AAiT
ADDIS ABABA INSTITUTE OF TECHNOLOGY
አዲስ አበባ ቴክኖሎጂ ኢንስቲትዩት
ADDIS ABABA UNIVERSITY
አዲስ አበባ ዩኒቨርሲቲ

Enterprise Systems and Network Administration

CHAPTER ONE
Introduction to Systems and Network Administration

Getnet M.
getnet.mamo@aau.edu.et

1.1. System and Network Administration

1.1. What is system administration?
1.2. What is network administration?
1.3. Roles of system and network administrator
1.4. Ethics
1.5. Review of computer network

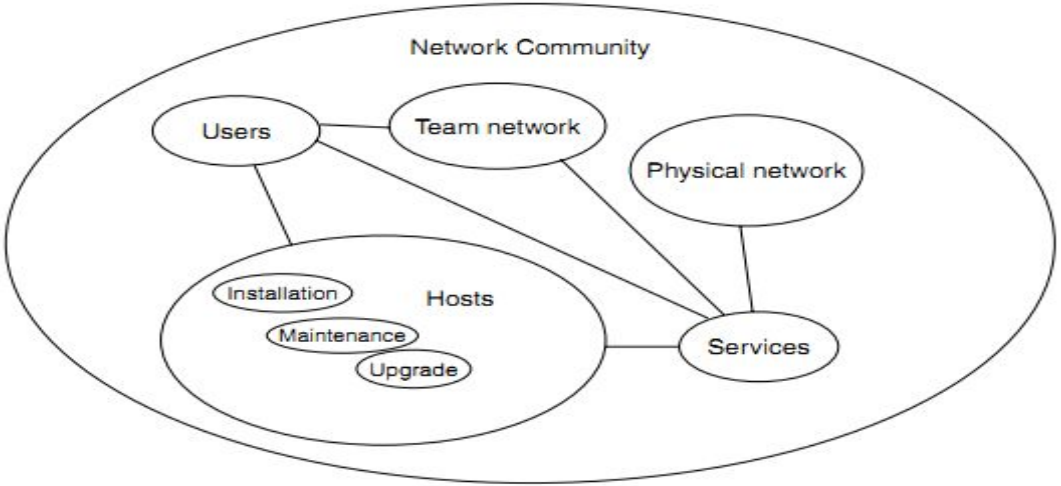
1.2 Review of Computer network

1.1. Basics of network
1.2. Network software and hardware
1.3. Types of network
1.4. Network protocols
1.5. IP4 addressing
1.6. Network devices

What is system administration?

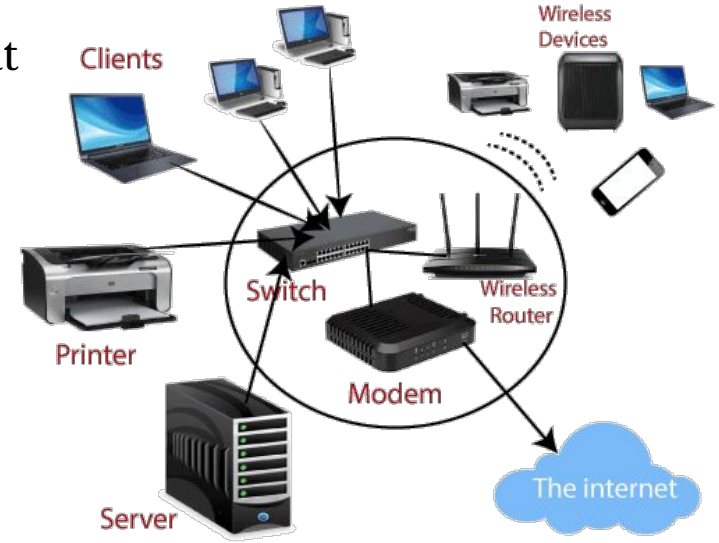
- What is System?
  - In system administration, the word **system** is used to refer both to the operating system of a computer and often, collectively the set of all computers that cooperate in a network.

- Has Structure, behavior and interconnectivity
- Specifically, it refers to *human – computer systems*



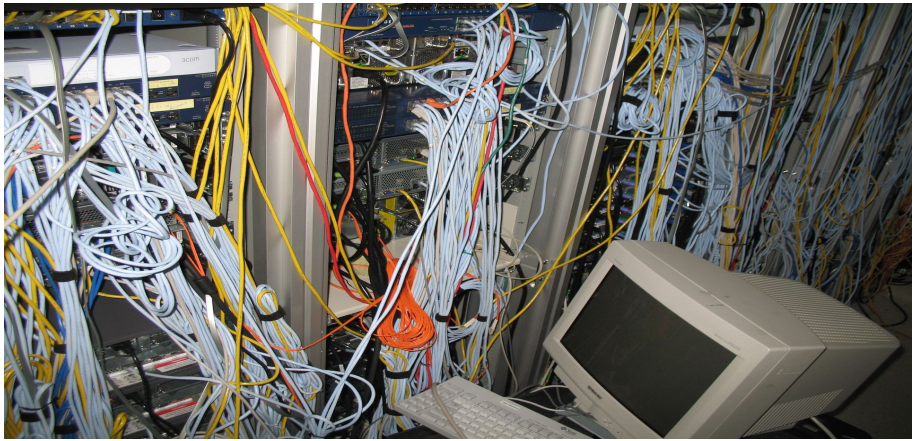
What is system administration?

- What is Human-Computer System?
  - Consists of three components:
    - **Humans** : who use and run the fixed infrastructure, and cause most problems.
    - **Host computers :** computer devices that run software. These might be in a fixed location, or mobile devices.
    - **Network hardware :** This covers a variety of specialized devices including the following key components:
      - Servers
      - Interconnecting devices
      - Communication medium



What is system administration?

- **System administrator**
  - **Anyone who manages a computer not solely for his/her own use.**
  - **Someone who takes care of the systems others are using.**
- System administration
  - Activities which directly support the operations and integrity of computing systems and their use and which manage their intricacies
- These activities minimally include:
  - **System installation**
  - **Configuration**
  - **Integration**
  - **Maintenance**
  - **Performance** management
  - **Data management**
  - **Security** management
  - **Failure analysis and recovery**
  - **User support.**



What is system administration?

- System administration requires:
  - Technical skills
  - People & communications skills
  - Problem solving & Common sense
  - Personal Commitment

"SA involves a tension between authority and responsibility on one hand and service and co-operation on the other."

What is system administration?

- Principles of System Administration:
  - Policy is the foundation: System administration begins with a policy – a decision about what we want and what should be, in relation to what we can afford.
  - Predictability: The highest level aim in system administration is to work towards a predictable system. Predictability has limits. It is the basis of reliability, hence trust and therefore security
  - Scalability: Scalable systems are those that grow in accordance with policy; i.e. they continue to function predictably, even as they increase in size.

Roles of System Administrator

System administration can be viewed in three dimensions:

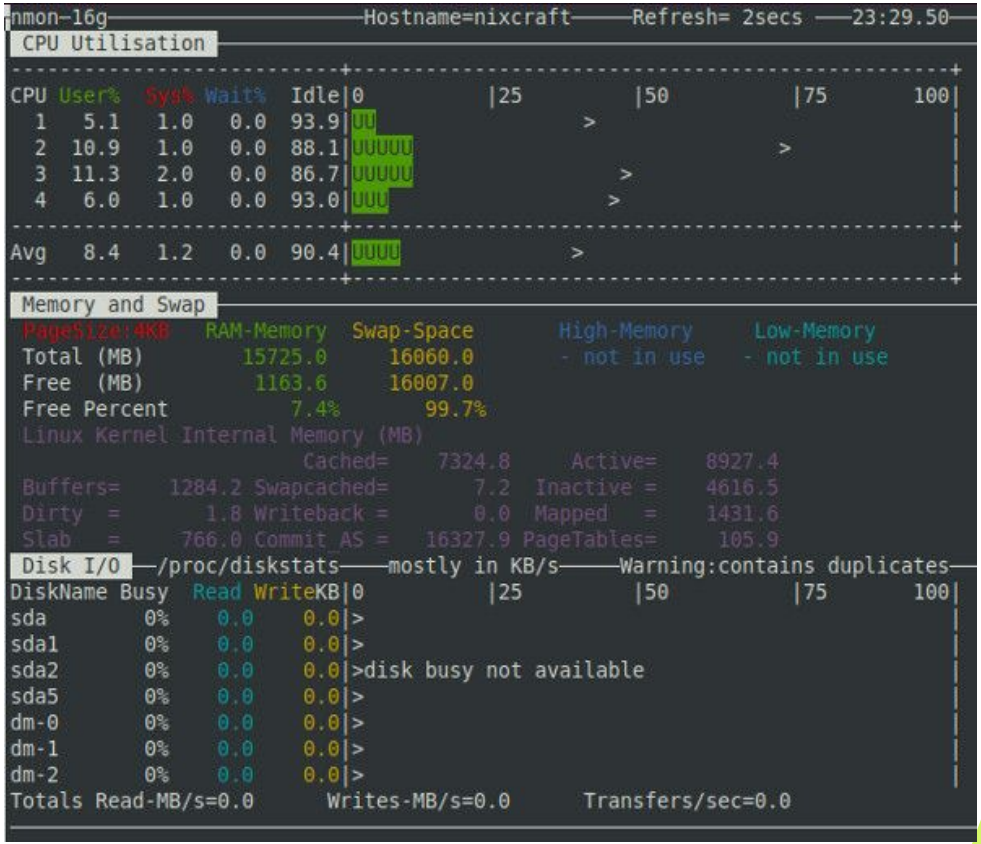
1. **Managing desktops**
   - Installation of OS and update system
   - Install and update applications
   - Configure network parameters
2. **Managing servers**
   - Security
   - Fault-tolerance (Replication, Redundancy, Diversity)
   - Backups
   - Redundant Power supply
3. **Managing services**
   - Get customer requirement
   - Budget
   - Favor simplicity
   - Vendor relationships
   - Machine independence
   - Supportive environment
   - Reliability
   - Restrict access
   - Centralization and standards
   - Performance
   - Monitoring
   - Service roll-out

