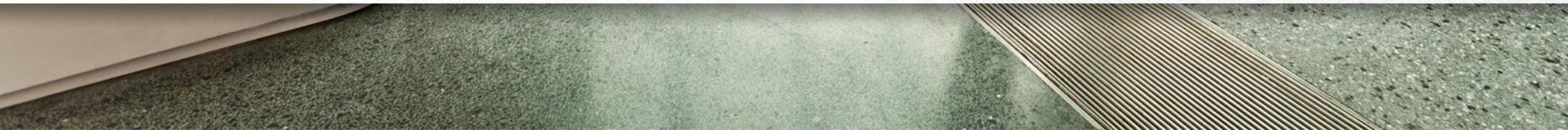
WAN Design Overview

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

Comments and Questions

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

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

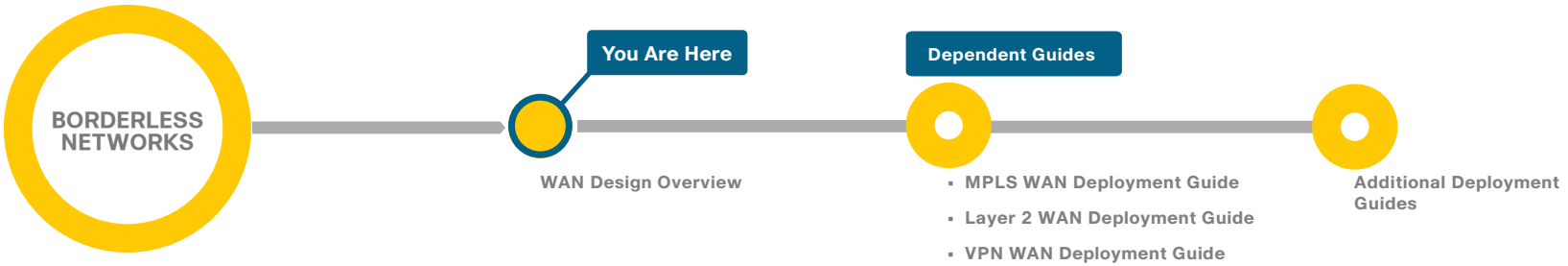
This *design overview* provides the following information:

- An introduction to a Cisco SBA design
- An explanation of the requirements that shaped the design
- A description of the benefits that the design will provide your organization

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

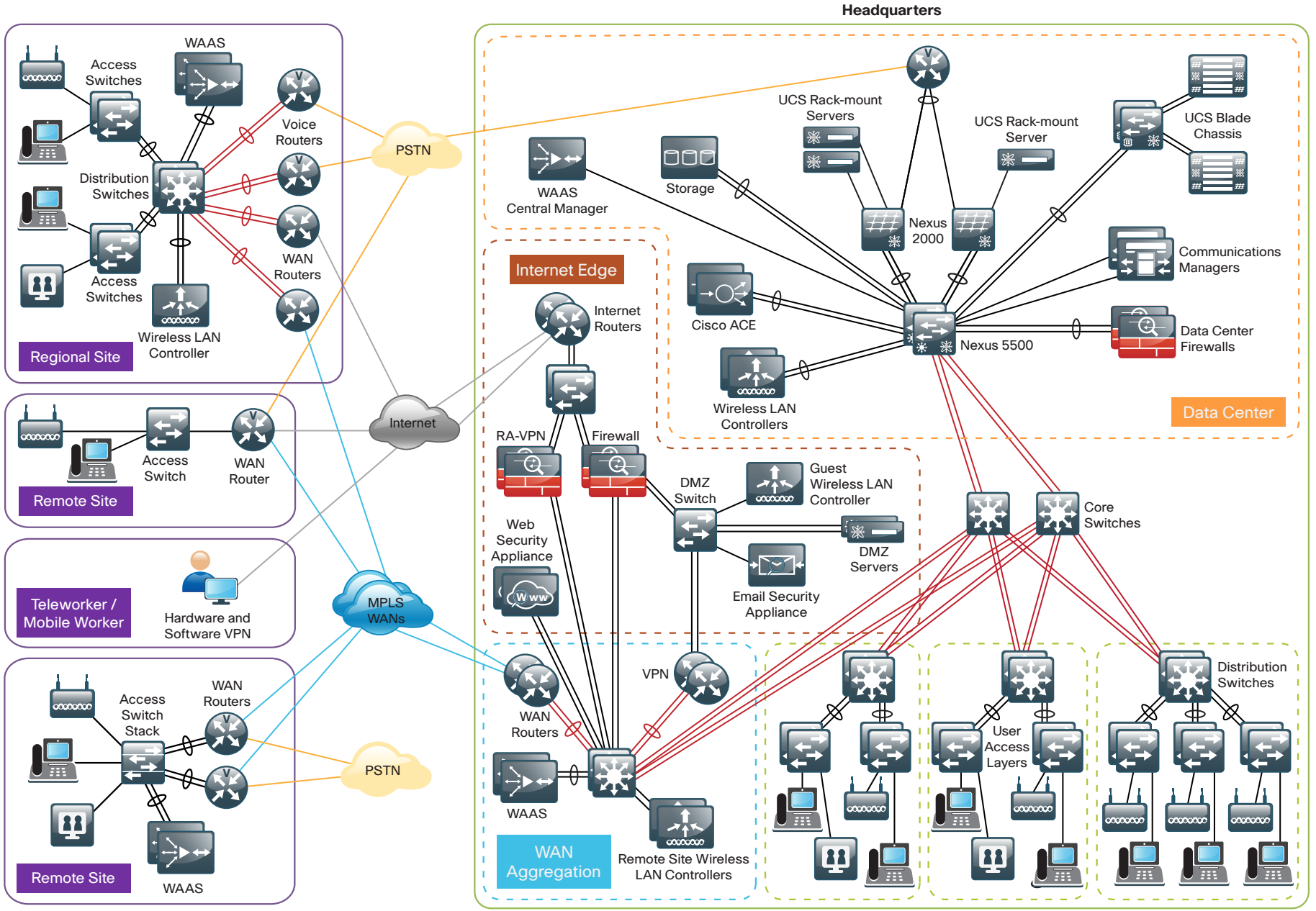
Cisco Smart Business Architecture (SBA) is a comprehensive design that incorporates LAN, WAN, security, application optimization, data center, and unified communications technologies to provide a complete solution for an organization's business challenges. The Cisco SBA—Borderless Network WAN architecture interconnects remote-site LANs to a primary site LAN or data center by using a variety of WAN technologies, including Multiprotocol Label Switching (MPLS), Layer 2 WAN, and VPN WAN over the Internet. Cisco SBA WAN is designed to support multiple resiliency options depending on the business requirements for the remote sites.

The WAN design methodology provides network access for remote sites with wired and wireless users, ranging from small remote sites with a few connected users to large sites with up to 5,000 connected users.

Cisco SBA WAN is the foundation for interconnecting remote sites to the primary sites or data centers, providing connectivity for users to the applications they require to do their job. The WAN plays a critical role in providing reliable and scalable interconnections to a broad range of remote sites.

Notes

Figure 1 - Cisco Smart Business Architecture overview



Cisco SBA tests network and user devices connected together to simulate an end-to-end deployment for your organization. This solution-level approach reduces the risk of interoperability problems between different technologies and components, allowing the customer to select the parts needed to solve a business problem. Where appropriate, the architecture provides multiple options based on network scalability or service-level requirements.

Cisco designed, built, and tested this architecture with the following goals:

- **Ease of deployment**—Organizations can deploy the solution consistently across all products included in the design. The reference configurations used in the deployment represent a best-practice methodology to enable a fast and resilient deployment.
- **Flexibility and scalability**—The architecture is modular so that organizations can select what they need when they need it, and it is designed to grow with the organization without requiring costly forklift upgrades.
- **Resiliency and security**—The design removes network borders in order to increase usability while protecting user traffic. It also keeps the network operational even during attacks or unplanned outages.
- **Ease of management**—Deployment and configuration guidance includes configuration examples of management by a network management system or by unique network element managers.
- **Advanced technology ready**—The network foundation allows easier implementation of advanced technologies such as collaboration.

Notes

Business Overview

Data networks are critical to an organization's viability and productivity. Online workforce-enablement tools are only beneficial if the data network provides reliable access to information resources. The number of users and locations in an organization can vary dramatically as an organization grows and adapts to changes in business activity. Providing a consistent user experience when users connect to the network increases their productivity. Whether users are sitting in an office at headquarters or working from a remote site, they require transparent access to the applications and files in order to perform their jobs.

