Pre lab 2 documentation

NOTE: These are not your lab 2 instructions!

This is a document you may need to refer to during the lab.

There is a separate document with the lab instructions.

Table of Contents:

1) How to perform IP configuration in Windows 11

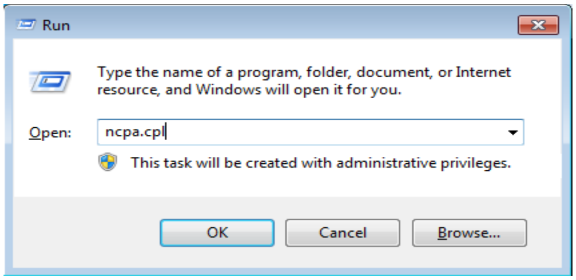
Important Note

The following information is for Windows 11; steps will differ if you are using a different operating system.

Step 1: Examine network property settings.

To have access to computer Network Properties settings.

1. Click **Start > Run.** In the dialog box, type **ncpa.cpl** and press **Enter.**

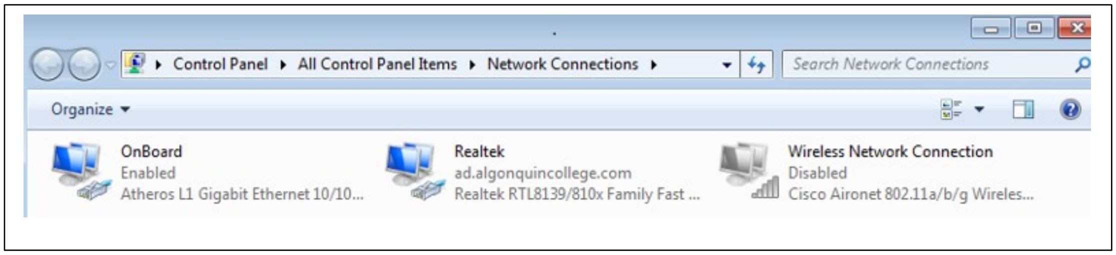


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: ncpa.cpl

This task will be created with administrative privileges.

2. This will bring up the **Network Connections Control Panel** listing all the network devices on your computer. Right-click **Realtek (your Ethernet NIC)** and choose **Properties**.
Note that your devices names may be different


Control Panel ▸ All Control Panel Items ▸ Network Connections ▸
Search Network Connections
Organize ▾

OnBoard
Enabled
Atheros L1 Gigabit Ethernet 10/10...

Realtek
ad.algonquincollege.com
Realtek RTL8139/810x Family Fast ...

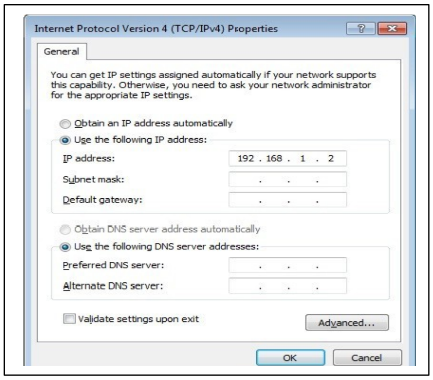
Wireless Network Connection
Disabled
Cisco Aironet 802.11a/b/g Wireles...

3. On the **Networking** tab, scroll down the list of items in the pane, select **Internet Protocol Version 4 (TCP/IPv4)**, and click the **Properties** button.

How to setup a Network Interface with a **Static** IP Address:

Select **Use the following IP address button**
Type your IP address, subnet mask, Default Gateway

1. Press the tab key, and the **Subnet mask** is should be automatically completed (otherwise, enter this address manually).
2. Click **OK**.
3. Set your default gateway IP if you have one.
4. Close the Local Area Connection Properties window (Otherwise, settings may not be saved).



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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: . . .
Default gateway: . . .

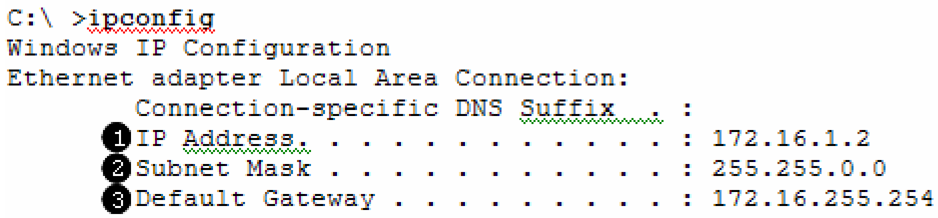
○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

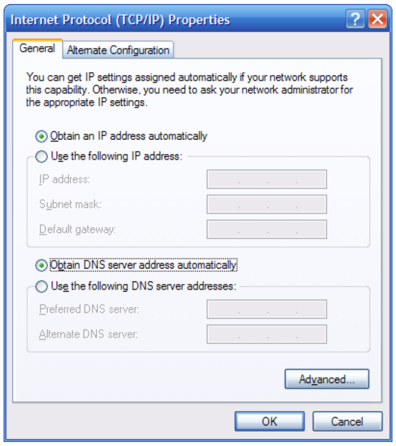
How to setup a Network Interface with a **Dynamic** IP Address:

1 - In the same network properties dialog above, choose, **obtain an IP address automatically**.

