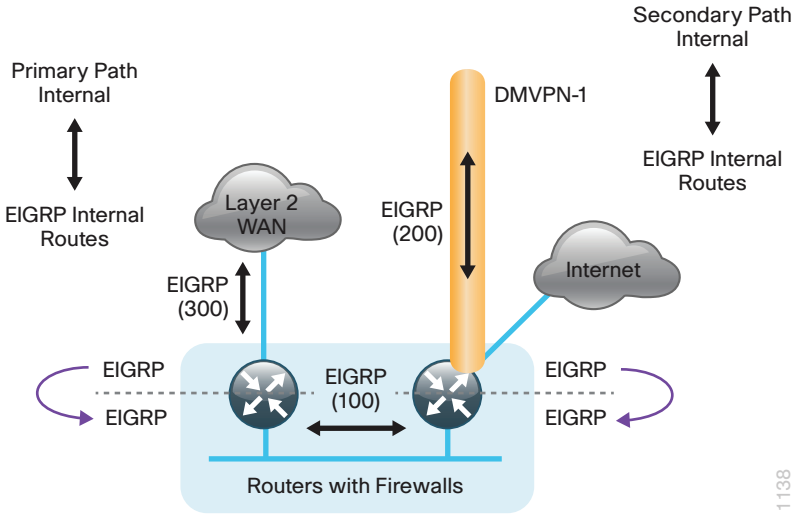


Internal traffic or traffic that stays within the organization will be routed primarily over the Layer 2 WAN connection on the primary router. If the L2 WAN fails, internal traffic will then be routed over an encrypted tunnel path to the central site by using DMVPN over the Internet on the secondary router.

Internal networks are advertised by using EIGRP over the L2 WAN and the DMVPN tunnel to each router. Preference for internal routing is determined by manual bandwidth and EIGRP default metric configurations.

Between the remote site routers, an additional EIGRP LAN process (AS100) is used over the transit network to exchange routing information. The EIGRP 300 process on the primary router is redistributed into EIGRP AS100. On the secondary router, EIGRP AS200 is redistributed into EIGRP AS100.

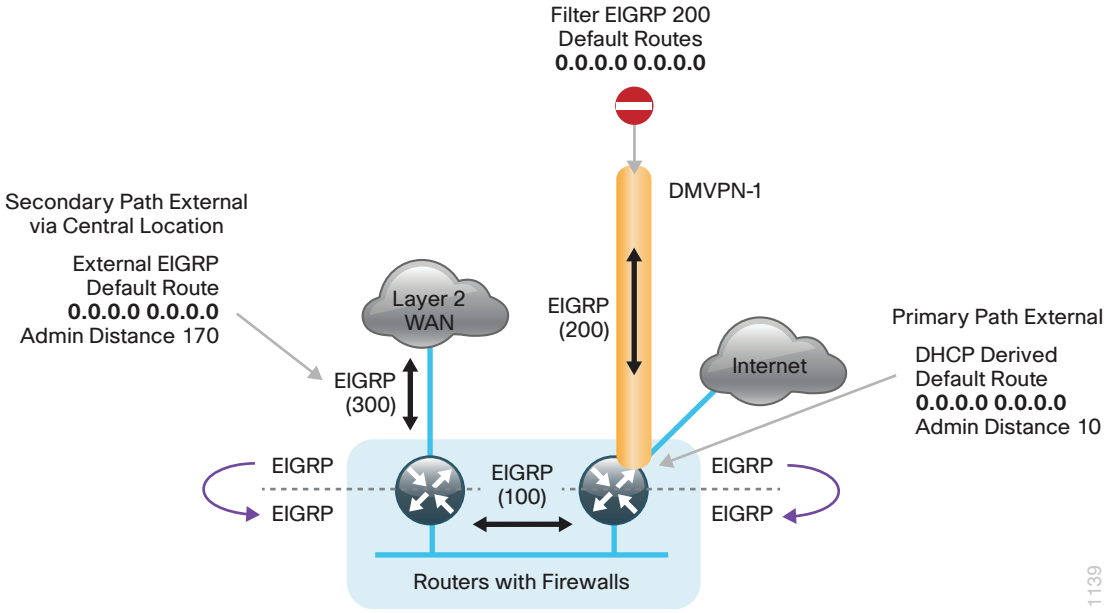
Figure 26 - Dual router Layer 2 WAN primary, DMVPN backup internal routing



In this configuration, the Internet-facing Ethernet interface on the secondary router is using DHCP to obtain an IP address from the ISP. This router is also using DHCP to install a default route into the local table. By default, this DHCP-installed static route has an AD value of 254.

In this design model, the default route to the local ISP should be preferred so the AD value is changed to 10 on the secondary router. This ensures this route is chosen over other protocols such as EIGRP and BGP.

Figure 27 - Dual router Layer 2 WAN primary, DMVPN backup default routing



By redistributing the DHCP-derived route into EIGRP AS100 on the secondary router, the default route will be advertised to the primary router with a default AD value of 170 (external EIGRP).

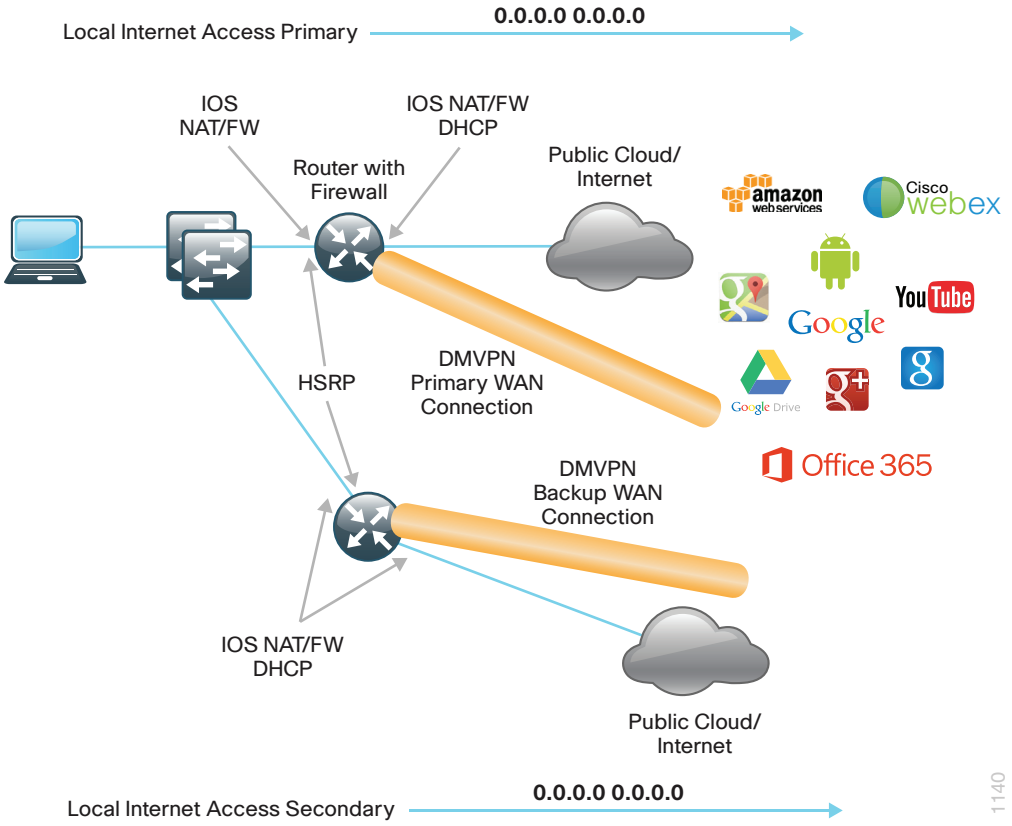
The central-site default route is advertised over the L2 WAN via EIGRP with an AD value of 170 on the primary router, but with a less desirable composite metric than the local default route. The L2 WAN connection will be used as a backup path for Internet traffic if the local Internet connection on the secondary router fails.

Once the VPN connection has been negotiated, the remote-site router will form an EIGRP adjacency with the DMVPN hub router and exchange routing information. The central site also has a local ISP default route used for central-site Internet access that is advertised by EIGRP. With a remote-site local Internet configuration, the default route received over the DMVPN tunnel from the central site must be filtered from the remote-site routing table.

DMVPN + DMVPN Remote Site (Dual Router, Dual Link)

In this design, the remote site is configured with dual routers for added resiliency by using dual Internet connections with DMVPN for as primary and backup connectivity.

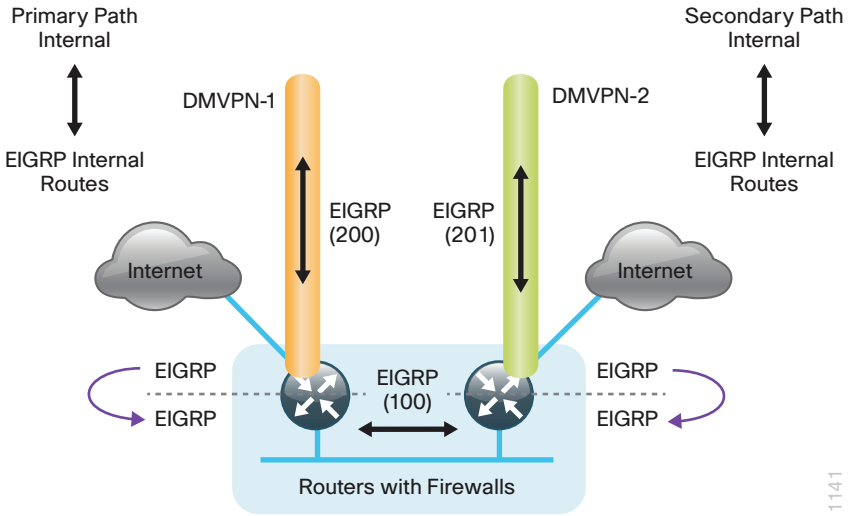
Figure 28 - Dual-Router, Dual Internet site



Internal traffic or traffic that stays within the organization will be encrypted and routed over the primary Internet (DMVPN-1) connection on the primary router. In the case of a failure on the primary ISP network, internal traffic will then be encrypted and routed over the secondary DMVPN tunnel (DMVPN-2) on the secondary router. Internal networks are advertised by using EIGRP over the DMVPN tunnels to each router and preference for internal routing is determined by manual bandwidth and default metric configurations.

Between the remote-site routers, an additional EIGRP LAN process (AS100) is used over the transit network. The WAN-facing EIGRP processes on each router are redistributed into EIGRP AS100.

Figure 29 - Dual-router, Dual-Internet internal routing

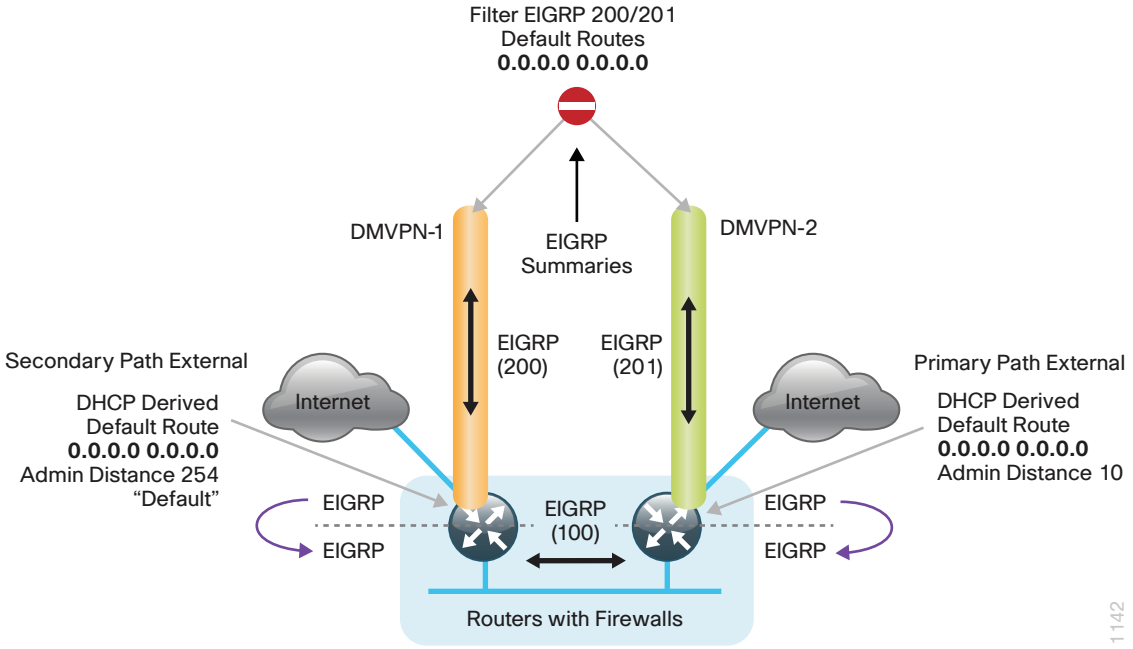


In this example, the Internet-facing Ethernet interfaces on the routers are using DHCP to obtain an IP address from the ISPs. The routers are also using DHCP to install default routes into the local tables on each router. By default, these DHCP-installed static routes have an AD value of 254. With two connections, preference needs to be configured for these routes.

In this configuration, preference is given to the local Internet connection on the secondary router by changing the AD value to 10 for the DHCP-derived default route and leaving the default value of 254 on the primary router. Using the secondary link as the primary path for external traffic provides more usable bandwidth during a normal network operational state.

The DHCP static routes are redistributed into EIGRP AS100 and exchanged between the remote -site routers. The default route will appear on the primary router with an AD value of 170 and will be installed in to the table over the local DCHP derived route with an AD value of 254. The backup path will appear on the secondary router with an AD value of 170 and will only be installed when the local primary default with the AD value of 10 is no longer in the table.

Figure 30 - Dual-router, dual-Internet default routing



Once the VPN connection has been negotiated, the remote-site router will form an EIGRP adjacency with the DMVPN hub router and exchange routing information. The central site also has a local ISP default route used for central-site Internet access that is advertised by EIGRP. With a remote-site local Internet configuration, the default route from the central location must be filtered from the remote site routing tables.

Tech Tip

The DMVPN spoke-to-spoke tunnel setup may not work properly with dual Internet configurations if the service providers implement security measures as outlined in RFC2827 per the guidelines of RFC 3013. These security measures are intended to reduce source address spoofing and denial of service (DoS) attack propagation by using ACLs and unicast RPF capabilities ingress at the ISP network edge.

Deployment Details

Follow the chart below and the corresponding configuration processes and procedures in order to deploy remote site routers with local Internet.

Reader Tip

The configurations that follow are remote site configurations only. For configuration details pertaining to the primary site WAN-aggregation routers, please see the MPLS WAN Technology Design Guide and the Layer 2 WAN Technology Design Guide.

For additional configuration details for DMVPN hub routers and design, please see the VPN WAN Technology Design Guide.

