Chapter 6: Applied Networking

Instructor Materials

IT Essentials v7.0

Chapter 6: Applied Networking

IT Essentials 7.0 Planning Guide

Chapter 6: Applied Networking

IT Essentials v7.0

Chapter 6 - Sections & Objectives

6.1 Device to Network Connection

- Configure devices for wired and wireless networks.
  - Explain MAC and IP addressing for computer networks.
  - Configure a NIC for wired and wireless networks.
  - Configure wireless networking in a small LAN.
  - Configure firewall settings.
  - Configure IoT devices.

6.2 Network Troubleshooting

- Troubleshoot problems and solutions related to networks.
  - Explain the six steps of the troubleshooting process for networks.
  - Troubleshoot common and advanced problems related to networks.

6.1 Device to Network Connection

Video Explanation – MAC Addressing

This is a video explanation about MAC Addressing:

- Communication analogy
- NIC MAC Address
- Physical Address
- OUI and Vendor Assigned
- Communication on the Same Network
- Communication on a Separate Network

Video Explanation – IPv4 Addressing

This is a video explanation about IPv4 Addressing:

- Communication analogy
- IPv4 Addresses vs. IPv6 Addresses
- Decimal vs. Binary vs. Hexadecimal
- Subnet Masks
- IPv4 Address Network and Host Portions
- IPv4 Addressing Example

Video Explanation – IPv6 Addressing

This is a video explanation about IPv6 Addressing:

- Hexadecimal Segments
- Address Compression Rules
- IPv6 Address Network and Host Portions
- IPv6 Addressing Example

Two Network Addresses

MAC Address Format

Address Format	Description
00-50-56-BE-D7-87	Two hexadecimal digits separated by hyphens
00:50:56:BE:D7:87	Two hexadecimal digits separated by colons
0050.56BE.D787	Four hexadecimal digits separated by periods

IPv4 Address Format

32 bits in dotted decimal notation

192.168.200.8

IPv6 Address Format

128 bits in hexadecimal format

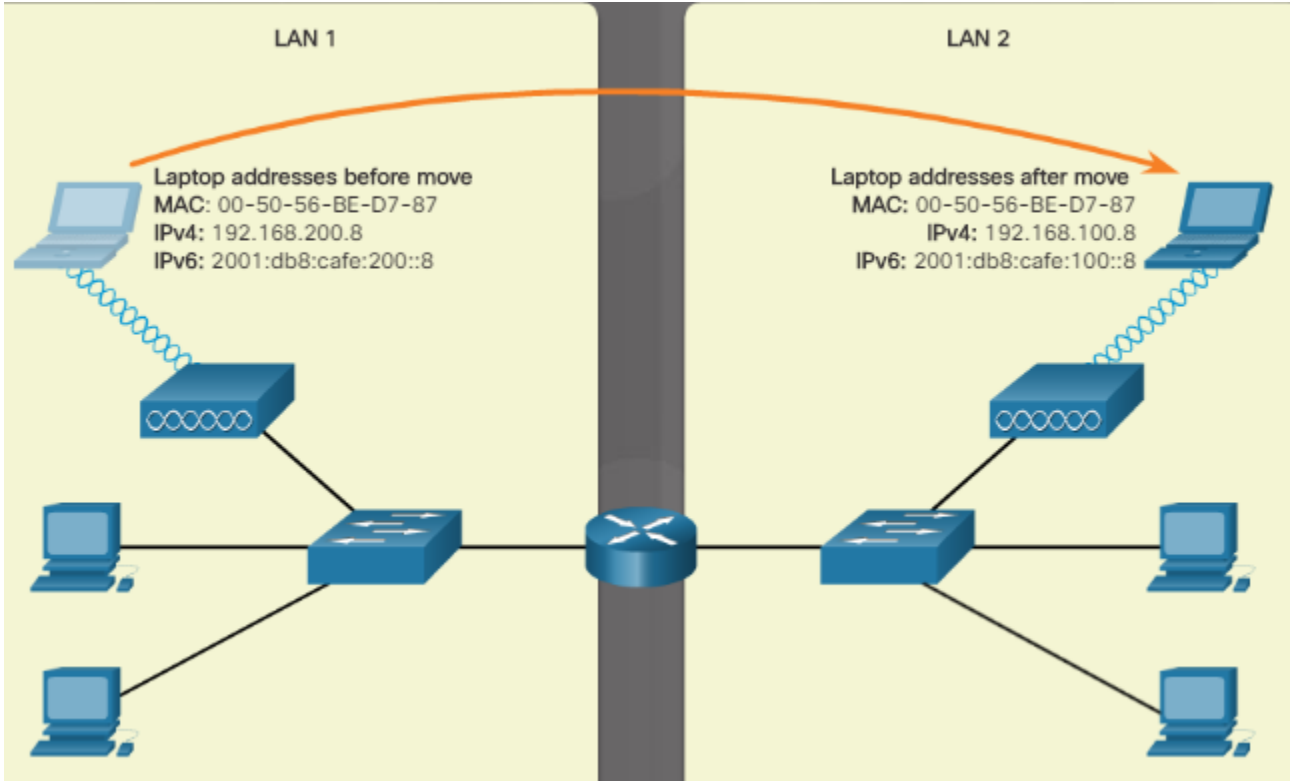
2001:0db8:cafe:0200:0000:0000:0000:0008

128 bits in compressed format

2001:db8:cafe:200::8

Two Network Addresses (Cont.)

- When a laptop is moved to a different network, the MAC address stays the same, but the IPv4 and IPv6 addresses change.
- A MAC address is a unique number that is part of the NIC.
- IP addresses are assigned by the company or internet provider.



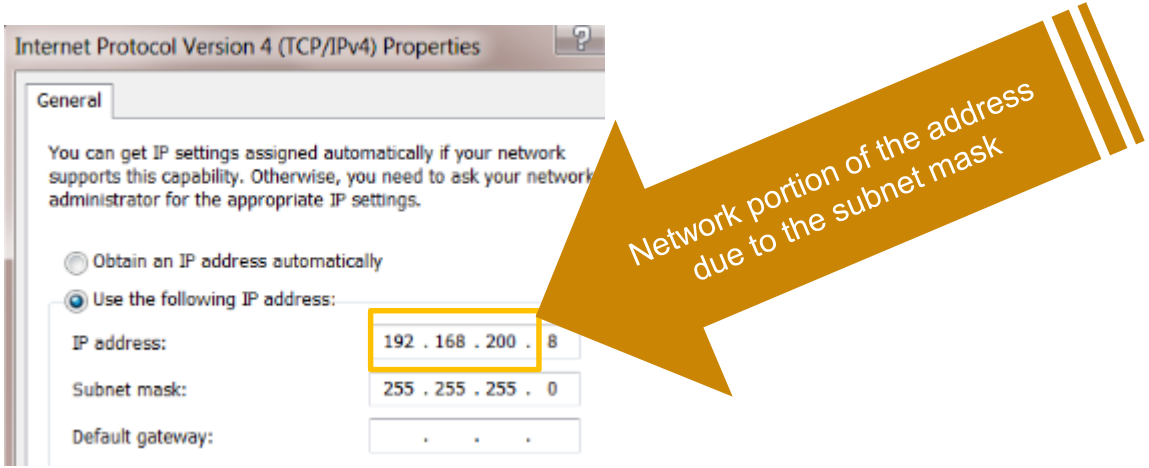
Displaying the Addresses

Use the `/all` switch with the `ipconfig` command to see the MAC (physical) address.

```
C:\> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : ITEuser
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-50-56-BE-D7-87
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:db8:cafe:200::8(Preferred)
   Link-local IPv6 Address . . . . . : fe80::8cbf:a682:d2e0:98a%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.200.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 2001:db8:cafe:200::1
                                       192.168.200.1
```

IPv4 Address Format

- Two parts of an IP address:
  - Network
  - Host
- The subnet mask determines which part of the address is the network part.



