

Computer Networks 1 | CN1

Summary

CONTENTS

1. Application Layer (7,6,5)	5
1.1. HTTP	5
1.2. Common Ports	6
1.3. DNS	6
1.3.1. Record types	6
1.4. E-Mail	6
2. Transport Layer (4)	7
2.1. Primary responsibilities	7
2.2. TCP	7
2.2.1. Reliability	8
2.2.2. Throughput	8
2.2.3. Flow control	8
2.2.4. Congestion control	9
2.3. UDP	10
2.4. QUIC	10
3. Network Layer (3)	10
3.1. Subnetting	10
3.2. IPv6	10
3.2.1. Glossary	11
3.2.2. Special addresses	11
3.2.2.1. Multicast	12
3.2.2.2. DHCPv6	12
3.2.3. Header	12
3.2.3.1. IPv6 Extension Headers currently defined	13
3.2.4. Neighbor Discovery Protocol (NDP)	13
3.2.4.1. Host - Router Discovery Functions	13
3.2.4.2. Host - Host Communication Functions	13
3.2.4.3. Packet types	14
3.2.5. Stateless Address Autoconfiguration (SLAAC)	14
3.2.5.1. Autoconfigure link-local address	14
3.2.5.2. Perform Duplicate Address Detection (DAD)	14
3.2.5.3. Router search	14
3.2.5.4. Generating global unicast address	14
3.2.6. DHCPv6	15
3.2.6.1. Flags	15
3.3. IPv4	15
3.3.1. Network classes (private nets)	15
3.3.2. Subnetting	15
3.3.2.1. Calculating subnet mask	15
3.3.2.2. Calculating increment	15
3.4. Routing	15

3.4.1. Data plane	15
3.4.2. Control plane	16
3.4.3. Dynamic	16
3.4.3.1. Dijkstra's algorithm (Link State)	16
3.4.3.2. OSPF (Open Shortest Path First) (Distance vector)	16
3.4.3.3. BGP (Border Gateway Protocol)	16
3.4.4. Fragmentation	16
4. Data Link Layer (2)	16
4.1. Ethernet	16
4.1.1. Carrier Sense Multiple Access with Collision Detection (CSMA/CD)	16
4.1.1.1. Collision domain	17
4.1.1.2. What happens when a collision occurs?	17
4.1.2. Half-duplex vs Full-duplex	17
4.1.3. Ethernet II Frame	17
4.1.4. IEEE 802.3 Frame	17
4.1.5. Frame Check Sequence (FCS)	17
4.2. MAC-Address	17
4.3. Address Resolution Protocol (ARP)	18
4.3.1. Discovery	18
4.3.2. Spoofing	18
4.4. Switch	18
4.4.1. Flooding	18
4.4.2. Filtering	18
4.4.3. Forwarding	18
4.5. VLAN	18
4.5.1. Trunking	19
4.5.2. 802.1Q	19
4.5.3. Inter-VLAN Routing	19
4.5.3.1. Attaching a Router	19
4.5.3.2. Using a Layer 3 Switch	19
4.5.4. Link Aggregation Group (LAG)	19
4.5.5. Link Aggregation Control Protocol (LACP)	19
4.5.6. Spanning-Tree Protocol (STP)	19
4.5.6.1. Procedure	20
4.5.6.2. Determining bridge priority	20
4.5.6.3. Port states	20
4.5.6.4. Topology change	20
4.5.7. Rapid Spanning Tree Protocol (RSTP)	20
4.6. Error detection	20
4.6.1. Cyclic Redundancy Check (CRC)	20
4.7. Wireless	21
4.7.1. Channel bonding	21
4.7.2. Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)	21
4.7.2.1. Hidden node	21
4.7.2.2. Distributed Coordination Function (DCF)	21
4.7.2.3. Network Allocation Vector (NAV)	21
4.7.3. Frame	21
4.7.4. Management features	21
4.7.4.1. Beacon	21

4.7.4.2. Association / Reassociation	21
4.7.5. Roaming	22
5. Physical Layer (1)	22
5.1. Encodings	22
5.1.1. Manchester encoding	22
5.1.2. RZ (Return-to-Zero)	23
5.1.3. NRZ (Non-Return-to-Zero)	23
5.1.4. 8b/10b (Clock recovery)	23
5.2. Power and dB	23
5.2.1. Law of 3s	23
5.2.2. Law of 10s	23
5.3. Modulation	23
5.4. Fiber media	23
5.4.1. Eye Diagram	24
5.4.2. Attenuation	24
5.4.3. Dispersion	24
5.4.4. Regeneration	24
5.5. Frequency	25
5.6. Calculations	25
5.6.1. Speed of Signals	25
5.6.2. Optical budget	25
6. Cisco	25
6.1. Router setup	25
6.2. Interfaces	25
6.2.1. Static IP Assignment	25
6.2.2. DHCP Assignment	25
6.2.3. Show	25
6.3. VLAN	26
6.3.1. Assign IP	26
6.3.2. Access Port	26
6.3.3. Access Port	26
6.3.4. VTP (Virtual Trunk Protocol)	26
6.3.4.1. Server	26
6.3.4.2. Client	26
6.3.5. LACP (Link Aggregation Control Protocol)	26
6.3.6. Load Balancing	26
6.3.7. STP (Spanning Tree Protocol)	26
6.3.7.1. Bridge priority	26
6.3.7.2. Interface costs	26
6.3.7.3. PortFast mode	26
6.3.7.4. Show	26
6.4. Routing	27
6.4.1. Static	27
6.4.1.1. IPv4	27
6.4.1.2. IPv6	27
6.4.2. OSPF	27
6.4.2.1. IPv4	27
6.4.2.2. IPv6	27
6.4.3. Show	27

6.5. DHCP	27
6.5.1. Create Pool	27
6.5.2. Relay Agent	27
6.6. NAT	27
6.6.1. IF Inside	27
6.6.2. IF Outside	27
6.6.3. ACL (Access Control List)	27
6.6.4. PAT (Nat overload)	28
6.7. IPv6	28
6.7.1. DHCPv6	28
6.8. Troubleshooting	28
6.8.1. Ping	28
6.8.2. Traceroute	28
7. Binary, Decimal, Hex	28

1. APPLICATION LAYER (7,6,5)

Combines Layers 7 (Application), 6 (Presentation) and 5 (Session).

