Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new 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.

Design Overview

SMART BUSINESS ARCHITECTURE

February 2012 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 new 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.

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 August 2011 are the "August 2011 Series".

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

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

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

How to Read Commands

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

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

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

```
Router# enable
```

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

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

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

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

Comments and Questions

If you would like to comment on a guide or ask questions, please use the forum at the bottom of one of the following sites:

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

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

An RSS feed is available if you would like to be notified when new comments are posted.

Table of Contents

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.

What's In This SBA Guide

About SBA

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.

For more information, see the *How to Get Started with Cisco SBA* document:

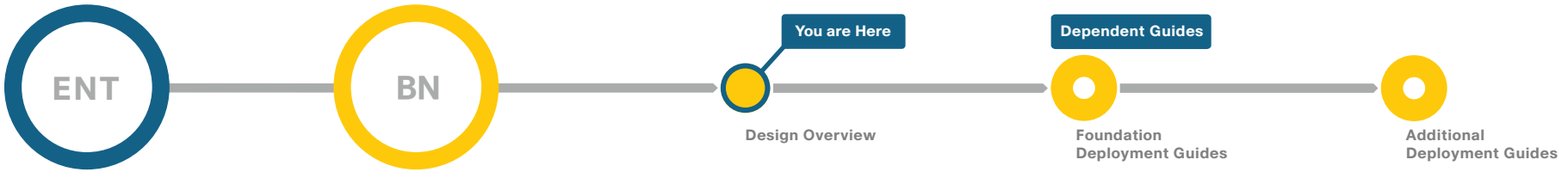
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

About This Guide

This *foundation design overview* provides the following information:

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

This information helps you understand the foundation deployment guides that follow this guide, as shown on the Route to Success below.



Route to Success

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: http://www.cisco.com/go/sba
For partner access: http://www.cisco.com/go/sbachannel

Introduction

The Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations is a comprehensive network design targeted at organizations with 2,000 to 10,000 connected users. The Borderless Network for Enterprise architecture incorporates local-area network (LAN) access for wired and wireless users, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure tested together as a solution. 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 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 like collaboration.

Notes

Architectural Benefits

There are many ways an organization can benefit by deploying a Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations architecture:

- Reduced cost of deploying a standardized design based on Cisco tested and supported best practices
- Flexible architecture that scales from the small locations to the large campus, to allow easy migration
- Focused approach on building a sound network foundation for organizations with 2,000 to 10,000 connected users and up to 500 remote sites in order to allow growth and stability
- Improved WAN performance through the use of application optimization, to help reduce circuit costs and delay bandwidth upgrades
- Secure Internet access design in a tiered approach, to add protection without compromising employee mobility
- Resiliency and availability of the network through proper use of redundancy and the hardening of link topology, platform features, and system security
- Summarized and simplified design choices so that IT workers with a CCNA® certification or equivalent experience can deploy and operate the network

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, the office, or from a hotel room, 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 even if the power or other facilities are out of order where you were planning to work because it provides mobile access, remote access, or the ability to move to another office and still have the same access to your applications and information.

Now that networks are critical to the operation and innovation of enterprise organizations, workforce productivity enhancements are built on the expectation of nonstop access to communications and resources. As networks become more complex 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.

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.

Architectural Components

In the context of building design, architecture means the art and science of designing and constructing buildings. In the context of computer design, architecture refers to the design, structure, and behavior of a computer system, microprocessor, or system program, including the characteristics of individual components and how they interact. The term service-oriented architecture refers to how two computing entities, such as programs, interact in such a way as to enable one entity to perform a unit of work on behalf of another entity. These definitions support the broader definition of the process that we used to create the Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations. Our process accounts for the surrounding landscape, the requirements and characteristics of those using that which is constructed, and the ability to combine both the micro- and macro-level interdependencies.

We created the Cisco Smart Business Architecture by using a structured process to help ensure the stability of the valuable business processes and assets it is designed to serve.

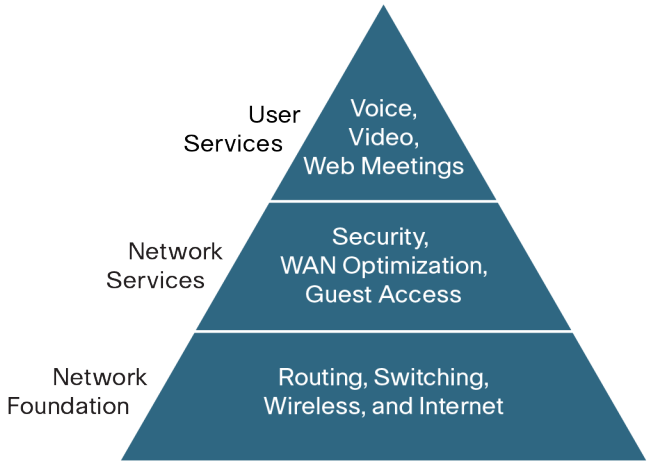
The Cisco Smart Business Architecture consists of three primary modular yet interdependent components. They are the Network Foundation, Network Services, and User Services, with a hierarchical interdependency.

Network Foundation

The key building block of the architecture is the network foundation. Similar to the foundation of any building, the network foundation provides the underpinning infrastructure that all other services and applications rely on. Delivered as a module of the overall architecture, the network foundation provides the seamless transport that ensures information can pass reliably from one location to another.

To the average user, the network foundation works transparently when it is implemented correctly. Users merely connect their desktops, laptops, or smart devices to the network, and they can update their email, process orders, or click on a web link, and it just works. The infrastructure of intelligent Cisco devices, such as the routers, switches, and wireless access points, make this all possible.