	Network Portion		Host Portion
192.168.200.8	11000000.10101000.11001000	.	00001000
255.255.255.0	11111111.11111111.11111111	.	00000000
192.168.200.0	11000000.10101000.11001000	.	00000000

IPv6 Address Format

- Rules:
  - Omit leading 0s – 0db8 can be db8
  - Omit all 0 segments – use double colons (::)

```
2001 : 0DB8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200

FE80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89AB : CDEF

FF02 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
```

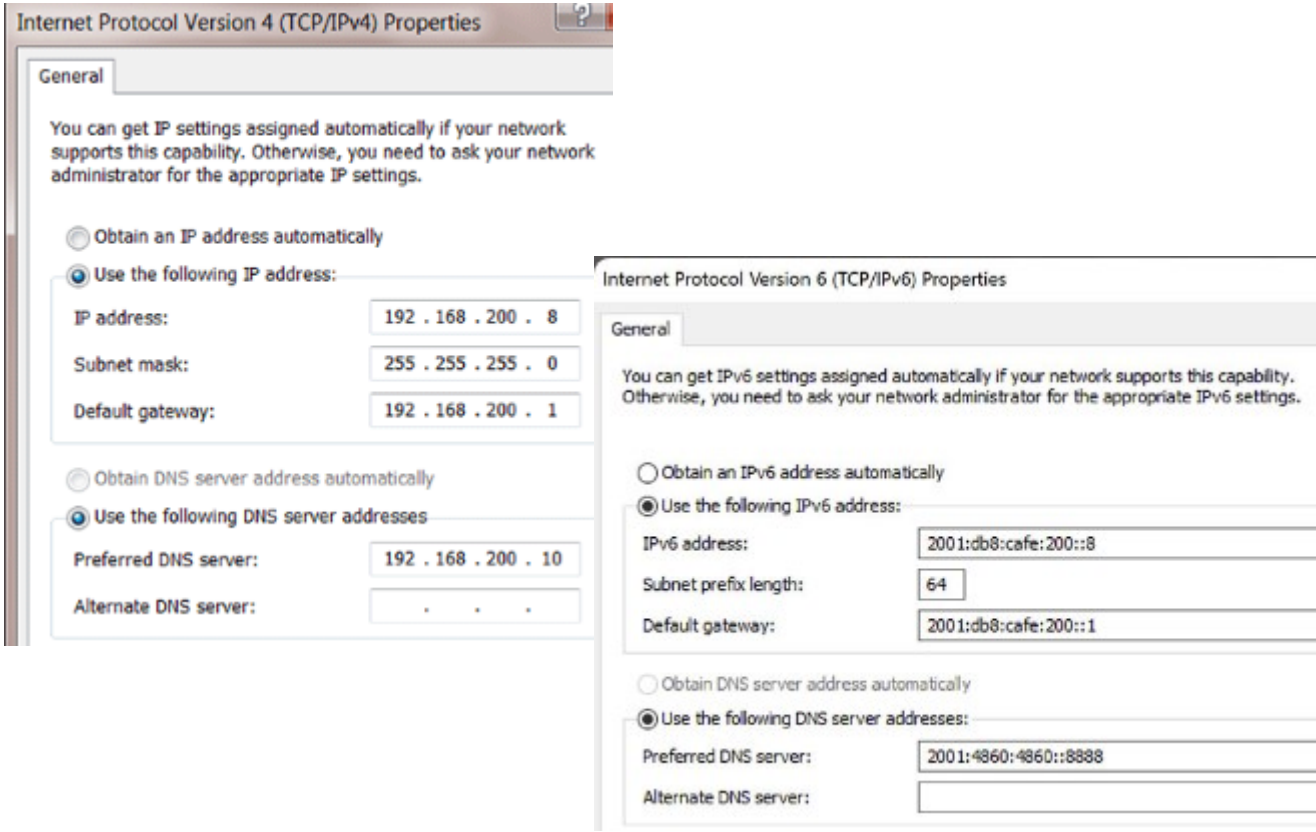
Fully expanded	2001:0db8:0000:1111:0000:0000:0000:0200
No leading 0s	2001: db8: 0:1111: 0: 0: 0: 200
Compressed	2001:db8:0:1111::200

Fully expanded	fe80:0000:0000:0000:0123:4567:89ab:cdef
No leading 0s	fe80: 0: 0: 0: 123:4567:89ab:cdef
Compressed	fe80::123:4567:89ab:cdef

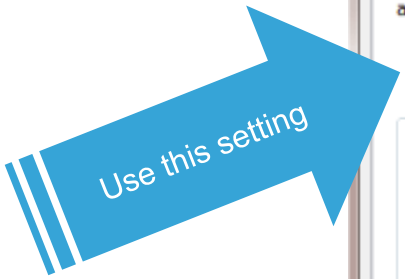
Fully expanded	ff02:0000:0000:0000:0000:0000:0000:0001
No leading 0s	ff02: 0: 0: 0: 0: 0: 0: 1
Compressed	ff02::1

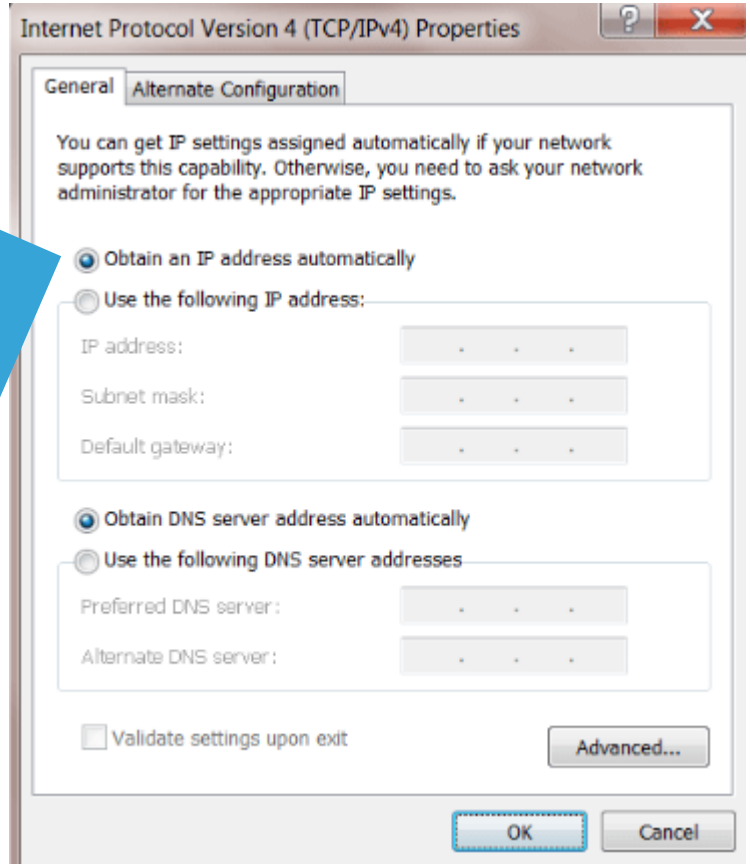
Static Addressing

- Static address information needed for communication with other networks and the internet:
  - IP address
  - Subnet mask
  - Default gateway (address of router so information can be sent to other networks)
  - DNS server (converts domain names or URLs to IP addresses for easy reachability or remote web sites and devices)



Dynamic Addressing

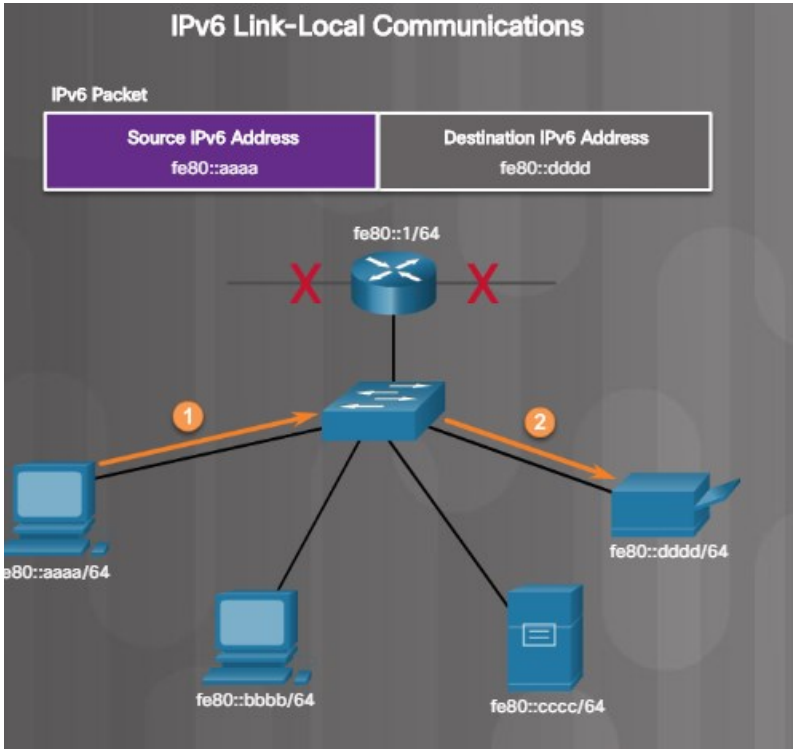




- IP addressing information comes from a DHCP server

Link-local IPv4 and IPv6 Addresses

- IPv4 device uses if the device cannot obtain an IPv4 IP address.
- IPv6 device must always have a dynamic or manually configured link-local IPv6 IP address.

