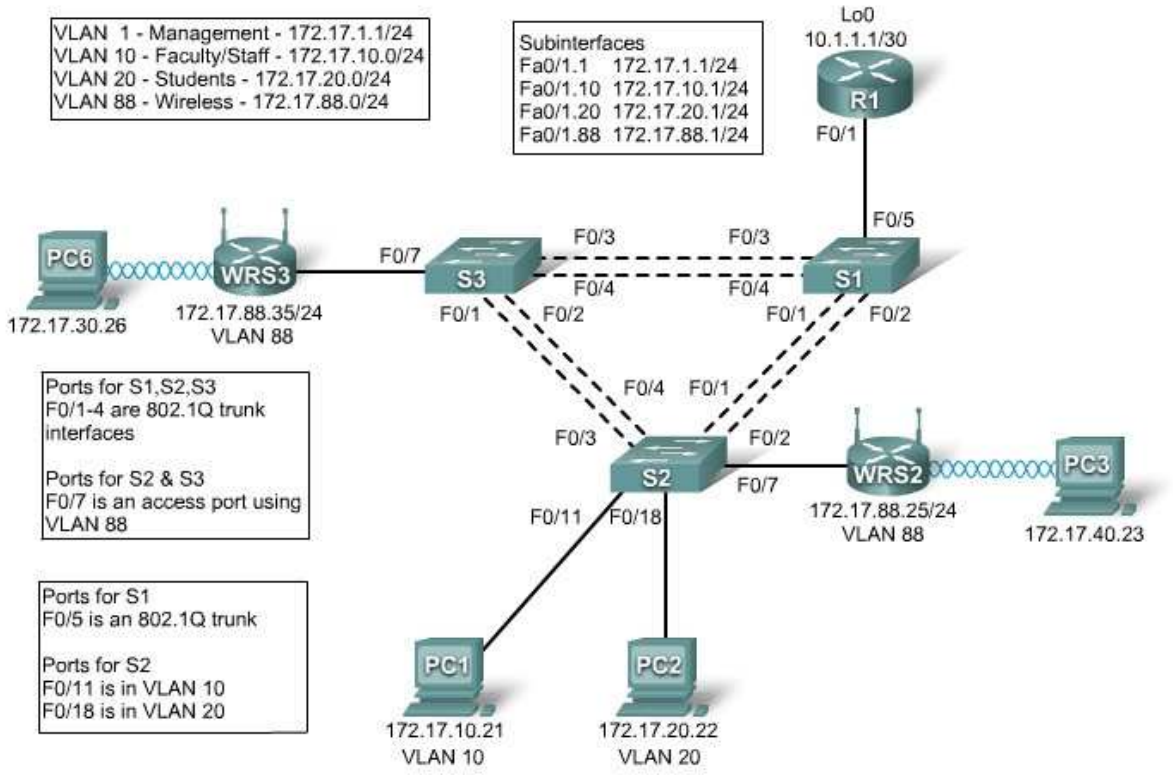
Cisco | Networking Academy®
Mind Wide Open™

CCNA Exploration 4.0

LAN Switching and Wireless
Instructor Lab Manual

Lab 7.5.2: Challenge Wireless Configuration (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/1.1**	172.17.1.1	255.255.255.0	N/A
	Fa0/1.10	172.17.10.1	255.255.255.0	N/A
	Fa0/1.20	172.17.20.1	255.255.255.0	N/A
	Fa0/1.88	172.17.88.1	255.255.255.0	N/A
	Lo0	10.1.1.1	255.255.255.252	N/A
WRS2	**WAN**	172.17.88.25	255.255.255.0	172.17.88.1
	LAN/Wireless	172.17.40.1	255.255.255.0	N/A
WRS3	**WAN**	172.17.88.35	255.255.255.0	172.17.88.1
	LAN/Wireless	172.17.30.1	255.255.255.0	N/A

PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Configure switch port VLAN information and port security.
- Hard reset a Linksys WRT300N router.
- Connect and verify connectivity to a wireless router.
- Navigate to a Linksys WRT300N's web utility page.
- Configure the IP settings of a Linksys WRT300N.
- Configure DHCP on a Linksys WRT300N.
- Configure static routes on both standard Cisco routers and on a WRT300N.
- Change the network mode and corresponding network channel on a WRT300N.
- Enable WEP encryption and disable SSID broadcast.
- Enable a wireless MAC filter.
- Configure access restrictions on a WRT300N.
- Configure router management password on a WRT300N.
- Enable logging on a WRT300N.
- Upgrade WRT300N firmware.
- Learn diagnosis, backup, restore, and confirmation mechanisms on a WRT300N.

Scenario

In this lab, you will configure a Linksys WRT300N, port security on a Cisco switch, and static routes on multiple devices. Make note of the procedures involved in connecting clients to a wireless network. Some configuration changes will cause clients to disconnect. These clients then have to reconnect after making changes to the configuration.

Task 1: Perform Basic Router Configurations

Step 1: Physically connect the devices based on the topology diagram.

Step 2: Configure R1 according to the following guidelines:

- Configure router hostname.
- Disable DNS lookup.
- Configure privileged EXEC password of **Cisco**.
- Configure FastEthernet 0/1 and its subinterfaces.
- Configure Loopback0.
- Configure synchronous logging, exec-timeout, and a password of **cisco** on the console port.


```
hostname R1
!
no ip domain-lookup
enable secret Cisco
!
interface FastEthernet0/1
  no shutdown
!
interface FastEthernet0/1.1
   encapsulation dot1 1
   ip address 172.17.1.1 255.255.255.0
!
interface FastEthernet0/1.10
   encapsulation dot1 10
   ip address 172.17.10.1 255.255.255.0
!
interface FastEthernet0/1.20
   encapsulation dot1 20
   ip address 172.17.20.1 255.255.255.0
!
interface FastEthernet0/1.88
   encapsulation dot1 88
   ip address 172.17.88.1 255.255.255.0
!
interface Loopback 0
   ip address 10.1.1.1 255.255.255.252
!
line con 0
 exec-timeout 0 0
 logging synchronous
 password cisco
 login
!
```

Task 2: Configure Switch Interfaces

Configure switch hostnames on S1, S2, and S3. Set the switches to transparent, clear the VLAN information, and create VLANs 10, 20, and 88.

<For all three switches>

```
hostname [S1, S2, S3]
!
vtp mode transparent
no vlan 2-1001
vlan 10,20,88
!
```

Step 1: Configure switch port interfaces on S1, S2, and S3.

Configure the interfaces on the S1, S2, and S3 switches with the connections from topology diagram.

Configure connections between two switches configure trunks.

Configure connections to a wireless router as access mode for VLAN 88.

Configure S2's connection to PC1 in VLAN 10 and PC2's connection in VLAN 20.

Configure S1's connection to R1 as a trunk.

Allow all VLANS across trunking interfaces.

S1

```
!
interface range FastEthernet 0/1-5
 switchport mode trunk
 no shutdown
!
```

S2

```
!
interface range FastEthernet 0/1-4
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/7
 switchport mode access
 switchport access vlan 88
 no shutdown
!
interface FastEthernet 0/11
 switchport mode access
 switchport access vlan 10
 no shutdown
!
interface FastEthernet 0/18
 switchport mode access
 switchport access vlan 20
 no shutdown
!
```

S3

```
!
interface range FastEthernet 0/1-4
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/7
 switchport mode access
 switchport access vlan 88
 no shutdown
!
```

Step 2: Verify VLANs and trunking.

