Shashank K

Comparison between OSI model & TCP/IP Architecture.

ISO OSI model	TCP/IP Architecture / Internet Model
(1) There are 7 layers	(1) There are 4 layers → in original Model Now there are 5 layers
(2) OSI is a model & not a protocol	(2) TCP/IP is a protocol not a model
(3) Was developed after TCP/IP	(3) was developed before OSI model
(4) In OSI model was devised first & then the protocols were invented.	(4) In TCP/IP the protocol was developed first & then the architecture was developed
(5) Clearly distinguishes between Service, interface & protocol	(5) Does not clearly distinguish between service, interface & protocols
(6) Do not support Internetworking	(6) Supports internetworking
(7) Supports both connectionless & connection oriented Communication in network layer.	(7) Supports both Connectionless & connection oriented Communication in transport layer but also supports only connectionless Communication in network layer
(8) OSI model is strictly layered	(8) TCP/IP Architecture is loosely layered
(9) Vertical Horizontal approach (Transport layer of source can directly talk to Trans layer of dest)	(9) ~~Horizontal Approach~~ Vertical Approach (each layer is stand

Network layer delivery	Transport layer delivery
① Best effort delivery (source to destination delivery)	① End to End delivery (process to process delivery)
② Does not gaurantee transmission	② Gaurantee Transmission
③ Not Reliable, does not provide error & flow control	③ Reliable, provides error & flow control.
④ Connectionless	④ connectionless or connection oriented.
⑤ packets or datagrams.	⑤ TCP segments UDP → datagrams SCTP → packets.
⑥ uses IP address	⑥ uses port address.

Data Link Layer Delivery

1) Reliable
2) Frames are used for information transfer
3) uses MAC address / phy / link / HW addr
   eg AB : C1 : 23 : 14 : 36 : F2
4) Node to Node Delivery (Hop-by-Hop)

Service Point Addressing (Port Addresses)	Logical Addressing	Physical Addressing
1) This is the port no of the application	This is the IP address of the machine	This is the MAC address of the machine.
2) It distinguishes applications on the m/c's (eg HTTP & SMTP)	It distinguishes two different machines Connected in Internet	It distinguishes two different m/c's connected in LAN
3) Also called port addressing	also called IP addressing	also called Hardware or Link or MAC addressing.
4) Not fixed always	Not fixed	fixed unless NIC is changed.
5) Done at transport layer	Done at Network layer	Done at data link layer.
6) TCP & UDP use port addressing	IP uses logical addressing	Ethernet, FDDI uses physical addressing.
Max port addr is 65535 Combination of IP & port addr is called Socket addr.		
7) 16-bit addr.	32-bit addr → IPV4 128-bit addr - IPV6	48 bit
8) 2^{16} addresses are possible	2^{32} addresses are possible.	2^{48} addresses are possible.
9) decimal format e.g. 753	dotted decimal format e.g. 192.3.2.1/24	Hex colon format e.g. AB:CD:11:22:FE:56

	Unit of communication (or data unit)	Way of communication	Addresses
Application	message or ALPDU	End-to-End	→ Application Specific addresses (Socket Address)
Transport	Segments → TCP Datagram → UDP packet → SCTP	End-to-End or process to process	→ Port Addresses
Network	packets/Datagrams	Source to Destination (end to end)	→ IP Address or Logical Address
Data link	frames	node to node	→ Physical Address or MAC Address or Hardware Address.
Physical	Bits	node to node.	

Fig: TCP/IP Stack

ALPDU: Application Layer protocol Data Unit

TCP: Transmission Control protocol

UDP: User Datagram protocol

SCTP: Stream Control Transmission protocol.

Comparison of Network Topologies

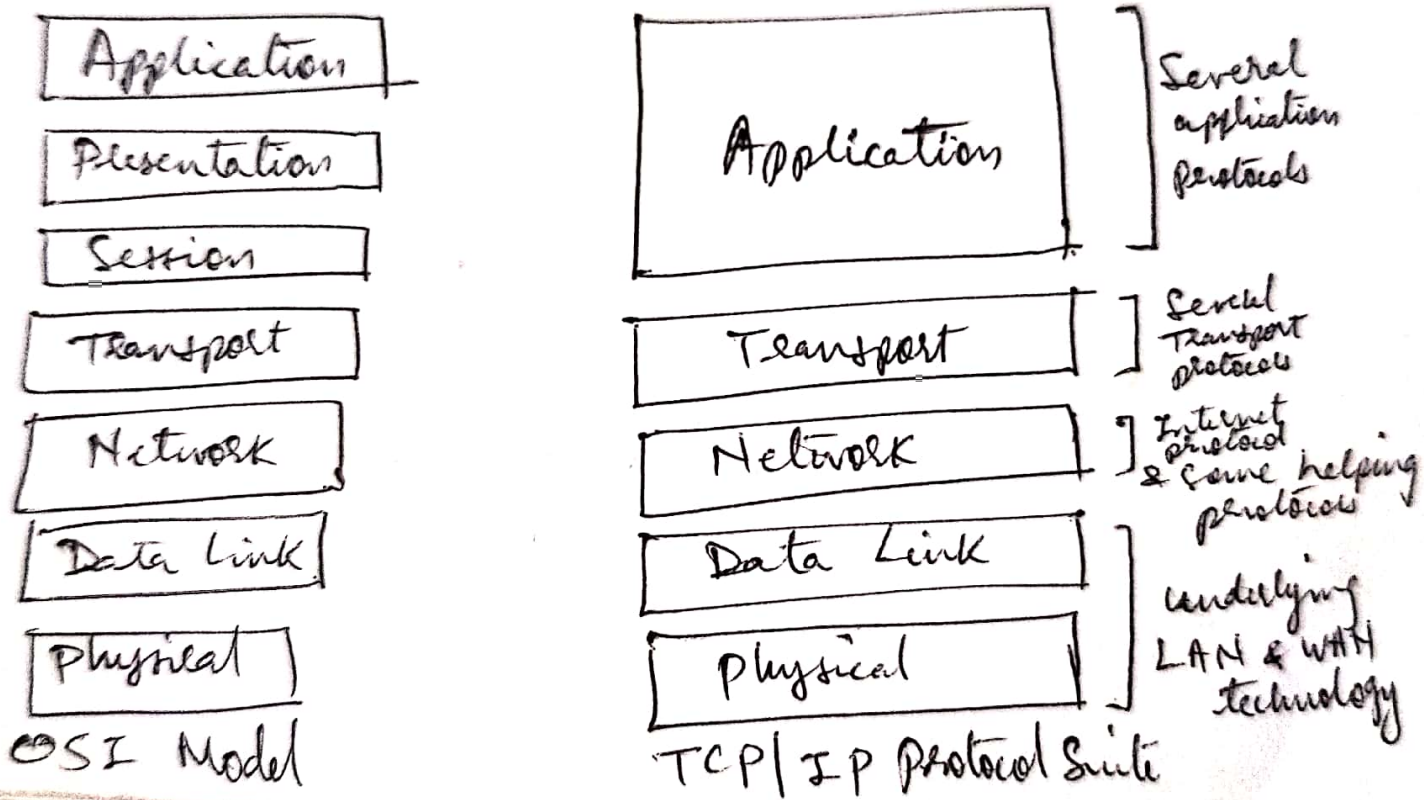
Topology	Total No. of Links	Privacy	I/O Lines with each device	Installation and Reconnection	Cost	Fault Identification and Isolation	Line Configuration	Application
Mesh	$\frac{n(n-1)}{2}$	Yes	$n-1$	Difficult	Expensive	Easy	P2P	Regional Telephone Offices
Star	n	No	one	Easy	Less Expensive	Easy	P2P	LANs, High Speed LANs
Bus	Single backbone with n drop lines	No	one	Difficult	Least Expensive	Difficult	Multi-point	Not used in large networks
Ring	n	No	one	Easy	Moderate	Easy	Multipoint	IBM token ring. Not referred in todays LANs

