Enterprise Network Fundamentals

Recall

Networks have had to evolve to keep up with huge increases in basic, mission-critical user needs and to handle bigger burdens like multimedia remote presentations, conferencing, and the like.
The challenge we need to address is how to connect relevant networks so all users can share the wealth of whatever services and resources they need, on site or remotely.

Some basics

one collision domain and one broadcast domain

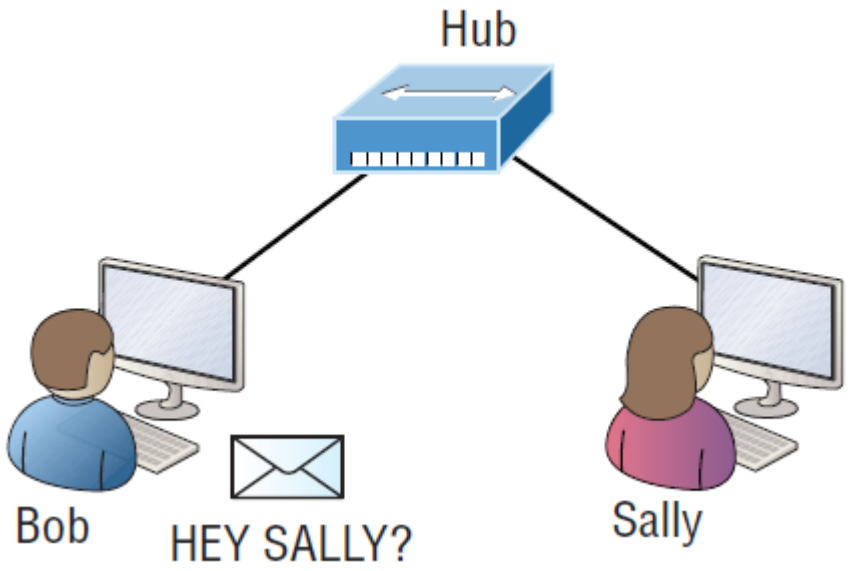


Figure 1 A basic SOHO network

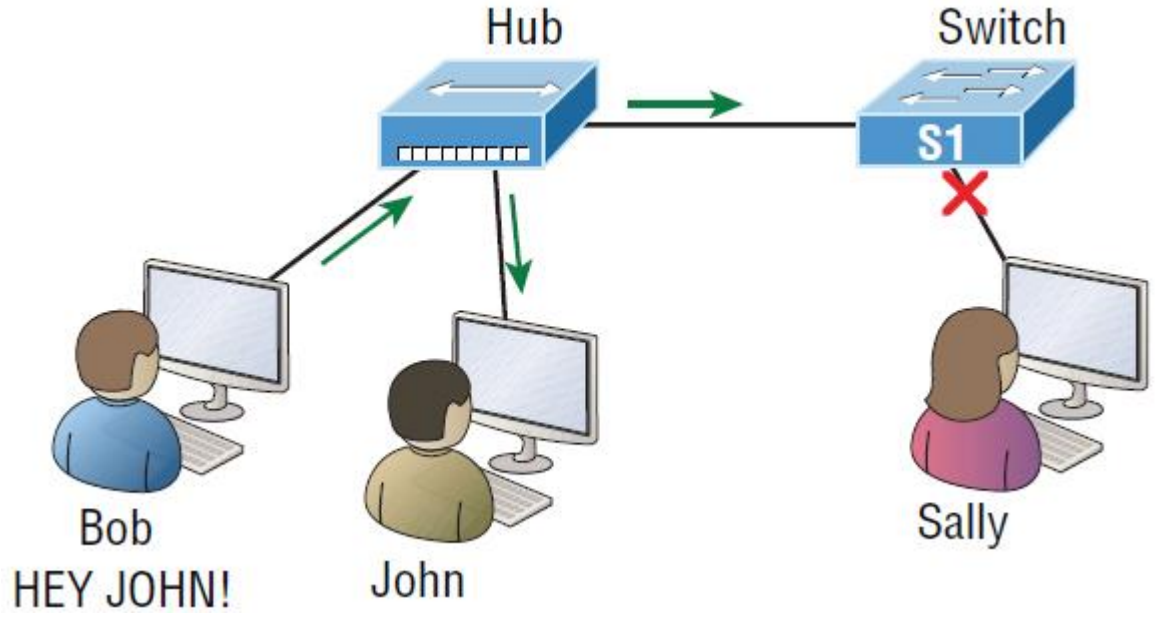


Figure 2 A switch can break up collision domains.

Note that this network is still just one, single broadcast domain. This means we've really only reduced our PC's chaos—not eliminated it.

Here's a list of some of the things that commonly cause LAN traffic congestion:
■■ Too many hosts in a collision or broadcast domain
■■ Broadcast storms
■■ Too much multicast traffic
■■ Low bandwidth
■■ Adding hubs for connectivity to the network
■■ A bunch of ARP broadcasts

Hubs don't segment a network; they just connect network segments. Basically, they are an inexpensive way to connect a couple of PCs, which can work for really simple home use.
Adding routers to a NW allows us to connect networks and route packets of data from one network to another. Routers are basically employed to efficiently break up a broadcast domain—the set of all devices on a network segment, which are allowed to "hear" all broadcasts sent out on that specific segment.

