Networking Infrastructure

Learning Outcomes

After completing these activities you should be able to:

- Setup and communicate via a wired local area network using a hub
- Setup and communicate via a wired local area network using a switch
- Derive network architecture by analyzing protocols in execution: ARP, ICMP, TCP
- Explain the following terms: collision domain, broadcast domain
- Compare and contrast a hub and switch regarding the following topics: collision domain, broadcast domain, communications media utilization, pillars of cyber security
- Capture and analyze network traffic using common network utilities

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

Documents

	Version		
Document	Student	Post/Solution	Due Date
Notes	-	-	-
Assignment	student	solution	15 Oct 2019
Student Collab Space Directory	`networkingInfrastructure`	-	10 Oct 2019

- Read (*Kulrose & Ross*) [Apply Textbook Reading Guidance (see *Networking Models*)]
  - Section 6.1 *Introduction to the Link Layer* (~6 pages)
  - Section 6.2 *Error-Detection and -Correction Techniques* (~6.5 pages)
  - Section 6.3 *Multiple Access Links and Protocols* (~16 pages)
  - Section 6.4.1, 6.4.2, 6.4.3 *Switched Local Area Networks* (~20 pages)
- Complete the activities included in *In Class*

In Class

Assignment

We will complete three main tasks in this lab. First, we will setup your Raspberry Pi that we will use for many of the labs. Second, we will setup a wired network using a hub. Third, we will setup a wired network using a switch.

You conduct the same tasks in the hub and switch portion of the lab; i.e. complete steps once connected via a hub, then repeat the steps once connected via a switch. At the end of the lab you will share the pcaps you capture with your classmates.

Raspberry Pi Setup

You will checkout a Raspberry Pi kit for use in SY205, you will return the Raspberry Pi kit at the end of the course. You will need to bring most of the Raspberry Pi kit to class from here on out; you will be told what days you will not need to bring the Raspberry Pi kit to class, e.g. exams, review days.

Activity: This is My Pi

1. Pick up a complete Raspberry Pi kit
2. You should have the following items in the kit:
    - Raspberry Pi 3 with Case
    - AC/DC MicroUSB-B Power Adapter
    - 32GB MicroSD Card
    - USB MicroSD Card Reader
    - USB 3.0 Gigabit Ethernet Adapter
    - 3' HDMI Cable
    - Anti-static bag
    - Raspberry Pi Safety Instructions and Quick Start Guide (element14)
    - Raspberry Pi GPIO Header Quick Reference (CanaKit)
    - CanaKit Raspberry Pi Quick-Start Guide (CanaKit)
    - CanaKit Raspberry Pi kit box

The following items form the in class Raspberry Pi kit, known as the *Pi Class Kit* (PiCK), and are needed for in class activities:

- Raspberry Pi 3 with Case
- AC/DC MicroUSB Power Adapter
- 32GB MicroSD Card with SY205 setup
- 3' HDMI Cable

- MIDN Laptop
- MIDN Laptop Power Supply (or Charged Battery for 2.5 hours of usage)

The following lab equipment will be utilized in class, and will stay in the lab room (MI300):

- Workstation Equipment:
    - Monitor
    - Keyboard
    - Mouse
- Various Ethernet Cables
- Various Networking Equipment: Ethernet hubs, Ethernet switches, Ethernet routers

Follow the below directions to setup of the Raspberry Pi for in class use. You will need to bring and setup your PiCK based on the directions for in class activities. At the end of the class you will be expected to break down your PiCK, and return the lab systems to their normal configuration. **Note:** Your instructor will give you a ten minute warning before the end of class.

Activity: PiCK Up Game (Beginning of Class PiCK Setup)

1. Pull up the notes for the day via your laptop
2. Disconnect the workstation peripherals:
    - USB Keyboard
    - USB Mouse
3. Insert microSD card into Raspberry Pi
   Note: MicroSD card is inserted with the nub facing down
4. Connect peripherals to Raspberry Pi:
    - Raspberry Pi HDMI to Monitor HDMI using HDMI Cable
    - USB Keyboard (from lab workstation)
    - USB Mouse (from lab workstation)
5. Connect Raspberry Pi Power Supply
   Note: As in the Fleet (PMS - Preventive Maintenance System), order matters; power on the RPi after peripherals are connected

