Introduction- Video 1

Hello, my name is Rafail Portnoy. Welcome to computer networking. Today, we're going to look at introduction. We're going to get a feel for the terminology. We're going to have a more in-depth look at some of the aspects of the course a little bit later. We're going to use internet as an example to learn about computer networking. In fact, there are many other technologies, but Internet is so popular these days. It's a great way to learn about computer network and using that as an example. We're going to look at what is the protocol? What is the network edge? We're going to discuss host, access networks, and physical media. We're going to look at network core. What is the packet? What is the circuit? We're going to discuss computer performance on a network. Look at things like delays and loss and then finally we'll talk a little bit about the history and security.

What is the Internet-Video 2

What is the internet? Let's take a look at the nuts and bolts view. We have millions of connected devices. We call them hosts. Those are the systems that run network applications. We have communication links: fiber optic, copper, radio. We used the term called bandwidth, which defines our transmission rate. How fast we move through the internet. We have our packet switches. Those are the devices that move little chunks of data. In the internet world, they referred to as switches and routers. What are some of the fun internet appliances that we have? Picture frames. Toasters. Sling boxes. phones. Lately we've even seen cars being connected to the Internet. How great is that? We also have a different perspective on the Internet. We look at it as network of networks. We use different types of protocols you may have heard about TCP, IP, HTTP meaning you probably have used Skype and then there are different types of standards that guide the internet. Request for comments typically referred to as RFCs and IETF Internet Engineering Task Force.

A Service Review- Video 3

And We have a service view of the Internet. Infrastructure that provides services to our applications. We have to have some kind of a foundation to run our web, our emails, our games, our e-commerce, social networks. It also provides programming interfaces to the applications. Many years ago, all the apps were standalone. You had a personal computer and you ran an application on it. But now everything is interconnected so all of these different technologies have to talk to each other. We have to be able to provide the service typical to postal where we can take an information from one device push it through the network through the internet and it's going to land somewhere else across the world on another device.

What is Protocol- Video 4

What is a protocol? Well, as humans, we use protocols. We asked about the time. We have a question. We use it through introductions. Inside our networks, we also have different types of protocols. They allow us and guide our communication activities. In fact, protocols define the format, order of the messages sent and received among network entitles, and actions taken on a message transmission or receipt. For example, the human protocol could go something like, “Hi”, "Hi", "Got the time?", "Two o’clock." Network protocol, if you ask for a HTTP file, from some kind of a website would go like, TCP connection request, TCP connection response. You are going to send the commend and you are going to get the file.

Network Structure 5

Let's now look at network edge. Let's discuss end systems, access networks, and links in more details. Let's take a closer look at network structure. What's comprises of the network edge. Well, we have hosts, our clients, our servers. Servers often reside in the data centers. As an example, many of you may be using Gmail. Gmail servers sit in Gmail data centers whereas your computer houses the Gmail client. Access networks and physical media. Those are referred to as wired and wireless communication links and then finally we have the network core. We only have interconnected routers there. That's what comprises and builds the network of networks. Let's look up now, let's take another look at access networks and physical medium. How do we connect end systems to the edge router ? how do we connect our devices, our phones, our computers to the Internet ? Well, we use residential access networks. We use institutional access networks for schools or companies. Nowadays we use mobile access networks that connect us through the phones right at the Internet. We have to keep in mind a couple of things, such as what is the bandwidth beats per second? How fast do we move the information through the net? Is it shared or dedicated? Well, let's look at some of the examples. This is a cable network, which many of us may be using at home. It uses a technology called frequency division multiplexing which uses different radio channels different frequencies to transmit the information. Cable network is a hybrid fiber coaxial infrastructure. It's asymmetric, which means that the information going downstream to our houses moves at a much faster rate than it moves upstream. Different type of network infrastructures may include DSL. It's also important to remember the cable network is shared. Everyone in the neighborhood shares the same cable so when everybody gets on the Internet. Guess what? It slows down. Another example of the access net is our home network. That's what we use at home. I like everyone to think about what are the other human protocols you can think of and perhaps talk to your friends about that.

