Basic Networking

Networking devices

Hubs

- Old school and stupid devices
- Design is similar to switches
- Sends data which is received on 1 port to all ports
- Not secure as information which needs to be sent between 2 devices is leaked to other devices

Switches

- Newer and smarter version of a hub
- Uses MAC(Media Access Control) Addresses
- Information which is sent across the network is called a frame
- Smart devices as they learn the MAC on the port from the Src MAC in Layer 2 of the frame and store it in the CAM table
- Devices can be connected by ether-net cables
- Can only be used in a local area network
- Stores MAC addresses in its Content Addressable Memory(CAM) Table which is in its memory

Routers

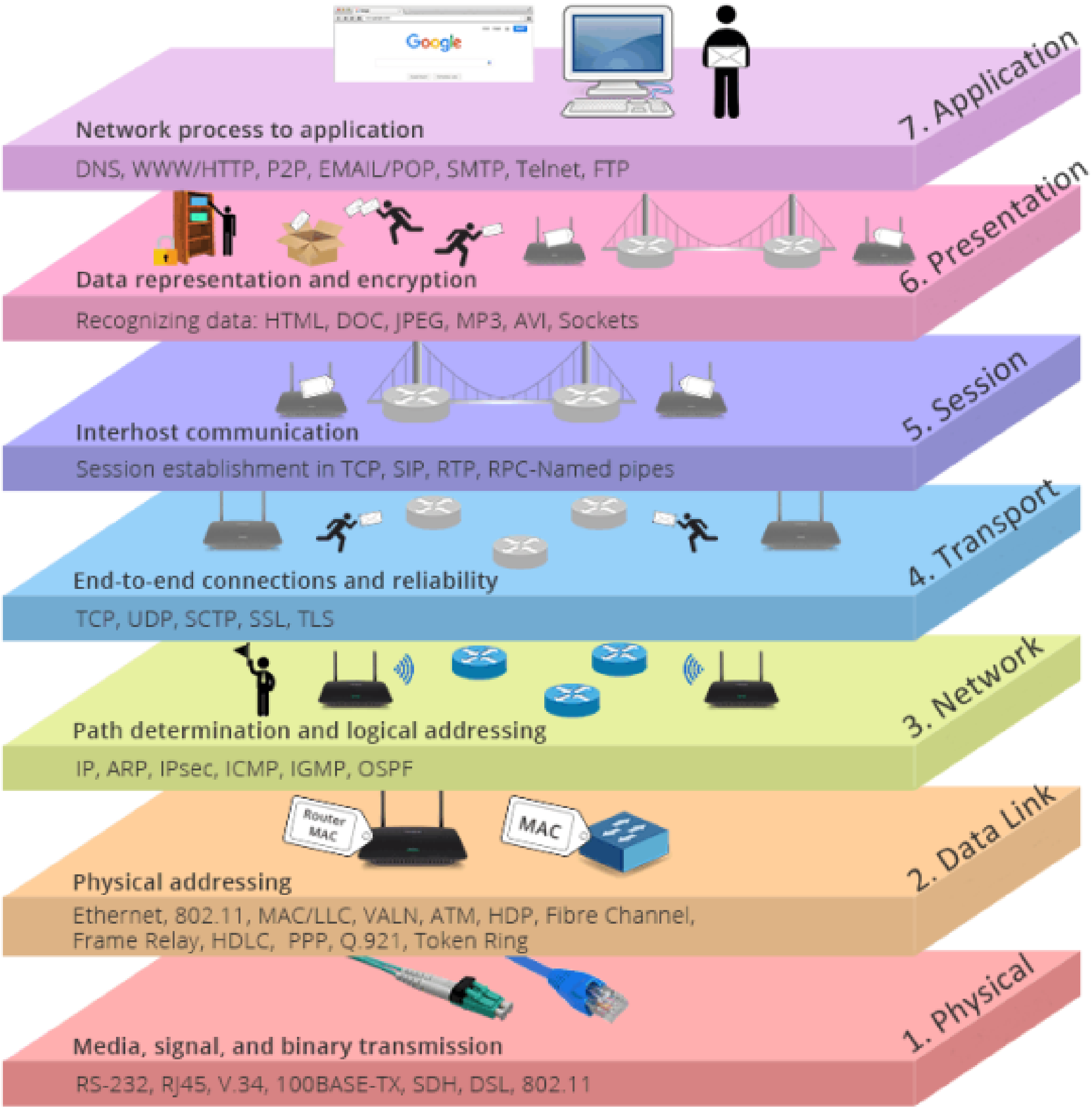
- Use IP(Internet Protocol) addresses
- Information which is sent across network(s) is called a packet
- Used to connect to different networks such as LAN to WAN to forward or receive packets
- To check all the networks a router is connected to, it checks its routing table
- Learn MAC addresses by sending ARP requests and receiving the ARP reply and it stores the MAC addresses in its ARP Cache