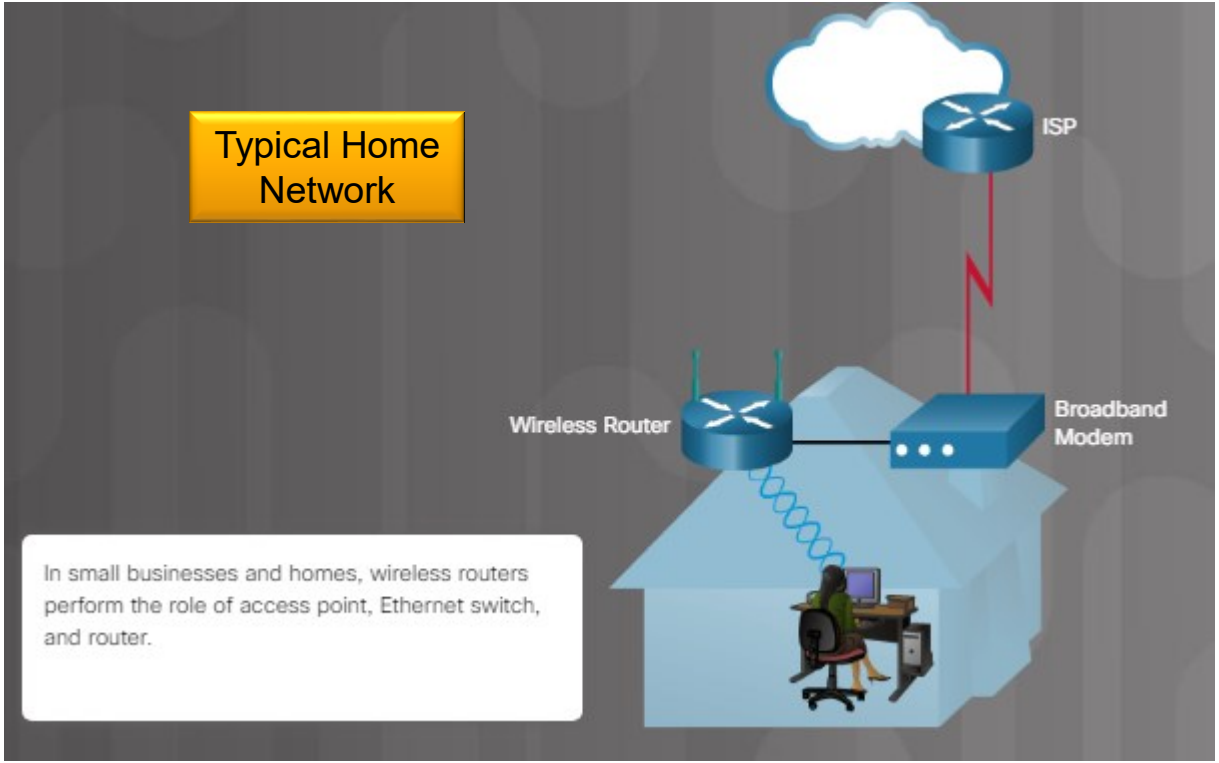


Packet Tracer – Add Computers to an Existing Network

In this Packet Tracer activity, you will configure the computers to use DHCP, configure static addressing, use ipconfig to retrieve host IPv4 information, and use ping to verify connectivity.

