Protocols and Services

IP sec

ESP

The IP Sec suite is a set of protocols that provide security for communications in the third layer of the OSI model.

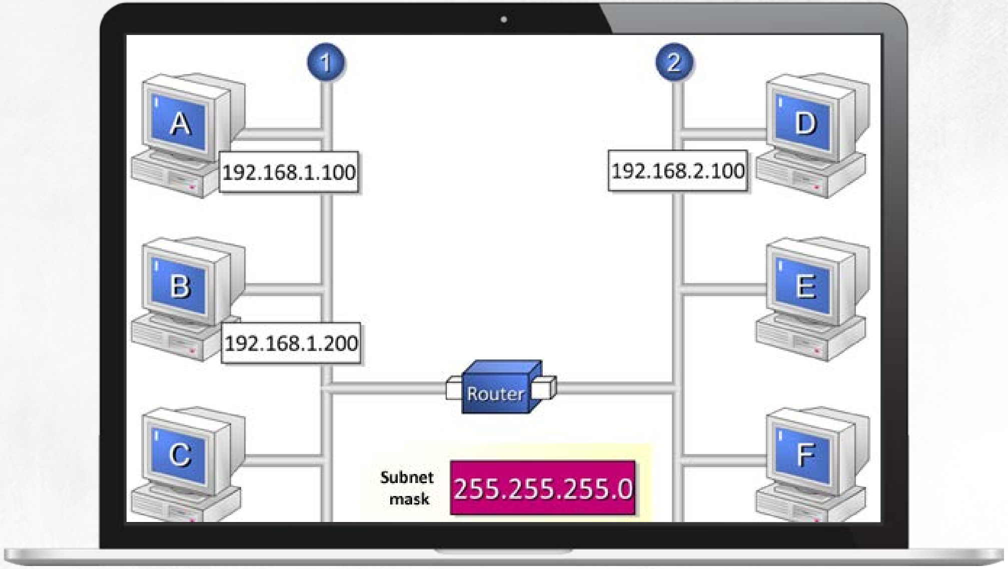
Unlike SSL, IP Sec operates at a lower layer of the OSI model and protects communications transparently and independently from web applications.

It also secures all communications between hosts, as opposed to only applying to transmissions made across selected applications

Subnetting

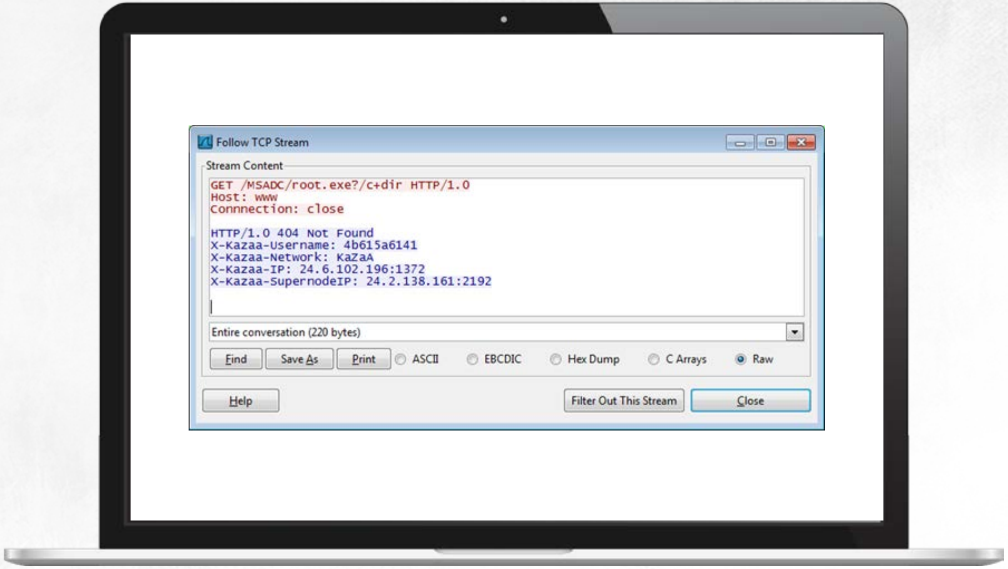
Using routers to subnet a network can mean:

- Better network performance (achieved through setting up data-exchanging computers in the subnetworks)
- Being able to monitor packets transmitted across routers
- Limit the availability and access to selected hosts



Subnetting

But if your subnets are connected through firewalls, you may be able to control traffic not only by filtering it based on source and destination IP addresses but also based on protocols and data sent across hosts



```
GET /MSADC/root.exe?/c+dir HTTP/1.0
Host: www
Connnection: close

HTTP/1.0 404 Not Found
X-Kazaa-Username: 4b615a6141
X-Kazaa-Network: KaZaA
X-Kazaa-IP: 24.6.102.196:1372
X-Kazaa-SupernodeIP: 24.2.138.161:2192
```

Entire conversation (220 bytes)

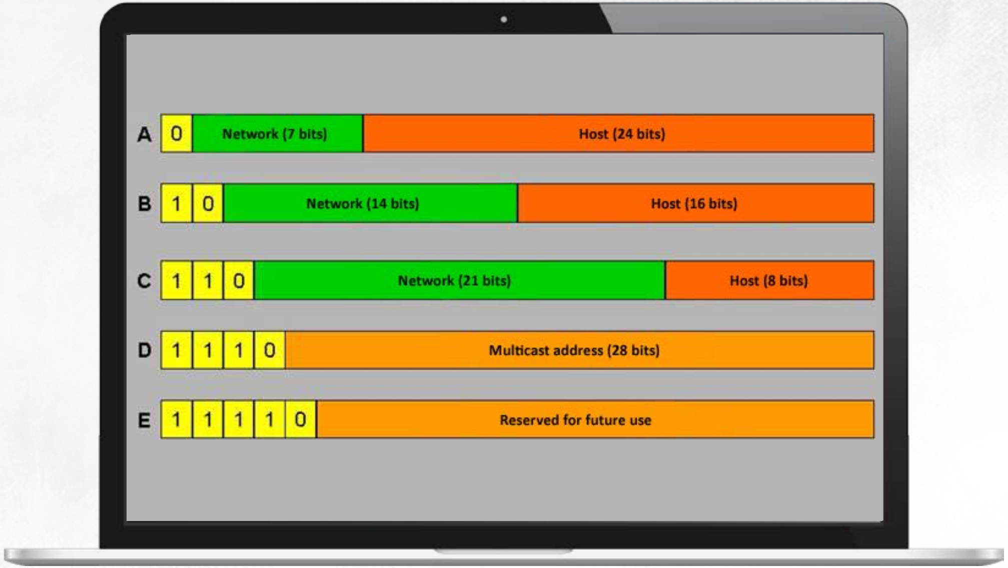
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Subnetting

IPv4

IPv4 address classes:

The value in an IPv4 address's first octet categorizes it into a specific class



A | 0 | Network (7 bits) | Host (24 bits)

B | 1 | 0 | Network (14 bits) | Host (16 bits)

C | 1 | 1 | 0 | Network (21 bits) | Host (8 bits)

D | 1 | 1 | 1 | 0 | Multicast address (28 bits)

