CISCO VALIDATED DESIGN

Traditional WAN Design Summary

March 2017

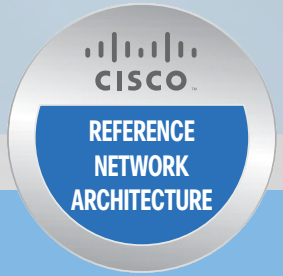


Table of Contents

WAN Strategy

This guide provides a high-level overview of several wide-area network (WAN) technologies, followed by a discussion of the usage of each technology at the WAN-aggregation site and remote sites. The intended audience is a technical decision maker who wants to compare Cisco's WAN offerings and learn more about the best practices for each technology. This guide should be used as a roadmap on how to use the companion traditional WAN deployment guides.

Reader Tip

For more information about deploying the traditional WAN topologies, see Design Zone for Branch WAN.

The days of conducting business with information stored locally 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 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 local-area network (WLAN) 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.

The Cisco Visual Networking Index (VNI) is an ongoing effort to forecast and analyze the growth and use of IP networks worldwide. The Global Mobile Data Traffic Forecast highlights the following predictions by 2019:

- There will be 5.2 billion global mobile users, up from 4.3 billion in 2014.
- There will be 11.5 billion mobile-ready devices and connections, more than 4 billion more than there were in 2014.
- The average mobile connection speed will increase 2.4-fold, from 1.7 Mbps in 2014 to 4.0 Mbps by 2019.
- Global mobile IP traffic will reach an annual run rate of 292 exabytes, up from 30 exabytes in 2014.

With increasing mobile traffic from employee devices, an organization must plan for expanded WAN bandwidth at remote sites and larger router platforms to accommodate the higher capacity links.

The enterprise series of Cisco Validated Designs (CVDs) incorporates local area network (LAN), WLAN, wide area network (WAN), security, data center, and unified communications technologies in order to provide a complete solution for an organization's business challenges.

There are many ways an organization can benefit by deploying a CVD enterprise WAN architecture:

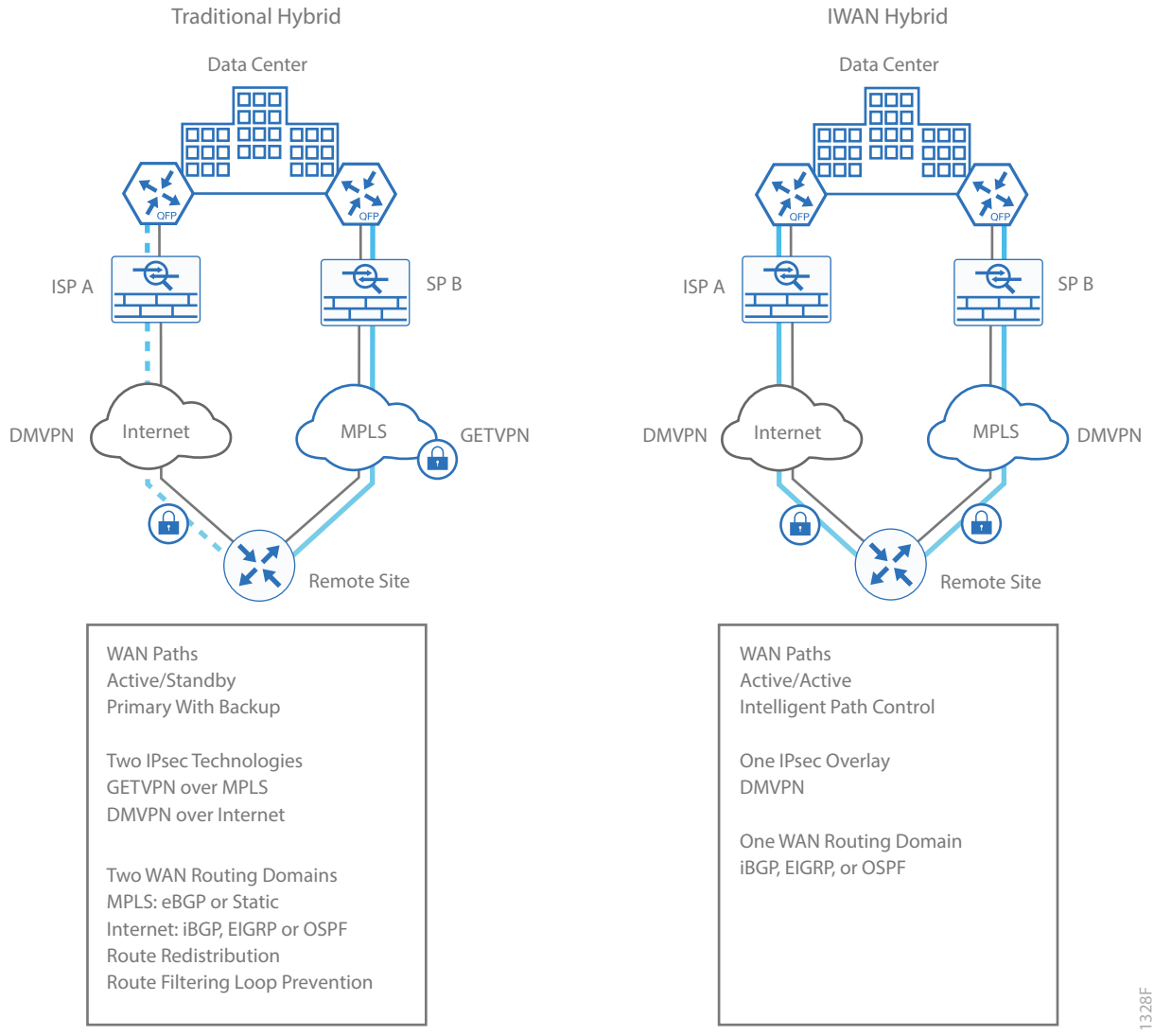
- Flexibility with multiple design models in order to address a variety of WAN technologies and resiliency options
- Increased reliability with multiple remote-site designs that provide for resiliency through the addition of WAN links and WAN routers, depending on business requirements
- Scalability provided by using a consistent method for remote-site LAN connectivity based on the CVD enterprise campus 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

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.

Hybrid WAN Designs: IWAN vs Traditional WAN

Hybrid WAN designs are becoming increasing popular because they allow an organization to choose the best transport options for their particular situation. Your organization can spend money on multiprotocol label switching (MPLS) services when the business needs require it. You can use Internet services when more bandwidth is needed for larger data transport requirements. There are some key differences between Intelligent WAN (IWAN) and traditional WAN hybrid designs, which are highlighted in the figure below.

Figure 1 *Hybrid WAN designs*



The IWAN design provides an active/active path for all WAN links and uses a single IPsec technology, which is not dependent on the underlying transport. The design also uses a single WAN routing domain without route redistribution or route filtering. The IWAN design is prescriptive in order to reduce the possible combinations, which lowers the cost and complexity for customers who want a simplified approach.

Reader Tip

For more information about IWAN design, see Intelligent WAN Design Summary and the associated IWAN deployment guides.

The traditional WAN hybrid design provides an active/standby path and two IPsec technologies based on the type of transport chosen. The design uses two WAN routing domains, which require route redistribution and route filtering for loop prevention. A traditional design has more transport options for customers who have varied needs, but because of the additional flexibility, the complexity is higher.

When planning your WAN strategy, Cisco recommends that you:

- Overprovision the WAN as much as possible.
- Replace some or all of your MPLS bandwidth with Internet bandwidth.
- Grow your existing WAN bandwidth with Internet bandwidth.
- Keep quality of service (QoS) as simple as possible.
- Use SDWAN management tools to automate and virtualize WAN connectivity.

Traditional WAN Introduction

The enterprise WAN architecture interconnects remote-site LANs to a primary site LAN or data center by using a variety of WAN technologies, including MPLS, Layer 2 WAN, and virtual private network (VPN) WAN over the Internet. CVD enterprise 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 that have 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 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 reference network 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 that enables 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 reference network foundation allows easier implementation of advanced technologies such as collaboration.

BUSINESS USE CASES FOR TRADITIONAL WAN

For remote-site users to effectively support the business, organizations require that the WAN provide services with sufficient performance and reliability. Because most of the applications and services that the remote-site worker uses are centrally located or hosted in the cloud, the WAN design must provide a common resource access experience to the workforce regardless of location. The following use cases are relevant for many organizations.

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

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

This design enables the following network capabilities:

- IP any-to-any WAN connectivity for up to 500 remote sites and one or two central hub site locations
- Deployment of single or dual MPLS service providers for resiliency using single or dual routers in remote site locations
- Static routing or dynamic border gateway protocol (BGP) peering with the MPLS service provider for site-to-site communications
- Support for Layer 2 or Layer 3 distribution switching designs
- Support for IP multicast using multicast VPN (mVPN) service provider-based offering
- QoS for WAN traffic such as voice, video, critical data applications, bulk data applications, and management traffic on the network

Use Case: Site-to-Site Communications Using Layer 2 WAN Services

Organizations deploy Layer 2 WAN in order to connect remote office locations over private cloud Layer 2 services. These WAN services can include provider-managed Ethernet over MPLS (EoMPLS) and virtual private LAN service (VPLS).

