

IPv4 Addressing and Routing

Learning Outcomes

After completing these activities you should be able to:

Addressing:

- Describe what layer of the OSI model, and TCP/IP stack IPv4 is associated with
- Describe *classful* subnetting scheme in IPv4
- Describe *Classless Inter-Domain Routing* (CIDR) subnetting scheme in IPv4
- Describe the use of the following and represent IPv4 addresses in the following notations: dotted-quad, CIDR
- Describe the purpose of, and use of a subnet mask
- Explain the *prefix* and *local* portion of an IPv4 address
- Calculate a prefix and local portion of an IPv4 address using a subnet mask
- Describe the purpose of *Dynamic Host Configuration Protocol* (DHCP)
- Describe and depict the lease request and renewal processes of DHCP

Routing:

- Describe what a *router* is, and its role in networking
- Describe what a *hop* is in information system networking
- Describe how a router uses and modifies the fields of a packet
- Derive network architecture by analyzing protocols in execution: IPv4

Outside of Class

In preparation for and reinforcement of in class activities, complete the following activities:

- Print and bring the assignment to class for in class work
- Review the below information and documents
- Complete the activities included in *In Class*

Documents

Document	Version		Due Date
	Student	Post/Solution	
Assignment	student	solution	24 Oct 2019

- Read (*Kulrose & Ross*)
 - Chapter 4 Introduction (~1 page)
 - Section 4.1 *Overview of Network Layer* (~8.5 pages)
 - Section 4.2 *What's Inside a Router?* (~3 pages)
 - Section 4.2.1 *Input Port Processing and Destination-Based Forwarding* (~2.5 pages)
 - Section 4.3 *The Internet Protocol (IP): IPv4, Addressing, IPv6, and More* (~1 page)

- Section 4.3.1 *IPv4 Datagram Format* (~2 pages)
- Section 4.3.2 *IPv4 Datagram Fragmentation* (~2 pages)
- Section 4.3.3 *IPv4 Addressing* (~10.5 pages)

In Class

Assignment

Important: Do not setup up your PiCK yet!

In this assignment we will explore various aspects of the Network layer and some of the core protocols that hosts use at the Network layer. We will capture packets and collect data for analysis from both the network lab machine and your PiCK. You will perform data analysis after you have captured and collected from both the network lab machine and your PiCK. We'll start with capturing and collecting from the network lab machine, and then capture and collect from your PiCK.

Internet Protocol v4 Introduction

Recall that the main purpose of the Network layer is to connect hosts on different local area networks; i.e. host-to-host communication (*Kurose & Ross*, pg. 305). Just like other protocols, the Network layer needs to identify who is communicating (source and destination). The Network layer also performs routing, that is the Network layer determines how to get a packet from Alice to Bob through the interconnected Data Link layer, local area, networks.

The Internet is the largest publicly available set of interconnected networks; the Internet is not the World Wide Web (www, web), the World Wide Web runs on top of the Internet. There are many other

note: The first rule of the Internet is you do not talk about IPv5. The second rule of the Internet is you do *not* talk about IPv5.

Application layer services that run on top of the Internet just like the web does. The Internet takes its name from the Network layer Internet Protocols: IPv4, ICMP. IPv6 and ICMPv6 are additional Network layer Internet Protocols that were designed to replace IPv4 and ICMP respectively. IPv6 and IPv4 provide the same high level service of connecting hosts on different networks, but there are differences in how the protocols provide that service. We will focus on IPv4 in these activities; we will discuss IPv6 later in the course.

Capture & Collect: Network Lab Machine

Activity: Subnetter

Complete this activity from a lab machine in the *Networking Lab*, not from your PiCK

1. Redirect the output of `ifconfig` for only the lab machine's Ethernet adapter to a file named `labMach-ifconfig-<YOUR_LASTNAME>.txt`
2. Ping a neighbor's lab machine; no need to save output from `ping`
3. Redirect the output of `arp` for only the lab machine's Ethernet adapter showing IPv4 addresses (not host names) to a file named `labMach-arp-<YOUR_LASTNAME>.txt`
4. Redirect the output of `dig` when resolving the IP address of `midn.cyber.usna.edu` to a file named `labMach-dns-midnCyber-<YOUR_LASTNAME>.txt`

Activity: I'm this IP Address?