OSI Model

Open Systems Interconnection Model

Layer No.	Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data link
1	Physical

All people say they never download playlists


7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
2. Data Link
Router MAC
MAC
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel, Frame Relay, HDLC, PPP, Q.921, Token Ring
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

Layers

Layer 7: The application provides protocols such as HTTP,HTTPS,SMTP,FTP for software to send and receive information in a network

Layer 6: The presentation layer prepares the data for the application layer. It defines how the data should be encoded/encrypted/compressed

Layer 5: The session layer creates the communication channel between the devices. It is responsible for opening, maintaining and closing connections

Layer 4: The transport layer is responsible for transmission of data in a network. It can use TCP/UDP. This layer will contains the source port and destination port and which protocol is to be used

Layer 3: The network layer is the layer which deals with IP Addresses and so this layer is used by routers and devices to forward and receive packets. It contains the source IP and destination IP

Layer 2: The data link layer is the layer which deals with MAC addresses and it is used by switches to forward or receive frames in a network. It contains the source MAC and destination MAC

Layer 1: The physical layer deals with all the physical/wireless equipment. It is the layer which tells a device on which the port a physical equipment is connected.

TCP/IP Model

Layer No.	Name
5	Application
4	Transport
3	Network
2	Data link
1	Physical

Similar to the OSI Model but the presentation and session layers are combined into the application layer

Important protocols

Name	Full Form	Default Port
TCP	Transmission Control Protocol	-
UDP	User Datagram Protocol	-
ARP	Address Resolution Protocol	-
ICMP	Internet Control Message Protocol	-
SSL	Secure Sockets Layer	-
FTP	File Transfer Protocol	21
TFTP	Trivial File Transfer Protocol	69
HTTP	Hyper Text Transfer Protocol	80
HTTPS	Hyper Text Transfer Protocol Secure	443
SMTP	Simple Mail Transfer Protocol	25
SSH	Secure Shell	22
RDP	Remote Desktop Protocol	3389
VNC	Virtual Network Computing	5800 and 5900
Telnet	Telnet	23
SMB	Server Message Block	445
DNS	Domain Name System	53
POP3	Post Office Protocol	110

Name	Full Form	Default Port
DNS	Domain Name System	53
DHCP	Dynamic Host Configuration Protocol	67 and 68
NFS	Network File Sharing	111

Layer 4: TCP,UDP and SSL

Layer 3: ICMP

Layer 2: ARP

The rest are Layer 7 protocols

Difference between TCP and UDP

TCP	UDP
Connection Oriented	Connection Less
Slower and less efficient	Faster and more efficient
Reliable as there is a guarantee that packets will reach the destination	Not reliable
Retransmission is possible	Retransmission is not possible
Used by SSH,FTP,HTTP	Used by DNS,Voip,Media Streaming