Activity: Shutdown (End of Class PiCK Break Down)

1. Stop and save any ongoing packet captures and analysis files
2. Disconnect Raspberry Pi from lab networking equipment
3. Shutdown the Raspberry Pi, enter: `$ sudo shutdown -h now`
4. Restore the workstation to its normal configuration:
    - USB Keyboard Connected

    - USB Mouse Connected

5. Unplug Raspberry Pi Power Supply and Ethernet cable
6. Leave lab equipment and cables as directed by instructor
7. Take your PiCK when you leave

Use the below credentials if you are prompted for username/password credentials; e.g. SSH, SFTP, `sudo` .

Enter Password to See Hidden Content

🔒

The following actions only need to be taken the first time you boot your Raspberry Pi using the SY205 microSD card.

Activity: If this is your first time, you have to (First Time Pi Boot Only)

1. Setup and boot the Raspberry Pi per the *PiCK Up Game* instructions
2. Observe the Pi boot into the Raspbian desktop environment
3. Open a shell session, click the *Terminal* icon in the task bar
4. Observe the shell prompt: `pi@sy205-13923e:~ $`
   Note: For many of you the hostname will be different than *sy205-13923e*, you still need to complete these instructions
5. Enter: `$ updateHostname.sh`
   To update your Pi's hostname based on its MAC address.
6. Observe the Pi reboot
7. Observe the Pi boot into the Raspbian desktop environment
8. Open a shell session and observe the changed hostname; i.e. not `sy205-13923e`

Activity: It's Your Jeep

1. Start Wireshark: `$ wireshark &`
2. Setup a new configuration profile:
    1. Open the *Wireshark Configuration Profiles* window: Edit → Configuration Profiles...
    2. Click the + button to create a new configuration profile
    3. Give the new configuration profile a descriptive name (course, your name/tag, etc.)
    4. Click *OK*
3. Return to the Wireshark Preferences window
4. Expand the *Appearances* branch

5. Select *Columns*
6. Review the below interface instructions:

    - Use + to add a column
    - Use - to delete a column
    - You may drag columns to change ordering
      Note: If the preferences window hangs, press *Alt-F4* to close the preferences and try again/another way
    - Double click a cell in a column to edit the value (text entry, list selection)

7. Configure your main Wireshark view according to the following:

SY205Minimum
Wireshark Columns

Type [→ Fields]
Number
Time (format as specified)
Custom → eth.src
Custom → eth.dst
Custom → ip.src
Custom → ip.dst
Source port
Destination port
Protocol
Information

Activity: Poker Face — Don't Tip Your Hand

1. Open the *Wireshark Preferences* window: Edit → Preferences
2. Select *Name Resolution* in the tree view
3. Uncheck (de-select) the following check boxes as necessary:

    - Resolve MAC addresses
    - Resolve transport names

- Resolve network (IP) addresses
- Use captured DNS packet data for address resolution
- Use an external network name resolver
- Only use the profile "hosts" file
- Resolve VLAN IDs
- Enable OID resolution
- Suppress SMI errors

4. Click *OK*

Activity: OCD (or Organized for Cyber Dominance)

We're going to capture and collect a lot of packets and data in a lot of files for each assignment; create a directory organization that works for you. At a minimum you need to create a directory for each set of meetings; e.g. a single directory for both Networking Infrastructure class meetings.

Capture & Collect: Hub

A hub is one of the most basic, and one of the lowest layer networking devices. A hub operates at the Physical layer, and is basically not much more than a repeater. A hub detects a digital signal on one physical port and retransmits that digital signal on all other physical ports. Hubs are not very common in modern enterprise wired networks due to their inefficient use of the communications medium. That being said hubs can serve as a crude network tap in a pinch — hubs are operationally relevant.

note: **Wireless Networks** Wireless networking equipment operates like a hub; i.e. all radios within range of a signal hear the signal. Additionally, wireless networking protocols have to detect and address message collisions just like hubs and protocols that run over hubs have to detect collisions. You will discuss wireless and mobile communications in much greater detail in SY312.

Hubs do not understand Data Link layer addressing, that is why hubs are considered Physical layer devices. The only portion of a Data Link layer protocol that a hub understands are the portions of the protocol associated with digital signals and connecting to the communications medium. A hub detects the start and end of a digital signal sent across the communications medium. A hub knows which interface, physical port, a signal is detected on, and retransmits that signal across the other interfaces.