Design Parameters

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

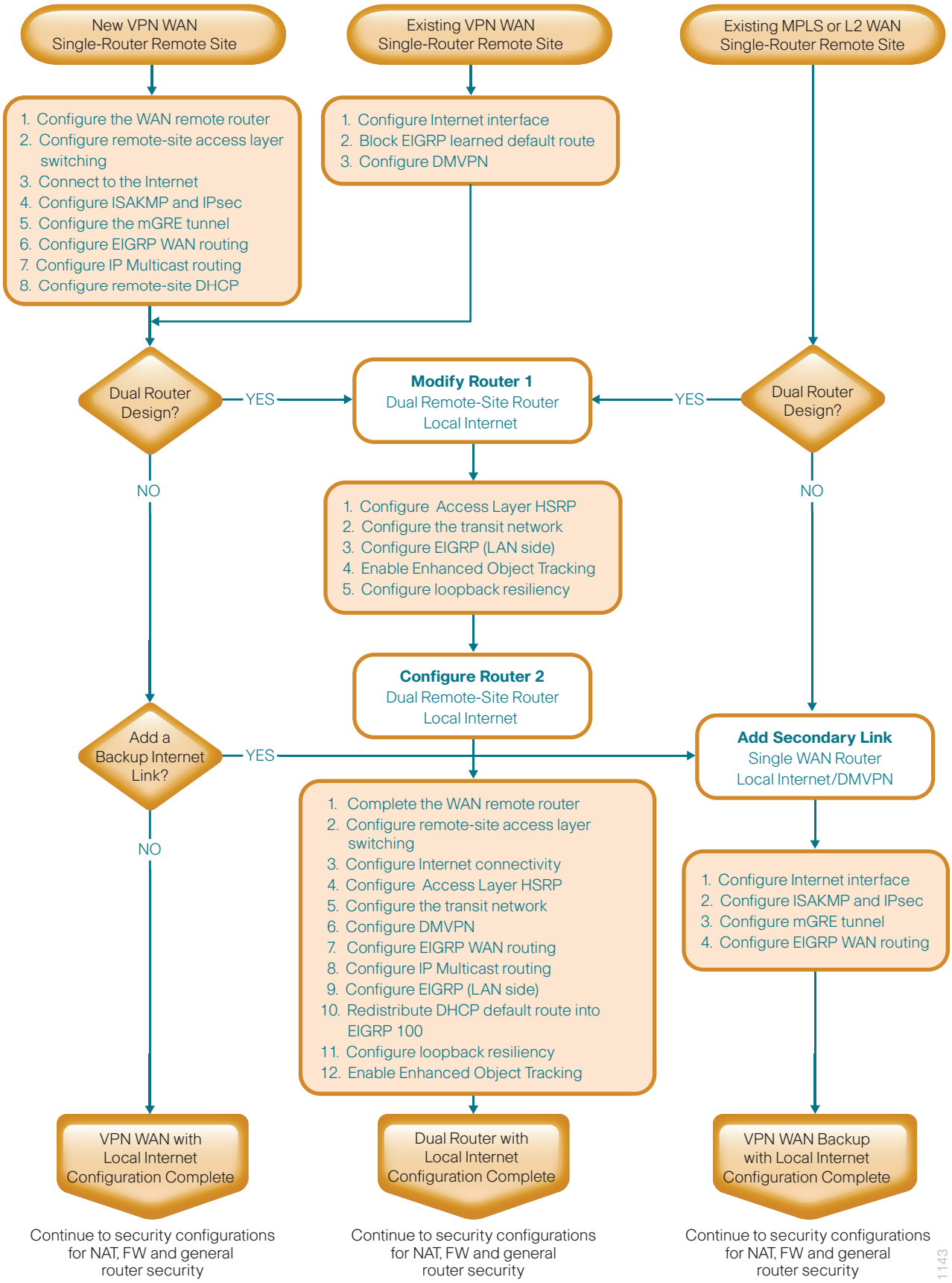
Table 6 - Universal design parameters

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

Tech Tip

This design guide uses a centralized DNS service from the primary site. The use of local DNS services to resolve for Internet resources based on proximity is outside of the scope of this guide.

Figure 31 - Configure new VPN WAN single-router remote sites with local Internet



PROCESS

Configuring a Spoke Router for a DMVPN Remote Site with Local Internet Access

1. Configure the WAN remote router
2. Configure remote-site access layer switching
3. Connect to the Internet
4. Configure ISAKMP and IPsec
5. Configure the mGRE Tunnel
6. Configure EIGRP WAN routing
7. Block EIGRP learned default route
8. Configure IP Multicast routing
9. Configure remote-site DHCP

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

You should also use this set of procedures when you configure a DMVPN + DMVPN remote site with local Internet. Use these procedures when you configure the first router of a dual-router, dual-link design.

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

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

Commands at a CLI or script prompt:

```
Router# enable
```

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

```
police rate 10000 pps burst 10000
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

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

Procedure 1 Configure the WAN remote router

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

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

```
hostname RS250-1941
```

Step 2: Configure a local login and password. The local login account and password provides basic access authentication to a router, which provides only limited operational privileges. The enable password secures access to the device configuration mode. By enabling password encryption, you prevent the disclosure of plain text passwords when viewing configuration files.

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

By default, HTTPS access to the router uses the enable password for authentication.

Step 3: If you want management access to the network infrastructure devices (SSH and HTTPS) to be controlled by authentication, authorization, and accounting (AAA), configure centralized user authentication.

As networks scale in the number of devices to maintain, there is an operational burden to maintain local user accounts on every device. A centralized AAA service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined in Step 2 on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

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

Step 4: Secure HTTP (HTTPS) and Secure Shell (SSH) are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Enable secure management of the network device by using the SSH and HTTPS protocols. Encrypt both protocols for privacy and turn off the unsecure protocols, Telnet and HTTP. Enable Secure Copy Protocol (SCP) to allow Cisco IOS code upgrades using Prime Infrastructure via the SSH-based SCP protocol.

Specify the transport preferred none on vty lines in order to prevent errant connection attempts from the CLI prompt. Without this command, if the ip name-server is unreachable, long timeout delays may occur for mistyped commands.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
ip scp server enable
line vty 0 15
 transport input ssh
 transport preferred none
```

Step 5: Enable synchronous logging. When synchronous logging of unsolicited messages and debug output is turned on, console log messages are displayed on the console after interactive CLI output is displayed or printed. With this command, you can continue typing at the device console when debugging is enabled.

```
line con 0
 transport preferred none
 logging synchronous
```

Step 6: Enable Simple Network Management Protocol (SNMP). This allows the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured both for a read-only and a read-write community string.

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

Step 7: If operational support is centralized in your network, increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network are able to access the device via SSH or SNMP.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
 access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```

Tech Tip

If you configure an access-list on the vty interface, you may lose the ability to use ssh to log in from one router to the next for hop-by-hop troubleshooting.

Step 8: Configure a synchronized clock. The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organization's network.

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

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

Step 9: Configure an in-band management interface. The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer 3 process and features are also bound to the loopback interface to ensure process resiliency.

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

```
interface Loopback 0
  ip address 10.255.251.250 255.255.255.255
  ip pim sparse-mode
```

Step 10: Bind the device processes for SNMP, SSH, PIM, TACACS+, and NTP to the loopback interface address. This provides optimal resiliency.

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

Step 11: Enable IP Multicast routing on the platforms in the global configuration mode. IP Multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than using multiple individual unicast streams or a broadcast stream that would propagate everywhere. IP Telephony MOH and IP Video Broadcast Streaming are two examples of IP Multicast applications.

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

This design, which is based on sparse mode multicast operation, uses Auto RP for a simple yet scalable way to provide a highly resilient RP environment.

```
ip multicast-routing
```

Step 12: Configure every Layer 3 switch and router to discover the IP Multicast RP with autorp. Use the **ip pim autorp listener** command to allow for discovery across sparse mode links. This configuration provides for future scaling and control of the IP Multicast environment and can change based on network needs and design.

```
ip pim autorp listener
```

Step 13: Enable sparse mode multicast operation for all Layer 3 interfaces in the network.

```
ip pim sparse-mode
```

Procedure 2 Configure remote-site access layer switching

Layer 2 EtherChannels are used to interconnect the remote site router to the access layer in the most resilient method possible. If your access-layer device is a single, fixed-configuration switch, a simple Layer 2 trunk between the router and switch is used.

Reader Tip

This guide includes only the additional steps to complete the access-layer configuration. For complete access-layer configuration details, see the Campus Wired LAN Technology Design Guide.

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 significant only locally.

Option 1: Layer 2 EtherChannel from router to access-layer switch

Step 1: Configure the port-channel interface on the router.

```
interface Port-channel1
 description EtherChannel link to RS250-A3650
 no shutdown
```

Step 2: Configure the EtherChannel member interfaces on the router. Ensure the physical interfaces tie to the logical port-channel by using the **channel-group** command. The number for the port-channel and channel-group must match.

```
interface GigabitEthernet0/1
 description RS250-A3650 Gig1/0/24
!
interface GigabitEthernet0/2
 description RS250-A3650 Gig2/0/24
!
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 1
  no shutdown
```

Tech Tip

Not all router platforms can support LACP to negotiate with the switch, so you configure EtherChannel statically.

Step 3: Configure EtherChannel member interfaces on the access-layer switch. Connect the router EtherChannel uplinks, which separate switches in the access-layer switch stack.

```
interface GigabitEthernet1/0/24
 description Link to RS250-1941 Gig0/1

interface GigabitEthernet2/0/24
 description Link to RS250-1941 Gig0/2
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport
 channel-group 1 mode on
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 load-interval 30
 macro apply EgressQoS
```

> **Tech Tip**
>
> The physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. Doing the configuration in this order allows for minimal configuration and reduces errors because most of the commands entered to a port-channel interface are copied to its members' interfaces and do not require manual replication.

Step 4: Configure EtherChannel trunk on the access-layer switch. Use an 802.1Q trunk for the connection, which allows the router to provide the Layer 3 services to all the VLANs defined on the access-layer switch. Prune the VLANs allowed on the trunk to only the VLANs that are active on the access-layer switch. When using EtherChannel, the interface type is port-channel, and the number must match the channel group configured in the previous step. Set DHCP Snooping and Address Resolution Protocol (ARP) inspection to trust.

```
interface Port-channel1
 description EtherChannel link to RS250-1941
 switchport trunk allowed vlan 64,69
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
 ip dhcp snooping trust
 load-interval 30
 no shutdown
```

> **Tech Tip**
>
> The Cisco Catalyst 3750 Series switches require the **switchport trunk encapsulation dot1q** command.

Option 2: Layer 2 trunk from router to access-layer switch

Step 1: Enable the physical interface on the router.

```
interface GigabitEthernet0/2
 description RS250-A3650 Gig1/0/24
 no ip address
 no shutdown
```

Step 2: Configure the trunk on the access-layer switch. Use an 802.1Q trunk for the connection, which allows the router to provide the Layer 3 services to all the VLANs defined on the access-layer switch. Prune the VLANs allowed on the trunk to only the VLANs that are active on the access-layer switch. Set DHCP Snooping and Address Resolution Protocol (ARP) inspection to trust.

```
interface  GigabitEthernet1/0/24
 description Link to RS250-1941 Gig0/2
 switchport trunk allowed vlan 64,69
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
```

```
logging event link-status
logging event trunk-status
ip dhcp snooping trust
load-interval 30
no shutdown
macro apply EgressQoS
```

Tech Tip

The Cisco Catalyst 3750 Series switches require the **switchport trunk encapsulation dot1q** command.

Procedure 3 Connect to the Internet

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

Step 1: Verify that the Internet-facing interface is disabled until the configuration is complete.

```
interface GigabitEthernet0/0
 shutdown
```

Step 2: Configure the Internet-facing interface to receive an IP address from the ISP via DHCP and to adjust the administrative distance of the default route.

```
interface GigabitEthernet0/0
 ip address dhcp
 ip dhcp client default-route distance 15
```

Tech Tip

Do not enable PIM on this interface because no multicast traffic should be requested from this interface.

Procedure 4 Configure ISAKMP and IPsec

Step 1: Configure the crypto keyring.

The crypto keyring defines a pre-shared key (PSK) valid for IP sources reachable within the DMVPN cloud. This key is a wildcard PSK (or password) 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 GLOBAL-KEYRING
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

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

The ISAKMP policy for DMVPN uses the following:

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

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

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

Step 3: Create the ISAKMP profile.

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

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

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:

- Encapsulating security payload (ESP) with the 256-bit AES encryption algorithm
- ESP with the Secure Hashed Algorithm (SHA) (Hashed Message Authentication Code [HMAC] variant) authentication algorithm

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

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

Step 5: Create the IPsec profile.

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

```
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile ISAKMP-INET-PUBLIC
```

Step 6: Increase the IPsec anti-replay window size.

```
crypto ipsec security-association replay window-size 1024
```

Tech Tip

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed.

It is recommended that you use the full 1024 window size in order to eliminate future anti-replay problems.

If you do not increase the window size, the router may drop packets and you may see the following error message on the router CLI:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
```

Procedure 5 Configure the mGRE Tunnel

First, 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.

Step 1: Configure the IP MTU to 1400 and the **ip tcp adjust-mss** to 1360. There is a 40-byte difference, which corresponds to the combined IP and TCP header length.

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

Step 2: Configure the tunnel.

DMVPN uses multipoint GRE (mGRE) tunnels. This type of tunnel requires a source interface only. The source interface should be the same interface used to connect to the Internet.

Enabling encryption on this interface requires you to apply the IPsec profile configured in the previous procedure.

```
interface Tunnel10
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN-PROFILE1
```

Step 3: Configure Next Hop Resolution Protocol (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 mGRE tunnel IP address of the DMVPN hub router. EIGRP (configured in the following Procedure 6, “Configure EIGRP WAN routing”) 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 7.

Table 7 - DMVPN tunnel parameters

DMVPN cloud	DMVPN hub public address (actual)	DMVPN hub public address (externally routable after NAT)	Tunnel IP address (NHS)	Tunnel number	NHRP network ID
Primary	192.168.18.10	172.16.130.1	10.4.34.1	10	101
Secondary	192.168.18.11	172.17.130.1	10.4.36.1	11	102

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

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

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

```
interface Tunnel10
 ip nhrp authentication cisco123
 ip nhrp map 10.4.34.1 172.16.130.1
 ip nhrp map multicast 172.16.130.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.34.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
```

Procedure 6 Configure EIGRP WAN routing

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

Step 1: Configure EIGRP for VPN WAN.

```
router eigrp WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  af-interface default
   passive-interface
  exit-af-interface
```

```
  af-interface Tunnel10
   no passive-interface
  exit-af-interface
  network 10.4.34.0 0.0.1.255
  network 10.5.0.0 0.0.255.255
  network 10.255.0.0 0.0.255.255
  eigrp router-id [IP address of Loopback0]
  eigrp stub connected summary
  exit-address-family
```

Step 2: Configure some specific requirements for the mGRE tunnel interface. Increase the EIGRP hello interval to 20 seconds and the EIGRP hold time to 60 seconds. This makes it so up to 500 remote sites can be accommodated on a single DMVPN cloud.

```
router eigrp WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  af-interface Tunnel10
   hello-interval 20
   hold-time 60
  exit-af-interface
  exit-address-family
```

Step 3: Configure EIGRP neighbor authentication. This allows EIGRP to form neighbor relationships with MD5 authentication in order to establish secure peering adjacencies and exchange route tables over the DMVPN WAN tunnel interface.

```
key chain WAN-KEY
 key 1
  key-string cisco
!
router eigrp WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  af-interface Tunnel10
   authentication mode md5
   authentication key-chain WAN-KEY
   no passive-interface
  exit-af-interface
 exit-address-family
```

Step 4: Advertise the remote-site LAN networks. The IP assignment for the remote sites was designed so that all of the networks in use can be summarized within a single aggregate route. The summary address as configured below suppresses the more specific routes. If any network within the summary is present in the route table, the summary is advertised to the DMVPN hub, which offers a measure of resiliency. If the various LAN networks cannot be summarized, then EIGRP continues to advertise the specific routes.

```
router eigrp WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  af-interface Tunnel10
   summary-address [summary network] [summary mask]
  exit-af-interface
         exit-address-family
```

Step 5: Configure tunnel routing affinity for hub traffic. This ensures traffic for the hub only routes via the local WAN interface.

```
ip route 172.16.130.1 255.255.255.255 GigabitEthernet0/0 dhcp
interface Tunnel10
  tunnel route-via GigabitEthernet0/0 mandatory
```

Procedure 7 Block EIGRP learned default route

In this configuration you need to filter the central-site default route from being received over the DMVPN tunnel.

Step 1: Create an access list to match the default route and permit all other routes.

```
ip access-list standard NO-DEFAULT
  deny 0.0.0.0
  permit any
```

Step 2: Create a route-map to reference the access list.

```
route-map BLOCK-DEFAULT permit 10
  match ip address NO-DEFAULT
```

Step 3: Configure an inbound distribute list.

