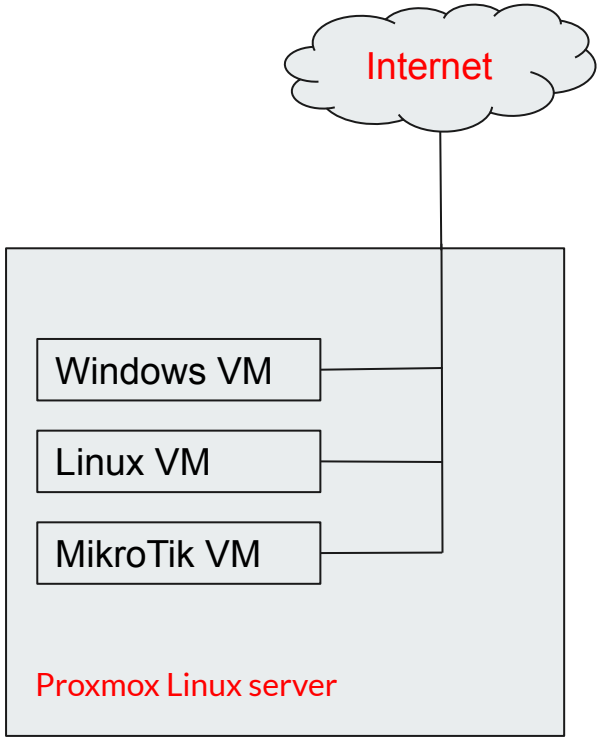
Networking 101

Lab Setup

Mohammad Reza Mollasalehi
info@mrsalehi.info

Lab components

- Proxmox is virtual environment to test and run virtual machine. We hosted 3 virtual machines there (Windows, Linux, MikroTik router OS)
- For connecting VMs to the internet, we use Linux bridge, so each VM can have specific interface, so it's possible to give each VM specific IP.



Networking 101

Wireshark

Mohammad Reza Mollasalehi
info@mrsalehi.info

What is Wireshark:

- Wireshark is a network **packet analyzer**. A network packet analyzer presents captured packet data in as much detail as possible.

- You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

What Wireshark is not!

- Wireshark isn't an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.

- Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things.

Demo 1 – Basic Run

1. Install & Run Wireshark
2. Run Wireshark on local interfaces
3. Run Wireshark on remote interfaces

Filters

- We are often not interested in all packets flowing through the network
- Use filters to capture only packets of interest to us
- Two kind of filters
    - Capture Filter: Filtered while capturing. Like TCPDump
    - Display Filter: More detailed filtering. Allows to compare values in packets. Not real time

Demo 2 - Filters

1. Capture only UDP packets --- “udp”
2. Capture only TCP packets --- “tcp”
3. Capture only UDP packets with destination port 53 (DNS requests) --- “udp dst port 53”
4. Capture only UDP packets with source port 53 (DNS replies) --- “udp src port 53”
5. Capture only UDP packets with source or destination port 53 (DNS requests and replies) --- “udp port 53”
6. Capture only packets destined to mrsalehi.info --- “dst host mrsalehi.info”
7. Capture both DNS packets and TCP packets to/ from mrsalehi.info --- “(tcp and host mrsalehi.info) or udp port 53”

Demo 3 - Display Filters

- **Different Syntax:**
  - ip.dst==81.19.210.0/25
- **More expressive:**
  - eth.src[1-2] == 00:83 [Check only bytes 1 and 2]
- **Go crazy with logical expressions:**
  - tcp.dst[0:3] == 0.6.29 xor udp.src[1] == 42

Demo 4 - Files

- Use TCPDump to get packet from target --- tcpdump -i tap101i0 -c 10 -w test.pcap
- Then open file using Wireshark

