

Purpose

- Examine typical configuration tasks for wireless access points.
- Implement DHCP in Cisco IOS.
- Work with a commercial integrated Access Point (AP) and NAT device.
- Capture and analyze 802.11 packets.

Before the Lab

- Read the description of DHCP and NAT commands in Cisco IOS.
- Complete the pre-lab.

Network port and addressing information

	Table 1	Table 2	Table 3	Table 4
Ethernet Interface on Buell	0/0	0/1	0/2	0/3
IPv4 Network on Buell	132.235.201.144 /29	132.235.201.176 /29	132.235.201.208 /29	132.235.201.240 /29
Buell IPv4 Address				
Netmask				
Linux IPv4 Address				
Ethernet Interface on Harley	0/0	0/1	0/2	0/3
IPv4 Network on Harley	132.235.201.128 /28	132.235.201.160 /28	132.235.201.192 /28	132.235.201.224 /28
Harley IPv4 Address				
Netmask				
DHCP Pool Name	dhcp1	dhcp2	dhcp3	dhcp4
Private Address Space	192.168.11.0/24	192.168.12.0/24	192.168.13.0/24	192.168.14.0/24
AP name	itl-ap-1	itl-ap-2	itl-ap-3	itl-ap-4
SSID	itl-ssid1	itl-ssid2	itl-ssid3	itl-ssid4
Radio Channel	1	5	8	11

Steps to Complete

1. Connect your Linux machine to your assigned Buell interface via a switch. Configure your interface on Buell, configure the Linux machine, and verify that it has internet connectivity. *You need to use the Linux machine for the next step to configure Harley.*

2. Connect the Student interface on the Windows machine to your Harley interface using a hub. **Disable the Admin interface.** Make sure the Student interface is set to receive both its address and name servers from DHCP.
3. Configure your interface on Harley. Install a route on Buell to send traffic to your subnet via the FDDI ring.

DHCP

4. Configure Harley to act as a DHCP server:
 - (a) In config mode, issue the command `ip dhcp excluded-address ...` (the last argument on the command line is the address of your interface on Harley).
 - (b) In config mode, type `ip dhcp pool pool-name` (where *pool-name* is the DHCP address pool name assigned to your table). This will put you into dhcp pool config mode. Enter the following dhcp pool commands:
 - `network net-number netmask` (fill in your assigned values from the resource table).
 - `default-router router-address` (fill in the address of your Harley interface).
 - `dns-server 132.235.64.1 132.235.64.2`
 - `lease 0 0 2` (set leases to 2 minutes)
 - `exit`
5. Verify that Windows receives DHCP information and has Internet connectivity.
6. Display and record the DHCP leases on Harley using the command `show ip dhcp binding`.

AP/Router *Note that all configuration on the AP will be done in the web browser. Once you change the settings on a screen, you have to click the Save Settings button, or the AP never sees your changes. (You will be rewarded with a “Changes Saved” screen for your troubles). For your lab report, use Alt-PrintScreen to make a copy of an image of a configuration screen you want to save, then paste the image into WordPad.*

7. Unplug your Student interface on Windows. Wire the Student interface directly to one of the LAN ports on the Linksys Router/AP at your table. Plug the AP in, and wait for Windows to get an IP address (in 192.168.1.0/24).
8. Browse from Windows to 192.168.1.1 – the configuration interface for the router. The default user name is blank, the default password is “*admin*”. Once you are connected, change the password to “*ouit!*”; you will need to log back in.
9. Change the private network the AP is using to the one assigned to your table, leaving the host address at “1”. You will need to get your Windows machine to renew its IP address (un-plug and re-connect the network cable) and connect your browser to the new address of the AP before you can continue.
10. Change the name, SSID, and radio channel of your AP to the values shown for your table on page 1.
11. Connect the WAN port of your AP to the hub that leads to your Harley interface. Confirm and record that the AP gets an address from your DHCP server.
12. Confirm that your Windows machine now has full Internet connectivity.

13. Save the output from `ipconfig` on Windows; capture the status and configuration screens from the AP, including the DHCP Client listing.