Use the **show ip interface trunk** command on S1 and the **show vlan** command on S2 to verify that the switches are trunking correctly and the proper VLANs exist.

```
S1#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1
Fa0/3       on           802.1q         trunking      1
Fa0/4       on           802.1q         trunking      1
Fa0/5       on           802.1q         trunking      1
```



```
Port      Vlans allowed on trunk
Fa0/1       1-4094
Fa0/2       1-4094
Fa0/3       1-4094
Fa0/4       1-4094
Fa0/5       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,88
Fa0/2       1,10,20,88
Fa0/3       1,10,20,88
Fa0/4       1,10,20,88
Fa0/5       1,10,20,88

Port        Vlans in spanning tree forwarding state and not pruned

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,88
Fa0/2       none          <-- blocked due to STP - varies based on root
Fa0/3       1,10,20,88
Fa0/4       1,10,20,88
Fa0/5       1,10,20,88>
```

S2#show vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/12, Fa0/13,Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17,Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22,Fa0/23
                                                 Fa0/24, Gi0/1, Gi0/2
10   VLAN0010                          active    Fa0/11
20   VLAN0020                          active    Fa0/18
88   VLAN0088                          active    Fa0/7
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

When you have finished, be sure to save the running configuration to the NVRAM of the router and switches.

Step 3: Configure the Ethernet interfaces of PC1 and PC2.

Configure the Ethernet interfaces of PC1 and PC2 with the IP addresses and default gateways according to the addressing table at the beginning of the lab.

Step 4: Test the PC configuration.

Ping the default gateway from the PC: 172.17.10.1 for PC1, and 172.17.20.1 from PC2.

Go to Start->Run->cmd and type ping 172.17.x.x


```
C:\Documents and Settings\Administrator>ping 172.17.10.1

Pinging 172.17.10.1 with 32 bytes of data:

Reply from 172.17.10.1: bytes=32 time<1ms TTL=255
Reply from 172.17.10.1: bytes=32 time<1ms TTL=255
Reply from 172.17.10.1: bytes=32 time<1ms TTL=255
Reply from 172.17.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.17.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Task 3: Connect to the Linksys WRT300N Router WRS3

Check with your instructor that the wireless router has its factory default settings. If it does not, you must hard reset the router. To do so, find the reset button on the back of the router. Using a pen or other thin instrument, hold down the reset button for 5 seconds. The router should now be restored to its factory default settings.

Step 1: Connect to the wireless router.

When the wireless router is returned to its default configuration, it will broadcast the default SSID of “linksys”. Step 1: Use Windows XP to connect to the wireless router.

Note: Before attempting to connect to the WRS3 router, make sure that the WRS2 router’s power cord is unplugged. Having both wireless routers powered on will cause the PC to find two wireless networks with an SSID of “linksys”, making it difficult to distinguish which router you are trying to connect to.

Locate the Wireless Network Connection icon in your taskbar, or go to **Start > Control Panel > Network Connections**. Right-click the icon and select View Available Wireless Networks.

You are prompted with the following display. Note that the factory default SSID of the router is simply “Linksys.”

Select **Linksys** and click **Connect**.

After a period of time you will be connected.

Step 2: Verify connectivity settings.

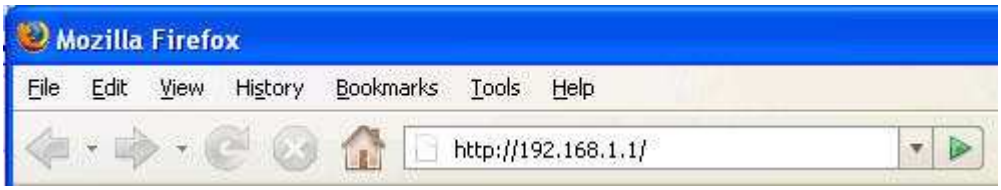
Verify the connectivity settings by going to **Start > Run** and typing **cmd**. At the command prompt, type the command **ipconfig** to view your network device information. Notice which IP address is the default gateway. This is the default IP address of a Linksys WRT300N.

