# MPLS WAN

## 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.

## Use Cases

This guide addresses the following technology use cases:

- **Site-to-Site Communications Using MPLS L3VPN Services**—Many organizations are deploying Multiprotocol Label Switching (MPLS) WAN services in order to connect remote locations over private cloud Layer 3 VPN-based provider-managed MPLS networks.

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

## Scope

This guide covers the following areas of technology and products:

- WAN design using Layer 3 MPLS services for central and remote sites
- Remote-site WAN redundancy options
- Routing policy and control for WAN aggregation and remote sites
- WAN quality of service (QoS) design and configuration

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

## Related CVD Guides


Campus Wired LAN Technology Design Guide


GET VPN Technology Design Guide


VPN WAN Technology Design Guide

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

# Introduction

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

## Related Reading

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.

## Technology Use Cases

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

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

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

### Use Case: Site-to-Site Communications Using MPLS L3VPN Services

This guide helps organizations deploy WAN services in order to connect remote locations over private cloud Layer 3 VPN-based provider managed MPLS services.

This design guide enables the following network capabilities:

- IP any-to-any WAN connectivity for up to 500 remote sites and one or two central hub site locations
- Deployment of single or dual MPLS service providers for resiliency using single or dual routers in remote site locations
- Static routing or dynamic Border Gateway Protocol (BGP) peering with the MPLS service provider for site-to-site communications.
- Support for Layer 2 or Layer 3 distribution switching designs
- Support for IP multicast using Multicast VPN (mVPN) service provider-based offering
- QoS for WAN traffic such as Voice over IP (VoIP) and business critical applications

# Design Overview

This guide, the *MPLS WAN Technology Design 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 document shows you how to deploy the network foundation and services to enable the following:

- MPLS WAN connectivity for up to 500 remote sites
- Primary and secondary links to provide redundant topology options for resiliency
- Wired LAN access at all remote sites

## WAN Design

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

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

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

The usage of an Internet VPN transport to provide a redundant topology option for resiliency is covered in the VPN WAN Technology Design Guide.

## 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 BGP to distribute VPN-related information. This peer-to-peer model allows enterprise subscribers to outsource routing information to service providers, which can result in significant cost savings and a reduction in operational complexity for enterprises.

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

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

## Ethernet WAN

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

## WAN-Aggregation Designs

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

The WAN transport options include MPLS VPN used as a primary or secondary transport. Each transport connects to a dedicated CE router. A similar method of connection and configuration is used for both.

This design guide documents multiple WAN-aggregation design models that are statically or dynamically routed with either single or dual MPLS carriers. The primary differences between the various designs are the usage of routing protocols and the overall scale of the architecture. For each design model, you can select several router platforms with differing levels of performance and resiliency capabilities.

Each of the design models is shown with LAN connections into either a collapsed core/distribution layer or a dedicated WAN distribution layer. There are no functional differences between these two methods from the WAN-aggregation perspective.

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

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

*Table 1 - WAN-aggregation design models*

| | MPLS Static | MPLS Dynamic | Dual MPLS |
|---|---|---|---|
| Remote sites | Up to 50 | Up to 100 | Up to 500 |
| WAN links | Single | Single | Dual |
| Edge routers | Single | Single | Dual |
| WAN routing protocol | None (static) | BGP (dynamic) | BGP (dynamic) |
| Transport 1 | MPLS VPN A | MPLS VPN A | MPLS VPN A |
| Transport 2 | – | – | MPLS VPN B |

The characteristics of each design are discussed in the following sections.

## MPLS Static Design Model

The MPLS Static design model (Figure 1):

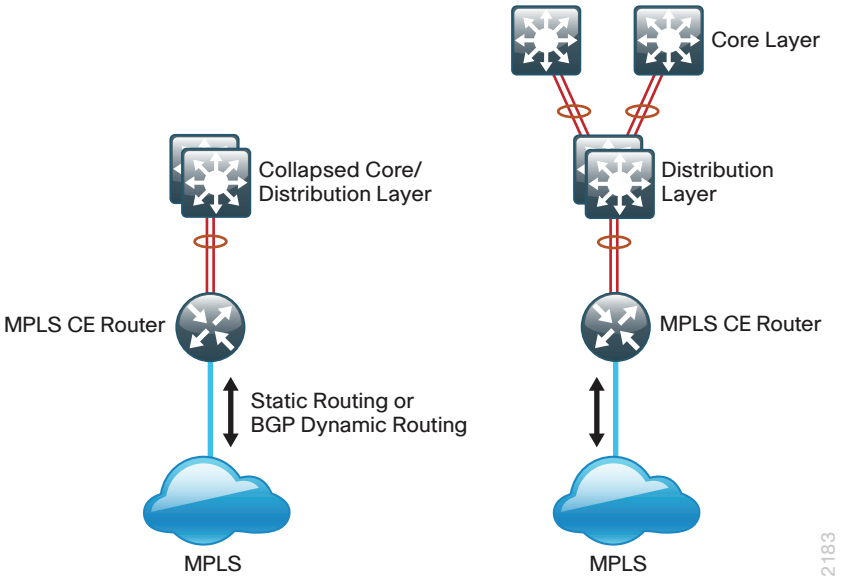
- Supports up to 50 remote sites.
- Has a single MPLS VPN carrier.
- Uses static routing with MPLS VPN carrier.

## MPLS Dynamic Design Model

The MPLS Dynamic design model (Figure 1):

- Supports up to 100 remote sites.
- Has a single MPLS VPN carrier.
- Uses BGP routing with MPLS VPN carrier.

*Figure 1 - MPLS Static and MPLS Dynamic design models (single MPLS carrier)*

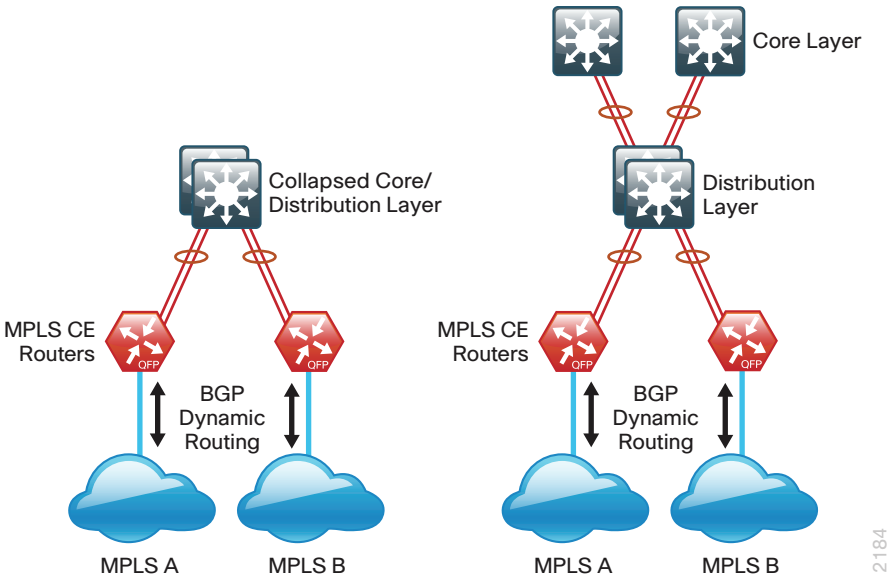


## Dual MPLS Design Model

The Dual MPLS design model (Figure 2):

- Supports up to 500 remote sites.
- Has multiple MPLS VPN carriers.
- Uses BGP routing with MPLS VPN carrier.
- Is typically used with a dedicated WAN distribution layer.

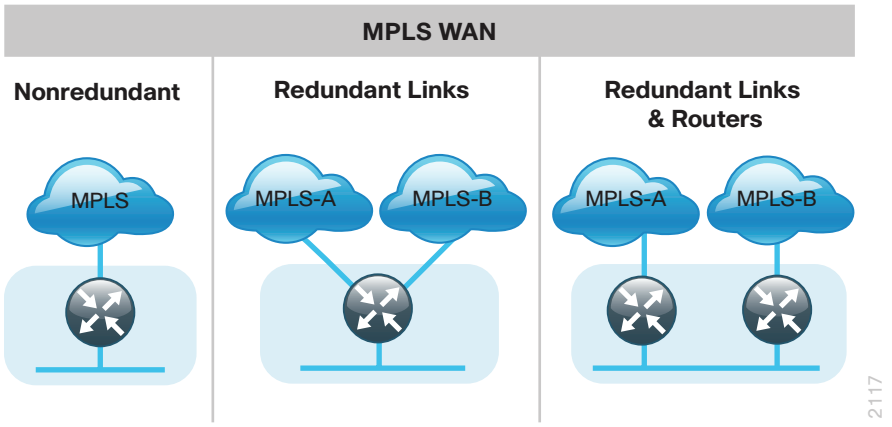
*Figure 2 - Dual MPLS design model*




## WAN Remote-Site Designs

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

*Figure 3 - WAN remote-site designs*



The remote-site designs include single or dual WAN edge routers. These are always MPLS CE routers.

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

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

*Table 2 - WAN remote-site transport options*

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

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

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

## WAN/LAN Interconnection

The primary role of the WAN is to interconnect primary site and remote-site LANs. The LAN discussion within this guide is limited to how the WAN-aggregation site LAN connects to the WAN-aggregation devices and how the remote-site LANs connect to the remote-site WAN devices. Specific details regarding the LAN components of the design are covered in the Campus Wired LAN Technology Design Guide.

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

*Table 3 - WAN remote-site LAN options*

| WAN remote-site routers | WAN transports | LAN topology |
|---|---|---|
| Single | Single | Access only<br>Distribution/access |
| Single | Dual | Access only<br>Distribution/access |
| Dual | Dual | Access only<br>Distribution/access |

## WAN Remote Sites–LAN Topology

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

*Table 4 - WAN remote-sites–VLAN assignment*

| VLAN | Usage | Layer 2 access | Layer 3 distribution/ access |
|---|---|---|---|
| VLAN 64 | Data | Yes | – |
| VLAN 69 | Voice | Yes | – |
| VLAN 99 | Transit | Yes<br>(dual router only) | Yes<br>(dual router only) |
| VLAN 50 | Router link (1) | – | Yes |
| VLAN 54 | Router link (2) | – | Yes<br>(dual router only) |

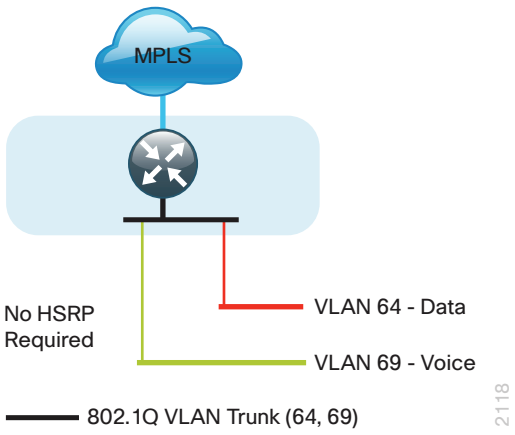
## Layer 2 Access

WAN remote sites that do not require additional distribution layer routing devices are considered to be flat or from a LAN perspective they are considered unrouted Layer 2 sites. All Layer 3 services are provided by the attached WAN routers. The access switches, through the use of multiple VLANs, can support services such as data 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.

Access switches and their configuration are not included in this guide. The Campus Wired LAN Technology Design Guide provides configuration details on the various access switching platforms.

