1 Networking Overview

1.1 History

1.2 **Protocol Standards – *networking protocols overview***

1.3 Reference Model (OSI, TCP/IP)

1.3.1 Overview, comparison OSI and TCP-IP

1.4 Windows and Linux Networking Basics -*overview*

1.5 Switching and Routing basics – *Circuit/packet/message switching, Unicast/multicast/broadcast/anycast routing overview*

1.1 History

- DARPA began as the Advanced Research Projects Agency (ARPA) created in 1958 by President Dwight D. Eisenhower for the purpose of forming and executing research and development projects to expand the frontiers of technology and science and able to reach far beyond immediate military requirements.
- The administration was responding to the Soviet launching of Sputnik 1 in 1957, and ARPA's mission was to ensure U.S. military technology be more sophisticated than that of the nation's potential enemies.
- DARPA’s original mission, established in 1958, was to prevent technological surprise like the launch of Sputnik, which signaled that the Soviets had beaten the U.S. into space. The mission statement has evolved over time.
- ARPA was renamed to "DARPA" (for Defense) in March 1972, then renamed "ARPA" in February 1993, and then renamed "DARPA" again in March 1996

- *1961-1972: Early packet-switching principles*
  - 1961: Kleinrock - queueing theory shows effectiveness of packet-switching.
  - 1964: Baran – packet-switching in military nets

  - 1967: ARPAnet conceived by Advanced Research Projects Agency.
  - 1969: First ARPAnet node operational

  - 1972:
    - ARPAnet public demonstration
    - NCP (Network Control Protocol) first host-host protocol
    - First e-mail program
    - ARPAnet has 15 nodes

- *1972-1980: Internetworking, new and proprietary nets*
  - 1970: ALOHAnet satellite network in Hawaii
  - 1974: Cerf and Kahn - architecture for interconnecting networks
  - 1976: Ethernet at Xerox PARC
  - Late70's: proprietary architectures: DECnet, SNA, XNA
  - late 70's: switching fixed length packets (ATM precursor)
  - 1979: ARPAnet has 200 nodes

- Cerf and Kahn's networking principles:

  - Minimalisem, autonomy – no internal changes required to interconnect networks
  - Best effort service model
  - Stateless routers
  - Decentralized control define today's Internet architecture
- 1983: deployment of TCP/IP
- 1982: smtp e-mail protocol defined
- 1983: DNS defined for name-to-IP-address translation
- 1985: FTP protocol defined
- 1988 TCP congestion control
- 1990, 2000's: Commercialization, the Web, new apps
  - Early 1990's: ARPAnet decommissioned.
  - 1991: NFS lifts restrictions on commericial use of NSFnet (decommissioned, 1995)
  - Early 1990's: Web
    - Hybertext [Bush 1945, Nelson 1960's]
    - HTML, HTTP: Berners-Lee
    - 1994: Mosaic, later Netscape
    - Late 1990's: commercialization of Web
- Late 1990's – 2000's:
  - More killer apps: instant messaging, P2P file sharing
  - Network security to forefront
  - Est. 50 million host, 100 million+users
  - Backbone links running on Gbps

- 2007:
  - ~500 million hosts
  - Voice, Video over IP
  - P2P applications: BitTorrent (file sharing), Skype (VoIP), PPLive (Video)
  - More applications: YouTube, gaming
  - Wireless, mobility

1.2 Protocols and Standards

Network Protocols

- Protocol suites are collections of protocols that helps network communication between hosts.
- A protocol is a formal description of a set of rules and conventions that govern a particular aspect of how devices on a network communicate.
- Protocols determine the format, timing, sequencing, and error control in data communication.
- Without protocols, the computer cannot make or rebuild the stream of incoming bits from another computer into the original format.

- Protocols control all aspects of data communication, which include the following:
  - How the physical network is built
  - How computers connect to the network

    - How the data is formatted for transmission
    - How that data is sent
    - How to deal with errors
  - These network rules are created and maintained by many different organizations and committees. Included in these groups are the Institute of Electrical and Electronic Engineers (IEEE), American National Standards Institute (ANSI), Telecommunications Industry Association (TIA), Electronic Industries Alliance (EIA) and the International Telecommunications Union (ITU).

