BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Introduction to Networks and the Internet

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

Disclaimer

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Agenda

- Introduction
- Network Basics
- How the Internet Works
- History of the Internet
- Basic Network Utilities
- Other Network Devices
- Advanced Network Communications Topics:
  – Network communication types
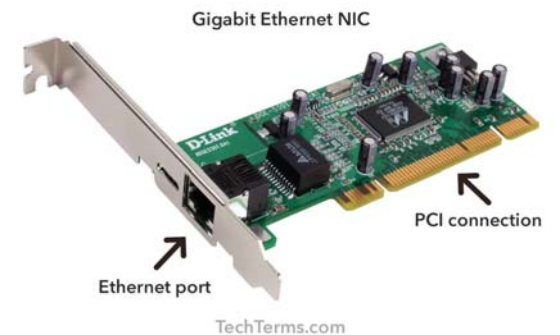 – Types of Networks
  – OSI Model
  – Network Protocols

Network Basics

Network Basics

Overview

- **Communication among computers**
  - Requires connecting them physically through cables or wirelessly
  - Cables are plugged either directly to another computer or into a device
    - This device will, in turn, connects to several other computers

- **Network Interface Card (NIC)**
  - Wireless communication relies on a physical device for transmitting the data
   - This device is called *network interface card* (NIC)

Gigabit Ethernet NIC

Ethernet port

PCI connection

TechTerms.com

Overview

- Connection slot (Ethernet port)
  - If the connection is through a cable, the part of the NIC that is external to the computer has a connection slot that looks like a telephone jack, only slightly bigger

- Radio signals
  - Wireless networks also use a NIC
  - Rather than a slot for connecting a cable, NIC uses radio signals to transmit to a nearby wireless router or hub

- Antenna
 - Wireless routers, hubs, and NICs have an antenna to transmit and receive signals

Gigabit Ethernet NIC

PCI connection

Ethernet port

TechTerms.com
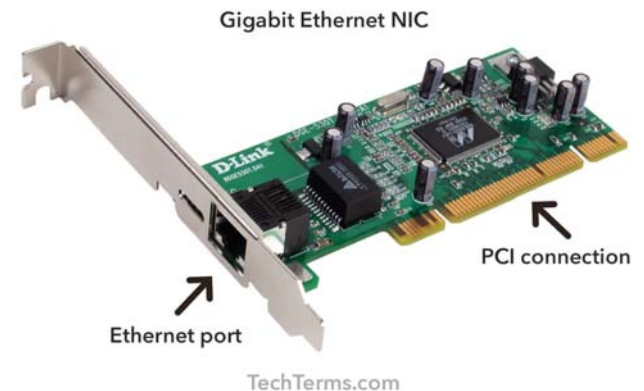
The Physical Connection: Local Networks

- RJ-45
  - The cable connection used with wired NICs is called an RJ-45 connection
  - RJ = Registered Jack, an international industry standard

- RJ-11
  - In contrast to the computer's RJ-45 jacks, standard telephone lines use RJ-11 jacks

- RJ-45 Vs. RJ-11
  - The key difference between jacks is the number of wires in the connector (also called the terminator)
  - Phone lines (RJ-11) have four wires (some have six wires), RJ-45 connectors have eight wires

- This standard connector jack must be on the end of the cable
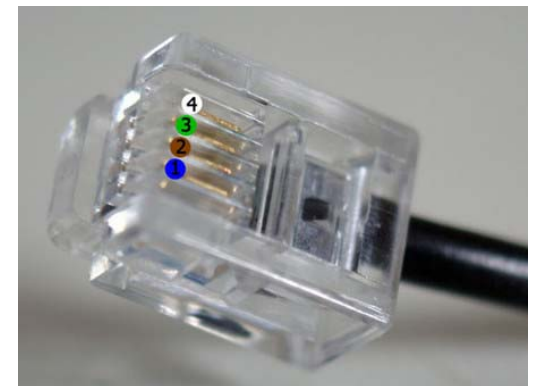
The Physical Connection: Local Networks

- Cat 5 or Cat 6 Cable
  - The cable used in most networks today is a Category 5 or 6 cable abbreviated as Cat 5 or Cat 6 cable

- Unshielded Twisted-Pair (UTP)
  - The cable used in connecting computers is referred to as *unshielded twisted-pair* (UTP) cable
  - The wires in the cable are in pairs, twisted together without additional shielding

