# Why IPv6 ?

## (Focus on Important Features of IPv6)

**B.K.NATH**

Director(TERM)
Himachal Pradesh, Shimla

(Ph : 2621999, Email : dirtermhp-dot@nic.in)

# What is an IP address?

- Each host on a TCP/IP network is uniquely identified at the IP layer with an address.
- An Internet Protocol (IP) address specifies the location of a host or client on the Internet.
- The IP address is also known as Protocol address
- The IPv4 address is 32 bits long
- The IPv6 address is 128 bit long

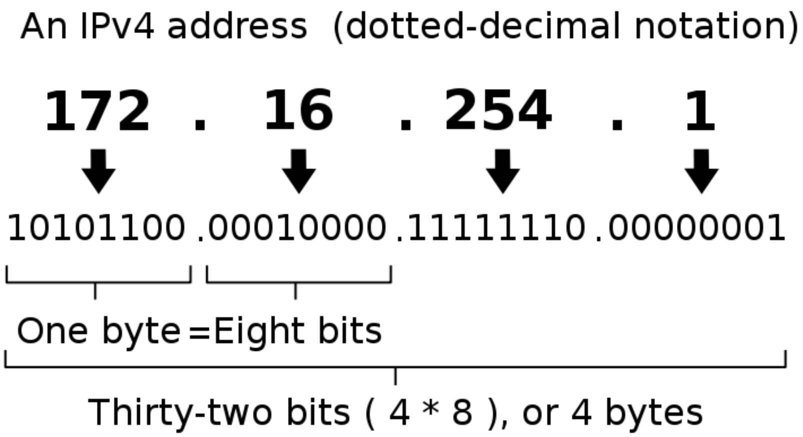
# Problems of IPv4

1. Addressing problem
2. Routing Crisis
3. End to End problem
4. Security
5. Mobility
6. Quality of Service (QoS)

# 1. Address Crisis

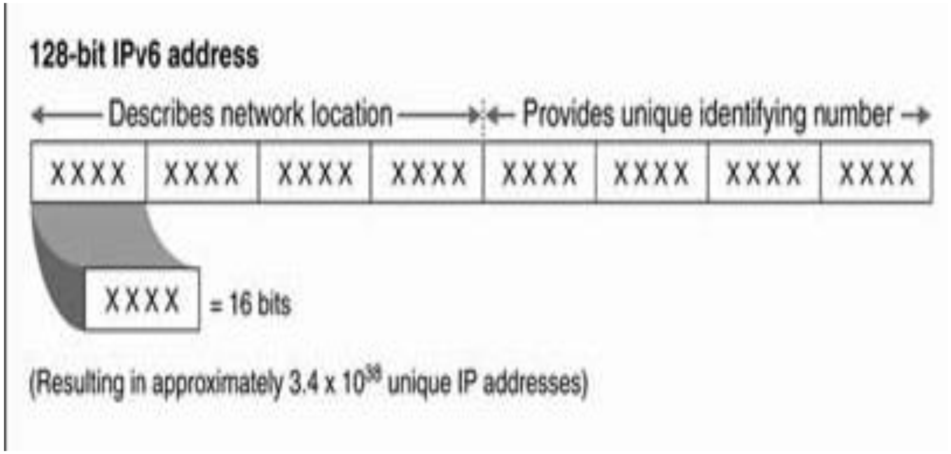
# IP Address Schemes

## IPV4 Address


An IPv4 address (dotted-decimal notation)
172 . 16 . 254 . 1
10101100 .00010000 .11111110 .00000001
One byte=Eight bits
Thirty-two bits ( 4 * 8 ), or 4 bytes

- Total Addresses = 2^32 = 4 billion
- Some addresses are reserved for special purposes like private networks or multicast addresses. However practicall only 250 million addresses are usable.

## IPV6 Address



(Resulting in approximately 3.4 x $10^{38}$ unique IP addresses)

Total Addresses = 2^128 = 340 billion, billion, billion, billion

5*10^28 addresses per person

No more room in IPv4

**Quite empty in IPv6**

# Larger Address Space

# IPv6 Address Types

- Unicast
  - Address is for a single interface (Packets sent to a unicast address are delivered to the node containing the interface identified by the address)
  - IPv6 has several types (for example: global unicast, IPv4 mapped, Local use unicast etc.)
- Multicast
  - One-to-many (Multicast addresses in IPv6 have the prefix ff00::/8)
  - Enables more efficient use of the network
- Anycast
  - One-to-nearest (allocated from unicast address space).
  - Multiple devices share the same address.
  - Source devices send packets to anycast address.
  - Routers decide on closest device to reach that destination.
  - Suitable for load balancing and content delivery services.

# IPv6 Address Scope

- Link-local: The scope is the local link (nodes on the same subnet)
- Site-local: The scope is the organization (private site addressing)
- Global: The scope is global (IPv6 Internet addresses)

# IPv6 Address Representation

- *x*:*x*:*x*:*x*:*x*:*x*:*x*:*x*, where *x* is a 16-bit hexadecimal field
- Leading zeros in a field are optional:
  - 2031:0:130F:0:0:9C0:876A:130B
- Successive fields of 0 can be represented as ::, but only once per address.

Examples:

**2031:0000:130F:0000:0000:09C0:876A:130B**

**2031:0:130f::9c0:876a:130b**

**FF01:0:0:0:0:0:0:1 >>> FF01::1**

**0:0:0:0:0:0:0:1 >>> ::1**

**0:0:0:0:0:0:0:0 >>> ::**

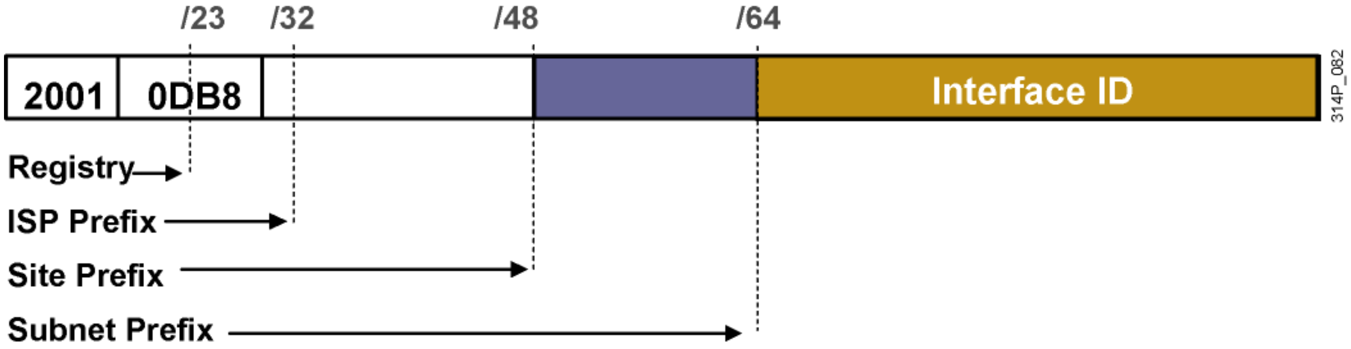
# IPv6 Address : Link Local

- Hosts on the same link (the same subnet) use these automatically configured addresses as soon as the routers are enabled.
- Neighbor Discovery provides address resolution.
- The prefix for link-local addresses is FE80::/64.

