CHAPTER 1

Hierarchical Network Design

Objectives

Upon completion of this chapter

- What are the structured engineering principles of network design?
- How do you apply the three hierarchical network layers in network design?
- What are the four basic modules in an enterprise campus network architecture that interconnect via the core?
- How do the modules of the Cisco Enterprise Architecture model differ?
- What are some trends that are challenging enterprise network architectures?
- How do the Borderless Network, Collaboration Network, and Data Center/Virtualization Network architectures address the network challenges?

Key Terms

This chapter uses the following key terms. You can find the definitions in the glossary.

small network *page 3*

medium-size network *page 3*

large network *page 3*

access layer *page 6*

distribution layer *page 7*

core layer *page 9*

three-tier hierarchical design *page 10*

two-tier hierarchical design *page 10*

collapsed core *page 10*

modular network design *page 11*

Cisco Enterprise Architecture model *page 14*

enterprise campus module *page 15*

enterprise edge module *page 17*

SP edge module *page 18*

enterprise branch module *page 21*

enterprise teleworker module *page 22*

enterprise data center module *page 22*

Cisco Borderless Network Architecture *page 24*

Cisco Collaboration Architecture *page 25*

Cisco Data Center/Virtualization Architecture *page 26*

Introduction (1.0.1.1)

Networks must meet the current needs of organizations and be able to support emerging technologies as new technologies are adopted. Network design principles and models can help a network engineer design and build a network that is flexible, resilient, and manageable.

This chapter introduces network design concepts, principles, models, and architectures. It covers the benefits that are obtained by using a systematic design approach. Emerging technology trends that will affect network evolution are also discussed.

Class Activity 1.0.1.2: Design Hierarchy

A network administrator is tasked with designing an expanded network for the company.

After speaking with network administrators in other branches of the company, it was decided to use the Cisco three-layer hierarchical network design model to influence the expansion. This model was chosen for its simple influence upon network planning.

The three layers of the expanded network design include

- Access
- Distribution
- Core

Hierarchical Network Design Overview (1.1)

The Cisco hierarchical (three-layer) internetworking model is an industry wide adopted model for designing a reliable, scalable, and cost-efficient internetwork. In this section, you will learn about the access, distribution, and core layers and their role in the hierarchical network model.

Enterprise Network Campus Design (1.1.1)

An understanding of network scale and knowledge of good structured engineering principles is recommended when discussing network campus design.

Network Requirements (1.1.1.1)

When discussing network design, it is useful to categorize networks based on the number of devices serviced:

- *Small network*: Provides services for up to 200 devices.
- *Medium-size network*: Provides services for 200 to 1,000 devices.
- *Large network*: Provides services for 1,000+ devices.

Network designs vary depending on the size and requirements of the organizations. For example, the networking infrastructure needs of a small organization with fewer devices will be less complex than the infrastructure of a large organization with a significant number of devices and connections.

There are many variables to consider when designing a network. For instance, consider the example in Figure 1-1. The sample high-level topology diagram is for a large enterprise network that consists of a main campus site connecting small, medium, and large sites.

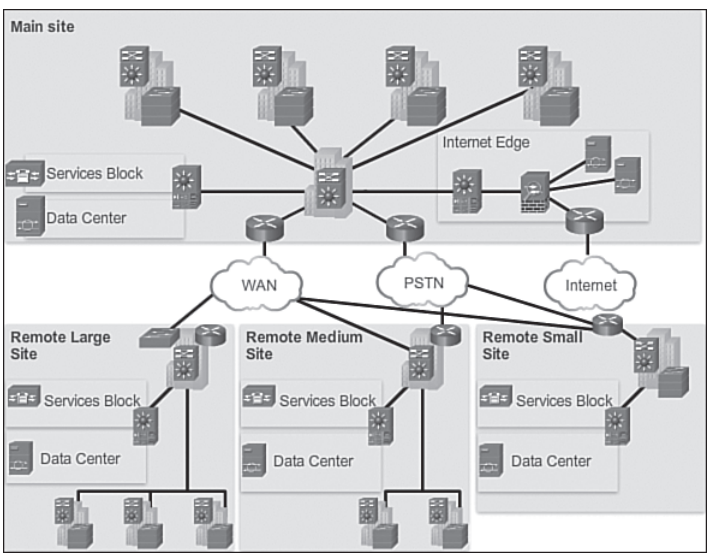

Figure 1-1 Large Enterprise Network Design

Network design is an expanding area and requires a great deal of knowledge and experience. The intent of this section is to introduce commonly accepted network design concepts.

Note

The Cisco Certified Design Associate (CCDA®) is an industry-recognized certification for network design engineers, technicians, and support engineers who demonstrate the skills required to design basic campus, data center, security, voice, and wireless networks.

Structured Engineering Principles (1.1.1.2)

Regardless of network size or requirements, a critical factor for the successful implementation of any network design is to follow good structured engineering principles. These principles include

- **Hierarchy**: A hierarchical network model is a useful high-level tool for designing a reliable network infrastructure. It breaks the complex problem of network design into smaller and more manageable areas.
- **Modularity**: By separating the various functions that exist on a network into modules, the network is easier to design. Cisco has identified several modules, including the enterprise campus, services block, data center, and Internet edge.
- **Resiliency**: The network must remain available for use under both normal and abnormal conditions. Normal conditions include normal or expected traffic flows and traffic patterns, as well as scheduled events such as maintenance windows. Abnormal conditions include hardware or software failures, extreme traffic loads, unusual traffic patterns, denial-of-service (DoS) events, whether intentional or unintentional, and other unplanned events.
- **Flexibility**: The ability to modify portions of the network, add new services, or increase capacity without going through a major forklift upgrade (i.e., replacing major hardware devices).

To meet these fundamental design goals, a network must be built on a hierarchical network architecture that allows for both flexibility and growth.

Hierarchical Network Design (1.1.2)

This topic discusses the three functional layers of the hierarchical network model: the access, distribution, and core layers.

Network Hierarchy (1.1.2.1)

Early networks were deployed in a flat topology as shown in Figure 1-2.

Hubs and switches were added as more devices needed to be connected. A flat network design provided little opportunity to control broadcasts or to filter undesirable traffic. As more devices and applications were added to a flat network, response times degraded, making the network unusable.

A better network design approach was needed. For this reason, organizations now use a hierarchical network design as shown in Figure 1-3.

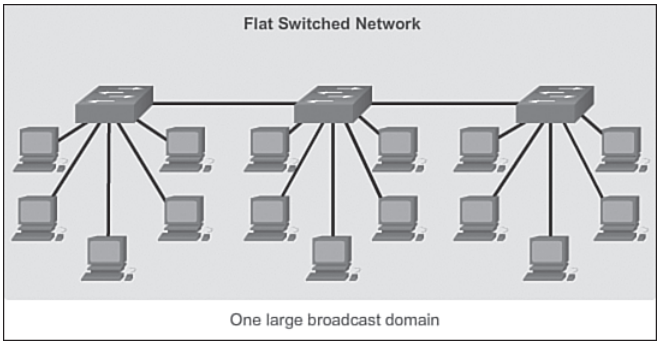

Figure 1-2 Flat Switched Network

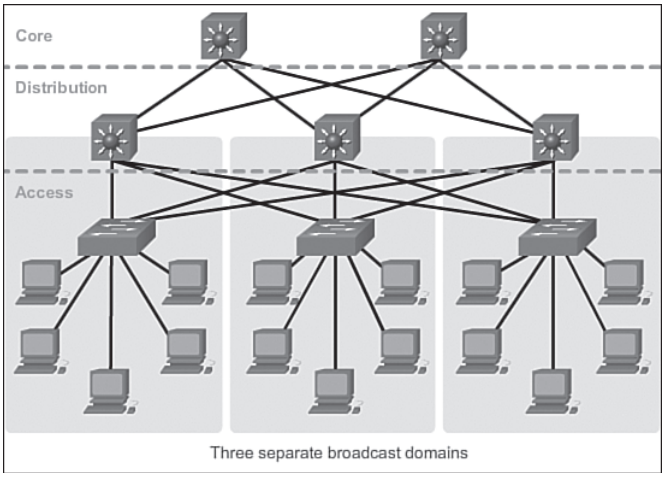

Figure 1-3 Hierarchical Network

A hierarchical network design involves dividing the network into discrete layers. Each layer, or tier, in the hierarchy provides specific functions that define its role within the overall network. This helps the network designer and architect to optimize and select the right network hardware, software, and features to perform specific roles for that network layer. Hierarchical models apply to both LAN and WAN design.