Activity: Ready Player One

Note: We will be using 4–8 port networking equipment for these activities. If you find yourself connecting to larger 24+ port networking equipment you are wrong; the networking lab is a shared resource with another networking course.

1. Assemble as a small group with other classmates as directed by your instructor
2. Decide who will play each of the following roles: Alice, Bob, Carlos, Dave.

Activity: Start Capture

1. Every group member needs to complete this activity before continuing to the next activity
2. Start Wireshark
3. Start capturing packets in *promiscuous* mode on only *eth0*:

    1. Select *Capture → Options*
    2. Click the *Start* button

4. Observe a *blank* main Wireshark view

Once all group members are synchronized at this point, you may continue.

Activity: Link Local

1. Ensure the *Normal/Uplink* button is in the *Normal* position on the hub
2. Connect your Pi to your groups' Ethernet hub, one of the following:

    - Netgear DS104
    - Netgear DS108
    - Netgear EN104TP

    It does not matter which port you connect to.

3. Open a shell session
4. Use `ifconfig` to display network information for only the `eth0` interface. Hint: `$ man ifconfig`
5. Save the `ifconfig` output to a file named *ethHub-ifconfig-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.txt*. Hint: Redirection is your friend.
6. Complete Question 1 on the assignment

As you connect your Pi's to the hub you should see packets in the main Wireshark view.

At this point you are connected via the hub using what are called *link local* addresses. Each of your Pi's has a unique link local IPv4 address, which is good because each host has to be uniquely identifiable at the Data Link and Network layers. We will talk about this in further detail when we discuss DHCP, for now the following summary will suffice. The packets you saw being captured were from each Pi requesting an IP address. The request went unanswered, so your Pi negotiated a unique link local address.

At this point you have not sent any direct communications to any of your group members.

Activity: Empty ARP

1. Enter: `$ arp -n -i eth0`
    To display the contents of your ARP cache for the eth0 interface.
2. Complete Question 2 on the assignment

Activity: Pinging Around

1. Ping each other in pairs:

    - Alice pings Bob
    - Bob pings Alice
    - Carlos pings Dave
    - Dave pings Carlos

   If you have an odd number of group members, then have one group member double up; e.g. Alice pings Carlos, Carlos pings Alice.

2. Ping your designated target via: `$ ping -c 3 <TGT_IP_ADDR>`
3. Display and save the contents of the eth0 ARP cache to a file named *ethHub-arpCache-ping-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.txt*
4. Complete Question 3 on the assignment

Activity: Can You Hear Me?

1. Use `nc` (netcat) to communicate in the following pairings:

    - Alice and Bob
    - Carlos and Dave

2. For each pair choose who will be the *server*, who will be the *client*
3. Server enter: `$ nc -l 50205  # Or an other 42000+ port number`
4. Client enter: `$ nc <SERVER_IP_ADDR> 50205  # Or other port used`
5. In support of data analysis have the first message say who you are and who you are talking to
6. Once connected exchange a few more innocuous messages.
7. Once complete end the communication by entering: *Ctrl-d* (End of File)
8. Display and save the contents of the eth0 ARP cache to a file named *ethHub-arpCache-nc-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.txt*

Activity: All Accounted For

1. Ping any group members you have not pinged or communicated with via `nc`
2. Display and save the contents of the eth0 ARP cache to a file named *ethHub-arpCache-allHere-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.txt*

Once all group members are synchronized at this point, you may continue.

Stop and save your current pcap to *ethHub-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.pcapng*.

Activity: Packet Storm

1. Restart capturing packets on the *eth0* interface
2. Read the `ping` man page regarding the `-f` option

3. Ping each other in a round-robin fashion as super user using the `-f` option:
   `$ sudo ping -f <TGT_IP_ADDR>`

4. Let this run for about a minute or so

5. To stop the ping flood enter: *Ctrl-c*

6. Stop and save the current pcap as *ethHub-pingFlood-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.pcapng*

Activity: Targeted Attack

1. Restart capturing packets on the *eth0* interface

2. Ping each other based on the below assignments using the `-f` option:

Role	Ping Target
Alice	Bob
Bob	Alice
Carlos	Bob
Dave	Bob

3. Let this run for about a minute or so

4. To stop the ping flood enter: *Ctrl-c*

5. Stop and save the current pcap as *ethHub-tgtAtk-<GROUP_ID<-<ROLE>-<YOUR_LAST_NAME>.pcapng*

Once all *groups* are synchronized at this point, you may continue.