1.1. HTTP

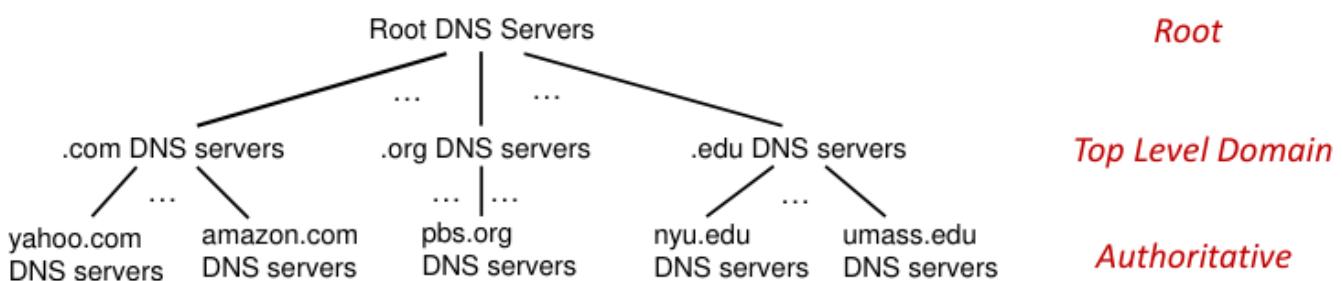
Feature	HTTP/1.0	HTTP/1.1	HTTP/2	HTTP/3
Connection Management	One request per connection	Persistent connections by default	Multiplexing allows multiple streams	Uses QUIC for multiplexing
Request Methods	Limited (GET, POST, HEAD)	Enhanced (PUT, DELETE, OPTIONS, etc.)	Same as 1.1	Same as 1.1
Caching	Basic caching support	Improved caching with validation	Advanced caching capabilities	Same as 2 but with improved mechanisms
Header Compression	None	None	HPACK (header compression)	QPACK (header compression)
Server Push	Not supported	Not supported	Supported (automatic resource pushing)	Enhanced support for server push
Performance Improvements	None	Minor improvements over 1.0	Significant improvements in performance and latency	Further improvements in speed and efficiency
SSL/TLS Support	Not inherent	Not inherent, but commonly supported	Built-in support with ALPN (Application-Layer Protocol Negotiation)	Uses QUIC, which incorporates TLS 1.3
Transport Protocol	TCP	TCP	TCP	QUIC

1.2. COMMON PORTS

Protocol	Port	Layer 4
DNS	53	UDP, TCP
HTTP	80	TCP
HTTPS	443	TCP
FTP	20, 21	TCP
SMTP	25 (server) 587 (client)	TCP
POP3	110	TCP
DHCP	67 (server) 68 (client)	UDP

1.3. DNS

Nameservers resolve domains to IP's through a distributed, hierarchical database.



Term	Definition
Iterated query	Local DNS server iteratively asks one server after the other, descending the domain name hierarchy step after step.
Recursive query	Local DNS server asks root server for domain, which in turn asks the TLD server, which in turn asks the authoritative server etc. until the “call stack” unwinds and returns the fully resolved domain to the query sender.
Caching	

1.3.1. Record types

Type	Name	Value
A	hostname	IPv4 address
AAAA	hostname	IPv6 address
CNAME	alias	canonical name
NS	domain	hostname of authoritative NS for this domain
MX	domain	name of mailserver

1.4. E-MAIL

Term	Definition
ding	
dong	
your	

Term	Definition
opinion	
is	
wrong	

2. TRANSPORT LAYER (4)

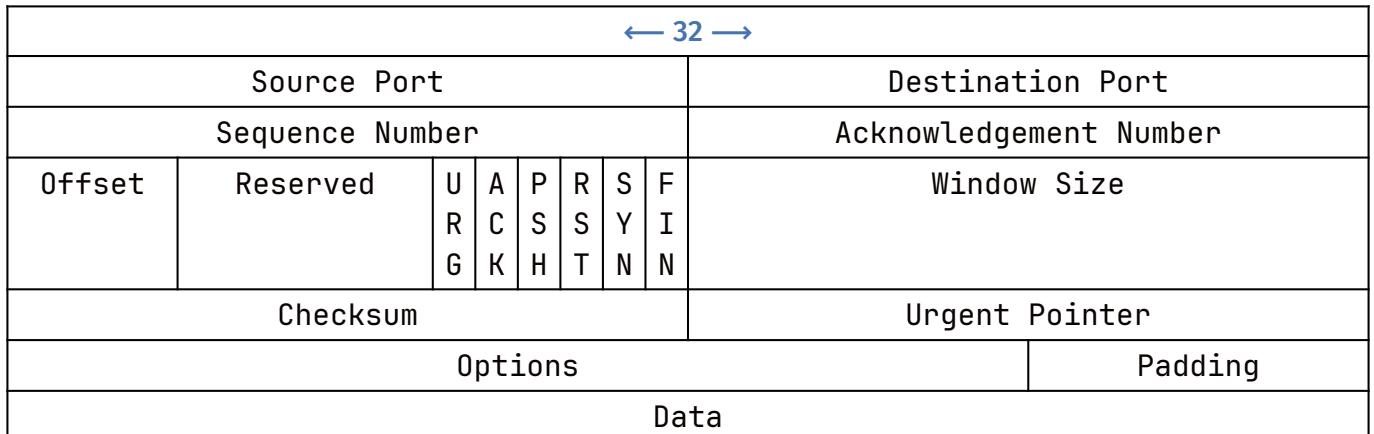
Segment size: 1440-1480b when using IPv4, <=1460b when using IPv6

2.1. PRIMARY RESPONSIBILITIES

- Process-to-process delivery (distinguish between multiple applications via ports)
- Ensure reliable transfer (acknowledgments, retransmissions & reordering)
- Flow control (sender does not overwhelm receiver)
- Congestion control (network is not overloaded)

Term	Definition
Port	16 bit long numbers (0-65535) for identifying applications to send packets to. Well-Known: 0-1023 for universal TCP/IP applications, managed by the IANA. Registered: 1024-49151 for known applications, also managed by the IANA. Private: 49152-65535 for custom applications, not managed by the IANA.
Socket	Combination of IP:Port .
Multiplexing	Sending data from multiple sockets at sender.
Demultiplexing	Delivering segments to correct socket at receiver.
Checksum	Detect errors (i.e., flipped bits) in transmitted segment.

2.2. TCP



TODO: explanations

Connection-oriented, bidirectional, reliable, managed data flow.

Term	Definition
Handshake	Agreement on starting sequence numbers, maximum segment size and window scaling . 1) SEQ 2) SEQ+ACK 3) ACK

Term	Definition
FIN	Termination of a connection. 1) FIN 2) FIN+ACK 3) ACK
Round Trip Time	RTT is the time it takes for a packet to be sent to the receiver and acknowledged back to the sender.
Buffer size	Maximum amount of data (measured in bytes) that can be stored in memory while waiting to be processed or transmitted.
Maximum Segment Size	MSS is the maximum payload size of a TCP packet. In IPv4 networks, typically, the size of the MSS is 1460 bytes because it is encapsulated in the data link layer Ethernet frame size of 1500 bytes .

2.2.1. Reliability

Term	Definition
Sequence numbers	SEQ ensures that the packets arrive or can be reassembled in order.
Acknowledgement	ACK ensures that the receiver gets all of the packets.
Retransmission timeout	If an acknowledgment is not received before the timer for a segment expires, a retransmission timeout occurs, and the segment is automatically retransmitted .
Packet loss rate	Measures how many packets of the ones being sent actually arrive.

2.2.2. Throughput

Term	Definition
Throughput	Denoted by T , is the amount of data that can be transmitted during a specified time. $T = \frac{W}{R} \leq C_{L3}$
Continuous sending	Sender transmits a stream of data packets in the given window size without waiting for acknowledgments .
Delayed ACK	Receiver waits for a short period to acknowledge multiple segments with a single ACK .
Selective ACK	Instead of asking for a retransmission of all missing segments, SACK (specified by the receiver) allows the sender to send only the lost segments, significantly improving efficiency.