Network Services:
- Web
- AAA
- DNS
- Email
- Proxy

Roles of System Administrator

Task of System Administration:

- Daily operations
  - emergencies
  - regular tasks (automate)
  - system monitoring
- Hardware and software
  - programming
  - evaluation
  - purchase
  - installation
  - testing and maintenance
  - upgrading
  - phasing out



Roles of System Administrator

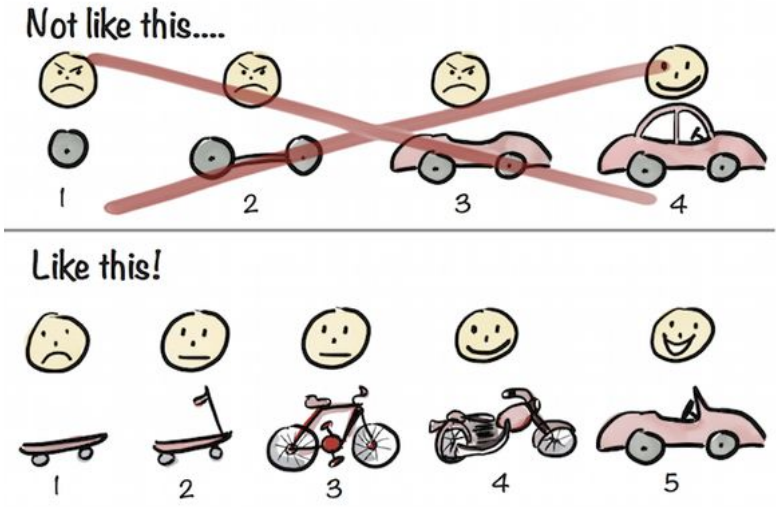
Task of System Administration:

- **Administration and planning**
  - documentation
  - time management
  - policy
  - self-education
  - planning
  - administrative tasks
- **Interaction with people**

Roles of System Administrator

Successful System Administrator:

- Need to find a balance between
  - Authority and responsibility
  - Service and cooperation
- A few Basic strategies
  - Plan it before you go it
  - Make it reversible
  - Make changes incrementally
  - Test, test, test before you unleash it on the world
  - Know how things REALLY work.



Example: editing system configuration files:

- Keep a copy before any change to the configuration file
  - For original version, using suffix of .dist, .orig
  - For further changes, using suffix of .old, .sav, .yymmdd, etc
- Keep the current modification date
- Plan how to back up if the change didn't work – say system does not even boot
  - Such as boot to single user mode and copy the old version back
- Test the change on a non-production environment first
- Eliminate the most obvious problems
- Make one major change at a time
- Make the test easier

What is Network Administration?

- An activity related with configuring, commissioning and maintenance of network infrastructure and services.
- Network administration is concerned with network infrastructure rather than users
- Network administrator is responsible to:
  - Ensure network connectivity
  - Network monitoring and management
  - Network security
  - Develop and enforce policy
  - Design and install network infrastructure

Roles of Network Administrator

- **Design network**
  - Deciding on the type of network that best suits the organization
  - It involves planning, budgeting and identifying the components
- **Setting up the network**
  - Installation and configuration of network equipments
  - It involves installing network hardware, configuring hosts, routers, switches, and network servers
- **Maintenance**
  - Making sure the network is available and it is providing the intended services
  - It is consists of day-to-day activities of network administration
  - Some of the activities are adding new hosts, administering network security, maintaining network services, troubleshooting network problems.
- **Expanding network**
  - Plan and design network expansion
  - Install and configure new network devices
  - Evaluate performance and security of network, and upgrade network hardware and software

Ethics

- What is ethics?
  - Conducting moral principles that govern a group of people
- A system administrator must be an ethical person
- Policies concerning computer use are generally either for users or admins

concerned with how computing professionals should make decisions regarding professional and social conduct.

Ten Commandments Of Computer Ethics

1. Thou Shalt Not Use A Computer To Harm Other People.
2. Thou Shalt Not Interfere With Other People's Computer Work.
3. Thou Shalt Not Snoop Around In Other People's Computer Files.
4. Thou Shalt Not Use A Computer To Steal.
5. Thou Shalt Not Use A Computer To Bear False Witness.
6. Thou Shalt Not Copy Or Use Proprietary Software For Which You have Not Paid.
7. Thou Shalt Not Use Other People's Computer Resources Without Authorization Or Proper Compensation.
8. Thou Shalt Not Appropriate Other People's Intellectual Output.
9. Thou Shalt Think About The Social Consequences Of The Program You Are Writing Or The System You Are Designing.
10. Thou Shalt Always Use A Computer In Ways That Insure Consideration And Respect For Your Fellow Humans.

Dr. Ramon C. Barquin, Computer Ethics Institute

Ethics: Code of conduct

- The integrity of a system and network administrator must be beyond reproach
  - Need to protect integrity and privacy of data
  - Must uphold law and policies as established for their systems
- A system and network administrator shall not unnecessarily infringe upon the rights of users
- The continuance of professional education is critical to maintaining currency as an administrator
  - Reading, study, training, and sharing knowledge and experiences are requirements

Ethics: Code of conduct

- A system administrator must maintain an exemplary work ethic
  - A sysadmin can have a significant impact on an organization – a high level of trust is maintained by exemplary behavior
- At all times system administrators must display professionalism in the performance of their duties
  - Need to be professional, even when dealing with management, vendors, users, or other sysadmins

Ethics: Code of conduct

- Need an Acceptable Use Policy
  - What is permitted and what is prohibited?
- Might combine with a monitoring/privacy policy
  - Explain that monitoring might happen as part of running the network/server
- There are many archived policies that are useful as starting points to develop new ones
  - Exercise: Surf for some policies

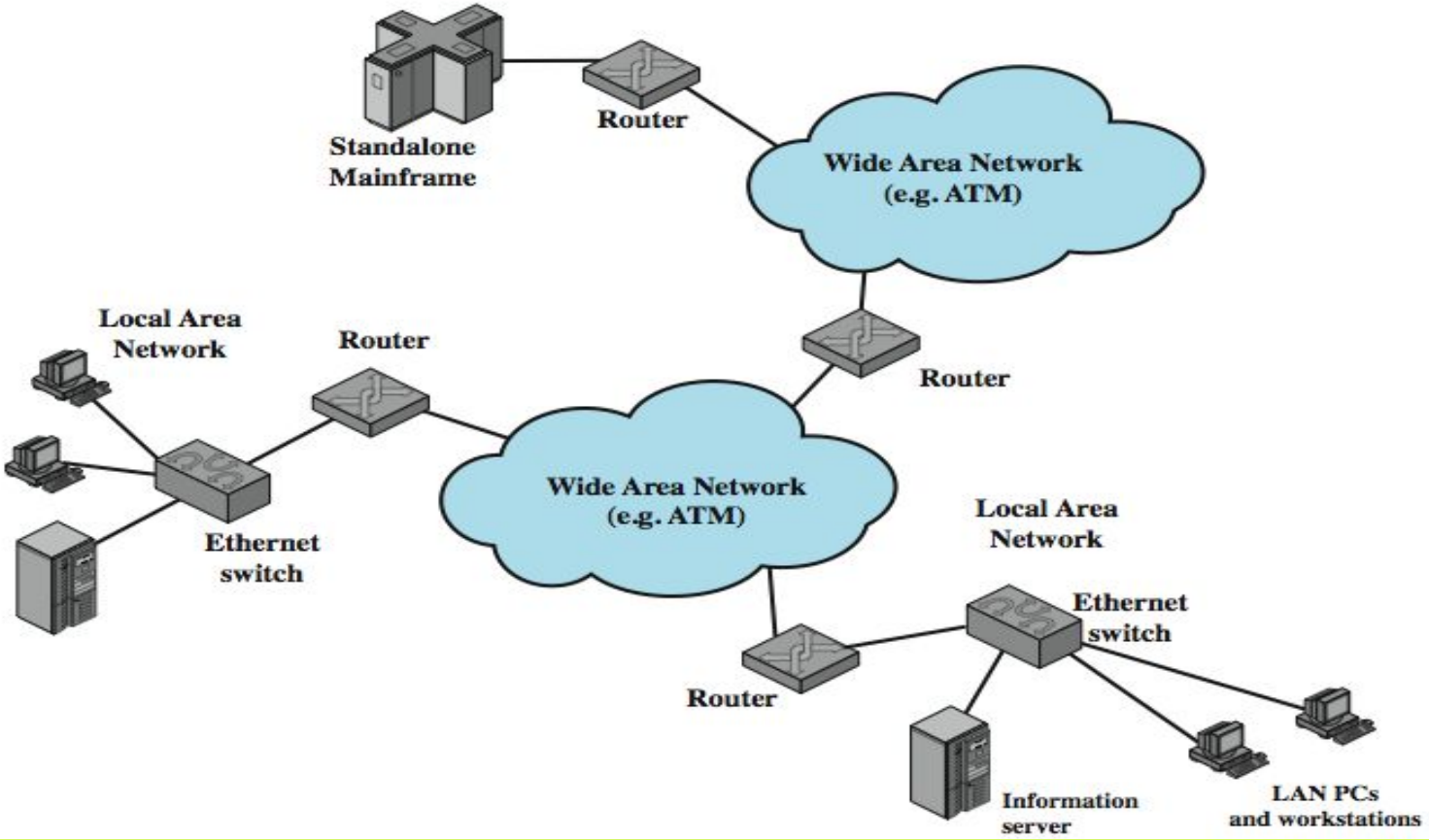
Review of Computer Networking

- What is Network?
  - *A network is a group of connected, communicating devices*
- What is internet?
  - *An internet is two or more networks that can communicate with each other.*
- What is *The Internet?*
  - A global internet based on the IP protocol
- Why do we need network?
  - *Share Resources, Information*

Requirements of Network

- Networks must be:
  - General Purpose
  - Open
- Networks are implemented by:
  - Hardware (hosts, media, switching elements)
  - Software (protocols and services)