Figure 1 - The Smart Business Architecture pyramid



Network Services

While any building architecture can be made of common building products, a well-architected structure considers the requirements of use for the architecture, to make it valuable to those using it. You may need a large lobby when you expect many guests, many windows for sunlight when you intend to house patients, high solid walls and secure doors for maximum security, or ventilation and air conditioning to control the environment. The consideration of these services and functions is essential to making the structure more than just four walls; considering the services enables the usability of the building. Network services provide more customization to your network environment even if you use standards-based devices. Even though the user may not be aware that their connection to the network is using a VPN for remote access or that they have seamlessly passed through a firewall, the existence of these services allows for greater freedom and usability. When away from the office, the user may only be aware of the need to click on a remote-access icon and provide a password, but the user does not know or care exactly how those services operate.

Cisco intelligent network services, such as firewalls, web security, WAN optimization, and guest access, are designed to interoperate to provide a seamless and transparent solution.

User Services

User services sit on top of the network foundation and network services to make it work for the end user. In a building environment, user services, such as elevators, office lighting, or telephones, are directly used by people in a building. In the morning, the elevator takes us to the floor where our desks are, we turn on the lights, and we push buttons on our phones to listen to voicemail. Network-reliant user services, such as telephony, Enterprise Resource Planning (ERP) applications, email, and other business applications, all depend on transferring information to and from the desktop or portable platform that we use to connect to the network. User services common to many network architectures include Cisco Unified Communications, Cisco WebEx collaboration, and Cisco TelePresence.

Notes

Network Foundation

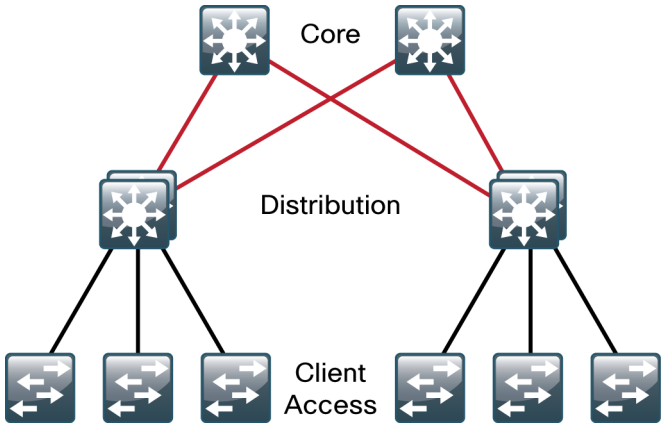
There is a tendency to discount the network as just simple plumbing, to think that all you have to consider is the size and the length of the pipes or the speeds and feeds of the links, and to dismiss the rest as unimportant. Just as the plumbing in a large stadium or high rise has to be designed for 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. Even with the large amount of bandwidth available to LAN backbones 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. Whether a user's network access is wired or wireless, at the headquarters or at a remote site, the network must provide intelligent prioritization and queuing of traffic along the most efficient route possible.

The LAN and Campus

Larger LANs are usually located at an organization headquarters or large campus location. When located at headquarters, the LAN not only provides connectivity for local users, but becomes the core for interconnecting the WAN, data center or server room, and Internet access, making it a critical part of the network. Along with traditional wired LAN connectivity, the architecture includes wireless LAN access to provide user mobility and to allow previously single-use areas like cafeterias to become temporary meeting locations with full access to network resources.

Large LANs or campus networks require a high availability (HA) design to support the mission-critical applications and real-time multimedia communications that drive the organizational operations. In many other LAN designs, the redundant links for resiliency stay in a backup status and remain unused. With the Cisco Smart Business Architecture—Borderless Network for Enterprise Organizations LAN design, all links are actively forwarding traffic for a higher-performance network while reducing complexity involved in traditional redundant designs.

Figure 2 - LAN hierarchical design



To accommodate growth from a small number of users to a very large number of users, network engineers build LANs in layers. We designed the Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations LAN to accommodate up to 5,000 users, and we employed a layered approach to allow intuitive and seamless scalability.

The access layer is the point at which user-controlled and user-accessible devices connect to the network. The access layer design can provide formerly expensive, high-speed connectivity like Gigabit Ethernet or 802.11n wireless as a standard configuration. Because the access layer connects client devices to network services, it plays an important role in protecting users, application resources, and the network itself from human error and malicious attacks. The access layer also provides automated services like Power over Ethernet, QoS settings, and VLAN assignment for IP telephones to reduce operational requirements.

The distribution layer of the network serves primarily as an aggregation point when multiple access layer switches are needed to support the required number of users at a location. Beyond simple aggregation, the distribution layer serves in many designs as the first point of IP Layer-3 packet switching, routing, and services. Because the distribution layer serves a larger number of users and access locations, it requires an HA design, which traditionally results in a highly complex interconnection of redundant links as well as protocols, such as Spanning Tree Protocol (STP) and First Hop Routing Protocol (FHRP), to manage availability and path selection. In the traditional, two-box distribution-layer design, if the same voice or data VLAN is used across multiple access-layer switches with redundant uplinks, it creates a loop that STP detects and mitigates by shutting down one of the redundant uplinks. The active STP loop avoidance has a few drawbacks—it

can be much slower to recover from link outages by unblocking redundant uplinks. It has to block redundant paths to prevent loops, which reduces useable bandwidth, and it can be error prone when misconfigured, misused, or subjected to one-way communication failures.