1. Open Wireshark
2. Start capturing traffic on the network lab machine's Ethernet interface

3. Open a new browser tab and go to: `https://www.myip.com/`

Remote Port is what My IP sees your Transport layer port as.

4. Complete Question 1 on the assignment; reload the web page for each trial

5. Stop capturing traffic

6. Save the captured packets to a file named `labMach-NAT-evidence-<YOUR_LASTNAME>.pcapng`

Activity: Upload Data - Lab Machine

1. Ensure your files are named according to the directions in the lab; i.e. includes your name at the end of the file name

2. Logon to your USNA account in a web browser

3. Upload your files to the associated directory in the SY205 Student Collaboration Space

a. Navigate to the sub-directory for this specific lab, `ip4AddressingRouting`

b. Click the + *New* button

c. Select *File Upload*

d. Navigate to and select the files to upload

e. Click the *Open* button

f. Observe files uploaded to SY205 Student Collaboration Space

Intermission

The remainder of the capture and collect activities will be done using the PiCK. Logout of the lab machine, and pull up this lab page on your laptop; Windows is fine, no need to be in your VM. Setup your

Activity: PiCK Up Game

1. Pull up the notes for the day in using your laptop

2. Disconnect the workstation peripherals:

- DVI-D Display Cable
- USB Keyboard
- USB Mouse

3. Insert microSD card into Raspberry Pi

MicroSD card is inserted with the nub facing down

4. Connect peripherals to Raspberry Pi:

- Raspberry Pi HDMI to Monitor DVI-D using lab HDMI to DVI-D Cable
- USB Keyboard
- USB Mouse

5. Connect an Ethernet cable to your Pi, but DO NOT connect the Ethernet cable to any other networking hardware

6. Connect Raspberry Pi Power Supply

Capture & Collect: PiCK

There is a standalone network in the Networking Lab; i.e. there is a separate physical network in the Networking Lab that is not connected to the Enterprise network or the public Internet. Actually, the standalone network is a standalone internet since it consists of interconnected networks. There are two student local area networks, one for the right side and one for the left side. The two student networks are interconnected via routers sitting on the tables in the back of the room. The routers additionally interconnect other networks in the standalone network.

Activity: A Little Bit of Traffic, For a Lot of Analysis

1. Open Wireshark
2. Start capturing traffic on your Pi's Ethernet interface
3. After you are capturing traffic, connect the Ethernet cable to one of four the 24-port Linksys switches sitting on top of the lab workstations
4. Observe packets being displayed in Wireshark

Activity: Warm Up

1. Redirect the output of `ifconfig` for only your Pi's Ethernet adapter to a file named `RPi-ifconfig-<YOUR_LASTNAME>.txt`
2. Ping a neighbor's Pi; no need to save output from `ping`
3. Redirect the output of `arp` for only your Pi's Ethernet adapter showing IPv4 addresses (not host names) to a file named `RPi-arp-<YOUR_LASTNAME>.txt`
4. Redirect the output of `dig` when resolving the IP address of `www.globocorp.com` to a file named `RPi-dns-globocorp-<YOUR_LASTNAME>.txt`
5. Complete Question 2 on the assignment

Activity: Hi There

1. Pair up with someone on the same local area network; i.e. someone connected to a switch on your side of the lab room
2. Use `nc` (netcat) to communicate with each other
3. For each pair choose who will be the *server*, who will be the *client*
4. Server enter: `$ nc -l 50205 # Or an other 42000+ port number`
5. Client enter: `$ nc <SERVER_IP_ADDR> 50205 # Or other port used`
6. In support of data analysis have the first message say who you are (real last name) and who you are talking to
7. Once connected exchange a few more innocuous messages.
8. Once complete end the communication by entering: *Ctrl-d* (End of File)
9. Display and save the contents of the eth0 ARP cache to a file named `RPi-arp-local-nc-<YOUR_LASTNAME>.txt`

