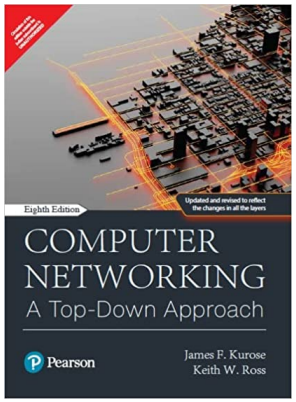
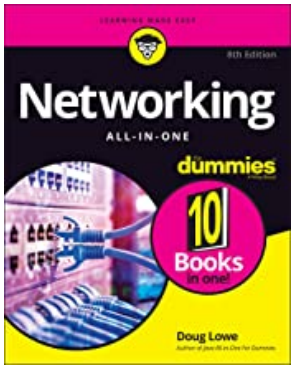
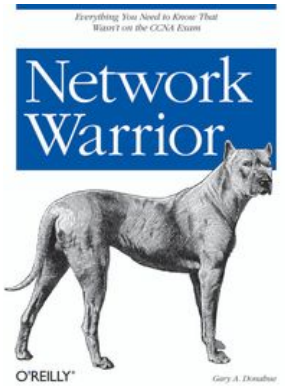
Best Books 2023 for beginners

- Computer Networking: A Top-Down Approach (6th Edition)
- Networking All-in-One For Dummies
- CCNA 200-301 Official Cert Guide Library
- Network Warrior

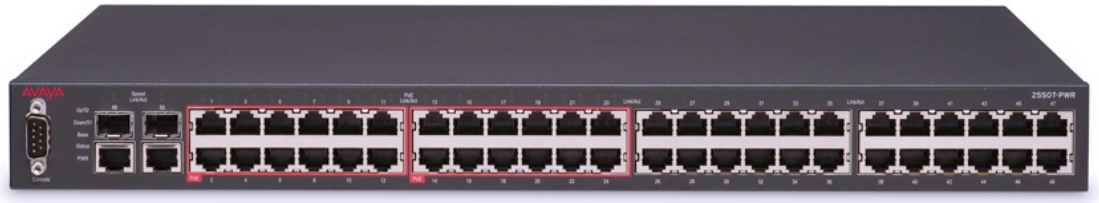
Referens: https://www.geeksforgeeks.org/best-computer-networks-books/





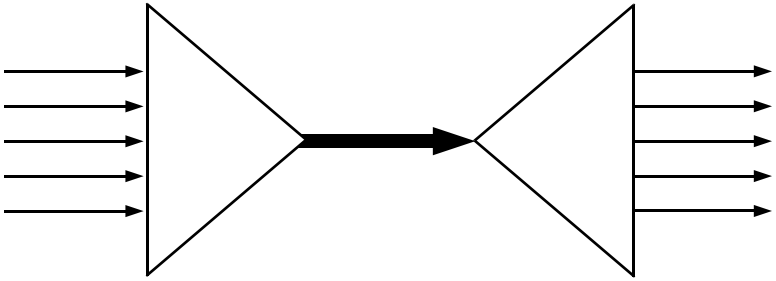


Ethernet Switch



- *Connects differents devices in a network.*
- *Distribute each packet to a corresponding device.*
- *Apply* **packet switching** *to receive/forward data.*
- *Improve effecienty and security.*
- *A switch is more intelligent than a Hub.*

Packet Switching



- *Packet switching is the primary basic for data communications.*
- *Packet switching has an* **header** *to direct the packet to its destination.*
- *Packet switching has also a* **payload** *used by OS or applications.*
- *Decrease* **latency** *that is the time it takes to cross a network.*

ATM Switch

- *ATM = Asynchronous Transfer Mode*
- *High speed switch (50 Mbps - 2.4 Gbps)*

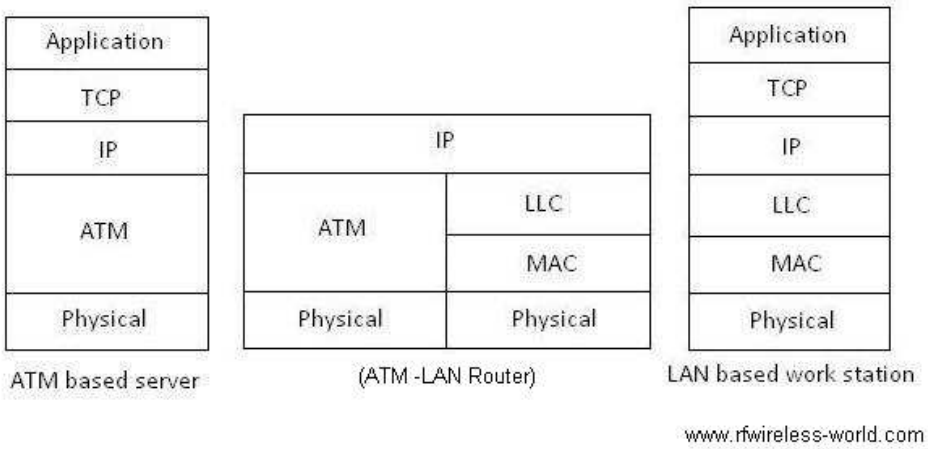
Ethernet Hub

- *Retransmits packets to all out ports.*
- *Unable to distinguish differents clients/devices.*
- *Detect and correct possible collisions (two demands at the same time).*