2 - To see the automatically set IP address, use the **ipconfig** command in the Command Prompt:



```
C:\ >ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
      ❶IP Address. . . . . . . . . . . . : 172.16.1.2
      ❷Subnet Mask . . . . . . . . . . . : 255.255.0.0
      ❸Default Gateway . . . . . . . . . : 172.16.255.254
```



Internet Protocol (TCP/IP) Properties

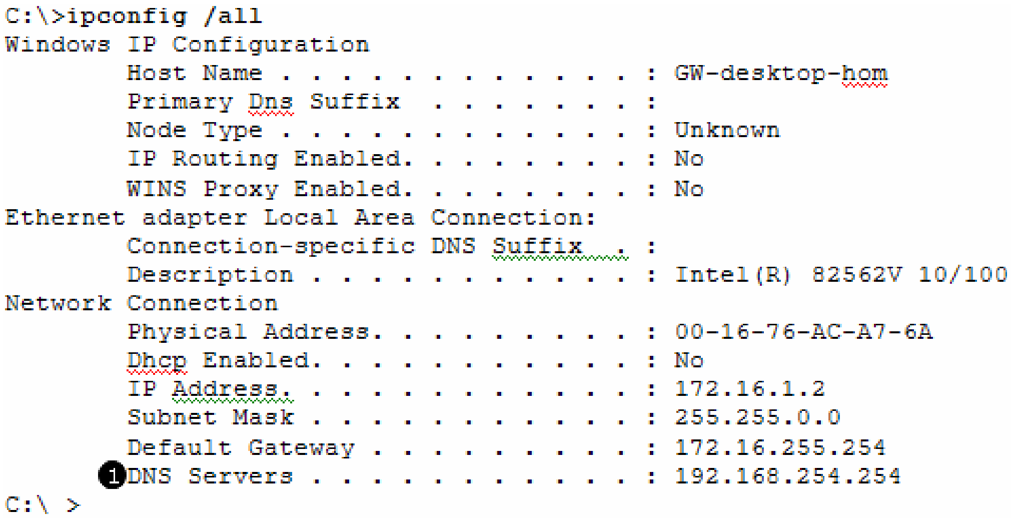
General | Alternate Configuration

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: . . .
Subnet mask: . . .
Default gateway: . . .

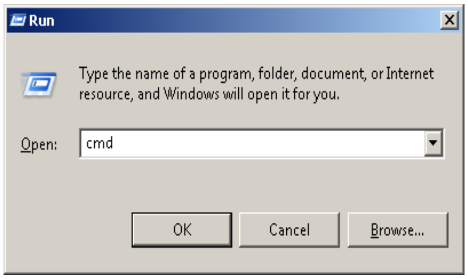
● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

To show the additional, detailed information about the network connections, use the command **ipconfig /all**. It shows IP, subnet mask, Default Gateway, Physical (MAC), and DNS address



```
C:\>ipconfig /all
Windows IP Configuration
        Host Name . . . . . . . . . . . . : GW-desktop-hom
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) 82562V 10/100
Network Connection
        Physical Address. . . . . . . . . : 00-16-76-AC-A7-6A
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 172.16.1.2
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.255.254
       ❶DNS Servers . . . . . . . . . . . : 192.168.254.254
C:\ >
```

How to verify Network Connectivity



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

1. On your computer, click **Start** and then click **Run**.
2. Type **cmd** in the Open box and then click **OK**.

   The Command Prompt (cmd.exe) window will appear.

