Designing & Deploying Network Solutions
for Small and Medium Business

Lecture (Chapter) 3

Network Infrastructure

Objectives

Describe wired network characteristics.

Choose an appropriate cable type for a given use.

Compare and contrast wired network topologies.

Describe the standards for wireless networks and their implementation.

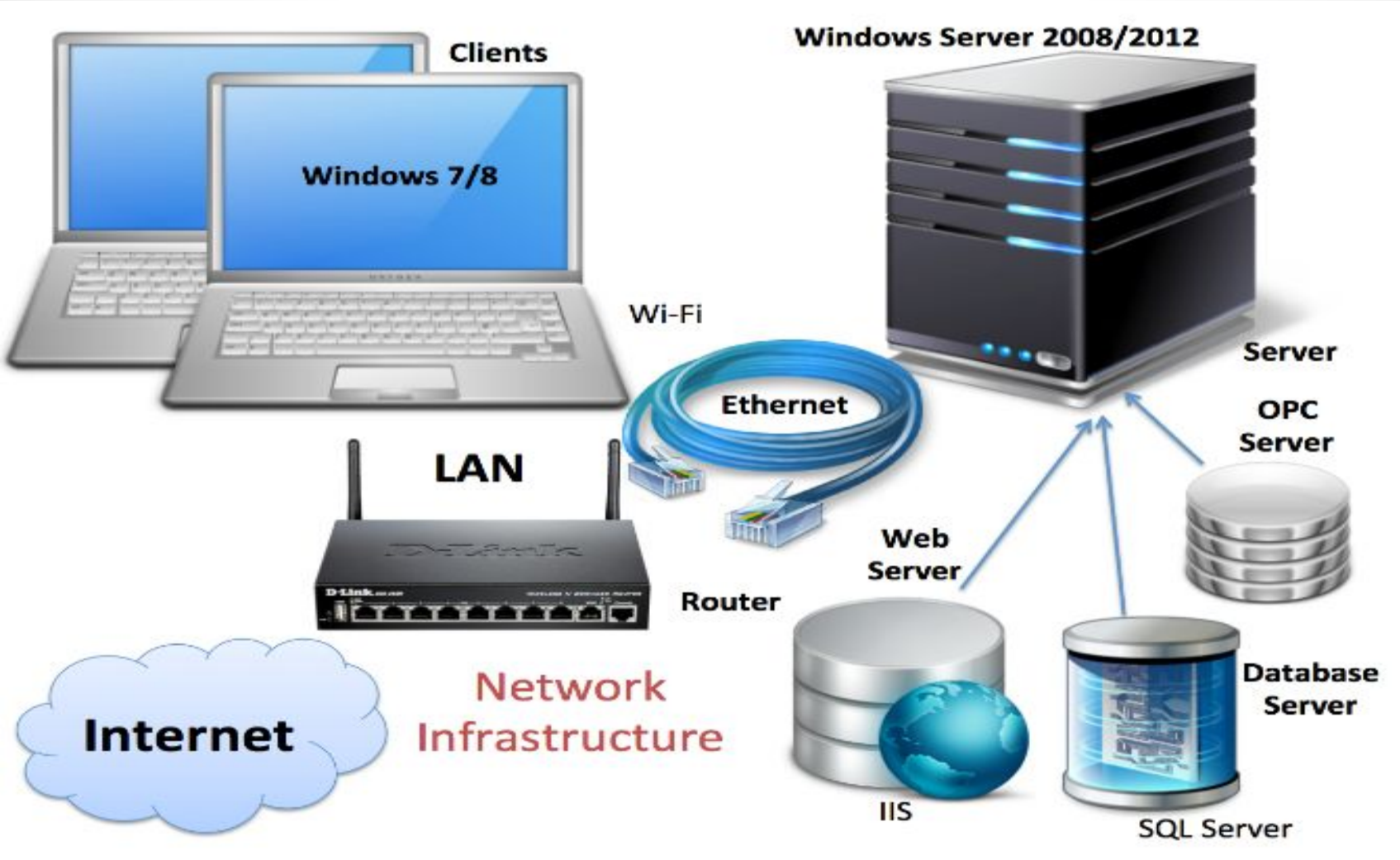
Compare wireless network security options.

Compare and contrast common wireless network configurations.

Describe the purpose and use of key network technologies:

- Subnet and VLAN
- NAT and PAT
- Firewalls and proxies
- VPN

Network Infrastructure



Network Infrastructure

The network infrastructure may consists of the Following parts:

- **Wired and Wireless Network with switches, routers and AP;**
- **Cables and Cabling;**
- **Windows Servers (local servers and central servers);**
- **Clients;**
- **SQL Server;**
- **Databases;**
- **Web Servers (IIS);**
- **Virtualization (HyperV and/or VMware).**

Wired Network Justifications

Availability

- Many commercial buildings are wired for networking when they are built. If they are not already wired, they are at least constructed with networking in mind, with routes for cables and wiring closets designed into the building.

Reliability

- Companies know that they can rely on wired networks. Wired networking equipment is based on established technologies. Most of the basic technologies have been in use for decades. After their installation, network components, including the cable plant and connectors, can go untouched for years. Sources of potential communication problems are well known and, in most situations, relatively easy to correct or avoid.

Wired Network Justifications

Established standards	• Components related to wired Ethernet deployments follow long-established standards implemented in the same basic way throughout the industry.
Flexibility	• Many options are available when designing and deploying a wired network. Rather than having to design a configuration completely from scratch, established designs can be modified to meet your needs.
Security	• In many ways, a wired network is more inherently secure than a wireless network, at least at the local level. Tapping into a wired cable and its data stream is more difficult than intercepting radio frequency transmissions. Tapping into a fiber optic cable is even more difficult.

Ethernet Implementations

The original Ethernet standards were based on coaxial cable installations. There were two initial standards:

- 10Base5
- 10Base2

The standard technology today uses either twisted pair or fiber optic cable. Cabling based on BaseT copper cable standards are the most prevalent. Copper cable standards that you are likely to see include:

- 10BaseT
- 100BaseT
- 1000BaseT
- 10GBaseT

Ethernet Implementations

There are also different Ethernet standards for fiber optic cable. The oldest of these is 10Base-FL. While limited to a maximum data rate of 10 Mbps, this standard supports cable segments of up to 1 km. Other fiber option standards include:

- 1000Base-LX
- 1000Base-SX
- 1000Base-ZX
- 10GBase-X

Ethernet Implementations

These fiber option standards support data rates of up to 1 Gbps, or, for 10GBase-X, 10 Gbps.

Maximum cable segment lengths vary between the standards, up to a maximum of 10 km for most common implementations.

Current fiber optic implementations are based upon the IEEE 802.3ah standard.

Higherspeed standards, including 40 Gb and 100 Gb Ethernet, are under development, and some devices operating at these speeds are currently available. However, most of these higher speed implementations are vendor-specific.

Wired Media

Are three basic types of wired network media. These are:

Coaxial

Twisted pair

- **Shielded twisted pair (STP)**
- **Unshielded twisted pair (UTP)**

Fiber optic

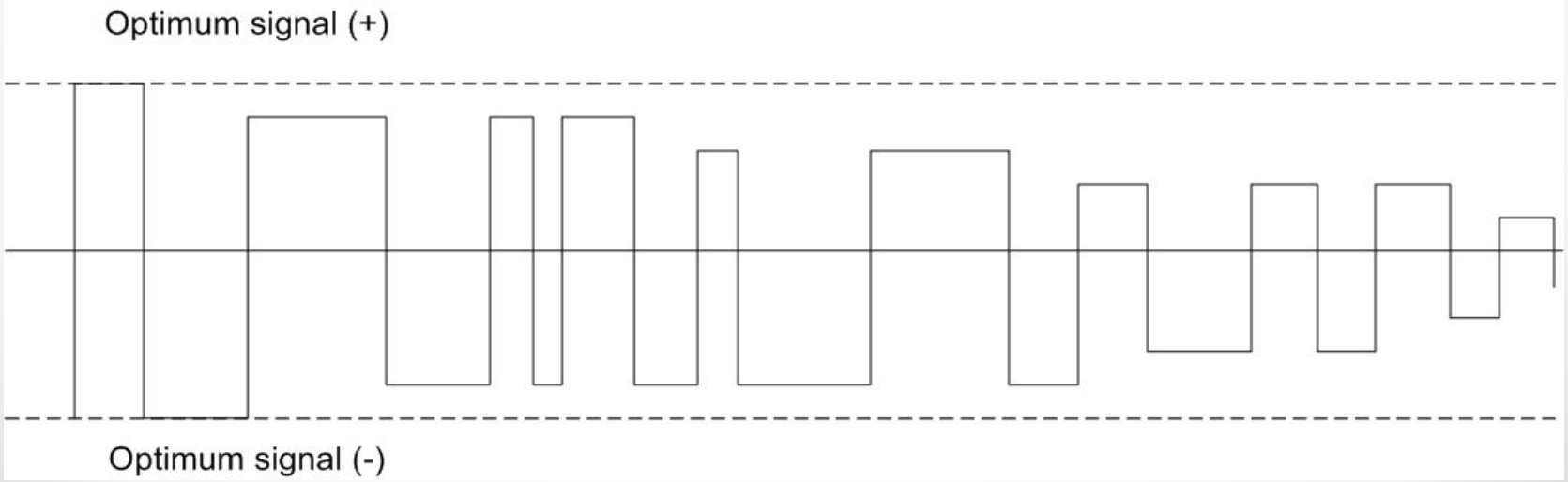
Coaxial Cable

The specifications of the cable required depend on whether you are supporting 10Base2 or 10Base5 Ethernet.

10Base2	• RG58 A/U cable. • Segment length maximum of 607 ft (about 185 m)
10Base5	• RG-11 cable. • Segment length maximum of 1640 ft (500 m)

Attenuation

Maximum cable lengths with any type of cable are due to physical characteristics of the cable and the signal it carries. A signal loses strength over distance, a process known as attenuation. After traveling a specific distance, the signal is no longer reliable. This is true of both wired and wireless transmissions.



