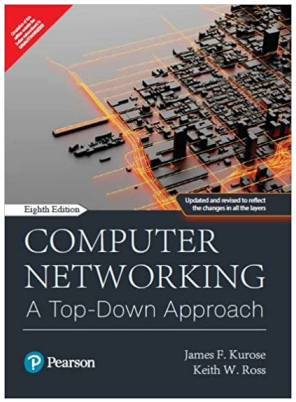
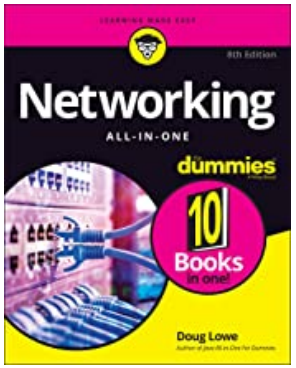
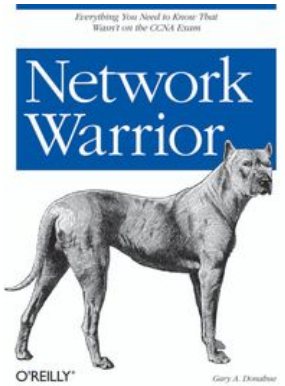
Best Books 2023 for beginners

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

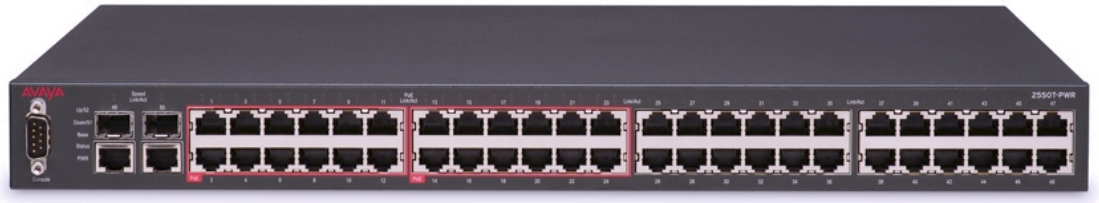
Referens: https://www.geeksforgeeks.org/best-computer-networks-books/





