Network Security

Pengwenlong GU
Associate Professor

Centre d'études et de recherche en informatique et communications (CEDRIC)
CNAM Paris

Mail: gup@cnam.fr
Office: 33.1.9B

09/10/2025

Overview

References

- **Textbook :**
  - Computer Networks (Fifthth edition) de Andrew S. Tanenbaum (online : https://csc-knu.github.io/sys-prog/books/Andrew%20S.%20Tanenbaum%20-%20Computer%20Networks.pdf)
- **Digital Library:**
  - IETF RFC (https://www.rfc-editor.org/search/rfc_search.php)
- **Software:**
  - Wireshark (https://www.wireshark.org/download.html)
  - Cisco Packet Tracer (https://www.netacad.com/fr/cisco-packet-tracer)

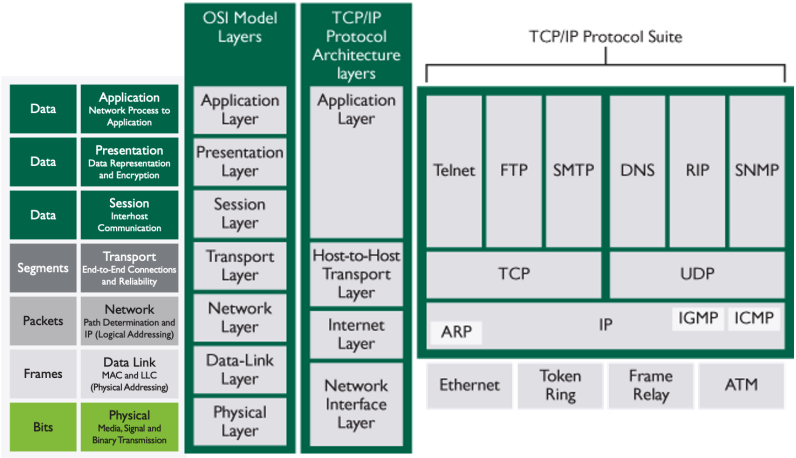
What is a Network?

- A frame or structure composed of elements or points, often referred to as nodes or vertices, related to each other by links or connections, ensuring their interconnection or interaction and whose variations obey certain rules of operation. (Wikipedia)
- Examples :
  - Electrical network
  - Transport network
  - Computer Network
  - Cellular network (4G/5G/6G)

Layered architecture

- ISO (International Standards Organisation)
  - An organisation made up of 171 bodies (Wikipedia)
  - developed the OSI (Open Systems Interconnection) model in 1970.
- The OSI model
  - A layered reference model describing the functions necessary for communication and the organisation of these functions.
  - 4 communication-oriented lower layers.
  - 3 application-oriented upper layers.
- One layer:
  - A homogeneous set intended to accomplish a task or render a service.

OSI and TCP/IP Models



The OSI Model

- The Physical Layer
  - Ensures the physical transport of data in digital or analogue form.
- The MAC layer (Link)
  - Manages shared access to the physical medium and makes it "apparently" weak.
- The network layer
  - Routing packets through the network (finding a path).
- The Transport layer
  - End-to-end message routing (fragmentation, sequence) and application addressing; notion of port (TCP and UDP).

The OSI model

- The Session Layer
  - Macroscopic synchronisation of exchanges, ensuring the consistency of the data exchanged.
- The Presentation layer
  - Authorises a common representation of data (masks heterogeneous encoding, encryption/decryption of data).
- The Application layer
  - Access point to network services.