```
IP Address. . . . . . . . . . . . : 192.168.1.100
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.1.1
```

Task 4: Configure the WRS3 Using the Web Utility

Step 1: Go to the default URL.

Using a web browser, navigate to **http://192.168.1.1** which is the default URL for the WRT300N.



Step 2: Enter authentication information.

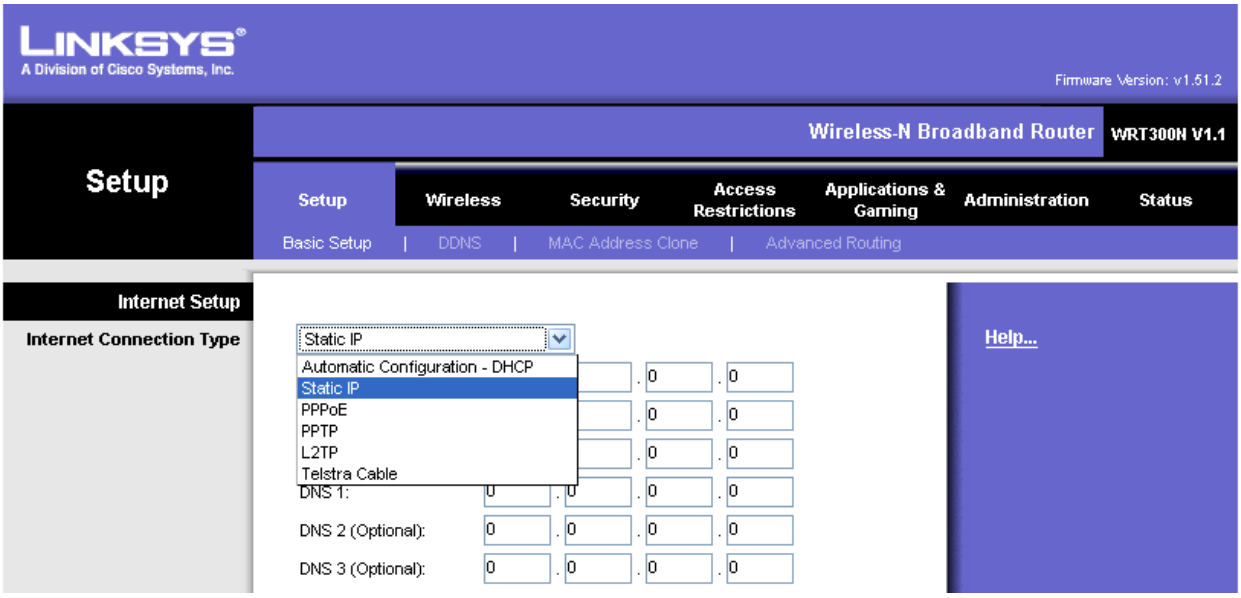
You are prompted for a username and password. Enter the WRT300N factory default password of **admin** and leave the username field blank.

You should now be viewing the default page of the Linksys WRT300N web utility.

Task 5: Configure IP Settings for the Linksys WRT300N

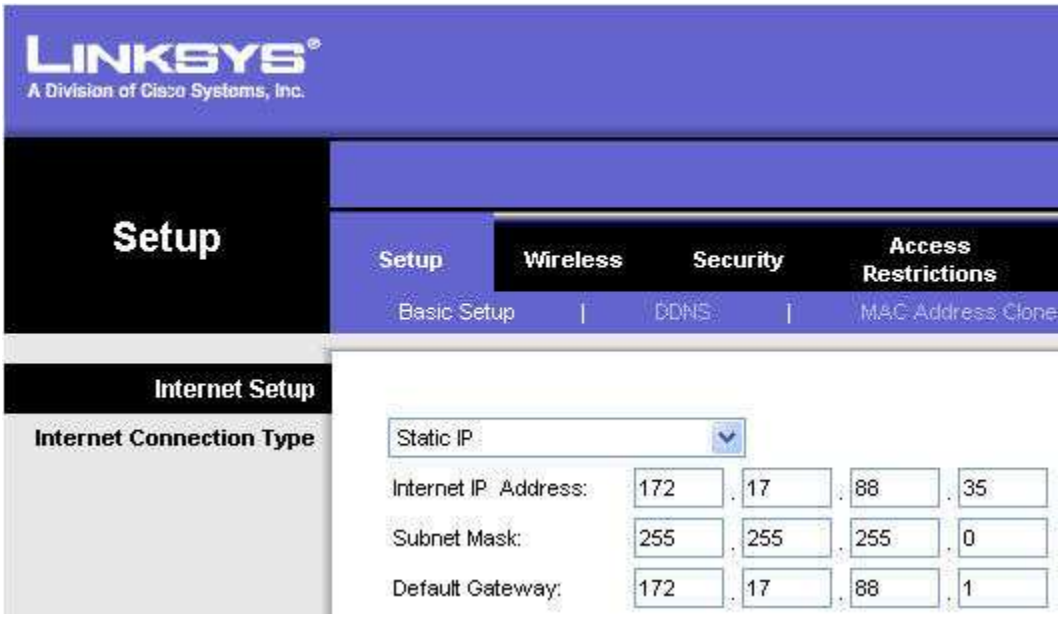
The best way to understand the difference between the **Internet Setup** and the **Network Setup** options is to think of the WRT300N as being similar to a Cisco IOS-based router with two separate interfaces. One of the interfaces, the one configured under **Internet Setup**, acts as the connection to the switches and the rest of the network. This connection would eventually lead out to the Internet, although in our topology there is no connection to the Internet. The other interface, configured under **Network Setup**, acts as the interface connecting to clients, both wireless and wired.

Step 1: Set the Internet connection type to static IP.

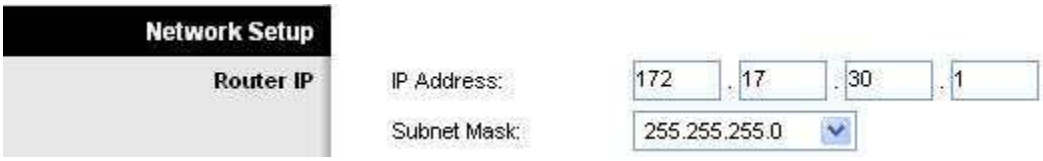


Step 2: Set the IP address settings for Internet Setup.

- Set the Internet IP Address to **172.17.88.35**.
- Set the Subnet Mask to **255.255.255.0**.
- Set the Default Gateway to **172.17.88.1** (the FastEthernet 0/1 VLAN 88 IP address of R1).



Step 3: Configure the Network Setup IP address to 172.17.30.1.



Step 4: Save the settings.

Click **Save Settings**. You are prompted to click **Continue**. Since you are connected wirelessly, you will not be redirected to the new URL of the web utility (**http://172.17.30.1**).

In order for the new IP address changes to take place, the PC has to release its old IP address and dynamically acquire a new one from the 172.17.30.0/24 network.

Step 5: Release the old Network Setup IP Address

In command prompt, use the command **ipconfig /release** to release the current DHCP address. To get a new IP address in the new network, issue the command **ipconfig /renew**. A new IP address should be pulled from the 172.17.30.0/24 network.

Step 6: View the PC IP configuration settings.

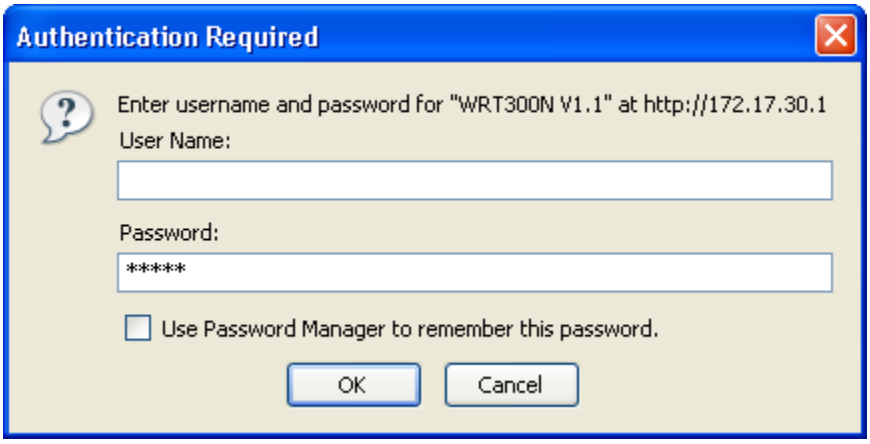
Go to command prompt and use the command **ipconfig**. If the address has not been updated to the 172.17.30.0/24 network, it will be necessary to release and renew the IP address on the client.

