Chapter 8: Applied Networking
Chapter 8 - Sections & Objectives

- **8.1 Computer to Network Connection**
  - Connect a computer to wired and wireless networks.

- **8.2 ISP Connection Technologies**
  - Explain the purpose and characteristics of ISP connection technologies.

- **8.3 Internet Technologies**
  - Explain Cloud concepts and networked-host services.

- **8.4 Common Preventive Maintenance Techniques Used for Networks**
  - Explain how to perform preventive maintenance on networks using common techniques.

- **8.5 Basic Troubleshooting Process for Networks**
  - Explain how to troubleshoot networks.

- **8.6 Chapter Summary**
8.1 Computer to Network Connection
Networking Cards

- A wired or wireless network interface card (NIC) is required to connect to the network.
- After it is installed, IP settings must be configured either manually or dynamically.
- You can also configure advanced settings, such as speed, duplex, Wake on LAN, and quality of service (QoS).
Selecting a NIC

- Most network interfaces for desktop computers are either integrated into the motherboard or are an expansion card that fits into an expansion slot.
- Most laptop network interfaces are either integrated into the motherboard or fit into a PC Card or ExpressBus expansion slot.
- USB network adapters plug into a USB port and can be used with both desktops and laptops.
- Most NICs will have two LEDs:
  - Indicates the presence of a connection
  - Indicates that data transfer activity is present
Install or Update a NIC Driver

- Manufacturers publish new driver software for NICs.
  - May enhance the functionality of the NIC.
  - May be needed for operating system compatibility.
- When installing a new driver manually, disable the virus protection and close all applications.
- Select Start > Control Panel > Device Manager
- If a new NIC driver does not perform as expected after it has been installed, the driver can be uninstalled, or rolled back, to the previous driver.
Configure the NIC

- Every NIC must be configured with the following information:
  - Protocols
  - IP address
  - MAC address

- Alternate IP configuration in Windows simplifies moving between a network that requires using DHCP and a network that uses static IP settings. Windows uses the alternate IP configuration assigned to the NIC if no access to DHCP

- **Network Profiles** are used to provide an easy way to configure or apply network functions based on the type of network to be joined.
Advanced NIC Settings

- **Duplex and Speed**
  - Duplex and speed settings for a NIC can slow down data transfer rates on a computer if they are not matched with the device to which they are connected.

- **Wake on LAN**
  - WoL settings are used to wake up a networked computer from a very low power mode state.

- **Quality of Service**
  - QoS, also called 802.1q QoS, is a variety of techniques that control the flow of network traffic, improve transmission speeds, and improve real-time communications traffic.
Wireless and Wired Router Configurations

- To connect to a network, attach a straight-through Ethernet cable to the NIC port.
- The other end connects to a router or to a telecommunications port that is wired so that data will reach the router.
- For wireless connections, configure the router with the following:
  - Network Mode (set the 802.11 standard)
  - Network Name (SSID)
  - Channel (important when there are multiple APs in the network)
  - Wireless Security (should be WPA2)
Connecting to the Router

- After connecting the network cable, activity should be verified by looking at the LEDs.
- Set the network location.
- Log into the router via web browser using 192.168.0.1.
  - This is the factory default on many routers.
Basic Router Setup

- It is good practice to change the following default settings:
  - Router Name
  - Default IP address and network
  - Default password
  - SSID name
  - Wireless password
  - Strong encryption and authentication
  - Network Device Access Permissions
  - Basic QoS
Basic Wireless Settings

Configure basic settings to secure and increase the speed of the wireless network:

- **Network mode** - A mixed-mode allows 802.11b, 802.11g, and 802.11n devices.
- **Service Set Identifier (SSID)** - The name of the wireless network.
- **Channel** - 1, 6 and 11 do not overlap and should be used to avoid interference from other nearby wireless devices. Use one of these three channels for best results.
- **Wireless security modes**
  - Wired Equivalent Privacy (WEP)
  - Temporal Key Integrity Protocol (TKIP)
  - Advanced Encryption Standard (AES)
  - Wi-Fi Protected Access (WPA)
  - Wi-Fi Protected Access 2 (WPA2)
Testing Connectivity