1.3 REFERENCE MODEL

- There are basically two reference model.
  - OSI model
  - TCP/IP model

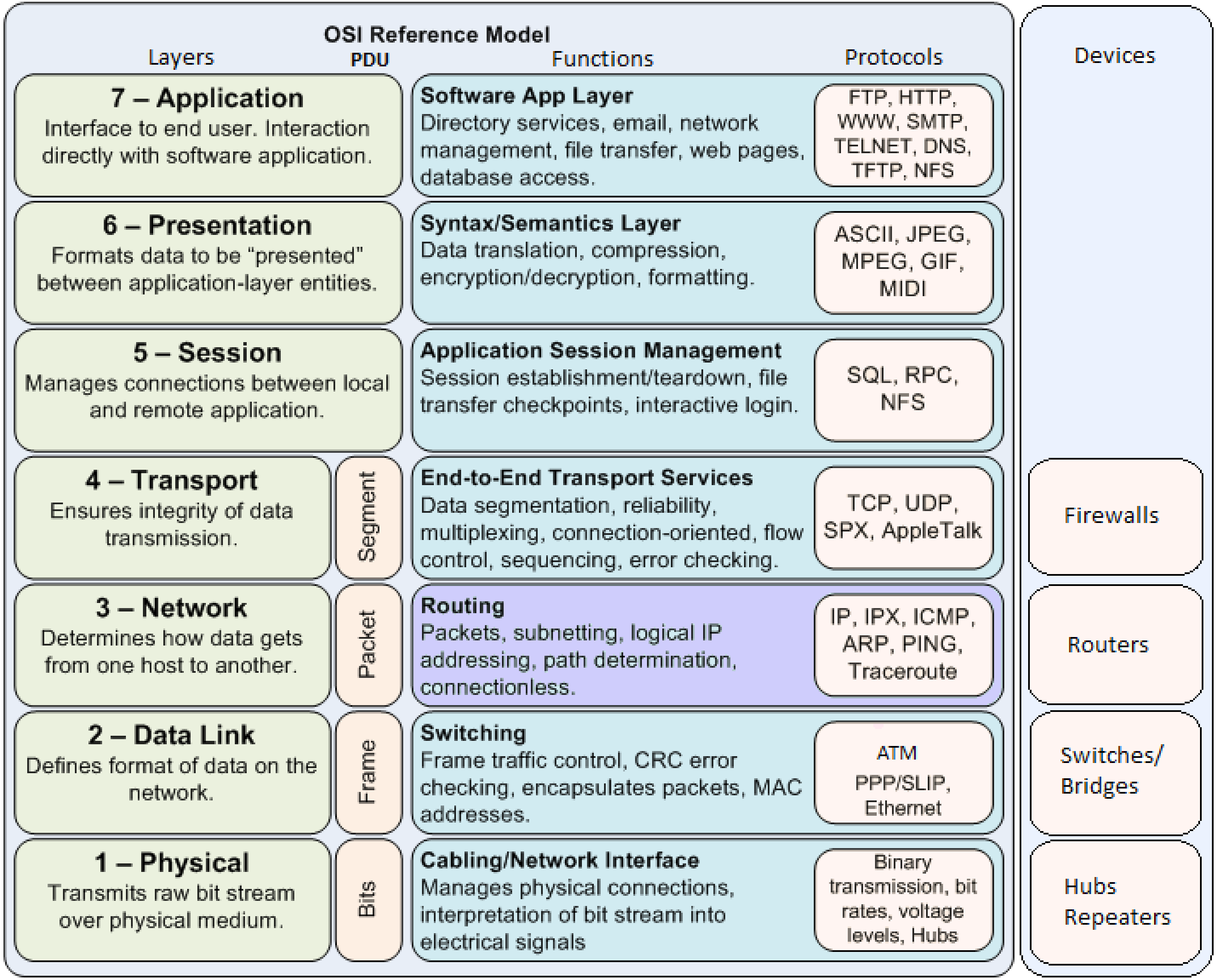
Open Systems Interconnection (OSI) Reference Model

- The OSI reference model is a framework that is used to understand how information travels throughout a network.
- The OSI reference model explains how packets travel through the various layers to another device on a network, even if the sender and destination have different types of network media.

- In the OSI reference model, there are seven numbered layers, each of which illustrates a particular network function. Dividing the network into seven layers provides the following advantages:
    - It breaks network communication into smaller, more manageable parts.
    - It standardizes network components to allow multiple vendor development and support.
    - It allows different types of network hardware and software to communicate with each other.
    - It prevents changes in one layer from affecting other layers.
    - It divides network communication into smaller parts to make learning it easier to understand.

OSI Reference Model

- In the OSI reference model, there are seven numbered layers, each of which illustrates a particular network function.



OSI Reference Model

Layers	PDU	Functions	Protocols	Devices
7 – Application Interface to end user. Interaction directly with software application.		**Software App Layer** Directory services, email, network management, file transfer, web pages, database access.	FTP, HTTP, WWW, SMTP, TELNET, DNS, TFTP, NFS	
6 – Presentation Formats data to be "presented" between application-layer entities.		**Syntax/Semantics Layer** Data translation, compression, encryption/decryption, formatting.	ASCII, JPEG, MPEG, GIF, MIDI	
5 – Session Manages connections between local and remote application.		**Application Session Management** Session establishment/teardown, file transfer checkpoints, interactive login.	SQL, RPC, NFS	
4 – Transport Ensures integrity of data transmission.	Segment	**End-to-End Transport Services** Data segmentation, reliability, multiplexing, connection-oriented, flow control, sequencing, error checking.	TCP, UDP, SPX, AppleTalk	Firewalls
3 – Network Determines how data gets from one host to another.	Packet	**Routing** Packets, subnetting, logical IP addressing, path determination, connectionless.	IP, IPX, ICMP, ARP, PING, Traceroute	Routers
2 – Data Link Defines format of data on the network.	Frame	**Switching** Frame traffic control, CRC error checking, encapsulates packets, MAC addresses.	ATM PPP/SLIP, Ethernet	Switches/ Bridges
1 – Physical Transmits raw bit stream over physical medium.	Bits	**Cabling/Network Interface** Manages physical connections, interpretation of bit stream into electrical signals	Binary transmission, bit rates, voltage levels, Hubs	Hubs Repeaters

Application Layer (Layer 7)

- Provides user interface using network application software
- Provide the different network services to the user eg, email, www, ftp, http, smtp etc
- Identification of network services is done using port numbers.

  HTTP →80

  FTP →20, 21

  SMTP→ 25

  TFTP→69

  SSH→22

- Protocol Data Unit (PDU): Data

Presentation Layer (Layer 6)

- Data representation
- Conversion of data into standard format eg, ASCII, JPEG, HTML, MP3
- Encoding and decoding
- Encryption and decryption
- Compression and decompression
- Protocol Data Unit (PDU): Data

Session Layer (Layer 5)

- Session Management
- Establish, maintain and terminate sessions
- Track all the event through the use
- Session ID keeps multiple sessions logically separate, for eg, multiple web pages can be opened and maintain different session simultaneously
- Protocol Data Unit (PDU): Data

Transport Layer (Layer 4)

- End to end connection
- Identifying service type (reliable or unreliable)
- Multiplexing and de-multiplexing
- Segmentation of messages
- Sequencing and reassembling
- Error correction
- Flow control and congestion control
- Protocol Data Unit (PDU): Segment/Datagram

Network Layer (Layer 3)

- Provides best path for data to reach the destination
- IP addressing (logical addressing)
- Routed and routing protocols
  - Routed protocols →IP, IPX
  - Routing protocols →RIP, OSPF
- Protocol Data Unit(PDU): Packet

