Important Protocols

IpSec

What is IpSec?

RFC 6071(IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap)

IPsec is a protocol that provides a secure tunnel between two computers. It is used to protect data that is transmitted over the internet.

so it is used for encrypted vpn tunneling. VPN tunnel is a logical tunnel. when IPSEc is enabled between 2 routers (and many pcs via switches under routers), the third router acting as MITM

IPsec helps mitigation against:

- eavesdropping
- theft
- replay attacks,
- Data corruption.

Ipsec operates in 2 different modes: tunnel mode and transport mode.

In ***tunnel mode***, everything is encapsulated in IPsec datagram. when data is transmitted, the layer 3 devices only use IPsec header to route the packet.

This is used basically in the site-to-site VPN and remote access VPN.

in ***transport mode***, all of the data is protected but the original IP header is not. Payload is protected by IPsec. This is used generally in P2P applications.

Here’s how IPSec creates a secure VPN tunnel:

- It authenticates data to ensure data packet integrity in transit.
- It encrypts internet traffic over VPN tunnels so data can’t be viewed.
- It protects against data replay attacks which can lead to unauthorized logins.
- It enables secure cryptographic key exchange between computers.
- It offers two security modes: tunnel and transport.

IPSec Protocols and Supporting Components IPSec Core Protocols

- **IPSec Authentication Header (AH)**: This protocol protects the IP addresses of the computers involved in a data exchange to ensure that bits of data are not lost, changed, or damaged during transmission. AH also verifies that the person who sent the data actually sent it, protecting the tunnel from infiltration by unauthorized users.

- **Encapsulating Security Payload (ESP)**: The ESP protocol provides the encryption part of the IPSec, which ensures the confidentiality of data traffic between devices. ESP encrypts the data packets/payload and authenticates the payload and its origin within the IPSec protocol suite. This protocol effectively scrambles internet traffic, so that anyone looking at the tunnel can't see what's there.

And for supporting components:

- **IPsec Security Association (SA)**: This is the key to IPSec. It is used to encrypt and authenticate the data packets. These contracts might define the type of encryption and hashing algorithms to be used. These policies are often flexible, allowing devices to decide how they want to handle things.
- **Internet Key Exchange** : For encryption to work, the computers involved in a private communication exchange need to share encryption keys. IKE allows two computers to securely exchange and share cryptographic keys when establishing a VPN connection.

IPSec provides the following security services:

- Data encryption: The IPsec sender encrypts the packet before transmitting it through the network.
- Data integrity: The IPsec receiver authenticates the packet sent by the sender to ensure that the data has not been tampered with during transmission.
- Data source authentication: IPsec at the receiving end can authenticate whether the sending end of the IPsec message is legal.
- Anti-replay: The IPsec receiver can detect and refuse to receive outdated or duplicate messages.

IPSec mainly uses encryption and verification methods. The authentication mechanism enables the data receiver of IP communication to confirm the true identity of the data sender and whether the data has been tampered with during transmission. The encryption mechanism guarantees the confidentiality of the data by encrypting the data to prevent the data from being eavesdropped during transmission. To provide security services for IP data packets.

The AH protocol provides data source authentication, data integrity verification and anti-message replay functions. It can protect communications from tampering, but it cannot prevent eavesdropping. It is suitable for transmitting non-confidential data. The working principle of AH is to add an identity authentication message header to each data packet, which is inserted behind the standard IP header to provide integrity protection for the data.

The ESP protocol provides encryption, data source authentication, data integrity verification and anti-message replay functions. The working principle of ESP is to add an ESP header to the standard IP header of each data packet, and to append an ESP tail to the data packet. Common encryption algorithms are DES, 3DES, AES, etc.

In actual network communication, you can use these two protocols at the same time or choose to use one of them according to actual security requirements. Both AH and ESP can provide authentication services, but the authentication services provided by AH are stronger than those provided by ESP.

IPsec with DMVPN:

DMVPN --> Dynamic Multicast VPN

DMVPN is not a protocol but a solution. NHRP (Next Hop Resolution Protocol) is used to resolve the next hop address of the destination for multple access points. then Multipoint Generic Routung Encapsulation allows for **single interface to support many IPsec tunnels**, then IPsec is working.

Ipsec building Blocks:

- first building block is **security protocols**

Ipsec Suite either uses **Authentication Header(AH)** or **Encapsulating Security Payload (ESP)**. One difference is that in the former, the data is encrypted.

ESP and AH both come with options of transport and tunnel.

In the AH transport mode, the payload is encrypted and the original IP header is not protected. In the tunnel mode, the payload is encrypted and the original IP header is protected. A new IP header is appointed to the packet in tunnel mode.

ESP transport and Tunnel modes can be used as it is or with AH.

ESP enapsulates the data so we have both header and trailer in the packet in Transport mode and in Tunnel mode.

in ESP header, different than AH header, there is no next header field and payload length field.

- After the headers, second one is **Security Association (SA)**.

Security Association in IPsec suite is a `unidirectional connection` that gives devices the capability to use AH or ESP services. for a bidirectional comms, a pair of SA is needed.