Activity: Packet Storm II

1. Disconnect the Ethernet cable to you Pi, you may leave the Ethernet cable connected to the hub

2. Connect the hubs between groups as directed by your instructor using additional longer Ethernet cables

3. Restart capturing packets on the *eth0* interface

4. Use `ifconfig` to display network information for only the `eth0` interface. Hint: `$ man ifconfig`

5. Read the `ping` man page regarding the `-f` option

6. Ping each other in a round-robin fashion as super user using the `-f` option:
   `$ sudo ping -f <TGT_IP_ADDR>`

7. Let this run for about a minute or so

8. To stop the ping flood enter: *Ctrl-c*

Activity: Pull the Plug

1. While you are still capturing packets on eth0, disconnect the Ethernet cable from the hub
2. Stop and save the current pcap as *ethHub-pingFlood2-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.pcapng*

Capture & Collect: Switch

Activity: Intermission

1. Once all Ethernet cables are disconnected from the hub, unplug the hub power supply from the hub and the surge protector
2. Plug in the switch, but do not plug any Ethernet cables into the switch yet

> **note: Managed Switches** There are more advanced switches than the simple switches discussed here. Managed switches can be configured, that configuration typically happens by logging into the managed switch via the network or via a console port. Managed switches are beyond the scope of SY205.

Switches are considered Data Link layer devices, because switches understand Data Link layer protocols. Switches perform all the functions that a hub can. Simple switches themselves are not parties in a communication; i.e. interfaces on a switch do not have Data Link layer addresses. Instead of blindly retransmitting a digital signal down each other interface a switch only repeats a digital signal down the interface the destination host is on.

A switch has a CAM (Content Addressable Memory) table that is used to store Data Link layer addresses and physical interface associations. When a frame arrives on an interface, the switch looks up the destination address in its CAM table. If the destination address is found in the CAM table, then the frame is only transmitted down the associated interface. The CAM table is an internal caching mechanism for the switch, after a while entries in the CAM table are removed due to age (stale data). Additionally, like all storage, CAM tables are limited in size; i.e. a CAM table can only hold so many entries.

What do you think a switch would do if a destination address is not in the CAM table?

⌄

If an address is not found in the CAM table, then the switch has no choice but to repeat the frame on each other interface just like a hub.

Student Thought. Okay, but how does the switch keep its CAM table up to date? When the switch sees a frame it looks at the source address, and creates or refreshes an entry in the CAM table. This updating process happens for each frame. Based on the current configuration of your Pi's the broadcast messages sent when a networking interface is connected are the only things the switch needs to start populating its CAM table.

Activity: Start Capture

1. Every group member needs to complete this activity before continuing to the next activity
2. Start capturing packets in *promiscuous* mode on only *eth0*:
    1. Select *Capture → Options*
    2. Click the *Start* button
3. Observe a *blank* main Wireshark view

Once all group members are synchronized at this point, you may continue.

Activity: Switch Hitter

1. Connect your Pi to your group's Ethernet switch; it does not matter which port you connect to.
2. Open a shell session
3. Use `ifconfig` to display network information for only the *`eth0`* interface.
4. Save the `ifconfig` output to a file named *ethSwitch-ifconfig-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.txt*.
5. Complete Question 6 on the assignment

Note: As you connect your Pi's to the hub you should see packets in the main Wireshark view.

Activity: Pinging Around

1. Ping each other in pairs:
    - Alice pings Bob
    - Bob pings Alice
    - Carlos pings Dave
    - Dave pings Carlos
2. Ping your designated target via: `$ ping -c 3 <TGT_IP_ADDR>`
3. Display and save the contents of the eth0 ARP cache to a file named *ethSwitch-arpCache-ping-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.txt*
4. Complete Question 8 on the assignment

Activity: Can You Hear Me?