BNC Connector

10Base2 had devices connecting directly to the cable in a branching or daisy-chain configuration. Connections were made using a BNC connector. Both types of cable had to be terminated at each end with a 50-ohm terminator to ensure signal quality.

There are several reasons why coaxial cable has fallen out of favor for network implementations. Compared to twisted pair cable, it is relatively difficult to work with, and coaxial cable is not flexible enough to bend at sharp angles. Coaxial-based configurations are also notoriously difficult to troubleshoot.

Twisted Pair Cable

Nearly all current network configurations use twisted pair cable. Most deployments use UTP cable, which is easier to use and less expensive than STP cable. STP cable is typically used only when environmental factors require it, such as EMI sources located near cable runs.

Twisted pair cable has several advantages over coaxial cable, which helped fuel its rapid adoption. Primary among these advantages were cost and ease of installation. It was simply less expensive to deploy a network using twisted pair rather than coaxial cable. In addition, most offices were already set up to support twisted pair cable runs for office phone systems.

Twisted Pair Specifications

Twisted pair cable standards are referred to as cable categories. There are several standards worldwide that define these categories.

Category	Transmission rates	Application
Cat 3	16 MHz	10BaseT
Cat 5/5e	100 MHz	Up to Gigabit Ethernet
Cat 6	250 MHz	Replacement for CAT 5E
Cat 6e	Up to 500 MHz	Up to 10 Gigabit Ethernet
Cat 7	600 MHz	10 Gigabit Ethernet

Cat 5e, Cat 6 and Cat 6e is available as either STP or UTP cable. Cat 7 cables are typically shielded and sometimes use nonstandard (not RJ-45) connectors. Maximum cable lengths are typically specified as 100 m (about 300 ft.).

Twisted Pair connections

In small installations, devices may connect directly to a central hub or switch. This is not practical in medium to large installations. Instead, connections are typically made at a distribution frame with multi-pair cables run to wall plates throughout the office. The final connection is made using a cable with an RJ-45 connector on each end.

Patch Panels

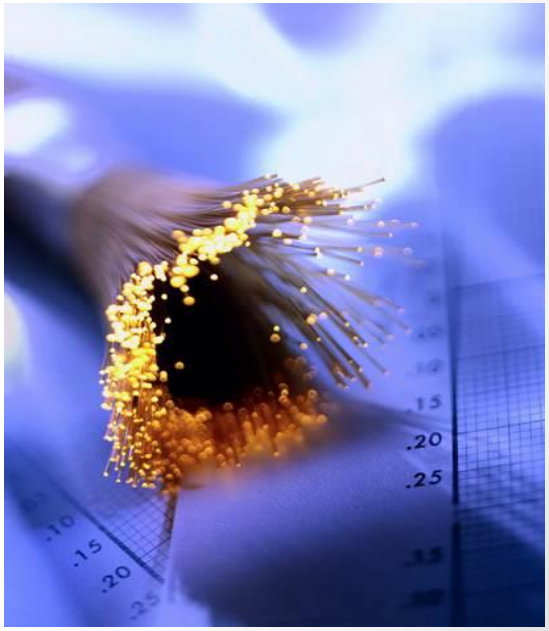
Older wiring closets sometimes have the same type of patch panels for both telephone and network support. These panels require punch-down blocks to make connections. Punch-down blocks are closely fit jaws that pierce individual wires to make a connection. They are somewhat difficult to use, and they also require specialized tools for connecting to the panel.

In most modern network installations, patch panels with modular connectors are used. Patch cables are run between the switch and the patch panel. From here, wiring is distributed throughout the premises.

Fiber Optic

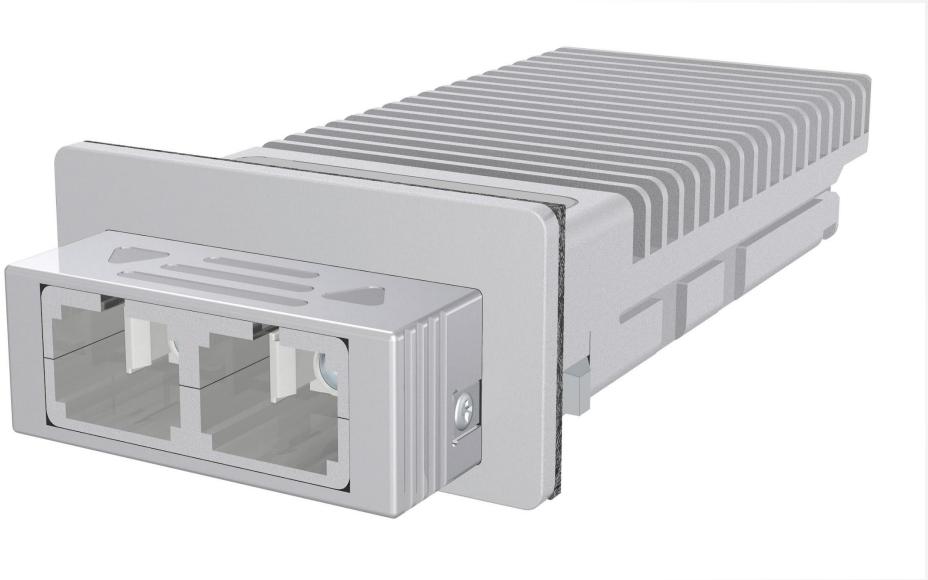
Fiber optic cable was initially seen as only justified for special applications, specifically when very long, very high speed connections were needed. It has found its way more and more into LAN configurations in situations where it is better suited than copper wire cable.

Advantages	• High speed • Long cable segments • Secure
Dis-advantages	• Fragile • Expensive • Difficult to install



Fiber Optic Connector

Computers that act as network servers may have built-in (or preinstalled) fiber optic adapters. The same is true of many top-end game machines.



Fiber optic connectors take different forms depending on the specific application supported. Most applications use two fibers, one to send and the other to receive. Devices that use fiber optic are connected in a daisy-chain configuration so that data passes through each device along the way toward its destination.

HP X130 10G SFP+ LC ER 40km Transceiver

Optical connections are commonly made using SFP (or SFP+) transceivers as the termination at the switch. There are transceiver types designed to support common multimode and single mode fiber standards.

Wired network topologies

Your network topology is somewhat dependent on your low-level communication protocol. Ethernet was originally designed to use a bus technology; whereas, Token Ring uses a ring topology. Before try to design or maintain a network, you need to understand network topologies and how they are used.

Our discussion focuses on four common network topologies:

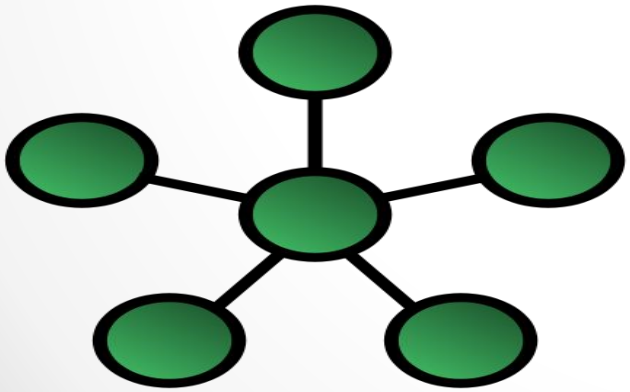
- Star
- Bus
- Ring
- Mesh

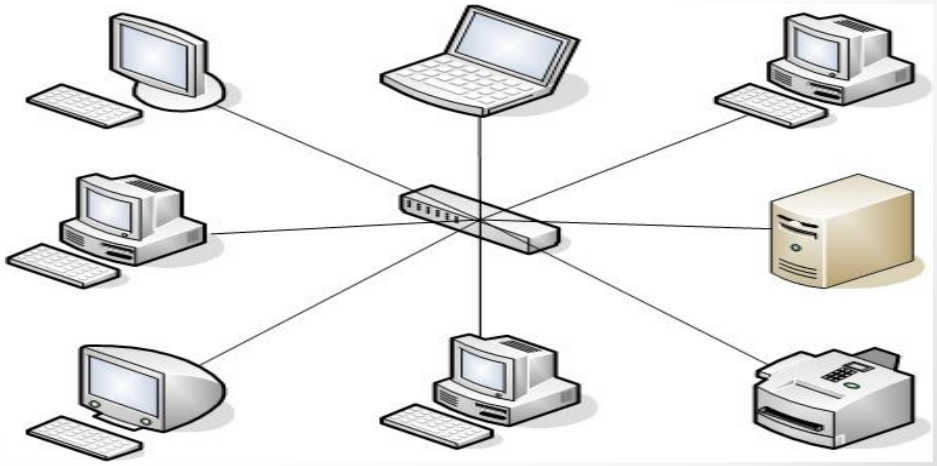
Star Topology

Star networks are one of the most common computer network topologies. In its simplest form, a star network consists of one central switch, hub or computer which acts as a router to transmit messages.

In a star topology, each node connects to a central hub or a switch through a point-to-point connection.

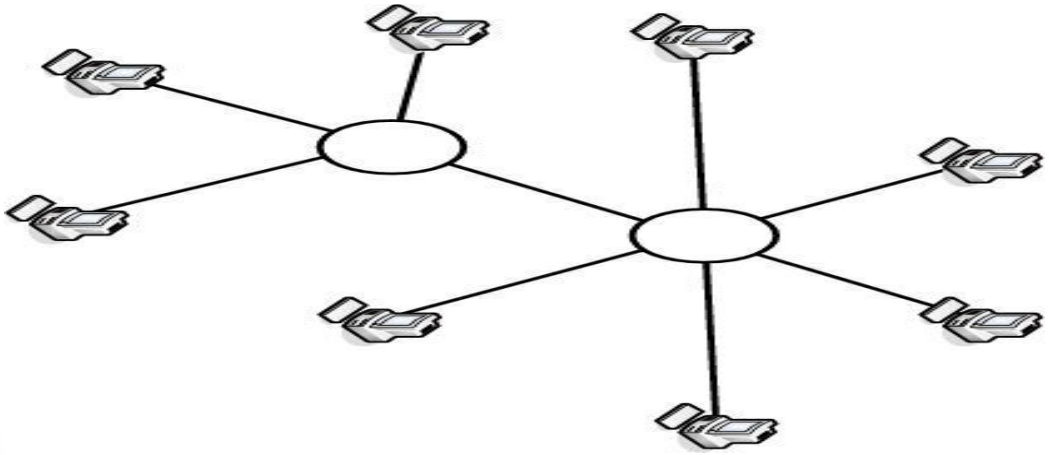
Data passes through the central hub to reach other devices on the network. Ethernet over unshielded twisted pair (UTP), whether it is 10BaseT, 100BaseT, or Gigabit, all use a star topology.