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

To control operational costs, the WAN must support the convergence of voice, video, and data transport onto a single, centrally managed infrastructure. As organizations move into multinational or global business markets, they require a flexible network design that allows for country-specific access requirements without increased complexity.

The performance, reliable service level, and broad availability of carrier-provided MPLS networks and Layer 2 WAN networks makes these technologies 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 and to add additional sites or resilient links makes MPLS an effective WAN transport for growing organizations.

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.

Carrier-based MPLS and Layer 2 WAN services are not always available or cost-effective for an organization to use for WAN transport to support remote-site connectivity. Internet-based IP VPNs adequately provide the primary or backup network transport for a remote site. A flexible network architecture should include Internet VPN as a transport option without significantly increasing the complexity of the overall design. VPN for a WAN transport performs well for many applications even without explicit quality of service (QoS) assurance from the Internet service providers.

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

Internet IP VPN access can also be provided by using a cellular WAN technology. This offers a mobility option for deploying a remote site that is ideal for rapid deployment or for short term and temporary deployments. In many cases, cellular WAN is the only available option, due to the availability constraints of wired services in certain areas. The bandwidth available using cellular technologies continues to increase and performance compares favorably with wired WAN technologies when used at smaller remote sites.

As organizations consider new business requirements, such as providing video and collaboration applications to its employees, IT departments face challenges associated with supporting all the different applications in the same network. IT needs to manage applications that have very different characteristics and requirements from the network. The IT challenges are exacerbated if you consider shrinking budgets and increasing end-user quality expectations, as video becomes pervasive in their everyday lives out of the office. Cisco Medianet technologies help your organization minimize and deal with these challenges.

Why Is a Cohesive Approach to the Network Architecture a Value to Your Organization?

The days of conducting business with information stored locally in files on your computer are disappearing rapidly. The trend is for users to access mission-critical information by connecting to the network and downloading the information or by using a network-enabled application. Users depend

upon shared access to common secured storage, web-based applications, and even cloud-based services. Users may start their day at home, in the office, or from a coffee shop, expecting to log on to applications that they need in order to conduct business, update their calendar, or check email—all important tasks that support your business. Connecting to the network to do your work has become as fundamental as turning on a light switch to see your desk; it's expected to work. Taken a step further, the network becomes a means to continue to function whether you are at your desk, roaming over wireless LAN within the facility, or working at a remote site, and you still have the same access to your applications and information.

Now that networks are critical to the operation and innovation of organizations, workforce productivity enhancements are built on the expectation of nonstop access to communications and resources. As networks become more complex in order to meet the needs of any device, any connection type, and any location, networks incur an enhanced risk of downtime caused by poor design, complex configurations, increased maintenance, or hardware and software faults. At the same time, organizations seek ways to simplify operations, reduce costs, and improve their return on investment by exploiting their investments as quickly and efficiently as possible.

There are many ways an organization can benefit by deploying a Cisco SBA WAN architecture:

- Flexibility with multiple design models to address a variety of WAN technologies and resiliency options
- Increased reliability with multiple remote-site designs that provide for resiliency through the addition of WAN links and WAN routers, depending on business requirements
- Scalability provided by using a consistent method for remote-site LAN connectivity based on the Cisco SBA LAN architecture
- Reduced cost of deploying a standardized design based on Cisco-tested and supported best practices
- Summarized and simplified design choices so that IT workers with a CCNA certification or equivalent experience can deploy and operate the network
- 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

Using a modular approach to building your network with tested, interoperable designs allows you to reduce risks and operational issues and to increase deployment speed.

Notes

Cisco SBA WAN Architecture

There is a tendency to discount the network as just simple plumbing, to think that all you have to consider is the size and the length of the pipes or the speeds and feeds of the links, and to dismiss the rest as unimportant. Just as the plumbing in a large stadium or high rise has to be designed for scale, purpose, redundancy, protection from tampering or denial of operation, and the capacity to handle peak loads, the network requires similar consideration. As users depend on the network to access the majority of the information they need to do their jobs and to transport their voice or video with reliability, the network must be able to provide resilient, intelligent transport.

Many businesses have remote locations that depend entirely on applications hosted in a centralized data center. If a WAN outage occurs, these remote locations are essentially offline and they are unable to process transactions or support other types of business services. It is critical to provide reliable connectivity to these locations.

The demand for WAN bandwidth continues to increase and there has been a recent trend towards using Ethernet as the WAN access media to deliver higher bandwidth. Even with the increased amount of bandwidth available to connect remote sites today, there are performance-sensitive applications affected by jitter, delay, and packet loss. It is the function of the network foundation to provide an efficient, fault-tolerant transport that can differentiate application traffic to make intelligent load-sharing decisions when the network is temporarily congested. Regardless of the chosen WAN technology, the network must provide intelligent prioritization and queuing of traffic along the most efficient route possible.

The Cisco SBA WAN design uses a variety of WAN transport technologies for primary links and backup links:

- MPLS WAN using Layer 3 VPN
- Layer 2 WAN as implemented using Virtual Private LAN Services (VPLS) or Metro Ethernet
- Internet with VPN WAN
- Internet 3G/4G with VPN WAN

This guide provides a high level overview of each technology followed by a discussion of the usage of each technology at the WAN-aggregation site and remote sites. This guide should also be used as a roadmap on how to use the companion WAN deployment guides.

WAN Transport Technologies

MPLS WAN

MPLS enables organizations and service providers to build next-generation intelligent networks that deliver a wide variety of advanced, value-added services like QoS and service level agreements (SLAs) over a single infrastructure. You can integrate this economical solution seamlessly over any existing infrastructure, such as IP, Frame Relay, ATM, or Ethernet.

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

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

The *MPLS WAN Deployment Guide* provides details on how to use MPLS VPN as a primary WAN transport or as a backup WAN transport (to an alternate MPLS VPN primary).

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, Point-to-Point Protocol (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 VPLS. The providers 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 a subscriber model in which the service provider is transparent and the organization 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 to provide transport of multiple VLANs on a single access trunk. Service providers often refer to a trunked service as *Q-in-Q tunneling (QinQ)*.

Layer 2 WAN transport is transparent to the traffic type, therefore IP multicast traffic is supported with no additional configuration required by the service provider.

The *Layer 2 WAN Deployment Guide* provides details on how to use Layer 2 WAN as a primary WAN transport.

Internet as WAN Transport

The Internet is essentially a large-scale public WAN composed of multiple interconnected service providers. The Internet can provide reliable high-performance connectivity between various locations, although it lacks any explicit guarantees for these connections. Despite its "best effort" nature, the Internet is a reasonable choice for a primary transport when it is not feasible to connect with another transport option. Additional resiliency for primary WAN transports like MPLS or Layer 2 WAN is provided by using the Internet as an alternate transport option.

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

The *VPN WAN Deployment Guide* provides details on how to use the Internet for VPN site-to-site connections as both a primary WAN transport and as a backup WAN transport (to a primary WAN transport).

Dynamic Multipoint VPN

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

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

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

Cellular Options for Remote Site Connectivity

Cellular connectivity enables the use of Internet WAN, without requiring any wired infrastructure or circuits and provides a flexible, high-speed, high-bandwidth option. There are two competing 3G technologies that provide high-bandwidth network WAN connectivity where cellular is the only option: Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM). Much of the world can select only one or the other of the CDMA and GSM options. There are now higher-speed 4G technology options based on Long Term Evolution (LTE) and WiMAX.

The *VPN Remote Site over 3G/4G WAN Deployment Guide* provides details on how to use a cellular connection to the Internet for VPN site-to-site connections as both a primary WAN transport and as a backup WAN transport (to a primary WAN transport).

WAN Transport Technology Summary

The Cisco SBA design allows for the use of any and all of the listed WAN transport technologies, which enables the network architect to choose the most appropriate technology based on their business requirements. In some cases, service providers are limited in their coverage, or there is a large cost differential between technologies—Cisco SBA allows the flexibility to consider multiple options. The primary benefit is that decisions can be made based on what is important to the organization.

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 works well only for applications that adapt gracefully to variations in latency, jitter, and loss. However, networks are multiservice by design and support real-time voice and video as well as data traffic. The difference is that real-time applications require packets to be delivered within specified loss, delay, and jitter parameters.

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

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

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

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

WAN-Aggregation Design Models

The Cisco SBA WAN design does not take a "one size fits all" approach. Cisco developed a set of WAN design models based on scaling requirements and other considerations including resiliency, the need for future growth, regional availability of WAN services, and ease of operation. Cisco also designed and tested the complete Cisco SBA WAN to accommodate the use of multiple concurrent design models, but also to support the usage of individual design models.

