6.1.1 Networking

**Networking**0:00-0:07

In this lesson, we're going to introduce you to the concept of a network.

**Computers and Devices**0:08-0:19

A network is a group of interconnected computers and other devices that are able to share information with each other. In order for any network to function, there are several key components that have to be in place.

**Nodes/Hosts**0:20-0:36

First, the network should have computers and devices that need to communicate with each other. These devices will often be referred to as network nodes or hosts. If you hear the term node or host, we're talking about the same thing. We're talking about the computers on the network.

**Connecting Media**0:37-0:56

In order to communicate, these computers and other devices must be connected together in some way. This is done using connecting media. You can use twisted pair cabling. You can use fiber optic cables. You can even use WiFi radio signals as a type of connecting media to connect all these different devices together.

**Network Interface**0:57-1:36

Each computer and device in the network also has to have a network interface. A network interface has a very special job. It converts the digital data that's coming from the computer into some type of signal that can be transmitted on the network medium. It sends that signal through the connecting medium.

The network interface may use an electrical signal. It could use a light signal. It could even use a radio signal to send that data on the medium. These signals are received by the other network interfaces on the network and are converted back into the digital data that the computers and other devices can process.

**Network Protocols**1:37-1:55

A network also needs standards in order to define how that data is going to be formatted. We call these standards network protocols. The important thing to remember is that if the computers on the network aren't using the same network protocol, then they're not going to be able to understand the data that's being communicated.

**Network Benefits**1:56-2:16

Networks are expensive to set up and expensive to maintain. You might ask why a company go to all the expense to set one up. The key thing to remember is that usually networks save an organization money in the long run. For example, networks allow users to share peripherals.

**Printer Sharing**2:17-2:56

Suppose you have a typical office with several employees and each employee has their own computer. Every day these users need to print documents. They need to print time sheets. They need to print expense reports. They need to print customer orders, and so on. Without a network, each individual user's workstation would need to have its own printer. If you think about it, how much time each day would that printer be used? Very little, right? You would have excess capacity that was expensive. With a network, you can implement only a few shared printers on the network. A shared printer is connected to the network and can be used by many different users.

**Storage Consolidation**2:57-3:39

Networks can also consolidate storage. Instead of requiring employees to store data on their local workstations, they can save data in a central location on a file server. They could even save data on a network-attached storage device.

This is very important because it reduces the amount of storage required on each workstation. It also makes life easier for the network administrator because it allows everyone to store sensitive company information in one location on a server. That makes it much easier to protect. Instead of having to back up everybody's workstation every night to protect that data, all you have to do is back up the shared storage on the server.

**Other Network Benefits**3:40-4:42

Networks also make work group collaboration easier. By consolidating storage, users are able to share files with each other. You can also implement email, instant messaging, or even social media to allow users working on a project to collaborate with each other. You can also implement workflow management applications. By doing this, you can track projects and organize them in a much more efficient manner.

You can even replace our traditional telephone service with a network. You can use Voice over IP (VoIP) to reduce telephone expenses. You can enhance external communications with partners or with customers. For example, an organization can more efficiently communicate with its clients or partners by setting up a website or utilizing social media. As an example, an organization's customers can order a new product or get replacement parts for a product they've already purchased by going to the company's website and placing an order. If a company is going to roll out a new product, they could organize a series of webcasts to introduce their customers to the new product.

**Summary**4:43-5:17

Summary

That's it for this lesson. In this lesson we introduced you to the concept of a computer network. Remember, a network is a group of interconnected devices that need to share information with each other. In order for that network to work, several key components are required. First, you must have the devices themselves that need to communicate with each other. You need some type of connecting medium. You need an appropriate network interface that connects to that network medium. Finally, you need some agreed upon set of communication standards to define our networking protocols.

We also talked about the fact that networks usually save the company more time and money than they cost to set up and maintain.

6.1.2 Network Types

## Network Types 0:00-0:22

In this lesson, we're going to spend time looking at different ways you can classify computer networks. We're going to focus on classifying networks according to the roles that the individual hosts on that network fulfill. Specifically, we're going to discuss two different types of networks. First, we're going to look at peer-to-peer networks.

## Peer-to-peer Network 0:23-1:46

Then we're going to look at client-server networks.

Let's first look at a peer-to-peer network. In a peer-to-peer network, the individual hosts don't have a specific role. Hosts on a peer-to-peer network do two things at the same time. They provide and consume network services. In a peer-to-peer network there could be many different computer systems. Each can fulfill a variety of networking roles.

For example, a workstation has a printer connected. If the printer is shared on the network, other network hosts can send print jobs to it. In addition, a host with a large hard disk drive can allow other network hosts to access this shared hard disk drive. This means a user with a file that needs to be saved can save it over the network connection to that system's hard disk drive.

As you can see, these network hosts both provide and consume network services. The host with the printer and the host with the hard disk drive provide a network service. One provides printing and the other provides storage. At the same time, all hosts consume services.

One host prints to another workstation's printer. A different workstation saves files to the hard drive on another workstation. They function as both a client and as a server at the same time.

## Advantages 1:47-2:22

Peer-to-peer networks have several different advantages. First, they're very easy to implement. You can create a peer-to-peer network using the existing workstations in your organization. There's no special software to buy. Once you've configured hosts in a peer-to-peer network, you can then share printers and storage devices on the network with minimal configuration. All you have to do is share your locally connected resources.

Another advantage of peer-to-peer networks is that they're relatively inexpensive to implement. With a peer-to-peer network, you just use your standard desktop operating system on each host. There's no special software to purchase and implement.

## Disadvantages 2:23-4:06

You might ask, "If peer-to-peer networks are so inexpensive and so easy to set up, why aren't there more of them?" It's because peer-to-peer networks also have several drawbacks. For example, a peer-to-peer network is not scalable. The bigger it gets, the harder it is to manage and keep running.

In addition, peer-to-peer networks are difficult to support because they lack centralized controls. For example, suppose you have shared storage on the hard drive in a particular workstation. The user who uses this workstation needs more storage space freed up to save files. That user goes through the hard disk looking for files that don't seem important and deletes them. Files that belong to other network users could potentially be deleted. Those users would lose their work.

In addition, suppose a workstation provides a shared printer that everybody in the network uses. The user who uses this workstation decides to take a day off of work. Before she leaves, she locks her office door and turns her computer off. When this happens, no one in the office can print anymore. If a host is down, then users can't send print jobs to the printer.

Another problem associated with peer-to-peer networks is the fact that data storage can end up being decentralized. For example, you could configure a shared folder on three systems. In this configuration, users could save sensitive company data in each of the shared folders on these different systems. In order to back up critical company data, the system administrator has to visit each of these hosts individually and back up each one every night.

This represents a lot of work. It also makes it difficult to keep this important data organized.

## Client-server Network 4:07-5:18

The second type of computer network that you need to be familiar with addresses a lot of the shortcomings of a peer-to-peer network. This is called a client-server network. Unlike a peer-to-peer network, in a client-server network the network hosts have specific roles assigned to them. For example, some hosts are assigned to be servers. A server provides network resources. The other hosts function as clients. A client does not provide network services, instead it consumes network services.

For example, you have a network with client workstations that do not have any kind of shared storage or shared printer attached to them. These services are provided by the server. You have a server with a very large hard drive installed. The server also manages a shared network printer. It could also have a web server running that provides web pages to these clients systems. In this scenario, the server provides the network resources and the clients simply use those resources.

In order to set up a client-server network, different operating systems have to be installed on the various systems.

## Client Operating Systems 5:19-5:34

First, client workstations need to use a desktop operating system that allows the users to do their daily work. They need to be able to run desktop applications. They also have to have some type of client software installed so they can connect to the server and use shared resources.

## Server Operating Systems 5:35-5:56

The server, on the other hand, has to use a specialized operating system optimized to perform only server tasks. It will not be used to perform client-type tasks, such as word processing, creating spreadsheets, and so on. Server operating systems are designed to do one thing only. That task is to provide network resources.

## Advantages 5:57-6:45

One of the main benefits of using a client-server network is that it is very scalable. It's relatively easy to expand the size of the network. You can add clients and you can add servers. It handles it really well. In addition, client-server networks are also much easier to support, because all of these services are centralized in a limited number of locations.

For example, you have a user with problems accessing files. With a client-server network, all you have to do is check the storage on the file server. Likewise, if you have users with trouble printing, all you have to do is check the printer managed by the server. Data protection is also a lot easier in a client-server network compared to a peer-to-peer network. The system administrator needs to back up the shared data only on the server. They don't have to go around to each client workstation and run a backup.

## Disadvantages 6:46-7:19

There are some drawbacks associated with a client-server network. For example, they are a lot more expensive to implement. Server hardware and server operating systems are much more expensive than those used by client workstations.

In addition, this type of network takes a lot more planning. With a peer-to-peer network, you tend to just throw things together and make it work. However, that will not work in a client-server network. In a client-server network, you have to plan which servers will host which services. You also have to plan where those servers are placed on the network before you install hardware and configure operating systems.

## Summary 7:20-7:41

That's it for this lesson. In this lesson we discussed the differences between peer-to-peer networks and client-server networks. In a peer-to-peer network, the individual hosts both provide and consume network services. In a client-server network, certain hosts are designated as servers to provide network services. All of the other hosts are clients and consume those services provided by the server.

6.1.3 Networking Terms

**Networking Terms**0:00-0:06

If you think about it, a network is really like a neighborhood.

**Addressing**0:07-2:53

For example, you have a neighborhood with a street running through it called Oak Street. Oak street has three different houses. Each house on this street has a unique address to distinguish it from the other houses on the same street. That way, postal workers know where they can deliver mail.

Take the address of the house at 732 Oak Street. Notice that the address of this house has two different parts. First, you have the house number. You also have the street name. Just like a house in a neighborhood, networks also use a two-part address to identify individual hosts on that network.

For example, you can have a computer on a network that has the number 1 assigned to it. This is the host address. The network it's connected to also has an address, in this case, 192.168.1. Just as a house in a neighborhood has a house number and street address, a computer on a network has a host address and a network address. If you combine the two together, you can uniquely identify a host on the network in the same way a house and a street address uniquely identifies a particular house in a neighborhood.

Suppose there's a second street in this neighborhood and this street is called Elm Street. It intersects with Oak Street and it's connected to several other houses. Just as on Oak Street, each of these houses has its own number. You may notice that this house on Elm Street has exactly the same number as the house on Oak Street.

Suppose you're a postal worker and you have an envelope that's addressed to house 732. Without a street address, you wouldn't know which of these houses should get that particular envelope. Should it be 732 Oak or 732 Elm? Because these houses each have a two-part address, 732 Elm and 732 Oak, you can identify which house a particular piece of mail goes to.

It works exactly the same way on a computer network. You could have two computers on two different networks that have the same host number assigned to them. You could have a host on one network that's assigned the number 1 and a host on another network that's assigned the number 1 as well. You can identify them uniquely from each other by looking at the network address.

One host has a network address of 192.168.1. The other host has a network address of 10.0.0. In the same way that you differentiate between two houses with the same house number that are on different streets, you can combine the host and network address to uniquely identify the host on these two networks.

**Subnet**2:54-3:36

Two networks can connect to each other, forming a larger network. This network could be connected to an even larger network. If the only word you had to describe these connections were "network," it would be difficult to know which network you're talking about. Therefore, we need to introduce some new terminology.

Each separate network represents a subnet. A subnet is a part of the network where all of the computers share the same subnet address. This works in much the same way that all houses on the same street share the same street address. Sometimes you'll hear a subnet address referred to as a network address. They're the same thing. Best practice is to use the term subnet address.

**LAN**3:37-4:04

You can connect subnets to each other by a device called a router. You can connect multiple networks together using multiple routers. You can have many different networks within a particular organization. When several networks within the same organization are connected together, they're collectively referred to as a Local Area Network (LAN).

**MAN**4:05-4:25

There will be many local area networks within the same city. They can all interconnect together using some type of connectivity. In this situation, all of the networks within the same metropolitan area connecting together constitute a Metropolitan Area Network (MAN).

**WAN**4:26-4:39

Many networks in many different cities can connect together. The connections between them are called Wide Area Network links (WAN links). The collection of connected networks is called a Wide Area Network (WAN).

**Network**4:40-5:03

Another way that you use the term network is to describe the connected devices that are under the control of one particular organization. Let's pretend you have a sporting goods store with its own local area network. You also have a software company with its own network. In this case, you would use the term network to describe the boundary between these two individual organizations.

**Internetwork**5:04-5:54

You can connect the two networks. When you do, you now have a WAN connection because there's a wide area link between the two organizations. When this happens, you won't refer to both networks together as a single network. Instead, you're going to use the term internetwork because you're taking two separate networks and you're connecting them together.

To review, a subnet is the section of a network where all the devices share the same subnet address. A LAN is a collection of connected subnets within the same organization. A MAN is a collection of interconnected networks within the same metropolitan area. A WAN is created by joining two or more LANs or MANs together. Finally, an internetwork is the collection of multiple networks that may be organized and managed by different organizations.

**Internet**5:55-8:46

Another term you need to be familiar with is internet. Of course, you've heard of the internet. You probably used the internet today, but we're going to talk about the internet today in terms of networking.

As its name implies, the internet is an interconnection of networks. Remember, we talked earlier that an internetwork is a connection between networks that aren't controlled by the same entity. That principle applies to the internet.

There are parts of the internet that are managed by large corporations or even nonprofit groups. In reality, the internet is a collection of many different networks owned by many different entities that all share information and communicate together. The internet connects devices all around the world.

There are cities scattered around the world that share a common way of connecting so that they can route signals between each other. At each spot, you will have one or more Internet Service Providers (ISPs). ISPs don't manage the main part of the internet network. Instead, they manage an access point to the internet.

If you think of the internet as a big freeway, then ISPs are the entity that manages the on-ramp to the freeway. They're responsible for building the on-ramp and keeping it maintained and open, but they're not responsible for the whole internet itself. The ISP is responsible for allowing both individual users, as well as companies with large networks, to connect to the internet.

For example, you could contract with an ISP to connect your network to the internet. In this scenario, there's typically a security boundary that separates your network from the public internet network. You may have devices on your network that access network servers, such as web servers and email servers. They're connected to the internet, but other computers that are on the internet cannot contact devices within your network.

This creates a division of sorts between networks. Public networks share all devices and they're freely available. Devices on a private network can access public network devices, but they can be accessed only by devices within the private network. There may be exceptions.

For example, you might have a particular server that you do want to make available to the public, such as a server that hosts a website for an organization. In order to do this, you have to place the web server outside of this security boundary so that devices in other locations can reach this website through the internet. When you do this, you've created a small public network that is connected to the larger internet.

**Intranet**8:47-9:31

A related term that you might hear from time to time is intranet. An intranet is like a miniature internet. An intranet is a private network, not a public one, but it uses many of the same technologies used on the internet. This intranet may or may not be connected to the public internet.

For example, you could have an email server within a private network. Only people within the private network can access it, even though the network is connected to the internet. This way, you're using internet technology on the local private network. Again, the security boundary would prevent devices on the internet from accessing the devices within the intranet.

**Extranet**9:32-10:41

Another term you might hear is extranet. An extranet essentially is an intranet that is made partially available to entities outside of your organization.

For example, let's say you have a company connected to the internet. You also have a partner company in another location. You need to make some of the information within your intranet available through the internet to that partner organization. To do this, you could establish an extranet that is connected to the internet. You implement controls on the extranet to make sure that this partner organization can access only the information that you want it to.

Any devices that are not part of the extranet, meaning they don't belong to the authorized partner corporation, would not be allowed to access the resources within the extranet. The internet is a large public network. An intranet is a private network that uses internet technologies and is available only to users within a particular organization. An extranet is a private network that is made available to authorized external users but not to the general public.

**Summary**10:42-10:56

In this lesson, we introduced you to many different networking terms. We talked about addressing, we talked about LANs, MANs, and WANs. We also talked about the internet, intranets, and finally, we ended this lesson by talking about extranets.

6.1.4 Networking Facts

A *network* is a group of computers that can share information through their connections. A network is made up of the following components:

* Computers (often called *nodes* or *hosts*).
* Transmission media, which provide a path for electrical signals between devices.
* Network interfaces, devices that send and receive electrical signals.
* Protocols, rules or standards that describe how hosts communicate and exchange data.

Despite the costs of implementation and maintenance, networks actually save organizations money by allowing them to:

* Consolidate (centralize) data storage.
* Share peripheral devices, like printers.
* Increase internal and external communications.
* Increase productivity and collaboration.

There are several ways to classify networks. The following table lists several ways to describe a network.

|  |  |  |
| --- | --- | --- |
| **Type** | **Classification** | **Description** |
| Host Role | Peer-to-Peer | In a peer-to-peer network, each host can provide network resources to other hosts or access resources located on other hosts. Each host is in charge of controlling access to those resources. Advantages of peer-to-peer networks include the following:   * Easy implementation * Inexpensive   Disadvantages of peer-to-peer networks include the following:   * Difficult to expand (not scalable) * Difficult to support * Lack centralized control * No centralized storage |
| Client-Server | In a client-server network, hosts have specific roles. For example, some hosts are assigned server roles, which allow them to provide network resources to other hosts. Other hosts are assigned client roles, which allow them to consume network resources. Advantages of client-server networks include the following:   * Easy to expand (scalable) * Easy to support * Centralized services * Easy to back up   Disadvantages of client-server networks include the following:   * Expensive server operating systems * Extensive advanced planning required |
| Geography | Personal Area Network (PAN) | A *personal area network* is a very small network used for communication between personal devices. For example, a PAN may include a notebook computer, a wireless headset, a wireless printer, and a smartphone. A PAN is limited to a few feet in range. A PAN is typically created using Bluetooth wireless technologies. |
| Local Area Network (LAN) | A *local area network* is a network in a small geographic area, like an office. A LAN typically uses wires to connect systems together. |
| Wireless Local Area Network (WLAN) | A wireless LAN covers an area that is roughly the same size as a standard LAN. It uses radio signals to connect systems instead of wires. |
| Metropolitan Area Network (MAN) | A *metropolitan area network* is a network that covers an area as small as a few city blocks to as large as an entire metropolitan city. MANs are typically owned and managed by a city as a public utility. Be aware that many IT professionals do not differentiate between a wide area network and a MAN, as they use essentially the same network technologies. |
| Wide Area Network (WAN) | A *wide area network* is a group of LANs that are geographically isolated, but are connected to form a large internetwork. |
| Wireless Mesh Network (WMN) | A *wireless mesh network (WMN)* is a group of wireless mesh nodes that communicate with one another to share the network connection across a large area. They provide the ability to stream voice, data, and video between arbitrary pairs of devices. Each device in the WMN uses the others as relays to avoid the need for infrastructure. |
| Wireless Wide Area Network (WWAN) | A wireless wide area network (WWAN) covers a large geographical area by connecting separate areas wirelessly. WLAN and WWAN both connect to the internet wirelessly, but they use different technologies to do it. WWANs are often referred to as 3G, 4G, or LTE networks because they usually use cellular network technologies as connection types. |
| Management | Network | The term *network* often describes a computer system controlled by a single organization. This could be a local area network at a single location or a wide area network used by a single business or organization. If two companies connected their internal networks to share data, you could call it one network. In reality, however, it is two networks, because each network is managed by a different company. |
| Subnet | A *subnet* is a portion of a network with a common network address.   * All devices on the subnet share the same network address, but they have unique host addresses. * Each subnet in a larger network has a unique subnet address. * Devices connected through hubs or switches are on the same subnet. Routers are used to connect multiple subnets. |
| Internetwork | A network with geographically dispersed WAN connections that connect multiple LANs is often called an *internetwork*. Additionally, connecting two networks under different management is a form of internetworking because data must travel between two networks. |
| Participation | Internet | The *internet* is a large, world-wide, public network. The network is public because virtually anyone can connect to it, and users or organizations make services freely available on the internet.   * Users and organizations connect to the internet through an internet service provider (ISP). * The internet uses a set of communication protocols (TCP/IP) for providing services. * Individuals and organizations can make services (such as a website) available to other users on the internet. |
| Intranet | An *intranet* is a private network that uses internet technologies. Services on an intranet are only available to hosts that are connected to the private network. For example, your company might have a website that only employees can access. |
| Extranet | An *extranet* is a private network that uses internet technologies, but its resources are made available to external trusted users. For example, you might create a website on a private network that only users from a partner company can access. |

Test Out Logo

**TestOut PC Pro***English 6.0.4*

Home

Outline

**Actions**

Click to View Actions Menu

Copyright © 2019

TestOut Corporation

All rights reserved.

