Cisco | Networking Academy®
Mind Wide Open™

CCNA Discovery 4.0

Networking for Home and Small Businesses
Student Packet Tracer Lab Manual

3.5.7.2 Learn to Use Packet Tracer

Objectives

- Develop an understanding of the basic functions of Packet Tracer.
- Create/model a simple Ethernet network using two hosts and a hub.
- Observe traffic behavior on the network.
- Observer data flow of ARP broadcasts and pings.

Hint: To ensure that the instructions always remain visible during an activity, click the "Top" check box in the lower left-hand corner of this instruction window.

Step 1: Create a logical network diagram with two PCs and a hub

The bottom left-hand corner of the Packet Tracer screen displays eight icons that represent device categories or groups, such as Routers, Switches, or End Devices.

Moving the cursor over the device categories will show the name of the category in the box. To select a device, first select the device category. Once the device category is selected, the options within that category appear in the box next to the category listings. Select the device option that is required.

a) Select **End Devices** from the options in the bottom left-hand corner. Drag and drop two generic PCs onto your design area.

b) Select **Hubs** from the options in the bottom left-hand corner. Add a hub to the prototype network by dragging and dropping a generic hub onto the design area.

c) Select **Connections** from the bottom left-hand corner. Choose a **Copper Straight-through** cable type. Click on the first host, **PC0**, and assign the cable to the **FastEthernet** connector. Click on the hub, **Hub0**, and select a connection port, **Port 0**, to connect to **PC0**.

d) Repeat Step c for the second PC, **PC1**, to connect the PC to **Port 1** on the hub.

*There should be green dots at both ends of each cable connection. If not, check the cable type selected.

Step 2: Configure host names and IP addresses on the PCs

a) Click on PC0. A PC0 window will appear.

b) From the PC0 window, select the **Config** tab. Change the PC **Display Name** to **PC-A**. (An error message window will appear warning that changing the device name may affect scoring of the activity. Ignore this error message.) Select the **FastEthernet** tab on the left and add the IP address of **192.168.1.1** and subnet mask of **255.255.255.0**. Close the PC-A configuration window by selecting the **x** in the upper right-hand corner.

c) Click on PC1.

d) Select the **Config** tab. Change the PC **Display Name** to **PC-B**. Select the **FastEthernet** tab on the left and add the IP address of **192.168.1.2** and subnet mask of **255.255.255.0**. Close the PC-B configuration window.

Step 3: Observe the flow of data from PC-A to PC-B by creating network traffic

a) Switch to **Simulation** mode by selecting the tab that is partially hidden behind the **Realtime** tab in the bottom right-hand corner. The tab has the icon of a stopwatch on it.

b) Click the **Edit Filters** button in the **Edit List Filters** area. Clicking the **Edit Filters** button will create a pop-up window. In the pop-up window, click the **Show All/None** box to deselect every filter. Select just the **ARP** and **ICMP** filters.

c) Select a **Simple PDU** by clicking the closed envelope on the right vertical toolbar. Move your cursor to the display area of your screen. Click on **PC-A** to establish the source. Move your cursor to **PC-B** and click to establish the destination.

**Notice that two envelopes are now positioned beside PC-A. One envelope is ICMP, while the other is ARP. The Event List in the Simulation Panel will identify exactly which envelope represents ICMP and which represents ARP.

d) Select **Auto Capture / Play** from the **Play Controls** area of the Simulation Panel. Below the **Auto Capture / Play** button is a horizontal bar, with a vertical button that controls the speed of the simulation. Dragging the button to the right will speed up the simulation, while dragging is to the left will slow down the simulation.

e) The animation will run until the message window *No More Events* appears. All requested events have been completed. Select OK to close the message box.

f) Choose the **Reset Simulation** button in the Simulation Panel. Notice that the ARP envelope is no longer present. This has reset the simulation but has not cleared any configuration changes or dynamic table entries, such as ARP table entries. The ARP request is not necessary to complete the **ping** command because PC-A already has the MAC address in the ARP table.

g) Choose the **Capture / Forward** button. The ICMP envelope will move from the source to the hub and stop. The **Capture / Forward** button allows you to run the simulation one step at a time. Continue selecting the **Capture / Forward** button until you complete the event.

h) Choose the **Power Cycle Devices** button on the bottom left, above the device icons.

i) An error message will appear asking you to confirm reset. Choose **Yes**. Now both the ICMP and ARP envelops are present again. The **Reset Network** button will clear any configuration changes not saved and will clear all dynamic table entries, such as the ARP and MAC table entries.