Distributed star

A common variation of the star topology is a distributed star. In a distributed star, you have hubs connected to each other to expand the network.



True star topology configurations are rarely seen in LAN implementations. However, the point-to-point connections made between hosts and switches look like a star topology. A star hub differs from an Ethernet switch or hub by how traffic is managed at the central connection.

Star Topology

Advantages of Star Topology.

- It is very easy to install and manage star network topology as it is the simplest of the lot when it comes to functionality.
- It is easy to troubleshoot this network type as all computers are dependent on the central hub which invariably means that any problem which leaves the network inoperable can be traced to the central hub.
- In star topology, the data packets don't have to make their way through various nodes which makes sure that the data transfer is fast.
- As the nodes are not connected to each other, any problem in one node doesn't hamper the performance of other nodes in the network.
- Adding new machines or replacing the old ones is a lot easy in this network topology, as disruption of the entire network is not required to facilitate the same.

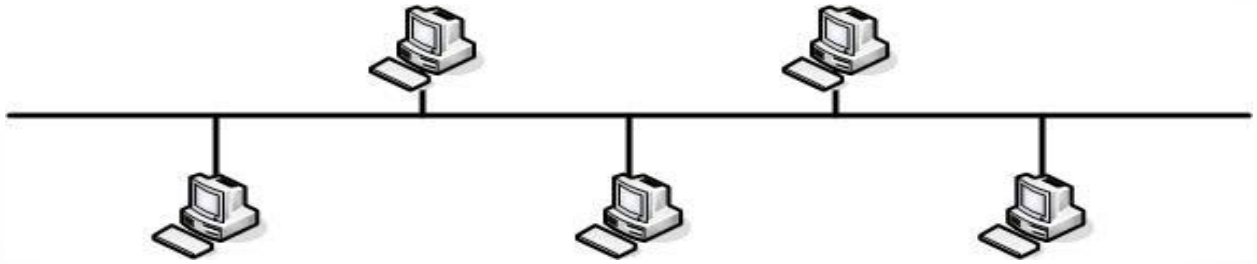
Star Topology

Disadvantages of Star Topology.

- The foremost problem with star network topology is the fact that it is highly dependent on the functioning of central hub.
- The size of the network is dependent on how many connections can be made to the hub.
- This network type requires more cable as compared to linear bus topology which means the expenses incurred would be relatively high.
- The performance of the entire network is directly dependent on the performance of the hub. If the server is slow, it will cause the entire network to slow down.
- If one of the numerous nodes utilizes a significant portion of the central hub's processing capability, it will reflect on the performance of other nodes.

Bus Topology

Ethernet was developed around a logical bus topology. All network nodes connect directly to the network cable. In theory, every node has equal, shared access to the cable segment. Because of the shared access, a bottleneck can develop and slow transmission when two nodes try to transmit at the same time.

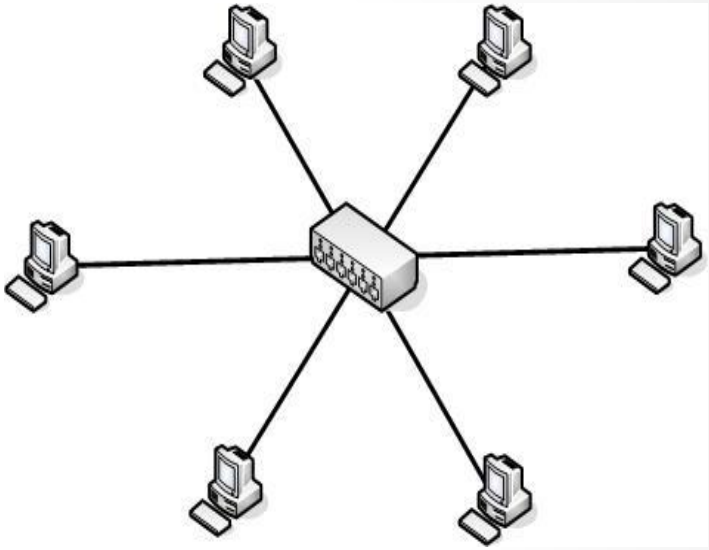


In a bus topology, all nodes receive every transmission at effectively the same time. If a transmission is not addressed to a specific node (or addressed as a broadcast), the node will ignore the transmission. This type of bus topology is sometimes called a linear bus.

Bus Topology

When wired using a hub (or switch), an Ethernet segment looks like a physical star.

A hub is internally wired as a bus connection at the central point. The hub acts as a central connection point, as if the nodes were tied together as one cable segment.



When a switch is used, it compensates for one of the weaknesses of the bus topology. The switch adds traffic control by buffering transmissions at the port, thereby avoiding most collisions. The switch ports can be configured so that they act as a single cable segment for addressing purposes.

Bus Topology

Advantages of Bus Topology.

- It is easy to set-up and extend bus network.
- Cable length required for this topology is the least compared to other networks.
- Bus topology costs very less.
- Linear Bus network is mostly used in small networks. Good for LAN.

Bus Topology

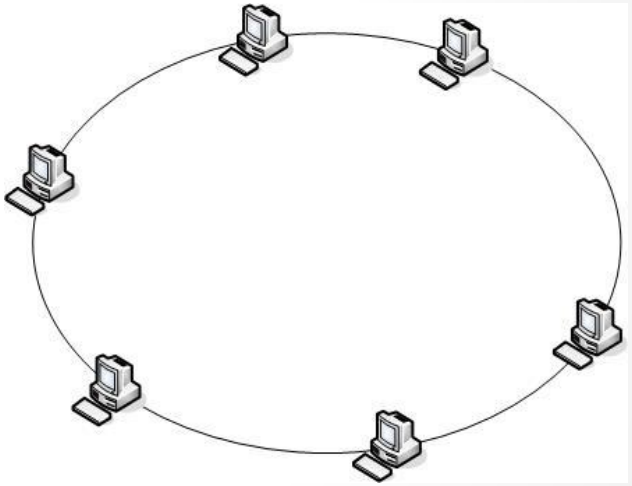
Disadvantages of Bus Topology.

- There is a limit on central cable length and number of nodes that can be connected.
- Dependency on central cable in this topology has its disadvantages. If the main cable (i.e. bus) encounters some problem, whole network breaks down.
- It is difficult to detect and troubleshoot fault at individual station.
- Efficiency of Bus network reduces, as the number of devices connected to it increases.
- It is not suitable for networks with heavy traffic.
- Security is very low because all the computers receive the sent signal from the source.

Ring Topology

In a ring topology, the output of one node is the input of the next node in a true daisy-chain configuration. Each node acts as a repeater, boosting the signal when transmitting to the next node.

A data packet, known as a token, is passed from node to node around the network. A node can load the token with data, which is passed around until it reaches its destination. At that point, the data is unloaded from the token and the empty token is passed to the next node.



Some ring topologies use a double ring, that is, two rings that send signals in opposite directions. This enables the ring to compensate for a break or a failing node until the problem can be repaired.

Ring Topology

Advantages of Ring Topology.

- This type of network topology is very organized. Each node gets to send the data when it receives an empty token. This helps to reduces chances of collision.
- In ring topology all the traffic flows in only one direction at very high speed.
- Even when the load on the network increases, its performance is better than that of Bus topology.
- There is no need for network server to control the connectivity between workstations.
- Additional components do not affect the performance of network.
- Each computer has equal access to resources.

Ring Topology

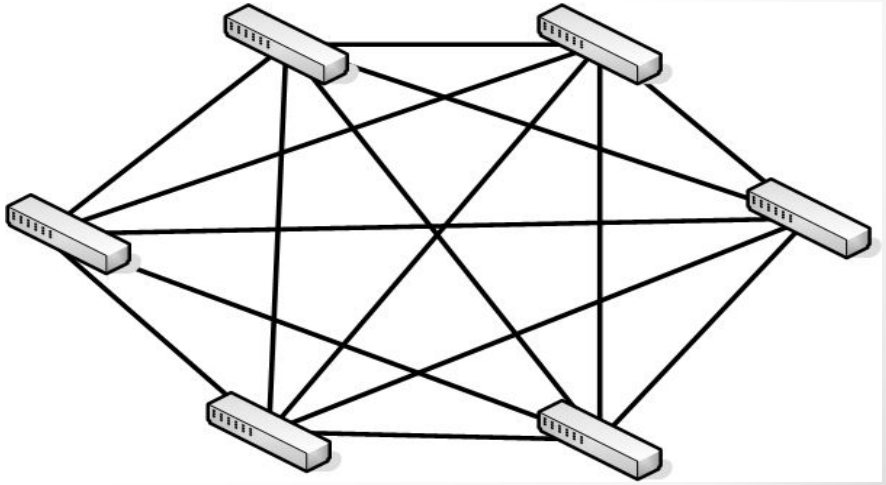
Disadvantages of Ring Topology.

- Each packet of data must pass through all the computers between source and destination. This makes it slower than Star topology.
- If one workstation or port goes down, the entire network gets affected.
- Network is highly dependent on the wire which connects different components.
- MAU's and network cards are expensive as compared to Ethernet cards and hubs.

Mesh Topology

In a full mesh, each node in the network is connected to every other node. There is no central node in this configuration. This provides multiple communication paths for data transmissions. This also requires a protocol that manages the routes taken by data to avoid loops. Traffic through these loops can result in network communication failure due to a broadcast storm.

One of the greatest strengths of this topology is that it can compensate for failures. The multiple connections make it possible to route data around failing nodes or breaks in the connecting cable plant.