Activity: Hello Over There

1. Pair up with someone on the other local area network; i.e. someone connected to a switch on the other side of the lab room
2. Use `nc` (netcat) to communicate with each other
3. For each pair choose who will be the *server*, who will be the *client*
4. Server enter: `$ nc -l 50205 # Or an other 42000+ port number`
5. Client enter: `$ nc <SERVER_IP_ADDR> 50205 # Or other port used`
6. In support of data analysis have the first message say who you are (real last name) and who you are talking to
7. Once connected exchange a few more innocuous messages.
8. Once complete end the communication by entering: *Ctrl-d* (End of File)
9. Display and save the contents of the eth0 ARP cache to a file named `RPi-arp-other-nc-<YOUR_LASTNAME>.txt`

Activity: Bad Selection

1. Send 5 pings to the target host below based on your side of the lab room:

- Left: 192.168.1.21
 - Right: 192.168.3.21
2. Redirect the `ping` output to a file named `RPi-ping-local-<YOUR_SIDE>--<YOUR_LASTNAME>`
 3. Send 5 pings to the target host below based on your side of the lab room:
 - Left: 192.168.3.21
 - Right: 192.168.1.21
 4. Redirect the `ping` output to a file named `RPi-ping-other-<OTHER_SIDE>--<YOUR_LASTNAME>`
 5. Send 5 pings to the target host 9.9.9.9
 6. Redirect the `ping` output to a file named `RPi-ping-quad9-<YOUR_LASTNAME>`

Activity: Tracing a Route

1. Read the `traceroute` man page
2. Use `traceroute`, with the `-I` option, to trace the route to a host on your local area network (someone on your side of the lab room)
3. Redirect the `traceroute` output to a file named `RPi-traceroute-local-<YOUR_SIDE>--<YOUR_LASTNAME>.txt`
4. Use `traceroute`, with the `-I` option, to trace the route to a host on the other student network (someone on the other side of the lab room)
5. Redirect the `traceroute` output to a file named `RPi-traceroute-other-<OTHER_SIDE>--<YOUR_LASTNAME>.txt`
6. Use `traceroute`, with the `-I` option, to trace the route to `www.globocorp.com`
7. Redirect the `traceroute` output to a file named `RPi-traceroute-globo-<YOUR_LASTNAME>.txt`
8. Use `traceroute`, with the `-I` option, to trace the route to `www.ic322.com`
9. Redirect the `traceroute` output to a file named `RPi-traceroute-netCrs-<YOUR_LASTNAME>.txt`

note: `sudo traceroute ...` If you do not have permissions to run `traceroute`, then run `traceroute` via `sudo`.

```
$ sudo traceroute ...
```

Activity: Shutdown (End of Capture & Collect, PiCK Break Down)

1. Stop the ongoing Wireshark packet capture
2. Save the pcap as `RPi-labNet-<YOUR_SIDE>--<YOUR_LASTNAME>.pcapng`
3. Disconnect Raspberry Pi from lab networking equipment
4. Shutdown the Raspberry Pi, enter: `$ sudo shutdown -h now`
5. Restore the workstation to its normal configuration:
 - DVI-D Display Cable Connected
 - USB Keyboard Connected
 - USB Mouse Connected
6. Unplug Raspberry Pi Power Supply and Ethernet cable
7. Leave lab equipment and cables as directed by instructor
8. Take your PiCK when you leave

Activity: Transferring Files Between SD Card and Linux VM:

1. Shutdown the Raspberry Pi (see above)

2. Remove the MicroSD card from the Raspberry Pi
3. Insert MicroSD card into adapter (USB, SD card)
4. Start up your Linux VM and login as normal
5. Once logged into your Linux VM
6. Insert the MicroSD card adapter into your computer
7. VMware will prompt you, asking whether you want to connect the device to your Host OS (Windows) or to the Guest OS (Linux VM); select *Guest OS* to connect the peripheral to your Linux VM
8. You should see a media icon appear on your desktop once the MicroSD card has been mounted
At this point the MicroSD card is accessible from the file system in your Linux VM, you just need to navigate to the files you want to transfer.
9. Open *Nautilus*, Gnome Desktop file browser: Applications → Accessories → Files
10. You should see the MicroSD card drive listed in the tree view on the left
11. Use the file browser to navigate to where you saved the files on your Raspberry Pi; likely:
`/<VM-mount-point>/home/pi/`, or something similar
12. It is recommended that you copy files from the SD card to your VM hard drive for analysis
13. Once the files have been copied to your VM, you can eject the MicroSD card from the Linux VM, which will unmount the file systems on the MicroSD card; i.e. minimize the potential to corrupt the MicroSD card file systems
14. You either need to eject the MicroSD card or completely shutdown the Linux VM before you physically remove the MicroSD card adapter
Sleep and hibernate are not equivalent to *shutdown*; if you put your VM to sleep/hibernate you may corrupt the file system on your MicroSD card

Activity: Upload Data - Pi

1. Transfer target files from the Raspberry Pi SD card to your Linux VM
2. Ensure your files are named according to the directions in the lab; i.e. includes your name at the end of the file name
3. Logon to your USNA account in a web browser in your Linux VM
4. Upload your files to the associated directory in the SY205 Student Collaboration Space
 - a. Navigate to the sub-directory for this specific lab, `ip4AddressingRouting`
 - b. Click the + *New* button
 - c. Select *File Upload*
 - d. Navigate to and select the files to upload
 - e. Click the *Open* button
 - f. Observe files uploaded to SY205 Student Collaboration Space

IPv4 Addressing Basics

IPv4 addresses are 32 bits long, which means there are 4.29 billion (2^{32}) IPv4 addresses. Which at first might sound like a lot, but there are an estimated 7.6 billion humans (as of Fall 2018). How many devices do you own that are connected to the Internet? I'm guessing it's more than one, so naive logic says many people would be unable to connect to the Internet, especially since you have multiple IP addresses. We'll get back to solving address space limitations in minute. First, let's continue our exploration of IPv4 addresses.

0000 0000	0000 0000	0000 0000	0000 0000	# 32 0's, spaced for readability
0000 1010	0010 0000	0010 0001	1011 1101	# Selected 32 bit string of 0's and 1's

We don't like to look at long strings of 0's and 1's, so we want a short hand. You might be thinking hexadecimal would be a great short hand, and you wouldn't be wrong. We represent MAC addresses as hex, why not IPv4 addresses? Suffice it to say, we commonly represent 32-bit IPv4 addresses in *dotted-quad* format. We break the 32 bits into four groups (quad) using periods as a separator (dotted). We then represent the bit groupings as decimal vice hexadecimal, this is why you may hear the term *dotted-decimal* or dotted-quad. The below is an example that continues from above.

```
0000 1010   0010 0000   0010 0001   1011 1101   # Selected 32 bit string of 0's and 1'
0000 1010 . 0010 0000 . 0010 0001 . 1011 1101 # Selected 32 bit string of 0's and 1'
      10   .      32   .      33   .      189   # Dotted-quad
```

An IPv4 address has two parts, a network portion and a local address portion. The network portion is called the *prefix*, and the local address portion is commonly called the *host [portion]*. Although we will see in some cases why it is not technically correct to call the local address portion the host portion, especially regarding routing.

IPv4 addressing involves the use of a *subnet mask*. Recall, that ARP is used to map between Data Link layer addresses and Network layer addresses on a *local area network*. In our previous labs our local hosts used data in the ARP table to correctly address packets to the destination host. You might be wondering how the local host knew to use the ARP table to map an IP address to a MAC address; that is how did your local host know the remote destination host was on the same local area network. That is exactly what a subnet mask is used for. A local host uses its own subnet mask to determine if a destination remote host is on the same local area network or not. Let's complete an activity to derive how the subnet mask is used.