- Use Windows GUI

![Wireless Network Connection Status Window](image)
Testing Connectivity

- Using Windows CLI
  - **Ipconfig** – displays basic configuration for all network adapters.
  - **Ping** – tests basic connectivity between devices.
  - **Net commands** – manage network computers, servers, and resources.
  - **Tracert** – trace the routes that packets take from your computer to a destination host.
  - **Nslookup** – tests and troubleshoots DNS servers.
Network Sharing

- All Windows computers on a network must be part of either a domain or a workgroup.
- Before computers can share resources, they must share the same domain name or workgroup name.
- Mapping a local drive is a useful way to access a single file, specific folders, or an entire drive between different operating systems over a network.
- Determine which resources will be shared over the network and the type of permissions users will have to the resources.
  - Read - user can view data in files and run programs
  - Change - user can add files and subfolders, change the data in files, and delete subfolders and files
  - Full Control - user can change permissions of files and folders
Sharing Resources in Windows 7 and Up

- Sharing and Discovery, located in the Network and Sharing Center, manages the settings for a home network.
  - Network discovery
  - File sharing
  - Public folder sharing
  - Printer sharing
  - Password protected sharing
  - Media sharing
- Access by using the following path:
  - Start > Control Panel > Network and Sharing Center
Network Shares and Drive Mapping

- Mapping a drive, which is done by assigning a letter (A to Z) to the resource on a remote drive, allows you to use the remote drive as if it was a local drive.

- The following are the permissions that can be assigned to the file or folder
  - **Read** – user can view and run program files
  - **Change** – In addition to Read permissions, the user can add files and subfolders, change the data in files, and delete subfolders and files
  - **Full Control** - In addition to Change and Read permissions, the user can change the permission of files and folders in an NTFS partition and take ownership of files and folders.
Remote Connections

- **Remote Desktop** allows technicians to view and control a computer from a remote location.
- **Remote Assistance** allows technicians to assist customers with problems from a remote location.
**Virtual Private Network (VPN)**

- **Virtual Private Network (VPN)** – a private network that connects remote sites or users together over a public network, like the internet.
- When connected via the VPN, users have access to all services and resources as if they were physically connected to their corporate LAN.
- Remote-access users must install the VPN client software which encrypts data before sending it over the Internet.
- VPN gateways establish, manage, and control VPN connections (also known as VPN tunnels).
- Secures confidential data when connecting to business services over unsecured connections.
Virtual Private Network (VPN)

- A Virtual Private Network (VPN) is a private network that uses a public network, like the Internet, to connect remote sites or users together.
8.2 ISP Connection Technologies
Internet Protocols

- Different applications have different transport reliability requirements
- TCP/IP provides two transport layer protocols:
  - **Transmission Control Protocol (TCP)**
    - Provides reliable delivery ensuring that all of the data arrives at the destination.
    - Uses acknowledged delivery and other processes to ensure delivery
    - Makes larger demands on the network – more overhead
  - **User Datagram Protocol (UDP)**
    - Provides just the basic functions for delivery – no reliability (datagrams are just sent)
    - Less overhead
    - Fewer delays in transmission
Internet Protocols

- TCP or UDP ???
  - There is a trade-off between the value of reliability and the burden it places on the network.
  - Application developers choose the transport protocol based on the requirements of their applications.
  - Port numbers - used by TCP and UDP to differentiate between applications and communication streams.
  - Checksum - checked to give assurance that data is not corrupted.
TCP and UDP Protocols and Ports

- A port is a numeric identifier used to keep track of specific conversations. Every message that a host sends contains both a source and destination port.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/IP</td>
<td>NA</td>
<td>A suite of protocols used to transport data on the Internet</td>
</tr>
<tr>
<td>NetBEUI/NetBIOS</td>
<td>137, 139, 150</td>
<td>A small, fast protocol designed for a workgroup network that requires no connection to the Internet</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>A communication protocol that establishes a request/response connection on the Internet</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>Uses authentication and encryption to secure data as it travels between the client and Web server</td>
</tr>
<tr>
<td>FTP</td>
<td>20/21</td>
<td>Provides services for file transfer and manipulation</td>
</tr>
<tr>
<td>SSH</td>
<td>22</td>
<td>Securesely connects to a remote network device</td>
</tr>
<tr>
<td>Telnet</td>
<td>23</td>
<td>Connects to a remote network device</td>
</tr>
<tr>
<td>POP3</td>
<td>110</td>
<td>Downloads email messages from an email server</td>
</tr>
<tr>
<td>IMAP</td>
<td>143</td>
<td>Downloads email messages from an email server</td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
<td>Sends mail in a TCP/IP network</td>
</tr>
</tbody>
</table>
Domain and Workgroup

