XC: RESUM IP NETWORKS

IP ADDRESSES: 32 bits (netid / hostid) IPv4 datagram: Version=4, IHL=5, Source/destination 32 bit IPV4 addresses, Protocol=6 means TCP, =17 means UDP, TTL, HEADER CHECKSUM ...
IPv6 similar conceps but 128-bit addresses. "network masks" help define which bits are used to describe the network part and which for the host part.
EXAMPLE: 147.83.2.0/30 mask bits → 255.255.255.252 subnet wasrk (or 0.0.0.3 subnet wildcard).
IP addresses are divided into classes: A (0.0.0.0 ~ 127.255.255.255), B (128.0.0.0 ~ 191.255.255.255), ((192.0.0.0 ~ 223.255.255.255), D (224.0.0.0 ~ 239.255.255.255) and E (240.0.0.0 ~ 255.255.255.255). D class is for multicast addresses and E's IP's are reserved. There are though special addresses:

- netid (xxx), host (all '0'): identifies a network, routing tables.
- netid (xxx), host (all '1'): broadcast in the net xxx.
- both net/host (all '0'): identifies "this host" in "this net". Source address in DHCP.
- both net/host (all '1'): broadcast in "this net". Destination address in DHCP.
- netid (127), host (xxx): host loopback (interprocess communication with TCP/IP).

Private addresses have been reserved for devices not using public addresses: A (1, 10.0.0.0), B (... 16, 172.16.0.0 ~ 172.31.0.0) and C (256, 192.168.0.0 ~ 192.168.255.0).

SUBNETTING: Allows adding bits from the hostid to the netid. Ex: for the ISP the network prefix is 24 bits. For the internal router the network prefix is 26 bits. The 2 extra bits allows 4 "subnetw.".
A mask is used to identify the size of the net+subnet prefix. **EXAMPLE:** 210.50.30.0/24 in 4 subnets?

- subnet s1: subnetid (00), ip. netadd. (210.50.30.0/26), range (210.50.30.0 ~ 210.50.30.63), broad (210.50.30.63), $2^6-2=62$
- subnet s2: subnetid (01), ip. add. (210.50.30.64/26), range (210.50.30.64 ~ 210.50.30.127), broad (210.50.30.127), $2^6-2=62$
- subnet s3: subnetid (10), ip. add. (210.50.30.128/26), range (210.50.30.128 ~ 210.50.30.191), broad (210.50.30.191), $2^6-2=62$
- subnet s4: subnetid (11), ip. addr. (210.50.30.192/26), range (210.50.30.192 ~ 210.50.30.255), broad (210.50.30.255), $2^6-2=62$

To reduce routing tables size we use aggregation: **EXAMPLE:** 200.1.10.0/24, 200.1.11.0/24 → 200.1.10.0/23, summarization: group of subnets summarized to classful range.

ROUTING TABLES: Routing can be direct (the destination is directly connected to an interface) or ... indirect (the datagram is sent to a router). The default route (0.0.0.0/0) is where to send all datagrams with a destination address not present in the R.T.. Datagram delivery protocol:

1. Check if the device itself is the destination:
2. Consult routing tables.
3. Forward the datagram. (if direct send it to the dest. address, if indirect send it to the gateway address).

ARP PROTOCOL: ARP transcates IP addresses to physical addresses (MAC address). Process:

1. If ARP table has the requested address, it is retuned,
2. Otherwise,
   - IP stores the datagram in a temporal buffer.
   - IP initiates a timeout and forwards the next datagram in the transmission queue.
   - If the timeout trissels before resolution, the datagram is removed.
   - If ARP returns the requested address, IP calls the driver with it.

ARP resolution in an ethernet net (broadcost net): A broadcost "ARP request" is sent indicating the IP address. The station having the requested IP address sends a unicast "ARP reply", and stores the requesting address in the ARP table. Upon receiving the answers, the requesting station return the IP call with it. A gratuitous ARP is useful to detect duplicated addresses and to update MAC's after IP change.

IP HEADER: the header checksum helps to detect header errors. TTL if 0, discard. Flags are used in fragmentation, which way occur:

- Router: fragmentation might be needed when two networks with different MTU are connected.
- Host: fragmentation may be needed using UDP. TCP segments are ≤ MTU.

