CCNA 3 v7.0 Curriculum: Module 11 – Network Design

itexamanswers.net/ccna-3-v7-0-curriculum-module-11-network-design.html

April 15, 2020

11.0. Introduction

11.0.1. Why should I take this module?

Welcome to Network Design!

You are a sought after spaceship designer! You have been asked to design a new spaceship. Your first questions are, “What will this ship be used for? How large is the crew? Will it be a war ship? A cargo ship? A science and exploration vessel?” What if the answer is, “The crew can be as few as 50 people, but it must be able to hold as many as 500. It will be used in a variety of ways.”? How do you design a ship like this? You must design the size and configuration of the ship, and the power it requires, wisely.

Designing a network to meet current requirements and to adapt to future requirements is a complex task. But it can be done, thanks to hierarchical and scalable network designs that use the right components. You know you want to learn about this. Even if you have not designed your current network, knowing about network design will increase your value to the organization as a great network administrator! And who doesn’t want that?

11.0.2. What will I learn to do in this module?

Module Title: Network Design

Module Objective: Explain the characteristics of scalable network architectures.

Topic Title	Topic Objective
Hierarchical Networks	Explain how data, voice, and video are converged in a switched network.
Scalable Networks	Explain considerations for designing a scalable network.
Switch Hardware	Explain how switch hardware features support network requirements.
Router Hardware	Describe the types of routers available for small to-medium-sized business networks.

11.1. Hierarchical Networks

11.1.1 Video – Three-Layer Network Design

11.1.2. The Need to Scale the Network

Our digital world is changing. The ability to access the internet and the corporate network is no longer confined to physical offices, geographical locations, or time zones. In today's globalized workplace, employees can access resources from anywhere in the world and information must be available at any time, and on any device. These requirements drive the need to build next-generation networks that are secure, reliable, and highly available.

These next-generation networks must not only support current expectations and equipment but must also be able to integrate legacy platforms. Businesses increasingly rely on their network infrastructure to provide mission-critical services. As businesses grow and evolve, they hire more employees, open branch offices, and expand into global markets. These changes directly affect the requirements of a network which must be able to scale to meet the needs of business.

A network must support the exchange of various types of network traffic, including data files, email, IP telephony, and video applications for multiple business units. All enterprise networks must be able to do the following:

- Support critical applications
- Support converged network traffic
- Support diverse business needs

- Provide centralized administrative control

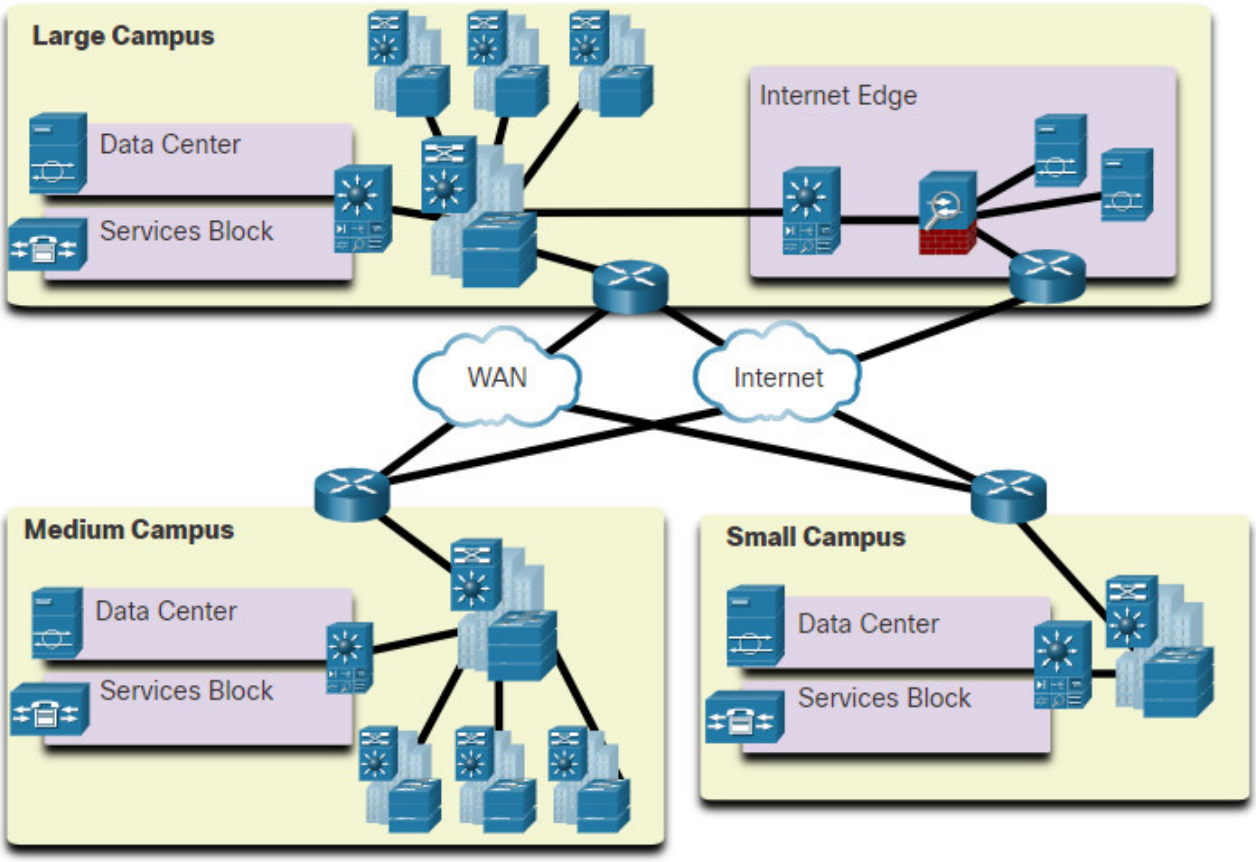
The LAN is the networking infrastructure that provides access to network communication services and resources for end users and devices. The end users and devices may be spread over a single floor or building. You create a campus network by interconnecting a group of LANs that are spread over a small geographic area. Campus network designs include small networks that use a single LAN switch, up to very large networks with thousands of connections.

11.1.3. Borderless Switched Networks

With the increasing demands of the converged network, the network must be developed with an architectural approach that embeds intelligence, simplifies operations, and is scalable to meet future demands. One of the more recent developments in network design is the Cisco Borderless Network.

The Cisco Borderless Network is a network architecture that combines innovation and design. It allows organizations to support a borderless network that can connect anyone, anywhere, anytime, on any device; securely, reliably, and seamlessly. This architecture is designed to address IT and business challenges, such as supporting the converged network and changing work patterns.

The Cisco Borderless Network provides the framework to unify wired and wireless access, including policy, access control, and performance management across many different device types. Using this architecture, the borderless network, shown in the figure, is built on a hierarchical infrastructure of hardware that is scalable and resilient.



By combining this hardware infrastructure with policy-based software solutions, the Cisco Borderless Network provides two primary sets of services: network services, and user and endpoint services under the umbrella of an integrated management solution. It enables different network elements to work together, and allows users to access resources from any place, at any time, while providing optimization, scalability, and security.

11.1.4. Hierarchy in the Borderless Switched Network

Creating a borderless switched network requires that sound network design principles are used to ensure maximum availability, flexibility, security, and manageability. The borderless switched network must deliver on current requirements and future required services and technologies. Borderless switched network design guidelines are built upon the following principles:

- **Hierarchical** – The design facilitates understanding the role of each device at every tier, simplifies deployment, operation, and management, and reduces fault domains at every tier.
- **Modularity** – The design allows seamless network expansion and integrated service enablement on an on-demand basis.
- **Resiliency** – The design satisfies user expectations for keeping the network always on.
- **Flexibility** – The design allows intelligent traffic load sharing by using all network resources.