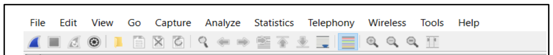
3. Use the **ping** command to test whether a host is reachable across the network or not. You should usually ping:
   - Ping your laptop IP address
   - Ping your laptop default gateway
   - Ping other computers

2) How Wireshark works

Using Wireshark™ to View Protocol Data Units (PDU)

Background

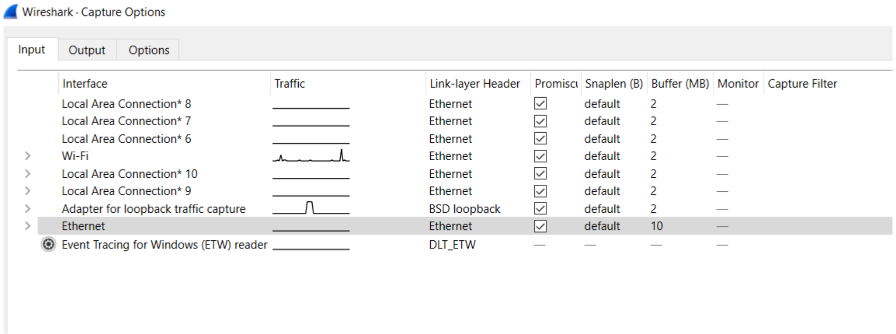
Wireshark is a software protocol analyzer, or "**packet sniffer**" application, used for network troubleshooting, analysis, software and protocol development, and education. A packet sniffer, also known as a network analyzer or protocol analyzer, is computer software that intercepts and logs data traffic passing over a data network. As data streams travel back and forth over the network, the sniffer "captures" each **protocol data unit (PDU)**



and can decode and analyze its content according to the appropriate RFC or other specifications.

To capture **PDUs,** the computer on which **Wireshark** is installed must have a working connection to the network, and Wireshark must be running **before** any data can be captured.

When Wireshark is launched, the following screen is displayed:



Wireshark · Capture Options

Interface	Traffic	Link-layer Header	Promiscu	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
Local Area Connection* 8		Ethernet	☑	default	2	—	
Local Area Connection* 7		Ethernet	☑	default	2	—	
Local Area Connection* 6		Ethernet	☑	default	2	—	
Wi-Fi		Ethernet	☑	default	2	—	
Local Area Connection* 10		Ethernet	☑	default	2	—	
Local Area Connection* 9		Ethernet	☑	default	2	—	
Adapter for loopback traffic capture		BSD loopback	☑	default	2	—	
Ethernet		Ethernet	☑	default	10	—	
Event Tracing for Windows (ETW) reader		DLT_ETW	—	—	—	—	

To start data capture, it is first necessary to select which **interface (or interfaces NIC**) you want to capture from. Click to select the **interface** you want to use, (Typically, for our labs, this will be the Ethernet Adapter) then click **Start**.

Setting Wireshark to capture packets in promiscuous mode.

Clicking the **Capture "Options**" button will allow you to set up options for the capture. Ensure "Use **promiscuous** mode on all interfaces" is checked.

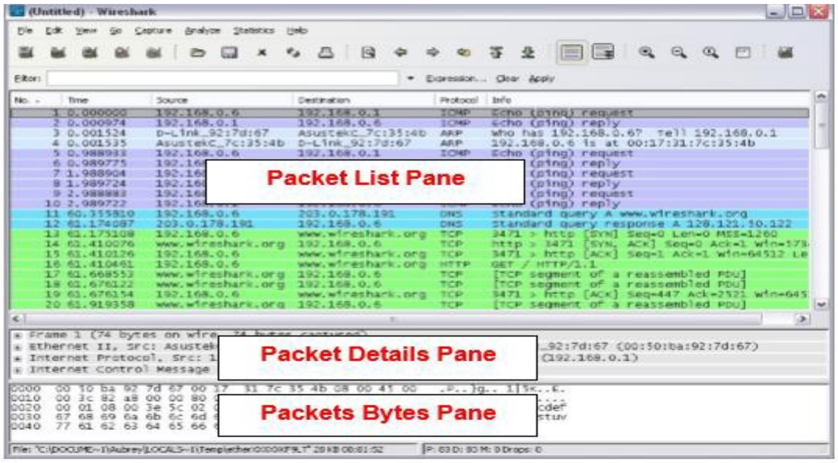
If this feature is NOT checked, only the PDUs destined for this computer will be captured. If this feature is checked, all PDUs destined for this computer AND all those detected by the computer NIC on the same network segment (i.e., those that "pass by" the NIC but are not destined for the computer) are captured.
Note: The capturing of these other PDUs depends on the **intermediary** device connecting the end device computers on this network. As you use different intermediary devices (hubs, switches, routers) throughout these courses, you will experience different Wireshark results.

Setting Wireshark for network name resolution

This option allows you to control whether Wireshark translates network addresses found in PDUs into names. Although this is a useful feature, the name resolution process may add extra PDUs to your captured data, perhaps distorting the analysis.