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

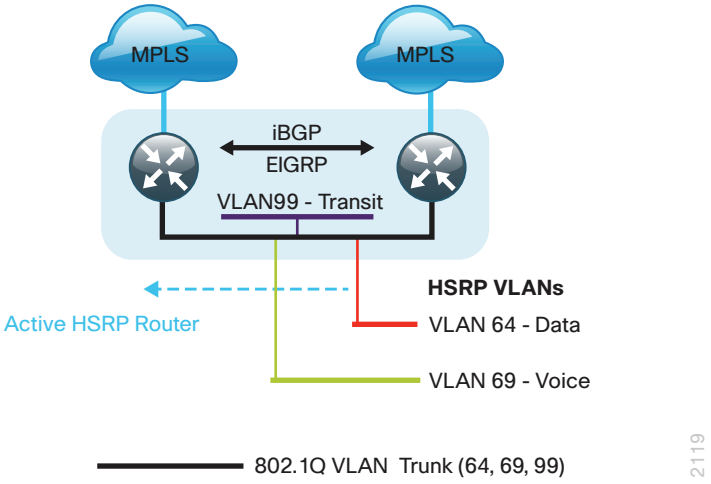
*Figure 4 - WAN remote site–Flat Layer 2 LAN (single router)*



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

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

*Figure 5 - WAN remote site–Flat Layer 2 LAN (dual router)*

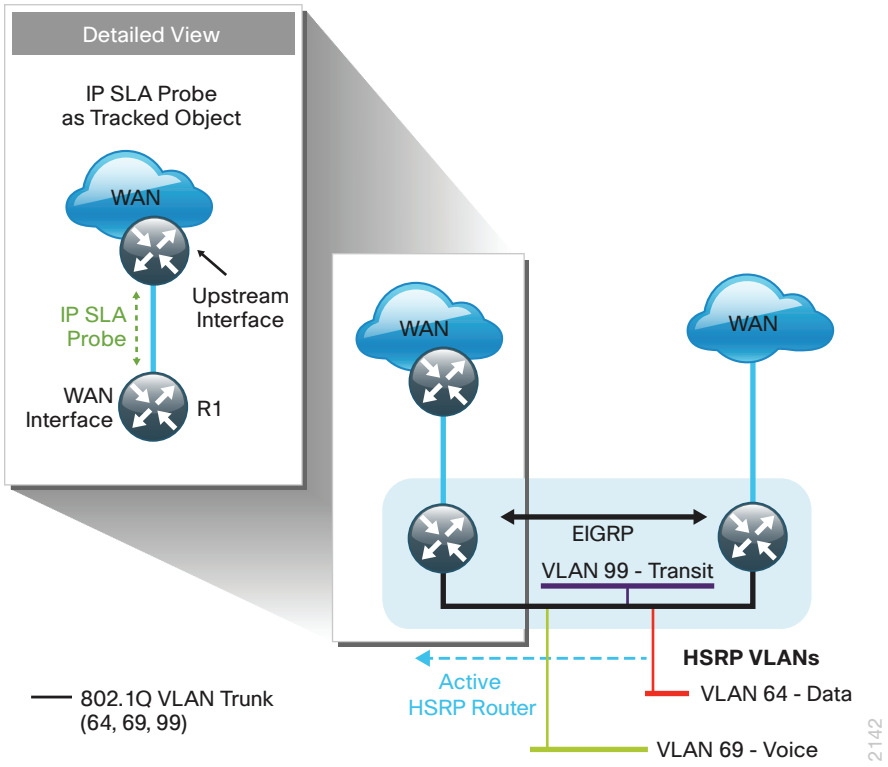



Enhanced Object Tracking (EOT) provides a consistent methodology for various router and switching features to conditionally modify their operation based on information objects available within other processes. The objects that can be tracked include interface line protocol, IP route reachability, and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

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

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

*Figure 6 - WAN remote-site–IP SLA probe to verify upstream device reachability*




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

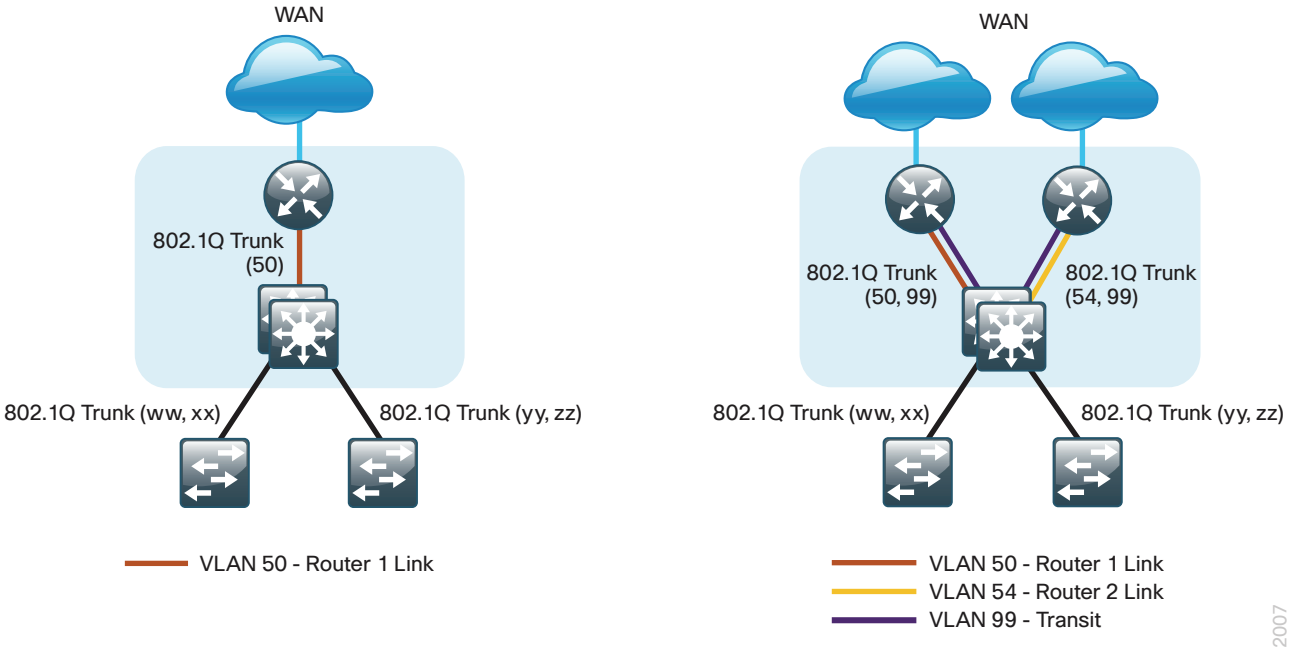
The dual router designs also warrant an additional component that is required for proper routing in certain scenarios. In these cases, a traffic flow from a remote-site host might be sent to a destination reachable via the alternate WAN transport (for example, an MPLS A + MPLS B remote site communicating with an MPLS-B-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.

## Distribution and Access Layer

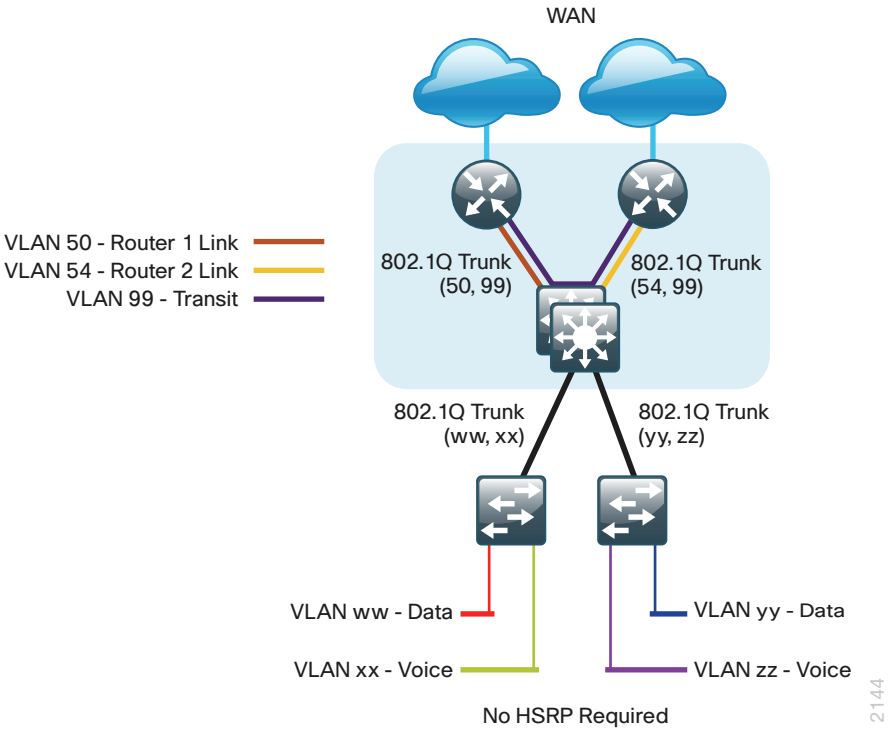
Large remote sites may require a LAN environment similar to that of a small campus LAN that includes a distribution layer and access layer. This topology works well with either a single or dual router WAN edge. To implement this design, the routers should connect via EtherChannel links to the distribution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

*Figure 7 - WAN remote site–Connection to distribution layer*




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

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



### IP Multicast

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

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

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

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

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

## Quality of Service

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

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

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

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

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

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

*Table 5 - QoS service class mappings*

| Service class | Per-hop behavior (PHB) | Differentiated services code point (DSCP) | IP precedence (IPP) | Class of service (CoS) |
|---|---|---|---|---|
| Network layer | Layer 3 | Layer 3 | Layer 3 | Layer 2 |
| Network control | CS6 | 48 | 6 | 6 |
| Telephony | EF | 46 | 5 | 5 |
| Signaling | CS3 | 24 | 3 | 3 |
| Multimedia conferencing | AF41, 42, 43 | 34, 36, 38 | 4 | 4 |
| Real-time interactive | CS4 | 32 | 4 | 4 |
| Multimedia streaming | AF31, 32, 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 |

# Overall WAN Architecture Design Goals

## IP Routing

The design has the following IP routing goals:

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

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

## LAN Access

All remote sites are to support both wired LAN access.

## High Availability

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

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

## Path Selection Preferences

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

The single WAN transport routing functions as follows.

MPLS VPN-connected site:

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

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

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

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

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

## Quality of Service (QoS)

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

## 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 |

# Design Overview

## WAN-Aggregation–MPLS CE Routers

The MPLS WAN designs are intended to support up to 500 remote sites with a combined aggregate WAN bandwidth of up to 1.0 Gbps. The most critical devices are the WAN routers that are responsible for reliable IP forwarding and QoS. The amount of bandwidth required at the WAN-aggregation site determines which model of router to use. The choice of whether to implement a single router or dual router is determined by the number of carriers that are required in order to provide connections to all of the remote sites.

Cisco ASR 1000 Series Aggregation Services Routers represent the next-generation, modular, services-integrated Cisco routing platform. They are specifically designed for WAN aggregation, with the flexibility to support a wide range of 3- to 16-mpps (millions of packets per second) packet-forwarding capabilities, 2.5- to 40-Gbps system bandwidth performance, and scaling.

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

This design uses the following routers as MPLS CE routers:

- Cisco ASR 1002-X router configured with an embedded service processor (ESP) default bandwidth of 5 Gbps upgradable with software licensing options to 10 Gbps, 20 Gbps, and 36 Gbps
- Cisco ASR 1002 router configured with an embedded service processor 5 (ESP5)
- Cisco ASR 1001 router fixed configuration with a 2.5 Gbps embedded service processor
- Cisco 4451X Integrated Services Router

All of the design models can be constructed using any of the MPLS CE routers listed in Table 7. You should consider the following: the forwarding performance of the router using an Ethernet WAN deployment with broad services enabled, the router's alignment with the suggested design model, and the number of remote sites.

*Table 7 - WAN aggregation–MPLS CE router options*

| Service | Cisco 4451X | ASR 1001 | ASR 1002 | ASR 1002-X |
|---|---|---|---|---|
| Ethernet WAN with services | 300 Mbps | 500 Mbps | 750 Mbps | 1Gbps |
| Software Redundancy Option | None | Yes | Yes | Yes |
| Redundant power supply | Option | Default | Default | Default |
| Supported Design Models | All | All | All | All |
| Suggested Design Model | MPLS Static | MPLS Dynamic | Dual MPLS | Dual MPLS |
| Suggested Number of Remote Sites | 25 | 100 | 250 | 250+ |

## Remote Sites–MPLS CE Router Selection

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

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

*Table 8 - WAN remote-site Cisco Integrated Services Router options*

| | 891[1] | 1941[2] | 2911 | 2921 | 2951 | 3925 | 3945 | 4451-X |
|---|---|---|---|---|---|---|---|---|
| **Ethernet WAN with services[3]** | 8 Mbps | 25 Mbps | 35 Mbps | 50 Mbps | 75 Mbps | 100 Mbps | 150 Mbps | 1 Gbps |
| **On-board FE ports** | 1 (and 8-port LAN switch) | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **On-board GE ports[4]** | 1 | 2 | 3 | 3 | 3 | 3 | 3 | 4 |
| **Service module slots[5]** | 0 | 0 | 1 | 1 | 2 | 2 | 4 | 2 |
| **Redundant power supply option** | No | No | No | No | No | Yes | Yes | Yes |

Notes:

1. The Cisco 891 Integrated Services Router is recommended for use at single-router, single-link remote sites.
2. The 1941 is recommended for use at single-router, single-link remote sites.
3. 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.
4. 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.
5. Not all service modules are supported in Cisco 4451-X ISR. Some service modules are double-wide.

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

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

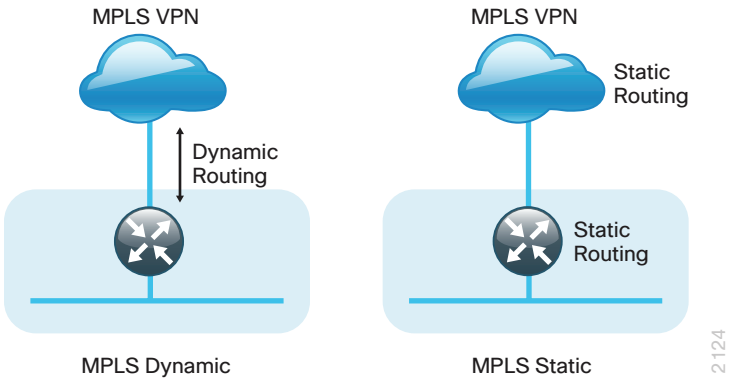
Dynamic routing makes it easy to add or modify IP networks at the remote site because any changes are immediately propagated to the rest of the network. MPLS VPN-connected sites require static routing in order to be handled by the carrier, and any changes or modifications require a change request to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

The smaller scale MPLS Static design uses static routing and relies on the carrier to configure the additional required static routes on the PE routers.