The approach to platform selection is straightforward. You determine which models of router to use by the amount of bandwidth required at the WAN-aggregation site. You determine whether to implement a single router or dual router by the number of carriers and WAN transports that are required in order to provide connections to all of the remote sites.

This guide covers nine design models, detailed in the following section:

- MPLS Static
- MPLS Dynamic
- Dual MPLS
- Layer 2 Simple Demarcation
- Layer 2 Trunked Demarcation
- DMVPN Only
- Dual DMVPN
- DMVPN Backup Shared
- DMVPN Backup Dedicated

MPLS WAN Design Models

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

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

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

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

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

Each MPLS carrier terminates to a dedicated WAN router with a primary goal of eliminating any single points of failure. The various design models are contrasted in Table 1.

Table 1 - WAN-aggregation design models

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

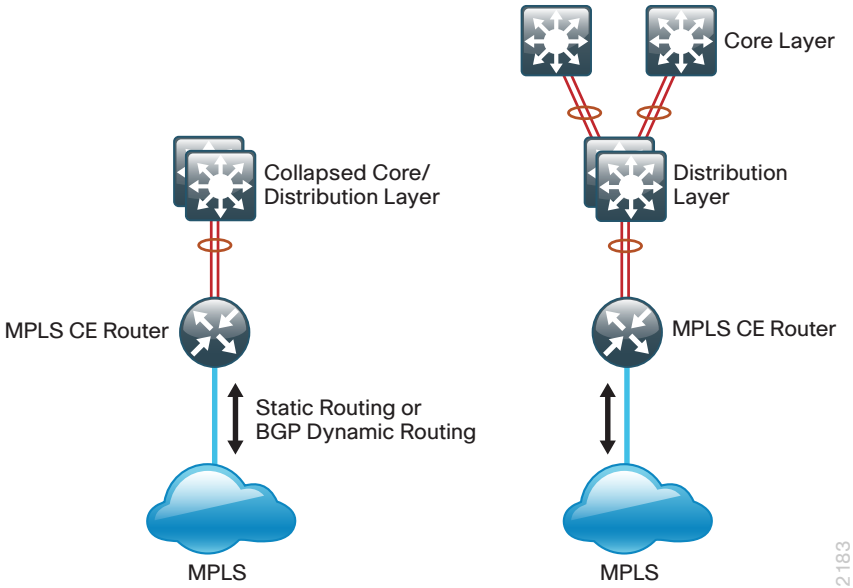
The characteristics of each design are as follows.

MPLS Static Design Model

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

The MPLS Static design model is shown in the following figure.

Figure 2 - MPLS Static and MPLS Dynamic design models (single MPLS carrier)



MPLS Dynamic Design Model

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

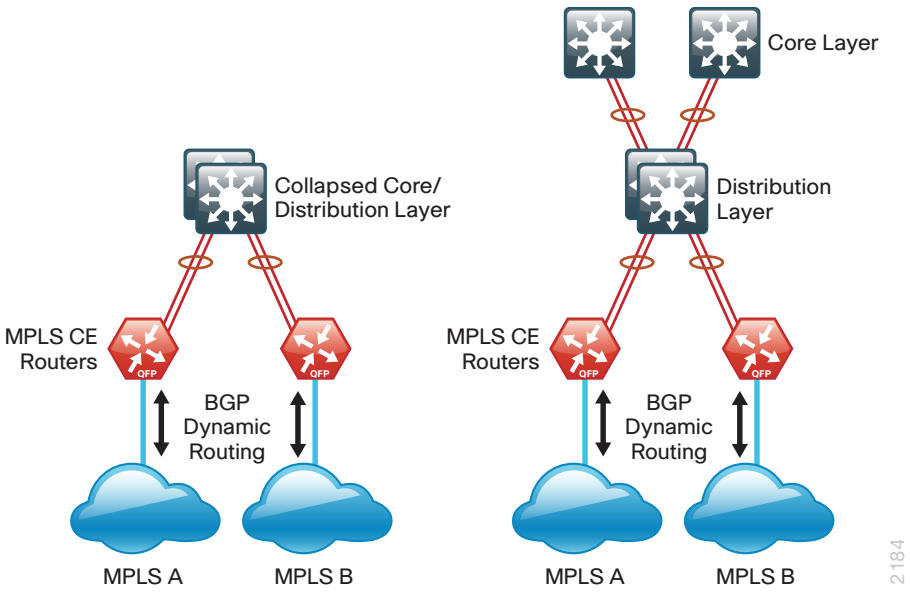
The MPLS Dynamic design model is shown in Figure 2.

Dual MPLS Design Model

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

The Dual MPLS design model is shown in the following figure.

Figure 3 - Dual MPLS design model



Layer 2 WAN Design Models

The Layer 2 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 CE router. The WAN edge router connects into a distribution layer.

This design guide documents two Layer 2 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 uses LAN connections into either a collapsed core/distribution layer or a dedicated WAN distribution layer. There are no functional differences between these two methods from the WAN-aggregation perspective.

In 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 such as application optimization and encryption, 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 2 - WAN-aggregation design models

	Layer 2 Simple Demarcation	Layer 2 Trunked Demarcation
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

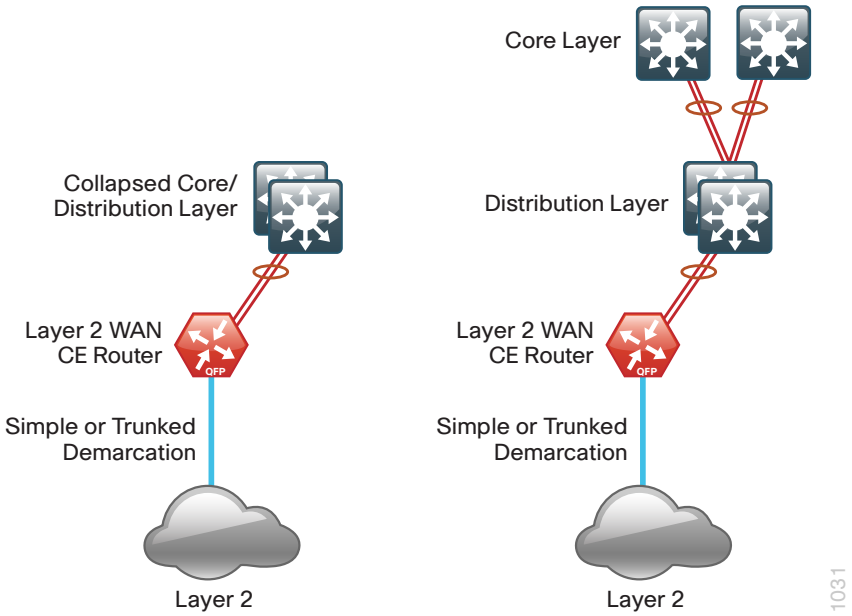
The characteristics of each design are as follows.

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 4 - 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 4.

VPN WAN Design Models

The VPN WAN-aggregation (hub) designs include either one or two WAN edge routers. WAN edge routers that terminate VPN traffic are referred to as VPN hub routers. All of the WAN edge routers connect into a LAN distribution layer.

The WAN transport options include traditional Internet access used as either a primary transport or as a secondary transport when the primary transport is MPLS VPN, Layer 2 WAN or Internet. Single or dual carrier Internet access links connect to a VPN hub router or VPN hub router pair, respectively. A similar method of connection and configuration is used for both.

There are multiple WAN-aggregation design models that are documented in this design guide. The DMVPN Only design model uses only Internet VPN as transport. The Dual DMVPN design model uses Internet VPN as both a primary and secondary transport, using dual Internet service providers. Additionally, the DMVPN Backup design models use Internet VPN as a backup to an existing primary MPLS WAN or Layer 2 WAN transport.

The primary difference between the DMVPN backup designs is whether the VPN hub is implemented on an existing MPLS CE router, which is referred to as DMVPN Backup Shared, or the VPN hub is implemented on a dedicated VPN hub router, which is referred to as DMVPN Backup Dedicated.

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

The various design models are contrasted in Table 3 and Table 4.

