IPv6, Datagram Headers and VLAN

Dr. G. Omprakash

Assistant Professor, ECE, KLEF

Internet Protocol: IPv6

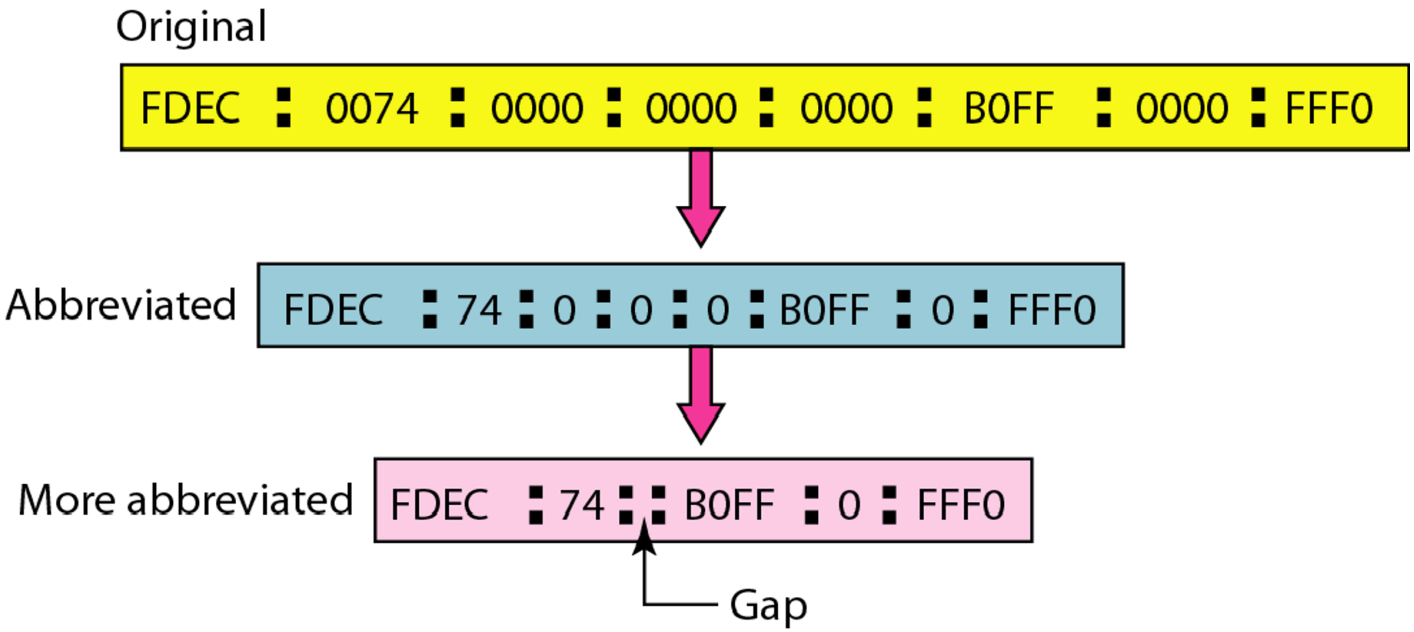
- IPv6 was developed to deal with the problem of IPv4 exhaustion.
- IPv6 uses 128-bit addresses; So address space is 2^{128}
- IPv6 use Hexa-Decimal format separated by colon (:)
- Notation:
  - Colon hexadecimal: FEF6:BA98:7654:3210:ADEF:BBFF:2922:FF00
  - Binary (128 bits): 1111111011101101011 ... 1111111100000000