This design enables the following network capabilities:

- WAN connectivity for up to 100 remote site locations
- Layer 2 adjacency between customer edge (CE) routers supporting 802.1Q and other Layer 2 protocols
- Direct CE-to-CE router peering with an Interior Gateway Protocol (IGP), such as Enhanced Interior Gateway Routing Protocol (EIGRP), transparent to the MPLS service provider
- Simplified IP multicast deployments, transparent to the MPLS service provider
- QoS for WAN traffic such as voice, video, critical data applications, bulk data applications, and management traffic

Use Case: Site-to-Site Connectivity Using 4G LTE Wireless Services

Organizations deploy 4G LTE WAN in order to connect remote sites over 4G LTE wireless services as a primary or secondary WAN solution with secure communications between sites.

This design enables the following network capabilities:

- 4G LTE wireless service for primary remote site WAN connectivity
- 4G LTE encryption services using Cisco Dynamic Multipoint Virtual Private Network (DMVPN)
- 4G LTE wireless service as a backup to the primary WAN service
- QoS for WAN traffic such as voice, video, critical data applications, bulk data applications, and management traffic

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

Organizations require encryption in order to secure communications between sites over private cloud services such as provider-managed MPLS.

This Group Encrypted Transport VPN (GET VPN) design enables the following network capabilities:

- Any-to-any secure encrypted communications well suited for MPLS-based WAN services, for up to 500 locations
- Encrypted traffic that follows the native routing path directly between remote sites, rather than following a tunnel overlay model
- Encryption services, with single or dual MPLS service providers, that support resilient designs using single or dual routers in remote-site locations
- Support for IP Multicast, allowing multicast replication after encryption within the service provider network
- Compatibility with WAN transport solutions that *do not* perform network address translation (NAT) after encryption
- QoS for WAN traffic such as voice, video, critical data applications, bulk data applications and management traffic

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

Organizations deploy Internet WAN in order to connect remote sites over public cloud Internet services with secure communications between sites.

This DMVPN design enables the following network capabilities:

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

Traditional WAN Architecture

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 in order 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.

WAN-AGGREGATION DESIGN

The CVD enterprise 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 designed and tested the complete CVD enterprise 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.

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 CVD enterprise WAN provides you can compare two combinations of design models.

The following figures show a CVD enterprise WAN implemented using the lowest and highest scaling design models.

Figure 2 *CVD WAN (lowest scale)—MPLS Static + DMVPN Backup Shared*

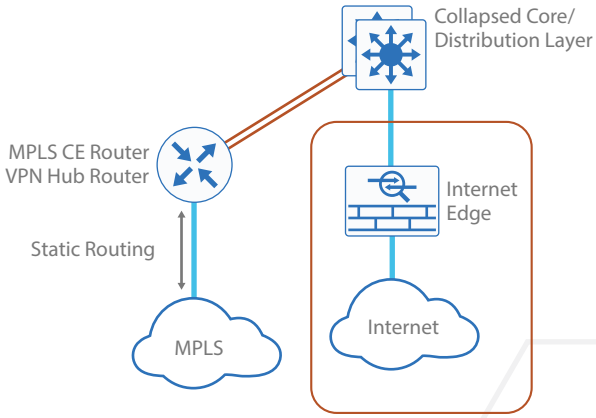
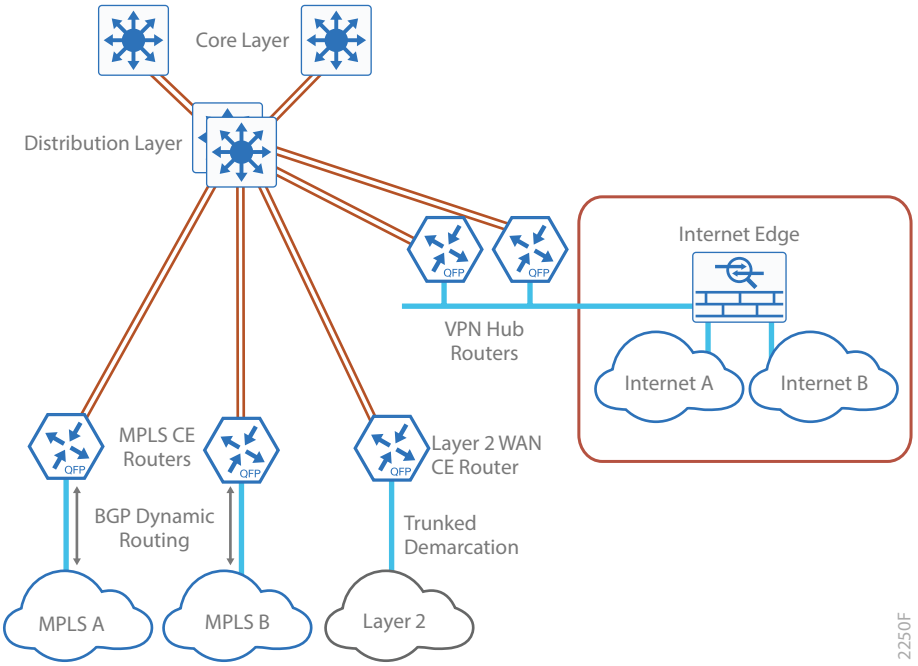


Figure 3 *CVD WAN (highest scale)–Dual MPLS + Layer 2 Trunked + Dual DMVPN*

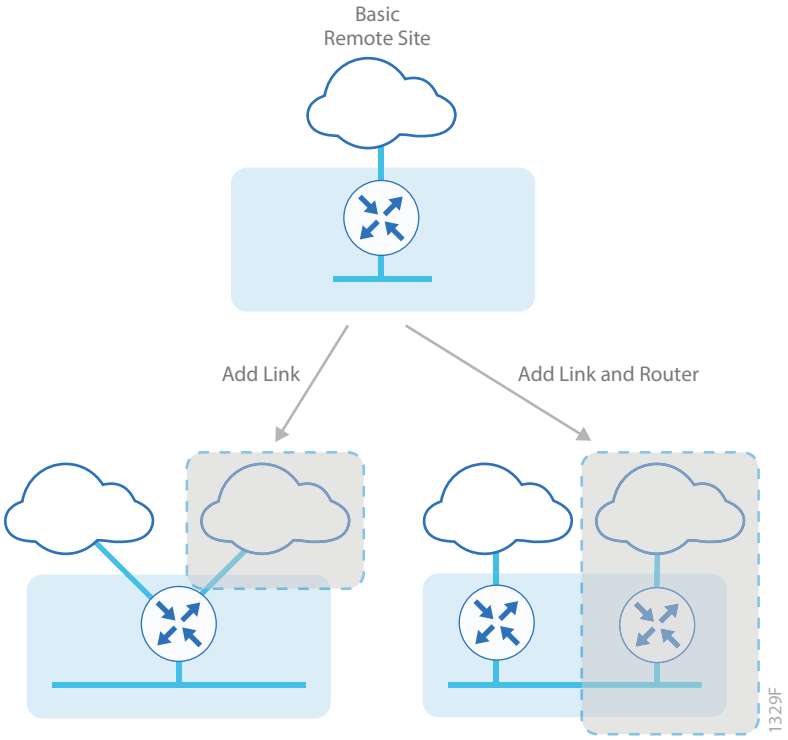


WAN REMOTE-SITE DESIGN

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. The three basic remote site types (in order of increasing resiliency) are: single-router, single-link (non-redundant); single-router, dual-link (redundant links); and dual-router, dual-link (redundant links and routers). 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.

Figure 4 *WAN remote-site designs*



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.

Remote-site LAN

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

At remote sites, the LAN topology depends on the number of connected users and physical geography of the site. Large sites may require the use of a distribution layer in order 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 are shown in the following table.

Table 1 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

For consistency and modularity, all WAN remote sites use the same VLAN assignment scheme, which is shown in the following table. This 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 2 Remote-site 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)

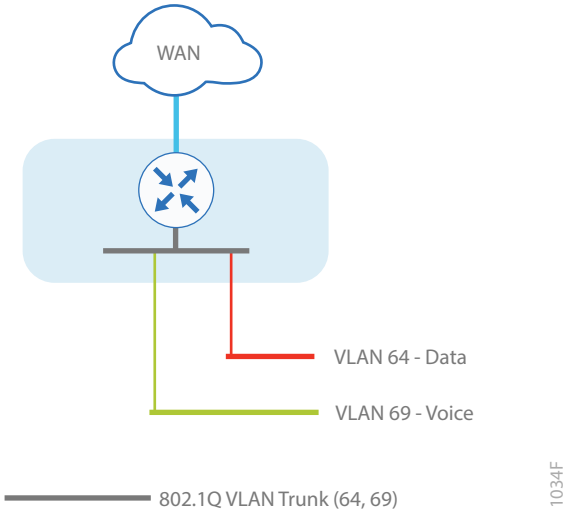
Remote-site Layer 2 Access

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 un-routed 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 the figure below 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 Campus Wired LAN Technology Design Guide provides configuration details on the various access switching platforms.

IP subnets are assigned on a per-VLAN basis. This design 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 sub-interfaces on the router that map to the respective VLANs on the switch. The various router sub-interfaces act as the IP default gateways for each of the IP subnet and VLAN combinations.