Demo 5 - Find password on HTTP site

- http://vbsca.ca/login/login.asp
  - http.host == vbsca.ca

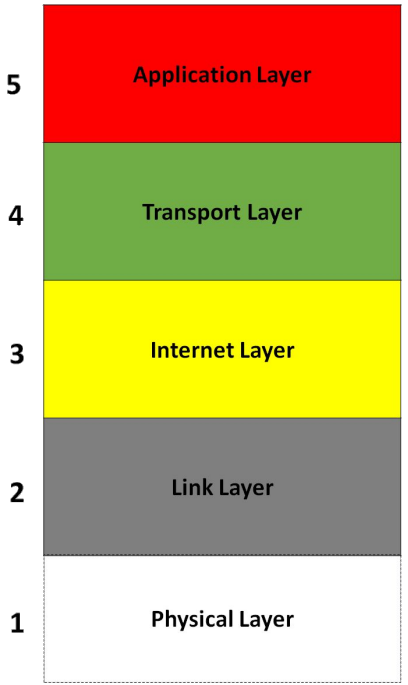
Networking 101

Protocols Section

Mohammad Reza Mollasalehi
info@mrsalehi.info

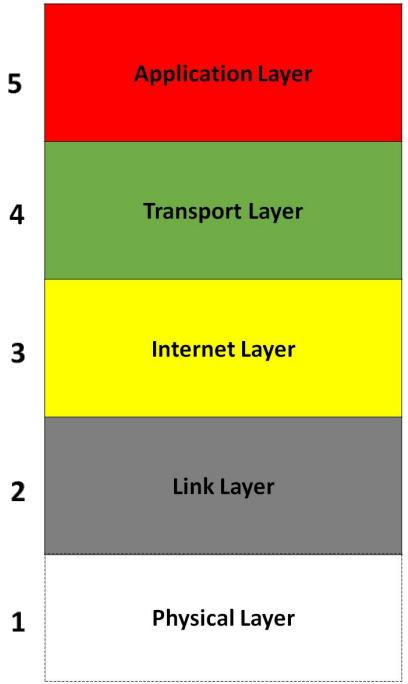
What is IP:

- Public IP Address vs Private IP Address
- Static IP vs Dynamic IP
- Multicast IP vs Broadcast IP
- Gateway
- IP works on which layer?



What is Port:

- Why we need ports?
- Ports works on which layer?
- Port is an address of a 16-bit unsigned integer number which ranges from 0 to 65535
- The ports 0 to 1023 are called well-known ports or system ports, these ports are especially associated with particular services.
- How many ports I have in my computer?

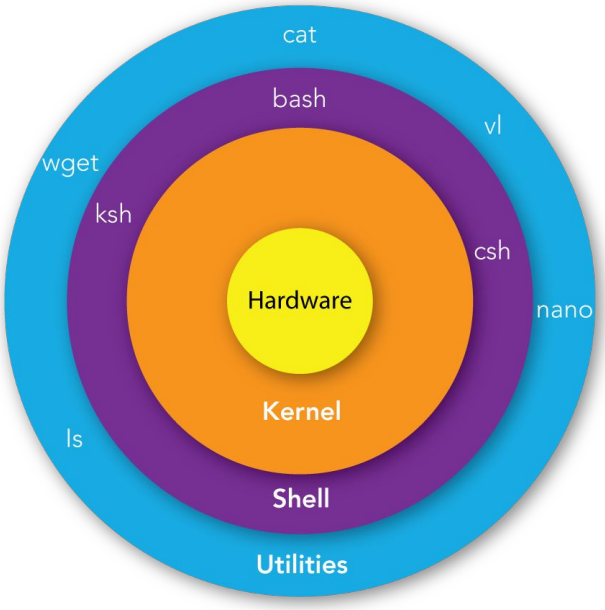


Known protocols sec 1

- Secure Shell (SSH)
- File Transfer Protocol/Secure (FTP/S)
- Domain Name System (DNS)
- Transmission Control Protocol (TCP) vs User Datagram Protocol (UDP)
- Hypertext Transfer Protocol/Secure (HTTP/S)
- Simple Mail Transfer Protocol (SMTP)
- Internet Message Access Protocol (IMAP) vs Post Office Protocol 3 (POP3)
- Internet Control Message Protocol (ICMP)
- Telnet

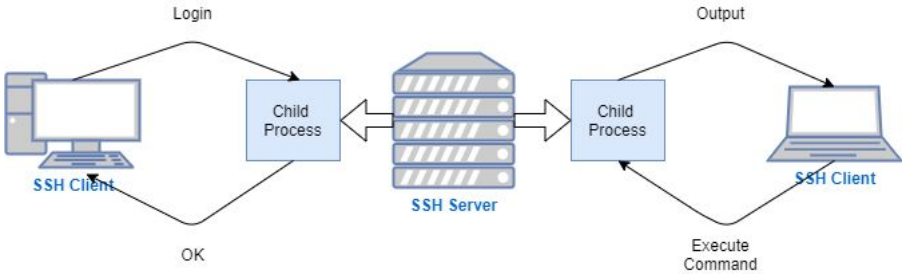
Secure Shell (SSH)

- What Is Shell?
- Demo



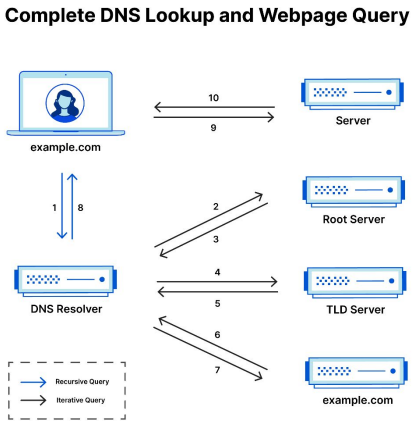
Secure Shell (SSH)

