Network Fundamentals and Security

By Neil Bloomberg

Bowie Computer Club
Spring 2018

INTRODUCTION

This presentation will cover the fundamentals of Computer Networks, explain how the Internet works and some fundamental concepts of Security.

AGENDA

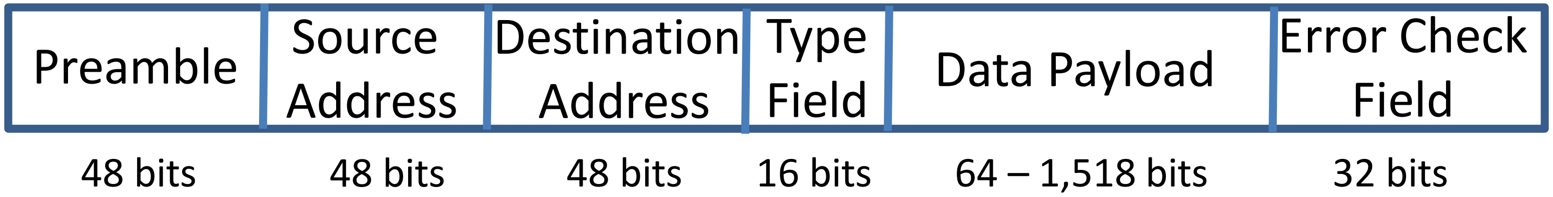
- Introduction of the Packet
- Network Modeling and Encapsulation
- Concept of Routing
- Security
- Q & A

Acknowledgements etc.

→All Click art used in this presentation was obtained from Wikipedia unless otherwise noted.

→ **Slide Take-Away Points are designed with an Arrow and highlighted at the bottom in bold RED.**

Introduction – A Packet (IPV4)

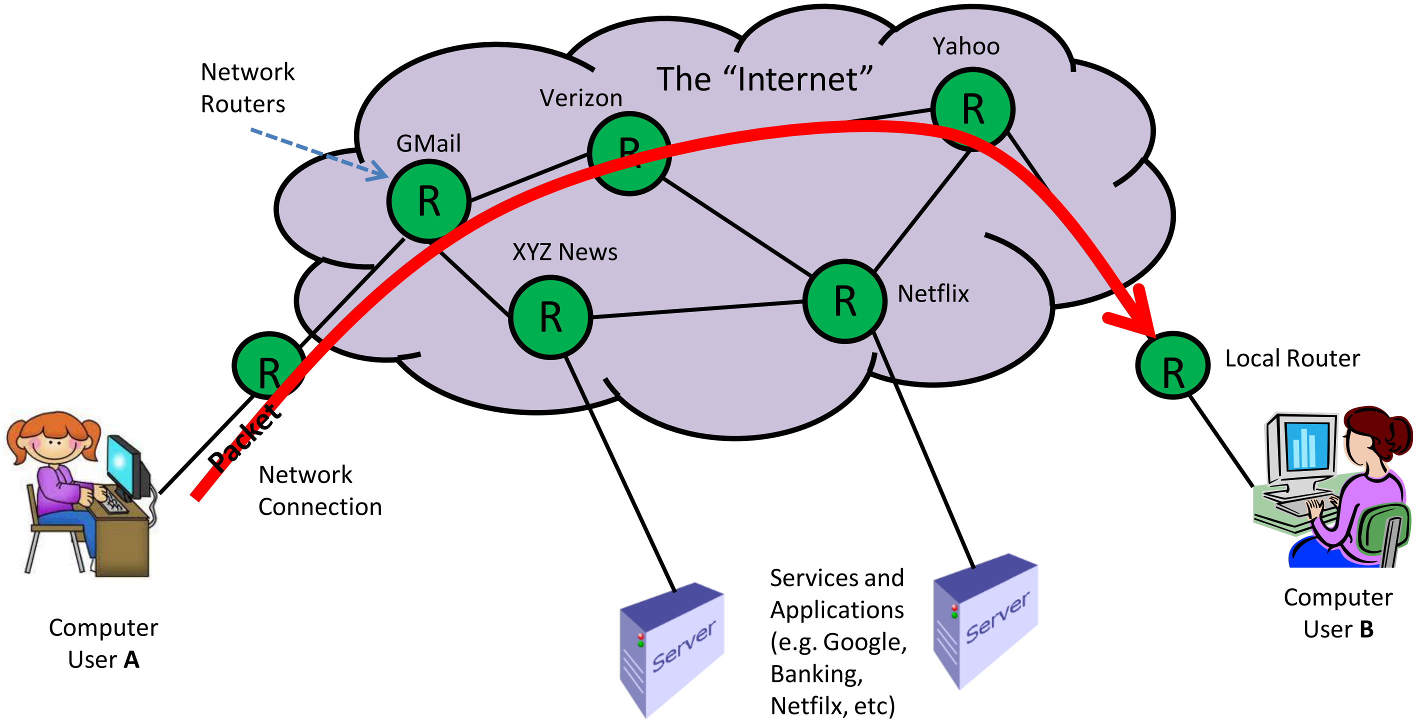


Preamble	Source Address	Destination Address	Type Field	Data Payload	Error Check Field
48 bits	48 bits	48 bits	16 bits	64 – 1,518 bits	32 bits

The Packet is the basic unit of information used to send data between two or more points within a Network:

- **Preamble** – 48 bits of alternating ‘1’s and ‘0’s ending with ‘11’ used to Synchronize the data at the receiving end.
- **Source Address** – A unique 48 bit Address of the sending device.
- **Destination Address** – A unique 48 bit address of where the packet is going.
- **Type Field** – A 16 bit value that specifies the Type of Payload within the packet (e.g. IP Payload, ICMP packet, Routing Information Packet, etc)
- **Data Payload** – The data type specified by the Type Field.
- **Error Check Field** – Typically a 32 bit “Cyclic Redundancy Check” mathematical equation used to detect single bit and multibit errors within the packet.

The Network



→ Routers are used to deliver Packets of information to the proper destination based upon either the least amount of hops or least congestion.

Definitions

- **Packet** – The basic unit of information exchanged between two entities on a Network.

- **Ethernet –** Is a Network communications technology that uses Packets based upon a specific set of rules to access a specific type of medium (fiber, coax, cables…) for the purposes of sending and receiving information. Based upon the IEEE 802 Standards.

- **Encapsulation** – Information contained in the “Payload” section of a packet.

- **Routing** – Getting information between two or more points within the Network based upon the IP Address within the Packet. This is done using Routers.

Ethernet Evolution Timeline
1970s to today

1973 Metcalfe & Boggs of Xerox PARC invented ALOHA packet-based network access protocol over a wired shared medium

→ 3 Mb/s operation

1982 "The Ethernet Blue Book" Digital, Intel, Xerox (DIX)

