< Previous Unit 3 of 6 ⌄ Next >

200 XP

Knowledge check

11 minutes

A network can't exist unless each of the devices can communicate with each other. This fact applies whether it's your organization's network or more extensive networks, like the web. All networks are built on the same principles.

In this unit, you learn about the term *network standards* and explore the hardware that forms the backbone of any network.

Network standards

While network protocols provide a unified method for communication, network standards govern the hardware and software that use them.

Today, there are hundreds of thousands of hardware suppliers. Yet all of their technology seamlessly integrates with your computer or network with minimal effort. Network standards provide a framework that enables the interoperability between devices.

Network standards improve the interoperability of different network-enabled devices and provide backward compatibility between product revisions and differing vendors. The official bodies that publish regulated standards are the International Telecommunication Union (ITU), the American National Standards Institute (ANSI), and the Institute of Electrical and Electronics Engineers (IEEE).

It would be impossible to build networks and connect network-enabled devices reliably without network standards.

The 802 family of standards

The 802 specification covers all the physical networking standards for both Ethernet and wireless. The following table shows some of the more widely used standards.

Expand table

802	Overview	Basics of physical and logical networking concepts
802.1	Bridging	LAN/MAN bridging and management of the lower sublayers of OSI Layer 2
802.2	Logical Link	Commonly referred to as the logical link control (LLC) specification
802.3	**Ethernet**	Provides asynchronous networking by using carrier sense, multiple accesses with collision detect (CSMA/CD) over coaxial cable, twisted-pair copper cable, and fiber media
802.5	Token ring	The token-passing standard for shielded copper cables and twisted-pair cable
802.11	Wi-Fi	Wireless local area network (WLAN) media access control (MAC) and physical layer (PHY) specification
802.11a	Wi-Fi	Specifies a PHY that operates in 5 GHz
802.11b	Wi-Fi	Enhances 802.11, adds higher data rate modes
802.11d	Wi-Fi	Enhances 802.11a/b, allows for global roaming
802.11e	Wi-Fi	Enhances 802.11, adds Quality of Service (QoS) features

802	Overview	Basics of physical and logical networking concepts
802.11g	Wi-Fi	Extends WLAN maximum data rate
802.11 h	Wi-Fi	Enhances 802.11a, now resolves interference issues
802.11i	Wi-Fi	Enhances 802.11, adds security for WLAN applications
802.11j	Wi-Fi	Enhances 802.11a for Japanese regulatory extensions
802.11n	Wi-Fi	Higher-speed standards
802.12	Demand Priority	Ethernet data rate increased to 100 Mbps
802.15	Wireless personal area networks	Support for wireless personal area networks (WPANs)
802.15.1	Bluetooth	Short-range (10 m) wireless technology
802.15.3a	UWB	Short-range, high-bandwidth ultra-wideband (UWB) link
802.15.4	ZigBee	Short-range wireless sensor networks
802.16	Wireless metropolitan area networks	Covers mobile and wireless broadband access in wireless metropolitan area networks (WMANs)