Table 3 - Design models using only VPN transport

	DMVPN Only	Dual DMVPN
Remote sites	Up to 100	Up to 500
WAN links	Single	Dual
DMVPN hubs	Single	Dual
Transport 1	Internet VPN	Internet VPN
Transport 2	—	Internet VPN

Table 4 - Design models using VPN transport as backup

	DMVPN Backup Shared	DMVPN Backup Dedicated
Remote sites	Up to 50	Up to 100/500
WAN links	Dual	Multiple
DMVPN hubs	Single (shared with MPLS CE)	Single/Dual
Transport 1 (existing)	MPLS VPN A	MPLS VPN A
Transport 2 (existing)	—	MPLS VPN B
Transport 3 (existing)	—	MetroE/VPLS
Backup transport	Internet VPN	Internet VPN

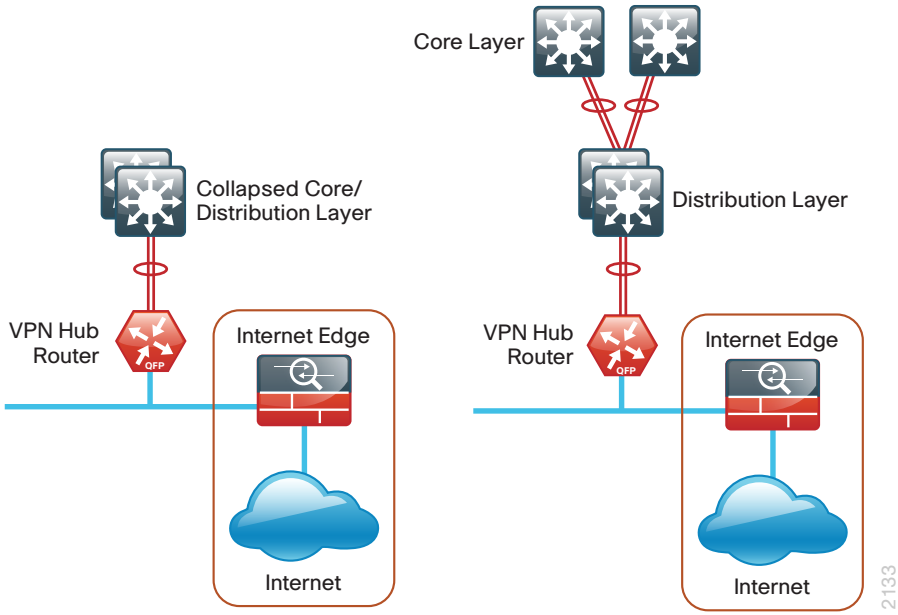
The characteristics of each design are as follows:

DMVPN Only Design Model

- Supports up to 100 remote sites
- Uses a single Internet link

The DMVPN Only design is shown in the following figure.

Figure 5 - DMVPN Only design model

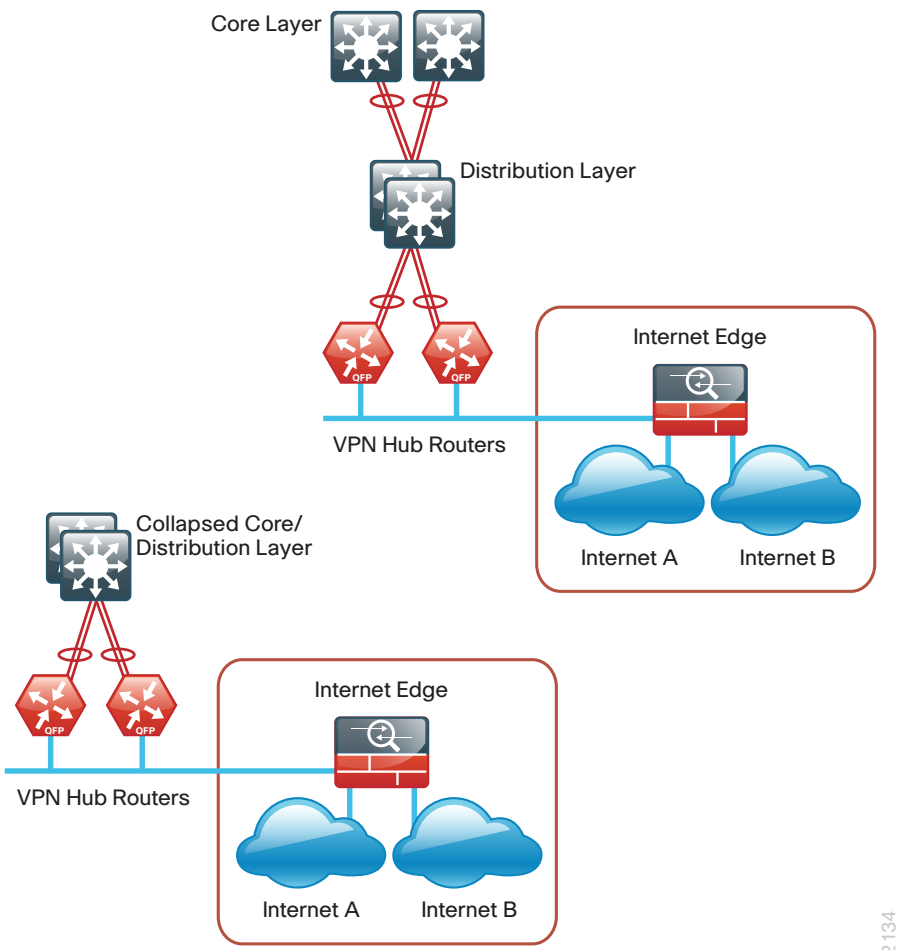


Dual DMVPN Design Model

- Supports up to 500 remote sites
- Uses dual Internet links
- Typically used with a dedicated WAN distribution layer

The Dual DMVPN design is shown in the following figure.

Figure 6 - Dual DMVPN design model



In both the DMVPN Only and Dual DMVPN design models, the DMVPN hub routers connect to the Internet indirectly through a firewall demilitarized zone (DMZ) interface contained within the Internet edge. For details about the connection to the Internet, see the *Firewall and IPS Deployment Guide*. The VPN hub routers are connected into the firewall DMZ interface, rather than connected directly with Internet service-provider routers.

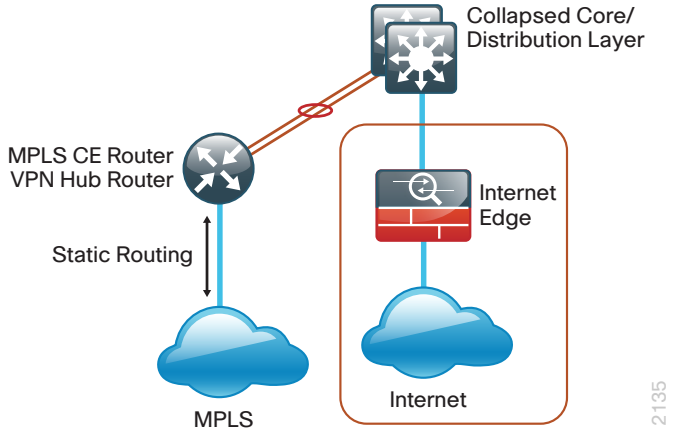
DMVPN Backup Shared Design Model

The DMVPN Backup Shared design model is intended for use by an organization that has already adopted the MPLS Static design model, and is not using BGP dynamic routing with their MPLS VPN carrier.

- Supports up to 50 remote sites
- Uses the same router for MPLS CE and VPN hub
- Has a single MPLS VPN carrier
- Uses static routing with MPLS VPN carrier
- Uses a single Internet link

The DMVPN Backup Shared design is shown in the following figure.

Figure 7 - DMVPN Backup Shared design model



In the DMVPN Backup Shared design model, the DMVPN hub router is also the MPLS CE router, which is already connected to the distribution or core layer. The connection to the Internet has already been established through a firewall interface contained within the Internet edge. A DMZ is not required for this design model. For details about the connection to the Internet, see the *Firewall and IPS Deployment Guide*.

DMVPN Backup Dedicated Design Model

- Supports up to 500 remote sites
- Has a single or dual MPLS VPN carriers or a single Layer 2 WAN
- Uses BGP routing with MPLS VPN carrier, or EIGRP routing within the Layer 2 WAN
- Uses a single Internet link

The variants of the DMVPN Backup Dedicated design are shown in the following figures.

