# Computer Networks

|  |  |  |
| --- | --- | --- |
|  | Assignment 4 Network Tools |  |

**MAC or Physical Address**. Each network interface card has a unique 48-bit MAC (physical) address that is used for forwarding data frames in a local area network. It is often written as 12 hexadecimal digits, with hyphen or colon after each group of two digits for readability.

1. Write the MAC address B0-83-FE-6A-47-FF in binary.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| B0 | 83 | FE | 6A | 47 | FF |
| 10110000 | 10000011 | 11111110 | 01101010 | 01000111 | 11111111 |

MAC addresses are often assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. A MAC address usually encodes the manufacturer's registered identification number in the first 24 bits (six hexadecimal digits). It does not mean that MAC addresses cannot be changed (spoofed) in software.

1. Access the site <http://www.macvendorlookup.com/>, enter the MAC address above and determine the vendor of the network interface card.

­­­­­­­­­­­Dell

**Telephone Number**. Consider someone outside the country trying to call my office. They have to dial a sequence of digits: 1, which is the country code for USA; 585, the area code for Rochester and neighborhood; 395, which is the local end office (exchange) code; and then 5181. It is customary to write a telephone number with hyphens separating the various parts for readability, i.e., write as 1-585-395-5181. Addresses used on the Internet also exhibit such hierarchical structure.

**Internet Address**. Each interface that is used to connect a device to the Internet must be assigned a unique IP address that is used for routing of packets. (For now ignore Internet sharing with NAT devices.) In IPv4, the IP address is 32 bits long. Each byte of 8 bits (octet in Internet terminology) is written in decimal, with dots placed in between for readability. For example, the PC on which I am working has the IP address 137.21.102.206. In IPv6, the IP address is 128 bits long and is written in hexadecimal notation.

1. Write the IPv4 address 137.21.102.206 in binary.

|  |  |  |  |
| --- | --- | --- | --- |
| 137 | 21 | 102 | 206 |
| 10001001 | 00010101 | 01100110 | 11001110 |

Note:

1. It is possible to have a device with two or more interfaces that connect to the Internet. Thus, it is possible for a device to have two or more Internet addresses.

Yes it is possible

1. All IP addresses on the Brockport network will start with 137.21. This is similar to saying that all land-line phone numbers in the Brockport village will start with 585, the area code.

Complete the following steps by typing appropriate commands in a **Command Prompt Window** of any PC in campus computer room, study the response carefully, determine the required information and complete the report. Alternatively, you may use your own machine remotely for the lab.

Identity of the machine: Laptop (Thinkpad T14), my couch

(**Room# and machine #, or your own machine and the place where you conducted the lab**)

1. Type the command **ipconfig /all** and report the following:

MAC address: A0-29-42-5B-F9-5A

IP address: 192.168.1.14

Subnet mask: 255.255.255.0

Default Gateway: 192.168.1.1

DHCP Server: 192.168.1.1

DNS Server(s):

2603:7080:1803:1e3::1

192.168.1.1

Lease Obtained: Sunday, April 30, 2023 11:17:50 PM

Lease Expires: Monday, May 1, 2023 11:17:50 AM

Note: This machine has been assigned an IP address on boot up using the dynamic host configuration protocol (DHCP). The lease refers to when the address was assigned and when it expires. It is possible to make a static assignment of IP address, so that the address does not change from time to time. A Windows-based computer that is configured to use DHCP can automatically assign itself an IP address (in the range 169.254.0.0-169.254.255.255) if a DHCP server is not available, but cannot really communicate with other devices on the Internet.

Which kind of devices should have static IP address – clients or servers?

Servers should be static because they should be consistent. If a server’s IP changes then clients won’t be able to access them.

Clients can use DHCP and get auto assigned an IP address upon connecting to a server

The above output shows several IP addresses. List those that you believe are static.

Subnet mask: 255.255.255.0

Default Gateway: 192.168.1.1

DHCP Server: 192.168.1.1

Does dynamic assignment of phone numbers make sense? Justify your remark.

No because a phone number should not change otherwise you’d have a hard time keeping in contact with others if your number keeps changing.

1. Type the command **ipconfig /release t**hen **ipconfig /all** and report the following:

IP address: 169.254.220.8

Subnet mask: 255.255.0.0

Default Gateway: fe80::5a2f:f7ff:fe60:70ea%3

Try to use Chrome, Firefox, or Edge to access the Internet. Did you succeed? State the problem, if any, and the reason.

­­­­­­­­­­Yes there was no issues

Type the command **ipconfig /renew** then **ipconfig /all** and report the following:

IP address: 192.168.1.14

Subnet mask: 255.255.255.0

Default Gateway: fe80::5a2f:f7ff:fe60:70ea%3

192.168.1.1

Try to use Chrome, Firefox, or Edge to access the Internet. Did you succeed? State the problem, if any, and the reason.

­­­­­­­­­­­­Yes there was no issues

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Has the IP address or the lease date/time changed?