2.2.3. Flow control

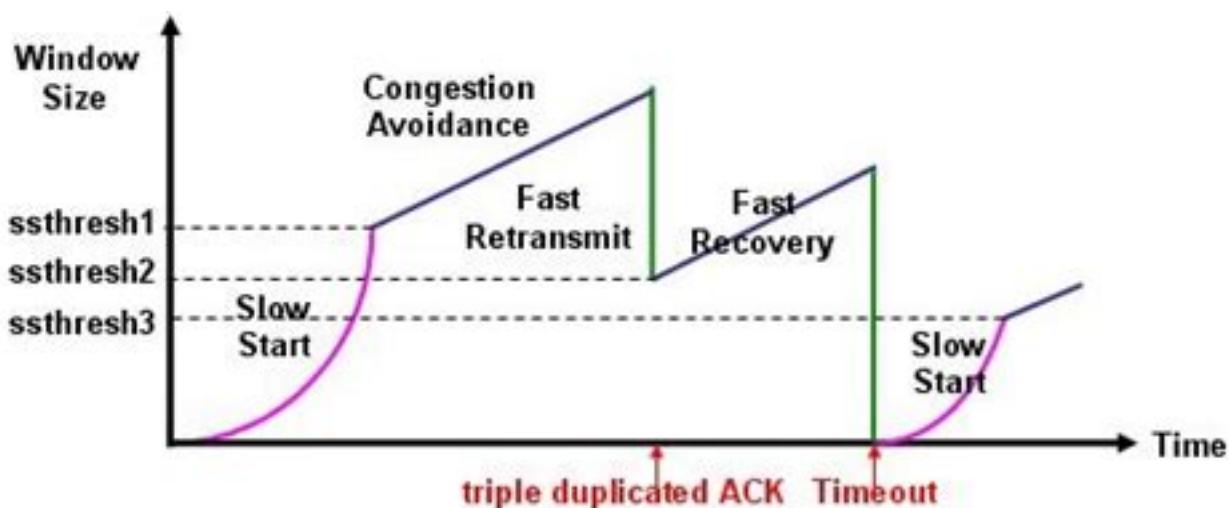
So that the sender does not overwhelm the receiver.

Term	Definition
Window Size	Denoted by W , is a 16 bit number sent with each packet by the receiver inside of the rwnd header field, indicating the amount of data he still has space for.

Term	Definition
Window scale	Used when the TCP window size needs to be increased beyond the traditional maximum of 65,535 bytes due to the demands of high-speed networks. If the handshake header includes the window scale option and the packet header includes the scaling factor then the effective window size is calculated as such: $\text{window size} * \text{scaling factor}$

2.2.4. Congestion control

To prevent network congestion.



Term	Definition
Congestion window	<p>The diagram illustrates the state of the congestion window (<code>cwnd</code>). It consists of a sequence of vertical bars representing packets. The first set of bars is green, labeled 'last byte ACKed'. The middle set is yellow, labeled 'sent, but not-yet ACKed ("in-flight")'. The final set is blue, labeled 'available but not used'. Red brackets above the bars indicate the boundaries of the window, and a red bracket below the bars indicates the 'last byte sent'.</p>
Sliding Window	Describes the process of the congestion window sliding to the right after receiving ACKs.
Slow start	Gradual growth (doubling <code>cwnd</code> every RTT) within the congestion window size at the start of a connection or after a period of state of no activity. Purpose: Allows the sender to probe the available bandwidth in a controlled way.
Congestion avoidance	Transition from sluggish start to congestion avoidance segment after accomplishing a threshold. Purpose: Maintains a truthful share of the community bandwidth even as heading off excessive congestion.

Term	Definition
Fast Retransmit	Detects packet loss through duplicate acknowledgments and triggers speedy retransmission without waiting for the retransmission timeout . Purpose: Speeds up the recuperation method with the aid of retransmitting lost packets without looking ahead to a timeout.
Fast Recovery	Enters a quick healing state after detecting packet loss, lowering congestion window and transitioning to congestion avoidance. Purpose: Accelerates healing from congestion by way of avoiding a complete go back to slow begin after packet loss.
AIMD	Adjusts the congestion window size based on network situations following the Additive Increase, Multiplicative Decrease principle. Purpose: Provides a balanced approach by way of linearly growing the window all through congestion avoidance and halving it on packet loss.

2.3. UDP

$\leftarrow 32 \rightarrow$	
Source Port	Destination Port
Length	Checksum
Data	

TODO: explanations

2.4. QUIC

TODO: header

Actually a layer 7 Protocol, running on top of UDP

3. NETWORK LAYER (3)

Packet size: **1500b**

3.1. SUBNETTING

Dividing a **/X** network into **n** amount of **/Y** subnets: $2^{Y-X} = n$.

Eg: Dividing a **/16** network into **/24** subnets will yield **256** subnets, because $2^{24-16} = 2^8 = 256$

3.2. IPV6

$\leftarrow 32 \rightarrow$		
Version	Traffic class	Flow label
Payload length	Next header	Hop limit
Source address (128 bits)		
Destination address (128 bits)		

TODO: explanations

3.2.1. Glossary

Term	Definition
Extension Header	Additional headers used in IPv6 to provide optional information. These can define aspects like payload size, routing, or fragmentation.
DHCPv6	Dynamic Host Configuration Protocol for IPv6; this allows servers to assign IPv6 addresses dynamically from a pool, similar to DHCP for IPv4.
NAT64	Network Address Translation from IPv6 to IPv4 and vice versa; it facilitates communication between IPv6 and IPv4 networks.
Neighbor Discovery Protocol (NDP)	A protocol in IPv6 for discovering other network nodes, determining their link-layer addresses, and ensuring that addresses are valid and reachable.
Internet Control Message Protocol (ICMPv6)	A crucial part of IPv6 that handles error messages and operational queries, with an expanded role compared to ICMP in IPv4.
MTU	Maximum Transmission Unit; the size of the largest packet that can be sent in a single frame over a network medium. IPv6 can handle larger MTUs compared to IPv4.
Multicast Listener Discovery (MLD)	IPv6 multicast routers can use MLD to discover multicast listeners on a directly attached link.
Path MTU Discovery (PMTUD)	Protocol for determining the Maximum Transmission Unit (MTU) size on the network path between two hosts, usually with the goal of avoiding IP fragmentation.

3.2.2. Special addresses

Term	Definition
Link-local Address	FE80::/10 Used for local communication between devices on the same network segment.
Global Unicast Address	2000::/3 A globally routable address, these addresses are equivalent to public IPv4 addresses and can be reached over the internet.
Unique Local Address (ULA)	FC00::/7 An address for local communication that is not routable on the global internet, similar to private addresses in IPv4.
Multicast Address	FF00::/8 An address that enables a single packet to be sent to multiple destinations simultaneously.
Anycast Address	An address assigned to multiple interfaces, where a packet sent to an anycast address is routed to the nearest (in terms of routing distance) interface.
Reserved Address	Certain ranges in IPv6 are reserved for future use or specific functions. For example, addresses starting with ::/128 are reserved for unspecified addresses.
Documentation Address	2001:DB8::/32 Designated specifically for use in documentation and examples, ensuring it does not conflict with real-world addresses.

