HSLU

Rotkreuz

Information & Cyber Security

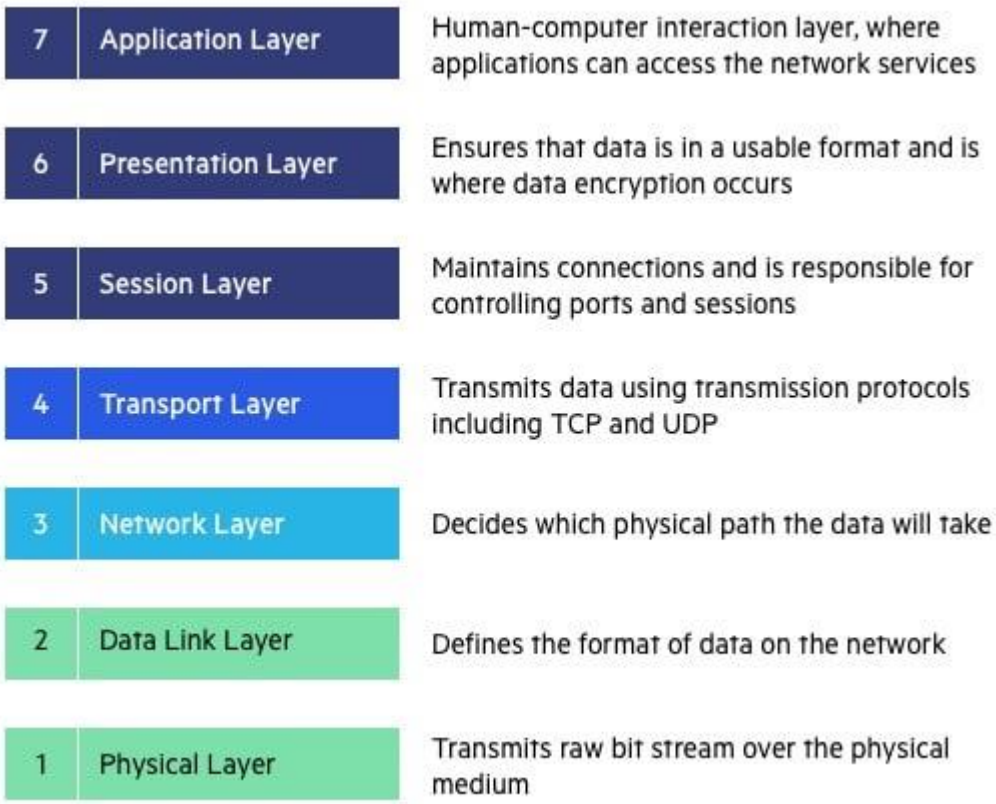
NETW Notes

David Jäggli

Table of contents

1 Layers

OSI:



- **Layer1:** Bits
- **Layer2:** Frames
- **Layer3:** Packets
- **Layer4:** Segments

1.1 Physical Layer

- Data communication is in raw bits.
- Networking Interface Cards (NIC)

1.1.1 Common Terms

Term	Meaning
Bandwidth	The capacity at which a medium can carry data.
Latency	Amount of time until the data reaches the destination.
Throughput	The number of bits sent in a given period of time.
Goodput	The amount of usable data: Goodput = Throughput – traffic overhead
Simplex	Only one way communication.
Half-Duplex	Two-way communication but only one direction at a time possible (WiFi).
Full-Duplex	Two-way communication at the same time possible.

1.1.2 Cables

UTP:

- No shielding
- Twisted pairs with opposite polarity to eliminate EMI.
- Different number of twists to prevent crosstalk.

STP:

- Same but shielded -> more expensive.