```
router eigrp WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  topology base
   distribute-list route-map BLOCK-DEFAULT in
  exit-af-topology
 exit-address-family
```

Procedure 8 Configure IP Multicast routing

This procedure includes additional steps for configuring IP Multicast for a DMVPN tunnel on a router with IP Multicast already enabled.

Step 1: Enable IP PIM sparse mode on the DMVPN tunnel interface.

```
interface Tunnel10
 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.

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

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

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

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

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

Procedure 9 Configure remote-site DHCP

(Optional)

The previous procedure assumes the DHCP service has been configured centrally and uses the **ip helper-address** command to forward DHCP requests to the centralized DHCP server.

If you choose to run a local DHCP server on the remote-site router instead of centralizing the DHCP service, complete this procedure. This procedure uses a local DHCP service on the router in order to assign basic network configuration for IP phones, wireless access points, users' laptop and desktop computers, and other endpoint devices.

> **Tech Tip**
>
> If you intend to use a dual-router remote-site design, you should use a resilient DHCP solution, such as a centralized DHCP server. Options for resilient DHCP at the remote site include using Cisco IOS Software on a distribution-layer switch stack or implementing a dedicated DHCP server solution.

Step 1: Remove the previously configured **ip helper-address** commands for any interface that uses a local DHCP server.

Step 2: Configure a DHCP scope for data endpoints, excluding DHCP assignment for the first 19 addresses in the subnet.

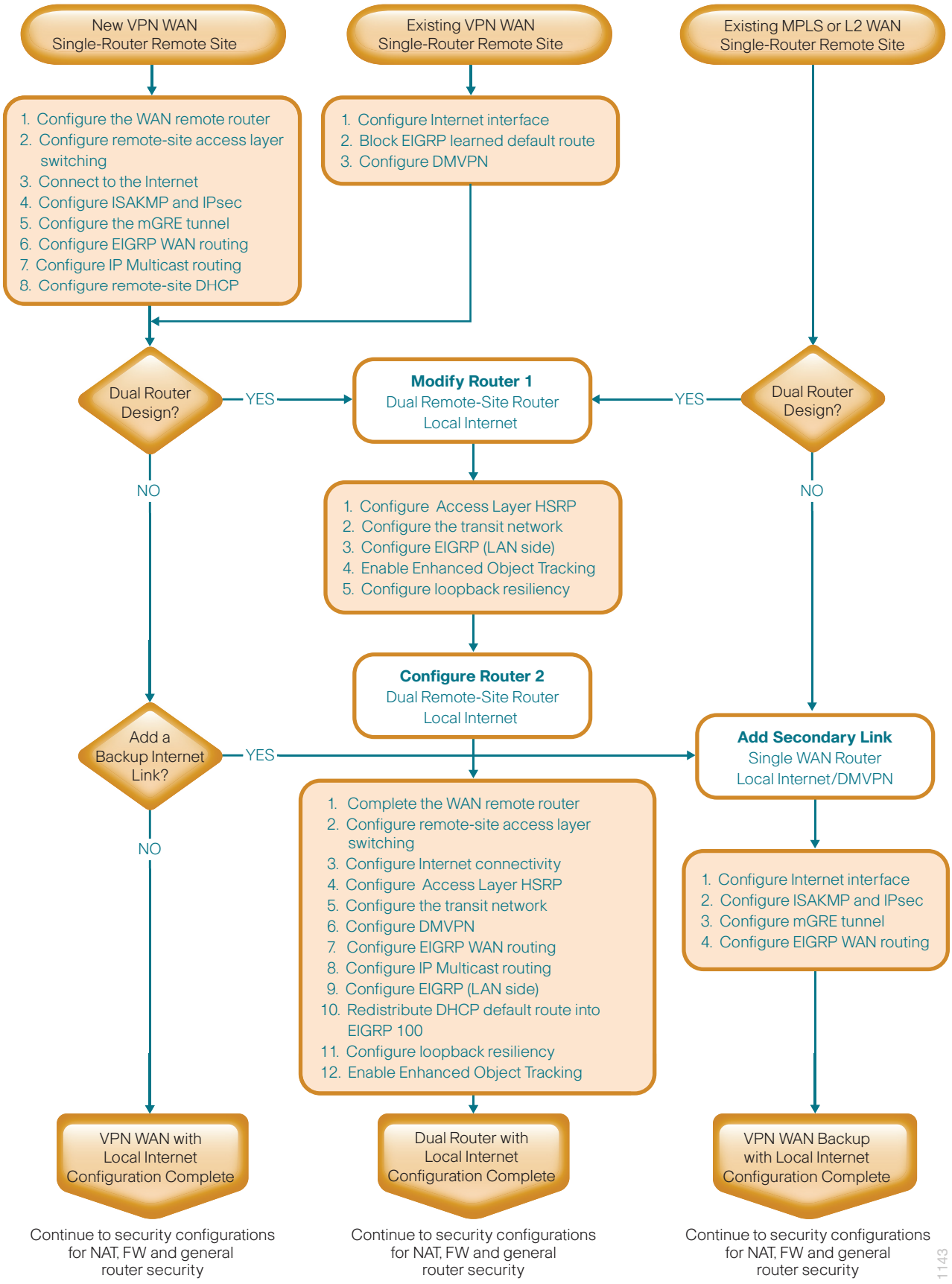
```
ip dhcp excluded-address 10.5.244.1 10.5.244.19
ip dhcp pool DHCP-Wired-Data
 network 10.5.244.0 255.255.255.0
 default-router 10.5.244.1
 domain-name cisco.local
 dns-server 10.4.48.10
```

> **Tech Tip**
>
> This design guide uses a centralized DNS service over the Internal WAN and does not address the potential need to provision split DNS services, allowing remote sites to resolve locally for external resources in better proximity to the remote office location.

Step 3: Configure a DHCP scope for voice endpoints, excluding DHCP assignment for the first 19 addresses in the subnet. Voice endpoints require an option field to tell them where to find their initial configuration. Different vendors use different option fields, so the number may vary based on the voice product you choose (for example, Cisco uses DHCP option 150).

```
ip dhcp excluded-address 10.5.245.1 10.5.245.19
ip dhcp pool DHCP-Wired-Voice
 network 10.5.245.0 255.255.255.0
 default-router 10.5.245.1
 domain-name cisco.local
 dns-server 10.4.48.10
```

Figure 32 - Existing VPN WAN single-router remote site



PROCESS

Converting Existing DMVPN Spoke Routers from Central to Local Internet

1. Configure Internet interface
2. Block EIGRP learned default route
3. Configure DMVPN

This section covers the configurations necessary to migrate an existing VPN WAN remote site router from centralized Internet access to local Internet. This process assumes the remote-site DMVPN spoke router was previously configured using the VPN WAN Technology Design Guide.

Figure 33 - Single-router DMVPN WAN site

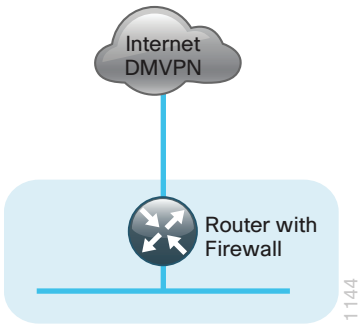
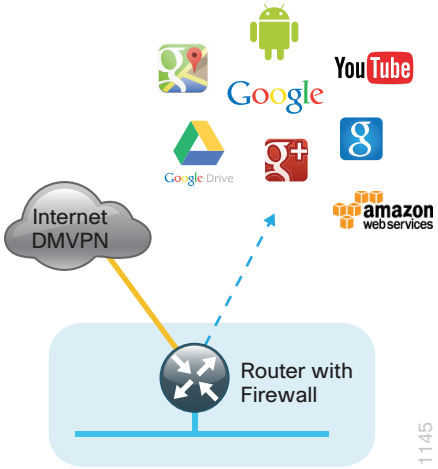


Figure 34 - Single-router DMVPN WAN site with local Internet



Procedure 1 Configure Internet interface

In this configuration, local Internet traffic will be routed using split-tunneling outside the DMVPN tunnel. VPN WAN remote sites can use either static or dynamically assigned IP addresses. Cisco tested the design with a DHCP assigned external address, which also provides a dynamically configured default route.

Tech Tip

If you are remotely connected to the remote-site router via SSH, you will be disconnected from the router console. Shutting down the Internet interface will drop the existing tunnel and isolate the router.

Step 1: Verify that the Internet facing is disabled until the configuration is complete.

```
interface GigabitEthernet0/0
 shutdown
```

Step 2: Remove the VRF from the Internet interface. This will automatically remove the IP address configuration from the interface.

```
interface GigabitEthernet0/0
 no ip vrf forwarding INET-PUBLIC1
```

Step 3: Configure the Internet-facing interface to receive an IP address from the ISP via DHCP and to adjust the administrative distance of the default route.

```
interface GigabitEthernet0/0
  ip address dhcp
  ip dhcp client default-route distance 15
```

Tech Tip

The default behavior is for the router to install a default static route in the local table with an AD value of 254. We are using an AD of 15 to ensure this path is preferred over other learned routes via protocols such as BGP and EIGRP.

Procedure 2 Block EIGRP learned default route

In this configuration we are need to filter the central-site default route from being received over the DMVPN tunnel.

Step 1: Create an access list to match the default route and permit all other routes.

```
ip access-list standard NO-DEFAULT
  deny 0.0.0.0
  permit any
```

Step 2: Create a route-map to reference the access list.

```
route-map BLOCK-DEFAULT permit 10
  match ip address NO-DEFAULT
```

Step 3: Configure an inbound distribute list

```
router eigrp WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  topology base
   distribute-list route-map BLOCK-DEFAULT in
  exit-af-topology
 exit-address-family
```

Procedure 3 Configure DMVPN

In this design, internal traffic will be routed over the Internet VPN WAN connection to the central site. This will require the removal of the Internet VRF and configurations that reference the VRF. Follow these procedures to reconfigure DMVPN for local Internet access.

Step 1: Remove protection from the tunnel interface.

```
interface Tunnel10
  no tunnel protection ipsec profile DMVPN-PROFILE1
```

Step 2: Remove the existing ISAKMP profile.

```
no crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
```

Step 3: Remove the exiting keyring configuration that references the Internet VRF.

```
no crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
```

Step 4: Remove the Internet VRF from the router configuration. This automatically removes the existing VRF configuration from the tunnel interface and the IP address configuration from any interfaces that were configured for vrf INET-PUBLIC1.

```
no ip vrf INET-PUBLIC1
```

The following message is generated when you delete the VRF:

```
% IPv4 addresses from all interfaces in VRF INET-PUBLIC1 have been removed
```

Step 5: Configure a new keyring in the global table and define the pre-shared key.

```
crypto keyring GLOBAL-KEYRING
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

Step 6: Configure a new ISAKMP profile referencing the new keyring.

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

Step 7: Configure the IPSEC profile so that it references the new ISAKMP profile.

```
crypto ipsec profile DMVPN-PROFILE1
 set isakmp-profile ISAKMP-INET-PUBLIC
```

Step 8: Configure tunnel routing affinity for hub traffic. This ensure traffic for the hub only routes via the local WAN interface.

```
ip route 172.16.130.1 255.255.255.255 GigabitEthernet0/0 dhcp
interface Tunnel10
  tunnel route-via GigabitEthernet0/0 mandatory
```

Step 9: Apply crypto map to the tunnel interface.

```
interface Tunnel10
  tunnel protection ipsec profile DMVPN-PROFILE1
```

Tech Tip

Local Internet routing will not function until you configure NAT (see the Configuring Cisco IOS NAT process in this guide). It is also recommended that you complete the ZBFW and general security configuration before enabling the Internet facing router interface.

PROCESS

Enabling DMVPN Backup on a Remote-Site Router

1. Configure Internet interface
2. Configure ISAKMP and IPsec
3. Configure the mGRE tunnel
4. GETVPN and DMVPN single router configuration
5. Configure EIGRP WAN routing
6. Configure IPSLA for DHCP route removal

Use this set of procedures for any of the following single router topologies: MPLS + DMVPN remote site, Layer 2 WAN + DMVPN remote site, or DMVPN + DMVPN remote site with local Internet.

This set of procedures includes the additional steps necessary to add a DMVPN backup link and local Internet to a remote-site router that has already been configured with a primary WAN link using one of the following processes.

In this guide:

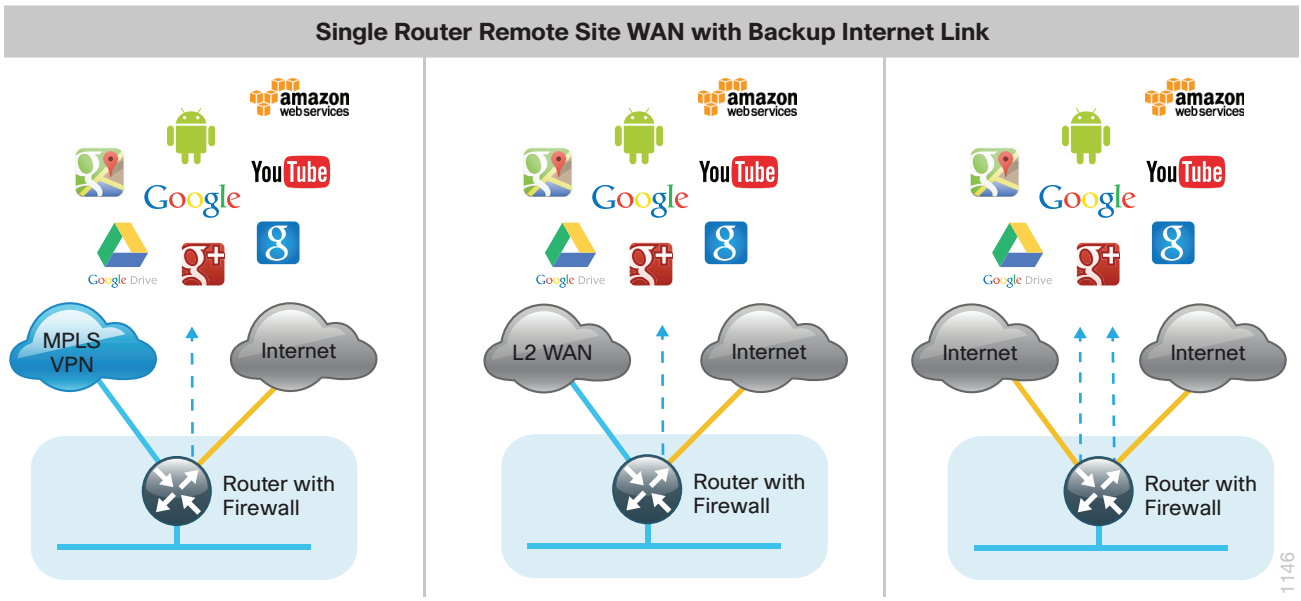
- Configuring a Spoke Router for a DMVPN Remote Site with Local Internet Access

Or in these guides:

- MPLS WAN Technology Design Guide–Remote-Site MPLS CE Router Configuration
- Layer 2 WAN Technology Design Guide–Remote-Site Layer 2 WAN CE Router Configuration

Only the additional procedures to add the DMVPN backup and local Internet access to the running remote-site router are included here.

Figure 35 - Single-Router WAN sites with local Internet



Procedure 1 Configure Internet interface

In this configuration, local Internet traffic is routed by using split-tunneling outside the DMVPN tunnel. VPN WAN remote sites can use either static or dynamically assigned IP addresses. Cisco tested the design with a DHCP-assigned external address, which also provides a dynamically configured default route.

Tech Tip

The default behavior is for the router to install a default static route in the local table with an AD value of 254. Using an AD value of 10 allows the secondary link to become the preferred path for Internet traffic.

Step 1: Verify that the Internet-facing interface is disabled until the configuration is complete.

```
interface GigabitEthernet0/1
 shutdown
```

Step 2: Configure the Internet-facing interface to receive an IP address from the ISP via DHCP and to adjust the administrative distance of the default route.