E | 1 | 1 | 1 | 1 | 0 | Reserved for future use

Subnetting

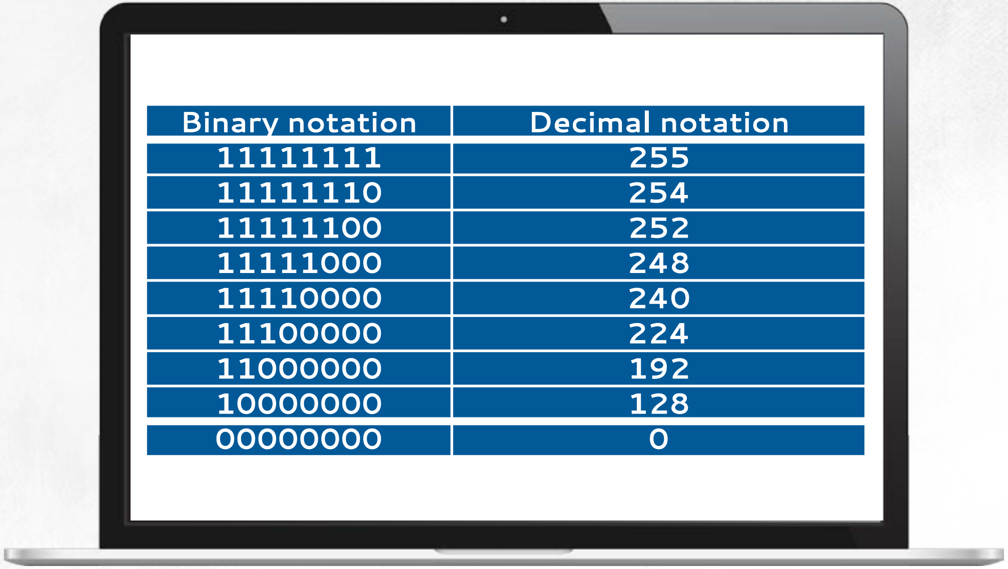
IPv4

CIDR :

In a valid subnet mask set bits are on the left side of the first non-set bit

Every octet in a subnet mask may be set to one of nine values

CIDR notation lets you split a single network into many subnets and connect them in one supernet



Binary notation	Decimal notation
11111111	255
11111110	254
11111100	252
11111000	248
11110000	240
11100000	224
11000000	192
10000000	128
00000000	0

Subnetting

IPv6

Current operating systems use both versions of IP by default: unfortunately, most firewalls and network intrusion detection systems support IPv6 only in a limited way

The conspicuous change is lengthening the IP address from 32 (v4) to 128 bits (v6). Longer addresses required a new notation system to be developed: rather than have octets divided with a dot, IP addresses have four-character groups of hexadecimals

Subnetting

IPv6

Unlike IPv4 addressing, IPv6 notation does not use variable-length network masks. Instead, the first half of the address (the old 64 bits) includes a network-identifying prefix (used to route packets), while the other half (the new 64 bits) is a host address. A network-identifying prefix can be further split into a 48-bit network prefix and a 16-bit subnet identifier. This means that all IPv6 networks can be subnetted into 65,536 subnetworks (216 = 65,536)

subnetting

IPv6

To improve readability, you can use these techniques for IPv6 notation:

- Replace groups of zeroes with single zeroes

  2001:0db8:0000:0000:0000:0000:1428:57ab → 2001:0db8:0:0:0:0:1428:57ab

- Skip groups of zeroes and replace them with a colon

  2001:0db8:0:0:0:0:1428:57a → 2001:0db8::1428:57ab

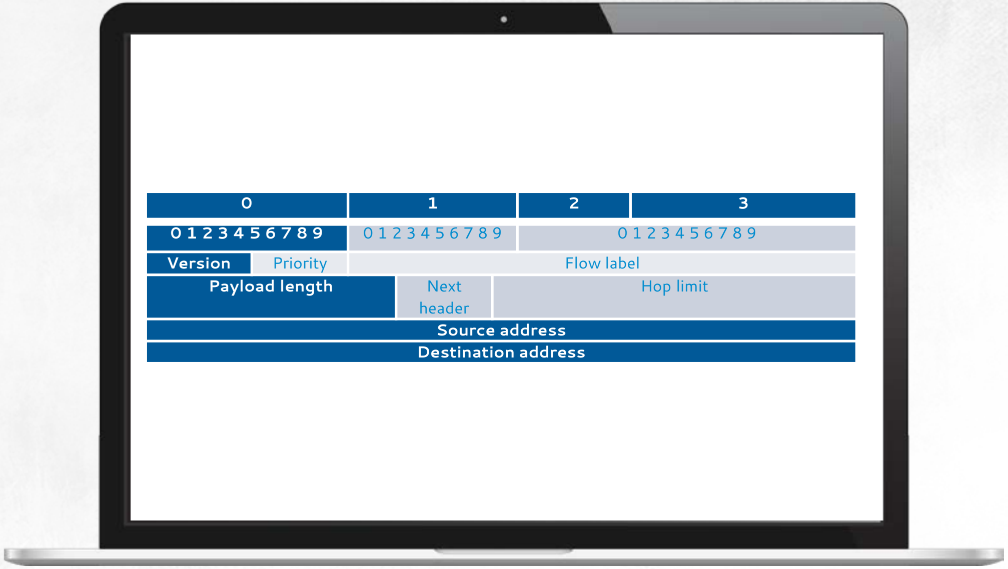
- Skip the leading zeroes

  2001:0db8::1428:57ab → 2001:db8::1428:57ab

Subnetting

IPv6

Extending the IP address space meant the IPv6 header format needed an upgrade. The datagram in version 6 consists of the basic IP header and is followed by optional other headers