P2P = Point to Point

Comparison of Network Topologies

n = no of nodes

Comparison Between OSI & TCP/IP protocol Suit



Comparison between TCP & UDP

Transmission control protocol (TCP)	User Datagram protocol (UDP)
① provides process to process Service.	① provides process to process Service.
② TCP is connection oriented protocol	② UDP is connectionless protocol.
③ The unit of communication is segment	③ The unit of communication is user Datagram.
④ provides reliable service	④ provides unreliable service
⑤ Implements Error control using checksums, acknowledgement and timeouts.	⑤ Implements minimal level of error control using checksum.
⑥ The use of checksum in TCP segment is Mandatory	⑥ The use of checksum in UDP datagram is optional.
⑦ TCP Header is 20 Bytes without options. TCP Header can extend upto 60 Bytes with options	⑦ UDP Header is 8 Bytes
⑧ Since Header occupies more bytes, TCP incurs more overhead	⑧ Less overhead in UDP as header is 8 bytes.
⑨ TCP provides flow Control	⑨ UDP does not provide flow control
⑩ TCP provides Congestion control	⑩ UDP does not provide congestion control
⑪ TCP is a byte stream service (Data is Transmitted as stream of Bytes)	⑪ UDP is a message service (Data is transmitted as messages)

TCP

(12) TCP provides more services with the use of options

(13) TCP provides full Duplex communication

(14) TCP uses pseudoheader for checksum calculation

(15) Value of protocol field for TCP in pseudoheader is 6

(16) TCP offers slow delivery due to ACK mechanism. Hence not suitable for audio & video transmission.

(17) TCP segments are encapsulated in IP packets.

(18) Well known ports used by TCP:

Port	protocol
20 & 21	FTP
23	TELNET
25	SMTP
53	DNS
67	BOOTP
79	finger
80	HTTP

UDP

(12) UDP provids less services as there are no options.

(13) UDP does not provide full duplex communication

(14) UDP uses pseudoheader for checksum calculation.

(15) Value of protocol field for UDP in pseudoheader is 17

(16) UDP offers fast delivery hence suitable for audio & video transmission.

(17) UDP Segments are encapsulated in IP packets.

(18) Well known ports used by UDP:

Port	protocol
53	DNS
67	BootpS ⇒ DHCPS
68	BootpC ⇒ DHCPC
69	TFTP
161	SNMP
162	SNMP (Trap)

TCP	UDP	RTP
• TCP is not suitable for interactive traffic	• UDP is more suitable for interactive traffic.	• RTP is most suitable for interactive traffic.
• TCP provides sequence numbers	• UDP does not provide sequence numbers.	★ • RTP provides sequence numbers.
• TCP does not provide timestamping	• UDP does not provide timestamping	★ • RTP provides timestamping
• TCP does not support multicasting	★ • UDP supports multicasting	• RTP does not support multicasting.
• TCP supports port numbers	★ • UDP supports port numbers	• RTP does not support port numbers
• TCP does not support mixing	• UDP does not support mixing	★ • RTP supports mixing.
• Retransmission in TCP upsets timestamping & playback in real time traffic	• No retransmission in UDP	• No retransmission in RTP

★ marked features of UDP & RTP are combined to handle real time traffic on Internet.

Link State Routing Versus Distance Vector Routing :

Distance Vector Routing	Link State Routing
• Neighbouring routers exchange the vectors stating the Distances to the Desired destination	• Each node floods the information about the state of the links that connects to its neighbours.
• Metric is number of hops	• metric is cost.
• Less convergence Speed	• High Convergence Speed.
• use Bellman ford algorithm to compute shortest path	• Use Dijkstras algorithm to compute Shortest path.
• Neighboring nodes eventually adapts to changes in n/w topology	• each node floods the information regarding changes in n/w topology
- eg. RIP	eg OSPF

Stop-and-Wait ARQ	Go-Back-N ARQ
• Transmits one frame at a time	• Transmits number of frames equal to the window size W_S
• If a frame is in error then it is retransmitted	• If a frame is in error then that frame & all subsequent frames are retransmitted
• Sequence number is one bit both for I-frame & ack frame.	• Sequence numbers m bits for I-frame & m bit for ack frame.
• No of Sequence numbers $= 2^1 = 2$ (i.e 0,1)	• No of Sequence numbers $= 2^m$ If $m = 3$ then No of Sequence numbers $= 2^3 = 8$ i.e. 0, 1, 2, 3, 4, 5, 6, 7.