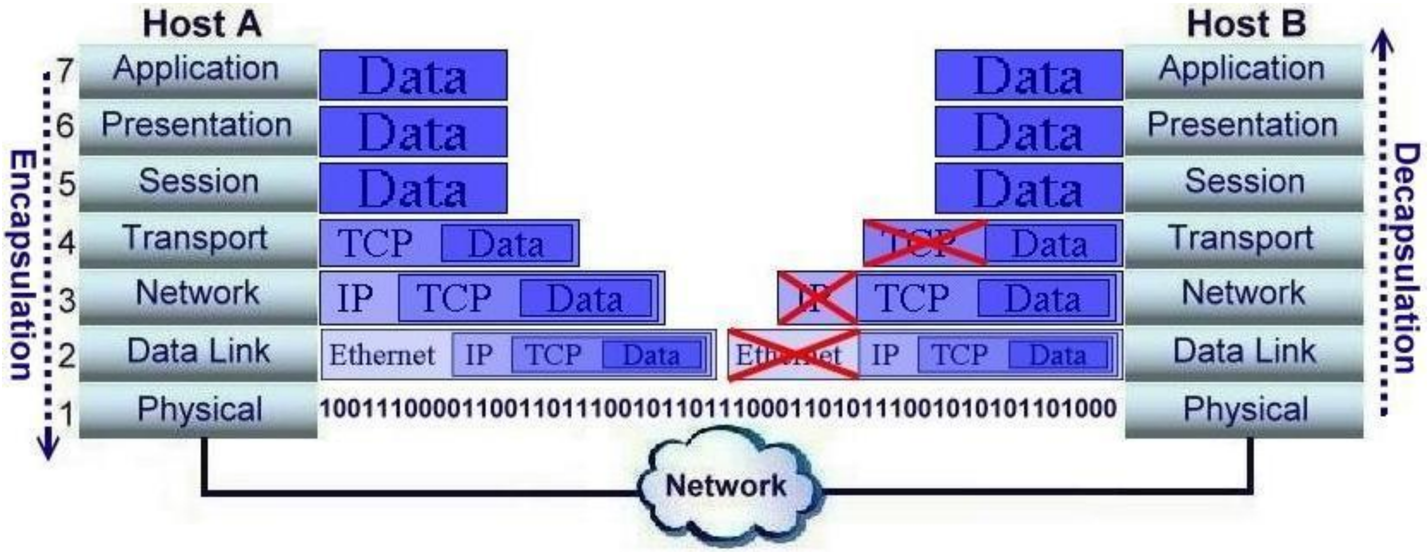
The Data Link Layer (Layer 2)

- Access to different media
- Transfer data between adjacent nodes with the help of physical address(MAC address)
- Sublayers
  - LLC(Logical Link Control)-deals with upper layer protocols
  - MAC(Media Access Control)- deals with lower layer protocols
- Error detection with the help FCS(Frame Check Sequence) field
- Protocol Data Unit(PDU): Frame

Physical Layer (Layer 1)

- Concern with data transmission
- Wires and their specification
- Connector for the system to connect
- Voltage (voltage at which the binary data is being assign and transmitted)
- Data rate (rate at which bit is transmit)
- Protocol Data Unit(PDU): bits

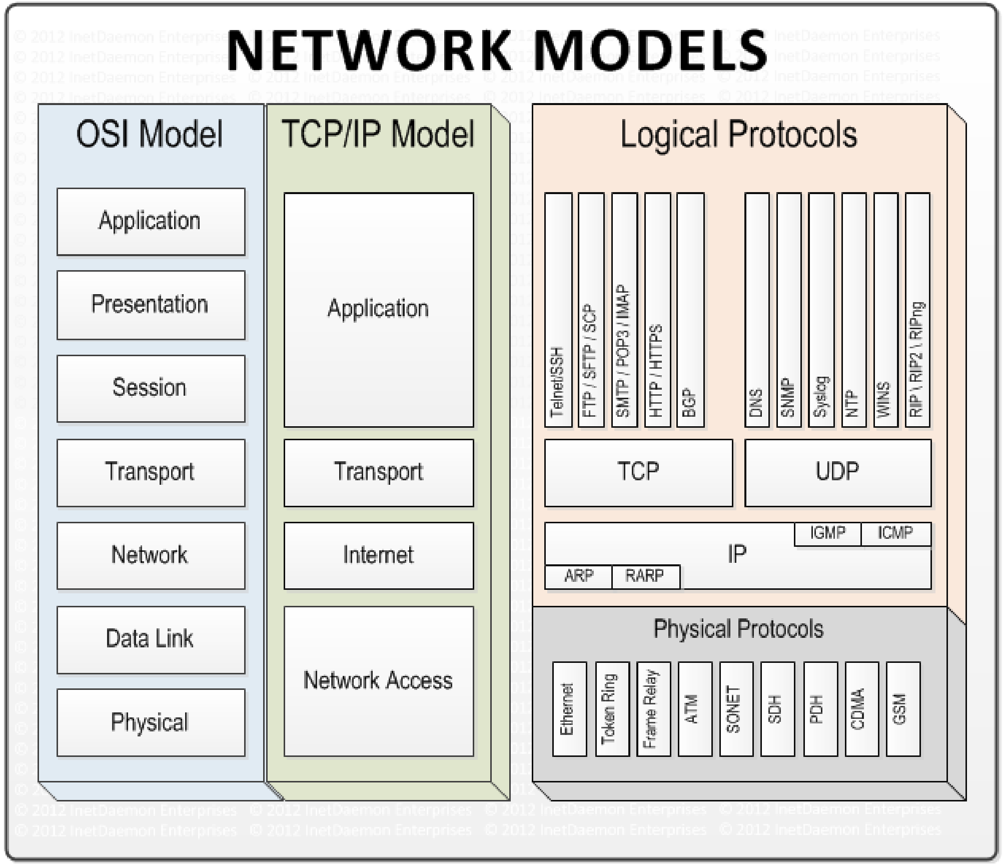
Data encapsulation and decapsulation process