The TCP/IP model

- Model used on the Internet
- The Network Access Layer
  - A combination of the physical and MAC layers of the OSI model
  - Signal conversion (analogue/digital)
  - Data routing on the link
- The IP layer
  - IP addressing
  - Interconnection of remote (heterogeneous) networks
  - Routing packets independently of each other to their destination

The TCP/IP model

- The Transport Layer
  - It allows paired entities to support a conversation
  - TCP : connection-oriented service : reliable end-to-end transfer
  - UDP : datagram service (same quality as IP, but at level 4, i.e. at the interface)
- The Application layer
  - Integrated protocol functionality (this layer contains all the high-level protocols)
  - No explicit layers 5 and 6 (the presentation and session layers appeared useless)

The TCP/IP model (Composition)

- Internet = gathering of websites (IP)
- An IP site
  - At least one gateway
  - Multiple gateways possible
  - A number of host machines
  - Links between gateway and hosts: free
- Interconnection between sites : Links between gateways
- Gateway role : routing (Gateway=router)

TCP/IP Layer 2 : Ethernet

- Direct physical link between devices
- Physical addressing of interfaces
  - Media access control address (MAC address)
  - MAC addresses are used in many technologies : Ethernet, Bluetooth, Wi-Fi, etc...
- Ethernet frame (IEEE 802.3)

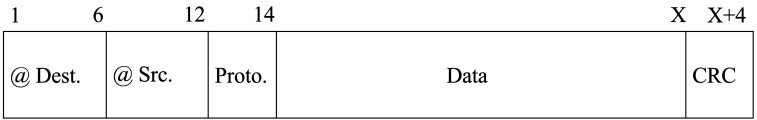
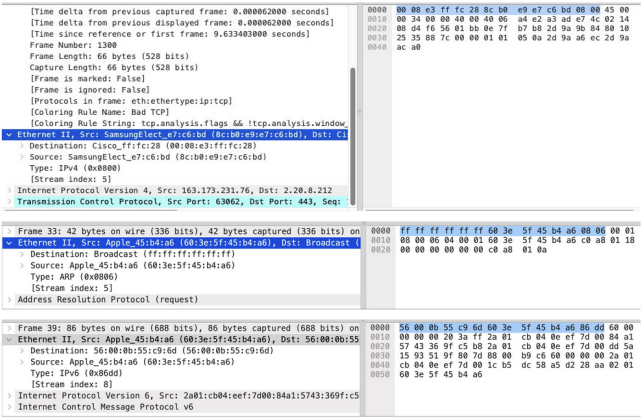


Figure: Ethernet frame ($64 \leqslant X \leqslant 1518$).

TCP/IP Layer 2 : Ethernet

- Traffic analysis

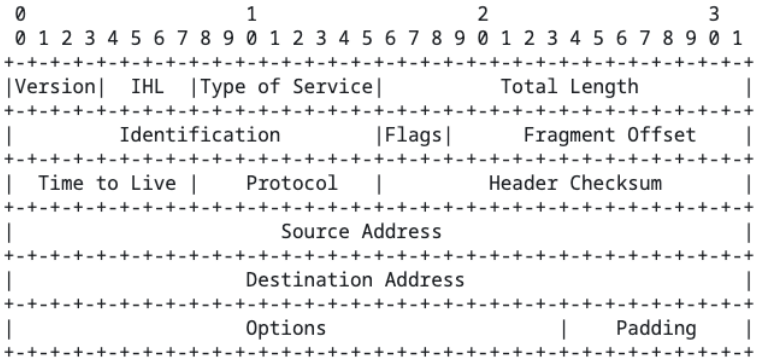


TCP/IP Layer 3 : IP

- IP = Internet Protocol (RFC 791)
- Service : Datagram (Unreliable communication)
- Unique format for data exchanges on the Internet
- Operating mode: Best-Effort
  - Until resources are exhausted (BP, CPU, RAM)
  - No resource reservation
  - Simple and economical solution
  - No guarantee of QoS (Quality of Service)

TCP/IP Layer 3 : IP

- IP packet header [RFC 791]