	Stop-and-wait ARQ	Go-Back-N ARQ	Selective Repeat ARQ
Transmission Efficiency	$\eta_{SW} = \eta_0 \cdot (1-P_f) = \frac{(1-\frac{n_0}{n_f}) \cdot (1-P_f)}{1+\frac{n_0}{n_f}+\frac{2(t_{prop}+t_{proc})R}{n_f}}$	$\eta_{GBN} = \frac{1-\frac{n_0}{n_f}}{1+(W_S-1)P_f}(1-P_f)$	$\eta_{SR} = (1-\frac{n_0}{n_f})(1-P_f)$
	Neglecting header & CRC overhead $\eta_{SW} = \frac{(1-P_f)}{1+\frac{2(t_{prop}+t_{proc})R}{n_f}}$	Neglecting header & CRC overhead $\eta_{GBN} = \frac{(1-P_f)}{1+(W_S-1)P_f}$	Neglecting header & CRC overhead $\eta_{SR} = (1-P_f)$
	Let $L = \frac{2(t_{prop}+t_{proc})R}{n_f}$ = Size of the pipe = multiples of frames = Delay BW product	In Go-Back-N $W_S = L+1$ $\therefore \eta_{GBN} = \frac{1-P_f}{1+(L+1-1)P_f}$	
	Then, $\eta_{SW} = \frac{(1-P_f)}{1+L}$	$\eta_{GBN} = \frac{1-P_f}{1+LP_f}$	$\eta_{SR} = 1-P_f$

Comments: 1) Go-Back-N ARQ is worse than Selective repeat ARQ by a factor of $(1+LP_f)$ & Stop-and-wait is worse than Selective repeat ARQ by a factor of $(1+L)$

2) If $LP_f << 1$ then $\eta_{GBN} = \eta_{SR}$

3) If P_f approaches 1 then LP_f becomes L & $\eta_{GBN} = \eta_{SW}$

Comparison of Stop-and-Wait, Go-Back-N and Selective repeat ARQ's.

Stop-and-Wait ARQ	Go-Back-N ARQ	Selective Repeat ARQ.
1) only one frame is transmitted at a time.	Number of frames transmitted depend on the window size	Number of frames transmitted depend on the window size.
2) one bit is reserved in the header of I-frame (ack frames) for sequence numbering.	m-bits are reserved in the header of I-frame (& ack frame) for sequence numbering.	m-bits are reserved in the header of I-frame (& ack frame) for sequence numbering
3) Not an example of Sliding window protocol	Example of Sliding window protocol. • Maximum window size is $W_S = 2^m - 1$ • Transmitter window size is W_S and receiver window size is only one frame.	Example of Sliding window protocol. • Maximum window size is $W_S = 2^{m-1}$ • Transmitter window size is W_S and receiver window size is W_R & they are equal. $W_S = W_R$
4) whenever a frame is in error it is retransmitted.	4) whenever a frame is in error, that frame & all subsequent frames are retransmitted	4) whenever a frame is in error only that frame is retransmitted.
	$W_S >$ Delay BW product	$W_S >$ Delay BW product.

Parameter	IPV4	IPV6
(1) Address	1) 32-bit Address 2) Address in dotted decimal format e.g 192.168.2.1/24 3) IPV4 Address allows CIDR notation e.g. 64.2.1.0/8 which implies that there are 8-bits in Network ID part. 4) 4 octet OR 4 Byte Address 5) Specifies binary prefix to classify addresses e.g. Binary prefix 0 Class A Address 10 Class B Address 110 Class C Address 1110 Class D Address 1111 Class E Address.	1) 128 bit address 2) Address in colon-Hex format 8000:0000:0000:0000:0123:4567:89AB:CDEF 3) IPV6 Address extends CIDR notation e.g. 12AB::CD30:0:0:0:0/60 which specifies the first 60 bits of the address or 12AB0000000CD3 in Hex. 4) 16 octets or 16 Bytes Address. (32-Hexadecimal digits Address) 5) Specifies binary prefix to classify address. e.g. Binary prefix 001 Aggregatable Global unicast 1111 1110 10 Link-Local unicast Address FE80::/64 1111 1110 11 Site-Local unicast Address FEC0::/10 1111 1111 Multicast Addresses.
Special Addresses	6) Loop back Address 127.0.0.0 to 127.255.255.255	6) Loop back Address 0:0:0:0:0:0:0:1

	7) IPV4 Address with all 0 bits in Host ID part is Universal N/w address A IPV4 Address with all 1 bits in Host ID part is Universal Broadcast Address	7) IPV6 Address with all 0's 0:0:0:0:0:0:0:0 is an unspecified Address which cannot be assigned to any computer or used as a destination. It is only used as a source address during bootstrap by a computer that has not yet learned its address.
	8) 2^{32} address Space 2^{32} =	8) 2^{128} Address Space 2^{128} =
	9) Address Space almost exhausted	9) Address Space cannot be exhausted in the foreseeable future
	10) Limited address space	10) Extended address Space.
Header	11) Does not Support authentication	11) Supports authentication
	12) Does not Support flow labeling	12) Supports flow labeling

13) IPV4 datagram
= IPV4 Header
+ Zero or more options
+ Data

14) 20-octets IPV4 Header

15) Does not support auto configuration (requires DHCP)

16) Does not support renumbering

17) IPV4 supports unicast & multicast addressing

13) IPV6 datagram
= IPV6 Header
+ Zero or more extension headers (options)
+ Data

14) 40-octets IPV6-Header.

15) Supports autoconfiguration (do not require DHCP.

16) Support renumbering.

17) IPV6 In addition to unicast & multicast addressing IPV6 ~~supports~~ defines Anycast address.

A single anycast address can be assigned to a set of computers; a datagram sent to the address is delivered to exactly one computer in the set (i.e. the computer closest to the source)

IPV4	IPV6
18) Does not gaurantee delivery of packets	18) Gaurantee Service
19) IHL field Type of service field Total length field	19) Flow label field
20) Total length field	20) payload length field.
21) Identification, flags & fragment offset field	21) corresponding fields not present.
22) Time to live field	22) Hop limit
23) protocol field	23) No protocol field (Next header field)
24) Header Checksum field	24) No Header Checksum field
25) IP V4 needs VLSM, CIDR	25) IP V6 eliminates the need for VLSM, CIDR.
26) IPV4 uses Subnet Mask (n/w prefix)	26) IPV6 do Subnet Mask is not used for IPV6.
27) Poor QoS	27) Better QoS.
28) Less real time performance.	28) Increased real time performance.

Table I

34

Key differences between IPV4 and IPV6.

