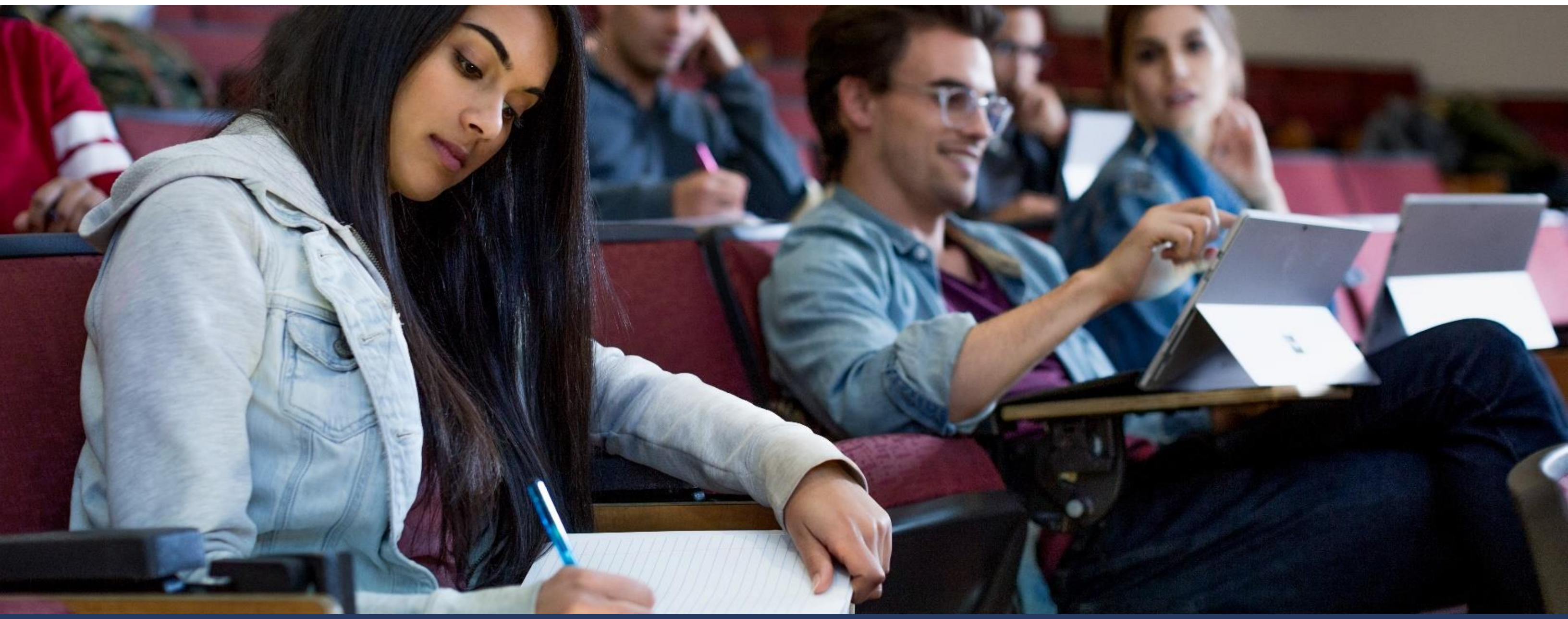


40555A Networking Fundamentals

Module 3: Media types

Contents

Learning objectives based on the Microsoft Technology Associate (MTA) exam objectives

#	Lesson title	Learning objectives	Exam objectives mapped
1	Cable types	• Describe coaxial cable. • Describe twisted-pair cable. • List and explain the Category X (CATx) cabling standards. • Describe the features of fiber optic cabling. • Explain susceptibility to interference. • Explain susceptibility to interception.	2.3.1 Cable types and their characteristics, including media segment length and speed 2.3.2 Fiber optic 2.3.3. Twisted pair shielded or unshielded 2.3.4 CATxx cabling 2.3.6 Susceptibility to external interference (machinery and power cables) 2.3.7 Susceptibility to electricity (lightning) 2.3.8 Susceptibility to interception

#	Lesson title	Learning objectives	Exam objectives mapped
2	Wireless networking	• Describe the wireless networking standards. • Explain wireless network security. • Explain wireless networking modes. • Explain how to configure wireless settings in the Windows 10 operating system.	1.4.1 Types of wireless networking standards and their characteristics (802.11a,b,g,n,ac including different GHz ranges) 1.4.2 Types of network security (WPA, WEP, 802.1X, and others) 1.4.3 Point-to-point (P2P) wireless 1.4.4 Ad hoc networks 1.4.5 Wireless bridging 2.3.5 Wireless

Module overview

To connect network devices together, you must implement either wired media types, a wireless network infrastructure, or both. In this module, we'll examine the different media types, their susceptibility to interference, and common wireless standards.