The benefit of dividing a flat network into smaller, more manageable blocks is that local traffic remains local. Only traffic that is destined for other networks is moved to a higher layer. For example, in Figure 1-3 the flat network has now been divided into three separate broadcast domains.

A typical enterprise hierarchical LAN campus network design includes the following three layers:

- **Access layer:** Provides workgroup/user access to the network
- **Distribution layer:** Provides policy-based connectivity and controls the boundary between the access and core layers
- **Core layer:** Provides fast transport between distribution switches within the enterprise campus

Another sample three-layer hierarchical network design is displayed in Figure 1-4. Notice that each building is using the same hierarchical network model that includes the access, distribution, and core layers.

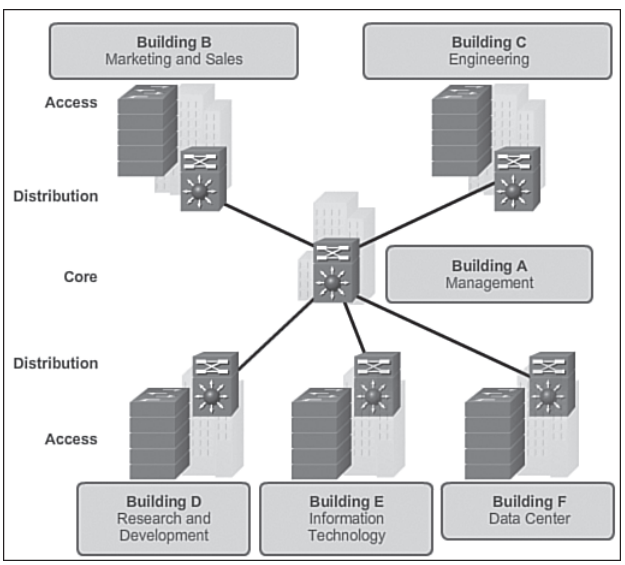

Figure 1-4 Multi Building Enterprise Network Design

Note

There are no absolute rules for the way a campus network is physically built. While it is true that many campus networks are constructed using three physical tiers of switches, this is not a strict requirement. In a smaller campus, the network might have two tiers of switches in which the core and distribution elements are combined in one physical switch. This is referred to as a collapsed core design.

The Access Layer (1.1.2.2)

In a LAN environment, the *access layer* highlighted grants end devices access to the network. In the WAN environment, it may provide teleworkers or remote sites access to the corporate network across WAN connections.

As shown in Figure 1-5, the access layer for a small business network generally incorporates Layer 2 switches and access points providing connectivity between workstations and servers.

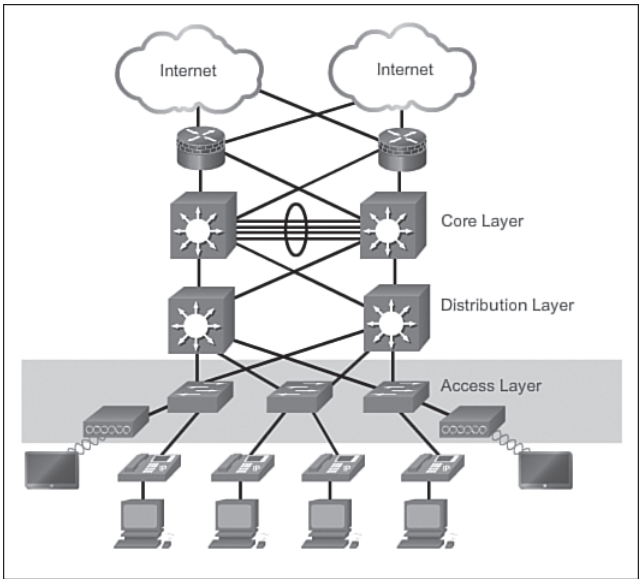

Figure 1-5 Access Layer

The access layer serves a number of functions, including

- Layer 2 switching
- High availability
- Port security
- QoS classification and marking and trust boundaries
- Address Resolution Protocol (ARP) inspection
- Virtual access control lists (VACLs)
- Spanning tree
- Power over Ethernet (PoE) and auxiliary VLANs for VoIP

The Distribution Layer (1.1.2.3)

The *distribution layer* aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. In Figure 1-6, the distribution layer is the boundary between the Layer 2 domains and the Layer 3 routed network.

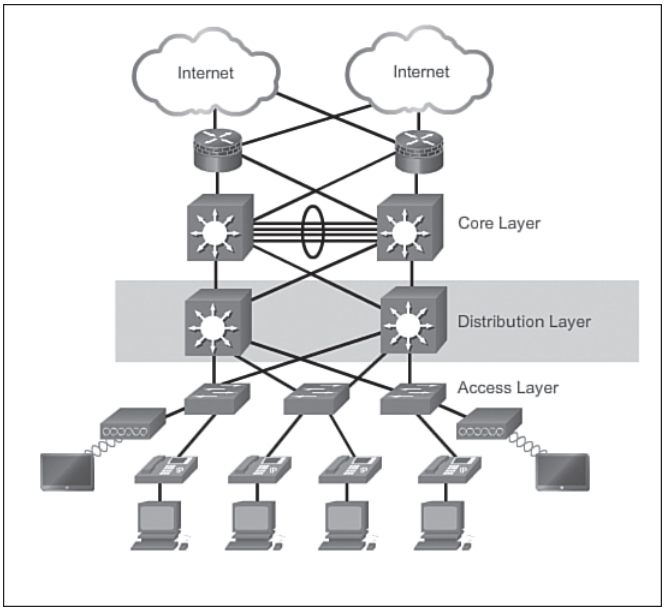

Figure 1-6 Distribution Layer

The distribution layer device is the focal point in the wiring closets. Either a router or a multilayer switch is used to segment workgroups and isolate network problems in a campus environment.

A distribution layer switch may provide upstream services for many access layer switches.

The distribution layer can provide

- Aggregation of LAN or WAN links.
- Policy-based security in the form of access control lists (ACLs) and filtering.
- Routing services between LANs and VLANs and between routing domains (e.g., EIGRP to OSPF).
- Redundancy and load balancing.
- A boundary for route aggregation and summarization configured on interfaces toward the core layer.
- Broadcast domain control, because routers or multilayer switches do not forward broadcasts. The device acts as the demarcation point between broadcast domains.

The Core Layer (1.1.2.4)

The *core layer* is also referred to as the network backbone. The core layer consists of high-speed network devices such as the Cisco Catalyst 6500 or 6800. These are designed to switch packets as fast as possible and interconnect multiple campus components, such as distribution modules, service modules, the data center, and the WAN edge.

As shown in Figure 1-7, the core layer is critical for interconnectivity between distribution layer devices (for example, interconnecting the distribution block to the WAN and Internet edge).