Components of Network



Standard Components of Network

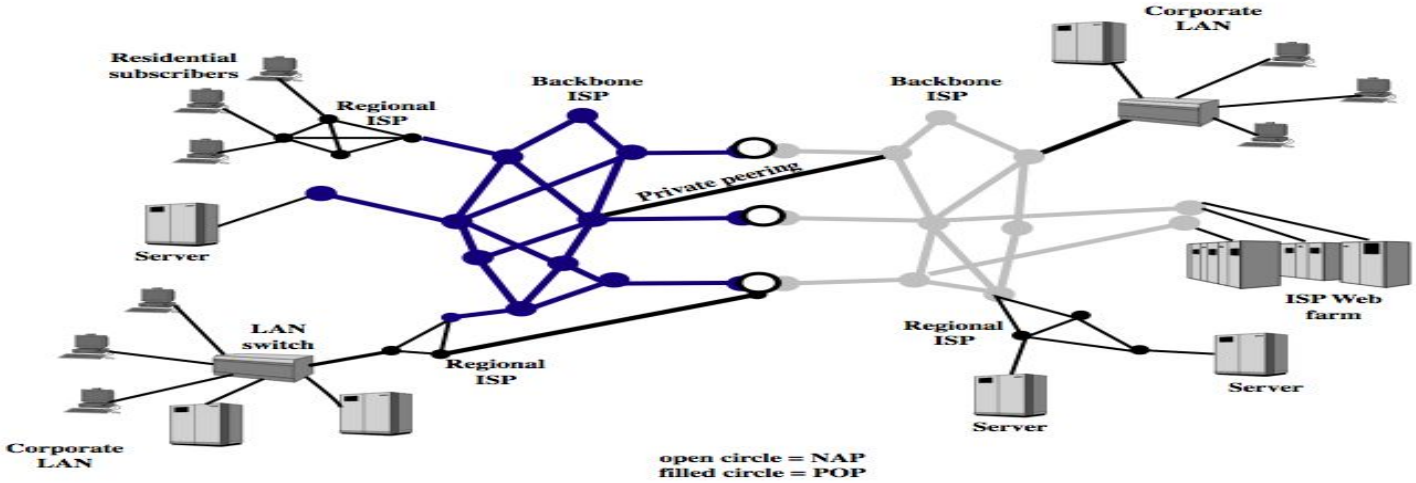
- Connection or cabling system:
  - Wired connection may be twisted-pair wiring, coaxial cable, or fiber optics.
  - Wireless connection may be infrared or radio-wave Transmission
- Interconnection devices:
  - Hubs, Switches, Routers, etc
- Microcomputer with interface card
- Network operating system

  Example: Ms Windows NT, Novell's NetWare, Linux

- Other shared devices
  - printers, fax machines, scanners, storage devices, and other peripherals

The Internet

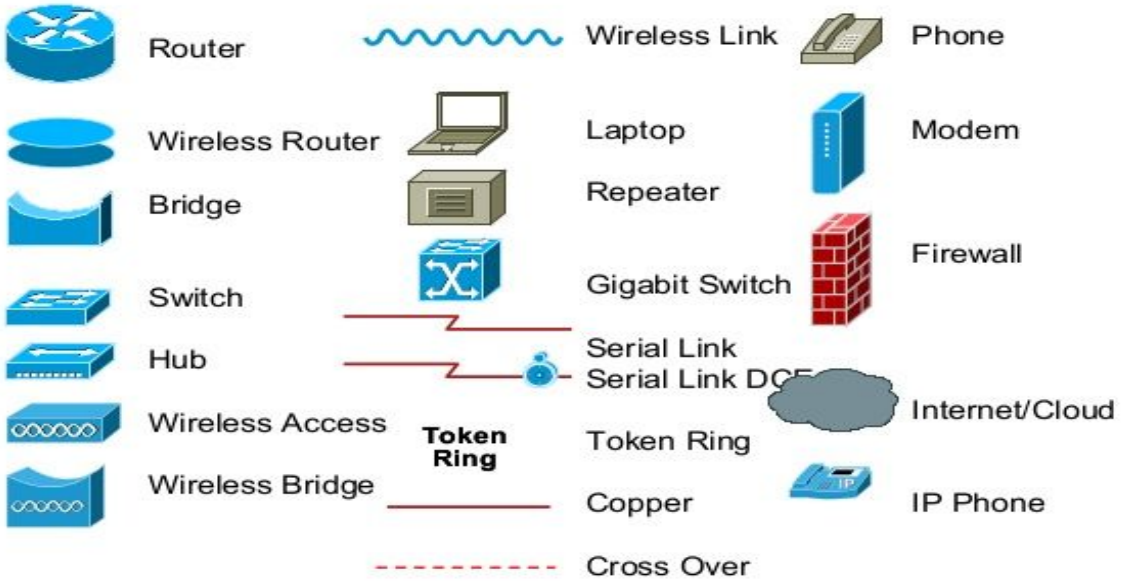
- Network of Networks
- The Internet is a global network of computers connecting individual computers and networks together into one huge network.
- Even if a main centre is not functioning, data can take a different route through the Internet to reach its final destination



Network Hardware

- Servers
  - File server
  - Database server
  - Mail server
  - Web server
  - Application server
  - DNS server
  - DHCP server
  - Proxy server

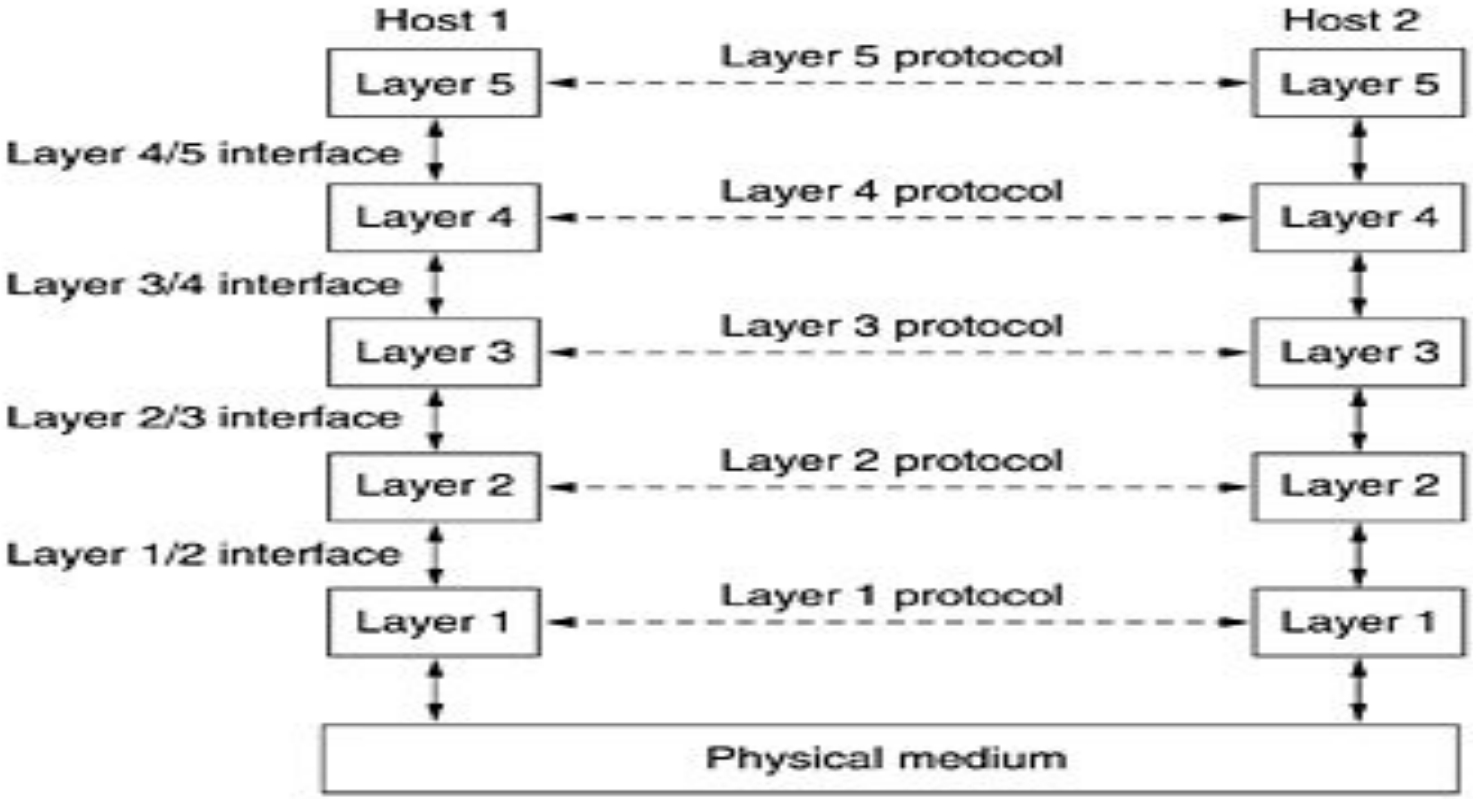
- **Interconnecting Devices**
  - Access point
  - Repeater
  - **Hub**
  - **Switch**
  - Bridge
  - Router
  - Firewall



Network Software

- Network software is now highly structured
- Most networks are organized as a stack of layers or levels, each one built upon the one below it.
- Layers differ from network to network
  - Name of each layer
  - Number of layers
  - contents of each layer
  - function of each layer
- The interface (between each adjacent layer) defines which primitive operations and services the lower layer makes available to the upper one

