\Network Training -

Wireshark -

What is wireshark -

Wireshark is free and open source software for analyzing packets, capturing packets, and analyzing network protocols. Wireshark is cross platform and works with many network interfaces such as wired, wireless, usb and more and packets can be sniffed from different types of networks such as Ethernet, PPP, IEEE 802.11 and loopback.

Wireshark has an advanced filtering system which can filter by protocol, ip address, mac address, and much more. wireshark works with universal packet formats so even packets that have been captured with other packet sniffing tools can be analyzed with wireshark. Wireshark also can decrypt encrypted conversations if the key is given to it, and can follow conversations so they are easier to analyze. Wireshark also “understands” the encapsulation process, and it shows the header of the packet so it is easier to follow the packet structure as defined in the RFC’s.

What is tcpdump -

tcpdump is also a packet sniffer, it is less sophisticated than wireshark, and it is listening on wired and wireless networks, and “dumps” the content of the headers of the packet into the terminal.

How packet listening works -

Firstly, put the NIC on promiscuous mode, this allows the NIC to listen to packets that are not intended for him on the network.

Secondly create a socket with parameters
socket(AF_PACKET, SOCK_RAW, ETH_P_ALL)
AF_PACKET means that this is a packet socket, and the kernel will copy and transfer each of the packets it is getting to this socket.
SOCK_RAW means that the kernel will not touch and strip any of the headers of the packet which means we get the packet as is, in a “Raw” state
ETH_P_ALL means that the kernel will copy every packet from every protocol under the Ethernet protocol

In windows, the capturing of packets is done with a driver that is in the Npcap lib

What is “Raw Socket” -
Raw socket means that the kernel don’t try to change any of the things that I get and receive, sending data on a raw socket literally makes the NIC to transmit what I sent bit by bit, and when receiving information in this kind of socket the kernel don’t trim any of the headers of the packet.

What is promiscuous mode?
Promiscuous mode, is a mode in the NIC that tells him to stop filtering packets, for example drop packets that don’t have it’s own mac address, and receive all the packets that it gets.

From NIC to PCAP
The packet arrives to the NIC **=>**
Kernel processes the packet **=>**
Because wireshark process has a AF_PACKET socket the packet is copied to it **=>**

The packet is processed by wireshark **=>**
The packet is saved on a temp pcap file by wireshark

PCAP file structure:

The PCAP header, which contains a magic number, format version, the max length for each packet, time zone, time accuracy, and the link layer type, for example wifi or ethernet.
The **Magic Number** is crucial for identifying whether the file is in little-endian or big-endian byte order, and is used for compatibility when reading across different systems.
Then each packet is saved one after the other, then data for each packet and the packet original length and captured length is stored and can be parsed to get the information of each layer based on the header structure.

How wireshark display the packet data:

Wireshark displays the packets as a list of them ordered by timestamp by default, we can click on each individual packet, and see all of its headers, and the data of the packet.

What is BPF (Berkeley packet filter):

This is a kernel level program that allows a user space process to tell the kernel which packets he wants him to transfer to it. for example “tcp port 80” for only http requests. This is very efficient for the kernel because now he needs to copy less packets for this process because he copies only the relevant ones.

Wireshark display filter:

The Wireshark display filter is very different, because the display filter is only for display, as the name suggests. the display filter works on packets that are already captured, and makes the view on these packets more nicely, because we filter and sort by which order we want.

Difference:

Display filter is on packets that are already captured so they are more flexible but make the pcap to be much larger because we capture all the packets, while the BPF is use to capture only specific packets, which can make our pcap much smaller if there a lot of packets that aren’t relevant.

OSI (Open Systems Interconnection) Model -

What is the use of the OSI model:

The use of the OSI model is to provide a conceptual way to standard the internet with protocols. The internet today doesn't follow this model exactly and it follows the TCP/IP model, which is very close, the main use of this model is to troubleshoot internet problems, and understand in which layer they accrue thus isolating the problem so we can check the physical device or protocol the work in that layer and make less unnecessary checks

Layer 1 - Physical Layer:

Purpose

transmit, encode and receive bits that are being transferred on a shared medium between the two or more computers, this layer has hardware like copper and optical cables, switches connectors, and NICs

Provides to next layer

Bit transmission and reception, Signal encoding, a way to send and receive data efficiently.