These are not independent principles. Understanding how each principle fits in the context of the others is critical. Designing a borderless switched network in a hierarchical fashion creates a foundation that allows network designers to overlay security, mobility, and unified communication features. Two time-tested and proven hierarchical design frameworks for campus networks are the three-tier layer and the two-tier layer models.

The three critical layers within these tiered designs are the access, distribution, and core layers. Each layer can be seen as a well-defined, structured module with specific roles and functions in the campus network. Introducing modularity into the campus hierarchical design further ensures that the campus network remains resilient and flexible enough to provide critical network services. Modularity also helps to allow for growth and changes that occur over time.

Click each button for an example of each design.

11.1.5. Access, Distribution, and Core Layer Functions

The access, distribution, and core layers perform specific functions in a hierarchical network design.

Click each button for a description of the functions of each layer.

Access Layer
The access layer represents the network edge, where traffic enters or exits the campus network. Traditionally, the primary function of an access layer switch is to provide network access to the user. Access layer switches connect to distribution layer switches, which implement network foundation technologies such as routing, quality of service, and security.

To meet network application and end-user demand, the next-generation switching platforms now provide more converged, integrated, and intelligent services to various types of endpoints at the network edge. Building intelligence into access layer switches allows applications to operate on the network more efficiently and securely.

Core Layer
The core layer is the network backbone. It connects several layers of the campus network. The core layer serves as the aggregator for all of the distribution layer devices and ties the campus together with the rest of the network. The primary purpose of the core layer is to provide fault isolation and high-speed backbone connectivity.

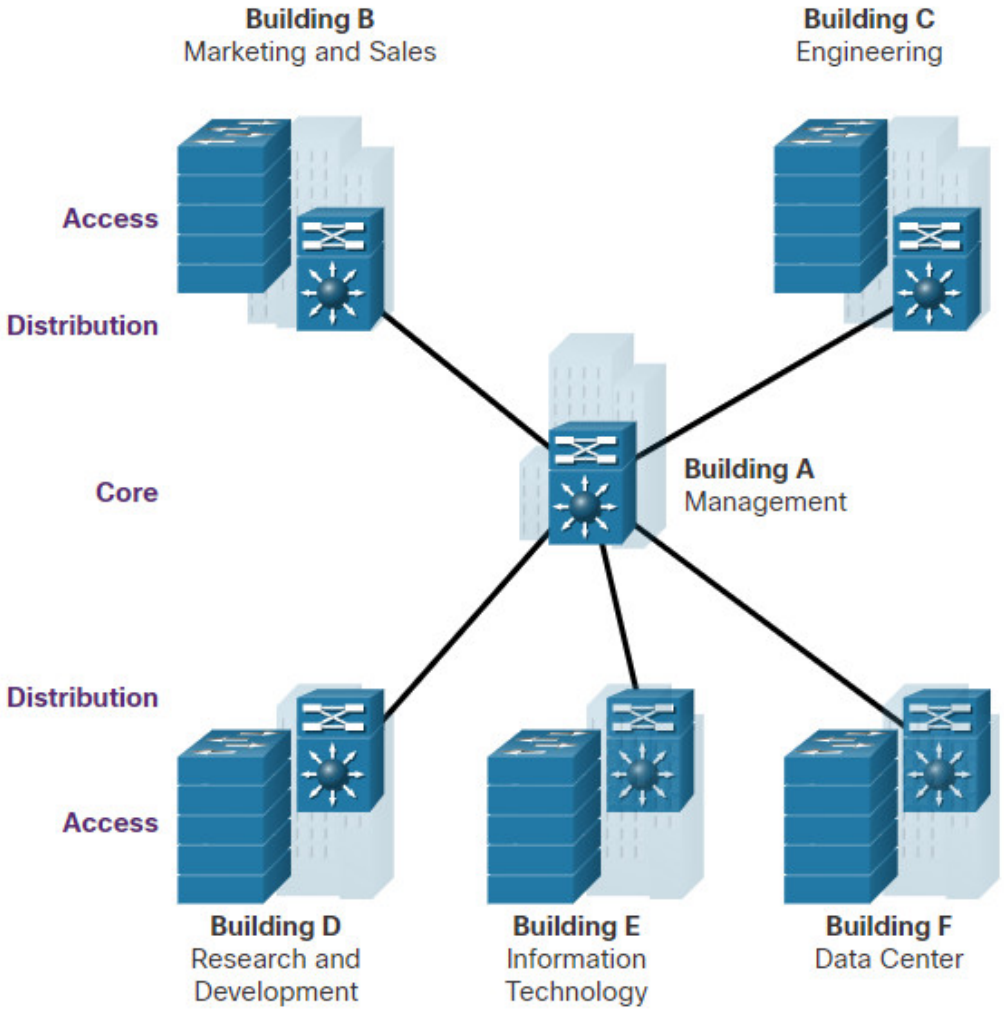
11.1.6. Three-Tier and Two-Tier Examples

Click each button for an example and explanation of a three-tier and two-tier design.

- Three-Tier Example
- Two-Tier Example

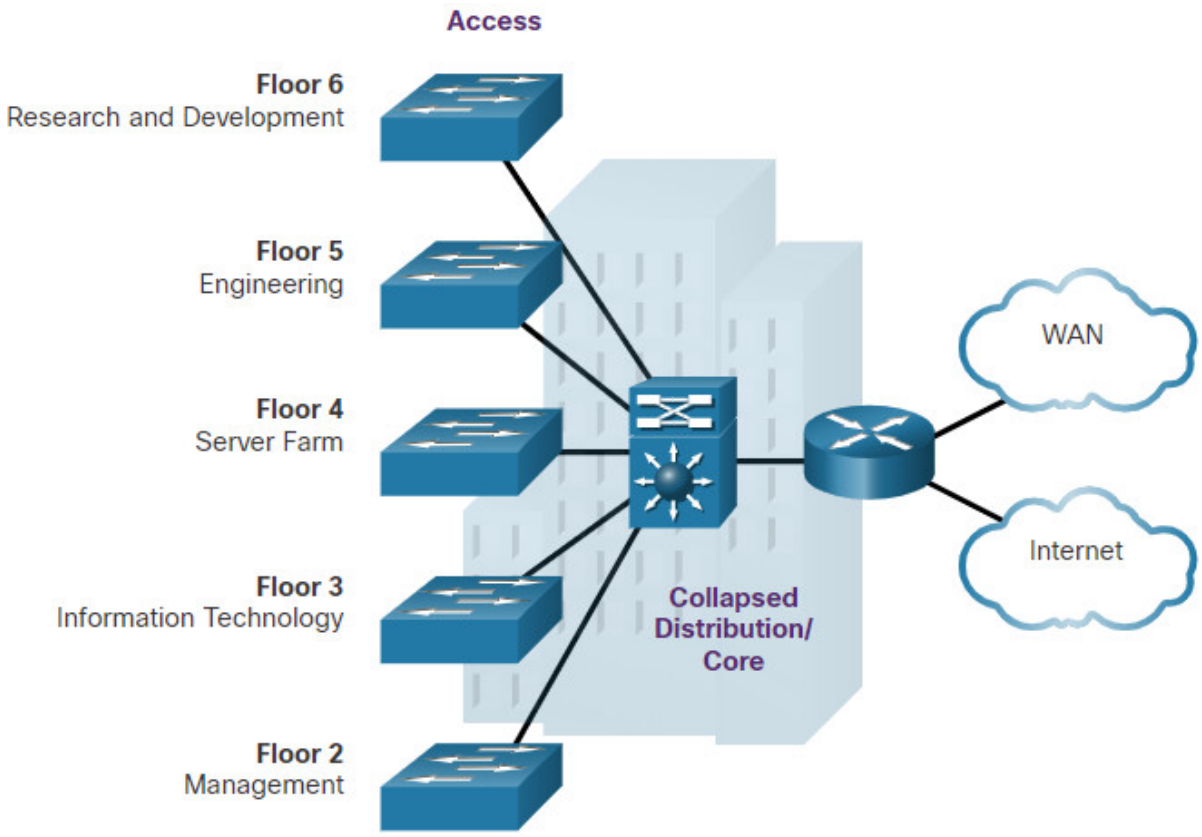
Three-Tier Example

The figure shows a three-tier campus network design for organizations where the access, distribution, and core are each separate layers. To build a simplified, scalable, cost-effective, and efficient physical cable layout design, the recommendation is to build an extended-star physical network topology from a centralized building location to all other buildings on the same campus.