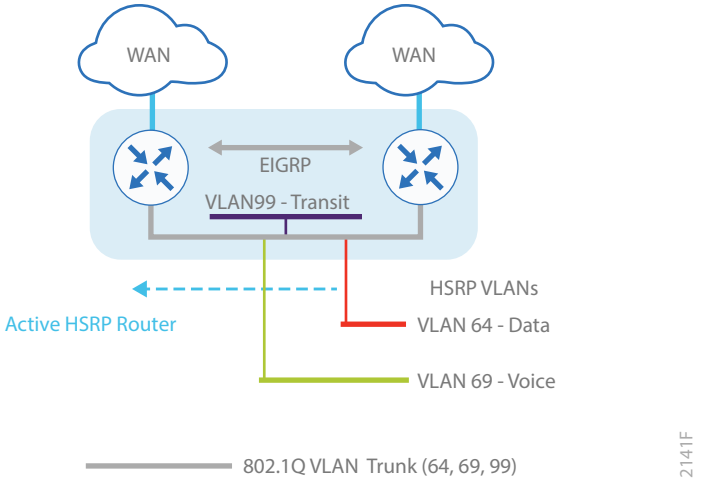
Figure 5 *Remote-site flat Layer 2 LAN (single router)*



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 EIGRP between the routers.

Because there are now two routers per subnet, you must implement a FHRP. For this design, Cisco selected 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 chosen for routing packets; the standby router takes over when the active router fails or when preset conditions are met.

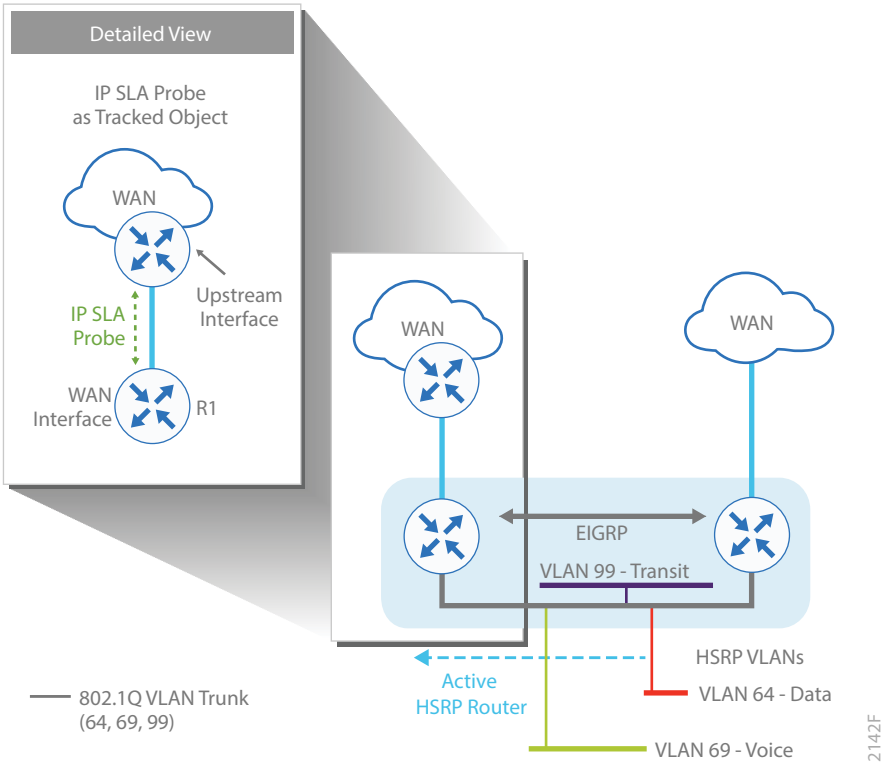
Figure 6 *Remote-site with flat Layer 2 LAN (dual router)*



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

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 7 *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) in order to ensure reachability of the next hop router. This is more effective than simply monitoring the status of the WAN interface.

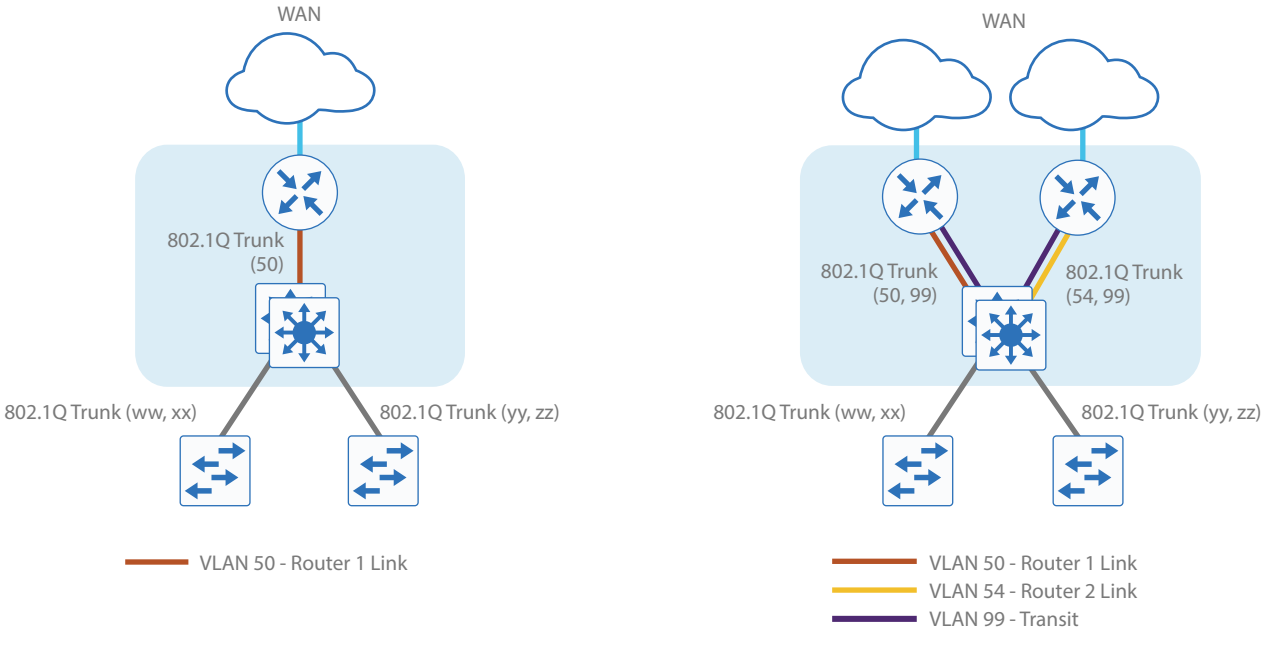
The dual-router designs also warrant an additional transit network component that is required for proper routing in certain scenarios. In these cases, a traffic flow from a remote-site host might be sent to a destination reachable via the alternate WAN transport (for example, a dual MPLS remote site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

Remote-site Distribution and Access Layer

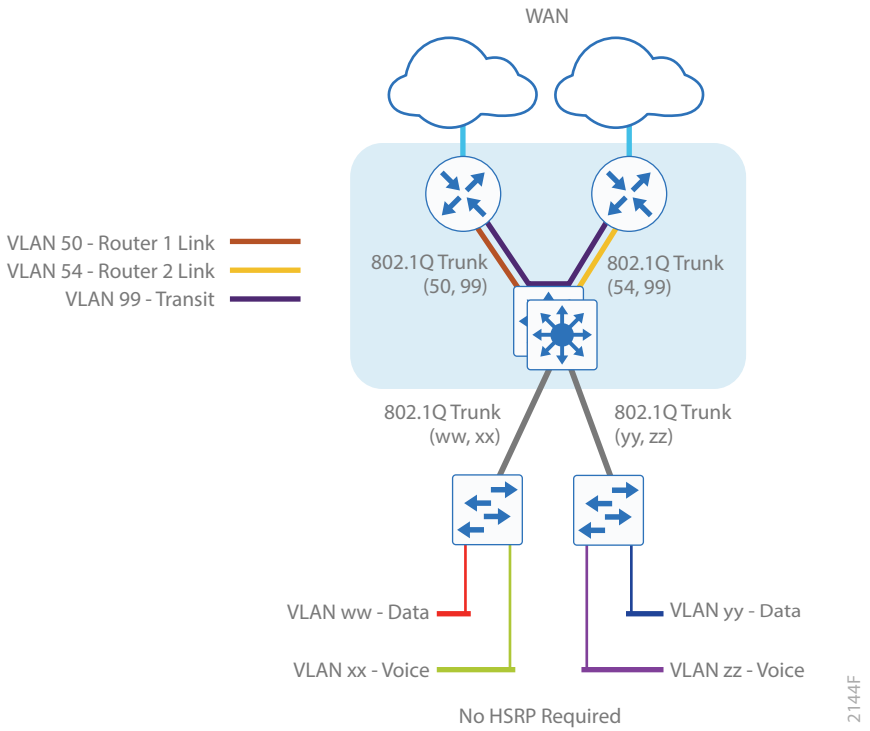
Large remote sites may require a LAN environment similar to that of a small campus LAN that includes a distribution layer and access layer. This topology works well with either a single- or dual-router WAN edge. To implement this design, the routers should connect via EtherChannel links to the distribution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



The LAN distribution switch handles 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 9 *Remote-site distribution and access layer (dual router)*



The Campus Wired LAN Technology Design Guide provides details on how to deploy wired LANs within your organization.

WAN Remote-site 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. The following table summarizes the WAN transport options.

Table 3 WAN-aggregation and WAN remote-site transport options

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

Remote-site Wireless LAN

With the adoption of smartphones and tablets, the need to stay connected while mobile has evolved from a nice-to-have to a must-have. The use of wireless technologies improves effectiveness and efficiency by allowing you to stay connected, regardless of the location or platform being used. As an integrated part of the conventional wired network design, wireless technology allows connectivity while you move about throughout the day.