Fibre optic:

- Hella expensive but complete immune to EMI

1.1.3 Wireless

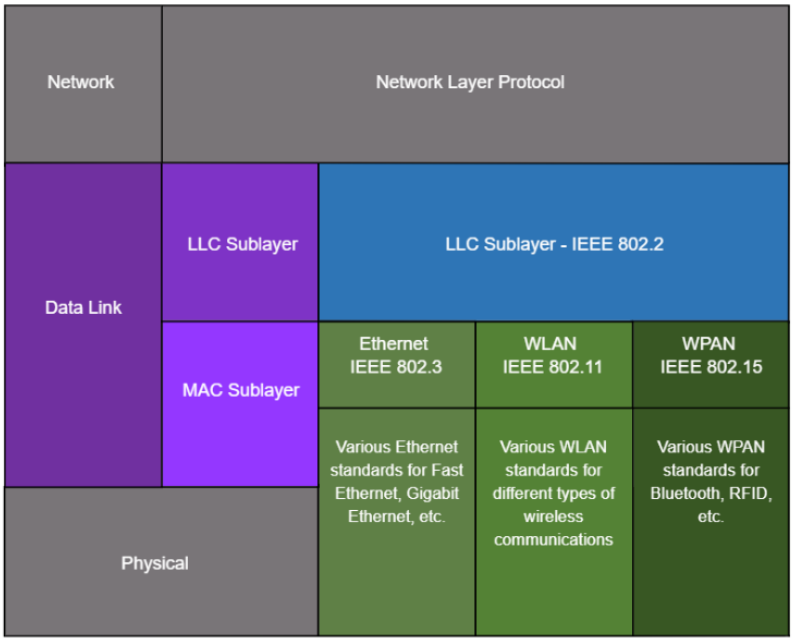
Limitations:

- Coverage area
- Interference
- Security
- Shared medium – half duplex -> only one device can send or receive at a time. Many users connected to the same WiFi reduces the bandwidth.

1.2 Data Link Layer / Switch level

Purpose of the Data Link Layer

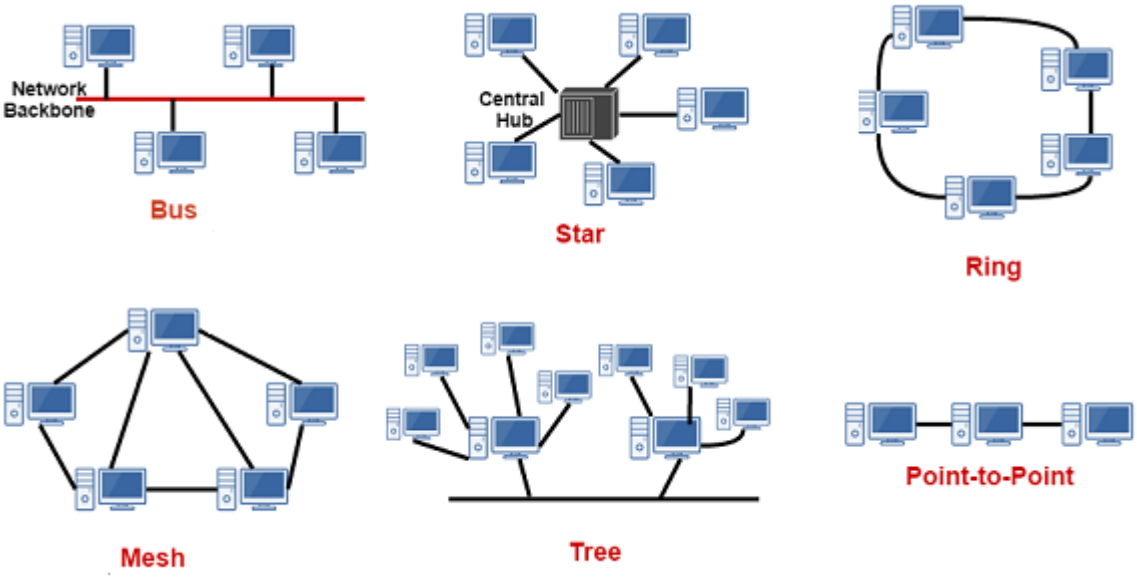
IEEE 802 LAN/MAN Data Link Sublayers



Term	Long	Meaning
LLC	Logical Link Control	communicates between the networking software at the upper layers and the device hardware at the lower layers.
MAC	Media Access Control	Data encapsulation and media access control.