Datagrams are reconstructed at the destination. Fields: packet identifier (16b) identifies fragments from the same datagram, flags (3b), Don't fragment (MTU path discovery) or More Fragments (0 in last fragment), and offset (13b) position of the fragment first byte in the original datagram in 8 byte words.

EXAMPLE: ORIGINAL DATAGRAM = 4464 bytes : 20 header + 4444 PAYLOAD'

FRAGMENT size = $\left\lfloor \frac{1500-20}{8} \right\rfloor = 185$ 8-byte-words (1480 bytes)

1st FRAS.: OFFset=0, M=1. 0 ~ 1479 PAYLOAD bytes.
2nd FIAS: OFFset=185, M=1. 1480 ~ 2959 PAYLOAD bytes.
3rd FIAS: OFFset=370, M=1. 2960 ~ 4439 PAYLOAD bytes.
4th FIAS: OFFset=555, M=0. 4440 ~ 4443 PAYLOAD bytes.

MTU PATH DISCOVERY: USED IN TCP. TCP by defaut chooses the maximum segment size, to avoid headers overhead. The goal is to avoid FRAGMENTATION: the DF flag is =1, SEGMENT size is reduced upon receiving ICMP error message "FRAG. needed but DF flag set".

ICMP Protocol: USED FOR ATTENTION AND ERROR MESSAGES. ARE ENCAPSULATED INTO AN IP DATAGRAM. RUNS ON TOP OF IP (in PARALEL TO TCP AND UDP). NO LOOPS. FORMAT: TYPE/CODE (identifies the message) AND CHECKSUM (is computed used ALL THE MESSAGE). TRIGGERED WHEN AN IP PACKET ENCOUNTERS A PROBLEM (EX: time exceeded or destination UNREACHABLE). ICMP PACKET SENT BACK TO THE SOURCEIP ADDRESS. Source host RECEIVES the ICMP PACKET. COMMON MESSAGES: ECHO REPLY (T/C=0,0), NET UNREACHABLE (T/C=3,0), host UNREACHABLE (T/C=3,1), PROTOCOL UNREACHAULE (T/C=3,2), PORT UNREACHABLE (T/C=3,3), FRAG. NEEDED AND DF bit SET (T/C=3,4), SOURCE QUENCH (T/C=4,0), REDIRCIT FOR NET (T/C=5,0), ECHO REQUEST (T/C=8,0), TIME EXCEEDED / TTL=0 (T/C=11,0).

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP): USED FOR AUTOMATIC NETWORK CONFIGURATION: ASSIGN IP ADDRESS AND MASK, DEFAULT ROUTE, HOSTNAME, DNS DOMAIN, CONFIGURE DNS SERVERS, ETC.... IP ADDRESS CONFIG. CAN BE: DYNAMIC (DURING A LEASING TIME), AUTOMATIC (UNLIMITED LEASING TIME) OR MANUAL (IP ADDRESSES ARE ASSIGNED TO SPECIFIC MAC ADDRESSES. Protocol MESSAGES:

- DHCPDISCOVER: CLIENT broadcasts to locate AVAILABLE SERVERS. source (0.0.0.0), dest (255....), source UDP port (64), dest (67). (CLIENT PORT, SERVER PORT)
- DHCP OFFER: SERVER TO CLIENT IN RESPONSE TO DHCPDISCOVER with OFFER OF CONFIGURATION PARAMETERS.
- DHCP REQUEST: CLIENT'S ANSWER BROADCAST (ALL SERVERS) with identifier OF CHOOSEN SERVER.
- DHCPACK: CHOOSEN SERVERS CONFIRMS THE CONFIGURATION with AN ACK MESSAGE.