Network Software

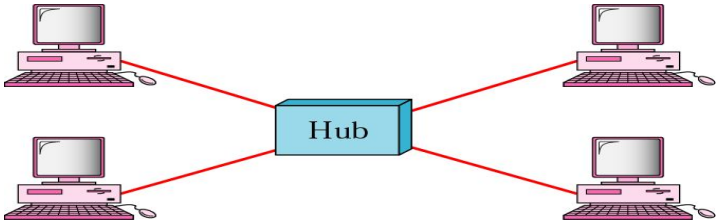


Network Software

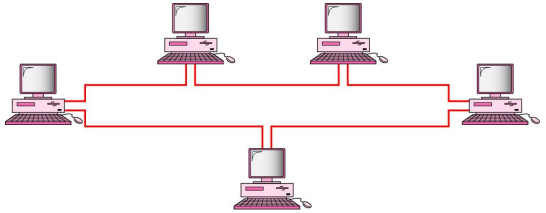
- A protocol is an agreement between the communicating parties on how communication is to proceed on a specific layer.
- A set of layers and protocols is called a network architecture
- The specification of an architecture must contain enough information to allow an implementer to write the program
- A list of protocols used by a certain system, one protocol per layer, is called a protocol stack
- Network architectures, protocol stacks, and the protocols themselves are the principal topics of this course

Network Topology

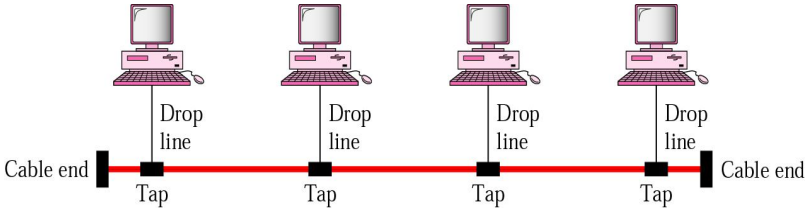
Star



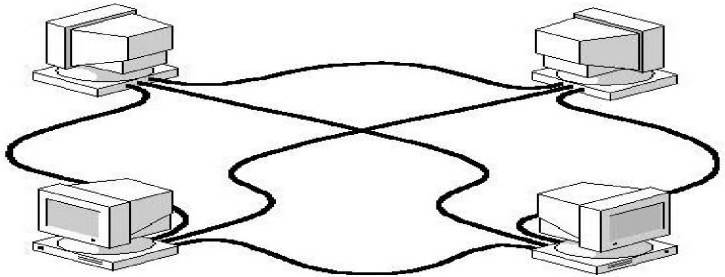
Ring



Bus



Mesh

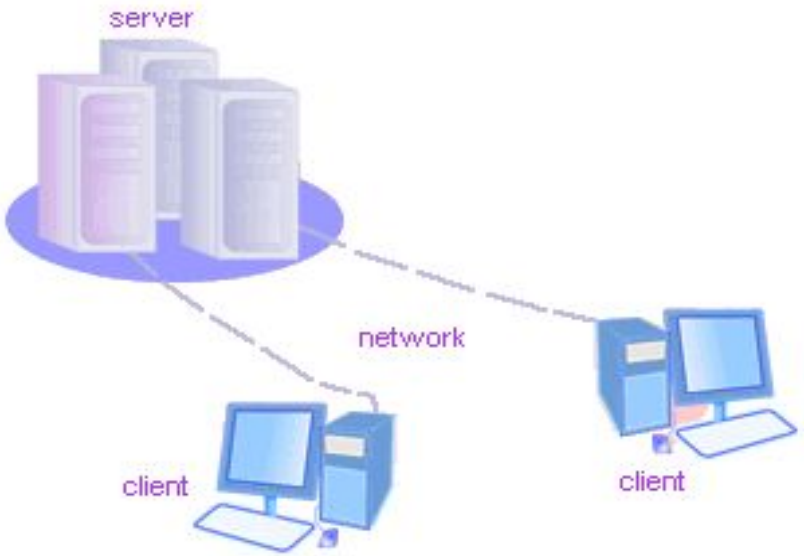


Types of Network

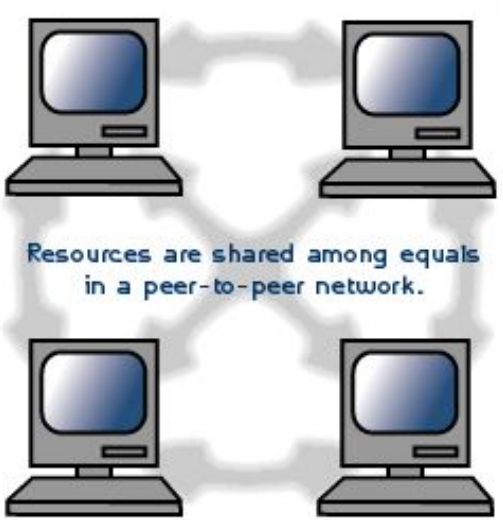
- Based on Architecture
  - Client-Server
  - Peer-to-Peer
- Based on geographical coverage
  - LAN
  - MAN
  - WAN

Types of Network

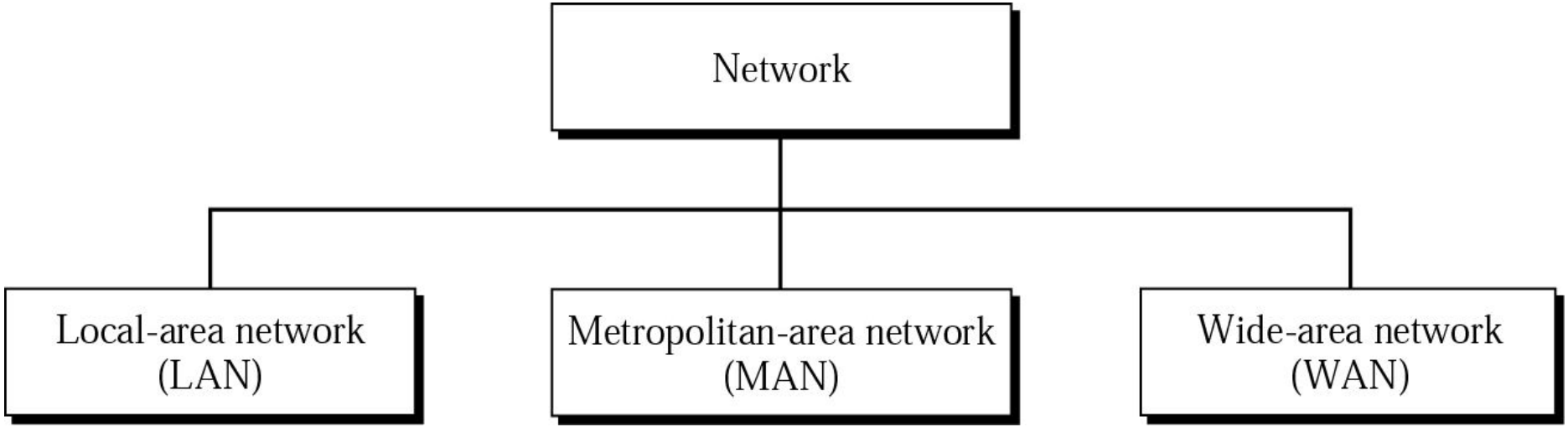
Client/Server



Peer-to-Peer



Types of Network



Protocols

- Cooperative action is necessary
  - computer networking is not only to exchange bytes
  - huge system with several utilities and functions.
  - Examples:
    - error detection
    - Encryption
    - Routing
    - etc.
- For proper communication, entities in different systems must speak the same language
  - there must be mutually acceptable conventions and rules about the content, timing and underlying mechanisms
- Those conventions and associated rules are referred as “PROTOCOLS”

Protocols Architecture

- Task of data transfer is broken up into some modules
  - Why?
  - How do these modules interact?
- For example, file transfer could use three modules
  - File transfer application
  - Communication service module
  - Network access module

- Two approaches (standard)
  - OSI Reference model
    - never used widely
    - but well known
  - TCP/IP protocol suite
    - Most widely used

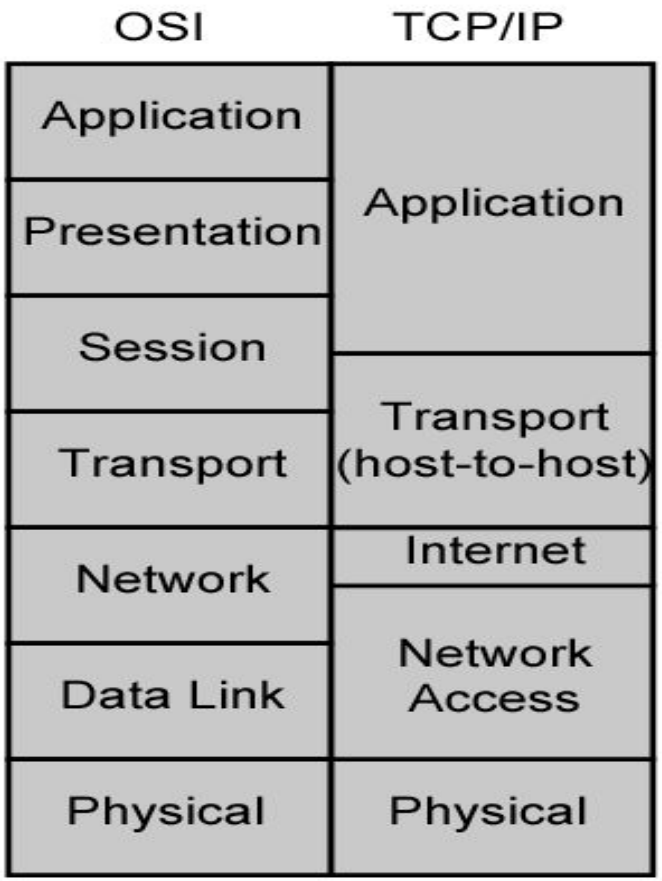
Protocols Architecture

7. Application	• Provides a user interface
6. Presentation	• Presents Data • Handles encryption and decryption
5. Session	• Maintains distinction between data of separate applications • Provides dialog control between hosts
4. Transport	• Provides End-to-End connections • Provides reliable or unreliable delivery and flow control
3. Network	• Provides Logical Addressing • Provides Path determination using logical addressing
2. Data Link	• Provides media access and physical addressing
1. Physical	• Converts digital data so that it can be sent over the physical medium • Moves data between hosts