Activity: Unmasked

1. Fill in the table in Question 3.a., except for the *derived* rows using `labMach-ifconfig-<YOUR_LASTNAME>.txt` and `labMach-arp-<YOUR_LASTNAME>.txt`
2. Fill in the table in Question 3.b., except for the *derived* rows using `labMach-ifconfig-<YOUR_LASTNAME>.txt` and `labMach-dns-midnCyber-<YOUR_LASTNAME>.txt` ; for the remote host use `midn.cyber.usna.edu` .

A host determines host network prefixes by using its own subnet mask and the Network layer addresses of the hosts; a host knows its own subnet mask, a host does not know *any* remote host's subnet mask. A host performs a bitwise boolean operation to determine if a destination host is on the same local area network as the local host or not. The operands of the bitwise boolean operation are the target host's (local host or destination host) Network layer address and the local host's subnet mask. The result of the bitwise boolean operation performed by the local host is the *network address* (Network layer network) that the local host determines the destination (remote) host is own. The boolean operation is performed two times, and the results are compared for equality. The local host first determines its own *prefix* using its own IPv4 address and its subnet mask. Next, the local host determines the destination host's prefix using the destination IPv4 address and its (local host) subnet mask. The two resulting prefixes are compared.

Hosts that are on the same local area network have the same Network layer network address; i.e. they have the *same* Network layer address prefix. Hosts that are on different local area networks have different Network layer address prefixes. The below diagram depicts the calculations and comparisons that the local host performs, you will derive the bitwise boolean operation used in the calculation as part of the assignment.

--- Calculations Performed by Alice (local host) ---

Alice IP Address	Bob IP Address
? Alice Subnet Mask	? Alice Subnet Mask
=====	=====
Result _A	Result _B

?: Bitwise Boolean Operation to be derived

if Res_A == Res_B: Alice and Bob are on *same* local area network

if Res_A != Res_B: Alice and Bob are on *different* local area networks

1. Review the *Bitwise Operations* material, and discuss with each other as needed to complete Question 3 on the assignment

Hint: In the subnet mask what bits are 1's, what bits are 0's.

2. Derive the bitwise Boolean operation used by a host to determine if a destination host is on the same local area network or not.

3. Complete the rest of Question 3.

In the early years of IPv4, IPv4 addresses followed a *classful* addressing scheme. That is there were three, and eventually five, classes of IP addresses. The different classes allowed for networks of different sizes, and purposes.

IPv4 Classful Address Scheme

Network Class	Network Prefix Length (bits)	Network Prefix Range (dotted-quad)	Network Prefix Range (binary)	Subnet Mask (dotted-quad)	Comments
Class A	8	0.0.0.0–127.0.0.0	0000 0000–0111 1111	255.0.0.0	Most significant bit is 0
Class B	16	128.0.0.0–191.255.0.0	1000 0000.0000 0000–1011 1111.1111 1111	255.255.0.0	Two most significant bits are 10
Class C	24	192.0.0.0–223.255.255.0	1100 0000.0000 0000 0000 –1101 1111.1111 1111 1111	255.255.255.0	Three most significant bits are 110
Class D	-	224.0.0.0–239.255.255.255	1110 0000.0000 0000 0000.0000 0000 –1110 1111.1111 1111 1111 1111 1111	-	Multicast address: Used for data streamed to multiple hosts
Class E	-	240.0.0.0–255.255.255.255	1111 0000.0000 0000 0000.0000 0000 –1111 1111.1111 1111 1111 1111 1111	-	Reserved for future use

Each IPv4 network has two addresses that a host on the network cannot use as its IP address. The first address is the *network address*, which is derived by a local host using its subnet mask. The network address for a network is the prefix, with a local address portion of all 0's.

Can you guess the bit sequence for the other address on a network that hosts on the network cannot be individually addressed by?



A local address of all 1's is the *broadcast address* for a network.