→ 10Mb/s operation based on the Xerox PARC concepts

1985 IEEE 802.3 Carrier Sense Multiple Access w/ Collision Detection (CSMA/CD)

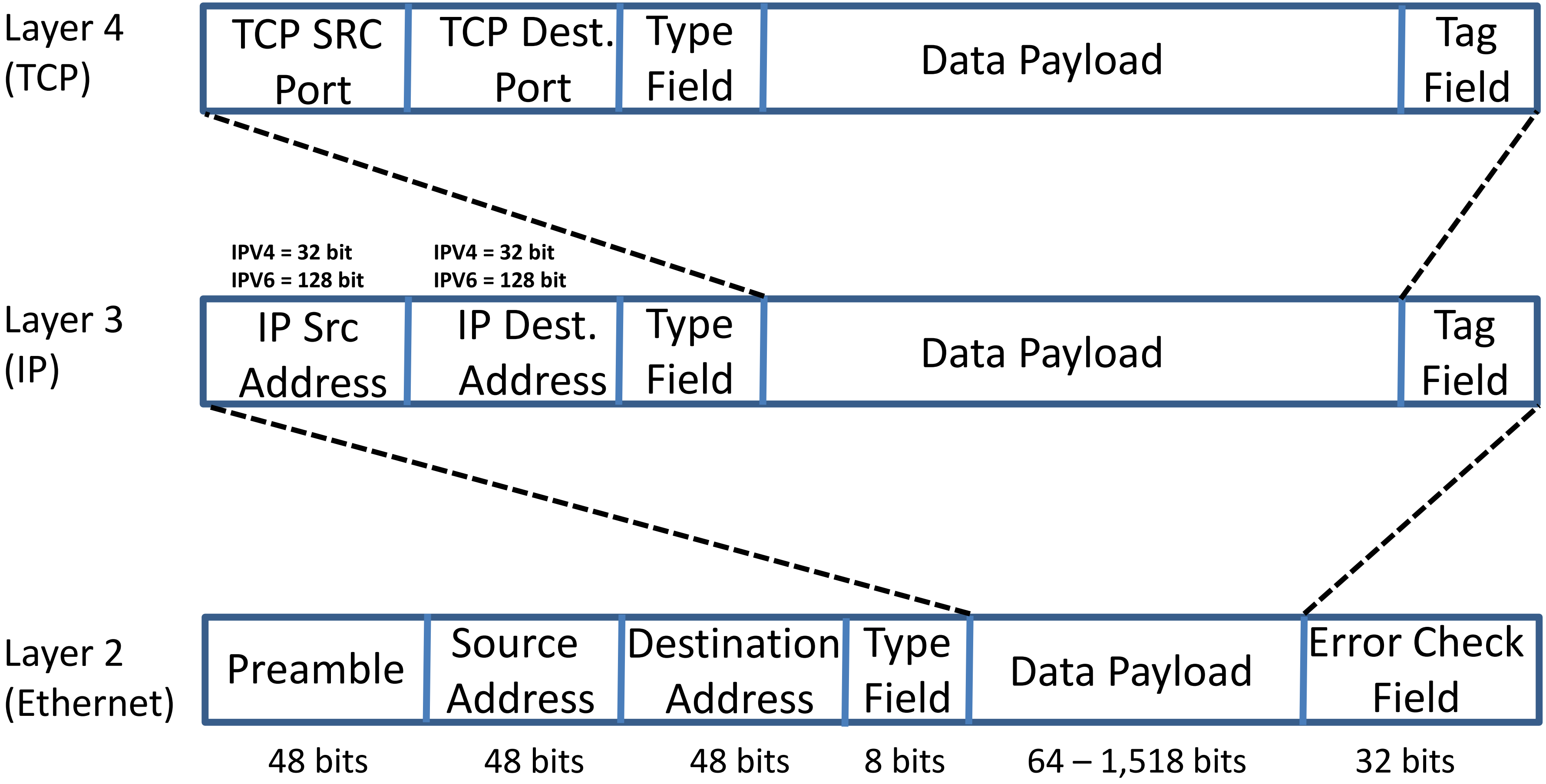
→ Formal standards definition, based on "Blue Book"

1999 Gigabit Ethernet standards ratified for use over copper twisted pair; vendors also implement fiber optic versions; 1000Base-T

→ IEEE 802.3ab

2000's Fiber standards ratified for single and multimode fiber; speeds evolve to 10, 40 and (eventually) 100Gbps

Data Encapsulation



Layer 4 (TCP)

TCP SRC Port	TCP Dest. Port	Type Field	Data Payload	Tag Field

Layer 3 (IP)

IP Src Address	IP Dest. Address	Type Field	Data Payload	Tag Field

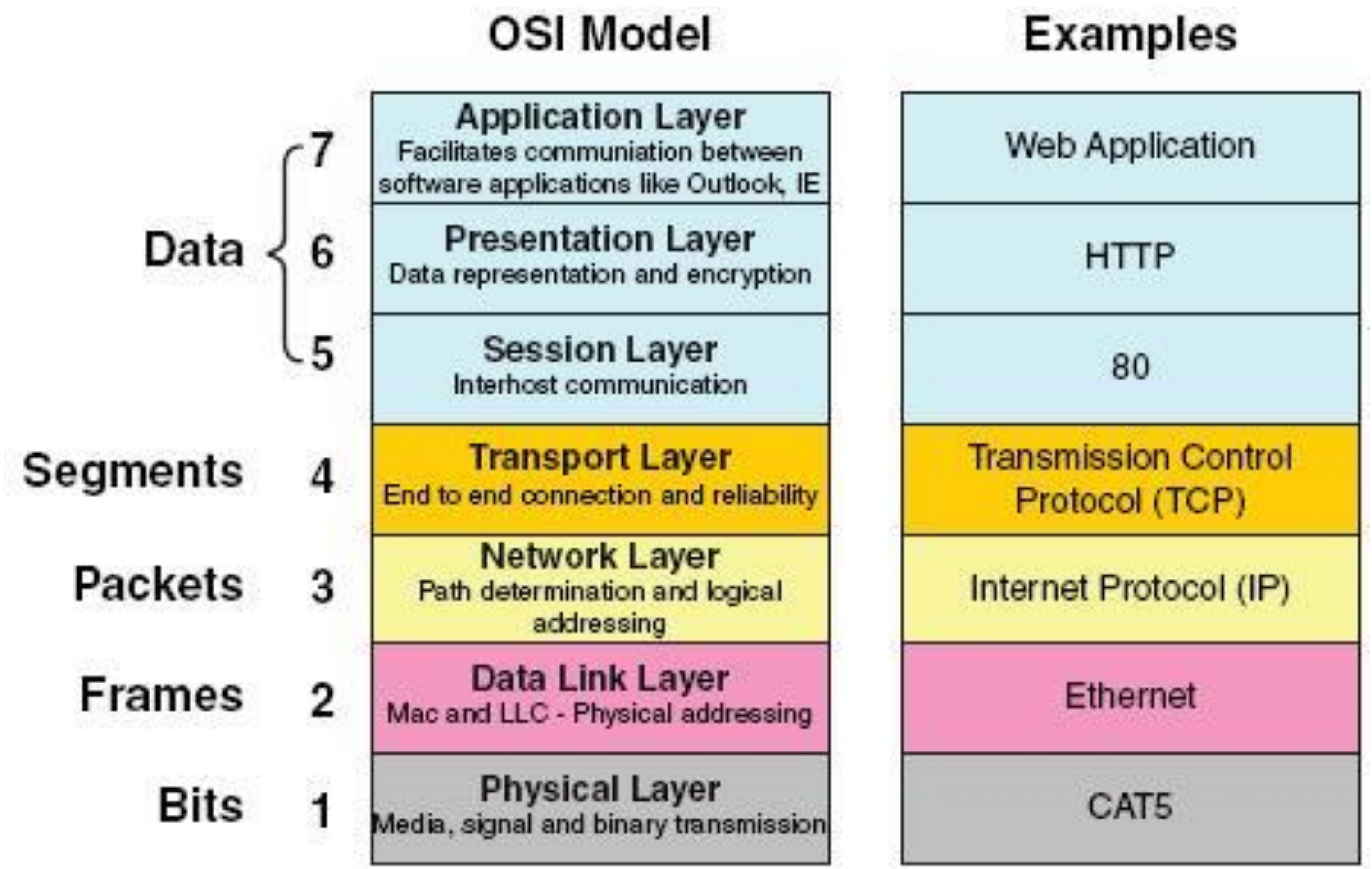
IPV4 = 32 bit
IPV6 = 128 bit
	IPV4 = 32 bit
	IPV6 = 128 bit			

Layer 2 (Ethernet)

Preamble	Source Address	Destination Address	Type Field	Data Payload	Error Check Field
48 bits	48 bits	48 bits	8 bits	64 – 1,518 bits	32 bits

→ Data Encapsulation is where one unit of information is contained within another unit of information.