Powered by Lab Sim

6.1.4 Networking Facts

Copy TextPrint Page

A *network* is a group of computers that can share information through their connections. A network is made up of the following components:

* Computers (often called *nodes* or *hosts*).
* Transmission media, which provide a path for electrical signals between devices.
* Network interfaces, devices that send and receive electrical signals.
* Protocols, rules or standards that describe how hosts communicate and exchange data.

Despite the costs of implementation and maintenance, networks actually save organizations money by allowing them to:

* Consolidate (centralize) data storage.
* Share peripheral devices, like printers.
* Increase internal and external communications.
* Increase productivity and collaboration.

There are several ways to classify networks. The following table lists several ways to describe a network.

|  |  |  |
| --- | --- | --- |
| **Type** | **Classification** | **Description** |
| Host Role | Peer-to-Peer | In a peer-to-peer network, each host can provide network resources to other hosts or access resources located on other hosts. Each host is in charge of controlling access to those resources. Advantages of peer-to-peer networks include the following:   * Easy implementation * Inexpensive   Disadvantages of peer-to-peer networks include the following:   * Difficult to expand (not scalable) * Difficult to support * Lack centralized control * No centralized storage |
| Client-Server | In a client-server network, hosts have specific roles. For example, some hosts are assigned server roles, which allow them to provide network resources to other hosts. Other hosts are assigned client roles, which allow them to consume network resources. Advantages of client-server networks include the following:   * Easy to expand (scalable) * Easy to support * Centralized services * Easy to back up   Disadvantages of client-server networks include the following:   * Expensive server operating systems * Extensive advanced planning required |
| Geography | Personal Area Network (PAN) | A *personal area network* is a very small network used for communication between personal devices. For example, a PAN may include a notebook computer, a wireless headset, a wireless printer, and a smartphone. A PAN is limited to a few feet in range. A PAN is typically created using Bluetooth wireless technologies. |
| Local Area Network (LAN) | A *local area network* is a network in a small geographic area, like an office. A LAN typically uses wires to connect systems together. |
| Wireless Local Area Network (WLAN) | A wireless LAN covers an area that is roughly the same size as a standard LAN. It uses radio signals to connect systems instead of wires. |
| Metropolitan Area Network (MAN) | A *metropolitan area network* is a network that covers an area as small as a few city blocks to as large as an entire metropolitan city. MANs are typically owned and managed by a city as a public utility. Be aware that many IT professionals do not differentiate between a wide area network and a MAN, as they use essentially the same network technologies. |
| Wide Area Network (WAN) | A *wide area network* is a group of LANs that are geographically isolated, but are connected to form a large internetwork. |
| Wireless Mesh Network (WMN) | A *wireless mesh network (WMN)* is a group of wireless mesh nodes that communicate with one another to share the network connection across a large area. They provide the ability to stream voice, data, and video between arbitrary pairs of devices. Each device in the WMN uses the others as relays to avoid the need for infrastructure. |
| Wireless Wide Area Network (WWAN) | A wireless wide area network (WWAN) covers a large geographical area by connecting separate areas wirelessly. WLAN and WWAN both connect to the internet wirelessly, but they use different technologies to do it. WWANs are often referred to as 3G, 4G, or LTE networks because they usually use cellular network technologies as connection types. |
| Management | Network | The term *network* often describes a computer system controlled by a single organization. This could be a local area network at a single location or a wide area network used by a single business or organization. If two companies connected their internal networks to share data, you could call it one network. In reality, however, it is two networks, because each network is managed by a different company. |
| Subnet | A *subnet* is a portion of a network with a common network address.   * All devices on the subnet share the same network address, but they have unique host addresses. * Each subnet in a larger network has a unique subnet address. * Devices connected through hubs or switches are on the same subnet. Routers are used to connect multiple subnets. |
| Internetwork | A network with geographically dispersed WAN connections that connect multiple LANs is often called an *internetwork*. Additionally, connecting two networks under different management is a form of internetworking because data must travel between two networks. |
| Participation | Internet | The *internet* is a large, world-wide, public network. The network is public because virtually anyone can connect to it, and users or organizations make services freely available on the internet.   * Users and organizations connect to the internet through an internet service provider (ISP). * The internet uses a set of communication protocols (TCP/IP) for providing services. * Individuals and organizations can make services (such as a website) available to other users on the internet. |
| Intranet | An *intranet* is a private network that uses internet technologies. Services on an intranet are only available to hosts that are connected to the private network. For example, your company might have a website that only employees can access. |
| Extranet | An *extranet* is a private network that uses internet technologies, but its resources are made available to external trusted users. For example, you might create a website on a private network that only users from a partner company can access. |

6.1.5 Networking Topologies

## Network Topologies 0:00-0:10

In this lesson, we're going to discuss the network topology. A topology is a graphical depiction of the layout of a computer network.

## Topology Overview 0:11-0:35

There are two different types of topologies. The physical topology describes the layout of the network, or how devices are connected. The logical topology describes how devices communicate with each other, or how data is transmitted on the network.

It's important to know the difference between the physical and logical topology because different types of networks may use one type of physical topology, but use an entirely different logical topology.

## Physical Topology 0:36-1:31

The physical topology refers to the way a computer network is physically wired. There are different types of physical topologies. A bus topology is created when the computers are all connected to a single cable. A ring topology is created when one computer is connected to another, and then another, until they form a ring.

Think of the physical topology like the roads in a city. If you were to look at a map of a city, you could see all the interconnecting roads. This is the physical topology of the roads in the city. Each road connects different buildings to different parts of the city in much the same way cables connect devices to each other on a network.

The physical topology doesn't necessarily dictate how data is transferred between computers. The way data is transferred is dictated by the logical topology of the network. Consider a house on the city map. There is a street that connects to the house. This is the physical topology.

## Logical Topology 1:32-2:45

The logical topology dictates how data is transferred on the physical topology. By way of analogy, the logical topology is similar to the traffic laws that dictate how traffic flows on a physical road. Suppose there are one-way streets and traffic lights. At the end of one road is a road block. These components make up the logical topology of our map. They control how cars can drive on the roads.

With a network, the logical topology describes how data travels on the network from source to destination. This means two different networks could have the same physical topology, but have completely different logical topologies.

For example, suppose you have two networks that share the same physical topology, a star topology. All the devices connect to a central connecting point. One network could have a bus logical topology, so that it functions in the same way that a bus topology functions. Its physical topology is a star topology, but its logical topology is a bus topology.

By way of contrast, the other network could have a logical topology that functions as a star topology. In this case, both the physical and logical topologies are star topologies. Let's review the different types of topologies available.

## Bus Topology 2:46-3:13

Let's begin with the bus topology. All devices are physically connected to each other by a single central cable. Suppose a computer wants to send data to the computer next to it on the central cable. In a logical bus topology, the data is sent to all the computers connected to the central cable. Each computer looks at the data it receives and determines whether the data is addressed to it or not. If the data isn't addressed to it, the computer discards the data. If the data is addressed to it, the computer accepts the data.

## Ring Topology 3:14-4:08

Let's look at the ring topology. In a physical ring topology there is no central connecting point. Instead, you have point-to-point connections between network devices. Each device is connected to the device before it and after it. In a ring topology, each device is connected to only two other devices. In a logical ring topology, data is forwarded along the network by each computer.

For instance, if one computer needs to send data to a computer on the other side of the ring, it sends the data to the computer next to it first. That computer checks to see if the data is for it, and since the data isn't, it forwards the data to the next computer in the ring. The computers keep doing this until the data reaches its destination.

If computers that are directly connected send data to each other, the data goes directly to that computer and doesn't need to be forwarded. Older networks used this topology, so you probably won't encounter deployments that use both physical and logical ring topologies today.

## Star Topology 4:09-5:04

A physical star topology uses a central connecting device. All the devices on the network connect to this central connecting device. This is the most commonly used physical topology today. With a logical star topology, data is sent directly to the intended device only. For example, when one computer wants to send data to another computer, the data is first sent to the central connecting device. The central connecting device then analyzes the data and forwards it to the intended computer.

Logical topologies can be implemented on top of a different physical topology. For instance, a star physical topology can use a bus logical topology. In this case, data from one computer would be sent to the central connecting device. The connecting device would then duplicate the data and send it to every computer connected to the device. Each computer would then look at the data and see if it is the intended recipient. If the computer isn't the intended recipient, then it would discard the data.

## Mesh Networking Topology 5:05-6:24

With the mesh networking topology, each device on the network has a point-to-point connection to every other device on the network. For example, each of four computers has a direct connection to the other three computers. With this topology, the more computers you add, the more connections you need.

Until recently, the mesh topology was theoretical. In order to create the point-to-point connections between every computer on the network, each device would need a separate network adapter for every other device on the network.

For example, if you had 50 devices on a network, each device would need 50 network adapters. This provides tremendous redundancy. A failed link can be compensated for by using redundant links. For this reason, this type of topology may be implemented on a network backbone. However, it is rarely implemented on a production network with workstations. The number of network interfaces required make this topology impractical to implement.

However, if you use a wireless networking medium, instead of a wired medium, the mesh topology becomes practical. If the connections were changed to a radio signal using a wireless network adapter, you would need only one network adapter in each of these devices. Each wireless network adapter can communicate directly with the wireless network adapter on any other device.

## Partial Mesh Topology 6:25-6:45

You may encounter a partial mesh topology. In this topology, some nodes are connected to all the other nodes using direct links, but some are connected to only one or two other nodes. This is less expensive and more practical to implement as compared to a full, mesh topology. However, it offers far less redundancy than a full, mesh topology.

## Summary 6:46-7:03

In this lesson we learned about network topology. We learned that there are two topology categories. There's the physical topology and the logical topology. The physical topology describes the way networks are physically wired. And the logical topology describes the way the network transmits data and operates.

6.1.6 Topology Facts

*Topology* is the term used to describe how devices are connected and how messages flow from device to device. There are two types of network topologies:

* The physical topology describes the way the network is wired.
* The logical topology describes the way messages are sent.

This lesson covers the following topics:

* Physical Topologies
* Logical Topologies

### Physical Topologies

The following table describes several common physical topologies.

|  |  |
| --- | --- |
| **Topology** | **Description** |
| Bus | A bus topology consists of a trunk cable with nodes either inserted directly into the trunk or tapped into the trunk using offshoot cables called drop cables. In a bus topology:   * Signals travel from one node to all other nodes. * A device called a *terminator* is placed at both ends of the trunk cable. * Terminators absorb signals and prevent them from reflecting repeatedly back and forth on the cable. * It can be difficult to isolate cabling problems.   A broken cable anywhere on the bus breaks the termination and prevents communications between any devices on the network. |
| Ring | A ring topology connects neighboring nodes until they form a ring. Signals travel in one direction around the ring; each device on the network acts as a repeater to send the signal to the next device. In a ring topology:   * Installation requires careful planning to create a continuous ring. * Isolating problems can require going to several physical locations along the ring. * A malfunctioning node or cable break can prevent signals from reaching nodes further along on the ring. |
| Star | A star topology uses a hub or switch to connect all network connections to a single physical location. Today, it is the most popular type of topology for a LAN. In a star topology:   * All network connections are located in a single place, which makes it easy to troubleshoot and reconfigure. * It is easy to add or remove nodes. * Cabling problems usually only affect one node. |
| Mesh | A mesh topology exists when there are multiple paths between any two nodes on a network. Mesh topologies are created using point-to-point connections. This increases the network's fault tolerance because alternate paths can be used when one path fails. Two variations of mesh topologies exist, partial mesh and full mesh. In a partial mesh topology, some redundant paths exist. In a full mesh topology, every node has a point-to-point connection with every other node.  Full mesh topologies are usually impractical in a standard LAN because the number of connections increases dramatically with every new node added to the network. A separate network interface and cable for each host on the network is required. However, a full mesh topology is commonly used to interconnect routers, providing alternate paths should one path go down or become overloaded. Mesh networks are also commonly used to create redundant paths between access points in a wireless network, providing alternate paths back to the wireless controller should one access point go down or become overloaded. With this topology, every access point can communicate directly with any other access point on the wireless network. |

### Logical Topologies

You should be able to identify the physical topology by looking at the way devices are connected. However, it is not as easy to identify the logical topology. As the following table shows, there is often more than one way for messages to travel in a given physical topology.

|  |  |  |
| --- | --- | --- |
| **Logical Topology** | **Physical Topology** | **Description** |
| Bus | Bus | Messages are sent to all devices connected to the bus. |
| Star |
| Ring | Ring | Messages are sent from device to device in a predetermined order until they reach the destination device. |
| Star |
| Star | Star | Messages are sent directly to (and only to) the destination device. |
| Mesh | Mesh | Messages are sent from one device to the next around the ring until they reach the destination device. |

Chapter 6: Networking

6.4 Ethernet

As you study this section, answer the following questions:

* What cable types can be used on an Ethernet network?
* What is the most common cable type and connector?
* What is the difference between a hub and a switch? Why should you choose a switch over a hub?
* When would you use a router on an Ethernet network?
* What cable type and speed are supported on a 1000BaseT network?
* What is the maximum cable length for a 100BaseTX network?

Key terms for this section include the following:

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Network Interface Card (NIC) | This card creates the signals sent along the networking medium. |
| Networking media | Ethernet supports such cable types as UTP, fiber optic, thinnet, and thicknet. |
| Connectivity devices | Ethernet uses such connectivity devices as hub, switch, router, bridge, patch panel, and PoE. |
| Ethernet standards | The standards that identify Ethernet transmission speeds and cable types. |
| Power over Ethernet (PoE) | PoE distributes electrical power and network data on twisted-pair CAT 5 or higher. |

This section helps you prepare for the following certification exam objectives:

|  |  |
| --- | --- |
| **Exam** | **Objective** |
| CompTIA 220-1001 | 3.1 Explain basic cable types, features, and their purposes   * Network cables   + Ethernet   + Cat 5   + Cat 5e   + Cat 6   + Fiber   + Coaxial   + Unshielded twisted pair   + Speed and transmission limitations |
| CompTIA 220-1002 | 2.2 Compare and contrast common networking hardware devices   * Routers * Repeater * Hub * Bridge * Patch panel * Ethernet over Power * Power over Ethernet (PoE)   + Switch * Network interface card   1.8 Given a scenario, configure Microsoft Windows networking on a client/desktop   * Establish networking connections   + WWAN (Cellular) |

6.4.1 Ethernet

**Ethernet**0:00-0:28

Ethernet is the most common local area networking standard for wired networks. Almost every wired network you'll encounter uses the Ethernet standard. In this lesson, we're going to look at a typical Ethernet network and the various components that allow communication.

In an Ethernet network you have computers, or hosts, some network connectivity devices, a server, and the connecting medium. Let's take a closer look at some of these components.

**Network Interface Card**0:29-1:01

Each host on a network needs to have a network interface card (NIC) installed in order to connect to an Ethernet network. In addition, the NIC should use the same connecting medium as the rest of the network.

Network interface cards have a few key components that are used for Ethernet network communication. The first is the transceiver. A NIC's transceiver is responsible for converting digital data, that is zeroes and ones, into electrical signals that are sent along the network medium. Each NIC also has a unique MAC address that is used for identification and communication purposes.

**Transmission Medium**1:02-1:20

The connecting medium in an Ethernet network is typically unshielded twisted pair copper cabling. Usually a Cat 5e or CAT 6 grade twisted pair cable. Some networks use fiber optic cabling as the connecting medium. Ethernet networks that use fiber optic cabling require fiber optic NICs in each host.

**Central Connection Point**1:21-1:29

Ethernet networks use what's called a star network topology. This means that hosts in the network connect to a central connection point, typically a switch.

**Switch**1:30-1:55

The switch must use the same connection medium as the hosts.

Some Ethernet switches are able to provide what's called power over Ethernet (PoE). Switches with PoE provide a small amount of power through the Ethernet cabling. That power can be used to power small devices such as IP phones and security cameras without the need of a power outlet. PoE can be provided using only a twisted pair cable. Fiber cannot provide this functionality.

**Ethernet Router**1:56-2:10

Connected to the switch is the router. Any Ethernet network that has an internet connection uses a router to forward packets from within the network out to external networks, such as the internet. The router is also responsible for filtering incoming packets to the appropriate subnet.

**Bridge**2:11-2:20

Some Ethernet networks also have a bridge. This is typically in the form of a wireless bridge which converts the Ethernet network medium into an unbounded wireless signal, and vice versa.

**Ethernet Naming Standards**2:21-4:04

The speeds of an Ethernet network depends on a lot of different factors. Most Ethernet networks have 100 Mbps transfer speeds. However, many networks are migrating to 1,000 Mbps, or 1 Gbps, transfer speeds. Ethernet networks that use CAT 6e or fiber cabling can have even faster speeds.

To identify the speed of an Ethernet network, you use specific Ethernet naming standards which consists of numbers and letters. The number at the beginning denotes the transmission speed. In this case it's 1,000, or 1,000 Mbps per second. Next you have the word BASE. This refers to base band signaling, which is the type of signaling used on Ethernet networks.

After that, you have a dash followed by a letter. This letter defines the transmission medium. The T stands for twisted pair. More specifically, unshielded twisted pair. The T also specifies maximum cable length of 100 meters. If this were CX, the maximum cable length would be 25 meters.

