Networking Models

Learning Outcomes

After completing these activities you should be able to:

- Describe the following networking terms: footer, header, host, network, packet, payload, protocol
- Explain the layers in the OSI networking model
- Explain the layers in the TCP/IP networking model
- Compare and contrast the OSI and TCP/IP networking models
- Describe what an RFC is
- Depict message exchanges using a protocol sequence diagram
- Explain and depict how messages are sent in a packet switched network
- Explain and depict the data encapsulation/de-encapsulation process

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	17 Sep 2019

- Read (*Kurose & Ross*)
  - Section 1.3, 1.3.1, 1.3.2 *The Network Core* (~10 pages)
  - Section 1.5 *Protocol Layers and Their Service Models* (~8 pages)
  - Section 1.6 *Networks Under Attack* (~4.5 pages)
  - Section 1.7 *History of Computer Networking and the Internet* (~6 pages)

note: Textbook Reading Guidance Review the learning outcomes for the discussion at hand. Use the learning outcomes to guide where you focus thorough reading. You will be tested on learning outcomes, but you need to be aware of broader points associated with a topic. In future courses, like the second networking course (SY312), you will cover some of the topics only introduced through reading in SY205.

- Section 1.8 *Summary* (~2 pages)

In Class

Introduction Discussion

> **note: and touch** We also communicate via touch, but that is beyond the scope of this course. E.g. various modern handheld devices provide haptic feedback.

One of the many traits that humans evolved is the ability to communicate. We communicate in visual and aural ways; digital communications are simply ways that we transmit visual or aural information. For millennia we have been advancing the way we communicate, we will continue to do so. Information networks are the result of continued advances in communication systems.

Communication Fundamentals

> **in the Fleet: Words Mean Things** Miss using terminology can lead to misunderstandings or errors in the most benign situations. In military operations misunderstandings or errors can lead to the unnecessary loss of life. Unfortunately, terms in one field mean something different in another field, and terms may be misused intentionally or unintentionally. In military operations it is critical for the parties communicating to agree on the meaning of the terms used.

In any field there is a set of terminology used to describe concepts, and facilitate the exchange (communication) of information. It is incumbent on veteran members of a field to inform new comers to the field of the terminology used in the field. We'll begin our formal discussion of networking by introducing terminology, and expanding that terminology into fundamental concepts; i.e. terminology and concepts that can be applied to communications in general.

At a high level, in a generic sense, how would you describe what *communication* is?

Your description likely identified some of the following concepts:

- [At least] two people talking
- Desire to exchange information between people talking
- Implied willingness of people to communicate
- Implied agreement on order of statements between people talking
- Implied agreement on format (syntax) of statements between people talking

Communication is so ingrained in being human that you probably didn't even think to list the *implied* features of communication. As individuals we learn to communicate and advance our communication skills from the day we are born. The digital communication systems we design and operate have to address the same concepts as human communications.

The first term we need to agree on in what we will call an entity that is communicating, in networking terminology this is a *host*.

host
A device participating in a communication.
A host is a device *not* the user of the device.
May be a physical device or virtual device (virtualized version of a physical device).
E.g. computer, laptop, cell phone, router, Internet of Things device

What do you think about when you hear the term *network*; i.e. how have your heard the term, or used the term network[ing]?

You likely came up with some of the below, or other concepts not listed:

- Connected hosts
- Social Media: Facebook, Twitter, Instagram
- Connections between people (I know a guy …)
- Technology devices that connect hosts

At a high level *network* is a simple, generic term that can have different connotations. All of these connotations boil down to a simple, generic definition.

network
A collection of entities that communicate with each other. (generic)
A collection of hosts that communicate with each other.

If you look back at the list of concepts that you came up with, you will see that the generic definition applies to each of them.

Having a generic definition for a term that can apply to many different situations is a good thing, particularly in computing. In engineering and science disciplines we like concepts that can be apply to different scales of a problem. We like ways to abstract away details to handle broader, high level concepts. We like ways to dive into the details of small problems. Having terminology that can scale with the size of the problem is a plus.