Two-Tier Example

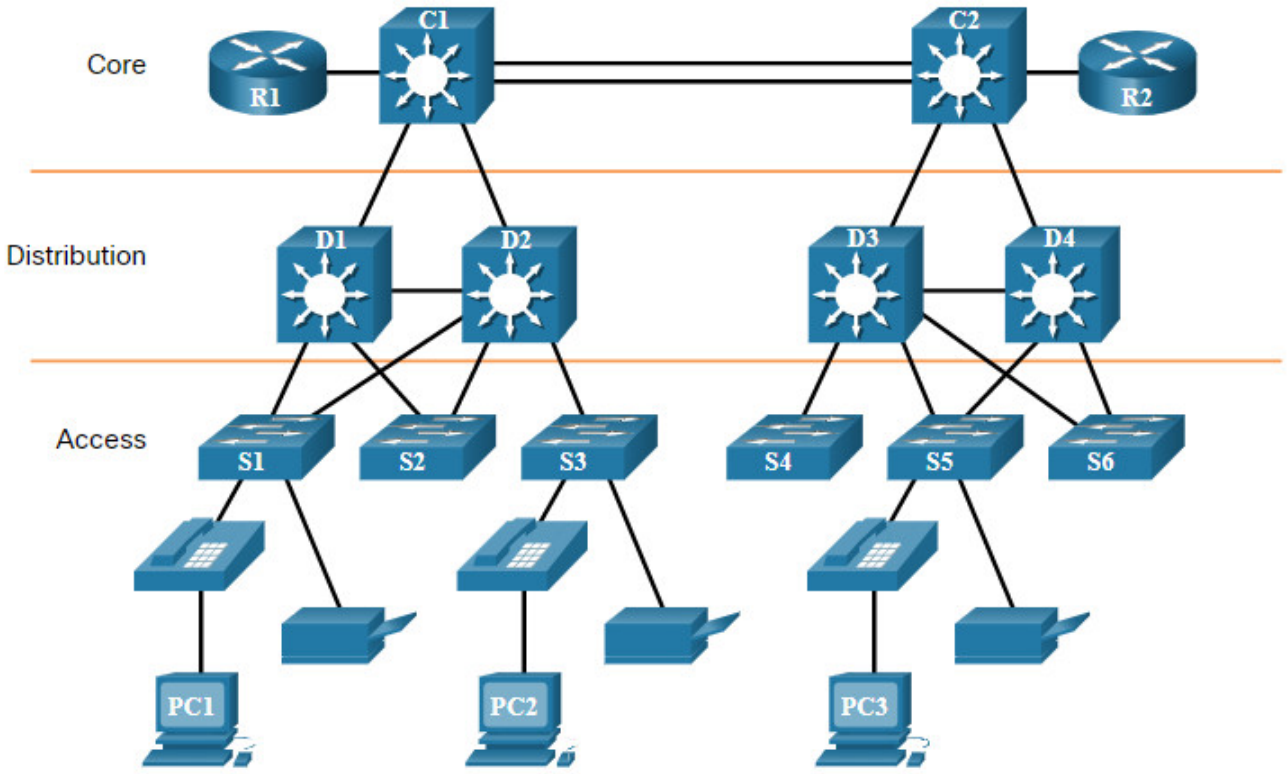
In some cases where extensive physical or network scalability does not exist, maintaining separate distribution and core layers is not required. In smaller campus locations where there are fewer users accessing the network, or in campus sites consisting of a single building, separate core and distribution layers may not be needed. In this scenario, the recommendation is the alternate two-tier campus network design, also known as the collapsed core network design, as shown in the figure.



11.1.7. Role of Switched Networks

The role of switched networks has evolved dramatically in the last two decades. It was not long ago that flat Layer 2 switched networks were the norm. Flat Layer 2 switched networks relied on the Ethernet and the widespread use of hub repeaters to propagate LAN traffic throughout an organization.

As shown in the figure, networks have fundamentally changed to switched LANs in a hierarchical network.



A switched LAN allows additional flexibility, traffic management, quality of service, and security. It also affords support for wireless networking and connectivity, and support for other technologies such as IP telephone and mobility services.

11.2. Scalable Networks

11.2.1. Design for Scalability

You understand that your network is going to change. Its number of users will likely increase, they may be found anywhere, and they will be using a wide variety of devices. Your network must be able to change along with its users. Scalability is the term for a network that can grow without losing availability and reliability.

To support a large, medium or small network, the network designer must develop a strategy to enable the network to be available and to scale effectively and easily. Included in a basic network design strategy are the following recommendations:

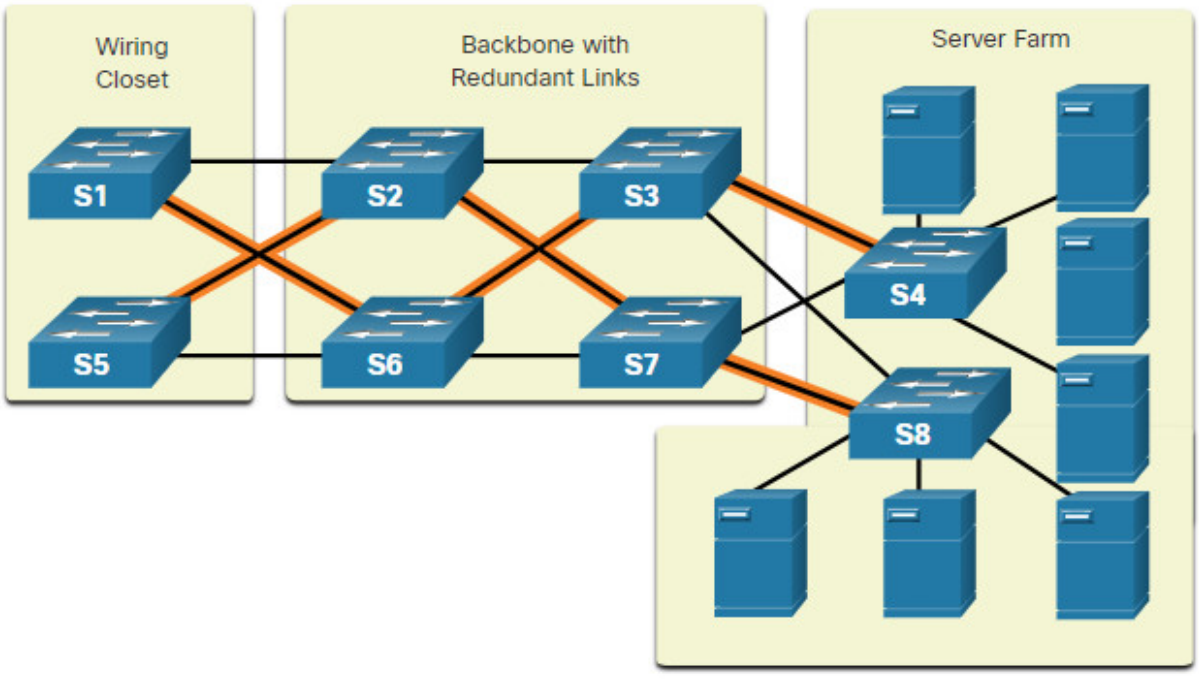
- Use expandable, modular equipment, or clustered devices that can be easily upgraded to increase capabilities. Device modules can be added to the existing equipment to support new features and devices without requiring major equipment upgrades. Some devices can be integrated in a cluster to act as one device to simplify management and configuration.