Access Networks- Video 6

Another example of the access network is our home network. Hey, look at this we have a wireless router. We have a router that connects us to the Internet. Many times, those are devices or plugged into the same box. We have wireless access point now we have speeds of up to 900 megabits per second moving the information back and forth. Wired Ethernet connections. Those are the ones that allow us to use the cable to plug into the internet. And, finally we use many of the different devices, TVs, phones, game consoles that connect through our home networks. Finally, on a larger scale, enterprise access networks primarily use Ethernet. Those are the ones that used in colleges, enterprises, law firms, and manufacturing facilities. They're the ones that use hard wired cables to connect different devices through. It's interesting to point out that the transmission rates vary and now we can transmit information up to 10 gigabyte per second.

Enterprise Access Networks- VIdeo 7

And finally, enterprise access networks. Also known as a defector Ethernet standard. Those are typically used in companies, universities, small or large organizations, they comprise up with different transmission rates. Many times, there is wireless access within the enterprise, but we still rely on our hardwired cabling across the organization to really deliver a consistent service. Today, most of the end systems typically connect into the Ethernet switch. If you are working at a company or sitting in the university at your desk, there is typically an institutional router or an organizational router which is a big device that connects all of the computers in that building or in that organization directly to the Internet.

Wireless Access Network- Video 8

And Finally let's look at wireless access networks. It's a shared wireless access through the medium that's available to all of us. We use wireless lens within the buildings. We use wide area wireless networks, which are provided typically by telco to connect our iPhones and Samsung Android devices. If you want to learn more about wireless access here is the link that you can go to the Wikipedia and learn everything from the transmission rates to the different type of information and different technologies that are used today. Let's take another look at the physical media. What is a bit? A piece of information that propagates between the transmission and receiver pairs. If you looked at the cable, that's actually what you would see. A number of different wires tied in together that allow us to move electrons by using electricity. What's the physical link? Well, it's something that lies between the transmitter and receiver. We use guided media, things like copper, fiber, or coax to move the signals through. We also have unguided media, for example, radio, and that's the technology that is used for wireless networks. Specifically, the guided media that is used mostly today is twisted pair. Two insulated copper wires, category five, category six, that are twisted together and allow us to move the electrons through. Coax and fiber are also different types of cables that are used to move the information through. Coaxial cable looks exactly like your TV cable, and it's a two cocentric copper conductors. It's bi-directional, and it's primarily used by broadband facilities such as cable internet.

Physical Media- Video 9a

Let's take a look at physical media. We have two types of media guided medium, where the signal propagates through a solid infrastructure copper fiber or coax cabling. We also have unguided media such as radio where the signal propagates freely. There is a physical link either cable or radio that lies between the transmitter and receiver. Finally, we have a bit, which is a piece of electrical signaling which propagates between the transmitter and receiver pairs. The factor we use twisted pair, which is two insulated copper wires inside a larger chunk of wires put together that allow us to connect computers together. Different types of category wiring allow for different transmission speeds. If we look at physical media such as coax and fiber, coaxial cables look exactly like our TV cables. It's two concentric copper conductors, which allows us to move bi-directional signaling in and out of the computers through the network. It's primarily used in broadband. Fiber optic cabling is a glass that carries light pulses where each light pole represents a bit. We usually use fiber optic cabling for high-speed operations. Fiber also has very low error rates because it's not subjected to electromagnetic induction, where the copper cabling is. If we look at radio as a physical medium, that's where we carry signals through electromagnetic spectrum. There is no physical wiring is bi-directional and it propagates through the environment. It's subjected the things like reflection obstruction of objects and interference.

Physical Media- Video 9b

There are different types of radio link types. There is terrestrial microwave. Local area networks that they used at homes or at universities or different enterprises. Wide area networks that primarily used for our phones and satellite connections which cover large geographical areas but should subject it to significant delays up to 270 milliseconds. You may think that's not that long, but actually in the world of networking. That's a huge delay. Finally, it brings us to the first engineering exercise of this course, let's look at the host that sends packets of data. Well, host takes the application message breaks it into smaller chunks, which we refer to as packets and then the length of that packet is something we refer to as L bits.

We then transmit that packet into the access network at the transmission rate R. The link transmission rate also known as the capacity also known as a length bandwidth is the parameters that are used to move the information through. We look at the first important definition of our network which is packet transmission delay. We need to know how long is going to take for us to move the packet from point A to point B, and we define and determine that rate as the L bits the length of the packets divided into the transmission rate of the channel. L over R bits over bits per second.

