6️⃣

Chapter 6 Applied Networking

Class	CompTIA A+
Created	@December 1, 2021 3:41 PM
Date	Wednesday
Importance	□
Materials	6.2.2.1 Common Problems and Solutions for Networking.pdf 6.2.2.2 Advanced Problems and Solutions for Network Connections.pdf 6.2.2.3 Advanced Problems and Solutions for FTP and Secure Internet Connections.pdf 6.2.2.4 Advanced Problems and Solutions Using Network Tools.pdf
Packet Tracer	6.1.5.3 Packet Tracer - Control IoT Devices.pka
Reviewed	☑
Study Schedule (Class notes)	
Type	Lecture

Device to Network Connection

Network addressing

Media Access Control (MAC) addressing

The MAC address is hard-coded onto the Ethernet or wireless network interface card (NIC) by the manufacturer. The address stays with the device regardless of what network the device is connected to.

- Ethernet LAN uses MAC addresses.
- An Ethernet MAC address, 48 bits, has two parts:
  - Organizationally unique identifier (OUI): the first 24 bits; this is the vendor or manufacturer portion of the address.
  - Vendor assigned (NIC, interface): the second 24 bits; it is assigned by the vendor and unique to that particular OUI.
- MAC addresses are typically represented in hexadecimal.
- Ethernet MAC addresses are used for NIC-to-NIC on the same network.
- A fingerprint is like a MAC address, which is used to uniquely identify you wherever your location; A mailing address is like an IP address, which can change.

Internet Protocol (IP) addressing

- IP addressing is assigned by network administrators based on the location within the network.

IPv4 addressing

- IP addresses allow devices to communicate with each other that are:
  - on the same network
  - on different network
- When your device prepares data to send out on the network, it must first determine whether to send data directly to the intended receiver or to a router. It will send it directly to the receiver if the receiver on the same network. Otherwise, it will send the data to a router. A router then uses the network portion of the IP address to route traffic between different network.
  - Routers are used to forward messages between IP networks.
- IPv4 addresses are 32-bit decimal addresses and divided into four 8-bit octets:
  - 192.168.1.100 as an example
  - 255.255.255.0 is a 32-bit subnet mask which has specific values, which are all 1 bits with the rest of the 32 bits all 0bits.
  - Subnet masks are also represented using a "/" followed by the number of 1 bits.
  - 255.255.255.0 can also be represented using /24
- An IP address has two parts:
  - Network portion: 192.168.1 is the network portion
  - Host portion: 100 is the host portion

IPv6 addressing

- IPv6 addresses are 128-bit hexadecimal addresses and divided into eight 16-bit octets.
- IPv6 typically represented in compressed format using 2 rules:
  - Leading zeros in any segment can be omitted.

    2001:0db8:acad:00a0:3700:0000:0000:a1000 ➡️ 2001:db8:acad:a0:3700:0:0:a100
  - A single string of contiguous all-zero segments can be replaced by a double colon "::"

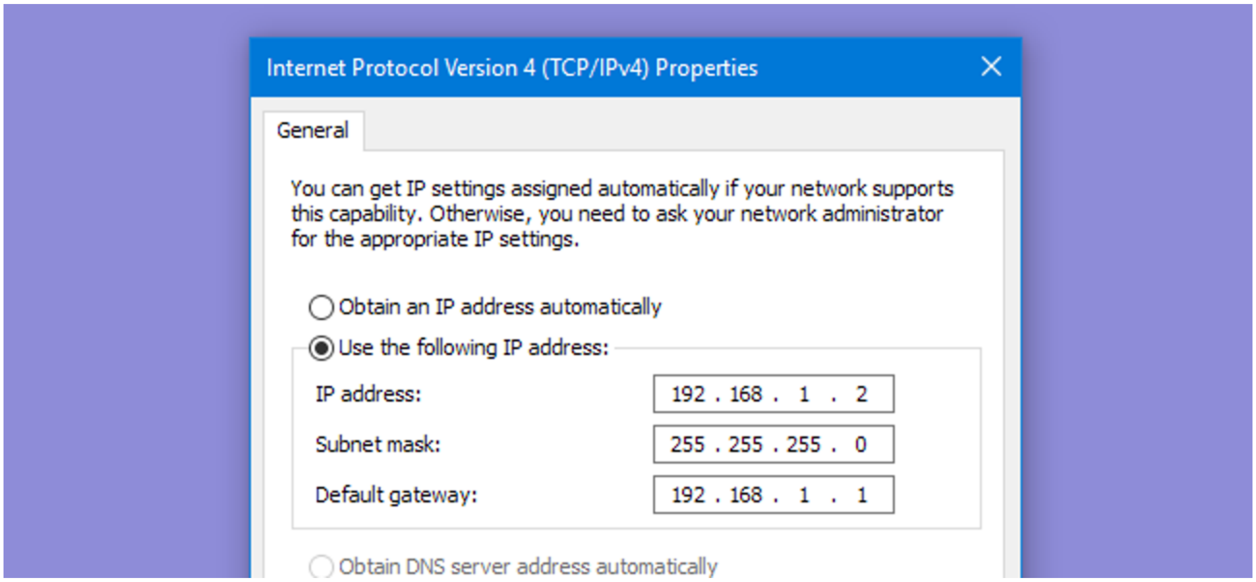
    2001:0db8:acad:00a0:3700:0000:0000:a1000 ➡️ 2001:0db8:acad:00a0:3700::a100
- IPv6 addresses use the "/" (prefix length) to indicate the network portion (prefix) from the host portion (interface ID): 2001:db8:acad:100:37ef:100:a765:1/64
  - If a computer move from one network to another one, the network portion of its IPv6 address will be changed, but the host portion will not.