Figure 8 - DMVPN Backup Dedicated design model for MPLS WAN

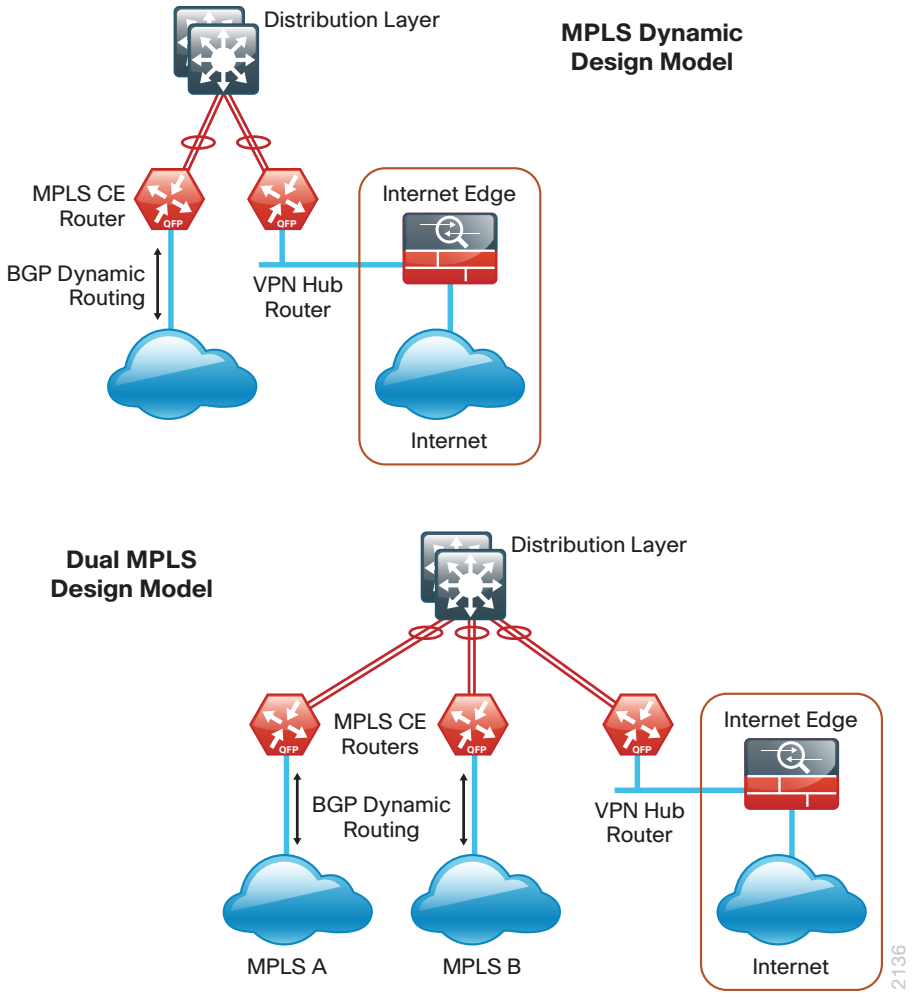
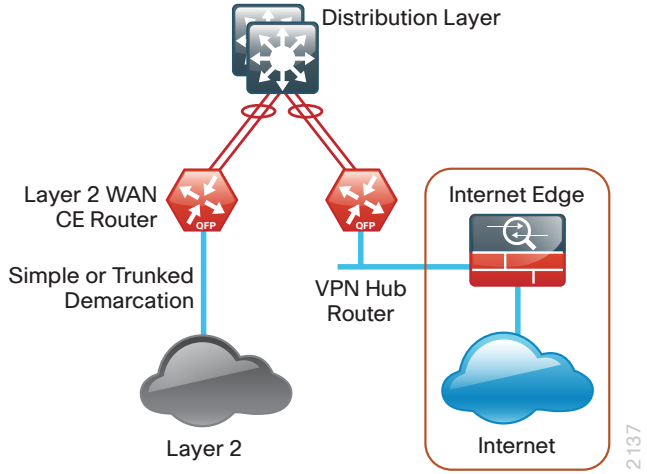


Figure 9 - DMVPN Backup Dedicated design model for Layer 2 WAN primary



In the DMVPN Backup Dedicated design models, the DMVPN hub routers connect to the Internet indirectly through a firewall DMZ interface contained within the Internet edge. For details about the connection to the Internet, see the *Firewall and IPS Deployment Guide*. The VPN hub routers are connected into the firewall DMZ interface, rather than connected directly with Internet service-provider routers.

Note that the DMVPN Only and Dual DMVPN design models can also provide DMVPN backup when paired with MPLS WAN and Layer 2 WAN design models.

WAN-aggregation Design Model Summary

The available design models can be grouped together in a number of ways to provide connectivity to the required numbers and types of remote sites. All design models provide a high level of performance and services. To illustrate the wide range of scale that Cisco SBA WAN provides you can compare two combinations of design models.

The following figures show Cisco SBA WAN implemented using the lowest and highest scaling design models.

Figure 10 - SBA-WAN (lowest scale)- MPLS Static + DMVPN Backup Shared

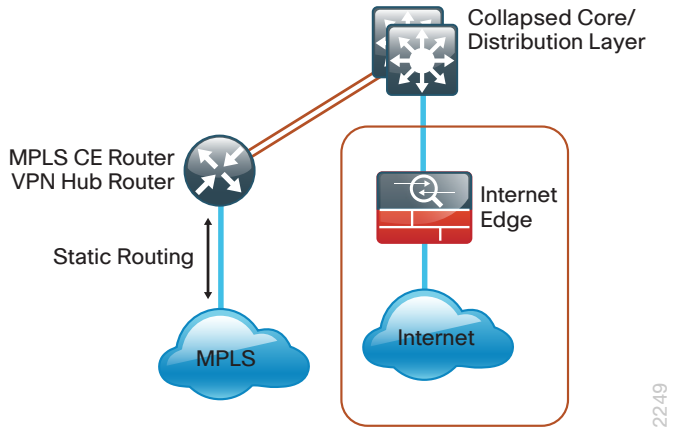
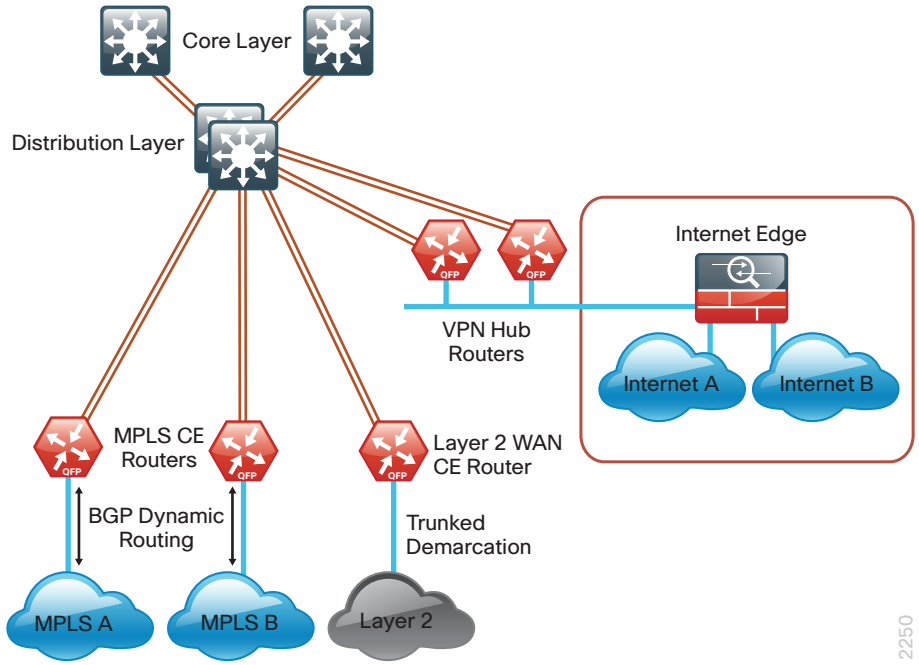


Figure 11 - SBA WAN (highest scale)- Dual MPLS + Layer 2 Trunked + Dual DMVPN



WAN Remote-Site Designs

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

Most remote sites are designed with a single-router WAN edge; however, certain remote-site types require a dual-router WAN edge. Dual-router candidate sites include regional office or remote campus locations with large user populations, or sites with business critical needs that justify additional redundancy to remove single points of failure. Similarly, the size of the remote-site LAN depends on factors such as number of connected users and the physical layout of the remote site.

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.