OSI Network Layer - Model



		OSI Model	Examples
Data	7	**Application Layer** Facilitates communiation between software applications like Outlook, IE	Web Application
	6	**Presentation Layer** Data representation and encryption	HTTP
	5	**Session Layer** Interhost communication	80
Segments	4	**Transport Layer** End to end connection and reliability	Transmission Control Protocol (TCP)
Packets	3	**Network Layer** Path determination and logical addressing	Internet Protocol (IP)
Frames	2	**Data Link Layer** Mac and LLC - Physical addressing	Ethernet
Bits	1	**Physical Layer** Media, signal and binary transmission	CAT5

→ Computer Network Applications follow a standardized layer model

Definitions

- **MAC Address** – The media access control **address** (**MAC address**) of a device is a unique identifier assigned to network interfaces for communications at the data link layer 2 of a network segment. **MAC addresses** are used as a network **address** for most IEEE 802.x network technologies, including Ethernet and Wi-Fi.

- **Switch** – Packets are received and sent from one port to another based upon the Destination MAC Address – Layer 2.

- **Router** – A Hardware Device that receives packets from one port and sends it to another port based upon an IP Address.

- **Gateway**– A hardware device that acts as a "gate" between two **networks**. It may be a router, firewall, server, or other device that enables traffic to flow in and out of the **network**. While a **gateway** protects the nodes within **network**, it also a node .

- Dynamic Host Configuration Protocol (**DHCP**) is a network protocol that enables a server to automatically assign an IP address to a computer from a **defined** range of numbers (i.e., a scope) configured for a given network.

TCP and UDP Protocols

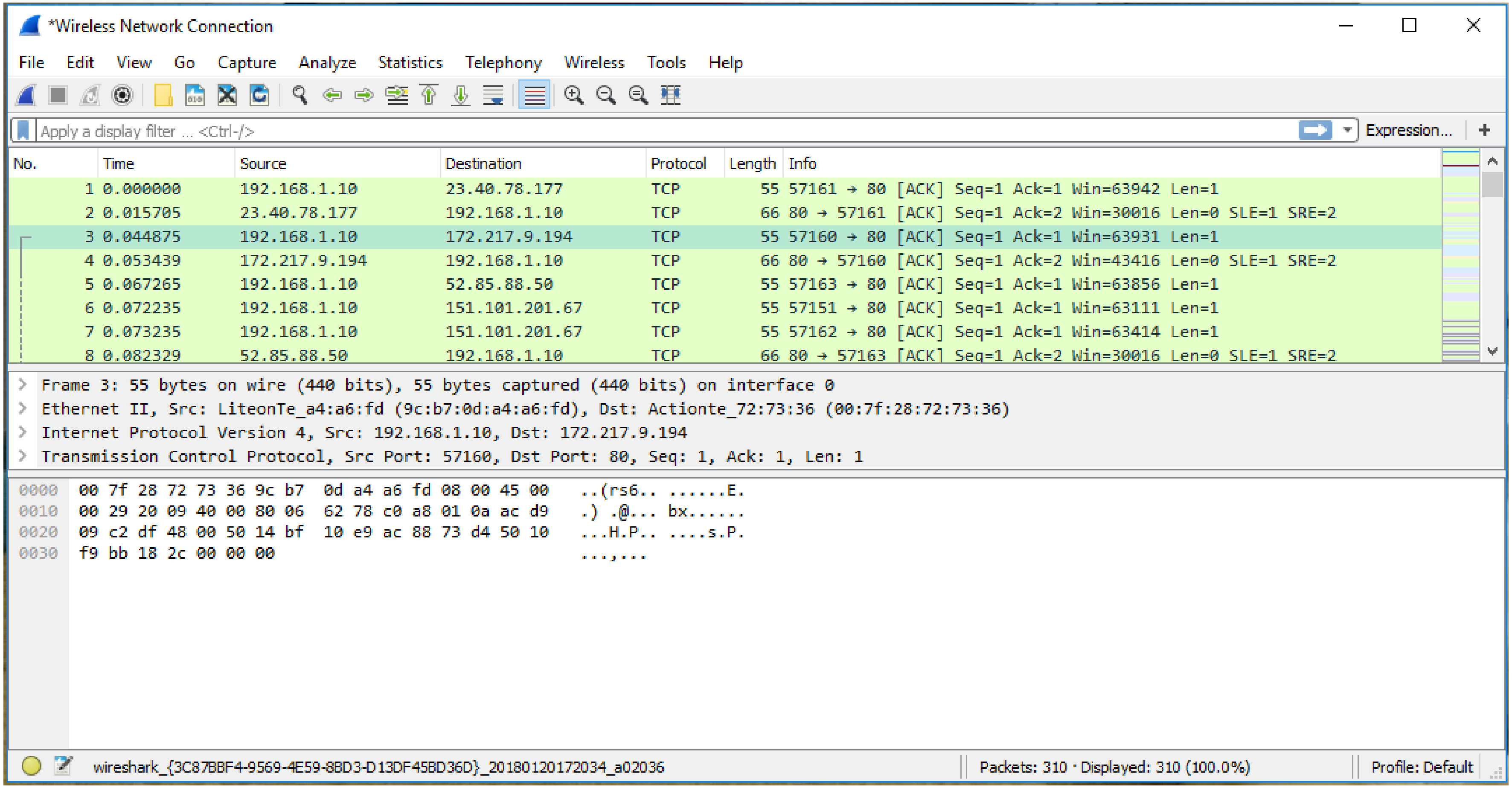
TCP – Transmission Control Protocol is a acknowledge protocol that involves a series of messages (handshakes) between the sender and receiver to ensure data transmission is received. Examples of TCP protocols are HTTP web browsers, SMTP Mail Protocol, FTP File Transfer Protocol.

UDP – Universal Datagram Protocol is a simple one way transmission of data between the sender and the receiver. Example of UDP protocols are: NTP Time Protocol, SNMP network Management, DNS Directory Name Services.

ICMP - Internet Control Message Protocol. It is an extension to the Internet Protocol (IP) Layer 3. Aka. a “ping”. Used to see if a device is reachable as well as delay time to reach the device.

→ TCP is used when data reliability is needed.