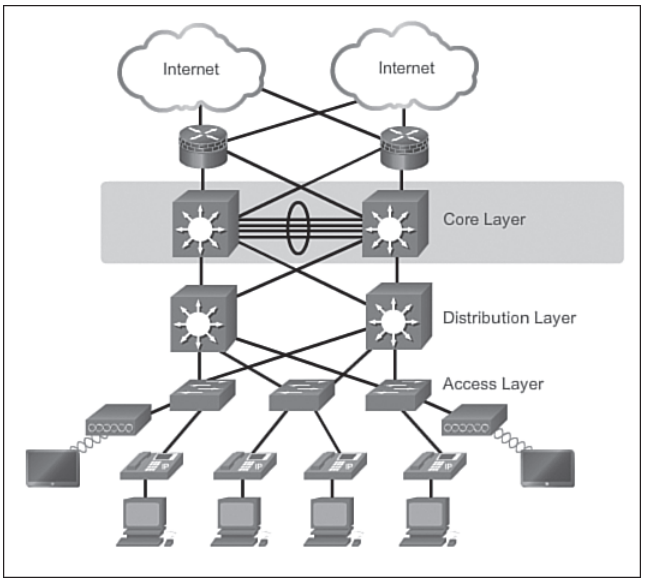

Figure 1-7 Core Layer

The core should be highly available and redundant. The core aggregates the traffic from all the distribution layer devices, so it must be capable of forwarding large amounts of data quickly.

Considerations at the core layer include

- Providing high-speed switching (i.e., fast transport)
- Providing reliability and fault tolerance
- Scaling by using faster, and not more, equipment
- Avoiding CPU-intensive packet manipulation caused by security, inspection, quality of service (QoS) classification, or other processes

Two-Tier Collapsed Core Design (1.1.2.5)

The *three-tier hierarchical design* maximizes performance, network availability, and the ability to scale the network design.

However, many small enterprise networks do not grow significantly larger over time. Therefore, a *two-tier hierarchical design* where the core and distribution layers are collapsed into one layer is often more practical. A "*collapsed core*" is when the distribution layer and core layer functions are implemented by a single device. The primary motivation for the collapsed core design is reducing network cost, while maintaining most of the benefits of the three-tier hierarchical model.

The example in Figure 1-8 has collapsed the distribution layer and core layer functionality into multilayer switch devices.

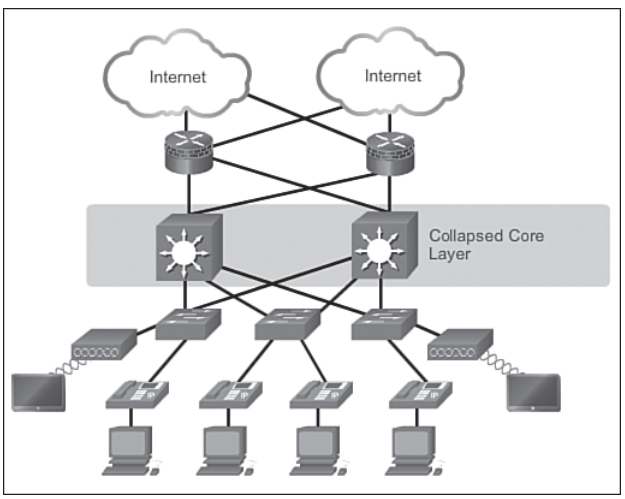

Figure 1-8 Two-Tier Hierarchical Design

The hierarchical network model provides a modular framework that allows flexibility in network design and facilitates ease of implementation and troubleshooting.

Interactive Graphic

Activity 1.1.2.6: Identify Hierarchical Network Characteristics

Go to the course online to perform this practice activity.

Cisco Enterprise Architecture (1.2)

The Cisco Enterprise Architecture is a modular approach to network design. This section identifies enterprise architecture modules that are commonly found in medium-to-large organizations.

Modular Design (1.2.1.1)

While the hierarchical network design works well within the campus infrastructure, networks have expanded beyond these borders. As shown in Figure 1-9, networks have become more sophisticated and complex. The central campus site now requires connections to branch sites and support for teleworking employees working from home offices or other remote locations. Large organizations may also require dedicated connections to offsite data centers.

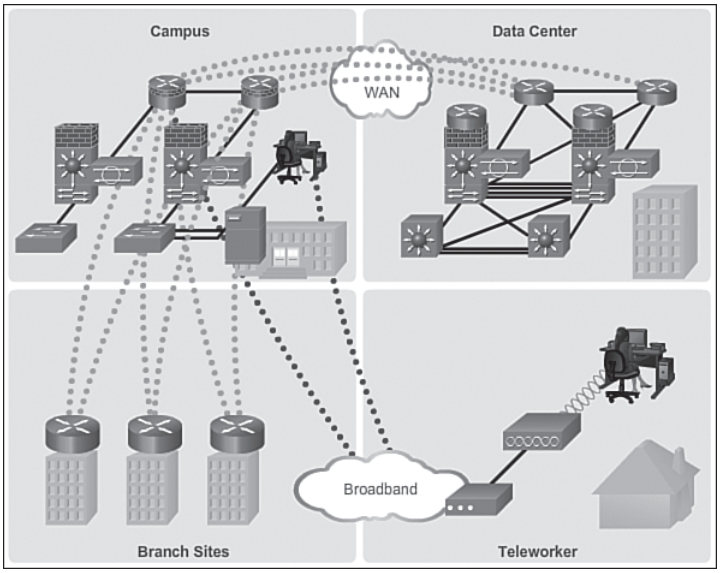

Figure 1-9 Expanding Beyond the Campus Infrastructure

As the complexity of the network increased to meet these demands, it became necessary to adjust the network design to one that uses a more modular approach.

A *modular network design* separates the network into various functional network modules, each targeting a specific place or purpose in the network. The modules represent areas that have different physical or logical connectivity. They designate where different functions occur in the network. Using a modular approach has several benefits, including

- Failures that occur within a module can be isolated from the remainder of the network, providing for simpler problem detection and higher overall system availability.
- Network changes, upgrades, or the introduction of new services can be made in a controlled and staged fashion, allowing greater flexibility in the maintenance and operation of the campus network.

- When a specific module no longer has sufficient capacity or is missing a new function or service, it can be updated or replaced by another module that has the same structural role in the overall hierarchical design.
- Security can be implemented on a modular basis allowing for more granular security control.

The use of modules in network design enables flexibility and facilitates implementation and troubleshooting.

Modules in the Enterprise Architecture (1.2.1.2)

A modular approach to network design further divides the three-layer hierarchical design by pulling out specific blocks or modular areas. These basic modules are connected together via the core of the network.

Basic network modules include

- **Access-distribution:** Also called the distribution block, this is the most familiar element and fundamental component of a campus design (see Figure 1-10).

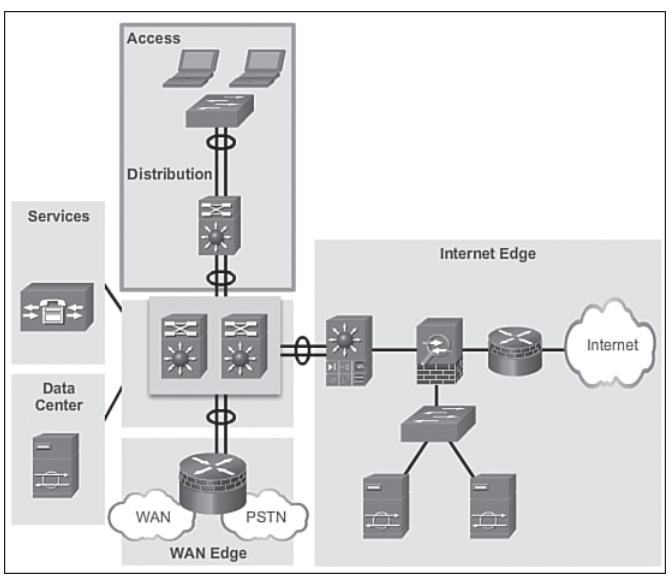

Figure 1-10 Access-Distribution Module

- **Services:** This is a generic block used to identify services such as centralized Lightweight Access Point Protocol (LWAPP) wireless controllers, unified communications services, policy gateways, and more (see Figure 1-11).