Objectives

After completing this module, you will be able to:

- Describe wired media types.
- Explain how to implement a wireless network.

Lesson 1: Cable types

Wired networks are still quite popular despite the growing number of wireless networks. Most organizations use wired networks for most of their on-site devices, enabling wireless access as needed. In this lesson, we'll explore the different network media types and describe their uses.

Objectives

After you complete this lesson, you will be able to:

- Describe coaxial cable.
- Describe twisted-pair cable.
- List and explain the CATx cabling standards.
- Describe the features of fiber optic cabling.
- Explain susceptibility to interference.
- Explain susceptibility to interception.

Coaxial cable

Coaxial cable was used widely in the early days of networking. Ethernet was wired by using a single length of thick coaxial cable. Figure 1 depicts the internal components of a typical coaxial cable:

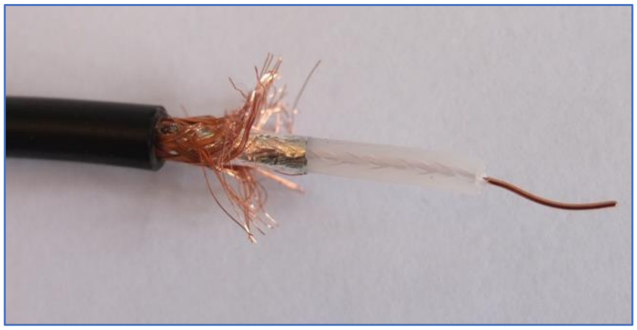


Figure 1. Coaxial cable

But what is coaxial cable? A coaxial cable consists of several elements. From the outside in, these are:

- An outer insulating sheath made of plastic
- A braided copper shield
- A foil separator
- An inner insulator, again made of plastic
- A solid copper core

Coaxial cables are used in a number of situations, including:

- Telephone cabling
- Broadband internet cabling
- Television cabling
- Radio cabling
- Data cabling

It's the last of these that interests us. Coaxial cable supports high-speed, high-frequency transmissions with lower data-loss. Consequently, it was used to support early networks.

Many different types of coaxial cabling exist, each suited to a different application. However, for data networking, the two predominant standards are:

- RG-8/U. This cabling is used for Ethernet and is known as *ThickNet*. It uses a baseband transmission system, and because the original speed of Ethernet was 10 megabits per second (Mbps), it was also known as *10Base5* (the 5 refers to the maximum distance run for the cable—500 meters).
- RG-58. This cabling is also used for Ethernet over 200-meter distances. RG-58 uses thinner coaxial cable and is often called *ThinNet*. When used for Ethernet, the cabling was sometimes known as *10Base2*.

Twisted pair

As discussed in Module 2, "Local area networks and wide area networks," most modern Ethernet systems are star wired using twisted-pair cabling. As suggested by the name, twisted-pair cabling comprises a series of cables that are twisted together in pairs. Sometimes these twisted pairs are shielded to provide high levels of protection against external interference.

Most twisted-pair cabling is based on four pairs of wires: two blue, two orange, two green, and two brown pairs. Each pair of wires are independently twisted together, and then the four twisted pairs are twisted together, as Figure 2 depicts:

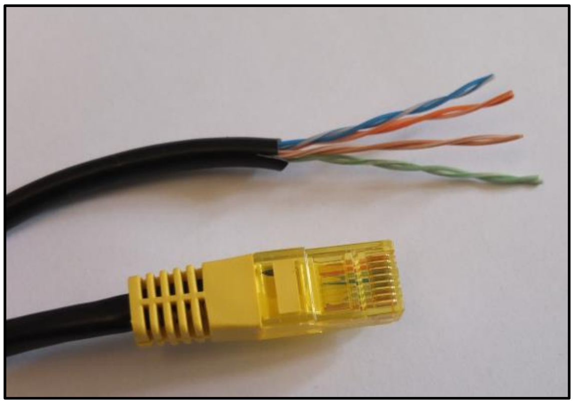


Figure 2. Twisted-pair cable and an RJ45 connector

Twisting the cables together helps reduce interference, which we'll discuss further in the next lesson.