**Tech Tip**

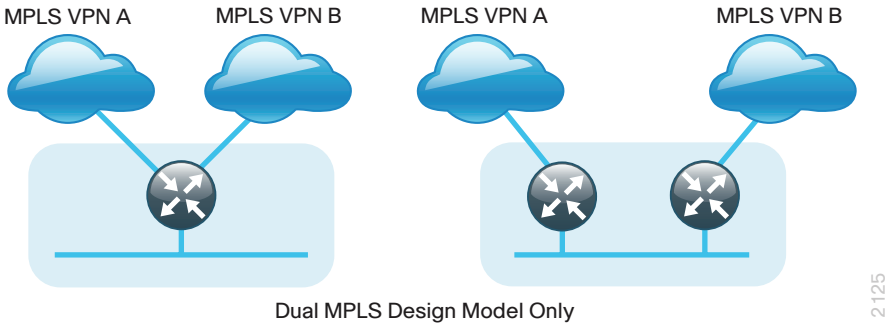
We recommend that you select the Dual MPLS or MPLS Dynamic designs if you intend to use resilient WAN links or want to be able to modify your routing configuration without carrier involvement.

*Figure 9 - MPLS WAN remote site (single-router, single-link)*




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

*Figure 10 - MPLS WAN dual-carrier remote site (dual-link options)*




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

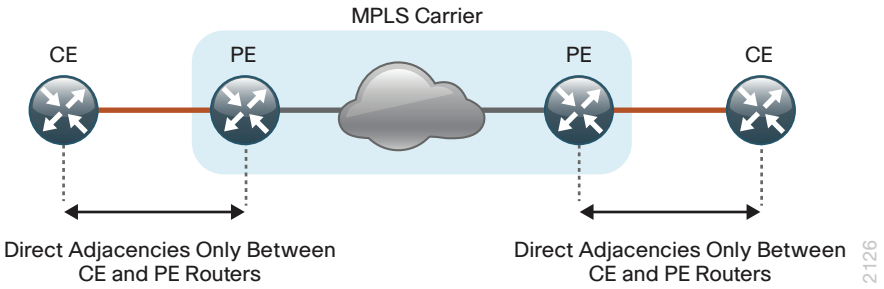
## Design Details

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

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

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

*Figure 11 - MPLS VPN (PE-CE connections)*




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

**Tech Tip**

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

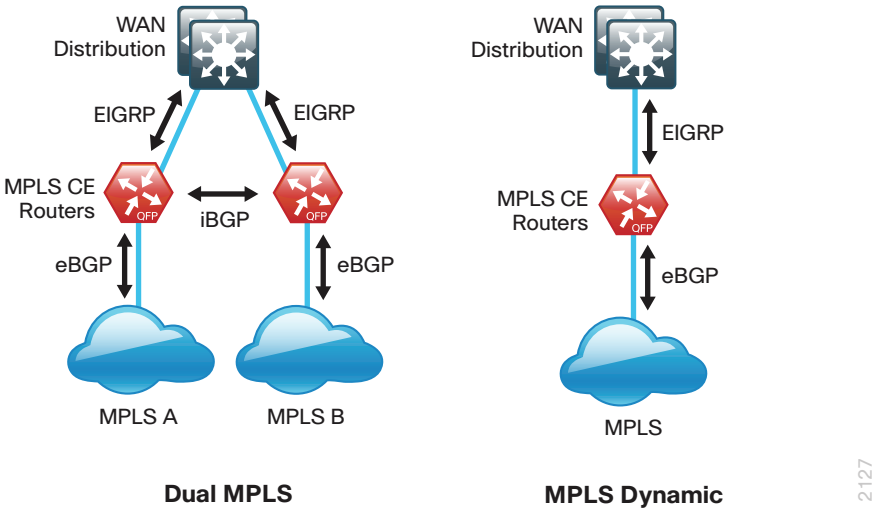
Sites with only a single WAN transport (a single-homed site) do not require dynamic PE-CE routing, and can rely on static routing because there is only a single path to any destination. This design recommends dynamic PE-CE routing to provide consistency with configurations across both single-homed and dual-homed sites. This also allows for easy transition from a single-homed to a dual-homed remote-site design by adding an additional link to an existing remote site. A static routing option is also included to support smaller scale requirements that do not require a dynamic routing protocol. Static routing is used in the MPLS Static design model.

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

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

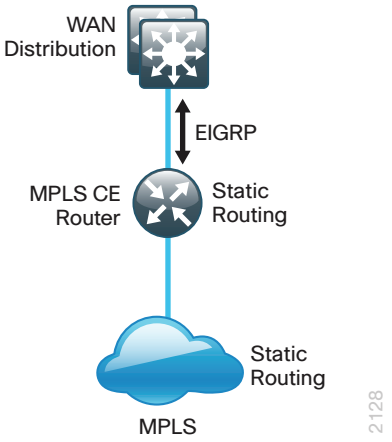
At the WAN-aggregation site, an MPLS CE router must be connected both to the distribution layer and to its respective MPLS carrier. Multiple routing protocols (EIGRP and BGP) are used to exchange routing information, and the routing protocol configurations are tuned from their default settings to influence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

*Figure 12 - Dual MPLS and MPLS Dynamic designs–MPLS CE routing detail*




The IP routing details for the single MPLS carrier WAN-aggregation topology with static routing are shown in the following figure.

*Figure 13 - MPLS Static Design–MPLS CE routing detail*




## EIGRP

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

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

> **Tech Tip**
>
> With EIGRP named mode configuration, EIGRP Wide Metric support is on by default and backward compatible with existing routes.

In this design, the primary EIGRP process (AS 100) is referred to as *EIGRP LAN* and uses EIGRP named configuration.

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

### BGP

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

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

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

# Deployment Details

## 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
```

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

*Table 9 - Parameters used in the deployment examples*

| Hostname | Loopback IP Address | Port Channel IP Address |
|---|---|---|
| CE-ASR1002-1 | 10.4.32.241/32 | 10.4.32.2/30 |
| CE-ASR1001-2 | 10.4.32.242/32 | 10.4.32.6/30 |

PROCESS

## Configuring the MPLS CE Router

1. Configure the distribution switch
2. Configure the WAN aggregation platform
3. Configure connectivity to the LAN
4. Connect to MPLS PE router
5. Redistribute WAN routes into EIGRP
6. Configure BGP

## Procedure 1 Configure the distribution switch

**Reader Tip**

This process assumes that the distribution switch has already been configured following the guidance in the Campus Wired LAN Technology Design Guide. Only the procedures required to support the integration of the WAN-aggregation router into the deployment are included.

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

**Tech Tip**

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

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

```
interface Port-channel1
 description CE-ASR1002-1
 no switchport
 ip address 10.4.32.1 255.255.255.252
 ip pim sparse-mode
 logging event link-status
 carrier-delay msec 0
 load-interval 30
 no shutdown
```

**Step 2:** Configure EtherChannel member interfaces.

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

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

```
interface GigabitEthernet1/0/1
 description CE-ASR1002-1 Gig0/0/0
!
interface GigabitEthernet2/0/1
 description CE-ASR1002-1 Gig0/0/1
!
interface range GigabitEthernet1/0/1, GigabitEthernet2/0/1
  no switchport

  carrier-delay msec 0
```

```
 channel-group 1 mode on
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 no shutdown
 load-interval 30
 macro apply EgressQoS
```

Step 3: Allow the routing protocol to form neighbor relationships across the port channel interface.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface Port-channel1
   no passive-interface
   authentication mode md5
   authentication key-chain LAN-KEY
  exit-af-interface
 exit-address-family
```

Step 4: If it is necessary to disable EIGRP stub routing on the WAN distribution switch, enter the following configuration.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
 no eigrp stub
 exit-address-family
```

Step 5: On the distribution layer switch, configure the layer 3 EIGRP interfaces connected to the LAN core to summarize the WAN network range.

**Tech Tip**

It is a best practice to summarize IP routes from the WAN distribution layer towards the core.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface Port-channel38
   summary-address 10.4.32.0 255.255.248.0
   summary-address 10.4.128.0 255.255.240.0
   summary-address 10.4.160.0 255.255.252.0
   summary-address 10.5.0.0 255.255.0.0
  exit-af-interface
 exit-address-family
```

**Step 6:** On the distribution layer switch, configure the Layer 3 EIGRP interface connected to the WAN aggregation routers to summarize the WAN remote-site network range.

> **Tech Tip**
>
> It is a best practice to summarize IP routes from the WAN distribution layer towards the MPLS WAN.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface Port-channel1
   summary-address 10.5.0.0 255.255.0.0
  exit-af-interface
 exit-address-family
```

Repeat this step as needed for additional WAN aggregation routers.

## Procedure 2 Configure the WAN aggregation platform

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

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

```
hostname CE-ASR1002-1
```

**Step 2:** Configure 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
```

**Step 3:** By default, HTTPS access to the router uses the enable password for authentication.

**Step 4:** (Optional) Configure centralized user authentication.

As networks scale in the number of devices to maintain it poses an operational burden to maintain local user accounts on every device. A centralized authentication, authorization, and accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

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 5:** Configure device management protocols.

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

Secure management of the network device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the unsecure protocols, Telnet and HTTP, are turned off. Secure Copy Protocol is enabled, which allows the use of code upgrades using Prime Infrastructure via SSH-based SCP protocol.

Specify the transport preferred none on vty lines 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 6:** 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 7:** 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 8:** If operational support is centralized in your network, you can 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 will be 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 login from one router to the next for hop-by-hop troubleshooting.

**Step 9:** Configure a synchronized clock.

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

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

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

**Step 10:** 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 router 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 router summarizes to the rest of the network.

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

**Step 11:** 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 12:** Configure IP unicast routing authentication key to be used for EIGRP neighbor authentication.

```
key chain LAN-KEY
 key 1
   key-string cisco
```

**Step 13:** Configure IP unicast routing using EIGRP named mode.

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

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
 network 10.4.0.0 0.1.255.255
 eigrp router-id 10.4.32.241
 nsf
 exit-address-family
```

**Step 14:** Configure IP Multicast routing.

IP Multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than 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.

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

```
ip multicast-routing
```

If you are using a Cisco ASR 1000 Series router, the **distributed** keyword is required.

```
ip multicast-routing distributed
```

**Step 15:** 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 16:** Enable sparse mode multicast operation for all Layer 3 interfaces in the network.

```
ip pim sparse-mode
```

## Procedure 3 Configure connectivity to the LAN

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

**Step 1:** Configure Layer 3 interface.

```
interface Port-channel1
  description WAN-D3750X
  ip address 10.4.32.2 255.255.255.252
  ip pim sparse-mode
  no shutdown
```

**Step 2:** Configure EtherChannel member interfaces.

Configure the physical interfaces to tie to the logical port-channel by using the **channel-group** command. The number for the port-channel and channel-group must match. Not all router platforms can support LACP to negotiate with the switch, so you configure EtherChannel statically.

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

**Step 3:** Configure the EIGRP interface.

Allow EIGRP to form neighbor relationships across the interface to establish peering adjacencies and exchange route tables. In this step, configure EIGRP authentication by using the authentication key specified in the previous procedure.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface Port-channel1
   no passive-interface
   authentication mode md5
   authentication key-chain LAN-KEY
  exit-af-interface
exit-address-family
```

## Procedure 4 Connect to MPLS PE router

**Step 1:** Assign the interface bandwidth.

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

The example shows a Gigabit interface (1000 Mbps) with a subrate of 300 Mbps.

```
interface GigabitEthernet0/0/3
 description MPLS PE Router
 bandwidth 300000
```

**Tech Tip**

Command reference:

**bandwidth** *kbps*

(300 Mbps = 300,000 kbps)

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

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

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

**Step 3:** Administratively enable the interface and disable CDP.

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

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

## Procedure 5 Redistribute WAN routes into EIGRP

The WAN-aggregation CE routers are configured either for dynamic routing with BGP or are statically routed. If you have a remote-site design that includes sites with dual WAN links, or do not wish to have your MPLS carrier make changes or modifications, then use the BGP option. This is the recommended approach.

If your remote-site design only uses single WAN links and you don't anticipate adding or modifying IP networks at the remote sites, then you can use the statically routed option. The MPLS carrier is responsible for configuring static IP routing within the MPLS network.

**Tech Tip**

If you do not use dynamic routing with BGP, then the MPLS carrier must configure a set of static routes on its PE routers for the WAN-aggregation site and for each of the remote sites. Site-specific routing details must be shared with your MPLS carrier.