NETWORK ADDRESS TRANSLATION (NAT): IN A PRIVATE NETWORK, the host have private ADDRESSES, but these CANNOT ACCESS to the INTERNET, SO when DATAGRAMS LEAVE THE PRIVATE NETWORK, NAT MODIFIES THE PRIVATE SOURCE ADDRESS FOR A PUBLIC ONE, AND WHEN DATAGRAMS RETURN TO THE PRIVATE NETWORK, the CHANGE IS ANNULED. A NAT TABLE IS USED FOR ADDRESS MAPPING. TYPES OF TRANSLATIONS:

- PORT AND ADDRESS TRANSLATION (PAT): THE SAME PUBLIC ADDRESS IS USED FOR MULTIPLE PRIVATE ADDRESSES. EACH NAT TABLE ENTRY HAS THE TUPLE: (private ADDRESS, internal port), (public ADDRESS, external port). So the port is used to undo the change. EACH CONNECTION REQUIRES ONE ENTRY.
- DESTINATION NETWORK ADDRESS TRANSLATION (DNAT): What IF WE WANT EXTENAL CONNECTIONS TO INTERNAL SERVERS? WHEN AN EXTERNAL CLIENT wants to ACCESS to A private NETWORK, first the destination ADDRESS is MODIFIED (so DATAGRAMS CAN ENTER PRIVATE NETWORK) AND WHEN they ARRIVE At the ROUTER, the NAT table has to be configured with the address of the accessible internal servers. The port is not modified. NAT TABLE ENTRIES will have to be static.

THE NAT TABLE ENTRIES CAN BE STATIC (A PUBLIC ADDRESS is ASSOCIATED TO EACH PRIVATE ADDRESS, ONLY THOSE PRIVATE ADDRESSES that have An associated public ADDRESS will be able to ACCESS the private network) OR dynamic (there's a set of public ADDRESSES that willbe assigned dynamically: when a host initiates A connection with internet, AN ENTRY is ADDED with the private ADDRESS AND the newly assigned public ADDRESS. IF A host stops using the entry AFTER some time, the entry is removed AND hosts can connect to that public ADDRESS. We need AS MANY public ADDRESSES AS hosts we want to ALLOW to ACCESS SIMULTANEOUSLY to INTERNET).

ROUTING ALGORITHMS: THEY CAN be static (ADDED MANUALLY OR USING DHCP..., ONCE SETTLED THE VALUE IS NOT CHANGED) OR DYNAMIC (AUTOMATICALLY UPDATE table entries via A ROUTING ALGORITHM).

- ROUTING INFORNATION PROTOCOL (RIP): THE METRIC is the NUMBER OF HOPS needed to REACH the destination. Routers exchange RIP messages every 30 seconds with known destinations AND their metrics. These messages use UDP with src./dst. port = 520. A neighbor is considered down if no RIP messages ARE SEEN DURING 180s. RIP v2 ALLOWS VARIABLE MASKS AND USES the MULTICAST dst. ADDRESS 224.0.0.9 instead of the broadcast. Uses the Algorithm Bellman-Ford.
  - count to infinity: SUPPOSE A NETWORK FORMED with R1 — N2 — R2 — N3 — R3 — N4, should R3 FAIL, R2 will know that N4 distance is 16, but receives from R1 that distance is 3, so think that N4 is ACCESSIBLE through R1, AND then R1 receives R2 AND changes the table AND the distance to N4 to 5, etc....
  - SPLIT HORIZON: TO AVOID the latter error, the messages remove the entries having A gateway in the iface. where the update is sent. So in the example, R1 wouldn't have sent the N4 entry to R2 AND R2 wouldn't have though that N4 was ACCESSIBLE through R1. TRIGGERED UPDATE FORCES THE ROUTER TO SEND UPDATES IF CHANGES.

XC : RESUM IP NETWORKS

ROUTING ALGORITHMS: SPLIT HORIZON with poisoned reverse consists of adding the entries having A gateway with metrics equals to 16 (infinity).

- Open Shortest PATH FIRST (OSPF): USED IN BIGGED AND MORE COMPLEX NETWORKS. Uses LINK STATE protocol: ROUTERS KEEP A DATABASE with the status of the whole network. EACH router manitois their directly connected networks AND the ones FROM their neighbor, AND SEND this information to ALL OSPF routers of the network (LSA: LINK STATE ADVERTISERS). But not ALL DESTINATIONS ARE SENT (RIP), just the directly connected.