```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : cisco.com
        IP Address. . . . . . . . . . . . : 172.17.30.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.17.30.1
```


Step 7: Go to the new URL and enter authentication information.

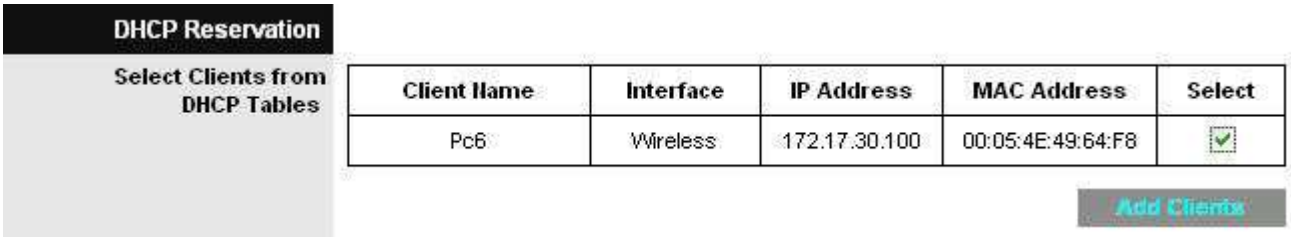
In your favorite web browser, navigate to **http://172.17.30.1** which is the new URL for the WRT300N. Enter the default username and password when you are prompted to do so.



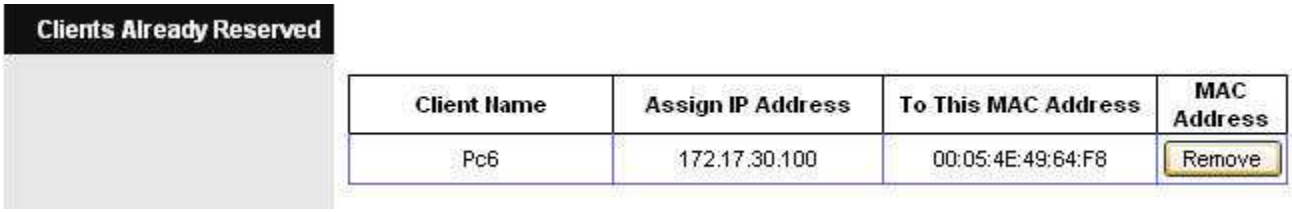
Task 6: Configure DHCP Settings and Router Time Zone Settings

Step 1: Give PC6 a static DHCP binding.

From the **Basic Setup** page in the **Network Setup** section, click **DHCP Reservations.** Find PC6 in the list of current DHCP clients. (Note that your PC may have a different name.) Click the check box in the correct row for the PC and then click **Add Clients**.

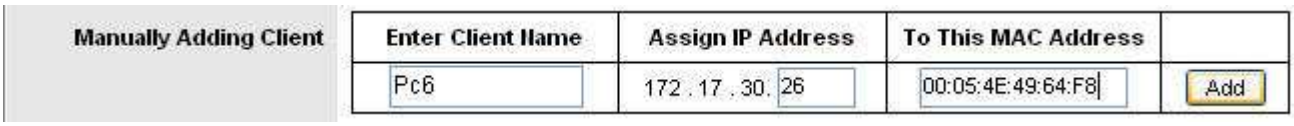


This gives PC6, the computer with a MAC address of 00:05:4E:49:64:F8, the same IP address, 172.17.30.100, whenever it requests an address through DHCP. This is only an example of a quick way to permanently bind a client to its current DHCP-given IP address. Now, you will assign PC6 the IP address in the topology diagram, not the one it received initially. Click **Remove** to assign a new address.



Step 2: Assign PC6 the 172.17.30.26 address.

By entering the PC6 address under Manually Adding Client, whenever PC6 connects to the wireless router, it receives the IP address 172.17.30.26 via DHCP. Save your changes.



Step 3: Verify the static IP address change.

Since we already have an IP address from DHCP we are not going to get the new address, 172.17.30.26, until we reconnect. We will wait and notice that later in Task 7, Step 6 and verify that this change has taken place.

Step 4: Configure the DHCP server.

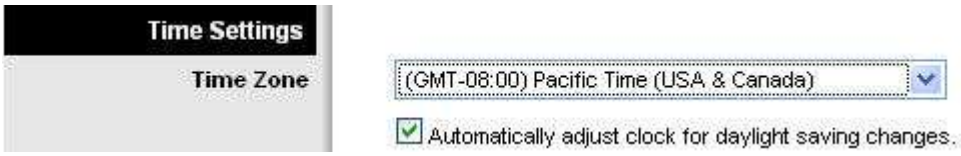
Set the start address to 50, the maximum number of users to 25, and the lease time to 2 hours (or 120 minutes).

These settings give any PC that connects to this router wirelessly requesting an IP address through DHCP, an address between 172.17.30.50–74. Only 25 clients at a time are able to get an IP address and can only have the IP address for two hours, after which time they must request a new one.

Note: IP Address Range does not update until you click **Save Settings**.

Step 5: Configure the router for the appropriate time zone.

At the bottom of the Basic Setup page, change the time zone of the router to reflect your location.



Step 6: Save your settings!

Click Save Settings**.** You are prompted to click **Continue.**

Task 7: Basic Wireless Settings

Step 1: Navigate to the Wireless page and set the network mode in the Basic Wireless Settings tab.

The Linksys WRT300N allows you to choose in which network mode to operate. Currently, the most used network mode for clients is Wireless-G and for routers is BG-Mixed. When a router is operating in BG-Mixed, it can accept both B and G clients. However, if a B client connects, the router must scale down to the slower level of B. For this lab, we are assuming all clients are running B only, so choose Wireless-B Only.

Step 2: Configure other settings.

Change the **Network Name (SSID**) to WRS3_[number], where the number is a unique ID number given to you by your instructor. Change the **Standard Channel** to the channel assigned to you by your instructor, and disable SSID Broadcast.

Why is it good to change the wireless channel to be different from the default channel?

_____

_____

To help prevent interference from other wireless routers

Why is it recommended to disable SSID broadcast?

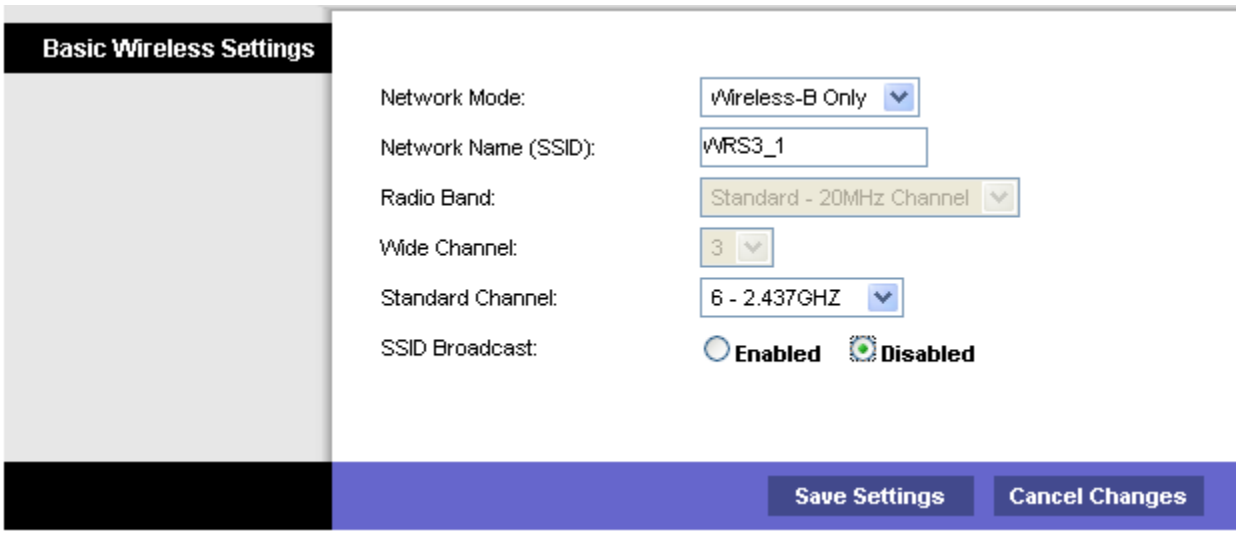
_____

_____

_____

_____

This allows a measure of security. Someone attempting to connect to the router minimally needs to know the SSID before being able to connect to it.



Step 3: Save Settings.

Select the **Save Settings** link to save all changes. Click **Continue** to continue to the next task.

Step 4: Verify that the SSID of the router is no longer being broadcast.