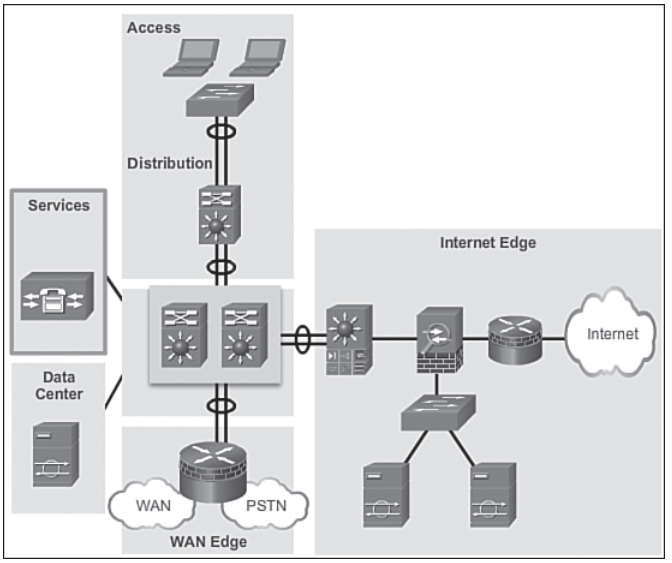

Figure 1-11 Services Module

- **Data center:** Originally called the server farm. This block is responsible for managing and maintaining many data systems that are vital to modern business operations. Employees, partners, and customers rely on data and resources in the data center to effectively create, collaborate, and interact (see Figure 1-12).

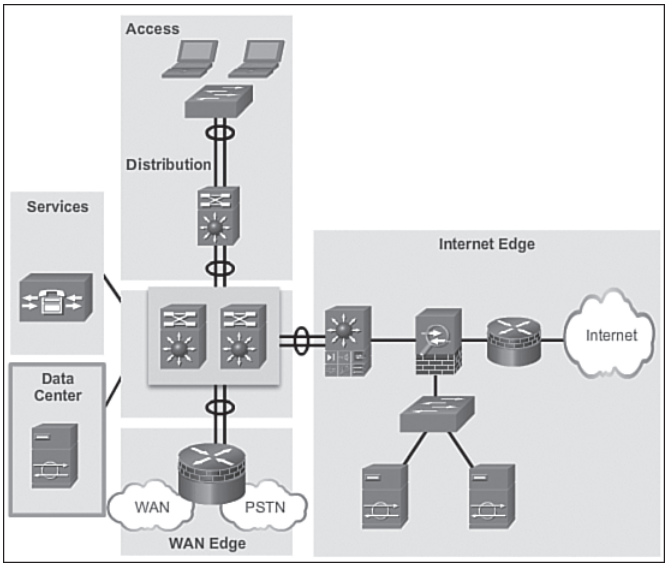

Figure 1-12 Data Center Module

- **Enterprise edge:** Consists of the Internet edge and the WAN edge. These blocks offer connectivity to voice, video, and data services outside the enterprise (see Figure 1-13).

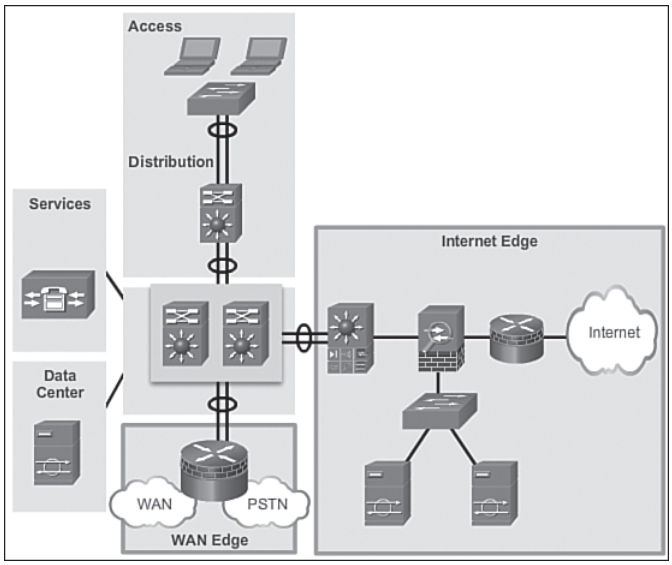

Figure 1-13 Enterprise Edge Module

Interactive Graphic

Activity 1.2.1.3: Identify Modules in a Network Design

Go to the course online to perform this practice activity.

Cisco Enterprise Architecture Model (1.2.2)

The Cisco Enterprise Architecture is a modular approach to network design. This topic discusses the enterprise campus module, enterprise edge module, and the service provider edge module.

Cisco Enterprise Architecture Model (1.2.2.1)

To accommodate the need for modularity in network design, Cisco developed the *Cisco Enterprise Architecture model*. This model provides all the benefits of the hierarchical network design on the campus infrastructure, and facilitates the design of larger, more scalable networks.

The Cisco Enterprise Architecture model separates the enterprise network into functional areas that are referred to as modules. The modularity that is built in to the architecture allows flexibility in network design and facilitates implementation and troubleshooting.

As shown in Figure 1-14, the following are the primary Cisco Enterprise Architecture modules:

- Enterprise campus
- Enterprise edge
- Service provider edge

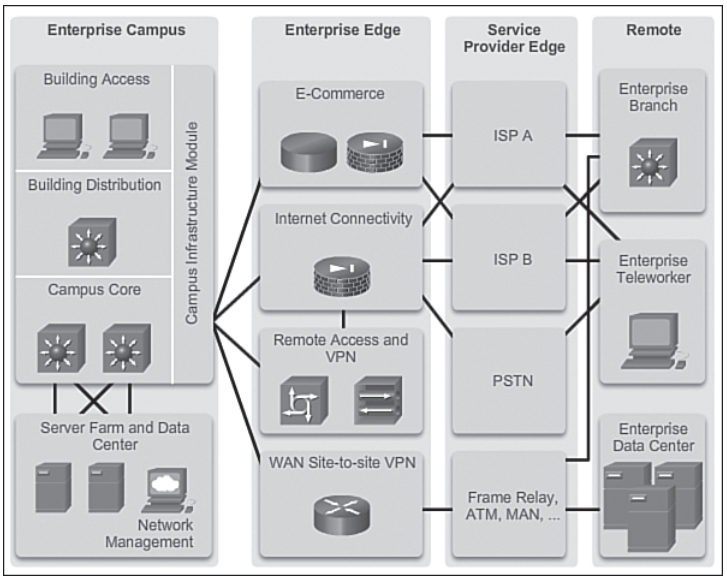

Figure 1-14 Cisco Enterprise Architecture Modules

Connected to the service provider edge are the remote modules, including

- Enterprise branch
- Enterprise teleworker
- Enterprise data center

Cisco Enterprise Campus (1.2.2.2)

A campus network is a building or group of buildings connected into one enterprise network that consists of many LANs. A campus is generally limited to a fixed geographic area, but it can span several neighboring buildings (for example, an industrial complex or business park environment). Regional offices, SOHOs, and mobile workers may need to connect to the central campus for data and information.

The *enterprise campus module* describes the recommended methods to create a scalable network while addressing the needs of campus-style business operations.

The architecture is modular and can easily expand to include additional campus buildings or floors as the enterprise grows.