- Shielded Twisted-Pair (STP)
  - There are other types of cable such as *shielded twisted-pair* (STP), but UTP is most commonly used

Cat5e VS Cat6		
Product Name	Cat5e UTP Cable	Cat6 UTP Cable
Speed	10BASE-T, 100BASE-TX(Fast Ethernet), 1000BASE-T (Gigabit Ethernet)	10BASE-T, 100BASE-TX(Fast Ethernet), 1000BASE-T (Gigabit Ethernet), 10G BASE-T (10-Gigabit Ethernet)
Frequency	100 MHz	250 MHz
Performance	Good	Better

Network Basics

The Physical Connection: Local Networks

- Table summarizes various categories of cable and their uses.

Cable Types and Uses

Category	Specifications	Uses
1	Low-speed analog (less than 1MHz)	Telephone, doorbell
2	Analog line (less than 10MHz)	Telephone
3	Up to 16MHz or 100Mbps (megabits per second)	Voice transmissions
4	Up to 20MHz/100Mbps	Data lines, Ethernet networks
5	100MHz/100Mbps	Most common a few years ago, still widely used
6	1000Mbps (some get 10Gbps)	Most common type of network cable
6a	10Gbps	High-speed networks
7	10Gbps	Very high-speed networks
8	40Gbps	Not yet commonly found

Network Basics

The Physical Connection: Local Networks

- Each subsequent category of cable is somewhat faster and more robust than the last

- Although Cat 4 can be used for networks, it almost never is used, as it is simply slower, less reliable, and an older technology

- We usually see Cat 5 cable and, increasingly, Cat 6

- We are focusing on UTP because that is what is found most often

- Other types of cable such as shielded twisted-pair (STP), but they are not nearly as common as UTP

The Physical Connection: Local Networks

- A key specification for cables is speed
  - measured in Mbps (megabits per second)

- Now a days, Gbps (gigabits per second) speeds are becoming more common

- Data specification for each cable indicated in the table is the maximum that the cable can handle
  - This is called *bandwidth* of a cable
  - E.g., a Cat 5 cable can transmit up to 100 mega (million) bits per second

- If multiple users simultaneously transmit data on a network, that traffic uses up bandwidth rather quickly
  - E.g., a scanned picture can easily take 2 megabytes (2 million bytes, or 16 million bits) or much larger
  - Streaming media, such as videos, are most demanding in terms of bandwidth

Network Basics

The Physical Connection: Local Networks

- Connecting two computers simply requires a cable to go directly from one computer to another
  - What about more than 2 computers or 100 computers?
- Three devices that can help accomplish this task:
  - The hub
  - The switch, and
  - The router
- These devices use Cat 5 or Cat 6 cable with RJ-45 connectors

The Hub

- A hub is a small electronic device into which network cables are plugged

- It can have 4 or more (commonly up to 24) RJ-45 jacks, each called a port

- A hub can connect as many computers as it has ports
  - E.g., an 8-port hub can connect eight computers

- Stacking
  - We can also connect one hub to another
  - This is referred to as "*stacking*" hubs

Downside of Hubs

- If a packet (a unit of data transmission) is sent from one computer to another
  - a copy of that packet is actually sent out from every port on the hub
- These copies leads to a lot of unnecessary network traffic
- This occurs because the hub, being a very simple device, has no way of knowing where a packet is supposed to go
- Therefore, it simply sends copies of the packet out all of its ports
- True hubs no longer exist, what we are really getting is a *switch*.

## The Repeater

- Is a device used to boost signal
- Basically if the cable needs to go further than the maximum length (which is 100 meters for UTP), then we need a repeater
- There are two types of repeaters: amplifier and signal
- Amplifier repeaters simply boost the entire signal they receive, including any noise
- Signal repeaters regenerate the signal, and thus don't rebroadcast noise.
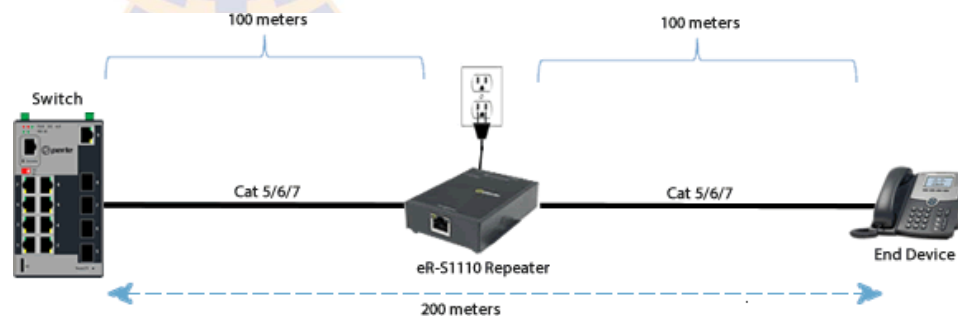
Network Basics