Scan for wireless networks. Locate the Wireless Network Connection icon in your taskbar, or go to **Start > Control Panel > Network Connections**. Right-click the icon and select View Available Wireless Networks.

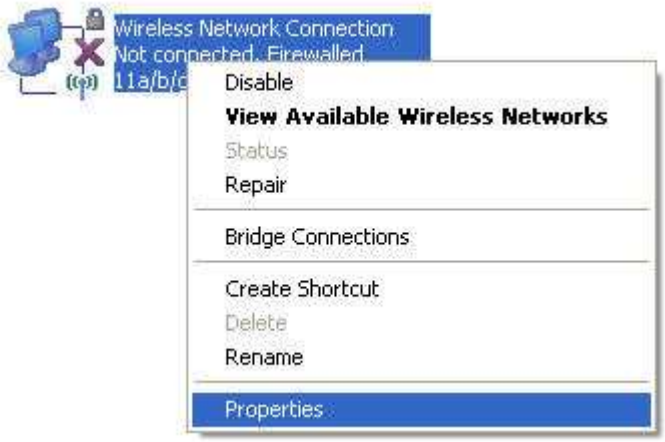
Does the SSID of the wireless router appear?

_____

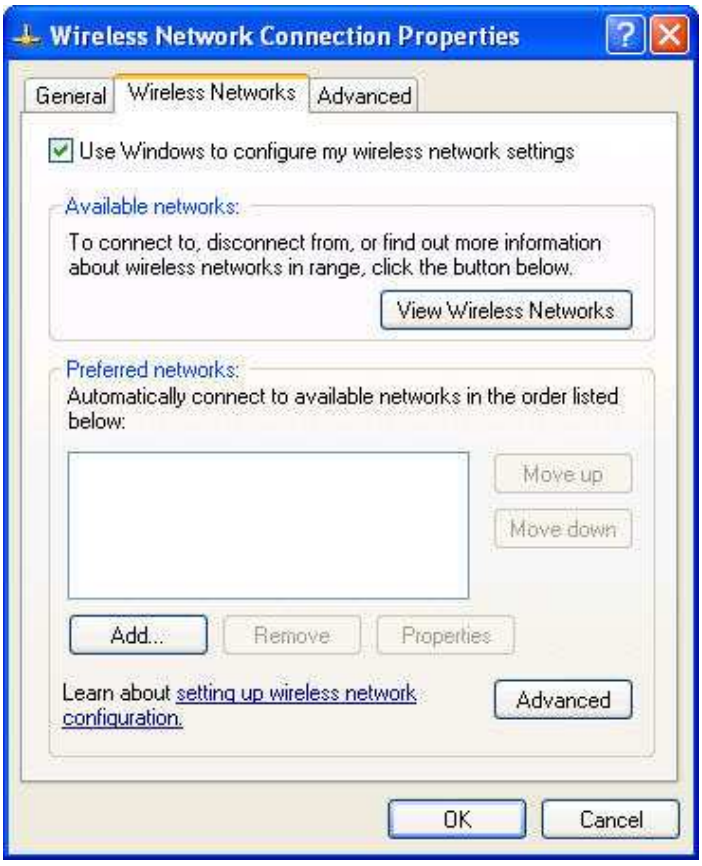
No

Step 5: Reconnect to the wireless network.

Navigate to **Start > Control Panel > Network Connections**, right-click the Wireless Network Connection icon, and select Properties.



In the Wireless Networks tab, select **Add**.



In the **Association** tab, enter WRS3_[number] as the SSID, and set the Data Encryption to **Disabled**. Select **OK**, and then select **OK** again. Windows should now try to reconnect to the wireless router.

Step 6: Verify the settings.

Now that you have reconnected to the network, you have the new DHCP settings that you configured in Task 6, Step 2. Verify this at the command prompt of PC6 with the **ipconfig** command.

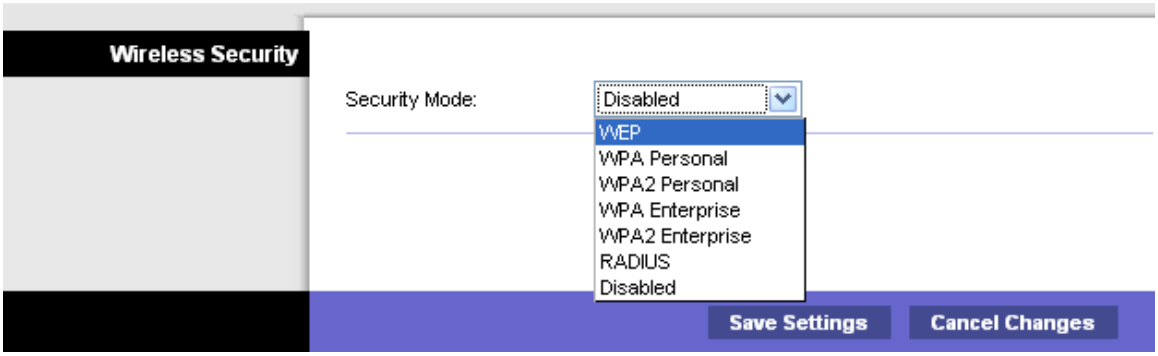
```
IP Address. . . . . . . . . . . . : 172.17.30.26
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 172.17.30.1
```

Task 8: Enable Wireless Security

Step 1: Reconnect to the router setup page (http://172.17.30.1).

Step 2: Navigate to the Wireless page and then select the Wireless Security tab.

Step 3: Under Security Mode, select WEP.



Step 4: Enter a WEP key.

A network is only as secure as its weakest point, and a wireless router is a very convenient place to start if someone wants to damage your network. By not broadcasting the SSID and requiring a WEP key to connect to the router, you are adding a few levels of security.

Unfortunately, there are tools that can discover networks that are not even broadcasting their SSID, and there are even tools that can crack WEP key encryption.

Add the WEP key **1234567890** as Key 1.

Step 5: Save your settings.

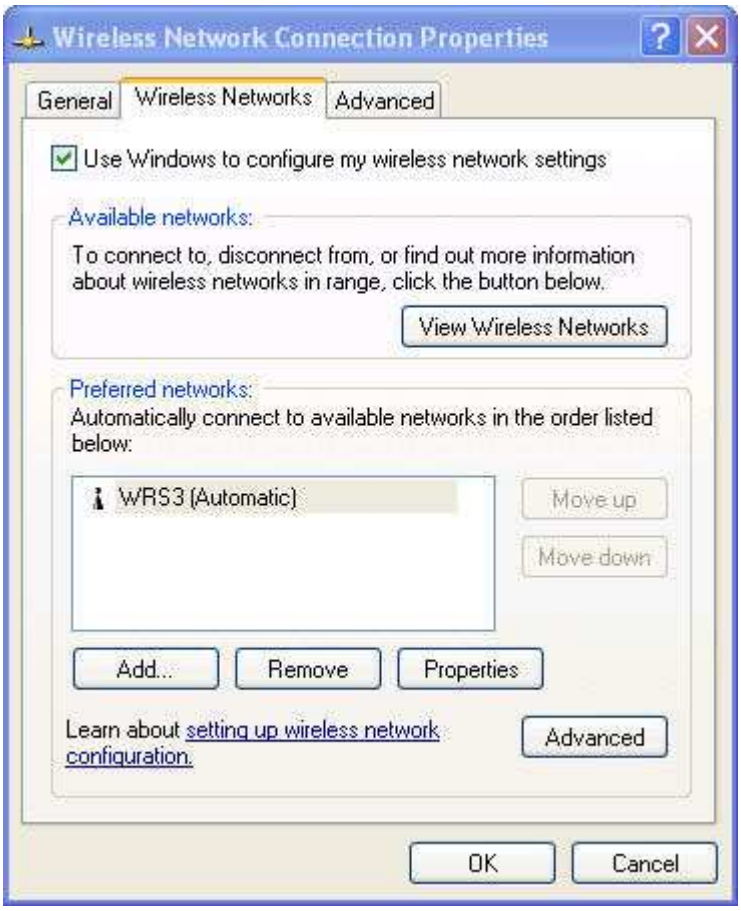
Now that WRS3 has been configured with WEP security, and PC6 is not configured with WEP, you will be disconnected from the network.

Step 6: Configure Windows to use WEP authentication.

Navigate to the Network Connections page again and right-click the **Wireless Network Connection** icon. In the Wireless Networks tab, locate the WRS3 network, and click **Properties**.

- Set Data Encryption to **WEP**.
- Uncheck This Key Is Provided For Me.
- Enter the network key of **1234567890**, as configured before on the router.
- Click **OK** and **OK**.

Windows should now reconnect to the network.



Task 9: Configure a Wireless MAC Filter

Step 1: Add a MAC filter.

- Navigate back to the web utility page of the router (http://172.17.30.1).
- Navigate to the Wireless page and then to the Wireless MAC Filter tab.
- Check Enabled.
- Select **Prevent PCs listed below from accessing the wireless network**.
- Enter the MAC address 00:05:4E:49:64:87.
- Click **Save Settings**.

This prevents any client with the MAC address 00:05:4E:49:64:87 from accessing the wireless network.

Step 2: Click Wireless Client List.

The **Wireless Client List** shows anyone currently connected to the router via a wireless connection. Also take note of the option **Save to MAC filter list**. Checking this option automatically adds the MAC address of that client to the list of MAC addresses to prevent or permit access to the wireless network.

What is an extremely robust way of only allowing clients of your choosing to connect to the wireless network?

_____

_____

_____

You could set the Access Restriction to Permit, which only allows MAC addresses listed in the table to connect wirelessly.

Why is this not feasible in large networks?

_____

_____

_____

You have to manually enter each MAC address.

What is a convenient way of adding MAC addresses if everyone to whom you wanted to allow access was already connected to the wireless network?

_____

_____

_____

You could simply go to the Wireless Client List and check Save to MAC filter list.

Task 10: Setting Access Restrictions

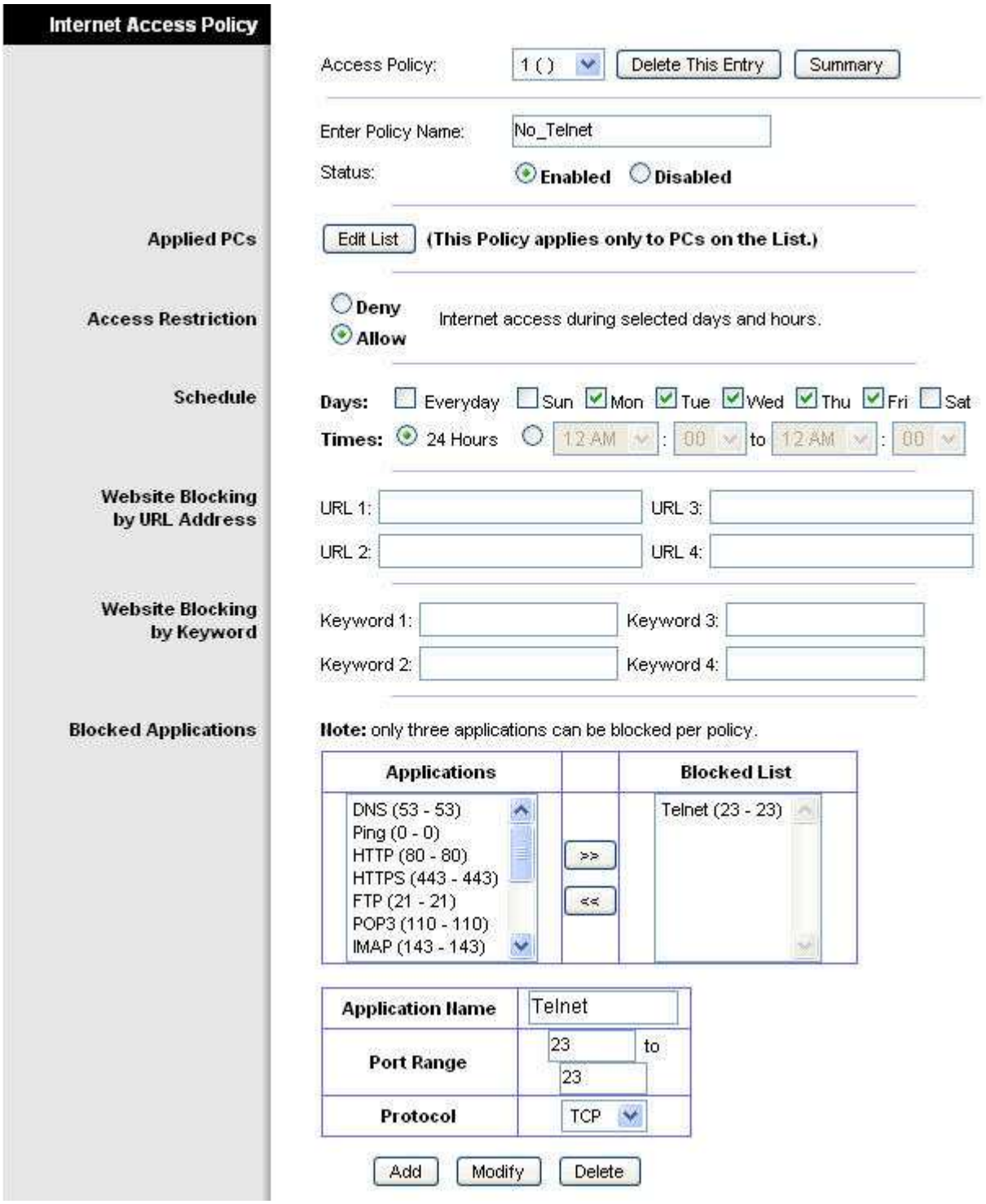