Term	Definition	
Link-local Multicast Address	FF02::/16 Part of the link-local address range; it enables devices to communicate within a local network without requiring an external routing address.	
Addresses	Range	Scope
Unspecified	::/128	n/a
Loopback	::1	Host
IPv4-Embedded	64:ff9b::/96	n/a
Discard-Only	100::/64	n/a
Link-Local	fe80::/10	Link
Global Unicast	2000::/3	Global
Unique Local (ULA)	fc00::/7	Global
Multicast	ff00::/8	Variable

3.2.2.1. Multicast

Term	Definition
ff02::1	All nodes, within scope 2 (link-local).
ff02::2	All routers, within scope 2 (link-local).
ff02::1:ffff:xxxx	The IPv6 node joins a solicited multicast address group from all the interfaces where unicast and anycast addresses are configured. Its scope is the link-local.

3.2.2.2. DHCPv6

Term	Definition
ff02::1:2	A link-scoped multicast address used by a client to communicate with neighboring (i.e., on-link) relay agents and servers. All servers and relay agents are members of this multicast group.
ff05::1:3	A site-scoped multicast address used by a relay agent to communicate with servers, either because the relay agent wants to send messages to all servers or because it does not know the unicast address of the servers.

3.2.3. Header

Term	Definition
Version	Always 6 with IPv6. IPv4 would be 4.
Flow Label	For identifying packets that require special handling, like real-time streaming.
Traffic Class	Priority or type of traffic.
Payload Length	Size of the payload in bytes.
Next Header	Type of optional header following the IPv6 header.
Hop Limit	Maximum number of hops a packet can take before being discarded.

3.2.3.1. IPv6 Extension Headers currently defined

<i>Term</i>	<i>Definition</i>
Routing	Extended routing, like IPv4 loose source route. The Routing header is used by an IPv6 source to list one or more intermediate nodes to be “visited” on the way to a packet’s destination. There are different types of routing headers defined for different uses.
Fragmentation	Fragmentation and reassembly. The Fragment header is used by an IPv6 source to send a packet larger than would fit in the path MTU to its destination.
Authentication	Integrity and authentication, security. The Authentication Header (AH) is used by IPsec to provide security services like integrity and data origin authentication to IPv6 traffic.
Encapsulating Security Payload	Confidentiality. Encapsulating Security Payload (ESP) Extension Header [RFC2406(opens in a new tab)] is used by IPsec to provide security services like confidentiality and/or integrity to IPv6 packets. The ESP Extension Header can be followed by an additional Destination Options Extension Header and the upper layer datagram.
Hop-by-Hop Option	Special options that require hop-by-hop processing. The Hop-by-Hop Options header is used to carry optional information that may be examined and processed by every node along a packet’s delivery path. The information is included in the form of one or more options using a TLV (Type-Length-Value) format.
Destination Options	Optional information to be examined by the destination node. The Destination Options header is used to carry optional information that is meant to be examined only by a packet’s destination node(s). The information is included in the form of one or more options using a TLV (Type-Length-Value) format.

3.2.4. Neighbor Discovery Protocol (NDP)

3.2.4.1. Host - Router Discovery Functions

<i>Term</i>	<i>Definition</i>
Router discovery	Hosts can locate routers residing on attached links.
Prefix discovery	Hosts can discover address prefixes that are on-link for attached links.
Parameter discovery	Hosts can find parameters (e.g., MTU).
Address autoconfiguration	Stateless configuration of addresses of network interfaces.
Redirect	Provide a better next-hop route for certain destinations.

3.2.4.2. Host - Host Communication Functions

<i>Term</i>	<i>Definition</i>
Address resolution	Mapping between IP addresses and link-layer addresses. This is equivalent to ARP for IPv4. This function allows to resolve the link-layer address of another node in the link when only the IPv6 address of that node is known.
Next-hop determination	Hosts can find next-hop routers for a destination.
Neighbor unreachability detection (NUD)	Determine that a neighbor is no longer reachable on the link.

Term	Definition
Duplicate address detection (DAD)	Nodes can check whether an address is already in use.

3.2.4.3. Packet types

Name	Type	Description
Router Solicitation (RS)	133	To locate routers on an attached link.
Router Advertisement (RA)	134	Used by routers to advertise their presence periodically or in response to a RS message.
Neighbor Solicitation (NS)	135	To find the MAC-address of the neighbor or to check if the neighbor is still reachable.
Neighbor Advertisement (NA)	136	To respond to a Neighbor Solicitation message.
Redirect	137	To point the host to a better first hop router for a destination.

3.2.5. Stateless Address Autoconfiguration (SLAAC)

A method for automatically configuring IPv6 addresses without a DHCP server, relying on local network information.

3.2.5.1. Autoconfigure link-local address

Mac address: **70:07:12:34:56:78**

- 1) Flip **7th** bit: 72:07:12:34:56:78. If it is “0”, the address is locally administered and if it is “1”, the address is globally unique.
- 2) Insert **FFEE** in the middle: 7207:12**FF:EE**34:5678
- 3) Combine with link-local prefix: **FE80::**7207:12FF:EE34:5678

New address: **FE80::7207:12FF:EE34:5678**

3.2.5.2. Perform Duplicate Address Detection (DAD)

To make sure that the address is actually unique in the local segment.

Upon configuring an IPv6 address, every node joins a **multicast group** identified by the address **FF02::1:FFxx:xxxx** where xx:xxxx are the **last 6 hexadecimal values** in the IPv6 unicast address, eg. FF02::1:**FF34:5678**

- 1) The host sends a Neighbor Solicitation message from the Unspecified Address (::) to the Solicited Node multicast address.
- 2) If the generated address is in use, the host using that address sends a Neighbor Advertisement back. The sending host then knows the tentative address can not be used.
- 3) The host then proceeds to generate a new address and sends a new Neighbor Solicitation message to the link.
- 4) If there is no reply after some time, the host informs all the other hosts that it uses this address and it sends a Neighbor Advertisement message to the All Nodes address.
- 5) The host assigns the address to the interface and now has an active IPv6 link. This is the so-called Link-local Address Assignment.

3.2.5.3. Router search

- 1) Router solicitation
- 2) Router advertisement

3.2.5.4. Generating global unicast address

Based on the information from the Router Advertisement, the host generates a global unicast address and wants to know if it is available to use, so it does the DAD process again. If it is not a duplicate, the host will use it.

3.2.6. DHCPv6

3.2.6.1. Flags

Term	Definition
A	Host can perform SLAAC to generate its own IPv6 address based on the prefix(es) contained in the RA message.
O	Host can fetch additional options from the DHCPv6. The DHCPv6 does not provide IPv6 addresses in this case.
M	Host will get its IP address and additional options from a DHCPv6 server.
L	The prefix shared in the RA is reachable on the link.