Cables

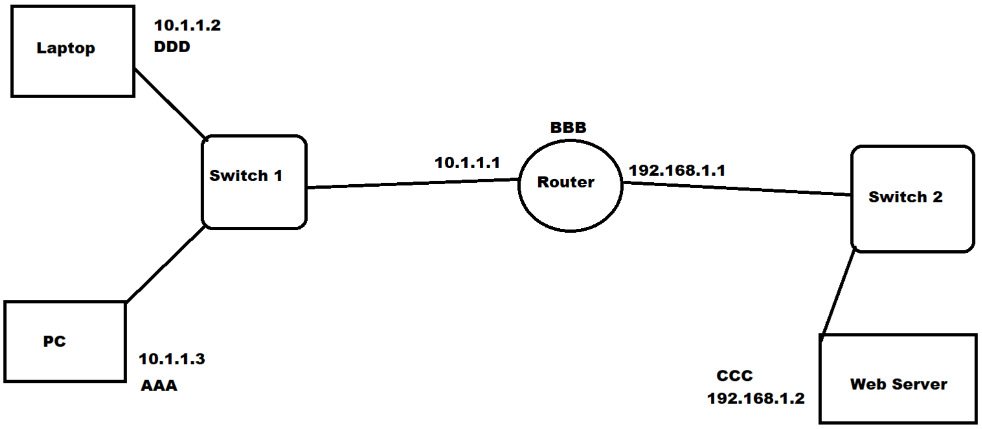
- Copper cross-over cables: Used to connect 2 similar devices such as 2 PCs or 2 laptops
- Copper straight-through cables: Used to connect 2 different devices such as a router and a switch

Switching and Routing

Switching is the forwarding and receiving of frames from 1 device to another device/devices by the means of a switch via the source MAC and destination MAC

Routing is the process of selecting a path to send or receive packets from one network to a completely different network by the means of a router

Routing table is a table stored in a router which lets the router know which networks it can access. Once a packet is received by a router which needs to be sent to a different network, the router checks its routing table. If that network exists in its table, the packet is forwarded to the network else it is sent to 0.0.0.0 which is a network where packets are sent when the destination network does not exist



In this network diagram, there are 2 switched networks 10.1.1.0/24 and 192.168.1.0/24 which are connected by a router

Case 1

The PC wishes to ping the laptop. It knows the MAC address of the laptop but the switch's CAM table is empty

- The PC sends the frame to ping the laptop to the switch. From this, the switch learns that on port 1, the MAC of AAA is living
- Since, the switch does not know which port the MAC of DDD is living on, it floods all its ports except the originating one, thus sending the frame to the router and laptop
- The device's Network Interface Card will check the Dst MAC of the received frame and compares it to their's
- The router's NIC will drop the packet but the laptop's NIC will analyze and open the packet since it's MAC and the Dst MAC are the same
- Since this is a ping, the laptop will respond with a reply. From this the switch learns that on port 2 the MAC of DDD is living.
- When looking at the Dst MAC address, the switch knows that this frame has been to be sent to the 1st port as it had stored the PC's MAC in the CAM table previously
- Now, the ping continues normally

Case 2

The PC wishes to ping the laptop. The CAM table of the switch is empty and the PC's ARP cache is empty

- Since the PC does not know the MAC of the Laptop, it will create an ARP request with its source MAC and IP and the Dst IP as 10.1.1.2 and the Dst MAC as FFFF.FFFF.FFFF
- This is then forwarded to the switch which will forward it to all devices. At the same time, the switch also learns from the source MAC, that on port 1, the MAC of AAA is living.
- The NIC of the devices will compare the Dst IP to their IP. It will send an ARP reply containing its source MAC if the IP matches else the request will be dropped
- In this case, the router drops the ARP request but the laptop sends an ARP reply to the switch
- From this, the switch learns that on port 2, the MAC of DDD is living. When it sees the Dst MAC, it knows it has to forward it to port 1 as it has already stored it in its CAM table.
- Once, the PC receives the ARP reply, the MAC of 10.1.1.2 is stored in its ARP cache and now the ping can continue normally

Case 3

The PC wants to visit the web server on the 2nd network. The CAM table of the switch is empty and the PC's ARP cache is empty