Network Bridge

- *Connect mutliple network.*
- *Works at layer 2 = data link layer*
- *Use Bridge table or forwarding database*

Router

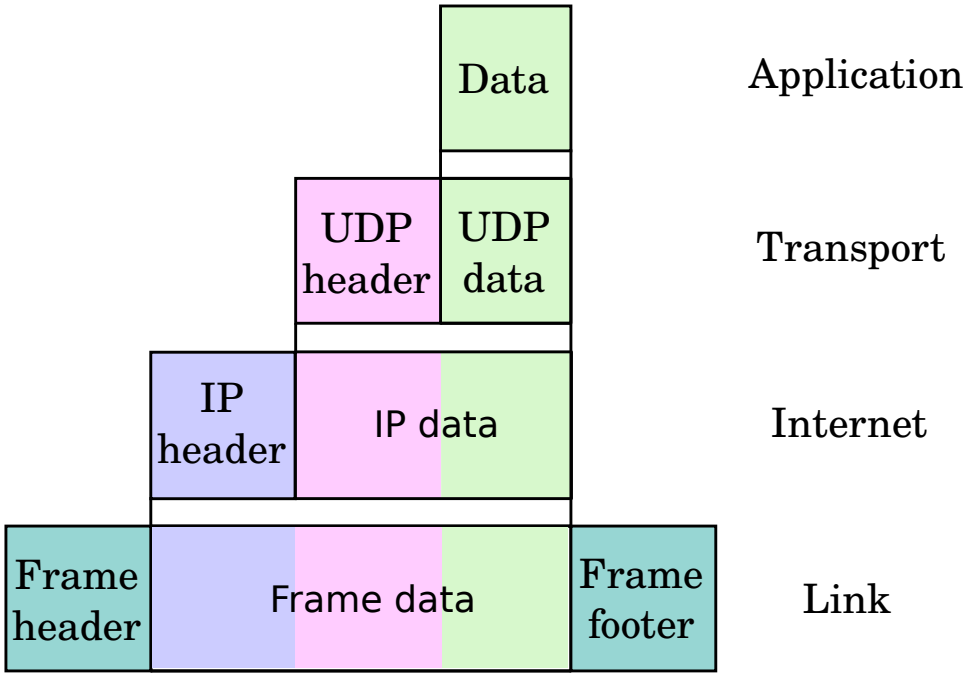


- *Device used to link two or more networks.*
- *Operates at OSI layer 3.*

Transmission Control Protocol (TCP)

- *It expand the Internet Protocol (IP) => (TCP/IP)*
- *TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes).*
- *It is a part of the Transport Layer (Layer 4 of the OSI Model)*
- *TCP is a connection-oriented i.e. connection is established before sending data.*
- *Retransmission and Errors detection improve reliability but increase latency*
- **Vulnerabilities:** *denial of service, connection hjacking, TCP veto and reset attack.*

User Datagram Protocol (UDP)



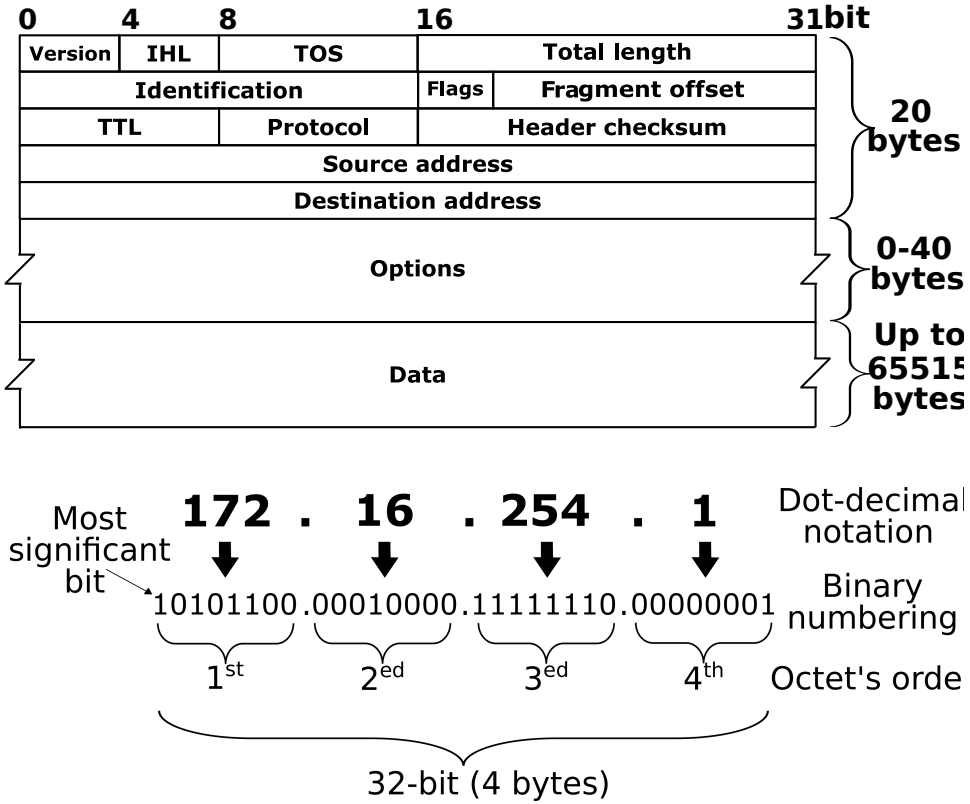
User Datagram Protocol (UDP)