Figure 3 - Traditional design when sharing VLANs

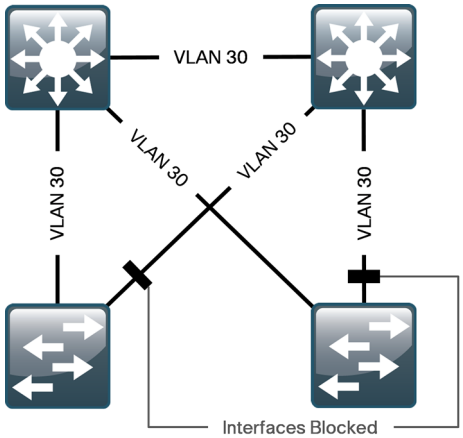
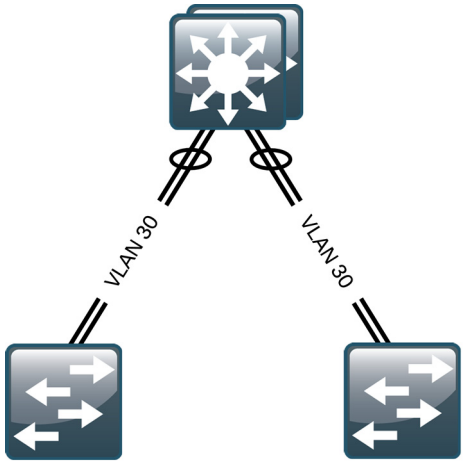


Figure 4 - Simplified design when sharing VLANs



The architecture improves on the traditional design by using a resilient virtual-switch design at the distribution layer. This virtual-switch design provides distribution-layer device redundancy by making two physical switches appear as a single switch or stack, or by using a single switch with redundant logic and power. This simplified design uses EtherChannel and Multi-Chassis EtherChannel to allow redundant access-layer uplinks to be actively forwarding. EtherChannel and Multi-Chassis EtherChannel provide sub-second failover for failed links and eliminate STP loops. The resilient design also eliminates the need for FHRPs, reduces the complexity of the configuration by over 50%, and makes the network easier to troubleshoot, while still providing fast recovery in the event of failures.

The simplified architecture provides the following benefits:

- Resilient distribution layer provides reduced complexity while improving failure recovery times
- Intelligent access layer provides user and network protection from malicious attacks while maintaining user transparency
- Redundant links forward traffic without creating dangerous Layer-2 loops in the network
- Consistent design practices from the smaller remote-site LANs to the larger high-density campus LANs reduce operational expenses
- User services are consistent whether users connect at the headquarters LAN or a remote-site LAN

The third and final layer of the LAN network is the core layer. This layer provides aggregation when multiple distribution layers exist in a single, collocated topology and is designed to use only Layer-3 IP-routed links. Because it is the core layer of the expanded LAN, the interconnect for the WAN and the Internet edge, and the connection point to a collocated data center, it has a 24x7x365 design criteria, the highest possible availability. We designed the core layer to eliminate high complexity or high-touch services in order to reduce planned or unplanned outages for upgrades, maintenance, or complex configuration changes. The core layer is based on two physically and logically separate switches, providing for increased availability without increasing the complexity of the distribution layer, where more access layer services are delivered.

The Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations LAN reduces the complexity of building a traditional LAN while improving overall usable network bandwidth, improving resiliency, and making the network easier to deploy, maintain, and troubleshoot.

Wireless

We can improve the effectiveness and efficiency of employees by providing the ability to stay connected regardless of employee location. As an integrated part of the wired-port networking design that provides connectivity when users are at their desks or at another wired location, wireless allows connectivity in transit to meetings and turns cafeterias or other meeting places into temporary conference rooms. Wireless networks enable the users to stay connected and the flow of information to continue regardless of physical building limitations.

In the Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations architecture, wireless uses Wi-Fi technology to transport data, voice, and even video traffic rather than using cellular technology.

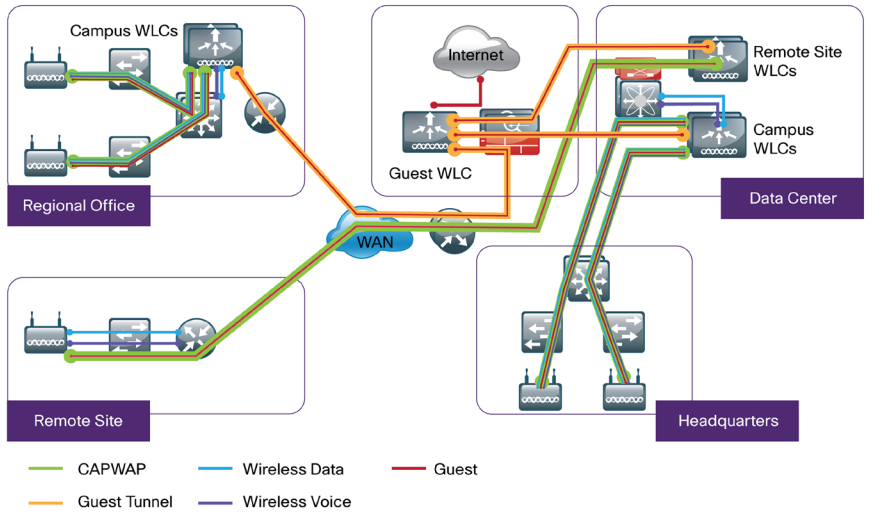
Users at remote sites or headquarters can connect to voice and data services via the same methods, creating a seamless environment for your enterprise.

