

Purpose

- Observe the operation of ARP
- Configure a DHCP server
- Use a router as a DHCP relay agent
- Examine DNS queries

Before the Lab

- Read the man pages for `dhcpcd` and `dhcpcd.conf` (they are on the web site).
- Complete the pre-lab, and get it signed when you come to lab.

Steps to Complete

1. Before you get started, copy the information for your table from the pre-lab to the network diagram. We have brought up the FDDI ring, and given Harley and Davidson default routes pointing via the ring to Buell.
2. Wire your Linux machine to your assigned interface on Harley, using a hub.
3. Using your Windows machine, configure the interface on Harley. (If you start a command window from Start/Run, use “cmd”, not the older 16-bit version called “command”).
4. Install a route on Buell pointing to your subnet on Harley via the FDDI ring.
5. Configure your Linux machine and confirm connectivity to the Internet.
6. Create and edit a `dhcpcd.conf` file in your `itladmin` home directory. At this time, add only the minimum information required to get DHCP working – you have to add at least the range of addresses and the network mask.
7. Delete the DHCP leases file (`sudo rm -f /var/lib/dhcp3/dhcpcd.leases` will do that), then create an empty file with `sudo touch /var/lib/dhcp3/dhcpcd.leases`. Follow this with `sudo chmod g+w /var/lib/dhcp3/dhcpcd.leases`.
8. Put your configuration file into the correct place, using `sudo cp dhcpcd.conf /etc/dhcp3/`. *You have to do this every time you make changes to your local file.*
9. Open a new terminal and start the DHCP server, using `sudo dhcpcd3 -f -d` (`-f` runs the server in the foreground so you can see the output, and `-d` makes sure messages appear in the command window). If the server finds problems in your configuration file, it will report them and exit. Otherwise, the server tells you which interfaces it will listen on and waits for client requests. The server will also print diagnostic messages in this command window, so save the content of the window periodically for your lab report. *When you decide to change your configuration, stop the server with “^C”, then edit your file, copy it to /etc/dhcp3, and start the server again.* Make sure you really stopped the server with “^C”; if two `dhcpcd` servers are running, results will be very unpredictable. If you think you have gotten into this situation, check with a lab instructor.
10. Start a file capture (Wireshark) on the Linux machine. In all packet captures for this lab, make sure to un-check **all** name resolution options, including “MAC Name Resolution”.

11. Configure your Mac OS machine for DHCP, and wire the Mac to the hub leading to your interface on Harley. As the Mac acquires its IP address, you should see the DHCP protocol steps in your packet capture. If you need to start the process over, set the Mac to manual addressing (the actual address does not matter) and click Apply. Then change back to DHCP and click Apply again. Or, use the “Advanced” button, and click the “Renew DHCP Lease” button in the advanced options panel.
12. Click the “Renew DHCP Lease” button and observe the DHCP packets that result. *Make sure to save the packets captures for this and the previous step.*
13. At this point try and use the Wireshark filtering option to make your packet capture easier to read. Start by clicking the +Expression button in the filter bar just above the packet list. Figure out how to have Wireshark display only UDP packets. Ask a lab instructor for assistance if needed. Note the actual syntax of the filter expression displayed in the filter bar. You can type this directly once you get a feel for the syntax.
14. Edit your dhcpd.conf file (remember to stop the server) to include more complete information. Add at least the router address, name servers, and set a short lease time (e.g. 2 minutes). Install the file and start your server.
15. Start a packet capture on Linux, then force the Mac to renew its lease. Observe the DHCP packets that result. Make sure the Mac can resolve names and reach the Internet. Display the routing table on the Mac to see what default route was installed. Save the routing table and the packet capture.
16. Look up the syntax for the ipconfig getpacket command on the Mac (use man ipconfig). Use this command to display and save the content of the last DHCP packet the Mac received.
17. On both the Mac and the Linux machine, clear the ARP cache with sudo arp -d. You delete a single entry by specifying the IP address of the arp entry you are trying to clear out; on the Mac you clear the table with sudo arp -d -a. Start a packet capture on the Mac (either display all packets or filter on ARP), then ping the Linux machine. While the ping is running, clear the arp cache again to force a new arp discovery. Display the arp cache and look at the packet capture to examine the ARP exchange. Use ifconfig on Linux to confirm that the Mac got the correct MAC address.
18. Clear the ARP cache again on the Mac, and (while still capturing packets) ping 132.235.64.1. Look at the ARP cache and the packet capture to see what ARP packets were exchanged.
19. Wire from your Davidson interface to a switch, *leave the Windows Student interface disconnected for now.*
20. Configure your router interface on Davidson, and install a route on Buell to send traffic for your Windows subnet to Davidson.
21. Install an ip helper command on your router interface on Davidson, pointing to your DHCP server (the Linux machine).
22. Stop your DHCP server, and add a section in your dhcpd.conf file for the Windows subnet. Install the dhcpd.conf file and restart your server.