Network infrastructure

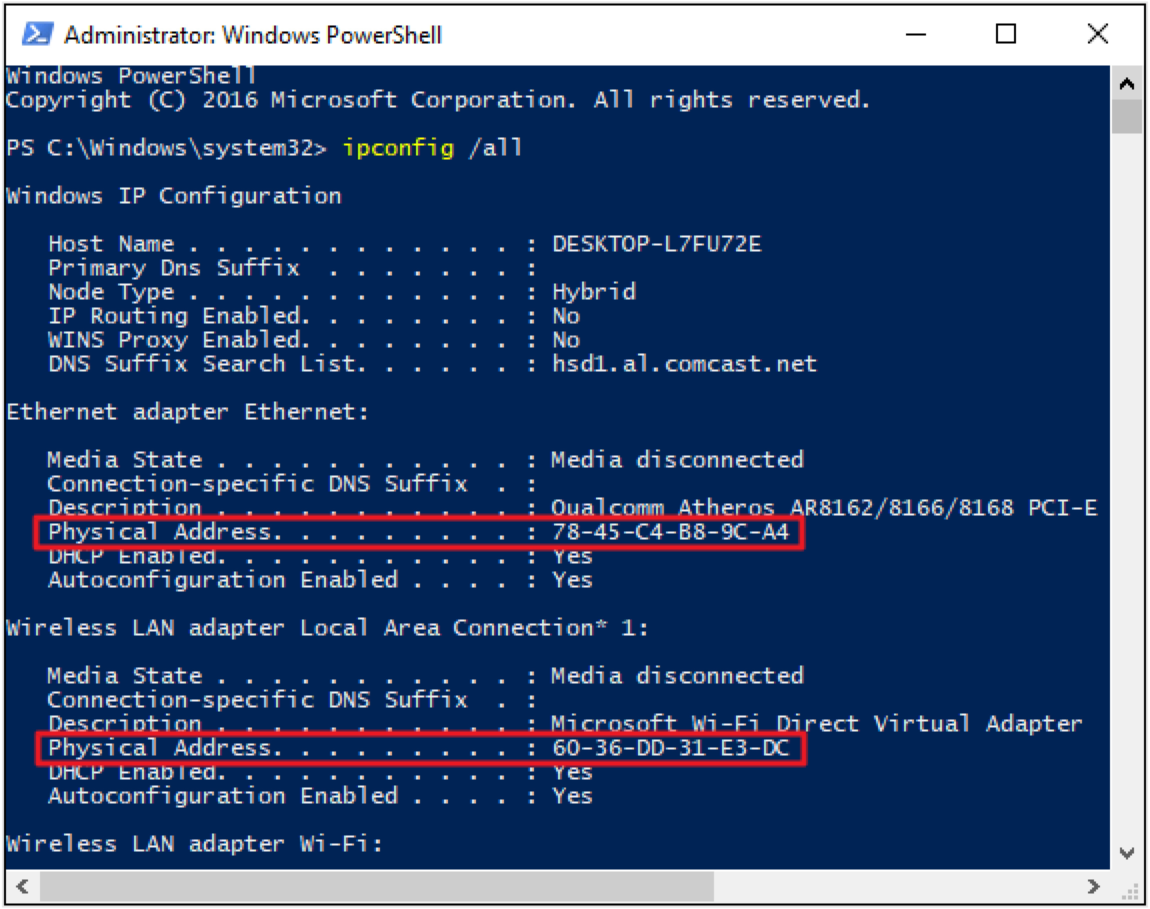
There are several network standard-compliant devices that make up the structure of your networks. Depending on the network's size, you might use several of these devices to build the backbone of your network. These devices are:

- Repeaters
- Hubs
- Bridges
- Switches
- Routers

Nearly all of these devices depend on a media access control or an Internet Protocol (IP) address to deliver data on the network.

What is a media access control address?

The media access control (MAC) address is a unique identifier assigned to every network-enabled device at the time of manufacture. It can be referred to as the burned-in address, the Ethernet hardware address, or a physical address.



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-L7FU72E
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : hsd1.al.comcast.net