Traffic destined for the broadcast address of a network will go to every host on the network. That is every host on a network will receive and process a packet sent to the broadcast address.

Within the Class A address space the 0.0.0.0 address is reserved, and no host is identified by the 0.0.0.0 IPv4 address. You will see 0.0.0.0 used with source code or configuration files for software systems. The all 0's address is used by programs to tell the operating system that the program will accept network communications on any of the

addresses associated with the local host. That's right, a single host may have multiple IP addresses. In fact, an IP address is associated to an interface on a host; that is each interface a host is connected via will each have a Network layer address associated to it.

Beyond the `0.0.0.0` address the entire Class A `0` network is designated as special purpose, and does not represent an actual network. Additionally the `127.0.0.0` Class A network is a special purpose network. The `127.0.0.0` network is the IPv4 local host network. Each IPv4 host has a `127.0.0.0` network that can be used to communicate using the TCP/IP stack within the local host. Recalling the Networking Intro material, an operating system typically handles Network layer services on a local host. Therefore, an operating system that supports the TCP/IP stack needs to internally support addresses on the `127.0.0.0` network in order to fully implement the TCP/IP stack.

All these special purpose addresses and special purpose networks result in less IP addresses being available to represent hosts at the Network layer. That is the theoretical maximum number of hosts that could be uniquely identified by an IPv4 address (~4.29 billion) is higher than the actual number of hosts that can be uniquely identified in practice. There are often differences between theory and implementations of theory (practice). Both theory and practice are important to the Cyber Operator. There have been vulnerabilities found in theory, and vulnerabilities found in implementations of theory; there will continue to be vulnerabilities found in theory and practice.

With this knowledge, complete Questions 4–5 on the assignment.

In your introductory programming class you are likely starting to realize that your first approach to solving a problem is not your final solution; that is once you have a solution working you begin to realize ways that you can improve upon that solution. Networking protocols are no different, in fact any system design and implementation is no different. We have refined and improved upon networking protocols over years of experimentation and practice.

One issue noted with classful IPv4 addresses is that they are rigid. The Class A, Class B, and Class C networks only supported networks of three different sizes. If you needed a network that was a different size, you only had a two options.

1. Use the larger class network, but have many unused addresses
2. Use multiple networks of the current class size, but increase the amount of Layer 3 networking equipment, and therefore administration

One big issue with Approach 1. is that using a larger class network contributes to the IPv4 address exhaustion problem. A big issue with Approach 2. is that routing packets between the networks would take up more resources (add complexity).

Over time *Classless Inter-Domain Routing* (CIDR) was developed. Instead having fixed network prefix lengths of 8, 16, or 24, CIDR allows the prefix to be 0–32. CIDR defines the meaning of some of the prefix lengths (0, 31, 32), and remains backwards compatible with the classful IPv4 addressing scheme. CIDR also introduced a new notation for IP addresses. E.g.

```
10.32.33.189/24
```

In the above example `/24` means that the prefix is 24 bits. In CIDR the prefix still starts at the left, the most significant bits. So the host's complete IP address is `10.32.33.189`, the host is in the `10.32.33.0` network. The host's subnet mask is `255.255.255.0`. As you can see CIDR notation allows a lot more information to be derived from its shorter representation compared to a classful scheme. Additionally, routers store routing information in the CIDR format; that is CIDR format is used in multiple ways at the Network layer.

With this knowledge, complete Question 6 on the assignment.

Routers

Routers are critical to the infrastructure that make up the Internet. Routers are the networking hardware that interconnect different networks; i.e. routers *are* the devices that make the Internet an internet. Routers route packets from one network to the next network, beginning from the source host all the way to destination host; assuming there is a route connecting the two hosts.

Recall a switch is Data Link layer device, a router is Network layer device. One of the differences between a switch and a router is that a router does play a role in the communication, usually a silent role from the perspective of the Application layer protocols/users. A router has an IP address, that is a router could be the source or destination in a network communication. In fact a router has an IP address on each of the networks the router interconnects. A router is part of multiple local area networks, and as a router its role is to forward packets between the local area networks it connects.