IPv6

Major goals in the new protocol

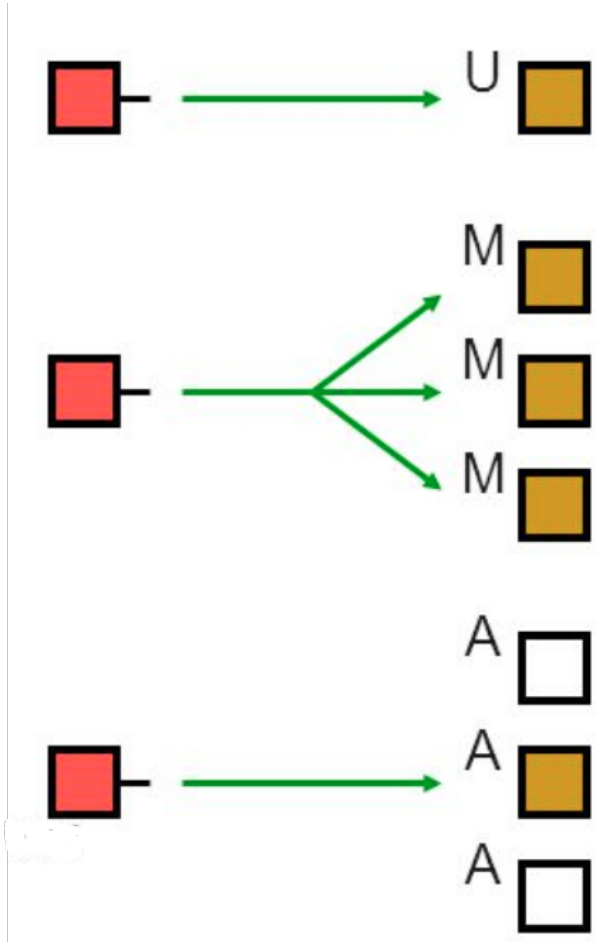
- Larger address space
- Reduce the size of the routing tables.
- Better header format
- Support for more security
- Support for resource allocation
- Make it possible for a host to roam without changing its address.
- Allow the protocol to evolve in the future.
- Permit the old and new protocols to coexist for years

Abbreviation



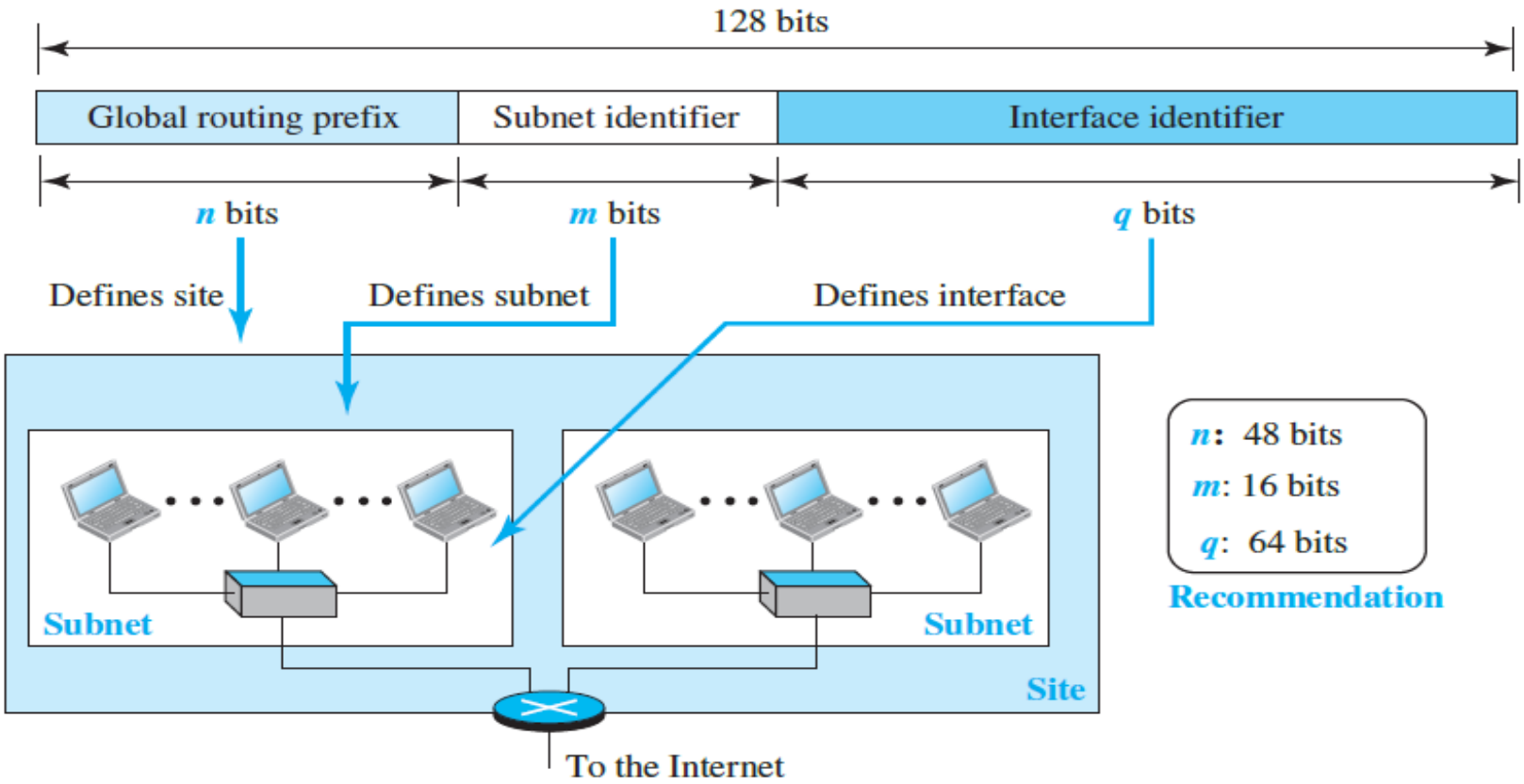
- The leading zeros of a section can be omitted
  - 0074 can be written as 74, 000F as F, 0000 as 0.
- Zero compression: if there are consecutive sections consisting of zeros only
  - This type of abbreviation is allowed only once per address
    - If there is more than one run of zero sections, only one of them can be compressed.