If you were to see a different letter, such as an L, LX, SX, etc. This would mean that the transmission medium is fiber optic cabling, not twisted pair cabling. As you can see, knowing how to decode the Ethernet specification naming is very useful.

Let's use another example. If you see 10GBASE-SR, using what you just learned, you could identify information about the Ethernet standard. Notice the number has a G after it. This G stands for gigabit. That tells you that the transmission speeds are 10 Gbps. It uses a base band signal and the network transmission medium is SR, or short range fiber optic.

**Summary**4:05-4:24

Summary

Those are some of the components and characteristics of an Ethernet network. Remember Ethernet networks typically use unshielded twisted pair cabling. However, some use fiber optic cabling. Ethernet networks also use a switch to connect hosts, creating a star network topology. Ethernet networks use a standard naming convention to identify transmission speeds and specifications.

6.4.2 Ethernet Facts

Ethernet is the most common local area networking standard for wired networks. The following table describes the various components that compose an Ethernet network:

|  |  |
| --- | --- |
| **Component** | **Description** |
| Network Interface Card | A network interface card (NIC) creates the signals that are sent along the networking medium.   * A transceiver built into the network adapter formats the binary data for transmission on the network medium. * Ethernet devices are identified using the MAC address, which is burned into the network interface card. |
| Networking Media | Ethernet supports the following cable types:   * Unshielded twisted-pair cables (UTP) with RJ45 connectors. This is the most common transmission medium used for Ethernet. * Fiber optic cables, which are used in high-speed applications (such as servers or streaming media). * Coaxial cable with F-type connectors for cable internet services. Coaxial cable is also used for older Ethernet implementations ( which are often called *thinnet* or *thicknet* networks). |
| Connectivity Devices | Ethernet uses the following connectivity devices:   * A hub provides a central connection for multiple media segments on the same subnet. When a hub receives a signal, it is repeated out to all other ports. Hubs operate in half-duplex mode, meaning devices can either send or receive data at any given time.   Hubs are rarely used in networking environments. You should avoid them if possible.   * A switch provides a central connection for multiple media segments on the same subnet. When a switch receives a signal, it forwards that signal only to the port where the destination device is connected.   + Switches use the MAC address to send frames to the destination device.   + Switches operate in full-duplex mode, meaning devices can send and receive data at the same time because transmission paths are dedicated to only the communicating devices.   + When possible, use switches instead of hubs. * A router connects two network segments that have different subnet addresses.   + A router has multiple network connections. Each connection is on a different subnet.   + Routers use the IP address within a packet to move packets between networks. * A bridge connects two segments within the same subnet that use different media types. For example, you can use a bridge to connect wireless clients to wired clients on the same network. * A patch panel is a device that is commonly used to connect individual stranded wires into female RJ45 connectors. For example, you might connect four pairs of wires from a punchdown block to a port on the patch panel. On the patch panel, you then connect drop cables (cables with RJ45 connectors) to the patch panel on one end and a computer on the other end. * An Ethernet over power device allows network communications to be transmitted over existing AC power lines. An Ethernet over power device is plugged in to one AC power outlet, and a second Ethernet over power device is connected to the same AC circuit. These devices multiplex the AC copper power lines to transmit digital network signals at a frequency higher than the AC electrical power already on the circuit. |
| Standards | Ethernet standards identify the transmission speed and the cable type. Data transfer rates range from 10 Mbps (very old Ethernet networks) up to 10 Gbps. Between 100 and 1000 Mbps are the most common speeds for most networks. |
| Distance | Ethernet standards define the maximum distance for cable lengths between two devices.   * The maximum cable length for UTP Ethernet "T" implementations is 100 meters for all standards. * The length for fiber optic cables varies depending on the cable type and specification, but typically ranges from 100 meters to 40 kilometers. |
| Power over Ethernet | Power over Ethernet (PoE) technology is used to distribute electrical power along with network data on twisted-pair Ethernet cabling (CAT 5 or higher). Power is usually supplied by a PoE-enabled Ethernet switch. PoE is commonly used to power network devices that are located where physical access to a power outlet may not be available. For example, a PoE-enabled surveillance camera mounted on a tall pole can be powered via its Ethernet cabling.  You can use a Power over Ethernet (PoE) injector to add PoE capability to regular non-PoE network links. PoE injectors can be used to upgrade existing LAN installations to PoE and provide a solution where fewer PoE ports are required. To upgrade a network connection to PoE, patch it through the PoE injector. Power injection is controlled and automatic. |

6.4.2 Ethernet Facts

Ethernet is the most common local area networking standard for wired networks. The following table describes the various components that compose an Ethernet network:

|  |  |
| --- | --- |
| **Component** | **Description** |
| Network Interface Card | A network interface card (NIC) creates the signals that are sent along the networking medium.   * A transceiver built into the network adapter formats the binary data for transmission on the network medium. * Ethernet devices are identified using the MAC address, which is burned into the network interface card. |
| Networking Media | Ethernet supports the following cable types:   * Unshielded twisted-pair cables (UTP) with RJ45 connectors. This is the most common transmission medium used for Ethernet. * Fiber optic cables, which are used in high-speed applications (such as servers or streaming media). * Coaxial cable with F-type connectors for cable internet services. Coaxial cable is also used for older Ethernet implementations ( which are often called *thinnet* or *thicknet* networks). |
| Connectivity Devices | Ethernet uses the following connectivity devices:   * A hub provides a central connection for multiple media segments on the same subnet. When a hub receives a signal, it is repeated out to all other ports. Hubs operate in half-duplex mode, meaning devices can either send or receive data at any given time.   Hubs are rarely used in networking environments. You should avoid them if possible.   * A switch provides a central connection for multiple media segments on the same subnet. When a switch receives a signal, it forwards that signal only to the port where the destination device is connected.   + Switches use the MAC address to send frames to the destination device.   + Switches operate in full-duplex mode, meaning devices can send and receive data at the same time because transmission paths are dedicated to only the communicating devices.   + When possible, use switches instead of hubs. * A router connects two network segments that have different subnet addresses.   + A router has multiple network connections. Each connection is on a different subnet.   + Routers use the IP address within a packet to move packets between networks. * A bridge connects two segments within the same subnet that use different media types. For example, you can use a bridge to connect wireless clients to wired clients on the same network. * A patch panel is a device that is commonly used to connect individual stranded wires into female RJ45 connectors. For example, you might connect four pairs of wires from a punchdown block to a port on the patch panel. On the patch panel, you then connect drop cables (cables with RJ45 connectors) to the patch panel on one end and a computer on the other end. * An Ethernet over power device allows network communications to be transmitted over existing AC power lines. An Ethernet over power device is plugged in to one AC power outlet, and a second Ethernet over power device is connected to the same AC circuit. These devices multiplex the AC copper power lines to transmit digital network signals at a frequency higher than the AC electrical power already on the circuit. |
| Standards | Ethernet standards identify the transmission speed and the cable type. Data transfer rates range from 10 Mbps (very old Ethernet networks) up to 10 Gbps. Between 100 and 1000 Mbps are the most common speeds for most networks. |
| Distance | Ethernet standards define the maximum distance for cable lengths between two devices.   * The maximum cable length for UTP Ethernet "T" implementations is 100 meters for all standards. * The length for fiber optic cables varies depending on the cable type and specification, but typically ranges from 100 meters to 40 kilometers. |
| Power over Ethernet | Power over Ethernet (PoE) technology is used to distribute electrical power along with network data on twisted-pair Ethernet cabling (CAT 5 or higher). Power is usually supplied by a PoE-enabled Ethernet switch. PoE is commonly used to power network devices that are located where physical access to a power outlet may not be available. For example, a PoE-enabled surveillance camera mounted on a tall pole can be powered via its Ethernet cabling.  You can use a Power over Ethernet (PoE) injector to add PoE capability to regular non-PoE network links. PoE injectors can be used to upgrade existing LAN installations to PoE and provide a solution where fewer PoE ports are required. To upgrade a network connection to PoE, patch it through the PoE injector. Power injection is controlled and automatic. |

6.4.3 Ethernet Standards

Ethernet standards are defined by the IEEE 802.3 committee. The following table compares the characteristics of the various Ethernet standards:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Standard** | **Bandwidth** | **Cable Type** | **Maximum Segment Length** |
| Ethernet | 10BaseT | 10 Mbps (half-duplex) 20 Mbps (full-duplex) | Twisted pair (Cat 4 or 5) | 100 meters |
| 10BaseFL | 10 Mbps (multimode cable) | Fiber optic | 1,000 to 2,000 meters |
| Fast Ethernet | 100BaseTX | 100 Mbps (half-duplex) 200 Mbps (full-duplex) | Twisted pair (Cat5 or higher) Uses 2 pairs of wires | 100 meters |
| 100BaseFX | 100 Mbps (multimode cable) | Fiber optic | 412 meters |
| Gigabit Ethernet | 1000BaseT | 1,000 Mbps (half-duplex) 2,000 Mbps (full-duplex) | Twisted pair (Cat5 or higher) | 100 meters |
| 1000BaseCX (short copper) | Special copper (150 ohm) | 25 meters, used within wiring closets |
| 1000BaseSX (short) | Fiber optic | 220 to 550 meters depending on cable quality |
| 1000BaseLX (long) | 550 meters (multimode) 10 kilometers (single-mode) |
| 10 Gigabit Ethernet | 10GBaseT | 10 Gbps (full-duplex only) | Twisted pair (Cat6, or 7) | 100 meters |
| 10GBaseSR/10GBaseSW | Multimode fiber optic | 300 meters |
| 10GBaseLR/10GBaseLW | Single-mode fiber optic | 10 kilometers |
| 10GBaseER/10GBaseEW | Single-mode fiber optic | 40 kilometers |

You should also know the following facts about Ethernet:

* The maximum cable length for UTP Ethernet "T" implementations is 100 meters for all standards.
* Ethernet standards support a maximum of 1024 hosts on a single subnet.

6.8 Internet Connectivity

As you study this section, answer the following questions:

* In which situations would a PSTN be the best internet option? Why?
* How does DSL enable you to talk on the phone and connect to the internet at the same time?
* What is the difference between BRI and PRI service levels when dealing with ISDN internet?
* Which internet connectivity options send digital signals over telephone lines?
* What is a disadvantage of cellular internet access?
* What is required for a satellite internet connection?
* What are the different ways a device can connect to a cellular internet connection?

In this section, you will learn to:

* Configure a cable internet connection
* Configure a DSL internet connection
* Configure a dial-up internet connection

Key terms for this section include the following:

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Dial-up | A connection that uses a modem connected to the phone line to connect to the internet. |
| Digital Subscriber Line (DSL) | Technology that provides broadband digital data transmission over existing telephone lines. |
| Integrated Services Digital Network (ISDN) | A digital service running over a switched network. The two versions are ISDN BRI and ISAND PRI. |
| Cable television | A network that uses a cable TV connection to create a wide area connection to the internet. |
| Cellular network | A network that uses a cellular phone infrastructure for internet access. |
| Satellite | A network that uses radio signals sent and received from a satellite. |
| Line of sight | Networks that use antennas pointed at a large antenna on land instead of a satellite require the antenna to have a clear line of sight, or unobstructed path, to the main antenna. |

This section helps you prepare for the following certification exam objectives:

|  |  |
| --- | --- |
| **Exam** | **Objective** |
| TestOut PC Pro | 1.5 Given a scenario, configure networking devices  1.5.1 Install and configure a wired and wireless network adapters and cables  1.5.2 Install and configure internet connection devices |
| CompTIA 220-1001 | 2.2 Compare and contrast common networking hardware devices   * Cable/DSL modem   2.3 Given a scenario, install and configure a basic wired/wireless SOHO network   * Cable/DSL modem configuration   2.7 Compare and contrast Internet connection types, network types, and their features   * Internet connection types   + Cable   + DSL   + Dial-up   + Fiber   + Satellite   + ISDN   + Cellular   + Tethering   + Mobile hotspot   + Line-of-sight wireless Internet service |
| CompTIA 220-1002 | 1.8 Given a scenario, configure Microsoft Windows networking on a client/desktop   * Establish networking connections   + Dial-ups   + Wired |

6.8.1 Internet Services

**Internet Services**0:00-0:32

In this lesson, we're going to look at the various internet technologies you can use to connect a home or a small office network to the internet.

We're going to look at only the internet connections you use in a home, home office, or in a small office environment. Larger businesses and corporations use enterprise level internet services that cost thousands of dollars per month. The internet connection types we're going look at use a similar technology but are implemented on a much smaller scale.

**Dial-Up**0:33-1:14

The first internet connection method you're going to look at is dial-up. Dial-up uses the public switched telephone network (PSTN). This type of internet connection requires the computer to have a modem installed. The modem converts digital signals into analog signals that can travel along the public switched telephone network.

With dial-up, the computer connects to a telephone line that is then used to dial into the internet service provider. Dial-up internet is very slow. Today it's very rarely used to connect to the internet. Therefore, this lesson is not going to go into very much detail about it. The main thing that you need to know is that dial-up internet uses a modem to connect to the public switched telephone network.

**Digital Subscriber Line (DSL)**1:15-3:59

The next internet connection type, one that's used quite a bit more than a dial-up connection, is called the digital subscriber line (DSL). Like dial-up, DSL uses the public switched telephone network but it does so in a very different way. With dial-up, the internet connection uses the entire bandwidth of the telephone line. That means that voice calls cannot occur while the computer is using the internet, and vice versa. However, DSL uses a special technique called multiplexing to allow for two simultaneous signals on the same line.

Multiplexing does this by dividing the telephone line's bandwidth into two signal ranges, effectively creating two channels. The first channel is used for standard telephone voice communications. It uses frequency ranges less than four kHz. The second channel is used for DSL communications. It uses frequency ranges four kHz and above.

The division of the phone line into two channels does cause some problems that you have to account for when implementing a DSL connection. For example, traditional telephones are not DSL aware. They aren't able to distinguish between the two channels on the line. They try to accept and process both signals as if they were one. This results in a lot of interference from the DSL communications.

To fix this, you implement a DSL filter on the telephones. This filter blocks DSL communications and allows only telephone frequencies through.

DSL providers frequently offer two types or levels of DSL service. The first type is called asymmetric DSL (ADSL). With ADSL, the upload speeds and the download speeds are not the same. They're asymmetric. That's why you call it asymmetric DSL. ADSL typically provides very fast download speeds but incredibly slow upload speeds. This allows you to access web pages, stream movies, or download large files at relatively fast speeds.

However, uploading files is not nearly so fast. If you are attaching a large file to an email or trying to save files to a cloud server, you'll find that the connection is a lot slower going that direction.

There is a second type of DSL called symmetric DSL (SDSL). SDSL uses the same upload and download speeds. That's why you call it symmetric.

ADSL is much cheaper than SDSL. If faster upload speeds are required for a particular implementation, then use SDSL instead of ADSL.

DSL internet connections require a special device called a DSL modem to connect the local network to the service provider's network.

**Integrated Services Digital Network (ISDN)**4:00-5:38

The next type of internet connection is similar to DSL in a lot of ways. It's called the Integrated Services Digital Network (ISDN). ISDN is kind of halfway between dial-up and DSL. It never really gained much popularity in North America due to several factors. However, it did see widespread implementation in Europe.

Similar to DSL, ISDN connects to the internet using standard phone lines and uses multiplexing to divide those lines into multiple communication channels. ISDN offers two levels of service. The basic level of service is basic rate interface (BRI).

BRI divides the standard phone line into three separate channels. First you have two 64-kbps data channels and one 16-kbps control channel. Just like DSL, voice communications can occur at the same time as the internet connection.

The second level of service is the primary rate interface (PRI). PRI also divides the line into multiple channels but instead of dividing it into just three channels, PRI divides the line into many channels. It can do this because PRI relies on higher quality connections than BRI does. Therefore, PRI can be installed only in locations that have very high quality phone lines installed. PRI provides up to 23 64-kbps data channels and just one 64-kbps control channel.

Thus far in this lesson you've looked at internet connection options that are provided through the phone line. Now, we'll shift gears and look at internet connections that are provided through different connecting media.

**Cable**5:39-6:39

The first is cable internet. Cable internet provides an internet connection using your existing cable TV coaxial cable infrastructure. With cable internet, cable TV companies use a portion of the coaxial cable's bandwidth to provide internet data communications. On the surface, this technology appears similar in many ways to DSL. However, the transmission medium and the network used is very different.

Cable internet providers usually offer faster download speeds than DSL providers. You need to be aware that cable internet bandwidth is usually shared. This means that the total internet bandwidth is shared among all the cable subscribers within a given area. Therefore, the transmission speeds for cable internet during peak times can be much slower than what is promised by the service provider.

Note that DSL provides a dedicated bandwidth. Meaning you don't share your bandwidth with anyone else.

Also, cable internet connections require a connectivity device called a cable modem in order to connect your local network to the service provider's network.

**Fiber**6:40-7:47

The next internet connection type we're going to look at is fiber optic. Fiber optic internet connections have the potential to be the fastest way to connect to the internet. Fiber internet uses fiber optic cabling to connect subscribers to the internet and, as you probably already know, fiber optic communications are extremely fast.

With fiber optic internet, a network of fiber optic cabling is installed within a geographic area to provide internet connectivity to subscribers. With fiber internet, most home subscribers connect to the fiber optic network using standard twisted pair copper cabling and an RJ45 connector. For larger business and corporations, a direct fiber connection is usually provided at a higher price.

Fiber internet can provide speeds much faster than DSL or cable for both upload and download speeds. Because it can't use an existing infrastructure the way cable and DSL do, fiber internet usually isn't available in most areas. In addition, creating a fiber infrastructure is very costly and takes a lot of planning to implement.

The last two internet connection types we're going to look at don't use a wired connection at all. Instead, they use radio waves to connect devices to the internet.

**Cellular**7:48-9:40

The first type is mobile broadband. You're probably already familiar with it. Mobile broadband connections use the cellular phone network to connect devices to the internet. For example, a phone or a tablet that has mobile broadband hardware implemented can connect through the cellular network to the internet. The service provider relays the internet traffic from the mobile broadband network to the internet and vice versa.

Devices that don't have mobile broadband hardware implemented can connect to the internet through a cellular network using several different options. One way is to install mobile broadband hardware in the device itself. For example, a USB mobile broadband adapter could be installed in a notebook system to enable cellular internet access.

Another option is to use an intranet-enabled smartphone as a hotspot. When enabled, the phone essentially creates a small 802.11 Wi-Fi network to which other wireless devices can then connect. Essentially the smartphone becomes a wireless access point and shares its mobile broadband connection.

Another option is to purchase a mobile hotspot from a cellular provider. The mobile hotspot creates a wireless network to which Wi-Fi capable devices can connect.

Cellular internet connections typically offer either 3G or 4G data connections, of which 4G is the fastest. The primary benefit of using a mobile broadband internet connection is simply mobility. Wherever you have phone service, you can have an internet connection.