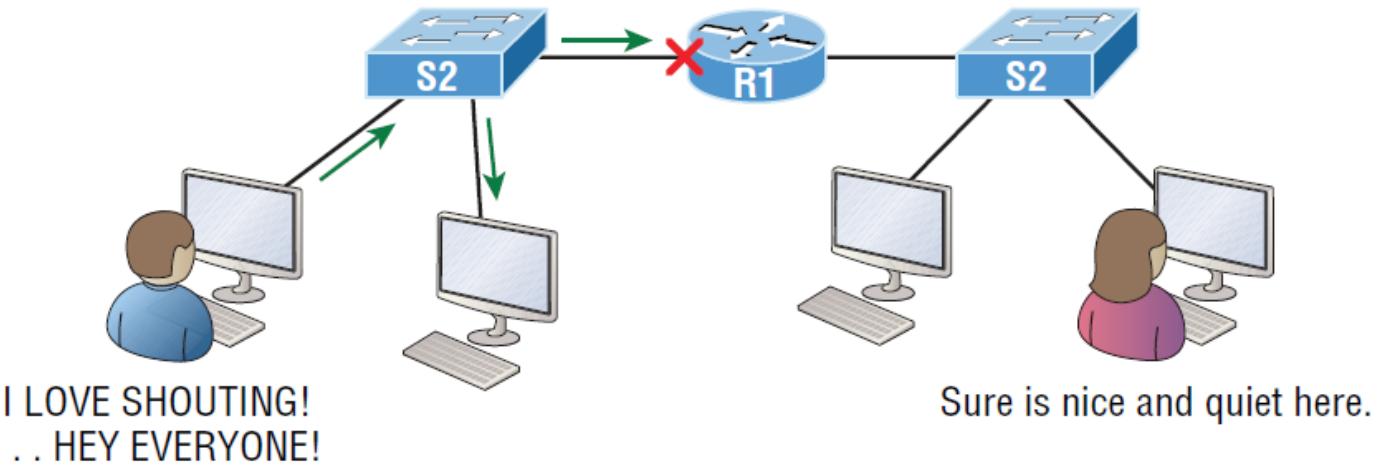


Figure 3 Routers create an internetwork.

In the network above (fig 3), each host is connected to its own collision domain because of the switch, and the router has created two broadcast domains. So now Sally is happily living in peace in a completely different neighborhood, no longer subjected to Bob's incessant shouting! If Bob wants to talk with Sally, he has to send a packet with a destination address using her IP address—he cannot broadcast for her!

But there's more… Routers provide connections to *wide area network (WAN)* services as well via a serial interface for WAN connections—specifically, a V.35 physical interface on a Cisco router.

Even though routers are known for breaking up broadcast domains by default, it's important to remember that they break up collision domains as well.
There are two advantages to using routers in your network:
■ They don't forward broadcasts by default.
■ They can filter the network based on layer 3 (Network layer) information such as an IP address.
The main purpose of layer 2 switches is to make a LAN work better
—to optimize its performance-by default, switches break up collision domains
—providing more bandwidth for the LAN's users.
Also, these switches don't forward packets to other networks like routers do. Instead, they only "switch" frames from one port to another within the switched network.

Collision domain is an Ethernet term used to describe a network scenario in which one device sends a packet out on a network segment and every other device on that same segment is forced to pay attention to it no matter what. If two devices transmit at the same time, a collision will occur, requiring both devices to retransmit, as is common with hubs. By contrast, each and every port on a switch represents its own collision domain, allowing network traffic to flow much more smoothly.

Layer 2 switching is considered hardware-based bridging because it uses specialized hardware called an *application-specific integrated circuit (ASIC).* ASICs can run up to high gigabit speeds with very low latency rates.

Latency is the time measured from when a frame enters a port to when it exits a port.

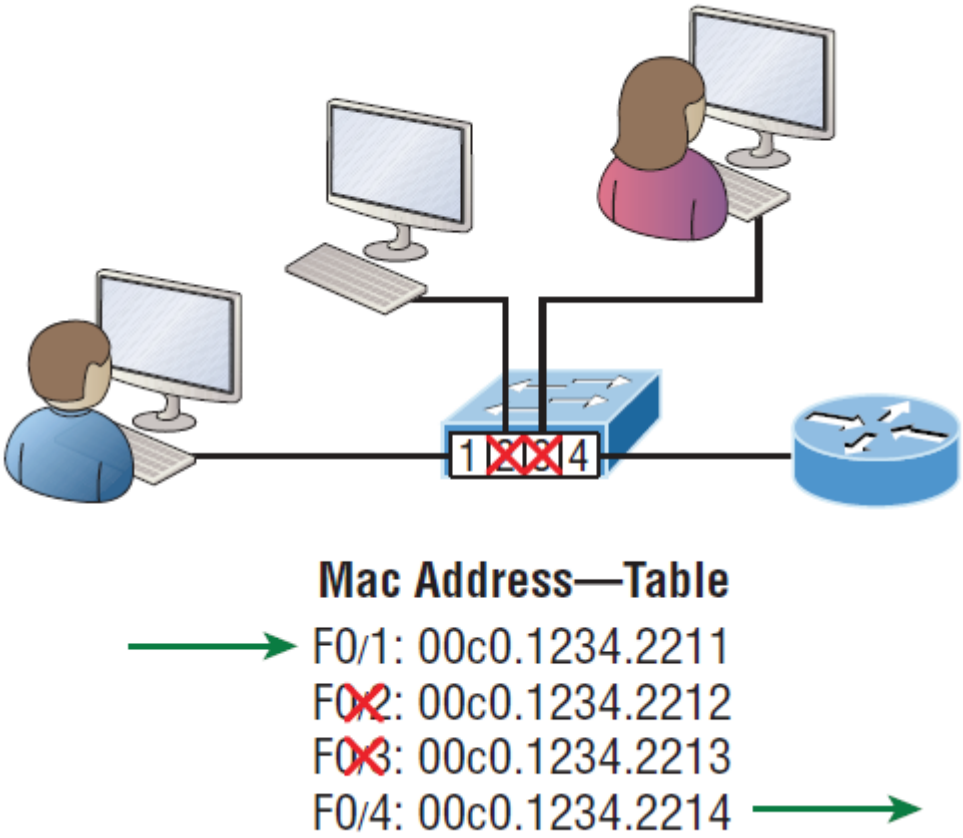


Figure 4 switches work at layer 2

Remember, networks are to routers as individual devices are to switches and bridges. Primarily, layer 3 machines, like routers, need to locate specific networks, whereas layer 2 machines like switches and bridges need to eventually locate specific devices.
All devices that the broadcast is forwarded to are considered to be in the same broadcast domain. This can be a problem because layer 2 devices propagate layer 2 broadcast storms that can seriously choke performance, and the only way to stop a broadcast storm from propagating through an internetwork is with a layer 3 device—a router!