In order SA to be established, the following steps are needed:

- **SPI**: Security Parameter Index. It is a unique number that is used to identify the SA.
- **Security Protocol Identifier**: It is a number that identifies the protocol that is used in the SA. (50 for AH or 51 for ESP)
- **Destination IP Address**
- For third block, **key management**, it is either done manually or automated using IKEv1 or IKEv2.

IKE (Internet Key Exchange) is a protocol that is used to establish a key management between two computers. default one is IKEv2.

- fourth and last building block is **Crypto Algorithm**.

These are used for Encryption , Authentication , Integrity and Pseudorandom Number Generation.

====

for SA estabblishement, there are couple of different protocols that are used.

- ISAKMP (Internet Security Association Key Management Protocol) : Used for procedures and formats to establish SA. It helps us build the SA.
- OAKLEY (One-Way Authentication Key Exchange Protocol) : gives key-exchange mechanissm. Used to exchange key over insecure connection using Diffie-Hellman.
- SKEME (Security Key Exchange Method) :gives anonimity and reputability through key-exchange techniques.
- IKE (Internet Key Exchange) : Uses combination of ISAKMP, OAKLEY, and SKEME

note: sha > md5!!

Ipsec in Enterprise

In enterprise level, there are **2 main uses** of IPsec:

- Site-to-Site VPN

connect 2 or more sites together. One type of Site-to-Site VPN is `DMVPN` (Dynamic Multicast VPN).

`logically` connects sites, protects `entire` network, provides corporate resources to other sites.

- Remote Access VPN

`logically` connect endpoint to another network. IPsec using the OS IP stack. protects `individual` devices.

useful in wifi hotspots.

Bu mesela bir isci evden calisirken isyerinin agina ulassin diye kullanilan vpn. ticari bireysel VPNler de bu tip, hotspotshield, NordVPN gibi.

uses OS IP stack.

as for IPsec implementations, there are **2 main types**:

- GRE over IPSec

way more commen.

encapsulates entire packet including Level 3. this is essentially DMVPN over IPSec.

- IPSec over GRE

much less common. only the payload is protected via IPsec. routing information stays visible in the GRE portion of the datagram.

IKEv2

What is IKE?

IKE is Intrnet Key Exchange that uses ISAKMP, OAKLEY, and SKEME for establishing SA for securing network traffic.

Although IKEv1 is still used, IKEv2 is the new standard and IKEv1 is obsolete.

V2 brought these:

- new authentication method EAP (Extensible Authentication Protocol) alongside PKS and PKI
- brought MOBIKE (Multicast Opportunistic Key Exchange) which allows dynamically change IP adresses without needing to re-establish the SA.
- in V1, SA lifetime was negotiated, in V2, SA lifetime is configured locally and faster negotiation.
- Flexible traffic selection per SA.

Some benefits of IKEv2 are:

remember, in V2, packets do not negotiate, it is V1!

- **It is more reliable:**

message flow system uses **requests followed by responses** so traffic happens in pairs. Initiator sends a request, and the responder sends a response. If the initiator does not receive a response, it will retry or drops the request. the reliability is on the initiator side.

- **It is more Mobile:**

using MOBIKE, keeps VPN conenction active when changing IP addresses. thanks to `multihoming`, when interface drops, the traffic is moved to another interface.

- **it enables `High Availability`:**

IKEv2 comes with `redirection` feature. if one server for VPN is taken down or went down, the users can be redirected to another server.

For authentication, IKEv2 uses `Pre-Shared Key` (PSK) and `Certificate Authentication`. Apart from that uses EAP.

compared to IKEv1 that wants exact parameters must be agreed upon and only one set per SA, IKEv2 allows multiple sets within each SA.

IKEv2 Modes:

- IKE_SA_INIT(phase 1) :
-     - 6 different proposals are sent.
-     - proposals containing algorithms, SA parameters, and keying material are sent to confirm availabile functionality.
-     - first 2 packets.

This phase is responseible for **establishing ISAKMP SA** for the parent SA's. these are used to securely transmist the information to build the child SA.(IPsec SA)

- IKE_AUTH(phase 2) :

- - IPsec Sa's are established.
- - creation of first child SA.
- - Authenticate and validate the pairs.
- - last 2 packets.

This phase is responsible for **establishing IPsec SA's** which are child SAs.

after the 4th packet, all set to go.

IPPSec Analysis and troubleshooting

All Ippsed packets are coming in pair: request and response.

ISAKMP/IKE establish the connection with the first 4 packets. The wireshark protocol is named as `ISAKMP` and first 2 of these 4 packets are `IKE_SA_INIT` (on UDP protocol) and other 2 is `IKE_AUTH`. For these 4 packets there are Initiator SPI and Responder SPIs where SPI stands for **Security Parameter Index**.

SPI is used for directing the traffic to the correct SA.

first 2 packets:

First packet sends initiator SPI with a value. it's responder SPI value is set to 0. also, from the flags we can see whether this packet is initiator or responder and whether this packet is request or response.

also it has a `message ID` which is used for identifying the packet and following the request. Message ID can be also used to detect and fight against replay attacks.

