Newer Cisco SBA Guides Available

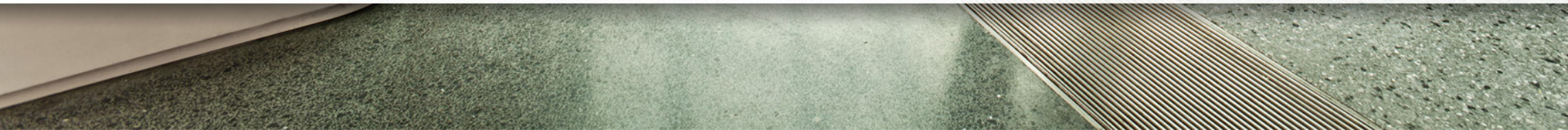
This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

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.

LAN Design Overview

SMART BUSINESS ARCHITECTURE

August 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 series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

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

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

month year Series

For example, the series of guides that we released in August 2012 are the "August 2012 Series".

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

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

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

How to Read Commands

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

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

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

```
Router# enable
```

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

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

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

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

Comments and Questions

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

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

Table of Contents

What's In This SBA Guide 1

Cisco SBA Borderless Networks 1

Route to Success 1

About This Guide 1

Introduction 2

Business Overview 4

Why Is a Cohesive Approach to the Network Architecture a Value to Your Organization? 4

Cisco SBA LAN Architecture 6

The Wired LAN 6

Guest and Partner Wireless Access 15

Summary 17

What's In This SBA Guide

Cisco SBA Borderless Networks

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

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

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

Route to Success

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

About This Guide

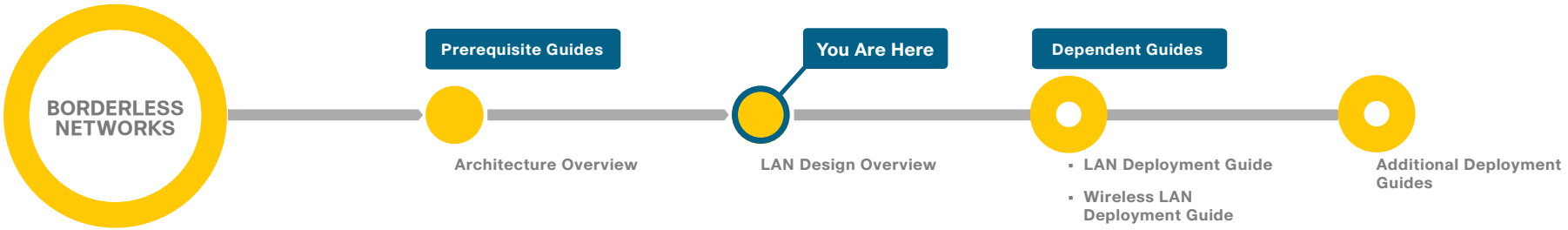
This *design overview* provides the following information:

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

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

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

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



Introduction

Cisco Smart Business Architecture (SBA) is a comprehensive design that incorporates LAN, WAN, security, application optimization, data center, and unified communications technologies to provide a complete solution for an organization's business challenges. The Cisco SBA—Borderless Network LAN architecture incorporates network access for wired and wireless users, ranging from small remote sites with a few connected users to large locations with up to 5,000 connected users.

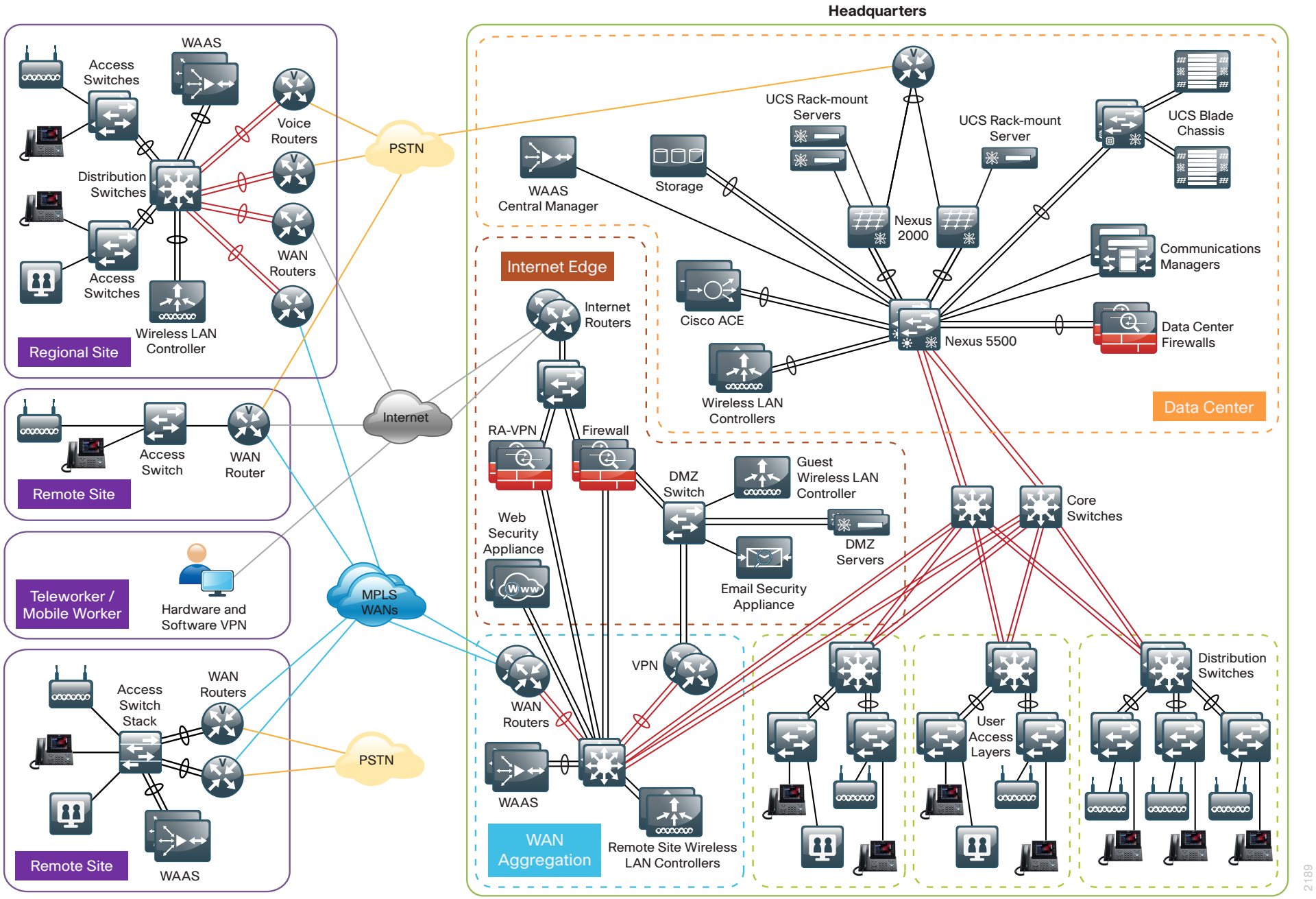
The Cisco SBA LAN provides the foundation network connectivity for users, printers, WAN routers, security, and all of the other devices that connect users to the applications they require to do their job. Because the LAN plays such an important role in providing the backbone interconnects for network communications, it's critical that the design is reliable, scalable, and interoperates transparently with devices connected to the LAN.