IPV4	IPV6
① Source and destination addresses are 32 bits (4 bytes) in length	① Source and destination addresses are 128 bits (16 bytes) in length.
② IPSec support is optional	② IPSec support is required.
③ No identification of packet flow for QoS handling by routers is present within the IPV4 header.	③ packet flow identification for QoS handling by routers is included in the IPV6 header using the flow label field.
④ Fragmentation is done by both routers and sending host	④ Fragmentation is not done by routers, only by the sending host.
⑤ Header includes a checksum	⑤ Header includes does not include a checksum.
⑥ Header includes options	⑥ All optional data is moved to IPV6 extension headers.

IPV4	IPV6
(7) Address Resolution protocol (ARP) uses broadcast ARP request frames to resolve an IPV4 address to a link layer address.	(7) ARP request frames are replaced with multicast neighbour solicitation messages.
(8) Internet Group Management protocol (IGMP) is used to manage local subnet group membership.	(8) IGMP is replaced with multicast listner discovery (MLD) messages.
(9) ICMP router discovery is used to determine the IPV4 address of the best default gateway and is optional	(9) ICMP Router Discovery is replaced with ICMPV6 Router solicitation and Router advertisement messages and is needed (required).
(10) Broadcast addresses are used to send traffic to all nodes on a subnet	(10) There are no IPV6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used.
(11) Must be configured either manually or through DHCP	(11) Does not require manual configuration or DHCP.

(12) Uses host address (A) resource records in the Domain Name System (DNS) to map host names to IPV4 addresses.

(13) Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPV4 addresses to host names.

(14) Must support a 576-byte packet size.

(12) Uses host address (AAAA) resource records in the Domain Name System (DNS) to map host names to IPV6 addresses.

(13) Uses pointer (PTR) resources records in the IP6.ARPA DNS domain to map IPV6 addresses to host names.

(14) Must support a 1280-byte packet size.

Table 2

IPV4 Addressing Concepts and Their IPV6 Equivalents

IPV4 Address	IPV6 Address
① Internet address classes	① Not applicable in IPV6.
② Multicast addresses (224.0.0.0/4)	② IPV6 multicast addresses (FF00::/8)
③ Broadcast addresses	③ Not applicable in IPV6.
④ Unspecified address is 0.0.0.0	④ Unspecified address is ::
⑤ Loopback address is 127.0.0.1	⑤ Loopback address is ::1
⑥ public IP addresses	⑥ Global unicast addresses.
⑦ private IP addresses (10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16)	⑦ Site-local addresses (FFC0::/10)
⑧ Autoconfigured addresses (169.254.0.0/16)	⑧ Link-local addresses (FF80::/64)
⑨ Text representation: Dotted decimal notation	⑨ Text representation: Colon hexadecimal format with suppression of leading zeros and zero compression IPV4-compatible addresses are expressed in dotted decimal notation.

(10) N/w bits representation: Subnet mask in dotted decimal notation or prefix length

(10) N/w bits representation: prefix length notation only.

(11) DNS name resolution: IPV4 host address (A) resource record

(11) DNS name resolution: IPV6 host address (AAAA) resource record.

(12) DNS reverse resolution: IN-ADDR.ARPA domain

(12) DNS reverse resolution: IP.ARPA domain.

Differences between the IPV4 and IPV6 header fields.

IPV4 Header field	IPV6 Header field
① Version	Same field but with different Version numbers.
② Internet Header length	Removed in IPV6. IPV6 does not include a Header length field because the IPV6 header is always a fixed size of 40 bytes. Each extension Header is either a fixed size or indicates its own size
③ Type of Service	Replaced by the IPV6 traffic class field
④ Total length	Replaced by the IPV6 payload length field, which only indicates the size of the payload
⑤ Identification Fragmentation flags Fragment offset	Removed in IPV6. Fragmentation information is not included in the IPV6 header. It is contained in a fragment extension header.
⑥ Time to live	Replaced by the IPV6 Hop limit field
⑦ protocol	Replaced by the IPV6 next Header field
⑧ Header checksum	Removed in IPV6. In IPV6, bit level error detection for the entire IPV6 packet is performed by the link layer.
⑨ Source Address	The field is the same except that IPV6 addresses are 128 bits in length.
⑩ Destination Address	The field is the same except that IPV6 addresses are 128 bits in length
⑪ Options	Removed in IPV6. IPV4 options are replaced by IPV6 extension headers.

	ALOHA	Slotted ALOHA
Vulnerable period	2X seconds	X seconds.
Synchronised transmission	No	Yes.
Maximum Throughput S	18.4% i.e. (1/2e)	36.8% i.e. (1/e)
Throughput explanation	$S = Ge^{-2G}$	$S = Ge^{-G}$
Average packet delay in ~~Slotted ALOHA~~	$E[T_{aloha}]$ $= X + t_{prop} + (e^{2G} - 1)[X + 2t_{prop} + B]$	$E[T_{slotaloha}]$ $= X + t_{prop} + (e^{G} - 1)[X + 2t_{prop} + B]$

© Congestion control

1) Congestion control makes sure that the subnet is able to carry the offered ~~load~~ traffic.

2) It is a global issue, involving the behaviour of all the hosts, all the routers, the store and forward processing within the routers, and all the other factors that tend to diminish the carrying capacity of the subnet

Flow control

1) Flow control relates to the point-to-point traffic between a given sender and a given receiver.

2) Its job is to make sure that a fast sender cannot continually transmit data faster than the receiver is able to absorb it.

(b) addresses

Circuit Switching	Virtual Circuit packet Switching	Datagram packet Switching
Dedicated transmission path	No dedicated path	No dedicated path
Continuous transmission of data	Continuous transmission of packets	Transmission of packets.
Messages not stored	packets stored until delivered	packets stored until delivered.
Path is established for entire Conversation	Route established for entire conversation.	Route established for each packet.
Call setup delay, negligible transmission delay	Call setup delay, packet transmission delay	packet transmission delay
Busy signal if called party busy	Sender notified of Connection denial	Sender may be notified if packet not delivered.
Electromechanical or computerised switching nodes	Small switching nodes	Small switching nodes
Fixed BW	Dynamic BW	Dynamic BW
No overhead bits after call setup	overhead bits in each packet	overhead bits in each packet.
No speed or code conversion	speed or code conversion	Speed or code conversion

Shubhangi Khetele

Congestion control	Flow control
• It ensures that the n/w carries offered load	It ensures that the Rx does not get overwhelmed i.e the rate of processing at receiver & rate of sending ~~processing~~ at Tx remains balanced.
• It is a global issue	It is a local issue performed at every transmission.
• It is performed by the tariff	• It is usually performed by the sender
• It is done during set up or link establishment.	• It is done as & when needed.

