Newer Design Guide Available

Cisco Smart Business Architecture has become part of the Cisco Validated Designs program.

For up-to-date guidance on the designs described in this guide, see http://cvddocs.com/fw/Aug13-235

For information about the Cisco Validated Design program, go to http://www.cisco.com/go/cvd

SBA

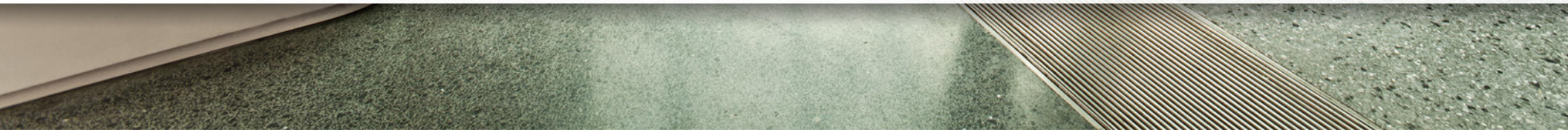
BORDERLESS NETWORKS

DEPLOYMENT GUIDE

Layer 2 WAN Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2013 Series



Preface

Who Should Read This Guide

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

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

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

Release Series

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

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

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

month year Series

For example, the series of guides that we released in February 2013 is the "February Series".

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

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

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

How to Read Commands

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

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

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

```
Router# enable
```

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

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

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

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

Comments and Questions

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

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

Table of Contents

What's In This SBA Guide

Cisco SBA Borderless Networks

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

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

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

Route to Success

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

About This Guide

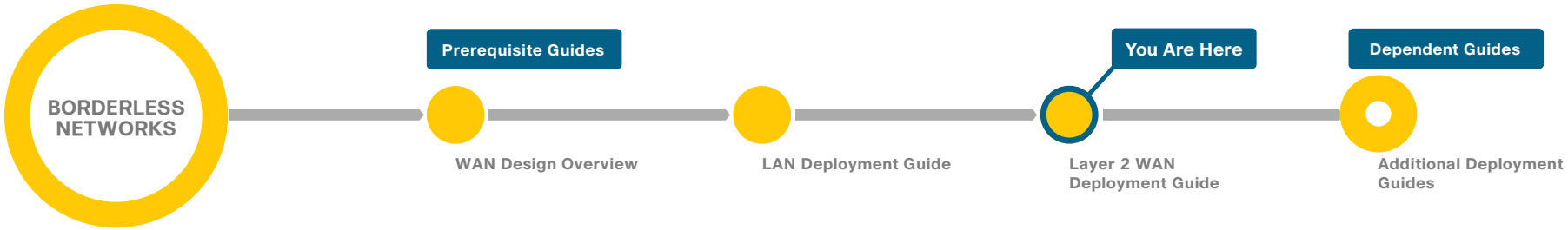
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

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

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

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



Introduction

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

The overall WAN architecture is described in the *WAN Design Overview*.

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

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

Each of these WAN deployment guides has a complementary WAN configuration guide.

Related Reading

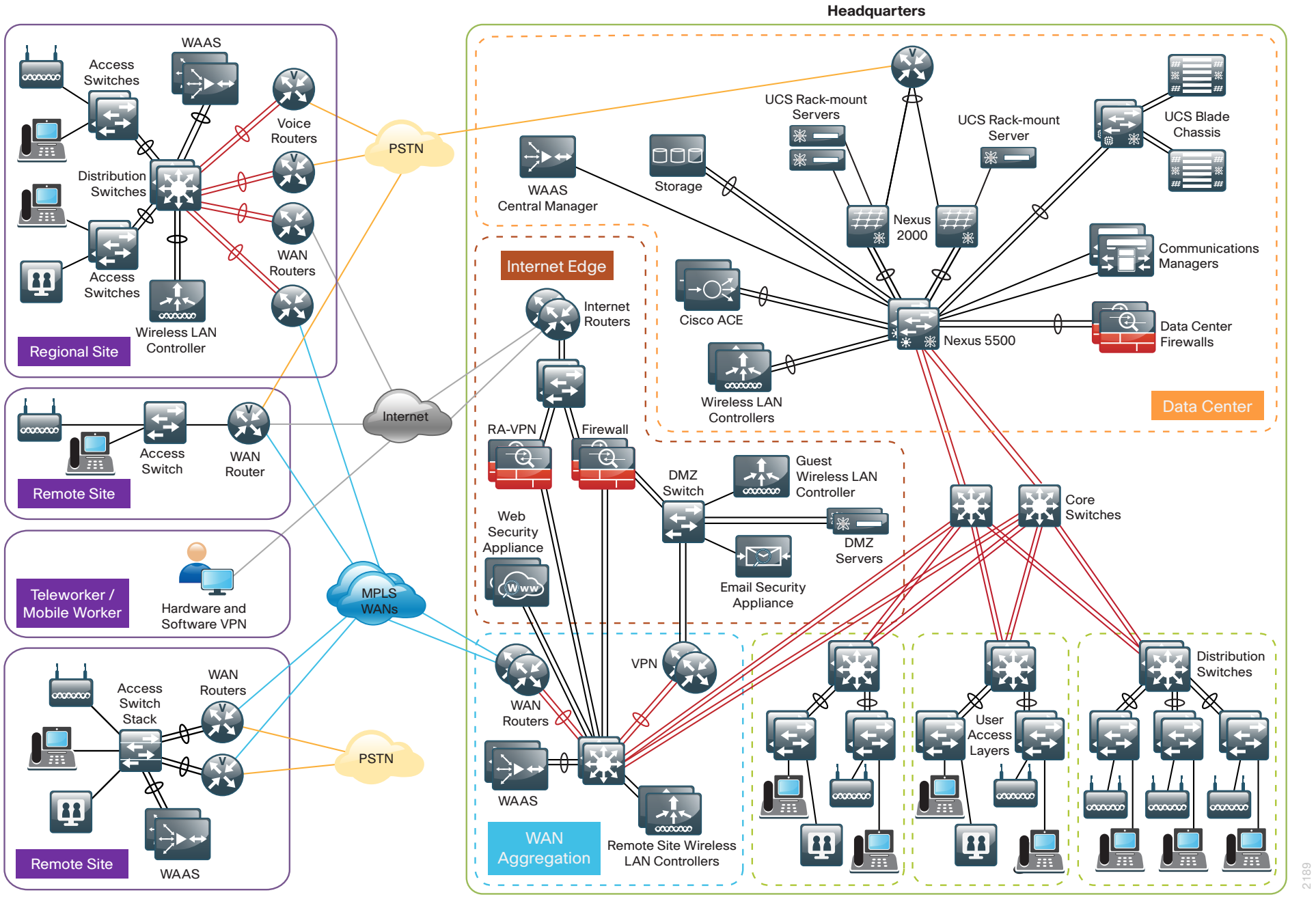
The *LAN Deployment Guide* describes wired network access with ubiquitous capabilities for both the larger campus-size LAN as well as the smaller remote-site LAN. Resiliency, security, and scalability are included to provide a robust communications environment. Quality of service (QoS) is integrated to ensure that the base architecture can support a multitude of applications, including low-latency, drop-sensitive multimedia applications coexisting with data applications on a single network.

Design Goals

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

Notes

Figure 1 - Borderless Networks for Enterprise Organizations Overview



Ease of Deployment, Flexibility, and Scalability

Organizations with100 to 10,000 users are often spread out among different geographical locations, making flexibility and scalability a critical requirement of the network. This design uses several methods to create and maintain a scalable network:

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

Resiliency and Security

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

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

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

Ease of Management

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

Advanced Technology–Ready

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

- Access switches provide Power over Ethernet (PoE) for phone deployments without the need for a local power outlet.
- The entire network is preconfigured with QoS to support high-quality voice, video, and collaboration applications.
- Multicast is configured in the network to support efficient voice and broadcast-video delivery.
- The wireless network is preconfigured for devices that send voice over the wireless LAN, providing IP telephony over 802.11 Wi-Fi (referred to as mobility) at all locations.
- Video and voice perform better through the use of medianet technologies, Cisco's recommended approach for video and collaboration, which simplifies, lowers the risks, cuts costs, and improves the quality of your video and voice deployments.

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

Architecture Overview

The *Cisco SBA—Borderless Networks Layer 2 WAN Deployment Guide* provides a design that enables highly available, secure, and optimized connectivity for multiple remote-site LANs.

The WAN is the networking infrastructure that provides an IP-based 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:

- Layer 2 WAN connectivity for up to 100 remote sites
- 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:

- Layer 2 WAN (primary)
- Internet VPN (secondary)

At a high level, the WAN is an IP network, and this transport 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 Deployment Guide.*

Layer 2 WAN Transport

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

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

Service providers implement these Ethernet services by using a variety of methods. MPLS networks support both Ethernet over MPLS (EoMPLS) and Virtual Private LAN Service (VPLS). You can use other network technologies, such as Ethernet switches in various topologies, to provide Ethernet Layer 2 WAN services. These offerings are also referred to as Carrier Ethernet or Metro Ethernet, and they are typically limited to a relatively small geographic area. This guide describes how to use a Layer 2 WAN to interconnect multiple sites independent of the various underlying technologies that are being used by the service providers.