However, be aware that the speeds provided by mobile broadband usually aren't as fast as those provided by wired internet connections. They also suffer from environmental interference. For example, trying to use a cellular internet connection from within a building or near high-power lines could result in interference issues.

In addition, throughput can be limited by movement. This means that if you're accessing the internet while you're driving down the freeway in a car, your throughput is going to be slower than if you were stationary. Essentially, the faster you move, the worse your connection will be.

**Satellite**9:41-11:33

The second wireless internet connection type is satellite internet. This option uses a satellite dish to connect to the internet via orbiting satellites. This type of internet connection is well suited to remote locations where other types of internet connectivity is not available. In fact, satellite internet is the only internet service that isn't dependent upon your location. It's available anywhere in the world as long as there's a clear line of sight to the sky.

Satellite internet access can provide reasonably fast download speeds. However, upload speeds are usually painfully slow. Satellite internet connections also typically experience excessive latency. This means it takes a long time for data to travel through the satellite network. The signal has to travel a very long distance.

For example, a computer that's using a satellite internet connection sends a request to access a website. That request is sent all the way to a satellite orbiting the Earth, usually at an altitude of about 22,000 miles. The satellite sends that signal back down another 22,000 miles to the provider's receiving system. The requested information then makes the same journey from the web server back to the source computer following the same path.

Because of the distances involved, it takes a long time to complete. This makes satellite internet a very poor choice for time-sensitive applications such as computer games, voice data, and video calls.

These are the different types of internet connectivity that are available for connecting residential and small businesses to the internet. In a lot of locations you'll be able to choose between all of these internet connectivity types. You'll be able to base your decision on speed, cost, and quality of service. However, in some locations you're going to have very limited options. For example, your choice might be limited to either DSL or dial-up. If that's the case, your decision should be pretty easy to make.

**Summary**11:34-11:44

That's it for this lesson. In this lesson, we discussed the options available to you to establish an internet connection. We looked at dial-up, DSL, cable, fiber optic, mobile broadband, and satellite connectivity.

6.8.2 Internet Connection Facts

Regardless of the method, internet connections are made from the subscriber location to an Internet Service Provider (ISP). The ISP might be the cable TV company, the phone company, or another company offering internet access. Internet requests are sent to the ISP, who then forwards the request to the internet.

Most wireless networks are local area networks that are connected to the internet using a wired method (such as DSL or another broadband solution). Some metropolitan areas provide free, city-wide wireless or wired internet connectivity. This type of network is known as a metropolitan area network (MAN). Because many internet service providers also provide other services (such as cable TV or telephone), you can often combine services to get internet access with other services.

The following table lists various services you can use to connect to the internet:

|  |  |
| --- | --- |
| **Method** | **Description** |
| Dial-Up | A dial-up connection uses a modem connected to the phone line to connect to the internet.   * Dial-up connections use the public switched telephone network (PSTN). Phone lines are sometimes referred to as POTS (plain old telephone service). * Multiple standards define how to send digital data over the analog phone lines at various speeds and compression ratios. * Dial-up connections are available anywhere a telephone line exists. * Data transfer rates include 28.8 Kbps, 33.3 Kbps, and 56 Kbps. * Dial-up connections cannot be used for both voice (phone calls) and data at the same time. |
| Digital Subscriber Line (DSL) | DSL provides broadband digital data transmission over existing telephone lines.   * DSL divides the telephone line into multiple channels. One channel is used for analog voice, while the remaining channels are used for digital data. * Filters are used to separate the analog voice data from digital data. * Several DSL standards exist, including ADSL, SDSL, and HDSL (collectively referred to as xDSL). * Depending on the type of DSL used, you can use the same line for simultaneous voice and data. * DSL is not available in all areas; the service location must be within a fixed distance of telephone switching equipment. |
| Integrated Services Digital Network (ISDN) | ISDN is a digital service, running over a switched network.   * There are two versions of ISDN:   + ISDN BRI divides the regular copper telephone line into three channels:     - 2 64-Kbps bearer (B) channels can transfer data up to 128 Kbps (data compression increases the data transfer rate). Only one B channel is used during phone use reducing maximum speed to 64 Kbps.     - 1 16-Kbps delta (D) channel for connection control.   + ISDN PRI requires different cables to be installed rather than the regular phone lines. The cable is divided into 24 channels:     - 23 B channels (each at 64 Kbps) for data transmission.     - 1 D channel (at 64 Kbps) for connection control. * ISDN is not available in all areas; subscribers are required to be within a certain proximity of telephone company equipment. * ISDN is more common in Europe than in the United States. |
| Cable | Cable networking uses a cable TV connection to create a wide area connection to the internet.   * A cable modem (router) connects the computer to the cable network for sending networking signals. * The same cable line is used to carry networking and cable TV signals, although in some cases a separate line is installed for internet access. * Cable networking requires the installation of a cable TV line to your location if one does not exist. |
| Cellular | Cellular networking uses the cellular phone infrastructure for internet access.   * Mobile phones with digital data plans use cellular signals to connect to the internet. * Devices can connect to a cellular internet connection in a variety of ways:   + Many smart phones use a technique known as *tethering* to provide cellular internet to another device. Tethering typically requires the smart phone to be connected via a USB cable.   + A mobile hotspot is a cellular device that provides internet access by creating a small Wi-Fi network to which multiple devices can connect. Most smart phones have built-in mobile hotspot functionality.   + Some mobile devices (e.g., notebook computers and tablets) have integrated cellular antennas.   + USB cellular adapters can be connected to most mobile devices to provide cellular access. * Cellular networking is a truly mobile solution. You can often be moving and still have internet access without manually having to reconnect. * Internet access is limited to areas with cell phone coverage. Coverage will be dictated by the service provider's network.   Cellular networks used for voice and data include the following types:   * 2G (second generation) networks were the first to offer digital data services. 2G data speeds are slow (14.4 Kbps) and were used mainly for text messaging and not internet connectivity.   + 2.5G was an evolution that supported speeds up to 144 Kbps.   + EDGE (also called 2.75G) networks are an intermediary between 2G and 3G networks. EDGE is the first cellular technology to be truly internet compatible, with speeds between 400 and 1,000 Kbps. * 3G (third generation) offers simultaneous voice and data. The minimum speed for stationary users is quoted at 2 Mbps or higher. * 4G (fourth generation) offers minimum speeds of around 38 Mbps, with up to 100 Mbps possible. |
| Satellite | Satellite networking uses radio signals sent and received from a satellite. Satellite networking is divided into two categories, Geostationary Satellites (GEOs) and Low Earth Orbit Satellites (LEOs). Geostationary Satellite (GEO):   * Uses a transmitter with an antenna (dish) directed skywards to a satellite * Requires line-of-sight to the satellite (dish placement is crucial) * Is affected by mild atmospheric and weather conditions (fog, rain, or snow can disrupt service) * May have a long delay time (latency) between requests and downloads * Can be a portable solution for cars or trucks with an attached satellite dish * Provides nearly 100% global coverage   Low Earth Orbit Satellite (LEO):   * Closer to the Earth than GEOs * Orbits at a distance of about 1200 miles above the Earth * Simpler and cheaper to make than GEOs * Fast, accurate communication and service * Coverage area is limited; needs more satellites to cover a bigger area   Some satellite internet access solutions are limited to download only. Another solution, such as dial-up, is required to provide upload capabilities. |
| Line of Site | Line of site internet access (also called fixed wireless broadband) is similar to satellite internet; however, instead of antennas being directed to a satellite in orbit, they are pointed at a large antenna on land. The antennas use radio signals--typically microwaves--to transmit and receive data. Line of site internet:   * Requires a direct line of site between two fixed antennas. A single, large antenna provides connections for all subscribers in an area * Provides internet access without needing to run cables or lines to each subscriber's premise * Can provide internet to remote areas by installing a single antenna * Ss affected by weather conditions, similar to satellite networking * Offers speeds of up to 1520 Mbps |
| Voice over IP (VoIP) | Voice over IP (VoIP) sends voice phone calls using the TCP/IP protocol over digital data lines.   * With VoIP, phone calls are made through your internet connection, not through a phone line. * When you make a phone call, the call is converted into digital data and sent through the internet. * VoIP is provided by many ISPs to replace existing analog telephone lines (even using the same phone number). * Desktop computers can be used to make VoIP calls by using VoIP software and the computer's microphone and speakers. The most common example of this is the VoIP application Skype. |

6.8.5 Create a Dial-up Internet Connection

**Create a Dial-Up Internet Connection**0:00-0:15

In this demonstration, we're going to discuss configuring a dial-up connection. Dial-up connections aren't used very often anymore, but there are still some situations where they're necessary, so we're going to walk through the steps you take to set one up.

**Adding a Connection**0:16-2:57

Now, notice, down here in my Notification area, when I hover over my network connection icon, I'm not connected. I have no network connection, wired or wireless. I have no access to the internet. So, to connect to the internet, I'm going to use a modem to dial another modem at my ISP site and establish a connection through the public switched telephone network.

I've already connected a modem and the necessary drivers to this system. I can use it to dial another modem at my ISP site through the telephone network. To do this, we need to click on our Windows icon, go to Settings, and then access Network and Internet. Within the Network and Internet settings, click on Dial-up in the left menu, here. Then we have to set up a new network connection, so I'll click this option and then Connect to the internet. It says we can use this option to set up a dial-up connection. That's what we want to do, so I'll click Next.

Now I have to specify how I want to connect. Do I want to connect using a DSL or cable connection, or do I want to establish a dial-up connection through the public switched telephone network? That's what we're going to do in this demonstration, so I'll click Dial-up.

In this screen, we have to configure the connection to the internet service provider's modem bank. The first thing we have to specify is the phone number. We have to specify our username and a password for connecting. You have to get this information from the ISP. In this case, our ISP phone number is 801-555-1234. My username on the ISP's network is iperson, and I'll enter my password. I have an option down here to remember this password. This option is very convenient. If I turn it on, then the next time I go to dial this connection, Windows will remember the password. However, it does represent a little bit of a security risk because that means someone else could potentially dial in and use my ISP account, so you have to decide whether you want to do that or not. On a desktop system, this option might be acceptable as long as the computer is kept in a secured area.

If you're dealing with a notebook system, I would turn that option off because you never know when you're going to accidentally leave your notebook in a taxi cab or a hotel room. I'm going to turn this option off.

Then we have to give the connection a name. Let's just call it My ISP. And then we have to decide whether we want to allow other users on the system to use this connection as well. Now, this isn't network connection sharing. All this does is allow the other user accounts that are configured on the system to also have this dial-up connection available in Network and Internet Settings and use it to dial in.

I'm going to turn that option off because I only want my iperson user account to be able to use this connection to dial in to my ISP. Create. So, the dial-up connection is defined. I'll click Close.

**Establish a Connection**2:58-3:50

Now, if I want to establish a dial-up connection, I come down to my network icon in the Notification area. I click on it. I notice that there's an option to dial my ISP. I'm going to go ahead and click it. And then, under dial-up, we'll click My ISP and then click Connect.

Because I specified that I did not want Windows to remember my password, I have to enter it here before I can go on, but the username and the number to dial were in the network connection profile. So, with that, I can click Dial, and then the connection will go ahead and dial the number and establish a network connection with my ISP.

You can also configure a dial-up connection through Control Panel. Let's come down here and type Control Panel in the search bar. Next, let's click on Network and Internet, and then Network and Sharing Center. Let's click on Set up a new connection or network, and then we can continue with the steps we demonstrated above.

**Summary**3:51-3:54

That's it for this demonstration. In this demo, we talked about how to set up a dial-up network connection.

Test Out Logo

**TestOut PC Pro***English 6.0.4*

Home

Outline

**Actions**

Click to View Actions Menu

Copyright © 2019

TestOut Corporation

All rights reserved.

Powered by Lab Sim

Chapter 6: Networking

6.9 Network Utilities

Copy textPrint page

As you study this section, answer the following questions:

* What are the similarities and differences between **ping** and **tracert**?
* When would you use **traceroute** instead of **tracert**?
* What information can you get from the **netstat** command?
* Which utilities can be used to perform remote management of servers?
* What is the difference between the **ifconfig** and **iwconfig** commands?
* Why should you use SSH over Telnet?

In this section, you will learn to:

* Explore configuration information
* Use **ifconfig**

Key terms for this section include the following:

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Ipconfig** | A Windows command that displays IP configuration information for network adapters. |
| **Ifconfig** | A Windows and Linux command that displays the installed network interfaces and the current configuration settings for each interface. |
| **Ping** | A command that sends an ICMP echo request/reply packet to a remote host. |
| **Tracert/traceroute** | A command similar to **ping** that also shows the path between the two devices. Use **tracert** on Windows and **traceroute** on Linux and Mac OS. |
| **Nslookup** | A command that resolves the IP address of the specified hostname. |
| **Netstat** | A command that displays IP-related statistics. |
| **Nbtstat** | A command that diagnoses issues regarding NetBIOS over TCP/IP. |
| Telnet | A remote server management network protocol. |
| Secure Shell (SSH) | A protocol similar to Telnet that also encrypts all communications and is much more secure. |

This section helps you prepare for the following certification exam objectives:

|  |  |
| --- | --- |
| **Exam** | **Objective** |
| TestOut PC Pro | 2.4 Given a scenario, configure PC networking  2.4.4 Use network utilities  4.3 Given a scenario, troubleshoot networking  4.3.2 Use networking utilities to view, test, and troubleshoot network configuration, communication, and connectivity issues |
| CompTIA 220-1002 | 1.4 Given a scenario, use appropriate Microsoft command line tools   * ipconfig * ping * tracert * netstat * nslookup   1.9 Given a scenario, use features and tools of the Mac OS and Linux client/desktop operating systems   * Basic Linux commands   + iwconfig/ifconfig   2.5 Compare and contrast social engineering, threats, and vulnerabilities   * DoS |

6.9.1 Network Utilities

**Network Utilities**0:00-0:29

There are a handful of TCP/IP network utilities that every PC technician should know how to use. These utilities are valuable when troubleshooting network issues. In this lesson, we're going to take a look at these utilities and show you what they do and how they can help identify networking issues.

Before we start, note that all these utilities are called command line utilities. This means they are run from within the command line and not the graphical interface of the operating system.

**Ping**0:30-2:12

The first utility that we're going to look at is ping. You can use ping to test whether or not a particular host on a TCP/IP network is reachable. If the ping succeeds then you know two things. First, the other host is up and running. Second, that the network connection between the two hosts is functioning properly.

Ping works by sending out an ICMP echo request packet to the target host. When the host receives the echo request it replies with an echo response. The good thing about ping is it can also be used to test the latency between two hosts. When you use ping, the sending host tracks the time it takes, in milliseconds, to receive the echo response from the target host. Ping also tracks packet loss. This is useful for several reasons.

For example, you ping a host on a network and the time it takes to receive the echo response is really long. Not only that, but only half of the ping requests make it to the other host; the rest are lost. What this tells you is that there is a problem on the network between the two hosts. It might be a bad cable or a faulty network card.

Ping does have some limitations, however. For example, a failed ping request doesn't always mean the target host is down. Some host-based firewalls, such as the one included with the Windows operating system, are designed to ignore ICMP requests.

Some routers also are designed to ignore ICMP requests. This protects against denial of service (DoS) attacks. A DoS attack attempts to bring down a target system by flooding it with thousands of ICMP responses in just a few seconds. To prevent this attack, firewalls and routers simply ignore all ICMP traffic.

If you want to be able to ping these systems on the network, it is possible to configure firewalls and routers to permit ICMP traffic.

**Tracert/Traceroute**2:13-3:55

The next TCP/IP utility is called traceroute. On Windows systems this utility uses the tracert command. Linux and Mac OS use the traceroute command.

Traceroute is similar to the ping utility in that it also uses ICMP echo requests and reply packets to test network connectivity. However, traceroute does this in a way that is a little different.

Traceroute tracks each router that packets pass through in order to reach the destination host. Using traceroute within a network isn't very helpful since the packets probably won't go through any routers. Where traceroute shines is when you use it to test a connection on another network.

For example, you use the traceroute utility from a host on the West Coast and are contacting a host on the East Coast. By using traceroute, you can see each router that the packet uses to reach the target system. Because of the way TCP/IP works, the packet may not be sent to the same routers each time. It might not even use the same number of routers. It's possible that one traceroute uses four routers and the next traceroute uses five or six.

By using traceroute, you can create a map between two points and identify the routers that are crossed to reach a specific destination. This allows you to identify where a connection fault may be. For example, a ping to one of your remote computers fails. This doesn't tell you much. You don't know if it's a problem with your network or the remote network.

So you use the traceroute utility and find that the ICMP packets fail after the second router hop. This tells you that the problem is somewhere between the second and third router.

**Ipconfig/Ifconfig**3:56-4:49

Next is the ipconfig utility. Windows systems use the ipconfig utility to obtain TCP/IP configuration information. When you use ipconfig, the IP address, subnet mask and default gateway of the primary Ethernet adapter will be displayed. This is useful when troubleshooting network connections. By using this utility you can quickly identify whether or not the Ethernet adapter is configured properly.

For example, if you were to run ipconfig and the IP address started with 169.254 you would know that APIPA's being used and there is a problem with DHCP. Either the server is down or the host isn't able to contact it. Or, maybe the network uses a subnet mask of 255.255.0.0 but the output from ipconfig is 255.255.255.0. This tells you the subnet mask is configured incorrectly.

On Mac OS and Linux systems, the ifconfig is used to display TCPIP configuration information.

**Nslookup**4:50-5:24

The next utility is nslookup. The syntax for using the nslookup utility is nslookup followed by a domain name such as "google.com." When you use nslookup, it displays the DNS server information and the IP address that the server has resolved to the specific domain name. If you enter an IP address, nslookup returns the domain name associated with the specific IP address.

You can use this utility to test two things. First, it tests that the DNS server is reachable. Second it tests if domain names are resolving properly.

**Netdom**5:25-5:45

The last utility is netdom. Netdom is a Windows administration tool that is typically used only on a server running Windows Server 2008 or later. It allows a network administrator to add hosts to Active Directory domains from the command line. If netdom is installed on a host, you can use it to join the host to a specified Active Directory domain.

**Summary**5:46-6:11

As you can see, these TCP/IP utilities are an invaluable addition to your troubleshooting toolbox. By understanding how each of these utilities work, you can use them to troubleshoot practically any networking issue. And remember, ipconfig and tracert are used on Windows systems. On Linux and Mac OS systems, the commands are ifconfig and traceroute. The functionality of both is the same but the command syntax is different.

6.9.2 Use ipconfig and ifconfig

## Use the ipconfig Command on Windows 0:00-0:17

In this demonstration, we're going to spend some time looking at several commands that you can use to verify the networking configuration of a work station. We're going to look at the IP config command on Windows and then we're going to look at the ifconfig command on Linux.