0 | 1 | 2 | 3

0 1 2 3 4 5 6 7 8 9 | 0 1 2 3 4 5 6 7 8 9 | 0 1 2 3 4 5 6 7 8 9

Version | Priority | Flow label

Payload length | Next header | Hop limit

Source address

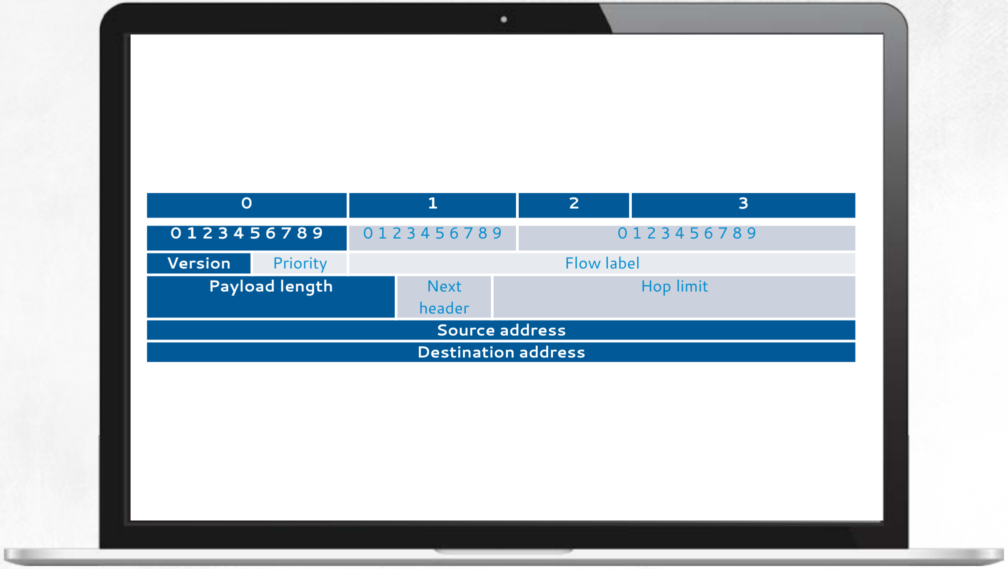
Destination address

Subnetting

IPv4

IPv6 addressing:

- The ::1 loopback address is equivalent to the 127.x.y.z IPv4 address and points back to the local computer
- Multicast addresses can be used to send packets to multiple computers at a time
- Unicast local addresses are equivalent to the 169.254.x.y IPv4 addresses
- Unique local addresses are equivalent to IPv4 private addresses
- Global addresses are equivalent to IPv4 public addresses