LSA special routing is needed; Flooding: send LSA to ALL interFACES but for the source. LSA are encapsulated into IP datagrams with multicast destination address 224.0.0.5 and protocol field = 89. LSA are only sent when changes in the neighborhood occur, or when A LSA request is received. Neighbor routers are monitored using A hello protocol ("hello" messages are sent multicast to ALL OSPF routers periodically, so if A router is down, the neighborst will know it because of the absence of the hello message). OSPF routers mantain A LS database with the information received with LSA. The shortest PATH First ALGORITHM (DIJKSTRA) is used to build optimal routing table entries. The metric is computed taking into account link bitiates, delays, etc...

SECURITY IN IP: there are multiple types of ATTACKS: RECONNAISSANCE (previous to an attack, discover AVAILABLE IP ADDRESSES, AVAILABLE SERVERS AND PORTS, types of OS, versions, etc... and eavesdropping), ACCESS (unauthorized access to an account or service), denial of service (DoS, disables or corrupts networks, systems, etc...) or viruses (worms, trojan horses, ..., malicious software that replicate itself). LUCKLY there are soutions:

- FIREWALLS: System of group of systems that enforces an ACCESS control policy to A network. There ARE MANY FIREWALL TYPES: FROM SIMPLE PACKET FILTERING BASED ON IP/TCP/UDP HEADER RULES, to STATE-FULL CONNECTION TRACKING AND APPLICATION-BASE FILTERING, DEFENSE AGAINST NETWORKS ATTACKS... EN UNA XARXA Hi A ZONE NAMED DMZ (DE-MILITARIZED ZONE) that is where we FIND THE UNIQUE hosts (tipically SERVERS) that WE WANT TO BE ACCESSIBLE FROM THE EXTERIOR. THE FIREWALL BLOCKS THE ACCESS TO DMZ FROM the EXTERIOR, EXCEPT FOR A FEW PORTS OF THE SERVERS.
  - IN the INTERNAL NETWORK WE USE PRIVATE ADDRESSES, SO the FIREWALL USES NAT to ALLOW the hosts to CONNECT TO THE EXTERIOR.
  - ACCESS CONTROL LIST (ACL): the firewall filters tha PACKETS that come FROM the EXTERIOR AND DON'T FULFILL CERTAIN CONDITIONS. ACL is APPLIED both in the ENTRANCE AND THE EXIT.

- VIRTUAL PRIVATE NETWORK (VPN): PROVIDES CONNECTIVITY FOR REMOTE USERS OVER A PUBLIC INFRASTRUCTURE, AS THEY would have OVER A PRIVATE NETWORK. TO ENSURE THE SECURITY, VPN USES THE FOLLOWING TECHNIQUES: AUTHENTICATION (to ALLOW AUTHORIZED USERS), CRYPTOGRAPHY (to avoid eavesdropping) AND TUNNELING (TO ISOLATE REMOTE LINKS FROM THE INTERNET). But there are problems:
  - FRAGMENTATION: FRAGMENTATION INSIDE THE TUNNEL WILL USE THE EXTERNAL HEADER, thus, the exit router of the tunnel may reassemble fragmented DATAGRAMS.
  - ICMP: ICMP messages sent inside the tunnel are ADDRESSED TO THE TUNNEL ENTRY.
  - MTU PATH DISCOVERY MAY FAIL.

TO SOLVE THESE PROBLEMS THE ROUTER ENTRY MAINTAINS A "tunnel state" AND GENERATE ICMP MESSAGES THAT would be GENERATED INSIDE the TUNNEL. Furthermore, the TUNNEL ENTRY MAY FRAGMENT DATAGRAMS, IF NEEDED, BEFORE ENCAPSULATION, to AVOID the exit router having to REASSEMBLE FRAGMENTED DATAGRAMS. TYPES OF TUNNELS:

- IP over IP: TUNNEL with A basic ENCAPSULATION OF AN IP DATAGRAM INSIDE ANOTHER IP DATAGRAM.
- GENERIC ROUTER ENCAPSULATION (GRE): ADDITIONAL HEADER THAT ALLOWS ENCAPSULATION OTHER PROTOCOLS.
- Point-to-Point tunneling protocol (PPTP): ADDS the PPP FUNCTIONALITIES.
- IPsec: The other tunnels are not encripted AND USE OTHER PROTOCOLS that ENCRIPT THE CHANNEL (shh). IPsec pretends to introduce AUTHENTICATION AND ENCRYPTION AND TUNNELING TO IP LAYER.