- Expand the address 0:15::1:12:1213 to its original.
- 0000:0015:0000:0000:0000:0001:0012:1213



In IPv6, a destination address can belong to one of three categories:

- **Unicast**: The packet sent to a unicast address will be routed to the intended recipient.
  - A unicast address defines a single interface (computer or router).
- **Anycast**: An anycast address defines a group of computers that all share a single address
  - A packet with an anycast address is delivered to only one member of the group, the most reachable one
  - An anycast communication is used, for example, when there are several servers that can respond to an inquiry
- **Multicast Address** also defines a group of computers
  - In multicasting each member of the group receives a copy of the packet


128 bits
Global routing prefix
Subnet identifier
Interface identifier
n bits
m bits
q bits
Defines site
Defines subnet
Defines interface
Subnet
Subnet
Site
To the Internet
n: 48 bits
m: 16 bits
q: 64 bits
Recommendation

IPv4 Datagram Header

IPv4 defines the format of a packet in which the data coming from the upper layer are encapsulated

- Packets used by the IP are called **datagrams**
- A datagram is a variable-length packet
  - consists of two parts: **Header** and **Payload**.
- Header is 20 to 60 bytes in length
  - first 20 bytes are essential
    - contains information essential to routing and delivery

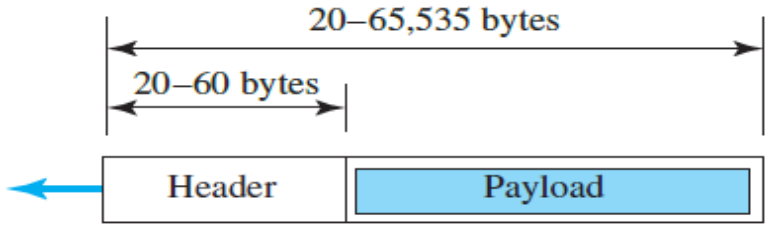
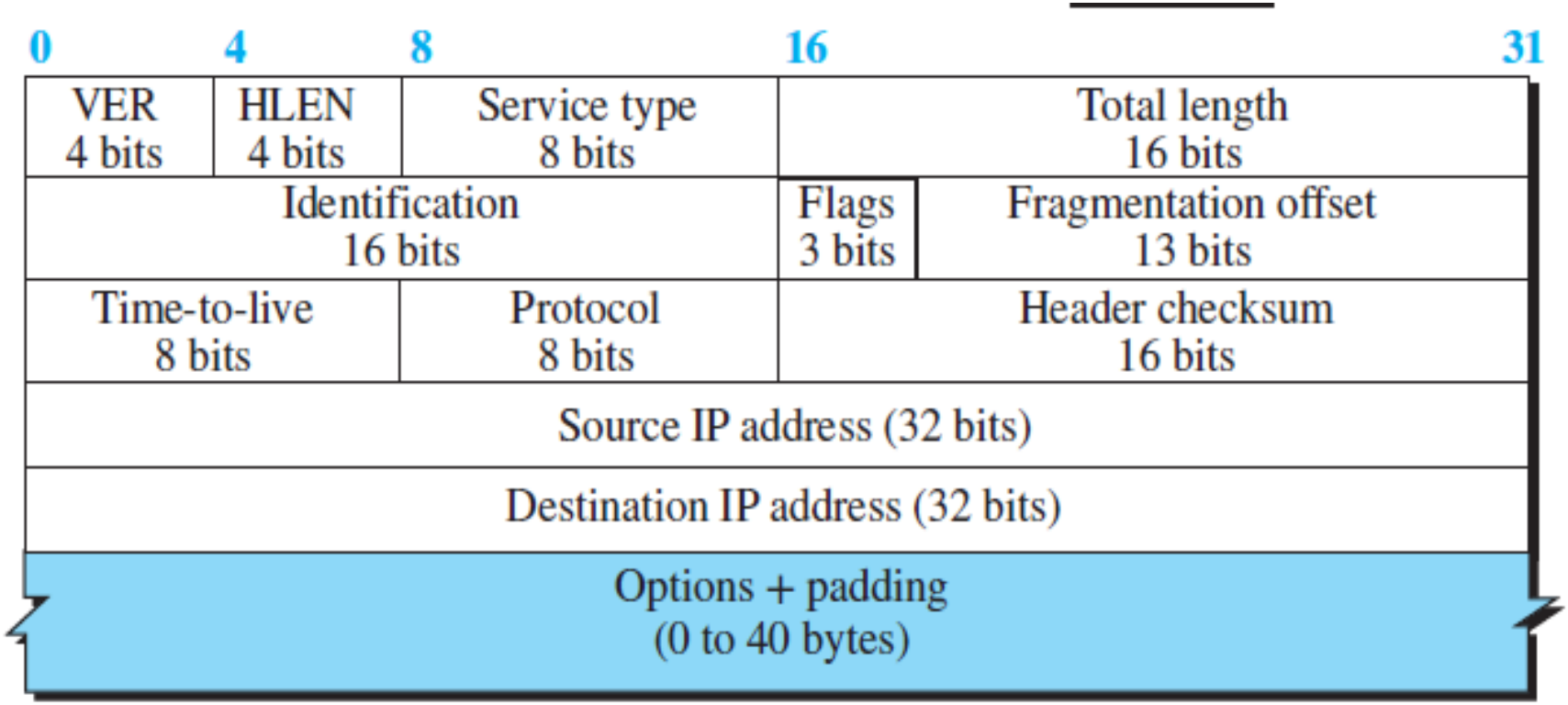