Step 4: View ARP Tables on each PC

a) Choose the **Auto Capture / Play** button to repopulate the ARP table on the PCs. Click **OK** when the *No More Events* message appears.

b) Select the magnifying glass on the right vertical tool bar.

c) Click on **PC-A**. The ARP table for PC-A will appear. Notice that PC-A does have an ARP entry for PC-C. View the ARP tables for PC-B and PC-C as well. Close all ARP table windows.

d) Click the **Select Tool** on the right vertical tool bar. (This is the first icon present in the toolbar.)

e) Click on **PC-A** and select the **Desktop** tab.

f) Select the **Command Prompt** and type the command **`arp -a`** and hit enter to view the ARP table from the desktop view. Close the PC-A configuration window.

g) Examine the ARP table for **PC-B**.

h) Close the PC-B configuration window.

i) Click the **Check Results** button at the bottom of the instruction window to verify that the topology is correct.

3.6.2.3 Prototyping a Network

Objectives

- Prototype a network using Packet Tracer

Background

A client has requested that you set up a simple network with two PCs connected to a switch. Verify that the hardware, along with the given configurations, meet the requirements of the client.

Step 1: Set up the network topology

a) Add two PCs and a Cisco 2950T switch.

b) Using straight-through cables, connect **PC0** to interface **Fa0/1** on **Switch0** and **PC1** to interface **Fa0/2** on **Switch0**.

c) Configure PC0 using the **Config** tab in the PC0 configuration window:

1. IP address: 192.168.10.10
2. Subnet Mask 255.255.255.0

d) Configure PC1 using the **Config** tab in the PC1 configuration window:

1. IP address: 192.168.10.11
2. Subnet Mask 255.255.255.0

Step 2: Test connectivity from PC0 to PC1

a) Use the **`ping`** command to test connectivity.

1. Click PC0.
2. Choose the **Desktop** tab.
3. Choose **Command Prompt**.
4. Type: **`ping 192.168.10.11`** and press *enter*.

b) A successful **`ping`** indicates the network was configured correctly and the prototype validates the hardware and software configurations. A successful ping should resemble the below output:

```
PC>ping 192.168.10.11
```

```
Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time=170ms TTL=128
Reply from 192.168.10.11: bytes=32 time=71ms TTL=128
Reply from 192.168.10.11: bytes=32 time=70ms TTL=128
Reply from 192.168.10.11: bytes=32 time=68ms TTL=128

Ping statistics for 192.168.10.11:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 68ms, Maximum = 170ms, Average = 94ms
```

Close the configuration window.

c) Click the **Check Results** button at the bottom of the instruction window to check your work.

4.2.3.2 Observing Packets Across the Network

Objectives

- Use **ping** and **tracert** to verify connectivity from source to destination.

This activity will begin showing 100% completion. This is because the activity is designed to demonstrate the behavior of ping and tracert. This activity is not designed to be graded.

Background

A network administrator wants to verify the path a packet takes to get to a destination web server.

Step 1: Verify connectivity from the source host to the destination host

a) Open the source host command prompt window and **ping** the destination

1. Select PC0.
2. Select the **Desktop** tab > **Command Prompt**
3. Type: **ping 192.168.3.2** and press *enter*.

*A Reply verifies connectivity from the host to the destination device. It does not indicate the path that was taken to reach it.

The first few **pings may time out while devices load. If all **pings** time out, repeat the command.

Step 2: Determine the path taken to the destination using tracert

a) From within the same **Command Prompt** window for PC0, type **tracert 192.168.3.2** and press *enter*l.
*The **tracert** should display four hops, the fourth hop is the actual destination. This not only verifies connectivity between the devices, but also provides the exact path the packets traveled to reach it.

b) Close the PC0 configuration window.