Packet Capture Example


*Wireless Network Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.1.10    23.40.78.177    TCP      55 57161 → 80 [ACK] Seq=1 Ack=1 Win=63942 Len=1
   2 0.015705  23.40.78.177    192.168.1.10    TCP      66 80 → 57161 [ACK] Seq=1 Ack=2 Win=30016 Len=0 SLE=1 SRE=2
   3 0.044875  192.168.1.10    172.217.9.194   TCP      55 57160 → 80 [ACK] Seq=1 Ack=1 Win=63931 Len=1
   4 0.053439  172.217.9.194   192.168.1.10    TCP      66 80 → 57160 [ACK] Seq=1 Ack=2 Win=43416 Len=0 SLE=1 SRE=2
   5 0.067265  192.168.1.10    52.85.88.50     TCP      55 57163 → 80 [ACK] Seq=1 Ack=1 Win=63856 Len=1
   6 0.072235  192.168.1.10    151.101.201.67  TCP      55 57151 → 80 [ACK] Seq=1 Ack=1 Win=63111 Len=1
   7 0.073235  192.168.1.10    151.101.201.67  TCP      55 57162 → 80 [ACK] Seq=1 Ack=1 Win=63414 Len=1
   8 0.082329  52.85.88.50     192.168.1.10    TCP      66 80 → 57163 [ACK] Seq=1 Ack=2 Win=30016 Len=0 SLE=1 SRE=2
```

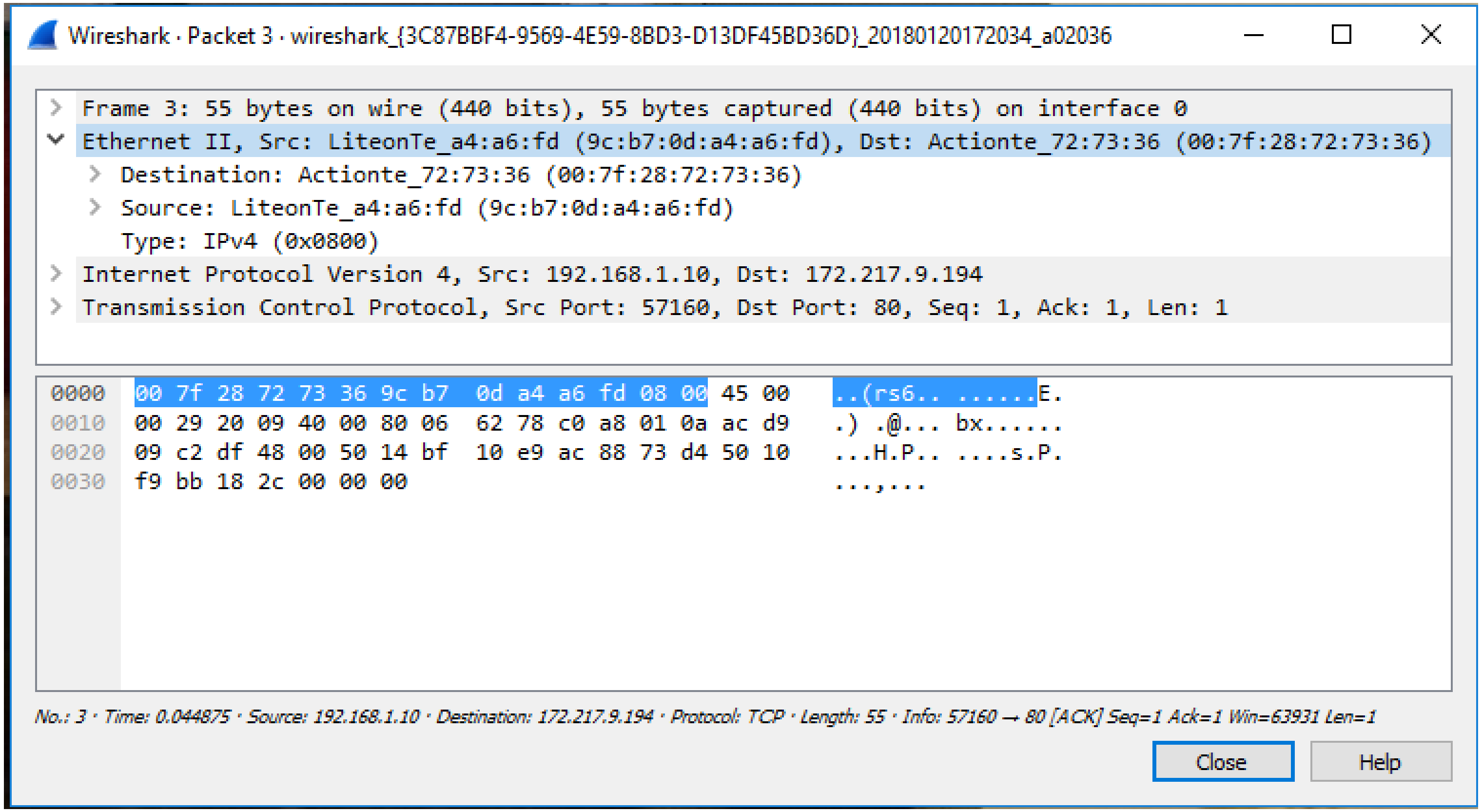
```
> Frame 3: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: LiteonTe_a4:a6:fd (9c:b7:0d:a4:a6:fd), Dst: Actionte_72:73:36 (00:7f:28:72:73:36)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 172.217.9.194
> Transmission Control Protocol, Src Port: 57160, Dst Port: 80, Seq: 1, Ack: 1, Len: 1
```

```
0000  00 7f 28 72 73 36 9c b7  0d a4 a6 fd 08 00 45 00   ..(rs6.. ......E.
0010  00 29 20 09 40 00 80 06  62 78 c0 a8 01 0a ac d9   .) .@... bx......
0020  09 c2 df 48 00 50 14 bf  10 e9 ac 88 73 d4 50 10   ...H.P.. ....s.P.
0030  f9 bb 18 2c 00 00 00                               ...,...
```

wireshark_{3C87BBF4-9569-4E59-8BD3-D13DF45BD36D}_20180120172034_a02036 | Packets: 310 · Displayed: 310 (100.0%) | Profile: Default

→ The above example shows the various TCP packets on the home computer Network using a packet analyzer.

Details of TCP Packet



Wireshark · Packet 3 · wireshark_{3C87BBF4-9569-4E59-8BD3-D13DF45BD36D}_20180120172034_a02036

```
> Frame 3: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
v Ethernet II, Src: LiteonTe_a4:a6:fd (9c:b7:0d:a4:a6:fd), Dst: Actionte_72:73:36 (00:7f:28:72:73:36)
   > Destination: Actionte_72:73:36 (00:7f:28:72:73:36)
   > Source: LiteonTe_a4:a6:fd (9c:b7:0d:a4:a6:fd)
     Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 172.217.9.194
> Transmission Control Protocol, Src Port: 57160, Dst Port: 80, Seq: 1, Ack: 1, Len: 1
```