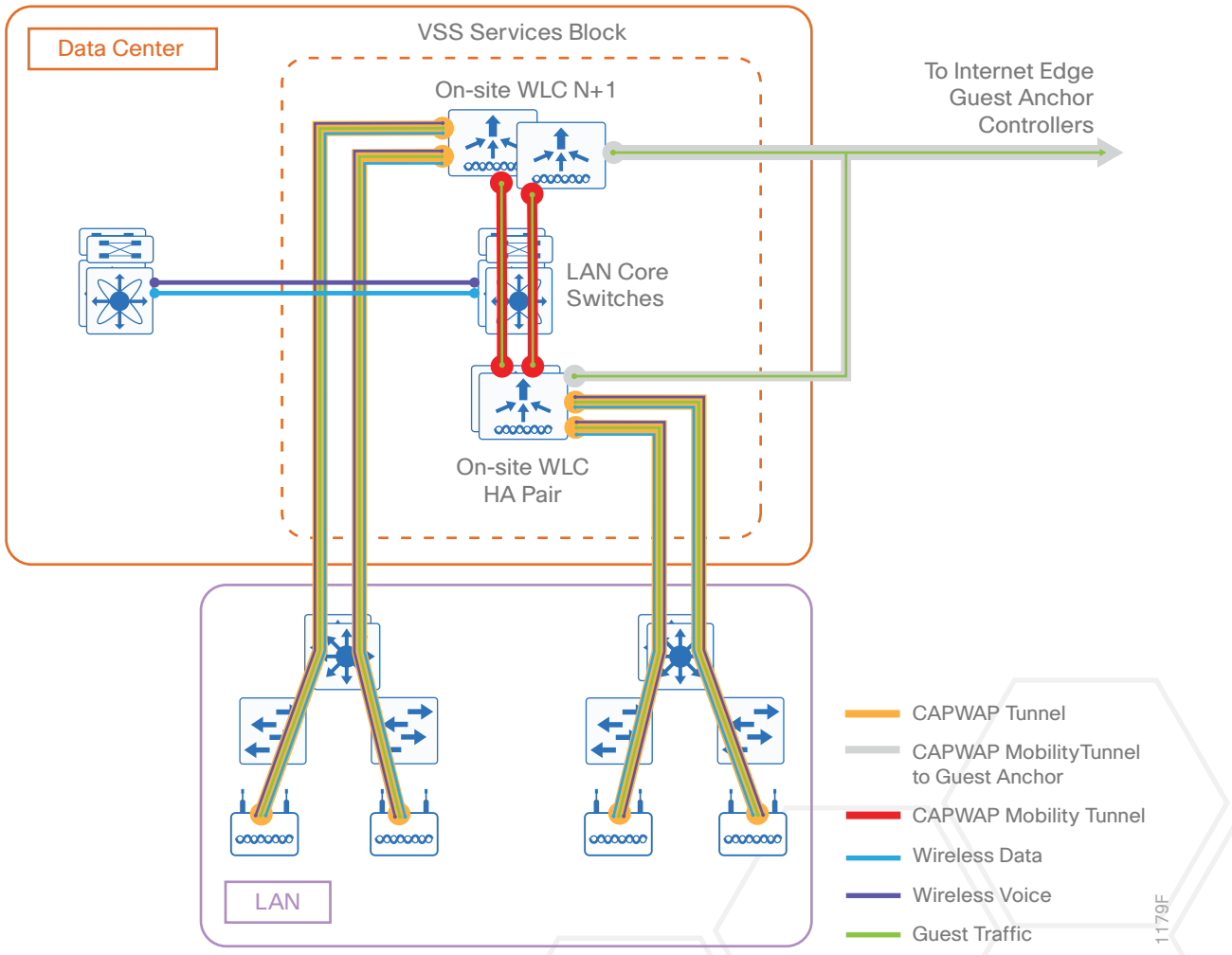
Wireless technologies have the capabilities to turn cafeterias, home offices, classrooms, and our vehicles into meeting places with the same effectiveness as being connected to the wired network. In fact, the wireless network has in many cases become more strategic in our lives than wired networks have been. Given reliance on mobility, network access for mobile devices, including guest wireless access, is essential.

Cisco Unified Wireless networks support two major design models: Local mode and Cisco FlexConnect.

Local-Mode Design Model

In a local-mode design model, the wireless LAN controller and access points are co-located. The wireless LAN controller can be connected to a data center services block or to a LAN distribution layer at the site. Wireless traffic between wireless LAN clients and the LAN is tunneled by using the control and provisioning of wireless access points (CAPWAP) protocol between the controller and the access point.

Figure 10 *Local-mode design model*



A local-mode architecture uses the controller as a single point for managing Layer 2 security and wireless network policies. It also enables you to apply services to wired and wireless traffic in a consistent and coordinated fashion.

If any of the following are true at a site, you should deploy a controller locally at the site:

- The site comprises a data center.
- The site has a LAN distribution layer.
- The site has more than 50 access points.
- The site has a WAN latency greater than 100 ms round-trip to a proposed shared controller.

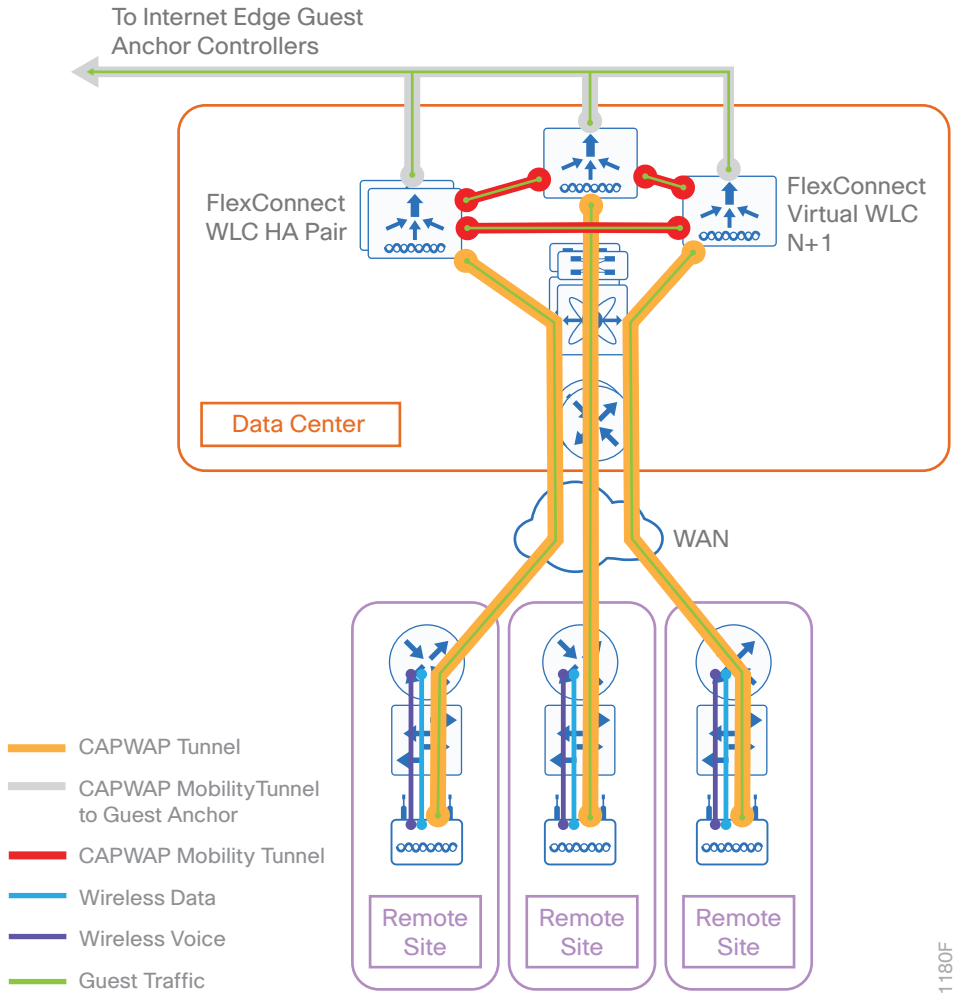
For resiliency, this design uses two wireless LAN controllers for the campus, although you can add more wireless LAN controllers in order to provide additional capacity and resiliency to this design.

Cisco FlexConnect Design Model

Cisco FlexConnect is a wireless solution for most remote-site deployments. It enables organizations to configure and control remote-site access points from the headquarters through the WAN, without deploying a controller in each remote site.

The Cisco FlexConnect access point can switch client data traffic out its local wired interface and can use 802.1Q trunking in order to segment multiple WLANs. The trunk's native VLAN is used for all CAPWAP communication between the access point and the controller. This mode of operation is referred to as FlexConnect local switching and is the mode of operation described in this guide.

Figure 11 *Cisco FlexConnect design model*



Cisco FlexConnect can also tunnel traffic back to the centralized controller, which is specifically used for wireless guest access.

If **all** of the following are true at a site, deploy Cisco FlexConnect at the site:

- The site LAN is a single access-layer switch or switch stack.
- The site has fewer than 50 access points.
- The site has a WAN latency less than 100 ms round-trip to the shared controller.

You can use a shared controller pair or a dedicated controller pair in order to deploy Cisco FlexConnect. In a shared controller model, both local-mode and FlexConnect configured access points share a common controller. Shared controller architecture requires that the wireless LAN controller support both Flex-Connect local switching and local mode.