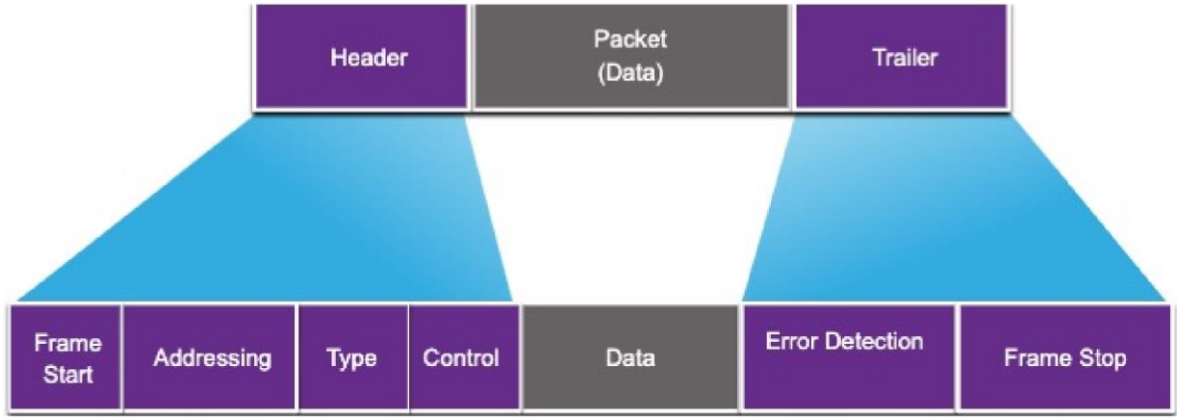
1.2.1 Topologies

- Physical Topology (How are the devices physically arranged / rooms)
- Logical Topology (networks / subnetworks)



- **Bus**: deprecated -> old LAN.
- **(extended) star:** very common LAN.
- **Mesh:** high availability but expensive.
- **Hub and Spoke:** similar to star.
- **Point to Point:** simplest and common WAN.

1.2.2 Frames



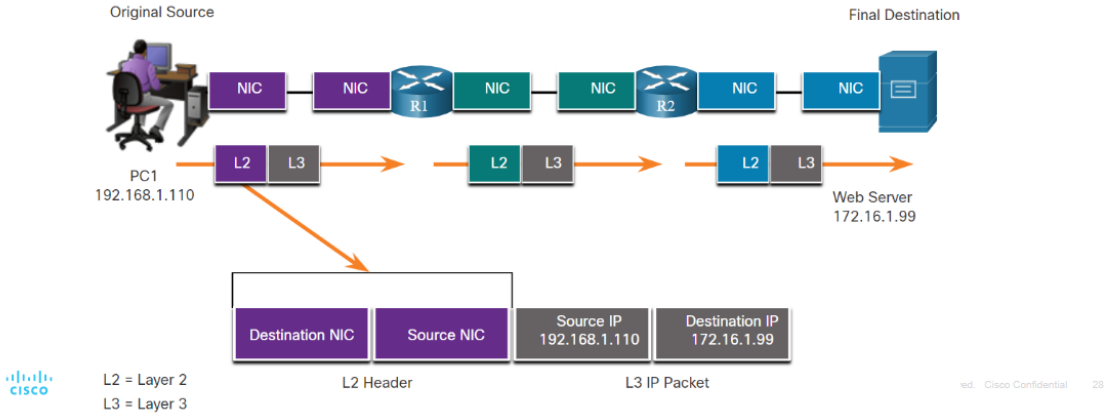
Field	Description
Start and Stop	Identifies beginning and end of frame
Addressing	Indicates source and destination nodes
Type	Identifies encapsulated Layer 3 protocol
Control	Identifies flow control services
Data	Contains the frame payload
Error Detection	Used for determining transmission errors

1.2.3 Layer 2 Addresses

Data Link Frame

Layer 2 Addresses

- Also referred to as a physical address.
- Contained in the frame header.
- Used only for local delivery of a frame on the link.
- Updated by each device that forwards the frame.