Step 3: View the packet path in simulation mode

a) Open the simulation window by clicking the **Simulation** tab. It is located behind the **Realtime** time tab in the lower right-hand corner.

b) Click the **Add Simple PDU** button. This is the closed envelope located on the right-hand side of the screen. Once this is selected, click PC0 and PC1. This will create a **ping** packet from source to destination

c) Click the **Edit Filters** button to open the filter list. Ensure that only ICMP is checked.

d) In the work area window, click the network cloud to expand it and view router devices connected within the cloud. The source and destination devices are off screen. The focus is on the Routers within the network cloud only and packets forwarded between these devices.

e) Use the **Auto Capture / Play** button in the Simulation Panel window and observe the path the packet travels to reach the destination.

*Notice within the Event List, there are three routers used between source and destination. This is the same path indicated in the earlier PC command prompt window using the **`tracert`** command.

5.1.1.2 Connecting to a Web Server Using IP

Objective

- Observe how packets are sent across the Internet using IP addresses

  This activity will begin showing 100% completion. This is because the activity is designed to demonstrate how to connect to a web server using IP. This activity is not designed to be graded.

Step 1: Verify connectivity to the web server

a) Open the source host command prompt window.

1. Select PC0.

2. Select the **Desktop Tab > Command Prompt**.

b) Verify connectivity to the web server.

1. At the command prompt, **`ping`** the IP address of the web server by typing **`ping 172.33.100.50`** and pressing the *enter* key.

   *A reply verifies connectivity from the client to the destination web server. The reply may time out initially while devices load and ARP is performed.

c) Close the command prompt window, by selecting the **x** in the upper right-hand corner of the command prompt window. Be sure to leave the PC0 configuration window open.

Step 2: Connect to the Web Server via the web client

a) Open the source host web browser client.

1. From within the PC0 desktop window, select the **Web Browser**, to open the web client utility.

b) Type **172.33.100.50** into the URL block and select "Go".

*The web client will connect to the web server via IP address and will open the web site.

c) Close the PC0 configuration window. The activity is complete.

5.3.3.3 Configuring DHCP on a Multi-function Device

Objective

- Connect three PCs to a Linksys-WRT300N, which is a multi-function device
- Change the DHCP setting to a specific network range
- Configure the clients to obtain an IP address via DHCP

Background

A home user wants to use a Linksys-WRT300N device to connect three PCs. All three PCs should obtain an IP address automatically from the Linksys device.

Step 1: Set up the network topology

a) Add three PCs to the work area.

b) Add a Linksys-WRT300N to the work area.

c) Connect each PC to an Ethernet port on the Linksys device using a straight through cable.

Step 2: Observe the default DHCP settings

a) Click the Linksys-WRT300N Router to open the configuration window.

b) Click the **Config** tab and change the **Display Name** to **DHCP Enabled Router**.
*Note: A popup window will appear when changing the Display Name warning that changing the Display Name may affect scoring. Proceed with changing the Display Name since it must match exactly for the activity to score correctly.

c) Select the **GUI** tab.
*This navigates to the **Setup / Basic Setup** page within the Linksys GUI.

d) Scroll through the Basic Setup page to view default settings, including the default IP address of the Linksys device.
*Note that DHCP is enabled, the starting address of the DHCP range and the range of addresses available to clients.

Step 3: Change the default IP address of the Linksys device

a) Within the **Router IP** section, change the IP address of the Linksys device to: **192.168.5.1**.

b) Scroll to the bottom of the GUI page and click **Save Settings**.

c) Scroll back up to the Router IP section to ensure the change is made.

Step 4: Change the default DHCP range of addresses

a) Notice the starting IP address in the DHCP Server Setting is updated to match the same network as the IP address of the Linksys device: **192.168.5.100**.

b) Change the **Starting IP Address** from **192.168.5.100** to **192.168.5.26**.

c) Change the **Maximum Number of Users** to **75**.

d) Scroll to the bottom of the GUI page and click **Save Settings**.

e) Scroll back up to the DHCP Setting section to ensure the change is made.
*Notice the range of address available to clients has updated to reflect the change.

f) Close the Linksys configuration window.

Step 5: Configure DHCP on the client workstations

a) Enable DHCP on **PC0**.