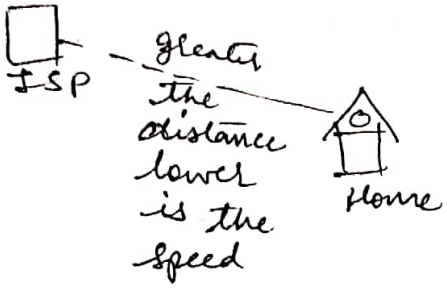
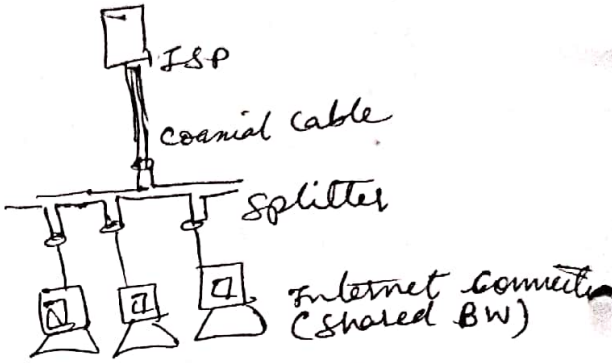
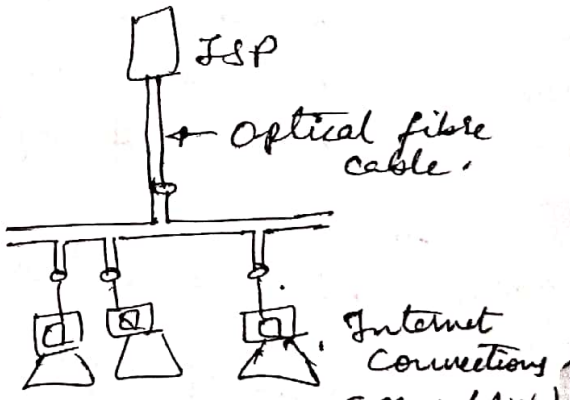
8.2. (a)

Circuit Switching	Datagram Packet Switching	Virtual Circuit packet Switching
Dedicated Transmission path	No dedicated path	No dedicated path (Virtual path)
Continuous transmission of Data	Transmission of packets	Transmission of packets
Fast enough for interactive	Fast enough for interactive	Fast enough for interactive
Messages are not stored	packets may be stored until delivered	Packets stored until delivered
The path is established for entire conversation	Route established for each packet	Route (logical or virtual) established for entire conversation.
Call set up delay; negligible transmission delay.	Packet transmission delay	Call set up delay, packet transmission delay.
Busy signal if called party is busy	Sender may be notified if packet not delivered.	Sender may be notified if packet not delivered.
Overload may block call set up, no delay for established calls	Overload increases packet delay	Overload may block call set up, increases packet delay.
Electromechanical or computerised switching	Small switching nodes	Small switching nodes.

Circuit Switching	Datagram Packet Switching	Virtual ckt packet Switching
User responsible for message loss protection	Network may be responsible for individual packets	Network may be responsible for packet sequences.
Usually no speed or code conversion	Speed & Code conversion	Speed & Code conversion.
Fixed BW	Dynamic use of BW	Dynamic use of BW.
No overhead bits after call set up	overhead bits in each packet	overhead bits in each packet.

Shubhangi K

Difference between DSL & VDSL

Digital Subscriber Line (DSL)	Very High Bit rate Digital Subscriber Line (VDSL)
• If distance between ISP & our home increases, then Internet speed becomes slow	• Works similar to cable Internet.
	
• This is because, in DSL the Internet connection is via the telephone lines which are made of copper (twisted pair) & these copper wires are much more susceptible to Electromagnetic interference So as distance increases Signal becomes weak & speed becomes slow.	fig. Cable Internet • VDSL Internet  fig: VDSL Internet • The connection between ISP & home computers is optical fibre cables. • So even if distance increases, no losses (& no EMI in OFC), the speed is maintained • Download speed 50-52 MBPS • Upload Speed 15-16 MBPS • freq: 12 MHz.

Shubhangi K

Dial-up Internet connection

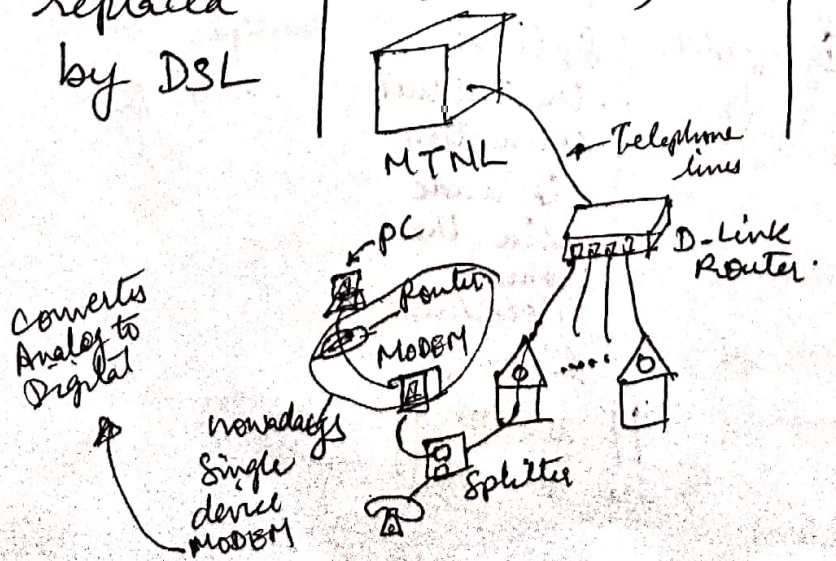
- Internet connection via Normal Telephone lines.
- ~~Whenever~~ Voice call & Data (Internet) connection over a single (same) telephone line.
  - So whenever there was a voice call coming in during the Internet connection then that connection would be terminated
  - Dial up is now replaced by DSL

DSL Internet connection

- Internet connection is via normal Telephone lines (twisted pairs) But 30% of the lines are used for voice connection & 70% of the lines are used for data (Internet) connection.