The Campus Wireless LAN Technology Design Guide provides details on how to deploy wireless LANs within your organization.

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 acting as a rendezvous point (RP). An RP maps the receivers to active sources so the end hosts 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 sub-interfaces.

QUALITY OF SERVICE

Most users perceive the network as 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. 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 in order to protect the network functionality and manageability under normal and congested traffic conditions.

There are twelve common service classes that are grouped together based on interface speed, available queues, and device capabilities. The treatment of the twelve classes can be adjusted according to the policies of your

organization. Cisco recommends marking your traffic in a granular manner in order to make it easier to make the appropriate queuing decisions at different places in the network. The goal of this design is to allow you to enable voice, video, critical data applications, bulk data applications, and management traffic on the network, either during the initial deployment or later, with minimal system impact and engineering effort.

The twelve mappings in the following table are applied throughout this design by using an eight-class model in the enterprise and a six-class model in the service provider network.

Figure 12 *QoS service 12-class mappings*

Application Class	Per-Hop Behavior	Queuing & Dropping	12-Class	8-Class for IWAN Router	6-Class for Tunnel	5-Class for Tunnel	4-Class for Tunnel
Internetwork Control	CS6	BR Queue	Net-Ctrl	NET-CTRL	~~CS6~~	~~CS6~~	~~CS6~~
VoIP Telephony	EF	Priority Queue (PQ)	Voice	VOICE	EF	EF	EF
Multimedia Conferencing	AF4	BR Queue + DSCP WRED	Interactive-Video	INTERACTIVE-VIDEO	AF41	AF31	AF31
Real-Time Interactive	CS4	BR Queue + DSCP WRED	Real-Time	INTERACTIVE-VIDEO	AF41	AF31	AF31
Broadcast Video	CS5	BR Queue + DSCP WRED	Broadcast-Video	STREAMING-VIDEO	AF31	AF31	AF31
Multimedia Streaming	AF3	BR Queue + DSCP WRED	Streaming-Video	STREAMING-VIDEO	AF31	AF31	AF31
Signaling	CS3	BR Queue	Call-Signaling	CALL-SIGNALING	AF21	AF21	AF21
Ops / Admin / Mgmt	CS2	BR Queue + DSCP WRED	Net-Mgmt	CRITICAL-DATA	AF21	AF21	AF21
Transactional Data	AF2	BR Queue + DSCP WRED	Transactional-Data	CRITICAL-DATA	AF21	AF21	AF21
Bulk Data	AF1	BR Queue + DSCP WRED	Bulk-Data	CRITICAL-DATA	AF21	AF21	AF21
Best Effort	DF	BR Queue + RED	Default	DEFAULT	Default	Default	Default
Scavenger	CS1	Min BR Queue	Scavenger	SCAVENGER	AF11	AF11	Default

6044F

Traditional WAN Best Practices

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

- MPLS WAN using Layer 3 VPN
- Layer 2 WAN using VPLS or Metro Ethernet
- Internet with VPN WAN
- Internet 4G LTE with VPN WAN
- Dynamic Multipoint VPN
- GET VPN

This section covers best practices from the traditional WAN perspective.

MPLS WAN USING LAYER 3 VPN

Cisco IOS software 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 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 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.

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 *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 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 the table below.

Table 4 *MPLS 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

Figure 13 *MPLS Static and MPLS Dynamic design models (single MPLS carrier)*

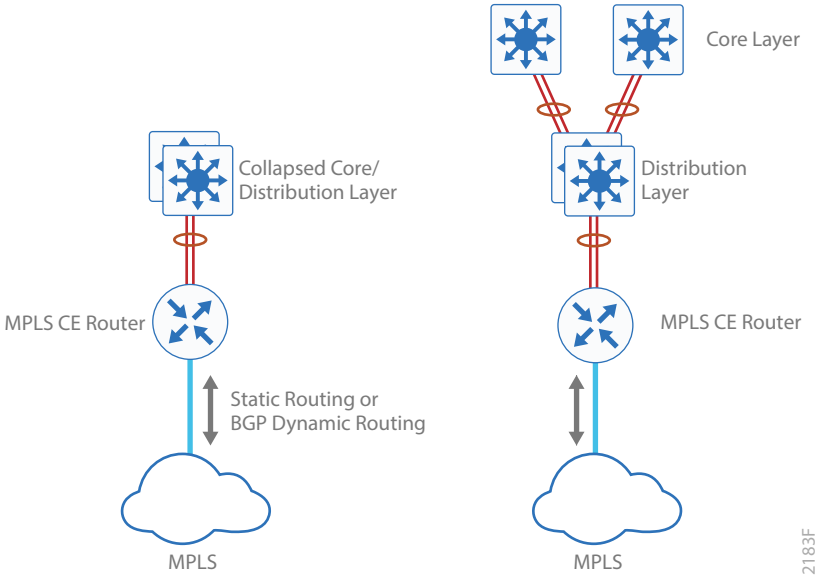
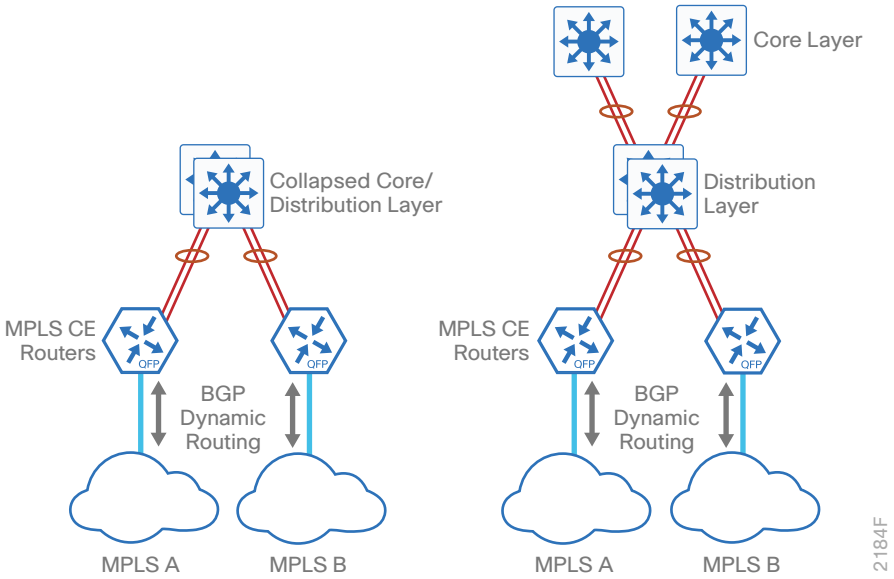


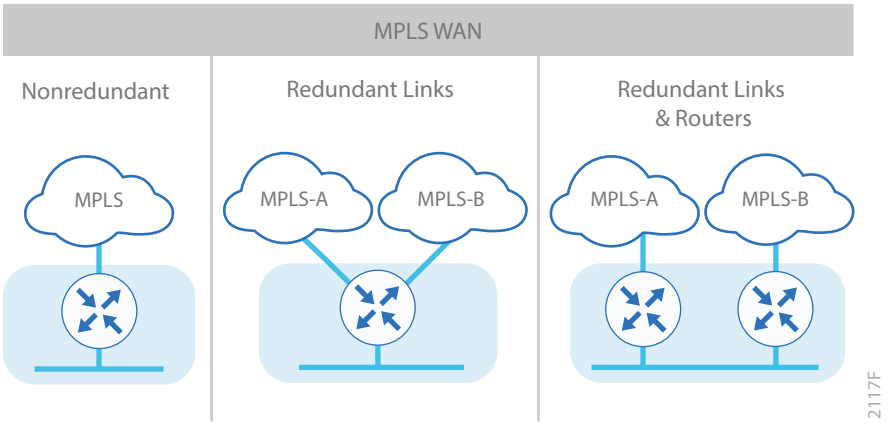
Figure 14 *Dual MPLS design model*



MPLS WAN Connected Remote Sites

The three variants of a MPLS connected remote site are shown in the figure below. 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 15 *MPLS WAN remote-site designs*



The MPLS WAN Technology Design Guide provides details on how to deploy MPLS VPN as a primary WAN transport or as a backup WAN transport (to an alternate MPLS VPN primary).

LAYER 2 WAN USING VPLS OR METRO ETHERNET

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, 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 using a variety of methods. MPLS networks support both 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.

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 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 in order to provide transport of multiple VLANs on a single access trunk. Service providers often refer to a trunked service as *Q-in-Q tunneling*.

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-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 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 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.

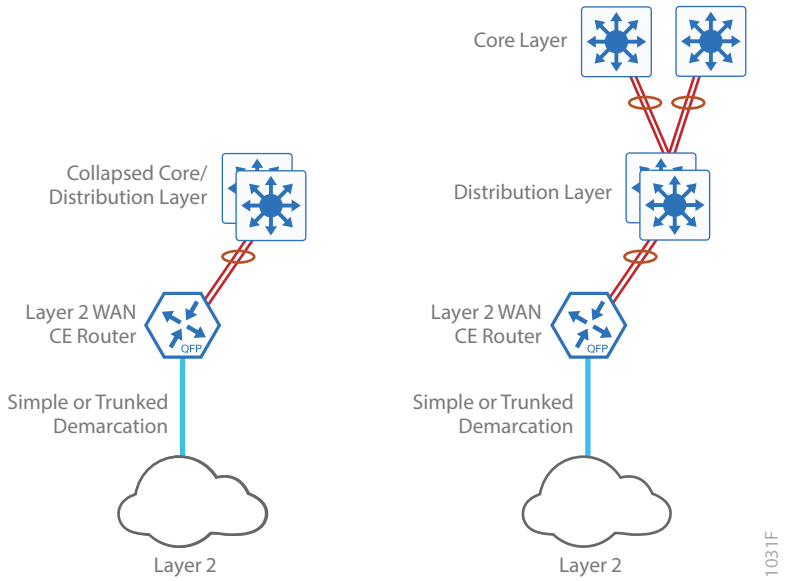
In the WAN-aggregation design, tasks such as IP route summarization are performed at the distribution layer. There are other various devices supporting WAN edge services, such as application optimization and encryption, and these devices should also connect into the distribution layer.