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

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

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

Figure 1 - Cisco Smart Business Architecture overview



Business Overview

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

Users are no longer expected to sit at their desk, tethered to a wired network connection for high-speed connectivity. Although wired network access to the user desktop provides the best performance, wireless network access provides the freedom of connecting the user to their applications while in meeting rooms, cafeteria, and other locations. The organization must build a LAN environment that provides reliable desktop and mobile access to improve user productivity.

Collaboration applications, such as those that use multimedia to bring users together, help an organization control the delays and costs associated with travel. Multimedia collaboration applications and content distribution rely on a high-speed, low-latency network infrastructure to provide an effective user experience. However, as networks become more complex, the level of risk increases for network availability loss or poor performance due to inadequate design, configuration errors, maintenance and upgrade outages, or hardware and software faults.

As organizations upgrade their IT infrastructure to support new business requirements, new technology can impose significant costs, from the perspective of the investment in the equipment, as well as the time and workforce investment required to deploy the new technology and establish operational readiness. When new technology is introduced, it takes time to understand how the technology operates and to ascertain how to effectively integrate the new technology into the existing infrastructure.

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

The days of conducting business with information stored locally in files on your computer are disappearing rapidly. The trend is for users to access mission-critical information by connecting to the network and downloading the information or by using a network-enabled application. Users depend upon shared access to common secured storage, web-based applications, and even cloud-based services. Users may start their day at home, in the office, or from a coffee shop, expecting to log on to applications that they need in order to conduct business, update their calendar, or check email—all important tasks that support your business. Connecting to the network to do your work has become as fundamental as turning on a light switch to see your desk; it's expected to work. Taken a step further, the network becomes a means to continue to function whether you are at your desk, roaming over wireless LAN within the facility, or working at a remote site, and you still have the same access to your applications and information.

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

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

- Reduced cost of deploying a standardized design based on Cisco-tested and supported best practices
- Multiple LAN scalability design models to address a variety of organization sizes and locations, to allow easy migration
- Focused approach on building a consistent and sound LAN foundation for organizations with LAN connectivity requirements at sites ranging from a few connected users to large locations with up to 5,000 connected users
- Wired and wireless LAN connectivity tested as a solution to address connectivity, mobility, and performance requirements
- Provide guest Internet access for visitors and contractors at your organization's locations in a convenient, cost-effective, and secure way
- Resiliency and availability of network access through proper use of network design 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

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

Notes

Cisco SBA LAN Architecture

There is a tendency to discount the network as just simple plumbing, to think that all you have to consider is the size and the length of the pipes or the speeds and feeds of the links, and to dismiss the rest as unimportant. Just as the plumbing in a large stadium or high rise has to be designed for scale, purpose, redundancy, protection from tampering or denial of operation, and the capacity to handle peak loads, the network requires similar consideration. As users depend on the network to access the majority of the information they need to do their jobs and to transport their voice or video with reliability, the network must be able to provide resilient, intelligent transport. 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 Cisco SBA LAN design incorporates both wired and wireless connectivity for a complete network access solution. This document will first explain the wired LAN foundation, and then second, how the wireless LAN extends secure network access for your mobile workforce by using 802.11 Wi-Fi technology, and finally how your 802.11 wireless LAN can provide guest access for contractors and visitors to your facilities.

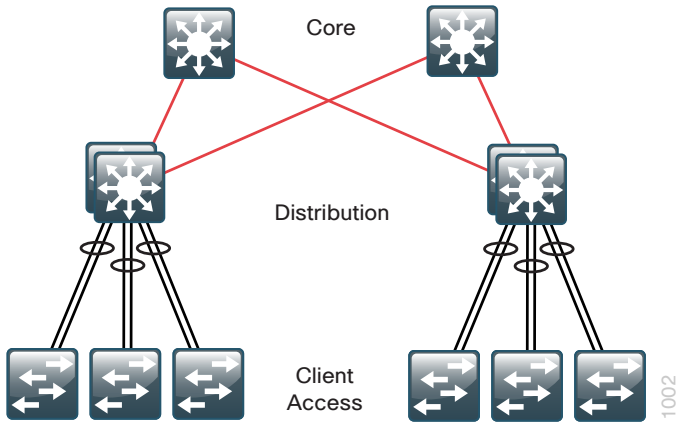
The Wired LAN

LAN access is typically provided at all of an organization's locations; however, larger LANs are usually located at organization headquarters or large campus locations. 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.