```
interface GigabitEthernet0/1
 ip address dhcp
 ip dhcp client default-route distance 10
```

Procedure 2 Configure ISAKMP and IPsec

For MPLS primary and L2 WAN primary configurations you will need to configure DMVPN ISAKMP and IPsec policies. VPN WAN configurations will already have these steps configured.

Step 1: If necessary, configure a crypto keyring in the global table and define the pre-shared key.

```
crypto keyring GLOBAL-KEYRING
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

Step 2: If necessary, configure the ISAKMP policy and Dead Peer Detection.

The ISAKMP policy for DMVPN uses the following:

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

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

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

Step 3: Create the ISAKMP profile.

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

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, you must configure the IPsec transform for transport mode.

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

Step 5: Create the IPsec profile.

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

```
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile ISAKMP-INET-PUBLIC
```

Step 6: Increase the IPsec anti-replay window size.

```
crypto ipsec security-association replay window-size 1024
```

Tech Tip

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec security association (SA) is needed.

It is recommended that you use the full 1024 window size in order to eliminate future anti-replay problems.

If you do not increase the window size, the router may drop packets and you may see the following error message on the router CLI:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
```

Procedure 3 Configure the mGRE tunnel

Follow these procedures to configure DMVPN for secure encrypted communications with the central-site location using a secondary Internet WAN link on a single WAN router.

When adding a backup link to an existing MPLS WAN or L2 WAN primary configuration, use the Primary DMVPN cloud (DMVPN1) for the backup connection to the primary site. For VPN WAN primary configurations, use the secondary DMVPN cloud (DMVPN-2) for the backup connection to the primary site.

Table 8 - Parameters for DMVPN configuration

Parameter	Primary DMVPN cloud (DMVPN-1)	Secondary DMVPN cloud (DMVPN-2)
crypto keyring	GLOBAL-KEYRING	GLOBAL-KEYRING
crypto isakmp profile	ISAKMP-INET-PUBLIC	ISAKMP-INET-PUBLIC
crypto ipsec profile	DMVPN-PROFILE1	DMVPN-PROFILE2
Tunnel number	Interface tunnel 10	Interface tunnel 11
Tunnel IP address (NHS)	10.4.34.1	10.4.36.1
NHRP network ID	101	102
EIGRP process name	WAN-DMVPN-1	WAN-DMVPN-2
EIGRP AS	**200**	**201**

Next, configure the basic interface settings.

Step 1: Configure the tunnel.

```
Interface Tunnel10
 ip address 10.4.34.240 255.255.254.0
 ip mtu 1400
 ip pim dr-priority 0
 ip pim nbma-mode
 ip pim sparse-mode
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN-PROFILE1
```

Step 2: Configure NHRP.

```
Interface Tunnel 10
 ip nhrp authentication cisco123
 ip nhrp map multicast 172.16.130.1
 ip nhrp map 10.4.34.1 172.16.130.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.34.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
Configure tunnel bandwidth.  The bandwidth setting should be set to match the
Internet bandwidth.
Interface Tunnel10
 bandwidth [bandwidth (kbps)]
```

Step 3: Configure tunnel routing affinity for hub traffic. This ensures traffic for the hub only routes via the local WAN interface.

```
ip route 172.16.130.1 255.255.255.255 GigabitEthernet0/1 dhcp

interface Tunnel10
  tunnel route-via GigabitEthernet0/1 mandatory
```

Step 4: Configure tunnel protection.

```
interface Tunnel10
 tunnel protection ipsec profile DMVPN-PROFILE1
```

Tech Tip

Local Internet routing will not function until you configure NAT in a subsequent process. It is recommended that you complete the ZBFW and general security configuration before enabling the Internet-facing router interface.

Procedure 4 GETVPN and DMVPN single router configuration

If you are configuring a secondary Internet link with DMVPN on an MPLS Primary router also running GETVPN, you need to use a single shared crypto keyring for GETVPN and DMVPN to work concurrently.

Step 1: If you already have a Global-Keyring as used in the GETVPN guide, ensure that the more specific pre-shared-keys are at the top of the list and the match-all pre-shared-key is at the bottom. Move the pre-shared keys for GETVPN to the global keyring.

```
Crypto keyring GLOBAL-KEYRING
  pre-shared-key address 10.4.32.151 key c1sco123
  pre-shared-key address 10.4.32.152 key c1sco123
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

Tech Tip

When a keyring is configured in the global table it takes precedence over other pre-shared key configurations.

When you add the following crypto keyring to configuration,

```
crypto keyring GLOBAL-KEYRING
 pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

the following ISAKMP pre-shared key statements become invalid.

```
crypto isakmp key c1sco123 address 10.4.32.151
crypto isakmp key c1sco123 address 10.4.32.152
```

Merge all ISAKMP pre-shared keys into the global crypto keyring if you required concurrent GET VPN and DMVPN in a non-VRF aware configuration.

For more information, see the GET VPN Technology Design Guide.

Procedure 5 Configure EIGRP WAN routing

Step 1: In this configuration we need to configure EIGRP to exchange internal routes with the central site and filter the central site default route for being received over the DMVPN tunnel.Configure the EIGRP WAN process.

For MPLS WAN and Layer 2 WAN configurations, EIGRP AS200 is configured on the router for the primary DMVPN cloud. All interfaces on the router are EIGRP AS200 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 WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  af-interface default
   passive-interface
  exit-af-interface
  af-interface Tunnel10
   no passive-interface
```

```
  exit-af-interface
 network 10.4.0.0 0.1.255.255
 network 10.255.0.0 0.0.255.255
 eigrp router-id 10.255.253.240
 eigrp stub connected summary
exit-address-family
```

Step 2: Configure EIGRP values for the mGRE tunnel interface.

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

```
       router eigrp WAN-DMVPN-1
address-family ipv4 unicast autonomous-system 200
  af-interface Tunnel10
   hello-interval 20
   hold-time 60
  exit-af-interface
exit-address-family
```

Step 3: Configure EIGRP neighbor authentication to allow EIGRP to form neighbor relationships with MD5 authentication in order to establish secure peering adjacencies and exchange route tables over the DMVPN WAN tunnel interface.

```
key chain WAN-KEY
 key 1
  key-string cisco
!
router eigrp WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  af-interface Tunnel10
   authentication mode md5
   authentication key-chain WAN-KEY
  exit-af-interface
 exit-address-family
```

Step 4: Configure EIGRP route summarization.

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

```
router eigrp WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  af-interface Tunnel10
   summary-address [summary network] [summary mask]
  exit-af-interface
 exit-address-family
```

Step 5: Create an access list to match the default route and permit all other routes.

```
ip access-list standard NO-DEFAULT
  deny 0.0.0.0
  permit any
```

Step 6: Create a route-map to reference the access list.

```
route-map BLOCK-DEFAULT permit 10
  match ip address NO-DEFAULT
```

Step 7: Block the default route on the tunnel interface on the EIGRP WAN process by using a distribute list referencing the route-map configured in the previous step.

```
router eigrp WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  topology base
   distribute-list route-map BLOCK-DEFAULT in
  exit-af-topology
exit-address-family
```

Procedure 6 Configure IPSLA for DHCP route removal

(Optional)

In many cases you may need to ensure connectivity issues with your ISP don't cause black-hole routing conditions. Failure conditions can exist where the DHCP address and route are not removed from the remote-site router when connectivity issues exist with the broadband service or local premise equipment. There may also be circumstances if certain services are unreachable within via the local ISP connection that you want to reroute to a secondary Internet service.

In this solution, an IPSLA probe is used to monitor the status of the ISP connection used as the primary path for local Internet traffic. In this example, the failure of probes to two different IP hosts triggers the removal of the default route. If either probe is active the route will remain.

Step 1: Configure the IPSLA probes.

```
ip sla 110
 icmp-echo 172.18.1.253 source-interface GigabitEthernet0/1
 threshold 1000
 frequency 15
ip sla schedule 110 life forever start-time now
ip sla 111
 icmp-echo 172.18.1.254 source-interface GigabitEthernet0/1
 threshold 1000
 frequency 15
ip sla schedule 111 life forever start-time now
```

Step 2: Configure the tracking parameters and logic for the IPSLA probes.

```
track 60 ip sla 110 reachability
track 61 ip sla 111 reachability
track 62 list boolean or
 object 60
 object 61
```

Step 3: Configure ACL and route map to match and set the next-hop for the IPSLA probe traffic. This ensures proper recovery when service is restored after a failure.

```
ip access-list extended SLA-SET-NEXT-HOP
 permit icmp any host 172.18.1.253
 permit icmp any host 172.18.1.254

route-map PBR-SLA-SET-NEXT-HOP permit 10
 match ip address SLA-SET-NEXT-HOP
 set ip next-hop dynamic dhcp
```

Step 4: Configure policy routing for local traffic.

```
ip local policy route-map PBR-SLA-SET-NEXT-HOP
```

Step 5: Bind the IPSLA probes and tracking to the DHCP assigned route.

```
interface GigabitEthernet0/1
 ip dhcp client route track 62
```

PROCESS

Modifying Router 1 for a Dual-Router Design

1. Configure Access Layer HSRP
2. Configure the transit network
3. Configure EIGRP (LAN side)
4. Configure default route administrative distance
5. Enable enhanced object tracking
6. Configure loopback resiliency

This process is required when the first router has already been configured by using one of the following processes.

In this guide:

- Configuring a Spoke Router for a DMVPN Remote Site with Local Internet Access
- Converting Existing DMVPN Spoke Routers from Central to Local Internet

Or in these guides:

- MPLS WAN Technology Design Guide–Remote-Site MPLS CE Router Configuration
- Layer 2 WAN Technology Design Guide–Remote-Site Layer 2 WAN CE Router Configuration

Procedure 1 Configure Access Layer HSRP

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

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

Table 9 - WAN remote-site HSRP parameters (dual router)

Router	HSRP role	Virtual IP address (VIP)	Real IP address	HSRP priority	PIM DR priority
Primary	Active	.1	.2	110	110
Secondary	Standby	.1	.3	105	105

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

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

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

Step 1: Configure HSRP. This procedure should be repeated for all data or voice subinterfaces.

```
interface [type][number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [LAN network 1 address] [LAN network 1 netmask]
 ip helper-address 10.4.48.10
 ip pim sparse-mode
 ip pim dr-priority 110
 standby version 2
 standby 1 ip [LAN network 1 gateway address]
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

Example: Layer 2 link

```
interface GigabitEthernet0/2
 no ip address
 no shutdown
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.252.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.252.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
!
interface GigabitEthernet0/2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.253.2 255.255.255.0
 ip helper-address 10.4.48.10
```

```
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.253.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

Procedure 2 Configure the transit network

The transit network is configured between the two routers. This network is used for router-router communication and to avoid hairpinning.

Step 1: Configure the transit network subinterface. 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 [type][number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [transit net address] [transit net netmask]
 ip pim sparse-mode
```

Example

```
interface GigabitEthernet0/2.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.248.1 255.255.255.252
 ip pim sparse-mode
```

Step 2: Add the transit network VLAN to the access layer switch. If the VLAN does not already exist on the access layer switch, configure it now.

```
vlan 99
 name Transit-net
```

Step 3: Add the transit network VLAN to existing access layer switch trunk.

```
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan add 99
```

Procedure 3 Configure EIGRP (LAN side)

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

Step 1: Configure the EIGRP LAN process (AS100) facing the access layer by using EIGRP named mode.

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 DMVPN mGRE interface in the EIGRP LAN process.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
 af-interface [Transit interface]
   no passive-interface
  exit-af-interface
 network [network] [inverse mask]
 eigrp router-id [IP address of Loopback0]
 exit-address-family
```

Step 2: Configure EIGRP neighbor authentication to allow EIGRP to form neighbor relationships with MD5 authentication in order to establish secure peering adjacencies and exchange route tables.

```
key chain LAN-KEY
 key 1
  key-string cisco
!
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface [Transit interface]
   authentication mode md5
   authentication key-chain LAN-KEY
  exit-af-interface
 exit-address-family
```

Step 3: Redistribute WAN routing protocol into the EIGRP LAN process.

The remote-site router is using either BGP for an MPLS connection or EIGRP for a Layer 2 WAN or DMVPN connection. The WAN-facing routing protocol in use needs to be distributed into the EIGRP LAN process.

EIGRP WAN processes are already configured in a DMVPN or Layer 2 WAN deployment, and routes from these EIGRP processes are redistributed. Since the routing protocol is the same, no default metric is required.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  topology base
   redistribute eigrp 200
  exit-af-topology
exit-address-family
```

BGP is already configured for a MPLS deployment. The BGP routes are redistributed into EIGRP with a default metric. By default, only the WAN bandwidth and delay values are used for metric calculation.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  topology base
   default-metric [WAN bandwidth] [WAN delay] 255 1 1500
   redistribute bgp 65511
  exit-af-topology
 exit-address-family
```

Example: EIGRP into EIGRP

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
  af-interface GigabitEthernet0/2.99
   authentication mode md5
   authentication key-chain LAN-KEY
   no passive-interface
  exit-af-interface
  topology base
   redistribute eigrp 200
  exit-af-topology
 network 10.4.0.0 0.1.255.255
 network 10.255.0.0 0.0.255.255
 eigrp router-id 10.255.253.242
exit-address-family
```

Example: BGP into EIGRP

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
  af-interface GigabitEthernet0/2.99
   authentication mode md5
   authentication key-chain LAN-KEY
   no passive-interface
  exit-af-interface
  topology base
   default-metric 100000 100 255 1 1500
   redistribute bgp 65511
  exit-af-topology
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 eigrp router-id 10.255.253.242
exit-address-family
```

Procedure 4 Configure default route administrative distance

In dual router remote sites you need to ensure the proper administrative (AD) distance for the default route is configured on the primary router. For MPLS WAN primary and VPN WAN primary options, the AD needs to be modified for the backup Internet path. Layer2 WAN configurations should not require any modification to the default route.

Option 1: MPLS WAN Primary

For this configuration, the default route to the central hub location comes into the remote site router through the MPLS connection via eBGP with an AD of 20. To ensure preference behavior for local Internet, change the AD of the eBGP default to a value of 254.

Step 1: Configure an access list matching the default route.

```
Ip access-list standard DEFAULT-IN
 permit 0.0.0.0
```

Step 2: Configure BGP to set the default route received from the eBGP neighbor to a value of 254. All other routes remain as AD 20. Using the **distance** command, reference the ACL created in the previous step.

```
router bgp 65511
 distance 254 192.168.4.50 0.0.0.0 DEFAULT-IN
```

Option 2: VPN WAN Primary

For this configuration the Internet WAN interface is the primary path for internal traffic over the DMVPN tunnel and secondary for local Internet connectivity. The default route to the Internet on this router needs to be configured with an AD of 254.

For dual-router configurations, you also need to redistribute this DHCP-originated default route into EIGRP AS100 for reachability on both WAN routers.

Step 1: Configure the Internet-facing interface to a DHCP default route with the default AD of 254.

```
interface GigabitEthernet0/0
 ip address dhcp
 ip dhcp client default-route distance 254
```

Step 2: Configure an access list to match the default route.

```
ip access-list standard DHCP-DEFAULT
 remark DHCP default route
 permit 0.0.0.0
```

Step 3: Configure a route map referencing the access list that matches the default route.

```
route-map LOCAL-DEFAULT permit 10
 match ip address DHCP-DEFAULT
```

Step 4: Redistribute the static default route installed by DHCP into the EIGRP LAN process (AS100) by using the route map.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  topology base
   redistribute static route-map LOCAL-DEFAULT
  exit-af-topology
exit-address-family
```

Procedure 5 Enable enhanced object tracking

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

The HSRP active router (MPLS CE, Layer 2 WAN CE, or primary DMVPN spoke) can use the IP SLA feature to send echo probes to an upstream neighbor router and if that 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.

Step 1: Enable the IP SLA probe.

Use standard ICMP echo (ping) probes, and send them at 15 second intervals. Responses must be received before the timeout of 1000 ms expires. If using the MPLS PE router as the probe destination, the destination address is the same as the BGP neighbor address. If using the Layer WAN CE router as the probe destination, then the destination address is either the CE router address when using the simple demarcation or the subinterface CE router address when using a trunked demarcation. If using the DMVPN hub router as the probe destination, then the destination address is the mGRE tunnel address.

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

Step 2: Configure EOT.

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

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

Step 3: Link HSRP with the tracked object.

All data or voice subinterfaces should enable HSRP tracking.

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

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

Example

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

Procedure 6 Configure loopback resiliency

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

Option 1: MPLS CE Router with BGP

Step 1: Configure BGP to advertise the adjacent router's loopback IP address.