1. Use `nc` (netcat) to communicate in the following pairings:
    - Alice and Bob
    - Carlos and Dave
2. For each pair choose who will be the *server*, who will be the *client*
3. Server enter: `$ nc -l 50205  # Or an other 42000+ port number`
4. Client enter: `$ nc <SERVER_IP_ADDR> 50205  # Or other port used`
5. In support of data analysis have the first message say who you are and who you are talking to

6. Once connected exchange a few more innocuous messages.

7. Once complete end the communication by entering: *Ctrl-d* (End of File)

8. Display and save the contents of the eth0 ARP cache to a file named *ethSwitch-arpCache-nc-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.txt*

Activity: All Accounted For

1. Ping any group members you have not pinged or communicated with via `nc`

2. Display and save the contents of the eth0 ARP cache to a file named *ethSwitch-arpCache-allHere-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.txt*

Once all group members are synchronized at this point, you may continue.

Stop and save your current pcap to *ethSwitch-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.pcapng*.

Intermission

Before we begin our analysis of the captured packets, we need to share our captured data with our collaborators. Remember the course policy, collaborating on packet captures and sharing packet capture data are allowed. We will each analyze data that we individually and collectively capture and collect. Follow the below generic steps to upload all of the files from this lab to the `networkingInfrastructure` directory in the SY205 Student Google Drive collaboration space (see below, course resources).

Activity: Upload Data

1. Using the MicroSD USB card reader, transfer target files from the Raspberry Pi SD card to your Linux VM (see Course Resources → Raspberry Pi → Transfer files...)

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 in the associated directory (`networkingInfrastructure`) in the SY205 Student Collaboration Space

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

   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

Analysis: Protocols In Action

Recall we captured packets in *promiscuous* mode, so if that packet came across the Ethernet cable our Raspberry Pi was connected to, then the packet ended up in the pcap.

We used protocol sequence diagrams to depict abstract protocols. Let's replace the abstract protocols with real world protocols.

You pinged the other hosts on your local network by IP address, not by MAC address. Recall, an IP address is a Network layer address, and a MAC address is a Data Link layer address. But the Data Link layer uses MAC addresses not IP addresses to identify devices on the local network. So, how did your host know who to address the ping to at the Data Link layer? Ahh, that's where ARP comes in, remember from last week.

We will explore ICMP (Internet Control Message Protocol) in greater detail, for now you just need to know that `ping` sends and receives ICMP messages.

Activity: Before the Ping

1. Open up your *ethHub-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.pcapng* (first pcap, not the `ping` flood pcap) from when you were connected via the Ethernet hub
2. Filter the packets so that you see ARP and ICMP that only your device was a part of (i.e. your MAC address is either source or destination)
3. When properly filtered you should be able to discern the ordering of the ARP and ICMP (`ping`) traffic
4. Explore the packet details and complete Question 9 on the assignment

Activity: Loud and Clear

1. Enter a new display filter to just show TCP traffic; i.e. the `nc` communications
2. Explore packet details, and follow streams in order to complete Question 10 on the assignment

Analysis: Network Architecture

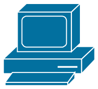
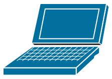
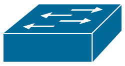
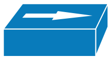
Networks can have different underlying architectures. How the transmission medium and physical hardware operate affect the network architecture. In other words details matter, just like in many other fields.

We use network diagrams to depict the physical architecture of a network. Like other aspects of networking and computing, we can scale the details in a network diagram. We can draw a detailed network diagram or reduce the details to depict a higher level network architecture, just like we scale the details in a protocol sequence diagram.

> **note:** Neatly Drawn The purpose of any diagram is to convey information. If your diagram is not neat enough for others to read, then you will not successfully convey information. (If you don't successfully convey information, then you wont receive full credit on an assignment.)

On the high end there is commercial software that specializes in developing network diagrams (as well as other types of diagrams). On the low end there are neatly, hand drawn network diagrams on white boards or paper. Regardless of the method used to develop a network diagram, we need to agree on (communications protocol) a set of symbols and their meaning. The below table lists the Cisco network symbols, the Cisco symbols are commonly used regardless of whether Cisco networking equipment is being used or not.