3.3. IPV4

$\leftarrow 32 \rightarrow$						
Version	IHL	DSCP	ECN	Total Length		
Identification			Flags	Fragment Offset		
Time to Live		Protocol		Header Checksum		
Source IP Address						
Destination IP Address						
Options (if IHL > 5)						
Data						

TODO: explanations

3.3.1. Network classes (private nets)

Term	Definition
A	10.0.0.0 - 10.255.255.255 (10/8 prefix)
B	172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
C	192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

3.3.2. Subnetting

3.3.2.1. Calculating subnet mask

$$/24 = \underline{1111} \underline{1111} . \underline{1111} \underline{1111} . \underline{1111} \underline{1111} . \underline{0000} \underline{0000} = 255.255.255.0$$

$$/10 = \underline{1111} \underline{1111} . \underline{1100} \underline{0000} . \underline{0000} \underline{0000} . \underline{0000} \underline{0000} = 255.192.0.0$$

3.3.2.2. Calculating increment

Address increment = $\frac{\text{amount of addresses}}{256}$ or $2^{8-(\text{mask mod } 8)}$

Let there be 4 subsequent networks starting with 10.0.0.0, each being /20

$$\text{Amount of addresses} = 2^{32-20} = 2^{12} = 4096. \text{ Increment} = \frac{4096}{256} = 16$$

$$\text{Alternatively: } 2^{8-(20 \bmod 8)} = 2^{8-4} = 2^4 = 16$$

$$\text{Networks} = 10.0.0.0/20, 10.0.\mathbf{16}.0/20, 10.0.\mathbf{32}.0/20, 10.0.\mathbf{48}.0/20$$

3.4. ROUTING

– routing table

3.4.1. Data plane

- local, per-router function
- determines how datagram arriving on router input port is forwarded to router output port

3.4.2. Control plane

- network-wide logic
- determines how datagram is routed among routers along end-to-end path from source to destination host

3.4.3. Dynamic

TODO

3.4.3.1. Dijkstra's algorithm (Link State)

3.4.3.2. OSPF (Open Shortest Path First) (Distance vector)

3.4.3.3. BGP (Border Gateway Protocol)

3.4.4. Fragmentation

- offset = transferred bytes / 8

4. DATA LINK LAYER (2)

TODO

Functions:

- error detection
- flow control
- addressing
- layer 2 packets change after each intermediary node (switch/router)
- switching
 - switch table
 - flooding
 - learning
- vlans
 - frame format

4.1. ETHERNET

Ethernet specifies and implements encoding and decoding schemes that enable frame bits to be carried as signals across both copper and fiber cables. Ethernet separates the functions of the data link layer into two sublayers: Logical Link Control and Media Access Control.

<i>Logical Link Control (LLC)</i>	<i>Media Access Control (MAC)</i>
Handles communication between the network layer and the MAC sublayer. Provides a way to identify the protocol that is passed from the data link layer to the network layer.	Data encapsulation: Includes frame assembly before transmission, frame parsing upon reception of a frame, data link layer MAC addressing and error detection. Media Access Control: Ethernet is a shared media and all devices can transmit at any time.

4.1.1. Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Defines how the Ethernet logical bus is accessed. It is in effect within a collision domain and if a device's network interface card (NIC) is operating in half-duplex mode. It helps prevent collisions and defines how to act when a collision does occur.

- **Carrier Sense:** Listen to the medium

- **Multiple Access**: Sending if medium is free, else waiting for a random time and try again
- **Collision**: The amplitude of the signal increases because a collision occurs.
- **Collision Detection / Backoff algorithm**: The nodes stop transmitting for a random period of time, which is different for each device.

After 16 tries, the host gives up the transmission attempt and discards the frame. The network is overloaded or broken.

4.1.1.1. Collision domain

TODO

4.1.1.2. What happens when a collision occurs?

- A jam signal informs all devices that a collision occurred.
- The collision invokes a random backoff algorithm.
- Each device on the Ethernet segment stops transmitting until their backoff timers expire.
- All hosts have equal priority to transmit after the timers have expired.

4.1.2. Half-duplex vs Full-duplex

Full-duplex requires point-to-point connection where only two nodes are present. The data is sent on a different set of wires than the received data, so no collisions will occur. When a NIC detects that it can operate in full-duplex mode, CSMA/CD is disabled. Half-duplex needs CSMA/CD for collision detection.

4.1.3. Ethernet II Frame

explanations

64B (1518 Bytes)

DA 6B	SA 6B	Type 2B	DATA (MAC SDU) 0 (+64 padding) ... 1500B	FCS 4B
-------	-------	---------	--	--------

Most common type in use today. Also called the DIX frame.

MAC PDU must be at least 64B to guarantee that all collisions can be detected. If it's smaller, the frame must be filled with Padding Bytes.

4.1.4. IEEE 802.3 Frame

64B (1518 Bytes)

DA 6B	SA 6B	Length 2B	LLC 802.2	LLC SDU	FCS 4B
-------	-------	-----------	-----------	---------	--------

4.1.5. Frame Check Sequence (FCS)

- The sender applies a math formula to the frame before sending it, storing the result in the FCS field.
- The receiver applies the same math formula to the received frame and compares with the sender's result.
- If the results are the same, the frame did not change. If the results are different, an error occurred, and the receiver discards the frame. The Ethernet device does not attempt to recover the lost frame.

4.2. MAC-ADDRESS

explanations

← 48 →	
Organizationally Unique Identifier (OUI)	NIC specific

Used for identifying interfaces.

7th bit: Globally unique (0) or locally administered (1)

8th bit: Unicast (0) or multicast (1)

4.3. ADDRESS RESOLUTION PROTOCOL (ARP)

shorten

Maps network addresses to data link layer addresses / resolves IPv4 addresses to MAC addresses. Entries in the ARP table are time stamped and can time out.

Entries are added by monitoring the traffic and adding source IP and MAC addresses of the incoming packets to the table. If no entry is found inside of the ARP table, then the node launches an ARP discovery process by sending an ARP broadcast request and receiving an ARP reply from the requested MAC addresses' host. When a node receives a packet with a destination IP address where no cached entry for the MAC address can be found, the encapsulation of the IPv4 packet fails and the packet gets dropped.

IPv6 does not need ARP because it uses the Neighbor Discovery Protocol (NDP).

4.3.1. Discovery

- 1) PC A sends a broadcast: "Who has the IP 10.10.10.30?"
- 2) The ARP Request is flooded
- 3) The PC with the sought IP sends his ARP Reply "I have the IP, here is my MAC Address". This is sent as a unicast because the Switch already knows PC A.
- 4) Now the PC A knows the MAC address of 10.10.10.30 and can send its Packet.

4.3.2. Spoofing

ARP has no validation if the sender of a frame is correct. ARP spoofing, also called ARP poisoning, refers to the method of inserting the wrong MAC address into ARP requests and responses by the node. An attacker can lead sent frames to the wrong destination and has the ability to read the traffic (MITM attack). Configuring static ARP entries is one way to prevent ARP spoofing.

4.4. SWITCH

- All devices connected to the switch ports form a **broadcast domain**
- All ports are full-duplex

4.4.1. Flooding

When a switch gets a data packet, and it did not know the DA, it floods the information to all ports but the one where it received the data. (Unicast flooding)

4.4.2. Filtering

When a switch gets a data packet, and already knows that the DA is on the same port as the SA, it filters the information and does not flood it, because the other switches do not need to know. This reduces traffic.

4.4.3. Forwarding

If the destination MAC address comes from another port within the switch, then the frame is sent to the identified port for transmission.