AirPCAP *For these steps you need the AirPCAP capture adapter for your Windows machine. If another table has that adapter in use, complete the steps labeled “NAT” and “Static NAT” first. If you had to connect the Mac to the network for one of these steps, use the Airport pull-down menu to turn the 802.11 interface off before you proceed with the AirPCAP steps.*

14. Connect the AirPCAP adapter to a USB port on the front of your Windows machine. Start Wireshark and select the AirPCAP interface in the capture dialog. Select to capture on your radio channel (click the “Wireless Settings” button to get to this dialog), and start the capture.
15. Use the Airport pull-down menu on the Mac to turn on the Airport (802.11) interface. If needed, connect to your wireless network by selecting it from the pull-down menu. Verify that the Mac can connect to the Internet by browsing to a web site (OU, Google, etc).
16. Stop and save the packet capture on Windows. Eject the AirPCAP adapter and return it to its central location for the next group.
17. Record the output of `ifconfig -a` on the Mac for your report. Record the IP address for your Mac on the network diagram, along with the MAC (Ethernet) address for the `en1` interface.
18. Recall the Wireshark capture file on Windows, and locate a Beacon frame for your network. Compare the information in this frame with the (default) wireless settings on the AP.
19. Locate the authentication and association packet exchanges related to the Mac joining the network. Locate an HTTP packet going to the Mac and examine the addresses contained in the 802.11 header.

NAT *Before you start the steps below, go to the Administration/Log panel in the AP, and turn logging on. Make sure to save your settings.*

20. Start Wireshark capture on the Student interface on Windows, and on Linux.
21. Ping from Windows to Linux. Compare the addressing information in the packets see leaving Windows and the ones arriving on Linux.
22. Use `ssh` to connect from Windows to Linux. Again examining the addressing information in a few packets as seen on Windows and Linux.
23. Capture the Outgoing Log information on the AP.

Static NAT *Note: if you had to skip the AirPCAP step, connect the Mac to the wireless network at this time. Turn the Airport interface off before you go back and complete the AirPCAP step.*

24. We want two types of access to work from the outside to our private network:
 - Web (port 80) connections to the web server on Windows.
 - SSH (port 22) connections to the Mac.
25. Configure your AP to implement the port forwarding arrangement above (look for the “Applications and Gaming” tab).

26. Test your setup by browsing from Linux to port 80 on the public address of your AP; then use ssh to connect to port 22. Run wireshark captures on all three machines to show the address translations.
27. Save the incoming log information from your AP.

Security

28. Start the “KisMac” program on the Mac, and review the list of wireless networks shown. Your own network should show up as not requiring encryption.
29. Browse from your Windows machine to the AP, and select “WPA2 Personal” as the security mechanism. Enter a WPA key of your choice.
30. Note that the display for your network in KisMac will have changed to reflect the new security setting. *Ethics sidebar: KisMac will also offer various methods of “cracking” the security of this network. Never do this on someone else’s network unless you have explicit permission.*
31. Exit KisMac (on 802.11 you can not connect and monitor at the same time). Re-connect your Mac noting that you will now have to supply your WPA shared key. **Do Not** store the key in the Mac’s “Keychain”.

Service Discovery *In these steps we will experiment with Service Discovery on Windows and the Mac. Both machines already run Apple’s Bonjour implementation.*

32. Let’s start by using the diagnostic application `dns-sd`, which is available on the Mac and on Windows. (You can use `man dns-sd` on the Mac to get help with running the command). Run Wireshark on Windows, then type the command `dns-sd -B _ssh._tcp local` which browses in the `.local` domain for the service type `_ssh._tcp`, which refers to SSH running over TCP. Record the output of `dns-sd`, and examine the packet capture to find out what queries were used to produce this output. `dns-sd` will continue to scan, so you will need “^C” to exit.
33. Repeat the last step, but this time browse for web services, `_http._tcp`.
34. Let’s see a more realistic example. Start Internet Explorer, and select the Bonjour icon on the far right of the tool-bar (click on the “>>” menu). You should see a web service advertised for the Mac. (Due to a software incompatibility IE won’t let you browse to this service).
35. Let’s try and advertise the main web page from the Mac. First, run the “Bonjour Browser” application on the Mac, and examine the web service advertisement.
36. In a command window on the Mac, create a service registration with the command `dns-sd -R <name> _http._tcp local 80`; you can pick any name you like for the service. This command will not exit; keep it running for now (you can stop advertising the service by exiting `dns-sd` with “^C”). The new service should show up in the Bonjour Browser, and in Internet Explorer. Confirm that you can select the new service in Internet Explorer and get the correct web page.
37. In a different command window on the Mac (leave `dns-sd` running in the first one), create another service registration with the command `dns-sd -R <name> _http._tcp local 80 path=/index-alt.html`; make sure you pick a different name for this service. Look for this additional service in the Bonjour Browser, and in Internet Explorer.