# IPv6 Address Representation: Site Local

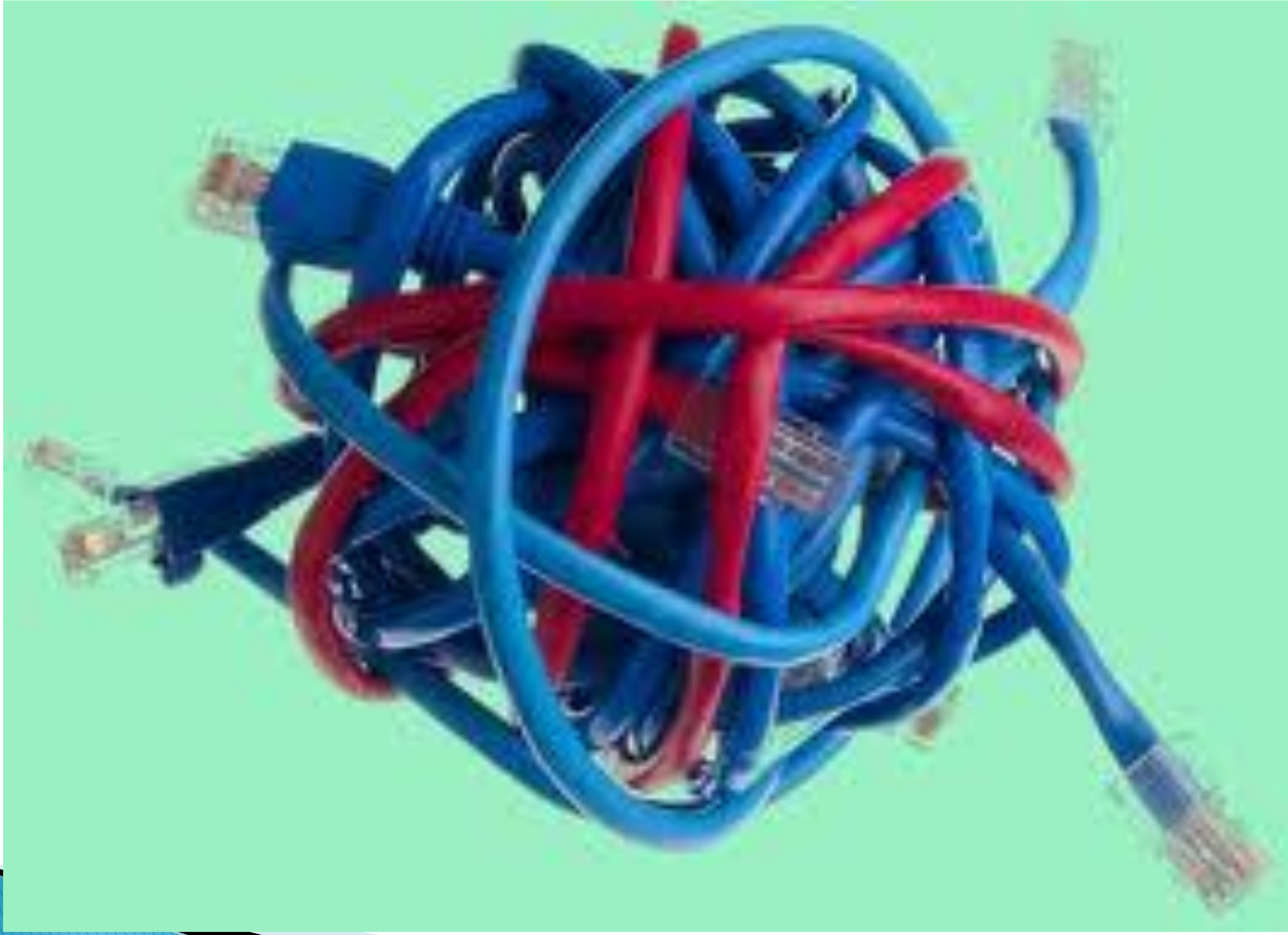
- IPv6 unicast Site-local addresses are similar to IPv4 private addresses.
- The scope of a Site-local address is the internetwork of an organization’s site. (You can use both global addresses and Site-local addresses in your network)
- The prefix for Site-local addresses is FC00::/8.

# IPv6 Address Representation: Global Unicast



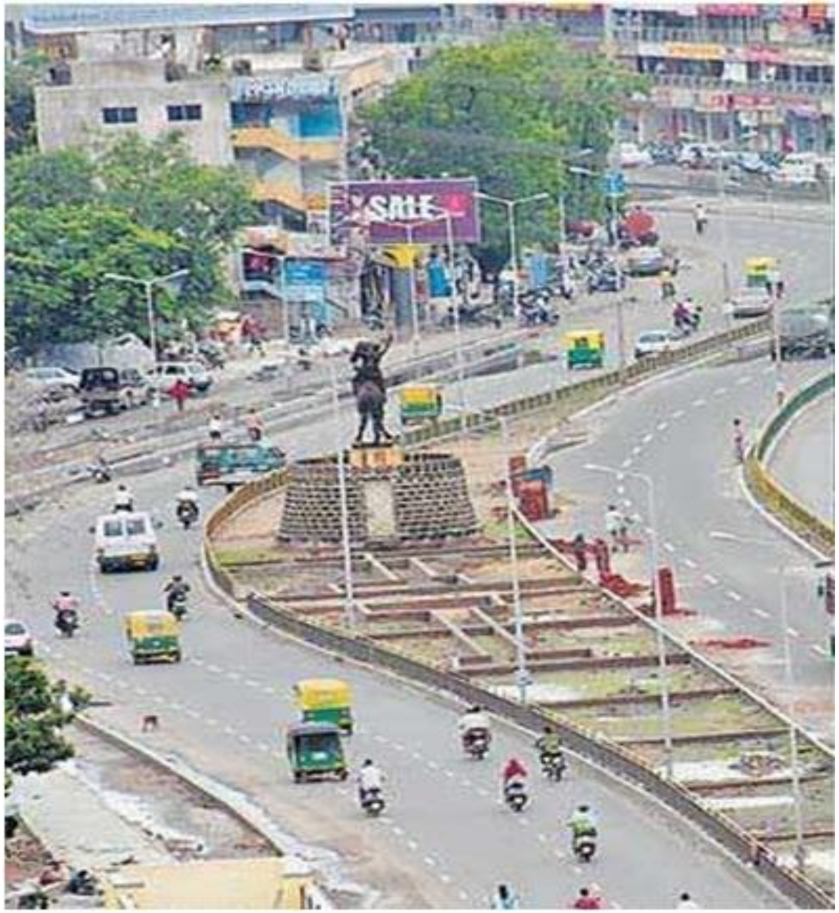
- **Global unicast and anycast addresses are defined by a global routing prefix, a subnet ID, and an interface ID.**

# 2. Routing Crisis



# Routing in IPv4 and IPv6

**IPv4 Situation**

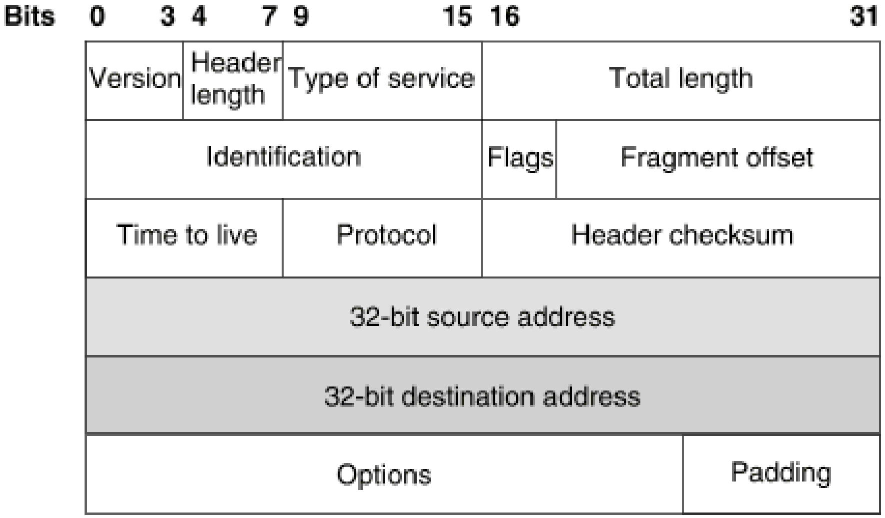


**IPv6 Situation**

# IPv6 Header Format (simplified)

- **IPv4: 20 Bytes + Options  IPv6: 40 Bytes + Extension Header**

## IPv4 Header

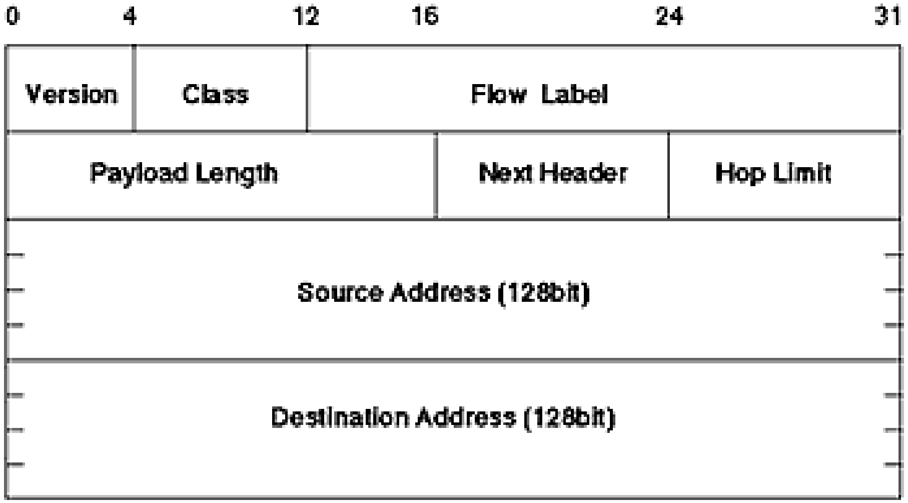


Bits 0 3 4 7 9 15 16 31

| | | | | |
|---|---|---|---|---|
| Version | Header length | Type of service | Total length | |
| Identification | | | Flags | Fragment offset |
| Time to live | | Protocol | Header checksum | |
| 32-bit source address | | | | |
| 32-bit destination address | | | | |
| Options | | | | Padding |

**Variable length due to options**

## IPv6 Header



0 4 12 16 24 31

| | | | | |
|---|---|---|---|---|
| Version | Class | Flow Label | | |
| Payload Length | | | Next Header | Hop Limit |
| Source Address (128bit) | | | | |
| Destination Address (128bit) | | | | |