The Network Core- Video 10

We're now going to look at the network core. Let's discuss packet switching, network structure, and take a look at the circuit switching. Network core is the mesh of interconnected router. Packet switching means that with host breaks the application layer message into the packets. It then forwards packets from one router to the next across the links on path from source to destination. It's important to remember that each packet is transmitted at the full- length capacity.

Packet Switching- VIdeo 11

We use store-and-forward technique in packet switching. That means that the entire packet has to arrive at a switch fully before it gets transmitted on to the link to the destination. One hub numerical example for the transmission delay of five seconds would be if we take a packet of the length of 7.5 megabits and we divide it over a link with the transmission rate 1.5 megabits per second. The Antonian delay is usually determined as 2 L over R if we assume that there is ZERO propagation delay. We're going to spend a little bit more time later in the course discussing different types of delays.

Packet Switching- Video 12

Another important parameter to remember when we discuss packet switching is queuing delay and loss. When does loss occur? When does queuing delay occur? Well, if the arrival rate of the link exceeds the transmission rate of the output link for a period of time, packets will queue and eventually they will get trap. That’s what happens. That’s sometimes you see on your phones or on your computers when you connect to something and it takes longer time. That means we are in a traffic. We have to remember there are two key network functions when we discuss computer networking. It is routing and forwarding. Routing determines the source destination route taken by packets. Forwarding means that we move the packets from the router’s input interface into the appropriate router’s output interface.

13?

Network of Networks- Video 14

Let's look at our internet structure. Let's look and try to understand how is the network of networks is actually connected. Well, given the millions of ISPs and billions of computers, how do we connect them together? You may think why don't we just connect each ISPs to each other? Well, unfortunately that's not possible. The connection there are going to be so many connections that the network will is actually not going to be able to scale. Well, one option to connect all of the ISPs together is to have a central transit ISP. Wouldn't it be great to run the central transit ISP and have the economic power of connecting every computing network in the world? Doesn't really work that way. Well, another option is of course to have a little bit of a competition. So, we're going to break that ISP into a smaller ones, that ones can run some part of the world together and then have them interconnected. How would we do that?

Well, we would have internet exchange points and peering links that would allow those regional ISPs that are independent of each other connect the local internet service providers and then connect them with each other. Sometimes we also have to use regional ISPs that are larger than our local internet service providers but smaller than those global companies that connect us throughout the world. And finally, within our internet structure we have content provider networks. Google, Microsoft, Facebook, Akama. Those are the organizations that house the data, and they try to position it closer to the consumers. Lately they have been creating their own ISPs, so they can bring the content and the services closer to us. So, here's an example of what the Internet can look like. We have tier one ISPs. Those global organizations that connect many local ISPs throughout the world together. We could have Google or possibly. Facebook as content providers in our picture and then usually we interconnect all of this different size ISPs and different size networks through the internet exchange points. The content providers themselves as we could see are becoming tier one providers.

15?16?17?

Example of a Tier- Video 18

Here's an example of a tier 1 ISP Sprint. Everybody knows them for being a wireless provider but in fact Sprint owns a lot of cables which they use to interconnect their customers throughout the United States and then connect us to other tier 1 ISPs in Europe and Asia. Here's an example of how the different connections happen. You have routers that connect to and from the customers. We also have routers that connect within the Sprint backbone, and then we have routers that connect sprint to other network providers such as AT&T and possibly Verizon. All of these different ISPs and network providers, because besides the internet access some customers may choose to have private network, all of those ISPs have different points of presence, which allow us actually to build the network that connects multiple different entities with each other. If you run a company and you decide to connect different buildings of your company together so you could have a private network you may call in Sprint and say please can we have a connection of a specified rate because we want to be able to move the information together. That's how the big companies and universities use different service providers such as network is building the private networks for their own use as well as connecting to the internet. Internet Structure Now let's take a look at the network of networks. Our fundamental internet structure and systems connect to the internet via access ISPs. Internet service providers. We use residential ISPs, company ISPs, or university ISPs. In turn, our own Internet service providers must be interconnected as well. The resulting network of networks is very complex. It's interesting that it's actually being developed in the evolution that has gone through the economics and national policies. Let's take a step by step approach to see how the current internet structure is configured.