TCP/IP Model

- The The U.S. Department of Defense (DoD) created the TCP/IP reference model, because it wanted to design a network that could survive any conditions, including a nuclear war.
- In a world connected by different types of communication media such as copper wires, microwaves, optical fibers and satellite links, the DoD wanted transmission of packets every time and under any conditions.
- This very difficult design problem brought about the creation of the TCP/IP model.
- TCP/IP was developed as an open standard. This meant that anyone was free to use TCP/IP. This helped speed up the development of TCP/IP as a standard.
- The TCP/IP model has the following four layers:
  - Application layer
  - Transport layer
  - Internet layer
  - Network access layer

TCP/IP Model


NETWORK MODELS
OSI Model
Application
Presentation
Session
Transport
Network
Data Link
Physical
TCP/IP Model
Application
Transport
Internet
Network Access
Logical Protocols
Telnet/SSH
FTP / SFTP / SCP
SMTP / POP3 / IMAP
HTTP / HTTPS
BGP
DNS
SNMP
Syslog
NTP
WINS
RIP \ RIP2 \ RIPng
TCP
UDP
IP
IGMP
ICMP
ARP
RARP
Physical Protocols
Ethernet
Token Ring
Frame Relay
ATM
SONET
SDH
PDH
CDMA
GSM
© 2012 InetDaemon Enterprises

1.4 Windows and Linux Networking Basics

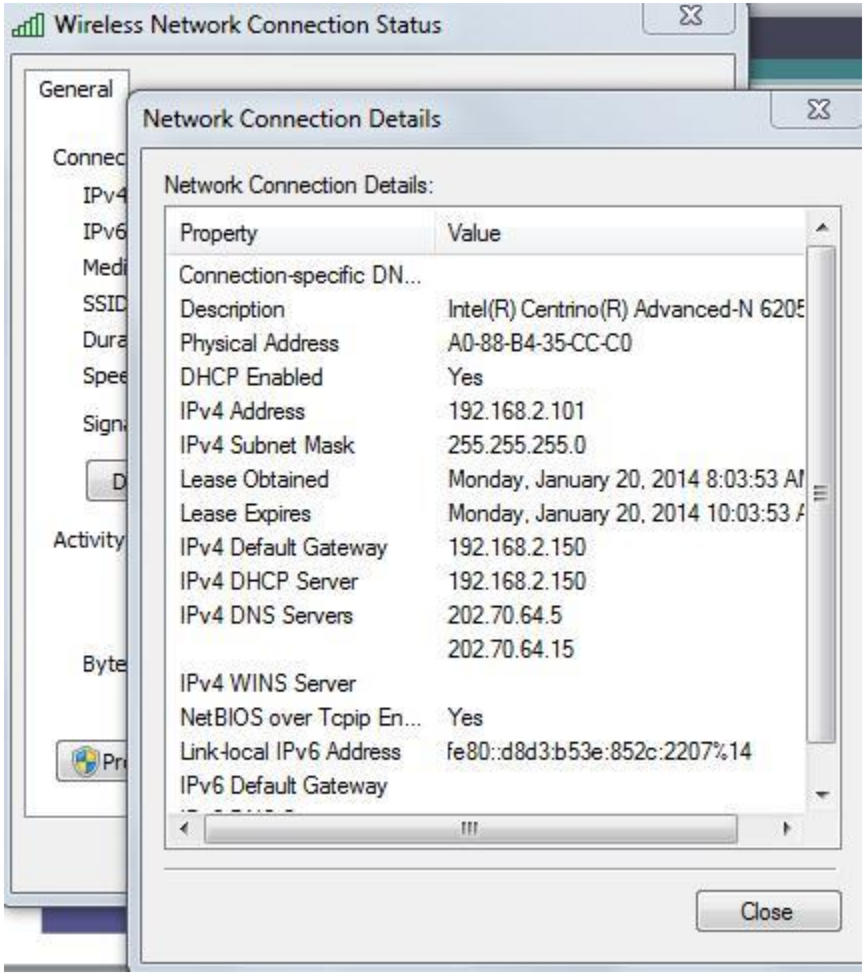
- Linux/Windows can be configured as a networked workstation, a DNS server, a DHCP server, a web server, a mail server, a file and print server, database server, a firewall, a gateway router and many more
- A server and a client computer must have an ip address so that it can be reach in network environment.
- Linux server can serves networking 365 days a year without any problem. It's a proof that Linux is a very stable and secure network operating system when properly configured and maintained.
- All that starts with setting up a network card and configure an ip address for the server.

Check IP address In Windows

```
• C:\Users>ipconfig /all
Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . :
Description . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6205
Physical Address. . . . . . . . . : A0-88-B4-35-CC-C0
DHCP Enabled. . . . . . . . . . . : Yes
IPv4 Address. . . . . . . . . . . : 192.168.2.101
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Monday, January 20, 2014 8:03:53 AM
Lease Expires . . . . . . . . . . : Monday, January 20, 2014 10:03:53 AM
```

Check IP address In Windows



Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Intel(R) Centrino(R) Advanced-N 6205
Physical Address	A0-88-B4-35-CC-C0
DHCP Enabled	Yes
IPv4 Address	192.168.2.101
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Monday, January 20, 2014 8:03:53 AM
Lease Expires	Monday, January 20, 2014 10:03:53 A
IPv4 Default Gateway	192.168.2.150
IPv4 DHCP Server	192.168.2.150
IPv4 DNS Servers	202.70.64.5
	202.70.64.15
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::d8d3:b53e:852c:2207%14
IPv6 Default Gateway	