Large LANs or campus networks require a high availability 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 SBA LAN design, all links are actively forwarding traffic for a higher-performance network while reducing the complexity involved in traditional redundant designs.

To accommodate growth from a small number of users to a very large number of users, network engineers build LANs in layers, as shown in Figure 2. Cisco designed the Cisco Smart Business Architecture—Borderless Networks LAN to accommodate up to 5,000 users. It employs a layered approach to allow intuitive and seamless scalability.

Figure 2 - LAN hierarchical design



LAN Access Layer

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. This protection includes making sure that the devices connecting to the network do not attempt to provide services to any end users that are not authorized, that they do not attempt to take over the role of any other device on the network, and, when possible, that they verify the device is allowed on the network. The access layer also provides automated services like Power over Ethernet (PoE), quality-of-service (QoS) settings, and VLAN assignment for IP telephones in order to reduce operational requirements.

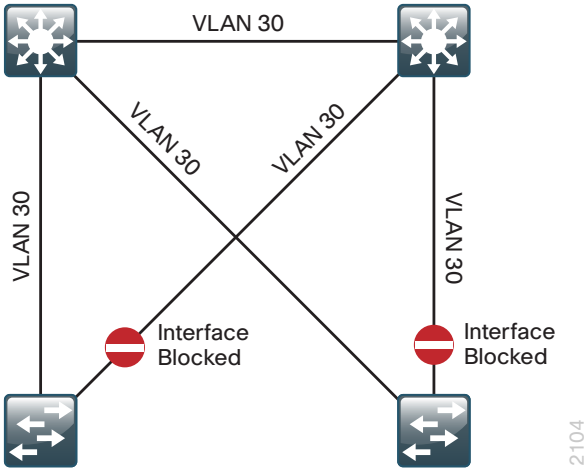
The Cisco SBA LAN access layer is a Layer 2 design to allow organizations to accommodate those scenarios where a specific VLAN is required to span multiple access-layer closets in order to satisfy an application requirement.

In the access layer, Cisco Catalyst 3560-X or 2960-S Series Switches are used for smaller density locations and can provide up to 48 access ports. For higher density wiring closets, a Cisco Catalyst 2960-S Series switch stack can provide up to 192 ports. For high-density wiring closets, modular Cisco Catalyst 4500 and 3750-X Series Switches provide 48-200+ ports. Cisco Catalyst 3750-X Series provides enhanced capabilities over Cisco Catalyst 2960-S Series in a switch stack application, with Cisco StackPower, medianet, and Cisco IOS Sensor. Cisco Catalyst 4500 Series provides modular upgrades, in-service software upgrades (ISSU), and sub-second failover with dual supervisor applications, medianet and IOS Sensor.

LAN Distribution Layer

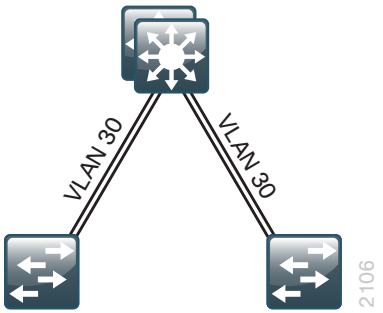
The distribution layer of the network serves primarily as an aggregation point when multiple access-layer switches are needed to support the required number of users at a location. Beyond simple aggregation, the distribution layer serves in many designs as the first point of IP Layer 3 packet switching, routing, and services. Because the distribution layer serves a larger number of users and access locations, it requires a high availability 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), in order 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, as shown in Figure 3. 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 in order 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



The Cisco SBA LAN 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, as shown in Figure 4, uses EtherChannel and Multi-Chassis EtherChannel to allow active forwarding of redundant access-layer uplinks. EtherChannel and Multi-Chassis EtherChannel (MCEC) 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.

Figure 4 - Simplified design when sharing VLANs



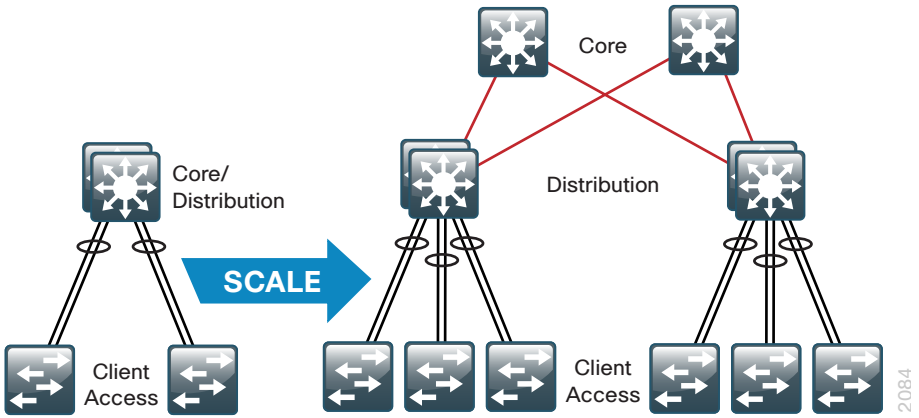
The simplified architecture provides the following benefits:

- 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

LAN Core Layer

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 point-to-point, Layer 3 IP-routed links. The core layer provides a natural migration from a smaller two-tier network to a larger three-tier network, by keeping a consistent distribution-layer design and adding the core layer for scalability.