```
router bgp 65511
 network 10.255.254.242 mask 255.255.255.255
```

Option 2: DMVPN Spoke Router or Layer 2 WAN CE Router with EIGRP

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

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

Example

```
ip access-list standard R2-LOOPBACK
 permit 10.255.254.242
!
route-map REDISTRIBUTE-LIST permit 10
 match ip address R2-LOOPBACK
```

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

Example: DMVPN Spoke Router

```
router eigrp WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  topology base
   redistribute eigrp 100 route-map REDISTRIBUTE-LIST
  exit-af-topology
eigrp stub connected summary redistributed
exit-address-family
```

Example: Layer 2 WAN CE Router

```
router eigrp WAN-LAYER2
 address-family ipv4 unicast autonomous-system 300
  topology base
   redistribute eigrp 100 route-map REDISTRIBUTE-LIST
  exit-af-topology
eigrp stub connected summary redistributed
exit-address-family
```

Tech Tip

The redistributed keyword permits the EIGRP Stub Routing feature to send redistributed routes to the hub. Without the configuration of this option, EIGRP will not advertise redistributed routes.

With the local Internet default route redistribution into EIGRP AS100 you must take great care to properly configure and apply the filtering during the redistribution process to allow only the R1 loopback address. If you inadvertently advertise a default route from a remote site back to the primary site, this will likely disrupt Internet access for all other sites.

PROCESS

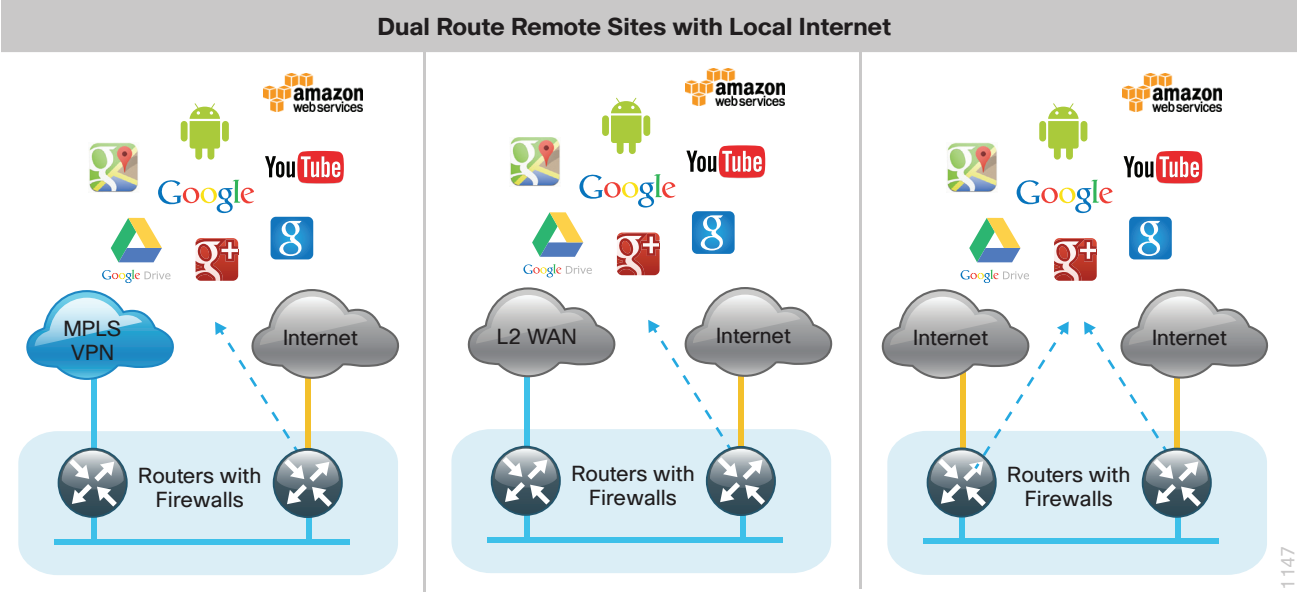
Configuring the Remote-Site DMVPN Spoke Router (Router 2)

1. Complete the WAN remote router
2. Configure remote-site access layer switching
3. Configure Internet connectivity
4. Configure access-layer HSRP
5. Configure the transit network
6. Configure DMVPN
7. Configure EIGRP WAN routing
8. Configure IP Multicast routing
9. Configure EIGRP (LAN side)
10. Redistribute DHCP default route into EIGRP
11. Configure loopback resiliency
12. Enable Enhanced Object Tracking

This section provides the deployment details needed to add a secondary router to single-router remote sites for added resiliency.

Follow this process to add an additional router for local Internet access to primary MPLS WAN, Layer 2 WAN, and VPN WAN locations.

Figure 36 - Dual-site with local Internet designs



Reader Tip

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

Procedure 1 Complete the WAN remote router

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

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

```
Hostname RS242-2951-2
```

Step 2: Configure the local login and password. The local login account and password provides basic access authentication to a router, which provides only limited operational privileges. The enable password secures access to the device configuration mode. By enabling password encryption, you prevent the disclosure of plain text passwords when viewing configuration files.

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

By default, HTTPS access to the router uses the enable password for authentication.

Step 3: If you want management access to the network infrastructure devices (SSH and HTTPS) to be controlled by authentication, authorization, and accounting (AAA), configure centralized user authentication.

As networks scale in the number of devices to maintain, there is an operational burden to maintain local user accounts on every device. A centralized AAA service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined in Step 2 on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

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

Step 4: Secure HTTP (HTTPS) and Secure Shell (SSH) are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Enable secure management of the network device by using the SSH and HTTPS protocols. Encrypt both protocols for privacy and turn off the unsecure protocols, Telnet and HTTP. Enable Secure Copy Protocol (SCP) to allow IOS code upgrades using Prime Infrastructure via the SSH-based SCP protocol.

Specify the transport preferred none on vty lines in order to prevent errant connection attempts from the CLI prompt. Without this command, if the ip name-server is unreachable, long timeout delays may occur for mistyped commands.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
ip scp server enable
line vty 0 15
 transport input ssh
 transport preferred none
```

Step 5: Enable synchronous logging. When synchronous logging of unsolicited messages and debug output is turned on, console log messages are displayed on the console after interactive CLI output is displayed or printed. With this command, you can continue typing at the device console when debugging is enabled.

```
line con 0
 transport preferred none
 logging synchronous
```

Step 6: Enable Simple Network Management Protocol (SNMP). This allows the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured both for a read-only and a read-write community string.

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

Step 7: If operational support is centralized in your network, increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network are able to access the device via SSH or SNMP.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
 access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```

Tech Tip

If you configure an access-list on the vty interface, you may lose the ability to use ssh to log in from one router to the next for hop-by-hop troubleshooting.

Step 8: Configure a synchronized clock. The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organization's network.

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

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

Step 9: Configure an in-band management interface. The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer 3 process and features are also bound to the loopback interface to ensure process resiliency.

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

```
interface Loopback 0
  ip address 10.255.254.242 255.255.255.255
  ip pim sparse-mode
```

Step 10: Bind the device processes for SNMP, SSH, PIM, TACACS+, and NTP to the loopback interface address. This provides optimal resiliency:

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

Step 11: Enable IP Multicast routing on the platforms in the global configuration mode. IP Multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than using multiple individual unicast streams or a broadcast stream that would propagate everywhere. IP Telephony MOH and IP Video Broadcast Streaming are two examples of IP Multicast applications.

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

This design, which is based on sparse mode multicast operation, uses Auto RP for a simple yet scalable way to provide a highly resilient RP environment.

```
ip multicast-routing
```

Step 12: Configure every Layer 3 switch and router to discover the IP Multicast RP with autorp. Use the **ip pim autorp listener** command to allow for discovery across sparse mode links. This configuration provides for future scaling and control of the IP Multicast environment and can change based on network needs and design.

```
ip pim autorp listener
```

Step 13: Enable sparse mode multicast operation for all Layer 3 interfaces in the network.

```
ip pim sparse-mode
```

Procedure 2 Configure remote-site access layer switching

Layer 2 EtherChannels are used to interconnect the remote site router to the access layer in the most resilient method possible. If your access-layer device is a single, fixed-configuration switch, a simple Layer 2 trunk between the router and switch is used.

Reader Tip

This guide includes only the additional steps to complete the access-layer configuration. For more information about access-layer configuration, see the Campus Wired LAN Technology Design Guide.

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.

Option 1: Layer 2 EtherChannel from router to access-layer switch

Step 1: Configure the port-channel interface on the router.

```
interface Port-channel1
 description EtherChannel link to RS242-A2960X
 no shutdown
```

Step 2: Configure EtherChannel member interfaces on the router. Configure the physical interfaces to tie to the logical port-channel by using the **channel-group** command. The number for the port-channel and channel-group must match.

```
interface GigabitEthernet0/1
 description RS242-A2960Xa Gig1/0/24
!
interface GigabitEthernet0/2
 description RS242-A2960Xb Gig2/0/24
!
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 1
  no shutdown
```

> **Tech Tip**
>
> Not all router platforms can support LACP to negotiate with the switch, so you configure EtherChannel statically.

Step 3: Configure EtherChannel member interfaces on the access-layer switch. Connect the router EtherChannel uplinks to separate switches in the access layer switch stack.

```
interface GigabitEthernet1/0/24
 description Link to RS242-2951-2 Gig0/1

interface GigabitEthernet2/0/24
 description Link to RS242-2951-2 Gig0/2
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport
 channel-group 2 mode on
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 load-interval 30
 macro apply EgressQoS
```

> **Tech Tip**
>
> The physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. Doing the configuration in this order allows for minimal configuration and reduces errors because most of the commands entered to a port-channel interface are copied to its members' interfaces and do not require manual replication.

Step 4: Configure EtherChannel trunk on the access-layer switch. Use an 802.1Q trunk for the connection, which allows the router to provide the Layer 3 services to all the VLANs defined on the access-layer switch. Prune the VLANs allowed on the trunk to only the VLANs that are active on the access-layer switch. When using EtherChannel, the interface type is port-channel, and the number must match the channel group configured in the previous step. Set DHCP Snooping and Address Resolution Protocol (ARP) inspection to trust.

```
interface Port-channel1
 description EtherChannel link to RS242-2951-2
 switchport trunk allowed vlan 64,69
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
 ip dhcp snooping trust
 no shutdown
```

> **Tech Tip**
>
> The Cisco Catalyst 3750 Series Switch requires the **switchport trunk encapsulation dot1q** command.

Option 2: Layer 2 trunk from router to access-layer switch

Step 1: Enable the physical interface on the router.

```
interface GigabitEthernet0/2
 description RS242-A2960Xa Gig1/0/24
 no ip address
 no shutdown
```

Step 2: Configure the trunk on the access-layer switch. Use an 802.1Q trunk for the connection, which allows the router to provide the Layer 3 services to all the VLANs defined on the access-layer switch. Prune the VLANs allowed on the trunk to only the VLANs that are active on the access-layer switch. Set DHCP Snooping and Address Resolution Protocol (ARP) inspection to trust.

```
interface  GigabitEthernet1/0/24
 description Link to RS242-2951-2 Gig0/2
 switchport trunk allowed vlan 64,69
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
 logging event link-status
 logging event trunk-status
 ip dhcp snooping trust
 no shutdown
 load-interval 30
 macro apply EgressQoS
```

> **Tech Tip**
>
> The Cisco Catalyst 3750 Series Switch requires the **switchport trunk encapsulation dot1q** command.

Procedure 3 Configure Internet connectivity

In this configuration, route local Internet traffic by using split-tunneling outside the DMVPN tunnel.

Step 1: Verify that the Internet-facing interface is disabled until the configuration is complete.

```
interface gigabit 0/0
 shutdown
```

Step 2: Configure the Internet-facing interface to receive a DHCP address.

```
interface gigabit 0/0
  ip address dhcp
```

Step 3: Configure the Internet-facing interface to install a default route with an AD value of 10.

```
interface gigabit 0/0
  ip dhcp client default-route distance 10
```

Tech Tip

The default behavior is for the router to install a default static route in the local table with an AD value of 254. We are using an AD value of 10 to ensure this path is preferred over other learned default routes. Using an AD value of 10 allows us to prefer this secondary link as the preferred path for Internet traffic.

Procedure 4 Configure access-layer HSRP

Configure HSRP to use a virtual IP (VIP) as a default gateway that is shared between two routers. The HSRP active router is primary WAN router, and the HSRP standby router is the router connected to the secondary WAN carrier or backup link.

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

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

Router	HSRP role	Virtual IP address (VIP)	Real IP address	HSRP priority	PIM DR priority
MPLS, L2, or VPN WAN (primary)	Active	.1	.2	110	110
VPN WAN (secondary)	Standby	.1	.3	105	105

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

Tech Tip

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

Step 1: Configure HSRP on the secondary router. Repeat this procedure for all data or voice subinterfaces.

```
interface [type][number].[sub-interface number]
 ip address [LAN network 1 address] [LAN network 1 netmask]
 ip pim dr-priority 105
 standby version 2
 standby 1 ip [LAN network 1 gateway address]
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

Example: Router (Secondary) with Layer 2 EtherChannel

```
interface Port-channel2
 no ip address
 no shutdown
!
interface Port-channel2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.252.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.252.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
!
interface Port-channel2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.253.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.253.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

Example: Router (Secondary) with Layer 2 Trunk

```
interface GigabitEthernet0/2
 no ip address
 no shutdown
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.252.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.252.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
!
interface GigabitEthernet0/2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.253.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.253.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

Procedure 5 Configure the transit network

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

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

Step 1: Configure the transit network interface.

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

Example: Secondary Router

```
interface GigabitEthernet0/2.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.248.2 255.255.255.252
 ip pim sparse-mode
```

Step 2: Add transit network VLAN to the access layer switches. If the VLAN does not already exist on the access layer switch, configure it now.

```
vlan 99
 name Transit-net
```

Step 3: Add transit network VLAN to existing access layer switch trunk.

```
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan add 99
```

Procedure 6 Configure DMVPN

Follow these procedures to configure DMVPN for secure encrypted communications with the central site location by using a secondary Internet WAN link on a secondary VPN WAN router.

When adding a backup link to an existing MPLS WAN or L2 WAN primary configuration, use the Primary DMVPN cloud (DMVPN1) for the backup connection to the primary site. For VPN WAN primary configurations, use the secondary DMVPN cloud (DMVPN-2) for the backup connection to the primary site.

Table 11 - Parameters for DMVPN configuration

Parameter	Primary DMVPN cloud (DMVPN-1)	Secondary DMVPN cloud (DMVPN-2)
crypto keyring	GLOBAL-KEYRING	GLOBAL-KEYRING
crypto isakmp profile	ISAKMP-INET-PUBLIC	ISAKMP-INET-PUBLIC
crypto ipsec profile	DMVPN-PROFILE1	DMVPN-PROFILE2
Tunnel number	Interface tunnel 10	Interface tunnel 11
Tunnel IP address (NHS)	10.4.34.1	10.4.36.1
NHRP network ID	101	102
EIGRP process name	WAN-DMVPN-1	WAN-DMVPN-2
EIGRP AS	**200**	**201**

Step 1: Configure a crypto keyring in the global table and define the pre-shared key.

```
crypto keyring GLOBAL-KEYRING
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

Step 2: Configure the ISAKMP policy.

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

Step 3: Configure Dead Peer Detection (DPD).

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

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

```
crypto isakmp keepalive 30 5
```

Step 4: Configure an ISAKMP profile referencing the new keyring.