The term *network* is a term that can scale with the size, or nature of the hosts that are communicating.

At a high level two parties that want to communicate exchange a series of messages. In networking we refer to a message transiting across a network as a *packet*.

packet [general information system networking]
A message used to communicate information between hosts.
A message that is transmitted across a network.

What are some of the different nouns you have used to name a message? What are some of the different types of "messages" that you have sent?

The below is a short list; there are other examples:

- speech, talk, presentation
- conversation, discussion, argument, debate
- statement, point
- email, post, tweet, blog, text
- letter

In networking a packet is an important thing. Sometimes when there are a lot of different versions of a thing, and the small differences between the different versions are important we use distinct names for each version — we do the opposite of using a single generic term that scales, we use multiple, different terms.

Just like you came up with a number of different names for a message, because the differences matter, we have different names for a packet in different situations. We will discuss the different names for a packet as we discuss each of the situations in more detail.

What are the common parts of a conversation? Think about how you begin a conversation, how you end a conversation, and in between.

You likely came up with the following generically named, high level parts:

- Greeting: way to begin a conversation
- Information Exchange: way to exchange information between parties
- Conclusion: way to end a conversation

Congratulations, you just described a communications protocol that we use in daily conversations. You've been learning and using communications protocols since you started learning how to speak.

The implied characteristics of communication above are so ingrained in our minds that we often forget about them. Those implied characteristics are what a *protocol* is.

protocol
An agreed upon set of rules that governs how communicating parties communicate.
The rules parties use to exchange information.
Covers ways to begin, conduct, and end a communication.
Includes message formats, ways to request information, expected responses to requests, and ways to detect and recover from errors (misunderstandings).

A packet is single message, a protocol covers the various messages and responses that could be used in a communication session. A given execution of a protocol will likely include multiple packets.

Communication Stacks

What are the two most common ways that you connect to a network?

- Wireless (most common)
- Wired (Actually used to be the most common)

So, why and what is a communications stack? A communications stack is an approach to break a complex problem into smaller, less complex problems. Instead of trying to solve all of the problems with digital, networked communications in a single monolithic solution, we break the problem down into smaller portions and solve the problems independently. Each layer of a stack focuses on and solves a specific part of the overall, larger problem. By stacking the layers on top of each other we solve the overall, larger problem.

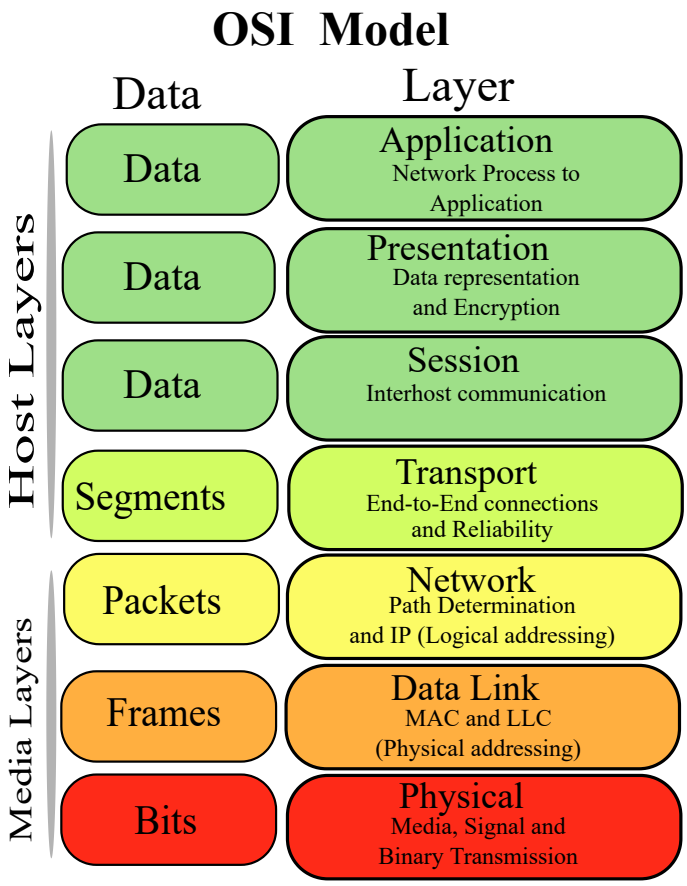
You can connect to a network wired or wirelessly and use the same web browser because of the layered approach of a communications stack. By separating out communication functions into separate layers and standardizing the interaction between layers, we can independently improve or change approaches at a given layer. A communication stack is an example of a modular approach to problem solving, the same approach you are learning to apply in your introductory programming course. You can switch between a wired and wireless network connection because of the protocols used and stacked upon each other in information system networks.