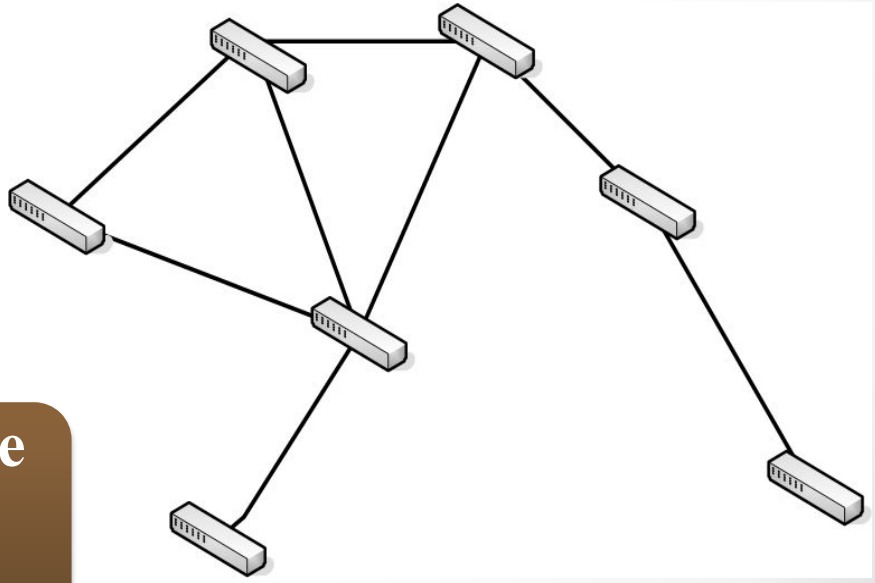


Partial Mesh

The best known example of a mesh network is the Internet with its innumerable connections. In many cases, these are a more limited mesh, or partial mesh, rather than a fully connected mesh.

Partial mesh.

- **Mesh topology where some nodes are not connected to every other node.**



Even in a partial mesh, there is still the possibility of creating an endless loop.

Mesh Topology

Advantages of Mesh Topology

- **Data can be transmitted from different devices simultaneously. This topology can withstand high traffic.**
- **Even if one of the components fails there is always an alternative present. So data transfer doesn't get affected.**
- **Expansion and modification in topology can be done without disrupting other nodes.**

Mesh Topology

Disadvantages of Mesh Topology

- There are high chances of redundancy in many of the network connections.
- Overall cost of this network is way too high as compared to other network topologies.
- Set-up and maintenance of this topology is very difficult. Even administration of the network is tough.

Wired network security overview

You should protect the physical network to prevent unauthorized persons from tapping into the network cable plant. Exposed cable should be kept to a minimum.

If your facility has a wiring closet, you should keep it secured at all times.

You should also take a periodic physical inventory of the network to make sure that there have not been any unauthorized (and possibly compromising) changes.

Wi-Fi Hotspots

Wireless computer networks have now become commonplace. They are popular in many office environments, especially because of their flexibility and relative ease of management. You even find public Wi-Fi networks in places where people congregate, such as libraries, colleges, and restaurants.

Some cities are even deploying city-wide Wi-Fi to provide all citizens with free Internet access. New Wi-Fi technologies and updated network devices are rolled out on a regular basis, continually expanding the capabilities of wireless networks.

Wireless Networks

Modern wireless devices are designed to support 802.11n, but are able to also support devices that have 802.11a/b/g wireless adapters. That way, you can continue to use older wireless devices without having to upgrade them.

There are several potential benefits available through wireless networking, including:

Ease of deployment	• **Equipment requirements are minimal, and there is typically no need to run cable.**
Support for mobile users	• **Mobile users intermittently can easily connect to the office network.**
Interconnection with wired network	• **You have the option of connecting your wireless network clients**

Wireless network configurations

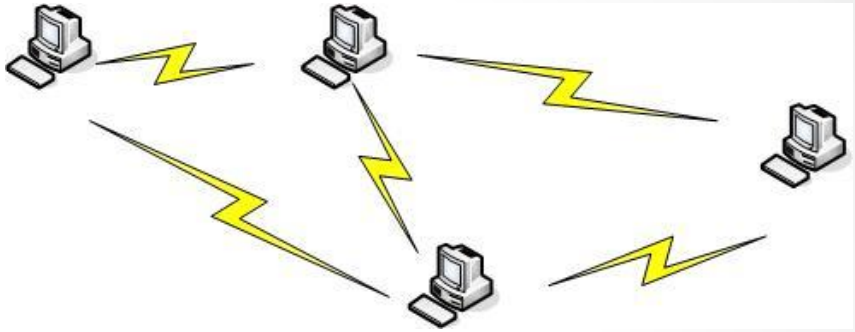
There are two basic configuration options supported for wireless networks:

- **Ad-hoc mode**
- **Infrastructure mode**

The mode you select will depend on your networking requirements. The operational mode is configured through the wireless adapter properties.

Ad Hoc Mode

Ad-hoc mode, also known as point-to-point mode, is the easiest configuration to implement, but is inappropriate for most SMB environments.



In ad-hoc mode, you configure wireless devices to communicate directly with each other. This enables the devices to share files and other resources with each other, but not with any wired network devices.

An ad-hoc network is limited to no more than nine client devices. Two devices must be within range of each other to share resources. There is no organized method for bridging or relaying data between devices.

Ad Hoc Mode

Ad hoc networks also work well as a temporary fallback mechanism if normally-available infrastructure mode gear (access points or routers) stop functioning.

To set up an ad-hoc wireless network, each wireless adapter must be configured for ad-hoc mode versus the alternative infrastructure mode.

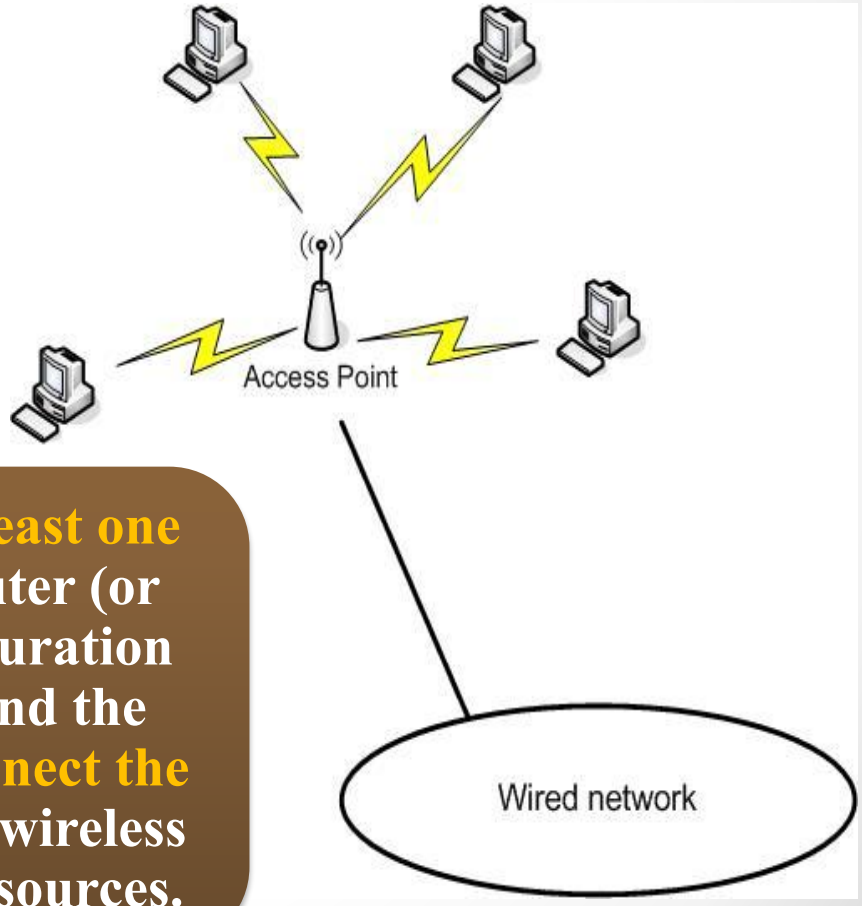
In addition, all wireless adapters on the ad-hoc network must use the same SSID (Service Set Identifier) and the same channel number.

Ad-hoc networks cannot bridge to wired LANs or to the Internet without installing a special-purpose gateway.

Ad hoc networks make sense when needing to build a small, all-wireless LAN quickly and spend the minimum amount of money on equipment.

Infrastructure Mode

The default configuration for most wireless adapters is to support infrastructure mode only. In infrastructure mode, wireless devices communicate through an access point, rather than communicating with each other directly.



Infrastructure mode requires at least one access point (AP) and one computer (or other wireless device). The configuration can include multiple APs to extend the network's range. You can also connect the AP to your wired network to give wireless clients access to wired network resources.

Access point (AP)

Central connection point for wireless networking. An accesses point provides connection between wireless devices and can support connection through to a wired network.

Wireless security overview

A common problem with wireless networking is that you might be providing an unintended hotspot to strangers. One way that unprotected or poorly protected wireless networks are discovered is through wardriving.

Wardriving

- **The process of driving through an area with a portable computer or signal detector to locate wireless network signals.**

If your network is discovered through wardriving, you might become a victim of warchalking. If you are, you will find this symbol written in chalk on the sidewalk outside your offices:

Warchalking

- **The marking of accessible wireless networks with chalk.**

Wireless security overview

The 802.11 and 802.1X standards define several security options to help you protect your network. Implementing these standards does not necessarily guarantee that your network will remain safe, but it will go a long way toward protecting it. This does not prevent warchalking. It does, however, change your network's status from unprotected Wi-Fi to protected Wi-Fi.