Challenges

Cables can tear down, Signal decays over distance, Data rate is constrained by the physical medium, Cables are physical materials cost money, Network bandwidth is determined by the weakest link

Solutions

Wireless connection for less cables, repeaters and signal amplifiers are used to increase the distance as well as high quality cables.
Cables are mostly isolated, and for wireless the signal is on a very specific frequency. so it’s more resistant to noise,
High quality cables take the signal longer, and repeaters and amplifiers are used to take the signal further as well as optical fibers.
Sophisticated encoding and better cables and multiplexing
Upgrading equipment, matching gear per use case

Main protocol in this layer

RJ45 ethernet connector, Cat5 & Cat6 cables
IEEE 802.3 which defines transmission rates, cables etc.
IEEE 802.11 which defines wifi network and signal frequency
 USB

Layer 2 - Data link layer:

Purpose

give reliable communication from node to node, giving address to each of the devices (MAC) on the network, and esure error detection and connection for reliable transmission.

Provides to next layer

reliable data transmission, and error checking

Challenges

collisions, frameloss, clock syncing, scalability,

How these problems are solved

CSMA/CD - Because all devices transmit on the same medium, and the communication is half duplex, means only on device can transmit, each devices waits for the medium to be idle, if so, it transmits while listening to it’s own transmit, if the information gets garbled, it detects a collision occurs and waits a random time so not both devices will try to transmit again in the same time.

CSMA/CA - in wireless communication, collisions are more common and more devices, maybe even from a different net can communicate on the same frequency, so devices send RTS/CTS(request to send / clear to send) so collisions are less likely
Switches and full duplex to avoid collisions - switches directly transfer the communication from one device to another, so each devices is it’s own segment which makes much less or even no collisions, and also makes full duplex possible so device can get info in one line and send in another, so communication is much less likely to collide.
clock
Autonegotiation - Ethernet devices may negotiate on parameters such as half or full duplex, speed etc before a connection is done, so there is optimal speed for both devices and no duplex mismatch.
Preamble - preamble is a sequence of bits that are sent before each packet for clock syncing, it is a stream of 1010101… ending in 11 (Start frame delimiter) meaning the header in starting after the 11, also the encoding of the ethernet frames 8b/10b or 64b/66b which makes clock recovery easier.
Interpacket gap - this is an idle state between each packet so clocks have time to recover and prepare for the next packet.

Main protocol in this layer
Ethernet, PPP (point to point protocol)

Layer 3 - Internet Layer -

Purpose

transfer variable length packets, from one network into another from a source host into a destination host via one or more networks.

Provides

Logical network addressing, and a way to message between networks, inter network communication, routers

Challenges

Addressing ->
Same IP configured on two devices, Not enough IP addresses, wrong segmentation on networks
Packet Size ->
Different MTU on different networks
Routing ->
Routing loops, packets take different paths to the same destination so packets don’t arrive in order.

Solutions

Addressing Solutions ->
DHCP gives a computer the needed parameters to communicate inside and out the network such as default gateway, ip address, nameservers etc.
NAT (network address translation) allows private and public ip’s so for example in a house the router may have a public IP but all the devices inside the network will have private ip

(192.168.. 172.16.. 10...) and every time they contact the outside the router actually sends the requests.
IPv6 allows much more addresses (128 bits instead of 32)

MTU Solutions ->
IP fragmentation, when a packet larger than the MTU of the network reaches the router, it may fragment it (depending on the Don’t fragment bit), and thus split it into smaller packets.
Path MTU is an algorithm that finds the max MTU of the route, and then sends the data with this MTU or lets a higher layer in the OSI protocol to handle this.

Routing Solutions ->
Dynamic Routing allows for dynamic paths each time which changes the topology if the network changes and prevents looping.
LAG Protocol allows different flows of packets to take different paths so transmission is more balanced.

Protocols
IPv4, ICMP

Layer 4 - Transport layer

The use of the transport layer is to transfer the data into the appropriate application process.

Provides

Connection oriented communication, Connection establishment and Termination (Session) , Error detection, Send data into a specific process.

Challenges

Reliable delivery on unreliable network
Latency and bandwidth
Congestion control

Solutions

In TCP, there is a slow start which is implemented as handshake, to see that both processes can establish connections, and small amount of data into each other.
TCP and UDP allow for ports, which help us to bring the data into a specific process.
TCP allows retransmission of packets that were lost or arrived with errors.
TCP provides segmentation of larger packets into smaller ones

Protocols

TCP, UDP

Session layer

Purpose

The purpose of the fifth layer is mostly to manage sessions, for example establishing the connection and terminating it, noticing a device is not responding or data isn’t coming although it should, so it restarts the connection etc.
Today it is integrated into the 4th layer for example in tcp.

Provides

provides session management and session stability and syncronization.