## Option 1: BGP dynamic routing with MPLS carrier

**Step 1:** Redistribute BGP into EIGRP.

A default metric redistributes the BGP routes into EIGRP. By default, only the bandwidth and delay values are used for metric calculation.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  topology base
   default-metric 300000 100 255 1 1500
   redistribute bgp 65511
  exit-af-topology
 exit-address-family
```

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

This design uses mutual route redistribution: BGP routes are distributed into EIGRP and EIGRP routes are distributed into BGP (covered in Procedure 6). It is important to tightly control how routing information is shared between different routing protocols when you use this configuration; otherwise, you might experience route flapping, where certain routes are repeatedly installed and withdrawn from the device routing tables. Proper route control ensures the stability of the routing table.

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

The specific route tags in use are shown below.

*Table 10 - Route tag information for WAN-aggregation MPLS CE routers*

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

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

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

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

```
route-map BLOCK-TAGGED-ROUTES deny 10
 match tag 65401 65402 65512
!
route-map BLOCK-TAGGED-ROUTES permit 20
!
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  topology base
   distribute-list route-map BLOCK-TAGGED-ROUTES in
  exit-af-topology
 exit-address-family
```

## Option 2: Static routing with service provider

**Step 1:** Configure static routes to remote sites' LANs on the WAN-aggregation CE router. It is a best practice to summarize the remote-site network ranges into a single route when possible.

```
ip route 10.5.0.0 255.255.0.0 192.168.5.2
```

**Step 2:** It is desirable to advertise a route for the MPLS PE-CE links, which includes the CE routers' WAN interfaces, so you can use this to determine router reachability, for troubleshooting. It is a best practice to summarize the PE-CE link ranges into a single route when possible.

```
ip route 192.168.5.0 255.255.255.0 192.168.5.2
```

**Step 3:** Configure routes to the remote-site router loopback addresses. A single summary route for the loopback range may be used when possible.

```
ip route 10.255.250.0 255.255.255.0 192.168.5.2
```

**Step 4:** Configure EIGRP to advertise the remote-site static routes. A default metric redistributes these routes into EIGRP. By default, only the bandwidth and delay values are used for metric calculation.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  topology base
   default-metric 300000 100 255 1 1500
   redistribute static
  exit-af-topology
 exit-address-family
```

## Procedure 6 Configure BGP

If you are using BGP dynamic routing with the MPLS carrier, complete this procedure.

**Step 1:** Enable BGP.

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

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

**Step 2:** Configure eBGP.

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

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

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

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

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

**Step 3:** Redistribute EIGRP into BGP.

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

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

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

**Step 4:** If you have dual MPLS carriers, configure a BGP link between the CE routers.

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

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

PROCESS

## Configuring the Remote-Site MPLS CE Router

1. Configure the WAN remote router
2. Connect to the MPLS PE router
3. Configure WAN routing
4. Connect router to access-layer switch
5. Configure access-layer routing
6. Configure remote-site DHCP
7. Configure access-layer HSRP
8. Configure the transit network
9. Configure EIGRP (LAN side)
10. Configure BGP
11. Enable enhanced object tracking

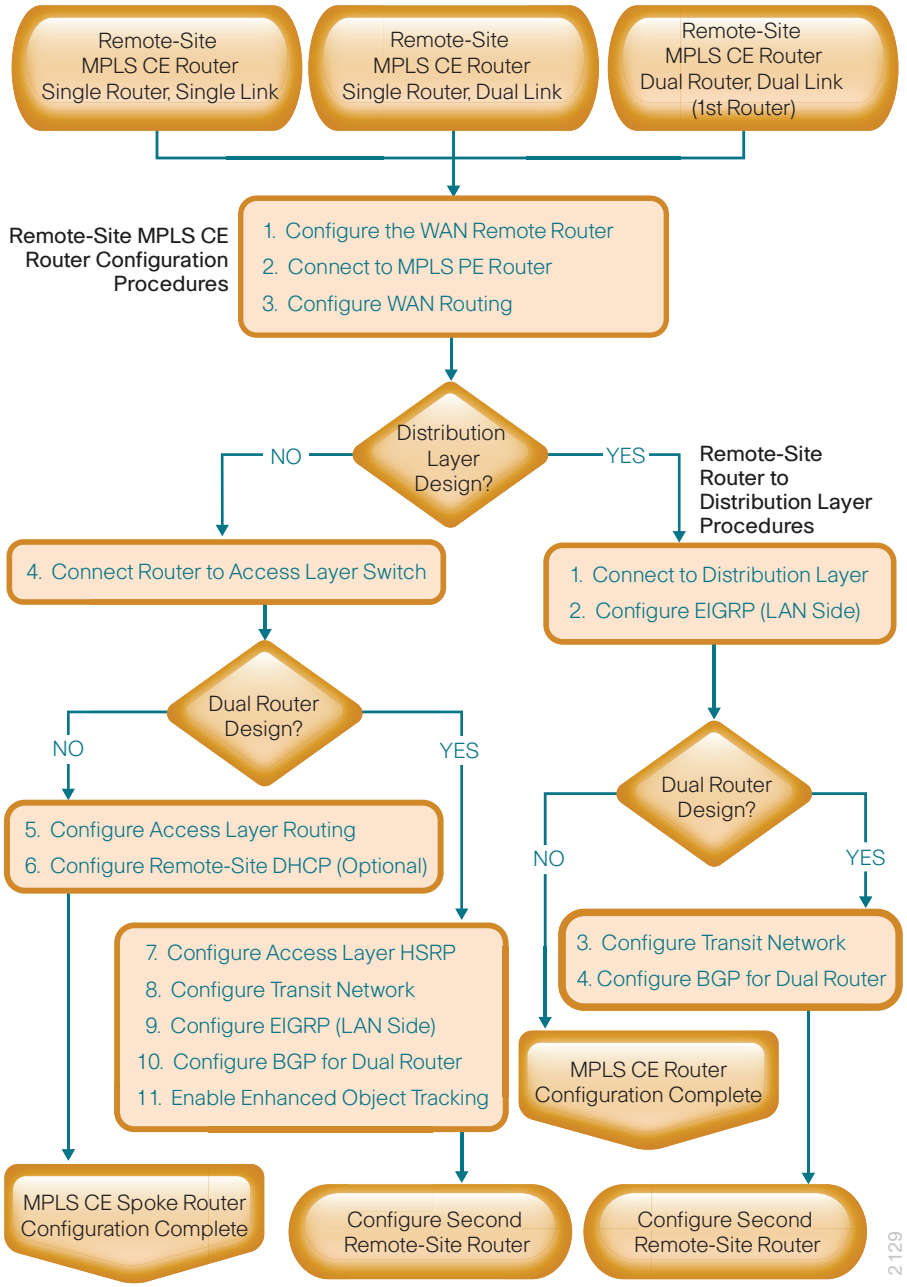
Use this process for the configuration of any of the following:

- MPLS CE router for an MPLS WAN remote site (single router, single link)
- MPLS WAN Dual Carrier remote site

Use the following procedures when performing the initial configuration of a dual-connected MPLS CE in the single-router, dual-link design or for configuring the first router of the dual-router, dual-link design.

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

*Figure 14 - Remote-site MPLS CE router configuration flowchart*



## Procedure 1 Configure the WAN remote router

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

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

```
hostname [hostname]
```

**Step 2:** Configure the local login and password.

The local login account and password provides basic access authentication to a router that 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
```

**Step 3:** By default, https access to the router uses the enable password for authentication.

**Step 4:** (Optional) Configure centralized user authentication.

As networks scale in the number of devices to maintain, it can be an operational burden to maintain local user accounts on every device. A centralized authentication, authorization, and accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

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 in order 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 5:** Configure device management protocols.

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

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

Protocol is enabled, which allows the use of code upgrades using Prime Infrastructure via SSH-based SCP protocol.

Specify the **transport preferred none** on vty lines 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 6:** 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 7:** Enable Simple Network Management Protocol (SNMP). This allows the network infrastructure devices to be managed by a Network Management System (NMS). Configure SNMPv2c both for a read-only and a read-write community string.

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

**Step 8:** If your network operational support is centralized, you can 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 will be 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 9:** Configure a synchronized clock.

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

NTP then distributes this time across the organization's network.

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

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

**Step 10:** 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 router 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 a unique network range that is not part of any other internal network summary range.

```
interface Loopback 0
  ip address [ip address] 255.255.255.255
  ip pim sparse-mode
```

**Step 11:** Bind the device processes for SNMP, SSH, PIM, TACACS+ and NTP to the loopback interface address for optimal resiliency:

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

**Step 12:** Configure IP Multicast routing.

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

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

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

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

```
ip multicast-routing
```

**Step 13:** 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 14:** Enable sparse mode multicast operation for all Layer 3 interfaces in the network.

```
ip pim sparse-mode
```

## Procedure 2 Connect to the MPLS PE router

**Step 1:** Assign the interface bandwidth.

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

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

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

### Tech Tip

Command Reference:

**bandwidth** *kbps*

10 Mbps = 10,000 kbps

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

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

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

**Step 3:** Administratively enable the interface and disable CDP. The use of CDP on external interfaces is not recommended.

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

### Example

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

## Procedure 3 Configure WAN routing

The remote-site CE routers are configured either for dynamic routing with BGP or are statically routed. If you have a remote-site design that includes sites with dual WAN links or you do not want to have your MPLS carrier make changes or modifications, use the BGP option. This is the recommended approach, and assumes that the WAN-aggregation CE router has already been configured for BGP.

If your remote-site design only uses single WAN links and you don't anticipate adding or modifying IP networks at the remote site, then you can use the statically routed option. The MPLS carrier is responsible for configuring static IP routing within the MPLS network.

**Tech Tip**

If you do not use dynamic routing with BGP, then the MPLS carrier must configure a set of static routes on its PE routers for the WAN-aggregation site and for each of the remote sites. Site-specific routing details must be shared with your MPLS carrier.

### Option 1: BGP dynamic routing with MPLS carrier

**Step 1:** Enable BGP.

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

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

**Step 2:** Configure eBGP.

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

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

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

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

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

```
router bgp 65511
 network [PE-CE link network] mask [PE-CE link netmask]
 network [Loopback network] mask 255.255.255.255
 network [DATA network] mask [netmask]
 network [VOICE network] mask [netmask]
 aggregate-address [summary IP address] [summary netmask] summary-only
 neighbor [IP address of PE] remote-as [carrier ASN]
```

**Example**

```
router bgp 65511
 no synchronization
 bgp router-id 10.255.251.206
 bgp log-neighbor-changes
 network 192.168.3.8 mask 255.255.255.252
 network 10.255.251.206 mask 255.255.255.255
 network 10.5.12.0 mask 255.255.255.0
 network 10.5.13.0 mask 255.255.255.0
 aggregate-address 10.5.8.0 255.255.248.0 summary-only
 neighbor 192.168.3.10 remote-as 65401
 no auto-summary
```

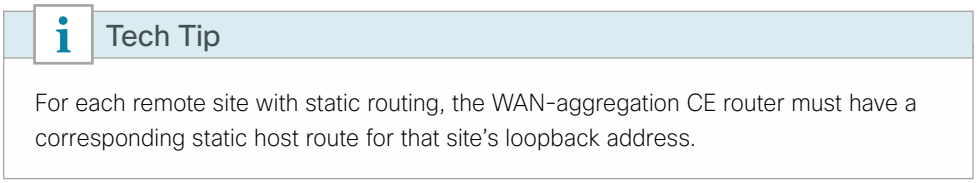
## Option 2: Static routing with service provider

This option has remote sites using static routing to the MPLS WAN to forward all traffic to the WAN-aggregation site.

Step 1: Enter a default route for traffic forwarded to the WAN-aggregation site.

```
ip route 0.0.0.0 0.0.0.0 192.168.3.10
```

Step 2: For the MPLS carrier for each remote site, provide the remote-site specific IP range and the chosen loopback IP address for the router. This properly configures the static routes to the remote site.



## Procedure 4 Connect router to access-layer switch

**Reader Tip**

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

If you are using a remote-site distribution layer, skip to the "Deploying a WAN Remote-Site Distribution Layer" chapter of this guide.

Layer 2 EtherChannels are used to interconnect the CE 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.

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 port-channel interface on the router.

```
interface Port-channel1
 description EtherChannel link to RS206-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. Not all router platforms can support LACP to negotiate with the switch, so you configure EtherChannel statically.

```
interface GigabitEthernet0/1
 description RS206-A2960X Gig1/0/24
!
interface GigabitEthernet0/2
 description RS206-A2960X Gig2/0/24
!
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 1
  no shutdown
```

**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, or in the case of the Cisco Catalyst 4507R+E distribution layer, to separate redundant modules for additional resiliency.

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.

Configure two physical interfaces to be members of the EtherChannel. Also, apply the egress QoS macro that was defined in the LAN switch platform configuration procedure to ensure traffic is prioritized appropriately.