Wireless Security Overview

Potential problems

- Unintended hotspot
- Unrestricted access
- Unauthorized use of your network and Internet connection
- Data loss or corruption

Security options

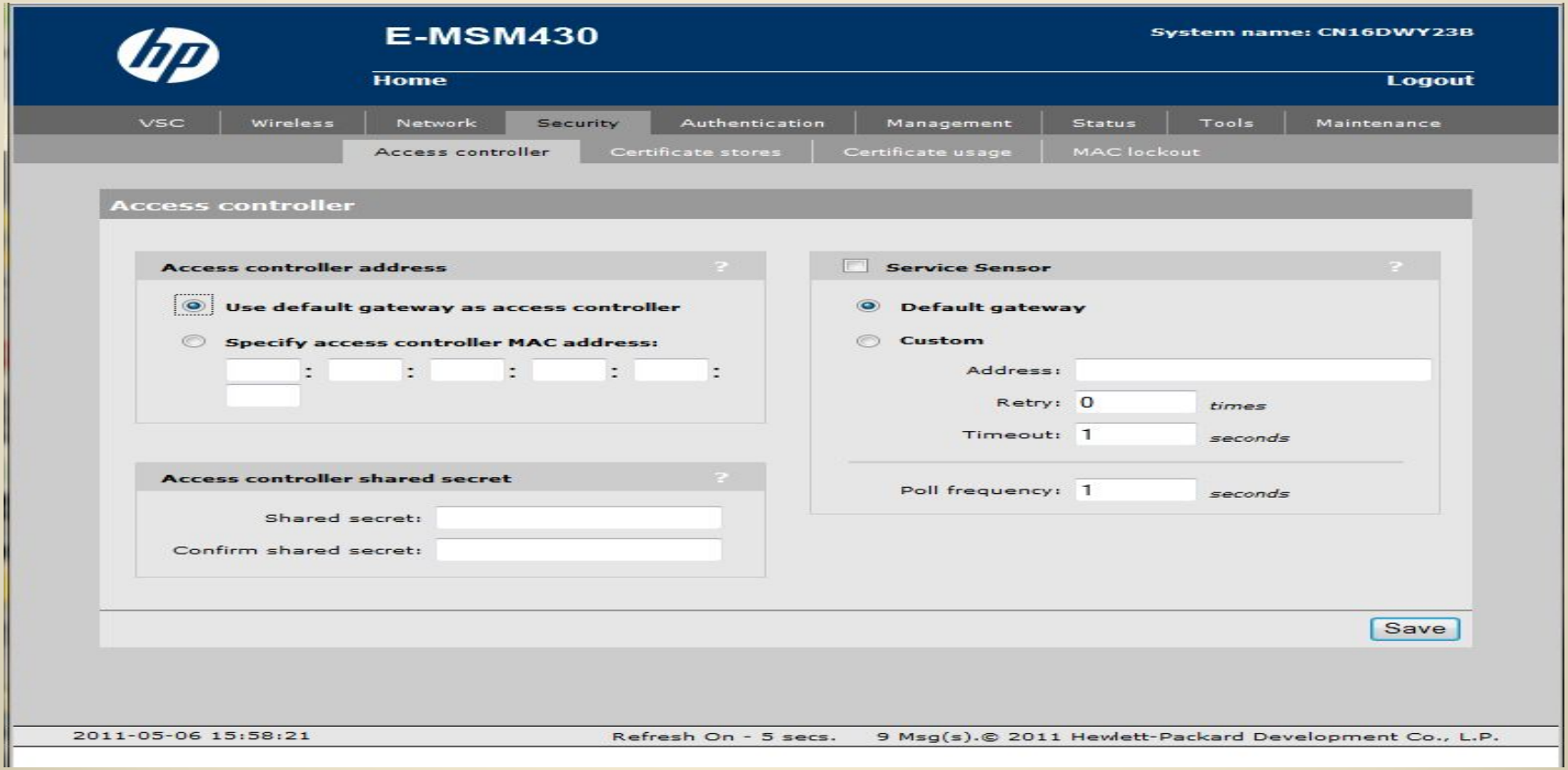
- MAC address filtering
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2)

Wireless Security - MAC address filtering

MAC address filters are often used as an added wireless security measure next to data encryption. A MAC address (or hardware address or physical address) is a unique code that is assigned to almost all-networking hardware such as Ethernet cards, routers, mobile phones, wireless cards and so on. You can use the MAC address to either allow or block a wireless network card that tries to connect to the wireless network.

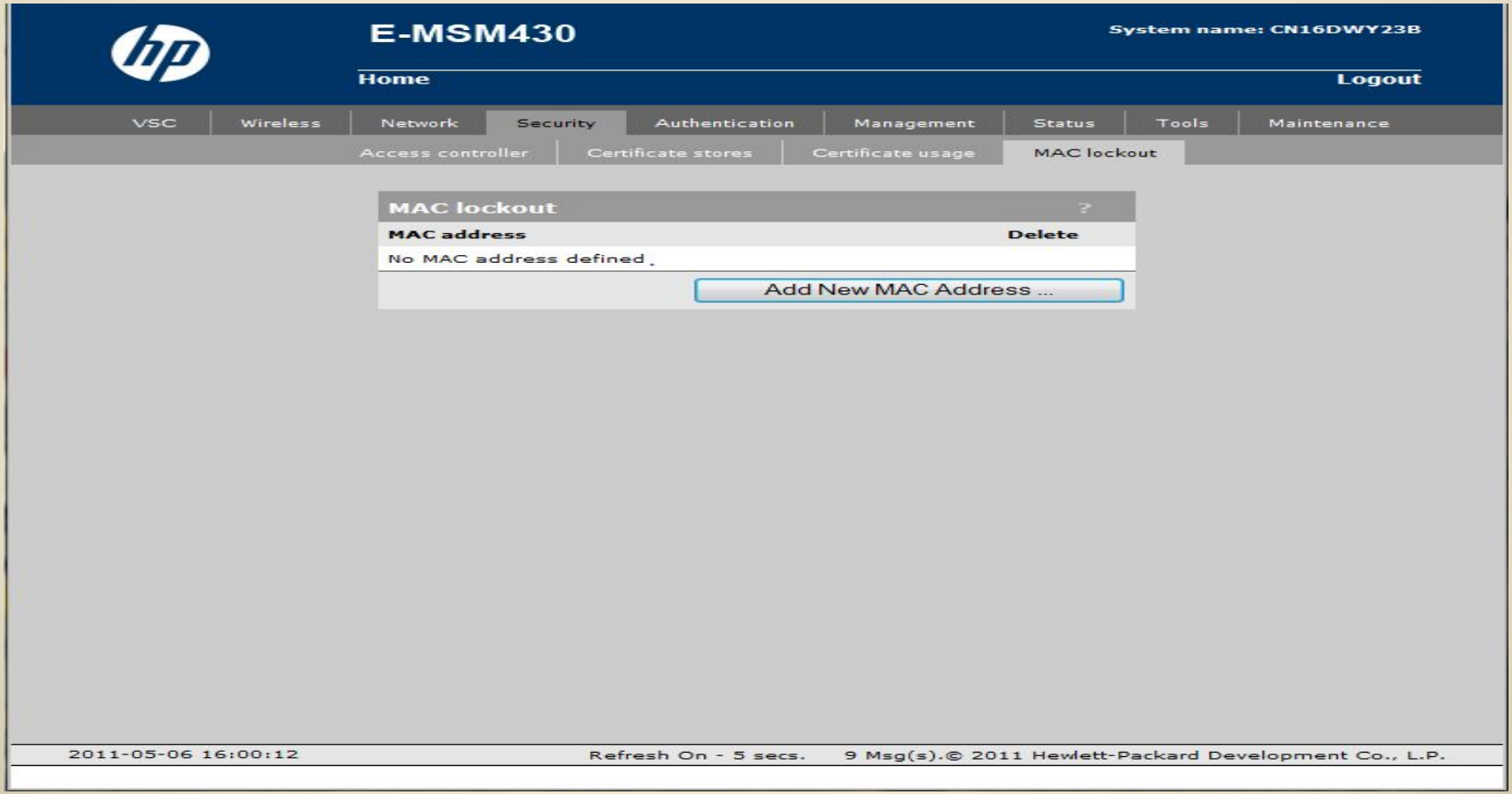
Security. Access Controller Screen

If you want to specify a different computer as controlling access, you must identify it by its MAC address.



Security. MAC Lockout

MAC lockout lets you identify devices that are specifically blocked from connecting to the AP



Wireless Security - WEP

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks.

Two methods of authentication can be used with WEP:

- **Open System authentication**
- **Shared Key authentication.**

In Open System authentication, the WLAN client need not provide its credentials to the Access Point during authentication. Any client can authenticate with the Access Point and then attempt to associate. In effect, no authentication occurs.

WEP. Shared Key authentication

In Shared Key authentication, the WEP key is used for authentication in a four step challenge-response handshake:

- The client sends an authentication request to the Access Point;
- The Access Point replies with a clear-text challenge;
- The client encrypts the challenge-text using the configured WEP key, and sends it back in another authentication request;
- The Access Point decrypts the response. If this matches the challenge-text the Access Point sends back a positive reply.

Wireless Security - WPA

Wi-Fi Protected Access (WPA) is a security protocols and security certification programs developed to secure wireless computer networks. WPA improves on the authentication and encryption features of WEP (Wired Equivalent Privacy).