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

Step 5: 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

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

Tech Tip

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

Step 6: Create the IPsec profile. The IPsec profile creates an association between an ISAKMP profile and an IPsec transform-set.

```
crypto ipsec profile DMVPN-PROFILE2
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile ISAKMP-INET-PUBLIC
```

Step 7: Increase the IPsec anti-replay window size.

```
crypto ipsec security-association replay window-size 1024
```

Tech Tip

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed.

It is recommended that you use the full 1024 window size in order to eliminate future anti-replay problems.

If you do not increase the window size, the router may drop packets and you may see the following error message on the router CLI:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
```

Step 8: Configure the DMVPN mGRE tunnel interface.

```
interface Tunnel 10
 ip address 10.4.34.242 255.255.254.0
 ip mtu 1400
 ip pim dr-priority 0
 ip pim nbma-mode
 ip pim sparse-mode
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
```

Step 9: Configure tunnel routing affinity for hub traffic. This ensures traffic for the hub only routes via the local WAN interface.

```
ip route 172.16.130.1 255.255.255.255 GigabitEthernet0/0 dhcp

interface Tunnel10
  tunnel route-via GigabitEthernet0/0 mandatory
```

Step 10: Configure NHRP.

```
interface Tunnel 10
 ip nhrp authentication cisco123
 ip nhrp map multicast 172.16.130.1
 ip nhrp map 10.4.36.1 172.16.130.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.36.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
```

Step 11: Configure tunnel bandwidth. The bandwidth setting should be set to match the Internet bandwidth.

```
interface Tunnel11
 bandwidth [bandwidth (kbps)]
```

Step 12: Configure tunnel protection.

```
interface Tunnel10
 tunnel protection ipsec profile DMVPN-PROFILE1
```

Reader Tip

For more information about DMVPN deployment details, see the VPN WAN Technology Design Guide.

Procedure 7 Configure EIGRP WAN routing

Step 1: In this configuration, you configure EIGRP to exchange routes internally with the central site and filter the central site default route for being received over the DMVPN tunnel. Configure an EIGRP process for DMVPN using EIGRP named mode.

For MPLS WAN and Layer 2 WAN configurations, EIGRP AS200 is configured on the router for the primary DMVPN cloud. All interfaces on the router are EIGRP AS200 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 WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  af-interface default
   passive-interface
  exit-af-interface
  af-interface Tunnel10
   no passive-interface
  exit-af-interface
network 10.4.34.0 0.0.1.255
network 10.5.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
eigrp router-id [IP address of Loopback0]
eigrp stub connected summary
exit-address-family
```

Step 2: Configure EIGRP values for the mGRE tunnel interface.

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

```
router eigrp WAN-DMVPN-1
address-family ipv4 unicast autonomous-system 200
  af-interface Tunnel10
   hello-interval 20
   hold-time 60
  exit-af-interface
exit-address-family
```

Step 3: Configure EIGRP neighbor authentication to allow EIGRP to form neighbor relationships with MD5 authentication in order to establish secure peering adjacencies and exchange route tables over the DMVPN WAN tunnel interface.

```
key chain WAN-KEY
 key 1
  key-string cisco
!
router eigrp WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  af-interface Tunnel10
   authentication mode md5
   authentication key-chain WAN-KEY
  exit-af-interface
 exit-address-family
```

Step 4: Configure EIGRP route summarization.

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

```
router eigrp WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  af-interface Tunnel10
   summary-address [summary network] [summary mask]
  exit-af-interface
 exit-address-family
```

Step 5: Create an access list to match the default route and permit all other routes.

```
ip access-list standard NO-DEFAULT
  deny 0.0.0.0
  permit any
```

Step 6: Create a route-map to reference the access list.

```
route-map BLOCK-DEFAULT permit 10
  match ip address NO-DEFAULT
```

Step 7: Block the default route on the tunnel interface on the EIGRP WAN process by using a distribute list referencing the route-map configured in the previous step.

```
router eigrp WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  topology base
   distribute-list route-map BLOCK-DEFAULT in
  exit-af-topology
exit-address-family
```

Procedure 8 Configure IP Multicast routing

This procedure includes additional steps for configuring IP Multicast for a DMVPN tunnel on a router with IP Multicast already enabled.

Step 1: Configure PIM on the DMVPN tunnel interface.

Enable IP PIM sparse mode on the DMVPN tunnel interface.

```
interface Tunnel10
 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.

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

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

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

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

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

Procedure 9 Configure EIGRP (LAN side)

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

Step 1: Enable the EIGRP LAN process (AS100) facing the access layer on both the primary and secondary WAN routers.

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 facing interfaces (MPLS, L2 WAN, VPN WAN) or mGRE tunnel interfaces as part of EIGRP AS100.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
 af-interface [Transit interface]
```

```
    no passive-interface
   exit-af-interface
  network [network] [inverse mask]
  eigrp router-id [IP address of Loopback0]
  exit-address-family
```

Step 2: Configure EIGRP neighbor authentication to allow EIGRP to form neighbor relationships with MD5 authentication in order to establish secure peering adjacencies and exchange route tables.

```
key chain LAN-KEY
 key 1
  key-string cisco
!
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface [Transit interface]
   authentication mode md5
   authentication key-chain LAN-KEY
  exit-af-interface
```

Step 3: Redistribute WAN routing protocol into the EIGRP LAN process.

The remote-site router is using either BGP for an MPLS connection or EIGRP for a Layer 2 WAN or DMVPN connection. The WAN-facing routing protocol that is in use needs to be distributed into the EIGRP LAN process.

For dual router, dual DMVPN WAN configurations redistribute EIGRP AS200 into EIGRP AS100 on the primary router and EIGRP AS201 into EIGRP AS100 on the secondary WAN router. Because the routing protocol is the same, no default metric is required.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  topology base
   redistribute eigrp 200
  exit-af-topology
exit-address-family
```

Example: Secondary Router (MPLS Primary with DMVPN Backup)

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
  af-interface GigabitEthernet0/2.99
   authentication mode md5
   authentication key-chain LAN-KEY
   no passive-interface
  exit-af-interface
  topology base
   redistribute eigrp 200
  exit-af-topology
 network 10.5.0.0 0.0.255.255
```

```
 network 10.255.0.0 0.0.255.255
 eigrp router-id 10.255.253.242
exit-address-family
```

Procedure 10 Redistribute DHCP default route into EIGRP

For dual-router configurations, you need to redistribute the DHCP-originated default route into EIGRP AS100 for reachability on both WAN routers.

Step 1: Configure an access list to match the default route.

```
ip access-list standard DHCP-DEFAULT
 remark DHCP default route
 permit 0.0.0.0
```

Step 2: Configure a route map referencing the access list that matches the default route.

```
route-map LOCAL-DEFAULT permit 10
 match ip address DHCP-DEFAULT
```

Step 3: Redistribute the static default route installed by DHCP into EIGRP AS100 by using the route map.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  topology base
   redistribute static route-map LOCAL-DEFAULT
  exit-af-topology
exit-address-family
```

Procedure 11 Configure loopback resiliency

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

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

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

Example

```
ip access-list standard R1-LOOPBACK
 permit 10.255.253.242
!
route-map REDISTRIBUTE-LIST permit 10
 match ip address R1-LOOPBACK
```

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

Example: DMVPN Spoke Router

```
router eigrp WAN-DMVPN-1
 address-family ipv4 unicast autonomous-system 200
  topology base
   redistribute eigrp 100 route-map REDISTRIBUTE-LIST
  exit-af-topology
eigrp stub connected summary redistributed
exit-address-family
```

Tech Tip

The redistributed keyword permits the EIGRP Stub Routing feature to send redistributed routes to the hub. Without the configuration of this option, EIGRP will not advertise redistributed routes.

With the local Internet default route redistribution into EIGRP AS100 you must take great care to properly configure and apply the filtering during the redistribution process to allow only the R1 loopback address. If you inadvertently advertise a default route from a remote site back to the primary site, Internet access will likely be disrupted for all other sites.

Procedure 12 Enable Enhanced Object Tracking

(Optional)

You may need to ensure that connectivity issues with your ISP don't cause black-hole routing conditions. Failure conditions can exist in which the DHCP address and route are not removed from the remote-site router when there are connectivity issues with the broadband service or local premise equipment. There may also be circumstances in which certain services are unreachable via the local ISP connection and you want to re-route those services to a secondary Internet service.

This solution uses an IPSLA probe to monitor the status of the ISP connection that is used as the primary path for local Internet traffic. In this example, the failure of probes to two different IP hosts triggers the removal of the dynamically assigned default route. If either probe is active, the route will remain.

Step 1: Configure the IPSLA probes.

```
ip sla 110
 icmp-echo 172.18.1.253 source-interface GigabitEthernet0/0
 threshold 1000
 frequency 15
ip sla schedule 110 life forever start-time now
ip sla 111
 icmp-echo 172.18.1.254 source-interface GigabitEthernet0/0
 threshold 1000
 frequency 15
ip sla schedule 111 life forever start-time now
```

Step 2: Configure the tracking parameters and logic for the IPSLA probes.

```
track 60 ip sla 110 reachability
track 61 ip sla 111 reachability
track 62 list boolean or
 object 60
 object 61
```

Step 3: Configure ACL and route map to match and set the next-hop for the IPSLA probe traffic. This ensures proper recovery when service is restored after a failure.

```
ip access-list extended SLA-SET-NEXT-HOP
 permit icmp any host 172.18.1.253
 permit icmp any host 172.18.1.254

route-map PBR-SLA-SET-NEXT-HOP permit 10
 match ip address SLA-SET-NEXT-HOP
 set ip next-hop dynamic dhcp
```

Step 4: Configure policy routing for local traffic.

```
ip local policy route-map PBR-SLA-SET-NEXT-HOP
```

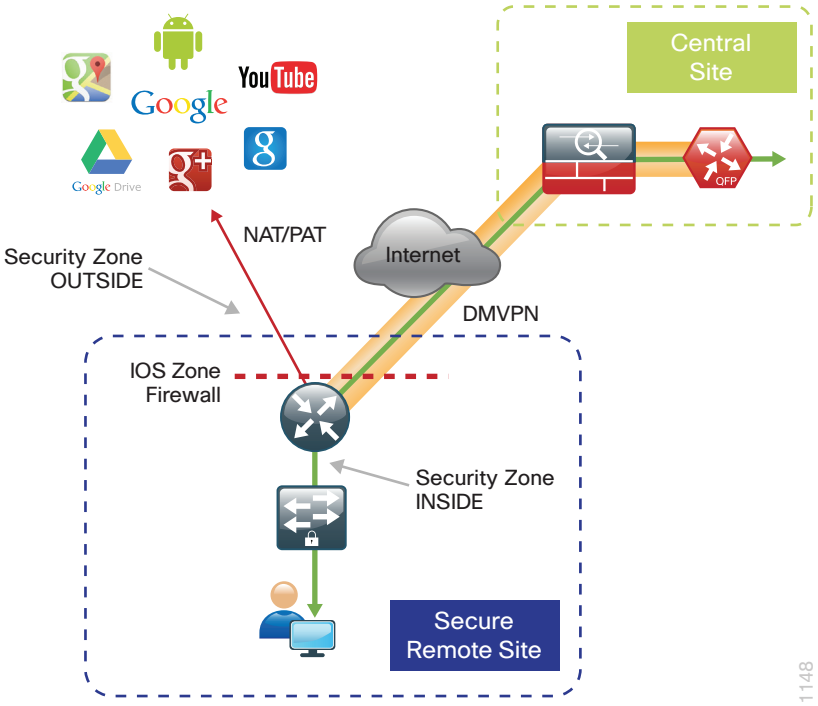
Step 5: Bind the IPSLA probes and tracking to the DHCP assigned route.

```
interface GigabitEthernet0/0
 ip dhcp client route track 62
```

Deploying Remote Site Security

Follow these procedures to secure a remote-site router with local Internet configurations. The following section provides general security recommendations for the implementation of NAT, ZBFW, and general guidelines for securing Cisco IOS Software.

Figure 37 - Secure remote site



PROCESS

Configuring Cisco IOS NAT

1. Define and configure Cisco IOS NAT policy
2. Configure NAT policy on a single router with dual Internet links

In this design, inside hosts use RFC 1918 addresses, and traffic destined to the Internet from the local site needs to be translated to public IP space. The Internet-facing interface on the remote-site router uses DHCP to acquire a publically routable IP address; the NAT policy here will translate inside private IP addressed hosts to this DHCP address by using Port Address Translation (PAT).

Procedure 1 Define and configure Cisco IOS NAT policy

Use this procedure to configure NAT on the primary Internet connection for local Internet access for both single router and dual router remote-site configurations.

Step 1: Define a policy matching the desired traffic to be translated. Use an ACL and include all remote-site subnets.

```
ip access-list standard NAT
 permit 10.5.240.0 0.0.7.255
```

Step 2: Configure the NAT policy.

```
ip nat inside source list NAT interface GigabitEthernet0/0 overload
```

Step 3: Enable NAT by applying policy to the inside router interfaces. Apply this configuration as needed to internal interfaces or sub-interfaces where traffic matching the ACL may originate, such as the data and transit networks and any service interfaces such as Cisco UCS-E or Cisco Services Ready Engine (SRE) interfaces.

```
interface GigabitEthernet0/2.64
 ip nat inside

interface GigabitEthernet0/2.99
 ip nat inside

interface ucse2/0
 ip nat inside
```

Tech Tip

If the VMWare hosts utilize the UCS-E internal interface and must access the Internet, then the UCS-E interface should be part of the NAT configuration.

Step 4: Configure the Internet-facing interfaces for NAT.

```
interface GigabitEthernet0/0
 description Internet Connection (ISP-A)
 ip nat outside
```

Tech Tip

When you configure NAT on the router interfaces, you will see **ip virtual-reassembly in** added to the configuration. This is automatically enabled for features that require fragment reassembly, such as NAT, Firewall, and IPS.

Step 5: Verify proper interfaces are configured for NAT.

```
RS240-3945#show ip nat statistics

Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 34, occurred 2w3d ago
Outside interfaces:
  GigabitEthernet0/0
Inside interfaces:
  GigabitEthernet0/2.64, GigabitEthernet0/2.69
Hits: 352091  Misses: 0
CEF Translated packets: 352091, CEF Punted packets: 0
```

Step 6: Verify NAT translations for intended sources that are using local Internet services.

```
RS240-3945#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 172.18.100.76:49694 10.5.244.30:49694 63.80.4.171:80     63.80.4.171:80
tcp 172.18.100.76:49696 10.5.244.30:49696 74.125.239.39:80   74.125.239.39:80
tcp 172.18.100.76:49697 10.5.244.30:49697 74.125.239.39:80   74.125.239.39:80
```

Procedure 2 Configure NAT policy on a single router with dual Internet links

(Optional)

Use this procedure if you want to configure NAT on the single router, dual Internet configuration. This procedure provides the NAT configurations required when connecting a single router to two different ISPs.

Step 1: Define a policy matching the desired traffic to be translated. Use an ACL and include all remote-site subnets.

```
ip access-list extended NAT
 permit ip 10.5.128.0 0.0.7.255 any
```

Step 2: Configure route maps matching the ACL and interfaces where NAT will be applied.

```
route-map ISP-A permit 10
 match ip address NAT
 match interface GigabitEthernet0/0

route-map ISP-B permit 10
 match ip address NAT
 match interface GigabitEthernet0/1
```

Step 3: Configure the NAT policies.

```
ip nat inside source route-map ISP-A interface GigabitEthernet0/0 overload
ip nat inside source route-map ISP-B interface GigabitEthernet0/1 overload
```

Step 4: Enable NAT by applying the policy to the inside router interfaces. Apply this configuration as needed to internal interfaces or sub-interfaces where traffic matching the ACL may originate, such as the data network.

```
interface GigabitEthernet0/2.64
 ip nat inside
```

Step 5: Configure the Internet-facing interfaces for NAT.

```
interface GigabitEthernet0/0
 description Internet Connection (ISP-A)
 ip nat outside

interface GigabitEthernet0/1
 description Internet Connection (ISP-B)
 ip nat outside
```

> **Tech Tip**
>
> When you configure NAT on the router interfaces, you will see **ip virtual-reassembly in** added to the configuration. This is automatically enabled for features that require fragment reassembly, such as NAT, Firewall, and IPS.

Step 6: Verify proper interfaces are configured for NAT.