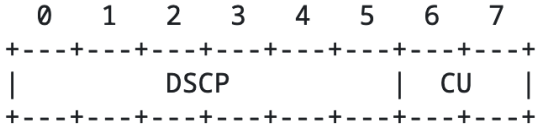


TCP/IP Layer 3 : IP

- 32-bit batch (line) organisation
- The fields :
  - Protocol version: IPv4, IPv6
  - IHL (Header Length): in 32-bit words (Min: 5, Max: 15)
  - TOS (RFC 791)=> (RFC 1349)=> Differentiated Services Code Point (DSCP) (RFC 2474)
  - Total length of the fragment (header + data): 64 Kb max.
  - Identification+Flag+Offset : Fragmentation
  - Time to Live (TTL): processing credit
  - Protocol: Identifies the higher level protocol (1: ICMP, 6: TCP, 17: UDP)
  - Header checksum: error detection
  - Options: optional (variable length) (RFC 1700)

TCP/IP Layer 3 : IP - DSCP

- The DS field structure [RFC 2474]



- Management with the Differentiated Service approach (by class)
- DSCP: differentiated services codepoint (32 service classes)
- CU: currently unused

TCP/IP Layer 3: IP - Fragmentation

- Fragmentation /Restitution :
  - Fragmentation: at the source or in the network
  - Restitution: always at the final receiver

  Transmission Unit (MTU): Maximum size that a link can transit
  - MTU defined per link
  - Ethernet MTU: 1500 bytes, minimum MTU on the Internet >= 576 bytes

- Internet MTU discovery procedure
  - Path MTU Discovery (PMTUD) : ICMP (RFC 1191)
  - Packetization Layer Path MTU Discovery (PLPMTUD): TCP, UDP (RFC 4821, RFC 8899)

TCP/IP Layer 3: IP - Fragmentation

- Identification: Used by the receiver to reconstitute the datagram (the fragments will have the same identification).
- Flags: 3 bits, 2 of which are used: (0, DF, MF)
  - DF: Don't Fragment (no fragmentation)
  - MF: More Fragment (non-terminal fragment)
- Offset: Relative position in the initial packet (Multiple of 8 bytes)
- Example: A packet of 1500 fragmented into 3
  - F1: offset= 0, MF= 1
  - F2: offset= 69= 552/8 (val. Max., because 560+20>576), MF=1
  - F3: offset= 138 (69*2), MF=0 (FIN)

TCP/IP Layer 3: IP - TTL

- Principle :
  - IP: datagram
  - Need to eliminate circular packets (because of the risk of loops in the event of routing problems)
- Initial idea:
  - Limitation expressed in time
  - Less easy to use than a credit
- Current use: routing continuation credit
  - Decrement (by 1) by each intermediate router
  - Destroy packet (by intermediate router) if TTL=0
  - An error message is sent back to the sender

TCP/IP Layer 3: IP - IP addressing

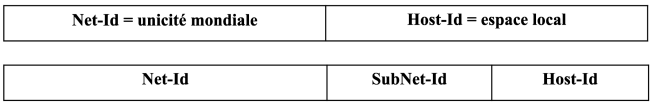
- Format :
  - 4 bytes (32 bits) in A.B.C.D. dotted decimal notation.
  - 163.173.231.76 (Cnam)
- Uniqueness throughout the World
- Contains location information
- Associated with each Network Interface (physical link)
- Consequence: a router (several links by definition) has as many IP addresses as interfaces

TCP/IP Layer 3: IP - IP addressing - Structure

- Principle: division into two parts
  - A first part for global identification (Net-Id)
  - A second part for local identification (Host-Id)
  - Structure: Net-Id (global) + Host-Id (local)
- Example : In 163.173.231.76 :
  - 163.173 refers to the Cnam network,
  - 231.76 refers to a station within this network
- Impact on routing
  - All packets destined for 163.173.x.y go in the same direction.
  - A single entry in the routing table.