Layer 2 WAN supports an enterprise subscriber model in which the service provider is transparent and the enterprise implements all Layer 3 routing. This allows for flexibility in the WAN design and interconnection of the remote sites.

Point-to-point service allows for the interconnection of two LANs. Point-to-multipoint (multipoint) transparent LAN service allows for the interconnection of more than two LANS. Other service variants include simple and trunked demarcations. By using trunk mode, you can interconnect LANs using 802.1Q VLAN tagging. Service providers often refer to a trunked service as Q-in-Q tunneling (QinQ).

Subscribers who need to transport IP multicast traffic are supported with no additional configuration required by the service provider.

The WAN uses Layer 2 WAN as a primary WAN transport.

WAN-Aggregation Designs

The WAN-aggregation (hub) design uses a single WAN edge router. When a WAN edge router is referred to in the context of the connection to a carrier or service provider, it is typically known as a *customer edge (CE) router.* The WAN edge router connects into a distribution layer.

The only WAN transport option used in this guide is Layer 2 WAN, which connects to a CE router.

This deployment guide documents two WAN-aggregation design models that use either simple demarcation or trunked demarcation. The primary difference between the Simple Demarcation and Trunked Demarcation design models is the number of broadcast domains or VLANs that are used to communicate with a subset of remote-site routers.

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

In the WAN-aggregation design, 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.

The Layer 2 WAN service terminates to a dedicated WAN router. The various design models are shown in the following table.

Table 1 - WAN-aggregation design models

	Layer 2 simple demarcation design model	Layer 2 trunked demarcation design model
Remote sites	Up to 25	Up to 100
WAN links	Single	Single
Edge routers	Single	Single
WAN routing protocol	EIGRP	EIGRP
Transport 1 type	MetroE/VPLS	MetroE/VPLS
Transport 1 demarcation	Simple	Trunked

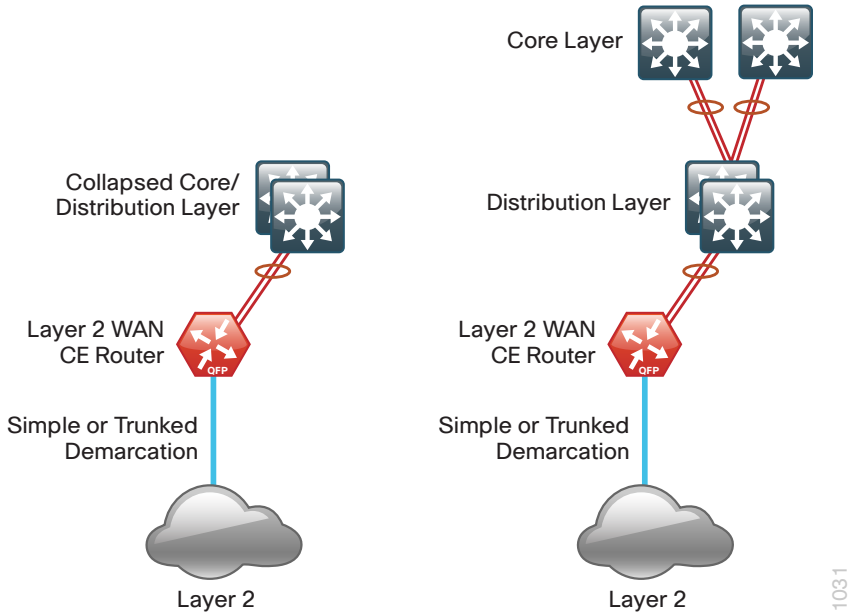
The characteristics of each design are as follows:

Layer 2 Simple Demarcation Design Model

- Uses a multipoint service
- Connects to a simple demarcation
- Supports up to 25 remote sites

The Layer 2 Simple Demarcation design is shown in the following figure.

Figure 2 - Layer 2 Simple Demarcation and Trunked Demarcation design models



Layer 2 Trunked Demarcation Design Model

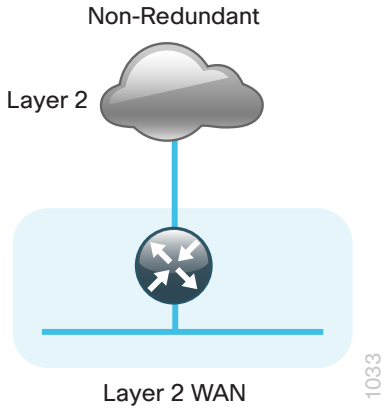
- Uses a multipoint service
- Connects to a trunked demarcation
- Supports up to 100 remote sites
- Logically separates the remote-site peering. Distributes router peers across multiple VLANs with maximum of 25 remote-site router peers per VLAN
- Typically used with a dedicated WAN distribution layer

The Layer 2 Trunked Demarcation design is shown in Figure 2.

WAN Remote-Site Designs

This guide documents a single remote-site WAN design that is based on a Layer 2 WAN transport.

Figure 3 - WAN remote-site design



The remote-site design includes a single WAN edge route, which is a Layer 2 WAN CE router.

Designs which include Internet VPN for additional resiliency are covered in the *VPN WAN Deployment Guide*.

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	MetroE/VPLS (simple)	-
Single	Single	MetroE/VPLS (trunked)	-

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

Both the 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 *LAN Deployment Guide*.

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

Table 3 - WAN remote-site LAN options

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

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 deployment guide uses a convention that is relevant to any location that has a single access switch and this model can also be easily scaled to additional access closets through the addition of a distribution layer.

Table 4 - WAN remote-sites—VLAN assignment

VLAN	Usage	Layer 2 access	Layer 3 distribution/ access
VLAN 64	Data	Yes	-
VLAN 69	Voice	Yes	-
VLAN50	Router link (1)	-	Yes

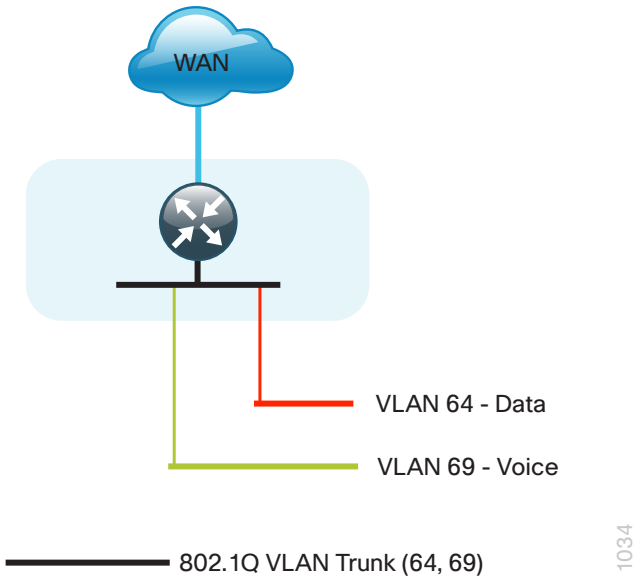
Layer 2 Access

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 *LAN Deployment Guide* provides configuration details on the various access switching platforms.

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

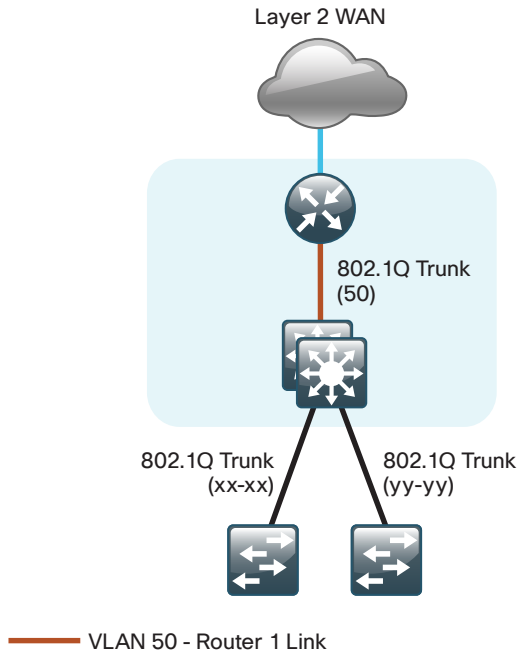
Figure 4 - WAN remote site - Flat Layer 2 LAN (single router)