Challenges

maintain session session connection
handling multiple sessions in “parallel”
session recovery
Session security (login and logout)

Solutions

- TCP handshake and keep alive for conversation starting and session maintaining.
- Sessions are managed concurrently in the os so many sessions can be established.
- Recovery points so if the connection fails at a checkpoint they will both retransmit a file for example from that checkpoint.
- Login and logout with tokens so for the entire period of the session the user won’t need to identify, only on login.

Protocols

NetBios, RPC, NFS

Presentation layer

Purpose

The purpose of the presentation layer is to prepare the data for the application layer

Provides

Data encryption and decryption, compression and decompression, converting into a common format so data that arrives is easier to handle.

Challenges

multiple formats for text, images etc, do all encryption and compression efficeitly even on low resources so it won’t slow the network.

Solutions

Standart formating like UTF-8 and asscii, efficient hasing like sha256 and encrytion like diffi hellman, and AES, with key with rsa

Protocols

SSL/TLS for encrypted data, standarts like mp3, jpeg, png for data compression, assci and unicode standarts for text.

Application Layer

Purpose

The application layer is the user interface, what the user interacts with and what he sees. It’s the interface between the end user and the application and all the underlying network protocols under it.

Provides

user interface, interface to all the layers before it, a “send” button

Challenges

cross platfrom, and standartization, protocols should be able to send data into computers from different brands with different OS

Security (attacks may abuse the high abstraction for example with sql injection)

latency

session management

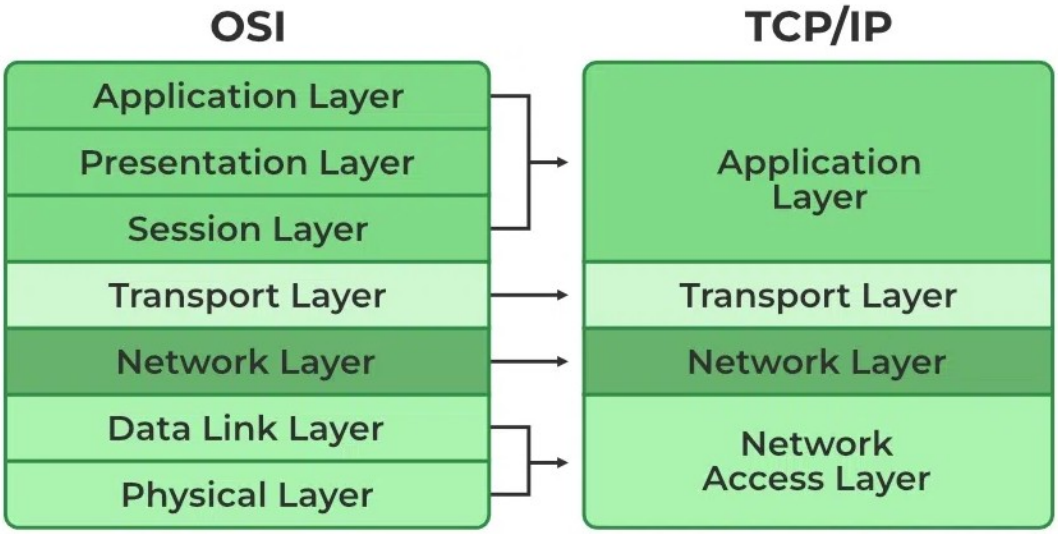
Solutions

- internet is starndart so all major OS and computer companies follow the TCP IP model which allows them all to talk to each other.
- Attacks can be mostly prevented with secure protocols like https, two factor authentication etc
- caching can segnificantly reduce the number of packets sent, and by that reducing latency
- Cookies save session information like user name and password so next time a session start it could automaticlly connect.

What is in use today

Today the osi model is not use, instead we use the TCP/IP model or the “Internet Protocol suite”, the OSI is more of a conceptual way of looking at the internet, with each layer having one main purpose, the TCP/IP model allows each layer

to have more resposibility and all the protocols we use today are based on those responsibilities.



Main protocols are
Ethernet, IPv4/6, TCP/UDP, HTTP
TCP/IP is more simple to understand and has the actual implementation of the idea of the internet as we know it today.