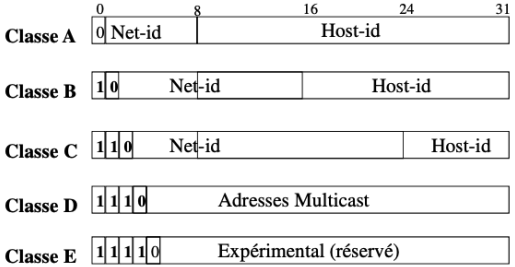
TCP/IP Layer 3: IP - IP addressing - Structure

- Iterative application of the slicing principle :
  - Within a given network, partitioning of the local identification space
  - Structure : Id. Network + [Subnet Id. + Host Id.]
  - Example:
    - the network 163.173.0.0 has a local space of two bytes (64K)
    - Working hypothesis: division into 256 sub-networks
    - Address 163.173.231.76 = Host #76 of subnet # 231
- Why: To facilitate organisation and routing
- Principle applicable iteratively



TCP/IP Layer 3: IP - IP addressing - Classes

- Initial definition :
  - 3 classes of individual addresses
  - 1 class of multicast addresses
  - 1 class (space) reserved



TCP/IP Layer 3: IP - IP addressing - Classes

- Class A :
  - 126 networks in total (127.x.y.z = special use) (From 1.0.0.0 to 126.0.0.0)
  - Examples: 17.0.0.0 (Apple), 18.0.0.0 (MIT)
  - VERY large networks (16 M stations/network)
- Class B :
  - 16382 (2^{14}) networks (From 128.0.0.0 to 191.254.0.0)
  - Examples : 163.173.0.0 (CNAM)
  - Networks of reasonable size: 64 K stations/networks
- Class C :
  - Many networks (2 Millons, 2^{21} - 2 = 2097150) (From 192.0.0.0 to 223.255.254.0)
  - Examples : 192.168.0.0
  - Small network: max. 254 stations

TCP/IP Layer 3: IP - IP addressing - CIDR

- Classless Internet Domain Routing (CIDR) (RFC 1338)
- Abolition of classes (especially class C)
  - Solve the shortage problem
- Notation for the length of the Net-Id
  - Example:163.173.0.0/16
- Rules for allocating contiguous blocks of addresses by geographical location
  - Reduce the number of entries in (large) routers
  - Otherwise two neighbouring networks in the address space can end up on two continents

TCP/IP Layer 3: IP - IP Addressing - Mask

- Need to recognise the Net-Id part (including SubNet-Id) in an address.
- Technique: use of a mask
- Mask: 32-bit binary sequence in which the first N bits are 1 and the remainder 0.
- N: length of Net-Id
  - Notation: network address / N
  - Example: 163.173.0.0 /16
- Mask = always associated with a network
  - M = 1111..... 111 0000
  - Idea: use an AND operation to display only the Net-Id part

TCP/IP Layer 3: IP - Specific addresses

- 127.0.0.1 (in general): loopback, localhost
  - Returned in its own entity
  - Application : test communication software (on the same machine)
- 0.0.0.0: machine without address
  - Diskless station using RARP
  - The default route (route add)
- All machine part bits set to 1: broadcast (Example:163.173.255.255)
- Addresses reserved for private networks (RFC1918)
  - Class A: 10.0.0.0
  - Class B: 172.16.0.0 to 172.32.0.0
  - Class C: 192.168.0.0 to 192.168.254.0

TCP/IP Layer 3: IP - ARP Protocol

- An IP entity = identified by an IP address
  - Internet = a virtual world based on physical links
- Transmission over a physical link
  - Need to identify the corresponding physical receiver
- Need for address resolution
  - Establishes a link between Adrs IP and Adrs Physiqe
- General procedure: correspondence list

TCP/IP Layer 3: IP - ARP Protocol

- Address Resolution Protocol (RFC 826)
- Initially developed for Ethernet
- Purpose: To find a MAC address from an IP address
- Scenario :
  - Two IP stations, A and B, on the same Ethernet segment
  - A wants to send a datagram to B : A knows B's IP address, but not its MAC address.
- ARP process :
  - A broadcasts (DA address = FFFFFF) a claim frame (type of this frame = 0x0806) which contains B's IP address in particular.
  - All machines on the local network receive the request
  - Only B replies to A giving its MAC address