- **Domain** - group of computers and electronic devices with a common set of rules and procedures administered as a unit.
- **Workgroup** - collection of workstations and servers on a LAN that are designed to communicate and exchange data with one another.
Windows 7 Homegroup

- Windows 7 computers that belong to the same workgroup can also belong to a homegroup.
- There can only be one homegroup per workgroup on a network.
- Computers can only be a member of one homegroup at a time.
- Homegroups allow for easy sharing of resources between members.
- The homegroup option is not available in Windows Vista and earlier.
- A standard user account with a network location profile of Home will allow a user to become a member of a homegroup.
Digital Subscriber Line (DSL)

- An "always-on" technology; there is no need to dial up each time to connect to the Internet.
- Uses the existing copper telephone lines to provide high-speed data communication between end users and telephone companies.
- Asymmetric DSL (ADSL) is currently the most commonly used DSL technology.
  - Has a fast downstream speed, up to 48 Mbps.
  - Upload rate of ADSL is slower.
  - Not the best solution for hosting a web server of FTP server.
# DSL Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ADSL</strong></td>
<td>Asymmetric DSL is most common. Downstream speed from 384 Kbps to 6 Mbps. Upstream speeds lower than downstream speeds.</td>
</tr>
<tr>
<td><strong>HDSL</strong></td>
<td>High Data Rate DSL provides equal bandwidth in both directions.</td>
</tr>
<tr>
<td><strong>SDSL</strong></td>
<td>Symmetric DSL provides the same speed, up to 3 Mbps, for uploads and downloads.</td>
</tr>
<tr>
<td><strong>VDSL</strong></td>
<td>Very High Data Rate DSL is capable of bandwidths between 13 and 52 Mbps downstream, and 16 Mbps upstream.</td>
</tr>
<tr>
<td><strong>IDSL</strong></td>
<td>ISDN DSL is DSL over ISDN lines. Uses ordinary phone lines. Requires ISDN adapters.</td>
</tr>
</tbody>
</table>
Line of Sight Wireless Internet Services

- Line of sight wireless Internet is an always-on service that uses radio signals for transmitting Internet access.
- Radio signals are sent from a tower to the receiver that the customer connects to a computer or network device.
- A clear path between the transmission tower and customer is required. The tower may connect to other towers or directly to an Internet backbone connection.
- The distance the radio signal can travel and still be strong enough to provide a clear signal depends on the frequency of the signal. Lower frequency of 900 MHz can travel up to 40 miles (65 km), while a higher frequency of 5.7 GHz can only travel 2 miles (3 km).
- Extreme weather condition, trees, and tall buildings can affect signal strength and performance.
WiMAX

- **Worldwide Interoperability for Microwave Access (WiMAX)** - 4G broadband, high-speed, mobile Internet access for mobile devices.
- **IEEE 802.16e**
- Download speeds up to 70 Mb/s and distances up to 30 miles.
- Uses low wavelength transmission, between 2 GHz to 11 GHz.
- **Fixed WiMAX** - A point-to-point or point-to-multipoint service with speeds up to 72 Mb/s and a range of 30 miles (50 km).
- **Mobile WiMAX** - A mobile service, like Wi-Fi, but with higher speeds and a longer transmission range.
Other Broadband Technologies

- **Cellular** – enables the transfer of voice, video, and data.
  - Recommend connection when people need access the Internet from many different locations.
  - 3G - Data speeds between 144 Kbs and 2 Mbs
  - 4G - Data speeds from 5.8 Mbs and up

- **Cable** - uses coaxial cable lines originally designed to carry cable television, a cable modem connects your computer to the cable company.
  - Capable of the fast transfer rates

- **Satellite** - uses a satellite dish for two-way communication.