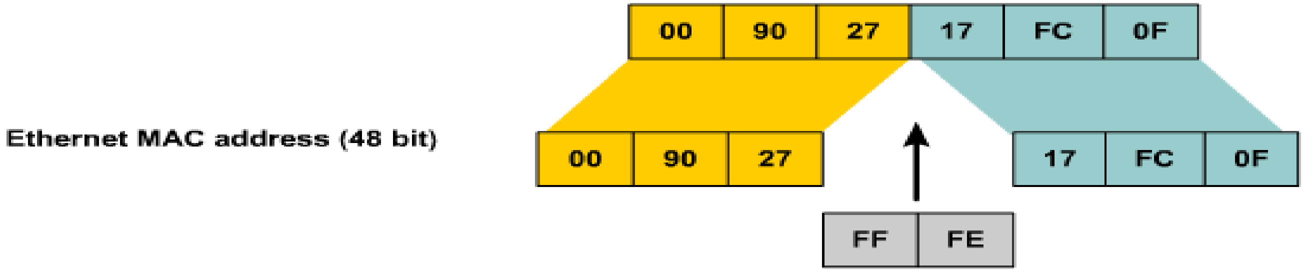
**Fixed length**

# Autoconfiguration – Stateless

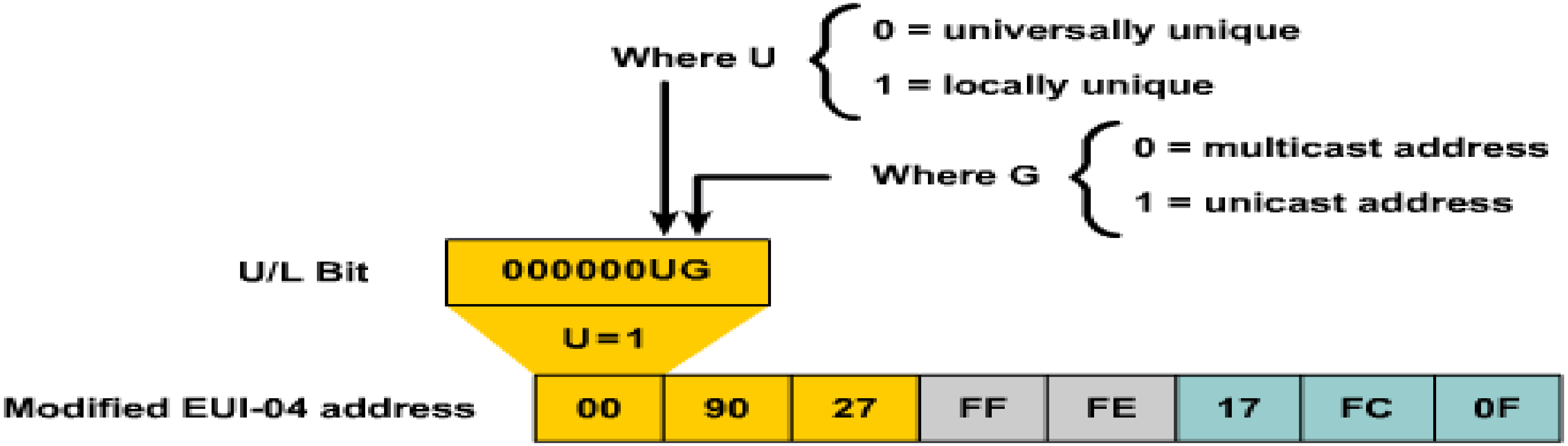
- Stateless Address Configuration (IP Address, Default Router Address)
- Router sends periodic Router Advertisement
- Node gets prefix information from the Router advertisement and generates the complete address using its MAC address
- Global Address=Link Prefix + EUI 64 Address
- Router Address is the Default Gateway

## IPv6 Address Representation EUI 64

- IPv6 uses the extended universal identifier (EUI)-64 format to do stateless autoconfiguration.
- This format expands the 48-bit MAC address to 64 bits by inserting “FFFE” into the middle 16 bits.
- To make sure that the chosen address is from a unique Ethernet MAC address, the universal/local (U/L bit) is set to 1 for global scope (0 for local scope).



# IPv6 Address Representation EUI 64



# Autoconfiguration – Stateful (DHCPv6)

- Stateful Configuration
- Provides not only IP address, also other configuration parameters like DNS

# DHCPv6

- Client
  - Initiates requests on a link to obtain configuration parameters
  - use its link local address to connect the server
  - Send requests to FF02::1:2 multicast address (All_DHCP_Relay_Agents_and_Servers)
- Relay Agent/ DHCPv6 Server
  - node that acts as an intermediary to deliver DHCP messages
  - between clients and servers
  - is on the same link as the client
  - Is listening on multicast addresses: All_DHCP_Relay_Agents_and_Servers (FF02::1:2)

# Neighbor Discovery

- IPv6 nodes which share the same physical medium (link) use Neighbor Discovery (NDP) to:
  - Discover their mutual presence
  - Determine link-layer addresses of their neighbors (equivalent to ARP)
  - Find routers
  - Maintain neighbors’ reachability information
- Uses Multicast Address

# Neighbor Discovery

Protocol features:

- Router discovery
- Prefix(es) discovery
- Parameters discovery (link MTU, Max Hop Limit, ...)
- Address auto-configuration
- Address resolution
- Next Hop determination
- Neighbor Unreachability Detection
- Duplicate Address Detection
- Redirect

# Neighbor Discovery

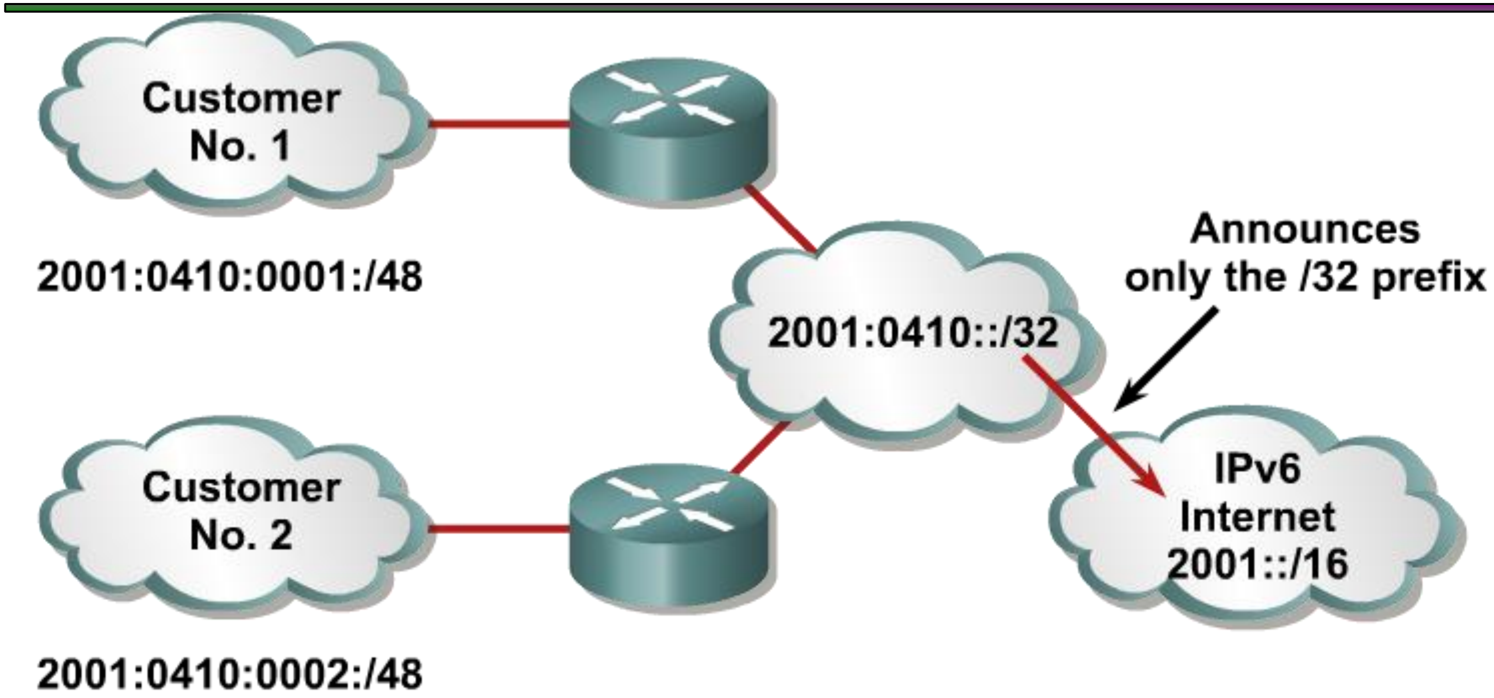
It provides the functionality of:

- ARP
- ICMP redirect

# Aggregation

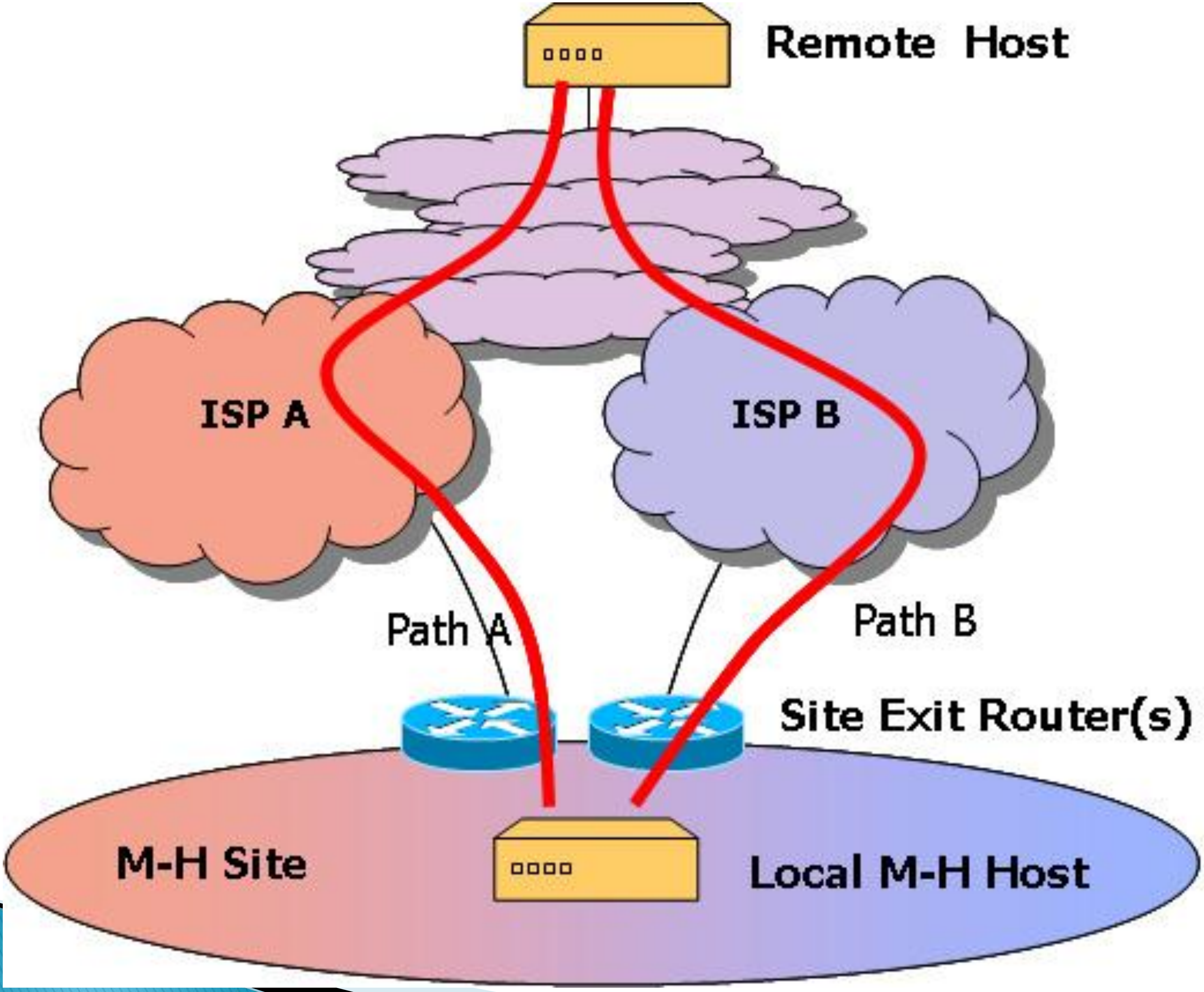
- Aggregation

# Routing in IPv6



- **Aggregation of prefixes announced in the global routing table**
- **Efficient and scalable routing**

# Multi-homing – Having multiple points of connection to the Internet


Remote Host
ISP A
ISP B
Path A
Path B
Site Exit Router(s)
M-H Site
Local M-H Host

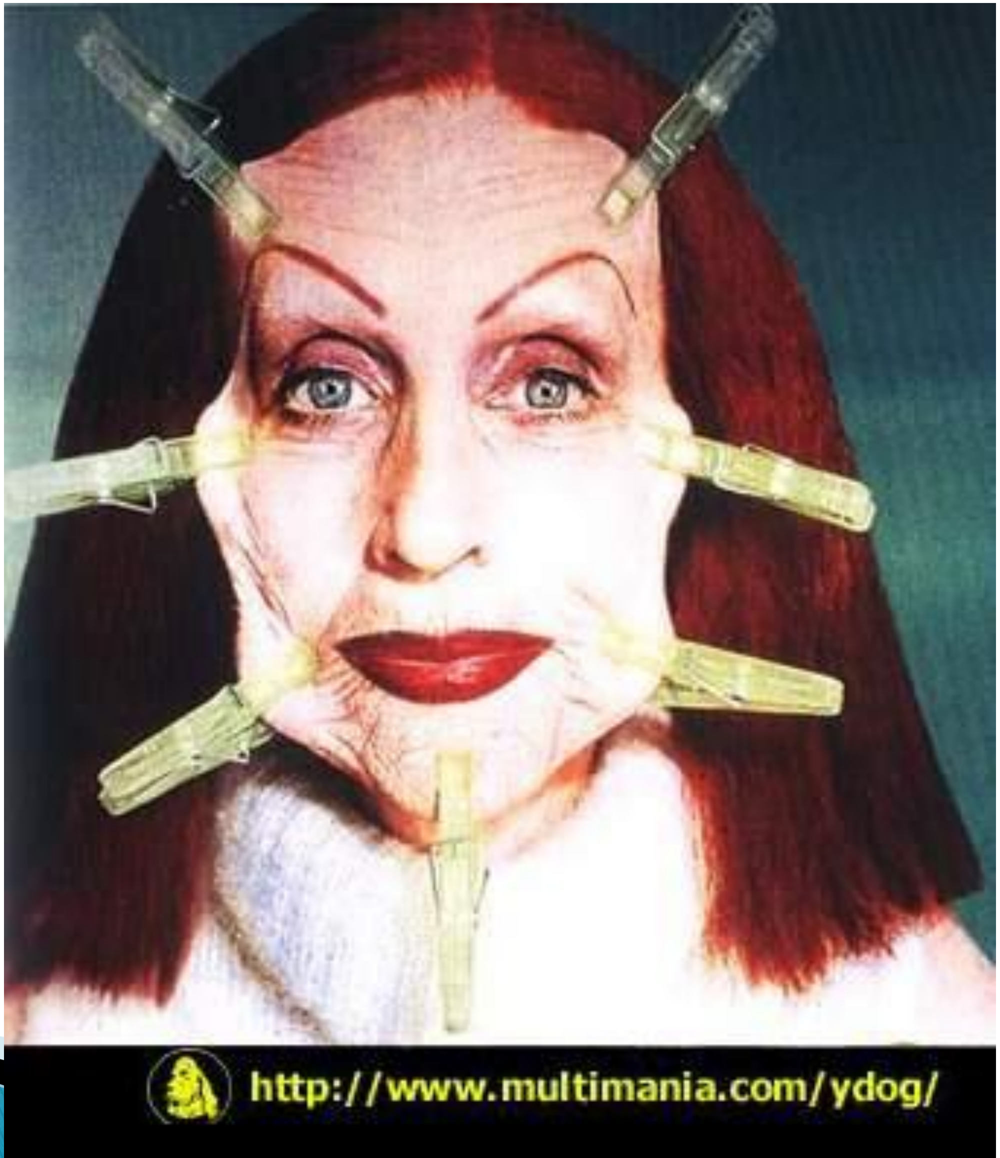
# Multihoming Issues

- Many sites are multihomed in the current Internet
  - reliability
  - stability – which provider will stay in business?
  - Competition

- In IPv4 we can use provider-independent addresses

- But all IPv6 addresses are provider-assigned!

# 3. End to End problem

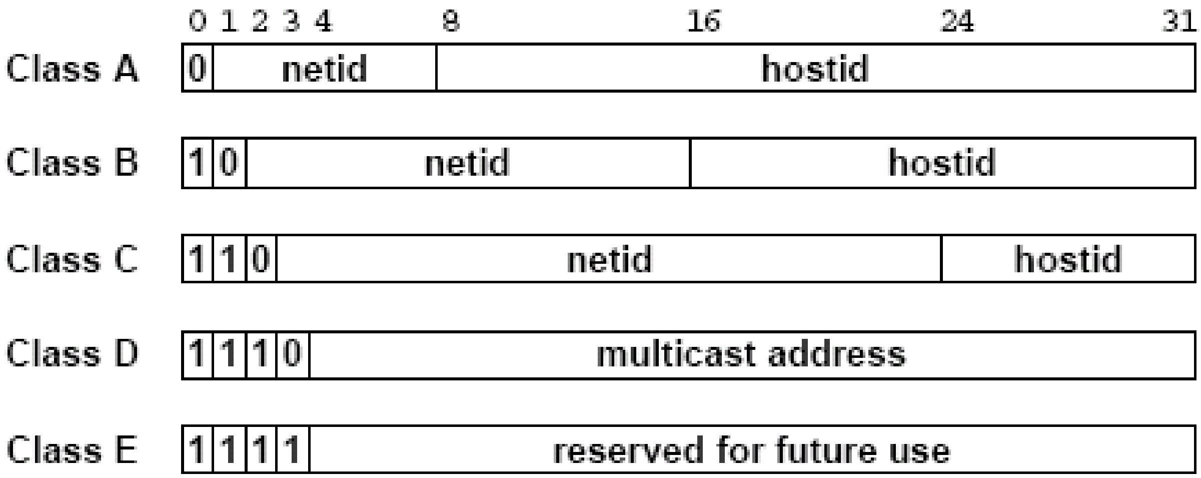


# MANAGING THE UNEXPECTED GLOBAL DEMAND FOR IP ADDRESSES

- **CIDR (Classless Inter-Domain Routing)** – RFCs 1517, 1518, 1519, 1520
- **VLSM (Variable Length Subnet Mask)** – RFC 1009
- **NAT/PAT (Network Address Translation / Port Address Translation)** – RFC
- **Private Addressing** – RFC 1918