Note

Twisted-pair cabling supports cable runs of up to 100 meters. Beyond this distance, you must extend the network with a repeater, a switch, or a router. You could also use another type of cabling, such as fiber optic, that supports longer cable runs.

Over the years, the order in which these pairs of wires are connected to an RJ45 connector have changed. The current standard is known as Telecommunications Industry Association/Electronics Industries Alliance (TIA/EIA)-568B, or 568B for short. This standard defines that the wires are connected as described in the following table. To connect the cable to the connector, you open the plastic connector, lay the cables onto the contacts in the correct order (refer to the cabling order table that follows), and then using a crimping tool, close the connector over the cables. The crimping and closing process makes the electrical connections through the cables.

An earlier standard, known as 568A, uses a different cabling order at the connector. Depending on the application, you might encounter both types of connections.

For example, you might use:

- Straight-through cable to connect a computer or other device to a wiring concentrator such as a hub, or more likely, a switch. A straight-through cable is connected by using the 568B arrangement at both ends. More information on hubs and switches is coming in the next module.

- Crossover cable to connect two devices back to back. For example, two computers can be connected via their RJ45 connections by using a crossover cable without requiring a hub or switch. To create a crossover cable, connect one end using the 568B pinouts and the other end using 568A pinouts.

Cabling order

The following table lists the correct cabling order for both the 568A and 568B standards.

PIN	568A	568B
1	White-green	White-orange
2	Green	Orange
3	White-orange	White-green
4	Blue	Blue
5	White-blue	White-blue
6	Orange	Green
7	White-brown	White-brown
8	Brown	Brown

Note

It’s worth noting that although four pairs of wires are available and all eight wires are connected, Ethernet (the predominant network topology), uses only half of these; specifically, pins one, two, three, and six. However, to only connect those wires would be foolhardy. It’s far easier to connect them all per the 568B standard and simply not use the other pins than to replace all the wiring and connectors if you later implement a technology that requires eight pins.

Shielded vs. unshielded twisted pair

Twisted-pair cabling can be shielded or unshielded. Let’s review the differences.

Shielded twisted pair

Shielded twisted pair (STP) was originally developed for use with IBM’s token ring network topology, which we discussed in Module 1, “Overview of networking.” STP has shielding that’s provided by a foil-wrapped braided copper jacket. These layers provide protection against interference, enable higher speeds, and support longer cable runs. However, STP cable is quite thick and unwieldy. Consequently, STP is only used when additional protection is needed or if a longer cable run is required.

Unshielded twisted pair

Unshielded twisted pair (UTP) is the most common cabling that you’ll likely encounter. Because it lacks the extra layering and uses only a thin plastic jacket, it’s far more flexible. Consequently, it’s ideal for wiring workstations and other desktop devices, and within tight spaces in wiring closets.

CAT cabling standards

UTP has been around for quite a while, but the standards that define the characteristics of the cabling and the applications for which it’s suited have evolved. These standards are known as the *CAT standards*. The following table identifies the different standards you’re likely to encounter.

Specification	Bandwidth	Use	Technical
Cat 3	10 Mbps	Suitable for networks that support a bandwidth of up to 10 Mbps	Ethernet over twisted pair, up to 100 meters
Cat 5	100 Mbps	Suitable for networks that support a	Ethernet and Fast Ethernet over twisted pair, up to 100 meters