1. Click PC0.
2. Click he **Config** tab. Go to the Interface **FastEthernet** sub-menu.
3. Enable DHCP by selecting the **DHCP** button in the IP Configuration panel.
*Notice that an IP address and subnet mask is automatically assigned.
4. Close the configuration window.

b) Observe the IP configuration of a client that does not have DHCP enabled.

1. Click PC1.
2. Click the **Desktop** tab > **Command Prompt**.
3. Type **ipconfig** and press *enter*.
*Notice that all settings are set to 0.0.0.0. No IP address is assigned statically, and the PC has not obtained an address automatically from DHCP.

c) Enable DHCP on PC1 and PC2, using the **Config** tab as outlined in Step 5a.
*Notice that a different IP address from the one assigned to PC0 is automatically assigned to PC1 and PC2.

d) Close the configuration window.

Step 6: Verify connectivity

a) Click PC1 and select the **Desktop** tab > **Command Prompt**.

b) Type **ipconfig** to view the IP configuration of PC1.

c) Type **ping 192.168.5.1** to ping the Linksys device.

d) Type **ping 192.168.5.26** to ping PC0.
*You should receive a reply from both devices.

e) Close the configuration window and click **Check Results** button at the bottom of the instruction window to check your work.

f) Choose the **Assessment Items** tab to view any configurations that were not done correctly.

5.4.3.2 Examining NAT on a Multi-function Device

Objective

- Examine the Linksys GUI for NAT configuration
- Set up four PCs to connect to the Linksys device with DHCP enabled.
- Examine traffic that crosses the network using NAT.

Step 1: Examine the Linksys external configuration

a) Click the Linksys device to access the configuration window.
*Note: this may take several seconds.

b) Access the Linksys GUI menu by clicking the **GUI** tab.

c) Click the **Status** menu option in the upper right-hand corner. It is the last menu option to the right on the Linksys GUI page. Once selected, this defaults you to the **Router** page.

d) Scroll down the **Router** page to the **Internet Connection** panel. The IP address assigned to the Linksys device is assigned by the ISP. If no IP address is present, 0.0.0.0 appears. (The Linksys device is in the process of obtaining an address from the ISP DHCP server.) If there is no IP address shown, close the window, wait for a few seconds and try again.
*The address shown is assigned to the Internet port on the Linksys device. Is this a private or public address?

Step 2: Examine the Linksys internal configuration

a) Click the **Local Network** sub-menu button within the blue menu bar.

b) Scroll down to examine the Local Network information. This is the address assigned to the internal Linksys network.

c) Scroll down further to examine the DHCP server information, and range of IP addresses that can be assigned to connected hosts.
*Are these private or public addresses?

d) Close the Linksys configuration window.

Step 3: Connect four PCs to the Linksys device

a) Add four PCs to the PT work area and connect them to the Linksys device with a straight-through cable. Wait for all link lights to turn green before moving to the next step. This can take several seconds.

b) Use the **Config** tab to enable each device to receive an IP address via the Linksys DHCP server.

c) Check the IP configuration of each PC using the **ipconfig /all** command in the **Command Prompt** found under the **Desktop** tab.
*Note: These devices will receive a private address. Private addresses are not able to cross the Internet, therefore, NAT translation must occur.

d) Close all PC configuration windows.

Step 4: View NAT translation across the Linksys

a) Enter Simulation mode by clicking the **Simulation** tab in the lower right-hand corner. The **Simulation** tab is located behind the **Realtime** tab and has a stopwatch symbol.

b) View traffic by creating a Complex PDU in Simulation mode

1. From the Simulation Panel, select **Edit Filters** and check only the boxes for TCP and HTTP.
2. Add a Complex PDU by clicking the open envelope located above the Simulation mode icon.
3. Click one of the PCs to specify it as the source.

c) Specify the Complex PDU settings by changing the following within the Create Complex PDU window:

1. Under PDU Settings > Select Application should be set to **HTTP**.
2. Click the **ciscolearn.nat.com** server to specify it as the destination device.
3. For the Source Port type **1000**.
4. Under Simulation Settings select Periodic Interval and type **120** seconds.
5. Create the PDU by clicking the box Create PDU in the Create Complex PDU window.

d) Double click the Simulation Panel to unlock it from the PT window. This allows you to move the Simulation Panel to view the entire network topology.

e) Observe the traffic flow by clicking the **Auto Capture / Play** button in the Simulation Panel. Speed up the animation by using the play control slider.
*When the Buffer Full window appears, close the window by clicking the **x** in the upper right-hand corner of the window.