Figure: IP Datagram

IPv4 Datagram Header



IPv4 Datagram Header

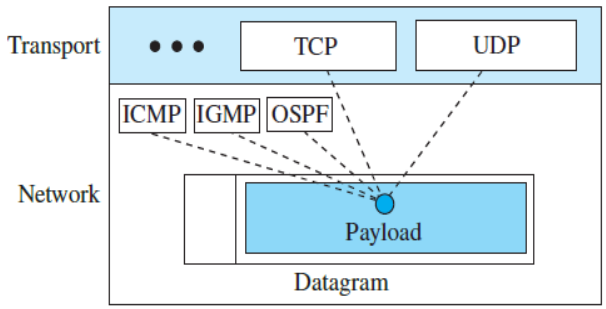
- **Version number (VER)**: Defines the version No of the protocol
- **Header Length (HLEN)**:Defines the total length of the datagram header (20-60 bytes)
  - Minimum value: 20/4=5; Maximum value: 60/4=15
- **Service type**: Divide applications into different classes according to their priority
  - Redefined in 1990 as *DiffServ* **Differentiated Services**
    - 3 bits: signal priority;
    - 3 bits to signal if host cared more about delay, throughput, or reliability
    - 2 bits : To carry congestion notification information
- **Total Length**: 16-bit field defines the total length (header plus data) of the IP datagram in bytes.
  - Maximum length is 65,535 bytes

IPv4 Datagram Header

- **Identification**: This allows the destination host to determine which packet a newly arrived fragment belongs to.
  - All the fragments of a packet contain the same Identification value.
- Unused bit: proposed using this bit to detect malicious traffic
- **(DF) Don't Fragment**: It was intended to support hosts incapable of putting the fragments back together again
- **(MF) More Fragments**: To know when all fragments of a datagram have arrived.
  - All fragments except the last one have this bit set.
- **Fragmentation offset** tells where in the current packet this fragment belongs
  - There is a maximum of 8192 (2^{13}) fragments per datagram

IPv4 Datagram Header

- **TTL (Time to live)** field is a counter used to limit packet lifetimes.
  - Maximum lifetime of $2^8 = 255$sec
    - Decremented on each hop/queued for a long time in a router
    - This feature prevents packets from wandering around forever
- **Protocol**: This field tells receiver which transport process to give the packet to.