The IP address changed but I think the lease and date remain the same

1. Access the site http://www.macvendorlookup.com/ and determine the vendor of the network interface card for the machine, using the MAC address determined in Step 4.

­­­­­­­­­­­­ No Vendor Exists

Idk if this is intentional or not?

7. Access http://www.educause.edu/edudomain and select **Whois Lookup** Search for **Brockport.edu** domain and determine externally registered domain name server for the Brockport campus. Also determine the date on which Brockport.edu domain was activated.

Domain name servers for Brockport.edu:

NS5.SUNY.EDU

NS6.SUNY.EDU

NS4.SUNY.EDU

NS3.SUNY.EDU

NS2.SUNY.EDU

NS.SUNY.EDU

Date on which Brockport.edu domain was activated:

Domain record activated: 09-Jan-1990

Date on which Brockport.edu domain record was last updated:

Domain record last updated: 25-Mar-2023

Date on which the domain expires (unless renewed)

Domain expires: 31-Jul-2023

Domain name servers contains records of several types. They are used for translating domain names to IP address or vice versa, mail exchange, determining canonical name, etc. Domain name servers provide crucial services and hence it makes sense that some of the Brockport domain name servers are **not** on Brockport network.

1. Determine the IP address of the UNIX/Linux machine courses.brockport.edu used in CSC 209 class by typing the command: **nslookup courses.brockport.edu**

Note that the output first identifies the domain name server providing the response. After that the result is presented. A non-authoritative answer indicates that the response is from the information cached by the server.

Domain name and IP address of server responding:

Server: 2603-7080-1803-01e3-0000-0000-0000-0001.res6.spectrum.com

Address: 2603:7080:1803:1e3::1

Name: courses.brockport.edu.lan

Address: 192.168.1.1

Domain name and IP address of **courses**:

Name: courses.brockport.edu.lan

Address: 192.168.1.1

1. Of those name servers identified in Step 7, some servers show only domain names (i.e., no IP address is seen). Determine the IP addresses of those three domain name servers.

IP address of NS5.DNSMADEEASY.COM: 192.168.1.1

IP address of NS6.DNSMADEEASY.COM: 192.168.1.1

IP address of NS7.DNSMADEEASY.COM: 192.168.1.1

1. The output of Step 4 showed several domain name servers. The EDUCAUSE site shows several servers. Which ones are missing in which list?

Which domain name server(s) is/are missing in the Output of Step 4?

NS5.SUNY.EDU

NS6.SUNY.EDU

NS4.SUNY.EDU

NS3.SUNY.EDU

NS2.SUNY.EDU

NS.SUNY.EDU

Which domain name server(s) is/are missing in the EDUCAUSE site?

2603:7080:1803:1e3::1

192.168.1.1

In total then, how many domain name servers have we identified? 8

1. Of those domain name servers identified, some are not on the Brockport network as can be seen from their IP addresses. (All IP addresses on the Brockport network will start with 137.21.) List them.

2603:7080:1803:1e3::1

192.168.1.1

Since I did this on my own laptop?

1. Find the IP address of the campus web server: **www.brockport.edu**

IP address of [www.brockport.edu](http://www.brockport.edu):

tracert www.brockport.edu

Tracing route to www.brockport.edu [146.20.54.132]

Is that machine on Brockport network? No

Wouldn’t it need to start with 137.21

Note that it is possible for the machine to be physically on Brockport campus but not on Brockport network. Look up “virtual private network”. Oh

The computer network diagnostic utility **ping** is used to test the reachability of a [host](https://en.wikipedia.org/wiki/Host_(network)) on an [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP) network and to measure the [round-trip time](https://en.wikipedia.org/wiki/Round-trip_time) for messages sent from the originating host to a destination computer and back. But it is possible to configure many devices, including routers, to ignore a ping request. Look up “ping of death”.

1. Try **ping www.albany.edu** and report your findings.

IP address of www.albany.edu:

[www.albany.edu.cdn.cloudflare.net](http://www.albany.edu.cdn.cloudflare.net)

104.18.6.212

2606:4700::6812:7d4

TTL set on ICMP packets:

Reply from 2606:4700::6812:7d4: time=38ms

Reply from 2606:4700::6812:7d4: time=40ms

Reply from 2606:4700::6812:7d4: time=30ms

Reply from 2606:4700::6812:7d4: time=54ms

Round trip times (in ms): Minimum = 30ms, Maximum = 54ms, Average = 40ms

1. Several years ago, the Department of Computing Sciences had a print server in Grace Laboratory. But it has since been discarded.

Try **nslookup 137.21.102.140** and report your findings.

Server: 2603-7080-1803-01e3-0000-0000-0000-0001.res6.spectrum.com

Address: 2603:7080:1803:1e3::1

Name: print1.cs.brockport.edu

Address: 137.21.102.140

Then, try **ping 137.21.102.140** and report your findings.

Pinging 137.21.102.140 with 32 bytes of data:

Request timed out.