Configure an access restriction that prevents Telnet access Monday through Friday to users getting a DHCP address from the preset pool (172.17.30.50 – 74).

Step 1: Navigate to the Access Restrictions tab.

In the Access Restrictions tab, set the following:

- Policy Name – No_Telnet

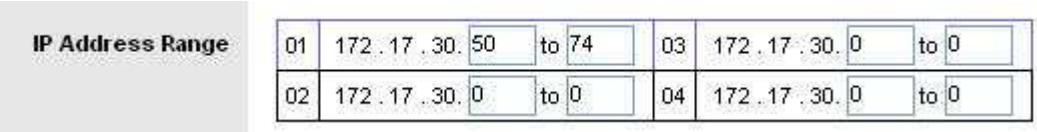
- Status – **Enabled**
- Access Restriction – **Allow**
- Schedule – Uncheck Everyday and recheck **Monday** through **Friday**
- Blocked Applications – Add **Telnet** to Blocked List



Step 2: Set the IP address range.

Apply this configuration to anyone that is using a default DHCP address in the range of 172.17.30.50 – 74.

Click the **Edit List** button at the top of the window and enter the IP address range. Save the settings.



Click the **Save Settings** button to save the access restriction settings. Click **Close** to close the window and continue with the next task.

Task 11: Managing and Securing the Web Utility of the Router

Step 1: Configure web access.

Navigate to the **Administration** section. Change the router password to **cisco**.

For **Web Utility Access**, select both HTTP and HTTPS. Selecting HTTPS access allows a network administrator to manage the router via https://172.17.30.1 with SSL, a more secure form of HTTP. If you choose to do this in the lab, you may have to accept certificates.

For **Web Utility Access via Wireless,** select **Enabled**. If you disabled this option, the Web Utility would not be available to clients connected wirelessly. Disabling access is another form of security, because it requires the user to be directly connected to the router before changing settings. However, in this lab scenario, you are configuring the router via wireless access, so disabling access would not be a good idea!

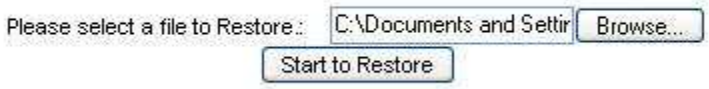
Click the **Save Settings** option at the bottom of the page. You may be prompted for the configured password. Enter **cisco** for the password and reconnect.

Now back up your configuration by clicking the **Backup Configurations** button. When prompted, save the file to your desktop.

Step 2: Restore your configuration.

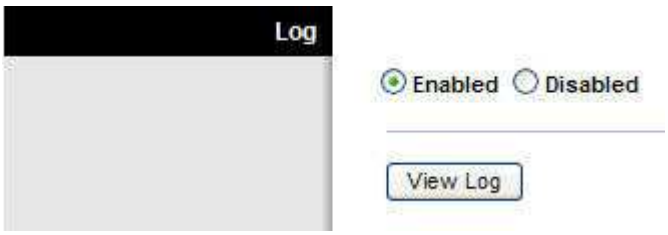
If your settings are accidentally or intentionally changed or erased, you can restore them from a working configuration using the **Restore Configurations** option located in the **Backup and Restore** section.

Click the **Restore Configuration** button now. In the Restore Configurations window, browse to the previously saved configuration file. Click the **Start to Restore** button. Your previous settings should be successfully restored.



Step 3: Enable logging.

Navigate to the **Log** tab of the **Administration** section and enable logging. You are now able to view the log of the router.

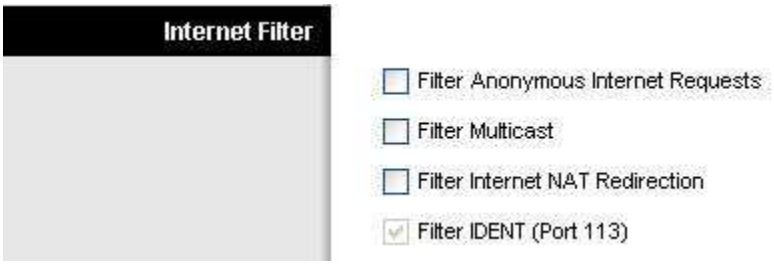


Step 4: Save your settings.

Task 12: Creating and Verifying Full Connectivity

Step 1: Filter anonymous Internet requests.

In the **Security** page, uncheck **Filter Anonymous Internet Requests**. Disabling this option allows you to ping the WRS3 internal LAN/wireless IP address, 172.17.30.1, from places connected to its WAN port. Don't forget to **Save** your settings.



Step 2: Disable NAT.

In the **Setup** page, click the **Advanced Routing** tab. Disable NAT. Don't forget to **Save** your settings.

Step 3: Connect to WRS2.

Now that WRS3 has been configured, it no longer broadcasts the default SSID of linksys. Power up the WRS2 wireless router and perform similar configurations. Review previous steps to connect PC3 to WRS2 via a wireless connection.

Set the IP address settings for Internet Setup.

- Set the Internet IP address to **172.17.88.25**.
- Set the Subnet Mask to **255.255.255.0**.

Set the Default Gateway to the FastEthernet 0/1 VLAN 88 IP address of R1, **172.17.88.1**.

Configure the Network Setup IP address to **172.17.40.1**.

Statically bind the MAC address of PC3 to the DHCP address **172.17.40.23**.

Change the wireless SSID to **WRS2**_[number].

Step 4: Configure R1 with static routes to the 172.17.30.0 and 172.17.40.0 networks.