Network Design

- Network components
- Network design



Selecting a NIC

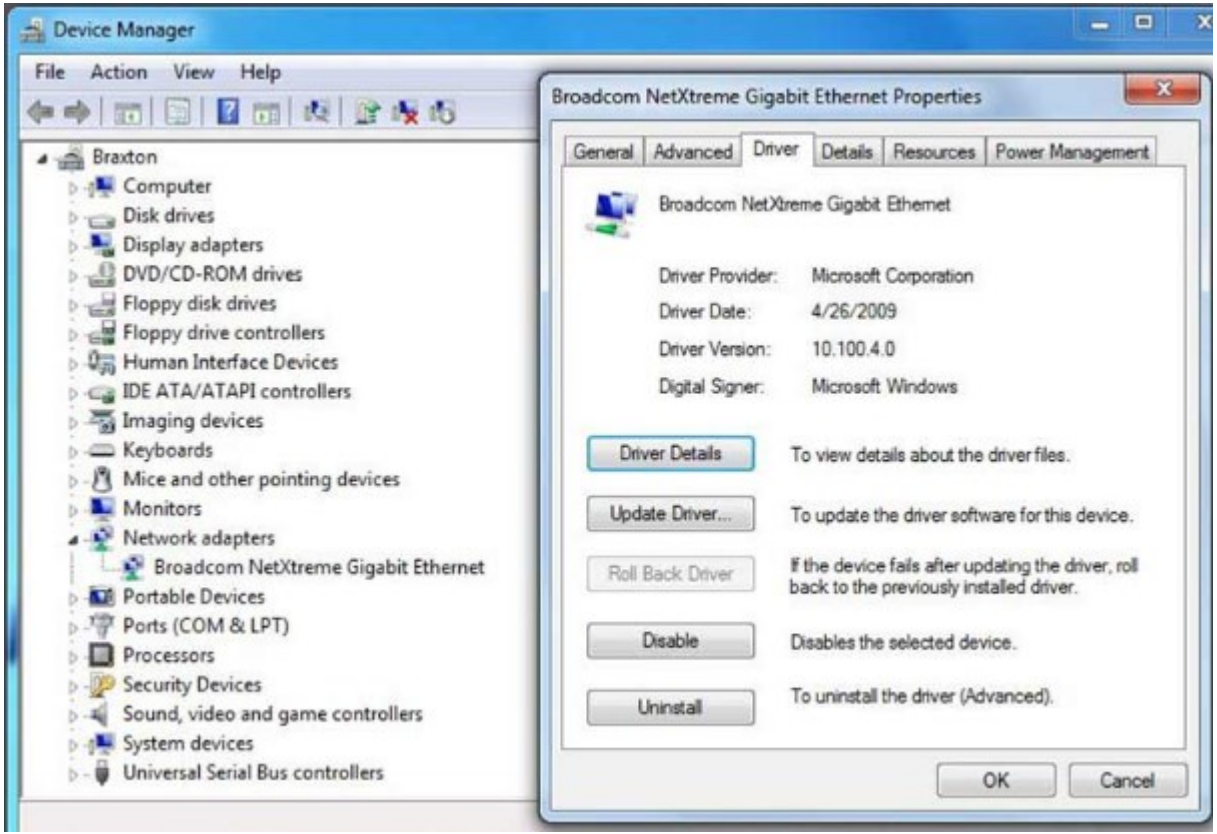
Wired Ethernet

Wireless Ethernet

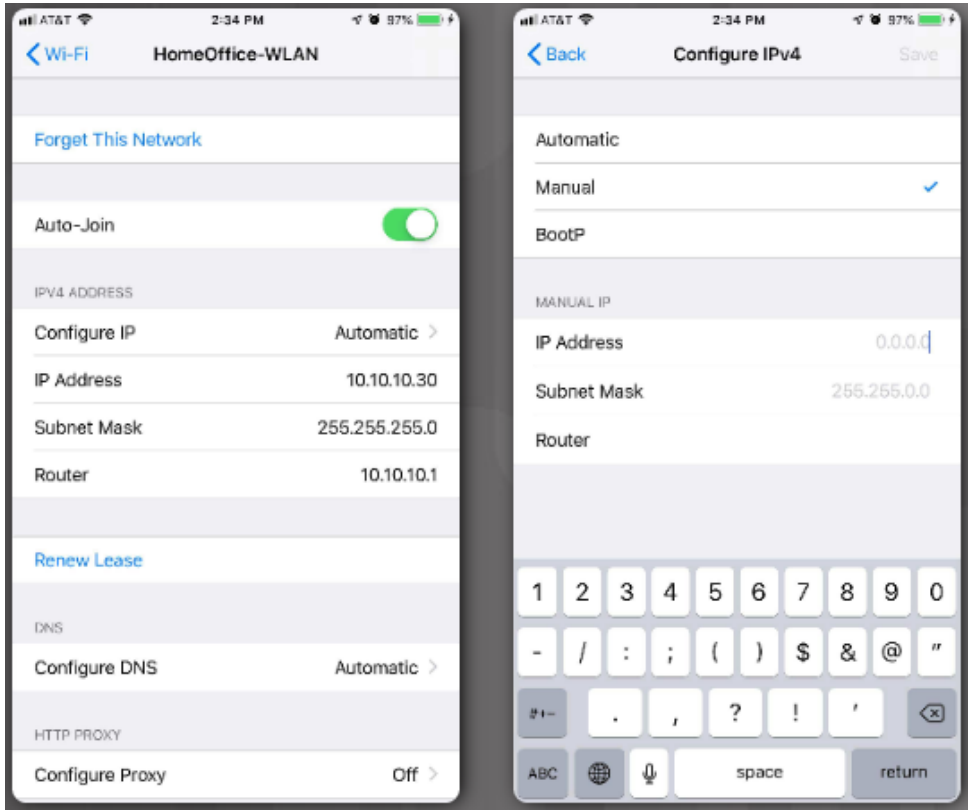
Wireless Ethernet

Installing and Updating a NIC

- If installing a wireless NIC, ensure antenna is positioned for optimum reachability
- Use **Device Manager** to view the driver details:
  - Expand the *Network adapters* category
  - Right-click on specific NIC > *Properties* or *Update driver*



Configure a NIC



- Wireless devices including smart phones also need IP addresses to participate on a wireless network.

ICMP

ping command switch options

```
C:\> ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

- Internet Control Message Protocol (ICMP) is used to test connectivity and send control and error messages.
- The **ping** command is part of ICMP.

```
C:\> ping cisco.com

Pinging e144.dscb.akamaiedge.net [23.200.16.170] with 32 bytes of data:
Reply from 23.200.16.170: bytes=32 time=25ms TTL=54
Reply from 23.200.16.170: bytes=32 time=26ms TTL=54
Reply from 23.200.16.170: bytes=32 time=25ms TTL=54
Reply from 23.200.16.170: bytes=32 time=25ms TTL=54