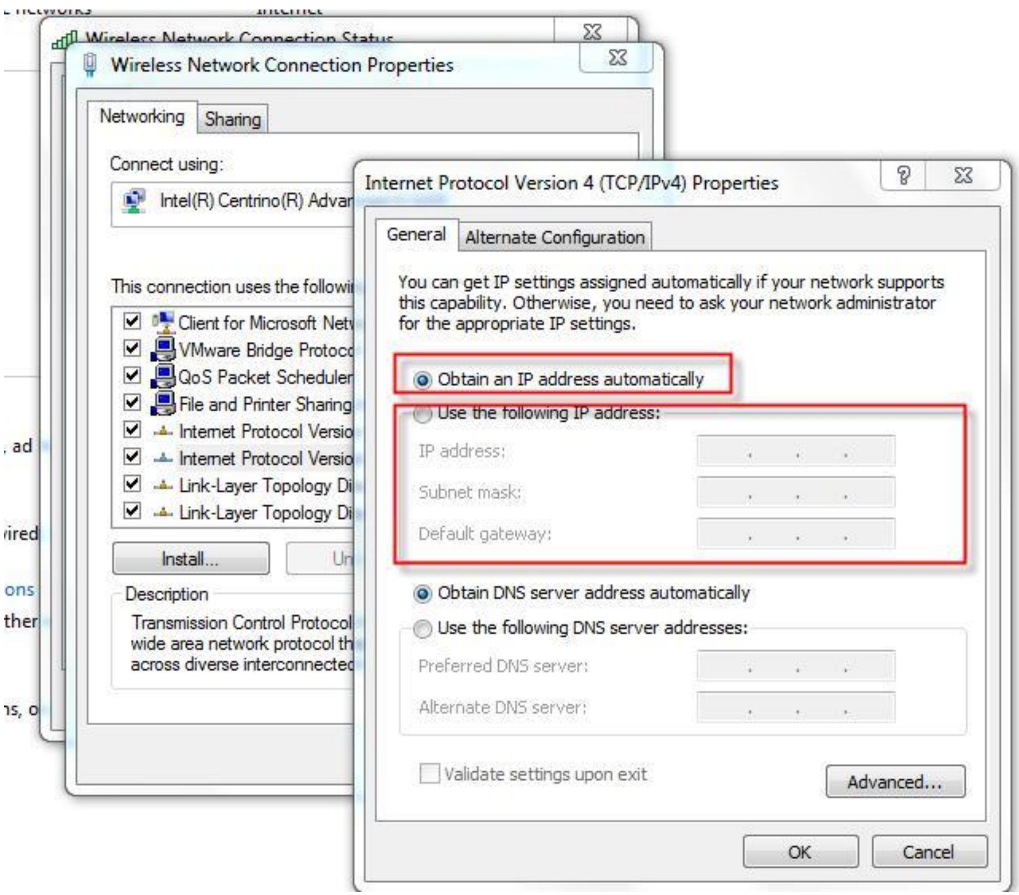
Set IP address from cmd in windows

- ***netsh interface ipv4 set address “local area connection” static 192.168.1.2 255.255.255.0 192.168.1.254***
- ***netsh interface ipv4 set dnsservers “local area connection” static 192.168.1.200***
- These commands will configure the Local Area Connection with a static IP, netmask, gateway, and DNS server.
- ***netsh interface ipv4 set address name=”local area connection” source=dhcp***
- ***netsh interface ipv4 set dnsservers name=”local area connection” source=dhcp***

Set IP Address in Windows Using GUI

Run and type

ncpa.cpl



Wireless Network Connection Status
Wireless Network Connection Properties
Networking
Sharing
Connect using:
Intel(R) Centrino(R) Advar
This connection uses the followi
☑ Client for Microsoft Netw
☑ VMware Bridge Protoco
☑ QoS Packet Scheduler
☑ File and Printer Sharing
☑ Internet Protocol Versio
☑ Internet Protocol Versio
☑ Link-Layer Topology Di
☑ Link-Layer Topology Di
Install...
Un
Description

Transmission Control Protocol
wide area network protocol th
across diverse interconnected

Internet Protocol Version 4 (TCP/IPv4) Properties

General
Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Check IP Address In Linux

```
[root@user ~]# ifconfig
eth0            Link encap:Ethernet HWaddr 98:4B:E1:66:E0:18
inet addr:202.44.42.10 Bcast:202.70.64.63 Mask:255.255.255.192
inet6 addr: 2407:1400::9a4b:e1ff:fe66:e018/64 Scope:Global inet6 addr: fe80::9a4b:e1ff:fe66:e018/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:1309835495 errors:0 dropped:0 overruns:0 frame:0
TX packets:962373448 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000
RX bytes:751156471551 (699.5 GiB) TX bytes:2252561585773 (2.0 TiB)
```

Set IP Address in Linux using Terminal

- **Set IP Address and gateway**
  - ifconfig eth0 192.168.1.2 netmask 255.255.255.0
  - Ifconfig eth0 192.168.100.1/24
  - ifconfig eth0 inet6 add 9901::2/64
  - route add –net default gw 192.168.100.254
- **Set Primary and Secindary DNS**
  - echo “nameserver 202.70.64.5” > /etc/resolv.conf
  - echo “nameserver 202.70.64.15” >> /etc/resolv.conf
- **Delete From Linux Interface**
  - Linux - IPv4 : "ifconfig eth1 del 2.2.2.3 netmask 255.255.255.0"
  - Linux - IPv6 : "ifconfig eth1 inet6 del 9901::2/64"

Set IP Address in Linux directly from network configuration file

```
#vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