Ethernet Protocol

This is the protocol for wired communication over the internet, it support very large numbers of bit rate, and optical fibers, it started with coexial cables into twisted pair
it provides mac addresses to give devices name on the local network, and has a check for damaged frames so they can be discarded

Fields

Preamble – Signals an Ethernet frame started with 7 bytes of 10101010 repeating

Start frame delimiter – 10101011, Signals the preamble has ended and the frame data starts

Destenation MAC – The MAC address of the receiving device

Source MAC – The MAC address of the sender

Ether type – The protocol that is encapsulated in the Ethernet frame if the number is less then 1500 it is referring to the length of the frame

Payload – The literal data the is being transfered

Frame check - Error detection code, calculation is done before send on the sender and stored here and by the receiver, comparing the code can tell if there was an error and sometimes also how to correct it.

Inter packet gap – pause of the powerline so clocks can sync, data can be processes, and different frames can be destiguished.

Physical Devices

Bridge – Bridge is a device that is ment to connect two seperate networks to each other, transferring only the necessery packets between the networks thus reducing latency and bandwidth usage. The bridge is transperent which means he knows to learn the network and which MAC addresses are in each network, and devices don’t need to do something special to use a bridge, they can just send the packet with a MAC address in the other network. Operates only on OSI layer 2

Hub – A hub is a device that broadcasts every frame it gets in one port into all the other ports, it also knows to detec collisions and most of the times it is combined with repeaters so it needs electricity but can be passive.

Switch – A switch is basically a multiport bridge, which allows multiple networks to connect to each other without them interfearring with each other, switches today are mostly used even for single computers, thus reducing dramatically the collision domain, and allowing full duplex communication. Switches today can be configured with vlans, managed with CLI, web or even through ssh, Switches may also work on OSI layer 3 and even OSI layer 4 and 7.

Bandwidth – Maximum possible data transfer rate
Latency – The time it takes a packet to go from the sender to the receiver.
RTT – The time it takes a packet to go from the sender into the receiver and then from the receiver back into the sender, RTT = Round Trip Time.

Broadcast in data link layer – Broadcasting is sending a packet for all of the network, in the data link layer it is send with the special MAC address of ff:ff:ff:ff:ff:ff which signals broadcast. With IPv4 it is send with a 255 at the end of the mask.

Media Access Control addresses

Mac address is an address that is given to a NIC when it is manufactured. It is a 48 bit address, of 6 octets

The first three octets are for the vendor of the NIC and the other 3 octets are for the ID of the NIC, there can be two addresses just not in the same LAN

Some NICs support in changing their MAC address, but mostly it is not changed

What can we inform from a MAC address

Manufacturer, globly unique or administrated assigned MAC, unicast or multicast MAC

Reserved MAC

ff-ff-ff-ff-ff-ff = Broadcast

01-00-5e-xx-xx-xx = Multicast IPv4

33-33-xx-xx-xx-xx = Multicast IPv6

02-00-xx-xx-xx-xx = localy administrated address

03-00-xx-xx-xx-xx = Reserved for future use of iEEE

00-00-00-00-00-00 = Null Address

00-00-00-00-00-01 = Testing purposes

00-00-0C-xx-xx-xx = Cisco Address

00-10-5A-xx-xx-xx = Intel Address

00-00-0A-xx-xx-xx = Resrved for ISO

Do Exercise on Ethernet.

Internet Protocol – IPv4

Header

Version – The version of the protoco (mostly 4)
Header Length – The length of the header in 32bit jumps (ie 5 20 bytes)
Type Of Service – used for traffic management, and controll flow for example giving priority for certain packets.
Total Length (Payload length) – The length of the payload in bytes
Identification – The identification number of the packet
IP flags – The flags of the packet (don’t fragment and fragment)
Fragment offset – The offset of the fragment if the packet was fragmentef
Time To Live – The number of hops the packet can take, each router decrement this value by 1 when a packet is visting him
Protocol – The protoco encapsulated in the payload (ie tcp=6, udp=17)
Header Checksum – The check sum of the header for error checking
Source Address – The source ip address
Destenation Address – The destenation ip address
IP Options – Options for the

Subnet

a subnet is a logical devision of IP addresses, addresses are devided into classes, A, B and C, each class has a limited number of addresses.

Classes

Class A –

has more then 16 million addresses example network
10.0.0.0 – 10.255.255.255

Class B -

has more then 65K addresses example network
192.168.0.0 – 192.168.255.255

Class C -

has 255 addresses example network
192.168.100.0 – 192.168.100.255

with class subnetting the network can be more organized in terms of addresses and classes of addresses can be sold and used instead of single addresses which at the start of the internet was more useful for companies.

IPv6

IPv6 has much more addresses then IPv4, so every computer can have it’s own public address

There is no need in NAT, which makes less overhead while the router parses the packet

Simplified network configuration, generate self inter network ipv6, and then communicate with the router with it to get global and global temp addresses.