Ping statistics for 23.200.16.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 26ms, Average = 25ms
```

Lab – configure a NIC to Use DHCP in Windows

In this lab, you will configure an Ethernet NIC to use DHCP to obtain an IP address and test connectivity between two computers.

Video Explanation – Configure a Wired and Wireless Network

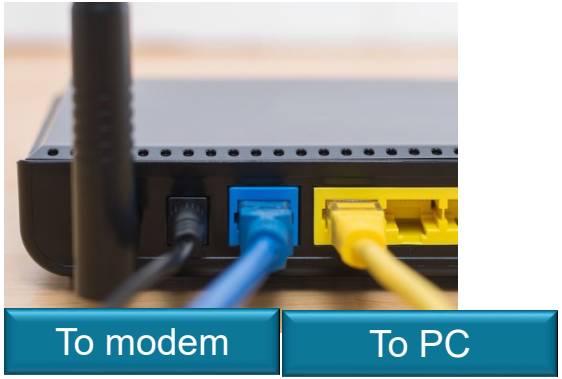
This is a video explanation about configuring a wired and wireless network:

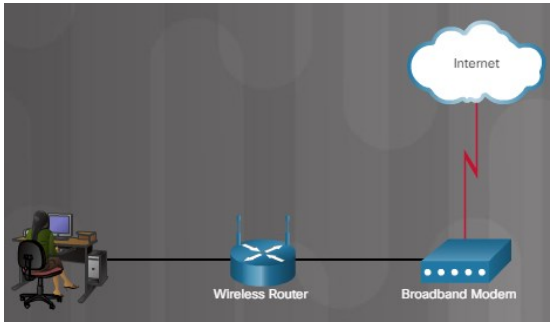
- Connect Cables
- Wireless Router Web Page
- Change Password
- WAN Settings
- LAN Settings
- Wireless Settings
- Connect to the Wireless Network

Connecting Wired Devices to the Internet

To connect a small office or home wired network device:

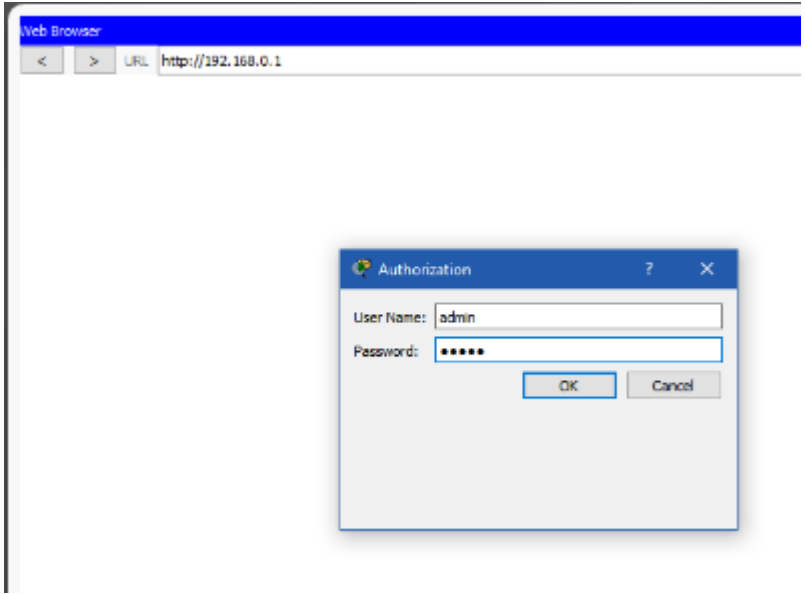
1. Connect the cable to device.
2. Connect other end of cable to switch (yellow port).
3. Connect cable between the wireless router (blue port) and the broadband modem.





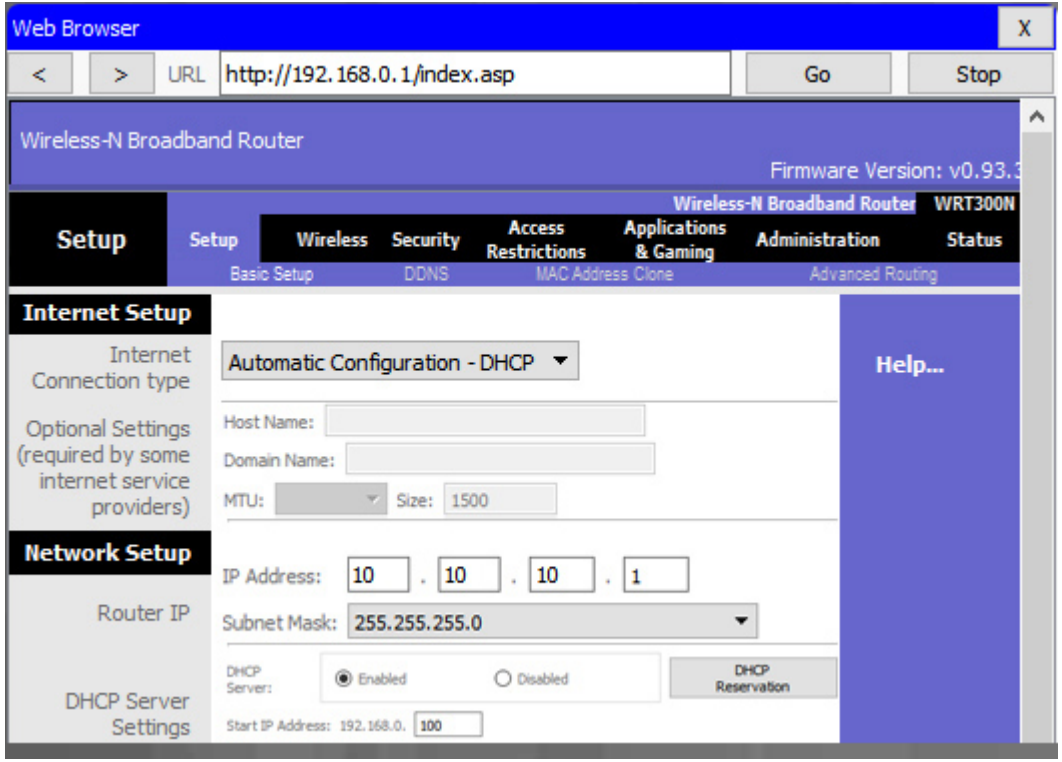
Logging into the Router

- Open a browser and enter the default IP address of the router.
- Change the default username and password immediately.



Basic Network Setup

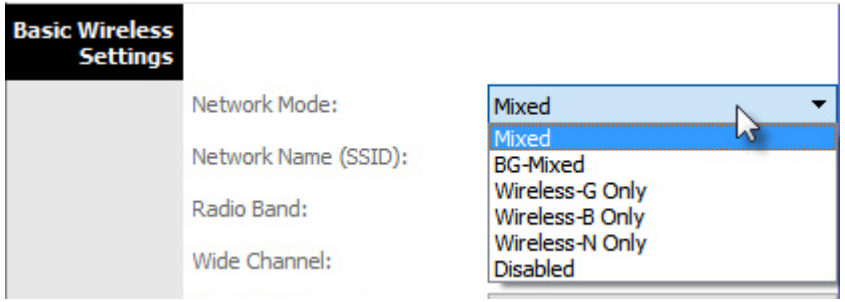
1. Log in to router.
2. Change the default password.
3. Log in with new password.
4. Set the DHCP address range
5. Renew IP addresses on devices (**`ipconfig /release`** and then **`ipconfig /renew`** commands).
6. Change default IP address and log in with new IP address.



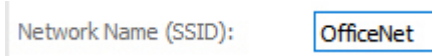
Basic Wireless Settings

1. View WLAN defaults.
2. Change the network mode.
3. Configure SSID.
4. Configure channel.
5. Configure security mode.
6. Configure the passphrase.

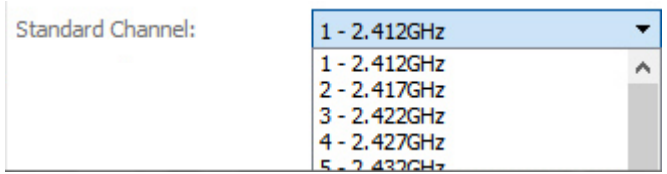
2.



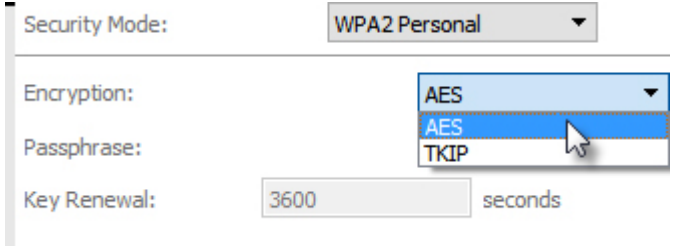
3.



4.

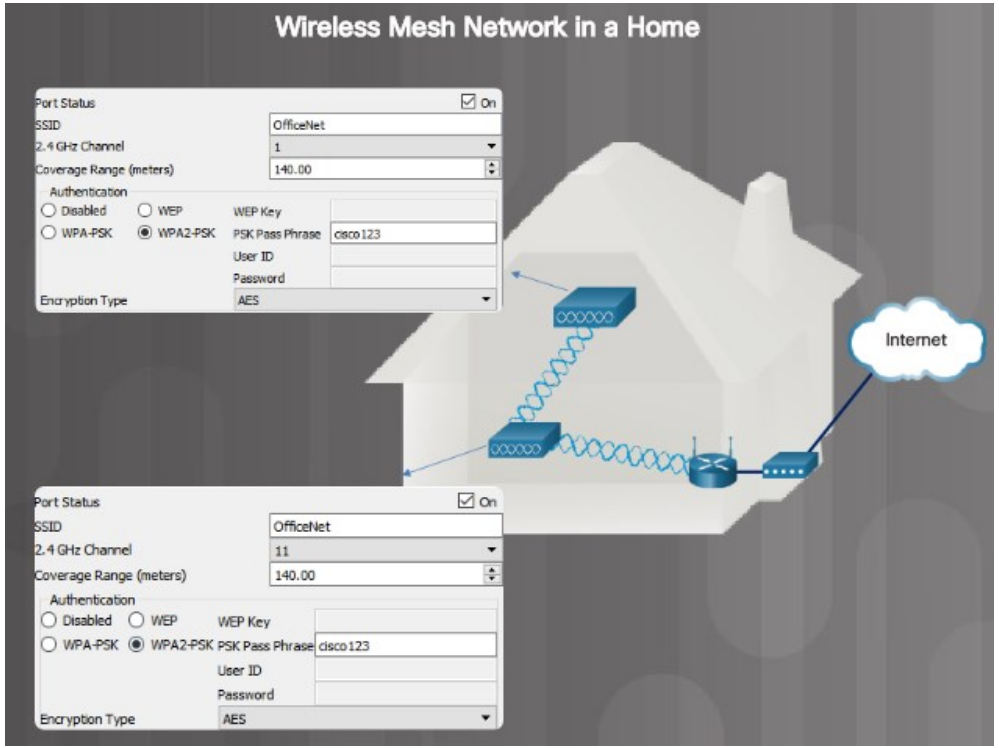


5.



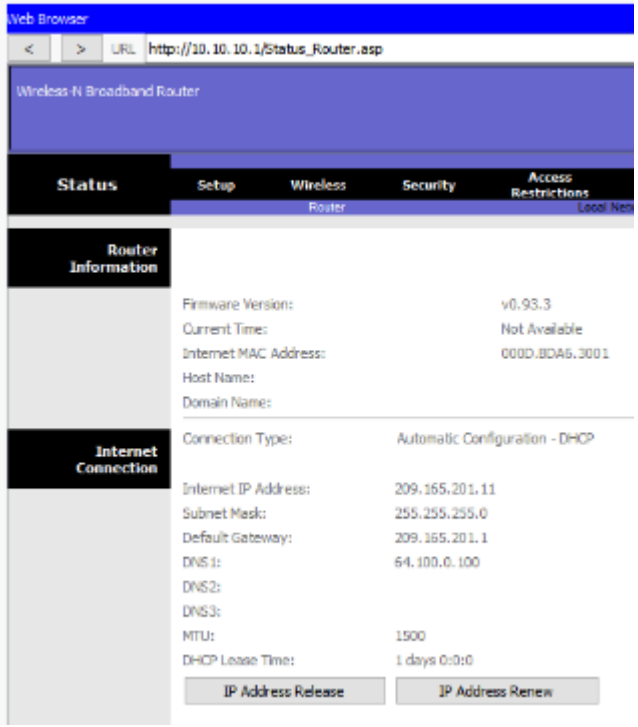
6.

Configure a Wireless Mesh Network



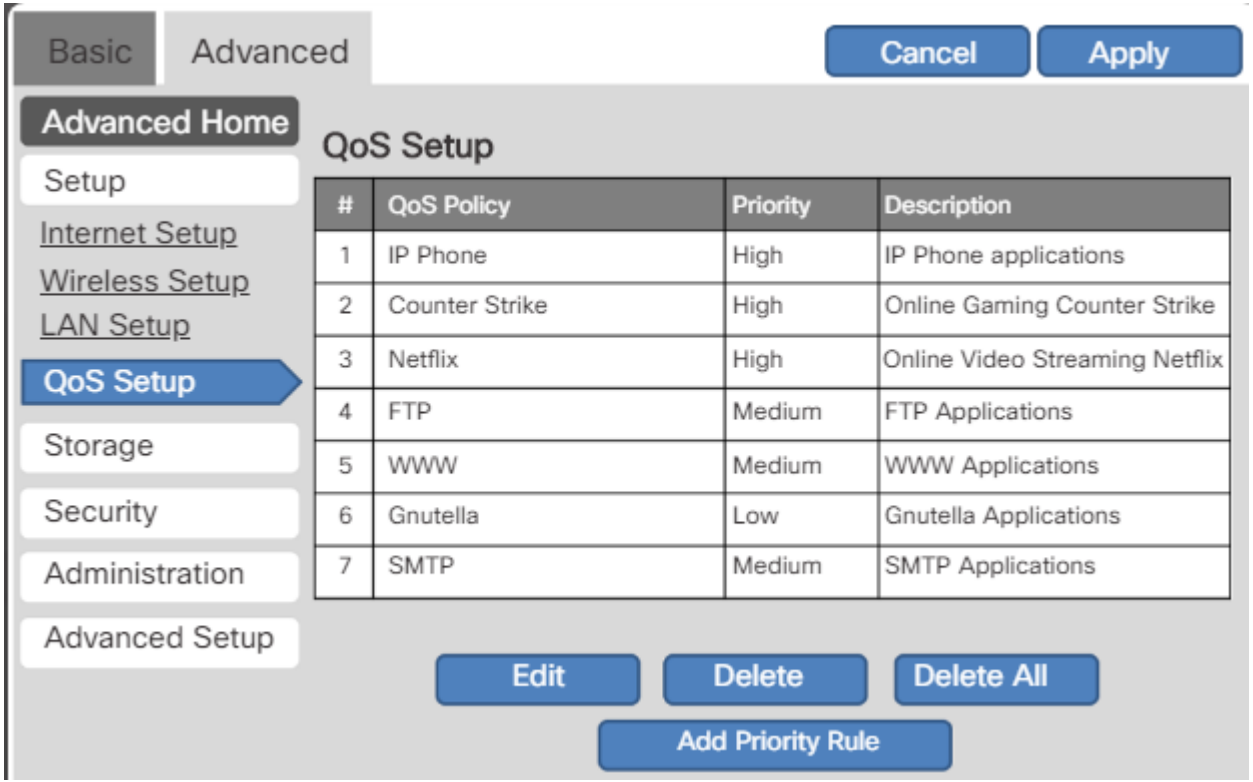
NAT for IPv4

- Network Address Translation (NAT) converts private IPv4 addresses to Internet-routable public IPv4 addresses.



Quality of Service

- Quality of Service (QoS) configuration allows prioritization of specific traffic types.



#	QoS Policy	Priority	Description
1	IP Phone	High	IP Phone applications
2	Counter Strike	High	Online Gaming Counter Strike
3	Netflix	High	Online Video Streaming Netflix
4	FTP	Medium	FTP Applications
5	WWW	Medium	WWW Applications
6	Gnutella	Low	Gnutella Applications
7	SMTP	Medium	SMTP Applications

Packet Tracer – Connect to a Wireless Network

In this Packet Tracer activity, you will configure a wireless router and an access point to accept wireless clients and route IP packets. You will also update some of the default settings.

Lab – Configure a Wireless Network

In this lab, you will configure basic settings on a wireless router and connect a PC to router wirelessly.

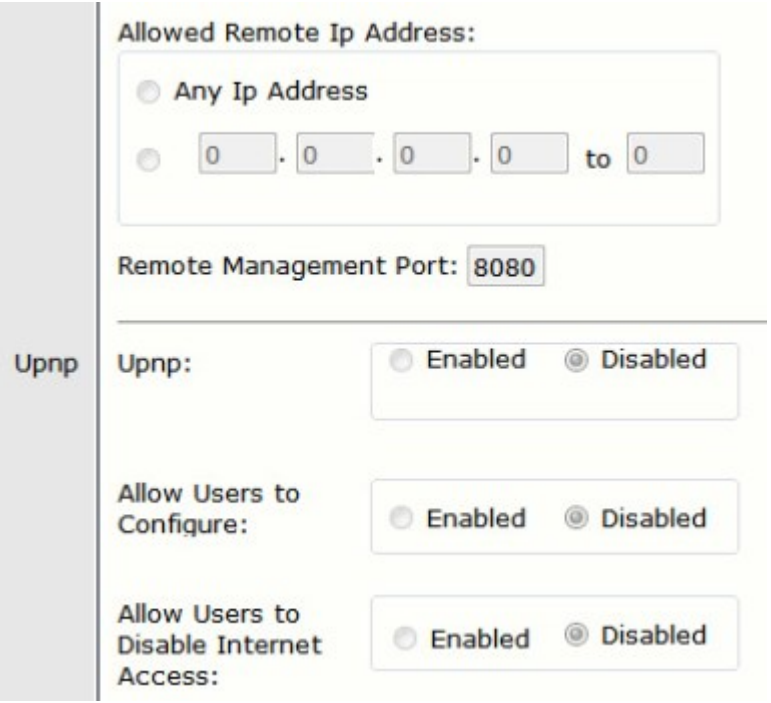
Video Explanation – Firewall Settings

This is a video explanation about Firewall Settings:

- DMZ configuration in LAN
- Firewall rules

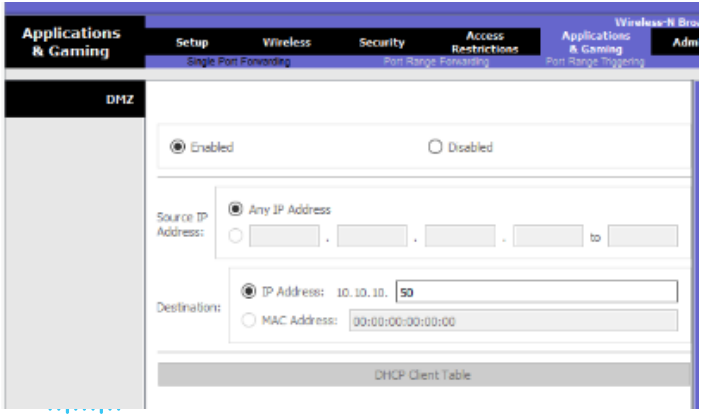
UPnP

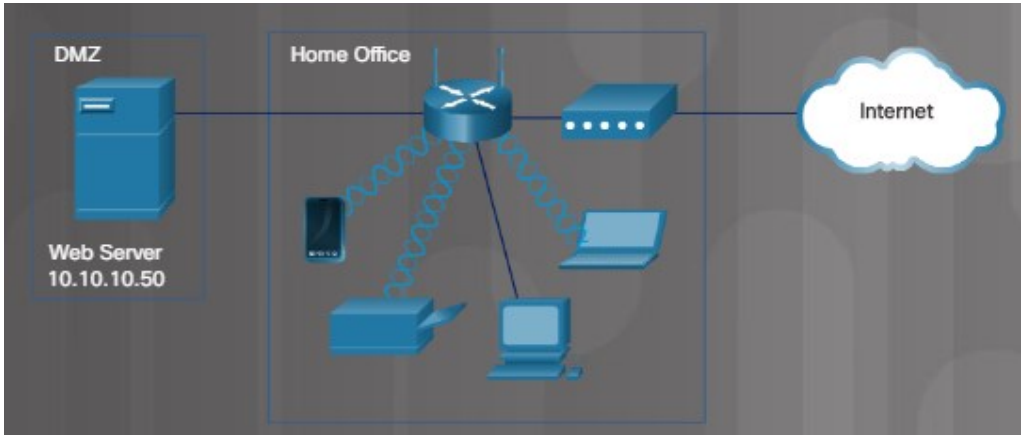
- Universal Plug and Play (UPnP) is not secure and is a security risk.
- UPnP allows devices to dynamically add themselves to a wireless network without intervention/configuration.



DMZ

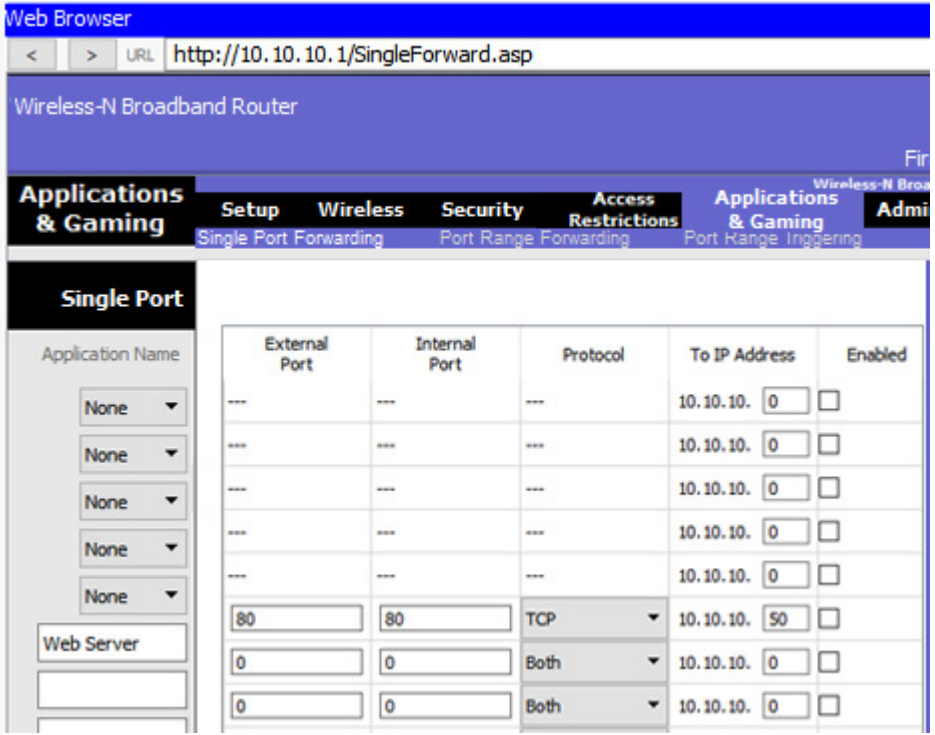
- A demilitarized zone (DMZ) is a network that provides services to an untrusted network.
- A DMZ often contains servers.
- Some wireless routers support the creation of a DMZ.





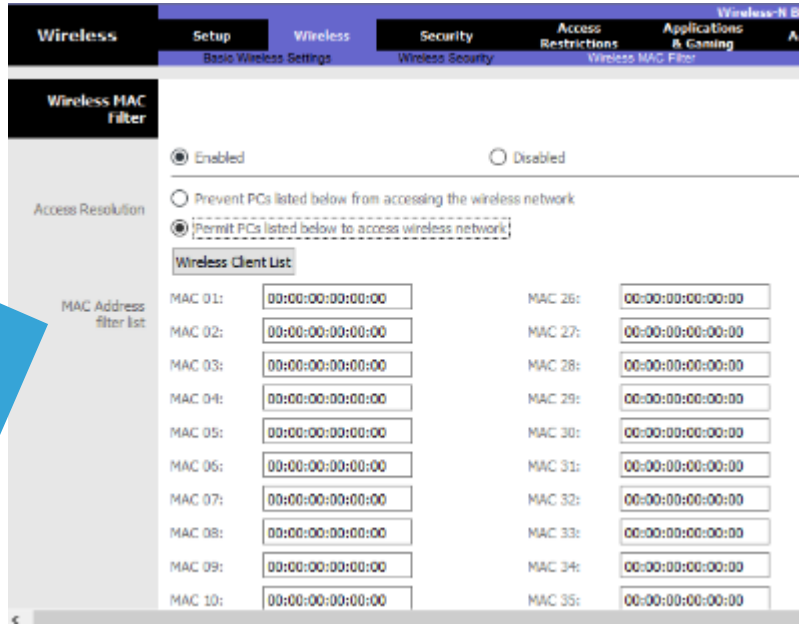