In a layered stack approach, lower layers can be viewed as providing services to higher layers. Having standard interfaces between layers allows solutions at a given layer to be changed independent of other layers; e.g. changing between a wired and wireless network connection.

In modern networking there are two communication stacks that are relevant. One is a generic, conceptual reference model; the other is the most prevalent reference model used in practice, i.e. includes actual protocols used in a communications stack. It is important to understand both reference models, how they are similar, and where they differ.

OSI Model

The Open Systems Interconnection (OSI) is the international standard reference model used in networking. In fact the OSI Model is an ISO (International Organization for Standardization) standard, ISO 35.100. The OSI model breaks network communications into seven layers. The below diagram depicts, and briefly describes the seven layers in the OSI model.



File:Osi-model-jb.svg. Wikimedia Commons. Retrieved 08 Sep 2018.

A common mnemonic to remember the layers in the OSI model is, "Please Do Not Throw Sausage Pizza Away". The *Data* column in the diagram also lists the names of packets at each of the layers. Each layer in the OSI model is intended to solve a problem of the complete set of problems associated with digital networked communications.

We briefly discuss the layers in the OSI Model here. We will explore the services provided by the layers in greater detail through the activities over the rest of course. Additionally, *Kurose and Ross* give a longer introduction of the layers in Chapter 1 (cough, read the assigned readings, cough).

Application
Top of networking stack.
Provides end user interface to protocol stack.
Implements protocol(s) that provide(s) services to end users.
Presentation
Data representation; allows applications to interpret meaning of data.
Includes data compression and data encryption.
Session
Data exchange synchronization.
Transport
Connects processes (running programs) on different hosts.
Network
Connects hosts on different networks.
Interconnects networks together.
Data Link
Directly connects hosts on a local network.

Converts between digital signals and digital data.
Physical
Bottom of networking stack.
Detects, transmits, and receives digital signals.

Remember, from the viewpoint of a higher layer, a lower layer is providing a service to the high layer.

TCP/IP Stack (Model)

Practice and theory sometimes do not converge; i.e. sometimes there are differences between implementation and theory. In practice the TCP/IP Stack is the widest used networking stack. There are other networking stacks, but over the decades the TCP/IP Stack has taken over and is by far the dominant communications stack. The TCP/IP Stack is so popular that the name *the Internet* comes from the IP in TCP/IP.

The *five* layers in the TCP/IP Stack are briefly discussed below.

Application
Top of networking stack.
Provides end user interface to protocol stack.
Implements protocol(s) that provide(s) services to end users.
Transport
Connects processes on different hosts.
Network
Connects hosts on different networks.
Interconnects networks together.
Data Link
Directly connects hosts on a local network.
Converts between digital signals and digital data.
Physical
Detects, transmits, and receives digital signals.

You might be wondering why there are two layers missing from the TCP/IP Stack. And, are asking yourself does the TCP/IP Stack not offer the services from the OSI Session and Presentation layers? The TCP/IP Stack does allow for the services provided by the OSI Session and Presentation.

What TCP/IP layer do you think implements (provides) the services provided by the OSI Session and Presentation layers?