As shown in Figure 1-15, the enterprise campus module consists of the following submodules:

- Building access
- Building distribution
- Campus core
- Data center

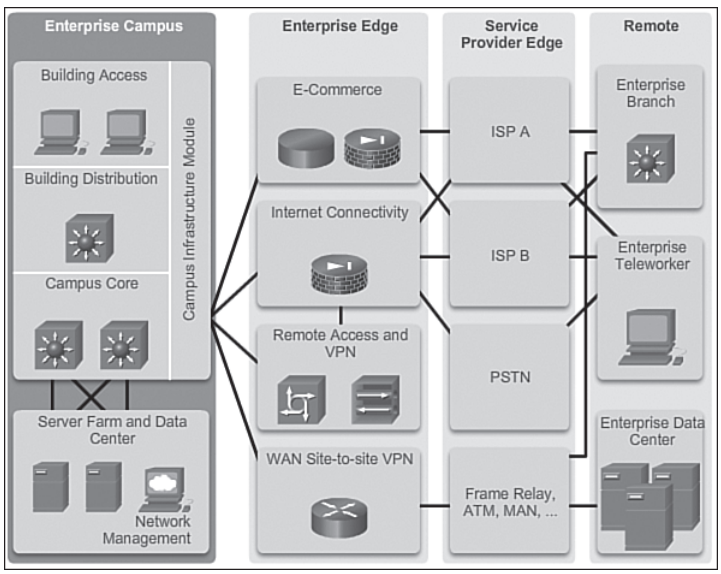

Figure 1-15 Enterprise Campus Module

Together these submodules

- Provide high availability through a resilient hierarchical network design
- Integrate IP communications, mobility, and advanced security
- Utilize multicast traffic and QoS to optimize network traffic
- Provide increased security and flexibility using access management, VLANs, and IPsec VPNs

The enterprise campus module architecture provides the enterprise with high availability through a resilient multilayer design, redundant hardware and software features, and automatic procedures for reconfiguring network paths when failures occur. Integrated security protects against and mitigates the impact of worms, viruses, and other attacks on the network, even at the switch port level.

A high-capacity, centralized data center module can provide internal server resources to users. The data center module typically also supports network management services for the enterprise, including monitoring, logging, troubleshooting, and other common management features from end to end. The data center submodule typically contains internal email and corporate servers that provide application, file, print, email, and Domain Name System (DNS) services to internal users.

Cisco Enterprise Edge (1.2.2.3)

The *enterprise edge module* provides connectivity for voice, video, and data services outside the enterprise. This module often functions as a liaison between the enterprise campus module and the other modules.

As shown in Figure 1-16, the enterprise edge module consists of submodules providing

- E-commerce services
- Internet connectivity
- Remote access and VPN access
- WAN site-to-site VPN access

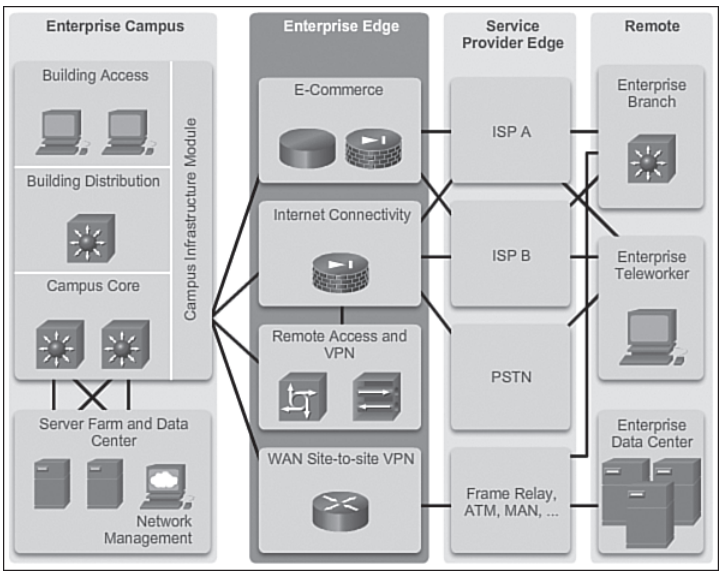

Figure 1-16 Enterprise Edge Submodules

Specifically, these submodules consist of:

- **E-commerce networks and servers**: The e-commerce submodule enables enterprises to support e-commerce applications through the Internet. It uses the high-availability designs of the data center module. Devices located in the e-commerce submodule include web, application, and database servers; firewall and firewall routers; and network intrusion prevention systems (IPS).
- **Internet connectivity and demilitarized zone (DMZ)** : The Internet submodule of the enterprise edge provides internal users with secure connectivity to Internet services such as public servers, email, and DNS. Connectivity to one or several Internet service providers (ISPs) is also provided. Components of this submodule include firewall and firewall routers, Internet edge routers, FTP and HTTP servers, SMTP relay servers, and DNS servers.
- **Remote access and VPN**: The VPN/remote access submodule of the enterprise edge provides remote-access termination services, including authentication for remote users and sites. Components of this submodule include firewalls, dial-in access concentrators, Cisco Adaptive Security Appliances (ASA), and network intrusion prevention system (IPS) appliances.
- **WAN**: The WAN submodule uses various WAN technologies for routing traffic between remote sites and the central site. Enterprise WAN links include technologies such as Multiprotocol Label Switching (MPLS), Metro Ethernet, leased lines, Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH), PPP, Frame Relay, ATM, cable, digital subscriber line (DSL), and wireless.

Service Provider Edge (1.2.2.4)

Enterprises use service providers (SPs) to link to other sites. As shown in Figure 1-17, the ***SP edge module*** can include

- Internet service providers (ISPs)
- WAN services such as Frame Relay, ATM, and MAN
- Public switched telephone network (PSTN) services

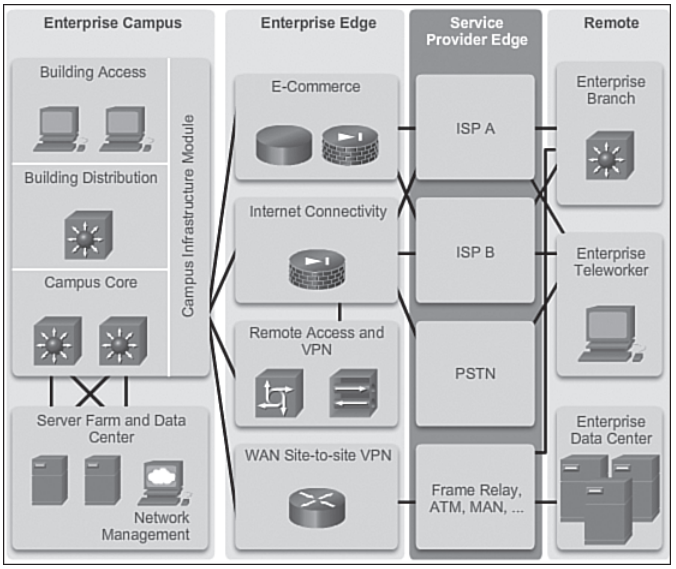

Figure 1-17 Service Provider Edge Module

The SP edge provides connectivity between the enterprise campus module to the remote enterprise data center, enterprise branch, and enterprise teleworker modules.

The SP edge module

- Spans across large geographic areas in a cost effective manner
- Converges voice, video, and data services over a single IP communications network
- Supports QoS and service level agreements
- Supports security using VPNs (IPsec / MPLS) over Layer 2 and Layer 3 WANs

When acquiring Internet services from an ISP, redundancy or failover should be considered. Redundant Internet connections vary depending if the enterprise is connecting to a single ISP or multiple ISPs.