Port Forwarding

- Port forwarding allows traffic to specific ports.
- Port triggering allows a temporary opening in the firewall to allow data to specific inbound ports or a port range for an application or game.



MAC Address Filtering

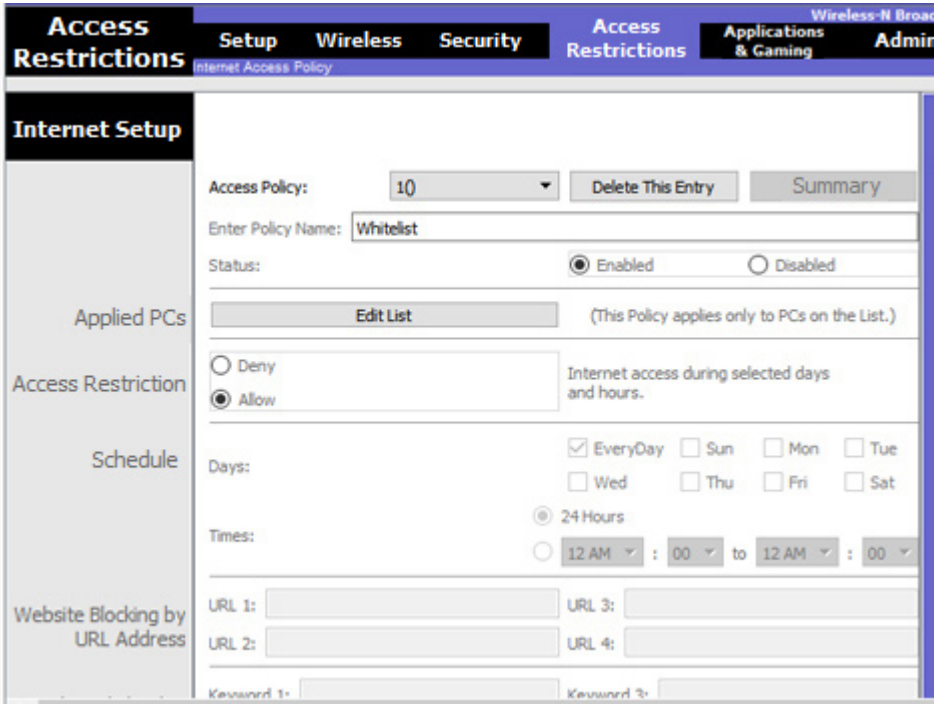
- MAC Address Filtering is used to specify the MAC addresses that are allowed on the wireless network.



The MAC addresses have not yet been entered into the MAC Address filter list on the wireless router configuration to the left.

Whitelisting and Blacklisting

- **Whitelisting** – allow users such as children or employees access to specific IP addresses.
- **Blacklisting** – block known web sites



Packet Tracer – Configure Firewall Settings

In this Packet Tracer activity, you will configure a wireless router to:

- Rely on MAC filtering to increase security
- Allow access to a server in the DMZ
- Disable the DMZ and configure support for Single Port Forwarding

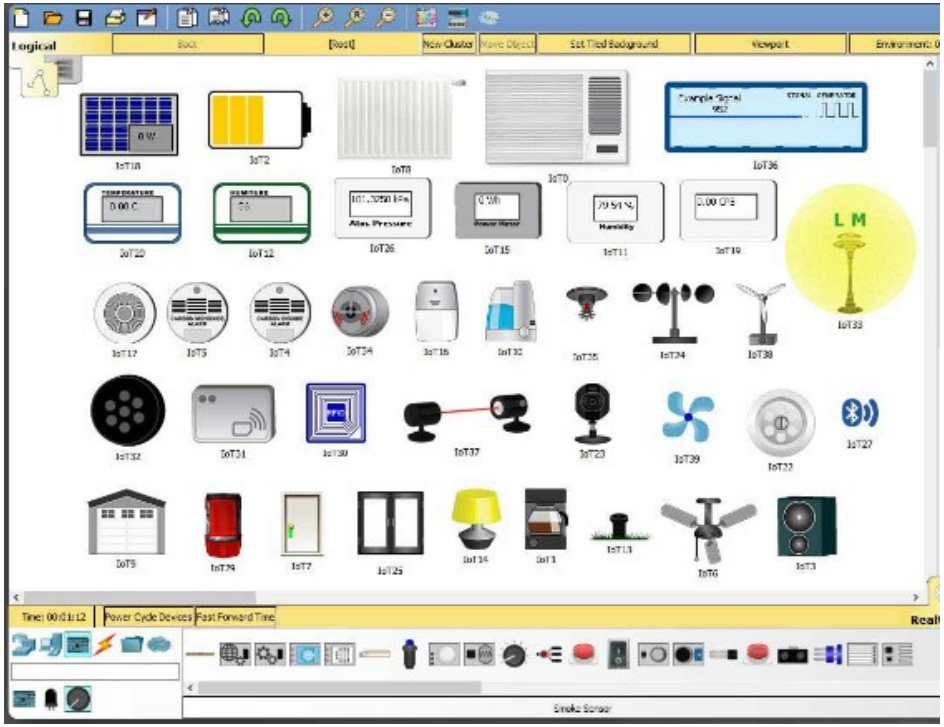
Lab – Configure Firewall Settings

In this lab, you will configure firewall settings to use MAC address filtering, a DMZ, and single port forwarding on a wireless router to manage the connections and traffic through the wireless router.

Internet of Things

- Internet of Things (IoT) may connect to a pre-existing network or a network of its own.
- A smart home contains IoT devices.

IoT Devices in Packet Tracer



Packet Tracer – Configure Firewall Settings

In this activity, you have just installed various IoT devices around the house and wish to configure them as a home security system. You will configure the home gateway to use a motion sensor, test and reset security features, and set the air conditioning.

6.2 Network Troubleshooting Process

The Troubleshooting Process

Step 1	Identify the problem.
Step 2	Establish a theory of probable cause.
Step 3	Test the theory to determine the cause.
Step 4	Establish a plan of action to resolve the problem and implement the solution.
Step 5	Verify full system functionality and if applicable, implement preventive measures.
Step 6	Document findings, actions, and outcomes.

The Six Steps to Troubleshoot a Network – Step 1

Step 1. Identify the problem.	
Open-ended questions	• What problems are you experiencing with your device? • What software has been installed on your device recently? • What were you doing when the problem was identified? • What error message have you received? • What type of network connection is the device using?
Closed-ended questions	• Has anyone else used your device 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? • Is anyone else having this problem? • Have there been any environmental or infrastructure changes to the network?

Network problems can be simple or complex, and can result from a combination of hardware, software, and connectivity issues. As a technician, you should develop a logical and consistent method for diagnosing network problems by eliminating one problem at a time.

For example, to assess the problem determine how many devices are experiencing the problem. If there is a problem with one device, start with that device. If problem with all devices, start the troubleshooting process in the network room where all the devices are connected.

The first step in the troubleshooting process is to identify the problem. Use the list of open-ended and closed-ended questions above as a starting point to gather information from the customer.

The Six Steps to Troubleshoot a Network – Step 2

Step 2. Establish a theory of probable cause.	