Specification	Bandwidth	Use	Technical
		bandwidth of up to 100 Mbps	
Cat 5e	1 Gbps	Suitable for networks that support a bandwidth of up to 1 gigabit per second (Gbps)	Ethernet, Fast Ethernet, and Gigabit Ethernet over twisted pair, up to 100 meters
Cat 6	10 Gbps	Suitable for networks that support a bandwidth of up to 10 Gbps	Gigabit Ethernet (100 meters) and 10G Ethernet (55 meters) over twisted pair
Cat 6a	10 Gbps	Suitable for networks that support a bandwidth of up to 10 Gbps	Gigabit Ethernet (100 meters) and 10G Ethernet (55 meters) over twisted pair
Cat 7	10 Gbps	Suitable for networks that support a bandwidth of up to 10 Gbps	Gigabit Ethernet and 10G Ethernet over twisted pair, up to 100 meters

Fiber optic

Copper cabling uses electrical signals (electrons) to transmit data. Fiber optic cable (fiber cable) uses light (photons) to transmit data. Fiber optic cable supports faster data transfer rates and longer cable runs. However, fiber cable is generally more expensive than UTP. Because of the cost difference, fiber cable is usually used for backbone networks and storage area networks where throughput is critical.

Fiber optic cable can support two modes of operation:

- Single mode. Single-mode fiber cable supports a single beam of photons and long cable runs—up to 70 kilometers (km).
- Multimode. Multimode fiber cable supports multiple beams of photons. Because more data is being carried, the cable runs are shorter, at around 550 meters (m).

The following table identifies the characteristics of various fiber cabling standards when implemented to support Ethernet.

Specification	Bandwidth	Mode	Distance
100Base-SX	100 Mbps	Multimode	550 m
100Base-BX	100 Mbps	Single	40 km
1000Base-SX	1 Gbps	Multimode	550 m
1000Base-LX	1 Gbps	Single	5 km
1000Base-ZX	1 Gbps	Single	70 km
10GBase-LR	10 Gbps	Single	25 km
10GBase-LRM	10 Gbps	Multimode	220 m
10GBase-ER	10 Gbps	Single	40 km

Susceptibility to interference

Any kind of wiring is potentially susceptible to interference. Broadly, the three types of interference are:

- Crosstalk. *Crosstalk* occurs when adjacent wires electromagnetically interfere with one another's signals. Crosstalk is less common with digital data over UTP, but it can occur. In these situations, you should use STP, which is less susceptible.

- Electromagnetic interference (EMI). The electrical devices that are all around us cause EMI. These can include heating and cooling systems, televisions, phone chargers, and electrical motors. All copper cabling is susceptible to EMI. As such:
  - Avoid running cables next to EMI sources.
  - Use STP where necessary to provide additional protection against EMI.
  - Consider shielding the source of the EMI.
- Radio frequency interference (RFI). Transmissions from AM/FM radio stations and from cellphone towers cause RFI. One obvious solution is to make sure that your offices aren't beneath a transmitter, but that's not always feasible. If you have problems with RFI, consider:
  - Installing filters in your network cabling infrastructure that absorb RFI.
  - Using STP where necessary to provide additional protection.

Susceptibility to interception

Security should always be a concern on any network because data is at risk when in transit. One common security threat is the potential for someone to eavesdrop on network traffic. Although eavesdropping (*interception*) is more of a concern with wireless networks, because a malicious hacker doesn't need physical access to your network to join it, wired networks are also at risk. This is because the electromagnetic field that cabling generates as it carries electrical signals around a network can be captured. To help avoid this issue, consider using the following mitigation options:

- Use shielded cabling where necessary.
- Use fiber cabling, which doesn't suffer from data emanation (the name given to this effect).

Another solution is to use additional networking protocols such as Internet Protocol security (IPsec), which enable authentication and encryption on the network media between devices. In this case, it won't matter if someone succeeds in capturing conversations because they will be unreadable without the required security settings.

Lesson 2: Wireless networking

An increasing number of devices use wireless connections as the primary method for accessing organizational intranets and the internet. Additionally, many users have come to expect a wireless infrastructure in a corporate workplace. Consequently, a good working knowledge of wireless connectivity is a requirement for network administrators. This lesson discusses various wireless standards and the configuration and support of Windows 10 wireless clients.

Objectives

After you complete this lesson, you will be able to:

- Describe the wireless networking standards.
- Explain wireless network security.
- Explain wireless networking modes.
- Explain how to configure wireless settings in the Windows 10 operating system.

Wireless networking standards

The 802.11 standard has been evolving since 1997, and many improvements in transmission speed and technology security have emerged since then. Each new standard is designated by a letter of the alphabet, as the following table indicates.