```
R1(config)#ip route 172.17.30.0 255.255.255.0 172.17.88.35
R1(config)#ip route 172.17.40.0 255.255.255.0 172.17.88.25
```

Step 5: Repeat steps 1 and 2 above for WRS2.

Disable the Filter anonymous Internet requests.

Disable NAT.

Step 6: Verify connectivity.

Verify that R1 has routes to PC3 and PC6 and that it can successfully ping them.

```
R1#sh ip route
<output deleted>

Gateway of last resort is not set

     172.17.0.0/24 is subnetted, 5 subnets
S       172.17.40.0 [1/0] via 172.17.88.25
S       172.17.30.0 [1/0] via 172.17.88.35
C       172.17.20.0 is directly connected, FastEthernet0/1.20
C       172.17.10.0 is directly connected, FastEthernet0/1.10
C       172.17.88.0 is directly connected, FastEthernet0/1.88
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback0


R1#ping 172.17.30.26

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.30.26, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms


R1#ping 172.17.40.23

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.40.23, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Verify that PC3 and PC6 can ping the loopback of R1.

Verify that PC3 and PC6 can ping each other.

Verify that PC3 and PC6 can ping PC1 and PC2.

```
        IP Address. . . . . . . . . . . . : 172.17.30.26
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.17.30.1

C:\Documents and Settings\Administrator>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time=1ms TTL=254
Reply from 10.1.1.1: bytes=32 time=1ms TTL=254
Reply from 10.1.1.1: bytes=32 time=1ms TTL=254
Reply from 10.1.1.1: bytes=32 time=1ms TTL=254

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\Administrator>ping 172.17.40.23

Pinging 172.17.40.23 with 32 bytes of data:

Reply from 172.17.40.23: bytes=32 time=1ms TTL=126
Reply from 172.17.40.23: bytes=32 time=1ms TTL=126
Reply from 172.17.40.23: bytes=32 time=1ms TTL=126
Reply from 172.17.40.23: bytes=32 time=1ms TTL=126

Ping statistics for 172.17.40.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\Administrator>ping 172.17.10.21

Pinging 172.17.10.21 with 32 bytes of data:

Reply from 172.17.10.21: bytes=32 time=1ms TTL=126
Reply from 172.17.10.21: bytes=32 time<1ms TTL=126
Reply from 172.17.10.21: bytes=32 time<1ms TTL=126
Reply from 172.17.10.21: bytes=32 time<1ms TTL=126

Ping statistics for 172.17.10.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

From PC6

To R1's loopback

To PC3

To PC1

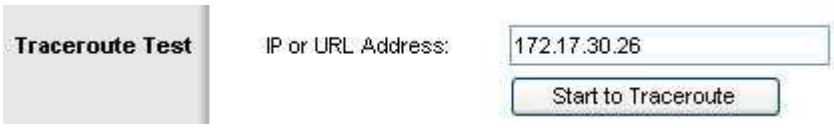
Task 13: Configuring Routing Efficiency

Step 1: Use Traceroute to view the network connection.

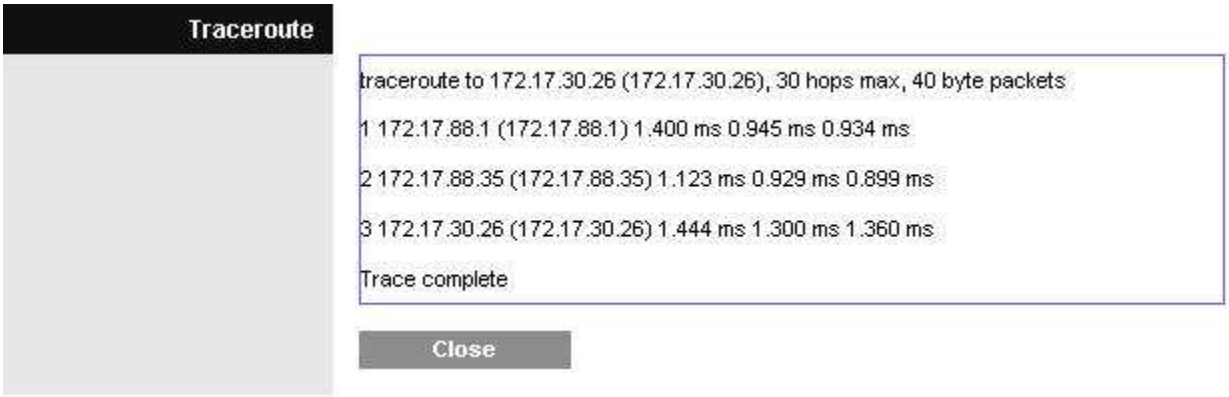
Because R1 is the default gateway, the Linksys router goes to R1 to get to a network it does not know how to get to, including the clients of the other Linksys routers.

A packet from PC3 to PC6 first reaches its default gateway of 172.17.40.1, then it is sent out the WRS2 WAN interface of 172.17.88.25 toward the WRS2 default gateway (172.17.88.1). From there, R1 send the packet to the WRS3 WAN interface, 172.17.88.35, where WRS3 handles it.

On WRS2, you can verify this in the **Diagnostics** tab in the Administration section. In the Traceroute Test field, enter the IP address of PC6, 172.17.30.26



Now click Start to Traceroute, a pop-up will appear.

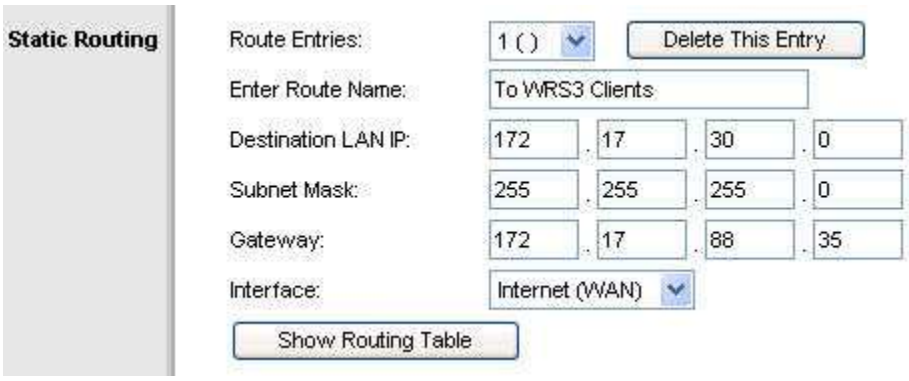


If WRS2 knew that it could get to the 172.17.30.0 network from 172.17.88.35 it would just directly send it to that IP address. So let's tell it!

Step 2: Configure a new route.

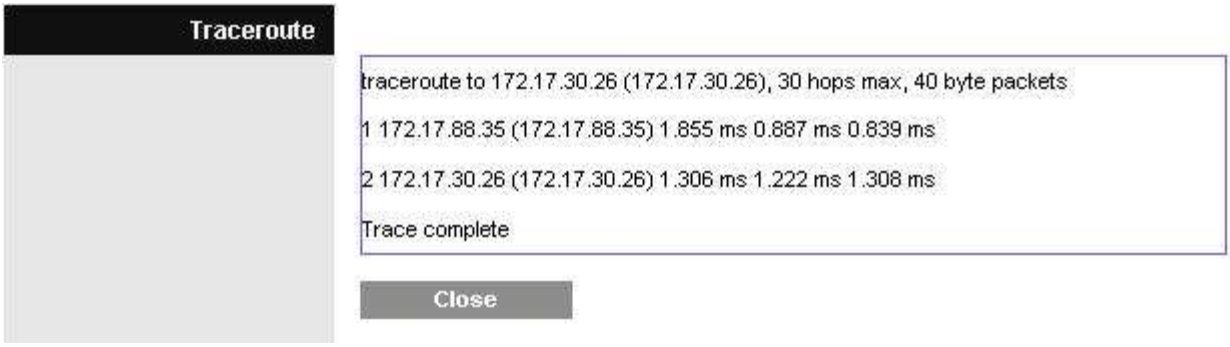
On WRS2, on the **Setup** page, click the **Advanced Routing** tab. For Static Routing, enter the following settings:

- In the **Route Name** field, enter **To WRS3 Clients**.