Easier communication with IoT and Phones

Special addresses in IPv4

255.255.255.255, 192.168.1.255 in 192.168.1.0/24

Broadcast address, send to everyone on the net

127.0.0.0/8

Loopback address, send to myself

169.254.0.0/16

device can assign this address to itself if there is not dhcp and it can’t find an address

10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12

Private Networks mostly behind NAT

224.0.0.0/4

This address in used for multicasting

0.0.0.0

Default route, no address has been given for the device unknown target

Fragmentation

fragmentation happens when a packet that is larger then the router can handle is sent, in this case the router will fragment the packet, which means the payload will be devided into multiple packets, all the fragmented packets will have the same identifier, and the fragment offset will increase as the packet is fragmented more. If the don’t fragment flag is on the router won’t try to fragment it, and instead will send an ICMP that he can’t handle the packet.

Fragmentation is not recommended, thus most of the transport later protocols handle the payload size before sending the packet. IPv6 is not supporting fragmentation.

MTU

Max Transmission Unit, this is the max size of a packet, the router, swith or computer can handle at once.

TTL

The number of hops allowed for the packet, each router will decrement this value by one every time a packet is processed by him.

Information from IP address

if it is a private IP we can detect the device role, for example if the address ends in 1 or 254 most of the time it is the router.
a public ip can reveal Geolocation, ISP, network details, if it is a known vpn provider or proxy
it can unable tracking this ip on the net.

TTL

In windows the common TTL is 128 and in linux the common TTL is 64, this is how we can detect os fingerprint in packets, and this is mostly a design choice

Address Resolution Protocol

Packet Stracture

Hardware Type – For example Ethernet with a value of 1
Protocol Type – For example IPv4 with value of 0x0800
Hardware Address Length – For example 6 for MAC
Protocol Address Length – For example 4 for IP
Operation Code – 1 for Request 2 for Reply
Sender Hardware Address – Sender MAC
Sender Protocol Address – Sender IP
Trager Hardware Address – Target MAC, zeros in request
Target Protocol Address – Trager IP

Protocol usage

When a computer want to send data for a computer inside it’s network, it does it with the MAC address , if it doesn’t have the computer MAC address in the cache, but has the computer IP address, the computer can broadcast an arp request, in this request, the computer puts his IP and MAC and the Sender Hardware Address and Sender Protocol Address, and puts the Target Protocol Address as the IP of the computer he wants to get his MAC and the Traget MAC as zeros, then the targeted computer or other computer on the network will send an ARP reply, including the MAC of the wanted computer. After the reply the Requesting computer will save this new entry in his cache.

Static and Dynamic ARP

Static arp is a predefined arp entry in the table that translates and IP into a MAC. Dynamic arp entry is made after the computer asked for a MAC from another computer, and the entry is made temorarly and will delete after some time. Static arp is not deleted (Static with arp -s)

Gratuitious ARP

This is an ARP anouncement of a reply or a request that is telling all the computers of the network a certain IP has a certain MAC and all the computers will update their arp cache because of it, this can be used as arp spoof attack for man in the middle

ARP spoofing

Spamming ARP replys or requests per second~ and thus spoofing all the cache of the computers on the LAN, this can be used for intercepting every packet on the network and also

Protction Against Spoofing

The attack Can’t be prevented because computers should be able to send arp requests and responses periodicly, what we can do is:

Using static entries.
monitoring system to detect in block arp spoofing.
Block arp requests and responses from unknown computers.

Routing

Routing is forwarding a packet of data from one network into another.

Direct vs Indirect

Direct forwarding means that the packet is sent to the same network as the sending computer, on a single ethernet cable with only switches, bridges or hubs, on the other hand indirect delivery means that a router is needed because the packet is on a different network

Forwarding Table

A table that exists on every host and router, this table tells the computer the known routes to certain IP prefixes, and also provides a default route, for packets that their destination is not in the routing table.
Each routing table entry contains the →
IP prefix of the network
The next hop IP address
The interface of the next address (e.g eth0, gig0/1)
The cost of the route
Flags (directly connected, static, dynamic)
Status

The internet backbone routers may have more then 400,000 entries in their tables, and most of the time save the information in binary tree data structure for efficient searching.

Default Gateway

Each forwarding table has some entries in it, if there is no route that matches the packet prefix, the router may send a routing error because he doesn’t know to which interface to send the packet, instead of that, most forwarding tables have a default route or a default gateway that the router sends packets to it, if he doesn’t have other entries to send to.

Most of the time the default gateway will be the router of the ISP or tier 1 or 2 networks which are the backbone of the internet.