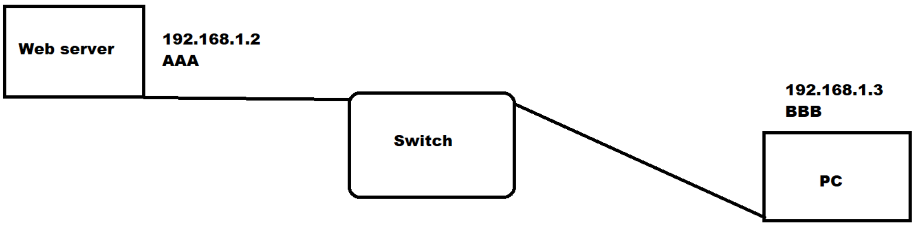
- Since the web server is on a different network, the PC has to send the packet to its gateway's IP i.e. the router
- First, the PC creates an ARP request to find the MAC of the router. This is then forwarded to the switch. The switch then learns that on port 1, the MAC of AAA is living
- The ARP request is then sent to all devices and the router sends an ARP reply. From this reply the switch learns that on port 3 the MAC of BBB is living. The ARP response is then forwarded to the PC as the switch remembers that AAA is living on port 1. The PC stores the MAC of the router in its ARP cache
- On receiving the ARP reply, the PC sends a frame to the switch, which forwards it in the form of a packet to the router. In this packet, the Src MAC and IP are of the PC's. The Dst IP is the web server's and the Dst MAC is the router's. Since the router does not know the MAC of the web server, it needs to send an ARP request
- It sends the ARP request to the 2nd switch and so the 2nd switch learns that on its 1st port, the MAC of BBB is living. It then forwards the ARP request to all devices i.e. in this case only the web server
- The web server then sends an ARP reply to the switch from which the switch learns that on port 2, the MAC of CCC is living. The ARP reply is then sent to the router, which stores the MAC in its ARP cache

- The router then changes the packet's Src MAC to it's MAC and the Dst MAC to the web server's and forwards the packet in the form of a frame.
- The 2nd switch forwards the frame in the form of a packet to the web server which sends a packet in the form of a frame back to the switch. The Src MAC and Src IP are it's but the Dst MAC is the router's and the Dst IP is the PC's.The switch forwards the frame to the router.
- The router,knowing the MAC of the PC from the earlier ARP request, then sends the packet in the form of frame to the switch which sends the packet to the PC. In this process, the IPs are not changing but the MACs are.

Note: Data is called a frame when dealing with layer 2 i.e. it is dealing with a switch and a packet when it is dealing with layer 3 i.e. routers and devices such as laptops and PCs

Encapsulation

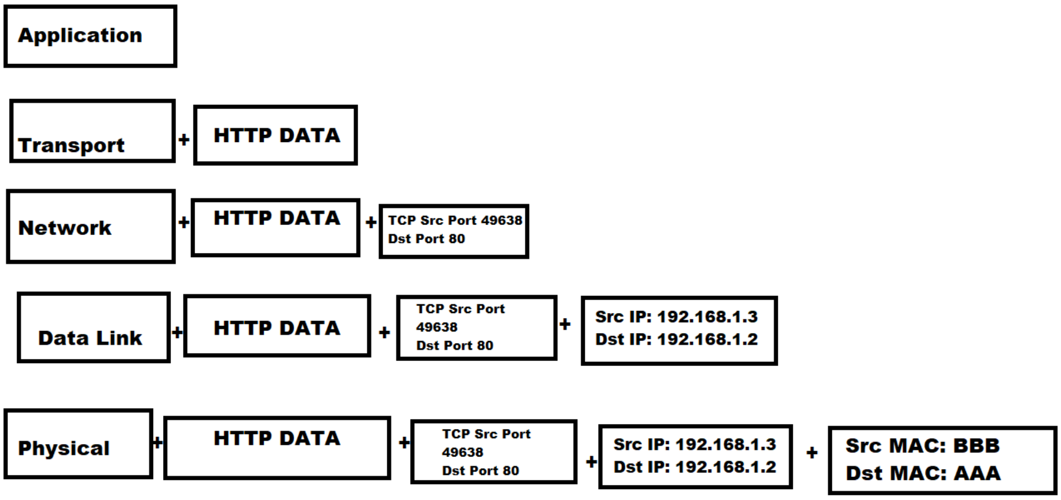
In a switched network, if one device has to send some data to another device, then that data will consist of all 7 layers combined into 1.
Encapsulation is the combination of the data/headers of an upper layer and a lower layer in the TCP/IP or OSI model to form 1 layer. So at the end of this process, the headers/data of the application layer, transport layer, network layer, data link layer and physical layer are combined into 1 layer