- Design a hierarchical network to include modules that can be added, upgraded, and modified, as necessary, without affecting the design of the other functional areas of the network. For example, creating a separate access layer that can be expanded without affecting the distribution and core layers of the campus network.
- Create an IPv4 and IPv6 address strategy that is hierarchical. Careful address planning eliminates the need to re-address the network to support additional users and services.
- Choose routers or multilayer switches to limit broadcasts and filter other undesirable traffic from the network. Use Layer 3 devices to filter and reduce traffic to the network core.

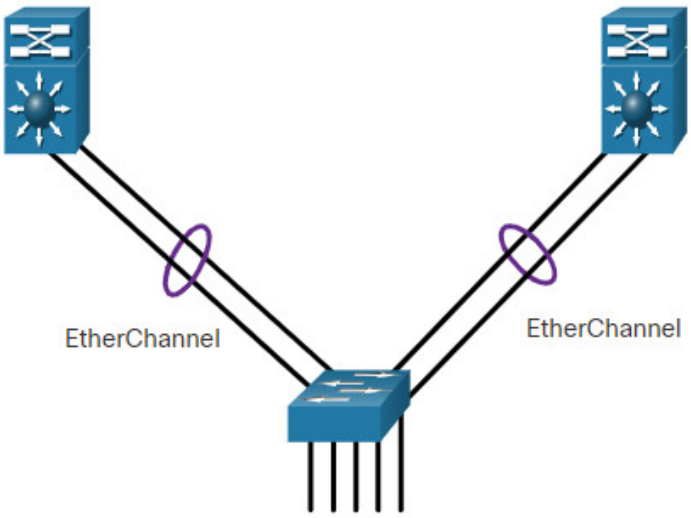
Click each button for more information about advanced network design requirements

- Redundant Links
- Multiple Links
- Scalable Routing Protocol
- Wireless Connectivity

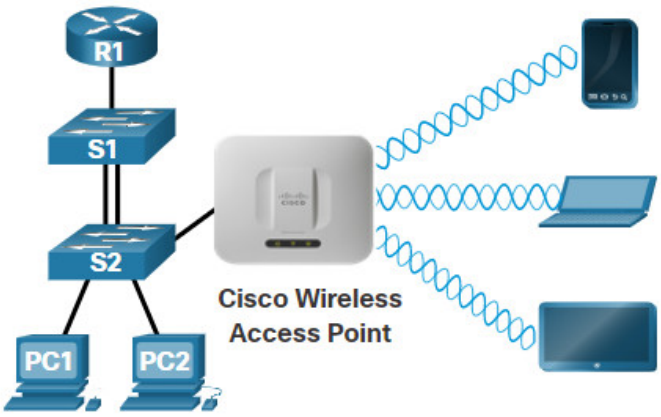
Redundant Links
Implement redundant links in the network between critical devices and between access layer and core layer devices.



Multiple Links
Implement multiple links between equipment, with either link aggregation (EtherChannel) or equal cost load balancing, to increase bandwidth. Combining multiple Ethernet links into a single, load-balanced EtherChannel configuration increases available bandwidth. EtherChannel implementations can be used when budget restrictions prohibit purchasing high-speed interfaces and fiber runs.

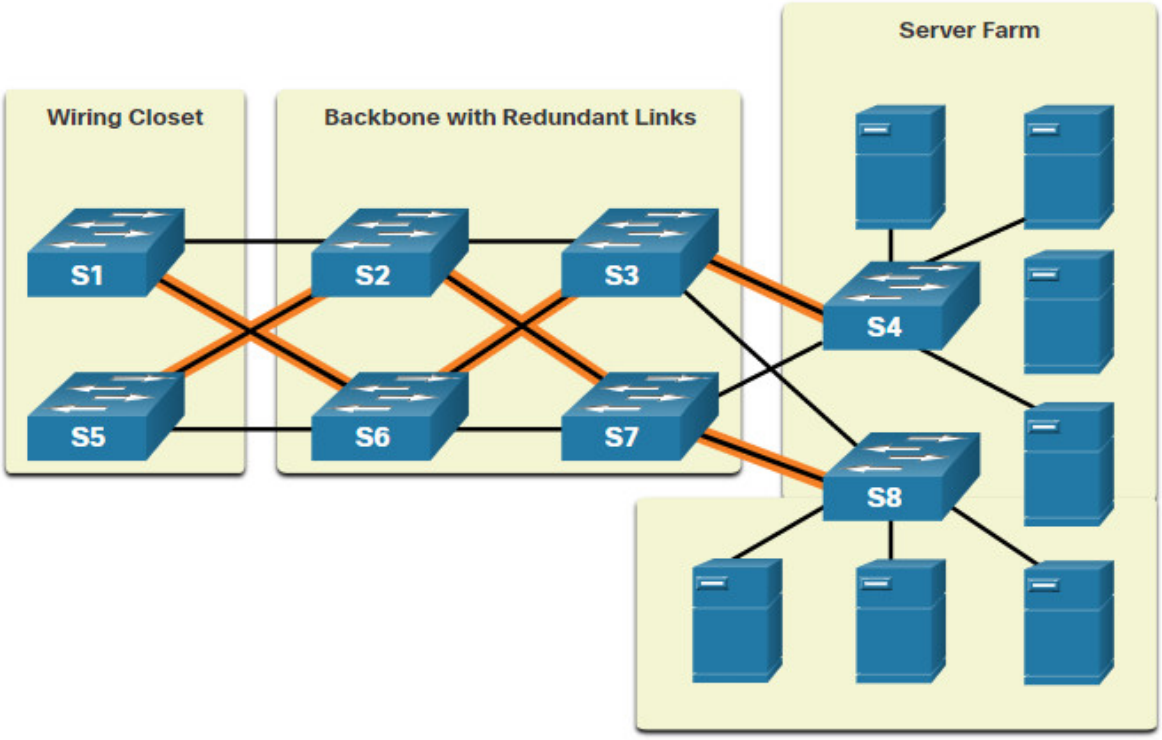


Wireless Connectivity
Implement wireless connectivity to allow for mobility and expansion.



11.2.2. Plan for Redundancy

For many organizations, the availability of the network is essential to supporting business needs. Redundancy is an important part of network design. It can prevent disruption of network services by minimizing the possibility of a single point of failure. One method of implementing redundancy is by installing duplicate equipment and providing failover services for critical devices.



Another method of implementing redundancy is redundant paths, as shown in the figure above. Redundant paths offer alternate physical paths for data to traverse the network. Redundant paths in a switched network support high availability. However, due to the operation of switches, redundant paths in a switched Ethernet network may cause logical Layer 2 loops. For this reason, Spanning Tree Protocol (STP) is required.

STP eliminates Layer 2 loops when redundant links are used between switches. It does this by providing a mechanism for disabling redundant paths in a switched network until the path is necessary, such as when a failure occurs. STP is an open standard protocol, used in a switched environment to create a loop-free logical topology.

Using Layer 3 in the backbone is another way to implement redundancy without the need for STP at Layer 2. Layer 3 also provides best path selection and faster convergence during failover.