Protocols Architecture

Layer #	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc…	Messages	n/a
4	Transport	TCP/UDP	Segments/ Datagrams	Port #s
3	Network or Internet	IP	Packets	IP Address
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address
1	Physical	10 Base T, 802.11	Bits	n/a

OSI vs TCP/IP

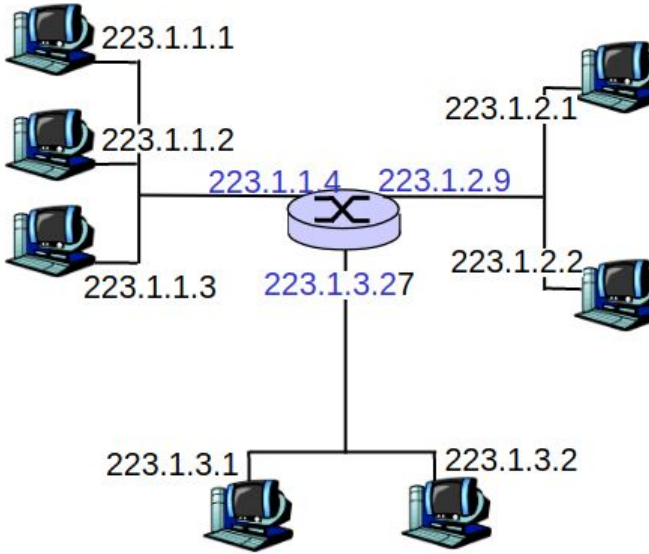

OSI
TCP/IP
Application
Presentation
Session
Transport
Network
Data Link
Physical
Application
Transport (host-to-host)
Internet
Network Access
Physical

Classful Addressing

- Class A – extremely large networks with more than 16 million host addresses.
- Class B – moderate to large size networks with more than 65,000 hosts.
- Class C – provide addresses for small networks with a maximum of 254 hosts.
- Class D – Multicasting
- Class E – Experimental

IP Addressing

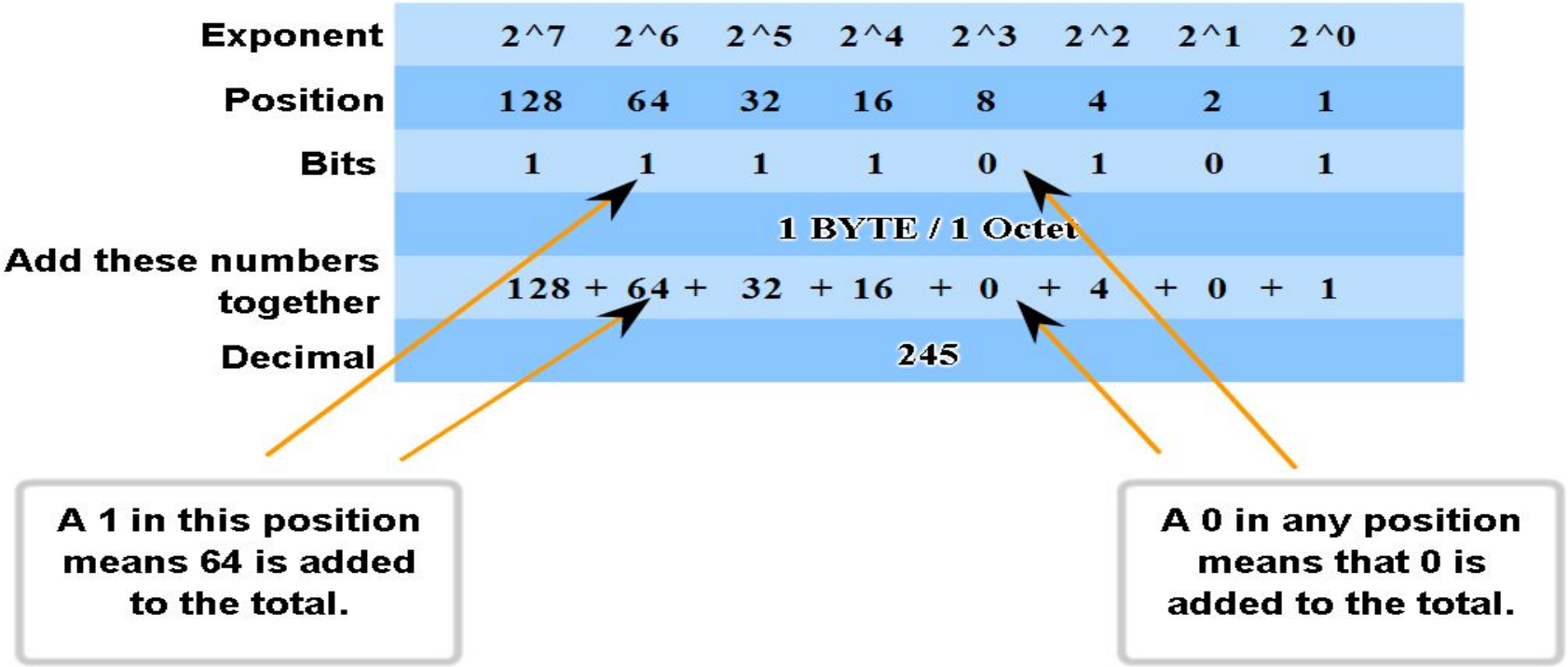
- IP address: 32-bit identifier for host, router *interface*
- *interface:* connection between host/router and physical link
  - router's typically have multiple interfaces
  - host typically has one interface
  - IP addresses associated with each interface



223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

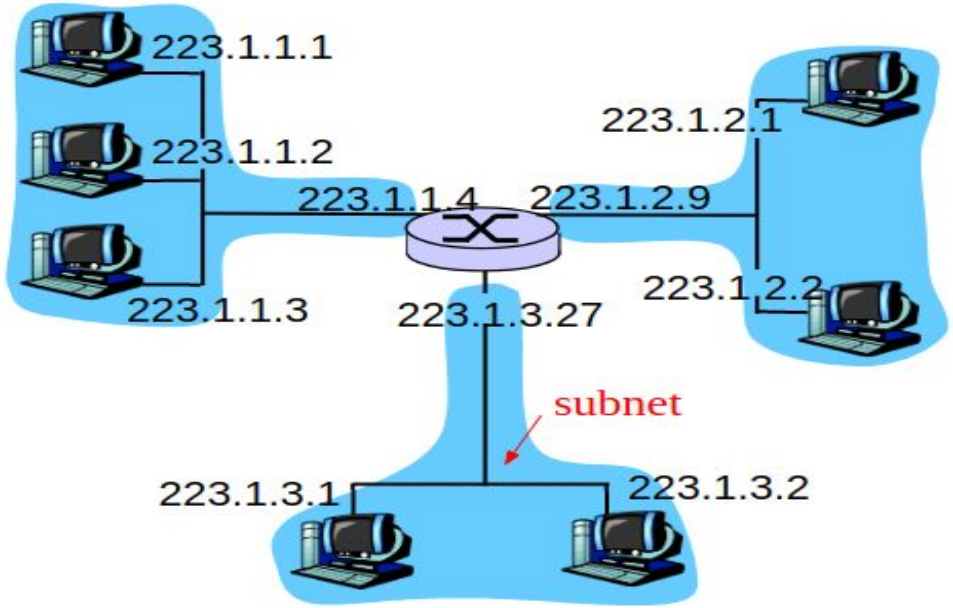
IP Addressing



11110101 in Binary = Decimal Number 245

IP Addressing

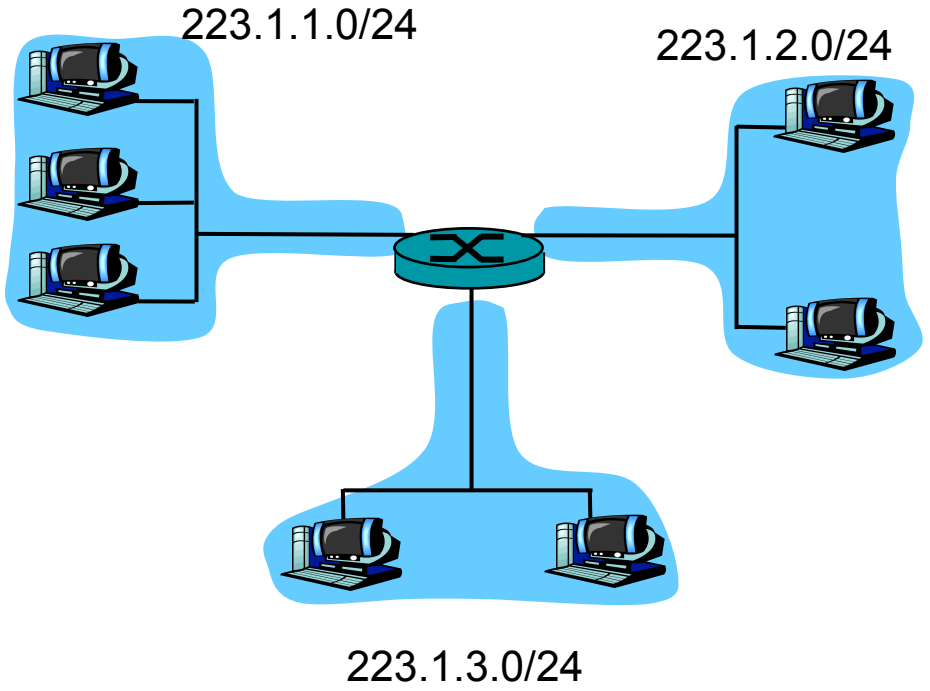
- IP address:
  - subnet part (high order bits)
  - host part (low order bits)
- *What's a subnet ?*
  - device interfaces with same subnet part of IP address
  - can physically reach each other without intervening router