MAC-Address

E0-93-22-33-33-44

Consists of two parts:

1. OUI: Vendor specific
2. Vendor assigned, unique combination.

Multicast

If destination MAC address starts with 01-00-5E:

- encapsulated data is an IPv4 multicast packet

If destination MAC address starts with 33-33:

- encapsulated data is an IPv6 multicast packet

flooded out on all eth-ports, except the incoming one. Not forwarded to routers by default.

Broadcast

Destination MAC address -> max -> FF:FF:FF:FF:FF:FF

Flooded out on all eth ports except incoming ones. Not forwarded by routers.

1.3 Network Layer / Router level

Address on which a host can listen to:

- Unicast
- Multicast
- Broadcast
- IPv6
- IPv6 Unicast

1.3.1 Network classes

How many Subnet bits:

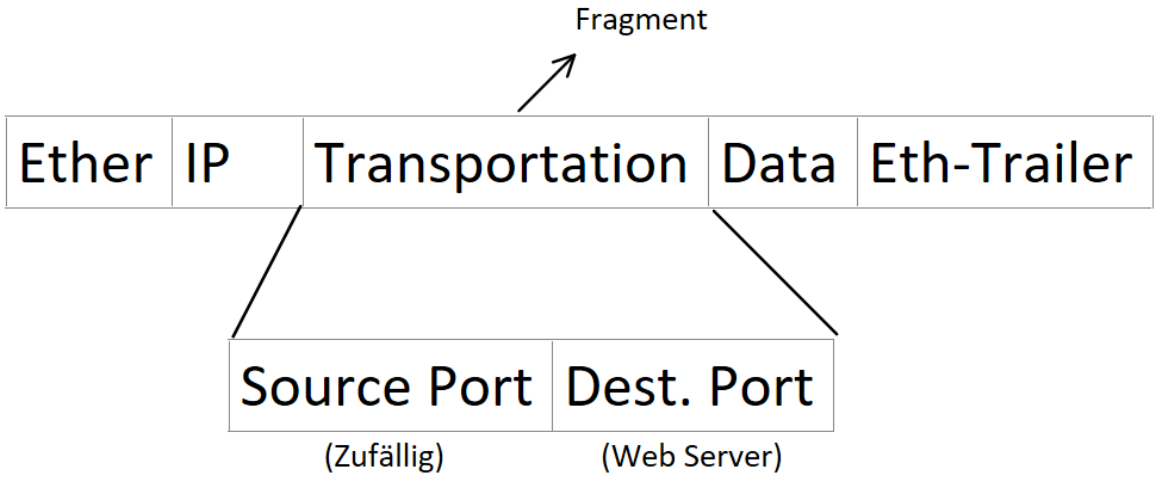
A: 24bit
B: 16bit
C: 8bit

192. … stands for a C-class network.
128. … stands for a B-class network.

1.3.2 Common terms

Term	Meaning
TTL (Time to live)/ Hop count, 1 Byte	How many times a packet can be forwarded.
IPv4 Packet Header, 8 bytes	Source & Destination IP, each 4 bytes.
IPv6 Packet Header, 16 bytes	Source & Destination IP, each 8 bytes.
Last resort route	Destination if initial destination address wasn't found.
Static route	Configure everything manually (hardcode path). • Recommended if only one way exists. • Requires less resources. • More secure
Dynamic route	Configures automatically. • Requires more performance. • Data flow not always traceable.

1.4 Transport Layer



1.5 Session Layer

1.6 Presentation Layer

1.7 Application Layer

2 Cisco commands

2.1 General information

startup-config

This is the saved configuration file that is stored in NVRAM. It contains all the commands that will be used by the device upon startup or reboot. Flash does not lose its contents when the device is powered off.

running-config

This is stored in RAM. It reflects the current configuration. Modifying a running configuration affects the operation of a Cisco device immediately. RAM is volatile memory.