Displaying the addresses

```
ipconfig /all
```

Static addressing

Static IP addressing is to assign a unique IP address to each host within the same network.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

Dynamic addressing

A dynamic host configuration protocol (DHCP) server automatically assigns IP addresses, which simplifies the addressing process.

Link-local IPv4 and IPv6 addresses

Link-local addresses for IPv4 and IPv6 are used by a device to communicate with other computers connected to the same network within the same IP address range. The major difference between IPv4 and IPv6 is:

- An IPv4 device uses the link-local address if the device cannot obtain an IPv4 address.
- An IPv6 device must always be dynamically or manually configured with a link-local IPv6 address.

Every IPv6 enabled device is required to have a link-local address. They are in the range of fe80:: to febf::

Configure a NIC

Network design

- Network components includes wired and wireless network interface cards (NIC) and network devices.
- Network design involves knowing how networks are interconnected to support the needs of a business.

1. Selecting a NIC
2. Installing and updating a NIC
3. Configure a NIC
4. Internet control message protocol (ICMP) is used by devices on a network to send control and error messages.

    ```
    ping cisco.com
    ping /?
    ```

Configure a wired and wireless network

1. Connect a network cable to the device
2. Connect the device to a switch port
3. Connect a network cable to the wireless router internet port
4. Connect the wireless router to the modem
5. Connect to the service provider's network

Basic network setup

1. Login to the router
2. Change the default password
3. Login with the new password
4. Change the DHCP IPv4 addresses
5. Renew IP address
6. Login at the new IP address

Basic wireless settings

1. View the WLAN defaults. The network name is called the Service Set Identified (SSID)
2. Change the network mode

3. Configure the SSID
4. Configure the channel

   Devices configured with the same channel within the 2.4GHz band may **overlap** and cause distortion, slowing down the wireless performance and potentially break network connections. Channels 1, 6, and 11 are non-overlapping.

5. Configure the security mode
6. Configure the passphrase

Configure a wireless mesh network

In a small office or home network, one wireless router may suffice to provide wireless access to all the clients. If you want to extend the range beyond approximately 45 meters indoors and 90 meters outdoors, you can add wireless access points.

The **Internet Control Message Protocol** (**ICMP**) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating success or failure when communicating with another IP address

NAT for IPv4

The router will use a process called network address translation (NAT) to **convert private IPv4 addresses to Internet-routable IPv4 addresses**. With NAT, **a private (local) source IPv4 address is translated to a public (global) address.**

Router is the ONLY way to interconnect two different networks.

Quality of Service (QoS)

By configuring QoS, you can guarantee that certain traffic types are prioritized over traffic that is not as time-sensitive.

Firewall settings

UPnP

Universal plug and play (UPnP) is a protocol that enables devices to dynamically add themselves to a network without the need for user intervention or configuration.

UPnP is **not secure**. It has no method for authenticating devices. So, it considers every device trustworthy.

DMZ

A demilitarized zone (DMZ) is a network that provides services to an untrusted network.