Step 5: View the header information of the packets that traveled across the network

a) Examine the headers of the packets sent between the PC and the web server.

1. In the Simulation Panel, double click the third line down in the Event List. This displays an envelope in the work area that represents that line.
2. Click the envelope in the work area window to view the packet and header information.

b) Click the **Inbound PDU Details** tab. Examine the packet information for the source (SRC) IP address and destination IP address.

c) Click the **Outbound PDU Details** tab. Examine the packet information for the source (SRC) IP address and destination IP address.
*Notice the change in SRC IP address.

d) Click through other event lines to view those headers throughout the process.

e) When finished, click the **Check Results** button at the bottom of the instruction window to check your work.

6.2.2.2 Observing Web Requests

Objective

View the client/server traffic sent from a PC to a web server when requesting web services.

This activity will begin showing 100% completion. This is because the activity is designed to demonstrate the flow of packets between a PC and a web server. This activity is not designed to be graded.

Step 1: Verify connectivity to the web server

a) Click the External Client and access the **Command Prompt** from the **Desktop** tab.

b) Use the **ping** command to reach the URL **ciscolearn.web.com**.
*Notice that the IP address is included in the ping output. This address is obtained from the DNS server. All traffic forwarded across the network uses IP address information.

c) Close the Command Prompt window, but leave the External Client desktop window open.

Step 2: Connect to the web server

a) From the desktop window, access the web browser.

b) In the URL block, type ciscolearn.web.com.
*Be sure to read the web page that is displayed. Leave this page open.

Step 3: View the HTML code

a) Click the ciscolearn.web.com server.

b) Click the **Config** tab > **HTTP** tab.

c) Compare the text written in the HTML coding on the server to the Web Browser display page on the External Client. This may require that you re-maximize the External Client window if it shrunk when you opened the server window.

d) Close both the External Client and web server windows.

Step 4: Observe traffic between the client and the web server

a) Enter Simulation mode by clicking the **Simulation tab** in the lower right-hand corner. The **Simulation** tab is located behind the **Realtime** tab and has a stopwatch symbol.

b) Double click the Simulation Panel to unlock it from the PT window. This allows you to move the Simulation Panel to view the entire network topology.

c) View traffic by creating a Complex PDU in Simulation mode

1. From the **Simulation Panel**, select **Edit Filters** and check only the boxes for TCP and HTTP.
2. Add a **Complex PDU** by clicking the open envelope located above the Simulation mode icon.
3. Click the External Client to specify it as the source. The complex PDU window will appear.
4. Click the **ciscolearn.web.com** server to specify it as the destination device. Notice the IP address of the web server will appear in the destination box within the complex PDU window.

d) Specify the **Complex PDU** settings by changing the following within the complex PDU window:

1. Under **PDU Settings** > **Select Application** should be set to **HTTP**.
2. For the Source Port type **1000**.
3. Under **Simulation Settings** select **Periodic Interval** and type **120** seconds.
4. Create the PDU by clicking the box **Create PDU** in the **Create Complex PDU** window.

e) Observe the traffic flow by clicking the **Auto Capture / Play** button in the Simulation Panel. Speed up the animation by using the play control slider.
*When the Buffer Full window appears, close the window using the **x**.

f) Scroll through the Event List. Notice the number of packets that traveled from source to destination. HTTP is a TCP protocol, which requires connection establishment and acknowledgement of receipt of packets, considerably increasing the amount of traffic overhead.

6.3.3.5 Viewing PDU Information Sent Between Client and Server

Objective

View the client server traffic sent from a PC to a server when requesting web services.

This activity will begin showing 100% completion. This is because the activity is designed to demonstrate the flow of traffic between a client and a server. This activity is not designed to be graded.