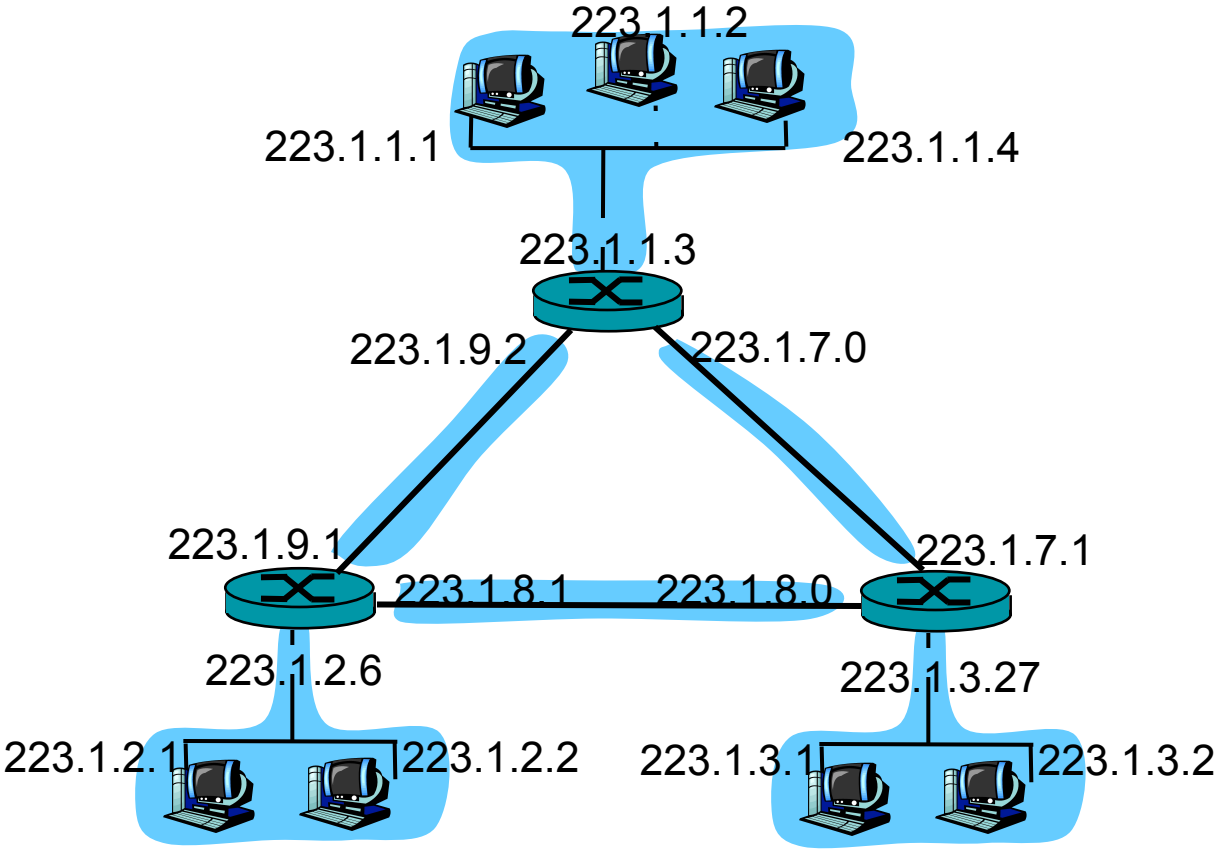
IP Addressing

Recipe

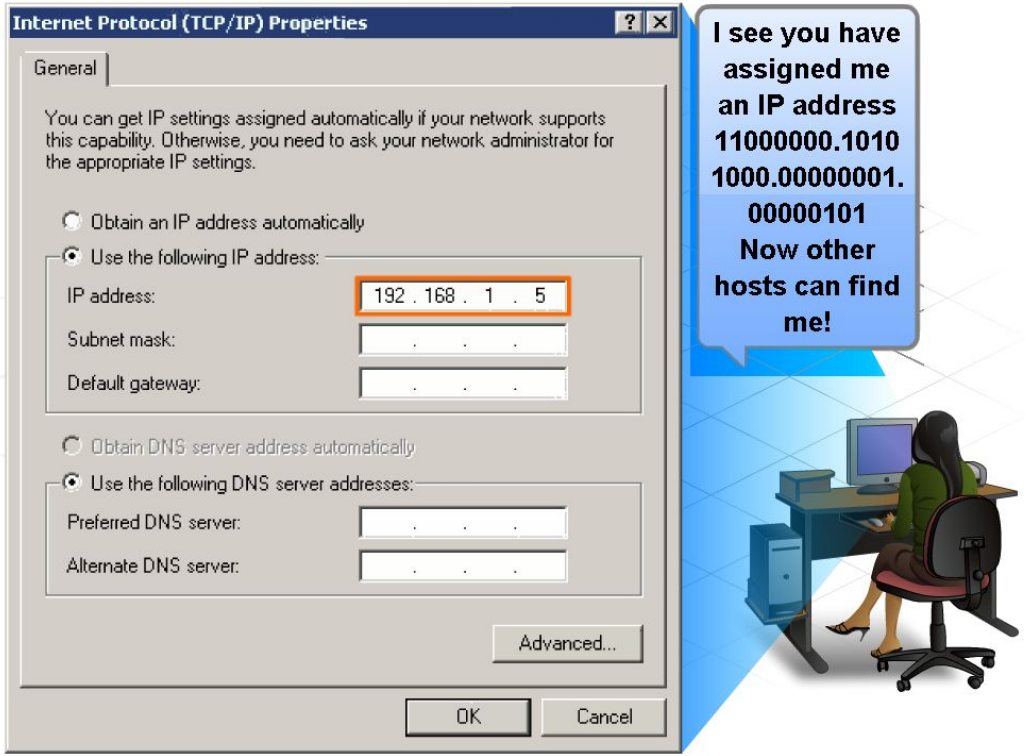
- To determine the subnets, detach each interface from its host or router, creating islands of isolated networks. Each isolated network is called a subnet.



IP Addressing



IP Addressing



IP version 4 (IPv4) is the current form of addressing used on the Internet.

IP Addressing

Network Address

Broadcast Address

Host Address

Address Types

	Network		Host
10	0	0	0
00001010	00000000	00000000	00000000
10	0	0	255
00001010	00000000	00000000	11111111
10	0	0	1
00001010	00000000	00000000	00000001

IP Addressing

- **Network**: The network address is a standard way to refer to a network.
  - AAU network can be referred 10.0.0.0/8
  - All hosts in AAU will address that starts with 10.0.0.0
  - The lowest address is reserved for the network address and the rest 0's are for the host address
- **Broadcast**
  - Special address for each network that allows communication to all the hosts in
  - AAU broadcast address is 10.255.255.255
  - The broadcast address uses the highest address in the network range
  - All the host bits are set to 1s.
  - in that network. To send data to all hosts in a network, a host can send a single packet that is addressed to the broadcast address of the network
- **Host**

  Every end device requires a unique address to deliver a packet to that host. In IPv4 addresses, we assign the values between the network address and the broadcast address to the devices in that network.

IP Addressing

- None of these addresses will be forwarded by a router and most can't be assigned to a device
  1. Network Address – FIRST address of any network
  2. Broadcast Address – LAST address of any network
  3. Default Route – 0.0.0.0 – (when a specific route is NOT available)
  4. Loopback Addresses – 127.0.0.1 – 127.255.255.255 – used to test the configuration of TCP/IP on the local host
  5. Link-Local Addresses - 169.254.0.0 to 169.254.255.255 These addresses can be automatically assigned to the local host by the OS in environments where no IP configuration is available.

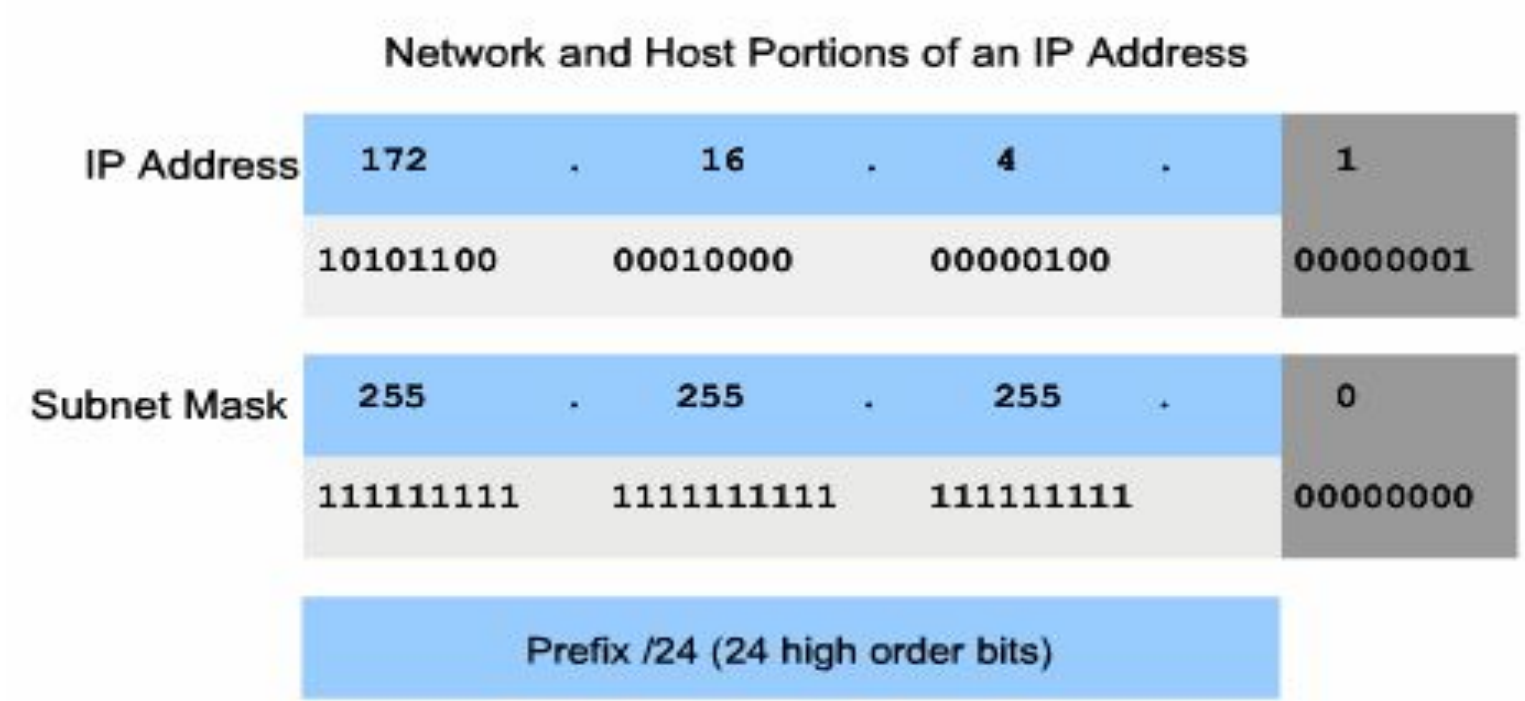
IP Addressing

Given the IP address **144.83.250.97/17**, Find:

Type	Last octet in Binary	Last octet in Decimal	Full address
Network	00000000	0	144.83.128.0
Broadcast	11111111	255	144.83.255.255
First usable IP	00000001	1	144.83.128.1
Last usable IP	11111110	254	144.83.255.254

IP Addressing

Determine the network portion of the host address and the role of the subnet mask



IP Addressing

Applying the Subnet Mask

A device with address 192.0.0.1 belongs to network 192.0.0.0

	High order bits Prefix /16		Low order bits	
	192 .	0 .	0 .	1
Host Address	11000000	00000000	00000000	00000001
Subnet Mask	255 11111111	255 11111111	0 00000000	0 00000000
Network Address	11000000	00000000	00000000	00000000
Network	192 .	0 .	0 .	0

- Use ANDing logic to determine an outcome

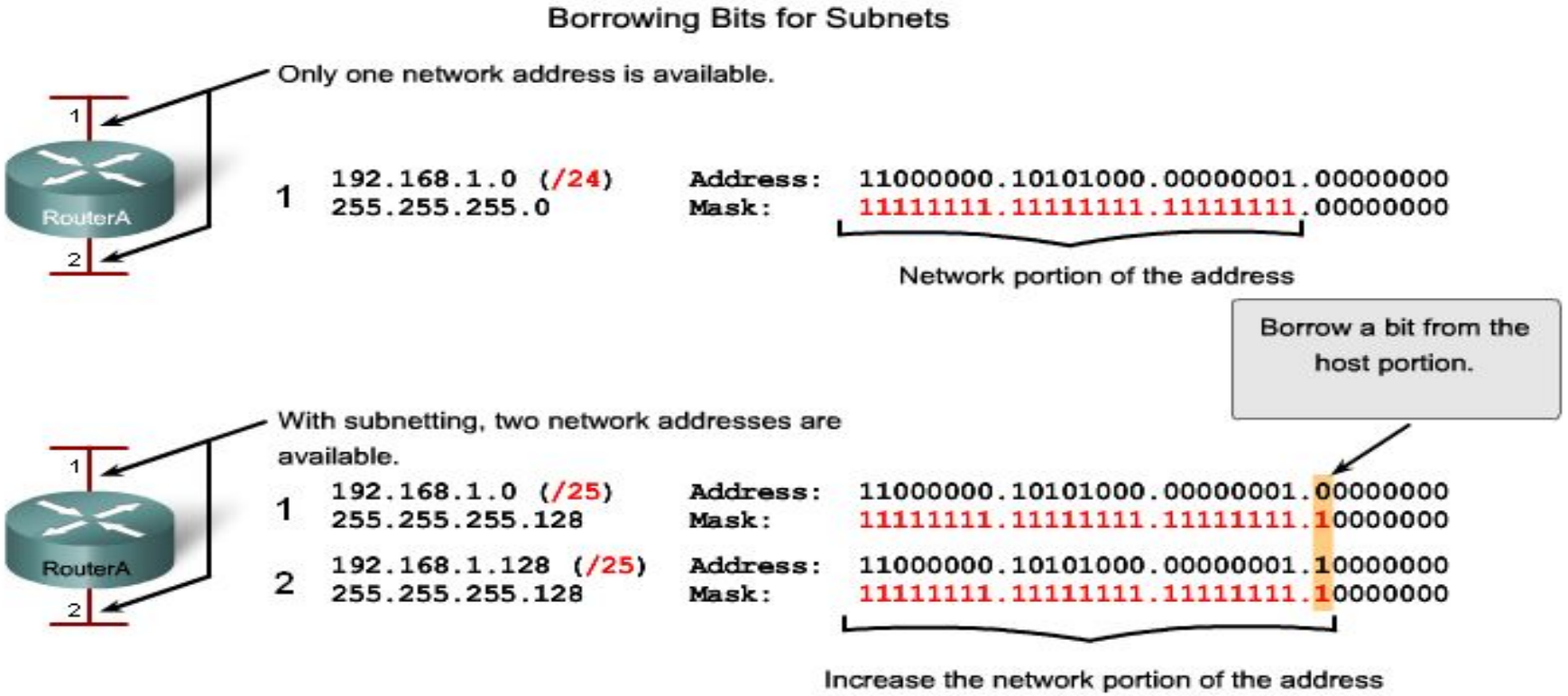
IP Addressing

Using the subnet mask to determine the network address for host 172.16.132.70/20

Convert binary network address to decimal

Host Address	172	16	132	70
Binary Host Address	10101100	00010000	10000100	01000110
Binary Subnet Mask	11111111	11111111	11110000	00000000
Binary Network Address	10101100	00010000	10000000	00000000
Network Address	172	16	128	0

IP Subnetting



- Use the subnet mask to divide a network into smaller networks

IP Subnetting

The 2 primary benefits of subnetting are:

- Fewer IP addresses, often as few as one, are needed to provide addressing to a network & subnetting.
- Subnetting usually results in smaller routing tables in routers beyond the local internetwork.

IP Subnetting

- Example of subnetting: when the network administrator divides the 172.20.0.0 network?
- We have to know how many bits should we borrow from the host number .
  - .i.e. $2^x>5$ when x is the minimum possible value .
  - X should be 3 , there for…….

IP Subnetting

- The key concept in subnetting is borrowing bits from the host portion of the network to create a subnetwork.
- Rules govern this borrowing, ensuring that some bits are left for a Host ID.
- The rules require that two bits remain available to use for the Host ID& that all of the subnet bits cannot be all 1s or 0s at the same time.

IP Subnetting

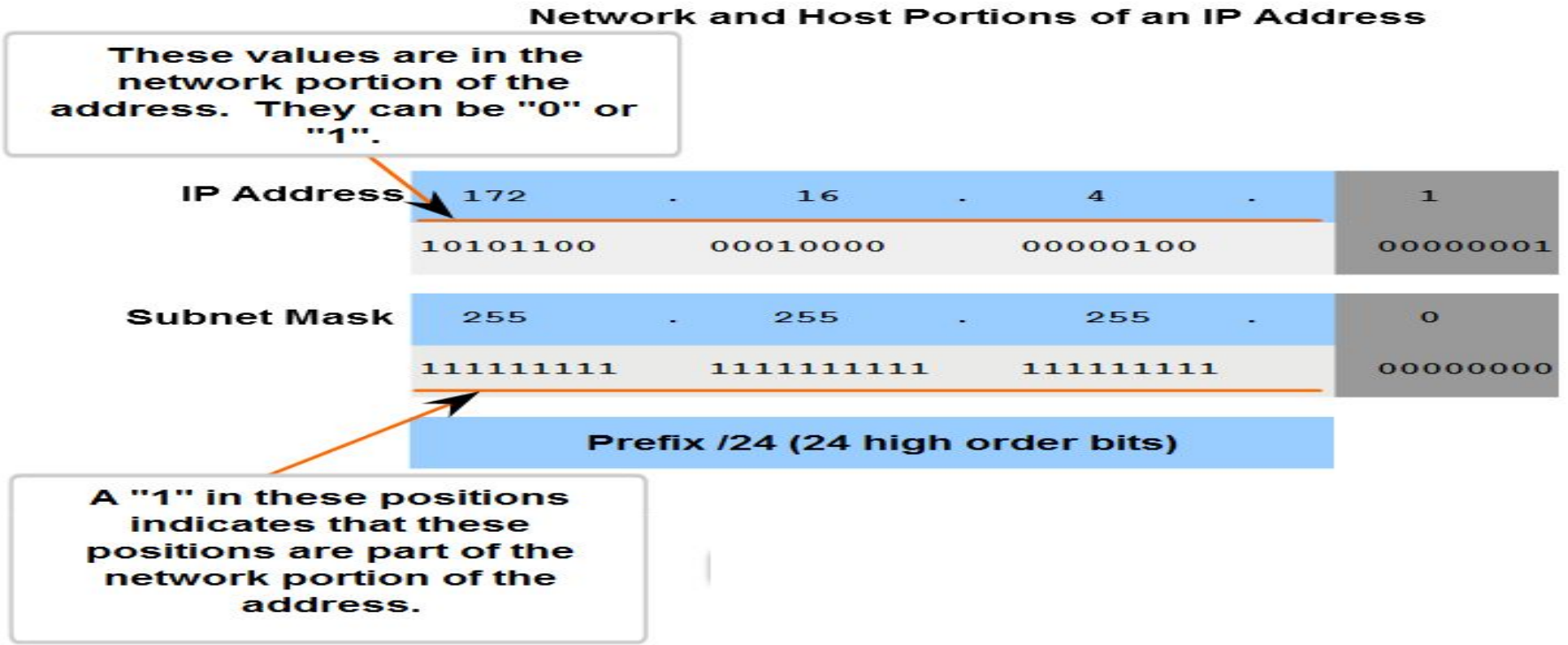
Mask	# Binary	#Subnet Bits	#Host Bits	Subnets	Hosts
255.255.255.128	10000000	1	7	2	126
255.255.255.192	11000000	2	6	4	62
255.255.255.224	11100000	3	5	8	30
255.255.255.240	11110000	4	4	16	14
255.255.255.248	11111000	5	3	32	6
255.255.255.252	11111100	6	2	64	2

IP Subnetting

- Suppose you are asked to determine the number of subnets available in 192.168.1.0/24
- Using the subnet & hosts formulas, the answers are easily calculated.
- Of course, you must know your powers of 2 to calculate the answers.
- How many subnets can be created in 192.168.1.0 with each subnet having at least 5 hosts?