IKE_SA_INIT packets are unencrypted.

==> Since ISAKMP and NAT does not work very well together, we can check the **NAT_DETECTION_SOURCE_IP** and **NAT_DETECTION_DESTINATION_IP** fields in the payloads option.

two packets will send and compare these values, if they are different, then it means that there is a NAT.

last 2 packets:

these are **IKE_AUTH** packets. they have less usefull information than the first 2 packets. We can see the Message ID and some flags, and rest of the data is **encrypted**.

These 2 packets are related to:

- Identity
- Secrets
- Creating the fist child SA

Rest of the traffic is also encrypted.

==> If Identity is not correctly set in the VPN, the traffic can be decrypted and fully qualified traffic notation can be seen. (mesela nereye baglanmak istemis.) these information can be found in the `IKE_AUTH` packets that had to be encrypted!

==> a very important piece of information to look at is **Traffic Selector** field. This field is used to select the traffic that is going to be encrypted. routes the traffic into the VPN or out of the VPN. if not set correctly, there can be unencrypted traffic flooding outside of the VPN.

Traffic selector field holds the following information:

- Traffic Selector Type
- Start port
- End port
- Source IP address
- Destination IP address

==> if ESP is used, the wireshark protocol will be seen as **ESP**. in an ESP packet, we can only see **SPI**(different than IKE SPI) and one **sequence number**.

sequence number is useful to see whether there is a drop or gap in the packet traffic also important to fight against replay attacks. when this number reaches to limit, we re-negotiate a SA.

==> lets say there is 2 pcs are talking. there should be only 2 **ESP SPI** values. if 3, we should be suspecting of a replay attack.

==> What do we need to decrypt IKEv2 packets?

we need initiator and the responder SPI values from the **second** packet which are carried out in plain text.

Second way to get it if we could not capture these packets is to ket **encryption keys** which are only visible during IKE SA creation. A software called **strongswan** can be used to get these keys.

this is only possible if one of the ends of VPN logs them. adding them to wireshark will enable wireshark to show the plaintext traffic.

==> What do we need to decrypt ESP packets?

these ESP packets are the ones that carry the user data hence are more intereting.

- SPIs for both endpoint (clearly visible in the packet)
- encryption and authentication algorithms (clearly visible in the packet)
- IKE SA encryption and authentication keys (**not** visible in the packet) you need to get these using **strongswan**. This is the most difficult part.

==> unencrypted IKE packets capture means there was mismatch in ESP settings and no proposal is selected by the RESPONDER. we need to check the settings and

==

MacSec

Macsec is defined in 802.1AE as `point2point security protocol` providing `data confidentialiity, integrity, and origin authenticity` (all CIA triad.) for traffic over LAyer 1 or Layer 2 links and is part of larger security ecosystem.

Technically, on the transmit side of the link,MAcsec adds `Mac Security Tag` (SecTag, 8 to 16 bytes) and `Integrity Check Value` (ICV, 8 to 16 bytes) to the packet and can optionally encrypt the packet. on the receive side of the link the MacSec engine can identify and decrypt the packet, check integrity, provide `replay protection` and remoce SecTag and ICV. Invalid frames are discarded or monitored.

There is a need to protec data that is transmitted over the in-vehicle ethernet that is connecting `ECU`s together.

Data security protocols like MacSec are often deployed in Ethernet Local Area Networks(LAN) that support `mission critical applications`.

Macsec prt the `IEEE 802.1AE` standard PREVENTS LAYER 2 SECURITY THREATS SUCH AS PASSIVE WIRETAPPING, INTRUSION, MITM, AND REPLAY ATTACKS BY OFFERING LINE-RATE ENCRYPTION AND PROTECTION OF TRAFFIC LASSING OVER LAYER 1 AND/OR LAYER 2 LINKS.

Although it is desirable, it is **not practical to secure the entire network against physical access** by determined attackers. **Macsec allows only authorized systems that attach to and interconnect LANs in a network** to maintain confidentiality and integrity of data and take measures against data theft.

- **Where does Macsec fit within OSI-layer model?**

On the layer 1, there is Automotive Ethernet Physical Layer (AEPL) which is the layer that connects the physical layer of the vehicle to the network. these are like 100baseT, 1000baseT etc.

On the next layer, which is Layer 2, there is IEEE Ethernet MAc + VLAN(802.1Q) + AVB(802.1Qav) + TSN + `MacSec`. Hence, macsec is a layer 2 protocol that is sitting on top of the bare metal.

On the layer 3, there is IPv4 and IPv6 which are protected by `IpSec`. Hence IpSec is a layer 3 protocol.

- **What are some common Security Threats?**

These are some of the common threats against Ethernet Lan:

- - Eavesdropping (compromising routers, links, DNS, or algorithms)
- - Sending arbitrary data including IP headers.
- - Replay attacks.
- - Tampering message in transit.
- - writing malicious code and deceiving people into running it.
- - exploiting bugs in software to take over machines ans use them as base for future attacks.

While IPsec is encryption at Layer 3, MacSec is encryption at Layer 2 which is Ethernet layer.