 The computer network diagnostic utility **traceroute** (**tracert** in Windows systems) is used for displaying the route (path) and measuring transit delays of [packets](https://en.wikipedia.org/wiki/Network_packet) across an [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP) network. The output will list routers encountered at each hop with delay times. Again, some routers may not cooperate. There may be incomplete lines shown with “**\***”.

1. Try **tracert en.wikipedia.org** and report your findings.

IP addresses of en.wikipedia.org: Tracing route to dyna.wikimedia.org [2620:0:861:ed1a::1]

Number of hops: 12

The **arp** command is used to determine the MAC address of a device with a known IP address. The command with option **–a** displays all entries in the PC’s **arp** table (cache). The dynamically learned addresses are differentiated from the statically configured addresses (by the user or the OS) in the type column.

1. Type the command **arp –a** and determine the MAC address of your subnet’s default gateway router, determined in Step 4.

IP address of your subnet’s default gateway: ­­­­­­­­­­­­­­­­­­­ 192.168.1.1

MAC address of your subnet’s default gateway: 58-2f-f7-60-70-ea

1. Use Wikipedia, search ARP Cache Poisoning, and write two sentences describing what it means.

Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network

An ARP spoofing, also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices.

In Step 8, we determined the IP address of courses.brockport.edu as 137.21.7.64. But when you use PuTTY to login on courses, you actually reach courses.brockport.edu with the IP address 137.21.7.65. This is because, courses.brockport.edu is only a load balancer that forwards the traffic to courses. But before it does so, it does some network address translation. Specifically, it changes the client IP address to 137.21.7.1. We will explore network address translation later.

A host such as courses.brockport.edu runs several applications. To establish a TCP/IP connection, we need to know not only the IP address of courses but also the **port number** associated with a specific application. For example, web service is often offered on port 80. Secure shell service is offered on port 22. Other applications have well-defined port numbers.

1. Close all network connections, all browser windows, email, etc. Use Chrome, Firefox, or Edge and connect to the following URL and study the response provided by the link. https://www.showmyipaddress.eu/

Your IP address: 67.240.197.240

1. Open **PuTTY** software and login on to **courses.brockport.edu**

Stay connected. Then, in the Windows command window (on your PC, rather than PuTTY SSH terminal) type the command: ***netstat –n***

Scan the output for an established connection to Courses. That is, the foreign address should correspond to the IP address of Courses, determined in the last step. The port number (22) on which you are connected is indicated after the colon.

Hint: (1) use ***w*** command. (2) use ***egrep*** command. (3) use ***netstat*** vs. ***netstat –n***.

As reported by your PC (on your PC)

Local IP address and port number: 127.0.0.1

Foreign (courses) IP address and port number: 49676

1. On PuTTY SSH terminal, execute the same command on the server courses and verify that the same information is reported by courses, with local and foreign addresses reversed.

As reported by **courses** (on the server)

Local IP address and port number: 137.21.7.65 33030

Foreign (PC) IP address and port number: 54.67.92.206 443

1. On your local computer (Windows), what is the command used to show the routing table on your computer?

Your answer:

route print

1. From the IPv4 Route Table, please find the row starting with Network Destination 0.0.0.0 that is the default routing for your computer, that is, if your computer cannot find the route, it will turn the IP packet to the gateway.

What is your finding (one row only)?

Your answer:

IPv4 Route Table

=====================================================================

Active Routes:

Network Destination Netmask Gateway Interface Metric

0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.14 35

127.0.0.0 255.0.0.0 On-link 127.0.0.1 331

127.0.0.1 255.255.255.255 On-link 127.0.0.1 331

127.255.255.255 255.255.255.255 On-link 127.0.0.1 331

192.168.1.0 255.255.255.0 On-link 192.168.1.14 291

192.168.1.14 255.255.255.255 On-link 192.168.1.14 291

192.168.1.255 255.255.255.255 On-link 192.168.1.14 291

192.168.56.0 255.255.255.0 On-link 192.168.56.1 281

192.168.56.1 255.255.255.255 On-link 192.168.56.1 281

192.168.56.255 255.255.255.255 On-link 192.168.56.1 281

224.0.0.0 240.0.0.0 On-link 127.0.0.1 331

224.0.0.0 240.0.0.0 On-link 192.168.56.1 281

224.0.0.0 240.0.0.0 On-link 192.168.1.14 291

255.255.255.255 255.255.255.255 On-link 127.0.0.1 331

255.255.255.255 255.255.255.255 On-link 192.168.56.1 281

255.255.255.255 255.255.255.255 On-link 192.168.1.14 291

=====================================================================

1. Please indicate what the corresponding gateway for the destination network 0.0.0.0 is.

Your answer: 192.168.1.1

1. Use ipconfig /all to find your Default Gateway.

Your answer: 192.168.1.1

1. Do they match each other?

Your answer: Yes

1. Please indicate what the corresponding interface for the destination network 0.0.0.0 is in the route table.

Your answer: 192.168.1.14

1. The corresponding interface seems an IP address. What is this IP address for?

Your answer: This current devices (my laptops) IP address.