Distribution and Access Layer

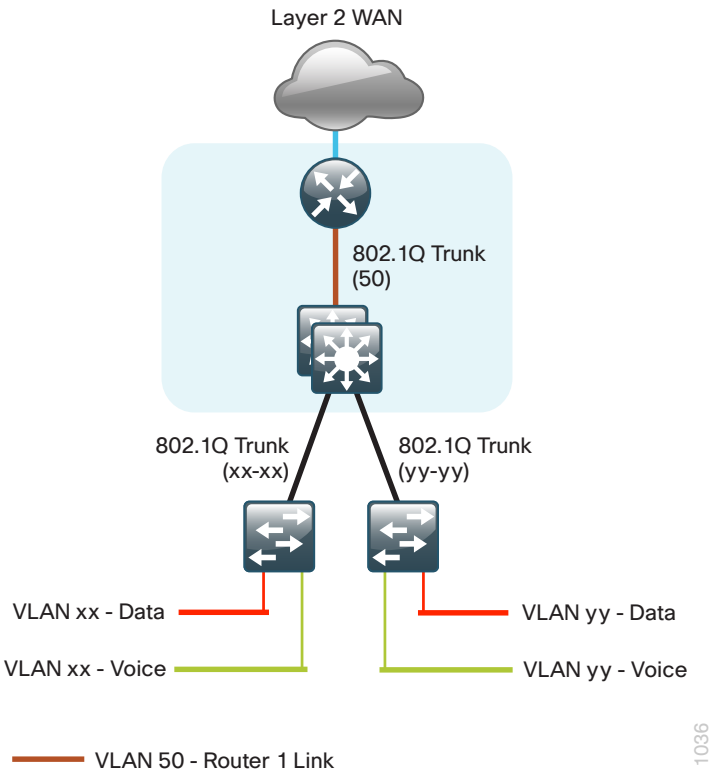
Large remote sites may require a LAN environment similar to that of a small campus LAN that includes a distribution layer and access layer. This topology works well with either a single or dual router WAN edge. To implement this design, the routers should connect via EtherChannel links to the distribution 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 5 - WAN remote site—Connection to Distribution Layer



The distribution switch handles all access layer routing, with VLANs trunked to access switches. A full distribution and access layer design is shown in the following figure.

Figure 6 - WAN remote site—Distribution and access layer



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 application has an appropriate share of the network resources to protect the user experience and ensure the consistent operation 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. 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.

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
- 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. 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

Resilient design options for a Layer 2 WAN connected remote site are covered in the *Cisco SBA—Borderless Networks VPN Remote Site Deployment Guide*.

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.

The Layer 2 WAN-connected site:

- Connects to a site on the Layer 2 WAN (same VLAN); the optimal route is direct within the Layer 2 WAN (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. This is referred to as hierarchical QoS (HQoS). 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.

Any multipoint WAN service that supports differing access speeds is susceptible to traffic overruns. Layer 2 WAN transports may be implemented with inherent QoS capabilities by the service provider, but this design assumes that the responsibility for implementing QoS falls on the subscriber and must be configured on all WAN Layer 2 CE devices.

The primary difference between the Layer 2 WAN transport QoS model and other SBA WAN QoS is specific to the WAN-aggregation CE router only. This router performs traffic-shaping both at the physical interface level and on a per-remote-site basis. This is referred to as HQoS with nested traffic-shaping.

Design Parameters

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

Table 6 - Universal design parameters

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

Notes

Deploying a Layer 2 WAN

Business Overview

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

Major market drivers for Layer 2 WAN services include surging bandwidth requirements and the increased availability of Ethernet building terminations. Carriers have the flexibility to provision bandwidth in flexible increments and deploy these services over their existing infrastructure.

To control operational costs, the WAN must support the convergence of voice, video, and data transport onto a single, centrally managed infrastructure. Layer 2 WAN services provide high-performance, cost-effective, and reliable services within metropolitan areas and, in some cases, for broader geographic areas. The ubiquity of carrier-provided Layer 2 WAN 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 makes Layer 2 WAN an effective WAN transport for growing organizations.

Technology Overview

WAN-Aggregation—Layer 2 WAN CE Routers

The Layer 2 WAN designs are intended to support up to 100 remote sites with a combined aggregate WAN bandwidth of up to 500 Mbps. 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.

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 Layer 2 WAN CE routers:

- Cisco ASR 1002 Aggregation Services Router configured with an Embedded Service Processor 5 (ESP5)
- Cisco ASR 1001 Aggregation Services Router fixed configuration with a 2.5 Gbps Embedded Service Processor

Both of the design models can be constructed using either of the Layer 2 WAN 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—Layer 2 WAN CE router options

Option	ASR 1001	ASR 1002
Ethernet WAN with services	250 Mbps	500 Mbps
Software Redundancy Option	Yes	Yes
Redundant power supply	Default	Default
Supported Design Models	All	All
Suggested Design Model	Simple Demarcation	Trunked Demarcation
Suggested Number of Remote Sites	25	100

Remote Sites—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 Layer 2 WAN CE routers, and the expected performance is shown in the following table.

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

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

Notes:

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

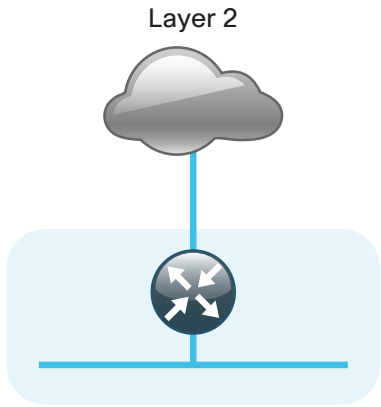
The CE routers at the WAN remote sites connect in the same manner as the WAN aggregation CE router at the WAN-aggregation site. Depending on the service provider, the demarcation may be simple access mode or 802.1Q trunk mode. It is not necessary to use multiple VLANs for connecting the remote-site routers, so if you are using a trunked demarcation, only a single VLAN should is necessary.

The single link Layer 2 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.

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. No configuration changes are required on the WAN-aggregation CE router or on other remote-site CE routers when you use dynamic routing.

Figure 7 - Layer 2 WAN remote site (single-router, single-link)



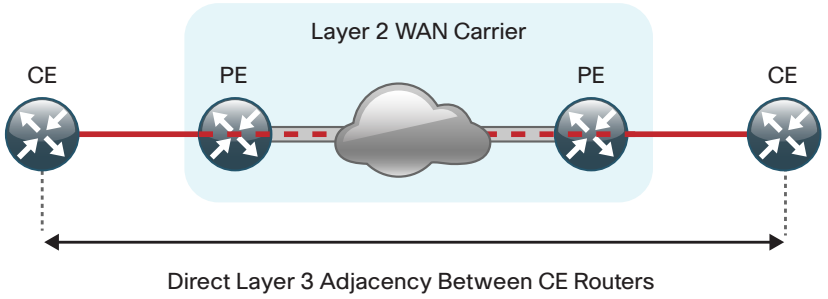
Design Details

The WAN-aggregation Layer 2 WAN CE router connects to a 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.

The Layer 2 WAN transport is explicitly focused on providing an Ethernet WAN service, so it is not relevant to document media types other than Ethernet.

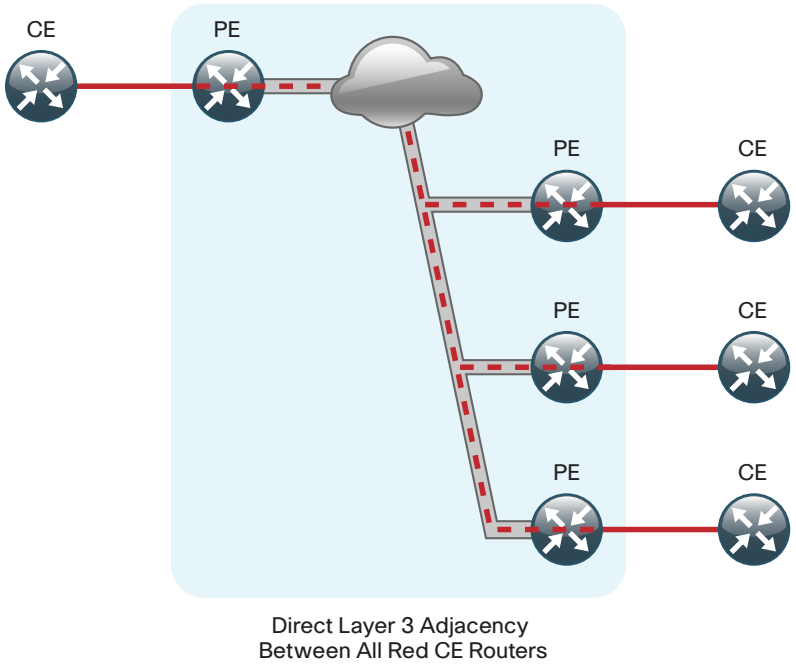
A Layer 2 WAN requires a link between a provider edge (PE) router and a CE router. However, the Layer 2 WAN PE routers are transparent from a Layer 3 perspective so the WAN-aggregation and remote-site CE routers are considered IP neighbors across the WAN link. CE routers are able to directly communicate with other CE routers across the Layer 2 WAN (CE-CE connections).