WPA provides stronger encryption than WEP through use of either of two standard technologies:

- **Temporal Key Integrity Protocol (TKIP)**
- **Advanced Encryption Standard (AES).**

Temporal Key Integrity Protocol (TKIP)

Like WEP, TKIP uses the RC4 stream encryption algorithm as its basis. The new protocol, however, encrypts each data packet with a unique encryption key, and the keys are much stronger than those of its predecessor. To increase key strength, TKIP includes four additional algorithms:

- **A cryptographic message integrity check to protect packets.**
- **An initialization-vector sequencing mechanism that includes hashing, as opposed to WEP's plain text transmission.**
- **A per-packet key-mixing function to increase cryptographic strength.**
- **A re-keying mechanism to provide key generation every 10,000 packets.**

Advanced Encryption Standard (AES)

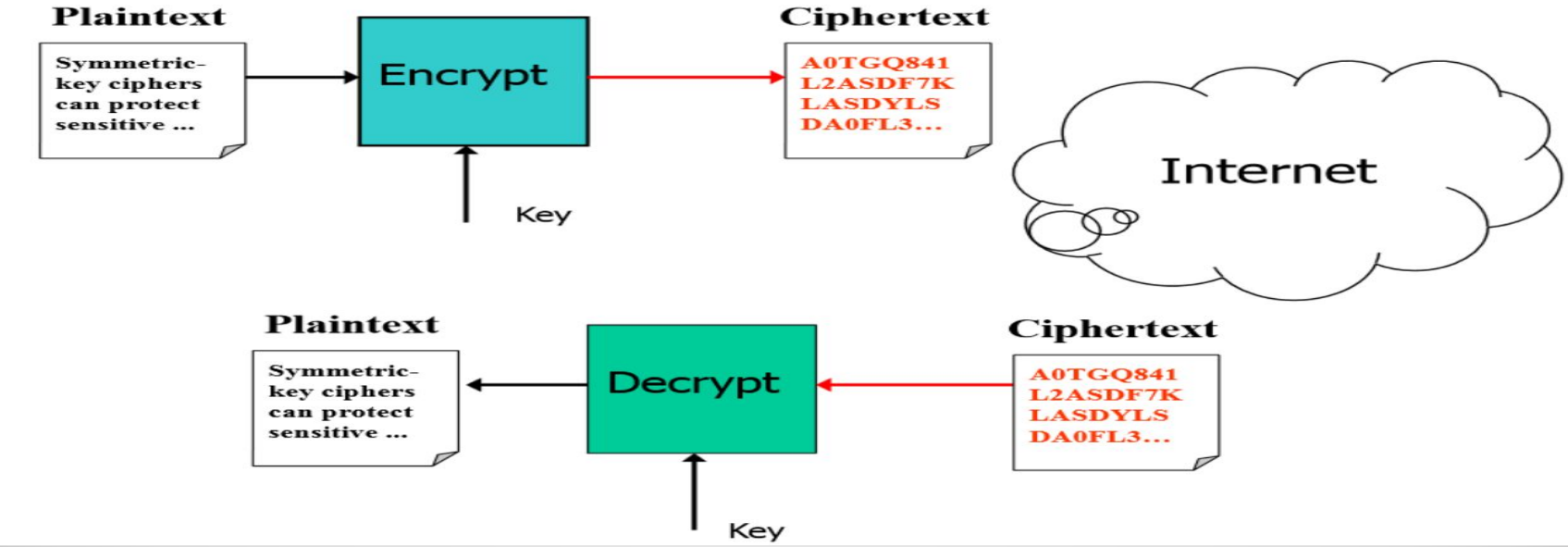
While TKIP is useful for upgrading security on devices originally equipped with WEP, it does not address all of the security issues facing WLANs and may not be reliable or efficient enough for sensitive corporate and government data transmission. The 802.11i standard specifies the Advanced Encryption Standard (AES) in addition to TKIP.

AES offers a higher level of security and is approved for government use, but requires a hardware upgrade for implementation. As organizations replace older wireless equipment, AES is expected to become the accepted encryption standard for WLAN security.

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.



Wireless Security - WPA

WPA also includes built-in authentication support that WEP does not offer. Overall, WPA provides comparable security to VPN tunneling with WEP, with the benefit of easier administration and use.

A variation of WPA designed for use on home networks is called WPA Pre Shared Key or WPA-PSK for short. WPA-PSK is a simplified but still powerful form of WPA.

Wireless Security – WPA2

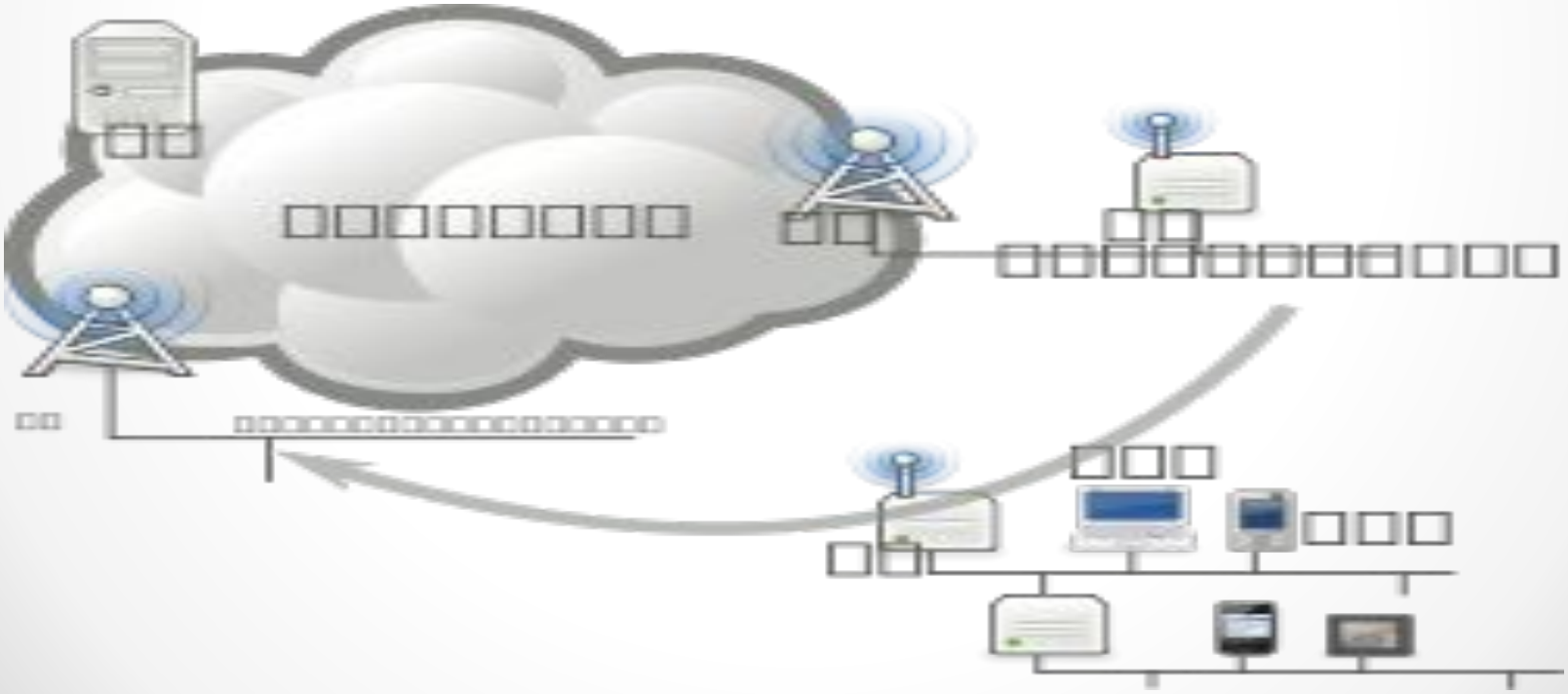
Wi-Fi Protected Access 2, the follow on security method to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks.

Based on the IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1x-based authentication.

There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA.

Hybrid Network

Many networks are best described as hybrid networks, bringing together different topologies and even different communication technologies, such as combining wired and wireless networking in one location, into an integrated whole. This becomes more common as networks become larger and more interconnected.



Key Network Technologies

We end this chapter with a brief discussion of some technologies and concepts that are central to understanding modern network infrastructures. The discussion is designed to serve only as an overview of the subject. These topics will be covered in much greater detail at later times throughout this course.