To save changes made to the running configuration to the startup configuration file, use:
copy running-config startup-config
in privileged EXEC mode.

Terminal	Description	How to change
Router>	User EXEC mode	
Router#	Privileged EXEC mode	Enable (en) / disable
Router(config)#	Configuration mode (in privileged EXEC mode)	Conf t / exit
Router(config-if)#	Interface config	Interface <int-id>
Router(config-line)#	Line level (vty, tty, async) within configuration	Line <line id>
Router(config-router)#	Routing engine level within configuration mode	

2.2 Basic Switch Config

Set hostname.

```
hostname [hostname]
```

Secure privileged EXEC mode.

```
enable secret [secret]
```

Secure user EXEC mode.

```
line console 0
password [password]
login
```

Secure all passwords in the config file.

```
service password-encryption
```

Set minimum password length.

```
security passwords min-length
```

Disable inactive EXEC mode.

```
exec-timeout [time]
```

Set MOTD banner.

```
banner motd [msg]
```

Configure default gateway.

```
ip default-gateway [192.168.10.1]
```

Secure remote Telnet/SSH access.

```
line vty 0 15
password [passwd]
login
```

2.3 Basic Router Config

See chapter 2.2 but without default gateway.

2.4 Show Commands

Command	Description
Show running-config	Verifies the current configuration and settings.
Show interfaces	Verifies the interface status and displays any error messages.
Show ip interface	Verifies the Layer 3 information of an interface.
Show arp	Verifies the list of known hosts on the local Ethernet LANs
Show ip route	Verifies the Layer 3 routing information
Show protocols	Verifies which protocols are operational
Show version	Verifies the memory, interfaces, and licenses of the device.
Show … brief	Shows shortened version
<cmd> ?	Displays help message

2.5 Securing a router

Secure all passwords in the config file.

```
service password-encryption
```

Set password min length.

```
security password min-length [8]
```

Block excessive login attempts.

```
login block-for [120] attempts [3] within [60]
```

Set a timeout for auto logout.

```
line vty 0 4
exec-timeout [10]
```

2.5.1 enabling SSH

Configure the IP domain name.

```
ip domain-name [spam.com]
```

Generate one-way-secret keys.

```
crypto key generate rsa general-keys modulus 4096
```

Verify or create a local database entry.

```
username [Bob] secret [cisco]
```

Enable VTY inbound SHH sessions.

```
line vty 0 4
transport input ssh
login local
```

Enable SSH Version 2.

```
ip ssh version 2
```

3 IPv4

3.1 Subnet masks

Makes a bitwise and operation on the IPv4 address to determine the network address.

CIDR Notation:

CIDR	DECIMAL	NETWORK BINARY	ADDRESSES
/16	255.255.0.0	FF.FF.0.0	65’534
/18	255.255.192.0	FF.FF.11000000.0	16’382
/20	255.255.240.0	FF.FF.11110000.0	4’094
/22	255.255.252.0	FF.FF.11111100.0	1022
/24	255.255.255.0	FF.FF.FF.0	254
/25	255.255.255.128	FF.FF.FF.10000000	162
/26	255.255.255.192	FF.FF.FF.11000000	62
/27	255.255.255.224	FF.FF.FF.11100000	30
/28	255.255.255.240	FF.FF.FF.11110000	14
/29	255.255.255.248	FF.FF.FF.11111000	6
/30	255.255.255.252	FF.FF.FF.11111100	2
/31	255.255.255.254	FF.FF.FF.11111110	0 (2)