- What Is Secure Shell?
- SSH works on which layer?
- SSH works on port TCP 22
- Demo
  - filter == ssh
  - ip.src == 45.147.231.29 || ip.dst == 45.147.231.29
- Secure Shell Commands:
  - ssh
  - sshd
  - ssh-keygen



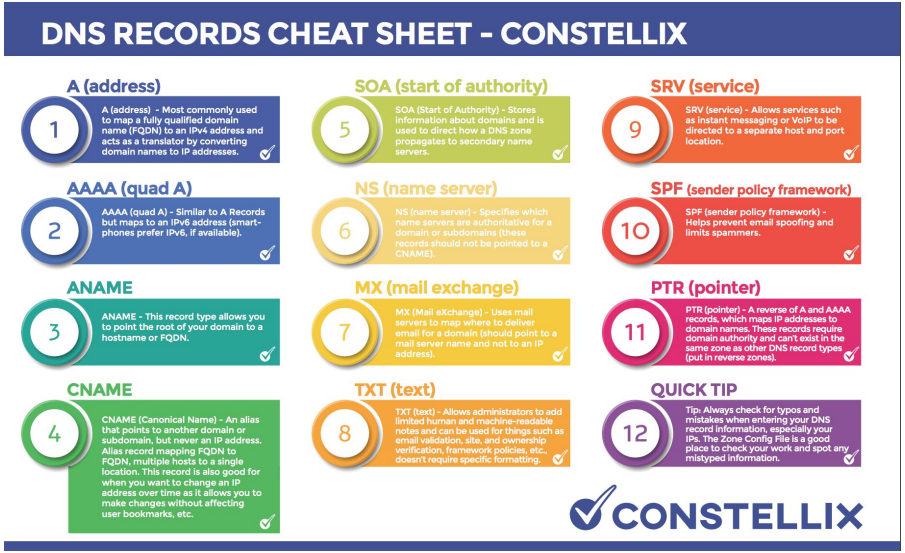
Domain Name System (DNS)

- What DNS do?
- Behind the scenes of DNS
- DNS works on port UDP 53
- What is DNS cache poisoning?
- DNS works on which layer?
- Demo



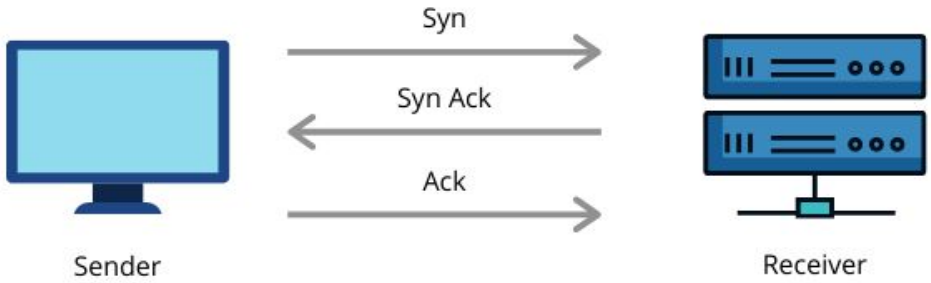
DNS Records

- A record
- AAAA record
- CNAME record
- MX record
- TXT record
- Demo



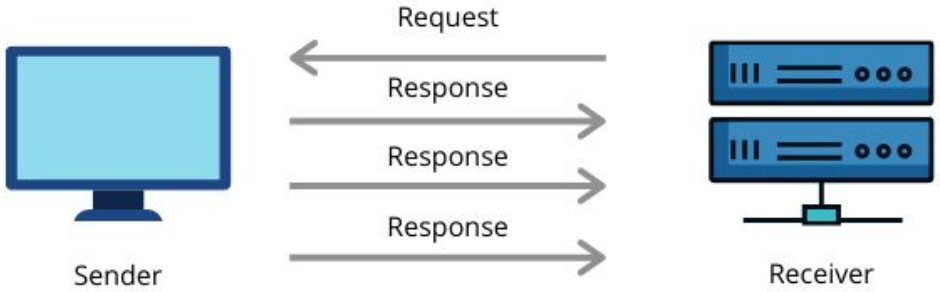
Transmission Control Protocol (TCP)

- What is TCP?
- TCP works on which layer?
- 3 way handshake
  - Syn
  - Syn-Ack
  - Ack



User Datagram Protocol (UDP)

- What is UDP?
- UDP works on which layer?
- Is UDP have checksum header?