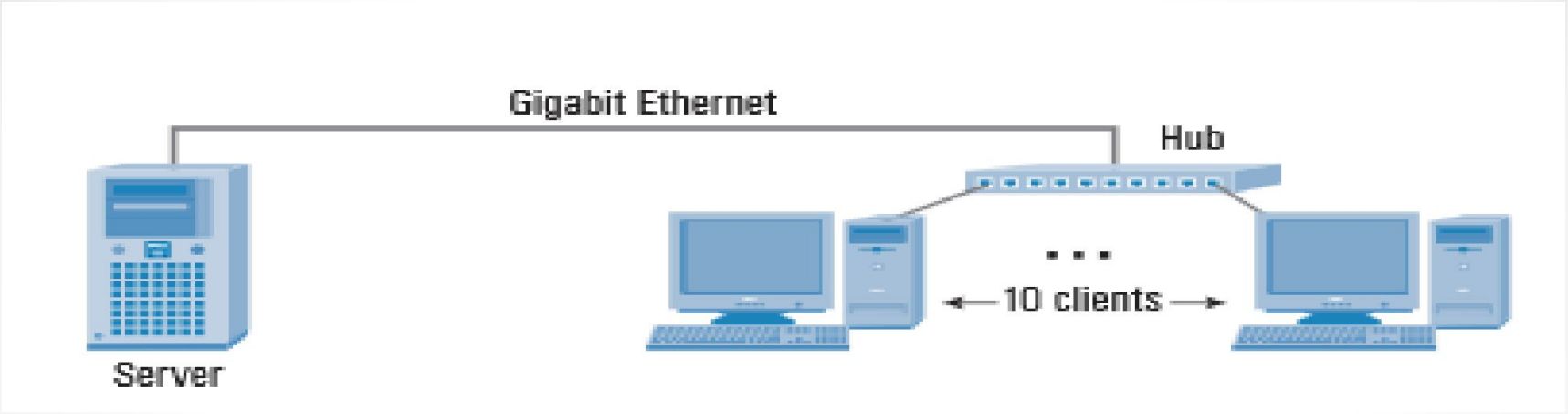
Network Segmentation

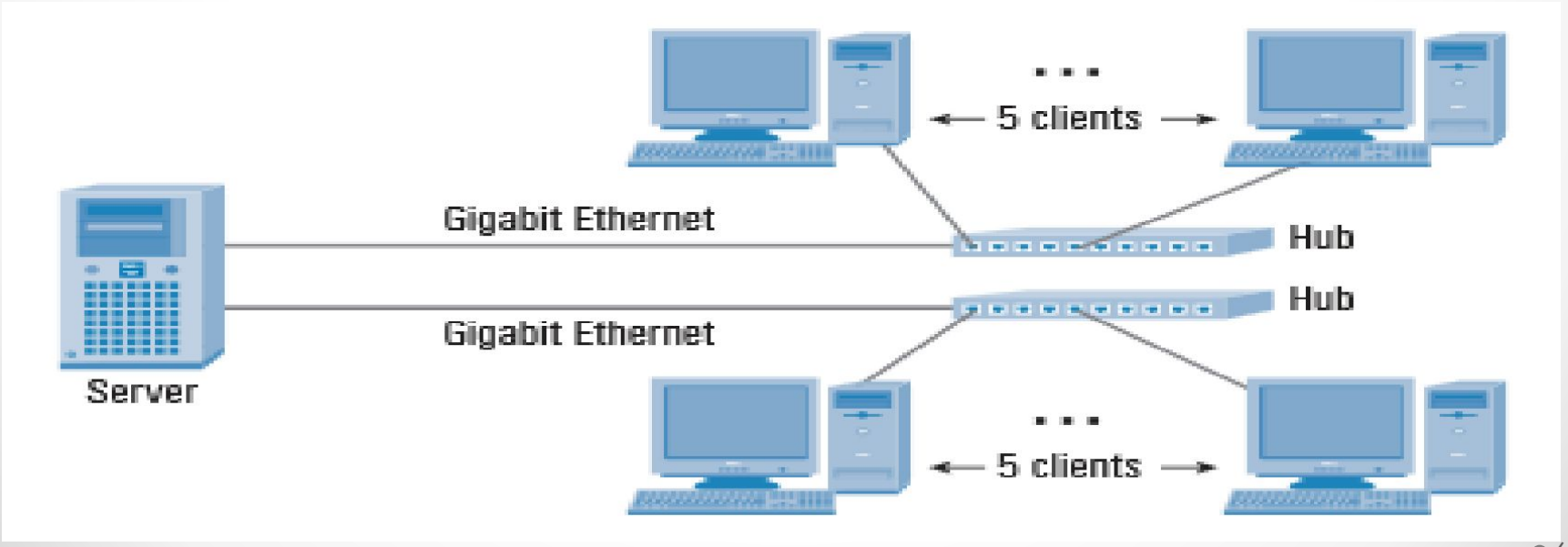
Network segmentation in computer networking is the act of splitting a computer network into subnetworks, each being a network segment or network layer.

There are several reasons why you might consider segmenting a network, including:

- **Optimizing network communication**
- **Improving the management of network traffic flows**
- **Enhancing network security management**

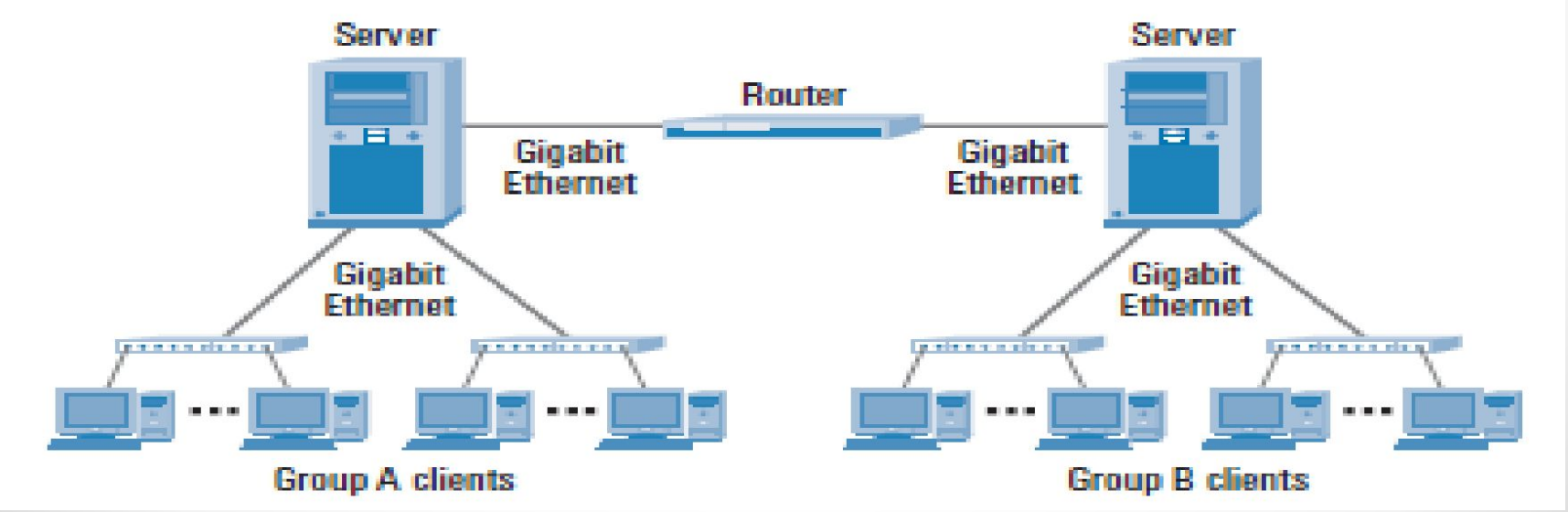
Network Segmentation





Network Segmentation

In this example, segmentation accommodates the needs of two diverse work groups. Both servers have reduced overhead and traffic because accounting rarely accesses the engineering side and vice versa. However, each side can still access the other's server for e-mail, budget reports, and other cross-enterprise activities.



Network Segmentation

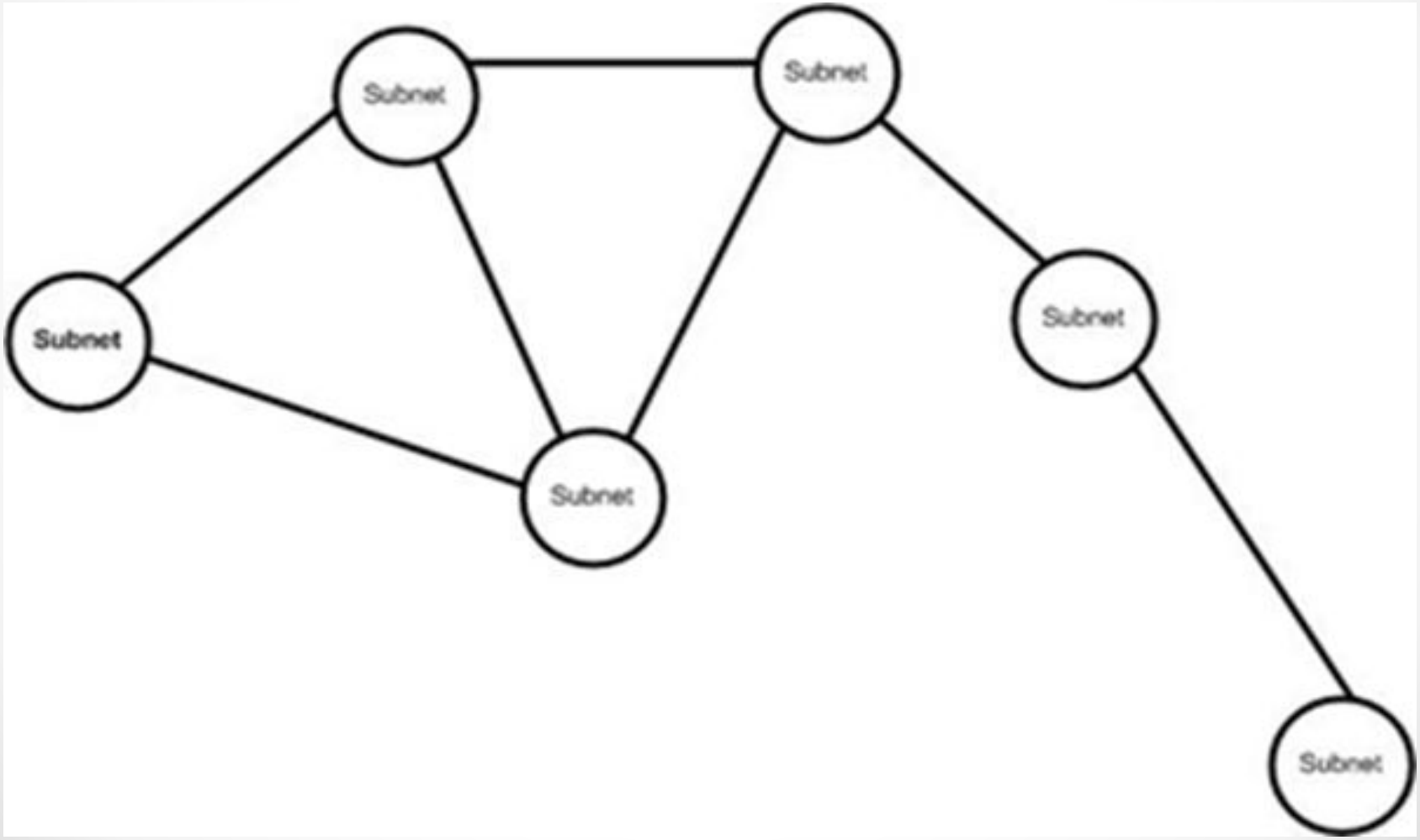
There are two primary methods used for segmenting a network:

subnetworks (subnets) and VLANs.

One of the most significant differences between the two is that subnets are implemented at Layer 3 of the OSI model, but VLANs are implemented at Layer 2.

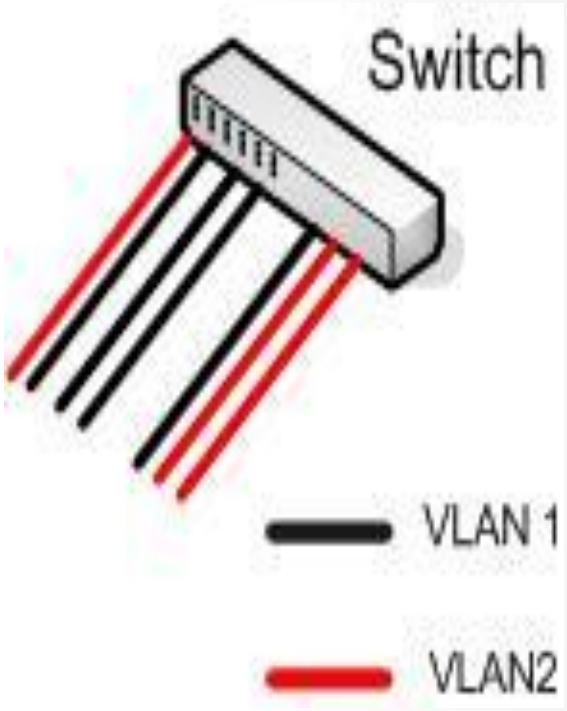
Routers or routing switches are required when using subnets to segment a network. Each subnet must have a different network address.