4 IPv6

4.1 Common Terms

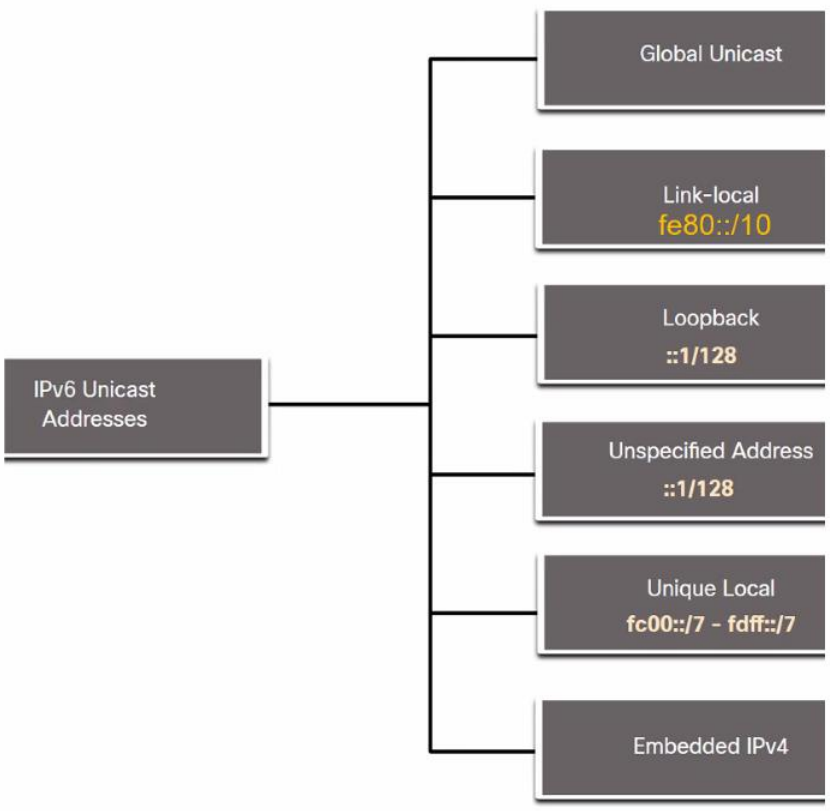
Term	Meaning
Dual stack	The devices run IPv4 and IPv6 protocol stacks simultaneously.
Tunnelling	Encapsulate an IPv6 packet into an IPv4 packet.
Translation	Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4.
Global Unicast	These are globally unique, Internet routable addresses.
Link-Local	Used to communicate with other devices on the same local link.
Unique Local	Used for local addressing within a site or between a limited number of sites.

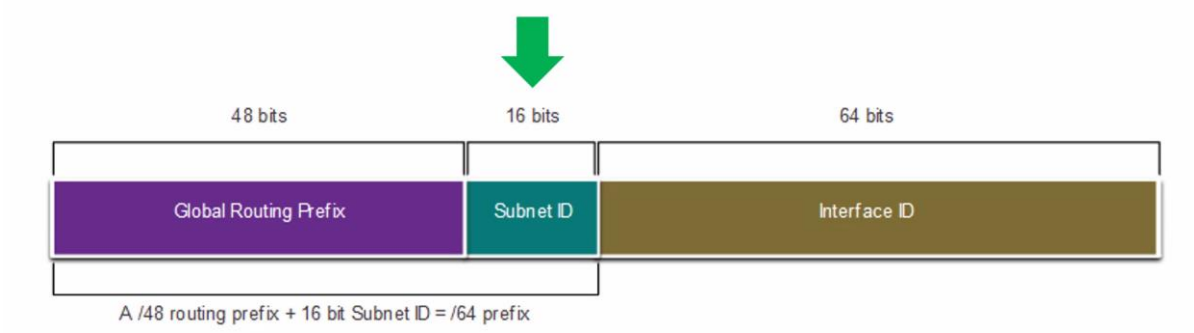
4.2 Simplify address

Type	Format
Preferred	2001 : **0**db8 : **000**0 : 1111 : **0000** : **0000** : **0000** : **0**200
Compressed	2001:db8:0:1111::200

4.3 Prefix

- range: from 0 to /128
- recommended: /64 (among other things because of SLAAC)