Hypertext Transfer Protocol (HTTP)

- What is in an HTTP request?
  - HTTP version type
  - a URL
  - HTTP request headers
  - Optional HTTP body
- What is an HTTP method?
  - GET
  - POST
- What is in an HTTP response?
  - an HTTP status code
  - HTTP response headers
  - optional HTTP body
- What's an HTTP status code?
  - 1xx Informational
  - 2xx Success
  - 3xx Redirection
  - 4xx Client Error
  - 5xx Server Error

▼ **Request Headers**

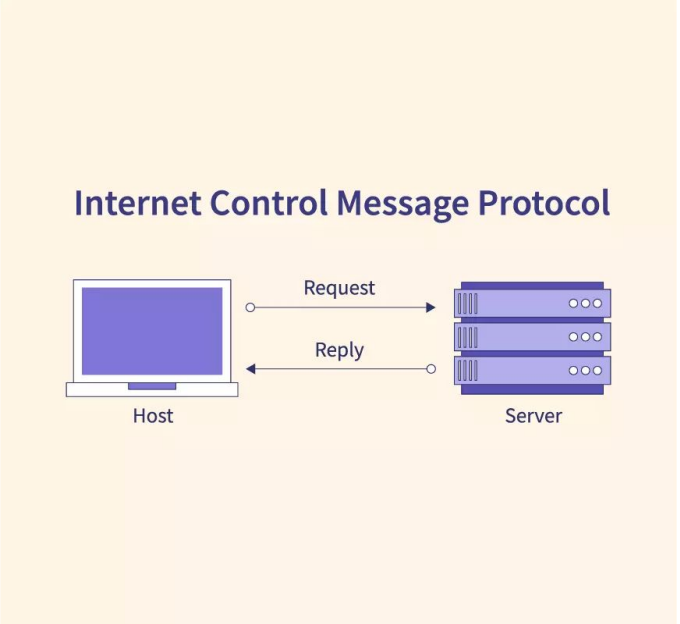
:authority: www.google.com
:method: GET
:path: /
:scheme: https
accept: text/html
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0

```
~ curl -IL google.com
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Date: Sun, 05 Mar 2023 18:32:55 GMT
Expires: Tue, 04 Apr 2023 18:32:55 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN

HTTP/1.1 200 OK
Content-Type: text/html; charset=ISO-8859-1
Date: Sun, 05 Mar 2023 18:32:56 GMT
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Transfer-Encoding: chunked
Expires: Sun, 05 Mar 2023 18:32:56 GMT
Cache-Control: private
Set-Cookie: AEC=ARSKqsL5gu-6Kn0sXL90FXc-1mzwuUjJ
n=.google.com; Secure; HttpOnly; SameSite=lax
```

Internet Control Message Protocol (ICMP)

- What is ICMP?
- ICMP Protocol in which layer?



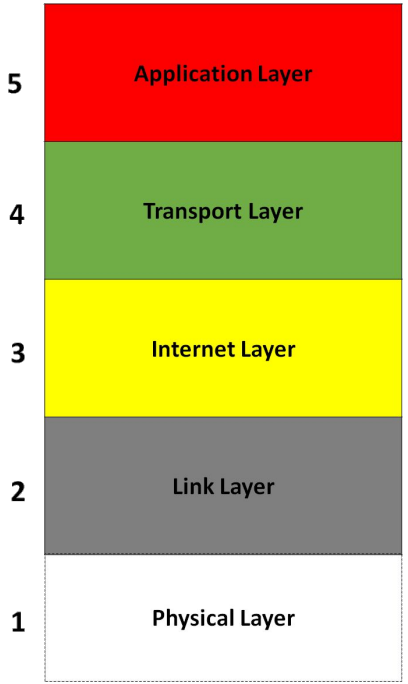
Networking 101

Network Layers

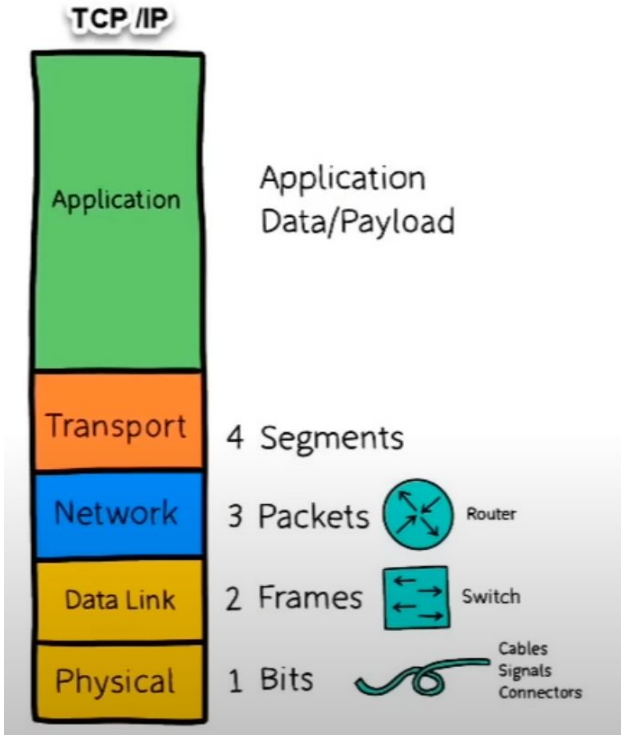
Mohammad Reza Mollasalehi
info@mrsalehi.info