TCP/IP Layer 3: IP - ARP Protocol - Cache

- ARP proceeds by broadcast
  - Cumbersome procedure
  - Additional delay
- Caching matches found by ARP
  - Direct routing table : Command "arp -a"
  - Operationally rather than "responses" received
- Advantage :
  - Less traffic
  - Fewer accesses (therefore less risk of collision)
  - Shorter delay

TCP/IP Layer 3: IP - ARP Protocol - Proxy

- Proxy = Agent = (here) a router
- Scenario :
  - Same as above except that A and B are on two segments
  - B will never be able to reply to the ARP frame
  - The router must reply instead of B
- Consequence
  - The router becomes an agent (proxy) of B
  - It attracts traffic towards B, and, in general, outgoing traffic.
- Potential security problem :
  - ARP takes all responses....

TCP/IP Layer 3: IP - ARP Protocol - Security Issue

- Vulnerability:
  - The machines in a network accept ARP Responses even if they haven't sent an ARP Request
  - The machines trust these ARP Responses without any verification
- ARP spoofing Attack
  - Hackers try to preempt the actual target computer in order to send a reply packet with incorrect information and manipulate the ARP table of the inquiring computer
  - To remain undetected, the intercepted data traffic is usually passed on to the actual target system
  - Then the hacker becomes a man in the middle

TCP/IP Layer 3: IP - RARP Protocol

- Reverse Address Resolution Protocol (RFC903)
- Dual ARP problem
  - Obtaining an IP address
  - Useful for machines with volatile memory.
- Same process as ARP
  - Broadcast a frame (type = 0x8035)
  - Only the RARP server responds with an IP address.
- Successor : Dynamic Host Configuration Protocol (DHCP) (RFC 2131)

TCP/IP Layer 3: IP - ICMP protocol

- ICMP = Internet Control Messages Protocol (RFC 792)
- Encapsulated in an IP datagram (protocol field = 1).
- Signalling protocol
- Used to control the correct operation of the IP protocol
- Two categories of messages
  - Query : Various information (Generated according to needs)
  - Error : Error reporting (Generated when an error is detected)

TCP/IP Layer 3: IP - ICMP Protocol - Examples

- Ping
  - Tests the accessibility of an end-to-end destination.
  - Round trip time measurement
- MTU Discovery
  - A fairly long packet with DF=1
  - ICMP return Tpye=3 Code=4 (fragmentation required) with MTU
- Traceroute (force routers to unmask themselves by sending an ICMP)
  - Loop started with TTL=1
  - Process stops when an ICMP 3/3 is received.

TCP/IP Layer 3: IP - ICMP Protocol - Security Issues

- Ping ICMP flood attack: By inundating a server, router, or network with a flood of requests, a ping ICMP flood DDoS attack can cause the performance of a device to become sluggish or to stop altogether, resulting in a denial of service to legitimate users and traffic.
- Different types of ping flood attacks
  - Targeted local disclosed: This ping flood attack targets a specific computer on a local network, using the specific IP address of the destination device.
  - Router disclosed: This type of attack targets routers to disrupt communications between computers on a network. Attackers must have the internal IP address of the local router or switch.
  - Blind ping: This attack uses an external program to discover the IP address of a target computer router before launching the attack.

TCP/IP Layer 3: IPv6 - Motivations

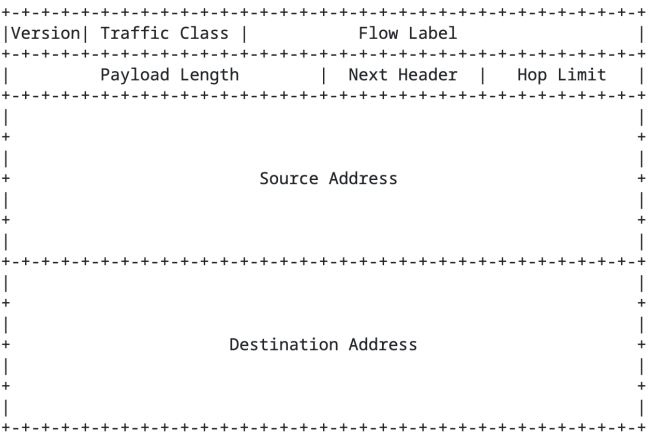
- Change of address format: Address scarcity (Class C)
- Needs: Traffic management with QoS, Mobility, Security
- Simplify the protocol for fast routing
- Potential for extension
  - IPv4 reminder: option = 40 oct
  - Authentication, billing, etc.
- Reduce the size of routing tables