# Migration from Classfull to Classless (CIDR)

## Classfull Addresses



0 1 2 3 4 8 16 24 31

Class A | 0 | netid | hostid

Class B | 1 | 0 | netid | hostid

Class C | 1 | 1 | 0 | netid | hostid

Class D | 1 | 1 | 1 | 0 | multicast address

Class E | 1 | 1 | 1 | 1 | reserved for future use

### What the Designers did not foresee ?

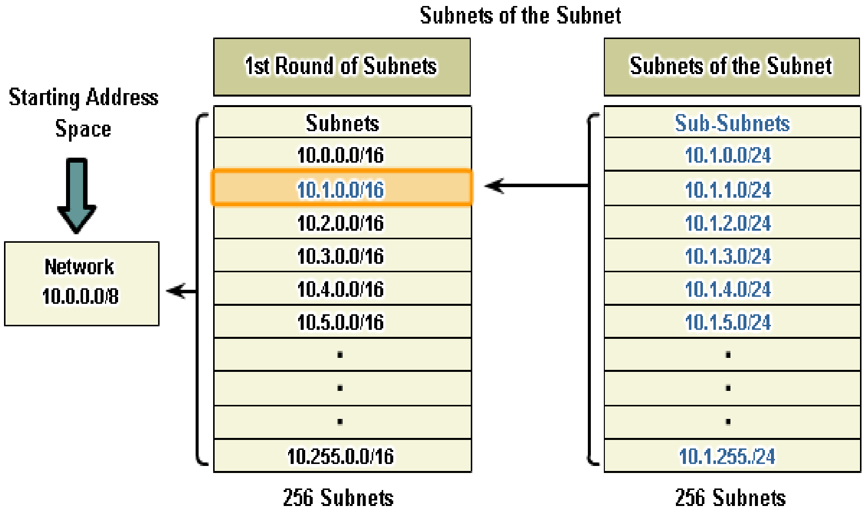
- Tremendous growth
- Large Routing Tables
- Exhaustion of IP Address one day

### Introduce CIDR

- Discard the concept of class
- A block of address space can have many different sizes, depending on network's need, represented by /n.
- n= number of bits "pre-set" e.g /28

# VLSM

- **VLSM** – the process of sub-netting a subnet to fit your needs
- **Example:**
  - Subnet 10.1.0.0/16, 8 more bits are borrowed again, to create 256 subnets with a /24 mask.
  - Mask allows for 254 host addresses per subnet
  - Subnets range from: 10.1.0.0 / 24 to 10.1.255.0 / 24



Subnets of the Subnet

Starting Address Space

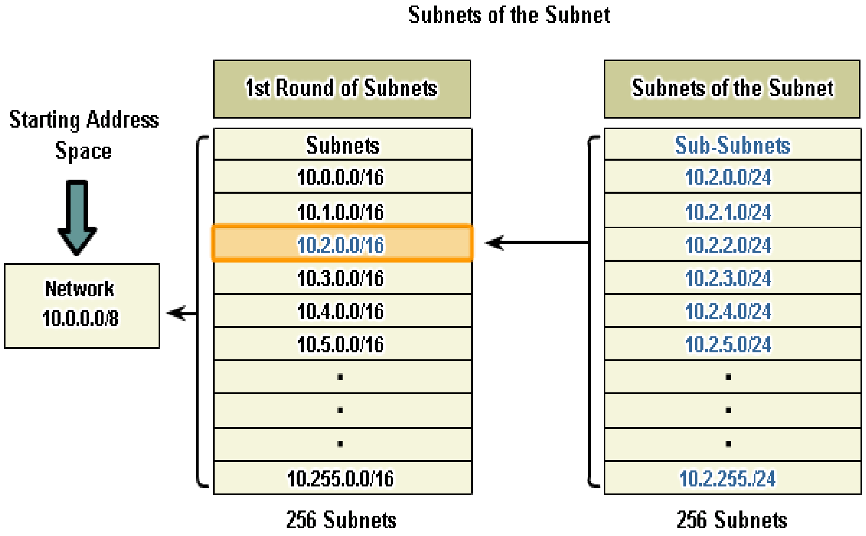
Network 10.0.0.0/8

| 1st Round of Subnets |
|---|
| Subnets |
| 10.0.0.0/16 |
| 10.1.0.0/16 |
| 10.2.0.0/16 |
| 10.3.0.0/16 |
| 10.4.0.0/16 |
| 10.5.0.0/16 |
| . |
| . |
| . |
| 10.255.0.0/16 |

256 Subnets

| Subnets of the Subnet |
|---|
| Sub-Subnets |
| 10.1.0.0/24 |
| 10.1.1.0/24 |
| 10.1.2.0/24 |
| 10.1.3.0/24 |
| 10.1.4.0/24 |
| 10.1.5.0/24 |
| . |
| . |
| . |
| 10.1.255./24 |

256 Subnets



Subnets of the Subnet

Starting Address Space

Network 10.0.0.0/8

| 1st Round of Subnets |
|---|
| Subnets |
| 10.0.0.0/16 |
| 10.1.0.0/16 |
| 10.2.0.0/16 |
| 10.3.0.0/16 |
| 10.4.0.0/16 |
| 10.5.0.0/16 |
| . |
| . |
| . |
| 10.255.0.0/16 |

256 Subnets

| Subnets of the Subnet |
|---|
| Sub-Subnets |
| 10.2.0.0/24 |
| 10.2.1.0/24 |
| 10.2.2.0/24 |
| 10.2.3.0/24 |
| 10.2.4.0/24 |
| 10.2.5.0/24 |
| . |
| . |
| . |
| 10.2.255./24 |

256 Subnets

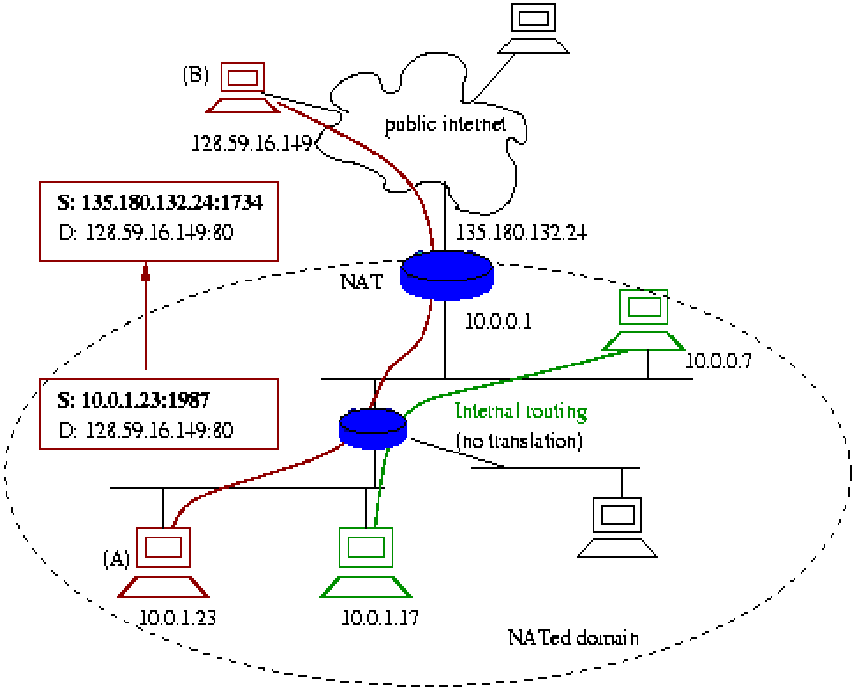
# NAT/PAT (Network Address Translation/Port Translation)

- Devised in 1994

- Translates an address used on local network to an address used on public network

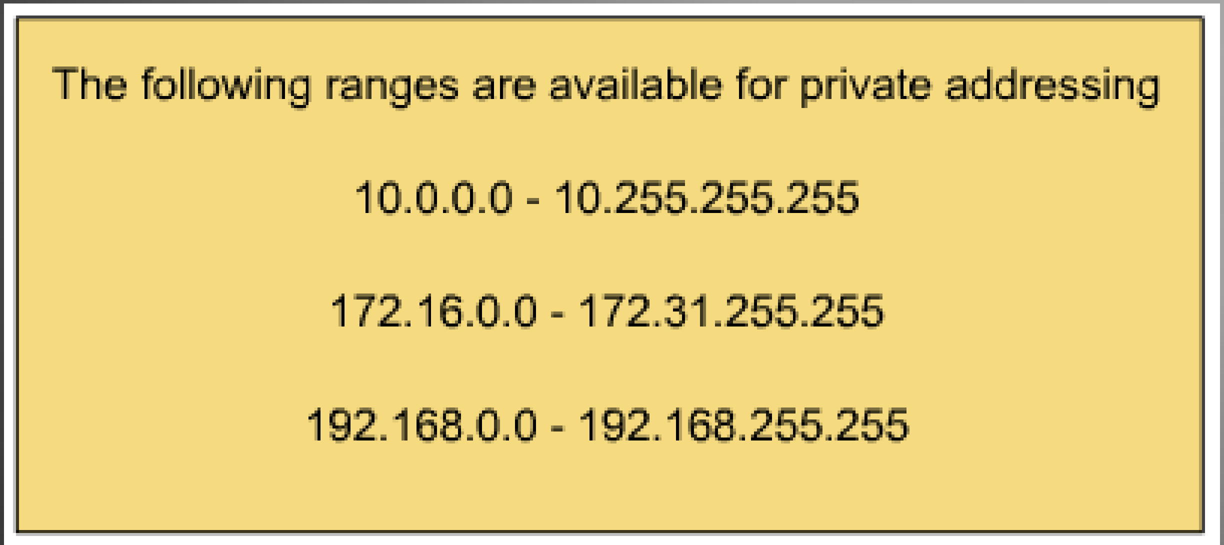
- Small number of public addresses “shared” between large number of hosts using private addresses