Remember this : ==> `IEEE 802.1AE`

Compared to IPsec:

- MacSec provides STRONGER ENCRYPTION performance at HIGHER SPEEDS.
- Macsec can encrypt user data at UP TO 800Gig Ethernet Speeds without any hardware offloading.
- Very little latency.
- Application to any network that relies on Ethernet so can be used in many places => so Data Center, Corporate environment, Service Provider, etc.
- Allows to protect all protocols virtually, including layer 2 protocols like AVB TP (IEEE 1722)
- The smallest attack surface on Ethernet-based links for attacks with physical access to a medium

IPSEC and TLS are software based but MacSec is hardware(phy and switches) based. so it makes it more robust and secure!

Packet Structure:

A captured MacSec packet has some options and payloads.

-> **802.1AE Security Tag.**

This Tag has some option flags like VER, ES, E.

E flag is set to 1 if the packet is `encrypted`.

-> **ICV Value**

ICV is a checksum that is used to verify the integrity of the packet.

-> **Port Identifier.**

shows on what port the packet was captured on.

-> **Data**

Data is the encrypted payload. looks like a random hash value.

MacSec Terminology:

1. **MacSec Key Agreement Protocol**

Used to discover Macsec capable peers and used to negotiate encryption keys. These keys are for `data encryption` and `Security Associataion Key Encryption`(SAK)

2. **Connectivity Association (CA)**

Similar to `IPSec SA` but for MacSec. Defines a secure relationship between MacSec peers.

After authentication and key exchange are performed, a secure communication link, called `Secure Channel` is established using Macsec from one node inside CA to another. in MAcSec protected network, each node has at least one `unidirectional secure channel`. The Secure channel does not expire and lasts for the duration of the communication between two nodes. Each secure channel is associated with an `identifier` : the `Secure Channel Identifier` SCI.

Within each secure channel(both transmit and receive), Secure Associations are defined. each Secure association has a corresponding `Secure Association Key` (SAK) and is identified by the Association Number field of the SecTag header. Secure Associations have limited duratuion. this is called Key Rotation.

3. **Connectivity Association Key(CAK) **

Static or Dynamic Key exchanged by macsec speakers. This can be seen as `primary key` that is used to device all other session keys.

So CAK is used to derive SAK keys and this SAK keys are used to encrypt the user data.

So this CAK can be statically confiugred or can be distributed by the server.

4. **Connectivity Association Key Name (CKN) **

Any name that defines a CAK.

5. **Primary and Fallback Keys **

Primary key is used to negotiate an MKA if this fails, Fallback key is used.

6. ** Security Association Keys(SAK)**

Derived from CAK used to encrypt data as mentioned earlier.

Within each Secure Association, `replay protection` can be performetd by checking the Packet Number field of SecTAG header agaisnt the packer number locally stored since ehac macsec packet has a uniqe sequential packet and each packet number can be used only once.

A `Key Server` generates SAK. If you have if you have one switch connected to another switch on ethernet link and MacSec is enabled on this switch, one of these switches will be a Key Server. You can either configure one of these switches as higher priority to make it key server

if you enable MacSec on an interface, it drops all frames except MAcsec encrypted frames. But you can configure macsec profile to allow unprotected traffic in macsec negotiation fails.

Some info on Automotive MKA(MAcSec Key Agreement)

it handles key exhcnage and comparison. in automotive in comparion to regular MKA, the key exhance timeout is reduced from 8 seconds to 30 miliseconds.

===

What is IEEE 802.1X

IEEE 802.1X is a network authentication protocol that opens ports for network access when a user's identity is authenticated it also authorizes them for acess to the network.

IEEE 802.1X is an Port-Based Network Access Control(PNAC) standard that provides protected authentication for secure network access.

an 802.1X network is `different from home networks in one MAJOR way`: it has an authntication server called `RADIUS Server` which checks user's credentials to see if they are an active member of the organization and , depending on the netwrk policies, ggrants them various access rights. This helps unique credential creation for each user, eliminating the reliance on single network password that can be easily cracked or stolen.

the RADIUS server is able to do it in various ways, typically over LDAP or SAML protocol.

What are possible MACsec use cases within Ethernet Network

If a hacker taps into the macsec disabled network, the flowing data can be obtained by hacker and can be used to perform attacks. Hacker can target switches, can tap into the network, or can monitor the device.

if macsec is enabled, tapping or eavesdropping, or replay attacks are not possible since packets are numbered, encrypted. **HOWEVER** hacker CAN disrupt the network using DOS attack if DOS prevention is disabled. in this case, neither hacker nor the vehicle can receive the packets. if DOS prevention is Enabled, the Video stream(i.e.) remains disturbed but DOS does not propogate through the Ethernet phy.

Macsec is cost-effective and could be used in combination with other technologies like IPsec, TLS, etc.

ARP & ArpSec

ARP is unauthenticated, insecure and primarily broadcast protocol.

this kind of broadcasts are stopped either by routers or alike Layer 3 devices on the network.

ARP's only job is to map logical address(IP) to physical address(MAC). Just like building numbers do not help you to figure out how to go to this house, IP addresses do not help you figure out how to traverse the network to reach a destination. Hence, ARP helps this traversing.