TCP/IP Layer 3: IPv6

- IPv6 = Internet Protocol version 6
- Heir to IPv4
- Specification : RFC2460 (dec. 1998)
- New address format (32 bits $->$ 128 bits)
  - 8 groups of 2 bytes are separated by a colon
  - Example: 1fff:0000:0a88:85a3:0000:0000:ac1f:8001
  - Available addresses : $3,4 \times 10^{38}$
- New features : Quality of Service (QoS), Security, Mobility, etc...

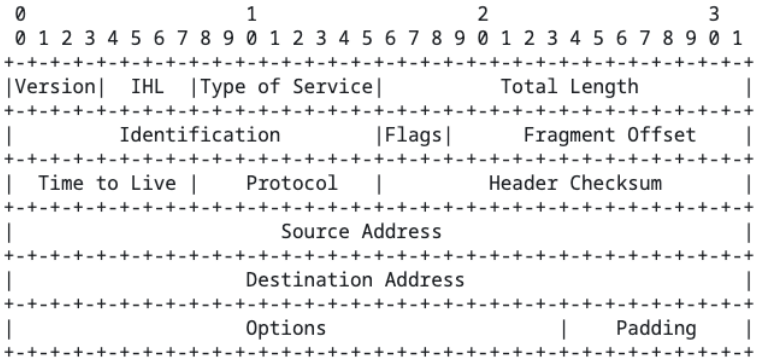
TCP/IP Layer 3: IPv6 - header

- IPv6 header [RFC 2460]



TCP/IP Layer 3: IP (Recall)

- Ipv4 header [RFC 791]



TCP/IP Layer 3: IPv6 - Header

- Traffic Class : priority or traffic classes
- Flow label : marking of packets having the same semantic membership (same application)
- Payload length : Data after header in bytes
- Next header : indicates the next header (protocol) (Reminder: TCP=6, UDP=17, ICMP=1)
- Hop limit: routing credit (-1 per router)

TCP/IP Layer 3: IPv6 - Change

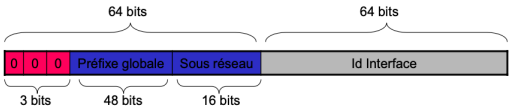
- Deletion
  - Header length : constant size
  - Type of Service : role extended by traffic class and flow label
  - Fragmentation (Identification, Flags, Offset) : forbidden en route
  - Header Checksum
  - Options
- Rename : TTL (Time-To-Live) $->$ Hop Limit (normalisation)
- Modification
  - Datagram length $->$ payload length
  - Protocol $->$ Next Header (extended functionalities)
- New : Traffic class, Flow Label

TCP/IP Layer 3: IPv6 - Addressing

- Specification : RFC 2373, RFC2374
- Consists of two parts:
  - Prefix (for routing)
  - Interface identifier (IID)
- Notation :
  - 8 groups of 16 bits separated by the sign :
  - It is permitted to omit 1 to 3 insignificant zeros in each group of 4 hexadecimal digits.
  - There can only be one occurrence of the sequence " :: " in the notation of an IPv6 address.
  - 1fff:0:a88:85a3::ac1f:8001 = 1fff::a88:85a3:0:0:ac1f:8001

TCP/IP Layer 3: IPv6 - Addressing

- Addressing types :
  - Unicast: 1 Address corresponds to a single machine



  - Multicast: 1 Address corresponds to a group of machines (i.e. unicast addresses)
  - Anycast: 1 Address corresponds to a group of machines but the caller only reaches the closest one in the sense of routing distance.
  - No broadcast