Network Topology Architectures

A hierarchy that helps us understand where things belong, how things fit together, and what functions go where. It brings order to otherwise complex models.

Hierarchy offers a lot of benefits in network design. When used properly, it makes networks more predictable and helps us to define which areas should perform certain functions. For example, you can use tools like access lists at certain levels within hierarchical networks and avoid them at others.

Large networks can be extremely complicated, involving multiple protocols, detailed configurations, and diverse technologies. Hierarchy helps us summarize a complex collection of details into an understandable model, bringing order from the chaos. Then, as specific configurations are needed, the model dictates the correct way to apply them.

The Cisco Three-Layer Hierarchical Model (3-Tier)

The Cisco hierarchical model can help you design, implement, and maintain a scalable, reliable, cost-effective hierarchical internetwork.

Cisco defines three layers of hierarchy, as shown in Figure 5, each with specific functions, and it's referred to as a 3-tier network architecture. Each layer has specific responsibilities. Keep in mind that the three layers are logical, so they aren't necessarily physical devices. Consider the OSI model, another logical hierarchy. Its seven layers describe functions but not necessarily protocols. Sometimes a protocol maps to more than one layer of the OSI model, and sometimes multiple protocols communicate within a single layer. In the same way, when we build physical implementations of hierarchical networks, we may have many devices in a single layer, or there may be a single device performing functions at two layers.

Just remember that the definition of the layers is logical, not physical!

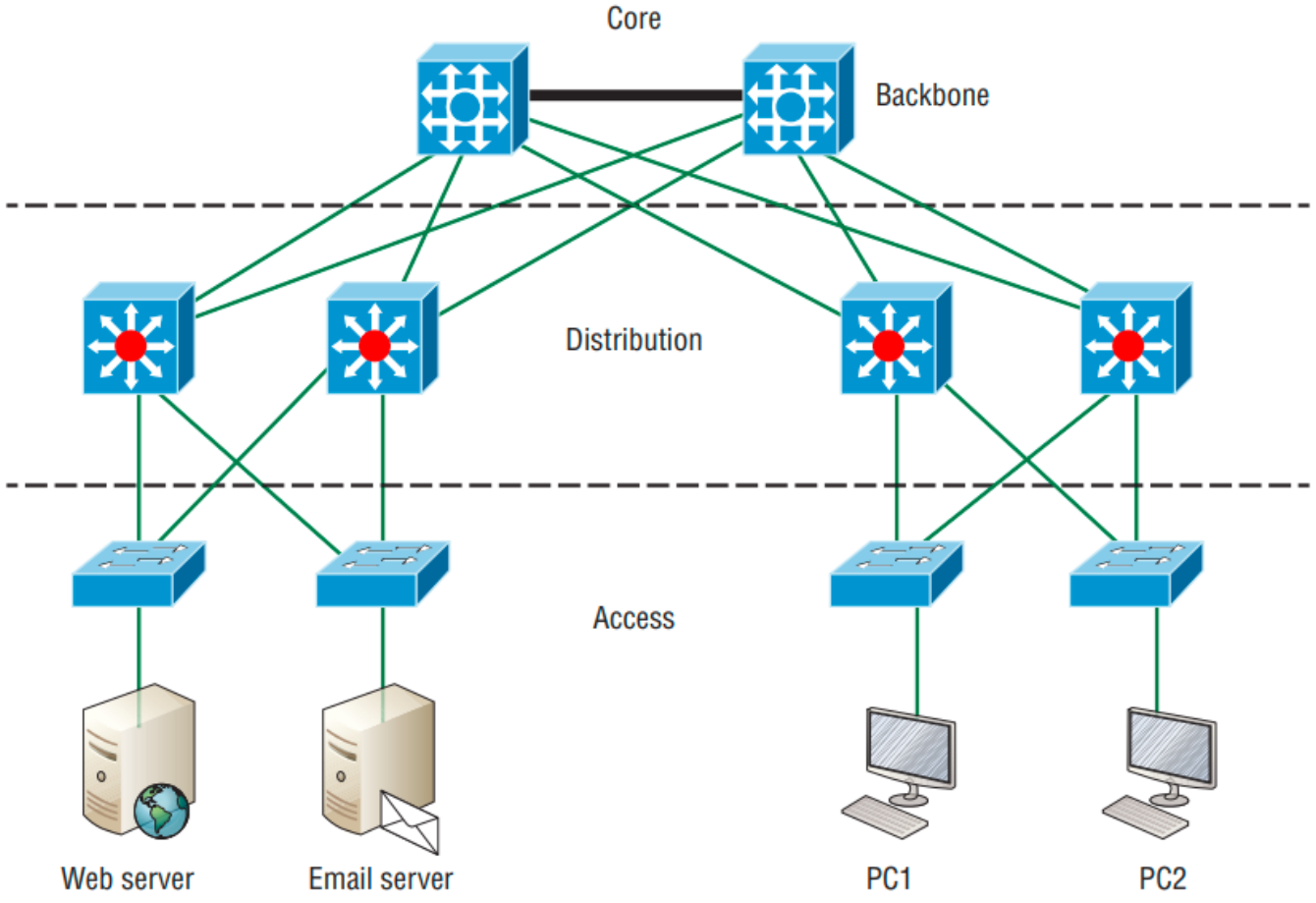


Figure 5 The Cisco hierarchical model

The Core Layer

It is the core of the network, at the top of the hierarchy.

It is responsible for transporting large amounts of traffic both reliably and quickly.

The prime purpose of the network's core layer is to switch traffic as fast as possible. The traffic transported across the core is common to a majority of users, but user data is processed at the distribution layer, which forwards the requests to the core if needed.

If there's a failure in the core, every single user can be affected! This is why fault tolerance at this layer is so important. The core is likely to see large volumes of traffic, so speed and latency are driving concerns here. Given the function of the core, some vital design specifics need be considered:

■ Never do anything to slow down traffic.