- For **Destination LAN IP**, enter the network behind WRS3: **172.17.30.0**.
- Enter a subnet mask of **255.255.255.0**.
- Enter a gateway of **172.17.88.35**.
- Set the interface to **Internet (WAN)**.
- Save your settings.



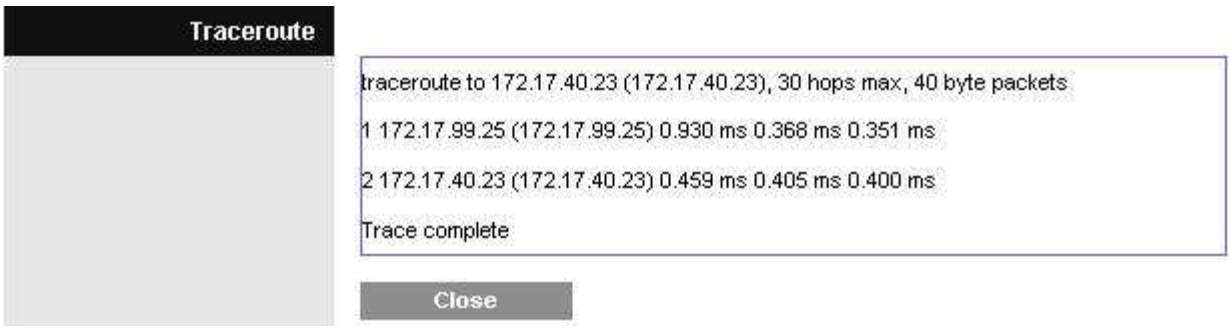
Step 3: Verify the new route.

In the **Diagnostics** tab in the Administration section, re-enter the IP address of PC3 in the Traceroute Test field. Click **Start to Traceroute** to see the route.



Notice WRS2 goes straight to WRS3 and saves us the extra hop to R1!

Do the same thing on WRS3 for the 172.17.40.0/24 network, pointing towards WRS2's WAN interface, 172.17.88.25.



Task 14: Configuring Port Security

Step 1: Configure PC1 port security.

Log on to switch S2. Configure the PC1 switch port, FastEthernet 0/11 with port security, and enable dynamic sticky MAC addresses.

Step 2: Configure PC2 port security.

Repeat for FastEthernet 0/18.

S2

```
!
interface FastEthernet 0/11
 switchport mode access
 switchport access vlan 10
 switchport port-security
 switchport port-security mac-address sticky
 no shutdown
!
interface FastEthernet 0/18
 switchport mode access
 switchport access vlan 20
 switchport port-security
 switchport port-security mac-address sticky
 no shutdown
```


Step 3: Generate traffic across the ports by pinging PC2 from PC1.

Step 4: Verify port security.

```
S2#show port-security address
          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                      Ports   Remaining Age
                                                              (mins)
----    -----------       ----                      -----   -------------
  10    0006.5b1e.33fa    SecureSticky              Fa0/11       -
  20    0001.4ac2.22ca    SecureSticky              Fa0/18       -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 6272

S2#show port-security interface FastEthernet 0/11
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0006.5b1e.33fa:10
Security Violation Count   : 0
```

Task 15: Restore WRT300N routers to factory defaults

Step 1: Clear settings of both WRT300N routers.

In order to clear both of the WRT300N routers to their factory defaults, navigate to the Administration page, click on **Factory Defaults,** and click the **Restore All Settings** button.

Final Configurations

R1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet0/1
 no shutdown
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1
 ip address 172.17.1.1 255.255.255.0
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 172.17.10.1 255.255.255.0
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 172.17.20.1 255.255.255.0
!
interface FastEthernet0/1.88
 encapsulation dot1Q 88
 ip address 172.17.88.1 255.255.255.0
!
!
ip route 172.17.30.0 255.255.255.0 172.17.88.35
ip route 172.17.40.0 255.255.255.0 172.17.88.25
!
line con 0
 exec-timeout 0 0
 logging synchronous
 password cisco
line aux 0
line vty 0 4
!
end
```

S1

```
hostname S1
!
vtp mode transparent
!
vlan 10,20,88
!
interface FastEthernet0/1
 switchport mode trunk
```



```
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport mode trunk
!
interface FastEthernet0/5
 switchport mode trunk
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```

S2

```
hostname S2
!
vtp mode transparent
!
vlan 10,20,88
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport mode trunk
!
interface FastEthernet0/7
 switchport mode access
 switchport access vlan 88
!
! PC1 and PC2's MAC address will appear after 'sticky' on ports 11
! and 18 respectively, after traffic traverses them
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky ffff.ffff.ffff
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
```