How router routes

The router has it’s forwarding table, which is ordered by the largest prefix (largest number), to the smaller prefix at the bottom which is the default gateway, when a router gets a packet, he looks of it’s mask and address and doing AND gate on them, then the router searches it’s routing table for the most matching prefix, then it resolves the MAC address of the device with ARP and sets the destination MAC of the device into this MAC address. Then it sends the packet with the matching interface.

If no entry was found, send routing error message.

How forwarding tables are updated

Path Vector - Each participating node sends his Forwarding Table to all the nodes he knows, the nodes then update the table with simple rules

if the new table has entries I don’t have add them

if the net table has entries more efficient then I have, switch them

Link State - In a link state algorithm, each router checks if the connected routers to him are up or down, and asks them about their connected routers, and then the router creates a map of the network and can calculate the shortest path to each destination

Internet Control Message Protocol

The purpose of the ICMP is to report error and messages to devices on the network and diagnosting internet connection.

ICMP packer header has inside it, the message type, and the code which is just a subtype, the checksum of the header and the message itself
If the ICMP is reporting an error it will have a copy of the problematic packet IP header and first 8 bytes of original datagram's data in it’s data section.

Packet Structure

Type – The type of the error
Code – Subtype, reason for type
Checksum – Checksum on the Header
Message Body – Additional data on the message

Use of ICMP

Error reporting and checking connection and if destination is reachable with ping

Common ICMP types

0 Echo Reply
3 Destination unreachable
5 Redirect Message
8 Echo Request
11 Time exceeded
12 Bad IP header
13 Timestamp Request
14 Timestamp Reply

Ping

Ping utility is an important tool in networking, it sends ICMP echo request and wits for an Echo reply, and it measures the round trip time of the packet, and also if the destination is even reachable

Trace Route

This is another utility that uses ping and the ICMP time exceeded, it sends ICMP echo request with a low TTL, of 1 then 2 etc.. and each router will decrease the TTL by 1 if it is 0 it will send ICMP time exceeded, with the source IP of the router, the algorithm is doing it until it gets echo reply from the wanted IP

User Datagram Protocol

Packet Structure

UDP source port – The port that the sender uses and replies should be send to.
UDP Destination port – The port on the receiver machine that gets the information
UDP message length – The message length
UDP checksum – The checksum on the pseudo IPv4-UDP header and the data.

Another Checksum

In IPv4 the checksum is performed only on the header, while the checksum of UDP is on a pseudo IPv4-UDP header and also the data and that’s why there is another one

What UDP provides

UDP provides ports which allow us to tell the kernel to which process to forward the packet of data, so we can now transfer a packet into a specific application.
The kernel provides each PID a port number, so when sending packets into this port number the kernel knows to which PID to transfer the packet.

Common Applications working on UDP

DNS, DHCPv6, Kerberos, LDAP

Transmission Control Protocol

Packet Structure

Source Port – The source port
Destination Port – The destination port
Sequence Number – A starting random number that tells how much bytes were sent
Acknowledgement Number – A number that tells how much bytes were received
Hlen – The header length
Reserved – Reserved for
Code Bits -
CWR – Reduce Congestion window
ECE – Indication of network congestion
URG – Urgent field is meaningful
ACK - Acknowledgement
SYN – Synchronize sequence numbers
RST – Reset a connection
PSH – Immediate send of data
FIN – Last packet from sender
Window – The max size of the receiving window, the buffer size
Checksum – Checksum on the pseudo TCP-IP header and the payload for error checking
Options – Options on the header like SACK, window scale,
Padding – complete header into 32 bytes (zeros)

Three way handshake

When an application needs to initiate connection, it starts with a Three way handshake in tcp, first sends a packet with the SYN flag and the random seq number, then the receiving application gets responds with SYN and ACK, means it got the

packet and also wants to sync the numbers, and the sender responds with ACK means he got the SYN ACK and data can flow.
Without one of the steps the application can’t know for sure if the other side got the messages and really wants to start connection.

ack and seq
the ack number represents how much bytes were received, and the seq number represents how much bytes were sent.

TCP addtions on UDP
handshake – see if the other side is available before sending data
slow start – start slowly and increase window size gradually
acknowledgement – wait for acknowledgements and retransmit in case of missing ones.

TCP is better for data that must arrive correctly to the application and can’t suffer packet loss and doesn’t need real time performance, like file transferring.

UDP is better for sending data without responsibility into the application, like streaming

TCP data orientation
each packet on tcp has the seq and ack numbers on it so the other side knows where to place it on the stream.