## Use ipconfig on Windows 0:18-6:27

So let's begin with Windows. Now if I were to come down to my search field on this Windows 10 system and type the command that I want to run, ipconfig. Notice that the IP config command is listed in the search results and if I click on it, it runs an exits so fast that I can't actually see the output from the command. Making it fairly not useful. So that's what we call the wrong way to run the IP config command. The right way is to come down to your Windows icon, right click, and then click on command prompt and then at the command prompt type the ipconfig command. Because we're running it within the command prompt we can actually see the output from the command. Now I'm going to make this window just a little bit bigger.

So we can see everything. Now notice that there are three different network adapters listed in the output of the IP config command. The first one is an Ethernet adapter and its name is Ethernet. We also have a tunnel adapter for isatap and we also have a tunnel adapter for Teredo. You might be asking, "Wait a minute. I only have one network interface in this system. How come three are showing up?" Well it's because these two are actually not real network interfaces. They're virtual network interfaces that are used for IPv6 to IPv4 compatibility.

So, these are not real network interfaces and for now you can kind of ignore them. They'll make more sense when we talk about IPv6. For now, we want to focus on this hardware adapter that's installed in the system. There is a physical network adapter installed that is connected to an Ethernet network and that's represented by the Ethernet adapter named Ethernet. Underneath this network adapter we can view information about it. We can view its DNS suffix which is set to eastsim.com. We can see that it has a link local IPv6 address assigned to it. It also has an IPv4 address assigned to it, 10.0.0.25. It has a subnet mask of 255.255.0 and the default gateway is 10.0.0.1

Now this network interface is set up to use DHCP to get this IPv4 addressing information. When the system first comes online, it will send out a DHCP discover packet trying to locate a DHCP server somewhere on the network. The appropriate DHCP server will respond. The two will negotiate and an IP address will be assigned and it will be assigned for a certain period of time, called the DHCP lease. Within that DHCP lease we should have an IPv4 address, we should have a subnet mass, we should have the default gateway router address, and we should also have a DNS server address. Now you'll notice that some of this information is not actually displayed in the output of the IP config command.

For example, we don't know which DHCP server provided this IPv4 address. We also don't know what the DNS server address is. So how do you view that information? You actually have to run the IP config command and use the Forward/All option with the command. This will cause the ipconfig command to display extended information about the network adapter. I'm going to go ahead and press Enter. Now you'll notice that a lot more information is displayed. Let's scroll up just a little bit here. First of all, under the windows IP configuration we can now see the host name of the system. This system is named Win10. Here's our DNS suffix which we saw before. Scrolling down we also see the DNS suffix which is eastsim.com

We also see the type of Ethernet hardware that's installed in the system to create this network connection. It's an Intel82574L gigabit Ethernet network connection. We also see the MAC address of this network adapter. We see that DHCP is enabled. Now we see some of the same information that we saw before as well. We see the IP address, we see the Subnet mask, and we see the default gateway router address that we saw with just the DHCP command alone, but notice that we see a lot more information about the DHCP lease. For example, we see the date and time that the DHCP lease was created, today at 10:23AM and it's going to expire at some point.

So at 12:14PM this lease is going to expire, in which case this system will have to contact the DHCP server and renew the lease so that it can keep using this IP address. Also notice that we now see the IP address of the DHCP server that provided this lease. It also has an IP address of 10.0.0.1 and we also see the IP address of the DNS server that's going to be used by this work station as well. To resolve DNS names into IP addresses as you can see that the config /all command provides a lot more information than just ipconfig alone. Now there's more you can do with ipconfig besides just view information.

Now remember earlier I said that this system is configured to use DHCP therefore when the adapter comes online it's going to contact the DHCP server and establish a DHCP lease. Well we can use the ipconfig command to actually release the current DHCP lease that it received from the DHCP server to do this you type ipconfig like we did before. This time use the release option. I hit enter, you'll notice that we lose our IP addressing information, we no longer have an IP address assigned to the system. We don't have a subnet mask, we don't have a default gateway router address, we don't have a DNS server address anymore either and you can tell that down here by the networking icon, notice that we have a yellow triangle with an exclamation point indicating that we don't have any addressing information and we have no internet access anymore.

In addition to releasing a DHCP lease the ipconfig command can also be used to renew a DHCP lease. Instead of using release, this time we'll use renew. So to release a DHCP we use ipconfig /release and then to renew a lease we type ipconfig /renew. When I do Windows will go out and contact the DHCP server and say "hey I need an IP address" the DHCP server will respond and notice that we now have the same IP addressing information assigned that we had before. 10.0.0.25 255.255.255.0 for the mask and 10.0.0.1 for the default gateway. So that is how you use ipconfig on a Windows workstation to manage IP addressing.

## Use ifconfig on Linux 6:28-12:49

Let's now switch over to a Linux system and use the ifconfig command. Now the ifconfig command on Linux functions in much the same way as the ipconfig command on Windows systems. Just like on Windows we run the ifconfig command on Linux from the command line, so, first thing I need to do on this Linux is open up a terminal session. On Windows we call it the command prompt, on Linux we call it a terminal session, and they're basically the same thing though. So I'm going to type term in my search field and then click on GNOME terminal.

Now I'm currently logged in to the system as my rtracy user, rtracy is a standard user and watch what happens if I try to type the ifconfig command as a standard user on Linux, it says, yeah you know what you might need superuser privileges to run this command. Now on Linux the name of the superuser is root. So before we run the ifconfig command we should switch to the root user, I'll type su - switch to my root user account I'll provide the root users password. Now I'm currently logged in as the root user which is a superuser instead of my standard rtracy user account. Now I can type the ifconfig command and when I do I see two network interfaces displayed in the output of the command the first one is named ENS32 and the second is named LO.

Now just like with the output of the ipconfig command, in this output of ifconfig we see one virtual network adapter and one hardware network adapter understand that all Linux systems will have a virtual network adapter installed and configured called LO, this is called the loopback adapter. The loopback adapter is used for services running on the same Linux system to communicate with each other without having to know a physical IP address. Just as we kind of ignored the IPv6 virtual adapters on the Windows system, we're going to kind of ignore the LO network adapter on this Linux system. The adapter we do want to focus on is this one right here, ENS32.

Now before we go any farther we need to talk about network interface naming on Linux. Back in the old days of Linux which really wasn't that long ago, about four or five years ago. It didn't matter what type of interface you connected to the system they were all named the same. The first network adapter in the system was named ETH0, that's E-T-H-0 the second one was ETH1 the third one was ETH2 and so on. That's no longer the case. With modern Linux distributions we used what's called predictable network naming. Instead of just naming the first interface in the system ETH0, what the Linux operating system does is look at the type of network interface, is it a wireless interface? Is it a wired interface? It looks at how that interface is installed in the system. Is it installed in a PCI slot? Is it integrated in the motherboard? Is it connected with a USB connector? And then it will use that information to dynamically generate an appropriate name for that interface. In this case the name that came up was ENS32.

Now as we said before this network name represents a hardware interface in the system, we know that because it tells us that it's an Ethernet interface right here. This is a wired Ethernet interface that's connected to an Ethernet switch. Here's the MAC address of the interface right here. Here's the IP address that's currently been assigned to this interface, 10.0.0.250. Here's the broadcast address for my local network segment. Here's the subnet mask that's been assigned to this interface. Now just like with the Windows system, this Linux system has IPv6 configured on it as well and so a link/local IPv6 address has been automatically assigned to this interface, I know that it's a link/local address because it tells me over here that the scope is link. Down here we learn that the interface is up, meaning that it's able to transmit and receive frames on the Ethernet network. Down here it tells us how many packets this interface has received. Here's the total number.

It tells us any errors or drops that were encountered as it was receiving packets as well. It didn't have errors but 39 packets were dropped. We can also see statistics about transmitted packets, you can see that we have the number transmitted and similar statistics displayed for transmits as well such as errors and drops. Here's the number of collisions that this network interface has detected on the network and this is a switched Ethernet network so we shouldn't be seeing any collisions at all and that is the case. And down here we see the number of bytes that have been received by this network interface and the number of bytes that have been transmitted by this network interface.

So as you can see the ifconfig command displays a lot of information much like the ipconfig command did on Windows. However there are a couple of parameters that aren't displayed in the output of ifconfig, for example we don't know what the IP address of the default gateway is nor do we know what the host name of this system is. To find out the host name of the system we type the host name command at the command prompt and we see that the host name of this system is proxy. Which you'll notice is also included in the command prompt itself. If we want to see what the default gateway router address is for this system we type "route" and the IP routing table is displayed and we see that the default gateway has an IP address of 10.0.0.1.

Now just as we could disable and re-enable a network interface on Windows using ipconfig we can do a similar thing with the ifconfig command on Linux but the two commands you use are related to ifconfig but they instead are ifdown to take the interface down and ifup to bring the interface back online. For example if we wanted to take down the ENS32 interface I would type 'ifdown EFS32', hit Enter. Oops, I typed it wrong. And now if I type the ifconfig command we see that ENS32 is gone, it's not even listed the only interface we have currently running is our virtual loopback adapter. To bring that interface back online I type 'ifup' followed by the name of the interface, ENS32. Wait just a minute while the interface comes back online.

Alright and you'll notice there's a little bit of an error listed here. We don't actually have to worry about it, one of the things about working with Linux is that the programmers who write these utilities love to display error messages on the screen whether they're really actually serious or not this is actually not a serious error message. In fact, if we were to type ifconfig again we should see that the ENS32 interface is back online and that it has an IP address assigned to it along with a subnet mask and everything is working great.

## Summary 12:50-13:00

That's it for this demonstration. In this demo, we talked about how to use command line tools to monitor network interface statistics. We first looked at the ipconfig command on Windows and then we looked at the ifconfig, ifdown and ifup commands on Linux.

6.9.9 TCP/IP Utilities

The following table describes the various command utilities you can use to troubleshoot network issues:

|  |  |
| --- | --- |
| **Utility** | **Description** |
| **ipconfig** (Windows OS) | **ipconfig** displays IP configuration information for network adapters. Use the **ipconfig** command as follows:   * Use **ipconfig** to view IP address, subnet mask, and default gateway configuration. * Use **ipconfig /all** to view detailed configuration information, including the MAC address and the DHCP server used for configuration. * Use **ipconfig /release** to release the IP configuration information obtained from the DHCP server. * Use **ipconfig /renew** to request new IP configuration information from the DHCP server. * Use **ipconfig /displaydns** and **ipconfig /flushdns** to view and manage the local DNS cache. The first command displays the contents of the local DNS cache that Windows maintains and updates every 24 hours. The second option flushes (or removes) all the entries in the current DNS cache. If the IP address of a network server is changed, your local cache will contain the old IP address until the cache is updated or the **flushdns** option is used. |
| **ifconfig** (Linux/macOS) | **ifconfig** is used on Linux and macOS systems and displays the installed network interfaces and the current configuration settings for each interface, including the MAC address, IP address, broadcast address, and subnet address. Use the **ifconfig** command as follows:   * Use **ifconfig *[interface\_name]* down** to disable the specified network interface. * Use **ifconfig *[interface\_name]* up** to enable the specified network interface.   Use the following utilities to display additional networking information not provided by ifconfig:   * The **hostname** command displays the system's hostname. * The **route** command displays the default gateway configuration settings.   On Linux systems, the **iwconfig** command is used to display information about wireless network interfaces. |
| **ping** | **ping** sends an ICMP echo request/reply packet to a remote host. A response from the remote host indicates that both hosts are correctly configured and a connection exists between them.  You can ping a host by IP address or use the DNS name. When the DNS name is used, the computer must look up the corresponding IP address before performing the ping test.   * **-a** looks up the hostname from a given IP address. * **-t** performs a continuous ping test (press **Ctrl** + **C** to stop sending the ping tests). * **-l *[size]*** specifies the packet payload size (in bytes) to use in the test. This can help determine whether packets above a certain size are being lost. |
| **tracert**, **traceroute** | **tracert** is similar to the **ping** utility because it tests connectivity between devices; however, **tracert** also shows the path between the two devices. Responses from each hop on the route are measured three times to accurately report how long the packet takes to reach the specific host and then return.   * On a Windows system, use the **tracert** command. * On Linux and macOS systems, use the **traceroute** command. |
| **nslookup** | **nslookup** resolves (looks up) the IP address of the specified hostname. It also displays additional name resolution information, such as the DNS server used for the lookup request. |
| **netstat** | **netstat** displays the following IP-related statistics:   * Current connections * Incoming and outgoing connections * Active sessions, ports, and sockets * The local routing table |
| **nbtstat** | **nbtstat** is used to diagnose issues regarding NetBIOS over TCP/IP. You can use the following options with **nbtstat**:   * **-c** displays the NetBIOS cache of remote machine names and their IP addresses. * **-n** displays NetBIOS names that have been registered on the local system. * **-r** displays names resolved by broadcast and via WINS. * **-R** clears and then reloads the remote cache name table. * **-S** displays current NETBIOS sessions with the destination IP addresses. * **-s** displays current NETBIOS sessions by NETBIOS names. |
| Telnet | The Telnet utility is used for remote server management.   * The Telnet protocol must be running and configured on the remote server in order for a Telnet session to be established. * By default, Telnet does not encrypt transmissions (they are sent as clear text). * Telnet is mostly used by specialized industrial and scientific devices.   In addition to sending transmissions in clear text, there are several well-known vulnerabilities in the Telnet protocol. Because of this, Telnet should not be used when sending sensitive information. |
| SSH | Like Telnet, the SSH utility is used for remote server management; however, SSH encrypts all communications and is much more secure.   * SSH can be used to remotely log onto a server and complete configuration tasks. * In order to establish an SSH session, the server must have the SSH process running and configured to allow remote connections. * Use the following syntax to establishing an SSH connection: **ssh *[username]*@*[server\_address]*** |

Chapter 7: Wireless Networking

7.1 802.11 Wireless

As you study this section, answer the following questions:

* What type of device is required to create an infrastructure wireless network configuration?
* What is the purpose of an SSID?
* Which wireless standards are typically backwards compatible with 802.11g?
* Two access points are part of the same wireless network. Should they use the same channel, or a different channel? Why?
* How does MIMO differ from channel bonding?
* What happens to the speed of a wireless connection as you move away from the access point?
* Which authentication and security method should be used on a wireless network?
* Why should default security settings be changed when dealing with wireless networking?

In this section, you will learn to:

* Connect to a wireless network
* Create a home wireless network
* Secure home wireless network
* Configure a wireless profile

Key terms for this section include the following:

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Ad hoc | A temporary peer-to-peer mode network. |
| Infrastructure wireless network | An infrastructure wireless network employs an access point that functions like a hub on an Ethernet network. |
| Service set identifier (SSID) | The network name. |
| Multiple-input multiple-output (MIMO) | An enhancement that allows multiple antennas to use the same radio frequency. |
| Channel bonding | Combining channels into one to increase bandwidth. |
| Multi-user multiple-input multiple-output (MU-MIMO) | An enhancement to MIMO that allows a set of devices with individual antennas, rather than just one device with an antenna, to communicate with each other. |
| Dual-band access point | A network devices that connects Wi-Fil devices to forma  Wi-Fi network. |
| Open authentication | An token-based authentication standard that requires a MAC address to use. |
| Shared key authentication | A wireless network access protocol that uses WEP. |
| 802.1x authentication | An authentication standard that uses username/passwords, certificates, or devices such as smart cards to authenticate clients. |
| Wired Equivalent Privacy (WEP) | An optional component of the 802.11 specifications. |
| Wi-Fi Protected Access (WPA) | A wireless security based on 802.11i specifications. |
| Wi-Fi Protected Access II (WPA2) | A wireless security that adheres to 801.11i specifications. |

This section helps you prepare for the following certification exam objectives:

|  |  |
| --- | --- |
| **Exam** | **Objective** |
| TestOut PC Pro | 1.5 Given a scenario, configure networking devices  1.5.1 Install and configure a wired and wireless network adapters and cables  1.5.2 Install and configure internet connection devices |
| CompTIA 220-1001 | 1.2 Given a scenario, install components within the display of a laptop   * Types   + WiFi antenna connector/placement   2.3 Given a scenario, install and configure a basic wired/wireless SOHO network.   * Wireless settings   + Encryption   2.4 Compare and contrast wireless networking protocols.   * 802.11a * 802.11b * 802.11g * 802.11n * 802.11ac * Frequencies   + 2.4Ghz   + 5Ghz   2.5 Summarize the properties and purposes of services provided by networked hosts.   * Server roles   + Authentication server   3.9 Given a scenario, install and configure common devices.   * Laptop/common mobile devices   + Wireless settings |
| CompTIA 220-1002 | 1.8 Given a scenario, configure Microsoft Windows networking on a client/desktop   * Establish networking connections   + Wireless   2.2 Explain logical security concepts.   * Certificates   2.3 Compare and contrast wireless security protocols and authentication methods.   * Protocols and encryption   + WEP   + WPA   + WPA2   + TKIP   + AES * Authentication   + RADIUS   + TACACS |

7.1.1 Wireless Networking

**Wireless Networking**0:00-0:28

In addition to copper wires or fiber optic cables, networks can also use radio waves as the communication medium. These types of networks are called wireless, or Wi-Fi networks.

Wireless networking has become commonplace in both the home and at work. Practically every network uses some sort of wireless component. Because of this, it's important that you know the structure of a Wi-Fi network and the characteristics of various wireless technologies.

**Wireless Ad-hoc Network**0:29-1:07

Wireless networks can typically operate in one of two modes. The first mode is called ad-hoc mode.

With ad-hoc mode, there's no central connection point. Instead, hosts connect directly to each other using a wireless network interface card. Each host is responsible for keeping track of communications with other devices. In addition, each host can be used to forward data for other hosts.

For example, a host could use two other hosts as a communication channel to communicate with another device.

A wireless ad-hoc network is considered a decentralized wireless network because it doesn't rely on any existing wireless infrastructure. It can be created anywhere on the fly.

**Infrastructure Implementation**1:08-1:26

The second mode is called infrastructure mode. With infrastructure mode, each wireless host connects to a central connecting device called a wireless access point (AP). In this configuration, hosts communicate with each other through the AP instead of directly with each other. The AP behaves much in the same way as a wired switch in this mode.

**Wireless Access Points**1:27-1:55

The wireless AP, plays a very important role in a network. Not only does it control communication between devices, but it is also able to bridge the wireless network with a wired network.

For example, an access point can be connected directly to the internet, allowing online communications for wireless devices. The AP can also be connected to an Ethernet switch, providing access to the entire network. It's also possible to connect multiple access points together in order to extend the range of a wireless network.

**SSID**1:56-2:30

There are few characteristics unique to wireless networks that you need to be aware of. The first is what's called the SSID, the Service Set Identifier.

The SSID is configured on the wireless access point and is used to identify a wireless network. For example, this access point can be configured with an SSID of Coffee Shop Wi-Fi. Wireless devices that are in range of this access point would see Coffee Shop Wi-Fi as an available wireless network.