The Switch

- A switch is basically an intelligent hub

- It works and looks exactly like a hub

- When a switch receives a packet, it sends that packet only out the port for the computer to which it needs to go

- A switch is essentially a hub that is able to determine where a packet is being sent

Network Basics

The Router

- A router is used to connect two or more *networks*
- A router:
  - a) is similar in concept to a hub or switch, as it does relay packets;
  - b) is far more sophisticated
- Routers can be programmed and controlled how they relay packets
- Most routers have interfaces that allow us to configure them
- The specifics of router programming differs from vendor to vender
- Unlike using a hub or switch, the two networks connected by a router are still separate networks

Network Basics

Faster Connection Speeds

Internet Connection Types

Connection Type	Speed	Details
DS0	64Kbps	Standard phone line.
ISDN	128Kbps	Two DS0 lines working together to provide a high-speed data connection.
T1	1.54Mbps	Twenty-four DS0 lines working as one. Twenty-three carry data, and one carries information about the other lines. This type of connection has become common for schools and businesses.
T3	43.2Mbps	672 DS0 lines working together. This method is the equivalent of 28 T1 lines.
OC3	155Mbps	All OC lines are optical and do not use traditional phone lines. OC3 lines are quite fast and very expensive. They are often found at tele-communications companies.
OC12	622Mbps	The equivalent of 336 T1 lines, or 8,064 phone lines.
OC48	2.5Gbps	The equivalent of four OC12 lines.

Network Basics

Wireless

- The Institute of Electrical and Electronics Engineers (IEEE) standard 802.11 provides guidelines for wireless networking

- Various letter designations are used to denote different wireless speeds

- The various wireless speeds, starting from the oldest to the most recent, are listed here

Network Basics

Wireless

Designation	Description
802.11a	• This was the first widely used Wi-Fi; it operated at 5GHz and was relatively slow
802.11b	• This standard operated at 2.4GHZ and had an indoor range of 125 feet with a bandwidth of 11Mbps
802.11g	• There are still many of these wireless networks in operation • We can no longer purchase new Wi-Fi access points that use 802.11g. • This standard includes backward compatibility with 802.11b. • 802.11g has an indoor range of 125 feet and a bandwidth of 54Mbps
802.11n	• This standard was a tremendous improvement over preceding wireless networks • It provides a bandwidth of 100Mbps to 140Mbps and operates at frequencies of 2.4GHz or 5.0GHz over an indoor range of up to 230 feet
IEEE 802.11n-2009	• This technology provides a bandwidth of up to 600Mpbs with the use of four spatial streams at a channel width of 40MHz • It uses multiple-input multiple-output (MIMO), in which multiple antennas coherently resolve more information than is possible using a single antenna

Network Basics

Wireless

Designation	Description
IEEE 802.11ac	• This standard was approved in January 2014 • It has a throughput of up to 1Gbps and at least 500Mbps • It uses up to 8 multiple-input multiple-output (MIMO)
IEEE 802.11ad Wireless Gigabyte Alliance	• Supports data transmission rates up to 7Gbps • This is more than 10 times faster than the highest 802.11n rate
IEEE 802.11af	• Also referred to as "White-Fi" and "Super Wi-Fi," • This standard was approved in February 2014 • It allows WLAN operation in TV white space spectrum in the VHF and UHF bands between 54MHz and 790MHz.
IEEE 802.11aj	• It is a rebranding of 802.11ad • It is used in the 45GHz unlicensed spectrum available in some regions of the world (specifically China).