- This includes making sure you don't use access lists, perform routing between virtual local area networks, or implement packet filtering.

■ Don't support workgroup access here.

■ Avoid expanding the core, e.g., adding routers as the internetwork grows. If performance becomes an issue in the core, go with upgrades over expansion.

Here's a list of goals we want to achieve as we design the core:

■ Design the core for high reliability. Consider data-link technologies that facilitate both speed and redundancy, like Gigabit Ethernet with redundant links or even 10 Gigabit Ethernet.

■ Design with speed in mind. The core should have very little latency.

■ Select routing protocols with lower convergence times.

- Redundant data-link connectivity is of no benefit here.

The Distribution Layer

The distribution layer is sometimes referred to as the workgroup or aggregation layer and is the communication point between the access layer and the core.

The primary functions of the distribution layer are to provide routing, filtering, and WAN access and to determine how packets can access the core, if needed. The distribution layer must determine the fastest way that network service requests are handled—for instance, how a file request is forwarded to a server. After the distribution layer determines the best path, it forwards the request to the core layer if necessary. The core layer then quickly transports the request to the correct service.

The distribution layer is where we implement policies for the network because we have a lot of flexibility in defining network operation here.

There are several things that should generally be handled at the distribution layer:

■ Routing

■ Implementing tools (like access lists), packet filtering, and queuing

■ Implementing security and network policies, including address translation and firewalls

■ Redistributing between routing protocols, including static routing

■ Routing between VLANs and other workgroup support functions

■ Defining broadcast and multicast domains

At the distribution layer, it’s key to avoid anything limited to functions exclusively belonging to one of the other layers!

The Access Layer

The access layer controls user and workgroup access to internetwork resources and is sometimes referred to as the desktop layer. The network resources most users need are available locally because the distribution layer handles any traffic for remote services.

Here are some of the tasks the access layer carries out:

■ Implementing access control and policies

■ Creation of separate collision domains (microsegmentation/switches)

■ Workgroup connectivity into the distribution layer

■ Device connectivity

Resiliency and security services

■ Advanced technology capabilities (voice/video, etc.)

■ QoS Marking

Collapsed Core (2-Tier)

The Collapsed core design is also referred to as 2-tier because it's only 2-layers.

Conceptually, it's like the 3-tier only less expensive and geared for smaller companies.

The design is meant to maximize performance and user availability to the network, while still allowing for design scalability over time.

In a 2-tier, the distribution is merged with the core layer, as shown in Figure 6.

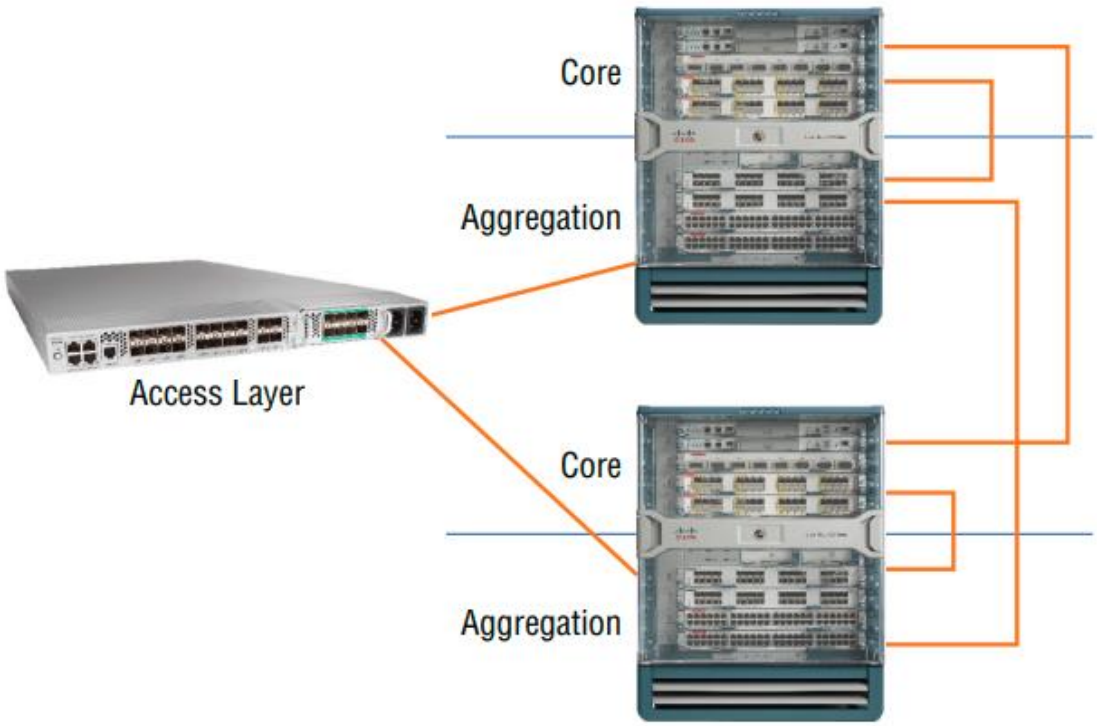


Figure 6 Real-life collapsed core (2-tier) Image

Here you see the Core and Distribution (also called Aggregation) are both running on the same large enterprise switch. The Access layer switches connect into the enterprise switch, only in the defined Aggregation ports.

This design is much more economical and it's still very functional in a campus environment, where your network many not really grow significantly larger over time.

It's known as a "collapsed core" in reference to its design in which the distribution layer and core layer functions are implemented by a single device.

The big reason the collapsed core design exists is for reducing network costs, while maintaining most of the benefits of the three-tier hierarchical model.

Spine-Leaf

A typical data center has racks filled with servers. In the leaf and-spine design, there are switches found at the top and end of each rack that connect to these servers, with a server connecting into each switch for redundancy, referred to as a top-of-rack (ToR) design because the switches physically reside at the top of a rack.