Specification	Description
802.11a	This is the first extension to the original 802.11 specification. It provides up to 54 Mbps and operates in the 5 gigahertz (GHz) range. However, it’s not compatible with 802.11b.
802.11b	This specification provides 11 Mbps and operates in the 2.4 GHz range.

802.11e	This specification defines Quality of Service and multimedia support.
802.11g	This specification is for transmission over short distances at speeds up to 54 Mbps. It's backward compatible with 802.11b and operates in the 2.4 GHz range.
802.11n	This specification adds multiple input and multiple output, thereby providing increased data throughput at speeds up to 100 Mbps. It vastly improves speed over previous specifications, and it supports both the 2.4 GHz and 5 GHz ranges.
802.11ac	This specification builds on 802.11n and can attain data rates of 433 Mbps. 802.11ac operates only in the 5 GHz frequency range.

Wireless networking security

Security is one of the biggest considerations for organizations that are planning a wireless implementation. Because wireless traffic travels across open airwaves, it's susceptible to interception. Therefore, organizations use several security technologies to address these concerns, and most wireless devices support multiple security standards. The following table describes the current security methods that are available for wireless networks.

Security method	Description
Wired Equivalent Privacy (WEP)	WEP is the oldest form of wireless security. Some devices support different versions of WEP: • WEP 64-bit key • WEP 128-bit key • WEP 256-bit key The security issues surrounding WEP are well documented, so you should avoid using WEP unless it's the only alternative.

Security method	Description
Wi-Fi Protected Access (WPA)	Developed to replace WEP, WPA has two variations: • WPA-Personal. This is for home and small business networks. Easier to implement than WPA-Enterprise, it involves providing a security password, and it uses a technology called Temporal Key Integrity Protocol. The password and the network Service Set Identifier (SSID) generate constantly changing encryption keys for each wireless client. • WPA-Enterprise. This is for organizational networks, and it uses a Remote Authentication Dial-In User Service (RADIUS) server for authentication.
WPA2	This is an improved version of WPA that has become the wireless network security standard. WPA2 employs the Advanced Encryption Standard (AES), which employs larger encryption key sizes.

The security methods that a wireless device supports depend on the vendor and the device's age. Most modern wireless devices support WPA2.

Wireless networking modes

You can use wireless networking in three different modes:

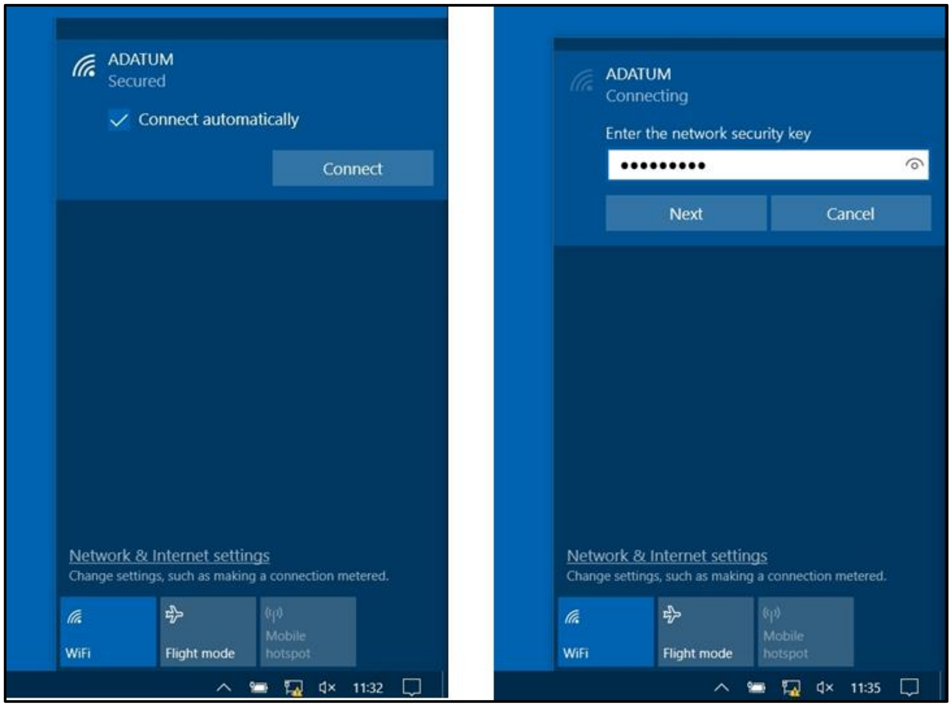
- Ad hoc. Ad hoc mode networks can connect wireless devices dynamically in a peer-to-peer configuration without using any infrastructure devices.
- Infrastructure wireless. These networks consist of wireless LANs (WLANs) and cellular networks, and they require using a device such as a wireless access point to enable communications between client wireless devices. You can manage infrastructure wireless networks centrally.
- Wi-Fi Direct. Similar to ad hoc mode, Wi-Fi Direct is used to connect peripheral devices to one another or to computer devices.