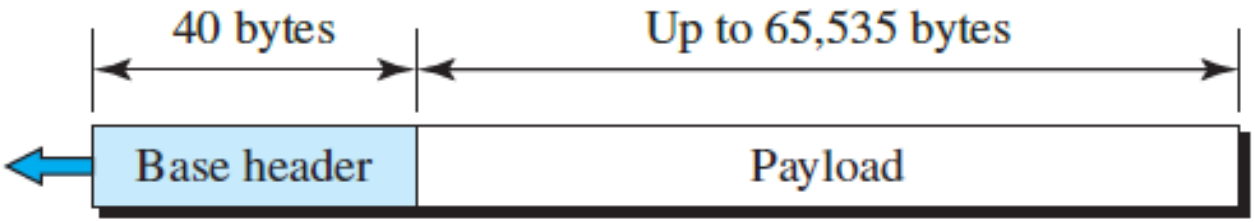


Some protocol values

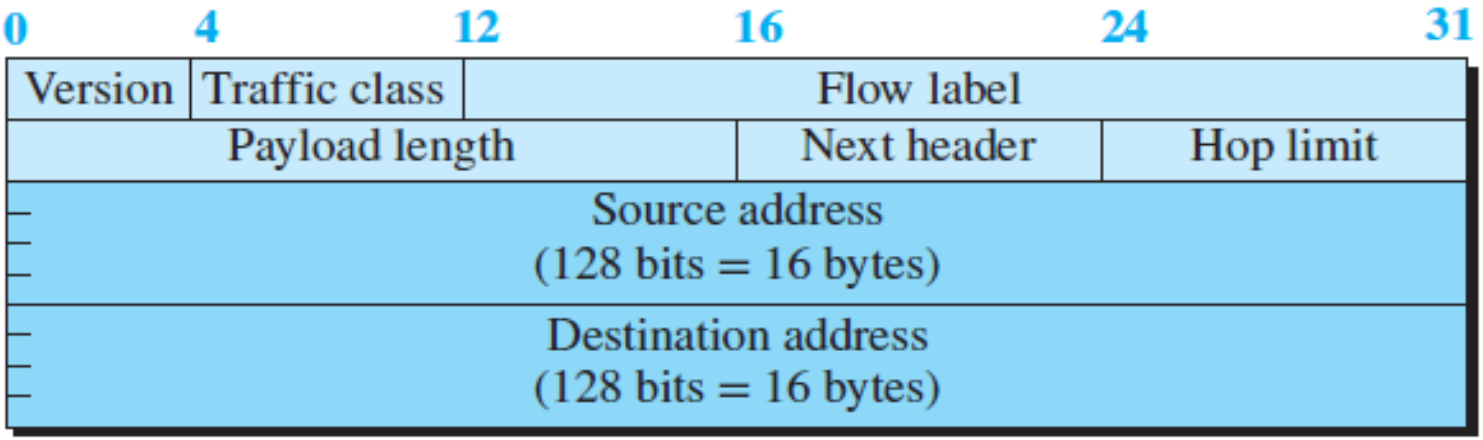
ICMP	01
IGMP	02
TCP	06
UDP	17
OSPF	89

- **Header Checksum**: The header carries vital information such as addresses, it rates its own checksum for protection.
  - add up all the 16-bit halfwords
  - It must be recomputed at each hop
- The **Source address** and **Destination address** indicate the IP address of the source and destination network interfaces
- **Options field** Designed to provide subsequent versions of the protocol to include information not present in the original design