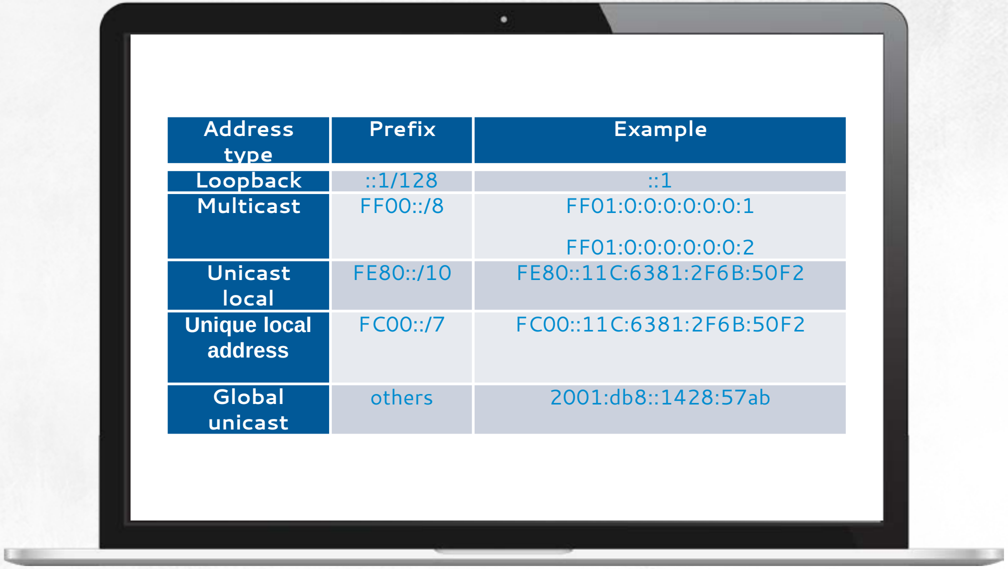
0	1	2	3
0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	
Version Priority	Flow label		
Payload length	Next header	Hop limit	
Source address			
Destination address			

Subnetting

IPv6

Subnetting IPv6 networks is easy. It’s enough to change the subnet identifier values separated by the : character, for example subnet the 2637:F238/32 network into the following subnetworks:

- 2607:F238:0000/48,
- 2607:F238:0001/48,
- 2607:F238:0002/48,
- 2607:F238:0009/48,
- 2607:F238:000a/48,
- etc.

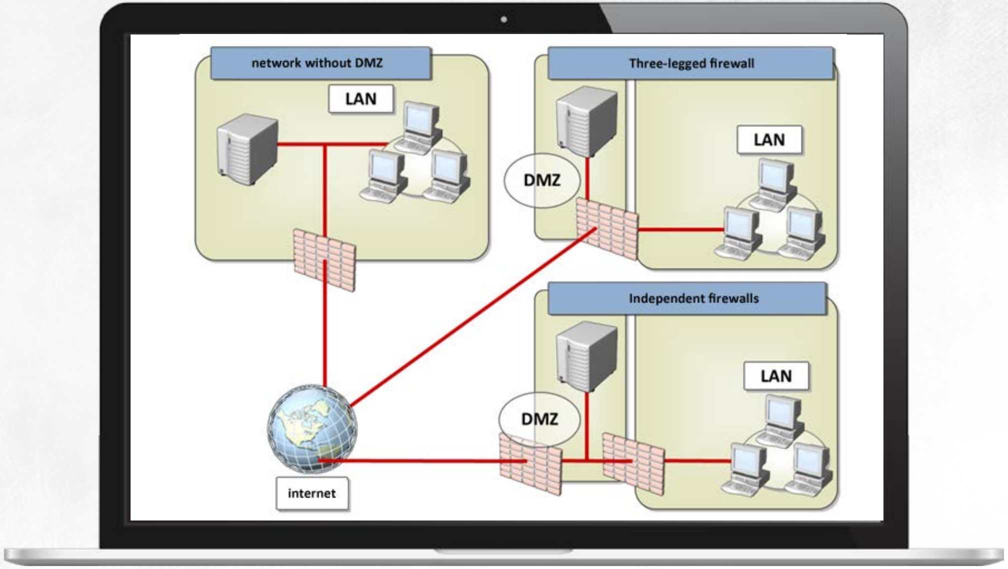


Address type	Prefix	Example
Loopback	::1/128	::1
Multicast	FF00::/8	FF01:0:0:0:0:0:0:1 FF01:0:0:0:0:0:0:2
Unicast local	FE80::/10	FE80::11C:6381:2F6B:50F2
Unique local address	FC00::/7	FC00::11C:6381:2F6B:50F2
Global unicast	others	2001:db8::1428:57ab

DMZ

If your computer system has some services that must be available online for the general public, you may find that one set of firewall access rules for all networked computers will not give you effective security

One solution is to place all computers that provide online services in a single subnet (a demilitarised zone) and setting up a firewall to separate it both from the Internet and from all other subnets