Figure 8 - Layer 2 WAN simple point-to-point



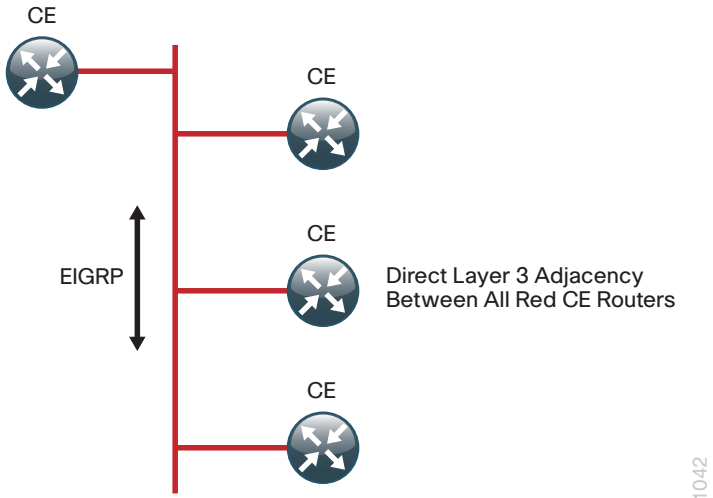
A service provider implements a multipoint Layer 2 WAN by extending the broadcast domain to multiple locations each with a corresponding PE router and attached CE router. A discussion of the underlying technologies used by the service provider to provision this service is beyond the scope of this guide. Cisco did not test the PE routers, and their configurations are not included in this guide.

Figure 9 - Layer 2 WAN simple point-to-multipoint



The device connections to a multipoint Layer 2 WAN transport are logically equivalent to the connections to a shared Ethernet segment. The service provider devices are transparent to the subscriber's CE routers. All CE routers are able to directly communicate with each other as if they were on the same LAN.

Figure 10 - Layer 2 WAN simple point-to-multipoint (logical view)



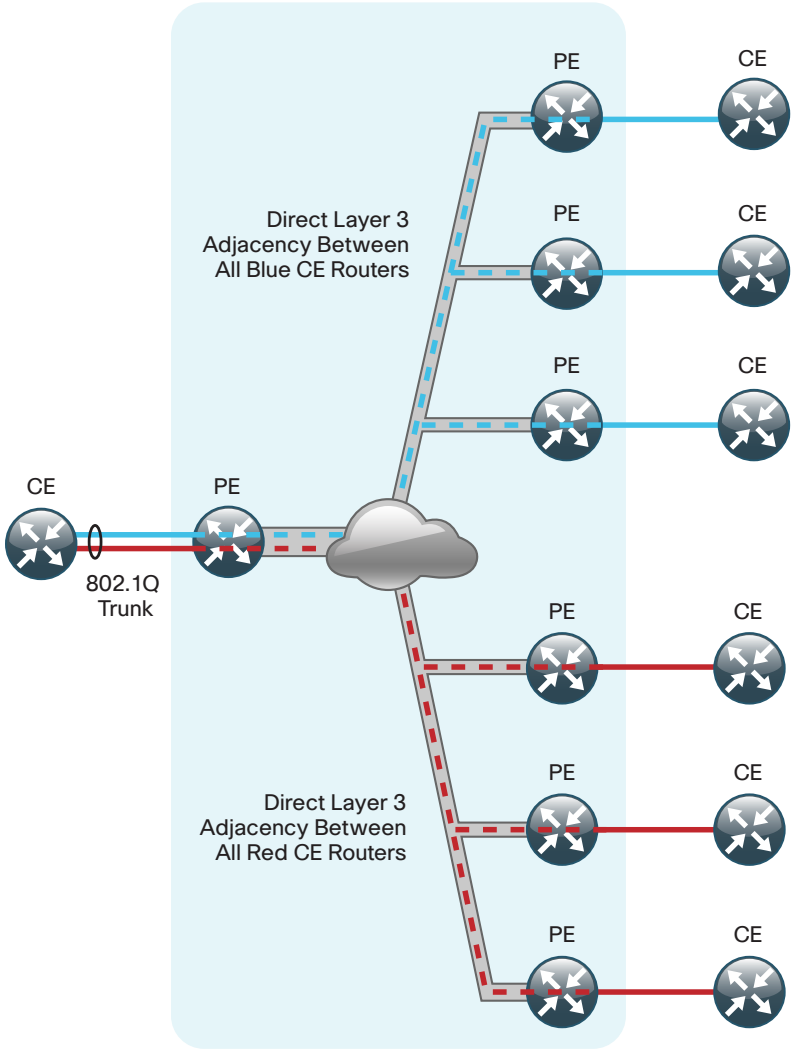
The CE routers are the only devices required to have IP-routing information to provide end-to-end reachability. No IP-routing information is required to be shared with the service provider. Maintaining this routing information typically requires a routing protocol, and we chose EIGRP for this purpose. The various CE routers advertise their routes to other CE router peers.

As the number of CE devices increases, there is a corresponding increase in the number of routing protocol neighbors sending and receiving updates to each other. There is a performance impact on the routers' CPU associated with the processing of the updates from the additional neighbors. This impact is most significant on the remote-site Layer 2 WAN CE routers, which are not designed to accommodate large numbers of routing protocol neighbors.

The limiting factor in the number of routing protocol neighbors on a broadcast media is the processing capability of the smallest router's CPU.

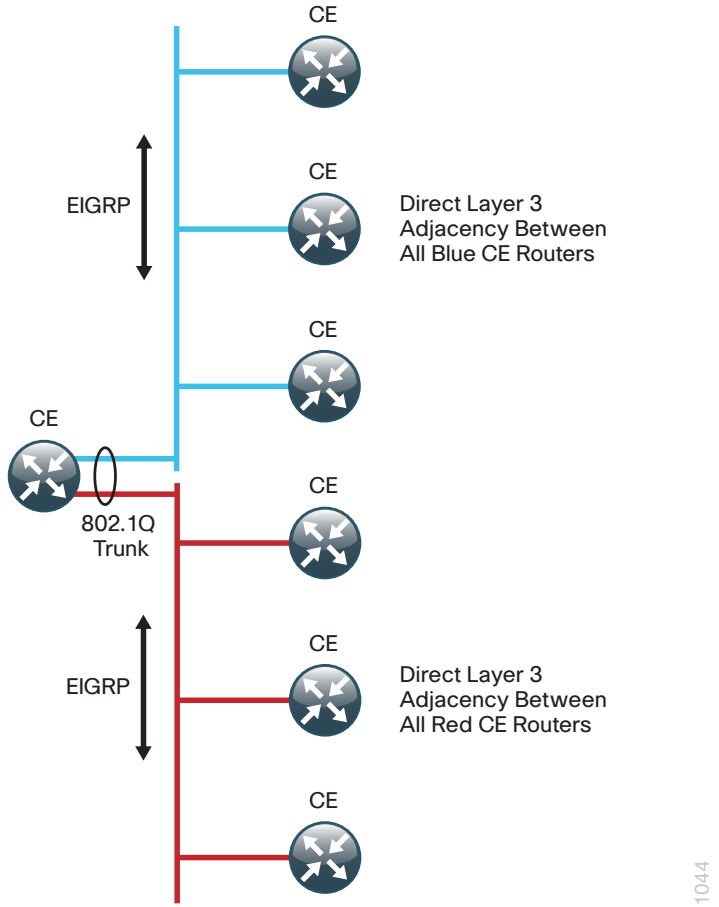
There are a variety of methods that can be used to limit the number of neighbors. It is straightforward to use VLANs in the Layer 2 WAN to isolate the remote-site Layer 2 WAN CE routers from each other. The primary difference is the use of a trunked demarcation which allows the use of 802.1Q tagged Ethernet frames. The service provider can provide this additional capability over the same infrastructure though a change in the edge configuration and by propagating VLAN tagged frames to other PE devices.

Figure 11 - Layer 2 WAN trunked point-to-multipoint



The device connections to a trunked multipoint Layer 2 WAN transport are logically equivalent to the connections to a common Ethernet that has implemented VLANs. The service provider devices are transparent to the subscriber's CE routers. All CE routers attached to a particular VLAN are able to directly communicate with each other. Devices connected to multiple VLANs, such as the WAN-aggregation Layer 2 WAN CE router, are able to communicate with multiple sets of CE routers.

Figure 12 - Layer 2 WAN trunked point-to-multipoint (logical view)



Two separate EIGRP processes are used, one for internal routing on the LAN (EIGRP-100) and one for the Layer 2 WAN (EIGRP-300). The primary reason for the separate EIGRP processes is to simplify the route selection at the WAN-aggregation site when connecting multiple remote-site types,

potentially including MPLS WAN as used in other SBA WAN guides. This method ensures that all WAN learned routes appear as EIGRP external routes after they are redistributed into the EIGRP-100 process used on the campus LAN.