IPv6 Datagram Header



a. IPv6 packet



b. Base header

IPv6 Datagram Header

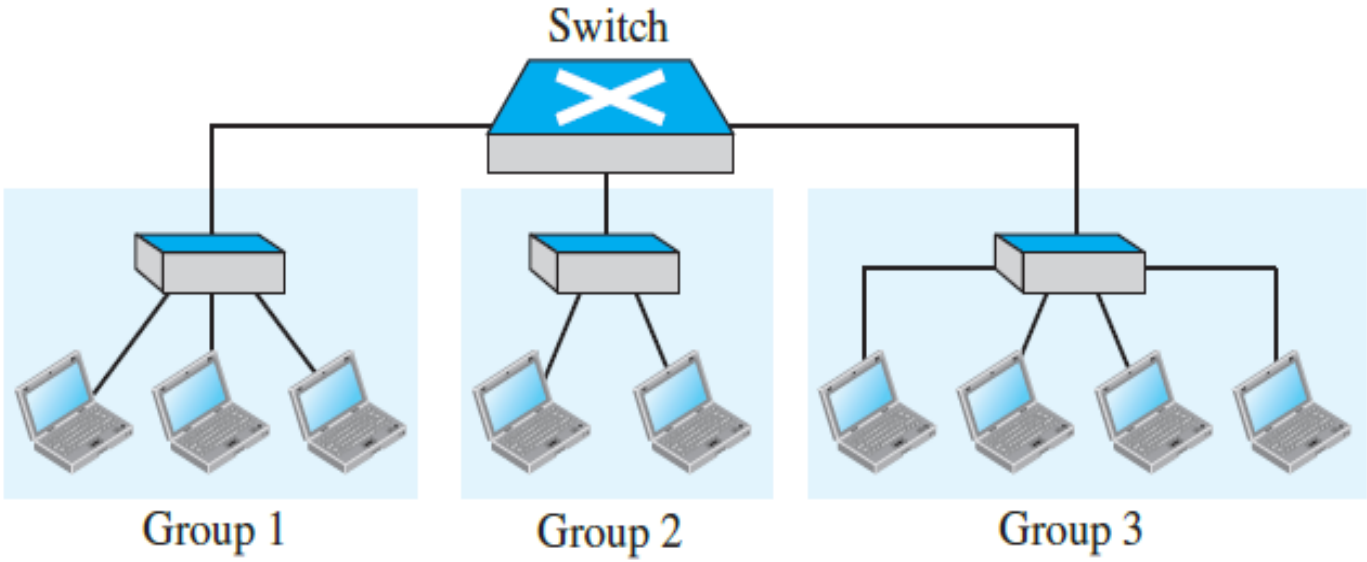
- **Version**: The 4-bit version field defines the version number (value: 6)
- **Traffic class** now called **Differentiated Services**
  - 3 bits: signal priority;
  - 3 bits to signal if host cared more about delay, throughput, or reliability
  - 2 bits : To carry congestion notification information
- **Flow label** To mark a group of packets which need reserved bandwidth.
  - Due to stringent delay requirements
  - Routers give special treatment to packets based on *Flowlabel*
- **Payload length** field tells how many bytes follow the 40-byte header
  - changed from the IPv4 *Total length*

- The **Next header** field tells which transport protocol handler (e.g., TCP, UDP) to pass the packet to.
- The **Hop limit** field is used to keep packets from living forever
  - Similar to *Time To Live* in IPv4
- **Source and destination address**: Source/destination address field is a 16-byte (128-bit) Internet address that identifies the source/destination

Virtual LANS

- A station is considered part of a LAN if it physically belongs to that LAN
- If we need a virtual connection between two stations belonging to two different physical LANs?
  - Define a **virtual local area network (VLAN)** (using software)
- The idea of VLAN technology is to divide a LAN into logical segments, instead of physical segments

VLAN Example



- LAN in an engineering firm in which 10 stations are grouped into three LANs that are connected by a switch.
- if the administrators needed to move two engineers from the first group to the third group, to speed up the project being done by the third group?
- Should we change LAN configuration? $\Longrightarrow$ Do rewiring?