Physical Layer

- Copper
  - Cat6, Cat6A, Cat 7, …
- Fiber
  - Cable types
  - Optic types
  - DAC
- Over Air
  - AP
  - P2P



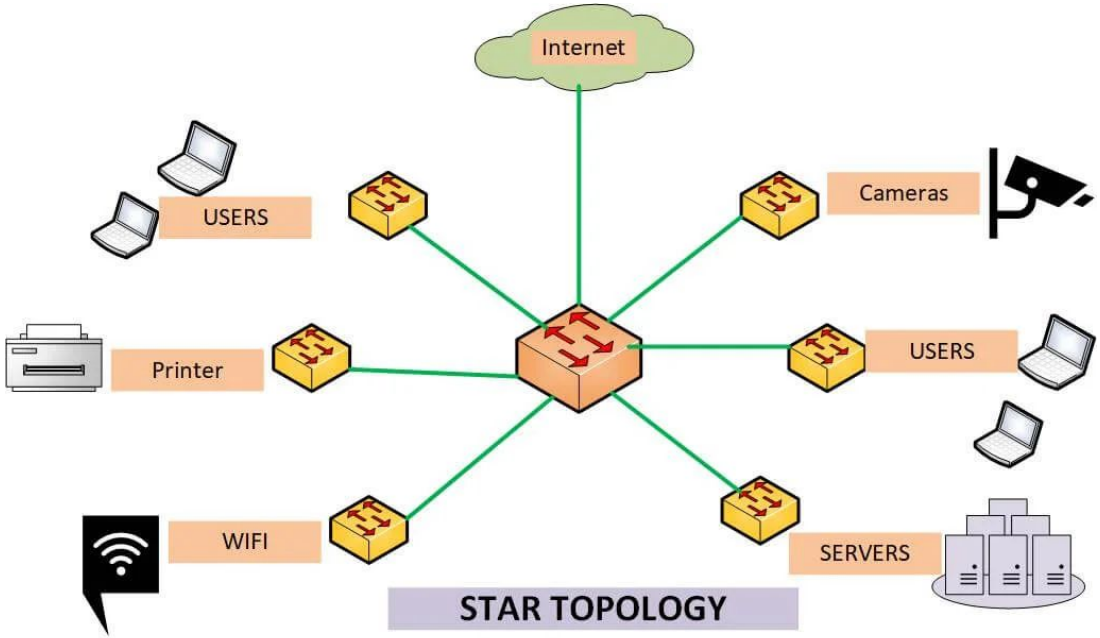
Network Layers



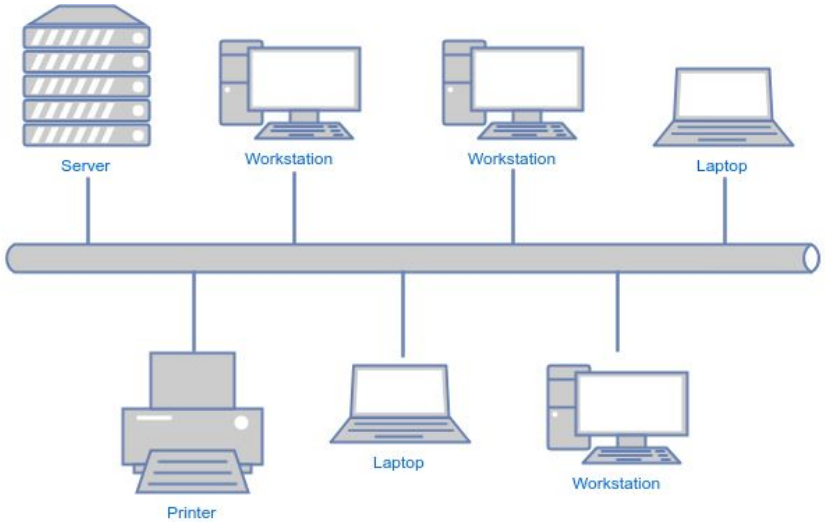
Layer 2

- What is physical address?
  - MAC address
  - L2 address
  - Ethernet address
  - BIA
- What is ARP protocol?
- What is ARP cache?