> In the TCP/IP Stack the Application layer protocol is responsible for providing, or not providing, the services associated with the Session, Presentation, and Application layers.

Assignment

Now that we have agreed upon some basic terminology, and the ways we can divide the large complex problem of networking into smaller, independent problems we can take a high level look at protocols in action. The tools and techniques we will introduce here can scale up or down as needed. We will see how they can be used for a single protocol, or multiple protocols in succession. We will see how they can be used for two hosts, or many hosts. Additionally, these fundamental techniques can be used for other networking stacks (non-TCP/IP stacks).

Protocols and Standards

Remember in order for two parties to communicate, they need to agree on the manner in which they communicate. There are a number of standards bodies and organizations associated with networking technologies. The three primary organizations are: Institute of Electrical and Electronics Engineers (IEEE, eye triple E), Internet Engineering Task Force (IETF, I-E-T-F), and Internet Assigned Numbers Authority (IANA, eye ana).

The IEEE focuses on technologies associated with digital signals; i.e. the Physical and Data Link layers. In fact, Ethernet, WiFi, and Bluetooth are all IEEE standards. IANA governs Internet addresses, domain names, and other Internet Protocol related resources.

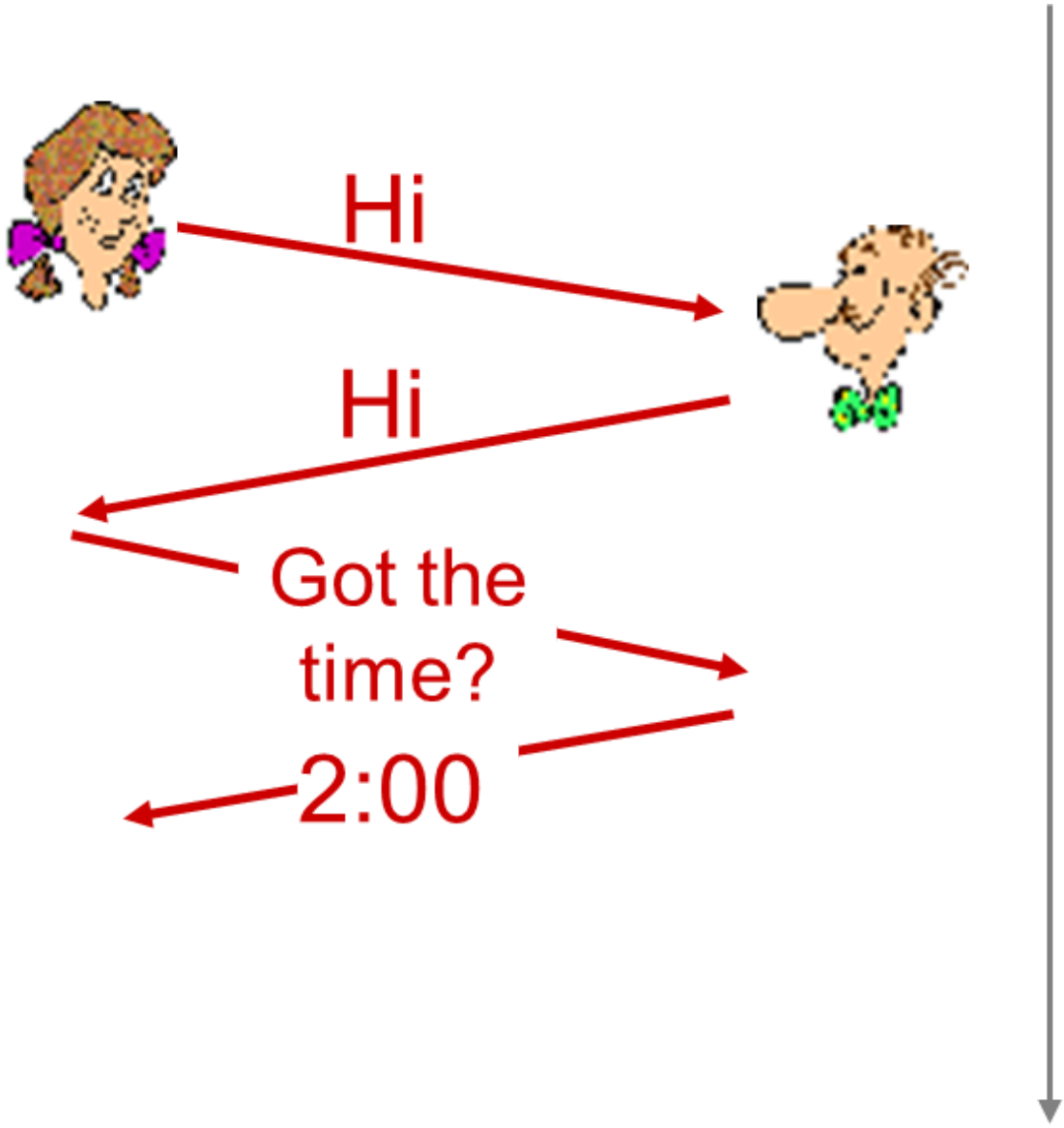
The IETF publishes *Request For Comments* (RFC); the networking protocols that you have heard of are published as RFCs. HTTP, DNS, DHCP, TCP, UDP, IPv4, IPv6, even email is an RFC. The protocols that we will analyze are all standardized as RFCs.