Securing Wi-Fi

- The methods for securing Wi-Fi have evolved over the years
  - First there was Wired Equivalent Privacy (WEP)
  - Next, Wi-Fi Protected Access (WPA)
  - Next, Wi-Fi Protected Access2 (WPA2)
  - Currently, Wi-Fi Protected Access3 (WPA3)

Network Basics
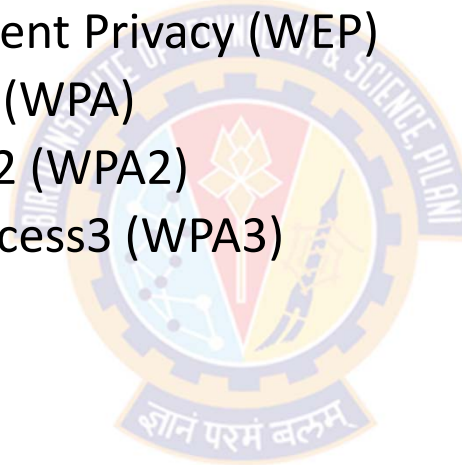
Securing Wi-Fi

- Wired Equivalent Privacy (WEP)
  - WEP uses the stream cipher RC4 algorithm to secure the data and a CRC-32 checksum for error checking
  - Standard WEP (known as WEP-40) uses a 40-bit key with a 24-bit initialization vector (IV) to effectively form 64-bit encryption
  - 128-bit WEP uses a 104-bit key with a 24-bit IV
  - Because RC4 is a stream cipher, the same traffic key must never be used twice
  - The purpose of an IV, which is transmitted as plain text, is to prevent any repetition
    - but a 24-bit IV is not long enough to ensure this on a busy network
  - The way its IV is used also opens WEP to a related key attack
  - For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets

Securing Wi-Fi

- Wi-Fi Protected Access (WPA)
  - WPA uses Temporal Key Integrity Protocol (TKIP)
  - TKIP is a 128-bit per-packet key
    - That is, it dynamically generates a new key for each packet

- Wi-Fi Protected Access (WPA2)
  - WPA2 is based on the IEEE 802.11i standard
  - Provides the Advanced Encryption Standard (AES) using the Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP)
    - This provides data confidentiality, data origin authentication, and data integrity for wireless frames

Securing Wi-Fi

- Wi-Fi Protected Access (WPA3)
  - WPA3 requires attackers to interact with your Wi-Fi for every password guess they make, making it much harder and time-consuming to crack
  - However, with WPA3' s "Wi-Fi Easy Connect," you can connect a device by merely scanning a QR code on your phone
  - One of the important new security features is that with WPA3, even open networks will encrypt your individual traffic
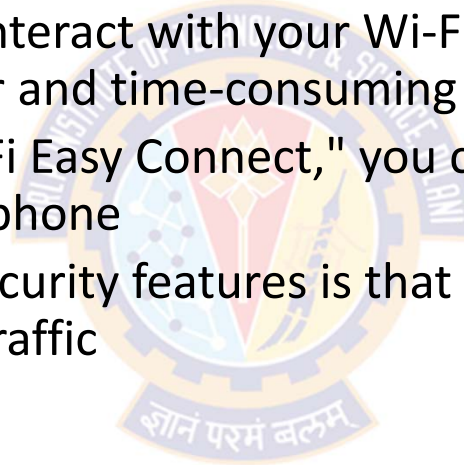
Bluetooth

- The name comes from king Harald "Bluetooth" Gormsson, a tenth-century Danish king who united the tribes of Denmark.
  - There are different explanations for the king's nickname
    - One is that he had a bad tooth that was blue
    - Another is that he was often clothed in blue

- The idea behind the Bluetooth technology is that it unites communication protocols

- It is a short-distance radio using the 2.4GHz to 2.485GHz frequency

- The IEEE standardized Bluetooth as IEEE 802.15.1, but it no longer maintains the standard
  - This standard enables devices to discover other Bluetooth devices within range

- The speed and range of Bluetooth depends on the version

Version	Bandwidth	Range
3.0	25Mbps	10 meters (33 feet)
4.0	25Mbps	60 meters (200 feet)
5.0	50Mbps	240 meters (800 feet)

Other Wireless Protocols

- ANT +:
  - This wireless protocol is often used with sensor data such as in bio sensors or exercise applications

- ZigBee:
  - This standard was developed by a consortium of electronics manufacturers for mainly residential applications of wireless devices related to appliances and security
  - It is based on the 802.15.4 standard
  - This standard is represented by the name "ZigBee" rather than a number
  - The term ZigBee is used similar to the way the term Wi-Fi is used

- Z-Wave:
  - This wireless communications protocol is used primarily for home automation
  - Uses a low-energy radio for appliance-to-appliance communication using a mesh network

Data Transmission

Overview

- How is data actually transmitted in the networks?