- Makes possible reuse of private addresses



This NAT box with external IP 135.180.132.24, creates a mapping from 10.0.1.23 port 1987 to its external IP 135.180.132.24 and port 1734. The packet is forwarded to node B, as if it was originated from the NAT box, by changing the source IP and port to 135.180.132.24 and 1734 respectively. NAT intercepts incoming packets, and changes the destination to 10.0.1.23 at port 1987. Node A thinks that it is connected to node B's IP, whereas node B thinks that it is connected to NAT's IP.
S= Source, D= Destination

# NAT uses Private Addresses



The following ranges are available for private addressing

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

# IPv6 – Discard NAT, Enable Global Reachability

From 32 bits to 128 bits addresses enables:

– Restore original end-to-end architecture of Internet

– Enable global reachability:

- No hidden networks, hosts
- All hosts can be reachable and be "servers”
- Application design simplified

# 4. Security Problem

# IPv6 Security

**IPv4 was not designed with security in mind.**

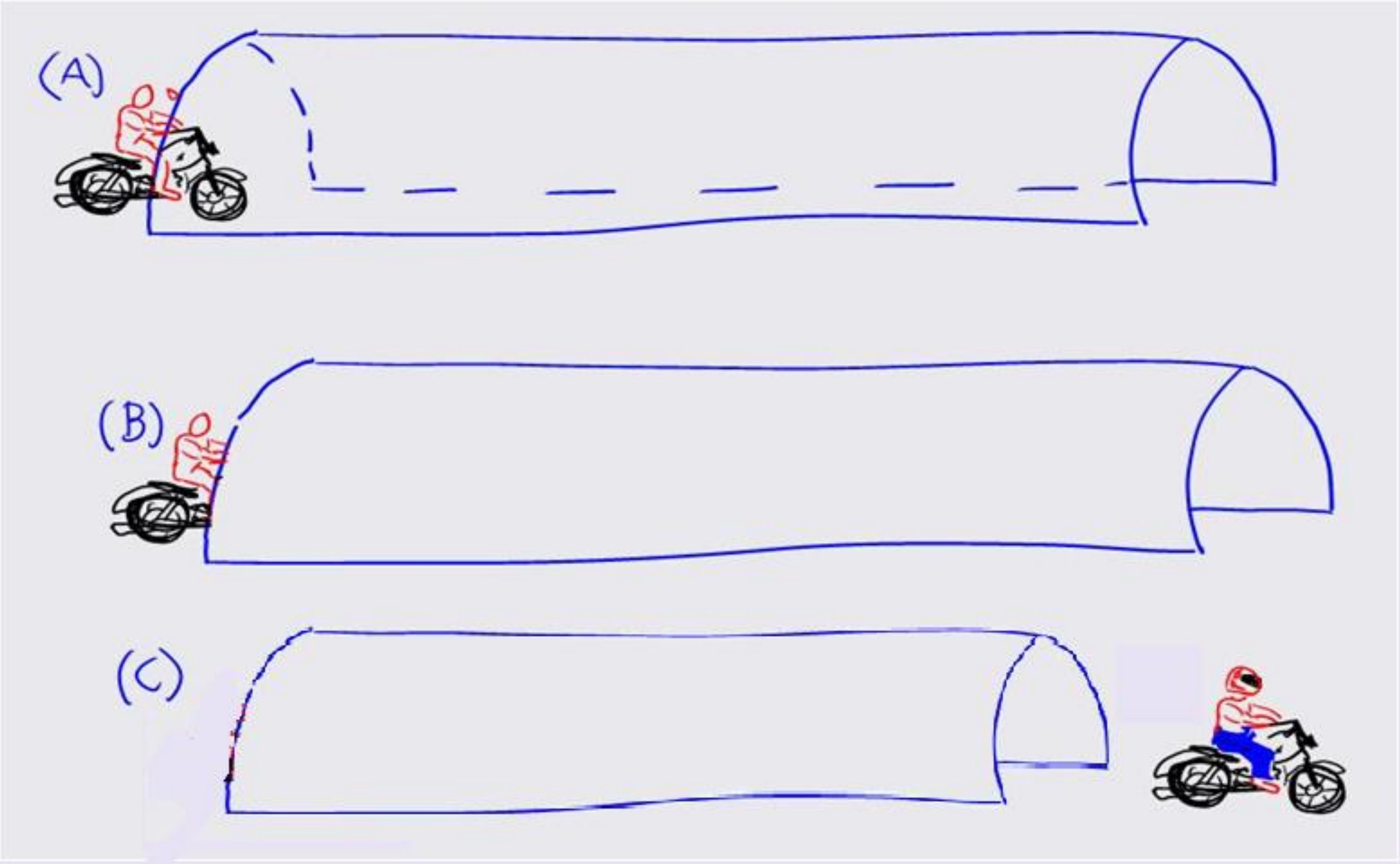
- **Packet Sniffing:** Due to network topology, IP packets sent from a source to a specific destination can also be read by other nodes, which can then get hold of the payload (for example, passwords or other private information).
- **IP Spoofing:** IP addresses can be very easily spoofed both to attack those services whose authentication is based on the sender's address
- **Connection Hijacking:** Whole IP packets can be forged to appear as legal packets coming from one of the two communicating partners, to insert wrong data in an existing channel.

# IPv6 Security

In IPv4, Security is implemented in:

- Applications – HTTPS, IMAPS, SSH etc.
- IPsec tunnels

# IPv6 - End to End Security



# Security in IPv6

- IPv4 – NAT breaks end-to-end network security
- IPv6 – Huge address range – No need of NAT

# Security in IPv6

## IPv6 is more difficult to break:

- Default subnets in IPv6 have $2^{64}$ addresses
- Scan with 10 Mpps will take more than 50 000 years
- Ping sweeps on IPv6 networks are not possible

# Security in IPv6

## Viruses and Worms In IPv6:

- Viruses and Email, IM worms: IPv6 brings no change.
- Other worms:
  - IPv4: reliance on network scanning
  - IPv6: not so easy
  - Worm developers will adapt to IPv6
- IPv4 best practices around worm detection and mitigation remain valid.
- IPS systems and Anti-viruses will not change.

# IPv6 IPsec

- Applies to both IPv4 and IPv6:
  - – Mandatory for IPv6
  - – Optional for IPv4
- Applicable to use over LANs, across public & private WANs, & for the Internet
- IPSec is a security framework
  - – Provides suit of security protocols
  - – Secures a pair of communicating entities
  - –Two different modes: Transport mode (host-to-host) and Tunnel Mode (Gateway-to-Gateway or Gateway-to-host)

# IPv6 IPsec Protocol

## IPsec Services

- Authentication: AH (Authentication Header – RFC 4302)
- Confidentiality: ESP (Encapsulating Security Payload – RFC 4303)
- Key management: IKEv2 (Internet Key Exchange – RFC4306)

When two computers (peers) want to communicate using IPSec, they mutually authenticate with each other first and then negotiate how to encrypt and digitally sign traffic they exchange. These IPSec communication sessions are called security associations (SAs).

# IPv6 IPsec Protocol

## Implementations

- Linux-kernel 2.6.x onwards
- Cisco IOS-12.4(4)T onwards
- Windows Vista onwards

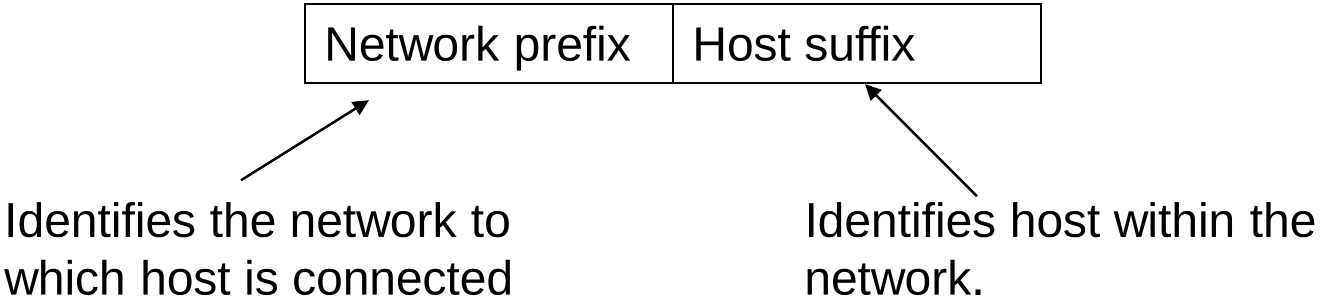
# 5. Easy Mobility with IPv6

# Mobility background

- Mobile devices with Internet connectivity are becoming increasingly common.
- Mobile phones are becoming Internet capable.
- Mobility in cellular systems and WLANs is currently handled mostly on the link layer and is invisible to applications and Internet Protocol (IP) layer.
- Trend for multiple network interfaces in mobile devices.