11.2.3. Reduce Failure Domain Size

A well-designed network not only controls traffic, but also limits the size of failure domains. A failure domain is the area of a network that is impacted when a critical device or network service experiences problems.

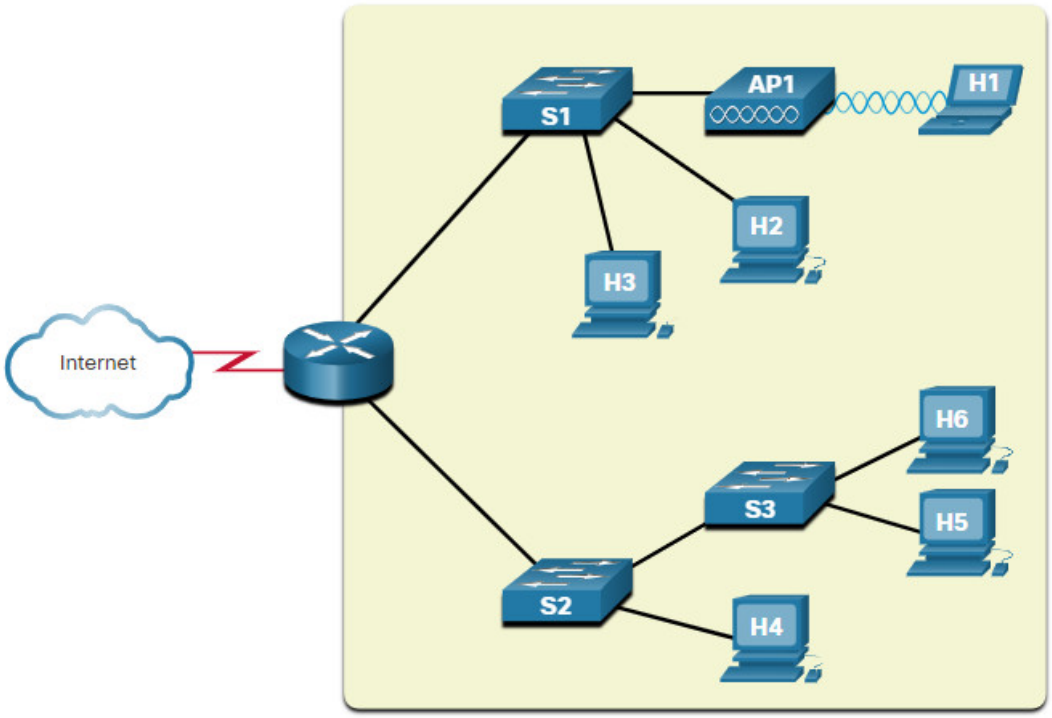
The function of the device that initially fails determines the impact of a failure domain. For example, a malfunctioning switch on a network segment normally affects only the hosts on that segment. However, if the router that connects this segment to others fails, the impact is much greater.

The use of redundant links and reliable enterprise-class equipment minimize the chance of disruption in a network. Smaller failure domains reduce the impact of a failure on company productivity. They also simplify the troubleshooting process, thereby, shortening the downtime for all users.

Click each button to see the failure domain of each associated device.

- Edge Router
- AP1
- S1
- S2
- S3

Edge Router



Limiting the Size of Failure Domains

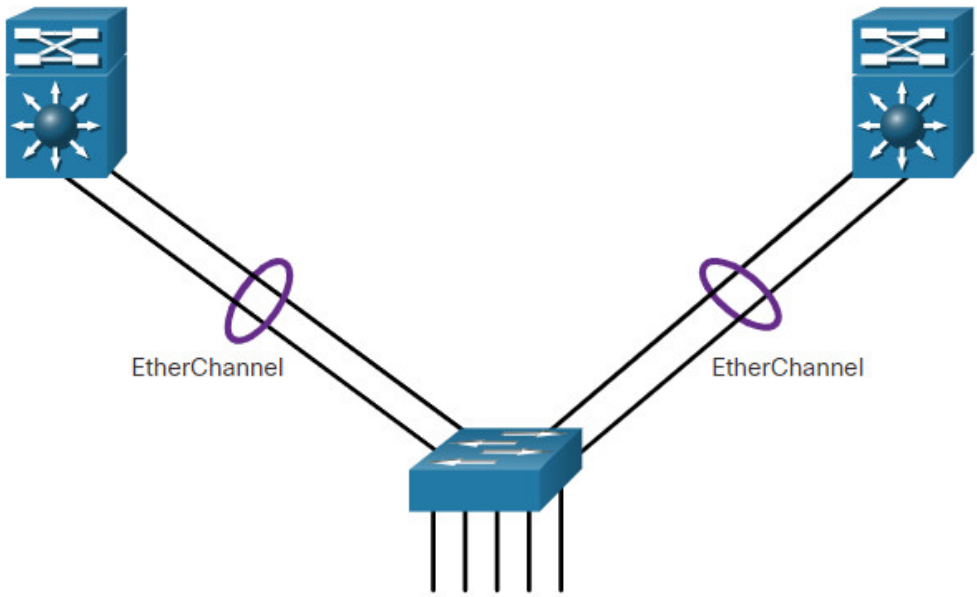
Because a failure at the core layer of a network can have a potentially large impact, the network designer often concentrates on efforts to prevent failures. These efforts can greatly increase the cost of implementing the network. In the hierarchical design model, it is easiest and usually least expensive to control the size of a failure domain in the distribution layer. In the distribution layer, network errors can be contained to a smaller area; thus, affecting fewer users. When using Layer 3 devices at the distribution layer, every router functions as a gateway for a limited number of access layer users.

Switch Block Deployment

Routers, or multilayer switches, are usually deployed in pairs, with access layer switches evenly divided between them. This configuration is referred to as a building, or departmental, switch block. Each switch block acts independently of the others. As a result, the failure of a single device does not cause the network to go down. Even the failure of an entire switch block does not affect a significant number of end users.

11.2.4. Increase Bandwidth

In hierarchical network design, some links between access and distribution switches may need to process a greater amount of traffic than other links. As traffic from multiple links converges onto a single, outgoing link, it is possible for that link to become a bottleneck. Link aggregation, such as EtherChannel, allows an administrator to increase the amount of bandwidth between devices by creating one logical link made up of several physical links.