- To transmit data, a packet is sent

- The basic purpose of a cable is to transmit packets from one machine to another

- It does not matter whether that packet is part of a document, a video, an image, or just some internal signal from the computer
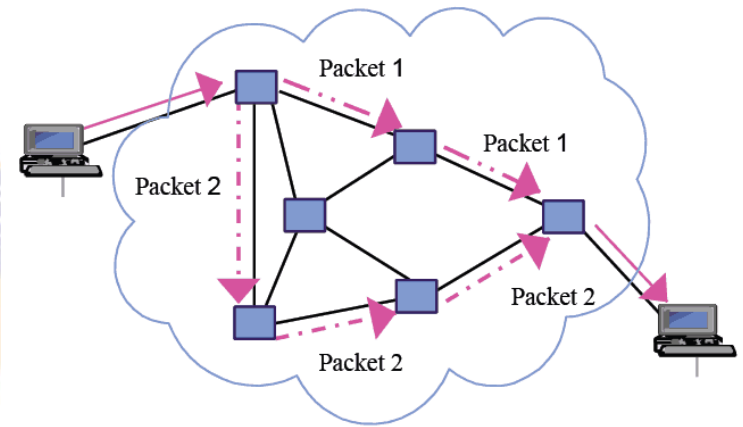
Data Transmission

Overview

- Now, what exactly is a packet?

- A packet is a certain number of bytes divided into a header and a body

- The header is 20-60 bytes at the beginning of the packet that tells where the packet is coming from, where it is going, and more

- The body contains the actual data, in binary format

- The routers and switches read the header portion of the packets that come to them and determine where the packet should be sent

Transmission Control Protocol (TCP) Header
20-60 bytes

source port number 2 bytes	destination port number 2 bytes
sequence number 4 bytes	
acknowledgement number 4 bytes	

data offset 4 bits	reserved 3 bits	control flags 9 bits	window size 2 bytes

checksum 2 bytes	urgent pointer 2 bytes

| optional data 0-40 bytes | |

Data Transmission

Protocols

- There are different types of network communications for different purposes

- These network communications are called *protocols*

- A *protocol* is, essentially, an agreed-upon method of communication

- In fact, this definition is exactly how the word protocol is used in standard, non-computer usage, too

- Each protocol has a specific purpose and normally operates on a certain port

Data Transmission

Protocols

- Some of the most important, and most commonly used, protocols are listed in table below (see next slide)

- All of these protocols are part of a suite of protocols referred to as TCP/IP (Transmission Control Protocol/Internet Protocol)

- But no matter what protocol is used, all communication on networks takes place via packets

- These packets are transmitted according to certain protocols, depending on the type of communication that is occurring

Data Transmission

Protocols

Protocol	Purpose	Port(s)
FTP (File Transfer Protocol)	For transferring files between computers	20 & 21
TFTP (Trivial File Transfer Protocol)	A quicker but less reliable form of FTP	69
SSH (Secure Shell)	Used to securely connect to a remote system	22
Telnet	Used to remotely log on to a system. You can then use a command prompt or shell to execute commands on that system. Popular with network administrators	23
SMTP (Simple Mail Transfer Protocol)	Sends email	25
Whois	A query and response protocol that provides information about the registered Domain Names, an IP address block, Name Servers, etc.	43
DNS (Domain Name System)	Translates URLs into web addresses.	53
HTTP (Hypertext Transfer Protocol)	Displays web pages	80
POP3 (Post Office Protocol version 3)	Retrieves email	110