The SSID is essentially the name of the wireless network. It helps differentiate the access point from other access points. It's also used when configuring wireless devices.

**IEEE 802.11 Specification**2:31-5:27

Another characteristic is the standard that the wireless network uses to communicate.

Remember, wireless networks use radio waves to communicate and radio waves come in a lot of different forms. Because of this, a group known as the Institute of Electrical and Electronics Engineers, or IEEE, got together and created the IEEE 802.11 specification. The 802.11 specification is used to define the standards and characteristics of wireless networks.

Over the years, the 802.11 specification has been improved upon and different versions have been released. These versions are identified by appending a letter to the 802.11 specification. For example, the 802.11g specification is the third version of the 802.11 specification. 802.11ac was created in 2013 and is one of the more recent iterations.

Each new 802.11 standard that is released typically improves on the previous version in speed, efficiency, and also security. In addition, each standard operates in a specific frequency.

Depending on the standard, wireless networks can operate in either the 2.4 GHz frequency or the 5 GHz frequency. Knowing which frequency a wireless network operates in is important for several reasons.

First, other devices might use the same frequency and cause interference. A cordless phone can operate in the 2.4 GHz frequency and affect wireless communications. In addition, networks that operate in the 5 GHz frequency aren't compatible with devices that can operate only in the 2.4 GHz frequency, and vice versa.

Transmission Speed and Distance

The 802.11 specification also identifies the transmission speed and distance specifications of a wireless network. Some of the original 802.11 specifications were very slow. For example, wireless networks using 802.11a had a maximum speed of 54 Mbps. In today's networking world, that is astronomically slow.

Luckily, newer specifications have implemented special techniques to achieve much faster transfer speeds. One such technique is MIMO, multiple-input multiple-output.

MIMO is a technique that uses up to eight antennae to create dedicated receive and send channels. For example, four antenna could be used only for sending, and the remaining four only for receiving. MIMO not only increases transmission speeds, but also the transmission distance.

Older specifications use only one antenna, which could either send or receive, but not at the same time.

Channel bonding is another technique that has been implemented in order to achieve faster speeds. Wireless networks broadcast only in a specific number of channels. For example, the 2.4 GHz frequency has 14 broadcast channels.

Other specifications broadcast only in a single channel, such as channel three. However, newer wireless networks use channel bonding to combine multiple channels into one. Thereby, increasing bandwidth and communication speeds.

**Summary**5:28-6:06

Well, that's it for this lesson. In this lesson, we looked at the structure of a wireless network, the different wireless network modes, and the role of the access point. We looked at the specifications and techniques used by wireless networks.

Remember, wireless networks use the IEEE 802.11 specification. Different iterations of this specification exist, and are denoted by appending a letter to the end of 802.11. Wireless networks broadcast in either the 2.4 GHz frequency or the 5 GHz frequency. And know that some IEEE 802.11 versions are not compatible with other versions. When selecting a wireless device and access point, make sure they use the same version.

7.1.3 Wireless Networking Facts

This lesson covers the following topics:

* Wireless networking architecture
* 802.11 standards
* 802.11n technologies
* 802.11ac technologies
* Additional speed facts
* Additional radio frequency facts
* Additional wireless standards facts

### Wireless Networking Architecture

The following table describes details of a wireless networking architecture:

|  |  |  |
| --- | --- | --- |
| **Characteristic** | **Description** | |
| Devices | An STA (station) is any device that is able to use the 802.11 protocol to communicate on a wireless network. Devices on a wireless network include:   * A wireless NIC for sending and receiving signals. * A wireless access point (AP) is a lot like a hub. It receives wireless signals from several nodes and retransmits them to the rest of the network. * A wireless bridge connects two wireless APs into a single network or connects your wireless AP to a wired network. Most APs today include bridging features.   Many wireless access points include ports (i.e., switches or routers) to connect the wireless network to the wired portion of the network. | |
| Connection Method | Ad hoc | An ad hoc network works in peer-to-peer mode. The wireless NICs in each host communicate directly with one another. An ad hoc network is difficult to maintain for a large number of hosts because connections must be created between a host and every other host, and special configurations are required to reach wired networks. You will typically use an ad hoc network only to create a direct, temporary connection between two hosts. |
| Infrastructure | An infrastructure wireless network employs an access point that functions like a hub on an Ethernet network. With an infrastructure network, you can easily add hosts without increasing administrative efforts (scalable), and the access point can be easily connected to a wired network, allowing clients to access both wired and wireless hosts.  You should implement an infrastructure network for all but the smallest of wireless networks. |
| Service Set Identifier (SSID) | The SSID, also called the network name, groups wireless devices together into the same logical network. All devices on the same network must use the same SSID. | |

### 802.11 Standards

The original 802.11 specification operated in the 2.4 GHz range and provided up to 2 Mbps. Additional IEEE subcommittees have further refined wireless networking, resulting in the following standards:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Specification** | **Standard** | | | | |
| **802.11a** | **802.11b** | **802.11g** | **802.11n** | **802.11ac** |
| Frequency | 5 GHz (U-NII) | 2.4 GHz (ISM) | 2.4 GHz (ISM) | 2.4 GHz (ISM) or 5 GHz (U-NII) | 5 GHz (U-NII) |
| Maximum speed | 54 Mbps | 11 Mbps | 54 Mbps | 600 Mbps | 1.3 Gbps |
| Maximum distance | 100 ft. | 150 ft. | 150 ft. | 300 ft. | 150 ft. |
| Channels (non-overlapped) | 23 (12) | 11 (3) | 11 (3) | 2.4 GHz: 11 (3 or 1) 5 GHz: 23 (12 or 6) | Depends on configuration |
| Modulation technique | OFDM | DSSS, CCK, DQPSK, DBPSK | DSSS (and others) at lower data rates; OFDM, QPSK, BPSK at higher data rates | OFDM (and others, depending on implementation) | OFDM |
| Backwards compatibility | N/A | None | 802.11b | 802.11a/b/g, depending on implementation | 802.11b/g/n |

### 802.11n Technologies

802.11n modified the previous 802.11a (5 GHz) and 802.11g (2.4GHz) standards in order to increase its potential bandwidth and transmission distance. This was done by implementing the following technologies:

|  |  |
| --- | --- |
| **Technology** | **Details** |
| Multiple-Input, Multiple-Output (MIMO) | MIMO increases bandwidth by using multiple antennas for both the transmitter and receiver.  A system is described by the number of sending and receiving antennas. The 802.11n specifications allow up to four sending and four receiving antennas. The benefit of adding additional antennas declines as the number increases; going above 3x3 provides a negligible performance increase. |
| Channel Bonding | Channel bonding combines two, non-overlapping 20 MHz channels into a single 40 MHz channel, resulting in slightly more than double the bandwidth.   * The 5 GHz range has a total of 23 channels, with 12 non-overlapping. This allows for a maximum of 6 non-overlapping bonded (combined) channels. * The 2.4 GHz range has a total of 11 channels, with 3 non-overlapping. This allows for a maximum of 1 non-overlapping bonded channel. For this reason, channel bonding is typically not practical for the 2.4 GHz range. |

### 802.11ac Technologies

802.11ac increased bandwidth and communication speeds by using the following technologies:

|  |  |
| --- | --- |
| **Technology** | **Details** |
| Multi-User MIMO (MU-MIMO) | *MU-MIMO* is an enhancement to MIMO that allows multiple users to use the same channel.  In addition to adding MU-MIMO, 802.11ac doubled the number of MIMO radio streams from four to eight. |
| Channel Bonding | Channel bonding is used to combine even more channels in the 5 GHz band, allowing for up to 160 MHz wide channels.  Even though 160 MHz wide channels are supported, most 802.11ac networks use 80 MHz wide channels. |

### Additional Speed Facts

* Transmission speeds are affected by distance, obstructions (such as walls), and interference.
* Maximum signal distance depends on several factors, including obstructions, antenna strength, and interference. For example, for communications in a typical environment (with one or two walls), the actual distance would be roughly half of the maximum.
* Because transmission speeds decrease with distance, you can either achieve the maximum distance or the maximum speed, but not both.

### Additional Radio Frequency Facts

* The ability of newer devices to communicate with older devices depends on the capabilities of the transmit radios in the access point. Some 802.11n devices are capable of transmitting at either 2.4 GHz or 5 GHz. However, a single radio cannot transmit at both frequencies at the same time.

When you connect a legacy device to the wireless network, all devices on the network operate at the legacy speed. For example, connecting an 802.11b device to an 802.11n or 802.11g access point slows down the network to 802.11b speeds.

* A dual band access point can use one radio to transmit at one frequency, and a different radio to transmit at a different frequency. For example, you can configure many 802.11n devices to use one radio to communicate at 5 GHz with 802.11a devices, and the remaining radios to use 2.4 GHz to communicate with 802.11n devices. Dual band 802.11a and 802.11g devices are also available.

### Additional Wireless Standards Facts

* When you configure an access point, some configuration utilities use the term *mixed mode* to designate a network with both 802.11n and non-802.11n clients. In this configuration, one radio transmitter is used for legacy clients, and the remaining radio transmitters are used for 802.11n clients.
* Many 802.11n access points can support clients running other wireless standards (802.11a/b/g). When a mix of clients using different standards are connected, the access point must disable some 802.11n features to be compatible with non-802.11n devices, which decreases the effective speed.
* Some newer 802.11a and 802.11g devices provide up to 108 Mbps using 802.11n pre-draft technologies (MIMO and channel bonding).

7.1.4 Wireless Security

## Wireless Security 0:00-0:25

Wireless networks are an unbounded network medium. This means the transmission broadcast can be picked up by anyone in a range of the wireless access point. And with some wireless networks, this could be over 150 feet away from the access point.

Because of this, wireless networks use two types of security measures in order to protect wireless communications and broadcasts. The first security measure is authentication.

## Authentication 0:26-0:45

The first thing that occurs when connecting a device to a wireless network is authentication. Authentication is the process of proving identity. You are essentially telling the wireless access point that you are allowed to be on the network. Wireless networks use a few different methods for authentication. The first method is open authentication.

## Open Authentication 0:46-1:20

Open authentication uses MAC address filtering to permit or deny connections, and there are two ways to implement this. The first is implicit deny. This means that all MAC addresses are denied access by default and only the MAC addresses on an allowed list are able to connect.

The second way is called explicit deny. With this method, all MAC addresses are allowed by default, and the list is instead used to deny specific MAC addresses.

While open authentication is a type of security, it's not very secure. Open authentication can be very easily bypassed using MAC addresses spoofing.

## Shared Key Authentication 1:21-1:37

The second authentication method is shared key authentication. With shared key authentication, devices are asked to provide a password before they can connect to the wireless network. If they provide the correct password, they're allowed access. Shared key authentication uses a single password that needs to be configured on all devices.

## 802.1x Authentication 1:38-2:14

The third authentication method is called 802.1x authentication. 802.1x uses individual usernames and passwords for authentication, much like the individual users on a computer. With 802.1x, users are asked to provide a username and a password. The authentication information is then sent to an authentication server which uses either RADIUS or EAP protocols. If the provided username and password are valid, then the connection is permitted.

Authentication is only one layer of wireless security. While it prevents unauthorized network connections, it doesn't protect the actual wireless transmissions.

## Encryption 2:15-2:38

Remember, anyone in a range of the wireless network can capture the information being transmitted. Things like bank account numbers, credit card numbers, and login credentials, these could all be very easily intercepted by a malicious individual.

To protect against this, wireless networks use a second layer of security called encryption. Just as with authentication, there are several different methods of encryption that can be used on a wireless network.

## WEP 2:39-3:14

The first method we'll talk about is Wired Equivalent Privacy, or WEP. WEP uses an encryption method called RC4 to encrypt and decrypt communications. WEP can be used with open authentication or shared key authentication. When using shared key authentication, the shared key itself is used to encrypt communications.

WEP is a very unsecure encryption method. With even a simple hacking tool, a WEP encryption can be cracked in a matter of minutes. In fact, the only reason we're learning about WEP is to let you know to never use it, ever.

## WPA 3:15-3:54

It's just too risky.

Let's take a look at the next encryption method, WPA.

WPA was created as a temporary replacement of WEP until a better, more secure encryption method was developed. WPA still uses RC4 encryption, but it does so using a protocol called TKIP.

TKIP uses a technique known as rotating keys, where a different encryption key is used for every packet being sent. This is in contrast to WEP, where the same key is used for all communications.

Even though WPA TKIP does have some weaknesses, it is largely more effective than WEP. But remember, it was created as a temporary replacement until a more complex method was developed, which was WPA2.

## WPA2 3:55-5:07

WPA2 was released a year after WPA and uses a much more complex and effective encryption mechanism. Instead of using RC4 and TKIP, WPA2 uses the Advanced Encryption Standard (AES). AES is a very strong encryption method and provides the best wireless security. This is the default encryption used by most wireless access points and should be the encryption method used in almost all situations.

Encryption and Authentication

Wireless access points use the encryption method in conjunction with the authentication method to create a more secure wireless network. When selecting a wireless security option on an access point, you might see WPA2 Personal or WPA2 Enterprise as the wireless security option. The first part is the encryption method. The second is the authentication method.

WPA2 Personal indicates the network will use shared key authentication. WPA2 Personal is sometimes written as WPA2 PSK. When you see Enterprise, 802.1x authentication, which requires a RADIUS or EAP server, is used.

WPA2 Personal is used in most wireless network environments. WPA2 Enterprise is typically used by larger companies or organizations.

## Additional Security Steps 5:08-6:24

In addition to configuring the encryption and authentication method on a wireless access point, there are other steps that should be taken to further secure a wireless network. One of the most important steps is to change the default administrator password.

To make configuration easier, wireless access points are preconfigured with a default password. Often times, the password is simply "admin" or "password". Even if it's a bit more complex, there are websites that have a list of all the default passwords used by each access point manufacturer. The first thing you should do when configuring a network device is change the default password.

Another thing you can do is change the default SSID. Default SSIDs, often times, contain information about the type of access point. This information might be used to exploit known vulnerabilities in that particular model.

You can also disable the SSID broadcast, if necessary. This makes it so the SSID isn't in the list of available networks on a wireless device. This is mostly a protection against the casual passerby. Even with the SSID broadcast disabled, it's actually relatively easy to obtain the SSID.

MAC address filtering is another security layer you can add. However, it's often times more of a nuisance for the person managing the network. MAC addresses of devices can be easily captured and spoofed by a determined hacker.

## Summary 6:25-6:42

Those are the different wireless security measures that are used to protect a wireless network. To review, wireless networks use both authentication and encryption to secure communications. Authentication and encryption are used in conjunction with each other. WPA2 Personal is the most common type of wireless security and uses AES encryption with shared key authentication.

7.1.5 Wireless Security Facts

This lesson covers the following topics:

* Authentication methods
* Wireless security standards

### Authentication Methods

Authentication to wireless networks is implemented using the following methods:

|  |  |
| --- | --- |
| **Method** | **Description** |
| Open | Open authentication requires that clients provide a MAC address in order to connect to the wireless network.   * You can use open authentication to allow any wireless client to connect to the AP. Open authentication is typically used on public networks. * You can implement MAC address filtering to restrict access to the AP to only known (or allowed) MAC addresses.   Because MAC addresses are easily spoofed, this provides little practical security. |
| Shared Key | With shared key authentication, clients and APs are configured with a shared key (called a *secret* or a *passphrase*). Only devices with the correct shared key can connect to the wireless network.   * All APs and all clients use the same authentication key. * Shared key authentication should be used only on small, private networks. * Shared key authentication is relatively insecure, as hashing methods used to protect the key can be easily broken. |
| 802.1x | 802.1x authentication uses usernames and passwords, certificates, or devices such as smart cards to authenticate wireless clients. Originally designed for Ethernet networks, the 802.1x standards have been adapted for use in wireless networks to provide secure authentication. 802.1x authentication requires the following components:   * A RADIUS or TACACS+ server to centralize user account and authentication information. A centralized database for user authentication is required to allow wireless clients to roam between cells but authenticate using the same account information * A PKI for issuing certificates. At a minimum, the RADIUS server must have a server certificate. To support mutual authentication, each client must also have a certificate   Use 802.1x authentication on large, private networks. Users authenticate with unique usernames and passwords. |

### Wireless Security Standards

Security for wireless networking is provided from the following standards:

|  |  |
| --- | --- |
| **Method** | **Description** |
| Wired Equivalent Privacy (WEP) | WEP is an optional component of the 802.11 specifications that were deployed in 1997. WEP has the following weaknesses:   * A static pre-shared key (PSK) is configured on the AP and the client. It cannot be dynamically changed or exchanged without administration. As a result, every host on large networks usually uses the same key. * Because key values are short and don't change, the key can be captured and easily broken.   Because of the inherent security flaws, avoid using WEP whenever possible. If using WEP cannot be avoided,  implement it only using open authentication. Shared key authentication with WEP uses the same key for both encryption and authentication, exposing the key to additional attacks. |
| Wi-Fi Protected Access (WPA) | WPA is the implementation name for wireless security based on initial 802.11i drafts that was deployed in 2003. It was intended to be an intermediate measure to take the place of WEP while a fully secured system (802.11i) was prepared. WPA:   * Uses Temporal Key Integrity Protocol (TKIP) for encryption * Supports both pre-shared key (WPA-PSK or WPA Personal) and 802.1x (WPA Enterprise) authentication * Can use dynamic keys or pre-shared keys * Can typically be implemented in WEP-capable devices through a software/firmware update   WPA keys can also be predicted by reconstructing the Message Integrity Check (MIC) of an intercepted packet, sending the packet to an AP, and observing whether the packet is accepted by the AP. |
| Wi-Fi Protected Access 2 (WPA2) or 802.11i | WPA2 is the implementation name for wireless security that adheres to the 802.11i specifications. It was deployed in 2005. It is built upon the idea of Robust Secure Networks (RSN). Like WPA, it resolves the weaknesses inherent in WEP. It is intended to eventually replace both WEP and WPA. WPA2:   * Uses Advanced Encryption Standard (AES) as the encryption method * Supports both pre-shared key (WPA2-PSK or WPA2 Personal) and 802.1x (WPA2 Enterprise) authentication * Can use dynamic keys or pre-shared keys |
| Wi-Fi Protected Access 3 (WPA3) | WPA3 is a new authentication launched in 2018. It is a more resilient version of WPA2. WPA3:   * Uses password-based authentication * Provides better protection against password guessing attempts by using Simultaneous Authentication of Equals (SAE) * Offers 192-bit cryptographic strength, giving additional protection for networks dealing with sensitive data |

When transmitting data on a wireless network, it's important to know if the channel you are using is encrypted. Information sent on unencrypted channels, where no security is being used, can be easily intercepted and viewed. If needed, IPsec can be used to provide security when sending information on an unencrypted channel.