Employing a wireless network provides the following benefits:

- Location-independent network access improves employee productivity
- Hard-to-wire locations receive connectivity without costly construction
- Centralized control of distributed wireless environment is easy to manage and easy to operate
- Wireless network core is a plug-and-play deployment, preconfigured to recognize new wireless access points that you connect to any wired access port

First-generation wireless LAN offerings were often unsecure, and network administrators found them difficult to manage. Administrators configured and operated wireless access points autonomously, which proved to be a non-scalable deployment and operation model. This traditional, standalone access point model can be a very costly way of providing a secure wireless infrastructure at remote sites and headquarters.

Figure 5 - Wireless topology



The design uses a centralized wireless LAN controller (WLC), which can control all access points at the headquarters and remote sites. The centralized approach of the WLC provides many benefits beyond centralized management of the wireless access points. To ensure secure access to the wireless LAN, the WLC enables all users to authenticate against a corporate directory, thus removing the need to maintain a separate username and password database on each access point. Via an integrated guest controller, you can grant access to guest and partner users who are important to the organization, and their traffic is kept separate from authenticated internal user traffic. You can cluster multiple WLCs to provide load balancing, scalability, and redundancy for maintenance and unexpected outage resilience.

While the WLC is centralized for headquarters and most remote sites, you can install local WLCs in larger locations, to provide optimal roaming capabilities while still managed from a central location. Wireless access points at remote sites without local WLCs provide direct access to the local LAN for non-guest traffic, avoiding traffic flow that would otherwise have to transit to the central controller and back to the remote site, wasting precious WAN bandwidth.

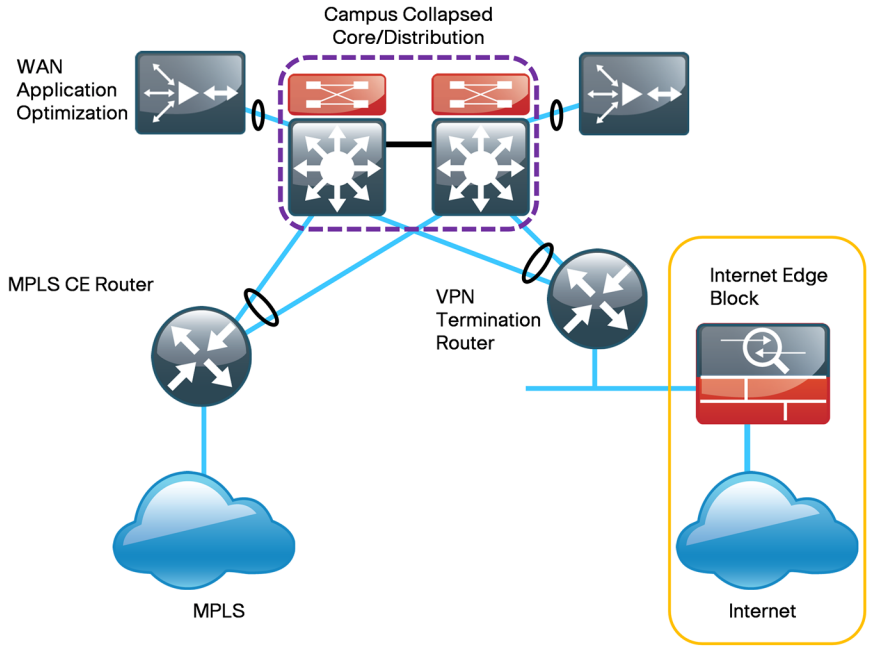
The WAN and Remote Sites

Whether you are at headquarters or a remote site, access to information and the flow of data is essential to your ability to conduct daily business. Because not all enterprises have the same requirements for headquarters and remote sites, the WAN architecture must be flexible and scalable. The Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations architecture provides a robust WAN design that scales from smaller WAN needs up to 500 remote sites, using common technology and techniques. This approach makes the architecture relevant to a wider range of customer deployments without radical customization. It also allows enterprises with smaller WANs to build and scale their WAN with consistency as their needs grow.

The WAN is the point where a remote-site's private network connects to a public transport. A remote site is defined as a remote location where employees conduct operations on behalf of the organization. A remote worker requires the same level of access to applications as workers at headquarters, but there are fewer workers at a remote site than in headquarters. Depending on the criticality of the remote-site operation and the ability to offload that operation elsewhere, you can employ varying levels of redundancy to protect communications from WAN outages. The typical enterprise WAN interconnects all locations and aggregates all remote-site traffic at the headquarters, where the collocated data center might be, or at an offsite facility where a primary or backup data center is located.

The primary function of the WAN router is to transport data between the remote sites and the main locations where applications are housed. The remote site is designed to support from a few to hundreds of users with computers, IP phones, and wireless voice and data. The remote-site router provides the common platform to deliver the growing number of services and increased performance requirements common in remote-site applications.

Figure 6 - WAN 100 design



The following are benefits from a remote-site WAN deployment:

- Common remote-site platform with integrated services reduces operating expenses
- IP-based transport design supports all major service-provider WAN connection offerings
- Flexible and scalable design increases design consistency and reduces complexity
- Information encryption protects business data as it transits public transport offerings
- Remote-site connectivity includes options for basic to highly resilient connectivity to meet a wide range of needs

Many options exist for public WAN transport, ranging from MPLS VPNs to Internet over broadband or traditional private lines. The design is based on IP-packet transport with integrated encryption for data privacy over the Internet, which makes it suitable for all public transport options. The flexibility of the design allows you to mix MPLS VPN service and Internet-based VPN overlay, providing options for multiple connections for resiliency while reducing complexity through the use of a reduced set of IP transport options. The benefit to the organization is a standard, modular approach for building the WAN to meet your needs.