# IPv6 addressing and mobility

- IPv6 addresses consist of two parts: a 64-bit network prefix and a 64-bit host suffix.



Network prefix | Host suffix

Identifies the network to which host is connected

Identifies host within the network.

- Network prefix of address depends on location.
- When a host moves from one IP network to another, it needs to change the network part of its address.

# IPv6 Mobility

- IPv6 has better support for mobility through extension headers.
- Large number of applications like data roaming services require support of mobile IP which is not supported by IPv4.

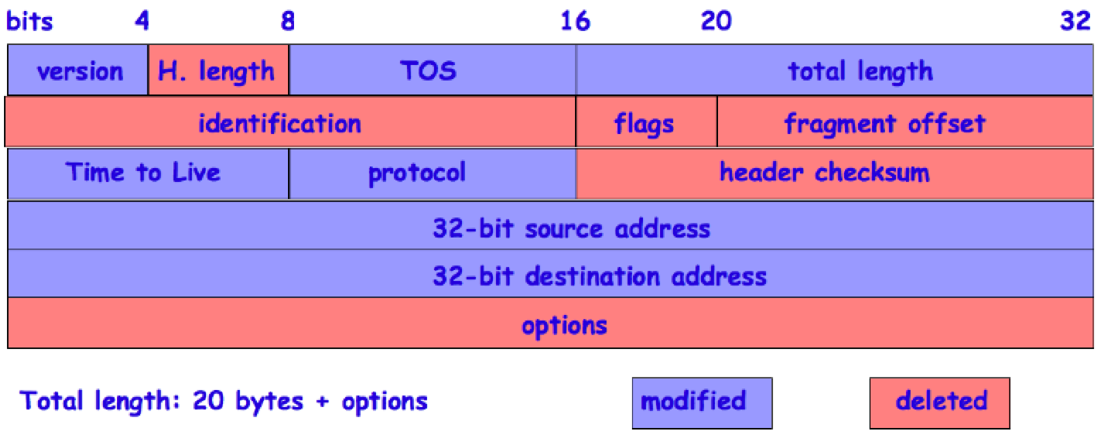
# 6. IPv6 QoS

- IPv4 networks typically give each and every packet a "best level of effort" service, even if the content of every packet isn't really important or time-sensitive data.
- An IPv4-based system has no way to differentiate between data payloads that are time sensitive, such as streaming video or audio, and those that aren't time-sensitive, such as status reports and file transfer.
- IPv6 provides a way for applications to request handling without delay throughout the WAN. Streaming audio and video requires low latency through high priority. Various application can share connection via priority level.

# Packet classification in IPv4

- Based on IPv4 header
  - Traffic Class

IPv4 Header Format



bits 4 8 16 20 32

version | H. length | TOS | total length

identification | flags | fragment offset

Time to Live | protocol | header checksum

32-bit source address

32-bit destination address

options

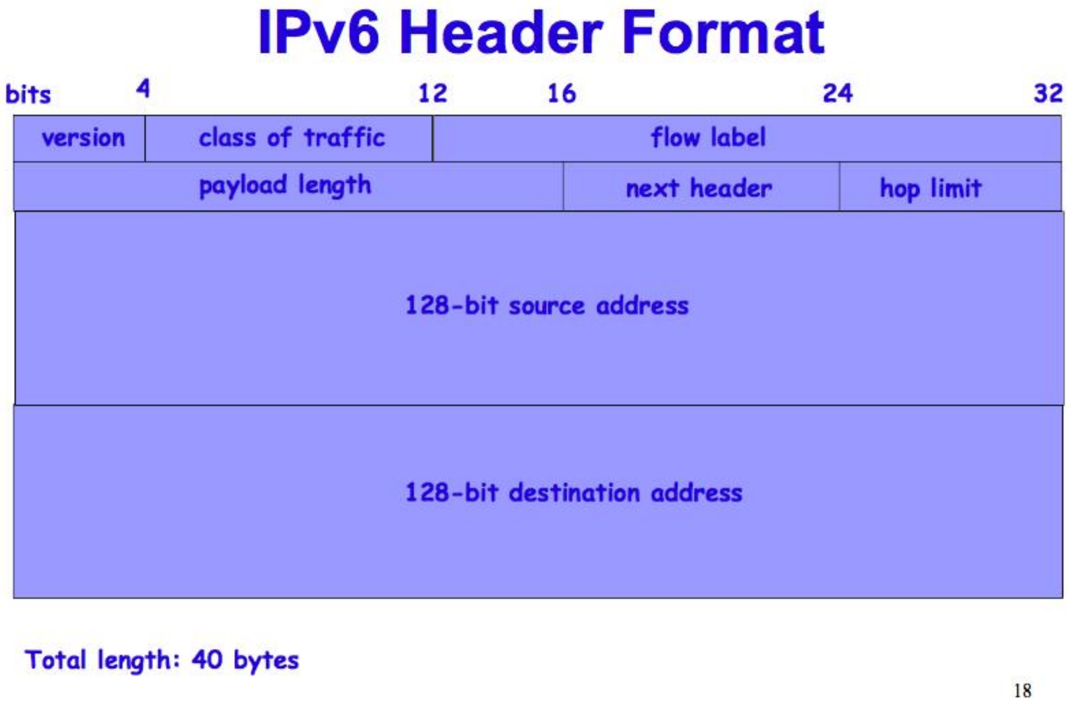
Total length: 20 bytes + options

modified

deleted

# Packet classification in IPv6

- Based on IPv6 header
  - Class of Traffic
  - Flow Label



IPv6 Header Format

bits 4 12 16 24 32

version | class of traffic | flow label

payload length | next header | hop limit

128-bit source address

128-bit destination address

Total length: 40 bytes

18

# Conclusion

Limitations of IPv4 and Advanced features in IPv6 make compelling reason for shifting to IPv6

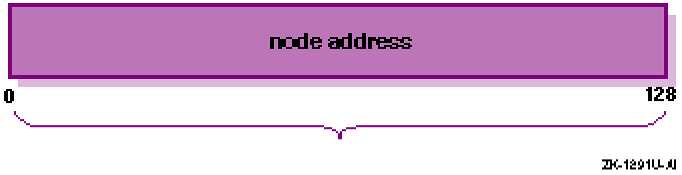
# Thank You

# Summary: Why IPv6?

- Shortage of IPv4 addresses
  - Internet is expanding very rapidly, especially in developing countries like India, China
  - New devices connecting to the Internet need IP address
- End-to-End Reachability is not possible without IPv6
- New Features like Autoconfiguration, better support for QoS, Mobility and Security, Route Aggregation, Jumbo Frames
  - Possibility of New and Innovative applications

# Unicast Addresses

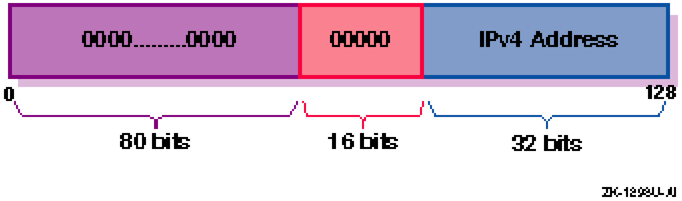
- LAN Unicast Address



- Unspecified Address 0:0:0:0:0:0:0:0

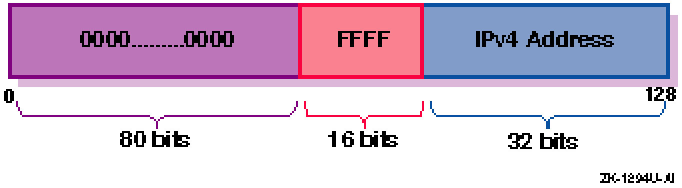
- Loopback address 0:0:0:0:0:0:0:1

- IPv6 Addresses with embedded IPv4 address
  - IPv4 compatible IPv6 address
  - (Used by IPv6 nodes to tunnel IPv6 packets across an IPv4 routing infrastructure. The IPv4 address is carried in the low-order 32-bits)



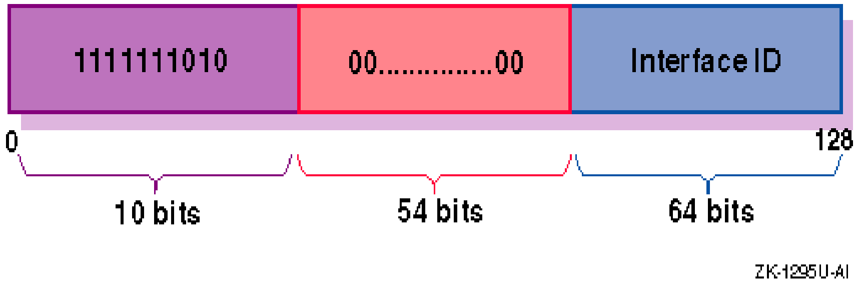
  - IPv4 mapped IPv6 address

(Used to represent an IPv4 address and to identify nodes that do not support IPv6 (IPv4-only nodes). It is not used in an IPv6 packet.)