==> ARP helps to figure out of **known** IP addresses to **unknown** physical addresses. For this end, physical address should be added into the datagram.

So once IP is resolved to MAc address, Destination MAc is added to the datagram. it is a `MUST`

First checks the memory (Arp cache) to see if the IP address is already known. if not,it dynamically resolves the mac address to the ip address.

**ARP Security **

*ARP broadcast storms

For ARP's working mentality, all the nodes in the system receive some sort of ARP messages and use them in their buffers.

Too much broadcast traffic is called `ARP broadcast storm` and can cause the network to become unstable. If storm becomes very strong, it causes Denial of Service.

This kind of problem also causes memory and processor overloads and sometimes crashing of the machines.

Why do Broadcast storms occur?

- Bad NIC or Pyhical Loop which is a hardware problem.
- `Spanning Tree Protocol`(STP) Loop or Device Misconfiguration , which is a software problem.
- Malicious Attacks.

Using HUB instead of switch is a bad idea for exampple because it is not programmable and not intelligent on protocols and it does not have flood avoidance.

Switches can handle this problem if `Spanning Tree Protocol` is enabled and there is no miscfguration.

how to avoid this or DDOS type of problems?

- **Rate-limiting** the traffic. Depending on the vendor, you can limit broadcast,directly limit ARP, or rate the packet/second, bit/second , percent of bandwidth.

To succesfully handle this, you need to know the baseline, `normal` traffic. There are also dangers of limiting legitimate traffics.

IDPS systems are also good ways to avoid this. they can help baseline setting, localize the source of the problems, can potentially help isolating network issues.

**CAM Table Flood*

Switches dynamically associate the MAC addresses of any attached devices with the port to which they are connected on the switch based on the source MAC addresses of the packets passing into the physical interface. Hence, they `allocate memory and buffer locations` called **content addressable memory (CAM)**.

There is , of course a limit for this listing.

Maximum is 4096 entries. when an attacker connects to this switch, one of the entries is written with his mac address. What happens when the list is full?

in the older switches, whether packet was multicast, unicast, or broadcast, they would flood out all active ports with the packets which turns our switch into a `hub`. this is `MAC table flood attack`.

If switch floods,it can be seen by unauthorized people or potentially can cause Dos.

To mitigate this `Port Security` should be implemented on `per-port` basis on switches. Port Security's primary function is to authenticate and validate decices to physical ports based on MAC address. It can use whitelisting for MAC addresses(this port accepts these MAC addresses)or can check `maximum allowed list entries`. These can be persistent or non-persistent and goes away on each reboot.

Even the attacker learn the whitelisted MAC addresses and spoof it, after trying to flood the switch, Port Security can terminate the port connection and deny attacker from flooding the entire table.

**Arp Poisoning, Blackhole, Spoofing, MITM*

ARP Poisoning is to manipulate the ARP table of the target device to change the MAC-IP binding of the target device to another desirable MAC address.

This is done by spoofing the default gateway. This is done by tricking the clients on the network that the IP address of the default gateway is at the attacker's MAC address. how? keep sending ARP messages to client with tricky message and fill their cache without giving them time to correct it. This way attacker becomes the gateway then the attacker attacks to the real gateway to trick it by changing the clients IP bound to attacker's MAC. From that point on, whenever the real gateway distributes the packets, it is redirected to the attacker.

from this point on, all the client packets are sent to attacker. If attacker does not forward but keep collecting these data this is called `blackhole` because attacker never sends these packets to the intended destination.

Mitigation is through `Port Security`.

Another mitigation is `802.1X` which is a network authentication protocol that opens ports for network access when a user's identity is authenticated it also authorizes them for acess to the network. This is superior to port security.

Another mitigation is `Dynamic ARP Inspection` which is a feature of switches that allows the switch to dynamically inspect the ARP table and determine if the ARP table entry is valid or not.

SSH

secure shell.

Just like HTTP and HTTPS, the protocols SSH and TELNET are also operate in the OSI model's layer 5 which is `session` layer.

In the OSI model, `Appliacation, Presentation, Session and Transport` layers are called `Host` layers while the remaninng `Network, Data Link and Physical` layers are called `Media` layers.

Network Layer ==> routers, Ipv4, Ipv6, ICMP. address assingment, routing between network nodes and control of moving network traffic possible.

Data Layer ==> Once the network is connected in the layer 3, Data Link layer transmits the data. A data frame is a data that holds link layer header.

A data link layer frame has the following parts: Frame Header: It contains the source and the destination addresses of the frame and the control bytes. Payload field: It contains the message to be delivered. Trailer: It contains the error detection and error correction bits.

SSH works in one of 3 ways:

- RSA rhost authentication (rhost and shost, but a bit weakly secured)
- Private-key authentication (cari olan islem bu.)
- Password authentication

Some Quick Notes on DHCP

used for endpoint configuration dynamically. otherwise static configuration would be required for each device in every network.