Confirm that you can select the additional service in Internet Explorer and get a different web page. Compare the two services in Bonjour Browser and note the difference in your lab report.

38. Service discovery does not have to use mDNS. Lets examine a variation using regular DNS. On the Mac, bring up the Network System Preference, select the AirPort interface, and click “Advanced”. Bring up the DNS tab and put the value `dns-sd.org` into the *Search Domain* field. The Bonjour Browser should now show an additional block of services (you may have to hit the “Reload Services” button).
39. Run Wireshark on the Mac, then use the command `dns-sd -L` to look up the contact information for one of the new services. Use `man dns-sd` to look up the syntax for this command variation.

iperf *Graduate Students:*

40. In the “Security” step above, KisMac saved a wireshark compatible packet dump file. Open this file in Wireshark and compare the Beacon frames before and after the point when your turned WPA on.
41. Run a 30 second iperf tcp performance measurement from the Mac to Windows (use default window sizes). You can use `iperf --help` to see a review of command line options.
42. Change the network type setting on the AP from the default to 802.11b only. Repeat the iperf test.
43. Run KisMac for a short time and examine its packet dump. What changed in the Beacon frame?

Lab Report Guidelines

Each report is to be written individually, although the data for the lab can be collected during the lab with your partner/group. They should be typed/word processed and brought to class in printed form.

Lab writeups are due **in class** on the Monday following the lab. They don't generally need to be more than a few (several) pages. Officially, they need to be "long enough to answer the questions". See the web page for detailed guidelines. Each lab writeup **must** have a header on the first page that includes:

- Your name
- The lab section that you attended
- Your affiliation (CS ugrad, CS grad, ITS ugrad, MCTP grad)
- Your lab partner's name
- Your lab partner's affiliation

Things you must include

- The patch panel worksheet
- The signed pre-lab.

Your report must answer these questions:

1. Show one example of the DHCP status information and explain the data shown.
2. Show the `ipconfig` output and the AP configuration and status after Windows is on-line.
3. In your AirPcap capture, isolate one beacon packet from your IP. In a full listing of the packet, show
 - That the beacon came from the MAC address (the BSSID) of your access point.
 - Highlight the SSID and the Access Point Name
 - Highlight three other pieces of information that the AP broadcasts in the beacon.
4. In the AirPCAP capture, isolate and show the association and authentication packets.
5. In your AirPcap capture, isolate a web traffic packet. In a fully expanded packet listing, highlight the source address, the destination address, and the address of the access point.
6. Show the AP (outgoing) log information captured during your NAT tests.
7. Isolate one ping packet in the Windows packet capture, then find the same packet in the Linux packet capture. Show and explain all changes (translations) that have occurred in the packet.
8. Repeat your analysis in the previous question for one ssh TCP packet.
9. Show the AP (incoming) log after your Static NAT tests.
10. Locate one HTTP TCP packet going to the Windows web server in your Linux packet capture. Find the same packet in the Windows capture and show/explain all translations.

11. Repeat the analysis above for one SSH TCP packet from Linux to the Mac.
12. Show the AP configuration with WPA2 filtering.
13. Show the output of `dns-sd -B` on windows, and show the packets that Windows used to collect the information displayed.
14. Show the first `dns-sd -R` command you issued on the Mac to advertise the main web server, and show all mDNS packets that enabled Windows to access this service.
15. Explain how the two web services you advertised from the Mac differed, using data from Bonjour Browser and your packet captures.
16. Show and explain all packets needed to connect to the wide area service you looked up on `dns-sd.org`.
17. *Graduate Student Questions:*
Show and explain your `iperf` results.
18. Highlight the differences found in the three beacons you captured: the original setting, the WPA2 configuration, and the 802.11b only setting.