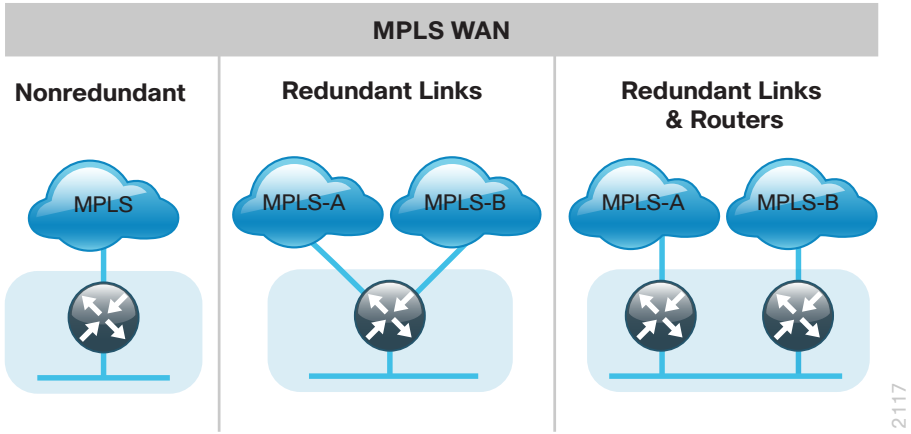
This guide covers fourteen remote-site designs detailed in the following section:

- MPLS WAN Non Redundant
- MPLS WAN with Redundant Link
- MPLS WAN with Redundant Link and Router
- Layer 2 WAN Non Redundant
- VPN WAN Non Redundant
- VPN WAN with Redundant Link
- VPN WAN with Redundant Link and Router
- MPLS WAN with VPN WAN Backup Link
- MPLS WAN with VPN WAN Backup Link and Router
- Layer 2 WAN with VPN WAN Backup Link
- Layer 2 WAN with VPN WAN Backup Link and Router
- VPN WAN (3G/4G) Non Redundant
- MPLS WAN with VPN WAN (3G/4G) Backup Link
- MPLS WAN with VPN WAN (3G/4G) Backup Link and Router

MPLS WAN Connected Remote Sites

The three variants of a MPLS connected remote site are shown in Figure 12. The non-redundant variant is the only one that is compatible with the single carrier design models (MPLS Static or MPLS Dynamic). The redundant variants are compatible with the Dual MPLS design model. If you have implemented the Dual MPLS design model, you may also connect a non-redundant remote site to either carrier.

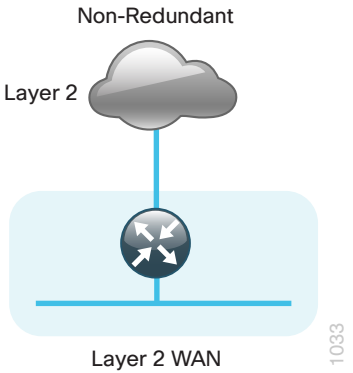
Figure 12 - MPLS WAN remote-site designs



Layer 2 WAN Connected Remote Sites

The Layer 2 WAN connected remote site is shown in Figure 13. This design is compatible with both the Simple Demarcation and Trunked Demarcation design models.

Figure 13 - Layer 2 WAN remote-site design

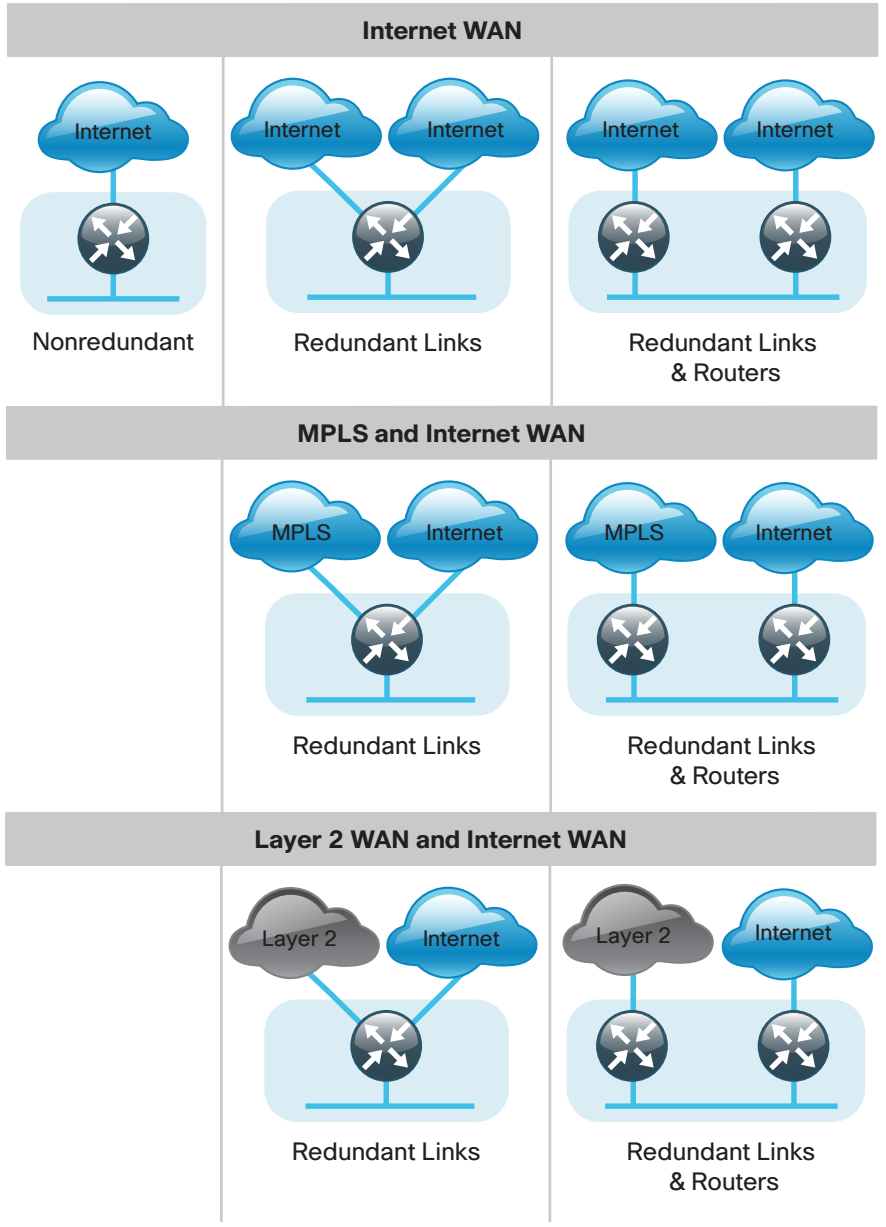


VPN WAN Connected Remote Sites

The multiple variants of a VPN WAN connected remote site are shown in Figure 14. The Internet WAN non-redundant variant is compatible with the DMVPN only and Dual DMVPN design models. Both of the Internet WAN redundant link variants are compatible with the Dual DMVPN design model.

The MPLS + Internet WAN single router (redundant links) variant is compatible with either the DMVPN Backup Dedicated or DMVPN Backup Shared design models. The MPLS + Internet WAN dual router (redundant links and routers) and both Layer 2 WAN + Internet WAN variants are compatible with the DMVPN Backup Dedicated design model.

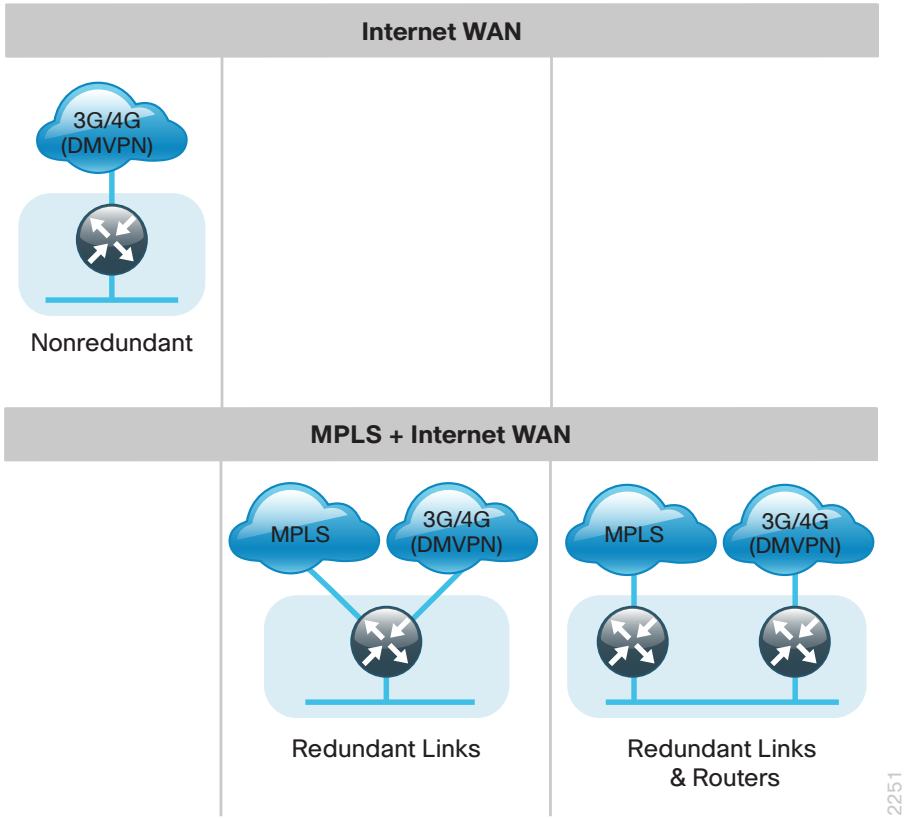
Figure 14 - VPN WAN remote-site designs



3G/4G VPN WAN Connected Remote Sites

The multiple variants of a 3G/4G VPN WAN connected remote site are shown in Figure 15. The Internet WAN non-redundant variant is compatible with the DMVPN only and Dual DMVPN design models. The MPLS + Internet WAN single router (redundant links) variant is compatible with the DMVPN Backup Dedicated or DMVPN Backup Shared design models. The MPLS + Internet WAN dual router (redundant links and routers) is compatible with the DMVPN Backup Dedicated design model.