7.1.6 Configure a Wireless Connection

## Configure a Wireless Connection 0:00-0:13

Connecting to WiFi is something pretty much everyone does these days, but there are some additional settings that many users are not aware of. In this demonstration, we are going to go and see where you can configure these additional settings.

## Connect to a Wireless from a Client 0:14-1:05

I have a laptop that has a wireless network interface card. The easiest way to connect to a wireless network is to click this network icon, down here.

When I click the icon, it shows all the wireless networks that are within the range of this device. Each wireless network is shown with a name, as well as the strength of wireless signal, and whether it's secure.

To connect to a wireless network, I find the SSID, which is right here. I can click it once and I'm able to click Connect. From here, I'm prompted for the passphrase. We have that set up to be MyWireL3ss. I can then click here to verify that I typed it in correctly and click Next.

It asks if I want my device to be discoverable on the network. I'm just going to say no. Right now, it's negotiating this adapter to the wireless access point. It looks like I'm connected.

## View Wireless Profiles 1:06-2:11

Let's look at our wireless profiles. To see these, we need to go to Start > Settings > Network & Internet > Wi-Fi > Manage Known Networks. Once you successfully connect to a wireless, the computer creates what's called a profile.

The profile identifies wireless networks that have been connected to it in the past. These profiles are saved so you can connect to the same network again later. Here, we have a list of wireless networks that we've connected to in the past.

You can edit the profile to change its properties about the connection. Let's select this one right here and click Properties.

The first thing I can do is tell this to connect automatically to this wireless. If it's one that you want to use as your default, you might want to have this turned to On.

You can choose to use random hardware addresses when using this network. I'm not interested in that, so I'll leave that alone.

If you pay for bandwidth, you might want to tell this connection that you're on a metered connection. This will help prevent things such as Windows Update from downloading large files while connected. This is nice because you can then avoid charges for data you didn't plan on using. Let's click up here and go back.

## Add a Wireless Network Manually 2:12-2:42

You might want to add a wireless profile manually. This might be if you're connecting to a wireless and there is no SSID broadcast.

To do this, we select Add a new network. We can then enter our network name here. I'll put in FreeWiFi and for Security type, I'll select WPA2-Personal AES from the list. I need to enter a security key. I then have the option to connect automatically and also to connect even if this network isn't broadcasting. I'll click Save here at the bottom, and we've added a network manually.

## Remove a Wireless Network 2:43-2:56

To remove a network you no longer want, you select the Wi-Fi connection that you want to remove and then click the Forget button. This button doesn't show you a confirmation dialog, so pay attention and make sure you're removing the right one. Let's go back again.

## Use Wi-Fi Services 2:57-3:29

Windows 10 offers two additional features that will help you get connected no matter where you're located. If you turn on the Find paid plans for suggested open hotspots near me option, you'll be able to purchase data plans on the Windows Store from the different affiliated networks.

Down here, you can also turn on the Connect to suggested open hotspots option, which allows your Windows 10 system to connect automatically to open wireless networks based on information from devices that Microsoft has gathered into a database. These networks may not be reliable or secure, so keep that in mind before connecting to these.

## Use Hotspot 2.0 Networks 3:30-4:01

We also have Hotspot 2.0 networks. This is a new networking standard for connecting to public Wi-Fi networks. If you're in a public place, like a restaurant or hotel, Hotspot 2.0 will identify and connect to the correct network automatically without having to go through a list of wireless networks that could be fake or malicious.

Hotspot 2.0 uses WPA2 Enterprise for authentication and encryption. Hotspot 2.0 networks is enabled by default on Windows 10. If you don't intend on using this feature, you can turn it off right here.

## Summary 4:02-4:10

That's it for this demo. In this demo, we looked at how to connect to a wireless network from a Windows 10 client. We then looked at a few new services Windows 10 offers to connect to wireless networks.

9.6 Mobile Device Networking

As you study this section, answer the following questions:

* How do you install apps on a mobile device?
* How do you connect a mobile device to a network?
* How do you secure a mobile device?
* How do you synchronize data between a mobile device and desktop PC or laptop computer?

In this section, you will learn to:

* Network mobile devices
* Synchronize mobile devices
* Configure email on mobile devices

Key terms for this section include the following:

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Bluetooth | Bluetooth is a wireless technology standard for exchanging data over short distances from fixed and mobile devices and for building personal area networks (PANs). |
| Hotspot | A hotspot is a physical location where you can obtain wireless Internet access using a wireless local area network (WLAN) with a router connected to an internet service provider. |
| Infrared port (IR) | A port on a mobile device that enables devices to exchange data without using cables. |
| Lightning | A proprietary computer bus and power connector created by Apple Inc. to replace its previous proprietary 30-pin dock connector. |
| Long-Term Evolution (LTE) | A mobile communications standard used by 5G. |
| Mobile Virtual Private Network (Mobile VPN) | A mobile virtual private network (mobile VPN) provides mobile devices with access to network resources and software applications on their home network when they connect using other wireless or wired networks. |
| Near Field Communication Connector | An NFC connector used to emulate cryptographic smart card functionalities for RFID tags or memory cards. |
| Tethering | Connecting one device to another. |

This section helps you prepare for the following certification exam objectives:

|  |  |
| --- | --- |
| **Exam** | **Objective** |
| TestOut PC Pro | 1.6 Given a scenario, manage mobile devices  1.6.2 Configure mobile device connectivity  1.6.3 Use common mobile device features  2.2 Given a scenario, use operating system features and utilities  2.2.2 Use core macOS or iOS features |
| CompTIA 220-1001 | 1.5 Given a scenario, connect and configure accessories and ports of other mobile devices.   * Connection types   + Wired     - Micro-USB/Mini-USB/USB-C     - Lightning     - Tethering     - Proprietary vendor-specific ports (communication/power)   + Wireless     - NFC     - Bluetooth     - IR     - Hotspot   1.6 Given a scenario, configure basic mobile device network connectivity and application support.   * Corporate and ISP email configuration   + POP3   + IMAP   + Port and SSL settings   + S/MIME * VPN   1.7 Given a scenario, use methods to perform mobile device synchronization.   * Synchronization methods   + Synchronize to the cloud   + Synchronize to the desktop   + Synchronize to the automobile * Types of data to synchronize   + Contacts   + Applications   + Email   + Pictures   + Music   + Videos   + Calendar   + Bookmarks   + Documents   + Location data   + Social media data   + E-books   + Passwords * Mutual authentication for multiple services (SSO) * Software requirements to install the application on the PC * Connection types to enable Synchronization   2.4 Compare and contrast wireless networking protocols.   * 3G * 4G * 5G * LTE   2.6 Explain common network configuration concepts.   * VPN   3.1 Explain basic cable types, features, and their purposes.   * Multipurpose cables   + Lightning   3.2 Identify common connector types.   * Lightning   3.9 Given a scenario, install and configure common devices.   * Laptop/common mobile devices   + Synchronization settings   + Wireless settings |

9.6.1 Networking Mobile Devices

**Networking Mobile Devices**0:00-0:07

In this demonstration, we're going to practice working with network settings on an iPad.

**802.11 Wireless Connection**0:08-1:09

Let's begin by configuring an 802.11 Wi-Fi wireless connection. To connect this iPad to an 802.11 wireless network, I need to come down here, to Settings, and then I need to select Wi-Fi.

You'll notice that I'm already connected to a network named NotYourWireless. You can tell that by the little blue checkmark that's located next to the network name. Now, if I need to connect to a different network, I have two different options for doing so.

First of all, if the network is broadcasting its network name, then it will appear under Choose a Network. As you can see here, I have another network called Tampico. If I wanted to connect to it, all I would have to do is tap on it and then provide the appropriate passphrase. But please be aware that there are a lot of wireless networks that, for security reasons, do not broadcast their SSID. If that's the case, you will not see that network listed under Choose a Network.

The wireless network is still there, and you can still connect to it. You just can't see it under Choose a Network. If this is the case, then you'll have to use another option to manually connect to that wireless network.

**Wireless Network Connection**1:10-2:30

So, let's take a look at using the first option, where we connect to a wireless network that's broadcasting its SSID.

To do this, I simply tap on the network that I want to connect to. In this case, that's the Tampico network. I have to enter the passphrase to connect. And then I tap Join. Now you can see that I'm connected to the Tampico wireless network instead of the other one, and you can tell that because there's a little blue checkmark next to Tampico now.

If you want to see the IP network configuration parameters that were assigned to the device when it connected to the wireless network, I just have to tap the little blue information icon. When you do, you can see how this connection is configured.

First of all, you can see that I'm connected automatically using DHCP and that I received an IP address from DHCP 192.168.1.106. My subnet mask is 255.255.255.0. My default gateway router is 192.168.1.1.

I tap on Configure DNS, and you can see my DNS settings.

Now, you're not stuck with using DHCP.

If I wanted to, I could come over here and select Automatic. Using a static option, I would them manually assign my IP addressing parameters.

But in this case, I really don't want to. I just want to go ahead and use DHCP. So we'll go back, and we'll leave it set that way.

**Forget This Network Option**2:31-3:24

Before we leave this screen, there is one other option that I want you to pay attention to. That's the Forget This Network option at the very top of the screen.

The key thing to remember with most mobile devices is that when you connect to a wireless network, the device will automatically remember that network and try to connect to it automatically the next time that network comes into range, and there may be times when you don't want that to happen. If this is the case, then you can tap Forget This Network at the top of the screen. When you do, the passphrase that you use to connect to that wireless network will be deleted. Of course, to connect to it again, you'll have to manually specify the appropriate passphrase again.

In the case of my networks, they're broadcasting its SSID. So even if I were to tap Forget This Network, they'll still appear in the list of available networks under Choose a Network on the previous screen. But the passphrase would be gone, so I'd have to enter that passphrase again to reconnect.

**Network Not Broadcasting SSID**3:25-4:58

So, let's suppose you need to connect to a wireless network that's not broadcasting its SSID, which, as I said before, is pretty common. In that case, you need to tap Other down here under Choose a Network. The first thing you're prompted to specify is the name of the network you want to connect to. In this case, let's connect back to the first wireless network that we were using before, which was named NotYourWireless.

As you saw earlier, the NotYourWireless network really is broadcasting. But let's say, for demonstration purposes, that it was a functioning wireless network that was not broadcasting. The administrator turned off SSID broadcast for security reasons.

In this situation, I would enter the name of the network in the name field. Then I would need to specify what type of security that network is using. Currently, it's set to None. I'm going to tap None so I can see a list of security options. I happen to know that this particular wireless network uses WPA2 personal, so I'll tap WPA2, and then we'll tap Other Network to go back. And now you can see that WPA2 is selected for the security mechanism.

The last thing I need to do is type the WPA2 passphrase that's used to connect to that network.

At this point, we're connected to the NotYourWireless network as before. If we want to see what IP address has been assigned to this device via DHCP again, we tap on the little blue information icon, and we now have new IP address information, which is different from previously because this is a different wireless system.

At this point, we've configured this iPad to connect to an 802.11 Wi-Fi network.

**Summary**4:59-5:03

That's it for this demonstration. In this demo, we talked about how to configure mobile device wireless network settings.

9.6.2 Mobile Device Connection Facts

The following table lists different mobile connection types:

|  |  |
| --- | --- |
| **Connection Types** | **Description** |
| Generations | Cellular networks used for voice and data include the following types:   * 2G (second generation) networks were the first to offer digital data services. 2G data speeds are slow (14.4 Kbps) and are used mainly for text messaging, not internet connectivity. 2.5G supports speeds up to 144 Kbps. * EDGE (also called 2.75G) networks are an intermediary, between 2G and 3G networks. EDGE is the first cellular technology to be truly internet-compatible, with speeds of 400–1,000 Kbps. * 3G offers simultaneous voice and data. Minimum speeds for stationary users are quoted at 2 Mbps or higher. The following extensions enhance 3G networks:   + HSPA+ (also known as *smart antenna*) uses multiple-input and multiple-output (MIMO). It significantly increases data throughput and link range without additional bandwidth or increased transmit power.   + Long Term Evolution (LTE) and LTE-Advanced increase downlink/uplink speeds to 100/50 Mbps and 1Gbps/500Mbps, respectively. * 4G is available with minimum speeds around 3–8 Mbps, with over 100 Mbps possible. 4G:   + Uses MIMO.   + Is not compatible with 3G; 4G requires a complete retrofit on the part of service providers and new equipment for the consumer.   + Utilizes Worldwide Interoperability for Microwave Access (WiMAX). WiMAX delivers high-speed internet service (up to 1 Gbps for stationary users) to large geographical areas. * 5G is able to achieve speeds twenty times faster that 4G; its peak speed is 20Gb per second.   + Uses MIMO.   + Includes lower frequencies than previous generations, down to 600 MHz.   + Uses Long-Term Evolution (LTE) for wireless connections. |
| Hotspot | A *hotspot* is a physical location where you can obtain wireless internet access using a wireless local area network (WLAN) with a router connected to an internet service provider. |
| Tethering | *Tethering* is connecting one device to another. In the context of mobile phones and tablet computers, tethering allows sharing the internet connection of the phone or tablet with other devices like laptops. Connection of the phone or tablet with other devices can be done over wireless LAN (Wi-Fi), over Bluetooth, or by physical connection using a cable like USB. |
| Airplane Mode | *Airplane mode* is a setting available on many smart phones, portable computers, and other electronic devices that suspends the device's radio-frequency signal transmitting functions, which disables telephone, Wi-Fi, and Bluetooth when activated. |
| VPN | A mobile virtual private network (mobile VPN) provides mobile devices with access to network resources and software applications on their home network when they connect using other wireless or wired networks. |
| Bluetooth | *Bluetooth* is a wireless technology standard for exchanging data over short distances from fixed and mobile devices and for building personal area networks (PANs). It can connect several devices, overcoming problems of synchronization. |
| NFC | An *NFC connector* is used to emulate cryptographic smart card functionalities for RFID tags or memory cards. |
| miniUSB/microUSB | A *mini-USB connector* is a small USB cable connector that is often used by handheld electronic devices like mobile phones, MP3 players, and digital cameras. On mobile phones it is often used for both USB data connectivity and charging. The new connector, called micro-USB, is smaller than the mini-USB connector and allows for even thinner device designs. |
| Lightning | *Lightning* is a proprietary computer bus and power connector created by Apple Inc. to replace its previous proprietary 30-pin dock connector. It is used to connect Apple mobile devices like iPhones, iPads and iPods to host computers, external monitors, cameras, USB battery chargers, and other peripherals. |
| IR | An *infrared port* is a port on a mobile device that enables devices to exchange data without using cables. |

9.6.4 Data Synchronization Facts

You can synchronize data between a PC system and a mobile device. You can also synchronize data between your PC or mobile device and the cloud, or even between a mobile device and a car. Use a USB cable or wireless connection to connect to a desktop or cloud to synchronize your data. You can also configure both a PC and a mobile device to use the same iCloud account.

Online services use mutual authentication or single signon to allow you to connect to their servers to sync data. Mutual authentication, also called two-way authentication, is a process or technology where both entities in a communications link authenticate each other. In a network environment, the client authenticates the server and vice-versa.

For example, iTunes requires you to authenticate using your Apple ID to its servers, while at the same time, Apple verifies that the iTunes app on your computer or device is the same app and computer used to access your iTunes account. Mutual authentication is used for multiple services like purchasing music and ebooks and saving content to the cloud.

Also, be aware of any software requirements needed to install the application on your PC or mobile device. Some software require a specific operating system and cannot run on any other operating system. For example, Android apps run on only Android devices. Apple apps run on only devices with iOS.

Types of data you can synchronize:

* Contacts
* Programs
* Email
* Pictures
* Music
* Videos
* Calendar
* Bookmarks
* Documents
* Location data
* Social media data
* eBooks
* Passwords

9.6.6 Mobile Email Configuration Facts

You can configure email accounts on your mobile device using email service providers. Well-known email providers include:

* Exchange
* Google/Inbox
* iCloud
* Outlook.com
* Yahoo

You can also add your email account and setup the IP addresses of your POP3, IMAP, or SMTP servers. To configure these email accounts, you may need to modify the port settings. To encrypt your email, configure the SSL and S/MIME settings. Both SSL and S/MIME securely sign and encrypt email to prove that the email actually came from the person claiming to be the sender.

Chapter 13: Security

13.9 Network Security

As you study this section, answer the following questions:

* How can you secure physical access to computer systems?
* What configuration changes could you make to prevent data loss on a Windows system?
* What are the characteristics of a strong password?
* How can you limit wired network connectivity to only authorized systems?
* How can you make it more difficult for an unauthorized person to connect to a wired network?
* Which network devices should be put in a DMZ? Which systems should not?
* What is the role of a content filter?
* What can you do to obscure a wireless network?
* How can you prevent data emanation from a wireless network?

Key terms for this section include the following:

|  |  |
| --- | --- |
| **Term** | **Definition** |
| MAC address filtering | A feature that restricts access to the wired network switch to hosts that have specific MAC addresses. |
| Wi-Fi Protected Setup (WPS) | A network security standard that makes wireless networks easier to manage. |

This section helps you prepare for the following certification exam objectives:

|  |  |
| --- | --- |
| **Exam** | **Objective** |
| CompTIA 220-1001 | 2.3 Given a scenario, install and configure a basic wired/wireless SOHO network.   * Firewall settings   + MAC filtering |
| CompTIA 220-1002 | 2.2 Explain logical security concepts.   * Port security * MAC address filtering   2.7 Given a scenario, implement security best practices to secure a workstation.   * Account management   + Disabling guest account   + Basic Active Directory functions   + Disable account   2.10 Given a scenario, configure security on SOHO wireless and wired networks.   * Wireless specific   + Changing default SSID   + Setting encryption   + Disabling SSID broadcast   + Antenna and access point placement   + Radio power levels   + WPS * Change default usernames and passwords * Enable MAC filtering * Assign static IP addresses * Firewall settings * Port forwarding/mapping * Disabling ports * Content filtering/parental controls * Update firmware * Physical security |

13.9.1 Wired Network Security Best Practices

**Wired Network Security Best Practices**0:00-0:13

In this lesson, we're going to review several best practices for securing a wired network. The goal is to make your network more difficult to compromise so it's less attractive to attackers.

**Physical Security**0:14-1:22

Security measures are easily to circumvent if the computer systems on your network are not physically secure, so let's start by looking at several things you can do to improve physical security.

First, keep server systems in a locked server room where only authorized people with access keys or codes are allowed in.

Make sure that screen savers on desktop workstations have a very short timeout period and that a password is required whenever a user tries to resume a session.

Make sure desktop workstations are configured to require the user to authenticate before they're allowed to resume a session from standby or hibernation.

Control access to the work area where user desktops and servers are located. For example, you could use a proximity badge reader to regulate access.

Ensure computers in low-security areas, such as a receptionist's desk, are secured with a cable lock.

Disable external ports on desktop and server systems, especially USB and FireWire ports. You can do this in the BIOS/UEFI configuration. Use a BIOS/UEFI password to protect the configuration.