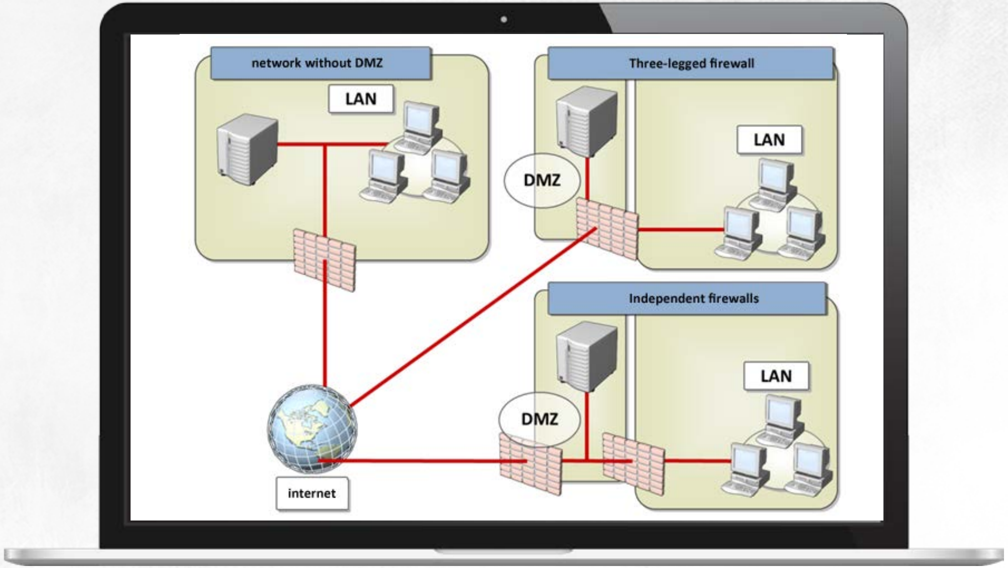


IT SECURITY ACADEMY
www.SecAcademy.com

DMZ

A DMZ may be created using one firewall with three network interfaces (a single-firewall DMZ architecture) or using two independent firewalls (a dual firewall DMZ architecture)

All hosts in a DMZ are high-risk



vlan

VLANs operate in the second OSI layer. This subnetting makes use of switches of this layer, not routers

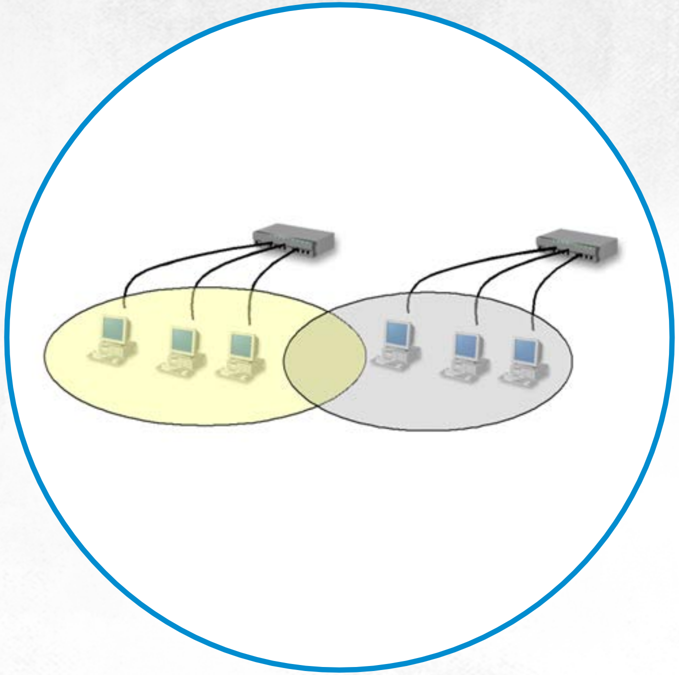
Since computers connected to the same switch or hub form a segment, why not use the ports of these devices for dividing networks into segments?