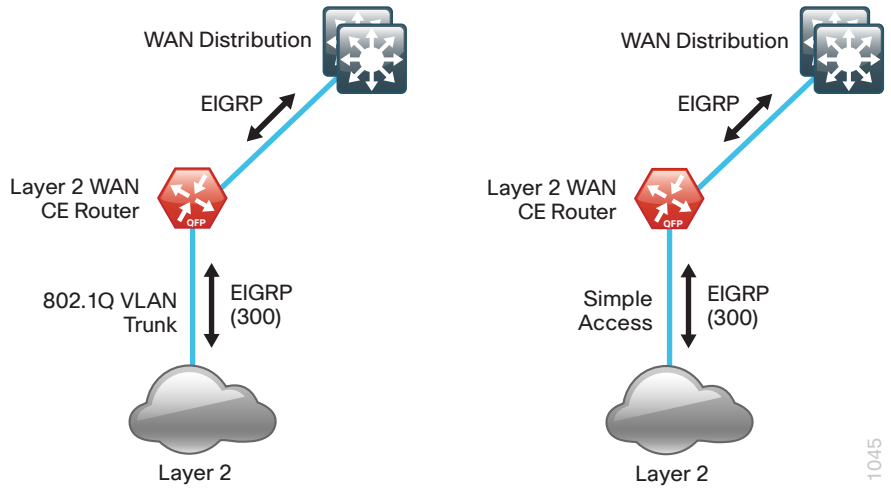
The Simple Demarcation design model assumes a simple demarcation for both the WAN-aggregation and remote-site routers. Therefore, in this design the WAN-aggregation CE router and all of the remote-site CE routers are EIGRP neighbors. The Trunked Demarcation design model assumes a trunked demarcation for both the WAN-aggregation and remote-site routers. Therefore, in this design the WAN-aggregation CE router and sets of remote-site CE routers are EIGRP neighbors. Only remote-site CE routers connected to the same VLAN are EIGRP neighbors.

Sites with only a single WAN transport (a single-homed site) do not require dynamic routing and can rely on static routing because there is only a single path to any destination. This design only includes dynamic WAN 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 Layer 2 WAN deployment requires the installation and configuration of CE routers at every location, including the WAN-aggregation site and every Layer 2 WAN-connected remote site.

At the WAN-aggregation site, a Layer 2 WAN CE router must be connected both to the distribution layer and to the Layer 2 WAN service provider. A single routing protocol (EIGRP with multiple instances) is 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 router interface for the Trunked Demarcation design model uses multiple subinterfaces that map to the various VLANs in use, whereas the Simple Demarcation design model uses only the single physical interface to connect to all of the remote sites. The IP routing details for both WAN-aggregation topologies are shown in the following figure.

Figure 13 - Trunked Demarcation and Simple Demarcation design models—Layer 2 WAN 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 utilization, and memory necessary to carry large route tables, as well as reduce convergence time associated with a link failure.

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

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

EIGRP process 300 is the Layer 2 WAN EIGRP process and is referred to as EIGRP-300.

EIGRP-300 is used to exchange routing information between the WAN-aggregation site Layer 2 WAN CE router and the remote-site Layer 2 WAN CE routers. You should configure EIGRP-300 for stub routing on all remote-site routers to improve network stability and reduce resource utilization.

Deployment Details

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

Table 9 - Parameters used in the deployment examples

Hostname	Loopback IP Address	Port Channel IP Address
METRO-ASR1001-1	10.4.32.245/32	10.4.32.34/30

Process

Layer 2 WAN CE Router Configuration

1. Configure the Distribution Switch
2. Configure the WAN Aggregation Platform
3. Configure Connectivity to the LAN
4. Connect to Layer 2 WAN
5. Configure EIGRP

Procedure 1 Configure the Distribution Switch

Reader Tip

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

The LAN distribution switch is the path to the organization's main campus and data center. A Layer 3 port-channel interface connects 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-channel5
 description METRO-ASR1001-1
 no switchport
 ip address 10.4.32.33 255.255.255.252
 ip pim sparse-mode
 logging event link-status
 carrier-delay msec 0
 no shutdown
```

Step 2: Configure EtherChannel member interfaces.

Configure the physical interfaces to tie to the logical port-channel using the **channel-group** command. The number for the port-channel and channel-group must match. Not all router platforms can support Link Aggregation Control Protocol (LACP) to negotiate with the switch, so EtherChannel is configured 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 METRO-ASR1001-1 Gig0/0/0
!
interface GigabitEthernet2/0/1
 description METRO-ASR1001-1 Gig0/0/1
!
interface range GigabitEthernet1/0/1, GigabitEthernet2/0/1
  no switchport
  macro apply EgressQoS
  carrier-delay msec 0
  channel-group 5 mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
```

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

```
router eigrp 100
  no passive-interface Port-channel5
```

Step 4: It is a best practice to summarize IP routes from the WAN distribution layer towards the core. On the distribution layer switch, configure the interfaces that are connected to the LAN core to summarize the WAN network range.

```
interface range TenGigabitEthernet1/1/1, TenGigabitEthernet2/1/1
 ip summary-address eigrp 100 10.4.32.0 255.255.248.0
 ip summary-address eigrp 100 10.5.0.0 255.255.0.0
```

Procedure 2 Configure the WAN Aggregation Platform

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

Step 1: Configure the device host name.

Configure the device host name to make it easy to identify the device.

```
hostname METRO-ASR1001-1
```

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
```

By default, https access to the router will use 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.

Reader Tip

The AAA server used in this architecture is the Cisco Authentication Control System. For details about ACS configuration, see the *Device Management Using ACS Deployment Guide*.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined 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 nonsecure protocols, Telnet and HTTP, are turned off.

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
line vty 0 15
 transport input ssh
 transport preferred none
```

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

```
line con 0
 logging synchronous
```

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

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

Step 5: (Optional) In networks where 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 login from one router to the next for hop-by-hop troubleshooting.

Step 6: 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 7: Configure an in-band management interface

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

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

```
interface Loopback 0
  ip address 10.4.32.245 255.255.255.255
  ip pim sparse-mode
```

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

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 8: Configure IP unicast routing.

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

```
router eigrp 100
  network 10.4.0.0 0.1.255.255
  no auto-summary
  passive-interface default
  eigrp router-id 10.4.32.245
```

Step 9: 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
```

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

```
ip multicast-routing distributed
```

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

```
ip pim autorp listener
```

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

```
ip pim sparse-mode
```

Procedure 3 Configure Connectivity to the LAN

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

Step 1: Configure Layer 3 Interface

```
interface Port-channel5
  ip address 10.4.32.34 255.255.255.252
  ip pim sparse-mode
  no shutdown
```

Step 2: Configure EtherChannel member interfaces.

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

```
interface GigabitEthernet0/0/0
 description WAN-D3750X Gig1/0/6
!
interface GigabitEthernet0/0/1
 description WAN-D3750X Gig2/0/6
!
interface range GigabitEthernet0/0/0, GigabitEthernet0/0/1
  no ip address
  channel-group 5
  no shutdown
```

Step 3: Configure the EIGRP interface.

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

```
router eigrp 100
  no passive-interface Port-channel5
```

Procedure 4 Connect to Layer 2 WAN

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 500 Mbps.

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

Tech Tip

Command reference:

```
bandwidth [kbps]
```

500 Mbps = 500000 kbps

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

The IP addressing used between CE routers must allow for sufficient host addresses to support a WAN-aggregation CE router, plus up to 25 remote-site CE routers. This design uses a netmask of 255.255.255.0, which is commonly used for LAN addressing. It may be more efficient to use a different netmask to conserve IP addresses. As a best practice, the VLAN number and the subinterface number should match.

Table 10 - Layer 2 WAN transport IP address information

Design Model	Interface	VLAN	Subinterface	Network	CE router address
Simple Demarcation	gig0/0/3	none	none	10.4.38.0/24	.1
Trunked Demarcation	gig0/0/3	38	gig0/0/3.38	10.4.38.0/24	.1
		39	gig0/0/3.39	10.4.39.0/24	.1

If connected to a simple demarcation use the following configuration.

```
interface [interface type] [number]
 ip address [IP address] [netmask]
 ip pim sparse-mode
```

Use the following configuration for each of the VLANs on a trunked demarcation.

```
interface [interface type] [number].[subinterface number]
 encapsulation dot1Q [Vlan number]
 ip address [IP address] [netmask]
 ip pim sparse-mode
```

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

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

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

Example (Simple Demarcation)

```
interface GigabitEthernet0/0/3
 bandwidth 500000
 ip address 10.4.38.1 255.255.255.0
 ip pim sparse-mode
 no cdp enable
 no shutdown
```

Example (Trunked Demarcation)

```
interface GigabitEthernet0/0/3
 bandwidth 500000
 no cdp enable
 no shutdown
!
interface GigabitEthernet0/0/3.38
 encapsulation dot1Q 38
 ip address 10.4.38.1 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet0/0/3.39
 encapsulation dot1Q 39
 ip address 10.4.39.1 255.255.255.0
 ip pim sparse-mode
```

Procedure 5 Configure EIGRP

The WAN aggregation Layer 2 WAN CE router uses two EIGRP processes. The primary reason for the additional process is to ensure that routes learned from the WAN remote sites appear as EIGRP external routes on the WAN distribution switch. If only a single process was used, then the remote-site routes would appear as EIGRP internal routes on the WAN distribution switch, which would be inconsistent with other SBA WAN deployment guides.

Step 1: Enable an additional process, EIGRP-300, for the Layer 2 WAN.

EIGRP-300 is configured for the Layer 2 WAN interface or subinterfaces. The Layer 2 WAN interface or subinterfaces are the only EIGRP-300 interfaces, and their network ranges should be explicitly listed. Repeat for all Layer 2 WAN interfaces as required.