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

Table 5 *Layer 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

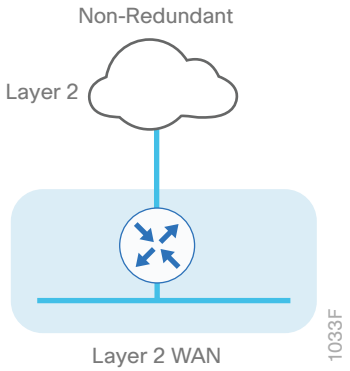
Figure 16 *Layer 2 Simple Demarcation and Trunked Demarcation design models*



Layer 2 WAN Connected Remote Sites

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

Figure 17 *Layer 2 WAN remote-site design*



The Layer 2 WAN Technology Design Guide provides details on how to deploy Layer 2 WAN as a primary WAN transport.

INTERNET WITH VPN WAN

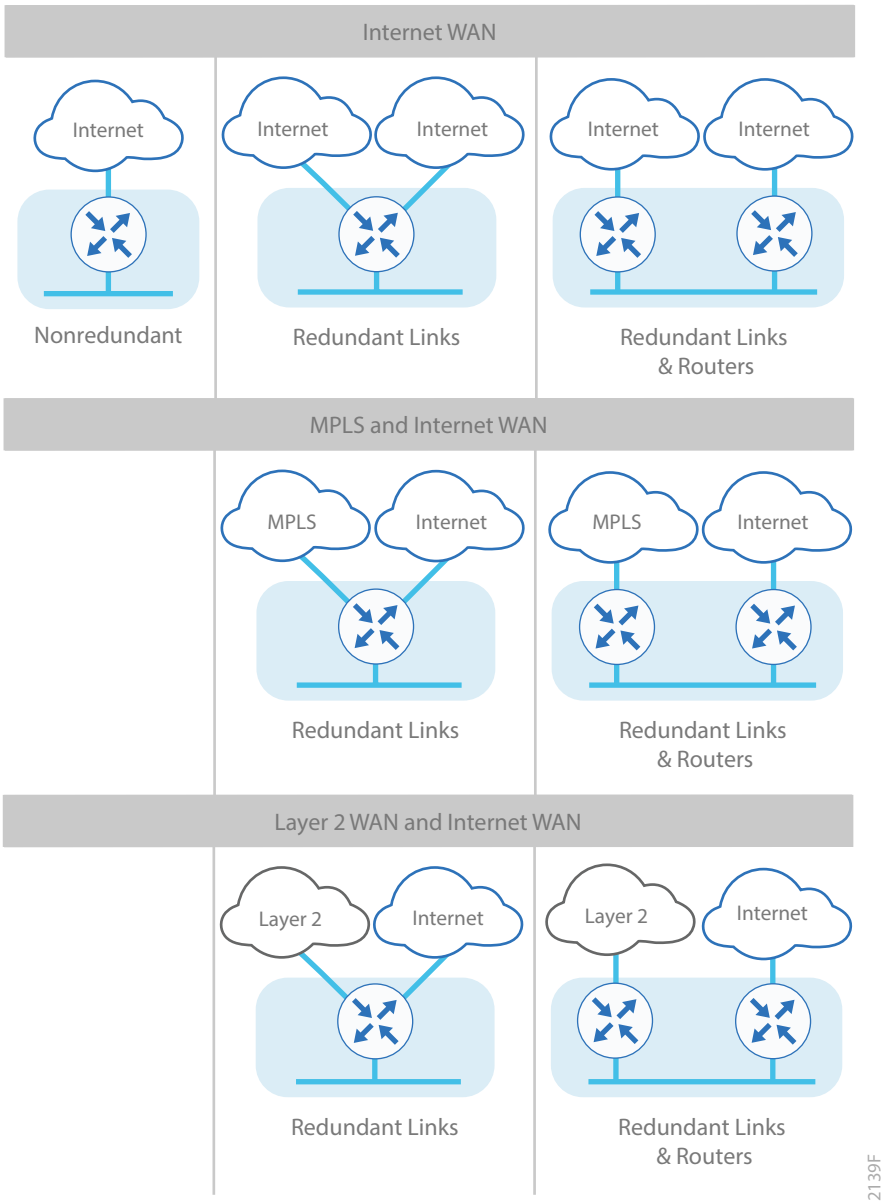
The Internet is essentially a large-scale public WAN composed of multiple interconnected service providers. The Internet can provide reliable high-performance connectivity between various locations, although it lacks any explicit guarantees for these connections. Despite its "best effort" nature, the 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 such as 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 multiple variants of a VPN WAN connected remote site are shown in the figure below. 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 18 *VPN WAN remote-site designs*



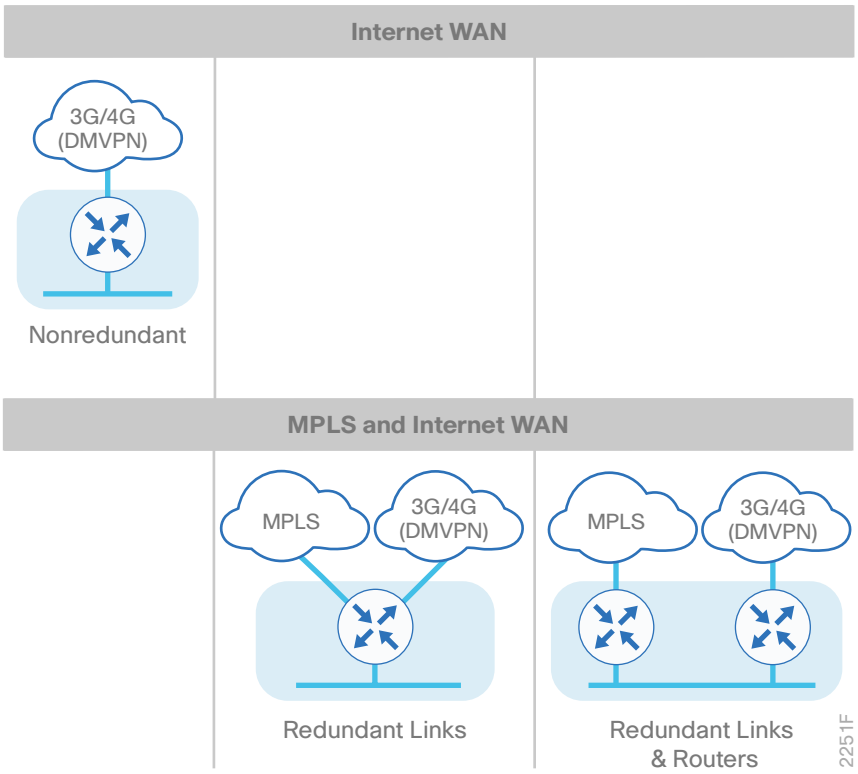
The VPN WAN Technology Design Guide provides details on how to use the Internet for VPN site-to-site connections as both a primary WAN transport and as a backup WAN transport (to a primary WAN transport).

INTERNET 4G LTE WITH VPN WAN

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 several 4G LTE technologies that are supported.

The multiple variants of a 4G LTE VPN WAN connected remote site are shown in the figure below. 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 either 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 19 *4G LTE VPN WAN remote-site designs*



The VPN Remote Site over 4G LTE Design 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).

DYNAMIC MULTIPOINT VPN

DMVPN is the recommended 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 CVD enterprise 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 mGRE tunnels in order 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.

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.

The DMVPN Only design model uses only Internet VPN as transport. The Dual DMVPN design model uses Internet VPN as 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 design models, 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.