```
RS251-2911#show ip nat statistics

Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 34, occurred 2w3d ago
Outside interfaces:
  GigabitEthernet0/0, GigabitEthernet0/1
Inside interfaces:
  GigabitEthernet0/2.64, GigabitEthernet0/2.69
Hits: 352091  Misses: 0
CEF Translated packets: 352091, CEF Punted packets: 0
```

Step 7: Verify NAT translations for intended sources that are using local Internet services.

```
RS251-2911#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 172.18.100.76:49694 10.5.244.30:49694 63.80.4.171:80     63.80.4.171:80
tcp 172.18.100.76:49696 10.5.244.30:49696 74.125.239.39:80   74.125.239.39:80
tcp 172.18.100.76:49697 10.5.244.30:49697 74.125.239.39:80   74.125.239.39:80
```

PROCESS

Configuring Cisco IOS Zone-Based Firewall

1. Configure base Cisco IOS Zone-Based Firewall parameters
2. Restrict traffic to the router
3. Enable and verify Zone-Based Firewall configuration

The following Cisco IOS firewall configuration is intended for use on Internet-facing remote site routers providing secure local Internet access. This configuration assumes DHCP and DMVPN are also configured to use the outside interface. To configure the required base firewall policies, complete the following procedures.

Procedure 1 Configure base Cisco IOS Zone-Based Firewall parameters

Step 1: If you have existing VPN WAN configurations, remove the inbound ACL from the Internet-facing router interfaces, and then shut down the interface before continuing. This prevents unauthorized traffic while the ZBFW is configured.

```
interface GigabitEthernet0/0
  shutdown
  no ip access-list extended ACL-INET-PUBLIC
```

Step 2: Define security zones. A zone is a named group of interfaces that have similar functions or security requirements. This example defines the names of the two basic security zones identified.

```
zone security INSIDE
zone security OUTSIDE
```

Step 3: Define a class map to match specific protocols. Class-maps apply **match-any** or **match-all** operators in order to determine how to apply the match criteria to the class. If **match-any** is specified, traffic must meet at least one of the match criteria in the class-map to be included in the class. If **match-all** is specified, traffic must meet all of the match criteria to be included in the class.

```
class-map type inspect match-any INSIDE-TO-OUTSIDE-CLASS
 match protocol ftp
 match protocol tcp
 match protocol udp
 match protocol icmp
```

Tech Tip

Protocols that use single ports such as HTTP, telnet, SSH, etc. can be statefully allowed with tcp inspection alone by using the **match protocol tcp** command.

Protocols such as **ftp** that use multiple ports (one for control and another for data) require application inspection in order to enable dynamic adjustments to the active firewall policy. The specific TCP ports that are required for the application are allowed for short durations, as necessary.

Step 4: Define policy maps. A policy is an association of traffic classes and actions. It specifies what actions should be performed on defined traffic classes. In this case, you statefully inspect the outbound session so that return traffic is permitted.

```
policy-map type inspect INSIDE-TO-OUTSIDE-POLICY
 class type inspect INSIDE-TO-OUTSIDE-CLASS
  inspect
 class class-default
  drop
```

Tech Tip

An action is a specific functionality that is associated with a traffic class. *Inspect*, *drop*, and *pass* are actions.

With the *inspect* action, return traffic is automatically allowed for established connections. The *pass* action permits traffic in one direction only. When using the *pass* action, you must explicitly define rules for return traffic.

Step 5: Define the zone pair and apply the policy map. A zone pair represents two defined zones and identifies the source and destination zones where a unidirectional firewall policy-map is applied. This configuration uses only one zone pair as all traffic is inspected and thus allowed to return.

```
zone-pair security IN_OUT source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE-TO-OUTSIDE-POLICY
```

Procedure 2 Restrict traffic to the router

The router itself is defined by Cisco IOS Software using the fixed name self as a separate security zone. The self zone is the exception to the default deny-all policy.

All traffic destined to or originating from the router itself (local traffic) on any interface is allowed until traffic is explicitly denied. In other words, any traffic flowing directly between defined zones and the router's IP interfaces is implicitly allowed and is not initially controlled by zone firewall policies.

This default behavior of the self zone ensures that connectivity to the router's management interfaces and the function of routing protocols is maintained when an initial zone firewall configuration is applied to the router.

Specific rules that control traffic to the self zone are required. When you configure a ZBFW rule that includes the self zone, traffic between the self zone and the other defined zones is immediately restricted in both directions.

Table 12 - Self-Zone firewall access list parameters

Protocol	Stateful inspection policy
ISAKMP	Yes
ICMP	Yes
DHCP	No
ESP	No

The following configuration allows the required traffic for proper remote-site router configuration with DMVPN. ESP and DHCP cannot be inspected and need to be configured with a "pass" action in the policy, using separate ACL and class-maps. ISAKMP should be configured with the "inspect" action and thus needs to be broken out with a separate ACL and class-maps for inbound and outbound policies.

> **Tech Tip**
>
> More specific ACLs than are shown here with the "any" keyword are recommended for added security.

Step 1: In the following steps, define access lists.

Step 2: Define an ACL allowing traffic with a destination of the router itself from the OUTSIDE zone. This includes ISAKMP for inbound tunnel initiation. This traffic can be inspected and is identified in the following ACL.

```
ip access-list extended ACL-RTR-IN
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit icmp any any echo
 permit icmp any any echo-reply
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any gt 1023 ttl eq 1
```

Step 3: Identify traffic for IPSEC tunnel initiation that will originate from the router (self zone) to the OUTSIDE zone. This traffic can be inspected.

```
ip access-list extended ACL-RTR-OUT
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit icmp any any
```

Step 4: Configure DHCP ACL to allow the router to acquire a public IP address dynamically from the ISP. This traffic needs to be defined separately for server and client and cannot be inspected.

```
ip access-list extended DHCP-IN
 permit udp any eq bootps any eq bootpc

ip access-list extended DHCP-OUT
 permit udp any eq bootpc any eq bootps
```

Step 5: Configure ESP ACL to allow the router to establish IPSEC communications for DMVPN. ESP needs to be explicitly allowed inbound and outbound in separate ACLs. ESP cannot be inspected.

```
ip access-list extended ESP-IN
 permit esp any any

ip access-list extended ESP-OUT
 permit esp any any
```

Step 6: Define class maps for traffic to and from the self zone. Separate class-maps are required for inbound and outbound initiated flows as well as for traffic that can be inspected by the router.

Class-map matching inbound traffic that can be inspected:

```
class-map type inspect match-any INSPECT-ACL-IN-CLASS
 match access-group name ACL-RTR-IN
```

Class-map matching outbound traffic that can be inspected:

```
class-map type inspect match-any INSPECT-ACL-OUT-CLASS
 match access-group name ACL-RTR-OUT
```

Class-map matching inbound traffic that is not able to be inspected:

```
class-map type inspect match-any PASS-ACL-IN-CLASS
 match access-group name ESP-IN
 match access-group name DHCP-IN
```

Class-map matching outbound traffic that cannot be inspected:

```
class-map type inspect match-any PASS-ACL-OUT-CLASS
 match access-group name ESP-OUT
 match access-group name DHCP-OUT
```

Step 7: Define policy maps. Create two separate policies, one for traffic inbound and one for traffic outbound.

Inbound policy-map that refers to both of the outbound class-maps with actions of inspect, pass, and drop for the appropriate class defined:

```
policy-map type inspect ACL-IN-POLICY
 class type inspect INSPECT-ACL-IN-CLASS
  inspect
 class type inspect PASS-ACL-IN-CLASS
  pass
 class class-default
  drop
```

Outbound policy-map that refers to both of the outbound class-maps with actions of inspect, pass, and drop for the appropriate class defined:

```
policy-map type inspect ACL-OUT-POLICY
 class type inspect INSPECT-ACL-OUT-CLASS
  inspect
 class type inspect PASS-ACL-OUT-CLASS
  pass
 class class-default
  drop
```

Tech Tip

Inspection for Layer 7 applications is not allowed for traffic going to and from the self zone to other zones. Cisco IOS firewalls support only inspection of TCP, UDP, and H.323 traffic that terminates on or originates from the router itself.

Traffic such as DHCP and ESP cannot be inspected and must be configured as “Pass” in the associated policy-map.

Step 8: Define the zone pair and apply policy maps to them.

Zone pair for traffic destined to the self zone of the router from the outside and associate the inbound policy-map defined in the previous step:

```
zone-pair security TO-ROUTER source OUTSIDE destination self
 service-policy type inspect ACL-IN-POLICY
```

Zone pair for traffic destined from the self zone of the router to the outside and associate the outbound policy-map defined in the previous step:

```
zone-pair security FROM-ROUTER source self destination OUTSIDE
 service-policy type inspect ACL-OUT-POLICY
```

Procedure 3 Enable and verify Zone-Based Firewall configuration

Step 1: Assign all router interfaces to security zones.

```
interface GigabitEthernet0/0
 description Internet Connection
 zone-member security OUTSIDE
interface GigabitEthernet0/2.64
 description Wired Data
 encapsulation dot1Q 64
 zone-member security INSIDE
interface GigabitEthernet0/2.69
 description Wired Voice
 encapsulation dot1Q 69
 zone-member security INSIDE

interface GigabitEthernet0/2.99
 description transit network
 encapsulation dot1Q 99
 zone-member security INSIDE
interface ucse2/0
 zone-member security INSIDE

interface Tunnel10
description DMVPN-1 tunnel interface
zone-member security INSIDE
```

Tech Tip

By default, traffic is allowed to flow between interfaces that are members of the same zone, while a default "deny-all" policy is applied to traffic moving between zones.

Depending on the remote site configuration, be sure to include MPLS, DMVPN tunnels, transit sub-interfaces, and service interfaces such as Cisco UCS-E members of the security zone INSIDE. Failure to include interfaces in to the INSIDE zone will cause traffic not to flow as expected.

In the case of single-router dual DMVPN configurations, ensure that both Internet-facing interfaces are defined as security zone OUTSIDE.

Loopback interfaces are members of the "self" zone and are not assigned to a defined security zone.

Step 2: Verify the interface assignment for the zone firewall and ensure all required interfaces for the remote site configuration are assigned to the proper zone.

```
RS240-3945#show zone security
zone self
  Description: System defined zone
zone INSIDE
  Member Interfaces:
    Tunnel10
    GigabitEthernet0/2.64
    GigabitEthernet0/2.69
    GigabitEthernet0/2.99
    ucse2/0zone OUTSIDE
  Member Interfaces:
    GigabitEthernet0/0
```

Step 3: Verify general firewall status.

```
RS240-3945#show policy-firewall stats
Global Stats:
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [18:683784]
        udp packets: [2557744:18668881]
        icmp packets: [62305:62226]

        Session creations since subsystem startup or last reset 63119
        Current session counts (estab/half-open/terminating) [2:0:0]
        Maxever session counts (estab/half-open/terminating) [43:20:14]
        Last session created 00:00:10
        Last statistic reset never
        Last session creation rate 6
        Maxever session creation rate 54
        Last half-open session total 0
```

Step 4: Verify firewall operation by reviewing the byte counts for each of the configured policies and classes.

```
RS240-3945#show policy-map type inspect zone-pair sessions

policy exists on zp IN_OUT
  Zone-pair: IN_OUT

  Service-policy inspect : INSIDE-TO-OUTSIDE-POLICY

    Class-map: INSIDE-TO-OUTSIDE-CLASS (match-any)
      Match: protocol ftp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol tcp
        78 packets, 2492 bytes
        30 second rate 0 bps
      Match: protocol udp
        4 packets, 226 bytes
        30 second rate 0 bps
      Match: protocol icmp
        1 packets, 40 bytes
        30 second rate 0 bps

   Inspect

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes

policy exists on zp TO-ROUTER
  Zone-pair: TO-ROUTER

  Service-policy inspect : ACL-IN-POLICY

    Class-map: INSPECT-ACL-IN-CLASS (match-any)
      Match: access-group name ACL-RTR-IN
        1123 packets, 50860 bytes
        30 second rate 0 bps

   Inspect

    Class-map: PASS-ACL-IN-CLASS (match-any)
      Match: access-group name ESP-IN
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: access-group name DHCP-IN
```

```
        66 packets, 20328 bytes
        30 second rate 0 bps
      Pass
        66 packets, 20328 bytes

    Class-map: class-default (match-any)
      Match: any
      Drop
        1 packets, 20 bytes

policy exists on zp FROM-ROUTER
  Zone-pair: FROM-ROUTER

  Service-policy inspect : ACL-OUT-POLICY

    Class-map: INSPECT-ACL-OUT-CLASS (match-any)
      Match: access-group name ACL-RTR-OUT
        52495 packets, 2331552 bytes
        30 second rate 0 bps

   Inspect

      Number of Established Sessions = 4
      Established Sessions
        Session 22C74B80 (172.18.100.166:4500)=>(172.17.130.1:4500) udp SIS_OPEN
          Created 3d12h, Last heard 00:00:03
          Bytes sent (initiator:responder) [57450792:307706508]
        Session 22C78A80 (172.18.100.154:4500)=>(172.16.130.1:4500) udp SIS_OPEN
          Created 01:24:43, Last heard 00:00:03
          Bytes sent (initiator:responder) [327428:5875644]
        Session 22C75980 (172.18.100.166:8)=>(172.18.1.253:0) icmp SIS_OPEN
          Created 00:00:10, Last heard 00:00:10
          ECHO request
          Bytes sent (initiator:responder) [36:36]
        Session 22C70200 (172.18.100.166:8)=>(172.18.1.254:0) icmp SIS_OPEN
          Created 00:00:09, Last heard 00:00:09
          ECHO request
          Bytes sent (initiator:responder) [36:36]

    Class-map: PASS-ACL-OUT-CLASS (match-any)
      Match: access-group name ESP-OUT
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: access-group name DHCP-OUT
        146 packets, 45602 bytes
        30 second rate 0 bps
      Pass
```

```
      146 packets, 45602 bytes

  Class-map: class-default (match-any)
    Match: any
    Drop
      6 packets, 258 bytes
```

Step 5: Add the following command to the router configuration in order to identify traffic dropped by the Cisco IOS zone firewall.

```
ip inspect log drop-pkt
```

Tech Tip

When you configure the command **ip inspect drop-pkt**, the following gets automatically added to the router configuration:

```
parameter-map type inspect global
 log dropped-packets enable
```

PROCESS

Configuring General Router Security

1. Disable IP ICMP redirects
2. Disable ICMP Unreachables
3. Disable Proxy ARP
4. Disable unused router services
5. Disable CDP and LLDP
6. Enable keepalives for TCP sessions
7. Configure Internal network floating static routes
8. Enable Internet interfaces

In addition to the security measures already taken in prior configuration tasks, this section introduces best practices recommendations to secure Internet-facing routers. Disabling unused services and features for networking devices improves the overall security posture by minimizing the amount of information exposed. This practice also minimizes the amount of router CPU and memory load that is required to process unneeded packets.

Tech Tip

These are general security guidelines only. Additional measures may be taken to secure remote site routers on a case-by-case basis. Care should be taken to ensure the disabling of certain features does not impact other functions of the network.

Procedure 1 Disable IP ICMP redirects

ICMP redirect messages are used by routers to notify that a better route is available for a given destination. In this situation, the router forwards the packet and sends an ICMP redirect message back to the sender advising of an alternative and preferred route to the destination. In many implementations, there is no benefit in permitting this behavior. An attacker can generate traffic forcing the router to respond with ICMP redirect messages, negatively impacting the CPU and performance of the router. This can be prevented by disabling ICMP redirect messages.

Step 1: Disable ICMP redirect messages on Internet-facing router interfaces.