```
router eigrp 300
 network [L2 WAN network 1] [inverse mask]
 network [L2 WAN network 2] [inverse mask] ! if necessary
 passive-interface default
 no passive-interface [L2 WAN interface 1]
 no passive-interface [L2 WAN interface 2] ! if necessary
 eigrp router-id [IP address of Loopback0]
 no auto-summary
```

Step 2: Configure route-maps for tagging routes and blocking routes.

This design uses mutual route redistribution; Layer 2 WAN routes from the EIGRP-300 process are distributed into EIGRP-100 and other learned routes from EIGRP-100 are distributed into EIGRP-300. Because the routing protocol is the same, no default metric is required.

It is important to tightly control how routing information is shared between different routing protocols when you use this mutual route redistribution; 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.

This router and other WAN routers in other SBA deployments use an inbound distribute list with a route map to limit which routes are accepted for installation into the route table. These routers are configured to block routes from certain other WAN sources. To accomplish this task, you must create a route map that matches any routes originating from the WAN as indicated by a specific route tag. This method allows for dynamic identification of the various WAN routes. The specific route tags in use are shown below.

This task also requires that the Layer 2 WAN learned WAN routes are explicitly tagged by the WAN aggregation CE router during the route redistribution process. To do this, you must create an additional route map to match the source interface of the routes.

Reader Tip

MPLS WAN deployment is covered in the *MPLS WAN Deployment Guide*. DMVPN deployment is covered in the *VPN WAN Deployment Guide*.

Table 11 - Route tag information for WAN aggregation Layer 2 WAN CE router

Tag	Route source	Tag method	Action
65401	MPLS VPN A	implicit	accept
65402	MPLS VPN B	implicit	accept
300	Layer 2 WAN	explicit	tag
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 use more or fewer tags.

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

Tech Tip

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

```
route-map BLOCK-TAGGED-ROUTES deny 10
 match tag 65512
!
route-map BLOCK-TAGGED-ROUTES permit 20
```

You need to appropriately tag the Layer 2 WAN routes to be consistent with other SBA deployments.

The Simple Demarcation design model requires a single interface in the match statement, whereas the Trunked Demarcation design model requires multiple subinterfaces.

```
route-map SET-ROUTE-TAG-METROE permit 10
 match interface GigabitEthernet0/0/3.38
GigabitEthernet0/0/3.39
 set tag 300
```

Step 3: Configure the EIGRP mutual route redistribution.

```
router eigrp 100
 distribute-list route-map BLOCK-TAGGED-ROUTES in
 redistribute eigrp 300 route-map SET-ROUTE-TAG-METROE
!
router eigrp 300
 redistribute eigrp 100
```

Example

```
route-map BLOCK-TAGGED-ROUTES deny 10
 match tag 65512
!
route-map BLOCK-TAGGED-ROUTES permit 20
!
route-map SET-ROUTE-TAG-METROE permit 10
 match interface GigabitEthernet0/0/3.38 GigabitEthernet0/0/3.39
 set tag 300
!
router eigrp 100
 distribute-list route-map BLOCK-TAGGED-ROUTES in
 redistribute eigrp 300 route-map SET-ROUTE-TAG-METROE
!
router eigrp 300
 network 10.4.38.0 0.0.0.255
```

```
network 10.4.39.0 0.0.0.255
redistribute eigrp 100
passive-interface default
no passive-interface GigabitEthernet0/0/3.38
no passive-interface GigabitEthernet0/0/3.39
eigrp router-id 10.4.32.245
```

Process

Remote-Site Layer 2 WAN CE Router Configuration

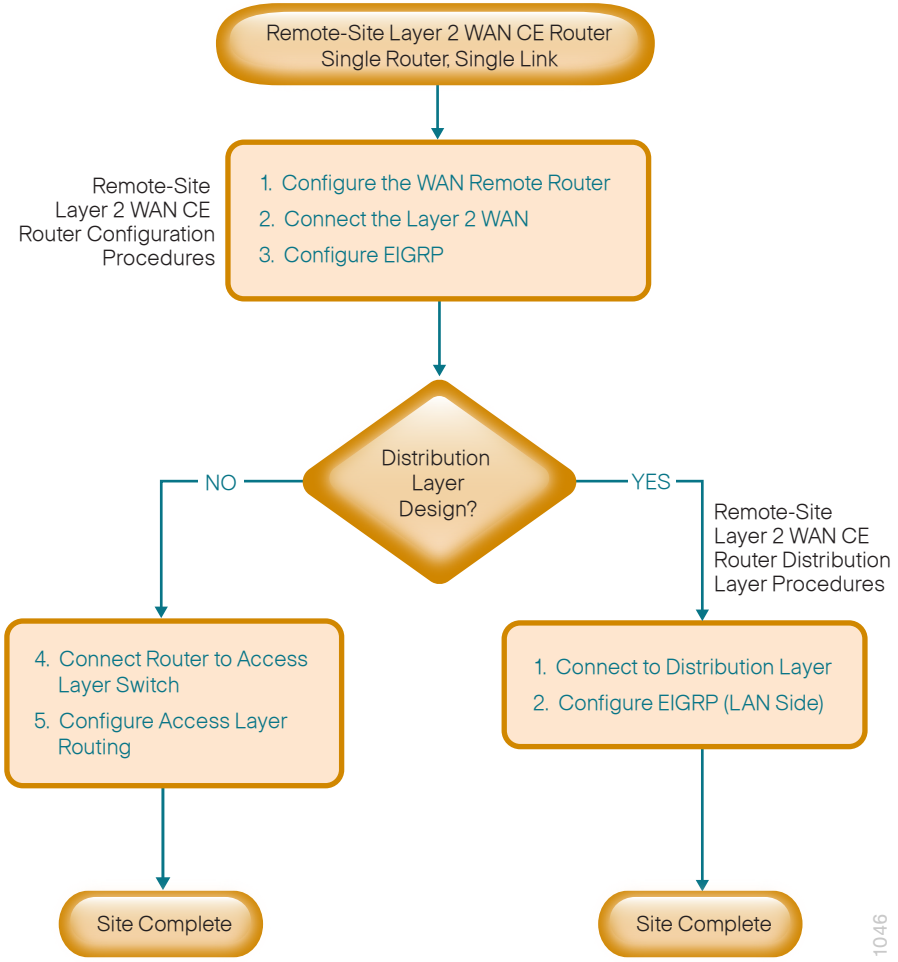
1. Configure the WAN Remote Router
2. Connect to the Layer 2 WAN
3. Configure EIGRP
4. Configure Router to Access Layer Switch
5. Configure Access Layer Routing

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

- Layer 2 WAN CE router for a Layer 2 WAN remote site (single router, single link).

The following flowchart provides details about the configuration process for a remote-site Layer 2 WAN CE router.

Figure 14 - Remote-site Layer 2 WAN 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.

Configure the device hostname to make 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, 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 will use 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.

Reader Tip

The AAA server used in this architecture is the Cisco Authentication Control System. For details about ACS configuration, see the *Device Management Using ACS Deployment Guide*.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined 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 nonsecure protocols, Telnet and HTTP, are turned off.

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
line vty 0 15
 transport input ssh
 transport preferred none
```

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

```
line con 0
 logging synchronous
```

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

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

Step 6: (Optional) In networks where 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 login from one router to the next for hop-by-hop troubleshooting.

Step 7: 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 8: Configure an in-band management interface.

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

The loopback address is commonly a host address with a 32-bit address mask. Allocate the loopback address from 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
```

The **ip pim sparse-mode** command will be explained in the next step.

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 9: 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
```

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

```
ip pim autorp listener
```

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

```
ip pim sparse-mode
```

Procedure 2 Connect to the Layer 2 WAN

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 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 routers must allow for sufficient host addresses to support a WAN aggregation CE router plus up to 25 remote-site CE routers. This design uses a netmask of 255.255.255.0, which is commonly used for LAN addressing. It may be more efficient to use a different netmask to conserve IP addresses. As a best practice, the VLAN number and the subinterface number should match.

Table 12 - Layer 2 WAN transport IP address information

Design Model	Interface	VLAN	Subinterface	Network	CE router address
Simple Demarcation	gig0/0/4	none	none	10.4.38.0/24	.1
Trunked Demarcation	gig0/0/4	38	gig0/0/3.38	10.4.38.0/24	.1
		39	gig0/0/3.39	10.4.39.0/24	.1

The configuration of the remote-site Layer 2 WAN CE router depends on whether the service provider has implemented a simple or trunked demarcation.

Use the following configuration for a simple demarcation. You can use this connection type even when the WAN aggregation Layer 2 WAN CE router is using a trunked demarcation. However, the service provider must configure the proper VLAN assignment for the remote site connection.

```
interface [interface type] [number]
 ip address [IP address] [netmask]
 ip pim sparse-mode
```

Use the following configuration for a trunked demarcation. The VLAN number and IP network must match those chosen on the WAN aggregation Layer 2 WAN CE router.

```
interface [interface type] [number].[subinterface number]
 encapsulation dot1Q [Vlan number]
 ip address [IP address] [netmask]
 ip pim sparse-mode
```

Step 3: Administratively enable the interface and disable Cisco Discovery Protocol. Cisco does not recommend the use of Cisco Discovery Protocol on external interfaces.