Users need seamless access to network services, whether they are located at headquarters or at any site across the WAN. The difference in available bandwidth to remote-site users versus headquarters users can be very large. Services such as application optimization and quality of service (QoS) can be implemented to improve performance over lower-speed WAN links. Application optimization performs traffic compression, protocol optimization, and repeat traffic caching to improve the performance of WAN bandwidth. QoS is programmed to prioritize latency and drop-sensitive multimedia traffic, and it can be used to prioritize business-critical data traffic over other traffic. The design provides wired and wireless data, voice, and video access for users at headquarters or at remote sites.

Internet Edge

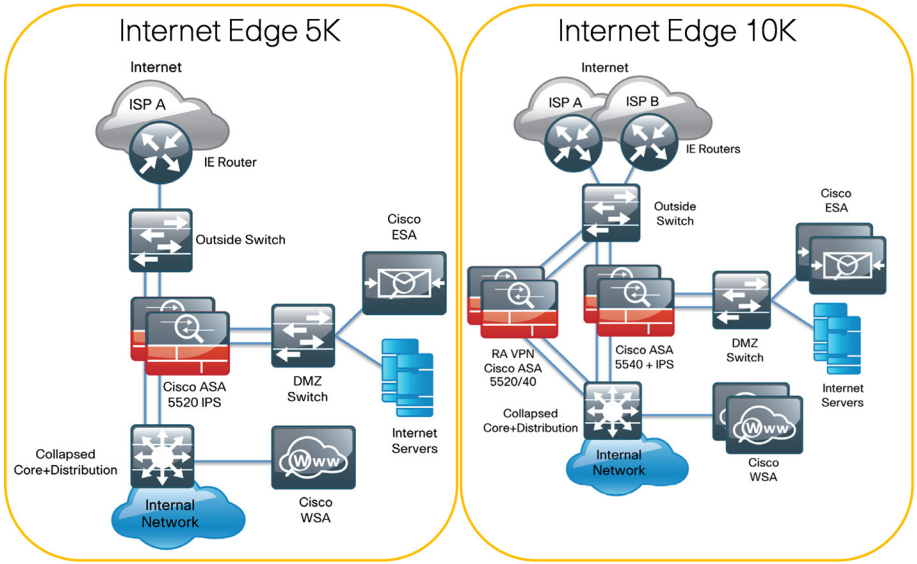
The Internet edge serves as an organization's gateway to the Internet. This gateway to the outside world must provide a secure infrastructure for email and web access as well as public access to company information for customers and partners. The challenge for organizations is how to provide this essential access in a secure manner that does not create an overly complex environment.

The following are benefits of an Internet edge:

- Provides fast, secure Internet access for increased productivity
- Helps secure critical assets from Internet attacks that could disrupt business
- Employs a resilient design to avoid single points of failure
- Delivers a secure and reliable environment for your web-facing applications

It is common to have a firewall, an intrusion protection device, and a VPN appliance at the Internet edge in order to provide protected access. Building this security gauntlet can require much time and expertise to assemble from multiple sources and manufacturers. The Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations architecture provides a simplified design that uses fewer network devices without sacrificing scalability, security, or resilience. Because each section of the Internet edge design offers options for scale, an organization can mix and match selections to match the organization's needs.

Figure 7 - Internet edge 5K and 10K designs



The firewall functionality of the Internet edge controls access for Internet hosts accessing DMZ services, internal hosts accessing Internet services, and DMZ hosts accessing both internal and external services. The specific policies regarding resource access and acceptable use are derived from the organization's security policy. As a part of the network foundation, the Internet edge design allows an organization the flexibility to control how users connect and what type of access is permitted. The configuration of the firewalls is fully redundant, and single or dual Internet access can be used to further reduce single points of failure for a high-availability design.

The Internet gateway exposes organizations to worms, viruses, botnets, and other threats. The integrated intrusion prevention system (IPS) modules in the firewalls provide a complementary inspection of traffic that is permitted by firewall policy, to detect and mitigate attacks. The IPS modules consider the reputation of the traffic source to simplify the decision of what traffic to block. Reputation-based filtering increases scalability by allowing the IPS modules to block twice the number of attacks based on source reputation and allows zero-day attack protection without signature reliance while decreasing the number of false positives.

The image of an organization is often based on the ability of web servers placed in an organization's Internet edge to provide customer or partner access to information or applications. IT organizations face significant challenges associated with the reliable delivery of these applications and resources. Application delivery technologies can help IT organizations improve the availability, performance, and security of their applications. The application-aware server load balancers (SLB) in the Internet edge provide core server load balancing to route sessions to the best server and to protect against dead services on a live server. Security and virtualization services allow for segmentation of servers and for granular, role-based administration. The combination of these services, along with advanced application acceleration, provides a robust architecture for your Internet-facing web applications.

To improve productivity, organizations continue to extend their reach, drive the mobility of their workforce, and reach research and business partners. It is cost prohibitive to provide this connectivity with traditional private lines or dial-up access. Another capability of the firewalls in the design is to provide integrated VPN for remote-access connectivity to the organization's network for employees, contractors, or partners. The remote-access connection is granted based on authentication and policy control that integrates with the organization's authentication resources. Flexible IPsec and SSL VPN access is provided with the same HA design that the firewall and IPS share.