Note

Wireless bridging, which some wireless access points support, enables you to connect wired networks together over a wireless connection.

Configure wireless network settings in Windows 10

Windows 10 supports wireless networking. However, first you must connect to, and configure, your wireless networking settings, as Figure 3 depicts:



Change settings, such as making a connection metered.

Change settings, such as making a connection metered.

Figure 3. Wireless connection dialog boxes

Connect to a wireless network

To connect to a wireless network, use the following procedure:

1. Select the wireless network icon in the notification area for a list of available wireless networks.

2. Select the network of your choice.

3. Select **Connect**.

4. When prompted, enter the required security information of the wireless hub to which you're connecting your device, and then select **Next**.

Configure wireless networks

To configure a wireless network, use the following procedure:

1. Open Settings.

2. On the Settings page, select Network & Internet.

3. On the **Network & Internet** page, select **Wi-Fi**.

4. On the **Wi-Fi** page, choose the following options:

    - Find paid plans for suggested open hotspots near me

    - Connect to suggested open hotspots

    - Let me use Online Sign-Up to get connected

5. At the top of the page, select **Manage known networks**.

6. On the **Manage known networks** page, select the network that you want to manage.

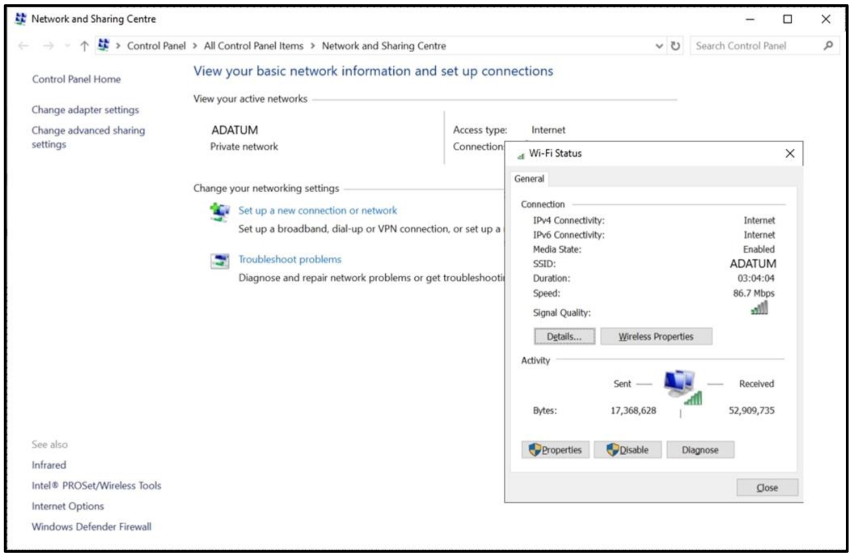
7. Select to either View Properties or Forget the network.

Configure advanced wireless properties

From the **Network and Sharing Center**, you can also configure advanced wireless properties, as Figure 4 depicts.