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

```
interface GigabitEthernet1/0/24
 description Link to RS206-3925-1 Gig0/1
interface GigabitEthernet2/0/24
 description Link to RS206-3925-1 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
```

**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 Step 3. Set DHCP Snooping and Address Resolution Protocol (ARP) inspection to trust.

```
interface Port-channel1
 description EtherChannel link to RS206-3925-1
 switchport trunk allowed vlan 64,69,99
 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
```

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 RS202-A3560X 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 RS201-2911 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
```

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

## Procedure 5 Configure access-layer routing

### Option 1: Layer 2 EtherChannel or Layer 2 trunk

**Step 1:** Create subinterfaces and assign VLAN tags.

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

```
interface [type][number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
```

**Step 2:** Configure IP settings for each subinterface.

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

When using a centralized DHCP server, routers with LAN interfaces connected to a LAN using DHCP for end-station IP addressing must use an IP helper. This is the preferred method. An alternate option for local DHCP server configuration is shown in the following procedure.

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

```
interface [type][number].[sub-interface number]
 description [usage]
 ip address [LAN network 1] [LAN network 1 netmask]
 ip helper-address 10.4.48.10
 ip pim sparse-mode
```

**Example**

```
interface GigabitEthernet0/2.64
 description Wired Data
 encapsulation dot1Q 64
 ip address 10.5.68.1 255.255.255.0
 ip helper-address 10.4.48.10
ip pim sparse-mode
```

## Procedure 6 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 IOS 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 10.5.4.1 10.11.4.19
ip dhcp pool DHCP-Wired-Data
 network 10.5.4.0 255.255.255.0
 default-router 10.5.4.1
 domain-name cisco.local
 dns-server 10.4.48.10
```

**Step 3:** Configure a DHCP scope for voice endpoints, excluding DHCP assignment for the first 19 addresses in the subnet.

**Step 4:** 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 10.5.5.1 10.11.5.19
ip dhcp pool DHCP-Wired-Voice
 network 10.5.5.0 255.255.255.0
 default-router 10.5.5.1
 domain-name cisco.local
 dns-server 10.4.48.10
```

Procedure 7 through Procedure 11 are only relevant for the dual-router design.

## Procedure 7 Configure access-layer HSRP

If you are using a dual-router design, complete this procedure.

You need to configure HSRP in order to enable the use of a virtual IP (VIP) address as a default gateway that is shared between two routers. The HSRP active router is the MPLS CE router connected to the primary MPLS carrier, and the HSRP standby router is the router connected to the secondary MPLS carrier or backup link.

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 11 - WAN remote-site HSRP parameters (dual-router design)*

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

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

The dual-router access-layer design requires a modification for resilient multicast. The PIM designated router (DR) should be on the HSRP active router. The DR is normally elected based on the highest IP address, and 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.

```
interface [type][number].[sub-interface number]
 ip address [LAN network 1 address] [LAN network 1 netmask]
 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
```

Step 2: Repeat this procedure for all data or voice subinterfaces.

### Example: Layer 2 link

```
interface GigabitEthernet0/2
 no ip address
 no shutdown
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.12.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.12.1
 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 10.5.13.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.13.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

## Procedure 8 Configure the transit network

If you are using a dual-router design, complete this procedure.

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

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

**Step 1:** On the primary MPLS CE router, configure the transit network 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**

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

**Step 2:** On the access-layer switch, add the transit network VLAN.

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

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

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

## Procedure 9 Configure EIGRP (LAN side)

If you are using a dual-router design, complete this procedure.

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:** On the router, configure the EIGRP LAN process facing the access layer.

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

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

```
 exit-af-interface
 af-interface [Transit link 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. Neighbor authentication enables the secure establishment of peering adjacencies and exchange route tables over the DMVPN tunnel interface.

```
key chain LAN-KEY
 key 1
  key-string cisco
!
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface [interface type] [number]
   authentication mode md5
   authentication key-chain LAN-KEY
   no passive-interface
  exit-af-interface
 exit-address-family
```

Step 3: On the router, redistribute BGP into the EIGRP LAN process.

A default metric redistributes the BGP routes into EIGRP. 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
```

**Tech Tip**

Command Reference:

**default-metric** *bandwidth delay reliability loading mtu*

*bandwidth*–Minimum bandwidth of the route in kilobytes per second

*delay*–Route delay in tens of microseconds.

**Example**

```
router eigrp 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 10.4.0.0 0.1.255.255
 network 10.255.0.0 0.0.255.255
 eigrp router-id 10.255.251.206
 exit-address-family
```

## Procedure 10 Configure BGP

If you are using a dual-router design, complete this procedure.

**Step 1:** On both remote-site MPLS CE routers, configure iBGP and enable the next-hop-self configuration option.

The dual-carrier MPLS design requires that a BGP link is configured between the CE routers. Because the CE routers are using the same ASN, this configuration is considered an *internal BGP* (iBGP) connection. This design uses iBGP peering using the transit network, which requires the next-hop-self-configuration option.

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

```
router bgp 65511
 neighbor [iBGP neighbor Transit Net IP] remote-as 65511
 neighbor [iBGP neighbor Transit Net IP] next-hop-self
```

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

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

Each router will apply this outbound to the neighbor for its respective MPLS carrier.

```
router bgp 65511
  neighbor [IP address of PE] route-map NO-TRANSIT-AS out
ip as-path access-list 10 permit ^$
!
route-map NO-TRANSIT-AS permit 10
 match as-path 10
```

**Tech Tip**

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

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

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

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

Apply a route-map inbound to the neighbor for the primary MPLS carrier only.

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

**Tech Tip**

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

**Step 4:** Add a loopback network for the secondary router.

```
router bgp 65511
 network [Secondary router loopback network] mask 255.255.255.255
```

## Procedure 11 Enable enhanced object tracking

If you are using a dual-router design, complete this procedure.

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

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

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

**Step 1:** Enable the IP SLA probe, and then send standard ICMP echo (ping) probes at 15-second intervals. Responses must be received before the timeout of 1000 ms expires. If you are using the MPLS PE router as the probe destination, the destination address is the same as the BGP neighbor address configured in Procedure 3.

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

**Step 2:** Configure EOT based on the IP SLA probe. The object being tracked is the reachability success or failure of the probe. If the probe is successful, the tracked object status is Up; if it fails, the tracked object status is Down.

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

**Step 3:** Link HSRP with the tracked object.

All data or voice subinterfaces should enable HSRP tracking.

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

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

### Example

```
interface GigabitEthernet 0/2.64
 standby 1 track 50 decrement 10
interface GigabitEthernet 0/2.69
 standby 1 track 50 decrement 10
!
track 50 ip sla 100 reachability
!
ip sla 100
 icmp-echo 192.168.3.10 source-interface GigabitEthernet0/0
 timeout 1000
```

```
 threshold 1000
 frequency 15
ip sla schedule 100 life forever start-time now
```

PROCESS

## Adding a Secondary MPLS Link on an Existing MPLS CE Router

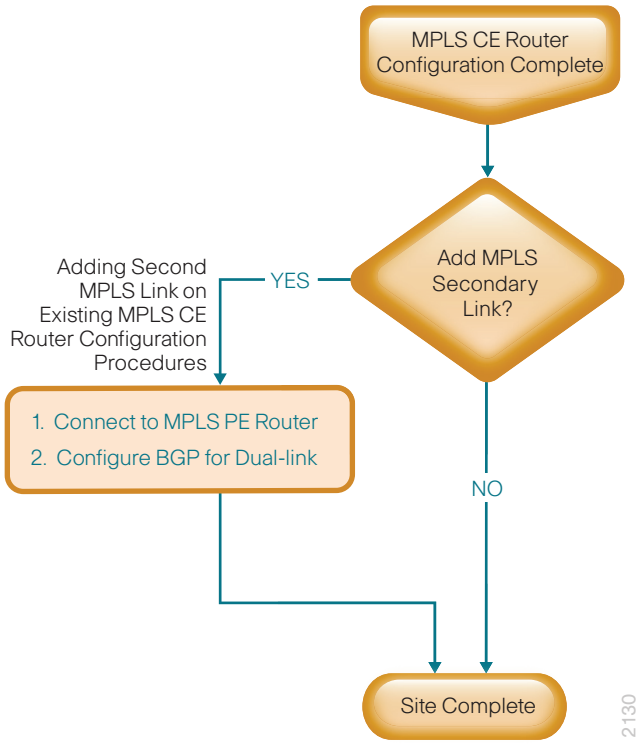
1. Connect to MPLS PE router
2. Configure BGP for dual-link design

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

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

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

*Figure 15 - Flowchart for adding an MPLS backup configuration*



## Procedure 1 Connect to MPLS PE router

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

**Step 1:** Assign an interface bandwidth value that corresponds to the actual interface speed.

If you are using a subrate service, use the policed rate from the carrier.

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

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

**Tech Tip**

Command Reference:

**bandwidth** *kbps*

10 Mbps = 10,000 kbps

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

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

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

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

It is not recommended that you use the Cisco Discovery Protocol on external interfaces.

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

### Example

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

## Procedure 2 Configure BGP for dual-link design

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

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

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

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

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

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

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

```
router bgp 65511
 neighbor [IP address of PE] route-map NO-TRANSIT-AS out
 neighbor [IP address of PE 2] route-map NO-TRANSIT-AS out
ip as-path access-list 10 permit ^$
!
route-map NO-TRANSIT-AS permit 10
 match as-path 10
```

**Tech Tip**

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

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

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

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

Step 4: Apply a route map inbound to the neighbor for the primary MPLS carrier only.

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

**Tech Tip**

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

### Example

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

PROCESS

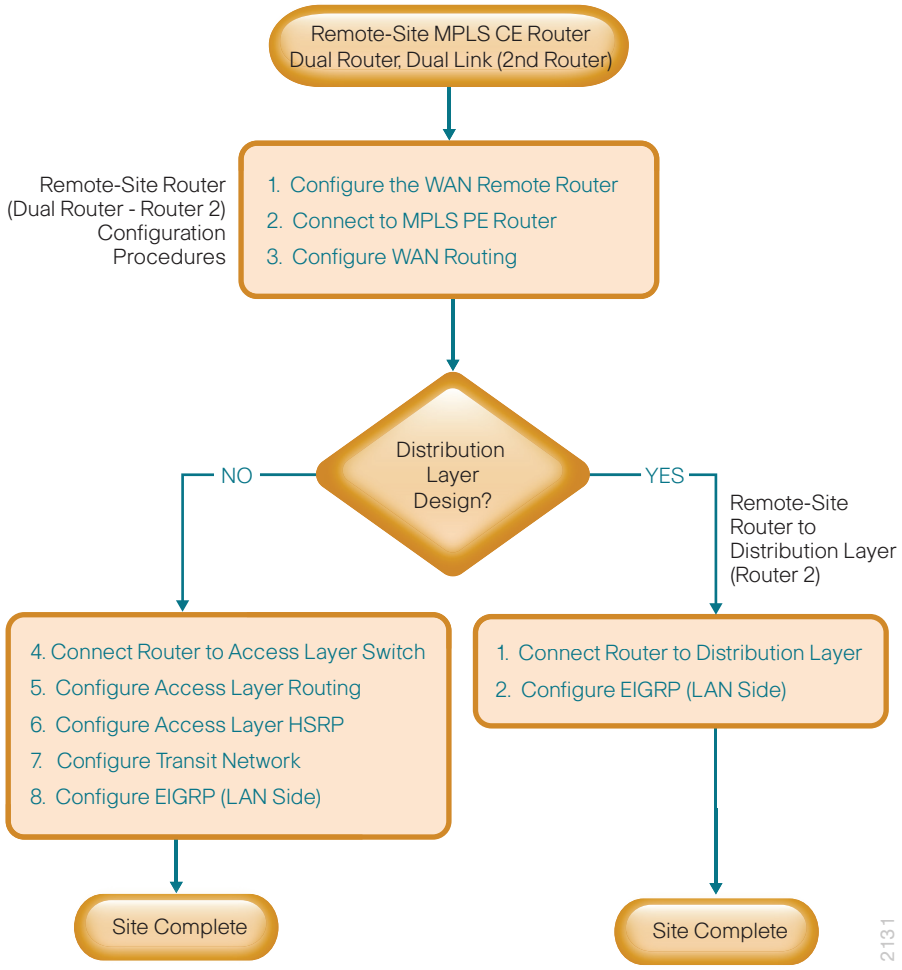
## Configuring the Secondary Remote-Site Router

1. Configure the WAN remote router
2. Connect to the MPLS PE router
3. Configure WAN routing
4. Connect router to access-layer switch
5. Configure access-layer routing
6. Configure access-layer HSRP
7. Configure the transit network
8. Configure EIGRP (LAN side)

If you are using a dual-router, dual-link design, complete this procedure in order to configure the secondary router in the MPLS WAN remote site.

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

*Figure 16 - Remote-site MPLS CE router 2 configuration flowchart*



## Procedure 1 Configure the WAN remote router

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

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

```
hostname [hostname]
```

**Step 2:** Configure local login and password.

The local login account and password provides basic access authentication to a router, and this access 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:** (Optional) Configure centralized user authentication.

As networks scale in the number of devices to maintain it poses an operational burden to maintain local user accounts on every device. A centralized authentication, authorization, and accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

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:** Configure device management protocols.

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

Secure management of the network device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy, and the unsecure protocols, Telnet and HTTP, are turned off. SCP is enabled, which allows the use of code upgrades using Prime Infrastructure via the SSH-based SCP protocol.