Data Transmission

Protocols

Protocol	Purpose	Port(s)
NNTP (Network News Transfer Protocol)	Used for network newsgroups (Usenet newsgroups). You can access these groups over the Web via www.google.com and selecting the Groups tab	119
NetBIOS	An older Microsoft protocol that is for naming systems on a local network	137, 138, or 139
IMAP (Internet Message Access Protocol)	More advanced protocol for receiving email. Widely replacing POP3	143
IRC (Internet Relay Chat)	Used for chat rooms	194
SMB (Server Message Block)	Used for Windows Active Directory	445
HTTPS	Encrypted HTTP; used for secure websites	443
SMTPS	Simple Mail Transfer Protocol Secure; Encrypted SMTP	465
POP3S	Post Office Protocol version 3 Secure; Encrypted POP3	995
IMAPS	Internet Message Access Protocol Secure; Encrypted IMAP	993

Ports

- In a physical sense, ports are the connection locations on the back of our computer
  - E.g., serial ports, parallel ports, and RJ-45 and RJ-11 ports
- In networking terms, a port is a connection point
- It is a numeric designation for a particular pathway of communications
- It can be thought of as a channel number on our television
- We may have one cable coming into our TV, but you can tune to a variety of channels

Data Transmission

Ports

- Regardless of the type of computer or operating system, there are 65,535 network communications ports on our computer

- The combination of our computer's IP address and port number is referred to as a *socket*

- All network communication (regardless of the port used) comes into our computer via the connection on our NIC

- So, a network consists of computers connected to each other via cables, hubs, switches, or routers

- These networks transmit binary information in packets using certain protocols and ports

How Internet Works

Overview

- https://www.youtube.com/watch?v=x3c1ih2NJEg&t=225s
- The Internet is essentially a large number of networks that are connected to each other
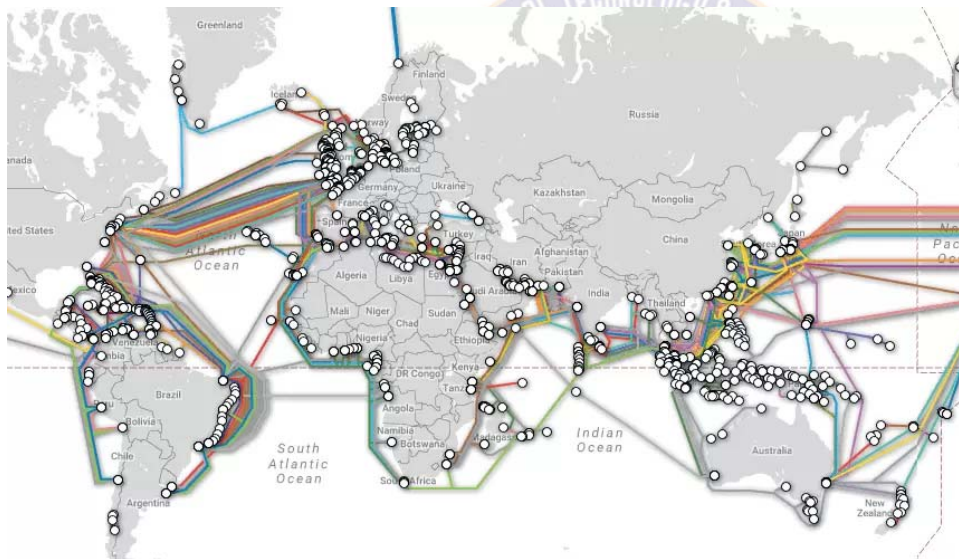
- These networks are connected into main transmission lines called *backbones*

Overview

- The points where the backbones connect to each other are called *network access points* (NAPs)

- The Internet works exactly the same way as a local network

- It sends the same sort of data packets, using the same protocols

- When we log on to the Internet, we typically use an *Internet service provider* (ISP)

- The ISP has a connection either to the Internet backbone or to yet another provider that has a backbone

- So, logging on to the Internet is a process of connecting the computer to ISP's network, which is, in turn, connected to one of the backbones on the Internet

IP Addresses

- When tens of thousands of networks and millions of individual computers communicate,
  - how to ensure that the data packets go to the correct computer?
- This task is accomplished in much the same way as traditional "snail" letter mail is delivered to the right person: via an address
- In network communications, this address is referred to as an "IP" address
- An IP address can be IP version 4 or version 6

IPv4

- An IP address is a series of four values, separated by periods
  - E.g., 107.22.98.198

- Each of the three-digit numbers must be between 0 and 255
  - For example, an address of 107.22.98.466 is not a valid one

- These addresses are actually four binary numbers; we just see them in decimal format

- Each of these numbers (being a decimal representation of 8 bits), are often referred to as octets

- A 8-bit binary number converted to decimal format will be between 0 and 255

- So there are four octets in an IPv4 address

- This rule gives a total of over 4.2 billion possible IP addresses

- There are methods already in place to extend the use of addresses

IPv4

- To extend the IPv4 address space, companies use private IPv4 addresses through a public-to-private address translation
  - This technique is known as network address translation (NAT).