Figure 5 - Two-tier to three-tier scalability



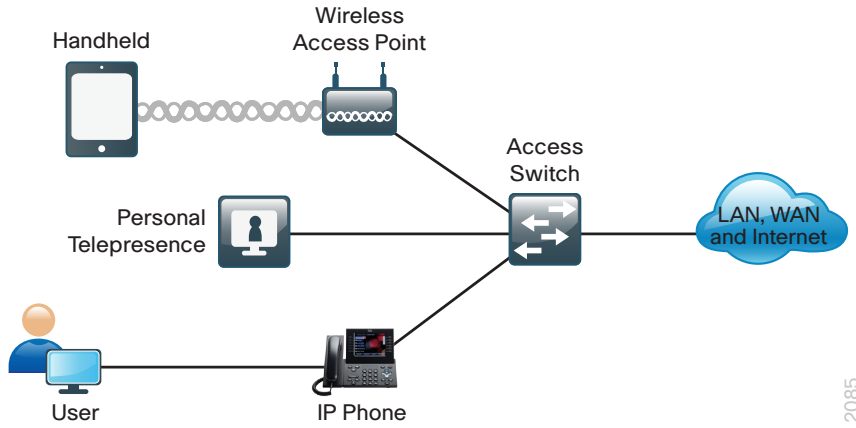
Because it is the core layer of the expanded LAN, the interconnect for the WAN and the Internet edge, and the connection point to a collocated data center, it has a 24x7x365 design criteria, the highest possible availability. Cisco designed the core layer to eliminate high complexity or high-touch services in order to reduce planned or unplanned outages for upgrades, maintenance, or complex configuration changes. The core layer is based on two high-performance 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 SBA LAN architecture provides a modular approach with multiple scale points in order to meet your organization's specific requirements.

Single-Tier LAN Design Model

Remote-site locations with a single wiring closet providing user connectivity can utilize a single access-layer switch for wired user access, WAN router, and wireless LAN access-point connectivity. Depending on the number of LAN ports required, you can install single Cisco Catalyst 3560-X or 2960-S Series Switch for up to 48 ports, and for higher density, a Cisco Catalyst 2960-S Series switch stack can provide up to 192 ports. For high-density wiring closets, the Cisco Catalyst 3750-X Series switch stack or a modular Cisco Catalyst 4500 Series switch can provide over 200 ports in a single wiring closet. The same access-layer functions, such as PoE, network security, and QoS, that are provided in larger locations are also provided in remote-site locations in order to ensure the same experience for connected users. The single or dual WAN router for the remote site provides all Layer 3 routing for the remote-site LAN.

Figure 6 - Single-tier remote-site LAN

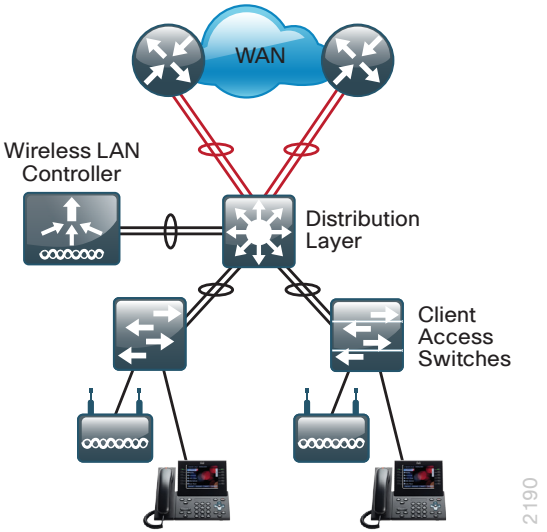


Two-Tier LAN Design Model

When a location has multiple wiring closets providing user connectivity, the distribution layer provides an aggregation point for connecting all of the wiring closets. In the Cisco SBA LAN design, the distribution layer provides Layer 3 services for the LAN according to the simplified design of a single physical or logical Layer 3 switch. Connections from the access-layer switches to the distribution layer use EtherChannel or MCEC for resiliency and STP loop-free connectivity.

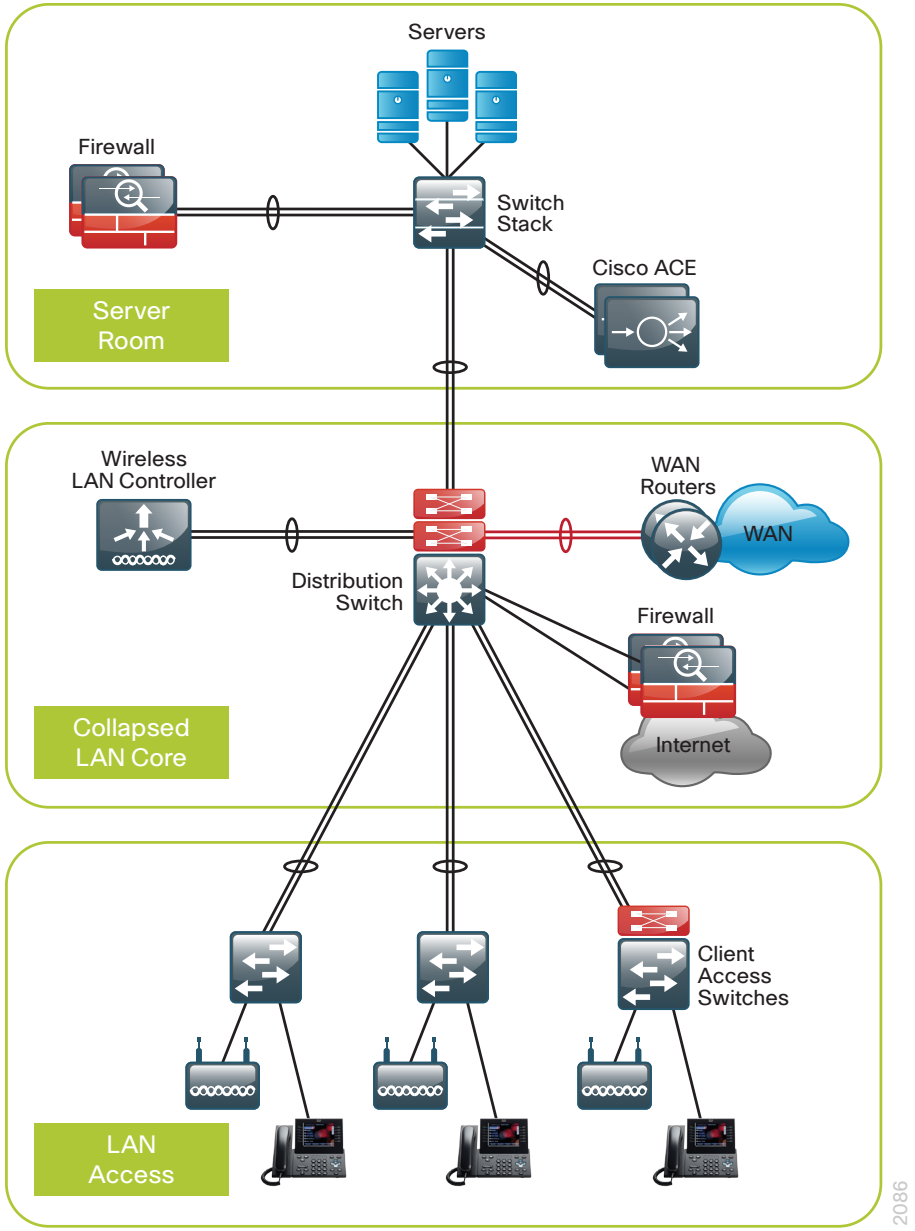
At a remote site, the distribution layer also provides connectivity for the WAN router or routers, and local wireless LAN controllers.