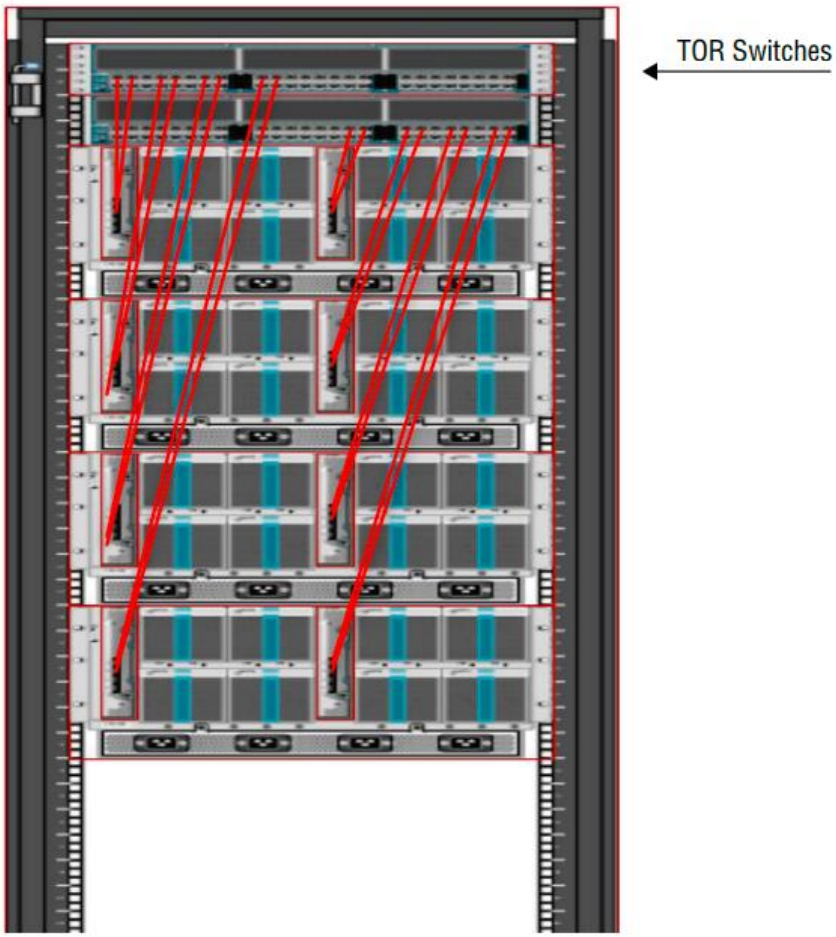


Figure 7 Top of Rack Network Design

These ToR switches act as the leaves within the leaf-and-spine topology. The ports in the leaf switches connect to a node, e.g., a server in the rack, a firewall, a load-balancing appliance, or a router leaving the data center, as well as to the spine switch.

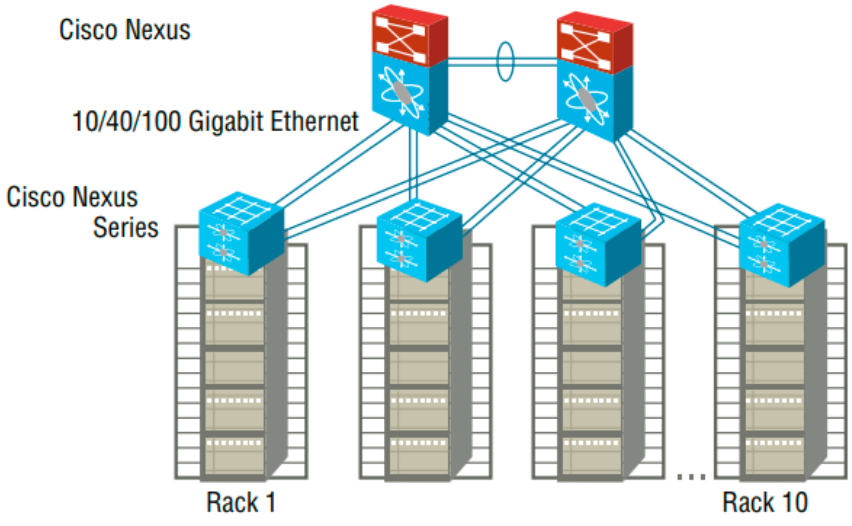


Figure 8 Spine-leaf design

Each leaf switch connects to every spine switch, which means we no longer need a numerous connections between switches. The spine only connects to leaf devices, not to servers or end devices. When you connect your ToR data center switches in a leaf and-spine topology, all of your switches are the same distance away from one another (single switch hop).

WAN

A major distinction between a WAN and a LAN is that while you generally own a LAN infrastructure, you usually lease a WAN infrastructure from a service provider.

There are several reasons why WANs are necessary in corporate environments today. LAN technologies provide pretty solid speeds—10/25/40/100Gbps.

We still need WANs in a communications environment because some business needs require connections to remote sites for many reasons:

■ People in the regional or branch offices of an organization need to be able to communicate and share data.

■ Organizations often want to share information with other organizations across large distances.

■ Employees who travel on company business frequently need to access information that resides on their corporate networks.

Characteristics of WANs:

■ WANs generally connect devices that are separated by a broader geographic area than a LAN can serve.

■ WANs use the services of carriers like telcos, cable companies, satellite systems, and network providers.

■ WANs use serial connections of various types to provide access to bandwidth over large geographic areas.

The first key to understanding WAN technologies is to be familiar with the different WAN topologies, terms, and connection types commonly used by service providers to join our LAN networks together.