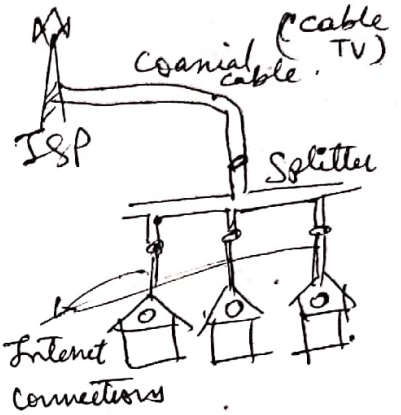
VTP

- Therefore voice calls & Internet connections can be simultaneously done. (which was not possible with Dialup Connection)



Cable Internet connection

- Internet connection via ~~Cable~~ Television cables (coaxial cables)



- Shared Bandwidth
- Slower than DSL

Shubhangi K

Comparison Between Dial up & DSL

Parameter	Dial up	DSL
• Speed	Dial-up access offers speeds upto a maximum of 56KbPS	DSL offers guaranteed speeds (symmetrical up to 1Mbits/s or 35 times faster than 28.8 Kbits/s analog modem) and assymetrical upto 7Mbits/s
• Flexibility	Dial-up access is capable of providing internet access to only one PC (end-user), thereby charging extra for each additional (PC or enduser) access.	DSL provides Internet access to multiple PC's (end users) on a single connection, thereby not charging extra for all additional PC (end user). DSL is fully scalable service possessing a wide range of potential speeds.
	Dial up access is not a scable service due to its Bandwidth limitations	
• Reliability	Has tedious process of dialing in for the Internet access	No time consuming dialing in for Internet access. Connection is dedicated so no disruptions.

Shubhangi K

DSL Vs Cable Modem

Parameters	DSL	Cable Modem
Speed	• DSL offers a wide range of guaranteed speeds as high as 1 MbPS (Symmetrical)	• Cable Modem exists on a shared n/w thereby making speed performance unpredictable; it is entirely contingent on network traffic volume.
Security	• DSL is on a closed dedicated circuit making it less susceptible to outside hackers	• Cable Modem is on a shared n/w making it more vulnerable to hackers.
Reliability	• DSL is on a closed dedicated circuit, thereby offering guaranteed speeds	• Cable Modem exists on a shared n/w thereby making speed performance unpredictable.
Accessibility	• DSL utilizes ubiquitous, 100-year old telephone infra-structure (RJ-11 jacks, copper phone wire, data backbones etc), which makes up nearly 100% Market accessibility	• Sporadic & inconsistent service availability. • Cable Modem has a slower rate of market infiltration ~~because of~~

Shubhangi K

	WiMAX	WiFi
Coverage	Vast, Broader Area (upto 40 miles)	Small (approx 100 feet)
Spectrum	Licensed	Unlicensed
Mobility	Anywhere, Anytime	Limited to Hotspot locations
Speed	Higher Speed (70MBPS or more)	Limited Speed (54 MBPS)
Quality of Service	Support Multimedia Applications (Guaranteed QoS)	Does not support Multimedia applications, Unreliable. (QoS is not gaurenteed)
Standard	Based on IEEE 802.16 Standard	Based on IEEE 802.11 Standard
Waves	Uses microwaves (Unidirectional)	uses radio waves (Omnidirectional)
Launched in year	2004	1997
Network	MAN	LAN
Channel Bandwidth	~~20MHz~~ Variable, 1.25 - 20 MHz	20 MHz
Subscribers	Unlimited	1-10 approx
Radio Technology	OFDM	Direct access / Spread Spectrum
Access protocol	CSMA/CA	Grant or Request.

Shubhangi.c

Wi-MAX (MAN)

Technical Specifications

Specifications	802.16 d (fixed access)	802.16 e (mobile access)
1) BW(MHz)	1.75 to 20 MHz	1.25 to 20 MHz
2) Operating frequency	2-11 GHz	2-6 GHz
3) Mobility	Fixed / (Roaming)	Mobile
4) Tx Technology (access method)	Multicarrier OFDMA	OFDMA
5) Spectrum assignment	Subchainelization	Subchainelization
6) Mode	TDD, FDD	TDD, FDD
7) Peak rate	75 MbPS	5, 30 MbPS
8) Modulation	BPSK, 16 QAM	64 QAM
9) Enhanced Techniques	Intelligent Antenna Systems MIMO, HARQ.	MIMO, HARQ
10) Energy Saving		Idle & sleep mode.

Shubhangi K

	FDM	TDM
Definition	1) Signals are transmitted at different frequencies but at the same time. (Multiplexing in frequency domain)	1) Signals are transmitted at different times but at the same frequency (Multiplexing in Time domain)
Type of Signal	2) FDM is usually preferred for analog signals	2) TDM is preferred for the digital signals
Synch	3) Synchronization is not required	3) Synchronization is required
Circuitry	4) FDM requires a complex circuitry at Tx & Rx	4) TDM requires simple circuitry
Crosstalk	5) FDM suffers from the problem of crosstalk due to imperfect BPF	5) In TDM the problem of crosstalk is not severe
Fading	6) Due to Bandwidth fading in the Tx medium, all the FDM channels are affected	6) Due to fading only a few TDM channels will be affected.

Shubhangi K

Advantages & Disadvantages of Multiplexing Techniques

Multiplexing Technique	Advantages	Disadvantages
Frequency Division Multiplexing	• Simple • Popular with radio, TV., Cable TV • All receivers such as cellular Telephones, do not need to be at the same location	• Noise problems due to analog signals • wastes Bandwidth • Limited by frequency ranges.
Synchronous Time Division Multiplexing	• Digital Signals • relatively Simple • commonly used with T-1, ISDN	wastes Bandwidth
Asynchronous (Statistical) Time Division Multiplexing	• Make efficient use of BW. • Frame can contain control & error information • packets can be of varying size	More complex than Synchronous time division Multiplexing

* T-1 lines used in North America
E-1 lines are used in Europe.