Table 6 *WAN-aggregation 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

Figure 20 *DMVPN Only design model*

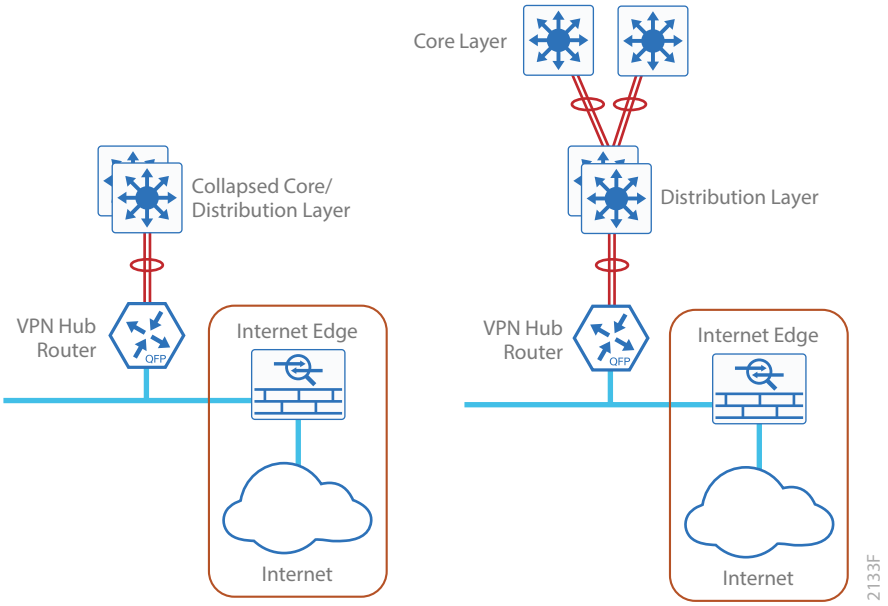
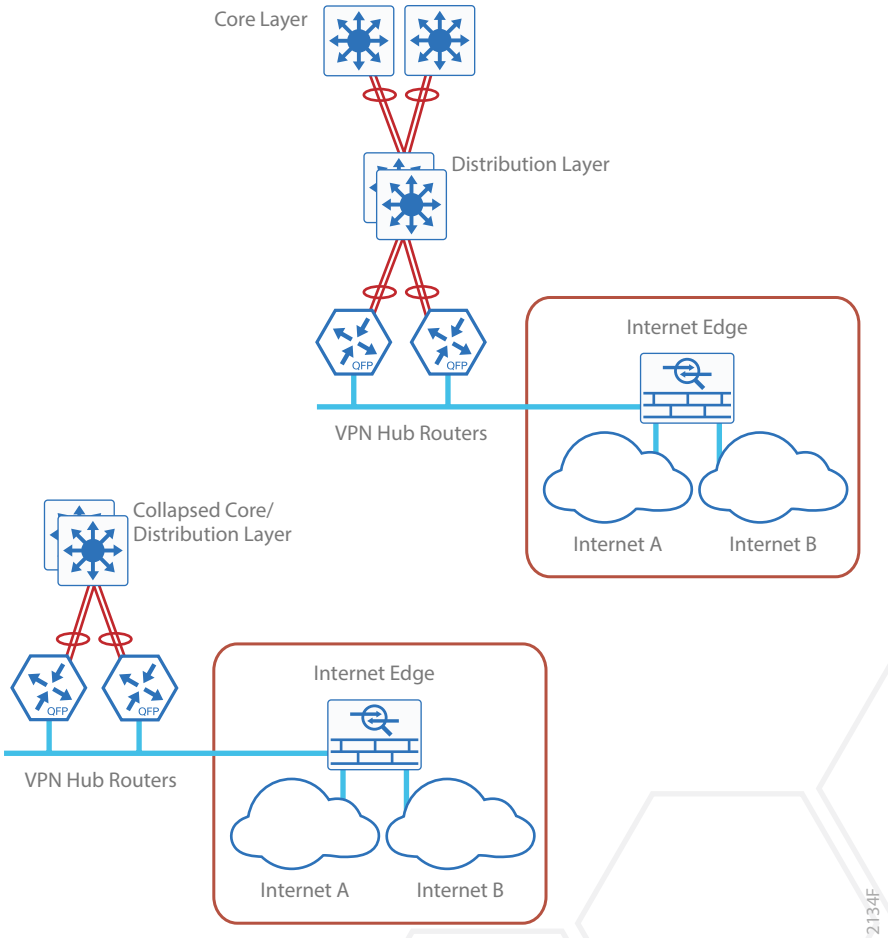


Figure 21 *Dual DMVPN design model*



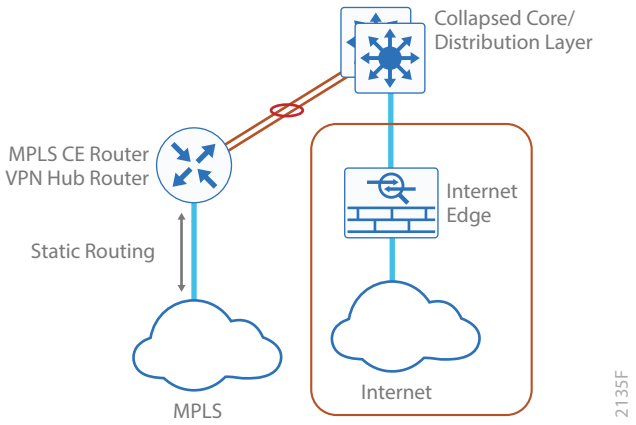
In both the DMVPN Only and Dual DMVPN design models, the DMVPN hub routers connect to the Internet indirectly through a firewall DMZ interface contained within the Internet edge. For details about the connection to the Internet, see the Firewall and IPS Design Guide. The VPN hub routers are connected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

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.

Table 7 *WAN-aggregation 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

Figure 22 *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 Design Guide.

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

Figure 23 *DMVPN Backup Dedicated design model for MPLS WAN*

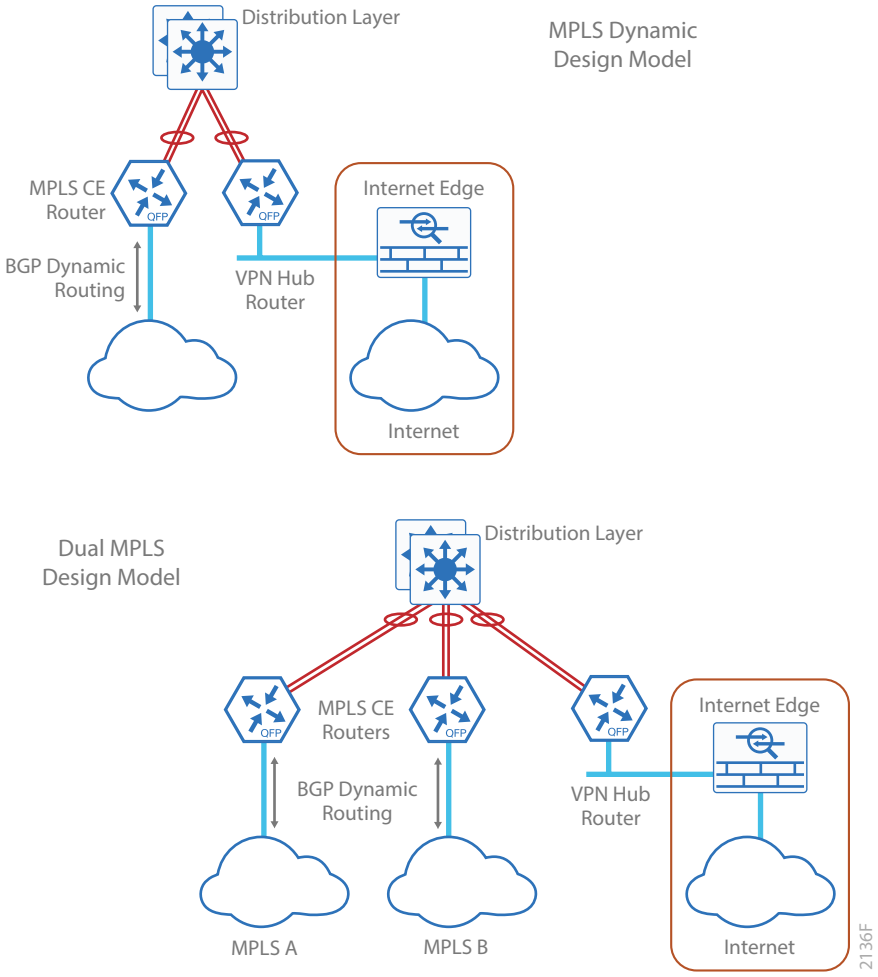
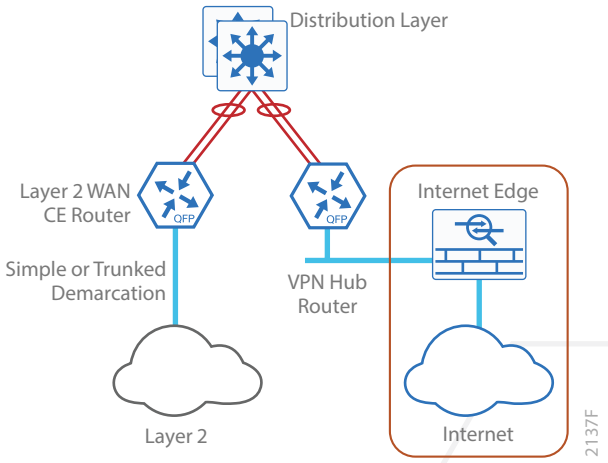


Figure 24 *DMVPN Backup Dedicated design model for Layer 2 WAN primary*



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 Design 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.