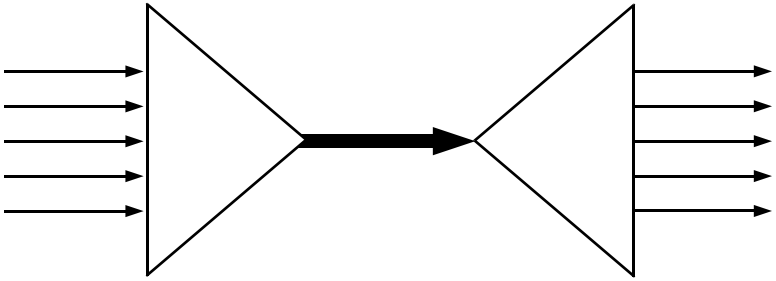


Ethernet Switch



- *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)*

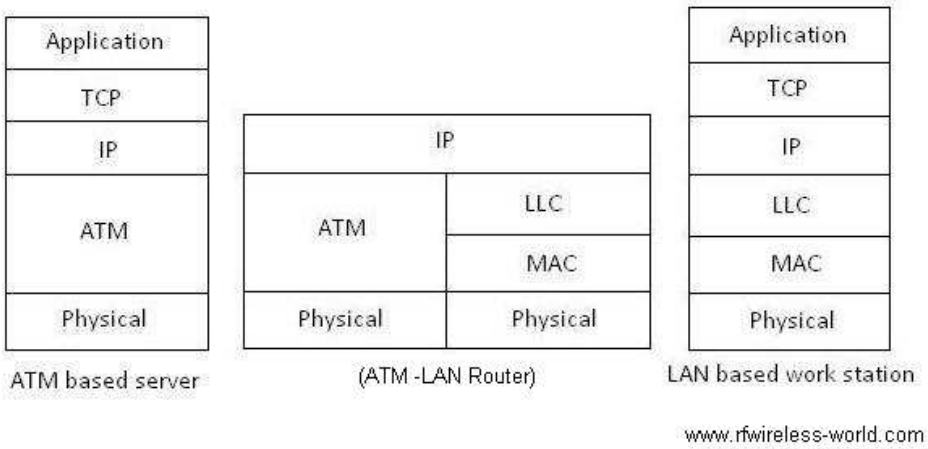
Ethernet Hub

- *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

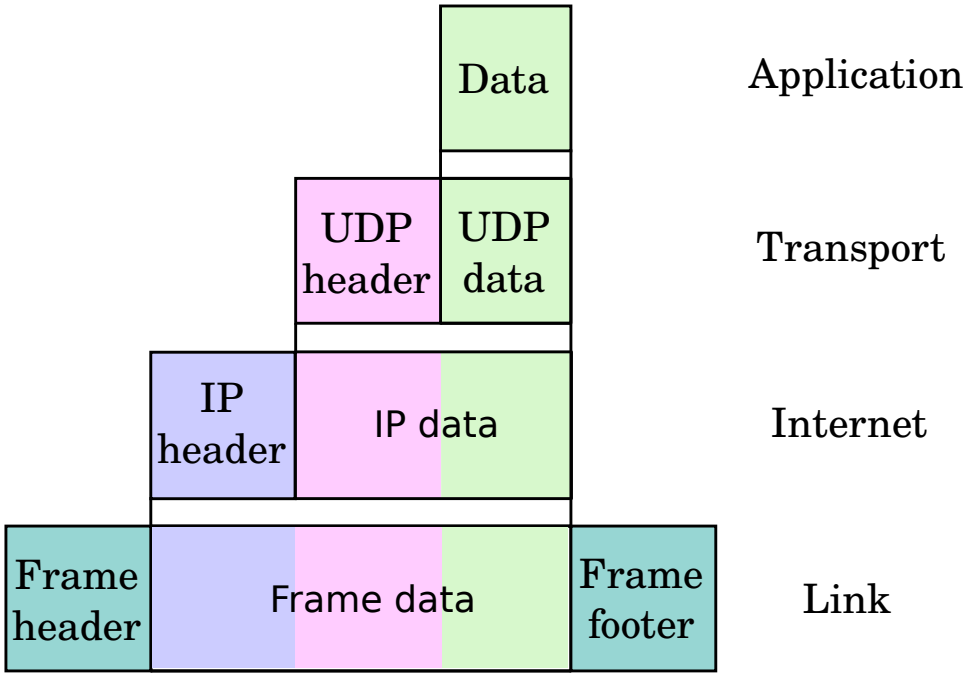


- *Device used to link two or more networks.*
- *Operates at OSI layer 3.*

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)



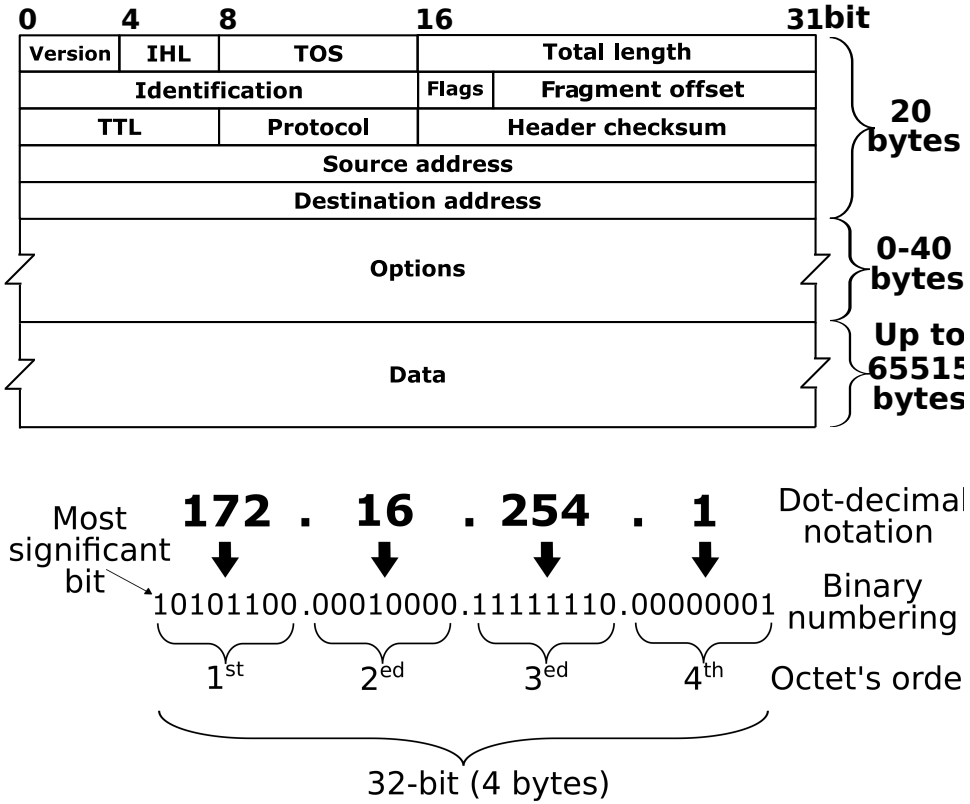
User Datagram Protocol (UDP)

- *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.*

References:

Ref: https://www.networkstraining.com/what-is-address-resolution-protocol-arp/

Challenge no 1

LIA 22 Project Specifications

You've just been employed at Cisco AB to work with one of their five IT-Infrastructure teams. Congratulation!!