Shubhangi K

Multiplexing Technique	Advantages	Disadvantages
Wavelength Division Multiplexing	• Very high capacities over fibre • Signals can have varying speeds • scalable	cost complexity
Code Division Multiplexing	• Large capacities Scalable	• Complexity • primarily a wireless technology

* Difference Between Hub & a Switch

Shubhangi Khatke

	Hub	Switch
Layer in OSI Model	Physical layer (Layer1 Device)	Data Link Layer (Layer 2 Devices)
Transmission Type	Only Broadcast	At Initial level Broadcast then Unicast & Multicast
Table	There is no MAC Table in Hub, Hub can't learn MAC address	Store MAC address in lookup table, Switch can Learn MAC address
Usage	LAN	LAN
Ports	4 Ports	24/48 Ports
Collision	In Hub Collision occurs	In Full duplex Mode no collision occurs
Transmission Mode	Half Duplex	Full duplex
collision domain	Hub has one collision domain	In switch, every port has its own collision domain
cost	Cheaper than Switches	3-4 times costlier than Hub
Broadcast Domain	Hub has one Broadcast Domain	Switch has one Broadcast Domain

Difference Between Switch & Router (networking devices)

Switch	Router
1) It is the LAN device	1) It is the WAN device
2) Switch maintains MAC tables	2) Router maintains IP tables (routing) tables
3) Switch understands MAC address (Hardware/Physical/Link) address	3) Router understands IP address (logical address)
4) Switch connects devices in a LAN or Switch connects devices belonging to two similar LAN's together	4) Router connects more than two dissimilar networks together. Router connects LAN to a WAN. Router can connect Ethernet LAN with token ring LAN (dissimilar n/w's)
5) Switch is an Intranetworking device (LAN)	5) Router is an Internetworking device (Connects diff n/w's in WAN or Internet)
6) Switch is Layer 2 networking device (used at Layer 2 of OSI model)	6) Router is Layer 3 networking device (used at Layer 3 of OSI model)
7) In full Duplex Switch no collision occurs	7) No collisions
8) Full Duplex Transmission	8) Full Duplex transmission
~~9) Speed: 1-10 Mbps (wireless) 100 Mbps (wired)~~	~~Speed 10/100 Mbps~~ 1 Gbps

	Switch	Router
9)	Speed → 10/100 MbPS, 1 GbPS	Speed 1–10 MbPS (wireless), 100 MbPS (wired)
10)	Switch has one Broadcast domain	Every port has its own Broadcast domain
11)	Takes more time for complicated Switching decision	Takes faster routing Decision

Shubhangi Khaslale

	Repeater	Hub	Switch	Bridge	Router
1)	Layer 1 (Phy) of OSI Model	Layer 1 (Physical) of OSI Model	Layer 2 (~~Phy~~) Datalink of OSI Model	Layer 2 (Data Link) of OSI Model	Layer 3 (Network Layer of OSI Model)
2)	Regenerates the signal (extends LAN Segments)	connects computers ~~to~~ together (Multiport repeater as it regenerates the signal)	connects computers in LAN or connects two similar LAN Segments together (Ethernet to Ethernet) or (Token ring to Token ring) → 10Base2 to 10Base F or 10Base T to 10Base F	connects two dissimilar LAN's together (Ethernet to Token ring) or (Ethernet to FDDI)	connects two dissimilar n/w's together (LAN to WAN) (Ethernet & FDDI LANs to WAN)
3)	Does not have filtering capability	Does not have filtering capability	~~Does not~~ Has filtering capability	fillets (Has filtering capability) frames	fillets packets
4)	Dumb device	Dumb device	Intelligent device	More Intelligent than Switch	Intelligent device

	Repeater	Hub	Switch	Bridge	Router
(5)	It has Two ports	usually has 4 ports 5th port connects to another Hub (Hubs generally have even no of ports 4, 8, 12, 16, 24 Maximum 24 ports	usually has even number of ports	less no of ports than Switch (2-3 ports)	Minimum two Interfaces (Maximum can be upto 100) Routers have Five ports 1) console port (connects to PC) 2) auxiliary port (connects to internet) 3) LAN port (RJ-45) (connects to Ethernet, Fast Ethernet or Gigabit Ethernet) 4) WAN Port (Serial Interface, RJ-11 ⇒ Telephone line) (Serial connects → Router to Router) 5) USB Port.
(6)	No Memory	No Memory	Memory to save MAC tables	Memory to save MAC tables Also has processing capability	Memory → RAM (• running OS • Running configuration file • IP routing tables, ARP Tables • Packet buffer); ROM (permanent OS • Bootstrapping); Flash (• IOS • other system files); NV-RAM (• start-up configuration)

Shubhangi Khaire

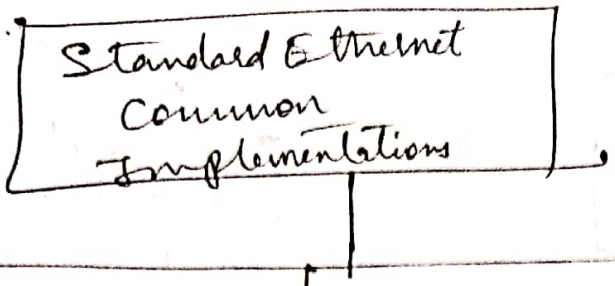
Scanned with CamScanner

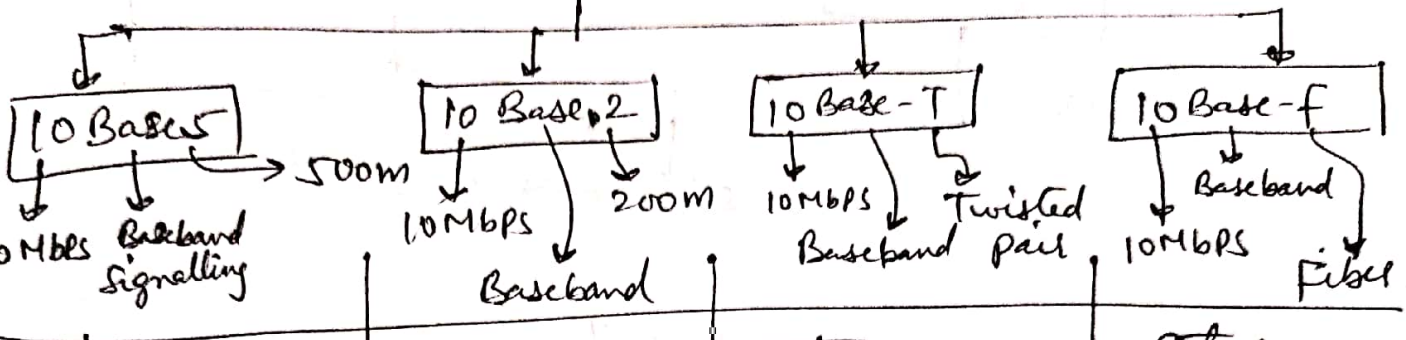
Repeater	Hub	Switch	Bridge	Router
	• Single collision domain • All ports (all m/c's) lie in single collision domain • Information is always Broadcasted	Separate collision domains (NO collision) (Each port of a switch lies in separate collision domain • Broadcasting when S/w is initialised later on unicasting or multicasting.	• Separate Broadcasting & collision domains	

Shubhangi Khurana.