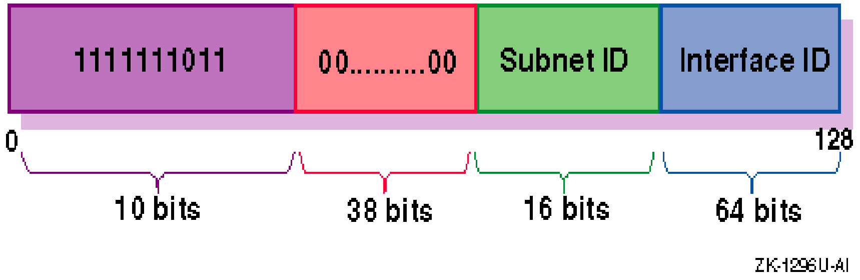


# Unicast Address – contd…

- Local-use IPv6 unicast addresses
  - Link Local (Used for addressing on a single link when performing address autoconfiguration, neighbor discovery, or when no routers are present)

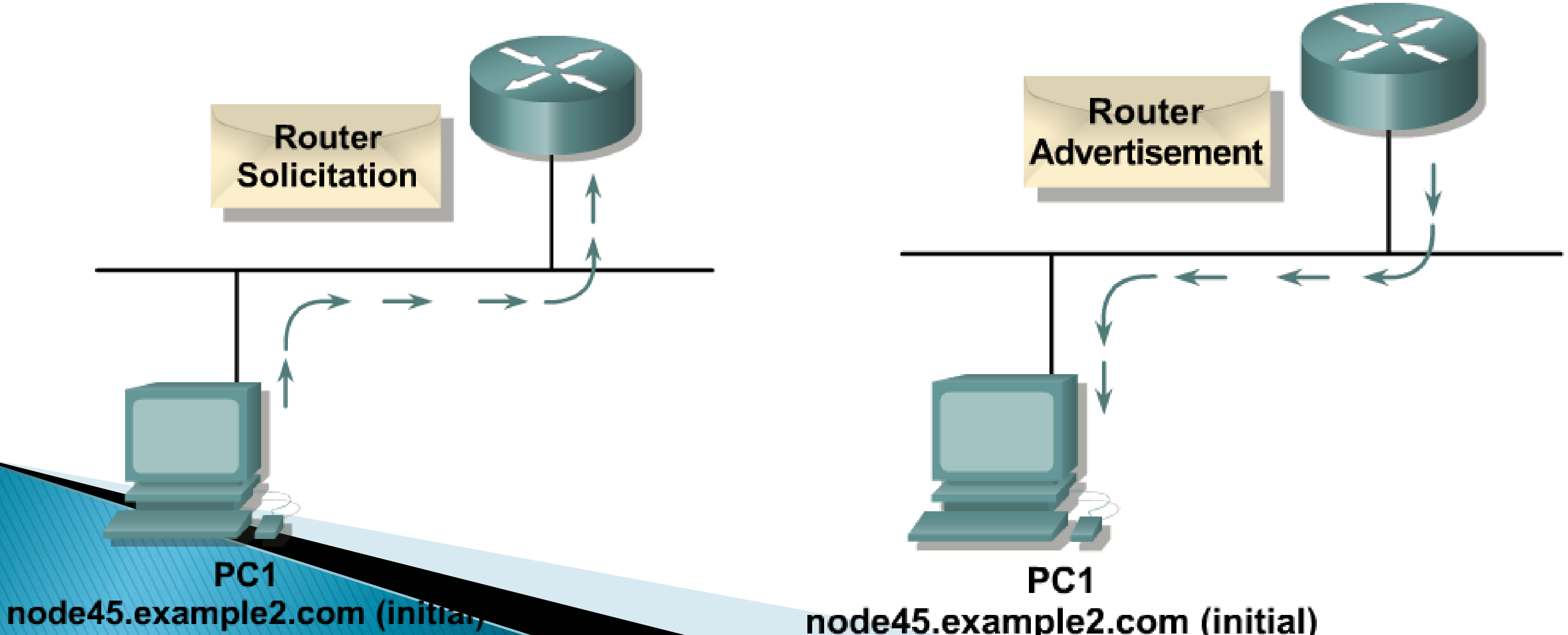


  - Site Local (Used for sites or organizations that are not connected to the global Internet)



# Stateless Autoconfiguration Example

- MAC address: 00:0E:0C:31:C8:1F
- EUI 64 Address: 02:0E:0C:FF:FE:31:C8:1F
- Router Solicitation is sent on FF01::2 (All Router Multicast Address) and Advertisement sent on FF01::1 (All Node Multicast Address)



# Neighbor Discovery

## ND specifies 5 types of ICMP packets:

- **Router Advertisement (RA) :**

  Periodic advertisement (of the availability of a router) which contains:

  »list of prefixes used on the link (autoconf)

  »a possible value for Max Hop Limit (TTL of IPv4)

  »value of MTU

- **Router Solicitation (RS) :**

  The host needs RA immediately (at boot time)

# Neighbor Discovery

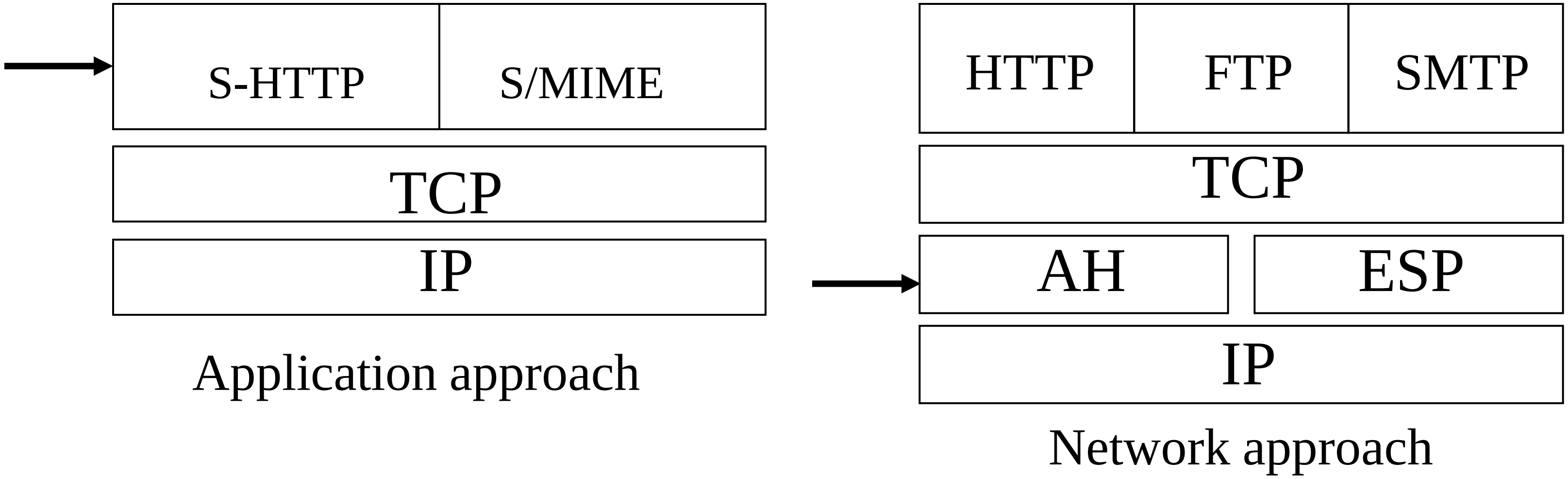
- **Neighbor Solicitation (NS):**
  »to determine the link-layer address of a neighbor
  »or to check its reachability
  »also used to detect duplicate addresses (DAD)

- **Neighbor Advertisement (NA):**
  »answer to a NS packet
  »to advertise the change of physical address

- **Redirect:**
  »Used by a router to inform a host of a better route to a given destination

# IPv6 IPsec Protocol

## IPsec Services



# IPv6 IPsec Protocol

## IPsec AH

IPv6 AH Packet Format

| | | | | |
|---|---|---|---|---|
| IPv6 Header | Hop-by-Hop Routing | Authentication Header | Other Headers | Higher Level Protocol Data |

IPv6 AH Header Format

| | | |
|---|---|---|
| Next Header | Length | Reserved |
| Security Parameters Index | | |
| Authentication Data (variable number of 32-bit words) | | |

# IPv6 IPsec Protocol

## IPsec ESP

ESP Format

| |
|---|
| Security Parameters Index (SPI) |
| Initialization Vector (optional) |
| Replay Prevention Field (incrementing count) |
| Payload Data (with padding) |
| Authentication checksum |

# Some Security Issues in IPv6

- IPsec Key Exchange Protocol not yet fully Standardized
- Scanning possible – If IP address assignment is poorly designed
- No protection against all denial of service attack (DoS attacks difficult to prevent in most cases)
- No many firewalls in market with V6 capability