```
DEVICE=”eth0”
BOOTPROTO=”static”
HWADDR=”98:4b:e1:66:e0:18”
ONBOOT=”yes”
TYPE=”Ethernet”
IPV6INIT=”no”
NM_CONTROLLED="yes“
IPADDR=”192.168.200.1”
NETMASK=”255.255.255.0”
```

Save and exit

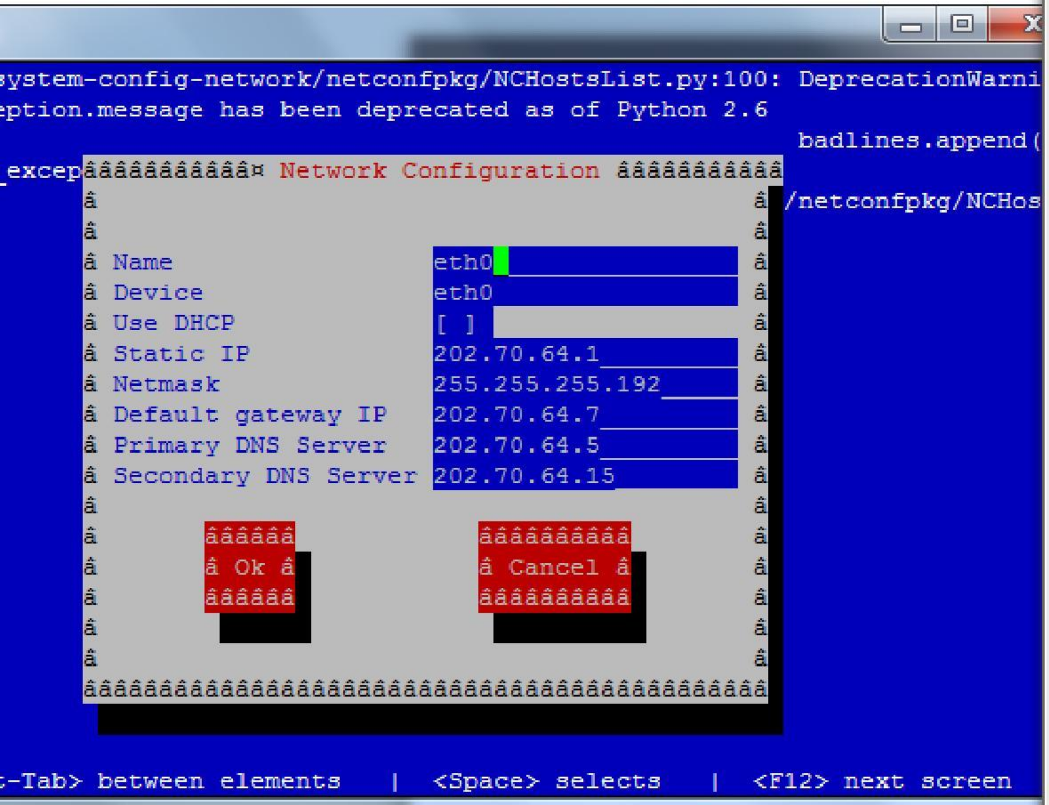
esc

:wq

```
#service network  restart
```

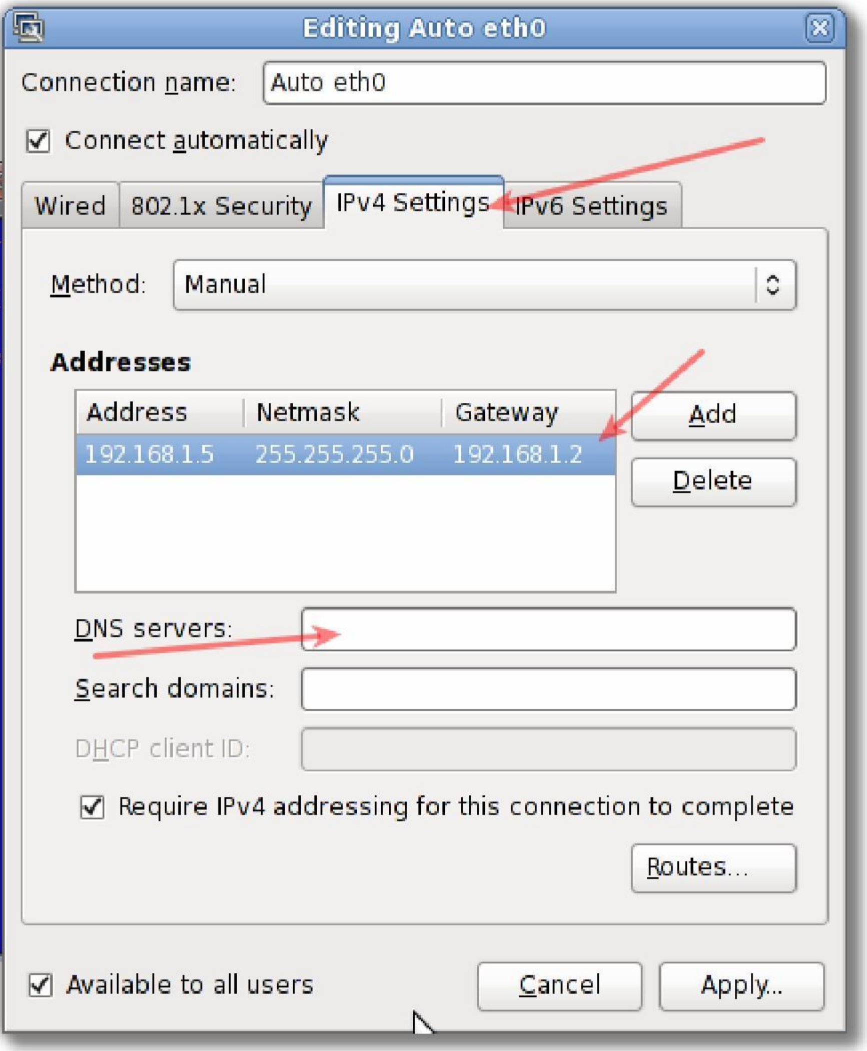
Set IP Address in Linux using graphical mode

# system-config-network



```
ystem-config-network/netconfpkg/NCHostsList.py:100: DeprecationWarni
eption.message has been deprecated as of Python 2.6
                                                    badlines.append(
_excepââââââââââââ¤ Network Configuration ââââââââââââ
      â                                             â /netconfpkg/NCHos
      â                                             â
      â Name                 eth0                   â
      â Device               eth0                   â
      â Use DHCP             [ ]                    â
      â Static IP            202.70.64.1_________   â
      â Netmask              255.255.255.192_____   â
      â Default gateway IP   202.70.64.7_________   â
      â Primary DNS Server   202.70.64.5_________   â
      â Secondary DNS Server 202.70.64.15________   â
      â                                             â
      â        ââââââ             âââââââââââ       â
      â        â Ok â             â Cancel â        â
      â        ââââââ             âââââââââââ       â
      â                                             â
      â                                             â
      âââââââââââââââââââââââââââââââââââââââââââââââ