- **Fiber Broadband** - provides the fastest connection speeds and bandwidth.
Selecting an ISP

- Four main considerations:
  - Cost
  - Speed
  - Reliability
  - Availability

<table>
<thead>
<tr>
<th>Type</th>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>POTS</td>
<td>Widely available</td>
<td>Very slow speeds cannot receive phone calls while connected</td>
<td>MAX 56 kbps</td>
</tr>
<tr>
<td>ISDN</td>
<td>Higher speeds than POTS</td>
<td>Still much slower than other broadband technologies</td>
<td>BRI - up to 128 kbps PRI - up to 2.048 Mb/s</td>
</tr>
<tr>
<td>DSL</td>
<td>Low cost</td>
<td>Distance from CO impacts speed</td>
<td>24 kbps - 100 Mb/s</td>
</tr>
<tr>
<td>Cable</td>
<td>Very high speed</td>
<td>Slow upload speeds</td>
<td>27 kbps - 160 Mb/s</td>
</tr>
<tr>
<td>Satellite</td>
<td>Available where DSL and cable are not</td>
<td>More expensive than other broadband technologies, and it is susceptible to weather conditions</td>
<td>9 kbps - 24 Mb/s</td>
</tr>
<tr>
<td>Cellular</td>
<td>Available to mobile users</td>
<td>Not accessible every where</td>
<td>20 kbps and up depending on the technology used</td>
</tr>
</tbody>
</table>
8.3 Internet Technologies
Data Centers and Cloud Computing

- Data center is a data storage and processing facility run by an in-house IT department or leased offsite.
- Cloud computing is an off-premise service that offers on-demand access to a shared pool of configurable computing resources.
- The three main Cloud services models are:
  - **Software as a Service (SaaS)** – best when an organization that does not have the technical knowledge to host and maintain applications at their local site.
  - **Platform as a Service (PaaS)**
  - **Infrastructure as a Service (IaaS)**
Data Centers and Cloud Computing

- Advantages of cloud:
  - The company only needs to pay for the amount of processing and storage capacity that it uses.
  - The company can increase processing and storage capacity as needed and then decrease capacity when it is no longer needed.
  - As the amount of data that the company uses increases, it becomes impractical for the data to be stored and processed in a single-tenant data center.
Data Centers and Cloud Computing

- The four Cloud deployment models are:
  - **Community Cloud** – built to meet a specific need
  - **Public Cloud** – services made available to the general population
  - **Hybrid Cloud** – made up of two or more clouds connected via a single architecture
  - **Private Cloud** – intended for a specific organization or entity, such as the government
Networked Host Services

- Hosts need a variety of services to securely access resources on the network and the Internet.
  - **Dynamic Host Configuration Protocol (DHCP)** dynamically assigns IP addressing information to hosts. (first service used on the PC.
  - **Domain Name Service (DNS)** is the method computers use to translate domain names into IP addresses.
  - Hypertext Transfer Protocol (HTTP) or the secure HTTP (HTTPS) are used by hosts to access web resources.
  - **File Transfer Protocol (FTP)** allows hosts to transfer data between a client and a server. Secure file transfer options include File Transfer Protocol Secure (FTPS), SSH File Transfer Protocol (SFTP), and Secure Copy (SCP).
  - **Simple Mail Transfer Protocol (SMTP)**, **Post Office Protocol (POP)**, and **Internet Message Access Protocol (IMAP)** are the protocols hosts used to send and receive email.
Networked Host Services (cont.)

- Hosts need a variety of services to securely access resources on the network and the Internet.
  - **Print servers** enable multiple computer users to access a single printer
  - **Proxy servers** are popularly used to act as storage or cache for web pages that are frequently accessed by hosts on the internal network.
  - **AAA** is a way to control who is permitted to access a network (authenticate), what they can do while they are there (authorize), and track what actions they perform while accessing the network (accounting).
  - **Intrusion Detection Systems (IDSs)** passively monitor traffic on the network while Intrusion Prevention Systems (IPSs) can detect and immediately address a network problem.
  - **Universal Threat Management (UTM)** include all the functionality of an IDS/IPS as well as stateful firewall services.
Network Devices