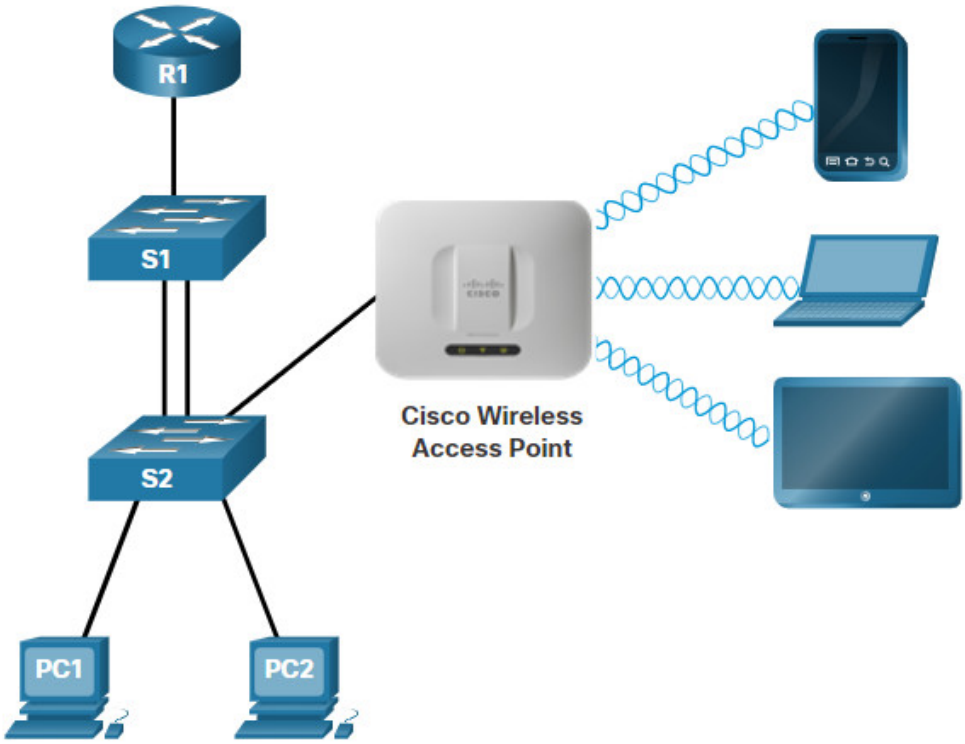


EtherChannel uses the existing switch ports. Therefore, additional costs to upgrade the link to a faster and more expensive connection are not necessary. The EtherChannel is seen as one logical link using an EtherChannel interface. Most configuration tasks are done on the EtherChannel interface, instead of on each individual port, ensuring configuration consistency throughout the links. Finally, the EtherChannel configuration takes advantage of load balancing between links that are part of the same EtherChannel, and depending on the hardware platform, one or more load-balancing methods can be implemented.

11.2.5. Expand the Access Layer

The network must be designed to be able to expand network access to individuals and devices, as needed. An increasingly important option for extending access layer connectivity is through wireless. Providing wireless connectivity offers many advantages, such as increased flexibility, reduced costs, and the ability to grow and adapt to changing network and business requirements.

To communicate wirelessly, end devices require a wireless NIC that incorporates a radio transmitter/receiver and the required software driver to make it operational. Additionally, a wireless router or a wireless access point (AP) is required for users to connect, as shown in the figure.

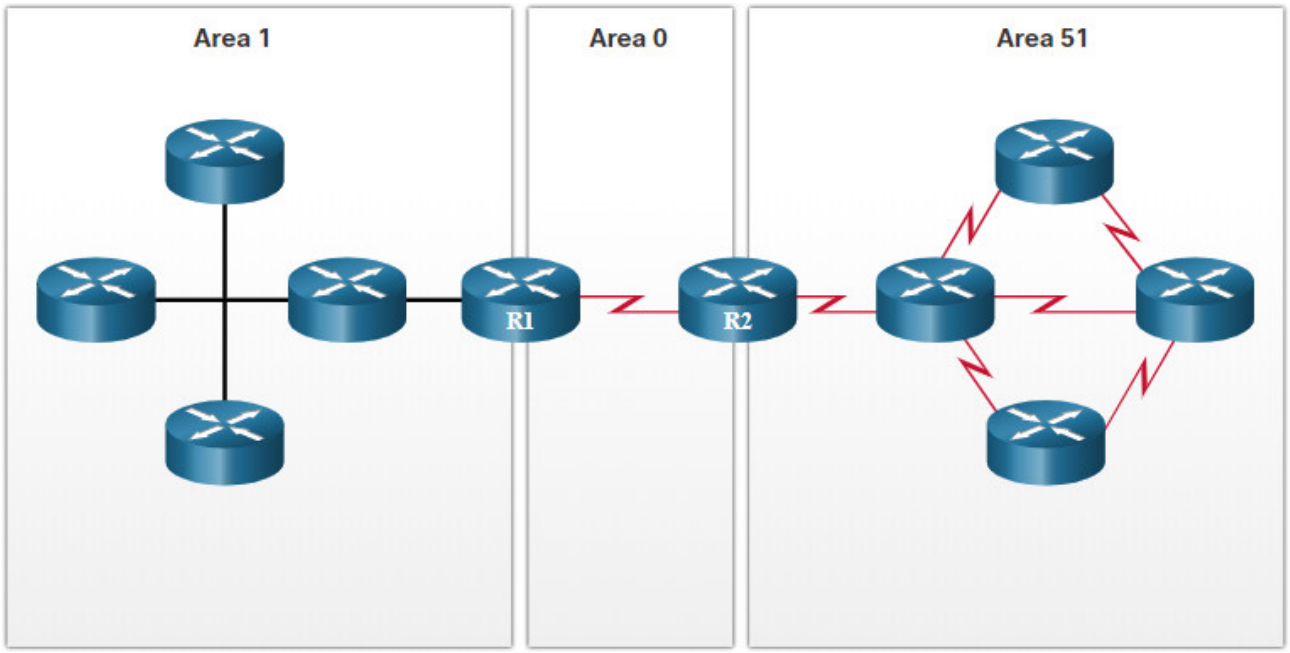


There are many considerations when implementing a wireless network, such as the types of wireless devices to use, wireless coverage requirements, interference considerations, and security considerations.

11.2.6. Tune Routing Protocols

Advanced routing protocols, such as Open Shortest Path First (OSPF), are used in large networks.

OSPF is a link-state routing protocol. As shown in the figure, OSPF works well for larger hierarchical networks where fast convergence is important. OSPF routers establish and maintain neighbor adjacencies with other connected OSPF routers. OSPF routers synchronize their link-state database. When a network change occurs, link-state updates are sent, informing other OSPF routers of the change and establishing a new best path, if one is available.



11.3. Switch Hardware

11.3.1. Switch Platforms

One simple way to create hierarchical and scalable networks is to use the right equipment for the job. There is a variety of switch platforms, form factors, and other features that you should consider before choosing a switch.

When designing a network, it is important to select the proper hardware to meet current network requirements, as well as to allow for network growth. Within an enterprise network, both switches and routers play a critical role in network communication.

Click each button for more information about the categories of switches for enterprise networks.

- Campus LAN Switches
- Cloud-Managed Switches
- Data Center Switches
- Service Provider Switches
- Virtual Networking

Campus LAN Switches
To scale network performance in an enterprise LAN, there are core, distribution, access, and compact switches. These switch platforms vary from fanless switches with eight fixed ports to 13-blade switches supporting hundreds of ports. Campus LAN switch platforms include the Cisco 2960, 3560, 3650, 3850, 4500, 6500, and 6800 Series.

Data Center Switches
A data center should be built based on switches that promote infrastructure scalability, operational continuity, and transport flexibility. The data center switch platforms include the Cisco Nexus Series switches.

Virtual Networking
Networks are becoming increasingly virtualized. Cisco Nexus virtual networking switch platforms provide secure multi-tenant services by adding virtualization intelligence technology to the data center network.

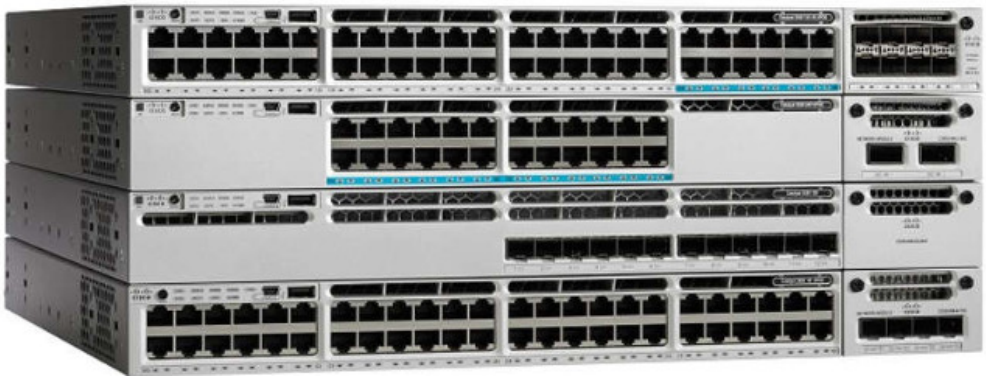
11.3.2. Switch Form Factors

When selecting switches, network administrators must determine the switch form factors. This includes fixed configuration, modular configuration, stackable, or non-stackable

Click each button for more information about switch form factors.