Figure 15 - 3G/4G VPN WAN remote-site designs



Notes

WAN Remote Site Designs Summary

The general topology used for the various remote sites is essentially the same regardless of the chosen WAN transport. The differences are apparent once you begin the deployment and configuration of the WAN routers.

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.

Table 5 - WAN remote-site transport options

WAN remote- site routers	WAN transports	Primary transport	Secondary transport	WAN-Aggregation design model (primary)	WAN-Aggregation design model (secondary)
Single	Single	MPLS VPN	—	MPLS Static MPLS Dynamic Dual MPLS	—
Single	Single	MetroE/VPLS	—	Layer 2 Simple Layer 2 Trunked	—
Single	Single	Internet	—	DMVPN Only Dual DMVPN	—
Single	Single	Internet 3G/4G	—	DMVPN Only Dual DMVPN	—
Single	Dual	MPLS VPN A	MPLS VPN B	Dual MPLS	Dual MPLS
Single	Dual	MPLS VPN	Internet	MPLS Static MPLS Dynamic Dual MPLS	DMVPN Backup Shared DMVPN Backup Dedicated
Single	Dual	MPLS VPN	Internet 3G/4G	MPLS Static MPLS Dynamic Dual MPLS	DMVPN Backup Shared DMVPN Backup Dedicated
Single	Dual	MetroE/VPLS	Internet	Layer 2 Simple Layer 2 Trunked	DMVPN Backup Dedicated
Single	Dual	Internet	Internet	Dual DMVPN	Dual DMVPN
Dual	Dual	MPLS VPN A	MPLS VPN B	Dual MPLS	Dual MPLS
Dual	Dual	MPLS VPN	Internet	MPLS Dynamic Dual MPLS	DMVPN Backup Dedicated
Dual	Dual	MPLS VPN	Internet 3G/4G	MPLS Dynamic Dual MPLS	DMVPN Backup Dedicated
Dual	Dual	MetroE/VPLS	Internet	Layer 2 Simple Layer 2 Trunked	DMVPN Backup Dedicated
Dual	Dual	Internet	Internet	Dual DMVPN	Dual DMVPN

Remote Site 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 6 - WAN remote-site LAN options

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

WAN Remotes Sites—LAN Topology

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

Table 7 - WAN remote sites—VLAN assignment

VLAN	Usage	Layer 2 access	Layer 3 distribution/ access
VLAN 64	Data 1	Yes	—
VLAN 69	Voice 1	Yes	—
VLAN 99	Transit	Yes (dual router only)	Yes (dual router only)
VLAN 50	Router Link (1)	—	Yes
VLAN 54	Router Link (2)	—	Yes (dual router only)

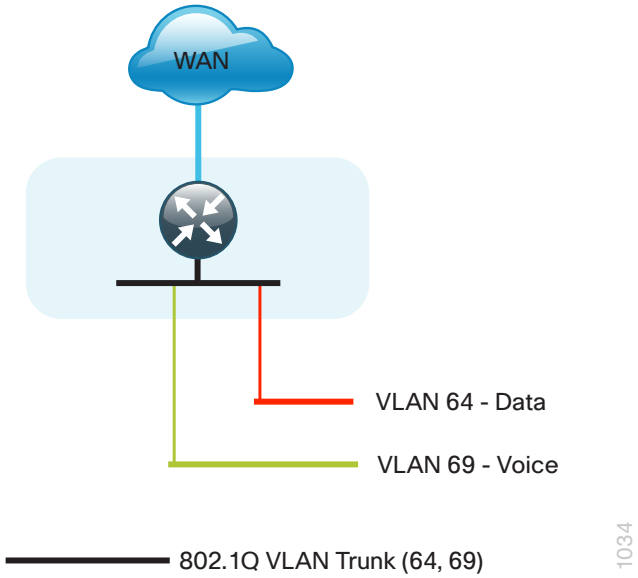
Layer 2 Access

WAN remote sites that do not require additional LAN distribution layer routing devices are considered to be flat or, from a LAN perspective, they are considered unrouted Layer 2 sites. The attached WAN routers provide all Layer 3 services. The access switches, through the use of multiple VLANs, can support services such as data and voice. The design shown in Figure 16 illustrates the standardized VLAN assignment scheme. The benefits of this design are clear: you can configure all of the access switches 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 allocates only 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.) You must configure the connection between the router and the access switch 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.

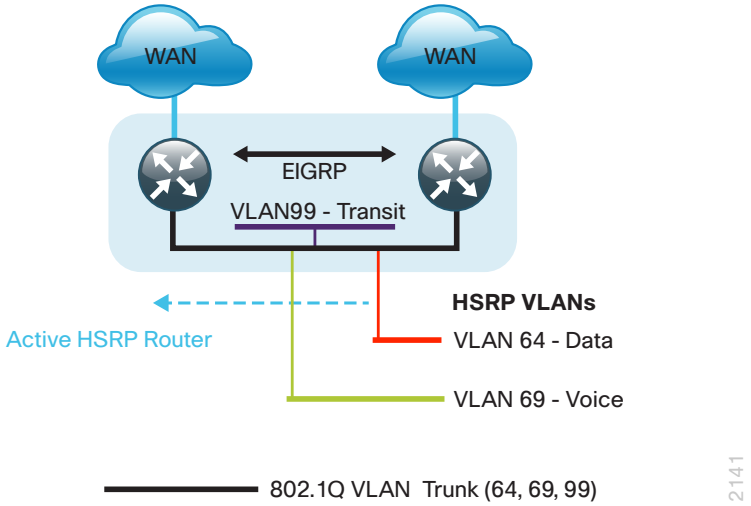
Figure 16 - WAN remote site—Flat Layer 2 LAN (single router)



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

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

Figure 17 - WAN remote site—Flat Layer 2 LAN (dual router)

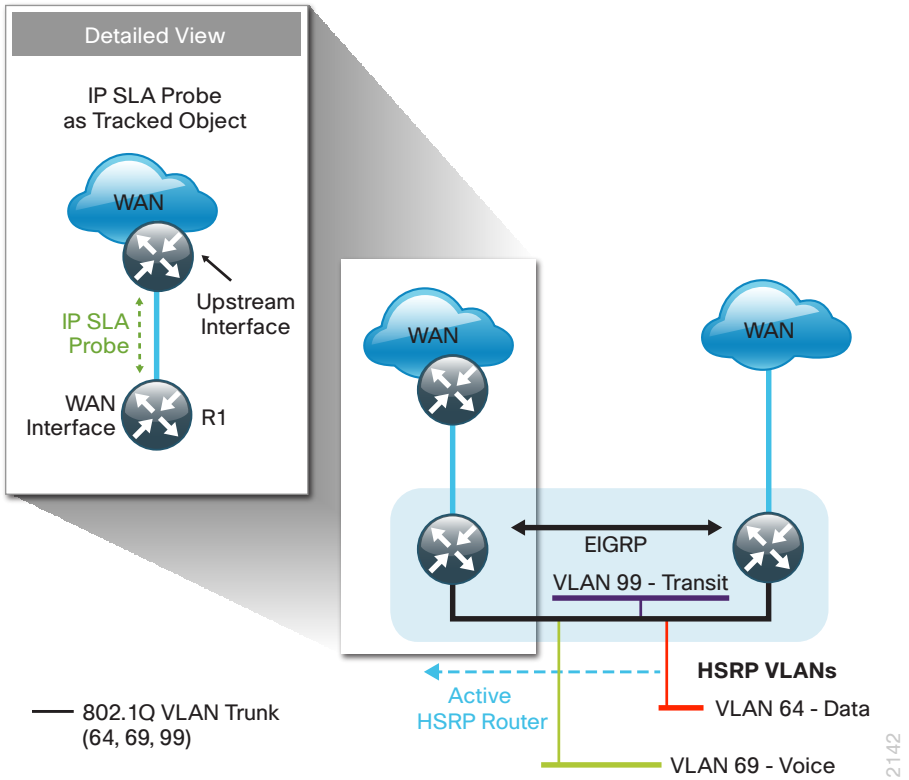


Enhanced Object Tracking (EOT) provides a consistent methodology for various router and switching features to conditionally modify their operation based on information objects available within other processes. The objects that can be tracked include interface line protocol, IP route reachability, and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