Disable or completely remove optical disc burners.

Uninstall any unnecessary software from servers and workstations.

**User Accounts and Passwords**1:23-2:09

In addition to these security measures, there are several important measures you need to take to increase the security of the user accounts and passwords in your organization.

Configure your systems to require strong passwords. A strong password is at least eight characters long, uses both upper- and lower-case letters, and includes numbers or non-alphabetic characters.

Don't allow users to write down their passwords on sticky notes.

Make sure all user accounts have passwords assigned.

Disable guest user accounts on servers and workstations.

And disable user accounts immediately when users leave the organization.

Change default usernames and passwords. Many network devices, such as routers and switches, use a default username and password for the initial setup. These default usernames and passwords are widely known and posted on the internet.

**MAC Address Filtering**2:10-3:29

Another thing you can do to increase a wired computer network's security is enable MAC address filtering. MAC address filtering allows you to control who connects to the wired network by filtering MAC addresses. You can do this using a whitelist or a blacklist.

A whitelist defines a list of MAC addresses that are allowed to connect to the switch.

A blacklist defines a list of MAC addresses that are not allowed to connect to the switch.

When a computer connects to the wired network with a drop cable, the switch checks the computer's MAC address. If the switch is configured to use a whitelist, it compares the MAC address to the whitelist. If the MAC address is listed on the whitelist of allowed MAC addresses, then the switch allows the host to connect and participate on the wired network. If the MAC address is not on the whitelist, then the host is denied access.

If your switch is configured to use a blacklist, the opposite occurs. If the host's MAC address is on the blacklist, the switch does not allow the host to connect to the network. If the MAC address is not on the blacklist, the switch allows the host to connect to the network.

For security reasons, it is more common to implement MAC address filtering with a whitelist. This configuration locks out all hosts except for those specifically allowed in the whitelist.

MAC address filtering provides a basic level of network security. It's not foolproof. It can be defeated by a determined attacker, but it does make your network harder to compromise.

**Static IP Addressing**3:30-4:36

Another way to increase the security of a wired network is to use static IP addressing instead of DHCP. To efficiently use IP addresses, many networks use a DHCP server to automatically assign an IP address to a host whenever it connects to the network.

However, this configuration opens a security hole in your network. If someone can successfully connect their system to an open network port in your wired network, they automatically receive all the configuration information they need to communicate with other hosts on the network.

To prevent this, use static IP addressing instead of DHCP. In this configuration, an attacker who manages to successfully connect to your wired network won't know which IP addressing information they should use. By default, their computer will probably revert to automatic IP addressing, which will prevent them from communicating with another host on the network.

Like MAC address filtering, using static IP addressing isn't a foolproof security measure. A determined attacker will eventually be able to determine the IP addressing scheme used on your network and configure the workstation appropriately. But it does make your network more difficult to compromise, making it a less-inviting target.

**Disable Unused Switch Ports**4:37-5:08

You can also increase the security of a wired network by disabling unused network jacks and switch ports.

If an unused network jack is left in an active state, it can be used to connect to the switch on your wired computer network. Likewise, any unused ports on the switch itself that are also left in an active state can provide an attacker with an easy way to connect to the wired network.

To prevent this from happening, disable all unused switch ports. This is especially true for switch ports connected to network jacks located in unsecure areas of your organization, such as the reception area.

**Firmware Updates**5:09-5:43

It is also important that you update your network devices' firmware, such as switches, routers, and firewalls.

The firmware contains software instructions that allow these devices to run and provide their functions. After these devices have been developed and released, security weaknesses are commonly discovered. To address these weaknesses, the hardware vendor should release updates to the device firmware.

Unlike standard software, which can be automatically updated over a network connection, firmware updates aren't usually automated. This requires the system administrator to watch for updates and manually download and install them when they become available.

**Firewall Configuration**5:44-6:38

You should also ensure that network hosts are protected by a firewall. A firewall monitors incoming and outgoing network traffic to make sure it is allowed by the organization's security policy. Firewalls should be implemented on each individual host and on the network itself.

The legitimacy of network traffic is determined by the access control list, or ACL, configured on the firewall. To increase the security of your wired network, you need to ensure your firewall ACLs are configured to allow only authorized traffic on your network.

The best way to do this is to start with all traffic blocked by default. This is usually enabled by default on most network firewalls using a preconfigured implicit deny rule in all ACLs. Then add ACL rules that allow specific types of traffic through the firewall that are permitted by your organization's security policy. If network traffic that does not match an Allow rule and the ACL tries to go through the firewall, it's denied.

**Content Filters**6:39-7:53

While the internet can be a very useful resource, it also contains illicit and illegal content. If your users access this type of content on your organization's network, then your organization could be liable for their actions.

To keep this from happening, you can implement a content filter that inspects network traffic to ensure that it meets your organization's acceptable use policy. Doing this helps prevent users from wasting time accessing content that is not work-related, accessing content that could be construed as creating a hostile work environment, and engaging in illegal activities.

Most content filters can be configured to use pre-defined blacklists of websites categorized according to content. However, there will always be unapproved sites that slip past these pre-defined blacklists. When this happens, most content filters allow you to manually add specific sites to the blacklists.

As with network firewalls, content filters can be implemented for an entire network or on individual network hosts.

A network-wide content filter usually sits near the network firewall and router, inspecting the contents of all incoming and outgoing network traffic.

A host-based content filter is implemented as software on a specific host. Some operating systems include parental controls that can function as a content filter.

**Port Forwarding/Mapping**7:54-8:58

You should also be familiar with security issues associated with port forwarding, which is also called port mapping.

Because of the wide-spread use of NAT routing to conserve registered IP addresses, some organizations, especially small businesses, implement port forwarding to allow access to internal network resources from the external network, such as communications between a web server and the internet. A NAT router can use port forwarding to redirect an incoming request from the external network to a different IP address and port number on the internal network.

However, doing this decreases the security of the internal network. By default, most network firewalls are preconfigured to block all requests that originate outside of the internal network. The NAT router itself does this to a degree as well by translating IP addresses between the internal and external network.

By implementing port forwarding, you allow external, untrusted traffic into the internal network, which should be an area of high security. In this configuration, you must rely on the security configuration of the internal host to protect the rest of the network. This is not an ideal configuration.

**DMZ**8:59-9:31

A better configuration is to use a higher-end router or network security appliance to create a demilitarized zone, or DMZ. A DMZ divides the network into three areas of differing levels of security: the external network with little or no security, the DMZ with moderate security, and the and internal network with high security.

In this configuration, network resources that need to be accessed externally can be placed in the DMZ. This prevents external traffic from directly entering the internal network. If the host in the DMZ is compromised by an external attacker, the rest of the network is not affected.

**Summary**9:32-9:46

In this lesson, we reviewed several best practices that you can employ to secure a wired network: physical security, user accounts and passwords, MAC address filtering, static IP addressing, disabling unused switch ports, firmware updates, firewall configuration, content filters, and port forwarding.

13.9.2 Wired Network Security Facts

As a system administrator, there are several best practices that you can employ to increase the security of a wired network. The goal is to make the network more difficult to compromise and accordingly less attractive to an attacker. These best practices are listed in the following table:

|  |  |
| --- | --- |
| **Best Practice** | **Description** |
| Maintain Physical Security | Technological security measures can be circumvented if the computer systems connected to the wired network are not physically secure. Consider the following physical security measures:   * Keep server systems in a locked server room where only authorized persons who have the appropriate keys or access codes are allowed in. * Ensure that the screen savers on workstations and notebook systems have a very short timeout period and require a password whenever a user tries to resume the session. * Ensure workstation and notebook systems require the user to authenticate before they're allowed to resume a session from sleep or hibernation. * Control access to work areas where computer equipment is used. For example, you could use a proximity badge reader on a locked door to regulate access. * Ensure computers in low security areas (such as a receptionist's desk) are secured with a cable lock. * Disable external ports on desktop and servers systems, especially USB and FireWire ports. This can be done in the BIOS/UEFI configuration or using Windows Group Policy. * Disable or completely remove optical disc burners. * Uninstall any software from servers and workstations that isn't necessary. |
| Protect User Accounts and Passwords | Consider implementing the following measures to increase the security of user accounts and passwords:   * Require strong passwords. A strong password is at least 8 characters long, uses upper- and lower-case letters, and includes numbers or non-alphabetic characters. * Don't allow users to write down their passwords. * Ensure all user accounts have passwords assigned. * Disable guest user accounts. * Change default user names (such as Administrator) to something less obvious (such as Winifred). * Immediately disable or remove accounts when users leave the organization. * Change default usernames and passwords. Many network devices, such as routers and switches, use a default user name and password for initial setup. These default user names and passwords are widely posted on the internet. |
| Implement MAC Address Filtering | MAC address filtering restricts access to the wired network switch to hosts that have specific MAC addresses. This can be done in two different ways:   * Use a whitelist, which defines a list of MAC addresses that are allowed to connect to the switch. * Use a blacklist, which defines a list of MAC addresses that are not allowed to connect to the switch.   With MAC address filtering enabled, a switch checks a computer's MAC address when it connects to the wired network. If the switch has been configured to use a whitelist, it will compare the computer's MAC address to the whitelist. If its address is listed in the whitelist of allowed MAC addresses, then the switch will allow the host to connect to the wired network. If the computer's MAC address is not in the whitelist, then the host will be denied access.  If the switch is configured to use a blacklist, the opposite occurs. If the computer's MAC address is on the blacklist, the switch will not allow the host to connect to the network. If its MAC address is not listed in the blacklist, the switch will allow the computer to connect to the network.  For security reasons, whitelists are usually the preferred option. This configuration locks out all hosts except for those specifically allowed in the whitelist. However, MAC address filtering provides only a basic level of network security and can be defeated by a determined attacker. However, it does make the network harder to compromise and hopefully less attractive to an attacker. |
| Implement Static IP Addressing | In order to use IP addresses efficiently, most networks use a DHCP server to automatically assign an IP address to hosts whenever they connect to the network. However, this configuration presents a security weakness. If attackers are able to successfully connect a system to an open network jack in your wired network, they automatically receive all the configuration information they need to communicate with other hosts on the network.  To prevent this, use static IP addressing instead of DHCP. In this configuration, an attacker who manages to successfully connect to your wired network won't receive any IP addressing information. Be aware that using static IP addressing isn't a fool-proof security measure. Determined attackers will eventually be able to determine the IP addressing scheme used on your network and configure their system appropriately. However, it does make your network more difficult to compromise. |
| Disable Unused Switch Ports | The security of a wired network can be increased by disabling unused network wall jacks and switch ports. If an unused network jack is left in an active state, it can be used to connect to the wired computer network. Likewise, an unused port on the switch that is left in an active state can provide an attacker with an easy way to connect to the wired network.  To prevent this from happening, disable all unused switch ports. This is especially true for switch ports connected to network jacks located in insecure areas of your organization, such as the reception area. |
| Install Firmware Updates | It is important that you keep the firmware of your network devices updated, including:   * Switches * Routers * Firewalls   The firmware contains software instructions that allow these devices to run. It's not unusual for security weaknesses to be discovered in the firmware of these devices when they are deployed in production environments. To address these weaknesses, the hardware vendor should release updates to the firmware. Unlike standard software, which can be automatically updated over a network connection, firmware updates must usually be installed manually. You should watch for updates for your devices to be released and install them when they become available. |
| Maintain Firewalls | You should ensure that network hosts are protected by a firewall. A firewall monitors incoming and outgoing network traffic to make sure it is allowed by the organization's security policy. Firewalls should be implemented:   * On each individual host * On the network itself   The validity of network traffic is determined by the access control list (ACL) configured on the firewall. To increase the security of your wired network, ensure your firewall ACLs are configured to allow only authorized traffic on the network. The best way to do this is to start with all traffic blocked. This is usually enabled by default on most network firewalls using a preconfigured *implicit deny* rule in all ACLs. Then add ACL rules that allow specific types of traffic through the firewall that are permitted by your organization's security policy. If network traffic that does not match any allow rules in the ACL tries to go through the firewall, it will be denied by default. |
| Implement a Demilitarized Zone (DMZ) | If internet users need to access internal network resources (such as a web server), do not allow their traffic to flow into the internal network. Instead, use a high-end router or network security appliance to create a DMZ and place the resource to which they need access within it. This divides the network into three areas of differing levels of security:   * **External network**: Little or no security * **DMZ**: Moderate security * **Internal network**: High security   In this configuration, external traffic enters the DMZ instead of the internal network. If a server in the DMZ is compromised by an external attacker, the rest of the network is not affected. |
| Use Content Filters | The internet contains illicit and illegal content. If your users access this type of content from your organization's network, then your organization could be held liable for their actions. To keep this from happening, implement a content filter that inspects network traffic to ensure that it meets your organization's Acceptable Use Policy (AUP). This prevents users from:   * Wasting time accessing content that is not work-related * Accessing content that could be construed as creating a hostile work environment * Engaging in illegal activities   Most content filters can be configured to use pre-defined blacklists of websites categorized according to content. However, there will always be unapproved sites that slip past these pre-defined blacklists. When this happens, most content filters allow you to manually add specific sites to the blacklists. As with network firewalls, content filters can be implemented for an entire network or on individual network hosts:   * A network-wide content filter usually sits near the network firewall and router, inspecting the contents of all incoming and outgoing network traffic. * A host-based content filter is implemented as software on a specific host. |
| Do Not Allow Port Forwarding | Because of the wide-spread use of NAT routing to conserve registered IP addresses, some organizations implement port forwarding to allow access to internal network resources (such as a web server) from the internet.  However, when you enable port forwarding you allow untrusted traffic into the internal network, which should be an area of high security. In this configuration, you must rely on the security configuration of the internal host that is being accessed externally to protect the rest of the network. For this reason, port forwarding implementations should be avoided. |

13.9.4 Wireless Network Security Facts

As a system administrator, there are several best practices that you can employ to increase the security of a wireless network. The goal is to make the network more difficult to compromise and accordingly less attractive to an attacker. These best practices are listed in the following table:

|  |  |
| --- | --- |
| **Best Practice** | **Description** |
| Change Default Usernames and Passwords | You should change the default username and password used on wireless access points. The default username and password assigned to a device by the manufacturer are widely known and posted on the internet. |
| Manage the SSID | There are several practices you can implement regarding your wireless network's SSID to increase the security of the wireless network:   * Change the SSID from the default. Lists of default SSIDs assigned by manufacturers are posted on the internet. If you use the default SSID, an attacker can quickly determine the make and model of your access point. Using this information, an attacker can:   + Identify the default username and password used by that device.   + Research known security weaknesses associated with that device, making it easier to compromise your wireless network. * Use a network name that is not easily associated with your organization. * Disable SSID broadcast. If SSID broadcast is enabled, then the name of the network is advertised to all wireless devices within range of your wireless access points. Disabling SSID makes your wireless network harder to locate. |
| Implement Encryption and Authentication | You should implement encryption and authentication on your wireless network using the strongest algorithms available:   * Avoid implementing an open (unencrypted) network. * Avoid using WEP to protect the network. A WEP key can be cracked quickly with software available on the internet. * Use one of the following versions of WPA2 to implement wireless encryption and authentication:   + WPA2-PSK is best suited for wireless networks used by home or small business users. WPA2-PSK requires the same pre-shared key to be configured on the access point and on each wireless client. This key is used to both authenticate the host to the wireless network and to encrypt transmissions.   + WPA2-Enterprise is a best suited for wireless networks that are part of a large corporate network. WPA2-Enterprise requires a separate authentication process to access the wireless network. Whenever a host wants to connect, credentials are forwarded to a RADIUS server for authentication. |
| Implement MAC Address Filtering | MAC address filtering restricts access to the wireless network to hosts that have specific MAC addresses. This can be done in two different ways:   * Use a whitelist, which defines a list of MAC addresses that are allowed to connect. * Use a blacklist, which defines a list of MAC addresses that are not allowed to connect.   With MAC address filtering enabled, the access point checks a computer's MAC address when it connects to the wireless network. If the access point has been configured to use a whitelist, it will compare the computer's MAC address to the whitelist. If its address is listed in the whitelist of allowed MAC addresses, then the access point will allow the host to connect to the network. If the computer's MAC address is not in the whitelist, then the host will be denied access.  If the access point is configured to use a blacklist, the opposite occurs. If the computer's MAC address is on the blacklist, the access point will not allow the host to connect to the network. If its MAC address is not listed in the blacklist, the access point will allow the computer to connect to the network.  For security reasons, whitelists are usually the preferred option. This configuration locks out all hosts except for those specifically allowed in the whitelist. However, MAC address filtering provides only a basic level of network security and can be defeated by determined attackers. However, it does make the network harder to compromise and hopefully less attractive to  attackers. |
| Implement Static IP Addressing | Most wireless access points provide a DHCP server function within the firmware of the device. Using DHCP makes it very easy for wireless hosts to connect to the wireless network. However, it also decreases the security of the network. With DHCP is enabled, the access point provides any wireless client with the appropriate information needed to communicate with other hosts on your network.  If you implement static IP addressing, then wireless hosts must be statically configured with this information. This increases security because it makes it more difficult for attackers to connect to your wireless network. Even if they manage to associate with the access point, they still have to figure out what IP addressing information is required. This won't stop determined attackers, but it does make their job more difficult.. |
| Manage Antenna Placement | You need to reduce data emanation as much as possible. If your network's radio signal emanates outside your facility, an attacker can intercept that signal and potentially gain access to your organization's computer network. You can minimize data emanation by doing the following:   * Consider where wireless access points are placed and where their antennae are transmitting the wireless network's radio signal. Be aware that omni-directional wireless access points transmit in all directions with equal signal strength. If placed near an exterior wall, these antennae will transmit the wireless network's radio signal outside the structure. * Implement directional antennas, which can be aimed in a certain direction. Use these antennae to ensure your wireless network's radio signal is aimed only towards the interior of your facility. |
| Manage Power Levels | Most wireless access points are set to run at maximum power by default. However, this can result in the wireless network's radio signal being transmitted outside of your facility. Usually you can decrease an access point's signal strength to reduce emanation. However, this will require additional access points to be deployed because the reduced signal strength can create areas of poor coverage. Usually, directional antennae are used in conjunction with customized power levels to provide the best coverage while reducing data emanation.  You should use a site survey tool to measure the strength of the wireless signal at various locations both inside and outside the structure to customize the configuration of each access point. This ensures appropriate wireless coverage with minimal emanation. |
| Disable Wi-Fi Protected Setup (WPS) | While WPS makes wireless networks easier to manage, it also introduces security issues. For example, devices that support the PIN number method have been found to be susceptible to brute-force attacks. An attacker can simply send one PIN number after another to an access point until the correct one is identified. If the access point is not physically secured (which is common in small business and in homes) then attackers can use the push-button or NFC methods to associate their device with the access point. Because of these issues, a best practice is to disable WPS functionality on the access point. |