WAN Terminologies

Before you order a WAN service type from a provider, you really need to understand the following terms that service providers typically use:

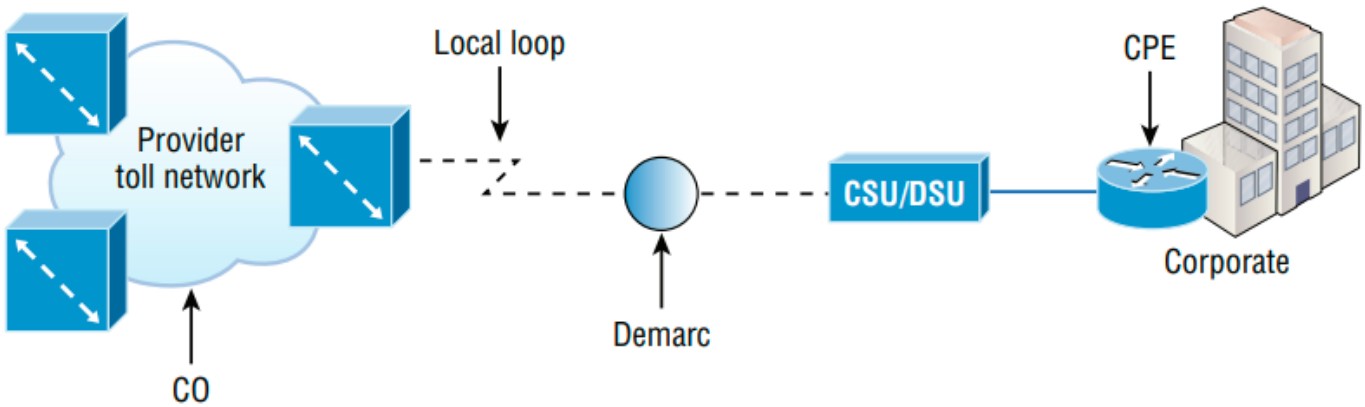


Figure 9 WAN terms

Customer premises equipment (CPE): Customer premises equipment (CPE) is equipment that's typically owned by the subscriber and located on the subscriber's premises.

CSU/DSU: A Channel Service Unit/Data Service Unit (CSU/DSU) is a device that's used to connect a DTE to a digital circuit like a T1/T3 line. *A device is considered DTE if it's either a source or destination for digital data—for example, PCs, servers, and routers.* In Figure 9 above, the router is

considered DTE because it's passing data to the CSU/DSU, which will forward the data to the service provider. Although the CSU/DSU connects to the service provider's infrastructure using a telephone or coaxial cable like a T1 or E1 line, it connects to the router with a serial cable. The CSU/DSU provides clocking of the line to the router.

Demarcation point: The demarcation point (demarc for short) is the precise spot where the service provider's responsibility ends and the CPE begins. It's generally a device in a telecommunications closet owned and installed by the telecommunications company (telco). It's your responsibility to cable (extended demarc) from this box to the CPE, which is usually a connection to a CSU/DSU.

Local loop: The local loop connects the demarc to the closest switching office, referred to as the central office.

Central office (CO)/Point of Presence (POP): This point connects the customer's network to the provider's switching network.

Toll network: The toll network is a trunk line inside a WAN provider's network. This network is a collection of switches and facilities owned by the Internet service provider (ISP).

Optical fiber converters: Even though not shown in Figure 9, optical fiber converters are used where a fiber-optic link terminates to convert optical signals into electrical signals and vice versa. You can also implement the converter as a router or switch module.

Make sure you're comfortable with these terms, what they represent, and where they're located, as shown in Figure 9, because they're key to understanding WAN technologies.

WAN Connection Bandwidth

Here are some important bandwidth terms used when referring to WAN connections:

Digital Signal 0 (DS0) This is the basic digital signaling rate of 64 Kbps, equivalent to one channel. Europe uses the E0 and Japan uses the J0 to reference the same channel speed. Typical to T-carrier transmission, this is the generic term used by several multiplexed digital carrier systems and is also the smallest-capacity digital circuit. 1 DS0 = 1 voice/data line.

T1 Also referred to as a DS1, a T1 comprises 24 DS0 circuits bundled together for a total bandwidth of 1.544 Mbps.

E1 This is the European equivalent of a T1 and comprises 30 DS0 circuits bundled together for a bandwidth of 2.048 Mbps.

T3 Referred to as a DS3, a T3 comprises 28 DS1s bundled together, or 672 DS0s, for a bandwidth of 44.736 Mbps.

OC-3 Optical Carrier (OC) 3 uses fiber and is made up of three DS3s bundled together. It's made up of 2,016 DS0s and avails a total bandwidth of 155.52 Mbps.

OC-12 Optical Carrier 12 is made up of four OC-3s bundled together and contains 8,064 DS0s for a total bandwidth of 622.08 Mbps.

OC-48 Optical Carrier 48 is made up of four OC-12s bundled together and contains 32,256 DS0s for a total bandwidth of 2488.32 Mbps.

Physical Interfaces and Cables

Ethernet was first implemented by a group called DIX, Digital, Intel, and Xerox. They created and implemented the first Ethernet LAN specification, which the IEEE used to create the IEEE 802.3 committee. This was a 10 Mbps network that ran on coax, then eventually twisted-pair and fiber physical media.

The IEEE extended the 802.3 committee to three new committees known as 802.3u (Fast Ethernet), 802.3ab (Gigabit Ethernet on category 5), and then finally 802.3ae (10 Gbps over fiber and coax). There are more standards evolving almost daily, like 100 Gbps Ethernet (802.3ba).

When designing your LAN, it's really important to understand the different types of Ethernet media available to you.

Sure, it would be great to run TenGigabit Ethernet to each desktop and 100 Gbps between switches, but would you to justify the cost of that network?! However, if you mix and match the different types of Ethernet media methods currently available, you can come up with a cost-effective network solution that still works really great.

The EIA/TIA (Electronic Industries Alliance and the newer Telecommunications Industry Association) is the standards body that creates the Physical layer specifications for Ethernet. The EIA/TIA specifies that Ethernet use a registered jack (RJ) connector on unshielded twisted-pair (UTP) cabling (RJ45). A.k.a 8-pin connector.

- Every Ethernet cable type has inherent attenuation, which is defined as the loss of signal strength as it travels the length of a cable and is measured in decibels (dB).
- The cabling used in corporate and home markets is measured in categories. A higher-quality cable will have a higher-rated category and lower attenuation.
  e.g. category 6 is better than category 5 because category 6 cables have cables have more wire twists per foot and therefore less crosstalk.
- Crosstalk is the unwanted signal interference from adjacent pairs in the cable.