Star Topology

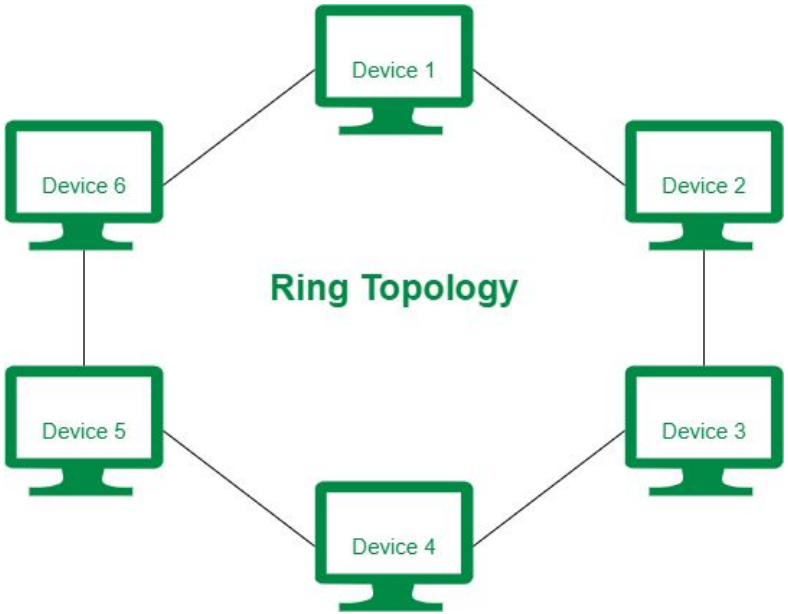


Bus topology

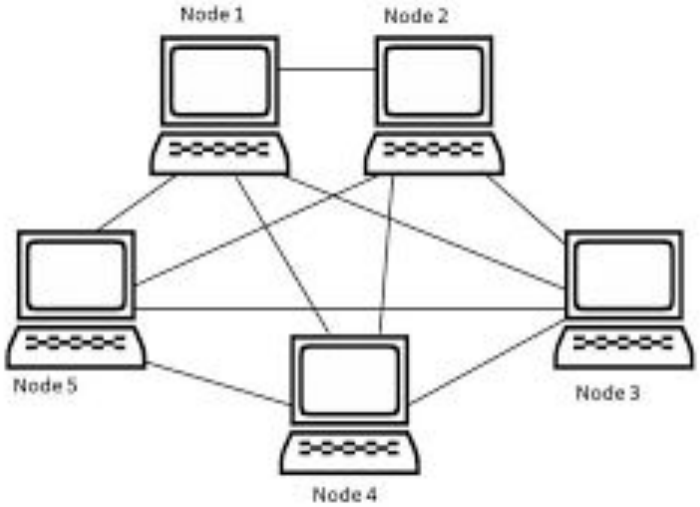


Bus Topology Network

Ring Topology



Mesh Topology



Hub vs Switch

- What is hub?
- Why hub is half duplex?
- What is switch?
- What is MAC learning?
- What happened when switch doesn't know MAC? (unicast flood)
- Broadcast problems …

VLAN(802.1Q)

- What is VLAN?
- What is the effect of VLAN on layer3?
- What is native VLAN?