- Fixed configuration switches
- Modular configuration switches
- Stackable configuration switches
- Thickness

Fixed configuration switches
Features and options on fixed configuration switches are limited to those that originally come with the switch.



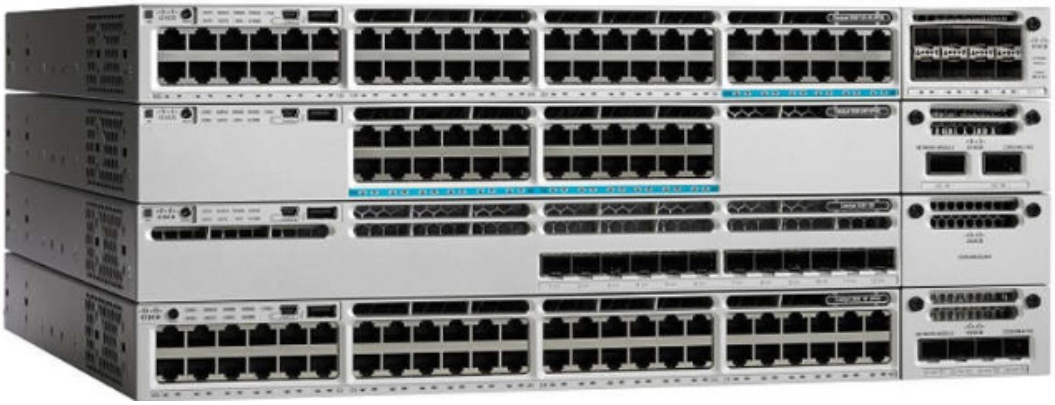
Modular configuration switches
The chassis on modular switches accept field-replaceable line cards.

11.3.3. Port Density

The port density of a switch refers to the number of ports available on a single switch. The figure shows the port density of three different switches.

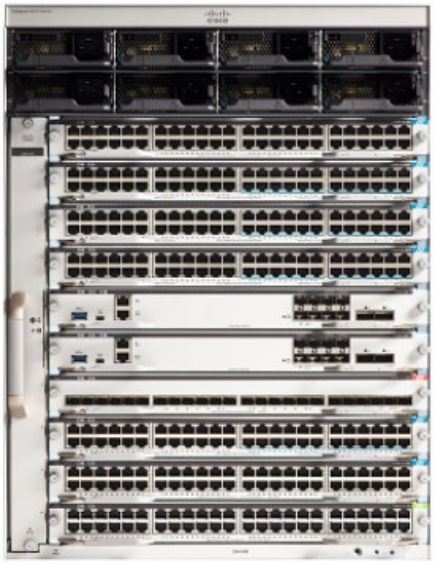
Fixed configuration switches support a variety of port density configurations. The Cisco Catalyst 3850 come in 12, 24, 48 port configurations, as shown in the figure. The 48-port switch has an option for additional ports for small form-factor pluggable (SFP) devices.

Cisco Catalyst 3850 Switches



Modular switches can support very high port densities through the addition of multiple switchport line cards. The modular Catalyst 9400 switch shown in the next figure supports 384 switchport interfaces.

Catalyst 9400 Switch



Large networks that support many thousands of network devices require high density, modular switches to make the best use of space and power. Without using a high-density modular switch, the network would need many fixed configuration switches to accommodate the number of devices that need network access. This approach can consume many power outlets and a lot of closet space.

The network designer must also consider the issue of uplink bottlenecks. A series of fixed configuration switches may consume many additional ports for bandwidth aggregation between switches, for the purpose of achieving target performance. With a single modular switch, bandwidth aggregation is less of an issue because the backplane of the chassis can provide the necessary bandwidth to accommodate the devices connected to the switchport line cards.

11.3.4. Forwarding Rates

Forwarding rates define the processing capabilities of a switch by rating how much data the switch can process per second. Switch product lines are classified by forwarding rates. Entry-level switches have lower forwarding rates than enterprise-level switches. Forwarding rates are important to consider when selecting a switch. If the switch forwarding rate is too low, it cannot accommodate full wire-speed communication across all of its switch ports. Wire speed is the data rate that each Ethernet port on the switch is capable of attaining. Data rates can be 100 Mbps, 1 Gbps, 10 Gbps, or 100 Gbps.

For example, a typical 48-port gigabit switch operating at full wire speed generates 48 Gbps of traffic. If the switch only supports a forwarding rate of 32 Gbps, it cannot run at full wire speed across all ports simultaneously. Fortunately, access layer switches typically do not need to operate at full wire speed, because they are physically limited by their uplinks to the distribution layer. This means that less expensive, lower performing switches can be used at the access layer, and more expensive, higher performing switches can be used at the distribution and core layers, where the forwarding rate has a greater impact on network performance.

11.3.5. Power over Ethernet

Power over Ethernet (PoE) allows the switch to deliver power to a device over the existing Ethernet cabling. This feature can be used by IP phones and some wireless access points, allowing them to be installed anywhere that there is an Ethernet cable. A network administrator should ensure that the PoE features are actually required for a given installation, because switches that support PoE are expensive.

Click each button to view PoE ports on different devices.

- Switch
- IP Phone
- WAP
- Cisco Catalyst 2960-C

Switch
PoE ports look the same as any other switch port. Check the model of the switch to determine if the port supports PoE.

WAP
PoE ports on wireless access points look the same as any other switch port. Check the model of the wireless access point to determine if the port supports PoE.

11.3.6. Multilayer Switching

Multilayer switches are typically deployed in the core and distribution layers of an organization's switched network. Multilayer switches are characterized by their ability to build a routing table, support a few routing protocols, and forward IP packets at a rate close to that of Layer 2 forwarding. Multilayer switches often support specialized hardware, such as application-specific integrated circuits (ASICs). ASICs along with dedicated software data structures can streamline the forwarding of IP packets independent of the CPU.

There is a trend in networking toward a pure Layer 3 switched environment. When switches were first used in networks, none of them supported routing. Now, almost all switches support routing. It is likely that soon all switches will incorporate a route processor because the cost of doing so is decreasing relative to other constraints.

The figure shows a Catalyst 2960. Catalyst 2960 switches illustrate the migration to a pure Layer 3 environment. With IOS versions prior to 15.x, these switches supported only one active switched virtual interface (SVI). With IOS 15.x, these switches now support multiple active SVIs. This means that the switch can be remotely accessed via multiple IP addresses on distinct networks.

11.3.7. Business Considerations for Switch Selection

The following table highlights other common business considerations when selecting switch equipment.

Consideration	Description

Consideration	Description
Cost	The cost of a switch will depend on the number and speed of the interfaces, supported features, and expansion capability.
Port density	Network switches must support the appropriate number of devices on the network.
Power	It is now common to power access points, IP phones, and compact switches user Power over Ethernet (PoE). In addition to PoE considerations, some chassis-based switches support redundant power supplies.
Reliability	The switch should provide continuous access to the network.
Port speed	The speed of the network connection is of primary concern to end users.
Frame buffers	The ability of the switch to store frames is important in a network where there may be congested ports to servers or other areas of the network.
Scalability	The number of users on a network typically grows over time; therefore, the switch should provide the opportunity for growth.