As shown in Figure 1-18, redundant connections to a single ISP can include

- **Single-homed:** A single connection to an ISP
- **Dual-homed:** Two or more connections to a single ISP

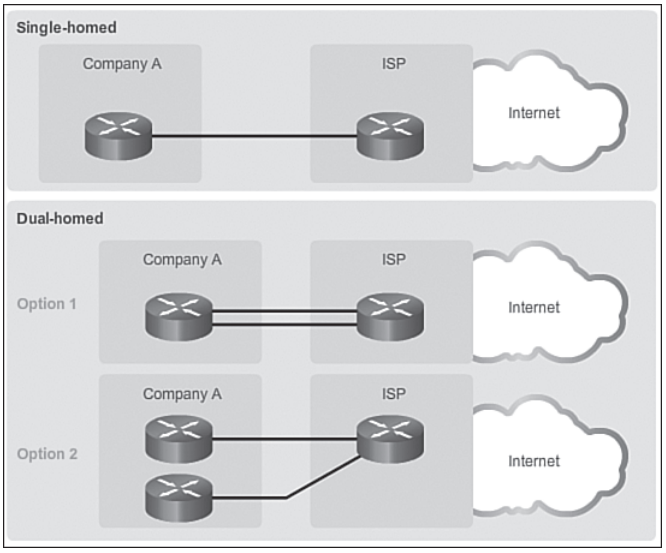

Figure 1-18 Connecting to a Single ISP

Alternatively, it is possible to set up redundancy using multiple ISPs, as shown in Figure 1-19. Options for connecting to multiple ISPs include

- **Multihomed:** Connections to two or more ISPs
- **Dual-multihomed:** Multiple connections to two or more ISPs

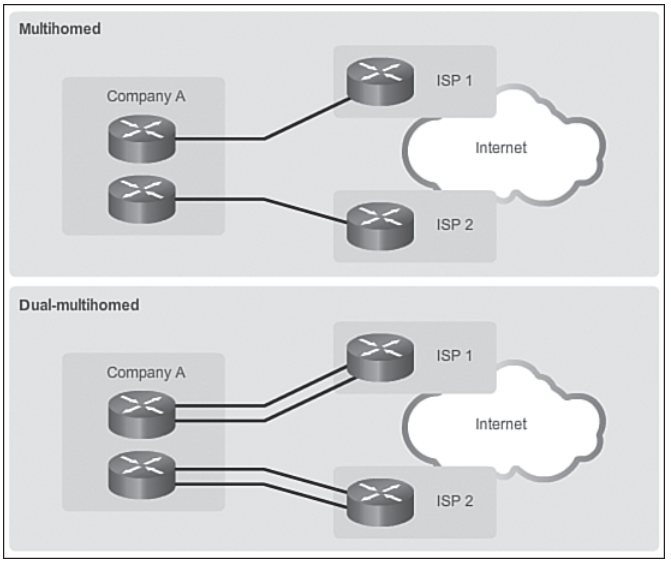

Figure 1-19 Connecting to Multiple ISPs

Remote Functional Area (1.2.2.5)

The remote functional area is responsible for remote connectivity options and includes the following modules, as shown in Figure 1-20.

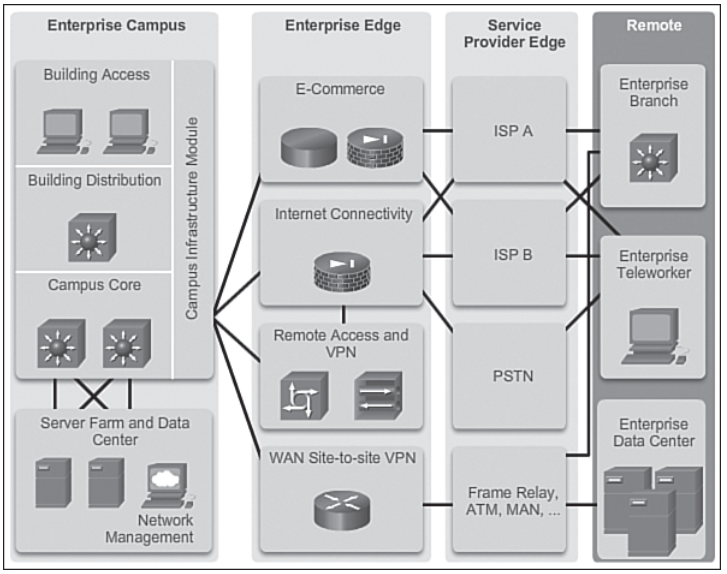

Figure 1-20 Remote Connectivity Areas

Enterprise Branch

The *enterprise branch module* includes remote branches that allow employees to work at noncampus locations. These locations are typically responsible for providing security, telephony, and mobility options to employees, as well as general connectivity into the campus network and the different components located inside the enterprise campus. The enterprise branch module allows enterprises to extend head-office applications and services, such as security, Cisco Unified Communications, and advanced application performance, to the remote branches. The edge device connecting the remote site to the central site varies depending on the needs and size of the site. Large remote sites may use high-end Cisco Catalyst switches, while smaller sites may use an ISR G2 router. These remote sites rely on the SP edge to provide services and applications from the main site. In Figure 1-20, the enterprise branch module connects to the enterprise campus site primarily using a WAN link. However, it also has an Internet link as a backup. The Internet link uses site-to-site IPsec VPN technology to encrypt corporate data.

Enterprise Teleworker

The *enterprise teleworker module* is responsible for providing connectivity for workers who operate out of different geographically dispersed locations, including home offices, hotels, or customer/client sites. The teleworker module recommends that mobile users connect to the Internet using the services of a local ISP, such as cable modem or DSL. VPN services can then be used to secure communications between the mobile worker and central campus. Integrated security- and identity-based networking services enable the enterprise to extend campus security policies to the teleworker. Staff can securely log in to the network over the VPN and gain access to authorized applications and services from a single cost-effective platform.

Enterprise Data Center

The *enterprise data center module* is a data center with all of the same functional options as a campus data center, but exists at a remote location. This provides an added layer of security as the offsite data center can provide disaster recovery and business continuance services for the enterprise. High-end switches such as the Cisco Nexus series switch use fast WAN services such as Metro Ethernet (MetroE) to connect the enterprise campus to the remote enterprise data center. Redundant data centers provide backup using synchronous and asynchronous data and application replication. Additionally, the network and devices offer server and application load balancing to maximize performance. This solution allows the enterprise to scale without major changes to the infrastructure.

Interactive Graphic

Activity 1.2.2.6: Identify Modules of the Cisco Enterprise Architecture

Go to the course online to perform this practice activity.

Evolving Network Architectures (1.3)

New technologies are constantly challenging network administrators. This section discusses new networking architecture trends.

IT Challenges (1.3.1.1)

As businesses have grown more dependent on networks for success, network architectures have evolved over the years. Traditionally, users, data, and applications were housed on premise. Users could only access network resources with company-owned computers. The network had distinct borders and access requirements. Maintaining

security, productivity, and services was simpler. Today, the network border has shifted, creating new challenges for IT departments. Networks are transforming from a data-only transportation system of connected LAN devices to a system that enables the connections of people, devices, and information in a media-rich, converged network environment.

As new technologies and end-user devices come to market, businesses and consumers must continue to adjust to this ever-changing environment. There are several new networking trends that continue to effect organizations and consumers. Some of the top trends include

- Bring your own device (BYOD)
- Online collaboration
- Video communication
- Cloud computing

These trends, while allowing for more advanced services than ever before, also introduce new security risks that IT must address.

Emerging Enterprise Architectures (1.3.1.2)

The speed of change in market and business environments is requiring IT to be more strategic than ever before. Evolving business models are creating complex technology challenges that IT must address.

To address these emerging network trends, new business network architectures are necessary. These architectures must account for the network design principles established in the Cisco Enterprise Architecture, as well as the overlaying policies and technologies that allow organizations to support emerging trends in a safe and manageable way.