Clicking on the **Start** button starts the data capture process, and the main screen is displayed. The examples below show the capture of a ping process and then accessing a web page.

When the **Stop** button is clicked, the capture process is terminated.
The main display window of Wireshark has **three** panes.



```
No. -  Time       Source             Destination        Protocol  Info
  1 0.000000    192.168.0.6        192.168.0.1        ICMP     Echo (ping) request
  2 0.000974    192.168.0.1        192.168.0.6        ICMP     Echo (ping) reply
  3 0.001524    D-Link_92:7d:67    AsustekC_7c:35:4b  ARP      Who has 192.168.0.67  Tell 192.168.0.1
  4 0.001535    AsustekC_7c:35:4b  D-Link_92:7d:67    ARP      192.168.0.6 is at 00:17:31:7c:35:4b
  5 0.988933    192.168.0.6        192.168.0.1        ICMP     Echo (ping) request
  6 0.989775    192.16                                          (ping) reply
  7 1.988904    192.16                                          (ping) request
  8 1.989724    192.16                                          (ping) reply
  9 2.988883    192.16                                          (ping) request
 10 2.989722    192.16                                          (ping) reply
 11 60.315810   192.168.0.6        203.0.178.191      DNS      Standard query A www.wireshark.org
 12 61.174087   203.0.178.191      192.168.0.6        DNS      Standard query response A 128.121.50.122
 13 61.175108   192.168.0.6        www.wireshark.org  TCP      3471 > http [SYN] Seq=0 Len=0 MSS=1260
 14 61.410076   www.wireshark.org  192.168.0.6        TCP      http > 3471 [SYN, ACK] Seq=0 Ack=1 Win=573
 15 61.410126   192.168.0.6        www.wireshark.org  TCP      3471 > http [ACK] Seq=1 Ack=1 Win=64512 Le
 16 61.410461   192.168.0.6        www.wireshark.org  HTTP     GET / HTTP/1.1
 17 61.668553   www.wireshark.org  192.168.0.6        TCP      [TCP segment of a reassembled PDU]
 18 61.676122   www.wireshark.org  192.168.0.6        TCP      [TCP segment of a reassembled PDU]
 19 61.676154   192.168.0.6        www.wireshark.org  TCP      3471 > http [ACK] Seq=447 Ack=2521 Win=645
 20 61.919358   www.wireshark.org  192.168.0.6        TCP      [TCP segment of a reassembled PDU]

+ Frame 1 (74 bytes on wire, 74 bytes captured)
+ Ethernet II, Src: Asustek                              _92:7d:67 (00:50:ba:92:7d:67)
+ Internet Protocol, Src: 1                              (192.168.0.1)
+ Internet Control Message

0000  00 50 ba 92 7d 67 00 17  31 7c 35 4b 08 00 45 00   .P..}g.. 1|5K..E.
0010  00 3c 82 a8 00 00 80 0                             ....
0020  00 01 08 00 3e 5c 02 0                             cdef
0030  67 68 69 6a 6b 6c 6d 6                             stuv
0040  77 61 62 63 64 65 66 6

File: "C:\DOCUME~1\Aubrey\LOCALS~1\Temp\ether0000XF9LT" 29 KB 00:01:52   P: 83 D: 83 M: 0 Drops: 0
```

1-The PDU (or Packet) **List Pane** at the top of the diagram displays a summary of each packet captured. By clicking on packets in this pane, you control what is shown in the other two panes.

2. The PDU (or Packet) Details Pane, located in the middle of the diagram, displays the packet selected in the Packet List Pane in greater detail.

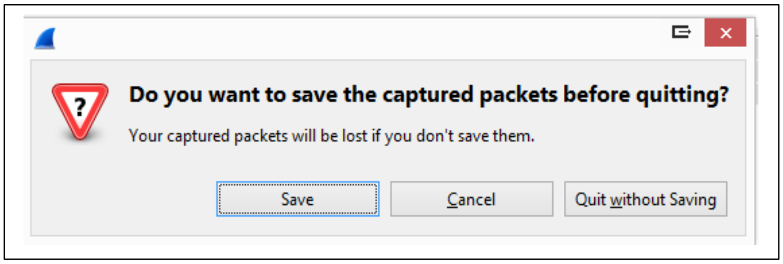
3-The PDU (or Packet) **Bytes Pane** at the bottom of the diagram displays the **actual data** (in hexadecimal form representing the actual binary) from the packet selected in the Packet List Pane and highlights the field selected in the Packet Details Pane.

Each line in the Packet List corresponds to one PDU or packet of the captured data. If you select a line in this pane, more details will be displayed in the "**Packet Details**" and "**Packet Bytes**" panes. The example above shows the PDUs captured when the ping utility was used and http://www.Wireshark.org was accessed. Packet number 1 is selected on this plane.