Here's a list of some of the most common IEEE Ethernet standards:

10Base-T (IEEE 802.3) 10 Mbps using category 3 unshielded twisted pair (UTP) wiring for runs up to 100 meters. Unlike with the 10Base-2 and 10Base-5 networks, each device must connect into a hub or switch, and you can have only one host per segment or wire. It uses an RJ45 connector (8-pin modular connector) with a physical star topology and a logical bus.

100Base-TX (IEEE 802.3u) 100Base-TX, most commonly known as Fast Ethernet, uses EIA/TIA category 5, 5E, or 6 UTP two-pair wiring. One user per segment and up to 100 meters long, it uses an RJ45 connector with a physical star topology and a logical bus.

100Base-FX (IEEE 802.3u) Uses fiber cabling 62.5/125-micron multimode fiber. Point-to-point topology and up to 412 meters long. It uses ST and SC connectors, which are media interface connectors.

1000Base-CX (IEEE 802.3z) Copper twisted-pair, called twinax, is a balanced coaxial pair that can run only up to 25 meters and uses a special 9-pin connector known as the High Speed Serial Data Connector (HSSDC). This is used in Cisco's Data Center technologies.

1000Base-T (IEEE 802.3ab) Category 5, four-pair UTP wiring up to 100 meters long and up to 1 Gbps.

1000Base-SX (IEEE 802.3z) This is the implementation of 1 Gigabit Ethernet, running over multimode fiber-optic cable instead of copper twisted-pair cable, using short wavelength laser.

Multimode fiber (MMF) using 62.5- and 50-micron core and uses an 850 nanometer (nm) laser that can go up to 220 meters with 62.5-micron, 550 meters with 50-micron.

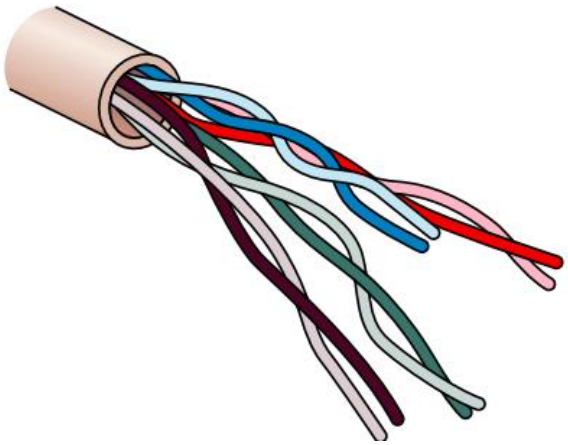
1000Base-LX (IEEE 802.3z) Single-mode fiber that uses a 9-micron core and 1300 nm laser that can go from 3 kilometers up to 10 kilometers.

1000Base-ZX (Cisco standard) 1000BaseZX, or 1000Base-ZX, is a Cisco specified standard for Gigabit Ethernet communication. 1000BaseZX operates on ordinary single-mode fiber-optic links with spans up to 43.5 miles (70 km). 10GBase-T (802.3.an)

10GBase-T is a standard proposed by the IEEE 802.3an committee to provide 10 Gbps connections over conventional UTP cables, (category 5e, 6, or 7 cables). 10GBase-T allows the conventional RJ45 used for Ethernet LANs and can support signal transmission at the full 100-meter distance specified for LAN wiring.

Ethernet Cabling

The most common Ethernet cable used today is the category 5 Enhanced Unshielded Twisted Pair (UTP).



Category 5 Enhanced UTP cable can handle speeds up to a gigabit with a distance of up to 100 meters. Typically we'd use this cable for 100 Mbps and category 6 for a gigabit, but the category 5 Enhanced is rated for gigabit speeds and category 6 is rated for 10 Gbps!

Figure 10 Category 5 Enhanced UTP cable

You need to really understand the following three types of cables:

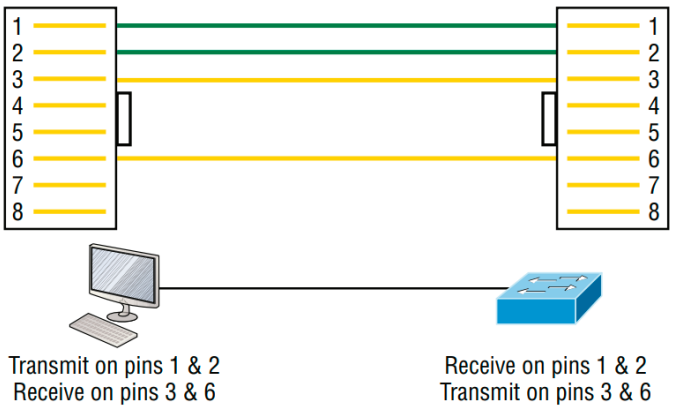
- Straight-through cable
- Crossover cable
- Rolled cable

Straight-Through Cable

The straight-through cable is used to connect the following devices:

- Host to switch or hub
- Router to switch or hub

Four wires are used in straight-through cable to connect Ethernet devices. NB: only pins 1, 2, 3, and 6 are used - connect 1 to 1, 2 to 2, 3 to 3, and 6 to 6. this would be a 10/100 Mbps Ethernet-only cable and wouldn't work with gigabit, voice, or other LAN or WAN technology.