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

Step 4: Configure EIGRP.

The remote-site LAN networks must be advertised. The IP assignment for the remote sites was designed so that all of the networks in use can be summarized within a single aggregate route. The summary address as configured below suppresses the more specific routes. If any network within the summary is present in the route table, the summary is advertised to the Layer 2 WAN, which offers a measure of resiliency. If the various LAN networks cannot be summarized, EIGRP continues to advertise the specific routes.

```
interface [interface type] [number].[subinterface number]
 ip summary-address eigrp [as number (Layer 2 WAN)]
[summary network] [summary mask]
```

Example (Simple Demarcation)

```
interface GigabitEthernet0/0
 bandwidth 10000
 ip address 10.4.38.210 255.255.255.0
 ip pim sparse-mode
 ip summary-address eigrp 300 10.5.144.0 255.255.248.0
 no cdp enable
 no shutdown
```

Example (Trunked Demarcation)

```
interface GigabitEthernet0/0
 bandwidth 10000
 no cdp enable
 no shutdown
!
interface GigabitEthernet0/0.38
 encapsulation dot1Q 38
 ip address 10.4.38.210 255.255.255.0
 ip pim sparse-mode
 ip summary-address eigrp 300 10.5.144.0 255.255.248.0
```

Procedure 3 Configure EIGRP

A single EIGRP-300 process runs on the remote-site Layer 2 WAN CE router. All interfaces on the router are EIGRP interfaces, but only the Layer 2 WAN interface is non-passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address. All remote-site Layer 2 WAN CE routers should run EIGRP stub routing to improve network stability and reduce resource utilization.

```
router eigrp 300
 network [L2 WAN network] [inverse mask]
 network [WAN loopback range] [inverse mask]
 network [WAN remote range] [inverse mask]
 passive-interface default
 no passive-interface [L2 WAN interface]
 eigrp router-id [IP address of Loopback0]
 eigrp stub connected summary
 no auto-summary
```

Example (Trunked Demarcation)

```
router eigrp 300
 network 10.4.38.0 0.0.0.255
 network 10.255.0.0 0.0.255.255
 network 10.5.0.0 0.0.255.255
 passive-interface default
 no passive-interface GigabitEthernet0/0.38
 eigrp router-id 10.255.255.210
 eigrp stub connected summary
 no auto-summary
```

Procedure 4 Configure Router to Access Layer Switch

Reader Tip

Please refer to the *LAN Deployment Guide* for complete access layer configuration details. This guide only includes the additional steps to complete the distribution layer configuration.

If you are using a remote-site distribution layer, skip to the "Deploying a WAN Remote-Site Distribution Layer" section 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 RS210-A2960S
 no shutdown
```

Step 2: Configure EtherChannel member interfaces on the router.

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

```
interface GigabitEthernet0/1
 description RS210-A2960S Gig1/0/24
!
interface GigabitEthernet0/2
 description RS210-A2960S 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 EtherChannel is configured statically.

```
interface GigabitEthernet1/0/24
 description Link to RS210-2921 Gig0/1
interface GigabitEthernet2/0/24
 description Link to RS210-2921 Gig0/2
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport
 macro apply EgressQoS
 channel-group 1 mode on
 logging event link-status
 logging event trunk-status
 logging event bundle-status
```

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

An 802.1Q trunk is used which allows the router to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access layer switch. When using EtherChannel the interface type will be port-channel and the number must match the channel group configured in Step 3. DHCP Snooping and Address Resolution Protocol (ARP) inspection are set to trust.

```
interface Port-channel1
 description EtherChannel link to RS210-2921
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 64,69
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
 ip dhcp snooping trust
 no shutdown
```

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

Option 2. Layer 2 trunk from router to access layer switch

Step 1: Enable the physical interface on the router.

```
interface GigabitEthernet0/2
 description RS210-A2960S 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. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access switch. DHCP Snooping and Address Resolution Protocol (ARP) inspection are set to trust.

```
interface  GigabitEthernet1/0/24
 description Link to RS210-2921 Gig0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 64,69
 switchport mode trunk
```

```
ip arp inspection trust
spanning-tree portfast trunk
macro apply EgressQoS
logging event link-status
logging event trunk-status
ip dhcp snooping trust
no shutdown
```

The Catalyst 2960 does not require the **switchport trunk encapsulation dot1q** command.

Procedure 5 Configure Access Layer Routing

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.

```
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 - Layer 2 EtherChannel

```
interface Port-channel1
 no ip address
 no shutdown
 !
interface Port-channel1.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.148.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface Port-channel1.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.149.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
```

Example - Layer 2 Link

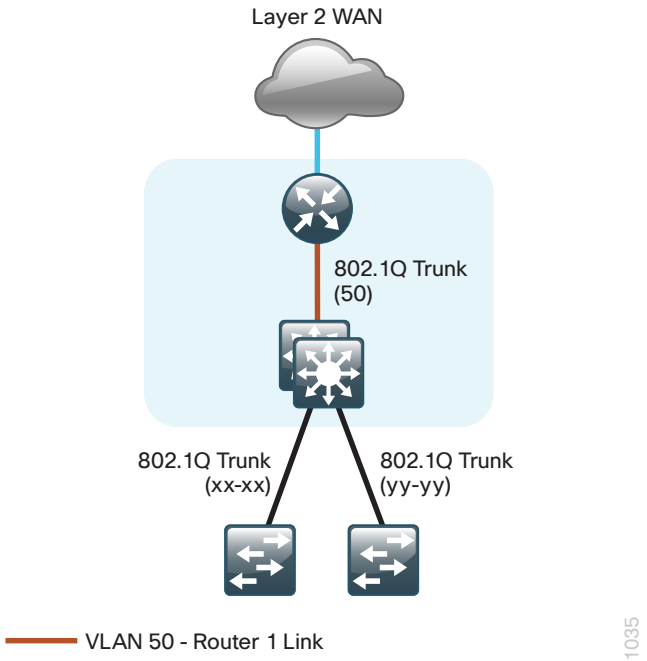
```
interface GigabitEthernet0/2
 no ip address
 no shutdown
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.148.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface GigabitEthernet0/2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.149.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
```

Deploying a WAN Remote-Site Distribution Layer

Use this set of procedures to configure a Layer 2 WAN CE router for a Layer 2 WAN remote site (single-router, single-link). This section includes all required procedures to connect to a distribution layer.

The distribution layer remote-site topology is show in the following figure.

Figure 15 - WAN remote site - Connection to distribution layer



Process

Remote-Site Layer 2 WAN CE Router Distribution Layer

1. Connect CE Router to Distribution Layer
2. Configure EIGRP (LAN Side)

Procedure 1 Connect CE Router to Distribution Layer

Reader Tip

Please refer to the *LAN Deployment 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 if necessary.

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

```
interface Port-channel1
 description EtherChannel link to RS212-D3750X
 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 10.5.168.1 255.255.255.252
 ip pim sparse-mode
```

Step 3: Configure EtherChannel member interfaces on the router.

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

```
interface GigabitEthernet0/1
 description RS212-D3750X Gig1/0/1
!
interface GigabitEthernet0/2
 description RS212-D3750X Gig2/0/1
!
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 1
  no shutdown
```

Step 4: Configure VLAN on the distribution layer switch.

If your VLAN does not already exist on the distribution layer switch, configure it now.

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

Step 5: Configure Layer 3 on the distribution layer switch.

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 10.5.168.2 255.255.255.252
 ip pim sparse-mode
 no shutdown
```

Step 6: Configure EtherChannel member interfaces on the distribution layer switch.

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 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 to ensure traffic is prioritized appropriately.

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

```
interface GigabitEthernet1/0/1
 description Link to RS212-2911 Gig0/1
interface GigabitEthernet2/0/1
 description Link to RS212-2911-1 Gig0/2
!
interface range GigabitEthernet1/0/1, GigabitEthernet2/0/1
 switchport
 macro apply EgressQoS
 channel-group 1 mode on
 logging event link-status
 logging event trunk-status
 logging event bundle-status
```

Step 7: Configure EtherChannel trunk on the distribution layer switch.

An 802.1Q trunk is used which allows the router to provide the Layer 3 services to all the VLANs defined on the distribution layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the distribution layer switch. When using EtherChannel the interface type will be port-channel and the number must match the channel group configured in Step 3. DHCP Snooping and Address Resolution Protocol (ARP) inspection are set to trust.

```
interface Port-channel1
 description EtherChannel link to RS212-2911
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 50
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
 ip dhcp snooping trust
 no shutdown
```

The Catalyst 4500 does not require 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: Enable EIGRP-100 on the router.

Configure EIGRP-100 facing the distribution layer. In this design, all distribution-layer-facing subinterfaces and the loopback must be EIGRP interfaces. All other interfaces should remain passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address.

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 passive-interface default
 no passive-interface [interface]
 eigrp router-id [IP address of Loopback0]
 no auto-summary
```

Step 2: Redistribute EIGRP-300 (Layer 2 WAN) into EIGRP-100.