The Packet Details pane shows the current packet (selected in the "Packet List" pane) in a more detailed form. This page shows the protocols and protocol fields of the selected packet. The protocols and fields of the packet are displayed using a tree, which can be expanded and collapsed.

The Packet Bytes pane shows the data of the current packet (selected in the "Packet List" pane) in what is known as "hex dump" style. The information captured for the data PDUs can be **saved** in a file.

When closing a data capture screen or exiting Wireshark, you are prompted to save the captured PDUs. Clicking on **Continue without saving** the file or exiting Wireshark without saving the displayed captured data.


Do you want to save the captured packets before quitting?

Your captured packets will be lost if you don't save them.

3) Cables

Cables and More Cables

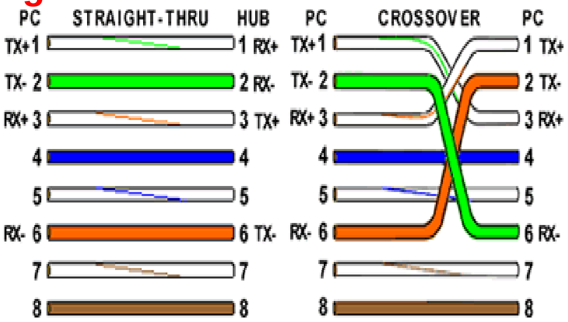
At the **Physical** layer (Layer 1) of the **OSI model**, end devices must be connected by **media** (cables). The type of media required depends on the type of device being connected. In the lab, you'll find three different types of cables:

1-Straight-through Cables:

Straight-through cable has connectors at each end that are terminated the same to either the T568A or T568B standards.

Use a straight-through cable for the following connections:

- Switch to the router Ethernet port
- Computer to switch.
- Computer to hub or switch



2-Crossover cable:

Directly connects two network devices of the **same** type over **Ethernet**. In T111, all the crossover cables are **orange** **or** **yellow.**

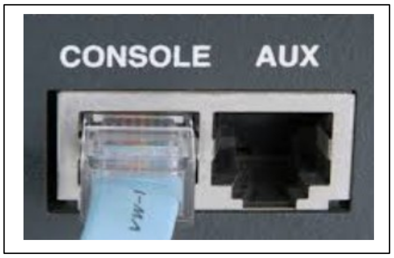
Use a **crossover** cable for the following connections:

- Switch to Switch
- Switch to hub
- Hub to hub

- Router-to-router Ethernet port
- Router to PC
- Router to server

3-Console Cables (Roll over cable)

Connect a computer to a Cisco device via the **console port**. Rollover cables have a DB9 connector at one end and an RJ45 connector at the other end. It is used to configure initial settings for the **Cisco** routers only.



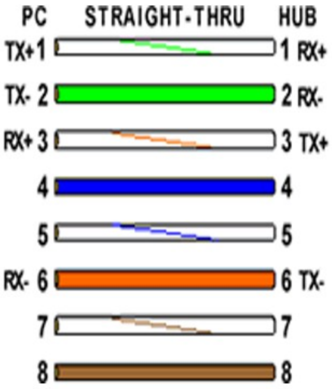
Use a console cable for the following connections:

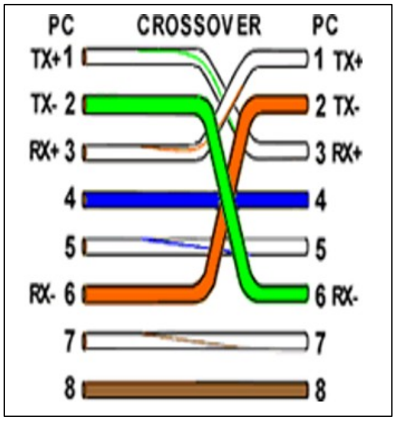
- Computer to a switch **console** port (Cisco)
- Computer to a router **console** port (Cisco)

- RJ45 adapter to USB cable. (for laptops **without an RJ45 port**)

Why are we using a crossover cable between routers and PCs/servers?