In the lab room (MI300) each side of the room (LEFT, RIGHT) had a router. The two routers were separately connected to each other, forming a local area network consisting of only the two routers.

By its name, and from its use, you likely realized that `tracert` can be used to trace the route between the local host and a remote destination host. `tracert` displays the *hop* count that it took to get to part of the route. In `tracert` output each listing before the final destination is a router; each router is where a hop occurs. A hop is a *Network layer* unit of measure, local area networks are not considered a hop. From the Network layer's perspective hosts on a local area network are directly connected, no hop.


hop

A count of the number of routers (Network layer device) a packet traverses through.
Data Link layer network devices are not counted as a hop.
The end hosts (communicating hosts) are not counted as a hop.
`tracert` does list a number for the end host in its output.

With this knowledge, complete Questions 7–8 on the assignment.

We use the below symbol to depict routers in a network diagram.

Common Network Diagram Symbols

Symbol	Description	Comments
	Router	Circle with arrows; arrows often depicted as crossing in middle (like an X)

The LEFT side of the classroom is the `192.168.1.0/24` network. The RIGHT side of the classroom is the `192.168.3.0/24` network.

Each local area network is its own broadcast domain.

With this knowledge, complete Questions 9–11 on the assignment.

Now that we have a general understanding of what a router does, and they fit into the networking picture. Lets take a deeper look at routers in action. As we mentioned routers are part of network communications. In general end hosts are not aware of the routers between them, a local host generally only knows about its gateway router.

We mentioned that routers interconnect different local area networks. The Internet is made up of millions of interconnected routers. Many routers are connected to many (more than two) networks. These interconnections mean that loops between routers could exist.

Interconnecting routers forming loops has the benefit of providing multiple routes for a packet traversing a network. This is a good thing for reliability; i.e. this can enhance the ability of the network to provide its service. Routers can detect slow or down routes and route traffic through other networks.

But loops are not without their issue. An issue that the designers of the Internet realized early on is that routing loops meant there was a potential for a packet to get stuck in a "routing loop". That is a packet could get stuck in a cycle between a set of routers being infinitely forward between the routers. Overtime a routing loop could bring down networks. More and more packets could stuck in the loop until the only packets passing between the routers are packets stuck in the loop.

To combat this issue IP datagrams include a Time To Live (TTL) field. Per protocol, each router decrements the TTL of each packet it receives. If the TTL field reaches 0, then the router discards (drops) the packet, and sends an error message back to the source host. The source host sets the initial value of the TTL field. Since the Network layer is provided as a service by modern day operating systems, the operating system sets the initial value of the TTL field.

in operations: TTL Different operating systems set a different initial TTL value. Overtime as the Internet has grown operating systems of increased their initial TTL value. This means that we derive network architecture and end host information based on TTL values.

Student Activity: Time To Live

For this analysis, use a communication between hosts with `192.168.0.0/16` IP addresses, do not use hosts with `169.254.0.0/16` IP addresses.

1. Start Wireshark, and open the pcap from your RPi session: `RPi-labNet-<YOUR_SIDE>-<YOUR_LASTNAME>.pcapng`
2. Apply a display filter to only display TCP traffic; i.e. the `nc` communication from the capture portion of the assignment
3. For this analysis we will be focusing on the IPv4 details of the packet
4. Complete Questions 12–13 on the assignment

Dynamic Host Configuration Protocol

At this point you might be wondering how a host is assigned an IP address, and other networking configuration information, to begin with. After all, you've communicated across a local area network and now between interconnected local area networks using your RPi, and looked up the network configuration of your RPi, but you never configured your IP address or subnet mask for that matter. So, how did your RPi get its networking information. Well, that is where Dynamic Host Configuration Protocol (DHCP) comes in.