23. Disable the “Admin” interface on Windows and make sure that the “Student” interface is configured for DHCP; select the option to get DNS servers automatically. Enable the “Student” interface.
24. Start packet captures on both the Linux and the Windows machines, then wire the Windows machine to the switch you earlier connected to Davidson. Make sure your Windows machine acquires an address and can reach the Internet. Save both packet capture. You can use `ipconfig /release` followed by `ipconfig /renew` to force Windows to start the DHCP process over.
25. Start a packet capture on Linux and run it long enough to see both Windows and Mac OS renewing their licenses once. Save this packet capture.
26. Start a packet capture on the Mac, and leave this capture running for the DNS-related steps following below.
27. Use the `dig` command to look up `www.ohiou.edu`, `www.osu.edu`, and `www.microsoft.com` and interpret what you see.
28. Use `dig` with the `+trace` option to resolve `www.itl.ohiou.edu`, and interpret the output.
29. Use `dig` to look records of type “NS” under `cs.ohiou.edu`.
30. Use `dig` to look records of type “SOA” under `cs.ohiou.edu`.
31. Use `dig` to look records of type “NS” under the root domain “.”.
32. Use `dig` to map the address `132.235.64.1` to its name (a “reverse” lookup).
33. Use `dig` to get MX records for `ohio.edu` and `osu.edu`, and interpret the output.
34. Make sure to save your packet capture.
35. *Graduate Students Only:* Install support for netbios name servers into the `dhcpd.conf` file, for the Windows subnet only. Use `132.235.197.38` as the netbios name server address. While capturing packets (Linux may be the most convenient place), force lease renewals on the Mac and the Windows machine. Use `ipconfig` on windows to see if the new option was installed. Use `ipconfig getpacket` on the Mac to see what was delivered to the Mac. Save the packet capture.

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 the content of your final `dhcpd.conf` file.
2. Show the packets that make up one full DHCP acquisition cycle from the Mac, starting with the DHCPDISCOVER (use the one with the complete configuration file).
 - (a) In each packet, circle the data that determines the DHCP type of the packet.
 - (b) In the DHCPACK packet, show the location in the packet that provide the IP address, the network mask, and the router address to the Mac.
 - (c) Show the output from `dhcpd` and `ipconfig getpacket` that corresponds to the DHCP cycle above and explain how the data in these two listings match up with the packet content.
3. Show the arp table on the Mac after you pinged the 132.235.64.1 address. Show the packet capture that shows how that arp entry was obtained. Compare the arp table with one outgoing ping packet; which hardware address is the ping packet being sent to. Can you tell what the hardware address of 132.235.64.1 is?
4. For a full DHCP acquisition from Windows (starting with DHCPDISCOVER), show the relevant packets captured on Windows and on Linux. Compare each packet and comment on what changes the relay makes in each packet. Show the ipconfig output from Windows.
5. Show the output from the dig commands for `www.ohiou.edu`, `www.osu.edu`, and `www.microsoft.com`. Explain what you see in the output; what is different for the output from Microsoft? For **one** of these queries, show the actual DNS request and reply packets.
6. Explain the output of the dig command with the `+trace` option. Show all DNS request packets that were created by this lookup.

7. Explain the output of the dig queries for NS records (cs.ohiou.edu and root domains).
8. Match the output of the cs.ohiou.edu SOA record to the example discussed in class.
9. Show both the dig output and the DNS query packets for the dig reverse and MX lookups.
10. *Graduate Student Question:* Show the `dhcpd.conf` file with the netbios name server option added. Show the ipconfig outputs from both Windows and the Mac. Use the DHCPREQUEST and DHCPACK packets (for both Windows and Mac) to show which machines requested the option, and how the server replied.

Pre-Lab

Fill in the required information below. When you determine a DHCP address range, use the lower half of the usable addresses. Assign the Linux machine the address just below the router.

	Table 1	Table 2	Table 3	Table 4
Harley	Ethernet 0/0	Ethernet 0/1	Ethernet 0/2	Ethernet 0/3
Davidson	Ethernet 0/0	Ethernet 0/1	Ethernet 0/2	Ethernet 0/3
Harley subnet	132.235.201.152/29	132.235.201.184/29	132.235.201.216/29	132.235.201.248/29
Davidson subnet	132.235.201.160/29	132.235.201.192/29	132.235.201.224/29	132.235.201.240/29
Harley IP				
Davidson IP				
Linux IP				
Harley DHCP range				
Davidson DHCP range				

On the next page, draft what you think should be in the dhcpd.conf file. Start with the example in the dhcpd man page and adapt it for your case. Where addresses are needed, indicate the correct values for all four tables.

Graduate Students: Review the man page (it is on the web site) for dhcp-options. In your draft configurations, include the option to send netbios name server addresses.

DHCP configuration for the Harley subnet

DHCP configuration for the Davidson subnet