Already today, your boss explained to you that the computer network has some critical issues that need to be solved before the Big conference that occurs in 8 weeks. New challenges will occur every Monday. Solutions need to be found and simulated using Packet Tracer (PT) from Cisco.

AT the end of the 8 weeks you'll have to present your solution in front of others IT-teams as well as your boss! and you have to deliver a copy of your final report.

The report need to have at least 10 pages long (in Times, 14pt). You'll describe in details using text, graphs, figures and references how your solution could be implemented physically and how it will solve all the issues of the physical network.

Each team will have to present a solution for every challenges that will occurs every weeks.

The company applies agilt/scrum working methodology. The sprint is one week long. Therefore, every Friday, your team will have to present in 15 minutes their solution of the challenge of the week, the problems they had and how they intended to solve these problems. Each teams will help and discuss every other team's solutions.

LIA Project Description

Your LIA project consists of four parts:

1) To install and understand how to use Packet Tracer (PT).
2) Find a solution to every week challenge using PT.
3) Participate at the Friday sprint discussions.
4) Write a final report of 10-20 pages.

Project Deadline*: Thursday the 16 of Mars at 11:59 pm.*

Presentation of all projects: *Friday the 17 of Mars between 9:00 and 12:00, (20 mn + 10 min discussion for each presentation)*

First challenge: Address resolution protocol

The first challenge is to:

1) Use **arp** *command for address resolution*
2) Use Wireshark/tcpdump to examine arp exchanges.

Task 1: Install and explore PT

Each team have to download, install and configure the computer network simulator Packet Tracer from Cisco. For that you need to create a free

account using your email address.

Start at:

https://www.netacad.com/courses/packet-tracer

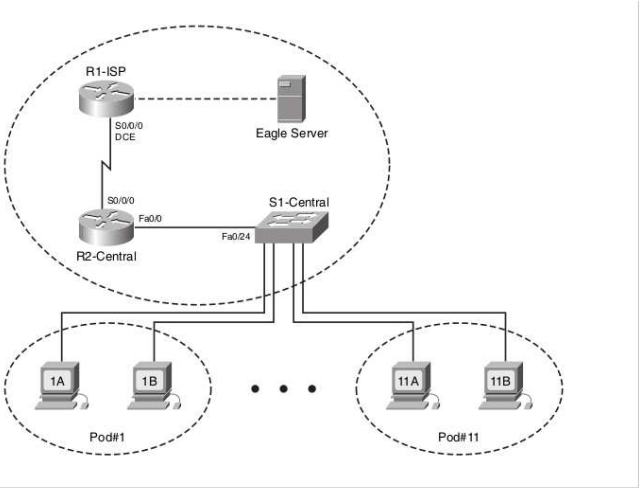
and then go to:
https://skillsforall.com/?utm_source=netacad.com&utm_medium=referral&utm_camp

And press "Get Started"

Open an account and you should be able to download Packet Tracer (PT).

Task 2: Create the network using PT

Create the following network using PT



Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	—
	Fa0/0	192.168.254.253	255.255.255.0	—
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	10.10.10.6
	Fa0/0	172.16.255.254	255.255.0.0	—
Eagle Server	—	192.168.254.254	255.255.255.0	192.168.254.253
	—	172.31.24.254	255.255.255.0	—
Host Pod#A	—	172.16.Pod#.1	255.255.0.0	172.16.255.254
Host Pod#B	—	172.16.Pod#.2	255.255.0.0	172.16.255.254
S1-Central	—	172.16.254.1	255.255.0.0	172.16.255.254

Task 3: Create the physical network

Create the same network using the physical devices available at Nackademin.

Task 4: ARP Lab

Apply **arp** to map a layer 3 IP address to a Layer 2 Mac address.

We consider the communication between hosts in the same network segment. To put a packet on the network segment, the sending host wraps the packet in a Layer 2 header, which must include the destination MAC address.

The sending host needs to know the receiver's MAC address before it can try to send the packet. If it doesn't know the MAC address, it

will try to find out using ARP.

On each host, run

```
arp -i eth1 -n
```

to see the entire ARP table for the eth1 interface (if there are any entries). If there are no ARP entries, the output will say

```
arp: in X entries no match found.
```

which is OK!

Observe that if there are any ARP entries, all the IP addresses displayed are on the same network segment.

If the "juliet" host (10.10.0.101) is already listed in an ARP table, then delete it with

```
sudo arp -d 10.10.0.101
```

Then, run

```
arp -i eth1 -n
```

again, and save the ARP tables from each host for your report.