Virtual LAN

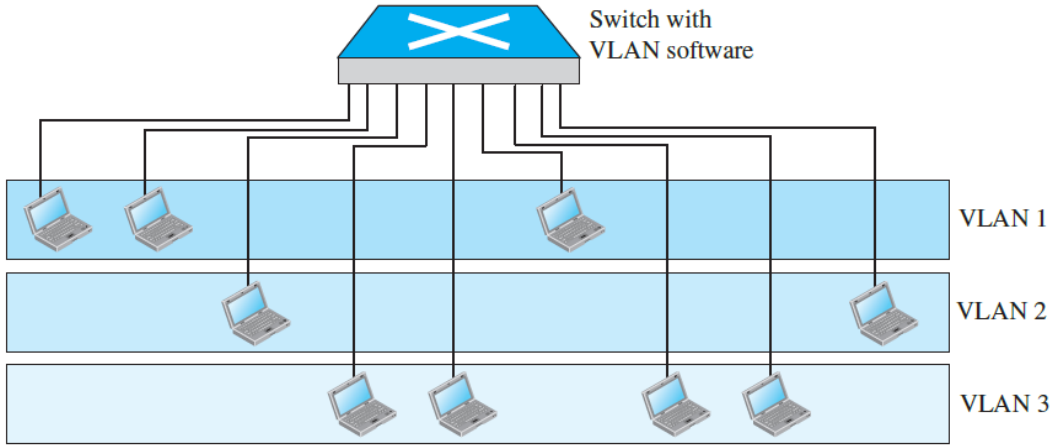
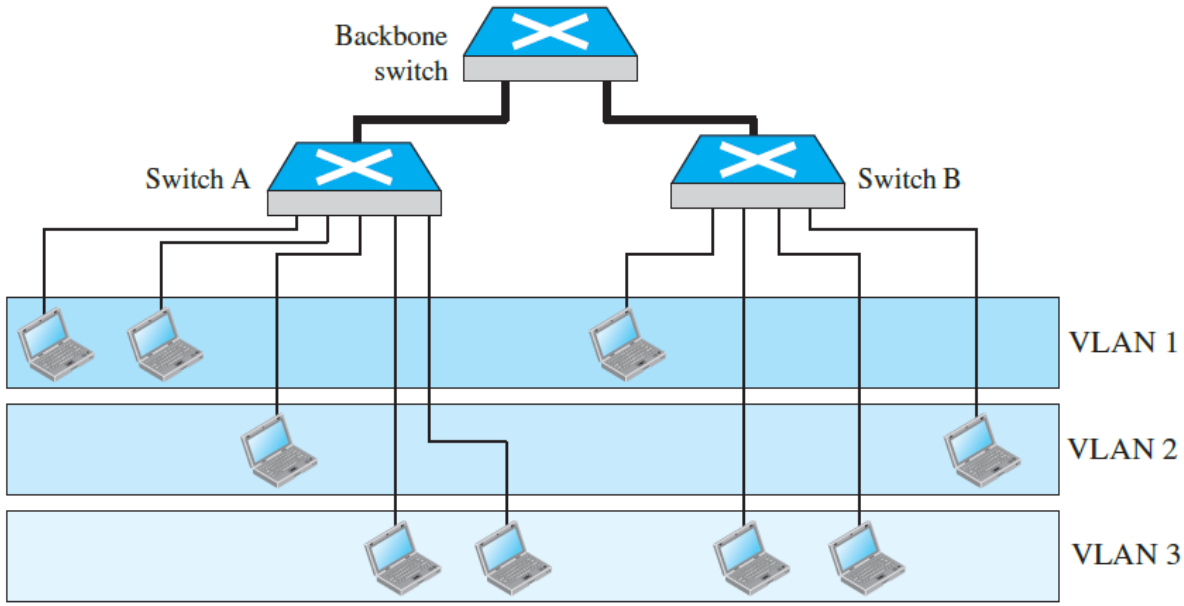


Figure: Switch using VLAN software

- Solution: Divide the LAN into logical segments, instead of physical segments
- All members belonging to a VLAN can receive broadcast messages sent to that particular VLAN
  - If a station moves from VLAN 1 to VLAN 2, it receives broadcast messages sent to VLAN 2
    - but no longer receives broadcast messages sent to VLAN 1.

Virtual LAN



- VLAN technology even allows the grouping of stations connected to different switches in a VLAN.
- Configuration for a company with two separate buildings. Each building can have its own switched LAN connected by a backbone