Figure 7 - Two-tier remote-site LAN



At a larger location or small headquarters, the distribution layer may function as a *collapsed core*, providing centralized connectivity for access-layer wiring closets, WAN routers, a server room, and Internet edge as an example.

Figure 8 - Two-tier collapsed LAN core



The Cisco SBA LAN design provides the following Layer 3 distribution layer platforms in order to provide a consistent, simplified distribution-layer design with multiple scale points:

- A highly resilient and scalable distribution layer with two modular chassis-based platforms using Cisco Catalyst 6500 Virtual Switching System (VSS) 4T, which acts as a single logical distribution-layer platform. This design allows for high-density aggregation of Gigabit Ethernet and 10-Gigabit Ethernet connected wiring closets and other platforms. Cisco Catalyst 6500 VSS 4T provides the most advanced feature set and the highest resiliency of the available platforms.
- A resilient modular Cisco Catalyst 4507R+E Series distribution-layer switch for locations where there is a mix of Gigabit Ethernet or 10-Gigabit Ethernet connected wiring closets and other platforms that need to be aggregated. The Cisco Catalyst 4507R+E switch with dual supervisors and dual power supplies provides resiliency with ISSU and sub-second failover.
- A stackable Cisco Catalyst 3750-X Series distribution-layer switch to accommodate locations where there is a small number of Gigabit Ethernet connected wiring closets and other platforms that need to be aggregated. Cisco Catalyst 3750-X Series provides a resilient platform with Cisco StackWise and Cisco StackPower, and it provides near-second failover from failed stack-member switches.

Three-Tier LAN Design Model

In larger LAN locations, a core layer is added to aggregate multiple distribution layers in order to accommodate the following situations:

- A large number of access-layer closets are spread over multiple floors or buildings
- Geographically dispersed clusters of remote buildings where running fiber from each access-layer switch to a central aggregation is not cost effective
- The number of network-service devices, WAN routers, and separate functional modules exceed the platform density or operational complexity of a two-tier design