4.4 Multicast

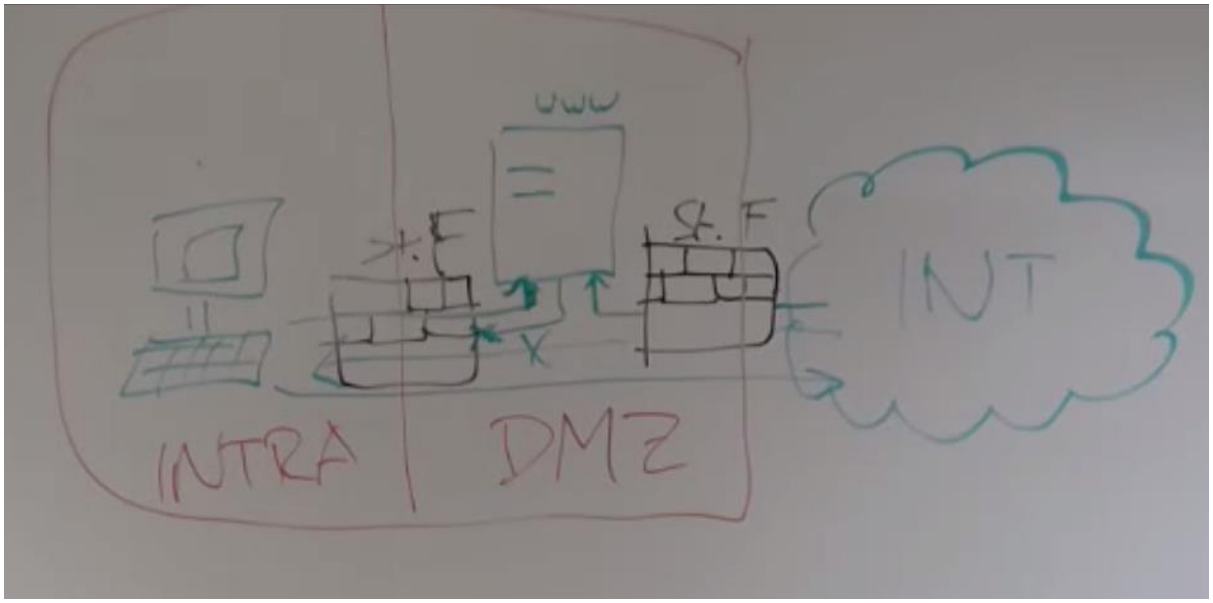
There are two common IPv6 multicast groups:

- **ff02::1**
  All-nodes multicast group
  multicast group that all IPv6-enabled devices join. A packet sent to this group is received and processed by all IPv6 interfaces on the link or network.
- **ff02::2**
  All-routers multicast group
  multicast group that all IPv6 routers join. A router becomes a member of this group when it is enabled as an IPv6 router with the ipv6 unicast-routing global configuration command.

5 Network Security Fundamentals

5.1 Stateful Firewall

Traffic from the Internet gets blocked unless it's a response from an inside request.



Split Network into two zones

- DMZ (Demilitarized zone) -> a server handling the responses from the internet and the requests from the Intranet
- Intranet -> not directly connected to the Internet and therefore not directly visible.

5.2 Type of Threats

1. Data Loss and manipulation
2. Information Theft
3. Identity Theft
4. Denial of service (DoS)

5.3 Types of Vulnerabilities

5.3.1 Technological

- TPC/IP – HTTP, FTP, ICMP
- OS Weakness
- Network equipment weakness

5.3.2 Configuration

- Unsecured user accounts (no/weak password).
- System accounts with easily guessed passwords.
- Misconfigured internet services (e.g. FTP has anonymous user -> no pw required).
- Unsecured default settings
- Misconfigured network equipment

5.3.3 Security policy

- Lack of written security
- Politics -difficult to implement a consistent security policy.
- Lack of authentication continuity – poorly chosen passwords.
- Logical access controls not applied – monitoring/logging.
- Software & Hardware changes – network changes and it's not secure anymore.
- Disaster recovery plan is non-existent – data center burns down, no one knows what to do.