Ports in VLAN

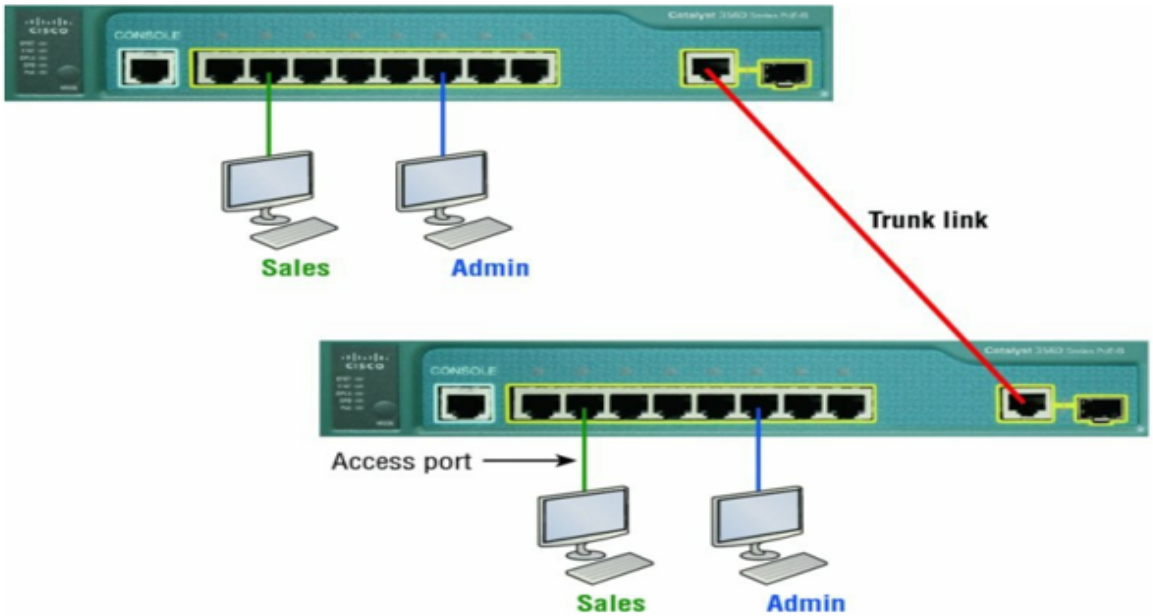


Figure: VLANs can span across multiple switches by using trunk links, which carry traffic for multiple VLANs

Ports in VLAN

- **Access Ports**:
  - An access port belongs to and carries the traffic of only one VLAN
  - Traffic is both received and sent in native formats with no VLAN tagging
  - Anything arriving on an access port is simply assumed to belong to the VLAN assigned to the port.
  - Switches remove any VLAN information from the frame before it's forwarded out to an access-link device
- **Trunk Ports**[1]
  - Trunk ports can carry multiple VLANs at a time.
  - A trunk link is a 100, 1,000, or 10,000 Mbps point-to-point link between
    - Two switches
    - Between a switch and router
    - Between a switch and server

[1] term trunk port was inspired by the telephone system trunks, which carry multiple telephone conversations at a time

Frame Tagging

Frame tagging in VLANs is a mechanism used to identify and differentiate VLAN traffic within a network.

The two most commonly used frame tagging standards are

- IEEE 802.1Q : Industry-standard frame tagging protocol for VLANs
  - Add a pair of 2-byte fields to ethernet header
  - Pri: User priority field (3 bits); CFI: Canonical Identifier format (1-bit)
  - VLAN ID (13-bit)
- ISL (Inter-Switch Link): Add 26-byte header to Ethernet frame
  - primarily used in Cisco networking environments (now replaced with 802.1Q)

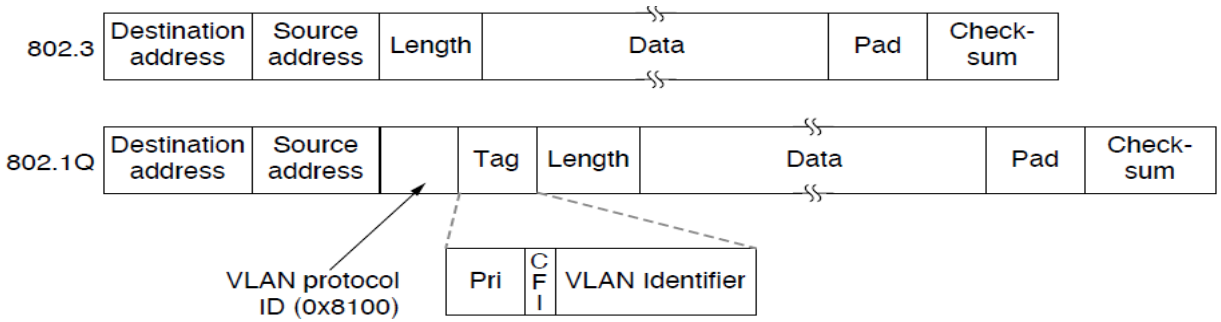


Figure: 802.3 (legacy) and 802.1Q Ethernet frame formats.

VLAN Membership

Vendors use the following characteristics to group VLAN

- **Interface Numbers**: Vendors use switch interface numbers as a membership characteristic
  - Stations connecting to ports 1, 2, 3, and 7 belong to VLAN 1
  - Stations connecting to ports 4, 10, and 12 belong to VLAN 2
- **MAC Addresses**: Vendors use the 48-bit MAC address as a membership characteristic
  - Admin can stipulate that stations having MAC addresses E2:13:42:A1:23:34 and F2:A1:23:BC:D3:41 belong to VLAN 1.
- **Combination**: The admin can choose one or more characteristics to define VLANs

Advantages of VLAN

- **Cost and Time Reduction**: VLANs can reduce the migration cost of stations going from one group to another. Physical reconfiguration takes time and is costly
- **Creating Virtual Work Groups**: For example, in a campus environment, professors working on the same project can send broadcast messages to one another without the necessity of belonging to the same department
- **Security**: VLANs provide an extra measure of security. People belonging to the same group can send broadcast messages with the guaranteed assurance that users in other groups will not receive these messages.

Acknowledge various sources for the images.
Thankyou