Step 1: Observe traffic between a client and a web server

a) Enter Simulation mode by clicking the **Simulation** tab in the lower right-hand corner. The **Simulation** tab is located behind the **Realtime** tab and has a stopwatch symbol.

b) View traffic by creating a Complex PDU in Simulation mode

1. From the **Simulation Panel**, select **Edit Filters** and check only the boxes for TCP and HTTP.
2. Add a **Complex PDU** by clicking the open envelope located above the Simulation mode icon.
3. Click the External Client to specify it as the source.

c) Specify the **Complex PDU** settings by changing the following within the **Create Complex PDU** window:

1. Under **PDU Settings** > **Select Application** should be set to **HTTP**.
2. Click the **ciscolearn.web.com** server to specify it as the destination device.
3. For the **Source Port** type **1000**.
4. Under **Simulation Settings** select **Periodic Interval** and type **120** seconds.
5. Create the PDU by clicking the box **Create PDU** in the **Create Complex PDU** window.

d) Double click the **Simulation Panel** to unlock it from the PT window. This allows you to move the Simulation Panel to view the entire network topology.

e) Observe the traffic flow by clicking the **Auto Capture / Play** button in the **Simulation Panel**. Speed up the animation by using the play control slider.
*When the **Buffer Full** window appears, close the window with the **x**.

Step 2: View the header information of the packets that traveled across the network

a) Examine the headers of the packets sent between the clients and server.

1. In the **Simulation Panel**, click any one of the lines in the Event List. This displays an envelope in the work area that represents that line.

2. Click the envelope in the work area window to view the packet and header information.

3. The **OSI Model** window displays within which layer of the OSI model the packet is being processed.
   *Notice that depending on the device that received the packet, the higher or lower the layer included. A switch will only display the packet to Layer 2. Whereas, the PC or Server will display the packet up to Layer 4.

4. In the **OSI Model** window, read the description of the packet.

5. Click the **Inbound PDU Details**, or **Outbound PDU Details** to view the actual packet sent.
   *Note the MAC address within the frame, the IP address information within the packet, and the source and destination port number within the segment.

6. Click through other event lines to read those descriptions as well

9.2.3.2 Using the Ipconfig Command

Objective

Use the **ipconfig** command to identify an incorrect configuration on a PC.

Background

A small business owner cannot connect to the Internet with one of the four PCs in the office. All of the PCs are configured with static IP addressing. Use the **ipconfig /all** command to identify which PC is incorrectly configured.

Step 1: Verify configurations

a) Access the **Command Prompt** on each PC and type the command: **ipconfig /all**.

b) Examine the IP address, subnet mask, and default gateway configuration on each PC.

*Be sure to record this IP configuration for each PC to help identify any PCs that are incorrectly configured.

Step 2: Correct any misconfigurations

a) Select the PC that is incorrectly configured and access the **Config** tab.

b) Click the **Desktop** tab > **IP Configuration** tab to correct the misconfiguration.

c) Click the **Check Results** button at the bottom of the instruction window to check your work.

9.2.4.3 Using the Ping Command

Objective

Use the **ping** command to identify an incorrect configuration on a PC.

Background

A small business owner learns that the user of PC2 is unable to access a website. All PCs are configured with static IP addressing. Use the **ping** command to identify the issue.

Step 1: Verify connectivity

a) Access the **Desktop** tab > **Web Browser** of each PC and type the URL **ciscolearn.more.com**.

b) Which PCs are unable to connect to the web server?
*Note: All of the devices require time to complete the boot process. Please allow up to one minute before receiving a web response.

Step 2: Ping the web server from PC2

a) On PC2, access the **Command Prompt** from the **Desktop** tab.

b) Type: **ping ciscolearn.more.com**.

c) Did the **ping** return a reply? What is the IP address returned, if any?

Step 3: Ping the web server from PC1

a) On PC1, access the **Command Prompt** from the **Desktop** tab.

b) Type: **ping ciscolearn.more.com**.

c) Did the **ping** return a reply? What is the IP address returned, if any?

Step 4: Ping the IP address of the web server from PC2

a) On PC2, access the **Command Prompt** from the **Desktop** tab.

b) Attempt to reach the IP address of the web server with the command **ping 192.15.2.10**.

c) Did the **ping** return a reply? If so, then PC2 is able to reach the web server via IP address, but not domain name. This could indicate a problem with the DNS server configuration on PC2.