- Special:
  - compatible/mapped IPv4
  - loopback

TCP/IP Layer 4: TCP/UDP

- The transport layer: end-to-end control
- Layer 3 of Internet = IP : datagram
- Need for reliable service : TCP
- Need a datagram service : UDP
- The transport layer :
  - TCP : connection-oriented communications
  - UDP : connectionless communications

TCP/IP Layer 4: TCP/UDP

- Communications identified by port numbers
- Port : interface between the transport layer and the application layer
- An Internet communication is identified entirely by : <source port, source address, protocol, destination port, destination address >
- Some ports are pre-defined - Some examples:
  - 20 : TCP/FTP Data port
  - 21 : TCP/FTP Control port
  - 23 : TCP/Telnet
  - 25 : TCP/SMTP
  - 80 : TCP-UDP/ HTTP
  - 161 : UDP/SNMP

TCP/IP Layer 4: TCP/UDP - Ports

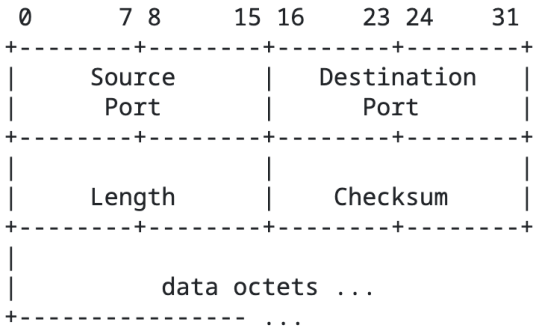
- numbers less than 1023 are reserved for the server side
  - numbers below 255 : reserved for public applications
  - numbers between 255 and 1023 : allocated to companies for marketable applications
- numbers above 1024 are not reserved and are used freely by customers
- For more information see www.iana.org and RFC 1700

TCP/IP Layer 4: TCP/UDP - UDP

- User Data Protocol (RFC 768)
- Service datagram = Unreliable transfer
- Suitable for certain applications which do not have to manage a connection (transactional applications) or applications (multimedia in particular) which have their own logic and reliability managers.
- Examples :
  - Internet name resolution - IP addresses: DNS (because it has to be fast)
  - Network management : SNMP (because it must work in the event of limited network load)
  - Voice over IP (because the transfer time is more important than correcting any errors)

TCP/IP Layer 4: TCP/UDP - UDP Header

- The UDP format is very simple [RFC 768]



TCP/IP Layer 4: TCP/UDP - UDP header

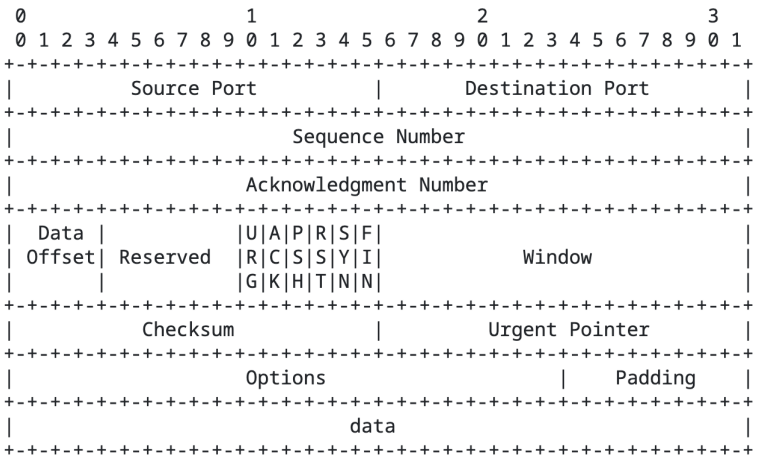
- Source Port: indicates the port from which the packet was sent.
- Destination Port: indicates to which port the packet should be sent
- Length: indicates the total length of the UDP segment (header and data). The minimum length is 8 bytes (header size).
- Checksum: used to ensure the integrity of the received packet when it is not zero. It is calculated over the entire UDP header and data.