4.5. VLAN

LAN: all devices in the same broadcast domain

VLAN: Virtual separation of LAN on a switch

Reasons for using VLANs:

- To reduce CPU overhead on each device by reducing the number of devices that receive each broadcast frame
- To reduce security risks by reducing the number of hosts that receive copies of frames that the switches flood (broadcasts, multicasts, and unknown unicasts)
- To improve security for hosts that send sensitive data by keeping those hosts on a separate VLAN

- To create more flexible designs that group users by department, or by groups that work together, instead of by physical location
- To solve problems more quickly, because the failure domain for many problems is the same set of devices as those in the same broadcast domain
- To reduce the workload for the Spanning Tree Protocol (STP) by limiting a VLAN to a single access switch

4.5.1. Trunking

With **trunking**, only a single cable is needed to carry traffic for all VLANs. VLAN trunking works by applying **VLAN tagging**, where the sending switch adds an extra header to each frame before sending it across the trunk link. This trunking header contains a VLAN Identifier (VLAN ID), allowing the receiving switch to determine the VLAN to which each frame belongs. Switch ports that are assigned to a single VLAN and carry traffic for only that VLAN are referred to as **access ports**. Ports that carry traffic for multiple VLANs using VLAN tagging are called **trunk ports**.

4.5.2. 802.1Q

The standard of how to tag an ethernet frame in a trunk is defined in IEEE 802.1Q. 802.1Q inserts an extra 4 byte 802.1Q VLAN header into the original frame's Ethernet header.

4.5.3. Inter-VLAN Routing

4.5.3.1. Attaching a Router

A router can be added to a switch using multiple VLANs. The cable from the switch to the router gets configured as a trunk. The router then can simply perform its usual routing logic between the subnets. This concept is called **Router-on-a-Stick**.

4.5.3.2. Using a Layer 3 Switch

With the use of a switch with layer 3 capabilities, the need for a separate router is omitted, as the switch brings the ability for routing by itself. Routing can be turned on that switch and packets between the VLANs get routed.

4.5.4. Link Aggregation Group (LAG)

Combine a number of physical ports together to one logical port.

4.5.5. Link Aggregation Control Protocol (LACP)

IEEE specification (802.3ad) that also enables several physical ports to be bundled together to form a LAG. LACP enables a switch to negotiate an automatic bundle by sending LACP packets to the peer.

4.5.6. Spanning-Tree Protocol (STP)

[cisco docs](#)

Prevents loops in the network (eg. broadcast).

Term	Definition
Root device	Bridge on the network that serves as a central point in the spanning tree
Root port	Port on each device that provides the most efficient path to the device
Designated port	Lowest path cost when forwarding packets from that LAN to the spanning-tree root
Disabled port	Port is disabled to prevent loops
BPDU	Bridge Protocol Data Unit. Destination address is multicast: 01:80:c2:00:00:00 Types: – Hello / configuration BPDU. Sent by the root bridge – Topology Change Notification (TCN). Sent by a different switch to the root

Term	Definition
CAM table	MAC address table, maps MAC addresses to ports. Entries have an aging limit

4.5.6.1. Procedure

When the bridges in a network are powered up, each bridge functions as the STP root. The bridges send configuration BPDUs and compute the spanning-tree topology.

When a bridge receives a configuration BPDU that contains information superior (lower bridge ID, lower path cost, and so forth), it stores the information for that port. If this BPDU is received on the root port of the bridge, the bridge also forwards it with an updated message to all attached LANs for which it is the designated bridge.

If a bridge receives a configuration BPDU that contains inferior information to that currently stored for that port, it discards the BPDU

4.5.6.2. Determining bridge priority

- 1) Lowest root bridge ID (BID) – Determines the root bridge.
- 2) Lowest cost to the root bridge – Favors the upstream switch with the least cost to root
- 3) Lowest sender bridge ID – Serves as a tiebreaker if multiple upstream switches have equal cost to root
- 4) Lowest sender port ID – Serves as a tiebreaker if a switch has multiple (non-EtherChannel) links to a single upstream switch, where:
 - Bridge ID = priority (4 bits) + locally assigned system ID extension (12 bits) + ID [MAC address] (48 bits); the default bridge priority is 32,768, and
 - Port ID = priority (4 bits) + ID (Interface number) (12 bits); the default port priority is 128.

4.5.6.3. Port states

Term	Definition
Disabled	Administratively disabled for various reasons. Does not participate in STP/PVST operation.
Blocking	After excluding disabled ports, the switch starts all ports in the blocking state. In this state, the port does not accept user frames. It accepts only BPDUs.
Listening	The first transitional state after the blocking state, in which the spanning tree determines that the interface should participate in frame forwarding
Learning	In this state, the switch builds the CAM table entries. The port accepts user frames but does not forward them. From the incoming frames, it learns the MAC addresses of the connected devices. It saves the learned MAC addresses in the CAM table.
Forwarding	Accepts and forwards user frames.

4.5.6.4. Topology change

TODO:

4.5.7. Rapid Spanning Tree Protocol (RSTP)

RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to accomplish this. While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within $3 \times \text{hello times}$ (default: 3×2 seconds) or within a few milliseconds of a physical link failure.

4.6. ERROR DETECTION

TODO: EDC

4.6.1. Cyclic Redundancy Check (CRC)

- D: data bits
- G: bit pattern

4.7. WIRELESS

- Different MAC address
- Hidden node problem
 - RTC/CTS
- RA, TA, DA, SA, BSSID + To/From DS
- (Fast) roaming
- Management features
 - Beacon
 - Probe Request / Response
 - ...
 - Association / Reassociation
- Handoff-Thresholds

4.7.1. Channel bonding

Two or more adjacent channels within a given frequency band are combined to increase throughput between two or more wireless devices.

4.7.2. Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)

In wireless, it is also possible to have collisions, because it is a shared medium.

- Client sends an RTS (request to send) “Can I send for xy time?”
- Access point answers with a CTS (clear to send), which all

connected devices get. “Access Point XY is now sending for xy amount of time (minus the time for the RTS)”

- Transmission

4.7.2.1. Hidden node

It is not possible to use CSMA/CD because we do not know if everyone receives everything. If there is a wall between two clients for example, the clients do not know if the other is sending at the same time.

4.7.2.2. Distributed Coordination Function (DCF)

Function which creates the backoff time for CSMA/CA. CTS, ACK and Block ACK (SIFS) have the highest priority and the shortest backoff time. PIFS have a middle priority and DIFS the lowest.

4.7.2.3. Network Allocation Vector (NAV)

Listening Stations can mark the medium as busy with the Network Allocation Vector (NAV), while another station is sending.

4.7.3. Frame

TODO: frame

4.7.4. Management features

4.7.4.1. Beacon

Term	Definition
BSSID	Every AP has a unique BSSID
ESSID / SSID	Every WLAN has an ESSID. Isn't unique.

Is needed to know which BSSIDs are available. All Access Points (AP) send beacons to advertise their BSSID.

4.7.4.2. Association / Reassociation

How does a client connect to an AP?