The firewall protection and IPS offer perimeter defense and detection, but how do you control acceptable use of Internet access by employees or guard against attacks embedded into authorized applications? The Internet edge design includes network security services for email filtering and web surfing security and control.

This integrated design developed by Cisco allows the Internet edge core security requirements to be met by a reduced number of appliances with a scalable solutions-based approach to the business needs.

Notes

Network Services

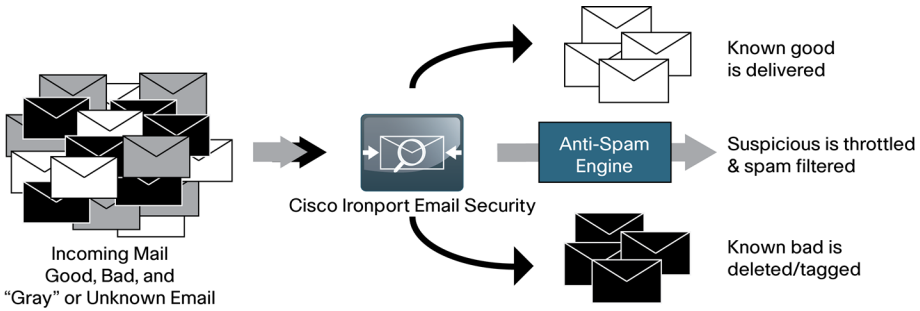
Security

Security is an integral part of every network deployment and can be part of the network foundation as is seen in the Internet edge, or it can be a service deployed to protect more specific use cases or applications. Regulatory compliance, information protection, and network and desktop reliability dictate that you design security services into the infrastructure rather than add them as an afterthought.

Network security provides the following benefits:

- Protects your email from SPAM and embedded threats
- Uses Internet-wide attack and outbreak information for the most reliable threat response
- Provides secure and reliable remote access for employees and partners
- Provides maximum flexibility for hardware-based and software-based VPN clients
- Web access acceptable-use control allows risk management of users browsing the Internet

Figure 8 - Email security



Email can be as important as telephone service to some organizations, yet two major problems plague email in networks. Floods of unwanted or unsolicited email (spam) can waste time and resources, and emails can use phishing attacks designed to trick users into releasing sensitive information. The Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations architecture transparently integrates an email security appliance-based solution that uses a variety of mechanisms to provide robust spam and virus filtering. The solution uses reputation-based and context-based filters that are kept current via automated, daily, attack-information updates to protect from spam as well as virus outbreaks.

The increasing need to access web applications in the Internet increases the risk of embedded attacks on unprotected users. Web security in the architecture is provided via a proxy service that uses category-based and reputation-based control, malware filtering, and data protection to protect assets from malicious web content. The system combines a constantly updated reputation database and dynamic content analysis to determine the nature of content in real time. Web security services also provide control for acceptable-use rules to ensure users are not accessing unacceptable content.

As organizations explore the benefits of a more mobile and flexible workforce, the ability to access the network from outside the walls of an office or remote site becomes highly desirable. Remote access enables the employee on the road or working from home to gain access to email, web applications, or update their calendar. Many companies are using remote access to allow partners to access resources in a trusted and secure way, while allowing policy to control what resources can be accessed. The design provides secure remote access for users via a software or hardware client. An SSL VPN solution offers maximum flexibility and provides secure connectivity for users and partners back to the organization's network, even from assets outside the organization's control, such as an employee's home computer. The solution also supports existing IPsec-based designs to allow organizations to tailor the design to their needs. As organizations deploy more teleworkers, a hardware VPN solution is required to support a more complete remote or home-office solution with 24x7 secure access for multiple devices such as desktops and a business-connected phone extension. The Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations solution provides teleworkers the same experience at home that they would have in the office.

Application Optimization

Application optimization improves the efficiency of the network by ensuring optimal use of WAN bandwidth through data redundancy elimination and caching services. In many cases, reducing existing non-optimized network traffic prevents organizations from having to add more bandwidth to WAN links to support a new application. Application optimization allows IT departments to centralize remote-site application servers in the data center while maintaining local LAN-like application performance by optimizing chatty LAN-developed protocols.

You can deploy an application optimization solution as clustered appliances at the WAN aggregation layer for scalable and resilient operation, and you can integrate the functionality in the remote-site routers for reduced footprint and operational simplicity. The design uses a consistent approach that simplifies the deployment and management, regardless of the form factor. The design transparently redirects traffic to application optimization engines to minimize application impact and reduce single points of failure. The tunnel-less approach of Cisco WAN optimization means that QoS policies can interoperate with optimized traffic and latency-sensitive multimedia traffic on the same links.

Application optimization provides the following benefits:

- Delays costly WAN bandwidth upgrades by optimizing the transported data
- Minimizes per-remote-site costs by centralizing the services driving IT consolidation, without sacrificing performance
- Centralizes management of all WAN optimization engines to simplify management and provide feedback on bandwidth savings
- Increases data protection by centralizing servers and storage

Guest and Partner Wireless Access

Organizations often have a wide range of visitors that require network access while they are on site. Visitors can include customers, partners, and vendors, and depending on their purpose, can vary in the locations they visit in your organization. To accommodate the productivity of this wide range of guest users and their roles, you should deploy guest access throughout the network and not only in lobby or conference room areas.

Providing wireless access to guests and partners has many benefits:

- Guests are more productive while on your premises to help your organization.
- A single infrastructure for employees and guests reduces cost and complexity.
- Secure transport keeps guest traffic segmented from the internal network.
- Guest access is controlled by IT but can be provided by administrative staff.