Specify the transport preferred none on vty lines 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, you can 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 will be 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 login 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 organizations network.

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

```
ntp server 10.4.48.17
ntp update-calendar
!
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 router 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 a unique network range that is not part of any other internal network summary range.

```
interface Loopback 0
  ip address [ip address] 255.255.255.255
  ip pim sparse-mode
```

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

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

**Step 10:** Configure IP Multicast routing.

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

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

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

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

```
ip multicast-routing
```

**Step 11:** 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 12:** Enable sparse mode multicast operation for all Layer 3 interfaces in the network.

```
ip pim sparse-mode
```

## Procedure 2 Connect to the MPLS PE router

**Step 1:** Assign an interface bandwidth value that corresponds to the actual interface speed.

If you are using a subrate service, use the policed rate from the carrier.

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

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

**Tech Tip**

Command Reference:

**bandwidth** *kbps*

10 Mbps = 10,000 kbps

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

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

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

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

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

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

### Example

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

## Procedure 3 Configure WAN routing

**Step 1:** Enable BGP.

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

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

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

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

**Step 2:** Configure eBGP.

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

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

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

The remote-site routers have in-band management configured via the loopback interface. To ensure reachability of the loopback interfaces in a dual-router design, you must list the loopbacks of both the primary and secondary routers as BGP networks.

**Tech Tip**

On the primary MPLS CE router, you must add a network statement for the loopback address of the secondary MPLS CE router. This is required for loopback resiliency.

```
router bgp 65511
 network [PE-CE link network] mask [PE-CE link netmask]
 network [Primary router loopback network] mask 255.255.255.255
 network [Secondary router loopback network] mask 255.255.255.255
 network [DATA network] mask [netmask]
 network [VOICE network] mask [netmask]
 aggregate-address [summary IP address] [summary netmask] summary-only
 neighbor [IP address of PE] remote-as [carrier ASN]
```

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

The dual-carrier MPLS design requires that a BGP link is configured between the CE routers. Because the CE routers are using the same ASN, this configuration is considered an internal BGP (iBGP) connection.

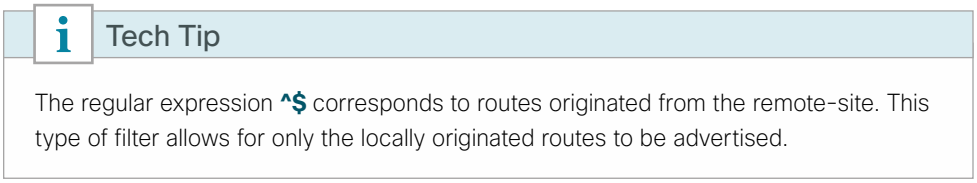
Note, the iBGP session will not be established until you complete the transit network and EIGRP (LAN side) steps.

```
router bgp 65511
 neighbor [iBGP neighbor Transit Net IP] remote-as 65511
 neighbor [iBGP neighbor Transit Net IP] next-hop-self
```

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

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

```
router bgp 65511
  neighbor [IP address of PE 2] route-map NO-TRANSIT-AS out
ip as-path access-list 10 permit ^$
!
route-map NO-TRANSIT-AS permit 10
 match as-path 10
```




### Example: MPLS CE Router (secondary)

```
router bgp 65511
 no synchronization
 bgp router-id 10.255.252.206
 bgp log-neighbor-changes
 network 192.168.4.8 mask 255.255.255.252
 network 10.255.251.206 mask 255.255.255.255
 network 10.255.252.206 mask 255.255.255.255
 network 10.5.12.0 mask 255.255.255.0
 network 10.5.13.0 mask 255.255.255.0
 aggregate-address 10.5.8.0 255.255.248.0 summary-only
 neighbor 10.5.8.1 remote-as 65511
 neighbor 10.5.8.1 next-hop-self
 neighbor 192.168.4.10 remote-as 65402
 neighbor 192.168.4.10 route-map NO-TRANSIT-AS out
 no auto-summary
!
ip as-path access-list 10 permit ^$
```

```
!
route-map NO-TRANSIT-AS permit 10
 match as-path 10
```

## Procedure 4 Connect router to access-layer switch

**Reader Tip**

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

If you are using a remote-site distribution layer, then skip to the "Deploying a WAN Remote-Site Distribution Layer" chapter of this guide.

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

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 a port-channel interface on the router.

```
interface Port-channel2
 description EtherChannel link to RS206-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. Not all router platforms can support LACP to negotiate with the switch, so you configure EtherChannel statically.

```
interface GigabitEthernet0/1
 description RS206-A2960X Gig1/0/23
!
interface GigabitEthernet0/2
 description RS206-A2960X Gig2/0/23
!
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 2
  no shutdown
```

**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, or in the case of the Cisco Catalyst 4507R+E distribution layer, to separate redundant modules for additional resiliency.

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.

Configure two or more physical interfaces to be members of the EtherChannel. It is recommended that they are added in multiples of two. Also, apply the egress QoS macro that was defined in the platform configuration procedure in order to ensure traffic is prioritized appropriately.

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

```
interface GigabitEthernet1/0/23
 description Link to RS206-3925-2 Gig0/1
interface GigabitEthernet2/0/23
 description Link to RS206-3925-2 Gig0/2
!
interface range GigabitEthernet1/0/23, GigabitEthernet2/0/23
 switchport
 macro apply EgressQoS
 channel-group 2 mode on
 logging event link-status
 logging event trunk-status
 logging event bundle-status
```

**Step 4:** Configure EtherChannel trunk on the access-layer switch.

Use an 802.1Q trunk for the connections. This 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 Step 2. Set DHCP Snooping and Address Resolution Protocol (ARP) inspection to trust.

```
interface Port-channel2
 description EtherChannel link to RS206-3925-2
 switchport trunk allowed vlan 64,69,99
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
 ip dhcp snooping trust
 no shutdown
```

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 RS206-A2960X Gig1/0/23
 no ip address
 no shutdown
```

**Step 2:** Configure the trunk on the access-layer switch.

Use an 802.1Q trunk for the connection. This 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, and then set DHCP Snooping and Address Resolution Protocol (ARP) inspection to trust.

```
interface  GigabitEthernet1/0/23
 description Link to RS206-3925-2 Gig0/2
 switchport trunk allowed vlan 64,69,99
 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
```

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

## Procedure 5 Configure access-layer routing

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

**Step 1:** Create subinterfaces and assign VLAN tags.

After the physical interface or port-channel has been enabled, you can map the appropriate data or voice subinterfaces to the VLANs on the LAN switch. The subinterface number does not need to equate to the 802.1Q tag, but making them the same simplifies the overall configuration.

```
interface [type][number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
```

**Step 2:** Repeat the subinterface portion of the previous step for all data or voice VLANs.

**Step 3:** Configure IP settings for each subinterface.

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

When using a centralized DHCP server, routers with LAN interfaces connected to a LAN using DHCP for end-station IP addressing must use an IP helper.

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

```
interface  [type][number].[sub-interface number]
 description [usage]
 ip helper-address 10.4.48.10
 ip pim sparse-mode
```

### Example: Layer 2 EtherChannel

```
interface Port-channel2
 no ip address
 no shutdown
 !
 hold-queue 150 in
!
interface Port-channel2.64
 description Data
 encapsulation dot1Q 64
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface Port-channel2.69
 description Voice
 encapsulation dot1Q 69
 ip helper-address 10.4.48.10
 ip pim sparse-mode
```

### Example: Layer 2 Trunk

```
interface GigabitEthernet0/2
 no ip address
 no shutdown
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface GigabitEthernet0/2.69
 description Voice
 encapsulation dot1Q 69
 ip helper-address 10.4.48.10
 ip pim sparse-mode
```

## Procedure 6 Configure access-layer HSRP

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

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 12 - WAN remote-site HSRP parameters (dual-router design)*

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

The dual-router access-layer design requires a modification for resilient multicast. The PIM designated router (DR) should be on the HSRP active router. The DR is normally elected based on the highest IP address, and 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.

```
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
```

Step 2: Repeat this procedure for all data or voice subinterfaces.

**Example: MPLS CE 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 10.5.12.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.12.1
 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 10.5.13.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.13.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

**Example: MPLS CE 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 10.5.12.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.12.1
```

```
 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 10.5.13.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.13.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

## Procedure 7 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: On the secondary MPLS CE router, 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**

```
interface GigabitEthernet0/2.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.8.2 255.255.255.252
 ip pim sparse-mode
```

## Procedure 8 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:** On the router, configure the EIGRP LAN process facing the access layer.

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

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
  af-interface [Transit link 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. Neighbor authentication enables the secure establishment of peering adjacencies and exchange route tables over the DMVPN tunnel interface.

```
key chain LAN-KEY
 key 1
  key-string cisco
!
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface [interface type] [number]
   authentication mode md5
   authentication key-chain LAN-KEY
   no passive-interface
  exit-af-interface
 exit-address-family
```

**Step 3:** On the router, redistribute BGP into the EIGRP LAN process.

A default metric redistributes the BGP routes into EIGRP. 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
```

**Tech Tip**

Command Reference:

**default-metric** *bandwidth delay reliability loading mtu*

*bandwidth*–Minimum bandwidth of the route in kilobytes per second

*delay*–Route delay in tens of microseconds.

### Example

```
router eigrp 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 10.4.0.0 0.1.255.255
 eigrp router-id 10.255.252.206
 exit-address-family
```

# Deploying a WAN Remote-Site Distribution Layer

## Deployment Details

PROCESS

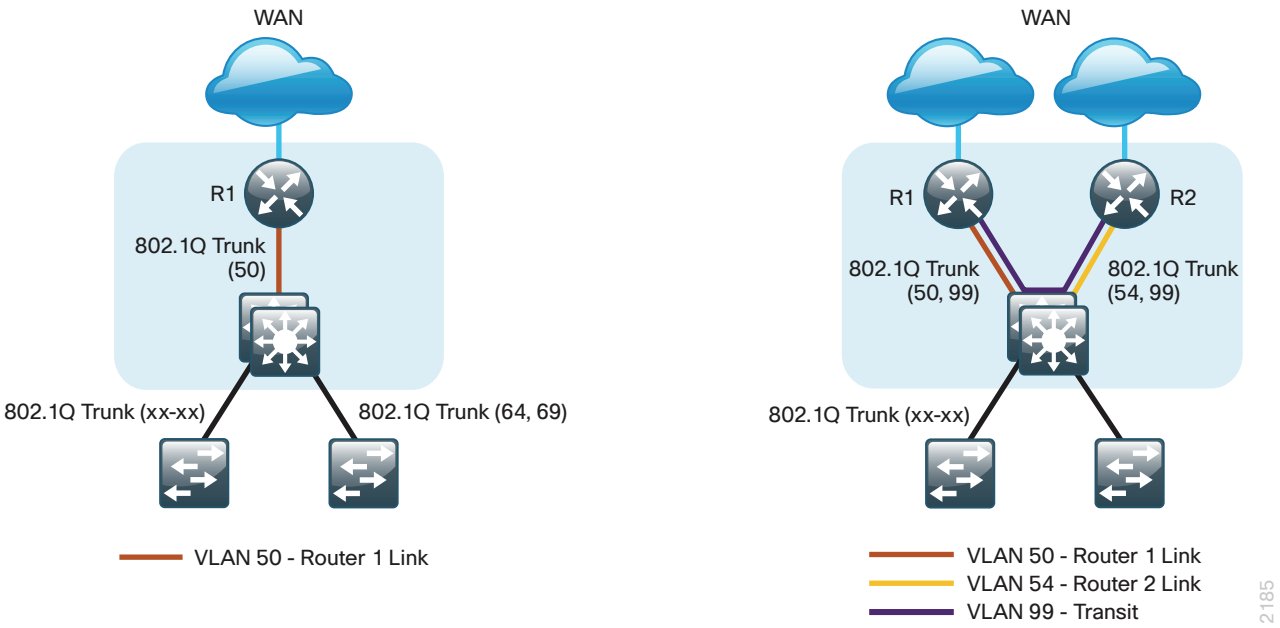
### Connecting the Single or Primary Remote-Site Router to the Distribution Layer

1. Connect router to distribution layer
2. Configure EIGRP (LAN side)
3. Configure the transit network
4. Configure BGP

If you are configuring an MPLS WAN remote-site that uses a single-router, single link design or a dual-router, dual-link design, complete this process. This process includes all required procedures in order to connect either the single-router in a single-link design or the primary router in a dual-link design to a LAN distribution layer.

Both distribution-layer remote-site options are shown in the following figure.

*Figure 17 - WAN remote site—Connection to distribution layer*



## Procedure 1 Connect router to distribution layer

### Reader Tip

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

Layer 2 EtherChannels are used to interconnect the CE router to the distribution layer in the most resilient method possible. This connection allows for multiple VLANs to be included on the EtherChannel as necessary.

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

```
interface Port-channel1
 description EtherChannel link to RS200-D4500X-VSS
 no shutdown
```

**Step 2:** Configure the port channel subinterfaces and assign IP addresses.

After you have enabled the interface, map the appropriate subinterfaces to the VLANs on the distribution-layer switch. The subinterface number does not need to equate to the 802.1Q tag, but making them the same simplifies the overall configuration.