Network-attached storage (NAS)
- Consists of one or more hard drives, an Ethernet connection, and an embedded operating system
- The NAS device connects to the network, allowing users on the network to access and share files, stream media, and back up data to a central location
Network Devices

- **VoIP phones** - carry telephone calls over the data networks and Internet.
- **Hardware firewalls** - use various techniques for determining what is permitted or denied access to a network segment.
- **Internet appliance** – web TV, game consoles, Blu-ray players etc.
- **Purchasing Authentic Networking Devices** - Computer and network problems can be related to counterfeit components.
# Physical Media

<table>
<thead>
<tr>
<th>Cable System</th>
<th>Speed</th>
<th>Cables and Connectors</th>
<th>Maximum Cable Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>10Base2 (ThinNet)</td>
<td>10 Mbps</td>
<td>Coaxial uses a BNC or F connector. RG-6 cable</td>
<td>185 Meters (607 ft)</td>
</tr>
<tr>
<td>10Base5 (ThickNet)</td>
<td>10 Mbps</td>
<td>Coaxial uses an AUI 15-pin D-shaped connector</td>
<td>500 Meters (1640 ft)</td>
</tr>
<tr>
<td>10BaseT (Twisted-Pair)</td>
<td>10 Mbps</td>
<td>UTP uses an RJ-45 connector</td>
<td>100 Meters (328 ft)</td>
</tr>
<tr>
<td>100BaseTX (Twisted-Pair)</td>
<td>100 Mbps</td>
<td>UTP uses an RJ-45 connector</td>
<td>100 Meters (328 ft)</td>
</tr>
<tr>
<td>10BaseF</td>
<td>10 Mbps,</td>
<td>Fiber-Optic cable uses an ST, SC, LC connector</td>
<td>Multi-Mode up to 2000 Meters</td>
</tr>
<tr>
<td></td>
<td>100 Mbps, or</td>
<td></td>
<td>(6562 ft)</td>
</tr>
<tr>
<td></td>
<td>1 Gbps</td>
<td></td>
<td>Single-Mode up to 3000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Meters (9842 ft)</td>
</tr>
</tbody>
</table>
8.4 Common Preventive Maintenance Techniques Used for Networks
Network Maintenance

- Preventive maintenance for networks includes the condition of cables, network devices, servers, and computers to make sure that they are kept clean and are in good working order.
- You should develop a plan to perform scheduled maintenance and cleaning at regular intervals.
- Inform the network administrator if you notice any of these issues to prevent unnecessary network downtime.
- Performing preventative maintenance at regular intervals reduces in network downtime.
Preventive Maintenance for Networks

- Common preventive maintenance techniques should continually be performed for a network to operate properly.
  - Keep network rooms clean and change air filters often.
  - Checking the various components of a network for wear.
  - Check the condition of network/patch cables because they are often moved, unplugged, and kicked.
  - Label the cables to save troubleshooting time later. Refer to wiring diagrams and always follow your company's cable labeling guidelines.
  - The **uninterruptible power supply (UPS)** should be tested to ensure that you have power in the case of an outage.

- Network maintenance also includes educating users on IT policies and procedures
8.5 Basic Troubleshooting Process for Networks
Troubleshooting for Networks

**Step 1** Identify the problem
**Step 2** Establish a theory of probable causes
**Step 3** Test the Theory to Determine cause
**Step 4** Establish a Plan of Action to Resolve the Problem and Implement the Solution
**Step 5** Verify Full System Functionality and Implement Preventative Measures
**Step 6** Document Findings, Actions, and Outcomes
Step 1- Identify the Problem

- **System Information**
  - Manufacturer, model, OS, network environment, connection type

- **Open-ended questions**
  - What problems are you experiencing with your computer or network device?
  - What software has been changed recently on your computer?
  - What were you doing when the problem was identified?
  - What error messages have you received?
  - What type of network connection is the computer using?