```
0000  00 7f 28 72 73 36 9c b7  0d a4 a6 fd 08 00 45 00   ..(rs6.. ......E.
0010  00 29 20 09 40 00 80 06  62 78 c0 a8 01 0a ac d9   .) .@... bx......
0020  09 c2 df 48 00 50 14 bf  10 e9 ac 88 73 d4 50 10   ...H.P.. ....s.P.
0030  f9 bb 18 2c 00 00 00                               ...,...
```

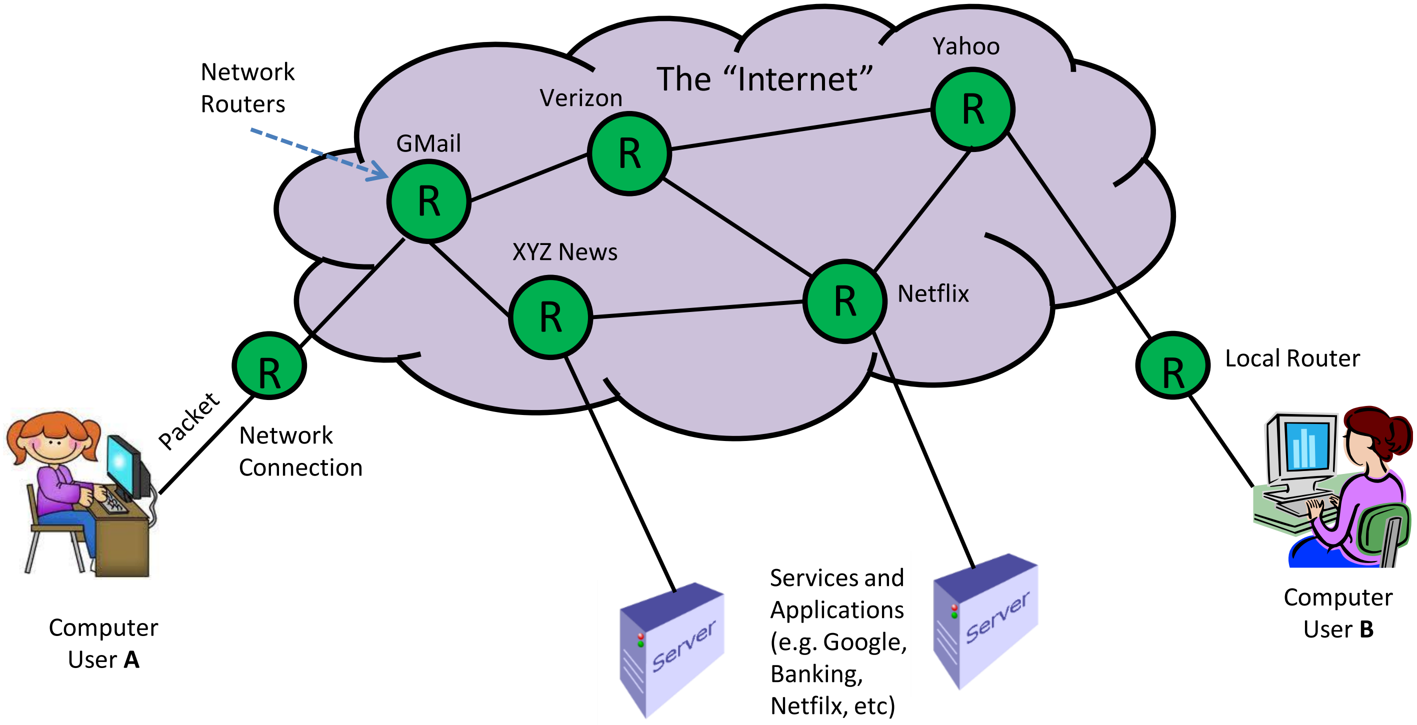
No.: 3 · Time: 0.044875 · Source: 192.168.1.10 · Destination: 172.217.9.194 · Protocol: TCP · Length: 55 · Info: 57160 → 80 [ACK] Seq=1 Ack=1 Win=63931 Len=1

→ The highlighted area shows the MAC Source and Destination Address of the Packet.

Routing

Simply put, Routers or Routing involves getting digital information from the sender to the intended final destination. With a Network that now spans the entire globe, this can be quite a challenge. To accomplish this, Routing Management protocols have been created as a means for routers to communicate to each other exchanging information such as: who are my router neighbors, data congestion between routers, and a list of IP addresses that map to Network Domains.

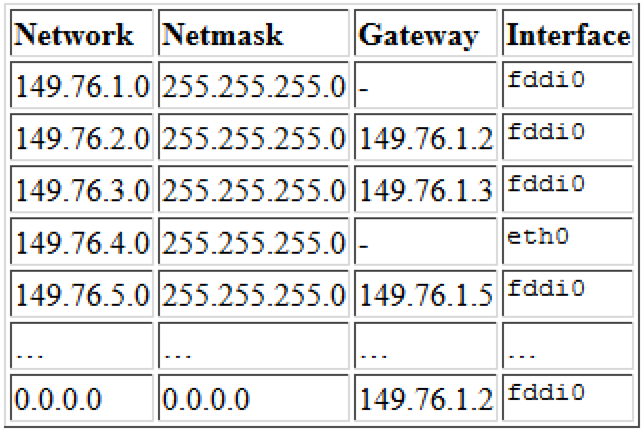
The Network



→ **Routers exchange information between each others to provide the quickest path for message delivery.**

Routing Tables

“In computer networking a **routing table**, or **routing information base (RIB)**, is a data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. The routing table contains information about the topology of the network immediately around it. The construction of routing tables is the primary goal of routing protocols. Static routes are entries made in a routing table by non-automatic means and which are fixed rather than being the result of some network topology "discovery" procedure.” *(2018, wikepedia.com)*



Network	Netmask	Gateway	Interface
149.76.1.0	255.255.255.0	-	fddi0
149.76.2.0	255.255.255.0	149.76.1.2	fddi0
149.76.3.0	255.255.255.0	149.76.1.3	fddi0
149.76.4.0	255.255.255.0	-	eth0
149.76.5.0	255.255.255.0	149.76.1.5	fddi0
...	...	...	...
0.0.0.0	0.0.0.0	149.76.1.2	fddi0

→ Using Routing Protocols to identify Routing Neighbors, they put together tables used to maximize routing efficiency.

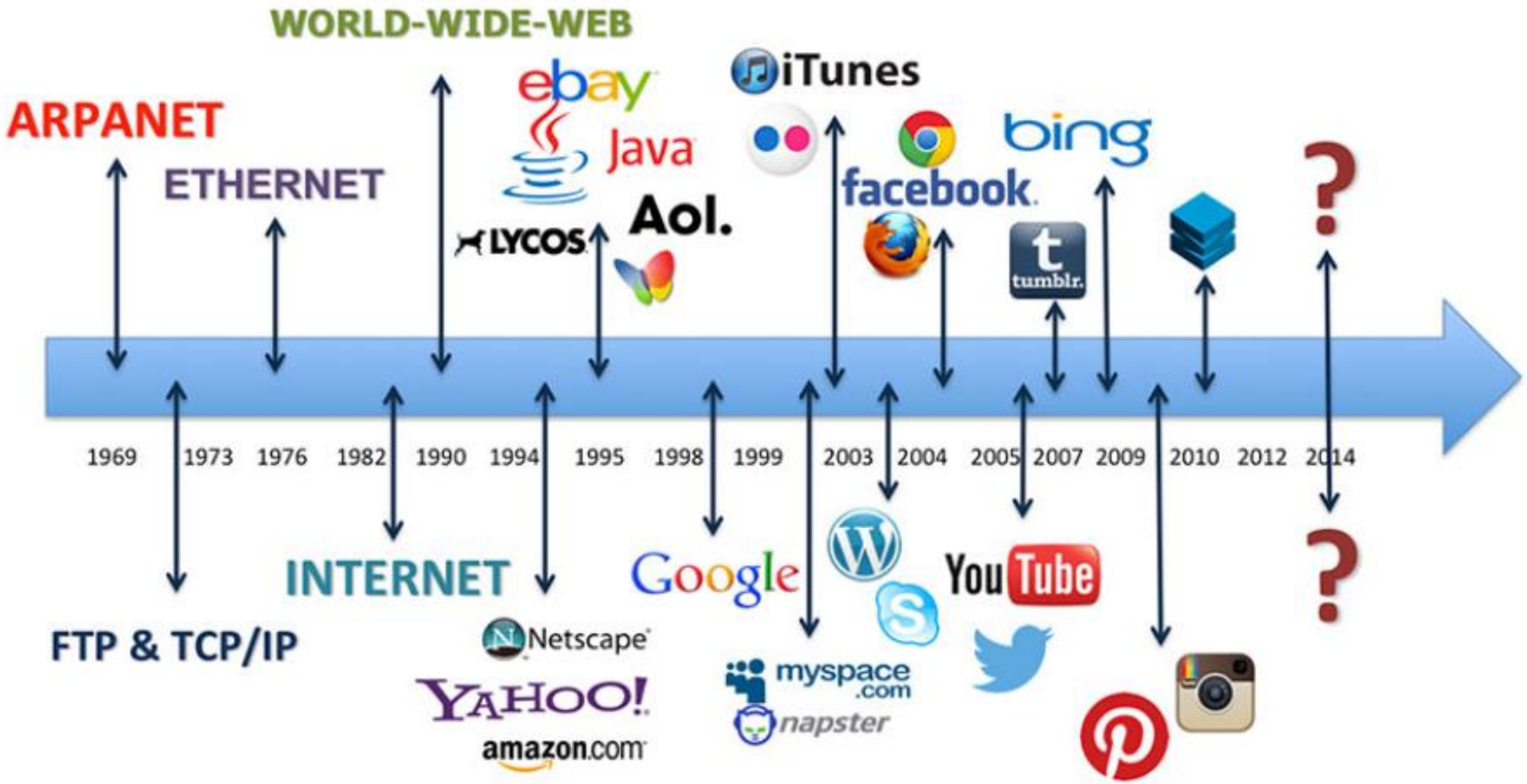
Routing Protocols

Routing protocols, according to the OSI routing framework, are layer management protocols for the network layer, regardless of their transport mechanism:

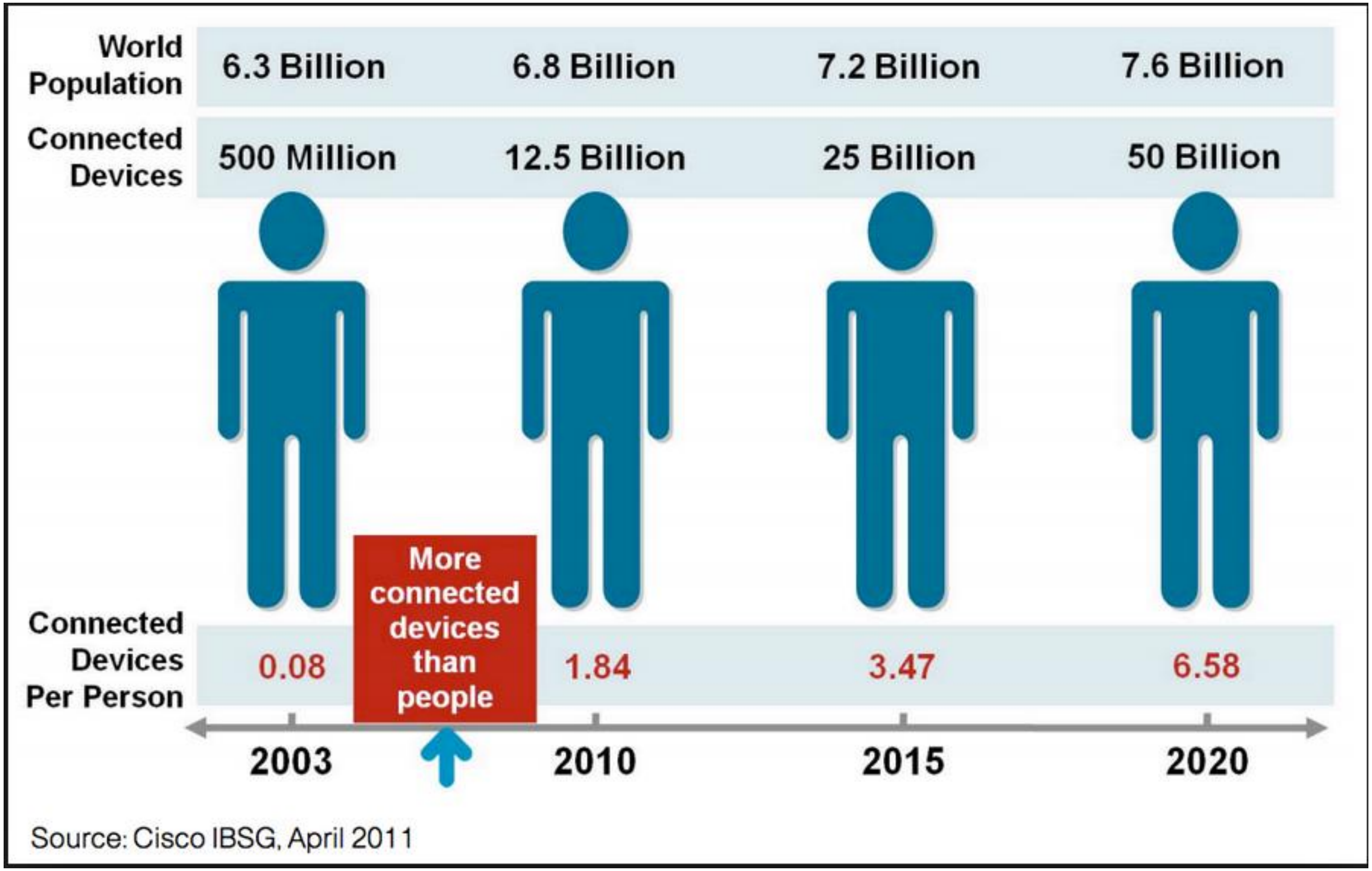
- **IS-IS** runs on the data link layer (Layer 2)
- Open Shortest Path First (**OSPF**) is encapsulated in IP, but runs only on the IPv4 subnet, while the IPv6 version runs on the link using only link-local addressing.
- IGRP, and EIGRP are directly encapsulated in IP. EIGRP uses its own reliable transmission mechanism, while IGRP assumed an unreliable transport.
- Routing Information Protocol (**RIP**) runs over the User Datagram Protocol (UDP). Version 1 operates in broadcast mode, while version 2 uses multicast addressing.
- **BGP** (Boarder Gateway Protocol) runs over the Transmission Control Protocol (TCP).

→ Sample of common routing protocols. Don't spend to much time on this slide!

The Internet of Things (IoT) History



The Internet of Things (IoT)



	2003	2010	2015	2020
World Population	6.3 Billion	6.8 Billion	7.2 Billion	7.6 Billion
Connected Devices	500 Million	12.5 Billion	25 Billion	50 Billion
Connected Devices Per Person	0.08	1.84	3.47	6.58

More connected devices than people

Source: Cisco IBSG, April 2011

IP Version 4

IPv4 (***I**nternet **P**rotocol **V**ersion **4***) is the fourth revision of the Internet Protocol (IP) used to identify devices on a network through an addressing system. The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks.

IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bit address scheme allowing for a total of 2^32 addresses (just over 4 billion addresses). With the growth of the Internet it is expected that the number of unused IPv4 addresses will eventually run out because every device -- including computers, smartphones and game consoles -- that connects to the Internet requires an address.

IP Version 6

A new Internet addressing system Internet Protocol version 6 (IPv6) is being deployed to fulfill the need for more Internet addresses. IPv6 (*Internet **P**rotocol **V**ersion **6***) is also called IPng (***I**nternet **P**rotocol **n**ext **g**eneration*) and it is the newest version of the Internet Protocol (IP) to replace the current version of IPv4.

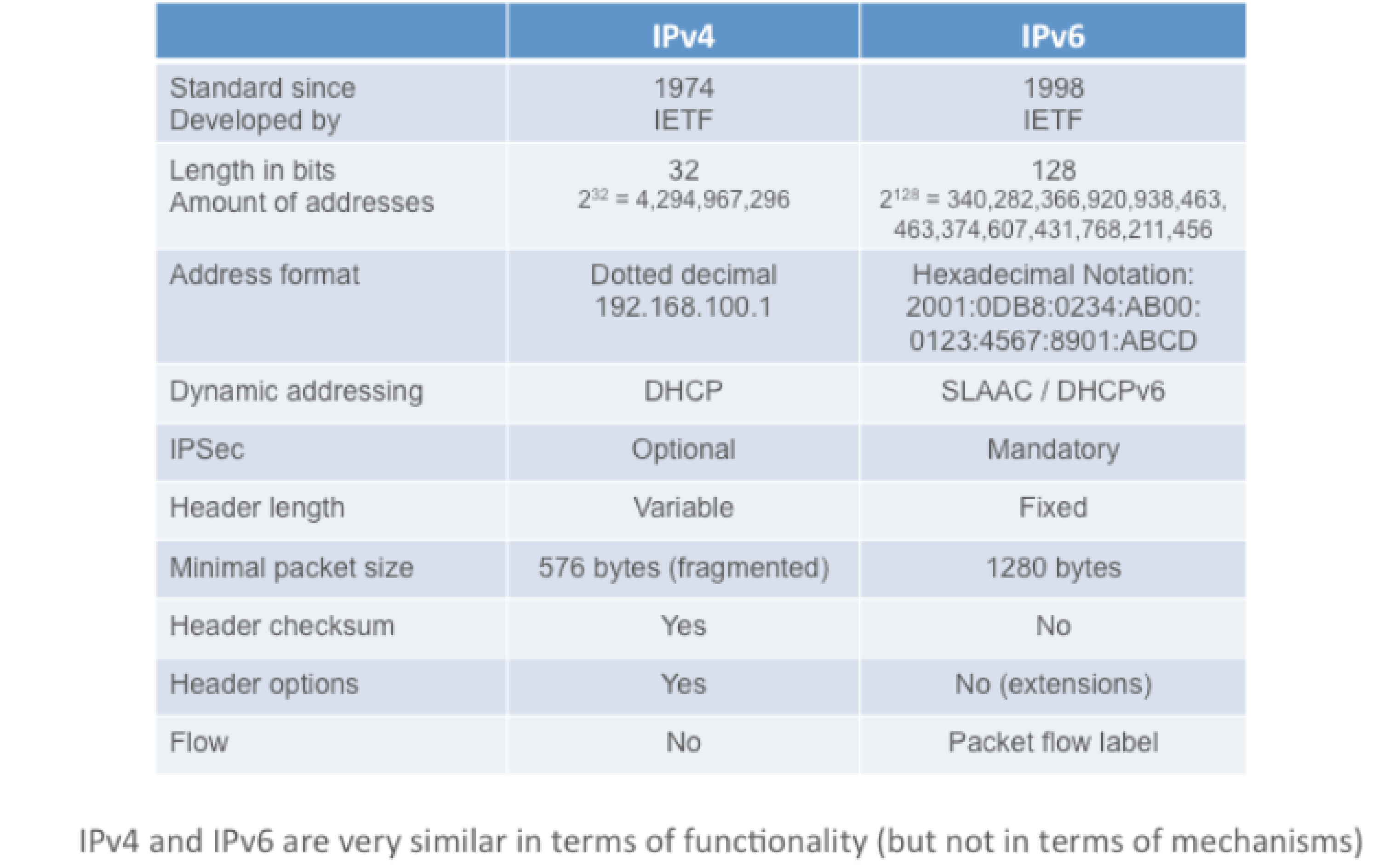
The Benefits of IPv6

While increasing the pool of addresses is one of the most often-talked about benefit of IPv6, there are other important technological changes in IPv6 that will improve the IP protocol:

- No more NAT (Network Address Translation)
- Auto-configuration
- No more private address collisions
- Better multicast routing
- Simpler header format
- Simplified, more efficient routing
- True quality of service (QoS), also called "flow labeling"
- Built-in authentication and privacy support (Full VPN Support)
- Flexible options and extensions
- Easier administration (say good-bye to DHCP)

→ Many nations have already migrated to IPV6.

IPV4 & IPV6 Differences at a Glance



	IPv4	IPv6
Standard since Developed by	1974 IETF	1998 IETF
Length in bits Amount of addresses	32 2^{32} = 4,294,967,296	128 2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456
Address format	Dotted decimal 192.168.100.1	Hexadecimal Notation: 2001:0DB8:0234:AB00: 0123:4567:8901:ABCD
Dynamic addressing	DHCP	SLAAC / DHCPv6
IPSec	Optional	Mandatory
Header length	Variable	Fixed
Minimal packet size	576 bytes (fragmented)	1280 bytes
Header checksum	Yes	No
Header options	Yes	No (extensions)
Flow	No	Packet flow label

IPv4 and IPv6 are very similar in terms of functionality (but not in terms of mechanisms)

There and Back Again: A Packet's Tale. How Does the Internet Work?

Go to the following URL to view this short video:

https://www.youtube.com/watch?v=ewrBalT_eBM

Standards and Organizations

- DSS – Digital Signature Standard
- IEEE – Institute of Electrical and Electronics Engineers
- IEFT – Internet Engineering Task Force
- FIPS – Federal Information Processing Standards
- NIST – National Institute of Standards and Technology
- OSI – Open Systems Interconnection

→ This slide is very useful if you have trouble falling asleep

Ethernet - Where are we today

- Currently most home routers are 10 & 100 Mbps compatible, High end routers up to 1000 Mbps
- Ethernet 400/200 Gbps to roll out sometime this year
- Ethernet 1000 Gbps Standard currently being reviewed by IEEE

Network Security

Network Security is a very broad topic that, in a nutshell, involves protecting computer assets from compromise, destruction, or theft. There are three basic area's that we will focus on in this section:

- **Availability** – That your Computer Services are available as needed.
- **Confidentiality** – That information sent between you and your intended recipients only can see confidential information.
- **Non-Repudiation** – That if you send information from you, the recipient can trust the message was indeed sent from you.

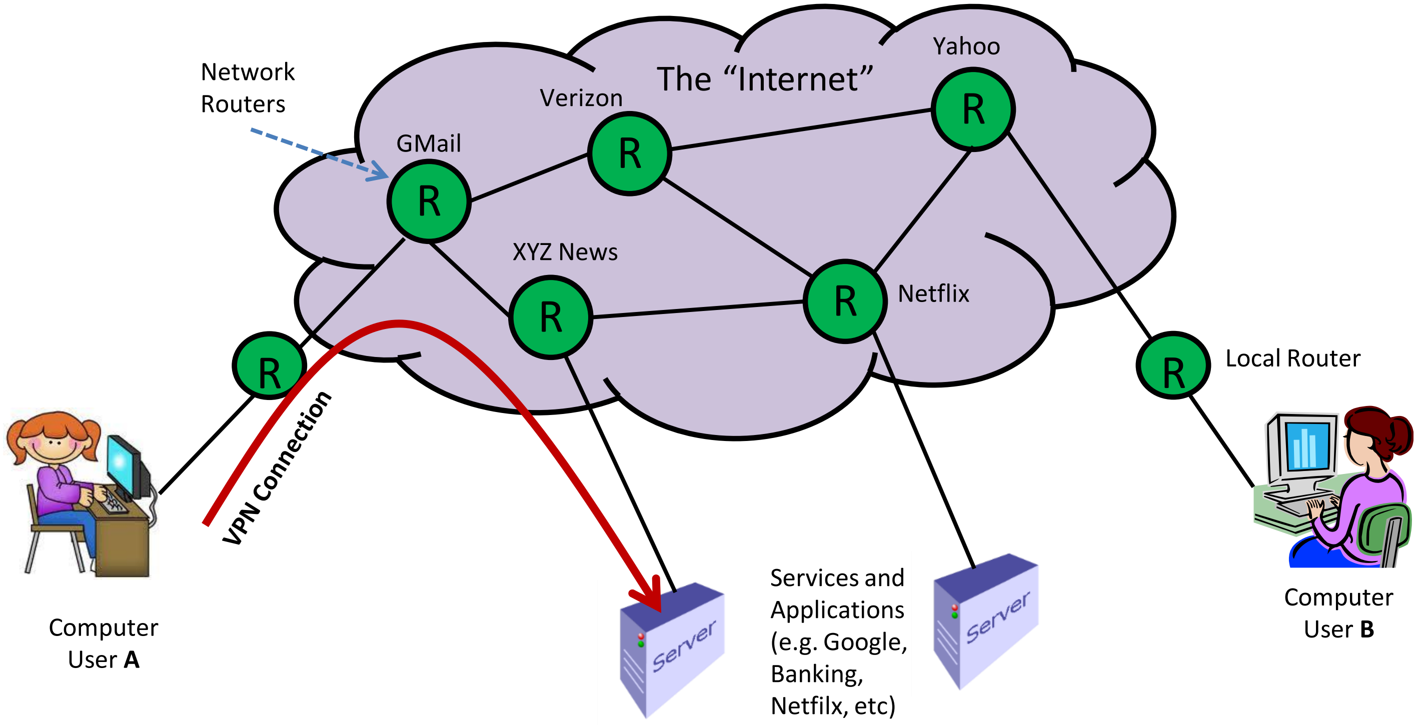
Network Encryption Services