Dynamic Host Configuration Protocol

How the protocol works

Dhcp protocol is ment to configure hosts on a network automaticly, without human interaction.

When a computer is connected into a network, and it support DHCP, the computer sends **DHCP Discover** to see if there is any DHCP server, and it sends it with the wanted parameters, typically Ip address, subnet mask, name server, gateway

After that the server returns a **DHCP Offer** which gives the computer the a server may give couple of offers for addresses, or there might be more then one DHCP servers, thus the client sends a **DHCP Request** with the chosen offer, and then the DHCP servers send him a **DHCP Acknowledgement** which tells the client the IP configuration is ok and it can start using the address.

Can a computer that uses DHCP to obtain an IPv4 address run a server? If so, how does
a client reach the server?

Why it is needed

The protocol is needed because it is hard for network managers to configure every computer with an IP address. It is much error prone to use an automatic configuration approach that the manager only needs to give the server pool of addresses and then configuration happens automatically

Solution to the user not having ip address

Firstly the use sends the discover message is a broad cast with ip of 0 and dst ip of 255.255.255.255 and mac of ff-ff-ff-ff-ff-ff so every computer on the network gets it, then the server knows its MAC address so it can communicate with him directly.

DHCP Relay

this is an agent like computer on each subnet that forwards dhcp requests from the subnet into the dhcp server, this is used in large networks so there can be only one dhcp server in the network and only relays in the subnets

Other flags

DhcpNACK – this is sent from the server to the client if the address the client asked for is already in use and the server can’t give it to him

DhcpDecline – this is sent from the client into the server that the address he offered him is already in use, the client can know this from other means, like arp tables.

Domain Name System

DNS is meant to give an IP address of a server or a host a name, because it is much easier to remember www.youtube.com instead of 142.250.75.142

Hierarchical Naming Scheme

In DNS every domain name is hierarchical, this means that to we go from a root or high level domain into the specific domain we search. So for example the name www.youtube.com, a DNS query is first sent into the root server, to obtain the top level domain .com and then to the domain of youtube, and them obtain the html webpage from www.

Dynamic DNS

Today with DHCP and other dynamic configurations, IP address may change frequently, so if we want to host a web server for example on a network that is behind a NAT or don’t have a global static IP address, we would want to have a single domain name for or website, for that we can obtain a dynamic DNS, this is most of the time software that update periodically the IP in the record

DNS Packet Structure

Transaction ID – The ID of the transaction
Flags ->
QR – Query or Response
Opcode – Type of Query or Response
AA – Authoritative Answer
TC - Truncation
RD – Recursion Desired
RA – Recursion Avilable
Z – Zero reserved
Rcode – Response Code
Question Count – number of queries
Answer Count – Number of answers
Authority Resource Record Count – Number of Authority RR
Additional Resource Record Count - Number of Additional RR

Resource Record Fields – Question
NAME – name of requested
TYPE – type of requested (A, AAAA)
CLASS – class, IN (internet)
Resource Record Fields - Answer
NAME – name of give
TYPE – type of given
CLASS – type of giveb
TTL – time to live in seconds
RDLength – Length of data field
RDATA – Additional Data

Recursive VS Authoritative

In recursive DNS request, the DNS resolver asks the ROOT domain first, then a Top Level Domain and then a sub domain if there is one and only then the domain that actually have the entry, Authoritative request is only made to destination and the servers of the way are discovered with recursive request.

DNS Architecture

ROOT→Top Level Domain→Specific Domain→Ip address

Root servers

There are 13 IP addresses of root nodes, each contains the Top level domains like com, org, il etc..
With the anycast routing, there are thousands of servers that supply the dns service.
Big companies and universities owns these servers and IP addresses, like NASA, Verisign, USC-ISI, University of Maryland and more.

Steps in DNS

The user types a domain name, for example “example.com”
The browser checks in the browser and the os cache for this domain, if it exists there, the user uses the ip there, if not, It makes a recursive request to a dns resolver, the resolver then also checks his cache and if it is not there, he makes an iterative request, which tries its best to return the closet server that has the answer, so root returns com and then another request into com which should have the entry for example, if there were a www so another request into example for www

DNS attacks

DNS Cache poisoning -
In DNS cache poisoning, attackers take advantage that a DNS server isn’t querying every time and instead caches responses so it won’t have to query every time. So when they send to the server a DNS request they very quickly send also a malicious response so the server caches the malicious response and every user that will search for example.com will get the malicious website.
Kaminsky’s DNS Vulnerability -
When a DNS Response is sent, in the authority and the additional section there is the authority that sent the request and the IP additional section.
The vulnerability is that the attacker sends a request for a non existent domain, and then because no other server will respond, the attacker spams responses, and one of them will correlate with the transaction ID of the request, the authority will be a common existing authority like “www.example.com” and the ip in the additional section will be a malicious one, so if this poisons the cache the attacker spoofed the resolver cache, thus can’t redirect people into his ip instead.