The flexibility of the Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations architecture allows the wireless network to provide guest access over the same infrastructure of wireless access points and controllers that provide employee wireless voice and data access. This integrated ability simplifies network operations and reduces capital and operational costs by leveraging a single infrastructure for multiple services.

The critical part of the architecture is to ensure that guest network access does not compromise the security of the network. Every access point at the headquarters and each remote site can be provisioned with controlled, open access to wireless connectivity. From the wireless access point, guest traffic is separately tunneled through the network to a guest wireless controller located in the Internet edge DMZ. Traffic is passed from the wireless guest network directly to the firewall protecting the organization's private assets.

To control guest and partner wireless connectivity, guest users are redirected to a web login screen and must present a username and password to connect to the guest network. Lobby ambassadors or other escorts can assign temporary guest accounts that require a new password daily or weekly. This design provides the flexibility to tailor control and administration for the organization's requirements while maintaining a secure network architecture.

User Services

Most users are familiar with the user-services layer because it enables the types of services or applications that they use daily. Everything else is built to support this layer, whether it's phoning someone, checking voicemail, checking email, or logging onto an enterprise resource planning (ERP) application, the user experience starts with the user-services layer. The design of user-oriented applications or products affects how easy it is to use, and how well the user service interacts with network services affects how it performs across the network. We designed the architecture to support the use of these data, voice, and video services on the network infrastructure.

Business Application Services

An organization's presence on the Internet plays a key role in its success. Downtime, even for simple information portals, can mean missed opportunities. Key applications such as email, e-commerce, web portals, and ERP must be available for use by both internal and external users around the clock to provide uninterrupted business service. Availability of these applications can be threatened by network overload, server failure, and application failure, or it can be degraded by poor resource utilization where some low-performance resources are overloaded and other high-performance resources remain idle. The high availability design of the Internet edge provides redundant firewalls, LAN switches, routers, ISP connections, and IPS to protect the application availability. One of the most critical high-availability services in the design is the application-level server load balancing, which has the ability to detect and react to application and server failures. Beyond the role of mainstream Layer 4 through 7 switching, server load balancing can also provide an array of acceleration and server-offload benefits, including TCP processing offload, SSL offload, compression, and various other acceleration technologies. The SLB environment can also be virtualized into separate logical partitions that can be independently configured in terms of topology, resource and functional usage, and management, providing a lower cost of ownership.

Communication and Collaboration Services

The evolution of communication and collaboration services is changing how we work and live. The role of the computer has developed over the years from document preparation and systems access to being integrated into how we communicate and collaborate. The desktop computer interacts with the desktop phone, the mobile phone, and other computers to share information in a variety of ways. Collaboration services are allowing us to change who we can communicate with, how we communicate with them, and when we communicate. Who we communicate with is becoming much more cross-functional as we utilize easy-to-use, secure collaboration tools to work with communities that are intra- and inter-company, including partners, customers, and knowledge workers. When we work is no longer fixed as organizations transform into anytime, anywhere workplaces to facilitate more rapid decision making that does not tether users to their offices for long hours. Where we work changes as the requirements of when we work changes. With mobility and wireless services, we can proceed with business from the office or from the comfort of our home for an early or late meeting, while we wait in an airport for a flight or use video collaboration to avoid the need for travel.

The following sections introduce some examples of Cisco communications and collaboration services available to your organization.

Unified Communications

The Cisco Unified Communications (UC) suite of products is designed to deliver voice and video communications that scale from a few users to tens of thousands of users. The IP communications solutions and endpoints let you extend consistent communications services to users in all workspaces, whether they are on a headquarters LAN, at a remote site, working from home, or on the road. Cisco Unified Communications Manager (Unified CM) is a scalable, distributable, and highly available enterprise-class IP telephony call-processing system that provides traditional telephony features as well as advanced capabilities, such as mobility, presence, and preference. The Cisco UC solution also enables companies to conduct highly secure, high-quality, voice and video telephone calls between companies across the Internet using their existing telephone numbers, increasing the effectiveness of the communications system.

Cisco Unified IP Phones support a range of requirements with support for interactive video, Wi-Fi integration, and high-definition voice, and when connected to the Cisco LAN switch, they communicate parameters to automate power, QoS, VLAN assignment, and infrastructure security settings. Cisco Unified Survivable Remote Site Telephony (SRST) runs in Cisco IOS on remote routers and provides backup call control for remote sites in the event of lost connectivity with the primary site, where the Unified CM is located. This ability to centralize call-processing resources reduces the cost of deployment while maintaining high availability that works with the network services provided by the remote-site routers.

WebEx—Video Collaboration

Meetings were once limited to face-to-face conferences in a single location, but meetings can now happen effectively across wide areas, spanning borders and time zones. The Cisco WebEx solution helps you meet the on-demand, borderless meeting requirement of your organization with the ability to serve broader workforce needs using any system, on any platform, and with any browser or device. WebEx uses the network foundation and services to provide a dedicated, carrier-grade, cloud-based service for dynamic, real-time web meetings, webinars, and webcasts. The WebEx Node gateway card for the Cisco ASR router provides a network service that delivers bandwidth savings by locally replicating data and video streams at the Internet edge versus sending all streams over the network. Meeting control and administration remain in the cloud for a seamless, transparent solution. WebEx functionality extends to wireless smartphones to accommodate the mobile user with application plugin modules that support simplified meeting access and the ability to view slides and other meeting collaboration tools.