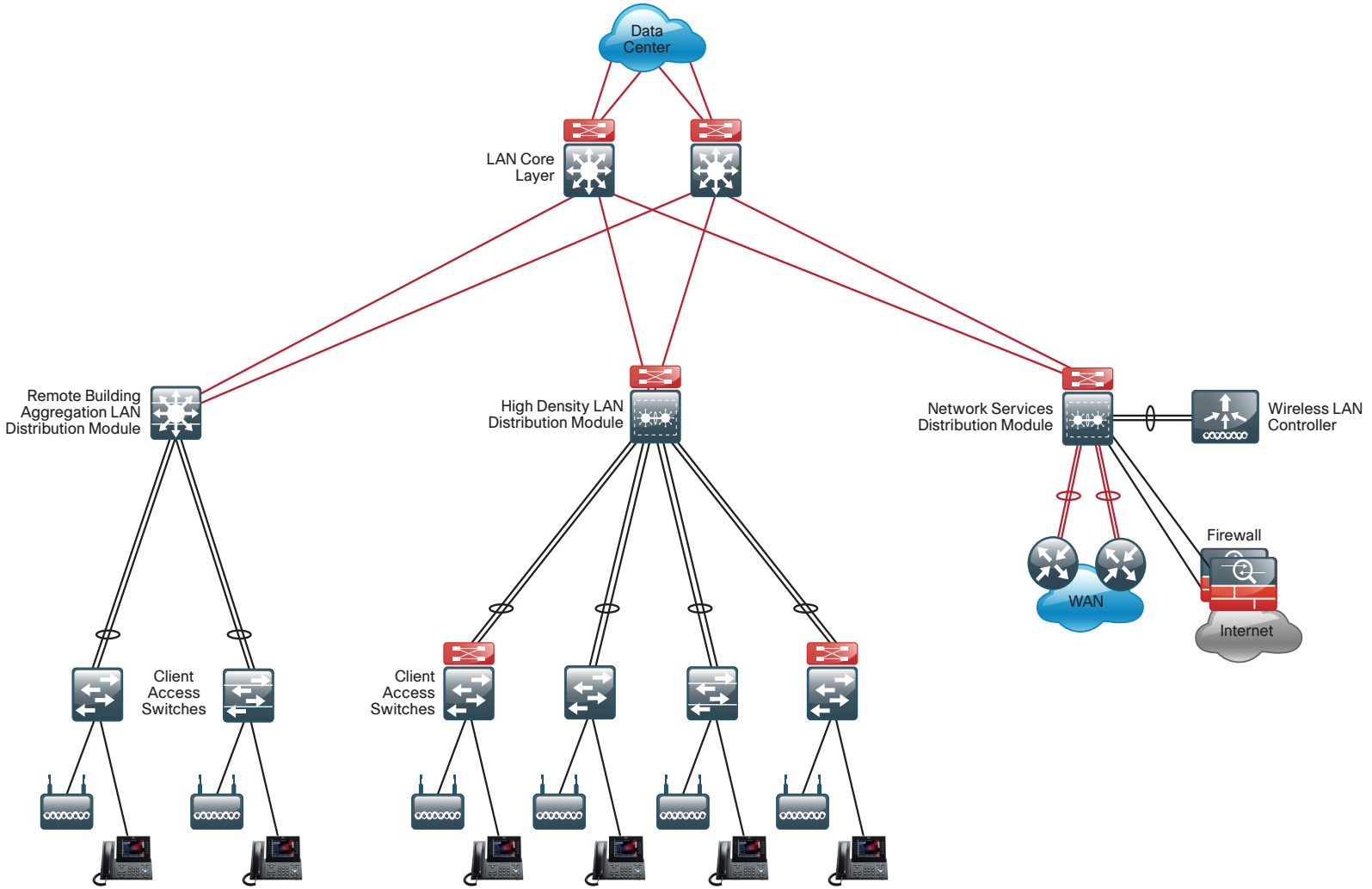
Notes

In the three-tier model, the addition of a separate "services" distribution layer provides:

- Modular growth for high densities of WAN headend routers and WAN services, such as a Cisco Wide Area Application Services appliance.
- Wireless LAN controller termination in a central location for larger campus populations.
- Fault domains separate from the LAN access for a more resilient overall network.
- IP address summarization from WAN or Internet edge toward the core of the network.

The core layer of the Cisco SBA LAN architecture uses two independent Cisco Catalyst 6500 Supervisor 2T Series switches to provide resilient high-density, high-bandwidth Layer 3 aggregation.

Figure 9 - Three-tier LAN design



The Wireless LAN

Providing the ability to stay connected regardless of employee location improves the effectiveness and efficiency of employees. 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 Cisco Smart Business Architecture, wireless uses Wi-Fi technology to transport data, voice, and even video traffic, rather than using cellular technology.

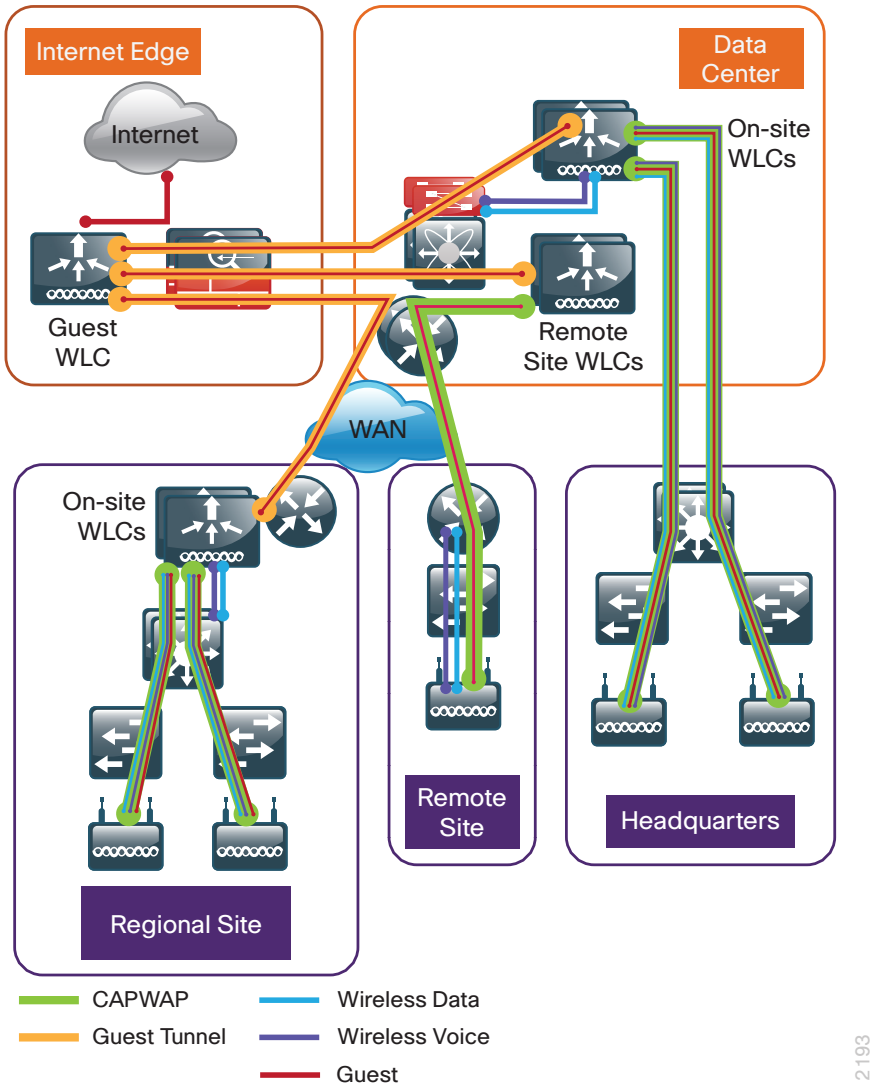
Users at remote sites or headquarters can connect to voice and data services via the same methods, creating a seamless environment for your enterprise.

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 10 - Cisco SBA wireless topology



The Cisco SBA wireless LAN 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.