Hyper Text Transfer Protocol

hyper text is a text that is displayed on computer screen and most of the time it includes hyperlink which can be triggered by mouse click which references another hyper text.
Uniform Resource Locator
this is a format of addressing to specify protocol, host or domain and a port with a specific file

HTML

Hyper Text Markup Language is the language that most of the web pages are written in, this is a text file with markups that should be rendered by the browser.

Common Client Server

http client can be a browser like firefox or google chrome
http server is the zone that handles get requests and put, and common ones are nginx or apache

HTTP Status codes

1XX – Information response, Request received continuing to process, 100-Continue
2XX – Success, Request processed successfully, 200-OK
3XX – Redirection, Further action needed 303 – See Other
4XX – Client Error, Request contains errors, 404 Not found
5XX – Server Errors, The server failed to to fulfill a valid request 503 service unavilable

Http methods

GET request data from a specific resource
POST send data to a server to update a resource
PUT Idempotent post, this means it won't put the same resource multiple times
HEAD get but without the response body, useful to see what get will return
DELETE remove specific resource
PATCH apply partial modification to a resource
OPTIONS communication option for target resource
CONNECT create a two way communication tunnel
TRACE check if proxies or other devices changing the request on the way

Non text over http

In the content-type section of the header specify image/jpg, video/mp4 etc.

Put vs Post

PUT is idempotent

PUT usually for updating or creating an exact resource at a specific */orders/100*

POST commonly used when client doesn’t know the exact resource and it is up to the server to decide to where the resource is, for example sending into */orders*

How Hebrew can be in the URL

most browsers supports different type of encoding like uft8, and this is automaticly converted into percent encoding

HTTP/1.1 vs HTTP/2

HTTP1.1

Uses multiple TCP connections

Uses text-based protocol where requests and responses are in text format

Has no prioritization

Only responds to client responses

HTTP/2

Uses single TCP connection, all requests and responses are on the same connection.

Uses binary based protocol, implements HPACK header compression, reducing the amount of data transferred, by compressing the header

User Agent

This is commonly includes the software that makes the http request. For example the user browser, operating system and device type. This can help identify which device accessed the network this may indicate malicious bots or scripts

Referrer

this indicates the URL from which the request originated
for example if user is going from page 1 into page 2, the request to page 2 will be in the referrer, lack of referrer can indicate use of automated tools

Access Control allow origin

Tells the browser which domains are permitted to access the resources on the server

Cookie

Sends stored data from the client to the server, this info is most of the time created by the server for reducing repetition, this section can include session_id, theme, language, tokens, cart, tracking information etc.

Content Type

this indicates the type of the resource in the http req or post, this can be an image, text, this can help identify content injection, on where attacker might insert malicious scripts.

Location

header used in http responses for particularly for redirects, and it includes the url for the resource
this can move users into malicious sites.

TLS + Certificates

What is a certificate, how it is used

Certificate is a digital document that a server is sending to a client to prove that he is a legitiment server, the certificate is approved by a 3rd party authority.

The certificate include: Domain name, organization, CA, CA digital signature, associated domains, issue date, expiration date, public key

What is TLS, why it was made

to provide secure connection over the internet

Certificates and TLS

Certificates provide authentication and allow encryption with public and private key, and later a session key

Difference between certificates

The difference is the domain names, and the public encryption and digital signature, most of the time the common things are the CA

Certificate Authority

how to generate certificate

generate rsa key

openssl genrsa -out rootCA.key 4096

generate certificate with the key

openssl req -x509 -new -nodes -key rootCA.key -sha512 -days 3650 -out rootCA.pem

how to validate certificate

Each computer has it’s own certificate authority pre-installed with the OS or the browser, the certificate is self signed by the CA.

When making a request, after tcp handshake, there is a tls handshake

the client hello sends the supported ciphers, and a random string

the server in the server hello sends the the chosen cipher and it’s certificate

when the certificate is sent the client needs to validate it with the signed Authority, at the end it will reach the local CA and will be verified with his public pre installed key, another way is to use OCSP, which sends the CA the wanted certificate and it sends back if it is ok, and signs it with his private key.

Then client and server transfer symetric key with one another, so symetric encryption can be achived