TelePresence—Video Collaboration

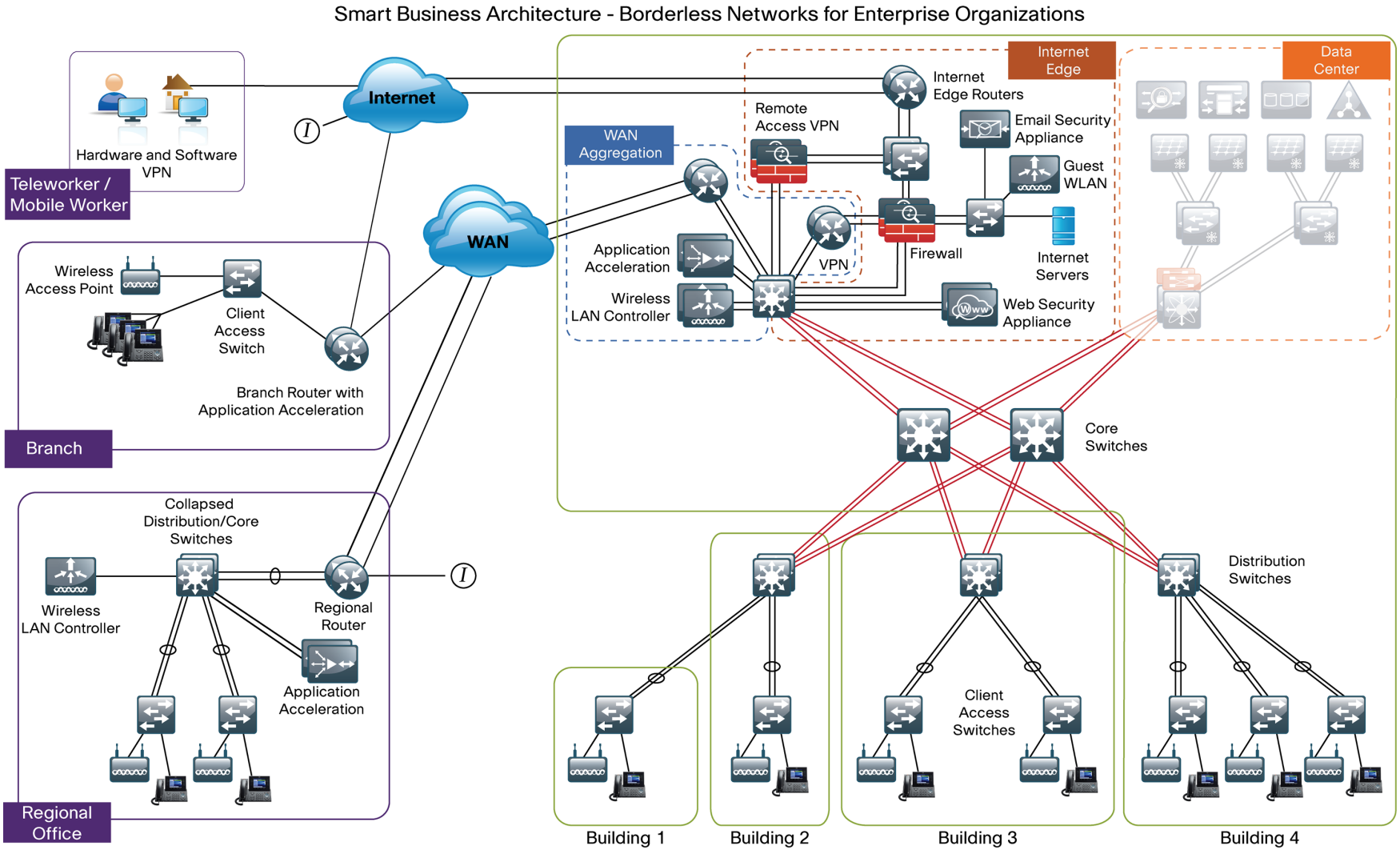
Many meetings call for face-to-face communications that previously required all participants to be in the same room. The Cisco TelePresence solution creates a live, lifelike, and life-sized communication experience like that of in-person meetings. The ability to efficiently transport high-definition video and audio across wide areas and to multiple locations simultaneously allows organizations to reduce travel costs and meeting delays. Integration with the Cisco Unified Communications solutions makes launching a meeting as simple as a phone call. WebEx collaboration and existing video conferencing systems can be added into a live session for increased versatility. Integration with the network helps ensure reliability with the resilient network foundation and QoS to provide the optimal experience.

Notes

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 the ability to deploy, operate, troubleshoot, and manage complexity and costs.

Figure 9 - Borderless Networks for Enterprise Organizations overview



The Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations is composed of three primary modular interdependent components. They are the network foundation, network services, and the user services, with hierarchical interdependencies between these three components. Each layer relies on the layer below. The three layers must work in a cohesive manner to deliver the data, voice, and video traffic that your organization needs to operate.

The Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations design provides a prescriptive solution based on best practices and tested topologies with network scalability choices to accommodate your organization's requirements. The companion deployment and configuration guides provide step-by-step guidance for deploying the solution. To enhance the Enterprise architecture, there are a number of supplemental guides that address specific functions, technologies, or features that may be important to solving your business problems. Cisco aims to simplify the process of purchasing, deploying, and maintaining your network while using the intelligence built into the selected products—products selected and tested to work together to build the Borderless Network.

Deploying the 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

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.**

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

B-0000117-1 12/11