```
interface GigabitEthernet0/0
 description Internet Connection
 no ip redirects
```

Procedure 2 Disable ICMP Unreachables

When filtering on router interfaces, routers send ICMP unreachable messages back to the source of blocked traffic. Generating these messages can increase CPU utilization on the router. By default, Cisco IOS ICMP unreachable messages are limited to one every 500 milliseconds. ICMP unreachable messages can be disabled on a per interface basis.

Step 1: Disable ICMP unreachable messages on Internet-facing router interfaces.

```
interface GigabitEthernet0/0
 description Internet Connection
 no ip unreachables
```

Procedure 3 Disable Proxy ARP

Proxy ARP allows the router to respond to ARP request for hosts other than itself. Proxy ARP can help machines on a subnet reach remote subnets without configuring routing or a default gateway as defined in RFC 1027. There are some disadvantages to utilizing proxy ARP, including the following:

- An attacker can impact available memory by sending a large number of ARP requests.
- A router is also susceptible to man-in-the-middle attacks where a host on the network could be used to spoof the MAC address of the router, resulting in unsuspecting hosts sending traffic to the attacker.

Proxy ARP can be disabled using the **interface** configuration command

Step 1: Disable proxy ARP on Internet-facing router interfaces.

```
interface GigabitEthernet0/0
 description Internet Connection
 no ip proxy-arp
```

Procedure 4 Disable unused router services

As a security best practice, all unnecessary services should be disabled that could be used to launch denial of service (DoS) and other attacks. Many unused services that pose a security threat are disabled by default in current Cisco IOS versions. The following services and features are recommended to be disabled.

Step 1: Disable Maintenance Operation Protocol (MOP) on Internet-facing router interfaces.

```
interface GigabitEthernet0/0
 description Internet Connection
 no mop enabled
```

Step 2: Disable Packet Assembler/Disassembler (PAD) service globally on the router.

```
no service pad
```

Step 3: Prevent the router from attempting to locate a configuration file via TFTP globally on the router.

```
no service config
```

Procedure 5 Disable CDP and LLDP

CDP and LLDP can be used by an attacker for reconnaissance and network mapping. Cisco Discovery Protocol (CDP) is a network protocol that is used to discover other CDP-enabled devices. CDP is often used by Network Management Systems (NMS) and for troubleshooting networking problems. Link Layer Discovery Protocol (LLDP) is an IEEE protocol that is defined in 802.1AB and is very similar to CDP. CDP and LLDP should be disabled on router interfaces that connect to untrusted networks.

Step 1: If necessary, disable CDP on Internet-facing router interfaces.

```
interface GigabitEthernet0/0
 description Internet Connection
 no cdp enable
```

Step 2: Disable LLDP on Internet-facing router interfaces.

```
interface GigabitEthernet0/0
 description Internet Connection
 no lldp transmit
 no lldp receive
```

Procedure 6 Enable keepalives for TCP sessions

This configuration enables TCP keepalives on inbound connections to the router and outbound connections from the router. This ensures that the device on the remote end of the connection is still accessible and half-open or orphaned connections are removed from the router.

Step 1: Enable the TCP keepalives service for inbound and outbound connections globally on the router. Configuration commands enable a device

```
service tcp-keepalives-in
service tcp-keepalives-out
```

Procedure 7 Configure Internal network floating static routes

In the event the DMVPN tunnel to the hub site fails, you will want to ensure traffic destined to internal networks does not follow the local Internet default route. It's best to have the network fail closed to prevent possible security implications and unwanted routing behavior.

Configuring floating static routes to null zero with an AD of 254 ensures that all internal subnets route to null0 in the event of tunnel failure.

Step 1: Configure static route for internal network subnets.

```
ip route 10.0.0.0 255.0.0.0 null0 254
```

Tech Tip

Configure the appropriate number of null 0 routes for internal network ranges, using summaries when possible for your specific network environment.

Procedure 8 Enable Internet interfaces

Now that the security configurations are complete, you can enable the Internet-facing interfaces.

Step 1: Enable the Internet-facing router interfaces.

```
interface GigabitEthernet0/0
 description Internet Connection
 no shutdown
```

Deploying WAN Quality of Service

When configuring the WAN-edge QoS, you are defining how traffic egresses your network. It is critical that the classification, marking, and bandwidth allocations align to the service provider offering to ensure consistent QoS treatment end-to-end. QoS policies for private and public WAN solutions differ as public Internet-based WAN using DMVPN is limited by nature of best effort Internet services.

PROCESS

Configuring Public Cloud WAN QoS

1. Create the QoS Maps to classify traffic
2. Add ISAKMP traffic to network-critical
3. Define the policy map to use queuing policy
4. Configure the physical interface S&Q policy
5. Apply WAN QoS policy to the physical interface
6. Configure Per-tunnel QoS NHRP policy on DMVPN spoke routers
7. Configure IPSEC anti-replay window size

With Internet-based WAN services, QoS preservation across the public Internet is not guaranteed. For best effort in this use case, egress traffic classification prioritizes traffic as it leaves the remote-site router, paying special attention to the priority of DMVPN ISAKMP traffic.

Use the following configuration to define a QoS policy for traffic using public Internet-based WAN services with DMVPN.

The Per-Tunnel QoS for the DMVPN feature allows the configuration of a QoS policy on a DMVPN hub router on a per-tunnel (spoke) basis. With Per-Tunnel QoS, a QoS policy is applied outbound for DMVPN hub-to-spoke tunnels, thus increasing per-tunnel performance for IPsec traffic.

Traffic is regulated from the central site (hub) routers to the remote-site routers on a per-tunnel (spoke) basis. The hub site is unable to send more traffic than a single remote site can handle and ensure that high bandwidth remote sites do not overrun other remote sites.

Procedure 1 Create the QoS Maps to classify traffic

This procedure applies to all WAN routers.

Use the **class-map** command to define a traffic class and identify traffic to associate with the class name. These class names are used when configuring policy maps that define actions you want 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 match any of the specified criteria. This keyword is followed by the name you want to assign to the class of service. After you have configured the **class-map** command, you define specific values, such as DSCP and protocols to match with the match command. You use the following two forms of the **match** command: **match dscp** and **match protocol**.

Using the following steps, configure the required WAN class-maps and matching criteria.

Step 1: Create the class maps for DSCP matching. Repeat this step for each of the six WAN classes of service listed in the following table.

You do not need to explicitly configure the default class.

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

Table 13 - QoS classes of service

Class of service	Traffic type	DSCP values	Bandwidth %	Congestion avoidance
VOICE	Voice traffic	ef	10 (PQ)	–
INTERACTIVE-VIDEO	Interactive video (video conferencing)	cs4, af41	23 (PQ)	–
CRITICAL-DATA	Highly interactive (such as Telnet, Citrix, and Oracle thin clients)	af31, cs3	15	DSCP based
DATA	Data	af21	19	DSCP based
SCAVENGER	Scavenger	af11, cs1	5	–
NETWORK-CRITICAL	Routing protocols. Operations, administration and maintenance (OAM) traffic.	cs6, cs2	3	–
default	Best effort	Other	25	random

Example

```
class-map match-any VOICE
 match dscp ef
!
class-map match-any INTERACTIVE-VIDEO
 match dscp cs4 af41
!
class-map match-any CRITICAL-DATA
 match dscp af31 cs3
!
class-map match-any DATA
 match dscp af21
!
class-map match-any SCAVENGER
 match dscp af11 cs1
!
class-map match-any NETWORK-CRITICAL
 match dscp cs6 cs2
```

Tech Tip

You do not need to configure a Best-Effort Class. This is implicitly included within class-default, as shown in Procedure 4, "Configure the physical interface S&Q policy."

Procedure 2 Add ISAKMP traffic to network-critical

For a WAN connection using DMVPN, you need to ensure proper treatment of ISAKMP traffic in the WAN. You classify this traffic by creating an access-list and adding the access-list name to the NETWORK-CRITICAL class-map created in Procedure 1, "Create the QoS Maps to classify traffic."

This procedure is only required for a WAN-aggregation DMVPN hub router or a WAN remote-site DMVPN spoke router.

Step 1: Create the access-list.

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

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

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

Procedure 3 Define the policy map to use queuing policy

This procedure applies to all WAN routers.

The WAN policy map references the class names you created in the previous procedures and defines the queuing behavior along with the maximum guaranteed bandwidth allocated to each class. This specification is accomplished with the use of a policy-map. Then, each class within the policy map invokes an egress queue, assigns a percentage of bandwidth, and associates a specific traffic class to that queue. One additional default class defines the minimum allowed bandwidth available for best effort traffic.

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. Most providers perform this remapping by matching on DSCP values cs6 and cs2.

Step 1: Create the parent policy map.

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

Step 2: Apply the previously created class-map.

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

Step 3: If you want, assign the maximum guaranteed bandwidth for the class.

```
bandwidth percent [percentage]
```

Step 4: If you want, define the priority queue for the class.

```
priority percent [percentage]
```

Step 5: If you want, define the congestion mechanism.

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

Step 6: Repeat Step 2 through Step 5 for each class in Table 13, including class-default.

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
 class class-default
  bandwidth percent 25
  random-detect
```

Tech Tip

Although these bandwidth assignments represent a good baseline, it is important to consider your actual traffic requirements per class and adjust the bandwidth settings accordingly.

Procedure 4 Configure the physical interface S&Q policy

With WAN interfaces using Ethernet as an access technology, the demarcation point between the enterprise and service provider may no longer have a physical-interface bandwidth constraint. Instead, a specified amount of access bandwidth is contracted with the service provider. To ensure the offered load to the service provider does not exceed the contracted rate that results in the carrier discarding traffic, you need to configure shaping on the physical interface. This shaping is accomplished with a QoS service policy. You configure a QoS service policy on the outside Ethernet interface, and this parent policy includes a shaper that then references a second or subordinate (child) policy that enables queuing within the shaped rate.

This is called a hierarchical Class-Based Weighted Fair Queuing (HCBWFQ) configuration. When you configure the **shape average** command, ensure that the value matches the contracted bandwidth rate from your service provider.

This procedure applies to all WAN routers. You can repeat this procedure multiple times to support devices that have multiple WAN connections attached to different interfaces.

Step 1: Create the parent policy map.

As a best practice, embed the interface name within the name of the parent policy map.

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

Step 2: Configure the shaper.

```
class [class-name]
  shape  [average | peak] [bandwidth (kbps)]
```

Step 3: Apply the child service policy.

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

Example

This example shows a router with a 20-Mbps link on interface GigabitEthernet0/0 and a 10-Mbps link on interface GigabitEthernet0/1.

```
policy-map WAN-INTERFACE-G0/0
 class class-default
  shape average 20000000
 service-policy WAN
!
policy-map WAN-INTERFACE-G0/1
 class class-default
  shape average 10000000
 service-policy WAN
```

Procedure 5 Apply WAN QoS policy to the physical interface

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

This procedure applies to all WAN routers. You can repeat this procedure multiple times to support devices that have multiple WAN connections attached to different interfaces.

Step 1: Select the WAN interface.

```
interface [interface type] [number]
```

Step 2: Apply the WAN QoS policy.

The service policy needs to be applied in the outbound direction.

```
service-policy output [policy-map-name]
```

Example

```
interface GigabitEthernet0/0
 service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
 service-policy output WAN-INTERFACE-G0/1
```

Procedure 6 Configure Per-tunnel QoS NHRP policy on DMVPN spoke routers

This procedure applies to all WAN remote-site DMVPN routers.

Step 1: Apply the NHRP group policy to the DMVPN tunnel interface on the corresponding remote-site router. Use the NHRP group name as defined on the hub router in the previous procedure.

```
interface Tunnel10
 ip nhrp group [NHRP GROUP Policy Name]
```

Example

The following shows a remote site using a 10-Mbps policy.

```
interface Tunnel10
  ip nhrp group RS-GROUP-10MBPS
```

The following shows corresponding hub site configuration NHRP policy mappings.

```
interface Tunnel10
  ip nhrp map group RS-GROUP-10MBPS service-policy output RS-GROUP-10MBPS-POLICY
```

Reader Tip

For more information about configuration details for VPN WAN Per-Tunnel QoS policies, see the VPN WAN Technology Design Guide.

Procedure 7 Configure IPSEC anti-replay window size

Cisco IOS Software provides anti-replay protection against an attacker duplicating encrypted packets.

IPsec security association (SA) anti-replay is a security service in which the decrypting router can reject duplicate packets and protect itself against replay attacks.

Cisco quality of service (QoS) gives priority to high-priority packets, which may cause some low-priority packets to be discarded. By expanding the IPsec anti-replay window you can allow the router to keep track of more than 64 packets.

Step 1: Increase the anti-replay window size.

```
crypto ipsec security-association replay window-size 1024
```

Tech Tip

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed.

It is recommended that you use the full 1024 window size in order to eliminate future anti-replay problems.

If you do not increase the window size, you may encounter dropped packets and the following error message on the router CLI:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
```

Appendix A: Product List

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco ISR 3945 w/ SPE150, 3GE, 4EHWIC, 4DSP, 4SM, 256MBCF, 1GBDRAM, IP Base, SEC, AX licenses with; DATA, AVC, and WAAS/vWAAS with 2500 connection RTU	C3945-AX/K9	15.3(3)M3 securityk9 feature set datak9 feature set uck9 feature set
	Cisco ISR 3925 w/ SPE100 (3GE, 4EHWIC, 4DSP, 2SM, 256MBCF, 1GBDRAM, IP Base, SEC, AX licenses with; DATA, AVC, WAAS/vWAAS with 2500 connection RTU	C3925-AX/K9	
	Unified Communications Paper PAK for Cisco 3900 Series	SL-39-UC-K9	
	Cisco ISR 2951 w/ 3 GE, 4 EHWIC, 3 DSP, 2 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with; DATA, AVC, and WAAS/vWAAS with 1300 connection RTU	C2951-AX/K9	
	Cisco ISR 2921 w/ 3 GE, 4 EHWIC, 3 DSP, 1 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with; DATA, AVC, and WAAS/vWAAS with 1300 connection RTU	C2921-AX/K9	
	Cisco ISR 2911 w/ 3 GE,4 EHWIC, 2 DSP, 1 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with; DATA, AVC and WAAS/vWAAS with 1300 connection RTU	C2911-AX/K9	
	Unified Communications Paper PAK for Cisco 2900 Series	SL-29-UC-K9	
	Cisco ISR 1941 Router w/ 2 GE, 2 EHWIC slots, 256MB CF, 2.5GB DRAM, IP Base, DATA, SEC, AX license with; AVC and WAAS-Express	C1941-AX/K9	15.3(3)M3 securityk9 feature set datak9 feature set

LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Stackable Access Layer Switch	Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.3.3SE(15.0.1EZ3) IP Base feature set
	Cisco Catalyst 3850 Series Stackable 24 Ethernet 10/100/1000 PoE+ Ports	WS-C3850-24P	
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	
	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 2x10GE or 4x1GE Uplink	WS-C3650-24PD	3.3.3SE(15.0.1EZ3) IP Base feature set
	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 4x1GE Uplink	WS-C3650-24PS	
	Cisco Catalyst 3650 Series Stack Module	C3650-STACK	
	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.2(1)E3 IP Base feature set
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
	Cisco Catalyst 2960-X Series 24 10/100/1000 Ethernet and 2 SFP+ Uplink	WS-C2960X-24PD	15.0(2)EX5 LAN Base feature set
	Cisco Catalyst 2960-X FlexStack-Plus Hot-Swappable Stacking Module	C2960X-STACK	
Standalone Access Layer Switch	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 4x1GE Uplink	WS-C3650-24PS	3.3.3SE(15.01EZ3) IP Base feature set

Appendix B: Device Configuration Files

To view the configuration files from the CVD lab devices that we used to test this guide, please go to the following URL:

http://cvddocs.com/fw/221-14b

Appendix C: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- We updated EIGRP named mode configurations.
- We updated EIGRP neighbor authentication configurations.
- We updated DMVPN Per-Tunnel QoS spoke configurations.
- We enabled Secure Copy Protocol (SCP) to simplify the use of Cisco Prime Infrastructure for device management.
- We added the **ip scp server enable** command to the router configuration.

Feedback

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

B-0000222-1 08/14