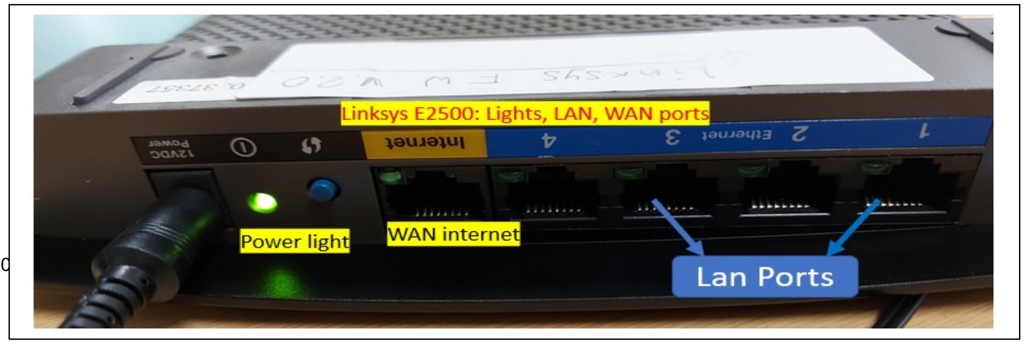
Since they use the same lines for sending (TX) and receiving (RX). We want "cross" these lines so on the line that one device sends, the other device "receives" and vice versa.