An email, web, or FTP server is often placed into the DMZ so that the traffic using the server doesn't come inside the local network. This **protects** the internal network from attacks by the traffic but does **not protect** the servers in the DMZ in any way. It is **common** for a firewall to manage traffic to and from the DMZ.

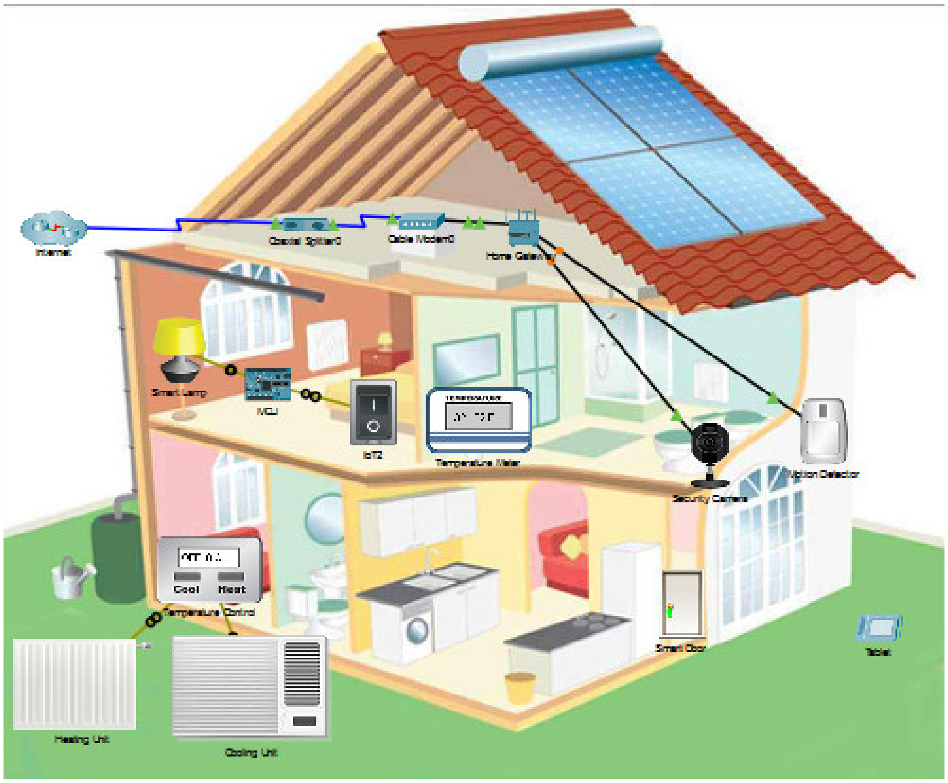
Port forwarding and MAC address filtering

MAC address filtering specifies exactly which device MAC addresses are allowed to or blocked from sending data on your network.

IoT device configuration

The evolving internet is becoming an Internet of Things (IoT).

IoT Devices in Packet Tracer



Basic Troubleshooting Process for Networks

Applying the troubleshooting process

The troubleshooting process

1. Identify the problem
    - Open-ended questions
    - Closed-ended questions
2. Establish a theory of probable cause
    - Loose cable connections
    - Improperly installed NIC
    - ISP is down
    - Low wireless signal strength
    - Invalid IP address
    - DNS Server issue
    - DHCP Server issue
3. Test the theory to determine the cause
    a. Check that all cables are connected to the proper locations
    b. Unseat and then reconnect cables and connectors
    c. Reboot the computer or network device
    d. Login as a different user
    e. Repair or re-enable the network connector
    f. Contact the network administrator
    g. Ping the device's default gateway
    h. Access a remote web page
4. Establish a plan of action to resolve the problem and implement the solution
    - Helpdesk repair logs
    - Other technicians
    - Manufacturer FAQ websites
    - Technical websites
    - News groups
    - Computer manuals

- Device manuals
- Online forums
- Internet search

5. Verify full system functionality and if applicable, implement preventive measures
    a. Use **ipconfig /all** command to display IP address information for all network adapters
    b. Using **ping** to check network connectivity. It will send a packet to the specified address and displays response information.
    c. Verify the device can access authorized resources like company email servers and the internet.
    d. Research additional commands or ask supervisor for help with other testing utilities.
6. Document findings, actions, and outcomes
    a. Discuss the solution implemented with the customer
    b. Have the customer verify problem has been solved
    c. Provide the customer with all paperwork
    d. Document the steps taken to the solve the problem in the work order and technician's journal
    e. Document any components used in the repair
    f. Document the time spent to solve the problem