Read the Internet Engineering Task Force *Standards Process*. Answer Questions 1–2 on the assignment.

Read RFC 2026 Sections 1–3. Answer Questions 3–4 on the assignment.

Protocol Sequence Diagrams

We (humans) are visual creatures, we to visualize concepts. We use *Protocol Sequence Diagrams* to visualize protocols in action; i.e. visualize the flow of data between hosts. The below protocol sequence diagram depicts a conversation between Alice and Bob, where Alice is asking Bob what time it is.



Protocol sequence diagrams are read top-down with the vertical axis representing time, starting at 0. That is the start of the conversation is at the top of the diagram, begins at time 0, and the end of the conversation is at the bottom, ending at some time greater than 0. Each party in the conversation is represented in their own column, there can be as many columns as needed to represent the parties in the conversation. A downward sloping arrow is used to indicate a message being sent from one party to another party. The downward sloping arrow represents the passage of time; i.e. the amount of time it takes the message to get from sender to receiver. Timing information can be included or not, with the units being an appropriate unit of time based on the amount of time the transmission takes to get from sender to receiver.

A great thing about protocol sequence diagrams is that they can scale with the level of detail desired. We can abstract away details when dealing with Application layer protocols. We can add details and columns to depict lower layer Data Link layer protocols. We can scale protocol sequence diagrams to meet our needs.

With this knowledge, complete Questions 5–6 on the assignment.

Packets

It is simple to replace the messages above with packets; i.e. each message transmitted is a transmitted packet instead. But a packet has structure, there is more to a packet than just the Application layer message being sent. A packet is comprised of the following parts: header, payload, footer.

header [packet]
Beginning of a packet.
Includes administration data needed by the protocol to provide services.
payload [packet]
The message associated with the packet.
footer [packet]
Includes administration data needed by the protocol to provide services.

Based on the components of a packet, which part of a packet do you think will be transmitted first?

> The header is the first part of the packet that is transmitted, followed by the payload, and ending with the footer.

With this knowledge, complete Question 7 on the assignment.

The visualizations above depicted above each message as a single, complete chunk; i.e. each message was sent as a complete message between the communicating parties. In practice that is an inefficient use of a communications path, especially if the messages Alice and Bob are exchanging are large. More parties can communicate if large messages are split into smaller chunks, with each chunk being sent individually. This is called *fragmentation*, large messages are broken up into smaller fragments. Each fragment is sent across the network to the recipient, the recipient reassembles the fragments into the larger message. We will see that depending on network congestion multiple packets may be sent from the sender in rapid succession.

With this knowledge, complete Question 8 on the assignment.