DHCP used UDP ports 67 and 68. Generally broadcast packets. Address assignment happens in 4 packets:

- Discover
- Offer
- Request
- Ack

It has 3 adress allocation methods:

- Dynamic : most common. address is leased for a fixed amount of time.
- Static : address is assigned by the administrator based on MAC adress. manually done.
- Automatic: Assigns a permanenet IP address using **DORA** method.

Common DHCP Options:

- Option 52 : Message type.
- Option 52: Lease time.
- Option 6 : Domain server
- Option 1: Subnet mask
- Option 3: Router
- Option 150: TFTP server

Network Address Translation (NAT)

Network address translation (NAT) is a method of remapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

Network Address Translation (NAT) is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.

As part of this capability, NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address. NAT offers the dual functions of security and address conservation and is typically implemented in remote-access environments. How does NAT work?

Basically, NAT allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their network.

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of private IP address to a public IP address is required.

TroubleShooting DHCP, UDP, TCP

DHCP Troubleshooting

ports 67 and 68 are used for DHCP.

DHCP problems can be categorized under 2 categories:

- connectivity (comms)
- configuration (Server Config)

==> Make sure Firewall is allowing UDP and broadcast/multicast traffic on the specified port.

==> Check cabling for **loops**

==> Check ACL(Access Control List) on router/switch for **deny** for UDP and/or multicast/broadcasts. In this case ICMP packet on wireshark will say administratively filtered.

==> make sure the **bridge** is set as **DHCP server** so router/switch/pc can obtain IP address.

==> check **DHCP NAK** packet, NAK stands for Negative Acknowledgement. in that case in the DHCP NAK packet, check **Relay Agent IP Address** field. this could mean forgotten DHCP relay config on the router/switch.

TCP Troubleshooting

==> TCP Firewall Issues

- source and destination misconfigured addresses or ports.
- incorrect firewall direction/zone.

Firewalls are direction based which are inbound,outbound, and local. local means traffic destined to firewall.

- incorrect order

==> TCP DNAT Issues

DNAT ==> Destination NAT. also called as **port forwarding**. used for mapping private IP address to public IP address. The most problematic issue is **port assignment**.

==> **TCP MTU(Maximum Transmission Unit) Issues- MSS Issues

==> MTU forces data fragmentations if they exceed the MTU. generally 1500 bytes.

==> MSS is the maximum segment size. MSS shows maximum amount of data that can be sent accross connection. MSS only cares about actual user data it is generally **MTU-40 bytes** , works alongside MTU.

==> Lets say you connected devices and ICMP can send ping but not traffic is happening. (timeout) **How to troubleshoot?**

both servers might be running 1500 mtu but connective devices can support 1300 mtu only. so traffic passes but packets are too large 😃

For better ones, refer to **wireshark.md**

UDP Troubleshooting

Main UDP Issues:

- inccorrect firewall config
- DNS problem
- Service Issues

==> UDP Firewall Issues: it is same as TCP Firewall Issues. but also adds a special caveat. The most common issues are DHCP related issues like blocking port 67 or 68 (DHCP address). Another issue is , **raw sockets bypass** firewall issues.

==> DNS related issues.

DNS operates on both UDP and TCP ports. everything that is 512 bytes or less is sent over UDP. anything larger is sent over TCP. sometimes problem arises thinking it is a UDP issue whereas it is TCP.

==> UDP Service issues:

TCP and UDP rely on services. USP service issues more common. Top 3 services are : **DHCP**, **DNS**, **NTP**.

These things are generally handled manually. if there is UDP problem happening, it is better to check the services are running correctly.

=============||||==========================||||

Transport Layer Protocols

The transport layer is the center of the entire hierarchy of the protocol. Two protocols display the transport layer.

1. UDP
2. TCP

What is UDP? The full form of UDP is User Datagram Protocol. It is a connectionless protocol. UDP is a transport-level end-to-end protocol that adds addresses of transport-level, control of errors in the checksum, and data lengths from the top laying. The UDP protocol packet is called a user datagram. A 16-byte header is shown in the user’s Data Chart below:

What is UDP?

In this, you will see the components such as

Destination Port Address: The address of the request process to receive the message is specified. The address of the destination port is 16-bit.

Checksum: The control is a 16-bit field used to detect errors.

Total Length: This determines the user datagram's total length in bytes. It's an area of 16 bits.

Source Port Address: The application process address that has sent a message is specified. The address of the source port is 16-bit. Examples of services and programs that are UDP are DNS, IP telephony, and DHCP.

Disadvantages of UDP

UDP can notice that there has been an error, but does not indicate which packet has been lost because it does not have an ID or a data sequence number. 3This does not have a sequence or reorder feature and when recording an error, it does not indicate the damaged package. UDP offers critical features required for end-to-end transmission delivery. What is TCP? TCP is also known as Transmission Control Protocol. It is a connection-oriented transport protocol. TCP is a protocol that specifies how network connections can be developed and maintained under which applications can share data. TCP uses the Internet Protocol (IP) to describe how computers transmit data packets to each other. Example of services and programs that uses TCP are HTTP, HTTPS, FTP as well as many computer games.

What is TCP?

Control Bits: Each control area operates independently and individually. The control bit specifies the operation of a segment or serves for certain fields as a validity test.