VPN – *virtual* ***private network*** (***VPN***) is a network that is constructed using public wires — usually the Internet — to connect remote users or regional offices to a company's private, internal network. A VPN secures the private network, using encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. This type of network is designed to provides a secure, encrypted tunnel in which to transmit the data between the remote user and the company network.

TLS - Transport Layer **Security** (**TLS**) is a protocol that provides privacy and data integrity between two communicating applications. ... **TLS** evolved from Netscape's **Secure** Sockets Layer (SSL) protocol and has largely superseded it, although the terms SSL or SSL/**TLS** are still sometimes used.

→ VPN and TLS Services are used to provide Data Confidentiality

VPN Connection



→ An Encrypted VPN connection is used to connect User A to a specific Service (e.g. the company Network)

Digital Signatures

Digital Signatures are used as a means of validating that a message received came from the person “claiming” to have sent it. This involves performing a cryptographic mathematical calculation of the message using the Senders Unique “Certificate Key” assigned by a Trusted Certificate Authority. The result is then appended to the end of the message. The receiver then performs the same cryptographic calculation to verify the senders identity. Any attempts to alter the message in any way will cause the verification process to fail. This is often referred to as non-repudiation.

The Digital Signature Standard (**DSS**) is defined by the National Institute of Standards and Technology (**NIST**)

Definitions

- **Firewall** – a **network** security system that monitors and controls incoming and outgoing **network** traffic based on predetermined security rules.

- An **intrusion detection system** (**IDS**) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.

→ Both Firewalls and Intrusion detection systems help prevent malicious packets from getting into a private network and/or provide a means of intrusion detection should it occur.

Spoofing and Hacking

- **Spoofing** – Using software to change the MAC Address, IP Address, or Identify of Information being sent. (e.g. introduce viruses, steal passwords, Identify Theft, etc)

- **Hacking** – Penetrating the Network defenses of a system in order to either steal information, compromise information, or create a “denial of service” to a service provider.

Virus Definition

A computer virus is a type of malicious code or program written to alter the way a computer operates and that is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

Viruses vs Malware

A **virus** is considered **malware**; therefore there really is no **difference**. The term '**malware**' is used as a way describe any malicious software including: adware, spyware, worms, trojans, and **viruses**. Common methods of spreading viruses include:

- Email attachments – opening attachments from unknown sites
- Downloading Programs that are infected
- Social Media
- On-line Ads that are really fakes
- Unpatched Software

Summary

- The Packet is the basic unit of information to exchange data on a computer Network.

- The OSI Network Model use a mechanism call data encapsulation to provide various services using packets.

- Routers are used to deliver Packets from the Sender to a specific destination based upon the IP address and routing tables used to find the fastest means of delivery.

- Firewalls and Intrusion Detection Systems provide a means of protection against malicious Users.