Both operations yield the same results. All computers inside a segment can communicate directly but cannot send Ethernet frames to hosts in a different segment

VLAN is a however only a logical division

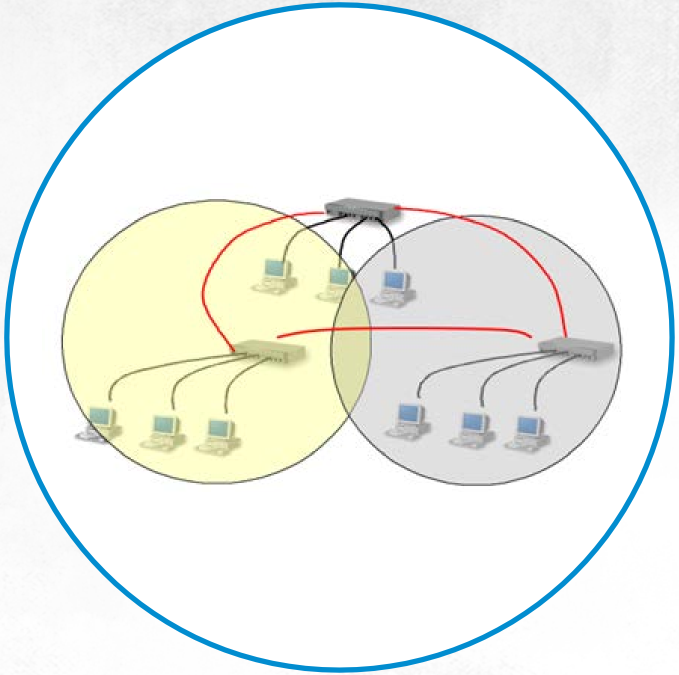
Dividing the network into virtual LANS may help you to:

- Reduce traffic
- Adjust network topology to your company's structure



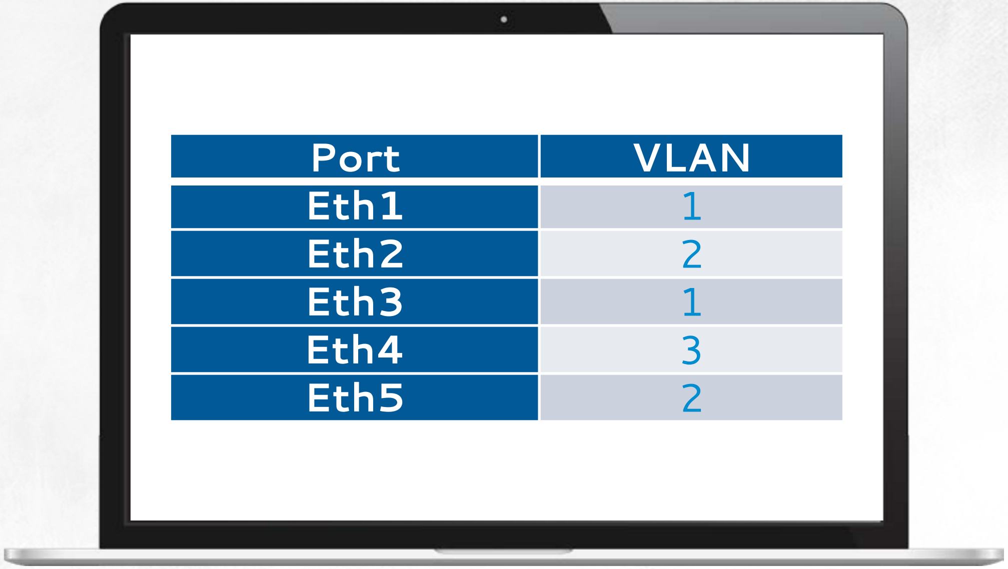
vlan

Even if the VLAN technology wasn’t designed to be a network security measure, implementing it may help you reduce the scope of potential attacks that can be executed in the second layer of the OSI model



VLAN

The simplest way to segment is to configure switch ports. This is how you create static VLANs