Common Network Diagram Symbols

Symbol	Description	Comments
	Host (Desktop)	Non-mobile host
	Host (Laptop)	Mobile host
	Switch	Rectangle with bi-directional arrows
	Hub	Rectangle with single direction arrow

Simple lines are commonly used to show connections between symbols in a network diagram. Collections of symbols may be surrounded by a circle, box, cloud, or other amoeba like shape to indicate a common relation between the symbols. For example, a group of hosts and servers may be surrounded by a cloud ( ) to indicate services or hosts in a cloud service provider. Additionally, hosts can be grouped into a collection to abstract away lower layer details; e.g. a Layer 3 diagram may omit Layer 2 switches and just encompass hosts via a circular shape.

Activity: ARP Build Up

1. View the contents of your *ethHub-arpCache-ping-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.txt*; your ARP cache after you pinged one other hosts on the network
2. Complete Question 12 on the assignment
3. View the contents of your *ethHub-arpCache-nc-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.txt*; your ARP cache after you communicated via `nc`
4. Complete Question 13 on the assignment
5. View the contents of your *ethHub-arpCache-allHere-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.txt*; your ARP cache after you pinged the other hosts on the network.
6. Complete Question 14 on the assignment

Analysis: Collision Domain

There are two terms associated with transmitting messages across a local area network (Data Link layer): *collision domain*, and *broadcast domain*. We will explore the meaning of both by analyzing the captured packets from the hub connected network and switch connected network.

collision domain
Collection of hardware devices in which only one device can transmit at a time (*Kozierok*).

A collision domain is also known as a *bus*; i.e. a communications bus. In the OSI and TCP/IP Stack Data Link layer protocols are responsible for detecting and handling frame collisions. There have been numerous research projects about ways to detect and recover from message collisions. A given technique may work better for a given transmission medium than another technique. In other words there is no one size fits all approach, network engineers need to understand the characteristics of the transmission medium and the hosts. You will cover the details of digital signaling, transmitting and receiving digital signals in SY312.

Many modern Data Link layer protocols provide CSMA/CD services, like Ethernet.

Carrier Sense Multiple Access/Collision Detection (CSMA/CD)
Carrier sense means that a sender can sense when another host is transmitting; i.e. the sender checks to see that no one is transmitting before it starts transmitting on the medium.
Multiple access means that multiple hosts can transmit on a given segment of the transmission medium.
Collision detection means that a sender can detect when another host started transmitting while the sender was still transmitting (propagation delay); i.e. a host can transmit and receive at the same time.

Capturing packets in promiscuous mode allows us to determine the hosts that the local host shares a collision domain with. That is, if we captured non-broadcast traffic that the local host was not part of, then we are in the same collision domain as the sending host.

Activity: Packet Collider

1. Review the networked communications in *ethHub-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.pcapng*
2. Analyze the `ping` (ICMP) and `nc` (TCP) traffic focusing on sender and receiver addresses
3. Complete Question 15 on the assignment

Analysis: Broadcast Domain

Recall that a switch is a Data Link layer device, where as a hub is a Physical layer device. The next set of activities will draw out the differences between a hub and switch; i.e. we will see how a switch performs the same function as a hub, but provides additional functions that a hub does not.

Activity: Switch <Insert Red and White Logo Here>

1. View the contents of your *ethSwitch-arpCache-ping-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.txt*; your ARP cache after you pinged one other hosts on the network
2. Complete Question 16 on the assignment
3. View the contents of your *ethSwitch-arpCache-allHere-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.txt*; your ARP cache after you pinged the other hosts on the network.
4. Complete Question 17 on the assignment

Activity: Something's Missing

For this activity you will analyze two pcaps: your *ethSwitch-<GROUP_ID>-<ROLE>-<YOUR_LAST_NAME>.pcap*, and a pcap from one of your group members that you did not communicate via `nc` with. That is if you are Alice or Bob, then you should analyze your own ethSwitch pcap, and either Carlos' or Dave's ethSwitch pcap. If you are Carlos or Dave, then you should analyze your own ethSwitch pcap, and either Alice's or Bob's ethSwitch pcap.