The subinterface configured on the router corresponds to a VLAN interface on the distribution-layer switch. Traffic is routed between the devices with the VLAN acting as a point-to-point link.

```
interface Port-channel1.50
 description R1 routed link to distribution layer
 encapsulation dot1Q 50
 ip address 10.5.0.1 255.255.255.252
 ip pim sparse-mode
```

**Step 3:** On the router, configure EtherChannel member interfaces.

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

```
interface GigabitEthernet0/1
 description RS200-D4500X-VSS Ten1/1/1
!
interface GigabitEthernet0/2
 description RS200-D4500X-VSS  Ten2/1/1
!
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 1
  no shutdown
```

**Step 4:** On the distribution-layer switch, configure the VLAN.

```
vlan 50
 name R1-link
```

**Step 5:** On the distribution-layer switch, configure Layer 3.

Configure a VLAN interface, also known as a *switch virtual interface* (SVI), for the new VLAN added. The SVI is used for point-to-point IP routing between the distribution layer and the WAN router.

```
interface Vlan50
 ip address 10.5.0.2 255.255.255.252
 ip pim sparse-mode
 no shutdown
```

**Step 6:** On the distribution-layer switch, configure EtherChannel member interfaces.

Connect the router EtherChannel uplinks to separate switches in the distribution layer.

If you are using a Cisco Catalyst 4507R+E chassis in the distribution layer, connect the uplinks to separate redundant modules. This provides additional resiliency.

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 member interfaces and do not require manual replication.

Configure two or more physical interfaces to be members of the EtherChannel. It is recommended that they are added in multiples of two. Also, apply the egress QoS macro that was defined in the platform configuration procedure to ensure traffic is prioritized appropriately.

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

```
interface GigabitEthernet1/0/1
 description Link to RS200-3925-1 Gig0/1
interface GigabitEthernet2/0/1
 description Link to RS200-3925-1 Gig0/2
!
interface range GigabitEthernet1/0/1, GigabitEthernet2/0/1
 switchport
 channel-group 1 mode on
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 load-interval 30
 macro apply EgressQoS
```

**Step 7:** On the distribution-layer switch, configure an EtherChannel trunk.

Use an 802.1Q trunk for the connection. This allows the router to provide the Layer 3 services to all the VLANs defined on the distribution-layer switch. Prune the VLANs allowed on the trunk to only the VLANs that are active on the distribution-layer switch. When using EtherChannel, the interface type is port-channel, and the number must match the channel group configured in Step 3. .

```
interface Port-channel1
 description EtherChannel link to RS200-3925-1
 switchport trunk allowed vlan 50
 switchport mode trunk
 spanning-tree portfast trunk
 no shutdown
```

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

## Procedure 2 Configure EIGRP (LAN side)

You must configure a routing protocol between the router and distribution layer.

**Step 1:** On the router, configure the EIGRP LAN process facing the distribution layer.

In this design, all distribution-layer-facing subinterfaces and the loopback must be EIGRP interfaces. All other interfaces should remain passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
  af-interface [Routed link 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. Neighbor authentication enables the secure establishment of peering adjacencies and exchange route tables over the DMVPN tunnel interface.

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

```
  no passive-interface
 exit-af-interface
exit-address-family
```

**Step 3:** On the router, redistribute BGP into the EIGRP LAN process.

A default metric redistributes the BGP routes into EIGRP. 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
```

On the distribution-layer switch VLAN interface, enable EIGRP.

EIGRP is already configured on the distribution-layer switch. The VLAN interface that connects to the router must be configured for EIGRP neighbor authentication and as a non-passive EIGRP interface.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface Vlan50
   authentication mode md5
   authentication key-chain LAN-KEY
   no passive-interface
  exit-af-interface
exit-address-family
```

**Step 4:** If it is necessary to define additional IP networks on the distribution-layer switch, enter the following configuration. If the additional IP networks are outside the existing remote-site summary range, you will need to add an EIGRP summary on the distribution switch.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface Vlan50
   summary-address [Summary address]
  exit-af-interface
 exit-address-family
```

**Step 5:** On the router, advertise the new IP network in BGP.

**Step 6:** Configure a BGP network statement with a mask matching the distribution-layer EIGRP summary route.

```
router bgp 65511
 network [network and mask]
```

### Example (router configuration)

```
router bgp 65511
 network 10.5.24.0 mask 255.255.248.0
!
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
  af-interface Port-channel1.50
   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 10.255.251.200
exit-address-family
```

### Example (distribution switch configuration)

```
interface Vlan153
 description Server Room RS-200
 ip address 10.5.26.1 255.255.255.128
!
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
  af-interface Vlan50
   summary-address 10.5.24.0 255.255.248.0
   authentication mode md5
   authentication key-chain LAN-KEY
   no passive-interface
  exit-af-interface
  topology base
  exit-af-topology
  network 10.4.0.0 0.1.255.255
  eigrp router-id 10.5.7.254
  eigrp stub connected summary redistributed
  nsf
 exit-address-family
```

## Procedure 3 Configure the transit network

If you are using a dual-router design, complete this procedure.

Configure the transit network between the two routers. You use this network for router-router communication and to avoid hairpinning. The transit network should use an additional subinterface on the EtherChannel interface that is already used to connect to the distribution layer.

The transit network must be a non-passive EIGRP interface.

There are no end stations connected to this network, so HSRP and DHCP are not required. The transit network uses Layer 2 pass-through on the distribution-layer switch, so no SVI is required.

**Step 1:** On the router, configure the transit net interface.

```
interface Port-channel1.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.0.9 255.255.255.252
 ip pim sparse-mode
```

**Step 2:** On the router, enable EIGRP on the transit network interface.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface Port-channel1.99
   authentication mode md5
   authentication key-chain LAN-KEY
   no passive-interface
  exit-af-interface
exit-address-family
```

**Step 3:** On the distribution-layer switch, configure the transit network VLAN.

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

**Step 4:** Add the transit network VLAN to the existing distribution-layer switch EtherChannel trunk.

```
interface Port-channel1
 switchport trunk allowed vlan add 99
```

## Procedure 4 Configure BGP

If you are using a dual-router design, complete this procedure.

**Step 1:** Configure iBGP between the remote-site MPLS CE routers.

The dual-carrier MPLS design requires that a BGP link is configured between the CE routers. Because the CE routers are using the same ASN, this configuration is considered an internal BGP (iBGP) connection. This design uses iBGP peering and requires the next-hop-self-configuration option.

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

```
router bgp 65511
 neighbor [iBGP neighbor Transit Net IP] remote-as 65511
 neighbor [iBGP neighbor Transit Net IP] next-hop-self
```

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

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

```
router bgp 65511
  neighbor [IP address of PE] route-map NO-TRANSIT-AS out
ip as-path access-list 10 permit ^$
!
route-map NO-TRANSIT-AS permit 10
 match as-path 10
```

**Tech Tip**

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

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

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

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

**Step 4:** Apply a route-map inbound to the neighbor for the primary MPLS carrier only.

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

**Tech Tip**

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

**Step 5:** Add a loopback network for the secondary router.

```
router bgp 65511
 network [Secondary router loopback network] mask 255.255.255.255
```

PROCESS

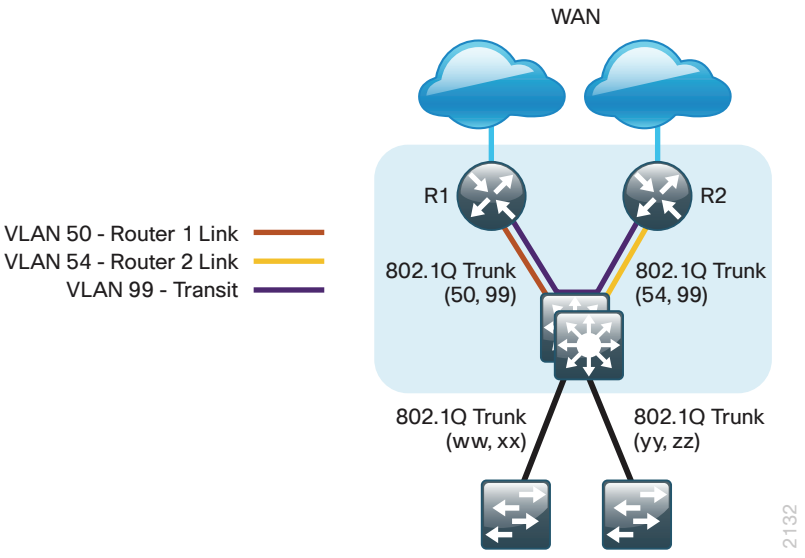
## Connecting the Secondary Remote-Site Router to the Distribution Layer

1. Connect router to distribution layer
2. Configure EIGRP (LAN side)

If you are using dual-carrier design for the MPLS WAN remote site, complete this process. This process connects the distribution layer to the second router of the dual-router, dual-link design. This design uses a separate routed link from the second router of the dual-router scenario to the LAN distribution-layer switch.

The dual-router, distribution layer-remote-site design is shown in the following figure.

*Figure 18 - WAN remote site–Connection to distribution layer*



## Procedure 1 Connect router to distribution layer

**Reader Tip**

Please refer to the Campus Wired LAN Technology Design Guide for complete distribution layer configuration details. This guide only includes the additional steps to complete the distribution layer configuration.

Layer 2 EtherChannels are used to interconnect the CE router to the distribution layer in the most resilient method possible. This connection allows for multiple VLANs to be included on the EtherChannel as necessary.

**Step 1:** On the secondary router, configure a port-channel interface.

```
interface Port-channel2
 description EtherChannel link to D4500X-VSS
 no shutdown
```

**Step 2:** Configure the port channel subinterfaces and assign IP address.

After you have enabled the interface, map the appropriate subinterfaces to the VLANs on the distribution-layer switch. The subinterface number does not need to equate to the 802.1Q tag, but making them the same simplifies the overall configuration.

The subinterface configured on the router corresponds to a VLAN interface on the distribution-layer switch. Traffic is routed between the devices with the VLAN acting as a point-to-point link.

```
interface Port-channel2.54
 description R2 routed link to distribution layer
 encapsulation dot1Q 54
 ip address 10.5.0.5 255.255.255.252
 ip pim sparse-mode
```

**Step 3:** On the router, configure the transit network interface.

```
interface Port-channel2.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.0.10 255.255.255.252
 ip pim sparse-mode
```

**Step 4:** On the router, configure the EtherChannel member interfaces.

Configure the physical interfaces to tie to the logical port-channel using by the **channel-group** command. The number for the port-channel and channel-group must match. Not all router platforms can support LACP to negotiate with the switch, so you configure EtherChannel statically.

```
interface GigabitEthernet0/1
 description RS200-D4500X-VSS Ten1/1/2
!
interface GigabitEthernet0/2
 description RS200-D4500X-VSS Ten2/1/2
!
```

```
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 2
  no shutdown
```

Step 5: On the distribution-layer switch, configure a VLAN.

```
vlan 54
 name R2-link
```

Step 6: On the distribution-layer switch, configure Layer 3.

Configure a VLAN interface, also known as a *switch virtual interface* (SVI), for the new VLAN added. The SVI is used for point-to-point IP routing between the distribution layer and the WAN router.

```
interface Vlan54
 ip address 10.5.0.6 255.255.255.252
 ip pim sparse-mode
 no shutdown
```

Step 7: On the distribution-layer switch, configure EtherChannel member interfaces.

Connect the router EtherChannel uplinks to separate switches in the distribution layer switches or stack, and in the case of the Cisco Catalyst 4507R+E distribution layer, to separate redundant modules for additional resiliency.

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 member interfaces and do not require manual replication.

Configure two or more physical interfaces to be members of the EtherChannel. It is recommended that they are added in multiples of two. Also, apply the egress QoS macro that was defined in the platform configuration procedure to ensure traffic is prioritized appropriately.

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

```
interface GigabitEthernet1/0/2
 description Link to RS200-3925-2 Gig0/1
interface GigabitEthernet2/0/2
 description Link to RS200-3925-2 Gig0/2
!
interface range GigabitEthernet1/0/2, GigabitEthernet2/0/2
 switchport
 channel-group 2 mode on
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 load-interval 30
 macro apply EgressQoS
```

**Step 8:** On the distribution-layer switch, configure an EtherChannel trunk.

Use an 802.1Q trunk for the connection. This allows the router to provide the Layer 3 services to all the VLANs defined on the distribution-layer switch. Prune the VLANs allowed on the trunk to only the VLANs that are active on the distribution-layer switch. When using EtherChannel, the interface type is port-channel, and the number must match the channel group configured in Step 4.

```
interface Port-channel2
 description EtherChannel link to RS200-3925-2
 switchport trunk allowed vlan 54,99
 switchport mode trunk
 spanning-tree portfast trunk
 no shutdown
```

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

## Procedure 2 Configure EIGRP (LAN side)

You must configure a routing protocol between the router and distribution layer.