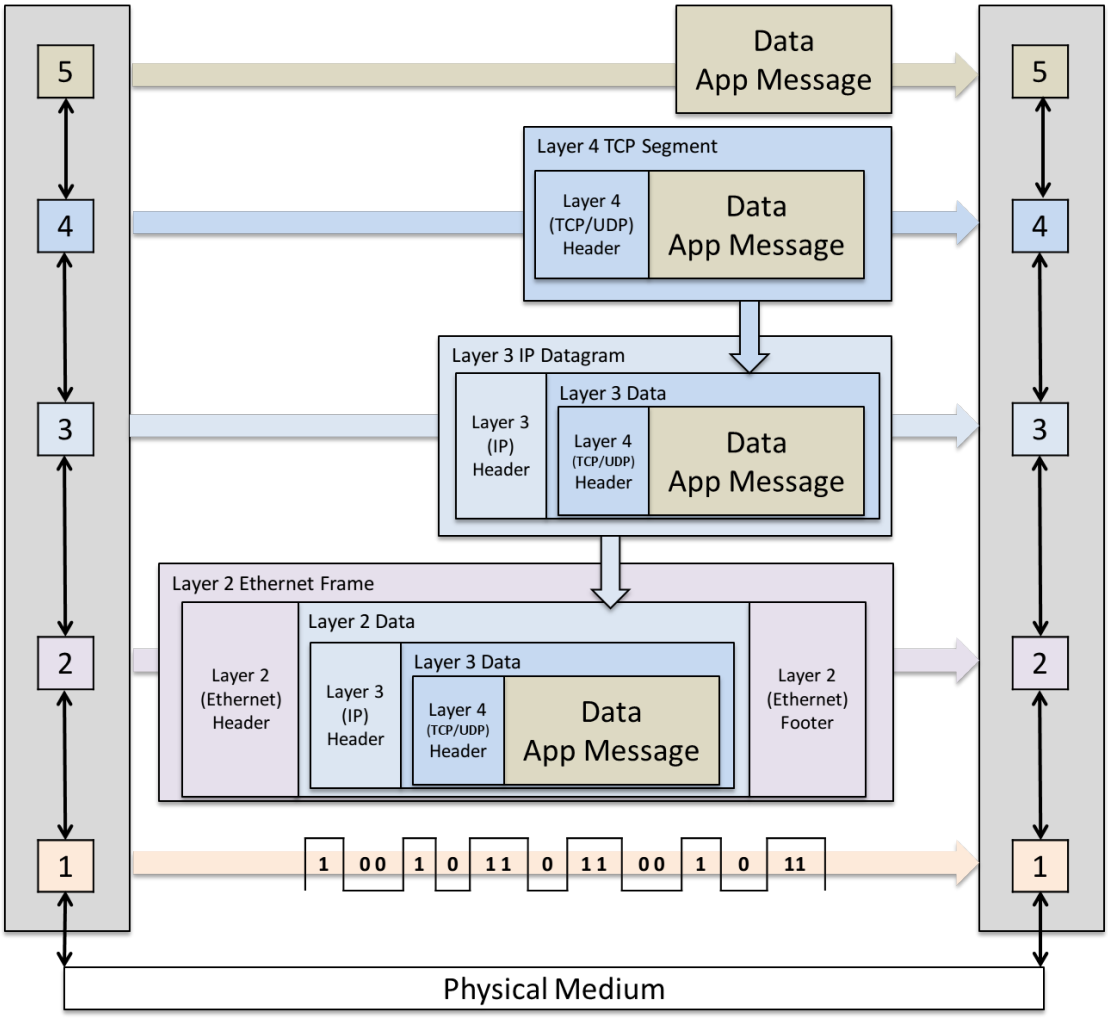
Data Encapsulation

At this point you might be thinking we talked about layers, but so far we have only visualized packets at a single layer. Each layer in a communications stack has the concept of a packet, each layer has a header and payload information. In practice only the Data Link layer uses a footer. The complete packet from an upper layer protocol becomes the payload of a lower layer protocol. A physical world