- The public IP addresses are for computers connected to the Internet

- Public IP addresses cannot be duplicate

- A private IP address, such as one on a private company network, only has to be unique in that network

- Often network administrators use private IP addresses that begin with a 10, such as 10.102.230.17.

IPv4

- The IP address of a computer tells us a lot about that computer
- The first byte (or the first decimal number) in an address tells you to what class of network that machine belongs
- Table below summarizes the five network classes

Network Classes

Class	IP Range for the First Byte	Use
A	0–126	Extremely large networks. No Class A network IP addresses are left. All have been used.
B	128–191	Large corporate and government networks. All Class B IP addresses have been used.
C	192–223	The most common group of IP addresses. Your ISP probably has a Class C address.
D	224–247	These are reserved for multicasting (transmitting different data on the same channel).
E	248–255	Reserved for experimental use.

IPv4

- The IP range of 127 (not listed in the table) is reserved for testing
- The IP address of 127.0.0.1 designates the machine you are on, regardless of that machine's assigned IP address
- This address is often referred to as the *loopback address*
- That address is often used in testing our machine and our NIC
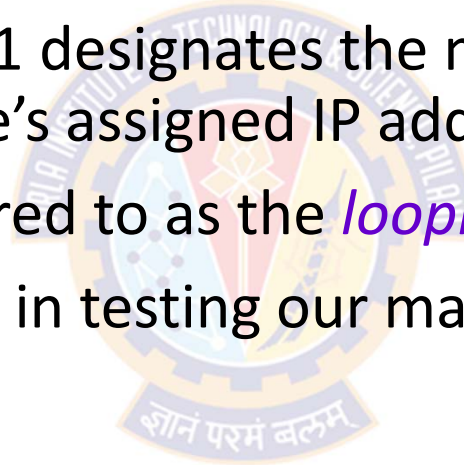
IPv4

- Special purpose IP addresses
  - Certain range of private IP addresses have been designated for use within networks
    - These cannot be used as public IP addresses but can be used for internal workstations and servers
      - 10.0.0.10 to 10.255.255.255
      - 172.16.0.0 to 172.31.255.255
      - 192.168.0.0 to 192.168.255.255

- The gateway router performs *network address translation* (NAT)

- NAT takes the private IP address on outgoing packets and replaces it with the public IP address of the gateway router
  - This allows the packet to be routed through the Internet

IPv4

- In the above network classes, one part of the address represents the network and the other part represents the node

- For example:

Network Bits = 8	Host Bits - 24			
1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0		Class A
255	0	0		

Network Bits = 16		Host Bits = 16		
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		Class B
255	255	0	0	

Network Bits = 14			Host Bits = 8	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			0 0 0 0 0 0 0 0	Class C
255	255	255	0	

Subnetting

IPv4 Prefix
200.200.10.0/25

Subnet 1
6 users

1.Subnet
200.200.10.48/29

Subnet 2
4 users

2.Subnet
200.200.10.56/29

Subnet 5
9 users

5. Subnet
200.200.10.32/28

Subnet 3
14 users

3. Subnet
200.200.10.0/28

Subnet 4
10 users

4. Subnet
200.200.10.16/28

ipcisco.com

- Subnetting is simply slicing a network into smaller portions

- For example
  - consider a network using the IP address 192.168.1.X (X is the address for specific computer), then we can allocate 255 possible IP addresses

- If we wish to divide these 255 IPs into two separate subnetworks,
  - subnetting is the way to go

- More technically, the subnet mask is a 32-bit number that is assigned to each host to divide the 32-bit binary IP address into network and node portions

Subnetting

- We already have a subnet mask even if you have not been subnetting
  - If we have a Class A IP address, then our subnet mask is 255.0.0.0.
  - If we have a Class B IP address, then our subnet mask is 255.255.0.0.
  - If we have a Class C IP address, then our network subnet mask is 255.255.255.0.