**Step 1:** On the router, configure the EIGRP LAN process facing the distribution layer.

In this design, all distribution-layer-facing subinterfaces and the loopback must be EIGRP interfaces. All other interfaces should remain passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
  af-interface [Routed link interface]
   no passive-interface
  exit-af-interface
  af-interface [Transit link 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. Neighbor authentication enables the secure establishment of peering adjacencies and exchange route tables over the DMVPN tunnel interface.

```
key chain LAN-KEY
 key 1
  key-string cisco
!
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface [interface type] [number]
   authentication mode md5
   authentication key-chain LAN-KEY
   no passive-interface
  exit-af-interface
 exit-address-family
```

**Step 3:** On the router, redistribute BGP into the EIGRP LAN process.

A default metric redistributes the BGP routes into EIGRP. 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
```

**Step 4:** On the distribution-layer switch VLAN interface, enable EIGRP.

EIGRP is already configured on the distribution-layer switch. The VLAN interface that connects to the router must be configured as a non-passive EIGRP interface.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface Vlan54
   authentication mode md5
   authentication key-chain LAN-KEY
   no passive-interface
  exit-af-interface
exit-address-family
```

**Step 5:** If it is necessary to define additional IP networks on the distribution-layer switch, enter the following configuration. If the additional IP networks are outside the existing remote-site summary range, you will need to add an EIGRP summary on the distribution switch.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface Vlan54
   summary-address [New Summary address]
  exit-af-interface
 exit-address-family
```

Step 6: On the router, advertise the new IP network in BGP.

Configure a BGP network statement with a mask matching the distribution-layer EIGRP summary.

```
router bgp 65511
 network [network and mask]
```

### Example (router configuration)

```
router bgp 65511
 network 10.5.24.0 mask 255.255.248.0
!
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
  af-interface Port-channel1.54
   authentication mode md5
   authentication key-chain LAN-KEY
   no passive-interface
  exit-af-interface
af-interface Port-channel1.99
   authentication mode md5
   authentication key-chain LAN-KEY
   no passive-interface
  exit-af-interface
  topology base
   default-metric 500000 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 10.255.252.200
 exit-address-family
```

### Example (Distribution switch configuration)

```
interface Vlan54
 ip address 10.5.0.6 255.255.255.252
 ip pim sparse-mode
!
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
  af-interface Vlan50
   summary-address 10.5.24.0 255.255.248.0
   authentication mode md5
   authentication key-chain LAN-KEY
```

```
 no passive-interface
exit-af-interface
af-interface Vlan54
 summary-address 10.5.24.0 255.255.248.0
 authentication mode md5
 authentication key-chain LAN-KEY
 no passive-interface
exit-af-interface
topology base
exit-af-topology
network 10.4.0.0 0.1.255.255
eigrp router-id 10.5.7.254
eigrp stub connected summary redistributed
nsf
exit-address-family
```

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.

# Deployment Details

PROCESS

## Configuring QoS

1. Create the QoS Maps to Classify Traffic
2. Create the policy map that marks BGP traffic
3. Define a policy map that defines the queuing policy
4. Configure shaping and queuing policy
5. Apply the shaping and queuing policy to a physical interface

### Procedure 1 Create the QoS Maps to Classify Traffic

The **class-map** command defines a traffic class and identifies traffic to associate with the class name. These class names are used when configuring policy maps that define actions you wish to take against the traffic type. The **class-map** command sets the match logic. In this case, the **match-any** keyword indicates that the maps 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**.

Use the following steps to configure the required WAN class maps and matching criteria.

**Step 1:** For each of the six WAN classes of service listed in Table 13, create a class map for DSCP matching.

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 (such as video conferencing) | cs4, af41 | 23 (PQ) | – |
| CRITICAL-DATA | Highly interactive (such as Telnet, Citrix, and Oracle thin clients) | af31, cs3 | 15 | DSCP-based |
| DATA | Data | af21 | 19 | DSCP-based |
| SCAVENGER | Scavenger | af11, cs1 | 5 | – |
| NETWORK-CRITICAL | Routing protocols; operations, administration and maintenance (OAM) traffic. | cs6, cs2 | 3 | – |
| default | Best effort | other | 25 | random |

Step 2: If you are using a WAN-aggregation MPLS CE router or a WAN remote-site MPLS CE router that is using BGP, create a class map for BGP protocol matching.

BGP traffic is not explicitly tagged with a DSCP value. Use NBAR to match BGP by protocol.

```
class-map match-any [class-map name]
 match ip protocol [protocol name]
```

**Example**

```
class-map match-any VOICE
 match dscp ef
!
class-map match-any INTERACTIVE-VIDEO
 match dscp cs4 af41
!
class-map match-any CRITICAL-DATA
 match dscp af31 cs3
!
class-map match-any DATA
 match dscp af21
!
class-map match-any SCAVENGER
 match dscp af11 cs1
!
class-map match-any NETWORK-CRITICAL
 match dscp cs6 cs2
!
class-map match-any BGP-ROUTING
 match protocol bgp
```

**Tech Tip**

You do not need to configure a best-effort class. This is implicitly included within class-default as shown in Procedure 4.

## Procedure 2 Create the policy map that marks BGP traffic

If you are using a WAN-aggregation MPLS CE router or a WAN remote-site MPLS CE router that uses BGP, complete this procedure.

To ensure proper treatment of BGP routing traffic in the WAN, you must assign a DSCP value of cs6. Although the class map you created in the previous step matches all BGP traffic to the class named BGP, you must configure a policy map to assign the required DSCP value to all BGP traffic.

**Step 1:** Create a policy map, and then assign it a DSCP value of cs6.

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

## Procedure 3 Define a policy map that defines the queuing policy

This procedure applies to all WAN routers.

The WAN policy map references the class names you created in the previous procedures and defines the queuing behavior along with the maximum guaranteed bandwidth allocated to each class. This specification is accomplished with the use of a policy map. Then, each class within the policy map invokes an egress queue, assigns a percentage of bandwidth, and associates a specific traffic class to that queue. One additional default class defines the minimum allowed bandwidth available for best-effort traffic.

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 in order 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:** (Optional) Assign the maximum guaranteed bandwidth for the class.

```
bandwidth percent [percentage]
```

**Step 4:** (Optional) Define the priority queue for the class.

```
priority percent [percentage]
```

Step 5: (Optional) Apply the child service policy.

This is an optional step only for the NETWORK-CRITICAL class of service with the MARK-BGP child service policy.

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

Step 6: (Optional) Define the congestion mechanism.

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

Step 7: Repeat Step 2 through Step 6 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
  service-policy MARK-BGP
 class class-default
  bandwidth percent 25
  random-detect
```

Tech Tip

Although these bandwidth assignments represent a good baseline, it is important to consider your actual traffic requirements per class and adjust the bandwidth settings accordingly.

## Procedure 4 Configure shaping and queuing 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 (bps)]
```

**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 the shaping and queuing policy to a physical interface

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

This procedure applies to all WAN routers. You can repeat this procedure multiple times to support devices that have multiple WAN connections attached to different interfaces.

Step 1: Select the WAN interface.

```
interface [interface type] [number]
```

Step 2: Apply the WAN QoS policy 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
```

# Appendix A: Product List

## WAN Aggregation

| Functional Area | Product Description | Part Numbers | Software |
|---|---|---|---|
| WAN-aggregation Router | Aggregation Services 1002X Router | ASR1002X-5G-VPNK9 | IOS-XE 15.4(2)S Advanced Enterprise feature set |
| | Aggregation Services 1002 Router | ASR1002-5G-VPN/K9 | |
| | Aggregation Services 1001 Router | ASR1001-2.5G-VPNK9 | |
| | Cisco ISR 4451-X Security Bundle w/SEC license PAK | ISR4451-X-SEC/K9 | IOS-XE 15.4(2)S securityk9 feature set |

## WAN Remote Site

| Functional Area | Product Description | Part Numbers | Software |
|---|---|---|---|
| Modular WAN Remote-site Router | Cisco ISR 4451 w/ 4GE,3NIM,2SM,8G FLASH, 4G DRAM, IP Base, SEC, AX license with: DATA, AVC, ISR-WAAS with 2500 connection RTU | ISR4451-X-AX/K9 | IOS-XE 15.4(2)S securityk9 feature set appxk9 feature set |
| | 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, AXlicenses 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 |
| Fixed WAN Remote-site Router | Cisco 891 Router | CISCO891W-AGN-A-K9 | 15.3(3)M3 securityk9 feature set datak9 feature set |
| | WAAS-Express/AVC/Advanced IP with upgrade up to 1GB DRAM for Cisco 800 Series Routers | FL-C800-APP | |

# LAN Access Layer

| Functional Area | Product Description | Part Numbers | Software |
|---|---|---|---|
| Modular Access Layer Switch | Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot | WS-C4507R+E | 3.3.1XO(15.1.1XO1) IP Base feature set |
| | Cisco Catalyst 4500E Supervisor Engine 8-E, Unified Access, 928Gbps | WS-X45-SUP8-E | |
| | Cisco Catalyst 4500E 12-port 10GbE SFP+ Fiber Module | WS-X4712-SFP+E | |
| | Cisco Catalyst 4500E 48-Port 802.3at PoE+ 10/100/1000 (RJ-45) | WS-X4748-RJ45V+E | |
| | Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot | WS-C4507R+E | 3.5.3E(15.2.1E3) IP Base feature set |
| | Cisco Catalyst 4500E Supervisor Engine 7L-E, 520Gbps | WS-X45-SUP7L-E | |
| | Cisco Catalyst 4500E 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports | WS-X4748-UPOE+E | |
| | Cisco Catalyst 4500E 48 Ethernet 10/100/1000 (RJ45) PoE+ ports | WS-X4648-RJ45V+E | |
| 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 |

# LAN Distribution Layer

| Functional Area | Product Description | Part Numbers | Software |
|---|---|---|---|
| Modular Distribution Layer Virtual Switch Pair | Cisco Catalyst 6800 Series 6807-XL 7-Slot Modular Chassis | C6807-XL | 15.1(2)SY3 IP Services feature set |
| | Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4 | VS-S2T-10G | |
| | Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4 | WS-X6904-40G-2T | |
| | Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module | CVR-CFP-4SFP10G | |
| | Cisco Catalyst 6500 CEF720 48 port 10/100/1000mb Ethernet | WS-X6748-GE-TX | |
| | Cisco Catalyst 6500 Distributed Forwarding Card 4 | WS-F6K-DFC4-A | |
| | Cisco Catalyst 6500 Series 6506-E 6-Slot Chassis | WS-C6506-E | |
| | Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4 | VS-S2T-10G | |
| | Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4 | WS-X6904-40G-2T | |
| | Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module | CVR-CFP-4SFP10G | |
| | Cisco Catalyst 6500 48-port GigE Mod (SFP) | WS-X6748-SFP | |
| | Cisco Catalyst 6500 Distributed Forwarding Card 4 | WS-F6K-DFC4-A | |
| | Cisco Catalyst 6500 24-port GigE Mod (SFP) | WS-X6724-SFP | |
| | Cisco Catalyst 6500 Distributed Forwarding Card 4 | WS-F6K-DFC4-A | |
| Extensible Fixed Distribution Layer Virtual Switch Pair | Cisco Catalyst 6800 Series 6880-X Extensible Fixed Aggregation Switch (Standard Tables) | C6880-X-LE | 15.1(2)SY3 IP Services feature set |
| | Cisco Catalyst 6800 Series 6880-X Multi Rate Port Card (Standard Tables) | C6880-X-LE-16P10G | |
| Modular Distribution Layer Virtual Switch Pair | Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot | WS-C4507R+E | 3.5.3E(15.2.1E3) Enterprise Services feature set |
| | Cisco Catalyst 4500E Supervisor Engine 7-E, 848Gbps | WS-X45-SUP7-E | |
| | Cisco Catalyst 4500E 12-port 10GbE SFP+ Fiber Module | WS-X4712-SFP+E | |
| | Cisco Catalyst 4500E 48-Port 802.3at PoE+ 10/100/1000 (RJ-45) | WS-X4748-RJ45V+E | |
| Fixed Distribution Layer Virtual Switch Pair | Cisco Catalyst 4500-X Series 32 Port 10GbE IP Base Front-to-Back Cooling | WS-C4500X-32SFP+ | 3.5.3E(15.2.1E3) Enterprise Services feature set |
| Stackable Distribution Layer Switch | Cisco Catalyst 3850 Series Stackable Switch with 12 SFP Ethernet | WS-C3850-12S | 3.3.3SE(15.0.1EZ3) IP Services feature set |
| | Cisco Catalyst 3850 Series 4 x 1GE Network Module | C3850-NM-4-1G | |
| | Cisco Catalyst 3850 Series 2 x 10GE Network Module | C3850-NM-2-10G | |
| | Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports | WS-C3750X-12S-E | 15.2(1)E3 IP Services feature set |
| | 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 | |

# 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/240-14b

# Appendix C: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- We added EIGRP Named mode configurations.
- We added EIGRP Authentication configurations.
- We added the **ip scp server enable** command.

## 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-0000245-1 08/14