-Tab> between elements   |  <Space> selects   |  <F12> next screen
```



Editing Auto eth0

Connection name: Auto eth0

☑ Connect automatically

Wired | 802.1x Security | IPv4 Settings | IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.1.5	255.255.255.0	192.168.1.2

DNS servers:

Search domains:

DHCP client ID:

☑ Require IPv4 addressing for this connection to complete

☑ Available to all users

1.5 Switching and Routing Basics

Comparision

- Switching involves moving packets between devices on the same network. Conversely, routing involves moving packets between different networks.
- Switches operate at layer 2 of the OSI Model. A switch, also referred to as a multi-port bridge, is able to determine where a packet should be sent by examining the MAC address within the data link header of the packet (the MAC address is the hardware address of a network adapter).
- A switch maintains a database called MAC address table which contains MAC addresses, VLAN number and what port they are connected to.
- Routers, on the other hand, operate at layer 3 of the OSI Model. A router is able to determine where to send a packet using the Network ID within the Network layer header.
- A router maintains a database called Routing tables which contains destination network address, next-hop IP, exit interface, administrative distance, metric to make decision by routing algorithm for best route.

Switching Types

I. Circuit Switching
II. Message Switching
III. Packing Switching

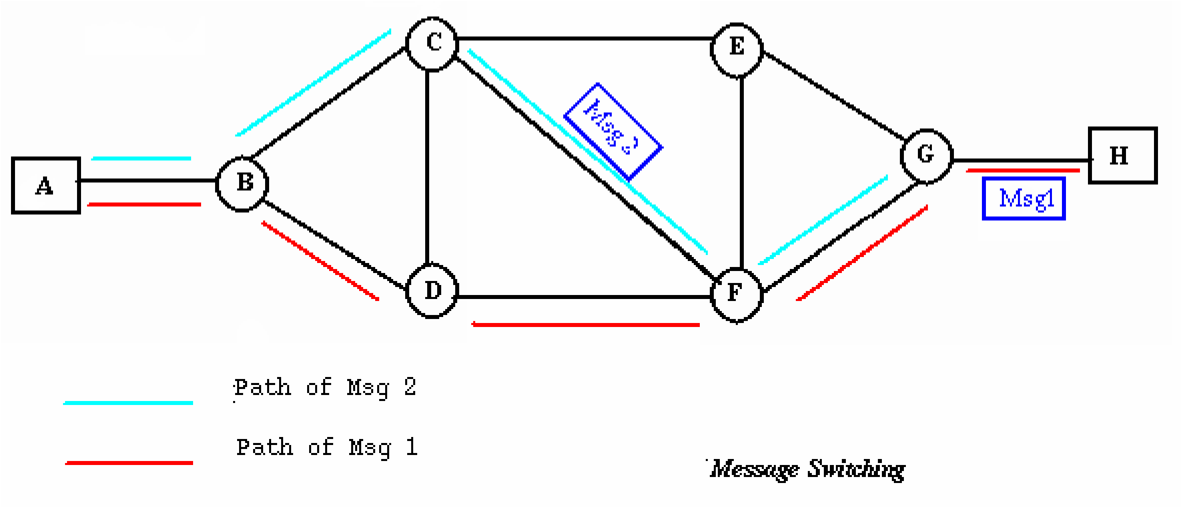
i. Circuit Switching

- **Circuit switching** is a technique that directly connects the sender and the receiver in an unbroken path.
- Telephone switching equipment, for example, establishes a path that connects the caller's telephone to the receiver's telephone by making a physical connection.
- With this type of switching technique, once a connection is established, a dedicated path exists between both ends until the connection is terminated.
- Routing decisions must be made when the circuit is first established, but there are no decisions made after that time.
- Circuit switching in a network operates almost the same way as the telephone system works.
- A complete end-to-end path must exist before communication can take place.
- The computer initiating the data transfer must ask for a connection to the destination.
- Once the connection has been initiated and completed to the destination device, the destination device must acknowledge that it is ready and willing to carry on a transfer.
-
- *Advantages:*
    - The communication channel (once established) is dedicated.
-

  Disadvantages:
    - Possible long wait to establish a connection, (10 seconds, more on long-distance or international calls.) during which no data can be transmitted.
    - More expensive than any other switching techniques, because a dedicated path is required for each connection.
    - Inefficient use of the communication channel, because the channel is not used when the connected systems are not using it.

ii. Message Switching

- With message switching there is no need to establish a dedicated path between two stations.
- When a station sends a message, the destination address is appended to the message.
- The message is then transmitted through the network, in its entirety, from node to node.
- Each node receives the entire message, stores it in its entirety on disk, and then transmits the message to the next node.
- This type of network is called a store-and-forward network



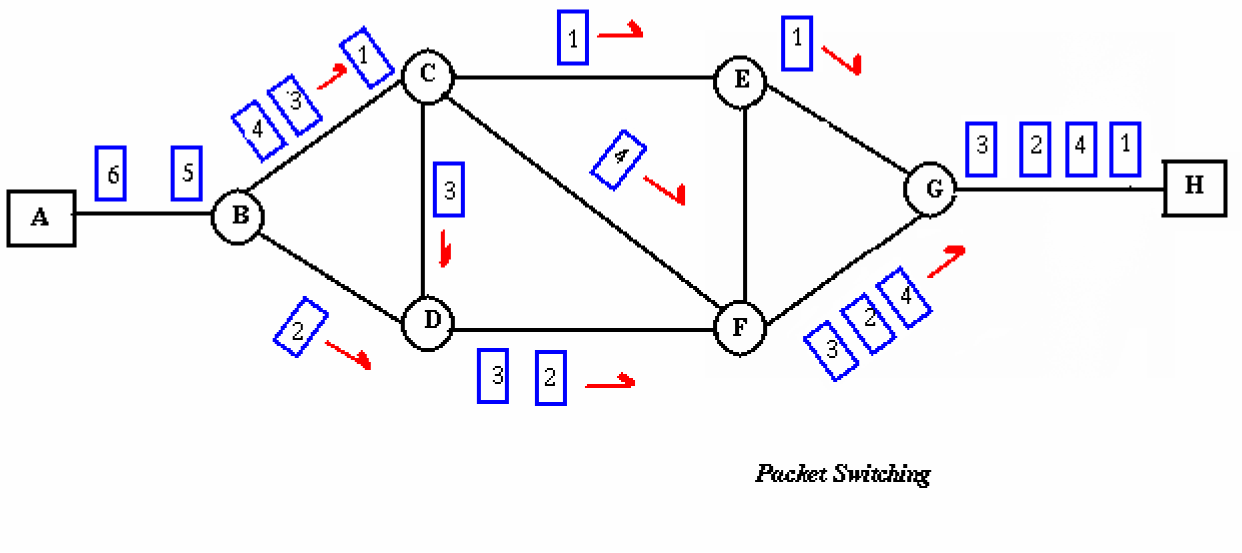
Message Switching

- A message-switching node is typically a general-purpose computer. The device needs sufficient secondary-storage capacity to store the incoming messages, which could be long. A time delay is introduced using this type of scheme due to store- and-forward time, plus the time required to find the next node in the transmission path.

- Advantages:
    - Channel efficiency can be greater compared to circuit- switched systems, because more devices are sharing the channel.
    - Traffic congestion can be reduced, because messages may be temporarily stored in route.
    - Message priorities can be established due to store-and-forward technique.
    - Message broadcasting can be achieved with the use of broadcast address appended in the message.