TCP/IP Layer 4: TCP/UDP - TCP

- TCP = Transport Control Protocol (RFC 793)
- Connection-oriented service (bidirectional) : guarantees reliable data transfer.
- Connection = flow of bytes (Flows divided into segments)
- Reliability acquired by ACK
- Loss detected by TimeOut
- Flow and congestion control (RFC 2581)

TCP/IP Layer 4: TCP/UDP - TCP Header

- TCP Header [RFC 793]



TCP/IP Layer 4: TCP/UDP - TCP Header

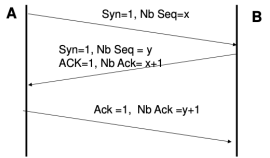
- Source/Dest port : 16 bits each
- Sequence number: Sequence number of the first byte of the segment.
- ACK number: next expected byte
- HLEN: Header size in 32-bit units
- The 6 flags
- Window size : size of the anticipation window
- Checksum : header protection

TCP/IP Layer 4: TCP/UDP - TCP Flags

- SYN=1: connection establishment
- FIN =1: connection release in one direction
- ACK =1: validation of the ACK number
- RST =1: re-synchronisation
- PSH (push) =1: Asks the receiver to hand over the data immediately.
- URG =1: Enables the Urgent Pointer (UP), the receiver must hand over the data up to UP (last byte containing urgent data).

TCP/IP Layer 4: TCP/UDP - TCP Connection

- 3-way handshake



- A sends a 1st segment without data with sequence number = X (randomly chosen)
- B accepts the connection A $->$ B with ACK=1 and ACK number = x+1
- B uses the same segment to establish the connection in direction B $->$ A with a sequence y
- A accepts the connection with ACK=1 and number ACK = y+1

TCP/IP Layer 4: TCP/UDP - TCP Liberation

- 2-step connection direction procedure
- A $->$ B
  - A sends a segment with FIN=1 to close the connection A $->$ B, B replies with an ACK
  - A can then no longer send data to B !
- B $->$ A
  - B performs the same type of operation, the connection B $->$ A is also closed
  - B can no longer send data to A !
- The TCP connection between A and B is then definitively closed.

TCP/IP Layer 4: TCP/UDP - TCP Timeout

- Each time TCP sends a segment it starts a timer
- Timeout
  - TCP assumes that the segment has been lost or corrupted and retransmits it.
  - It is impossible to know a priori how quickly ACKs can be returned to the source.
  - The round trip time (RTT) varies from moment to moment.
- TCP making no assumption about the transit time in the networks traversed
  - it is impossible to know a priori the time of arrival of an acknowledgement
  - the time taken to pass through routers and gateways depends on the load on the network, which itself varies over time
  - TCP uses an adaptive algorithm to take these variations into account
  - the sender estimates the time required to receive the acknowledgement

TCP/IP Level 4 : TCP/UDP - TCP Reliability

- Connection-oriented : Segments delivered in order, without loss or duplication.
- Sequence number: enables anomaly detection
- Positive acknowledgement
- In case of loss :
  - Detection via TimeOut
  - GoBack-N re-transmission
- More complex implementation because link much more complex (link through Internet)

TCP/IP Level 4 : TCP/UDP - TCP Security Issue

- TCP SYN Flood: Known as a "half-open attack," a SYN flood attack exploits a common vulnerability in the TCP/IP handshake to overwhelm a server with TCP connections, preventing it from providing service to legitimate traffic and legitimate connections.
- SYN flood attacks may be carried out in three ways:
  - Non-spoofed IP addresses: When this method is deployed, it's easier for the targeted server to identify attribution and mitigate it, but doing that safely is a challenge.
  - Spoofed IP addresses: Attackers spoof the source IP address of a trusted server or internet-connected device, making it harder to trace the packets and prevent the attack.
  - Distributed IP addresses: Uses a botnet to send malicious packets from a distributed network of infected devices that may use their own IP address or a spoofed address to launch an attack that is more complex, larger in scale, and harder to mitigate.

Thank You