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Qualcomm Atheros AR8162/8166/8168 PCI-E
   Physical Address. . . . . . . . . : 78-45-C4-B8-9C-A4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 60-36-DD-31-E3-DC
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:
```

The MAC address has a standard composition of six hexadecimal numbers separated by a colon or dash. The first three numbers of the MAC address define the manufacturer's organizationally unique identifier (OUI), and the remaining three numbers uniquely identify the device. For example, if the MAC address is `AA-6A-BA-2B-68-C1`, then the OUI is `AA-6A-BA` and the device ID is `2B-68-C1`.

Repeater

A repeater is a two-port device that repeats network signals. Repeaters are used when network devices are some distance from each other. The repeater doesn't modify or interpret data packets before it resends them, and it doesn't amplify the signal. Instead, it regenerates the data packet at the original strength, bit by bit.

Bridge

A bridge divides a network into network segments and can filter and forward data packets between these segments. Bridges use the network device's MAC address to determine the data package's destination. Typically, a bridge is used to improve network performance by reducing unnecessary network traffic on network segments.

Hub

A hub acts as a multiport repeater on a network. Hubs are used to connect more than one device and to structure the layout of a network. For example, you can cascade hubs to create network branches, or use as an endpoint to create a star layout with multiple-user-type devices. Hubs contain multiple ports that act as an input/output Ethernet connection between the hub and a network device. A hub can operate at only one speed, which is the speed of the slowest network device on the network. It doesn't interpret or filter data packets, and sends copies of each data packet to all attached devices.

Types of hubs

- **Fast Ethernet**: This hub is used for 100-Mbps networks, and comes as Class I and Class II type hubs. The primary difference between the two is the amount of delay in data transmission. A Class I hub introduces a signal delay of up to 140-bit times. A Class II hub has a delay of up to 96-bit times. The delay allows for the transcoding of data between different base types. Only two Class II hubs can be used in a hub-based network. Class II hubs increase the likelihood of packet collisions because of their higher speeds.
- **Dual speed**: With a traditional hub network, the slowest attached device governs the speed of the network. For example, if you had 10-Mbps and 100-Mbps devices connected to a network, the speed of the whole network was only 10 Mbps. Dual-speed hubs solve the problem by acting as a bridge between the two different-speed devices.

Hubs are used for small ad-hoc networks of a few devices, but are rarely used at an enterprise level.

Switch

A switch combines the functionality of a bridge and a hub. It segments networks and can interpret and filter packet data to send it directly to an attached network device. Switches use the network device's MAC address to determine the data package's destination. A switch operates in full-duplex mode, which means it can send and receive data to and from network devices at the same time.

Features

Modern Ethernet-based switches offer more functionality and capabilities than an Ethernet hub.

- An Ethernet switch can adjust the connection speed of an inbound packet to match the connection speed of the destination network.
- Many switches now support Power over Ethernet (PoE). PoE allows certain network devices, such as Voice over IP (VoIP) phones, to get power from the switch without needing a separate power supply.
- Other modules can be attached to the switch to enable functions like port mirroring, packet sniffers, and intrusion-detection systems.

Types of Ethernet switch

The two distinct types of switch are *unmanaged* and *managed*.

Unmanaged

This type of switch has no configuration capability and is designed for small-office or home-office environments. Packet switching occurs automatically.

Managed

This type of switch offers the means to adjust the configuration, behavior, and operation of the switch. Access to the switch configuration is either through a command-line interface (CLI) that uses Telnet or Secure Shell (SSH), Remote Console, or a web interface.

Here's a list of the more commonly available options to configure on a managed switch. Keep in mind that switch manufacturers might offer different configuration options.

Expand table

Switch option	Description
Quality of Service	Manage LAN traffic so that critical systems are given higher priority. An example is voice-data packets, which need to be delivered quickly.
Virtual LANs	Create logical groups of devices in their own virtual LAN. Traffic in one virtual LAN doesn't cross over into another virtual LAN. This logical group of devices can improve the security and performance of the network.
Spanning Tree Protocol (STP)	Build resilience into your network by defining alternative network routes in case a cable or device fails.
Port mirroring	Use with a network analyzer to diagnose network issues and problems. During setup, the switch exports a copy of the network traffic to a single port.
Bandwidth rate-limiting	Allow fine control of the bandwidth used by specific ports. For example, allowing a high bandwidth for ports handling database or VoIP, and lower bandwidths for email.

Switch option	Description
MAC address filtering	Control by which network devices gain access through the switch.
SNMP client	Set up and configure SNMP with your network monitoring tools.

There are two subtypes of managed switches:

- **Smart**: A smart switch is a halfway point between an unmanaged and a managed switch. They tend to offer only a web-based interface to manage the configuration. The available options are virtual LANs, port mirroring, and bandwidth rate-limiting.
- **Enterprise**: The fully managed switch service previously described.

Router

Routers link networks with different ranged addresses together. They can interpret and filter data packets, and then forward them to the correct network. Routers use the network device's IP address information to route the data package to its destination. Most routers can now detect issues with data traffic that flows to any attached network and route or reroute it around the issue. A router is also called a gateway. When you configure network devices, you usually configure them with a default gateway IP address.

Interconnectivity

Routers in an interconnected network maintain a routing table that lists the preferred route between each of the networks. The router acts as the start of authority for all the network devices on its network. Routing information is shared between routers by using a routing protocol like the Border Gateway Protocol (BGP).

Types

Most routers use the BGP to share routing information. The type of information shared depends on the usage of the router and the functions they use.

There are several distinct classifications or types of routers available to service different network needs.

- **Access routers**: These routers tend to be low-cost devices with a simple routing need and are typically used in a home or in small satellite offices.
- **Distribution routers**: These routers compile traffic routing data from multiple routers. Distribution routers come with more significant memory and processing power. This type of router is designed to hold vast quantities of routing information and is often used to manage and control the quality of service across a WAN.
- **Edge routers**: An edge router operates at the boundary between your network and other networks, such as your local network and the internet. They act as gateways to filter traffic and route it internally or forward it based on the packet header. An edge router often comes with access control or firewalls to improve the security. It might also handle DHCP and DNS services.
- **Core routers**: Sometimes called enterprise routers, these routers are designed for higher bandwidths. They're used to connect different buildings or geographic locations together. Core routers usually have fewer features than edge routers because their primary focus is on minimizing packet loss and preventing congestion. They typically forward packets to edge routers.

Wireless router

This network device provides all the routing capabilities of a regular access router, but it also offers wireless access point functions. A wireless router or wireless access point is designed to provide a non-wired connection to your network. An edge router associated with your network handles any provision to access the internet or other networks. A wireless router lets you build a different type of network called a wireless local area network.

A wireless router shouldn't be confused with a wireless modem. A wireless modem is what you receive from your ISP for your home or office. It's the device that converts the signal from the ISP into one that's usable on a computer network. Wireless modems are typically combined with routers to let you create a private home or office network.

Azure options

Two Azure options can help with routing and managing network traffic.

Azure hub-spoke

Hub-spoke network topology in Azure is a reference architecture.

- The hub is usually an Azure virtual network that acts as the central connection point between the cloud and an on-premises network.
- Each spoke is also an Azure virtual network, connected to the hub via a peer network.

Connections between the cloud and the on-premises network can be made through a VPN gateway or Azure ExpressRoute.

Azure ExpressRoute

An ExpressRoute connection is a dedicated circuit between an on-premises network and the cloud that uses a higher bandwidth than a regular VPN gateway connection. A connectivity partner hosts an ExpressRoute circuit and provides a super-resilient connection.

Check your knowledge

1. What are network standards used for? *

○ To ensure that hardware conforms to a minimum standard necessary for a good network development.

○ To ensure that software is tightly constrained and meets the needs of the organization's network.

○ To ensure that hardware and software made by different vendors can work together seamlessly.

2. What is the primary purpose of a hub? *

○ A hub allows one Ethernet network device to send data packets to a specific Ethernet device.

○ A hub allows the connection of multiple Ethernet devices to make them act as a single network segment.

○ A hub allows multiple Ethernet network devices access to the internet.

3. What is the principal difference between hub routing and switch routing? *

○ Hub routing sends all packets to all connected devices. Switch routing sends packets to specific devices.

○ Hub routing sends packets to specific locations. Switch routing is only used to route traffic between switches.

○ Hub routing sends all packets to all connected devices. Switch routing is only used to route traffic between switches.

4. What does a router do? *

○ A router is a network device that determines the fastest and most efficient way to send data across a network.

○ A router is a network device that forwards data packets around faults in your network.

○ A router is a network device that forwards data packets between computer networks.

Check your answers

Check your answers