Multiple Subnets



Network Segmentation

With VLANs, switches are used to segment the network, and segmentation is usually by port. A VLAN can be made up of ports assigned from a single switch or made up of ports gathered from multiple switches. Each VLAN will have a different ID number and a different assigned IP address. A VLAN can be associated with multiple subnets.



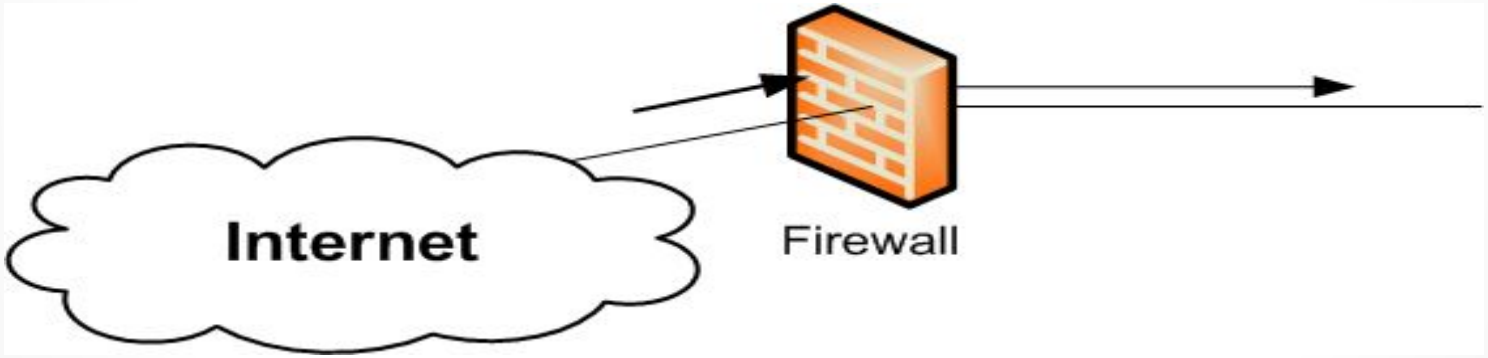
VLANs have become a popular segmentation option for LANs. Routers are still the primary means of segmenting over a wider area and between wide area links.

Network Segmentation

Network segmentation is the physical division of network into separate parts. A network segment can contain just one machine or many machines. Each network segment can have it's own hub or switch. In most cases a contiguous range of IP addresses will be assigned to each segment. Using a FireRack **firewall**, each segment can be protected from the other segments using it's own set of firewall rules. Any data moving between segments must pass through the **firewall**.

Firewall

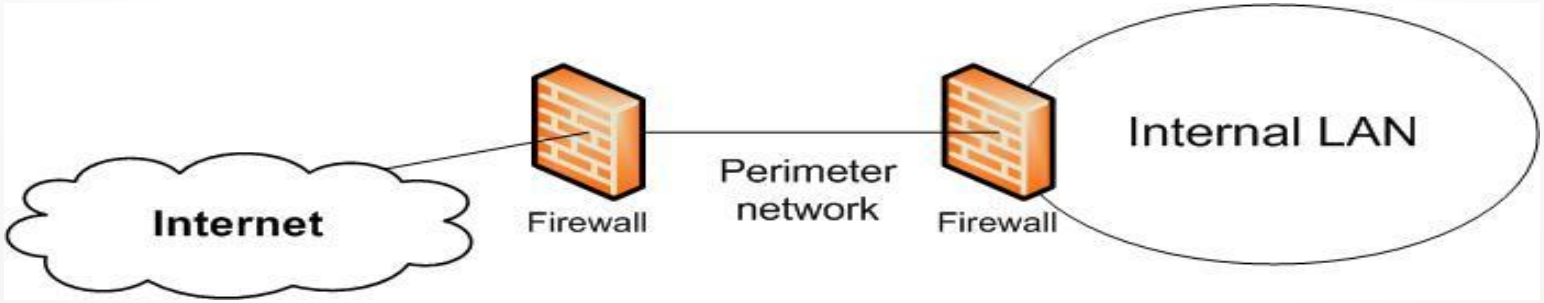
A firewall is a security device that can filter the traffic into or out of the perimeter network. A firewall can be a separate, specialized device or, most commonly, be implemented through functionality provided in a router.



That way you can limit traffic to certain types of communication, block access of potentially hazardous applications, and even place restrictions on source and destination address information.

Perimeter Network

One specialized type of segmentation is a perimeter network. A perimeter network is a screened subnet that sits between the internal LAN and the outside world, specifically the Internet. The term DMZ is sometimes used to refer to a perimeter network. The perimeter network acts as a buffer to protect your network. It is designed to help prevent unauthorized access into your network, as well as targeted attacks against it.

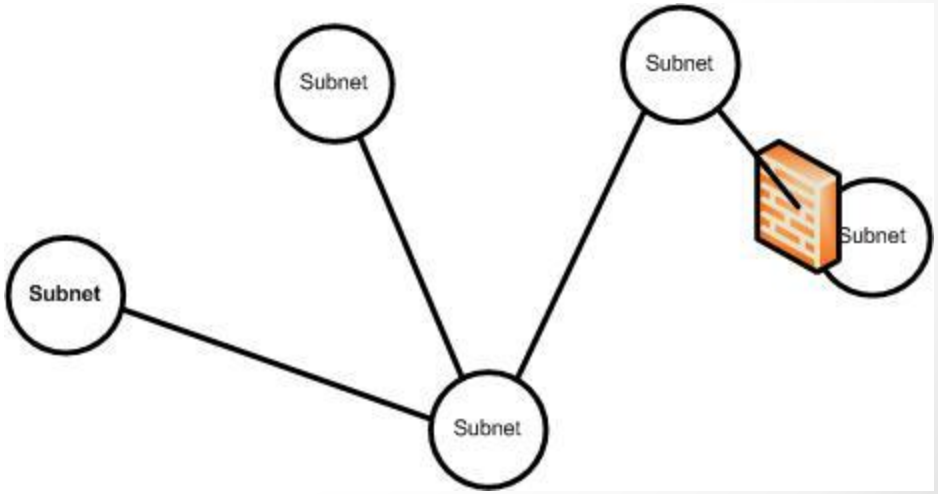


The primary purpose of a perimeter network is that it gives you a place to deploy devices that you want to share with the world at large.

Screened Subnet

You might see an internal network variation on the perimeter network, referred to simply as a screened subnet. In this case, the subnet is part of your internal network, but the boundary into the subnet is protected by a Firewall.

One reason for configuring your network this way is to provide additional security for the computers deployed on the screened subnet.



Address translation

Address translation is another important technology for when devices on an internal network need to access the outside world. Therefore, you should always hide the IP addresses of your LAN computers. You should also often use private IP addresses to configure internal hosts. When you use private IP addresses, you must use address translation when accessing the Internet.

Private IP addresses.

- **IP address ranges that can be assigned as internal LAN addresses, but cannot be used for communication on the Internet.**

You can hide the IP addresses of LAN computers and use private addresses on your network by using a Network Address Translation (NAT) server or Network and Port Address Translation (NAPT or PAT) server. A NAT server substitutes a valid Internet address for a host's actual address.

Proxy Server

One type of specialized server you might find in a perimeter network is a proxy server, which one manages Internet access .

Clients can access a proxy server by going through the following steps:

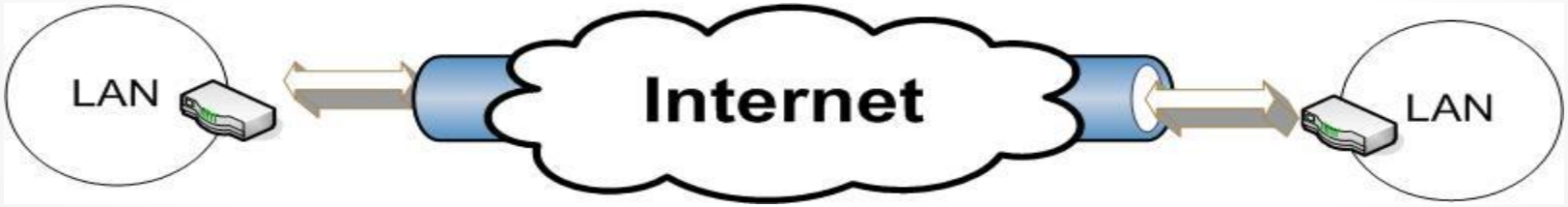
- **The client makes a request to the proxy server.**
- **The proxy server queries the Internet resource and retrieves the result.**
- **The proxy server passes the result to the requesting client.**

The use of a proxy server helps to improve network security. It also adds a layer of administrative control, letting you restrict users' access to Web sites you do not want them browsing.

Proxy servers also help reduce the amount of traffic between your network and the Internet. As information is retrieved from the Internet, it is buffered on the proxy server.

Virtual Private Network (VPN)

A VPN is designed to provide a secure, reliable communication path over a less secure communication media. The most common use of a VPN is to provide secure communication between two remote sites, using the Internet as your carrier. With a VPN, a communication session is established between two endpoints. The two most common scenarios are LAN-to-LAN communication and computer-to-LAN communication.



At each end, a device, typically a router, is configured as the VPN endpoint. Communication is typically encrypted between the two endpoints only. VPNs rely on the use of tunneling protocols to carry data between the endpoints. The endpoints must be able to mutually authenticate each other when a communication session is established to ensure security.

Summary

- Justifications for wired networks.
- Wired network standards.
- Wired network cable options and twisted pair cable categories.
- The purpose and use of patch panels.
- Wired network topologies.
- Wireless network justifications.
- Wireless network configurations.
- Ad-hoc and infrastructure modes.
- The use of hybrid networks.
- Reasons for network segmentation.
- Use of perimeter networks.
- Justification for proxy and address translation (NAT, PAT, and NAPT) servers.
- VPN fundamentals.