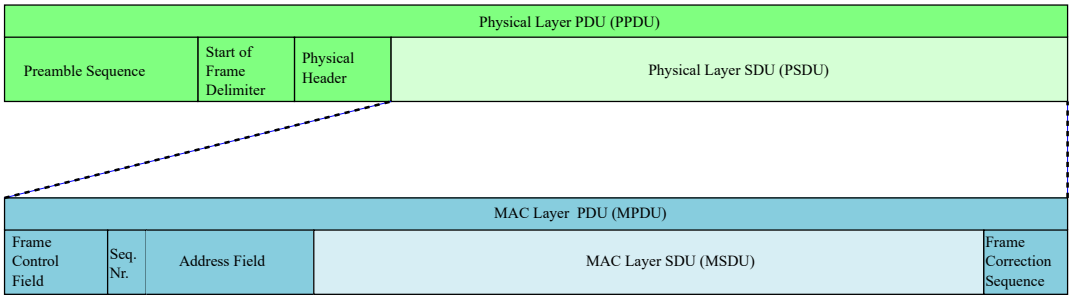
> **note: No Footers** In practice Data Link layer protocols use footers, and other layer protocols do not. Protocols at other layers are not prohibited from using footers. It's just that footers are excellent for error detection techniques called *cyclic redundancy checks*, and that is what many Data Link layer protocols use a footer for. Conversely the error detection techniques performed by higher layers do not need a footer.

example is Amazon putting *Kulrose and Ross* in a box and shipping the box to you; the book is the Application layer message which is the payload put into the box at the packaging layer. The address label on the box is the header information needed for the shipping layer.

The process of taking a higher layer message and wrapping a lower layer header/footer around the message is called *encapsulation*. As data moves down the communications stack each layer encapsulates the message from above with more data. As data moves back up the communications stack each layer deencapsulates (removes) the header and footer from the current layer before passing the payload up to the higher layer in the stack. The below diagram represents the encapsulation process as an Application layer message moves down the stack. The diagram depicts real protocols and uses terms that we will explore in greater detail.



The OSI model gives us generic terminology for a packet at an arbitrary layer of the stack and its payload. The generic term for the header, payload, and footer at an arbitrary later is *Protocol Data Unit* (PDU). The generic term for just the payload is *Service Data Unit* (SDU). The SDU at layer N is the PDU of layer N+1. You can think of the PDU as providing a service to the SDU. The below diagram depicts a PDU and SDU; again the diagram uses some terms that we will explore in greater detail, other terms used will be explored in the second networking course.



File:Pdu_and_sdu.svg. Wikimedia Commons. Retrieved 10 Sep 2018.

Like Iñupiaq having names for different types of snow, we have a specific name for a packet at each layer of the stack. At the Application layer the PDU is called a *message*. At the Transport layer the PDU is called a *segment*. At the Network layer the PDU is called a *packet* or *datagram*. At the Data Link layer the PDU is called a *frame*. At the Physical layer the PDU is called *bits* or a *signal*.

With this knowledge, complete Question 10 on the assignment.

This layering and encapsulation comes at a cost. Each layer provides a service, but that service comes at the cost of overhead. There is overhead in processing, and in how much data needs to be transmitted. Further protocols have a maximum payload size. As we encapsulate the data down the stack more and more of the Application layer message becomes a smaller portion of the overall PDU.

This leads to two relevant calculations: how many packets will the Application layer take up, and what percentage of a packet will be used for networking overhead. We can calculate the number of packets required by determining how many bytes are left for the Application layer message after accounting for the headers and footers of the Network layer and Transport layer per packet, and dividing that by the size of the Application layer message. Ethernet is the predominant wired Data Link, as such the common practice is to use the Ethernet protocol's payload size of 1500 bytes (octets) when calculating required number of packets and overhead. Remember we don't send half a packet, we round up any floating point remainders; i.e. take the Integer ceiling of the number of packets.