The PC wishes to visit the web server located at 192.168.1.2. In this case, the switch knows the MACs of the devices and The PC knows the MAC of the web server.
Note: This in accordance with the TCP/IP model

- The fifth layer will be the application layer and will contain the HTTP data
- The fourth layer will be the transport layer. It will contain a random source port and a destination port of 80(HTTP). The content of the application layer will be combined with the header of the fourth layer.
- The third layer will be the network layer. It will contain the source IP and destination IP. The content of the application layer and the header of the transport layer will be combined with the header of the third layer
- The second layer will be the data link layer. It will contain the source MAC and destination MAC. The content of the application layer and headers of the transport layer and network layer will be combined with the header of the second layer

- Finally, the The content of the application layer, and the headers of the transport layer, network layer and data link layer are combined with the physical layer and sent to the switch in the form of electric waves



- Now, this packet is sent in the form of electric waves to the switch
- When the switch receives this frame, it opens the layer 2 header of the frame and checks the source and destination MAC addresses
- Now, this frame is forwarded to the web server which first opens the packet's layer 2 header to confirm that it's MAC and the destination MAC address are the same
- Next it opens the layer 3 header to check if the Destination IP and its IP are the same
- Next it opens the layer 4 header to check which port the PC wants to access. If the port is 80 and the web server is active then it proceeds.
- Finally it opens the layer 7 header to have a look at the HTTP data. The web server has now verified that this packet is for it
- This is called De-Encapsulation
- Then the web server, performs the exact same process as the PC did and sends the web pages to the PC

Setting up a switched network in Cisco Packet Tracer

- Drag in a switch such as a PT-Switch or a 2960 Switch or a 2950T Switch
- Next we bring in our end devices; Laptops,PCs,Servers,etc
- To connect these devices to the switch, we use copper straight-through cables
- Connect the cable to FastEthernet0 of a device and to a port on the switch such as FastEthernet0/4. Do this for all devices
- Finally, go into the configuration of each device and assign an IP to them such as 10.1.1.2 and 10.1.1.3. Note: If the IP of one device is 10.1.1.2 then the IP of another device cannot be 192.168.1.2 or anything different as they are on the same subnet

Setting up a router in Cisco Packet Tracer

- Drag in a switch such as a PT-Switch or a 2960 Switch or a 2950T Switch
- Next we bring in our end devices; Laptops,PCs,Servers,etc
- To connect these devices to the switch, we use copper straight-through cables
- Connect the cable to FastEthernet0 of a device and to a port on the switch such as FastEthernet0/4. Do this for all devices
- Finally, go into the configuration of each device and assign an IP to them such as 10.1.1.2 and 10.1.1.3. Note: If the IP of one device is 10.1.1.2 then the IP of another device cannot be 192.168.1.2 or anything different as they are on the same subnet
- Do the above process again but for a completely different network with a different range of IPs
- Bring in a router such as 2901 Router of 2911 Router
- Connect a port of the switch to a port of the router using copper straight through cables such as FastEthernet0/4 to GigabitEthernet0/1. Do this for both networks
- Assign an IP to the router on the port for the respective network i.e. for example on 1 port the IP should be something such as 10.1.1.5 and on the other port it should be something such as 192.168.1.6. After doing this, turn on the port
- Now, in the configuration of the devices in the 10.1.1.0 network, assign the gateway IP as the IP of the router in the network
- In the configuration of the devices in the 192.168.1.0 network, assign the gateway IP as the IP of the router in the network
- Both of the networks have been connected to each other and can send and receive packets

Cheatsheets

Cisco CLI Commands

TCP and UDP Ports