- Disadvantages
    - Message switching is not compatible with interactive applications.
    - Store-and-forward devices are expensive, because they must have large disks to hold potentially long messages.

iii. <u>Packet Switching</u>

- Packet switching can be seen as a solution that tries to combine the advantages of message and circuit switching and to minimize the disadvantages of both.
- In packet switching methods, a message is broken into small parts, called packets.
- Each packet is tagged with appropriate source and destination addresses.
- Since packets have a strictly defined maximum length, they can be stored in main memory instead of disk, therefore access delay and cost are minimized.



Packet Switching

- ➢ Also the transmission speeds, between nodes, are optimized.
- ➢ With current technology, packets are generally accepted onto the network on a first-come, first-served basis. If the network becomes overloaded, packets are delayed or discarded (``dropped'').
- ➢ Advantages:
  - o Packet switching is cost effective, because switching devices do not need massive amount of secondary storage.
  - o Packet switching offers improved delay characteristics, because there are no long messages in the queue (maximum packet size is fixed).
  - o Packet can be rerouted if there is any problem, such as, busy or disabled links.

- The advantage of packet switching is that many network users can share the same channel at the same time. Packet switching can maximize link efficiency by making optimal use of link bandwidth

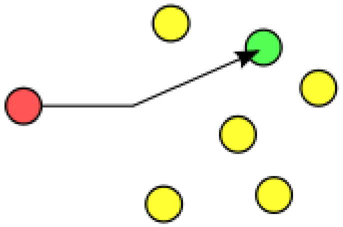
- Disadvantages:
  - Protocols for packet switching are typically more complex.
  - It can add some initial costs in implementation.
  - If packet is lost, sender needs to retransmit the data.
  - Another disadvantage is that packet-switched systems still can’t deliver the same quality as dedicated circuits in applications requiring very little delay - like voice conversations or moving images.

Routing Types

i. Unicast routing
ii. Multicast routing
iii. Broadcast routing
iv. Anycast routing

i. Unicast routing

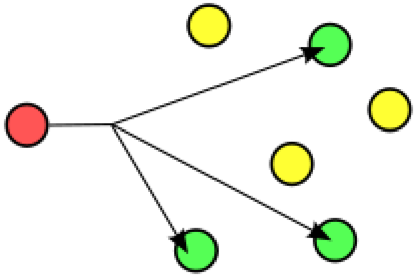
- In Unicast routing data is sent from one source address to one destination address
- In this case only one sender and one receiver
- If some device needs to send a message to multiple devices, it will have to send multiple unicast messages, each message addressed to a specific device
- IPv4 and IPv6 both uses unicast routing, in IPv6 such unicast address is known as global unicast address
- standard unicast applications are http, smtp, ftp, telnet etc



ii. Multicast routing

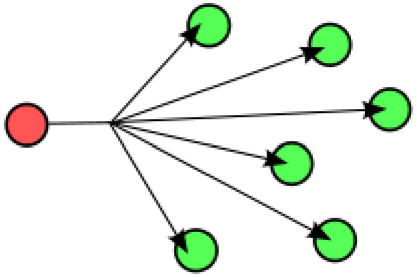
- In multicast routing data is sent from one or many source address to group of destination address
- In this case one or many sender and many receiver
- Multicasting uses the Internet Group Management Protocol (IGMP) to identify groups and group members

- IPv4 and IPv6 both uses multicast routing
- One example of an application which may use multicast is a video server sending out networked TV channels



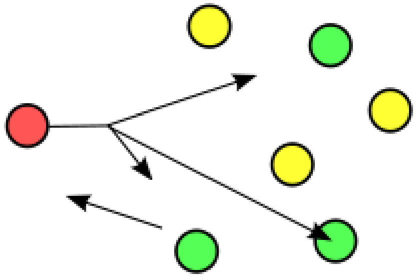
iii. **Broadcast routing**

- In broadcast routing data is sent from one source address to all of the destination address on a network segment
- In this case one sender and all receiver on the network segment ie on broadcast domain or a subnet
- Only IPv4 uses broadcast no more broadcast on IPV6
- e.g. the address resolution protocol (arp) uses this to send an address resolution query to all computers on a LAN



iv. Anycast routing

- Anycast is a network addressing and routing methodology in which datagrams from a single sender are routed to the topologically nearest node in a group of potential receivers
- Only IPv6 uses anycast routing but such analogy in IPv4 can be achieved by clever use of DNS
- It is used by Content Delivery Network (CDN) providers such as google, Akamai that delivers the contents from geographically nearest node.



response from nearest node

References

1. https://msandccna.blogspot.com/2017/03/osi-reference-model.html
2. https://sites.google.com/site/tvcc110111mb198065/network-network
3. http://validni.blogspot.com/2011/01/osi-model-during-past-two-decades-there.html
4. https://www.stemjar.com/osi-vs-tcp-ip-model/