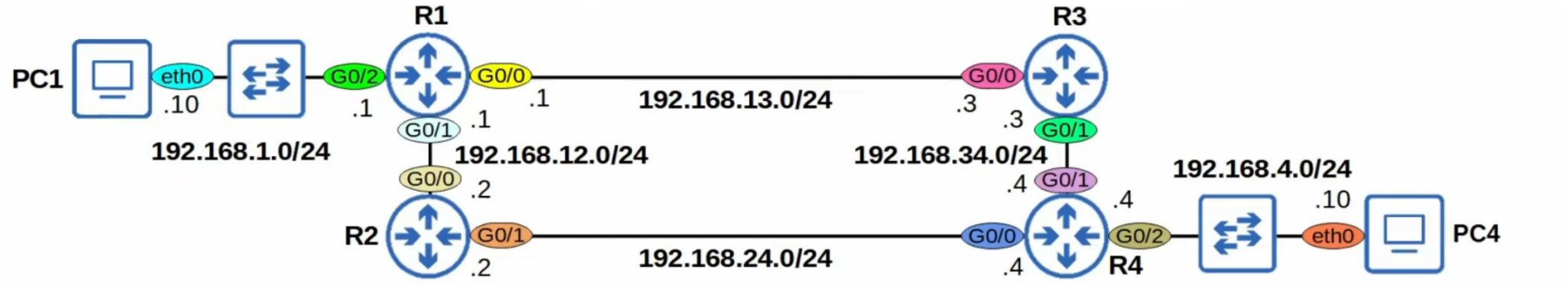
Real configuration

- Labels
- Hostname
- IPs
- Passwords
- Ssh & telnet

Layer 3

- Route
- Routing table
  - Static route
  - Dynamic route

Example

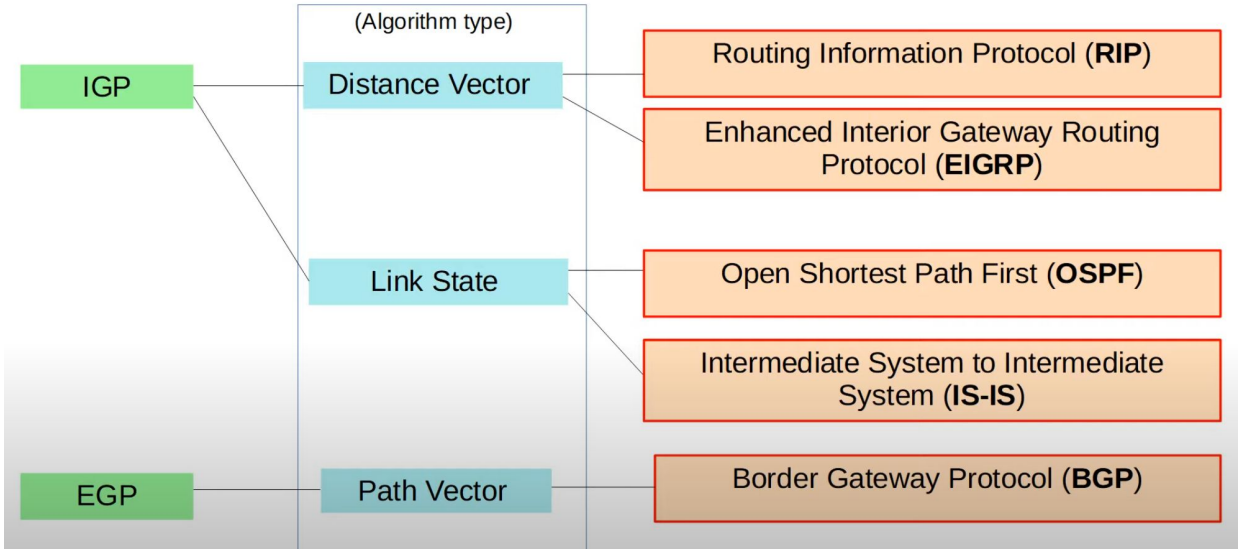

R1
R3
PC1
eth0
.10
G0/2
.1
G0/0
.1
192.168.13.0/24
G0/0
.3
.3
G0/1
192.168.1.0/24
G0/1
.1
192.168.12.0/24
192.168.34.0/24
G0/0
.2
.4
G0/1
.4
192.168.4.0/24
.10
R2
G0/1
.2
192.168.24.0/24
G0/0
.4
G0/2
R4
eth0
PC4

Set static Route & Default route

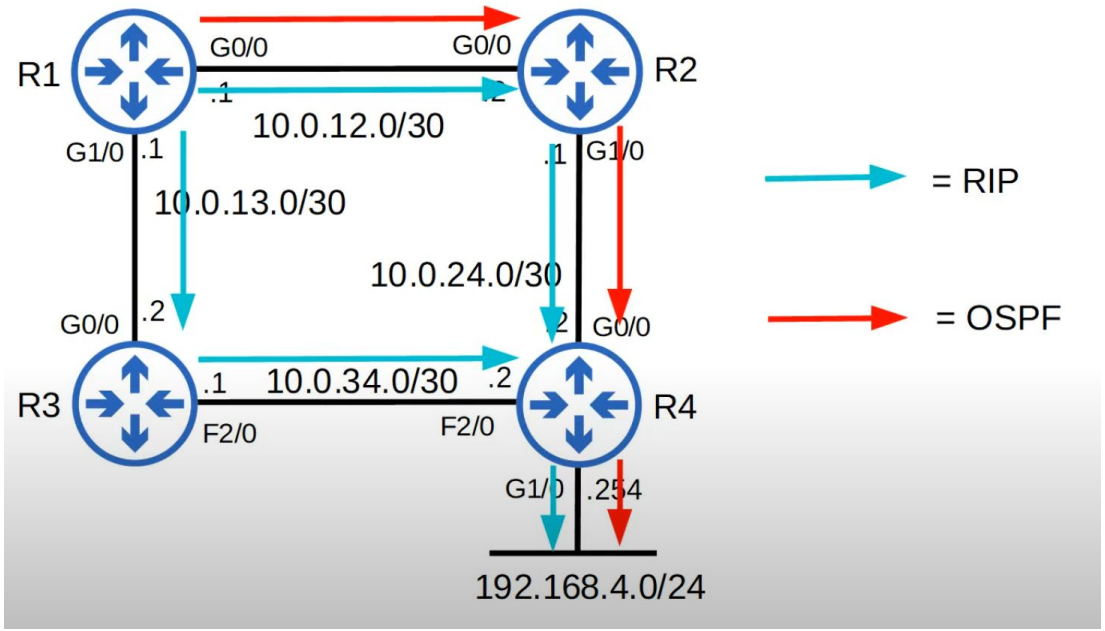
- **ip route** ip-address netmask next-hop
- **ip route** ip-address netmask exit-interface (Proxy ARP)
- **ip route** ip-address netmask exit-interface next-hop
- **ip route** 0.0.0.0 0.0.0.0 192.168.1.1