Packet Delay- Video 19

And it's really exciting to talk about the delay and loss in our networks. Let's look at this a little bit more specifically. How do loss and delay occur? Well, packets queue inside routers buffers. When the packet arrival rate - as we discussed - to the link temporarily exceeds the output link capacity, we have to store it somewhere. Think about a train station where a lot of trains are arriving at the same time they have to wait their turn to get into the train station. Very similar this is what happens on the network. There are four sources of packet delay. There is something called nodal processing and queuing delay. The difference between them is nodal processing delay is where we check for bit errors and typically it's very ,very, very, very small. Tiny.

Human delay is the time waiting and an output link for transmission. That depends on a congestion level of the router. As you can see on this picture. There is a transmission, propagation, nodal processing, and queuing. The other two, which are more important, and we're going to spend a little bit more time talking about them are transmission delay and propagation delay. Transmission delay, as we learned before, is where we have the length of the packet over the link bandwidth and that's how long it takes us to transmit the packet onto the link. Propagation delay is how long it takes our packet to move through the entire link. Those two are very different and both are very, very important

Caravan Analogy- Video 20

Let's look at the caravan analogy now to understand the transmission and propagation delays. Let's imagine that there are a number of cars, ten, that propagate at a hundred kilometers per hour. Decent speed. The tollbooth takes 12 seconds to service a car. We pull up. We pay the money. We continue to go. We're going to imagine that's a big transmission time. In our example, car would be bit and caravan would be a packet. The time to push the entire caravan through tolls onto the highway is going to be a hundred and twenty seconds, right. Twelve second delay times ten cars. Time for the last car to propagate from first to second tollbooth is a hundred kilometers over 100 km/h is an hour. so it's going to take a sixty two minutes to move this caravan of cars from tollbooth one to tollbooth two. Well, what happens if the cars propagate and the higher speed? A thousand kilometers per hour. I don't know any car would do that, but it's actually pretty interesting. If you will go through the calculations, we will actually determine that right after seven minutes the first car is going to arrive at the second booth. Three cars are still going to be at the first booth. If you remember when we discussed store and forward technology, even though we now have a much faster link to tollbooth, our transmission delay is still playing a big part in our speeds.

Queueing Delay- Video 21

And now let's take another look at the queuing delay. Well, if you ever dreaming an empty highway, you know you can go as fast as the speed limit allows you. But as there's more cars arrive, we actually slow down in a geometric regression. Similar things happen on a network. As the traffic intensity increases, we have to do more work to move the cars through. We have to do more work to move the bits through. There is a dependency not only related to the transmission delay in propagation delay, but also to the amount of traffic moving through our network.

Packet Loss- Video 22

Let's take another look at packet loss. Well, the preceding link in the buffer has a finite capacity. The waiting air inside the router gets filled very quickly. If we think about the doctor's office and a line at some point if the doctors are not moving fast enough that waiting area is going to keep filling up. Similar things happen on a network inside the router. When the packets arrived to a full queue, they have to be dropped. That's where the packet loss occurs. Which brings us to a throughput slide where we define the rate at which bits transferred between the sender and receiver. Even though we may have something called instantaneous rate. You may have seen advertisements from cable companies and our telecom company saying, "we can give you 300 megabits per second, 400 megabits per second." We all know that's not really true. It depends on how busy the network is. We look at the throughput as an average rate over a longer period of time. As an example, inside in an Internet scenario when we discuss the throughput. We can see that the larger pipes are needed at the core because that's where the consolidated traffic coming from all of our different enterprises and universities and the follows phones are coming from the endpoint devices.

Protocol Layers- Video 23

Well, now the time has come to talk about the protocol layers and the service models. Networks are inherently complex. They are built of many different pieces. There are hosts. There are routers. There is different links. There is different applications. There is different hardware. How do we organize the structure of the network? How do we make all of these elements to work together? Well, we actually use layering approach. As an example, if we think about the organization of the air travel, it's a series of consecutive loosely coupled steps. You have to purchase a ticket first. You have to check in your baggage. You have to go to the gates. Get under the airplane and then somebody is going to route our airplane through the air until to our destination. We then going to go through the reverse procedure and unloaded the gates. Get the baggage and then possibly complain about our ticket.