Common causes of network problems	• Loose cable connections • Improperly installed NIC • ISP is down • Low wireless signal strength • Invalid IP address • DNS Server issue • DHCP server issue

After you have talked to the customer, you can establish a theory of probable causes. The list above provides some common probable causes for network problems.

The Six Steps to Troubleshoot a Network – Step 3

Step 3. Test the theory to determine the cause.	
Common steps to determine cause	• Check that all cables are connected to the proper locations. • Unseat 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 the device's default gateway. • Access a remote web page such as http://www.cisco.com.

After you have developed some theories about what is wrong, test your theories to determine the cause of the problem. The list above shows some quick procedures that you can use to determine the exact cause of the problem or even correct the problem. If a quick procedure does correct the problem, you can then verify full system functionality. If a quick procedure does not correct the problem, you might need to research the problem further to establish the exact cause.

The Six Steps to Troubleshoot a Network – Step 4

Step 4. Establish a plan of action to resolve the problem and implement the solution.	
If no solution is achieved in the previous step, further research is needed to implement the solution.	• Helpdesk repair logs. • Other technicians. • Manufacturer FAQ websites. • Technical websites. • News groups. • Computer manuals. • Device manuals. • Online forums. • Internet search.

After you have determined the exact cause of the problem, establish a plan of action to resolve the problem and implement the solution. The list above shows some sources you can use to gather additional information to resolve an issue.

The Six Steps to Troubleshoot a Network – Step 5

Step 5. Verify full system functionality and if applicable, implement preventive measures.	
Verify full system functionality and if applicable, implement preventive measures.	• Use **ipconfig /all** command to display IP address information for all network adapters. • Use **ping** to check network connectivity. It will send a packet to the specified address and displays response information. • Verify the device can access authorized resources like company email servers and the internet. • Research additional commands or ask a supervisor for help with other testing utilities.

After you have corrected the problem, verify full functionality and, if applicable, implement preventive measures. The list above shows a few steps to verify the solution.

The Six Steps to Troubleshoot a Network – Step 6

Step 6. Document findings, actions, and outcomes.	
Document findings, actions, and outcomes.	• Discuss the solution implemented with the customer. • Have the customer verify problem has been solved. • Provide the customer with all paperwork. • Document the steps taken to solve the problem in the work order and technician's journal. • Document any components used in the repair. • Document the time spent to solve the problem.

In the final step of the troubleshooting process, document your findings, actions, and outcomes, as shown in the list above.

Common Problems and Solutions for Networking

Identify the Problem

- NIC LED lights are not lit.
- User cannot use secured shell (SSH) to access a remote device.
- Device cannot detect the wireless router.
- Windows computer has an IPv4 address of 169.254.x.x.
- Remote device does not respond to a ping request.
- A user can access the local network but cannot access the internet.