Q & A ?????

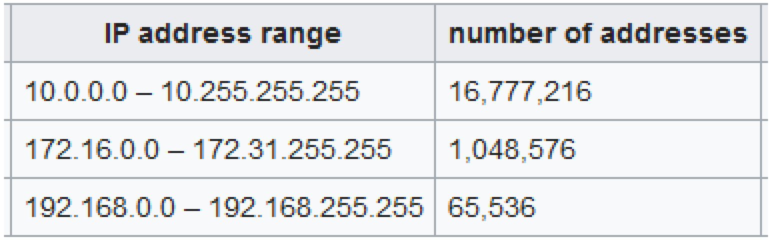
Backup Slides

Network Address Translation

Network address translation (**NAT**) is a method of remapping one IP address space into another by modifying **network** address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

- A public IP address is an IP address that can be accessed over the Internet. Like postal address used to deliver a postal mail to your home, a public IP address is the globally unique IP address assigned to a computing device. Your public IP address can be found at What is my IP Address page.

- Private IP address, on the other hand, is used to assign computers within your private space without letting them directly expose to the Internet. For example, if you have multiple computers within your home you may want to use private IP addresses to address each computer within your home. In this scenario, your router gets the public IP address, and each of the computers, tablets and smartphones connected to your router (via wired or wifi) gets a private IP address from your router via DHCP protocol.



IP address range	number of addresses
10.0.0.0 – 10.255.255.255	16,777,216
172.16.0.0 – 172.31.255.255	1,048,576
192.168.0.0 – 192.168.255.255	65,536

Virus Definitions – Part 2

- **Viruses**: A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.

- **E-mail viruses**: An e-mail virus travels as an attachment to e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book. Some e-mail viruses don't even require a double-click -- they launch when you view the infected message in the preview pane of your e-mail software [source: Johnson].

- **Trojan horses**: A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk). Trojan horses have no way to replicate automatically.

- **Worms**: A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.

WiFi

The Wi-Fi Alliance says Wi-Fi is any "wireless local area network" (WLAN) that follows the IEEE 802.11 specification.   A Wi-Fi device can work with any Wi-Fi network anywhere in the world. The word Wi-Fi is a play on words with hi-fi, and was invented to replace the name "IEEE 802.11b Direct Sequence Spread Spectrum". There are many types of Wi-Fi standards, known as 802.11 a, b, g, n, and recently ac & ad. These specifications are different in terms of speed and how far away you can use them.

As of 2013, most wireless networks use one of two radio frequency bands. These are not the only two bands, but are the most used. One of the bands is at around 2.4 GHz, and the other is at 5 GHz. The 2.4 GHz band is widely used, and devices are usually cheaper.

Bluetooth

Bluetooth is a protocol for wireless communication over short distances. It was developed in the 1990s, to reduce the number of cables. Devices such as mobile phones, laptops, PCs, printers, digital cameras and video game consoles can connect to each other, and exchange information. This is done using radio waves. It can be done securely. Bluetooth is only used for relatively short distances, like a few meters. There are different standards. Data rates vary. Currently, they are at 1-3 MBit per second. Typical Bluetooth applications are to connect a headset to a mobile phone, or to connect a computer mouse, keyboard or printer.

Bluetooth devices use the ISM Band around 2.4 GHz. This can be used worldwide, without the need to pay license fees, but many other devices, like wireless phones, smart tags with RFID, baby monitor use it too. Bluetooth uses the same bands as some WLANs (WiFi) , but the modulation technique is different. Bluetooth uses Frequency-hopping spread spectrum.