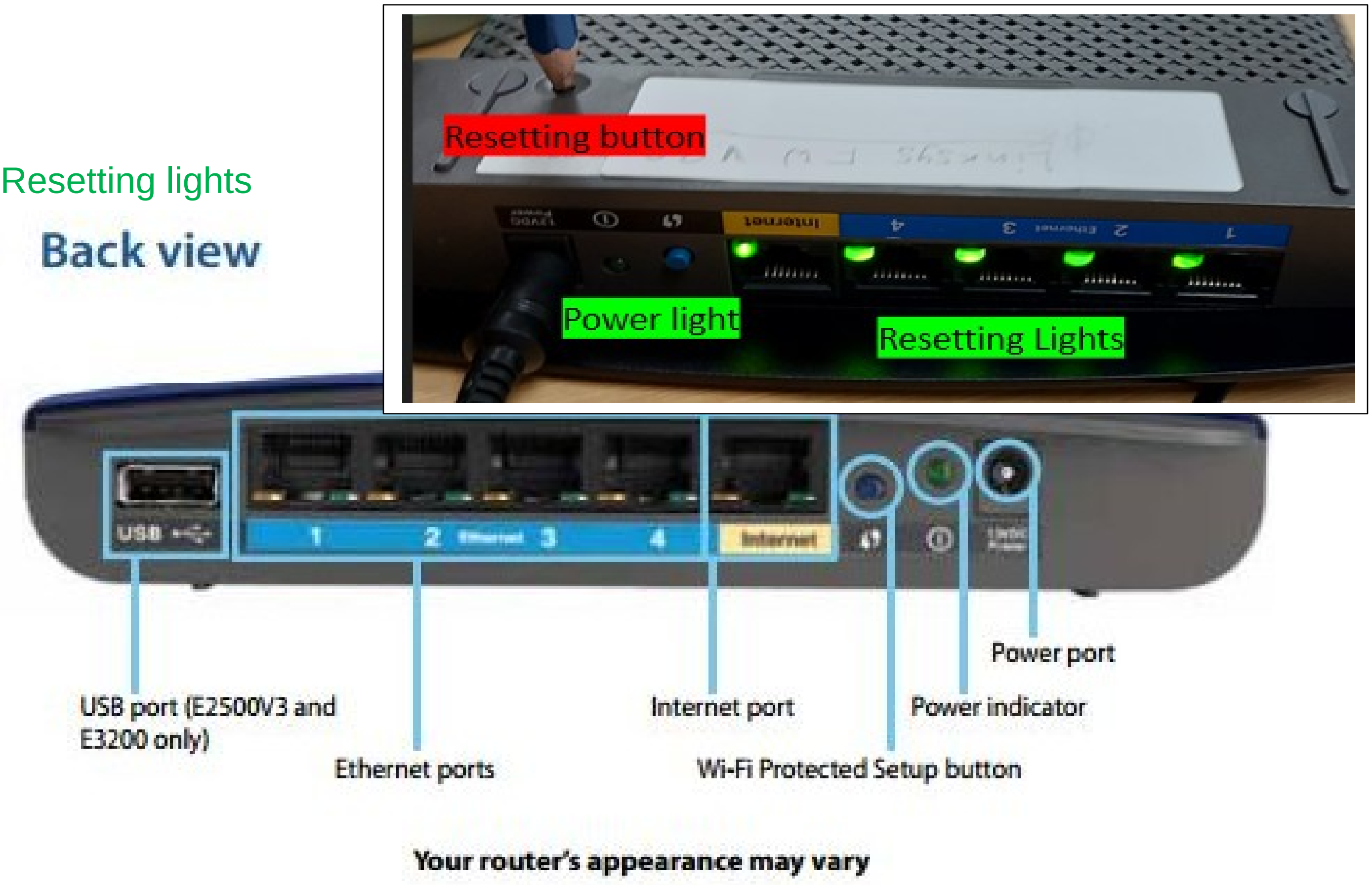


4) Linksys E2500 router/DHCP

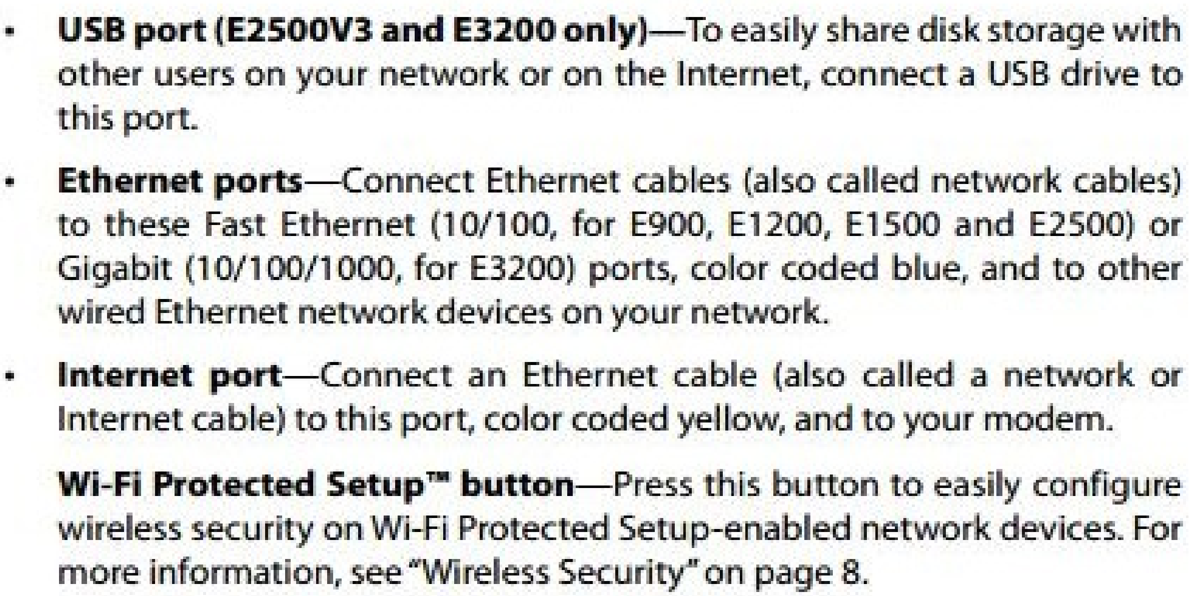
power light



Resetting lights



Your router's appearance may vary



- **USB port (E2500V3 and E3200 only)**—To easily share disk storage with other users on your network or on the Internet, connect a USB drive to this port.
- **Ethernet ports**—Connect Ethernet cables (also called network cables) to these Fast Ethernet (10/100, for E900, E1200, E1500 and E2500) or Gigabit (10/100/1000, for E3200) ports, color coded blue, and to other wired Ethernet network devices on your network.
- **Internet port**—Connect an Ethernet cable (also called a network or Internet cable) to this port, color coded yellow, and to your modem.

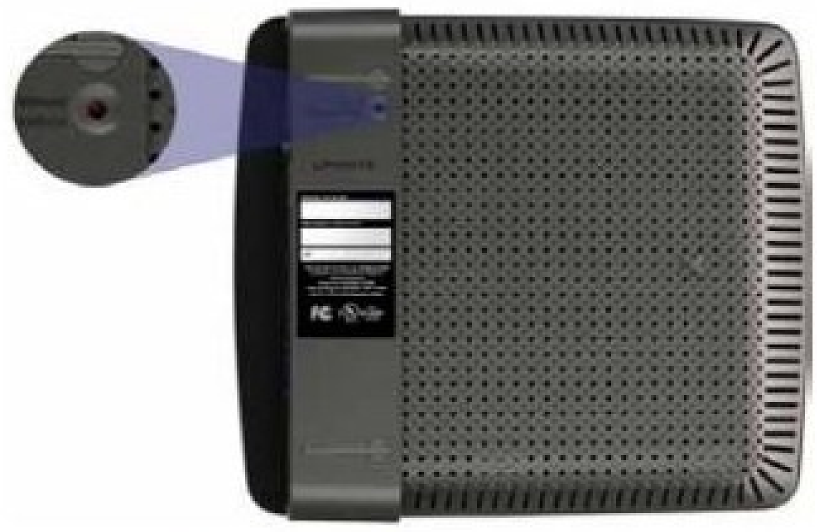
Wi-Fi Protected Setup™ button—Press this button to easily configure wireless security on Wi-Fi Protected Setup-enabled network devices. For more information, see "Wireless Security" on page 8.