- 1) Client sends Probe
- 2) AP Sends Probe Response

- 3) Client selects best AP
- 4) Client sends auth request to selected AP
- 5) AP confirms authentication and registers client
- 6) Client sends association request to selected AP
- 7) AP confirms association and registers client

4.7.5. Roaming

Switching to another AP with better signal strength. A client is connected to an AP. If there is an AP that is at least say 10dB better and the signal strength of the current AP is below a limit of say 75dB (handoff threshold), a handover occurs.

- 1) Station sends probe
- 2) AP sends Probe response
- 3) Client selects best AP
- 4) Client sends a reassociation request to the new AP
- 5) New AP sends a reassociation response
- 6) Client sends a disassociation request to the old AP
- 7) The old AP sends the unacknowledged data to the new AP, using the inter Access Point Protocol (802.11f)

Roaming usually takes (too much) time because of the many steps listed above. There are ways to improve roaming, for example with direct handover from AP to AP without re-authentication (802.11r).

5. PHYSICAL LAYER (1)

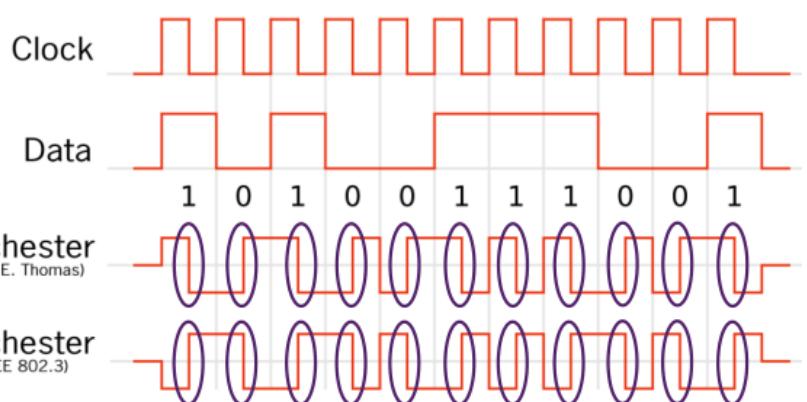
- responsibilities
 - Representing bits as physical signals (electrical voltage, light pulses, radio waves)
 - Defining cables, connectors, modulation methods, and wireless frequencies
 - Synchronization of transmitter and receiver
 - Data rates and physical medium characteristics
- Wi-Fi
- synchronisation,clock rates
- copper,fiber,wireless
- signal degradation,distance,interference
- signal bits (start-bit,data-bits,parity-bit,stop-bit)
- 10/100BASE-TX transceiver components
- single-in,single-out / multiple-input,multiple-output

5.1. ENCODINGS

Encoding converts the stream of bits into a format recognizable by the next device in the network path.

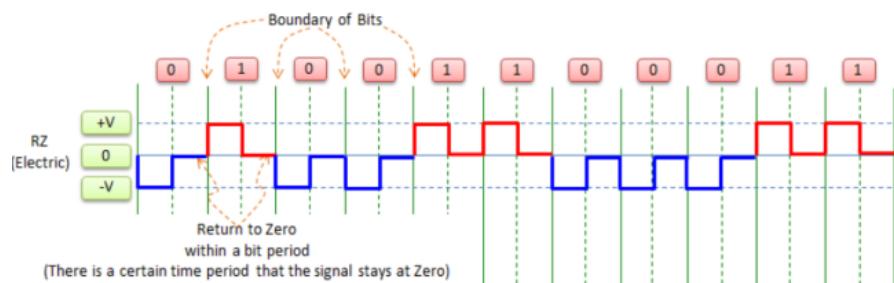
5.1.1. Manchester encoding

- Self-clocking
- 1 = Falling
- 0 = Rising
- Requires twice as much bandwidth as binary encoding



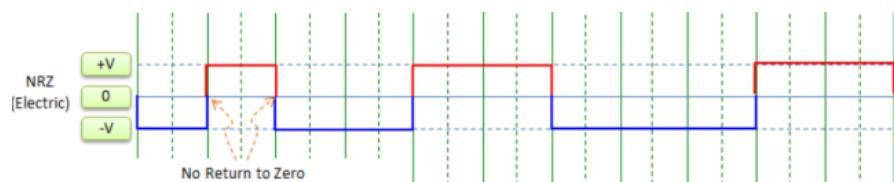
5.1.2. RZ (Return-to-Zero)

- Self-clocking
- Refinement of NRZ



5.1.3. NRZ (Non-Return-to-Zero)

- Not self-clocking



5.1.4. 8b/10b (Clock recovery)

Maps 8-bit words to 10-bit symbols – prevents too many zeros or ones in a row (relevant for NRZ).

5.2. POWER AND DB

Term	Definition
dB	decibel
dBm	decibel ratio to 1mW
dBi	antenna gain compared to isotropic radiator
RSSI	Received signal strength indication
SNR	Signal to Noise Ratio
Receiver Sensitivity	up to which level signals can be received successfully

$$\text{decibels} = 10 \cdot \log_{10}(\text{milliwatts})$$

$$\text{milliwatts} = 10^{\frac{\text{decibels}}{10}}$$

5.2.1. Law of 3s

- A value of 3 dB means that the power value of interest is double the reference value
- A value of -3 dB means the power value of interest is half the reference

5.2.2. Law of 10s

- A value of 10 dB means that the power value of interest is 10 times the reference value
- A value of -10 dB means the power value of interest is 1/10 of the reference

5.3. MODULATION

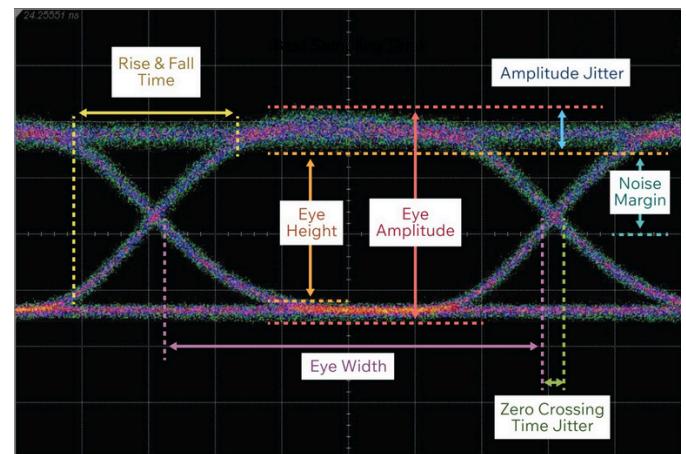
Altering the carrier signal.