Dynamic Route

- IGP
- EGP



IGP	Metric	Explanation
RIP	Hop count	Each router in the path counts as one 'hop'. The total metric is the total number of hops to the destination. **Links of all speeds are equal.**
EIGRP	Metric based on bandwidth & delay (by default)	Complex formula that can take into account many values. By default, the bandwidth of the **slowest link in the route** and the total delay of all links in the route are used.
OSPF	Cost	The cost of each link is calculated based on bandwidth. The total metric is the total cost of each link in the route.


R1
R2
R3
R4
G0/0
G0/0
.1
.2
10.0.12.0/30
G1/0
.1
10.0.13.0/30
.1
G1/0
10.0.24.0/30
G0/0
.2
.2
G0/0
.1
10.0.34.0/30
.2
F2/0
F2/0
G1/0
.254
192.168.4.0/24
= RIP
= OSPF

Route protocol/type	AD
Directly connected	0
Static	1
External BGP (eBGP)	20
EIGRP	90
IGRP	100
OSPF	110

Route protocol/type	AD
IS-IS	115
RIP	120
EIGRP (external)	170
Internal BGP (iBGP)	200
Unusable route	255

Routing Information Protocol (RIP)

- What is RIP?
- RIPv1 vs RIPv2
- RIP update routing table 30s
- RIP message types (224.0.0.9)
    - Request: to find enable neighbor router and get their tables
    - Response: to send local routing table
- Broadcast vs Multicast

RIP configuration

- router rip
- version 2
- no auto-summary
- network 10.0.0.0 (network class full)(just active)
- network 172.16.0.0 (NOT 172.16.0.0/16)
- passive-interface g0/2
- default-information originate
- show ip protocols
- maximum-paths 10

Network Address Translation (NAT)

- What is NAT?
- Why we are using NAT?
- Source NAT
  - Static NAT
  - Dynamic NAT
  - Dynamic PAT

Static NAT

```
R1(config-if)# ip nat inside
R1(config-if)# ip nat outside
R1(config)# ip nat inside source static inside-local-ip inside-global-ip
R1# show ip nat translations
R1# show ip nat statistics
R1# clear ip nat translation *
```

Dynamic NAT

- ip nat inside
- ip nat outside
- access-list <LIST ID> permit <PRIVET RANGE> <WILD CARD>
- ip nat pool <POOL NAME> <START IP> <END IP> netmask <SUBNET>
- ip nat inside source list <LIST ID> pool <POOL NAME>

NAT overload (PAT)

- ip nat inside
- ip nat outside
- access-list <LIST ID> permit <PRIVET RANGE> <WILD CARD>
- ip nat pool <POOL NAME> <START IP> <END IP> netmask <SUBNET>
- ip nat inside source list <LIST ID> interface <INTERFACE> overload
- ip nat inside source list <LIST ID> pool <POOL NAME> overload

Inter VLAN routing

- Traditional way (multi interface)
- Router on stick (single interface)
- Multilayer switch

Router on stick

- interface g0/0
- ip address 172.16.10.1 255.255.255.0
- interface g0/0.10
- encapsulation dot1Q 10
- ip address 192.168.1.1 255.255.255.0
- interface g0/0.20
- encapsulation dot1Q 20
- ip address 192.168.2.1 255.255.255.0
- interface g0/0
- no shutdown

Multilayer switch

- int vlan 10
- ip address 192.168.1.1 255.255.255.0
- int vlan 20
- ip address 192.168.2.1 255.255.255.0