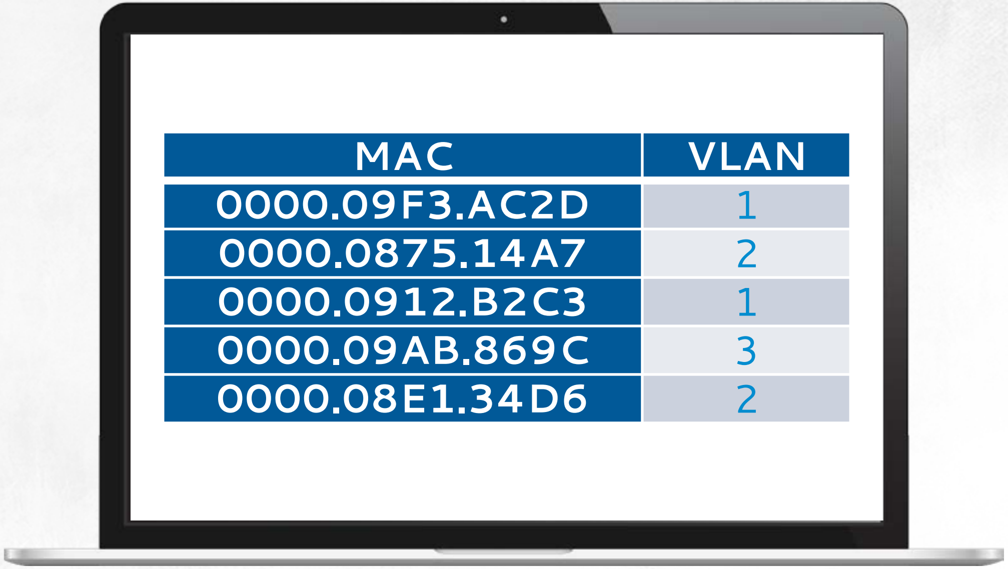


Port	VLAN
Eth1	1
Eth2	2
Eth3	1
Eth4	3
Eth5	2

VLAN

You can also dynamically assign hosts (using their MAC addresses for example) to segments, creating dynamic VLANs

To only send frames to an intended VLAN and enabling them to be sent to hosts in the same VLAN but connected to different switches requires you to tag Ethernet frames with VLAN IDs and enable all frames to be sent across switches (trunk ports can be used for this purpose)

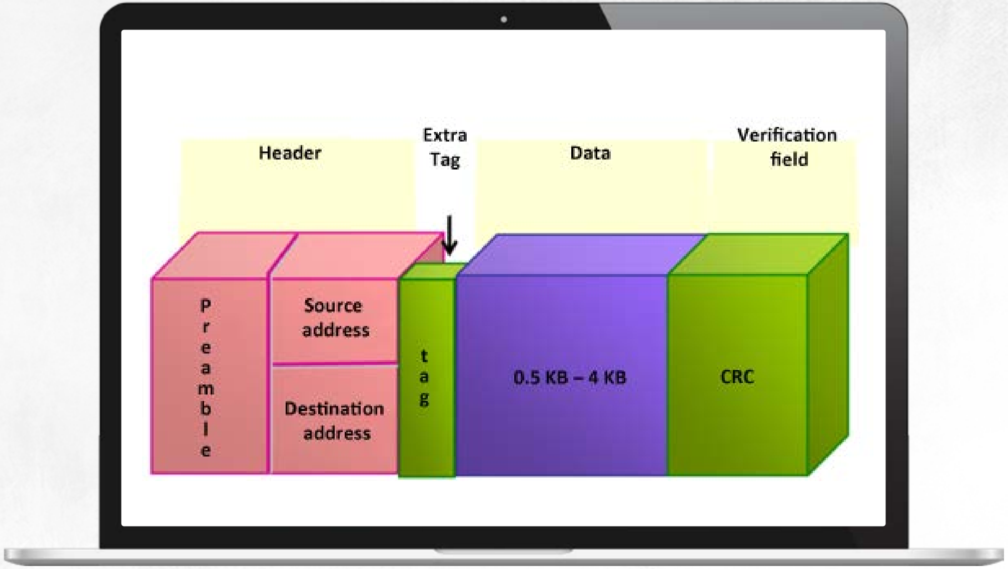


MAC	VLAN
0000.09F3.AC2D	1
0000.0875.14A7	2
0000.0912.B2C3	1
0000.09AB.869C	3
0000.08E1.34D6	2

VLAN

This solution is defined in the IEEE 802.1Q standard

Network device manufacturers use also proprietary solutions, for example Cisco uses ISL and 3Com uses VLT



THANKS

IT SECURITY ACADEMY

www.SecAcademy.com