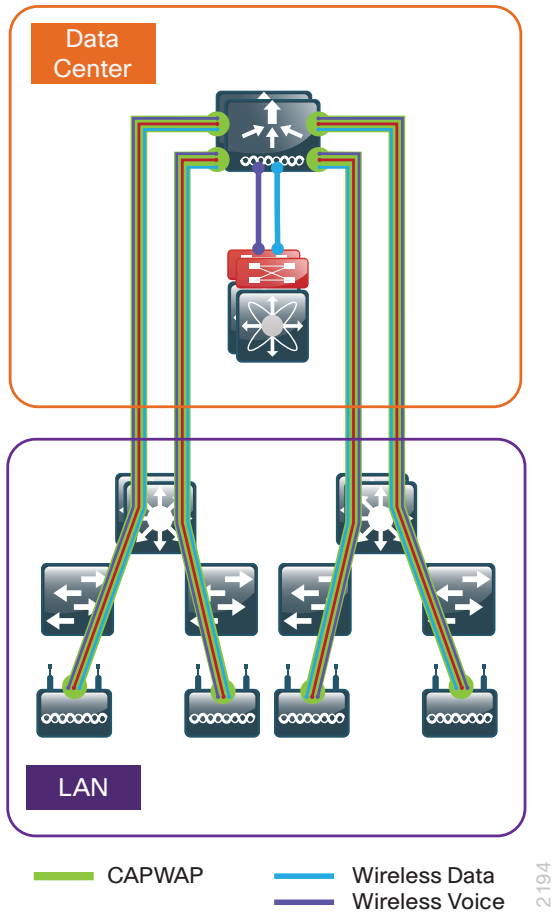
While the WLC is centralized for headquarters and most remote sites, you can install local WLCs in larger locations, to provide optimal roaming capabilities while still managing from a central location. Wireless access points at remote sites without local WLCs provide direct access to the local LAN for 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 Cisco SBA wireless LAN design uses the flexibility of the Cisco Unified Wireless Network to support two major design models: local mode and Cisco FlexConnect.

Local-Mode Deployment

In a local-mode deployment, as shown in Figure 11, the wireless LAN controller and access points are co-located at the same site. The wireless LAN controller is connected to a LAN distribution layer at the site, and traffic between wireless LAN clients and the LAN is tunneled in Control and Provisioning of Wireless Access Points (CAPWAP) protocol between the controller and the access point.

Figure 11 - Cisco SBA wireless local-mode deployment



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

In addition to providing the traditional benefits of a Cisco Unified Wireless Network approach, the local-mode deployments have the following customer demands:

- **Seamless mobility**—In a campus environment, it is crucial that users remain connected to their session even while walking between various floors or adjacent buildings with changing subnets. The local controller–based Cisco Unified Wireless Network enables fast roaming across the campus.
- **Ability to support rich media**—As wireless network access has become pervasive in many campus environments, voice and video applications have grown in significance. Local-mode deployments enhance robustness of voice with Call Admission Control (CAC) and multicast with Cisco VideoStream technology.
- **Centralized policy**—The consolidation of data at a single place in the network enables intelligent inspection through the use of firewalls, as well as application inspection, network access control, and policy enforcement. In addition, network policy servers enable correct classification of traffic from various device types and from different users and applications.

If any of the following are true at a site, Cisco recommends deploying a controller locally at the site:

- 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

In a deployment with these characteristics, Cisco SBA recommends using either a Cisco 2500 or 5500 Series Wireless LAN Controller. For resiliency, the design uses two wireless LAN controllers, although you can add more wireless LAN controllers to provide additional capacity and resiliency to this design.

Cisco FlexConnect Deployment

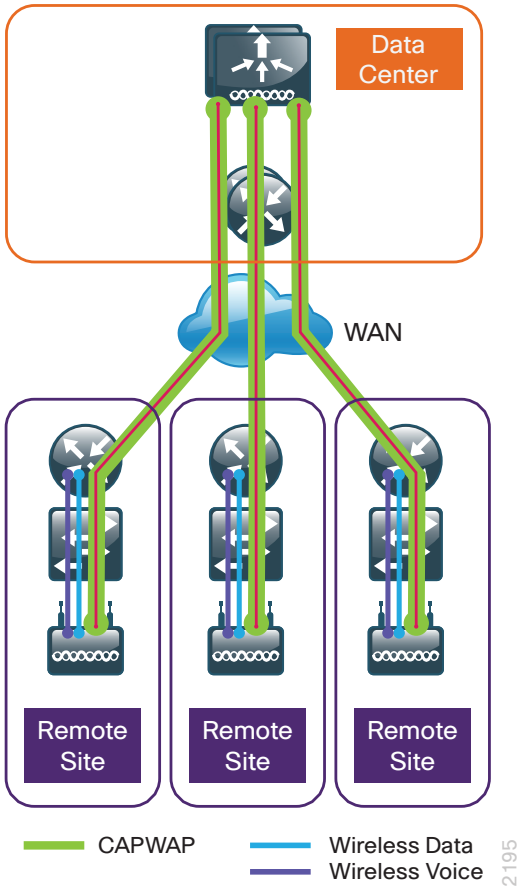
Cisco FlexConnect is a wireless solution for remote-site deployments. It enables organizations to configure and control access points in a remote site from the headquarters through the WAN without deploying a controller in each remote site.

If all of the following are true at a site, Cisco recommends deploying 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

The Cisco FlexConnect access point switches client data traffic out its local wired interface and uses IEEE 802.1Q trunking in order to segment multiple WLANs. The trunk native VLAN is used for all CAPWAP communication between the access point and the controller.

Figure 12 - Cisco SBA wireless Cisco FlexConnect deployment



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

You can deploy Cisco FlexConnect using a shared controller pair or a dedicated controller pair.

If you have an existing local-mode controller pair at the same site as your WAN aggregation, and if the controller pair has enough additional capacity to support the Cisco FlexConnect access points, you can use a shared deployment. In a shared deployment, the controller pair supports both local-mode and Cisco FlexConnect access points concurrently.

If you don't meet these requirements, you can deploy a dedicated controller pair using either the Cisco 5500 Series Wireless LAN Controller or a Cisco Flex 7500 Series Cloud Controller. The controller should be connected to the server room or data center. For resiliency, the design uses two controllers for the remote sites, although you can add more controllers to provide additional capacity and resiliency to this design.