Acknowledgment Number: The data of other communication devices is acknowledged by a 32-field acknowledgment number. If ACK is set to 1, the sequence number the receiver expects to receive is specified.

Header Length: The TCP header in 32-bit words will be specified. The header is 5 words in minimum size and the header is 15 words in full size. There are also 60 bytes for the TCP header, and 20 bytes for the UDP header.

Source Port Address: It is used in a source machine for specifying the application's address. It's a space of 16 bits.

Sequence Number: A data stream is divided into two or more parts of TCP. The 32-bit number sequence field is the location of the data within an original data stream.

Destination port Address: This is used in a destination machine to identify the address of an application program. It's a field of 16 bits.

Features of TCP Protocol

Multiplexing is a method of accepting and forwarding data on separate computers from various applications to each server. The data is sent to the right device at the receiver's end. It is called demultiplexing. Through using the logical channels known as ports, TCP transmits the packet to the appropriate program.

Full Duplex: TCP offers Full Duplex operation, i.e. simultaneously data flux in both directions. Can TCP have buffers sent and received so that the segments can flow in both directions for full-duplex services? TCP is a protocol that binds. Assume that process A requires the data from process B to be sent and received.

Flow Control: Once TCP receives a data packet, it returns to the sender displaying the number of bytes without exhausting the internal buffer. In ACK, the number of bytes is sent as the highest sequence number, which it can easily obtain. It is also known as the window process

Logical Connections: A logical relation is called the combination of sockets, sequence numbers, and window sizes. The pair of sockets used by sending and receiving processes are used to classify each connection.

Subnetting-Supernetting.

What is Subnetting?

Subnetting is a technique that is used to divide the individual physical network into a smaller size called sub-networks. These sub-networks are called a subnet. An internal address is made up of a combination of the small networks segment and host segment. A subnetwork is designed by accepting the bits from the IP address host portion; then, they are uses to assign a number of small-sized sub-networks in the original network. In the subnetting process, network bits are converted into host bits. Subnetting process is performed to slow down the depletion of the IP addresses. It allows the administrator to divide the single class A, class B and class C into small segments. Subnetting makes use of VLSM (Variable Length Subnet Mask) and FLSM (Fixed Length Subnet Mask). The process of partitioning the IP address space into a subnet of different size is called a Variable Length Subnet Mask. VLSM reduces the wastage of memory. The process of partitioning the IP address space into a subnet of the same size is called a Fixed Length Subnet Mask. Advantages and Disadvantages of Subnetting: Below are some advantages and disadvantage of subnetting:

Advantages:

Subnetting increases the number of allowed hosts in the local area network. Subnetting decreases the volume of broadcast, hence minimize the number of network traffic. Sub networks are easy to maintain and manage. Subnetting increases the flexibility of address. Network security can be readily employed between sub networks rather than employing it in the whole network.

Disadvantages:

The process of subnetting is quite expensive. To perform subnetting process, we need a trained administrator.

What is Supernetting?

Supernetting is the process that is used to combine several sub networks into a single network. Its process is inverse of the subnetting process. In supernetting, mask bits are moved towards the left of the default mask; network bits are converted into hosts bits. Supernetting is also called router summarization and aggregation. It creates a more number of host addresses at the expense of network addresses. The Internet service provider performs the supernetting process to achieve the most efficient IP address allocation.

It uses the CIDR method, i.e. Classless inter-domain routing method, to route the network traffic across the internet. CIDR combines several sub networks and combined them together for routing network traffic. In other words, we can say that CIDR organizes the IP Addresses in the sub networks independent of the value of the Addresses.

Advantages and Disadvantages of Supernetting: Below are some advantages and disadvantage of supernetting:

Advantages:

Supernetting reduces the traffic of the network over the internet. Supernetting increases the speed of routing table lookup. As it is summarized the number of routing information entries into a single entry, the size of the router’s memory table decreased, hence saving the memory space. Provision for the router to isolate the topology changes from the other routers.

Disadvantages:

The combination of blocks should be made in power 2 alternatively; if the three blocks are required, then there must be assigned four blocks. While merging several entries into one, it lacks covering different areas. The whole network must exist in the same class.

TCP-IP Protocols

3. TCP/IP Protocols The TCP/IP based protocols are further classified into the following:

a-Web Protocols

- **HTTP** – It stands for HyperText Transfer Protocol, the format of messages, transmission, and this protocol manages web actions associated at client and server-end. The Worldwide web uses it. It runs on port 80.
- **HTTPS** – It stands for HyperText Transfer Protocol Secure, so it seems to enhance HTTP only. This is used for secure communication; hence whenever you are out of the local host world, then go by this.
- **TLS** – It stands for Transport Layer Security; this is a cryptographic protocol that provides end to end communications security over networks, commonly used in transactions; the security is maintained by forgery prevention, data leak prevention, etc.