1. Use `tshark` and other command line utilities (`sort` , `uniq`) in the following analysis steps
   Hint: Review the *Packet Analysis Fundamentals* material as needed.
2. Using your ethSwitch pcpap, enter a command sequence to list the pairs of IP addresses that you saw communicating via TCP; i.e. the `nc` communications that your host saw
3. Using your group member's ethSwitch pcap, enter a command sequence to list the pairs of IP addresses that they saw communicating via TCP; i.e. the `nc` communications that your group member's host saw
4. Complete Question 18 on the assignment

⌄

Deeper analysis of the previous activity can highlight a functional characteristic of a switch, and one of the big differences between a switch and hub. When you were connected via a hub and capturing packets in promiscuous mode your host received the packets for the `nc` communication between the other group members. But your host did not receive the packets when connected via a switch. The lack of packets is evidence that the switch did not retransmit traffic down a network segment that the traffic was not destined for; i.e. a switch divides each physical interface of the switch into separate collision domains.

The collision domain network topology a switch provides is called a *star*, as opposed to a bus by a hub. The reason for using the term star will be clearer once you complete the next question. The switch sits at the center (intersection) of separate collision domains; i.e. when visualized via a diagram the switch is the center object that signals radiate from.

But what about a *broadcast domain*, what is that? Networks have broadcast addresses, each host on a network accepts traffic sent to the broadcast address. In the Ethernet and IPv4 protocols each have the concept of broadcast address. You have already seen the broadcast MAC address in use from your analysis of ARP.

The broadcast MAC address is all 1's; i.e. 48-bits of 1's. From the analysis you did on the hub network traffic you can see that there is no difference between the collision domain and broadcast domain for a hub. That is since a hub always retransmits a signal on each other physical interface regardless of Data Link layer addressing, the collision and broadcast domains are the same.

But what about a switch, is there a difference between the collision and broadcast domains? How could we determine this? Well, you just identified the collision domains for a switch. Now we just need to look at some broadcast traffic, if only we had some Data Link layer protocol broadcast traffic to analyze.

note: **Got Jokes?** What did the networking seal say to the other networking seal?

›

We know we are in the same broadcast domain as another host if we receive a message from them destined for the broadcast address. If a host does not receive a broadcast message from a host, then they are in different broadcast domains.

With this knowledge, complete Question 19 on the assignment.

Analysis: A Jump to Conclusions Mat

The Pillars of Cyber Security apply to all aspects of the cyber domain, not just software and higher level concepts. Hardware can support, or not support, the pillars of cyber security. The pillars of cyber security need to be incorporated into all design aspects of a system. We can't just try to secure the application, when the apps run on top of an operating system. We can't stop at securing the operating system (OS), when the OS runs on top of hardware. We can't stop at securing the host hardware when we interconnect hosts via networks.

Different networking technologies have different strengths and weaknesses regarding the pillars of cyber security and cyber operations. The following definitions are a refresher from SY110.

confidentiality [pillar of cyber security]
Protection of information from disclosure to unauthorized individuals, systems, or entities.
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information (*CNSSI 4009*).
Confidentiality is *data* oriented.
integrity [pillar of cyber security]
Protection of information, systems, and services from unauthorized modifications or destruction.
The property that data has not been altered in an unauthorized manner; covers data in storage, during processing, and while in transit (*CNSSI 4009*).
Integrity is *data* oriented.
availability [pillar of cyber security]
Timely, reliable access to data and information services for authorized users (*CNSSI 4009*).
Ensuring timely and reliable access to and use of information (*CNSSI 4009*).
Availability is *service* oriented.
non-repudiation [pillar of cyber security]
The ability to correlate, with high certainty, a recorded action with its originating individual or entity.
Protection against an entity falsely denying having performed a particular action; provides the capability to determine whether a given entity took a particular action (*CNSSI 4009*).
Non-repudiation is *entity* oriented.
authentication [pillar of cyber security]
The ability to verify the identity of an individual or entity.
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system (*CNSSI 4009*).
A security measure designed to protect a communications system against acceptance of fraudulent transmission or simulation by establishing the validity of a transmission, message, originator, or a means of verifying an individuals' eligibility to receive specific categories of information (*CNSSI 4009*).
Authentication is *entity* oriented.

Adapted from CNSSI 4009: Committee on National Security Systems (CNSS) Glossary, *Committee on National Security Systems*, 06 Apr 2015.

Recall that networks them selves provide the service of interconnecting hosts. With this knowledge, complete the remainder of the assignment.