5.4. FIBER MEDIA

Single-Mode	Multimode
Very small core	Larger core
Expensive lasers	Less expensive LEDs
Long-distance applications	up to 10Gbps over 500 meters
	LEDs transmit at different angles

5.4.1. Eye Diagram

- An eye diagram results from superimposing the "0"s and "1"s of a high-speed digital data stream.
- An eye diagram shows a relative performance of the signal
- For a good transmission system, the eye opening should be as wide and open as possible
- Horizontal shift is called jitter, which can be caused by imprecise clocks



5.4.2. Attenuation

- Absorption by the fiber material
- Scattering of the light from the fiber

Term	Definition
Microbends	Caused by small distortions of the fiber in manufacturing
Macrobends	Caused by wrapping fiber around a corner with too small a bending radius
Back reflections	Caused by reflections at fiber ends, like connectors
Fiber splices	Caused by poor alignment or dirt
Mechanical connections	Physical gaps between fibers

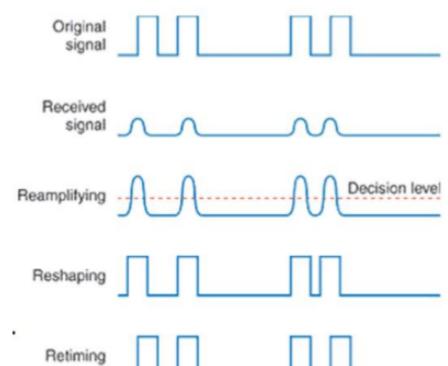
5.4.3. Dispersion

Term	Definition
Chromatic Dispersion	<ul style="list-style-type: none"> - Different wavelengths travel at different speeds - Causes spreading of the light pulse
Polarization Mode Dispersion (PMD)	<ul style="list-style-type: none"> - Single-mode fiber supports two polarization states - Fast and slow axes have different group velocities - Causes spreading of the light pulse

5.4.4. Regeneration

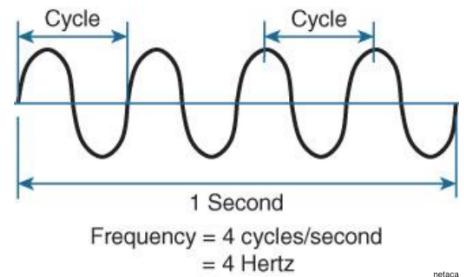
Fixes the dispersion.

Term	Definition
Re-amplifying	Makes the analog signal stronger (i.e. makes the light brighter)
Reshaping	Restores the original pulse shape that is used to distinguish 1's and 0's.
Retiming	Restores the original timing between the pulses. Usually involves an Optical-Electric- Optical (O-E-O) conversion.



5.5. FREQUENCY

Term	Definition
Hertz (Hz)	Number of cycles per second
Bandwidth	Width of frequency space required within the band
Wavelength	Measure of the physical distance that a wave travels over one cycle. Increases as the frequency decreases



5.6. CALCULATIONS

5.6.1. Speed of Signals

In fiber glass, signals travel about 2/3 of the speed of light (200'000km/s).

The Time a Signal needs is calculated as follows:

$$T(s) = \frac{\text{Length of cable (km)}}{\text{Speed of signal (km/s)}}$$

5.6.2. Optical budget

Transmission power - Receiver sensitivity

6. CISCO

6.1. ROUTER SETUP

Router> enable

Router# configure terminal

Router(config)#

6.2. INTERFACES

6.2.1. Static IP Assignment

Router(config)# interface GigabitEthernet 0/0/1

Router(config-if)# ip address 172.16.0.0 255.255.255.252

Router(config-if)# no shutdown

Router(config-if)# exit

6.2.2. DHCP Assignment

Router(config)# interface GigabitEthernet 0/1/1

Router(config-if)# ip address dhcp

Router(config-if)# no shutdown

Router(config-if)# exit

6.2.3. Show

Router(config)# do show ip interface brief

Router# show ip interface brief

Router# show ip interface GigabitEthernet 0/0/1

6.3. VLAN

```
Switch(config)# vlan 120
Switch(config-if)# name vlan-server
Switch(config-if)# exit
```

6.3.1. Assign IP

```
Switch(config)# interface vlan 120
Switch(config-if)# ip address 10.120.0.10 255.255.255.0
```

6.3.2. Access Port

```
Switch(config)# interface GigabitEthernet 0/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 120
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet 0/0/1-5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 120
Switch(config-if)# exit
```

6.3.3. Access Port

```
Switch(config-if)# switchport mode trunk
```

6.3.4. VTP (Virtual Trunk Protocol)

6.3.4.1. Server

```
Switch(config)# vtp domain ins
Switch(config)# vtp mode server
```

6.3.4.2. Client

```
Switch(config)# vtp domain ins
Switch(config)# vtp mode client
```

6.3.5. LACP (Link Aggregation Control Protocol)

```
Switch(config-if)# channel-group 5 mode active
Switch(config-if)# channel-group 5 mode passive
```

6.3.6. Load Balancing

```
Switch(config)# port-channel load-balance <strategy>
```

6.3.7. STP (Spanning Tree Protocol)

6.3.7.1. Bridge priority

```
Switch(config)# spanning-tree vlan 1 priority <priority>
```

6.3.7.2. Interface costs

```
Switch(config-if)# spanning-tree cost 100
```

6.3.7.3. PortFast mode

```
Switch(config-if)# spanning-tree portfast
```

6.3.7.4. Show

```
Switch# show spanning-tree
```

```
Switch# show spanning-tree root
```

6.4. ROUTING

6.4.1. Static

6.4.1.1. IPv4

```
Router(config-if)# ip route <destination_network_id> <subnet_mask>
<next_hop_router> <administrative_distance>?
```

```
Router(config-if)# ip route 10.0.0.0 255.0.0.0 192.168.1.1
```

6.4.1.2. IPv6

```
Router(config-if)# ip route <ipv6_prefix> <outgoing_interface> <next-
hop> <administrative_distance>?
```

```
Router(config-if)# ipv6 route 2001:db8:2103:a::/64
```

```
GigabitEthernet1/0/1 fe80::ba27:ebff:fea8:3e50
```

6.4.2. OSPF

6.4.2.1. IPv4

```
Router(config)# router ospf <process-id>
```

```
Router(config-if)# ip ospf <process-id> area <area-nr>
```

6.4.2.2. IPv6

```
Router(config)# ipv6 router ospf <process-id>
```

```
Router(config-if)# ipv6 ospf <process-id> area <area-nr>
```

6.4.3. Show

```
Router# show ip route
```

```
Router# show ip ospf route
```

6.5. DHCP

6.5.1. Create Pool

```
Router#(config-if) ip dhcp pool DEV
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 1.1.1.1 8.8.8.8
lease 5
domain-name enterprise.com
```

6.5.2. Relay Agent

```
Router(config-if)# ip helper-address 176.16.12.10
```

6.6. NAT

6.6.1. IF Inside

```
Router(config-if)# ip nat inside
```

6.6.2. IF Outside

```
Router(config-if)# ip nat outside
```

6.6.3. ACL (Access Control List)

```
Router(config-if)# access-list 1 permit 192.168.1.0 0.0.0.255
```

6.6.4. PAT (Nat overload)

```
Router(config-if)# ip nat inside source list 1 interface  
GigabitEthernet0/1 overload
```

6.7. IPV6

```
Router(config-if)# ipv6 enable
```

6.7.1. DHCPv6

```
Router(config-if)# ipv6 dhcp client pd MY_PREFIX  
Router(config-if)# ipv6 address autoconfig default
```

6.8. TROUBLESHOOTING

6.8.1. Ping

```
Router# ping <destination-ip> source <interface-name>
```

6.8.2. Traceroute

```
Router# traceroute <destination-ip> source <interface-name> numeric
```

7. BINARY, DECIMAL, HEX

0xA4 6A = 0b1010 0100 0110 1010 = 0d42'090

0x04 B0 = 0b0100 1011 0000 = 0d1'200

0x01 D4 C0 = 0b0001 1101 0100 1100 0000 = 0d120'000