Guest and Partner Wireless Access

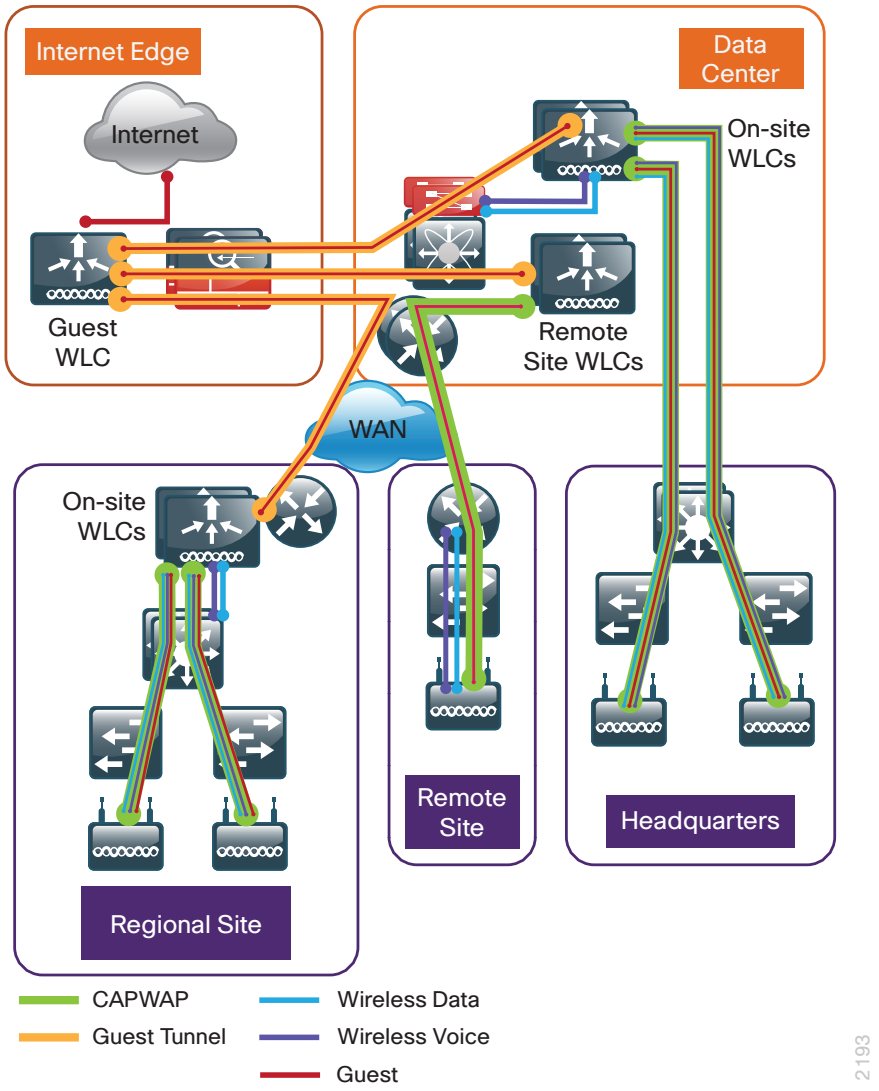
Organizations often have a wide range of visitors that require network access while they are on site. Visitors can include customers, partners, and vendors, and depending on their purpose, can vary in the locations they visit in your organization. To accommodate the productivity of this wide range of 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 SBA LAN 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.

Figure 13 - Cisco SBA guest access over wireless LAN



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 demilitarized zone (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.

Using the organization's existing WLAN for guest access provides a convenient, cost-effective way to offer Internet access for visitors and contractors. The wireless guest network provides the following functionality:

- Provides Internet access to guests through an open wireless Secure Set Identifier (SSID), with web access control
- Supports the creation of temporary authentication credentials for each guest by an authorized internal user
- Keeps traffic on the guest network separate from the internal network to prevent a guest from accessing internal network resources
- Supports both local-mode and Cisco FlexConnect deployment models

You can deploy a wireless guest network using a shared controller pair or a dedicated controller in the Internet DMZ.

If you have one controller pair for the entire organization and that controller pair is connected to the same distribution switch as the Internet edge firewall, you can use a shared deployment. In a shared deployment, a VLAN is created on the distribution switch to logically connect guest traffic from the WLCs to the DMZ. The VLAN will not have an associated Layer 3 interface or Switch Virtual Interface (SVI), and the wireless clients on the guest network will point to the Internet edge firewall as their default gateway.

If you don't meet the requirements for a shared deployment, you can deploy a dedicated guest controller using the Cisco 5500 Series Wireless LAN Controller. The controller is directly connected the Internet edge DMZ, and guest traffic from every other controller in the organization is tunneled to this controller.

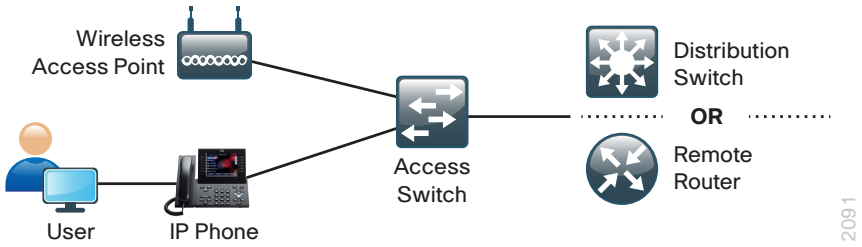
In both the shared and dedicated guest-traffic deployment model, the Internet edge firewall restricts access from the guest network. The guest network is only able to reach the Internet and the internal Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) servers.

Summary

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

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

Figure 14 - Consistent user connectivity



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

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

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

Notes

Feedback

Click here to provide feedback to Cisco SBA.

SMART BUSINESS ARCHITECTURE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

B-0000225-1 8/12