DHCP is an *Application* layer protocol, but is specifically designed to configure Network layer settings. DHCP is used to configure the following network settings for a host, among other settings:

- IP address
- Subnet mask
- Default route[r]
- DNS server IP address

There are four main messages associated with DHCP: Discover, Offer, Request, Acknowledge; often referred to by the *DORA* acronym. DHCP messages occur in DORA order between the host needing network settings configured and a DHCP server. Let's explore the DORA sequence of messages.

Student Activity: Link's Up

1. Start Wireshark, and open the pcap from your RPi session:

note: BOOTP vs. DHCP BOOTP and DHCP serve similar purposes, and use the same Transport layer protocol and ports, but there are differences between BOOTP and DHCP. On modern networks BOOTP has largely been replaced by DHCP. DHCP is based on BOOTP, but adds features not found in BOOTP. Since

DHCP is based on BOOTP, Wireshark uses *bootp* as the display filter for BOOTP and DHCP.

RPi-TabNet-<YOUR_SIDE>-<YOUR_LASTNAME>.pcapng

2. Apply a display filter to only display packets associated with your MAC address
(`eth.addr == <YOUR_RPI_MAC_ADDR>`); the `addr` field (attribute) will match either the source or destination address
3. Observe the remaining packets
4. Modify the display filter so that only *bootp* packets associated with your MAC address are displayed
bootp is part of the display filter protocol syntax like http, arp
5. From the displayed packets, select the last *DHCP Discover* packet
We want to analyze a complete DORA sequence, disregard any earlier DHCP Discover packets that were unanswered due to in class lab equipment configurations.
6. Complete Questions 14–16 on the assignment

Once the DORA sequence of messages is complete, once the DHCP server sends the *DHCP Acknowledge* the IP address lease is in effect; i.e. the lease has been signed. But, the requesting host is not done yet. Now that the local host has an IP address, how should the host inform other local area hosts about its Network layer address? Hmmmm, what protocol can the local host use to map a Data Link layer address for the local area network to a Network layer address?



The local host can use the Address Resolution Protocol (ARP).

Student Activity: DORA, ARP, ARP

1. Continuing from the above Wireshark session
2. Modify the display filter that only *bootp* [logical] or *arp* packets associated with your MAC address are displayed
3. Observe the remaining packets
4. Recall the packet number of the DHCP Discover packet from the successful DORA sequence (see beginning of Question 14 on the worksheet)
5. Complete Question 17 on the assignment

The first set of ARP packets following a DORA sequence deserves further explanation. You are probably wondering why the local host starts asking about itself? The answer goes back to the sound engineering performed by the protocol designers.

Large organizations, think enterprise networks like the USNA intranet, have many internal networks with many different types of hosts (heterogeneous mix of platforms [operating systems, architectures]). If you look back at the DORA sequence the DHCP server addressed the packets specifically to the requesting client, not broadcast to every host on the local area network. The protocol designers realized they need to account for the possibility that hosts and the DHCP server may become out of sync for any number of reasons. Specifically, the designers needed to address the possibility that the DHCP server thinks a lease has expired or does not exist, but a host on the network thinks a lease is still in affect; like when the DHCP server is rebooted after a crash or upgrade.

After receiving the DHCP Acknowledge message the local hosts checks to see if any other host on the local area network is using the IP address the DHCP server leased to it. If no one responds, then all is well and the local host uses the agreed upon network settings. If another host does respond, then the requesting host sends a DHCP Decline message back to the server indicating that another host is using the associated IP address.

Student Activity: Lease is Up

1. Resuming the Wireshark session

2. Modify the display filter so that only *bootp* packets associated with your MAC address are displayed; i.e. filter out ARP packets
3. Observe the remaining packets
4. Complete Questions 18–19 on the assignment

References

- Cotton, M., et al., "Special-Purpose IP Address Registries", RFC 6890, IETF, Apr 2013.
- Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, IETF, Mar 1997.
- s
- Fuller, V., and T. Li, "Classless Inter-Domain Routing (CIDR)", RFC 4632, IETF, Aug 2006.
- Reynolds, J., and J. Postel, "Assigned Numbers", RFC 990, IETF, Sep 1986.