To configure advanced wireless properties:

1. Open **Settings**.
2. On the **Settings** page, select **Network & Internet**, and then select **Network and Sharing Center**.
3. In the **Network and Sharing Center**, select the name of your wireless network adapter.
4. Select **Wireless Properties** to review additional information, including the security settings of the connection, as Figure 4 depicts:



View your basic network information and set up connections

View your active networks

ADATUM
Private network

Access type: Internet
Connection

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up or VPN connection, or set up a

Troubleshoot problems
Diagnose and repair network problems or get troubleshooti

Connection
IPv4 Connectivity: Internet
IPv6 Connectivity: Internet
Media State: Enabled
SSID: ADATUM
Duration: 03:04:04
Speed: 86.7 Mbps
Signal Quality:

Bytes: 17,368,628 52,909,735

Figure 4. Network and Sharing Center and a Wi-Fi Status dialog box

Learning in action: Implement media types

Scenario

Lucerne Publishing hired you to help with a major rollout of new branch offices and retail outlets. These sites are spread out around the United Kingdom. You've been planning the cabling and infrastructure for these new locations.

Questions

1. **How should Lucerne Publishing approach wiring its branch offices?**

   A. Use STP

   B. Use wireless

   C. Use UTP

2. **In one of the locations, a printing office is located about 1 km away from the nearest branch office. Assuming the necessary local authority permissions are granted, what fiber networking standards support cable runs of this distance?**

   A. 100Base-SX

   B. 1000Base-SX

   C. 1000Base-LX

   D. 10GBase-LRM

3. **You decide to deploy twisted-pair cabling at the branch office in Windsor. You must support Gigabit Ethernet. What could you use?**

   A. Cat 3

   B. Cat 5

   C. Cat 5e

   D. Cat 6

4. **Wireless access is important at all branches to support users' own devices and to facilitate guest access to the internet. What wireless standard should you implement?**

   A. 802.11a

   B. 802.11ac

   C. 802.11b

   D. 802.11n

5. **What kind of wireless security will you implement in the branch offices?**

   A. WEP

   B. WPA-Enterprise

   C. WPA2

Test your knowledge

1. **Which coaxial cable standard is also known as ThinNet when implemented to support Ethernet?**

   A. RG-8/U

   B. RG-58

   C. 100Base-T

   D. 10Base-5

2. **Which of the following types of interference is caused by proximity to radio and cellphone transmission towers?**

   A. Crosstalk

   B. EMI

   C. RFI

3. **Which of the following wireless networking standards supports 100 Mbps speeds and higher? Choose all that apply.**

   A. 802.11a

   B. 802.11e

   C. 802.11n

   D. 802.11ac

Fill in the blanks for the following questions.

4. **Using thin coaxial cable, I can connect Ethernet devices up to a maximum of ( ) meters.**
5. **A straight-through UTP cable uses ( ) pinouts at both ends.**
6. **Cat ( ) is the minimum standard for cabling that will support speeds of up to 1 Gbps.**
7. **True or false: Wi-Fi Direct requires a wireless access point.**

   True

   False

8. **True or false: Multimode fiber cables support longer cable runs than single-mode fiber cables.**

   True

   False

Study the following scenario and answer the question.

9. **Josh, the owner of Fourth Coffee, wants to use wiring to connect various office devices in a LAN. He also wants to interconnect the point-of-sale devices.**

   What sort of wiring should you install in the coffee shops to address his needs? And what network standard should be met?

Study the following scenario and answer the question.

10. **Josh just read an article online about data security. He's concerned about eavesdropping and worries that customers could take advantage of data emanation. Josh is also worried about the iPads his employees use. These connect wirelessly to the network via a wireless access point that is cabled into the network.**

    What single thing could you do to alleviate Josh's concerns and solve the data emanation and wireless eavesdropping problems?

Glossary

Term	Definition
568A	An older cabling standard for twisted pair
568B	The current cabling standard for twisted pair
802.11x	Wireless networking standards, including 802.11a, 802.11b
Coaxial cable	A cable consisting of multiple concentric layers used for broadband, television, telephone, and radio cabling
CAT standards	Defines the characteristics of UTP cabling applications
Crosstalk	Occurs when adjacent wires electromagnetically interfere with each other's signals
Multimode fiber cable	Supports multiple beams of photons. Because more data is being carried, the cable runs are shorter, at around 550 meters
Single-mode fiber cable	Supports a single beam of photons. Single-mode fiber cable supports long cable runs up to 70 km
Twisted-pair wire	Four wiring pairs twisted together. Twisted-pair wire is commonly used in data networking
WPA2	An improved version of WPA that has become the wireless network security standard