- So we are literally "masking" the portion of the network address that is used to define the network, and the remaining portion is used to define individual nodes

CLASS A (1-126)
Default subnet mask = 255.0.0.0

Subnets/Hosts

| Network | Host | Host | Host |

255 . 0 . 0 . 0

CLASS B (128-191)
Default subnet mask = 255.255.0.0

Subnets/Hosts

| Network | Network | Host | Host |

255 . 255 . 0 . 0

CLASS C (192-223)
Default subnet mask = 255.255.255.0

Subnets/Hosts

| Network | Network | Network | Host |

255 . 255 . 255 . 0

Subnetting

- Now if we want fewer than 255 nodes in our subnet, then we need something like 255.255.255.240 for our subnet

- If we convert 240 to binary, it is 11110000

- That means the first three octets and the first 4 bits of the last octet define the network

- The last 4 bits of the last octet define the node

- That means we could have as many as 1111 (in binary) or 15 (in decimal) nodes on this subnetwork

- This is the basic essence of subnetting

Network Bits																												Host Bits			
28																															
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0
255								255								255								240							

Subnetting

- Another approach is *Classless InterDomain Routing* (CIDR)

- Rather than define a subnet mask, we have the IP address followed by a slash and a number

- That number can be any number between 0 and 32, which results in IP addresses like these:
  - 192.168.1.10/24 (basically a Class C IP address)
  - 192.168.1.10/31 (much like a Class C IP address with a subnet mask)

- When we use this (rather than having classes with subnets) we have *Variable-Length Subnet Masking* (VLSM) that provides classless IP address

- This is the most common way to define network IP addresses today

- https://www.youtube.com/watch?v=q7wNcYliJ1Q

Subnetting

- Class A (CIDR Value = /8 = Total number of network bits)
- IP Address: 1-126
- Default Subnet Mask: 255.0.0.0
- 8 bits are reserved for network and the remaining 24 bits are reserved for the host

Network Bits = 8								Host Bits = 24																								
1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
255								0								0															

CIDR = Classless Inter Domain Routing

Subnetting

- Class B (CIDR Value = /16 = Total number of network bits)
- IP Address: 128-191
- Default Subnet Mask: 255.255.0.0
- 16 bits are reserved for network and the remaining 16 bits are reserved for the host

Network Bits			Host Bits		
16			16		
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0
255	255	0	0

CIDR = Classless Inter Domain Routing

Subnetting

- Class C (CIDR Value = /24 = Total number of network bits)
- IP Address: 192-223
- Default Subnet Mask: 255.255.255.0
- 24 bits are reserved for network and the remaining 8 bits are reserved for the host

Network Bits			Host Bits
24			8
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			0 0 0 0 0 0 0 0
255	255	255	0

CIDR = Classless Inter Domain Routing

Subnetting – Example – Class C

- 192.168.1.0/24

255								255								255								0							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								0							
8 Bits								8 Bits								8 Bits								8 Bits							
Block 1								Block 2								Block 3								Block 4							

- Default subnet mask for class C = 255.255.255.0
- CIDR Value = 24 = Total number of network bits
- We can calculate the subnet mask only from the network bits not the host bits

Subnetting – Example – Class C

- 192.168.1.0/25

255								255								255								**128**							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**	0	0	0	0	0	0	0
$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								**2^7**							
8 Bits								8 Bits								8 Bits								8 Bits							
Block 1								Block 2								Block 3								Block 4							

- Default subnet mask for class C = 255.255.255.0
- But, CIDR Value = 25. So, we need one extra bit. We borrow that from host
- The new subnet mask = 255.255.255.128

Subnetting – Example – Class C

- 192.168.1.0/25

255								255								255								**128**							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0

- Number of networks
  - 2^n (Where, n = number of bits borrowed from the host)
  - $2^1 = 2$ (We can create only two networks)
- Number of IP addresses on each network
  - 2^b (Where, b = number of remaining host bits)
  - $2^7 = 128$ (On each network we can have 128 IP addresses)
- Number of hosts on each network (IPs that can be assigned to devices)
  - $2^b - 2$ (Where, b = number of remaining host bits)
  - $2^7 - 2 = 126$ (We can assign 126 IP addresses to devices)

Note:
In every network, the first IP address is reserved for the network ID and the last IP address is reserved for broadcast ID

Thank You!