- **SSL** – It stands for Secure Sockets Layer, establishes an encrypted link between browser and server, the web server requires an SSL certificate. A public and a private key are created cryptographically.

b-File Transfer Protocols

- **FTP** – File Transfer Protocol is used for file transfer between client and server on a computer network.
- **TFTP** – Trivial File Transfer Protocol is how the client can get a file and put it into a remote host, the nodes that boot from LAN use it.
- **SFTP** – SSH File Transfer Protocol provides a secure connection to transfer files and traverse the file system on local and remote systems.
- **FTPS** – It's a secure File Transfer Protocol; TLS support and SSL are added here; we are not using a secure shell-based protocol.
- **SMB** – Server Message Block, which is used by windows, allows computers within the same network to share files.
- **NFS** – Network File system is a distributed file system used in UNIX generally to access files among computers on the same network.

c-Mail Protocols

- **SMTP** – Simple Mail Transfer Protocol is a push protocol to send an email, Post Office Protocol, or Internet Message Access Protocol, which is used to retrieve those at the receiver side. It is implemented at the application layer.

d-Management Protocols

- **Telnet** – It is used on the internet and LAN for bilateral text communication; it uses a virtual terminal connection.
- **SSH** – It is a secure shell-based remote login from one computer into another computer. Authentication and security can be taken care of too.
- **SNMP** – Simple Network Management Protocol is used for collecting and organizing information about devices in the network and modify the information.

e-Media Protocols

- **RTP** – Real-time transport protocol is used for audio and video communication over the network.
- **RTSP** – Real-time streaming protocol is a protocol for streaming; it establishes media sessions between endpoints.

TCP-IP Basic fundamental

The Basic Fundamental Of Networking Presentation Layer

This layer converts or does the job of translating data such as character encoding like the Unicode or the UTF8, encryption/decryption and data compression between a networking device and a software application. Few examples would be of JSON, XML, HTML, CSS and many more. This Layer is more useful when doing secure transactions such as banking and transferring money to account for the data needs to be encrypted and decrypted on the go. This layer is also responsible for converting formats like the UTF8 to ASCII and similar stuff

The Basic Fundamental Of Networking Session Layer

In Networking, the session layer is responsible for opening, closure, and managing a session for an end-user application. This session can include multiple requests and responses occurring inside the software. If disconnection occurs or if there are any packet losses, the OSI session layer Ip protocol tries to recover the connectivity, and if it fails to do so, then it tries to totally close and opens a new connection. This can either be a full or a half-duplex operation. This layer also handles the combining of packets and sorting in proper order. E.g., when you download something from Bit torrent, you see packets get downloaded, but they are not in a synchronized manner. This session layer then combines packets from different streams and allows them to be properly synchronized.

The Basic Fundamental Of Networking Transport Layer

The transport layer is the one that communicates with the application layer to transfer data to the appropriate hosts. The two most important protocols used almost everywhere at transport layers are the TCP and the UDP protocols Both have their own set of pros and cons and are used as per their requirement. TCP distributes the data received from the application layer into specifically sized chunks of data and then transfers these packets part by part into the network. It first acknowledges the packets it receives, requests acknowledgements for the packets sent, and then sets response timeouts to retransmit any packet if their acknowledgement is not received before the timeout expires. This is the main reason why this is considered a reliable connection since it takes care that every single packet transmitted is received by the opposite host. This protocol is mainly used when downloading and uploading large files since the loss in packets may result in corruption in the uploaded or the downloaded data.

UDP, on the other hand, is much simpler but unreliable than Transmission Control Protocol. In UDP, there is no acknowledgement done for any data sent or received to and from the host. Thus there are high chances of packet drops and leaks. This is the main reason why UDP is not used where quality data transmission is required and thus, is considered unreliable. This type of protocol is mostly used in YouTube or Vimeo when streaming a video since a few packets drops won't hamper the user experience. The Basic Fundamental Of Networking Network Layer This specific layer is alternatively known as the Internet Layer as well. This layer is responsible for routing data over networks, and the IP protocol is used to differentiate between addresses.

The most popular ICMP and the IFMP are used in this layer. The ICMP or Internet Control Message Protocol which is used in the ping command to check whether the host is active or down, is used here. The ICMP is one of the most important protocols of the IP protocol suite. ICMP is also used to send error messages over the network about whether a host is down or is not responding or if it's only available via the wake on Lan feature and similar stuff. The Basic

Fundamental Of Networking Data Link Layer

This layer provides the drivers for different devices present in the Operating system and is alternatively known as the Network Interface Layer. These drivers are of the NIC or the Network Interface Card present in the system. The network cards and their properly configured device drivers are responsible for communicating and transferring data onto networks. Without a network interface card, communication is not possible. This data is transferred either wirelessly via routers and Wi-Fi or via cables like the cross-wired or the RJ-45 cable. The protocols used to transfer data here are the ARP and the PPP, i.e. Point to Point Protocol.

=======

Small note on **duplexing**:

Duplex is a bidirectional communication system that allows both end nodes to send and receive communication data or signals, simultaneously and one at a time. Both nodes have the ability to operate as sender and receiver at the same time, or take turns sending or receiving data.

There are two types of duplex, as follows:

- Full duplex: Sends and receives simultaneously
- Half Duplex: Can send or receive, one path at a time

================DONE=====================================