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

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

Figure 18 - WAN remote site—IP SLA probe to verify upstream device reachability



HSRP is configured to be active on the router with the highest priority WAN transport. EOT of IP SLA probes is implemented in conjunction with HSRP so that in the case of WAN transport failure, the standby HSRP router associated with the lower priority (alternate) WAN transport becomes the active HSRP router. The IP SLA probes are sent from the remote-site primary WAN router to the upstream neighbor (MPLS PE, Layer 2 WAN CE, or DMVPN hub) to ensure reachability of the next hop router. This is more effective than simply monitoring the status of the WAN interface.

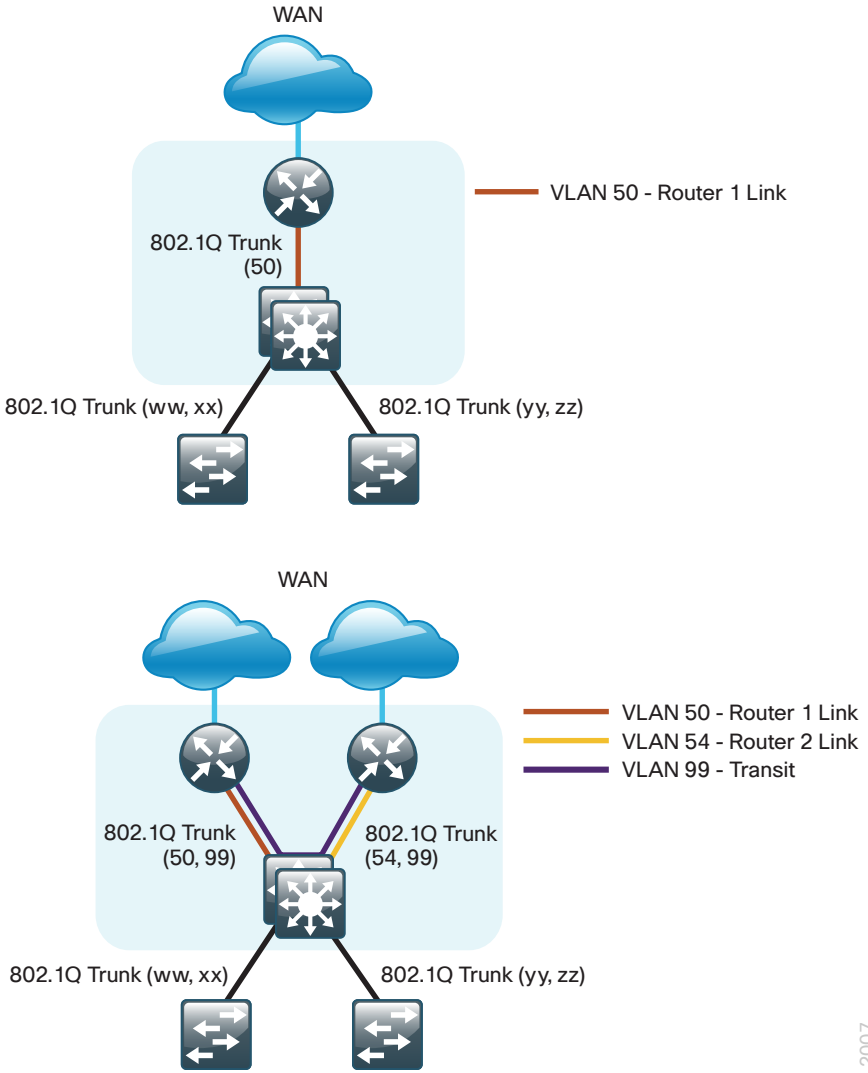
The dual-router designs also warrant an additional transit network component that is required for proper routing in certain scenarios. In these cases, a traffic flow from a remote-site host might be sent to a destination reachable via the alternate WAN transport (for example, a dual MPLS remote site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

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

Distribution and Access Layer

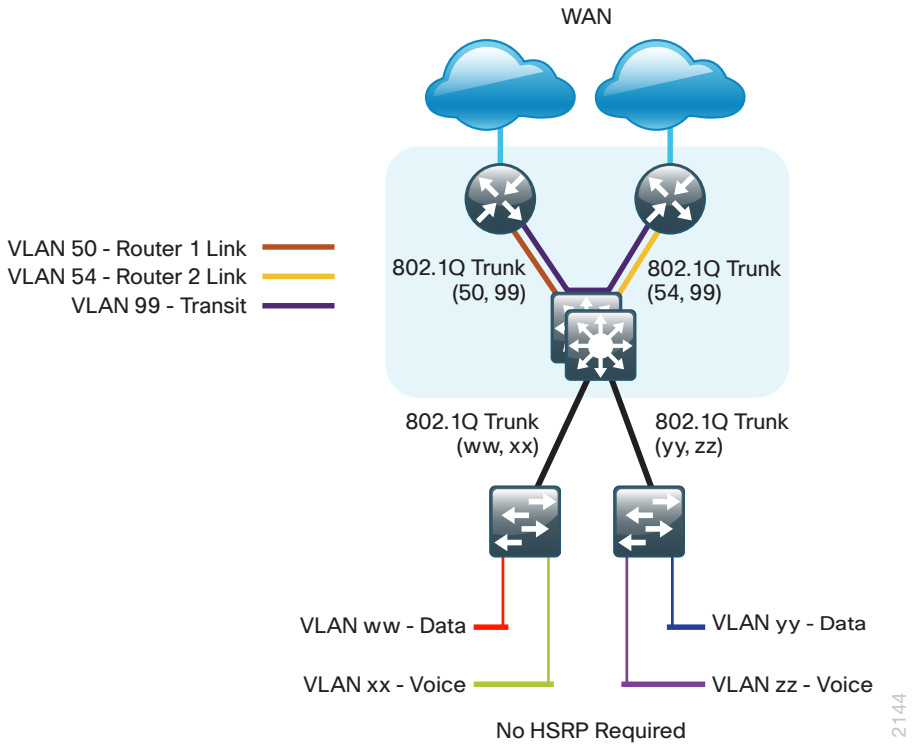
Large remote sites may require a LAN environment similar to that of a small campus LAN that includes a distribution layer and access layer. This topology works well with either a single- or dual-router WAN edge. To implement this design, the routers should connect via EtherChannel links to the distribution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

Figure 19 - WAN remote site—Connection to distribution layer



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

Figure 20 - WAN remote site—Distribution and access layer (dual router)



Summary

The flow of information is a critical component of how well an organization runs. Organizations struggle with the ability to combine data, voice, and video on a single robust network and with the ability to deploy, operate, troubleshoot, and manage complexity and costs.

The Cisco SBA—Borderless Networks WAN architecture provides a prescriptive solution, based on best practices and tested topologies, to accommodate your organization's requirements. The Cisco SBA WAN architecture provides a consistent set of features and functionality for network access whether the users are located at a primary site, a remote campus location, or a smaller remote site, to improve user satisfaction and productivity and reduce operational expense.

The Cisco SBA WAN architecture provides a consistent and scalable methodology for building your WAN, improving overall usable network bandwidth and resilience, and making the network easier to deploy, maintain, and troubleshoot.

The companion Cisco SBA WAN deployment and configuration guides provide step-by-step guidance for deploying the solution. To enhance the Cisco SBA WAN architecture, there are a number of supplemental guides that address specific functions, technologies, or features that may be important to solving your business problems.

Deploying Cisco Smart Business Architecture for your network helps ensure a reliable, robust, and secure network infrastructure to carry the flow of information vital to your organization's success.

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-0000340-1 1/13