To meet this need, Cisco has introduced the following three network architectures:

- Cisco Borderless Network Architecture
- Collaboration Architecture
- Data Center/Virtualization Architecture

Note

Network architectures continually evolve. The intent of this section is to provide an introduction and overview of emerging architecture trends.

Emerging Network Architectures (1.3.2)

Cisco has been at the forefront of network design for decades. They consistently adopt existing networks and develop new network architectures. This topic introduces the Cisco Borderless Network Architecture, the Collaboration Architecture, and the Data Center and Virtualization Architecture.

Cisco Borderless Networks (1.3.2.1)

The *Cisco Borderless Network Architecture* is a network solution that allows organizations and individuals to connect securely, reliably, and seamlessly to the corporate network in a BYOD environment. It is based on wired, wireless, routing, switching, security, and application optimization devices working in harmony to help IT balance demanding business challenges and changing business models.

It is not a static solution, but an evolving solution to help IT evolve its infrastructure to deliver secure, reliable, and seamless user experiences in a world with many new and shifting borders.

It enables an IT department to architect and deploy its systems and policies efficiently to all end user devices that require connection to the network. In doing this, it provides secure, reliable, and seamless access to resources from multiple locations, from multiple devices, and to applications that can be located anywhere.

Specifically, the Cisco Borderless Network Architecture delivers two primary sets of services:

- **Borderless end-point/user services:** As highlighted in Figure 1-21, borderless end-point/user services connect the various devices to provide access to network services. Devices that can connect to the borderless network can range from PCs to tablets and smartphones. It removes the location and device borders, providing unified access to wired and wireless devices. End-point/user services define the user experience and enable the attributes of secure, reliable, and seamless performance on a broad range of devices and environments, as shown in Figure 1-21. For example, most smartphones and tablets can download and use the Cisco AnyConnect software. It enables the device to establish a secure, persistent, policy-based connection for a seamless user experience.
- **Borderless network services:** As highlighted in Figure 1-22, borderless network services unify the approach to securely deliver applications to users in a highly distributed environment. It securely connects internal users and remote users and provides access to network resources. The crucial element to scaling secure access is a policy-based architecture that allows IT to implement centralized access controls.

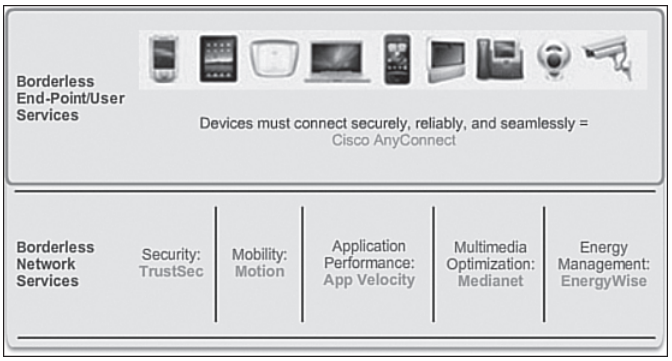

Figure 1-21 Borderless Network Architecture

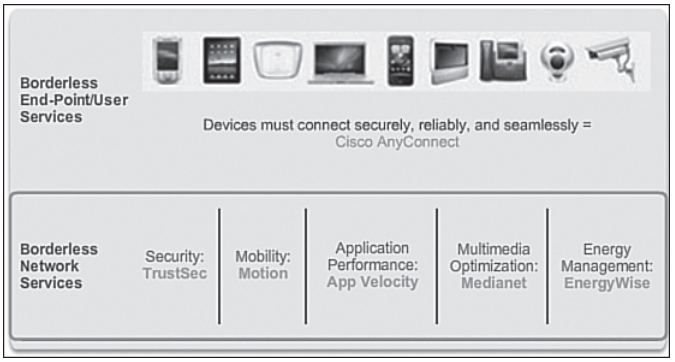

Figure 1-22 Services Supported in Borderless Networks

The borderless network architecture supports a highly secure, high-performing network that is accessible to a wide range of devices. It needs to be flexible enough to scale in its support for future growth in terms of business expansion, including BYOD, mobility and cloud computing and must be able to support the growing requirements for online voice and video.

Collaboration Architecture (1.3.2.2)

Working in a collaborative environment helps increase productivity. Collaboration and other types of groupware are used to bring people together for one reason or another: such as to socialize, to work together, to cooperate and contribute to the production of something, and to innovate.

The *Cisco Collaboration Architecture* comprises a portfolio of products, applications, software development kits (SDKs), and APIs. The individual components work together to provide a comprehensive solution.

As shown in Figure 1-23, Cisco's collaboration architecture is composed of three layers:

- **Application and Devices:** This layer contains unified communications and conference applications such as Cisco WebEx Meetings, WebEx Social, Cisco Jabber, and TelePresence. The applications within this layer help users stay connected and productive. These applications include voice, video, web conferencing, messaging, mobile applications, and enterprise social software.
- **Collaboration Services:** This layer supports collaboration applications including the following services: presence, location, session management, contact management, client frameworks, tagging, and policy and security management.
- **Network and Computer Infrastructure:** This layer is responsible for allowing collaboration anytime, from anywhere, on any device. It includes virtual machines, the network, and storage.

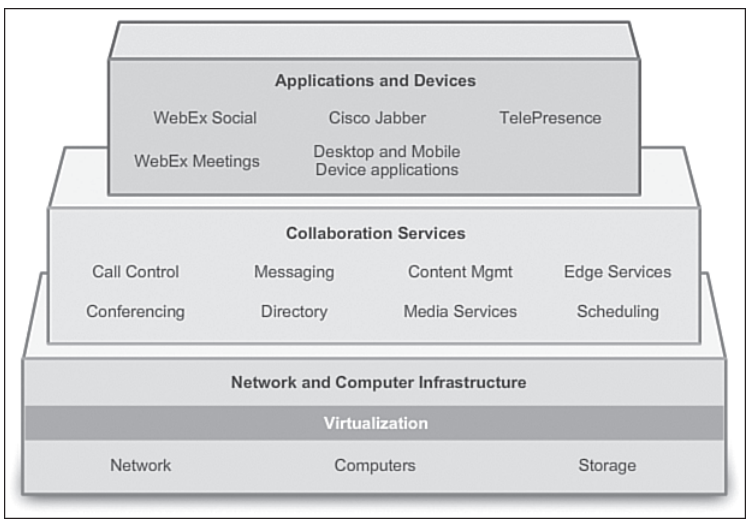

Figure 1-23 Cisco Collaboration Architecture

Data Center and Virtualization (1.3.2.3)

The *Cisco Data Center/Virtualization Architecture* is built upon Cisco Data Center 3.0. It comprises a comprehensive set of virtualization technologies and services that bring the network, computing, storage, and virtualization platforms together.

The Data Center Architecture consists of three components, as shown in Figure 1-24:

- **Cisco Unified Management Solutions:** Management solutions simplify and automate the process of deploying IT infrastructure and services with speed and enterprise reliability. Solutions operate transparently across physical and virtual resources in cloud environments.

- **Unified Fabric Solutions:** Flexible network solutions deliver network services to servers, storage, and applications, providing transparent convergence, scalability, and sophisticated intelligence. Solutions include Cisco Nexus switches, Catalyst switches, Cisco Fabric Manager, and Cisco NX-OS software.
- **Unified Computing Solutions:** Cisco's next-generation data center system unites computing, network, storage access, and virtualization into a cohesive system designed to reduce total cost of ownership (TCO) and increase business agility. The Cisco Unified Computing System (Cisco UCS) is built with blade servers, rack-mount servers, fabric interconnects, and virtual interface cards (VICs).