11.4. Router Hardware

11.4.1. Router Requirements

Switches are not the only component of a network that come with a variety of features. Your choice of router is another very important decision. Routers play a critical role in networking by connecting homes and businesses to the internet, interconnecting multiple sites within an enterprise network, providing redundant paths, and connecting ISPs on the internet. Routers can also act as a translator between different media types and protocols. For example, a router can accept packets from an Ethernet network and re-encapsulate them for transport over a serial network.

Routers use the network portion (prefix) of the destination IP address to route packets to the proper destination. They select an alternate path if a link goes down. All hosts on a local network specify the IP address of the local router interface in their IP configuration. This router interface is the default gateway. The ability to route efficiently and recover from network link failures is critical to delivering packets to their destination.

Routers also serve other beneficial functions as follows:

- They provide broadcast containment by limiting broadcasts to the local network.
- They interconnect geographically separated locations.
- The group users logically by application or department within a company, who have command needs or require access to the same resources.

- They provide enhanced security by filtering unwanted traffic through access control lists.

11.4.2. Cisco Routers

As the network grows, it is important to select the proper routers to meet its requirements. There are different categories of Cisco routers.

Click each button for more information about the categories of routers.

Branch Routers
Branch routers, shown in the figure, optimize branch services on a single platform while delivering an optimal application experience across branch and WAN infrastructures. Maximizing service availability at the branch requires networks designed for 24x7x365 uptime. Highly available branch networks must ensure fast recovery from typical faults, while minimizing or eliminating the impact on service, and provide simple network configuration and management. Shown are the Cisco Integrated Services Router (ISR) 4000 Series Routers.

11.4.3. Router Form Factors

Like switches, routers also come in many form factors. Network administrators in an enterprise environment should be able to support a variety of routers, from a small desktop router to a rack-mounted or blade model.

Click each button for more information on various Cisco router platforms.

Cisco 900 Series
This is a small branch office router. It combines WAN, switching, security, and advanced connectivity options in a compact, fanless platform for small and medium-sized businesses.

Cisco 800 Industrial Integrated Services Router

This router is compact and designed for harsh environments.

Routers can also be categorized as fixed configuration or modular. With the fixed configuration, the desired router interfaces are built-in. Modular routers come with multiple slots that allow a network administrator to change the interfaces on the router. Routers come with a variety of different interfaces, such as Fast Ethernet, Gigabit Ethernet, Serial, and Fiber-Optic.

A comprehensive list of Cisco routers can be found by searching Cisco's website www.cisco.com.

11.5. Module Practice and Quiz

11.5.1. Packet Tracer – Compare Layer 2 and Layer 3 Devices

In this Packet Tracer activity, you will use various commands to examine three different switching topologies and compare the similarities and differences between the 2960 and 3650 switches. You will also compare the routing table of a 4321 router with that of a 3650 switch.

11.5.1 Packet Tracer – Compare Layer 2 and Layer 3 Devices

11.5.2. What did I learn in this module?

Hierarchical Networks

All enterprise networks must: support critical applications, support converged network traffic, support diverse business needs, and provide centralized administrative control. The Cisco Borderless Network provides the framework to unify wired and wireless access, including policy, access control, and performance management across many different device types. The borderless network is built on a hierarchical infrastructure of hardware that is scalable and resilient. Two proven hierarchical design frameworks for campus networks are the three-tier layer and the two-tier layer models. The three critical layers within these tiered designs are the access, distribution, and core layers. The access layer represents the network edge, where traffic enters or exits the campus network. Access layer switches connect to distribution layer switches, which implement network foundation technologies such as routing, quality of service, and security. The distribution layer interfaces between the access

layer and the core layer. The primary purpose of the core layer is to provide fault isolation and high-speed backbone connectivity. Networks have fundamentally changed to switched LANs in a hierarchical network, providing QoS, security, support for wireless connectivity and IP telephony and mobility services.

Scalable Networks

A basic network design strategy includes the following recommendations: use expandable, modular equipment, or clustered devices; design a hierarchical network to include modules that can be added, upgraded, and modified; create a hierarchical IPv4 and IPv6 address strategy; and choose routers or multilayer switches to limit broadcasts and filter other undesirable traffic from the network. Implement redundant links in the network between critical devices and between access layer and core layer devices. Implement multiple links between equipment, with either link aggregation (EtherChannel) or equal cost load balancing, to increase bandwidth. Use a scalable routing protocol and implementing features within that routing protocol to isolate routing updates and minimize the size of the routing table. Implement wireless connectivity to allow for mobility and expansion. One method of implementing redundancy is by installing duplicate equipment and providing failover services for critical devices. Another method of implementing redundancy is to create redundant paths. A well-designed network not only controls traffic, but also limits the size of failure domains. Switch blocks act independently of the others, so the failure of a single device does not cause the network to go down. Link aggregation, such as EtherChannel, allows an administrator to increase the amount of bandwidth between devices by creating one logical link made up of several physical links. Wireless connectivity expands the access layer. When implementing a wireless network, you must consider the types of wireless devices to use, wireless coverage requirements, interference considerations, and security. Link-state routing protocols such as OSPF, work well for larger hierarchical networks where fast convergence is important. OSPF routers establish and maintain neighbor adjacencies with other connected OSPF routers, they synchronize their link-state database. When a network change occurs, link state updates are sent, informing other OSPF routers of the change and establishing a new best path.

Switch Hardware

There are several categories of switches for enterprise networks including campus LAN, cloud-managed, data center, service provider, and virtual networking. Form factors for switches include fixed configuration, modular configuration, and stackable configuration. The thickness of a switch is expressed in number of rack units. The port density of a switch refers to the number of ports available on a single switch. Forwarding rates define the processing capabilities of a switch by rating how much data the switch can process per second. Power over Ethernet (PoE) allows the switch to deliver power to a device over the existing Ethernet cabling. Multilayer switches are typically deployed in the core and distribution layers of an organization’s switched network. Multilayer switches are

characterized by their ability to build a routing table, support a few routing protocols, and forward IP packets at a rate close to that of Layer 2 forwarding. Business considerations for switch selection include cost, port density, power, reliability, port speed, frame buffers, and scalability.

Router Hardware

Routers use the network portion (prefix) of the destination IP address to route packets to the proper destination. They select an alternate path if a link or path goes down. All hosts on a local network specify the IP address of the local router interface in their IP configuration. This router interface is the default gateway. Routers also serve other beneficial functions:

- They provide broadcast containment by limiting broadcasts to the local network.
- They interconnect geographically separated locations.
- They group users logically by application or department within a company, who have command needs or require access to the same resources.
- They provide enhanced security by filtering unwanted traffic through access control lists.

Cisco has several categories of routers including branch, network edge, service provider and industrial. Branch routers optimize branch services on a single platform while delivering an optimal application experience across branch and WAN infrastructures. Network edge routers deliver high-performance, highly secure, and reliable services that unite campus, data center, and branch networks. Service provider routers differentiate the service portfolio and increase revenues by delivering end-to-end scalable solutions and subscriber-aware services. Industrial routers are designed to provide enterprise-class features in rugged and harsh environments. Cisco router form factors include the Cisco 900 Series, the ASR 9000 and 1000 Series, the 5500 Series, and the Cisco 800. Routers can also be categorized as fixed configuration or modular. With the fixed configuration, the desired router interfaces are built-in. Modular routers come with multiple slots that allow a network administrator to change the interfaces on the router. Routers come with a variety of different interfaces, such as Fast Ethernet, Gigabit Ethernet, Serial, and Fiber-Optic.

11.5.3 Module Quiz – Network Design

Download Slide Powerpoint (PPT)

CCNA 3 v7.0 Curriculum: Module 11 - Network Design.pptx

1 file(s) 17.87 MB

Download

Tags:ccna 3 v7 modules