IP Subnetting

- Prefix length /subnet mask specifies the number of bits for the network
- 172.16.4.1/24



IP Subnetting

Applying the Subnet Mask

A device with address 192.0.0.1 belongs to network 192.0.0.0

	High order bits Prefix /16		Low order bits	
	192 .	0 .	0 .	1
Host Address	11000000	00000000	00000000	00000001
Subnet Mask	255 11111111	255 11111111	0 00000000	0 00000000
Network Address	11000000	00000000	00000000	00000000
Network	192 .	0 .	0 .	0

IP Subnetting

- Dividing the Network into right size:
  - Every network within the internetwork of a corporation or organization is designed to accommodate a finite number of hosts.
  - Some networks, such as point-to-point WAN links, only require a maximum of two hosts.
  - Other networks, such as a user LAN in a large building or department, may need to accommodate hundreds of hosts.
- Network administrators need to devise the internetwork addressing scheme to accommodate the maximum number of hosts for each network.

IP Subnetting

- Network Administrators must Consider the following points:
  - Determine the Total Number of Hosts: This includes end user devices, servers, intermediate devices, and router interfaces
  - Determine the Number and Size of the Nets based on common groupings of hosts
  - We subnet our network to overcome issues with location, size, and control.
  - Grouping based on common geographic location
  - Grouping hosts used for specific purposes
  - Grouping based on ownership

IP Subnetting

- Given an address block of 192.168.1.0 /24, we need to create two subnets.
  - We borrow one bit from the host portion by using a subnet mask of 255.255.255.128, instead of the original 255.255.255.0 mask.
  - The most significant bit in the last octet is used to distinguish between the two subnets.
  - For one of the subnets, this bit is a "0" and for the other subnet this bit is a "1".
- Formula for calculating subnets we can create by borrowing bits of host address
  - 2^n where n = the number of bits borrowed
  - In this example, the calculation looks like this:
    - 2^1 = 2 subnets

IP Subnetting

- Formula for calculating the number of hosts in the subnet
  - 2^n - 2 where n = the number of bits left for hosts
- Applying this formula, (2^7 - 2 = 126) shows that each of these subnets can have 126 hosts.
- For each subnet, examine the last octet in binary. The values in these octets for the two networks are:
  - Subnet 1: 00000000 = 0
  - Subnet 2: 10000000 = 128

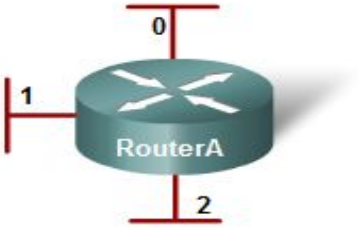
Addressing Scheme: Example of 2 networks

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255

IP Subnetting

- Example 2: consider an internetwork that requires three subnets. Again we start with the same 192.168.1.0 /24 address block.
- To provide more networks, we change the subnet mask to 255.255.255.192 and borrow two bits.
- Calculate the subnet : 2^2 = 4 subnets
- calculate the number of hosts, begin by examining the last octet:
  - Subnet 0: 0 = 00000000
  - Subnet 1: 64 = 01000000
  - Subnet 2: 128 = 10000000
  - Subnet 3: 192 = 11000000
- Apply the host calculation formula:
    - 2^6 - 2 = 62 hosts per subnet

IP Subnetting



Borrowing Bits for Subnets

-	192.168.1.0 (/24)	Address:	11000000.10101000.00010100.00000000
	255.255.255.0	Mask:	11111111.11111111.11111111.00000000
0	192.168.1.0 (/26)	Address:	11000000.10101000.00010100.00000000
	255.255.255.192	Mask:	11111111.11111111.11111111.11000000
1	192.168.1.64 (/26)	Address:	11000000.10101000.00010100.01000000
	255.255.255.192	Mask:	11111111.11111111.11111111.11000000
2	192.168.1.128 (/26)	Address:	11000000.10101000.00010100.10000000
	255.255.255.192	Mask:	11111111.11111111.11111111.11000000
3	192.168.1.192 (/26)	Address:	11000000.10101000.00010100.11000000
	255.255.255.192	Mask:	11111111.11111111.11111111.11000000

Two bits are borrowed to provide four subnets.

Unused address in this example.

A 1 in these positions in the mask means that these values are part of the network address.

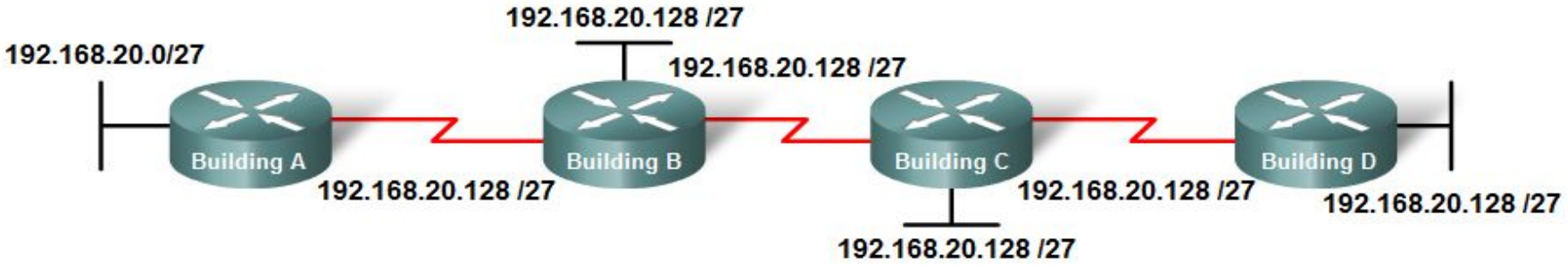
IP Subnetting

- Given an IP address 192.168.1.0/24
- Create four subnets and identify range of host addresses.

Addressing Scheme: Example of 4 networks

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

IP Subnetting



Subnet Number	Subnet Address
Subnet 0	192.168.20.0/27
Subnet 1	192.168.20.32/27
Subnet 2	192.168.20.64/27
Subnet 3	192.168.20.96/27
Subnet 4	192.168.20.128/27
Subnet 5	192.168.20.160/27
Subnet 6	192.168.20.192/27
Subnet 7	192.168.20.224/27

- Given an IP address 192.168.20.0/24
- Create eight subnets and identify range of host addresses.

Network Devices Configuration

Active Network Devices:

- Routers
- Switches
- Firewalls
- Wireless Controllers
- Access Points
- AA servers

Network Devices Configuration

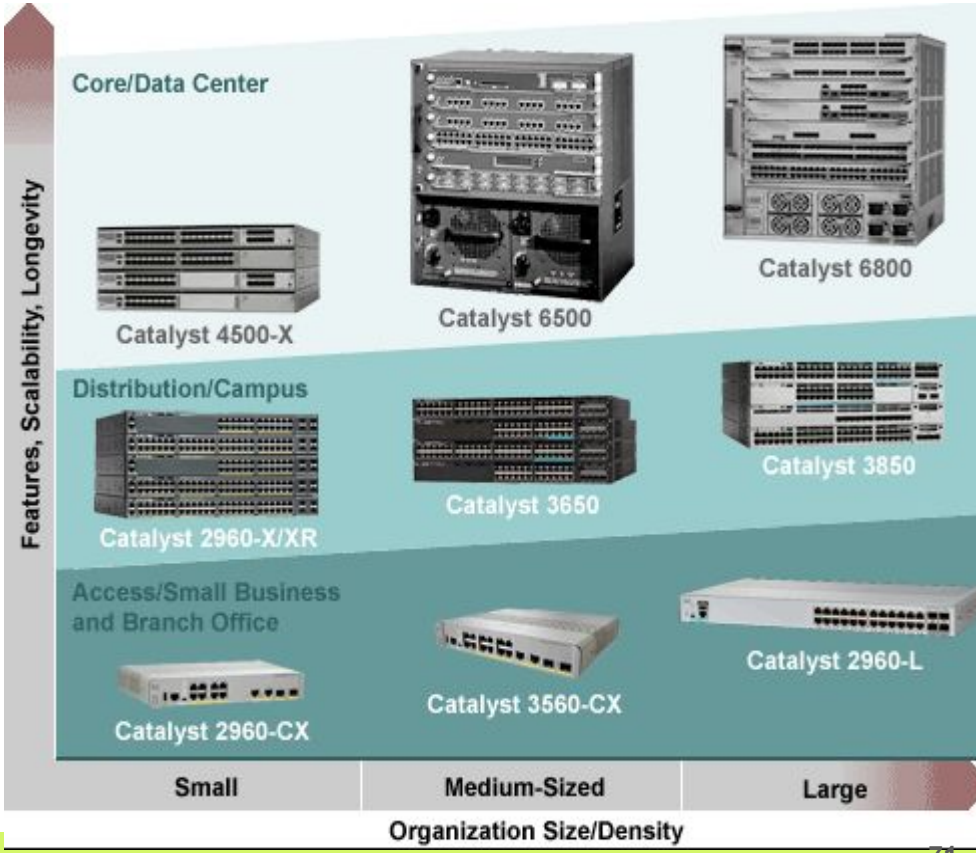
Router configuration (L3):

- Static Routing
- Dynamic Routing
- Security
- Interfaces
  - address
  - bandwidth
  - clock
  - duplex
- DHCP
- Access control

Network Devices Configuration

Switch configuration (L2):

- Port
- Security
- VLAN
- Remote management
- Access control



Network Devices Configuration

Firewall Configuration:

- Interfaces
- Routing and interfaces
- Access List
- Application inspection
- QoS
- VPN
- NAT
- Availability
- Access Control

Thank you.

Getnet M.
getnet.mamo@aau.edu.et