Layering of Airline- Video 24

Layering of airline functionality allows us to implement all of these different processes independently of each other, but yet being dependent. Well, it allows us to do not to have redundancy in the system. If you get to the gate, we can already be sure that your baggage has been checked in and your ticket has been purchased. If you make it to your destination, you are exiting the gate. We would know that your baggage has been checked your runaway takeoff process has been completed. So, we're able to implement this loosely coupled functions, somewhat independently, but yet relying on each other. This allows us to change one of the service elements without changing the integrity of the entire process.

Layering and the Internet 25

Why do we choose layering? Well, dealing with complex systems allows us to create a reference model for the discussion. We can have ease of maintenance within each of those elements without addressing the overall integrity of the procedure. We all have seen aircrafts been taken off the service for maintenance. It doesn’t change our modular approach of air travel. We still have to go through the same routines. We still have to purchase the ticket. We still have to check in the baggage. Layering allows us to deal with a very complex system without actually addressing the entire system as one but rather as making each individual element work independently. Internet protocol stack is in fact a number of different layers. We have application layer, which supports network applications. You may have heard the term HTTP, SNTP or FTP. Those are all network applications. They rely on a transport layer which is process to process data transfer. Things like TCP and UDP which stands for the transmission control protocol and user datagram protocol. That layer then relies on a network layer to route our datagram from source to destination. That is where the IP routing takes place. We then rely on a link layer. Finally rely on a physical layer, which moves our bit through the wire.

ISOOSI 26

While a regional layered reference network model was called ISO OSI reference model and which stands for the open system interconnect. It had substantially more layers. There was a presentation layer and a session layer. Those layers are now missing in internet stack. What really happened? Well, with the proliferation of the technology, we can integrate those layers, those functions, that we had to call out into the system. We have faster processors. We have more memory. We don't have to have those layers anymore. This is similar toward before to purchase the ticket you have to go to the airport, stand in the counter, and buy things and now you can order through the internet. So in the internet stack those two functions are now implemented as part of our larger stack and as part of our application layer within the internet stack.

Network Security- Video 27

Let's take a look at network security. The field of network security covers substantially number of different areas. How can bad actors attack our computers? How can we defend the network against those attacks? How can we design architectures and structures to make the networks immune to the attacks? It's important to remember the original o of the internet did not have security in mind. We just decided we are going to have a group of mutual trusted users connected together through transparent network. Over the years, the internet protocol designers had to be playing catch up to ensure the security exists at every single layer.

Network Security- Video 28 (?)

Bad Guys Malware- Video 29

Bad road at rogue actors can put malware into the host via the internet. Malware can get into the host either as a virus which is a self-replicating infection by receiving in executing an object or as a warm, which is a self-replicating infection by passively receiving an object that gets itself executed. Spyware malware can record keystrokes, websites visited, or upload information into different rogue sites. Finally, infected hosts can be enrolled in a botnet which are used for spam which then can generate something called DDoS attacks, distributed denial-of-service attacks. What is it? Well, denial of service attack means that the attackers make resources such as servers or bandwidth unavailable for legitimate traffic by overwhelming our hosts with bogus traffic, number of different requests. Imagine if a group of people is asking you questions all the time before you get a chance to answer, you get overwhelmed with information. That's exactly what the distributed denial of service attack is.

Bad Guys Packet- Video 30

Well, bad actors can also sniff packets either through the wired network which is usually much harder or through the wireless. That's why it's important if you go and connect to a wireless host somewhere in Europe use encryption because somebody can get a hold of your password. Finally, bad actors can also use fake addresses pretend they are someone else on the Internet. We don't know where the host is and they can use fake information to position themselves as somebody we expect the information from, steal it, and then use it against us or someone else.

Conclusion 31

Well, we covered tons of materials in this lesson. We looked at the Internet. We discussed what the protocol is. We looked at the network edge, core, access network. Discussed a little bit about packet switching. Looked at the performance, delay, and throughput. Discussed layering service model and touching security. Wow, this was a lot of stuff. Thank you for being with us. Goodbye. We finally see the picture of how all these different layers work together. We called this process encapsulation. Our source, the host, takes all of the five different layers. In every layer, we add a header to the original message and we push it through the network. At our destination reverse process takes place, where each layer individual headers are striped. The message can get push through to the application and use.

It's important to remember that end systems, our hosts, use all of our different service layers, such as application, transport, network, link, and physical. Our network devices only use link and physical if it is a switch. Network, link, and physical, if it is a router. We will learn more about why is that in the later chapters.