- The network is fully functional but the wireless device cannot connect to the network.
- Local resources such as file shares or printers are unavailable.

NIC LED lights are not lit.

Probable Causes	Possible Solutions
• The network cable is unplugged or damaged.	• Reconnect or replace the network connection to the computer.
• The NIC is damaged.	• Replace the NIC.

Show PDF

Advanced Problems and Solutions for Network Connections

Identify the Problem

- A device can connect to a network device by the IP address but not by the host name.
- The device does not obtain or renew the IP address on the network.
- An IP address conflict message displays when connecting a new device to the network.
- A device has network access but does not have internet access.
- Users are experiencing slow transfer speeds, weak signal strength, intermittent connectivity on the wireless network.

A device can connect to a network device by the IP address but not by the host name.

Probable Causes	Possible Solutions
Incorrect host name.	Re-enter the host name.
Incorrect DNS settings.	Re-enter the IP address of the DNS server.
DNS server is not operational.	Restart the DNS server.

Show PDF

Advanced Problems and Solutions for FTP and Secure Internet Connections

Identify the Problem

- A user cannot access the FTP server.
- The FTP dient software cannot find the FTP server.
- A device cannot access a specific HTTPS site.

A user cannot access the FTP server.

Probable Causes	Possible Solutions
FTP is being blocked by the firewall at the router.	Ensure that ports 20 and 21 are allowed through the router's outbound firewall.
FTP is being blocked by the Windows firewall.	Ensure that ports 20 and 21 are allowed through the Windows outbound firewall.
The maximum number of users has been reached.	Increase the maximum number of simultaneous FTP users on the FTP server.

Show PDF

Advanced Problems and Solutions Using Network Tools

Identify the Problem

- A device on one network cannot ping a device on another network.
- The computer cannot Telnet into a remote computer.
- The nslookup command reports "Can't find server name for address {ip-address}: timed out", where ip-address…
- The ipconfig /release or ipconfig /renew command results in the following message: "No operation can be performed…"
- The ipconfig /release or ipconfig /renew command results in the following message: "The operation failed as no adapter is…"

A device on one network cannot ping a device on another network.

Probable Causes	Possible Solutions
There is a broken link between the two networks.	Use tracert to locate which link is down and fix the broken link.
Internet Control Message Protocol (ICMP) is blocked at the router.	Configure the router to allow ICMP echo requests and echo replies.
ICMP is blocked at the Windows firewall.	Configure Windows firewall to allow ICMP echo requests and echo replies.

Show PDF

Lab – Troubleshoot Network Problems

In this lab, you will diagnose the causes of network problems and solve them.

6.3 Chapter Summary

Chapter 6: Applied Networking Summary

6.1 Device to Network Connection

- Configure devices for wired and wireless networks.
  - Explain MAC and IP addressing for computer networks.
  - Configure a NIC for wired and wireless networks.
  - Configure wireless networking in a small LAN.
  - Configure firewall settings.
  - Configure IoT devices.

6.2 Network Troubleshooting

- Troubleshoot problems and solutions related to networks.
  - Explain the six steps of the troubleshooting process for networks.
  - Troubleshoot common and advanced problems related to networks.

CISCO