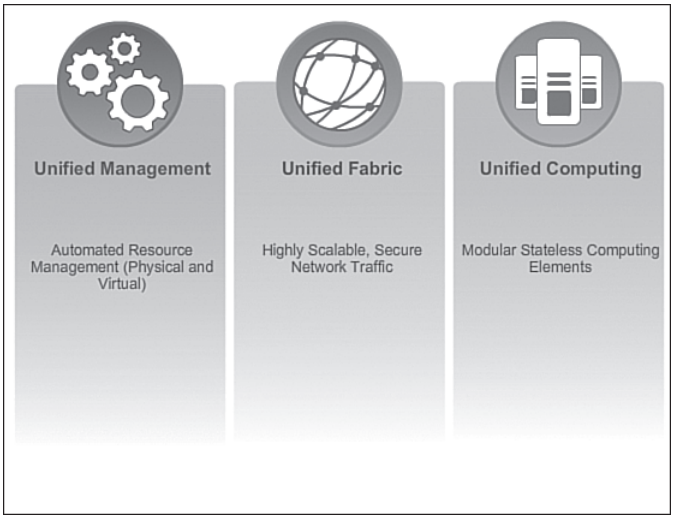

Figure 1-24 Components of the Data Center Architecture

Video

Video 1.3.2.3: Cisco Unified Fabric

Go to the course to see a short video on the Cisco Unified Fabric.

Expanding the Network (1.3.2.4)

These three architectures are built on an infrastructure of scalable and resilient hardware and software. Components of the architecture come together to build network systems that span an organization from network access to the cloud, and provide organizations with the services they need.

Building off the basic network infrastructure, organizations can use these network architectures to grow their network over time, adding features and functionality in an integrated solution.

One of the first steps in growing the network is expanding from the campus infrastructure to a network that connects remote sites through the Internet and through the WAN.

Interactive Graphic

Video 1.3.2.4: Evolution of a Corporate WAN

Go to the course to see a short video on the evolution of a network to a WAN infrastructure.

Interactive Graphic

Activity 1.3.2.5: Identify Evolving Network Architecture Terminology

Go to the course online to perform this practice activity.

Summary (1.4)

Class Activity 1.4.1.1: Borderless Innovations - Everywhere

You are the network administrator for your small- to medium-size business. Borderless network services interest you as you plan your network's future.

While planning for network policies and services, you realize that your wired and wireless networks need manageability and deployment design.

Therefore, this leads you to consider the following Cisco borderless services as possible options for your business:

- **Security:** TrustSec
- **Mobility:** Motion
- **Application performance:** App Velocity
- **Multimedia performance:** Medianet
- **Energy management:** EnergyWise

Packet Tracer Activity 1.4.1.2: Skills Integration Challenge

This Packet Tracer Activity provides an opportunity to review skills from previous coursework.

Your business has just expanded into a different town and needs to expand its presence across the Internet. You are tasked with completing the upgrades to the enterprise network, which includes dual-stacked IPv4 and IPv6 as well as a variety of addressing and routing technologies.

Packet Tracer Activity 1.4.1.3: Skills Integration Challenge - EIGRP

You are a network technician new to a company that has lost its last technician in the middle of a system upgrade. You are tasked with completing upgrades to the network infrastructure that has two locations. Half of the enterprise network uses IPv4 addressing, and the other half uses IPv6 addressing. The requirements also include a variety of routing and switching technologies.

The structured engineering principles of good network design include hierarchy, modularity, resiliency, and flexibility.

A typical enterprise hierarchical LAN campus network design includes the access layer, distribution layer, and the core layer. In smaller enterprise networks, a "collapsed core" hierarchy, where the distribution layer and core layer functions are implemented in a single device, can be more practical. The benefits of a hierarchical network include scalability, redundancy, performance, and maintainability.

A modular design that separates the functions of a network enables flexibility and facilitates implementation and management. The basic module blocks that are connected by the core include the access distribution block, the services block, the data center, and the enterprise edge. The Cisco Enterprise Architecture modules are used to facilitate the design of large, scalable networks. The primary modules include the enterprise campus, enterprise edge, service provider edge, enterprise data center, enterprise branch, and enterprise teleworker.

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion Connecting Networks Lab Manual (978-1-58713-331-2). The Packet Tracer Activity PKA files are found in the online course.

Class Activities

Class Activity 1.0.1.2: Design Hierarchy

Class Activity 1.4.1.1: Borderless Innovations - Everywhere

Packet Tracer Activities

Packet Tracer Activity 1.4.1.2: Skills Integration Challenge - OSPF

Packet Tracer Activity 1.4.1.3: Skills Integration Challenge - EIGRP

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix, "Answers to the 'Check Your Understanding' Questions," lists the answers.

1. What are the four structured design principles?

   A. Availability, flexibility, modularity, and security
   B. Availability, hierarchy, modularity, quality of service (QoS)
   C. Flexibility, hierarchy, modularity, resiliency
   D. Flexibility, modularity, resiliency, and security
   E. Hierarchy, quality of service (QoS), resiliency, and security
   F. Hierarchy, modularity, resiliency, and security
   G. Modularity, quality of service (QoS), resiliency, and security

2. Which layer of the hierarchical network design model is often called the backbone?

   A. Access
   B. Core
   C. Distribution
   D. Network
   E. WAN
   F. Workgroup

3. Which network architecture combines individual components to provide a comprehensive solution allowing people to cooperate and contribute to the production of something?

   A. Cisco Collaboration Architecture
   B. Cisco Enterprise Campus Architecture
   C. Cisco Enterprise Branch Architecture
   D. Cisco Enterprise Data Center Architecture
   E. Cisco Borderless Network Architecture
   F. Cisco Enterprise Teleworker module

4. At which layer of the hierarchical network model do users connect to the network?

   A. Access
   B. Application
   C. Core
   D. Distribution
   E. Network

5. Which two statements regarding the Cisco AnyConnect software are true? (Choose two.)

   A. It is part of the borderless end-point/user services.
   B. It is part of the borderless network services.
   C. It is used to connect any device to the network.
   D. It is used to connect from anywhere.
   E. It is used to connect without an Internet connection.
   F. It is used to establish a secure, persistent, policy-based connection.

6. Which three devices are found in the access layer of the hierarchical network model? (Choose three.)

   A. Firewall appliance
   B. Layer 2 switch
   C. Layer 3 switch
   D. Modular multilayer switch
   E. VoIP phones
   F. Wireless access point

7. Which two statements correctly describe a collapsed core network design? (Choose two.)

   A. Also called a two-tier hierarchical network design
   B. Also called a three-tier hierarchical network design
   C. Consists of the access layer and distribution layer in one device
   D. Consists of the access layer and core layer in one device
   E. Consists of the distribution and core layer in one device

8. Which goal can be accomplished by implementing the Cisco enterprise teleworker module?

   A. It allows the enterprise to add large branch sites that span geographic areas.
   B. It allows the enterprise to deliver secure voice and data services to workers no matter where or when they work.
   C. To reduce remote security threats, it forces users who are located at main sites to log on to resources.
   D. It satisfies telephony requirements for users who are located at medium to large enterprise sites.

9. What should be considered first when starting the network design?

   A. Connectivity to the data center
   B. Connectivity to the branch site
   C. Protocols required
   D. Size of the network
   E. Type of security implemented
   F. Type of applications

10. Which network architecture functions through a combination of technologies that include wired, wireless, security, and more?

    A. Cisco Borderless Network
    B. Cisco Enterprise Branch
    C. Cisco Enterprise Campus
    D. Cisco Enterprise Edge
    E. Cisco Enterprise Teleworker

11. What does the application and device layer of the Cisco Collaboration Architecture do?

    A. It contains applications such as Cisco WebEx Meetings, Cisco Jabber, and TelePresence to help users stay connected and productive.
    B. It is responsible for allowing collaboration anytime, from anywhere, on any device.
    C. It supports collaboration applications with presence, location, session management, contact management, client frameworks, tagging, and policy and security management.