- *Prioritizes* **time** *over* **reliability**.
- *Simple protocol: checksums for integrity and no handshakin*
- *Suitable for time-sensitive (real-time) applications*

Internet protocol (IP)

- *Relay datagrams/packets (header+payload) accross network.*
- *Operate on the network layer (Layer 3).*
- *1982: Internet Protocol Version 4 (IPv4)*
- *2006: Internet Protocol Version 6 (IPv6)*

IPV4


0
4
8
16
31bit
Version
IHL
TOS
Total length
Identification
Flags
Fragment offset
TTL
Protocol
Header checksum
Source address
Destination address
Options
Data
20 bytes
0-40 bytes
Up to 65515 bytes
Most significant bit
172 . 16 . 254 . 1
Dot-decimal notation
10101100.00010000.11111110.00000001
Binary numbering
1st
2ed
3ed
4th
Octet's orde
32-bit (4 bytes)

Special address blocks

Address block	Address range	Number	Scope	Description
0.0.0.0/8	*0.0.0.0-0.255.255.255*	16777216	Software	*Current network*
10.0.0.0/8	*10.0.0.0-10.255.255.255*	16777216	*Private network*	*Local private network*
127.0.0.0/8	*127.0.0.0-127.255.255.255*	16777216	Host	*Loopback locsl host*
192.88.99.0/24	*192.88.99.0-192.88.99.255*	256	Internet	*Reserved IPv6 to IPv4*

Reference: Wikipedia, https://en.wikipedia.org/wiki/Internet_Protocol_version_4

Open Systems Interconnection Model (OSI Model)

It's a framework that describes the functions of a network.

The 7 Layers of the OSI Model

1. **Application Layer**
Communications between User and Applications.
Convert data to a human form.

2. **Presentation Layer**
Take care of getting data for the applicatio layer.
Also compress, encrypt and decrypt data.

3. **Session Layer**
The time during which communications are
open and closed between
two interacting devices.

4. **Transport Layer**
End-to-end communications between devices.
Reassemble the segments of divided data in the session.
Control errors.

5. **Network Layer**
Used for communcations between two networks.
Divide **segments** *into* **packets**.
Works also as a router to find the optimal route.

6. **Data Link Layer**
Between two devices on the same network.
Data are broke into **frames**. *Check for errors.*
Contains two sublayers:
Media Access Control (Mac) and Logical Link Control (LLC)

7. **Physical Layer**
Data are converted into bits (0,1).
Include switchar, hub, cables etc.

Address Resolution Protocol (ARP)

- *A Protocol that convert an IP address (32 bits) to a MAC address (48 bits).*

  Example (IP) 192.168.1.6 and (MAC) 0c:2f:b0:bd:41:1a
- *An* **IP address** *also known as* **network layer** *A* **Mac address** *(Media Access Control) start/end a connection between two devices.*
  A Mac address is also know as the **data link**

Teori

- *ARP is a protocol that enables network devices to communicate with the TCP/IP protocol. Without ARP, no efficient method exists to build the datagram Layer 2 destination address.*
- *When a frame is placed on the network, it must have a destination MAC address. To dynamically discover the MAC address of the destination device, an ARP request is broadcast on the LAN. The device that contains the destination IP address responds, and the MAC address is recorded in the ARP cache.*
- *With no cache, ARP must continually request address translations each time a frame is placed on the network. This adds latency to the communication and could congest the LAN.*
- *ARP is a potential security risk. ARP spoofing, or ARP poisoning, is a technique used by an attacker to inject the wrong MAC address association into a network. An attacker forges a device's MAC address, and frames are sent to the wrong destination. Manually configuring static ARP associations is one way to prevent ARP spoofing.*

How it works?

***ARP** provides a dynamic mapping from an IP address to the corresponding hardware address.*

- *An ARP request is initiated. If the IP address is for the local network, the source host checks its **ARP cache** to find out the Mac of the destination computer.*
- *If the correspondence Mac is not found, **ARP broadcasts** the request to all the local hosts.*
- *All hosts receive the broadcast and check their own IP address. If no match is discovered, the request is ignored.*
- *The destination host that finds the matching IP address sends an **ARP reply** to the source host along with its hardware address.*

  The ARP cache is then updated with the hardware address of the destination host.

RARP *Reverse Address Resolution Protocol: Used by some hosts such as diskless workstation that do not know their own IP address when they are booted.*