- **Closed-ended questions**
  - Has anyone else used your computer recently?
  - Can you see any shared files or printers?
  - Have you changed your password recently?
  - Can you access the Internet?
  - Are you currently logged into the network?
Step 2 - Establish a Theory of Probable Causes

- Create a list of the most common reasons why the error would occur and list the easiest or most obvious causes at the top with the more complex causes at the bottom.
  - Loose cable connections
  - Improperly installed NIC
  - ISP is down
  - Low wireless signal strength
  - Invalid IP address
Step 3 - Test the Theory to Determine cause

- Testing your theories of probable causes one at a time, starting with the quickest and easiest.
  - Check that all cables are connected to the proper locations.
  - Disconnect and then reconnect cables and connectors.
  - Reboot the computer or network device.
  - Login as a different user.
  - Repair or re-enable the network connection.
  - Contact the network administrator.
  - Ping your default gateway.
  - Access remote web pages.

- If exact cause of the problem has not been determined after you have tested all your theories, establish a new theory of probable causes and test it.
Step 4 - Establish a Plan of Action to Resolve the Problem and Implement the Solution

- Sometimes quick procedures can determine the exact cause of the problem or even correct the problem.
- If a quick procedure does not correct the problem, you might need to research the problem further to establish the exact cause.
- Divide larger problems into smaller problems that can be analyzed and solved individually.

<table>
<thead>
<tr>
<th>Step 4: Establish a Plan of Action to Resolve the Problem and Implement the Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>If no solution is achieved in the previous step, further research is needed to implement the solution</td>
</tr>
<tr>
<td>• Helpdesk repair logs</td>
</tr>
<tr>
<td>• Other technicians</td>
</tr>
<tr>
<td>• Manufacturer FAQ websites</td>
</tr>
<tr>
<td>• Technical websites</td>
</tr>
<tr>
<td>• News groups</td>
</tr>
<tr>
<td>• Computer manuals</td>
</tr>
<tr>
<td>• Device manuals</td>
</tr>
<tr>
<td>• Online forums</td>
</tr>
<tr>
<td>• Internet search</td>
</tr>
</tbody>
</table>
Step 5 - Verify Full System Functionality and Implement Preventative Measures

- Verifying full system functionality and implement any preventive measures if needed.
  - **Ipconfig /all** is used to display IP Address information.
  - **Ping** is used to check network connectivity.
  - **Nslookup** is used to query Internet domain name server.
  - **Tracert** is used to determine the route taken by packets when they travel across the network.
  - **Net View** is used to display a list of computers in a workgroup.
- Have the customer verify the solution and system functionality.
Step 6 - Document Findings, Actions, and Outcomes

- Discuss the solution with the customer.
- Have the customer confirm that the problem has been solved.
- Document the process.
  - Problem description
  - Solution
  - Components used
  - Amount of time spent in solving the problem
Common Problems and Solutions for Networks

- Network problems can be attributed to hardware, software, or configuration issues.
- Common networking problems include:
  - Network cables are damaged or unplugged
    - Wrong duplex setting
  - Legitimate users are denied remote access
  - Device lacks sufficient addressing information
    - APIPA address assigned – check the NIC LED lights first and then the DHCP connection.
  - Users cannot access the Internet
    - The target web server is down.
    - DNS service is unavailable on the customer network.
  - User cannot map a drive or share a folder on the network
    - Check **Network Connection Details** in the Windows GUI for the appropriate network connection
  - Wireless issues
    - The wireless router is not broadcasting the SSID
    - The network does not support the wireless protocol in use by the laptop
8.6 Chapter Summary
Summary

- This chapter introduced the operation of computer networks. The following concepts from this chapter are important to remember:
  - Each device must have appropriate addressing in order to access network resources.
  - Wired devices are attached to a network using an Ethernet cable. Wireless devices authenticate and associate with a wireless access point.
  - Mapping a local drive is a useful way to access a single file, specific folders, or an entire drive between different operating systems over a network.
  - VPNs allow private connections over public networks.
  - Remote Desktop allows network administrators to remotely control a computer.
  - Examples of broadband technologies include DSL, cable, and cellular.
  - Data centers are facilities that provide data storage services.
  - Cloud computing use data centers to provide cloud services in a variety of deployment models.
  - Networked host services include DHCP, DNS, HTTP, FTP, SMTP, proxies, AAA, IPSs, and UTMs.
  - Networks require a systematic preventive maintenance and troubleshooting methodology.