- **Power indicator**—Stays on steadily while power is connected and following a successful Wi-Fi Protected Setup connection. Flashes slowly during bootup, during firmware upgrades, and during a Wi-Fi Protected Setup connection. Flashes quickly when there is a Wi-Fi Protected Setup error.
- **Power**—Connect the included AC power adapter to this port.

> **CAUTION**
> Use only the adapter that came with your router.

- **Power button**—Press | (on) to turn on the router.

Bottom view



Your router's appearance may vary

- **Reset button**—Press and hold this button for 5-10 seconds (until the port lights flash at the same time) to reset the router to its factory defaults. You can also restore the defaults using the browser-based utility.

5) The ICMP Protocol

The Internet Control Message Protocol (ICMP) was first defined in RFC 792. ICMP operates on the TCP/IP **Network layer** and is used to exchange information between devices.

When a router cannot deliver a packet to a destination network or host, an informational message is returned to the source. Also, the **ping** and **tracert** commands send ICMP messages to destinations, and destinations respond with ICMP messages.

Understand the Format of ICMP Packets.

Figure 1. ICMP Message Header

The ICMP header fields are common to all ICMP message types. Each ICMP message starts with an 8-bit Type field, an 8-bit Code field, and a computed 16-bit Checksum. The ICMP message type describes the remaining ICMP fields. The table in Figure 2 shows ICMP message types from RFC 792:

Value	**Meaning**
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply

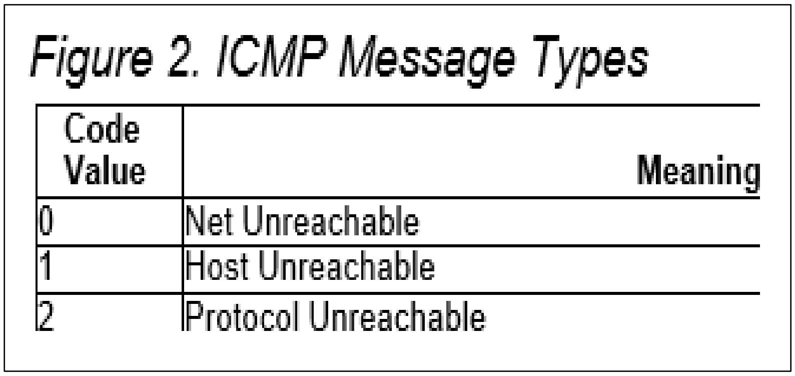


Figure 2. ICMP Message Types

Code Value	Meaning
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable

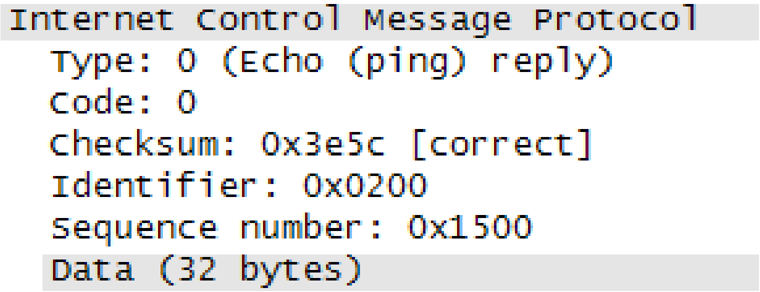
Codes provide additional information to the Type field. For example, if the Type field is **3, the destination is unreachable**, and additional information about the problem is returned in the Code field. The table in Figure 3 shows message codes for an ICMP Type 3 message, destination unreachable, from RFC 1700:

3	Port Unreachable
4	Fragmentation Needed and Don't Fragment Was Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Communication with Destination Network is Administratively Prohibited
10	Communication with the Destination Host is Administratively Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service

Figure 3. ICMP Type 3 Message Codes

Using the ICMP message capture shown in Figure 4, fill in the fields for the ICMP packet echo request. Values beginning with 0x are hexadecimal numbers:

Figure 4. ICMP Packet Echo Reply



```
Internet Control Message Protocol
   Type: 0 (Echo (ping) reply)
   Code: 0
   Checksum: 0x3e5c [correct]
   Identifier: 0x0200
   Sequence number: 0x1500
   Data (32 bytes)
```

On the TCP/IP Network layer, communication between devices is not guaranteed. However, ICMP does

Provide minimal checks for a reply to match the request.