GET VPN

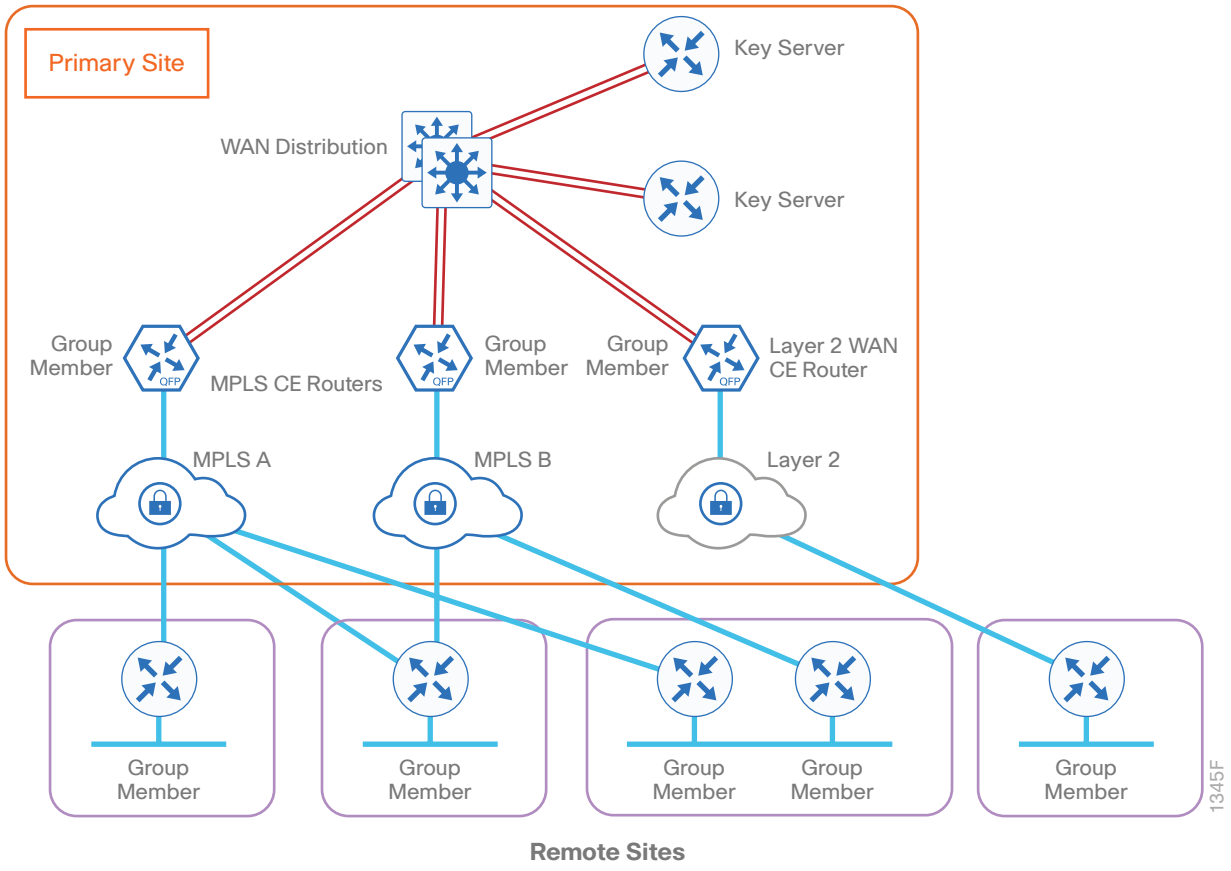
Cisco GET VPN is a tunnel-less VPN technology based on the IETF standard (RFC 3547). The technology provides end-to-end data encryption for network infrastructure while maintaining any-to-any communication between sites. You can deploy it across various WAN core transports, such as MPLS or Layer 2 networks. GET VPN leverages the GDOI protocol in order to create a secure communication domain among network devices.

GET VPN is recommended for organizations who want centralized policy management and group keys. GET VPN is also recommended for Dynamic Site to Site VPNs. To think of it another way, GET VPN makes a network private rather than creating a Virtual Private Network. (that is, it secures an already existing network, much like regular crypto maps.)

The benefits of GET VPN include the following:

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

Figure 25 *Secure WAN using GET VPN*

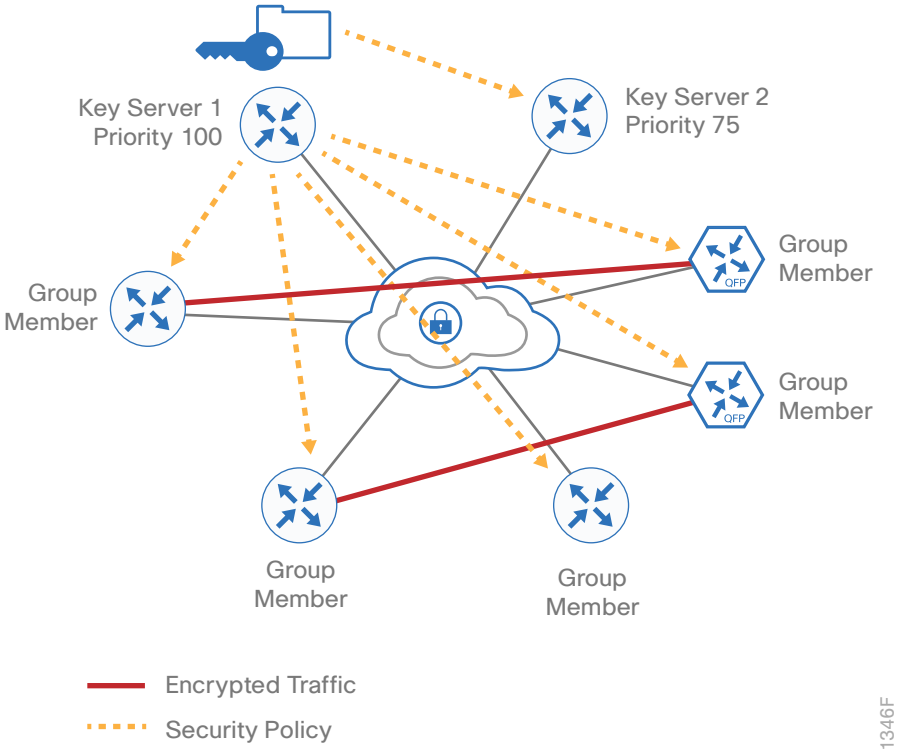


GET VPN Components

A *group member* (GM) is a router running Cisco IOS that encrypts and decrypts the data traffic. A GM registers with a key server to obtain the encryption keys necessary for encrypting and decrypting traffic streams traversing through the device. The GM also performs routing between secure and unsecure domains. Lastly, the GM participates in multicast communications that have been established in the network.

A *key server (KS)* is the brain of the GET VPN operation. It is responsible for authenticating GMs. The KS manages security policies that determine which traffic should be encrypted. The KS distributes session keys for traffic encryption and the security policies through GDOI protocol to GMs. There are two types of keys that the KS sends out to GMs: the key encryption key (KEK) and the traffic encryption key (TEK). The KS uses the KEK to secure communication between the KS and GMs. GMs use the TEK for bulk data encryption of traffic traversing between GMs.

Figure 26 *GET VPN components*

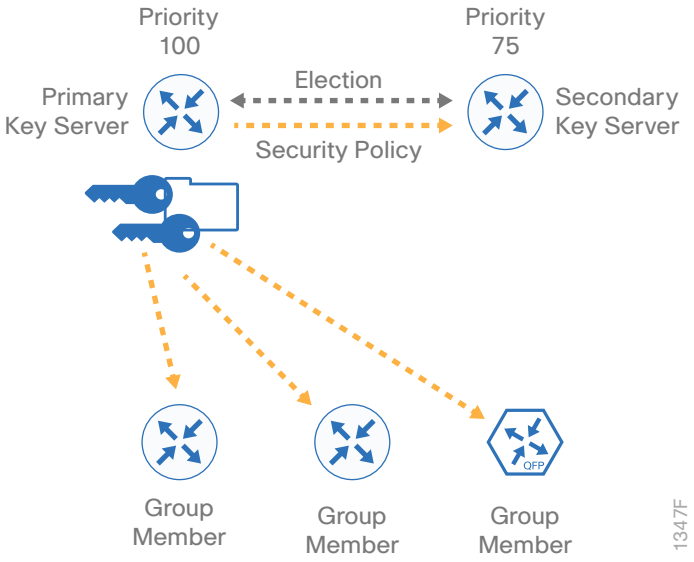


The KS sends out rekey messages as needed. The rekey message contains new encryption policy and encryption keys to use when the old IPSec Security Association (SA) expires. The rekey message is sent in advance of the SA expiration, which helps ensure that the new keys are available to all GMs.

The KS is an essential component in the GET VPN deployment. If the KS becomes unavailable, new GMs will not be able to register and participate in the secure communication, and the existing GMs will not receive new rekeys and updated security policies when the existing ones expire.

To help ensure a highly available and resilient GET VPN network, redundant KSs operate in cooperative mode. Cooperative key servers (COOP KSs) share the GM registration load by jointly managing the GDOI registration of the group. When COOP KSs start up, they go through an election process and the KS with the highest priority assumes the primary role, while the other KSs remain in secondary roles. The primary KS is responsible for creating and redistributing the security policies and keys to GMs, as well as synchronizing the secondary KSs.

Figure 27 *COOP KS synchronization flow*



The GET VPN Technology Design Guide provides details on how to use GET VPN to encrypt your site-to-site connections over an MPLS or Layer 2 transport.

Summary for Traditional WAN

Cisco Enterprise WAN architectures are proven solutions that scale to all remote-site sizes over any transport. With rich application and security services on a single platform, IT can scale to hundreds of sites. Also, customers can maintain granular control, from the remote site, to the data center, and out to the public cloud. The traffic is dynamically routed based on application, endpoint, and network conditions to help ensure the best user experience. IT can confidently roll out critical business services such as consolidated data centers, SaaS, IP telephony, and video without overwhelming the WAN.

Reader Tip

For more information about deploying the traditional WAN topologies, see the Design Zone for Branch WAN.

Appendix A: Changes

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

- Removed the Intelligent WAN section and moved the information into its own guide

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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