On "romeo", run

```
sudo tcpdump -i eth1 -w $(hostname -s)-arp.pcap
```

Leave this running. Then, open a second SSH session to "romeo", and in that session, run

```
ping -c 1 10.10.0.101
```

to send an ICMP echo request to 10.10.0.101 ("juliet").

Terminate tcpdump with Ctrl+C.

Run

```
arp -i eth1 -n
```

on each host, again. Save the new ARP tables for your report.

The tcpdump application will have saved a new file named "romeo-arp.pcap" in your home directory on the "romeo" node. You can "play back" a summary of the capture file in the terminal using

```
tcpdump -enX -r $(hostname -s)-arp.pcap
```

Note: You'll see that a new line is added to juliet's ARP table with romeo's address, even though "juliet" did not send an ARP request to resolve romeo's address!

When "juliet" receives and responds to an ARP request for its own

address, it will also update its ARP table to include the IP address and MAC address of the host that sent the ARP request.

Next, run

```
sudo tcpdump -i eth1 -w $(hostname -s)-no-arp.pcap
```

on "romeo", and in a second terminal on "romeo", run

```
ping -c 1 10.10.0.101
```

again. Terminate tcpdump with Ctrl+C. Then "play back" a summary of the capture file in the terminal using

```
tcpdump -enX -r $(hostname -s)-no-arp.pcap
```

Use scp to transfer both packet capture files to your laptop. Then, you can open them in Wireshark for further analysis.

Note: In your packet capture, depending on the timing of your experiment, you may observe an ARP request and reply after the ICMP echo request and response are exchanged. And if you look closely at this unexpected ARP request, you may notice that the destination MAC address is not the broadcast address (as with a *regular* ARP request, when the sender needs to resolve an IP address and does not know the associated MAC address) this ARP request has a unicast destination MAC address. This type of ARP request is an **ARP poll**. ARP polls can be sent by a host that wants to confirm the validity of an existing entry in their ARP table, for example an entry that might be getting a little bit old.

In your report:

Show the summary tcpdump output for both packet captures. In the first case, an ARP request was sent and a reply was received before the ICMP echo request was sent.

In the second case, no ARP request was sent before the ICMP echo

request. Why? Show evidence from the output of the arp commands to support your answer.

From the first saved tcpdump output, answer the following questions:

1) What is the target IP address in the ARP request?
2) At the MAC layer, what is the destination Ethernet address of the frame carrying the ARP request? Why?
3) What is the frame type field in the Ethernet frame?
4) Of the four hosts on your network segment, which host sends the ARP reply? Why?
5) When an ARP request and ARP reply appear on a network segment, which hosts on the network segment will add the target of the ARP request to their ARP table?
6) Which hosts on the network segment will add the sender of the ARP request to their ARP table? Explain in general, as well as for the specific case of this network.
   Use the ARP tables you captured to support your answer.

Task 5: ARP for a non-existent host

For this lab, you will need three terminal windows on the "romeo" host.

On the "romeo" host, run

```
sudo tcpdump -i eth1 -w $(hostname -s)-eth1-nonexistent.pcap
```

In a second terminal window on "romeo", run

```
sudo tcpdump -i lo -w $(hostname -s)-lo-nonexistent.pcap icmp
```

to capture ICMP traffic on the loopback interface (i.e. ICMP messages sent from romeo to itself).

Then, in a third terminal window on "romeo", run

```
ping -c 1 10.10.0.200
```

Note that there is no host with this IP address in your network configuration.

Wait for it to finish. Terminate both tcpdump processes with Ctrl+C.

The message "Destination Host Unreachable" in the ping output reflects that an ICMP message of type Destination Unreachable with code Host Unreachable was received! This message is sent by the host to itself when it cannot resolve an IP address (e.g. due to ARP timeout).

"Play back" a summary of the loopback capture file in the terminal using

```
tcpdump -enX -r $(hostname -s)-lo-nonexistent.pcap
```

Observe this message in the loopback interface capture.

Also, "play back" a summary of the Ethernet capture file in the terminal using

```
tcpdump -enX -r $(hostname -s)-eth1-nonexistent.pcap
```

You can also use scp to transfer the packet captures to your laptop, and open them in Wireshark to see these packets in more detail.

In your report:

Show the summary tcpdump output from the Ethernet interface, and use it to answer the following questions:

In the previous exercise, after sending an ARP request and receiving a reply, "romeo" sends an ICMP echo request. In this exercise, is an ICMP echo request ever sent? Why or why not? From the tcpdump output, describe how the ARP timeout and retransmission were performed.

How many attempts were made to resolve a non-existing IP address? How much time separates each attempt?

Show the ICMP message you captured on the loopback interface, and

answer these