Crossover Cable

The crossover cable can be used to connect these devices:

- Switch to switch
- Hub to hub
- Host to host
- Hub to switch
- Router direct to host
- Router to router

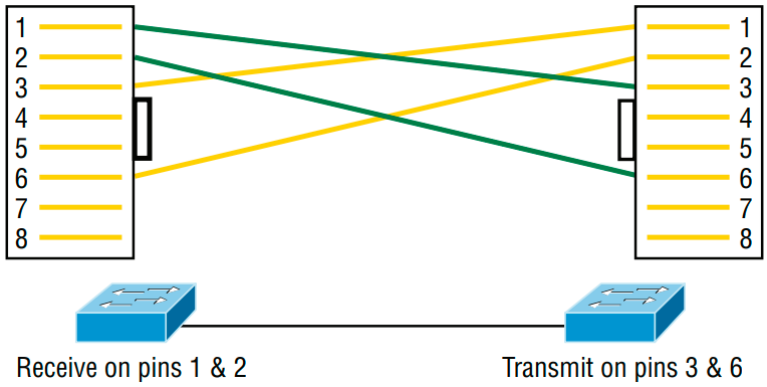


Figure 11 Crossover Ethernet cable

The same four wires used in the straight-through cable are used in this cable; we just connect different pins together. Figure 11 shows how the four wires are used in a crossover Ethernet cable. Notice here that instead of connecting 1 to 1, 2 to 2, and so on, here we connect pins 1 to 3 and 2 to 6 on each side of the cable.

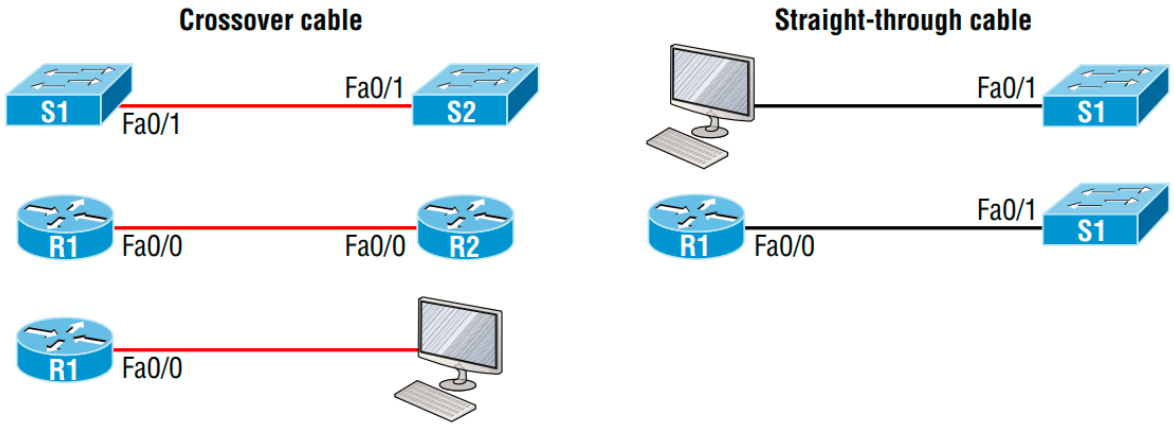
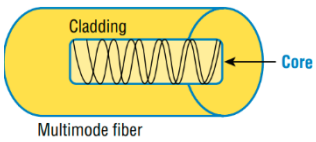


Figure 12 Typical uses for straight-through and cross-over Ethernet cables

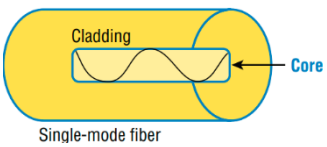
The crossover examples in Figure 12 are switch port to switch port, router Ethernet port to router Ethernet port, and router Ethernet port to PC Ethernet port. For the straight-through examples used are PC Ethernet to switch port and router Ethernet port to switch port. It's very possible to connect a straight-through cable between two switches, and it will start working because of autodetect mechanisms called auto-mdix.

Fiber Optic

Fiber optics has been used to go very long distances, as in intercontinental connections, but it's becoming more and more popular in Ethernet LAN networks due to the fast speeds available. Also, unlike UTP, it's immune to interference like crosstalk.



There are two major types of fiber optics: single-mode and multimode. Single-mode is more expensive, has a tighter cladding, and can go much farther distances than multimode. The difference comes in the tightness of the cladding, which makes a smaller core, hence only one mode of light will propagate down the fiber. Multimode is looser and has a larger core so it allows multiple light particles to travel down the glass. These particles have to be put back together at the receiving end. This means the distance is less than that with single-mode fiber, which allows only very few light particles to travel through the fiber.



Power over Ethernet (802.3af, 802.3at)

Power over Ethernet (PoE and PoE+) technology describes a system for transmitting electrical power, along with data, to remote devices over standard twisted-pair cable in an Ethernet network. This technology is useful for powering IP phones (Voice over IP, or VoIP), wireless LAN access points, network cameras, remote network switches, embedded computers, and other appliances. These are all situations where it would be inconvenient, expensive, and possibly not even feasible to supply power separately.

Figure 13 gives you an example of a Cisco Next Generation Firewall (NGFW). It has eight ports that can be routed or switched ports, and ports 7 & 8 are listed as PoE ports at 0.6A.

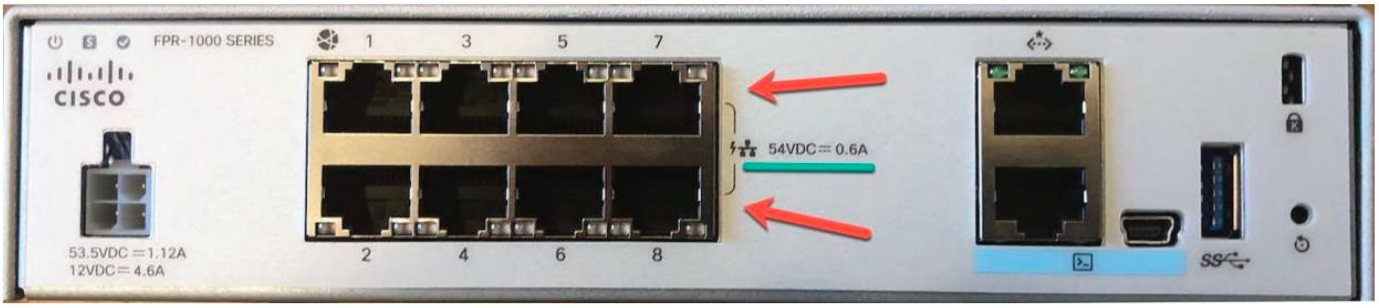


Figure 13 NGFW ports provide PoE