Step 5: Compare the DNS server information on PC2 with other PCs on the local network

a) Access the **Command Prompt** of PC1.

b) Using the command **ipconfig /all**, examine the DNS server configuration on PC1.

c) Access the **Command Prompt** of PC2.

d) Using the command **ipconfig /all**, examine the DNS server configuration on PC2.
Do the two configurations match?

_____

Step 6: Make any necessary configuration changes on PC2

a) Using the **Config** tab of PC2, make any necessary configuration changes.

b) Using the **Web Browser** within the **Desktop** tab, connect to **ciscolearn.more.com** to verify that configuration changes resolved the problem.

c) Click the **Check Results** button at the bottom of the instruction window to check your work.

9.3.5.2 Troubleshooting a Wireless Connection

Objective

Identify and correct an incorrectly configured wireless device.

Background

A small business owner learns that a wireless user is unable to access the network. All devices are configured with static addressing. Identify and correct the issue.

Step 1: Verify connectivity

a) Access the desktop > web browser of each wireless device and type the URL: **ciscolearn.more.com**. Identify any devices that are not connecting to the web server.

*Are all wireless devices unable to connect to the web server, or only the single device?

**Note: All devices require time to complete the boot process. Please allow up to one minute before receiving a web response.

Step 2: Examine IP configuration of devices.

a) On a device that is not able to connect, access the command prompt from the desktop tab.

b) Type: **ipconfig /all**.

*Is IP addressing information available?

Step 3: Examine the Wireless Settings on the Wireless Client

a) Access the config tab of any devices unable to connect

b) Click the wireless tab to examine wireless settings

c) Record the SSID, Security Configurations, and IP address Configurations

*Do the two configurations match?

Step 4: Examine the Wireless Settings on the linksys Device

a) Access the linksys GUI

b) On the basic setup page, examine the DHCP configurations. Are they enabled?

c) Click on the Wireless tab

d) Examine the basic wireless setup information. What is the SSID? Does it match that configured on the client?

e) Click on the Wireless security submenu.

f) Examine security settings. Is WEP enabled? Does the key match that configured on the client?

Step 5: Make any necessary configuration changes

a. Using the config tab, make any necessary configuration changes.

b. Using the web browser within the desktop tab, connect to ciscolearn.more.com to verify that configuration changes worked.

c. Click Check Results to check your work.

9.3.5.2 Troubleshooting a Wireless Connection

Objective

Identify and correct any misconfiguration of a wireless device.

Background

A small business owner learns that a wireless user is unable to access the network. All of the PCs are configured with static IP addressing. Identify and resolve the issue.

Step 1: Verify connectivity

a) Access the **Desktop** > **Web Browser** of each wireless PC and type **ciscolearn.more.com** into the URL. Identify any PCs that are not connecting to the web server.

b) Which wireless PCs are unable to connect to the web server?
*Note: All of the devices require time to complete the boot process. Please allow up to one minute before receiving a web response.

Step 2: Examine the IP configuration of PCs

a) On the PC that is unable to connect, access the **Command Prompt** from the **Desktop** tab.

b) Type the **ipconfig /all** command.

c) What IP addressing information is available?

Step 3: Examine the Wireless Settings on the Wireless Client

a) Access the **Config** tab of any PC that is unable to connect.

b) Click the **Desktop** tab > **Wireless** tab to examine the wireless settings.

c) Record the SSID, Security Configurations, and IP address Configuration.

Step 4: Examine the Wireless Settings on the Linksys Device

a) Access the Linksys GUI.

b) On the **Basic Setup** page, examine the **DHCP Server Setting** configuration. Is DHCP enabled?

c) Click the **Wireless** tab.

d) Examine the information under the **Wireless** tab. What is the SSID? Does it match the SSID configured on the client?

e) Click the **Wireless Security** submenu.

f) Examine the security settings. Is WEP enabled? Does the key match the key configured on the client?

Step 5: Make any necessary configuration changes on the Wireless Clients

a) Using the **Config tab**, make any necessary configuration changes to the wireless PC.

b) Using the **Web Browser** within the **Desktop** tab, connect to **ciscolearn.more.com** to verify that the configuration changes resolved the problem.

c) Click the **Check Results** button at the bottom of the instruction window to check your work.