EIGRP-300 is already configured for the Layer 2 WAN interface. Routes from this EIGRP process are redistributed. Because the routing protocol is the same, no default metric is required.

```
router eigrp [as number]
redistribute eigrp [as number (Layer 2 WAN)]
```

Example

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 300
 passive-interface default
 no passive-interface Port-channel1.50
 eigrp router-id 10.255.255.212
 no auto-summary
```

Step 3: Enable EIGRP on distribution layer switch VLAN interface.

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 100
 no passive-interface Vlan50
```

Deploying WAN Quality of Service

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

Process

QoS Configuration

1. Create the QoS Maps to Classify Traffic
2. Implement the Queuing Policy
3. Configure Per-Site Shapers
4. Configure Physical Interface S&Q Policy
5. Apply WAN QoS Policy to Physical Interface

Procedure 1 Create the QoS Maps to Classify Traffic

Use the **class-map** command to define a traffic class and identify traffic to associate with the class name. These class names are used when configuring policy maps that define actions you want to take against the traffic type. The **class-map** command sets the match logic. In this case, the match-any keyword indicates that the maps match any of the specified criteria. This keyword is followed by the name you wish to assign to the class of service. After you have configured the **class-map** command, define specific values, such as DSCP and protocols to match with the **match** command. Use the following two forms of the **match** command: **match dscp** and **match protocol.**

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

Step 1: Create the class maps for DSCP matching.

Repeat this step to create a class-map for each of the six WAN classes of service listed in the following table.

You do not need to explicitly configure the default class.

```
class-map match-any [class-map name]
 match dscp [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	cs4, af41	23 (PQ)	—
CRITICAL-DATA	Highly interactive	af31, cs3	15	DSCP based
DATA	Data	af21	19	DSCP based
SCAVENGER	Scavenger	af11, cs1	5	—
NETWORK-CRITICAL	Routing protocols	cs6, cs2	3	—
default	Best effort	other	25	random

Example

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

Tech Tip

You do not need to configure a Best-Effort Class. This is implicitly included within class-default as shown in Procedure 5.

Tech Tip

The local router policy maps define seven classes while most service providers offer only six classes of service. The NETWORK-CRITICAL policy map is defined to ensure the correct classification, marking, and queuing of network-critical traffic on egress to the WAN. After the traffic has been transmitted to the service provider, the network-critical traffic is typically remapped by the service provider into the critical data class. Most providers perform this remapping by matching on DSCP values cs6 and cs2.

Procedure 2 Implement the Queuing Policy

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.

Option 1. Defining Per-Remote-Site Policy Maps

This procedure applies to the WAN aggregation Layer 2 WAN CE router only. This procedure will be repeated multiple times—once for each Layer 2 WAN connected remote site.

Step 1: Create a remote-site specific policy map for all Layer 2 WAN connected remote sites.

```
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. Note, when using a priority queue an implicit policer for this traffic type is applied.

```
priority percent [percentage]
```

Step 5: (Optional) Define the congestion mechanism.

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

Step 6: Repeat Step 2 through Step 5 for each class in Table 13, including class-default.

Option 1 Example (partial policy, showing sites 210 and 211)

```
policy-map POLICY-MAP-RS210
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
 class class-default
  bandwidth percent 25
  random-detect

policy-map POLICY-MAP-RS211
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
 class class-default
  bandwidth percent 25
  random-detect
```

Option 2. Defining Single Global Policy Map

This procedure applies to the remote-site WAN routers only.

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. Note, when using a priority queue an implicit policer for this traffic type is applied.

```
priority percent [percentage]
```

Step 5: (Optional) Define the congestion mechanism.

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

Step 6: Repeat Step 3 through Step 5 for each class in Table 13 including class-default.

Option 2 Example

```
policy-map WAN
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
 class class-default
  bandwidth percent 25
  random-detect
```

Tech Tip

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

Procedure 3 Configure Per-Site Shapers

This procedure applies to the WAN-aggregation Layer 2 WAN CE router only.

An additional set of shaping policies is applied at the child level to avoid traffic overruns that may occur if a service provider has smaller contracted rates for remote sites than the primary site. The shaping policies apply uniquely to each remote site depending on the destination network addresses and the contracted bandwidth rate for the remote site.

Step 1: Create an IP extended access list to match the destination network range for each remote site.

```
ip access-list extended [ACL name site 1]
 permit ip any [site 1 network] [site 1 inverse mask]
```

Step 2: Create a class map for each remote site. Associate the destination network access list with the class map.

```
class-map match-all [Class map name site 1]
 match access-group [ACL name site 1]
```

Step 3: Repeat steps 1-2 for each remote site.

Step 4: Create a child policy map to reserve bandwidth for NETWORK-CRITICAL traffic and enable traffic shaping to the remote sites.

```
policy-map [child policy-map-name]
 class [class-name]
  bandwidth percent [percentage]
```

Table 14 - Layer 2 WAN remote-site network and bandwidth parameters

Site	Network	Contracted rate (Mbps)
210	10.5.144.0/21	10
211	10.5.152.0/21	10
212	10.5.168.0/21	20
213	10.5.176.0/21	20

Step 5: Configure the shapers for each remote site using the parameters in Table 13.

```
class [class-name]
  shape  [average | peak] [bandwidth (kbps)]
```

Step 6: Apply the child service policy.

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

Step 7: Repeat steps 5 and 6 for each remote site.

Example

```
ip access-list extended RS210-10.5.144.0
 permit ip any 10.5.144.0 0.0.7.255
ip access-list extended RS212-10.5.168.0
 permit ip any 10.5.168.0 0.0.7.255
class-map match-all CLASS-MAP-RS210
 match access-group name RS210-10.5.144.0
class-map match-all CLASS-MAP-RS212
 match access-group name RS212-10.5.168.0
policy-map POLICY-MAP-L2-WAN-BACKBONE-WITH-PER-SITE-SHAPERS
 class NETWORK-CRITICAL
  bandwidth percent 3
 class CLASS-MAP-RS210
  shape average 10000000
  service-policy POLICY-MAP-RS210
 class CLASS-MAP-RS212
  shape average 20000000
  service-policy POLICY-MAP-RS212
```

Procedure 4 Configure Physical Interface S&Q Policy

With WAN interfaces using Ethernet as an access technology, the demarcation point between the enterprise and service provider may no longer have a physical-interface bandwidth constraint. Instead, a specified amount of access bandwidth is contracted with the service provider. To ensure the offered load to the service provider does not exceed the contracted rate that results in the carrier discarding traffic, you need to configure shaping needs 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 aggregation and all remote site WAN routers. This procedure may be repeated multiple times to support devices that have multiple WAN connections attached to different interfaces.

Step 1: Create the parent policy map.

As a best practice, embed the interface name within the name of the parent policy map.

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

Step 2: Configure the shaper.

```
class [class-name]
  shape  [average | peak] [bandwidth (kbps)]
```

Step 3: Apply the child service policy.

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

Example (WAN aggregation Layer 2 WAN CE Router)

This example shows a router with a 500-Mbps link on interface GigabitEthernet0/0/3 and a child shaper policy.

```
policy-map WAN-INTERFACE-G0/0/3
 class class-default
  shape average 500000000
 service-policy POLICY-MAP-L2-WAN-BACKBONE-WITH-PER-SITE-SHAPERS
```

Example (Remote-site CE Router)

This example shows a router with a 20-Mbps link on interface GigabitEthernet0/0.

```
policy-map WAN-INTERFACE-G0/0
class class-default
  shape average 20000000
 service-policy WAN
```

Procedure 5 Apply WAN QoS Policy to Physical Interface

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

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

Step 1: Select the WAN interface.

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

Step 2: Apply the WAN QoS policy.

The service policy needs to be applied in the outbound direction.

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

Example

```
interface GigabitEthernet0/0
 service-policy output WAN-INTERFACE-G0/0
```

Appendix A: Product List

WAN Aggregation

Functional Area	Product Description	Part Numbers	Software
WAN-aggregation Router	Aggregation Services 1002 Router	ASR1002-5G-VPN/K9	IOS-XE 15.2(2)S2 Advanced Enterprise license
	Aggregation Services 1001 Router	ASR1001-2.5G-VPNK9	

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.1(4)M5 securityk9 license datak9 license
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9	

LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) IP Base license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE IP Base license
	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	

Functional Area	Product Description	Part Numbers	Software
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(2)SE IP Base license
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-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	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(2)SE LAN Base license
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

LAN Distribution Layer

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

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We made changes to improve the readability and technical accuracy of this guide.
- We updated the code version for the Cisco ASR and ISR platforms.

Notes

Feedback

Please use the feedback form to send comments and suggestions about this guide.

SMART BUSINESS ARCHITECTURE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

B-0000235-1 1/13