> **note:** *Data Link or No Data Link?* Whether the overhead from the Data Link layer is included in the calculations is dependent on the situation. When considering a packet that is sent across the Internet the overhead from the Data Link layer is not considered in the calculation. The rationale is that different Data Link layer protocols have different overhead costs. Additionally, there is no way for the two end hosts to know how many and what kind of Data Link protocols at the local network are being used. If you knew all of the Data Link protocols used as a packet travels between the communicating hosts then you could include that information in the calculations.

To calculate the networking overhead costs, we determine how many bytes were used for overhead per packet and multiply by the number of packets. That gives the total number of bytes used for networking overhead. We can divide the number of overhead bytes by the total bytes (networking overhead plus Application layer message size) to determine the what overall percentage of the traffic was devoted to networking overhead.

With this knowledge, complete the remaining questions in the *Data Encapsulation* section of the assignment.

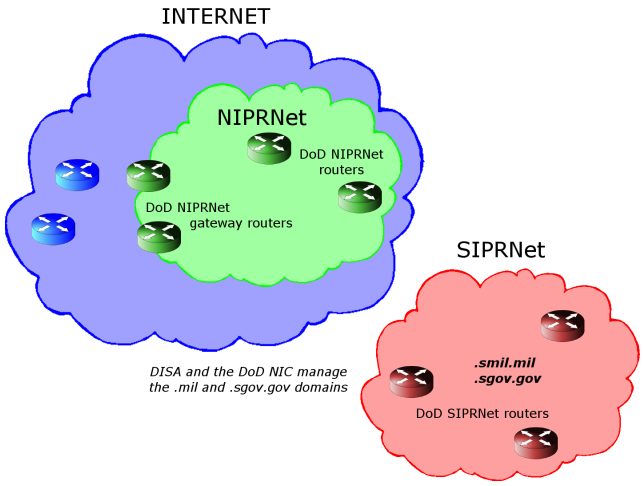
The above approaches were simple introduction problems, as we explore protocol details we will discuss additional factors we need to consider to determine data throughput and overhead.

So What?

We will explore the TCP/IP stack in detail, but the fundamental concepts we cover apply to all types of communication systems. Many DoD networks employ the exact same TCP/IP stack and protocols that we will cover in this course. In other words best practices for securing and operating TCP/IP stack technologies directly apply to DoD networks. This also means that vulnerabilities in TCP/IP stack technologies can directly apply to DoD networks. The Internet is a double edged sword, as operators we need to be aware of the capabilities and vulnerabilities that the Internet offers.

We need to be able to apply techniques, tactics, and procedures (TTPs) from the Internet to DoD communications networks. We need to apply lessons learned from the Internet and develop TTPs for Defensive Cyber Operations (DCO), and DoD Information Network Operations (DoDIN OPS). Similarly, we need to apply techniques, tactics, and procedures from the Internet in Offensive Cyber Operations (OCO).

in the Fleet: NIPRNet "Nippernet" is the colloquial name for the DoD subset of the Internet that carries sensitive but UNCLASSIFIED IP data. Access to the NIPRNet is tightly controlled: all data crossing the NIPRNet/Internet boundary must pass through a DoD-owned router, and hosts on the NIPRNet resolve names using DNS servers operated by the DoD Network Information Center. The DoD also owns and operates the SIPRNet (pronounced Sippernet), for classified data.



Both the NIPRNet (Non-secure Internet Protocol Router Network) and SIPRNet (Secret Internet Protocol Router Network) use the TCP/IP Stack that we will focus on in SY205. Ships and other war fighting platforms that you will operate are connected to the NIPRNet, and SIPRNet.

Additionally, there are communications systems used by military systems that do not follow the TCP/IP stack model. But, those communications systems still have to address the same fundamental problems that the TCP/IP stack does. We can apply the same fundamental concepts from the OSI model, and analysis and visualization techniques for non-TCP/IP stack communications systems.