- Removes congestion
- Does Traffic Management.

Physical Layer of Standard Ethernet

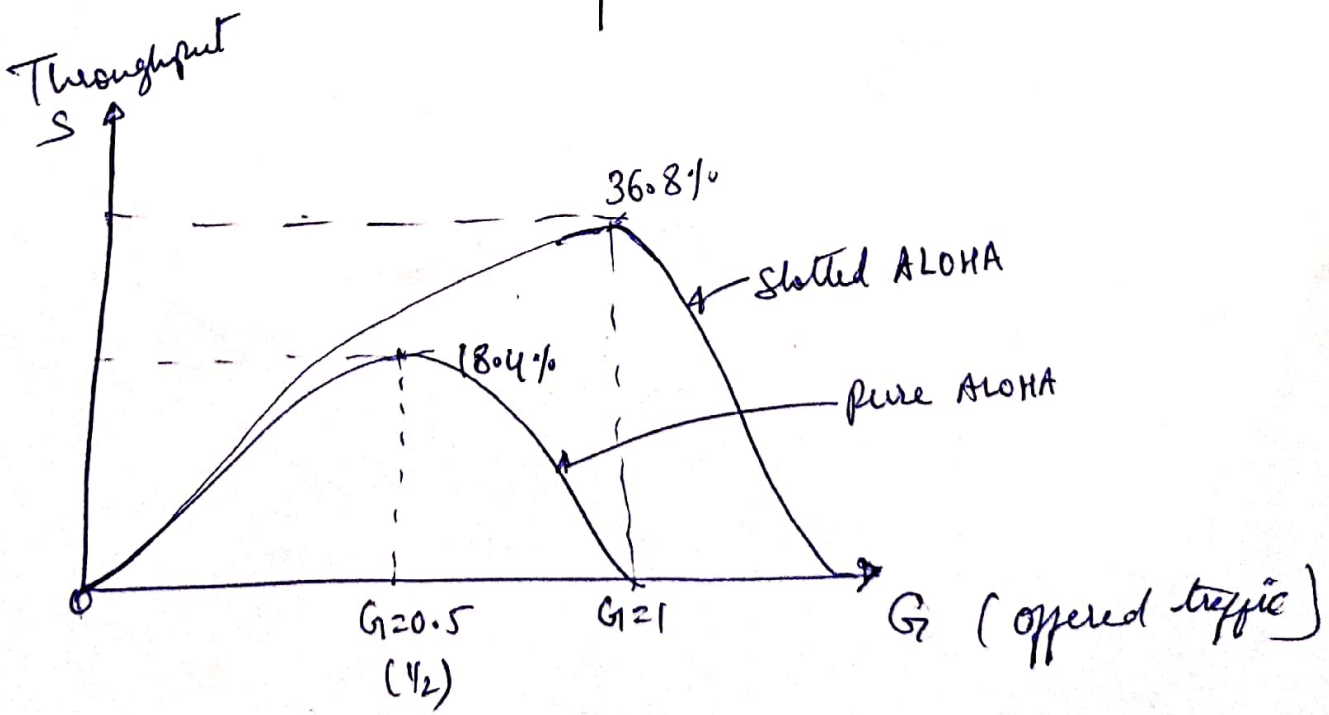




	10 Base5	10 Base2	10 Base-T	10 Base-f
Topology	Bus	Bus	Star	Star
Physical media	Thick coaxial	Thin coaxial	UTP (2 pairs)	Fiber (2 in number)
Maximum Length	500 m	185 m	100 m	2000 m
Line encoding	Manchester	Manchester	Manchester	Manchester
Called as	Thick Ethernet or Thicknet	Thin Ethernet or cheapernet	Twisted pair Ethernet	Fiber Ethernet

Shubhangi Khaire.

Pure ALOHA	Slotted ALOHA
1) No Synchronised Transmission	1) Synchronised Transmission (At the beginning of every time slot)
2) Vulnerable period $= 2 \times T_{fr}$	2) Vulnerable period $= T_{fr}$
3) Maximum throughput $S_{max} = 0.184$ $= 18.4\%$ at $G = \frac{1}{2}$	3) Maximum throughput $S_{max} = 0.368$ $= 36.8\%$ at $G = 1$
throughput $S = G e^{-2G}$	throughput $S = G e^{-G}$



Distance Vector Vs Link State Routing protocols

Distance Vector Routing Protocol	Link State Routing Protocol
• Entire routing table is sent as an update	• Updates are incremental and entire routing table is not sent as update.
• Send periodic update (Every fixed interval of time) at every 30 or 90 Second.	• Updates are triggered not periodic.
• Updates are broadcasted (not in RIPV2) Due to this large BW is used	• Updates are Multicasted. No unnecessary BW consumption.
• updates are sent to directly connected neighbor only.	• update are sent to entire network
• Routers don't have end to end visibility of entire network	• Routers have visibility of entire network of that area only
• Prone to routing loops	• No routing loops

	RIP	OSPF	EIGRP
Nature	Distance Vector	Link State	Hybrid
Scale	Small networks	Enterprise networks	Medium
Routing	Classful routing, loop counter mechanism	Classless	Classless 100% loop free
Metrics	Number of hops	The inverse of BW of links	Available BW, delay, load MTU & the link Reliability
Updates	Periodic (Broadcasts)	Incremental	Incremented updates (multicasts)
Failure Recovery	Slow convergence	Generally faster than RIP	DUAL Algorithm
Load Balancing	only supported on equal-cost paths	Support six equal cost paths, but difficult to implement	Supports six equal cost paths but commonly ignored due to its complexity & instability

Features	RIP		OSPF
	Version 1	Version 2	
Algorithm	Bellman Ford		Dijkstra
path selection	Hop based		Shortest Path
Routing	Classful	classless	classless
Transmission	Broadcast	Multicast	Multicast
Administrative Distance	120		110
Hop count limitation	15		No Limitation
Authetication	No	MD5	MD5
Protocol	UDP		IP
Convergence Time	More		Less