Network Layer

DAT610 – Wireless Communications

Naeem Khademi

Associate Professor, IDE/UiS

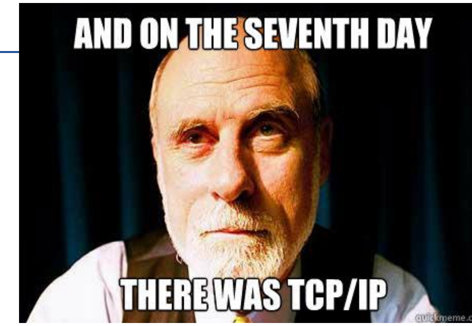
naeem.khademi@uis.no

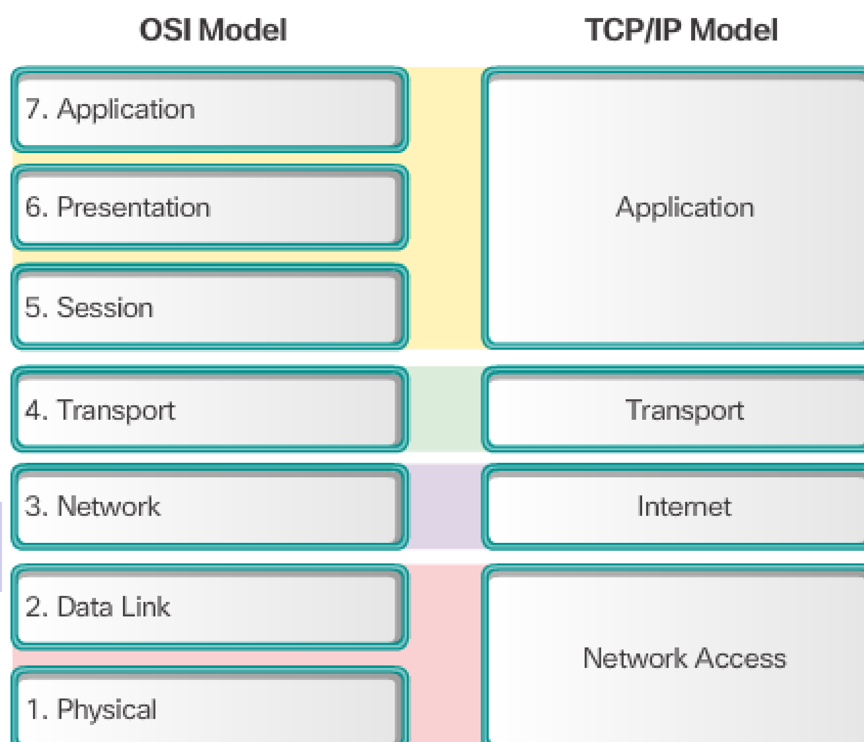
Universitetet i Stavanger

TCP/IP vs OSI Model

Open Systems Interconnection (OSI) by **ISO & ITU**
Developed/adopted
Late 70's, early 80's

Vint Cerf and **Robert Kahn** (1974); standards maintained by the IETF





Presentation layer: Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption

Session layer: Managing communication sessions, i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes

Transport layer: **Reliable end-to-end communication** for services/applications, with flow control, multiplexing and connection-oriented communication

Network layer: Multi node/network data transfer, with **network addressing**, **routing** and **traffic control**

Datalink layer: **Reliable transmission** of data frames between two nodes **connected by a physical layer**

Physical layer: **Raw bit streams** over physical transmission medium

The Network Layer

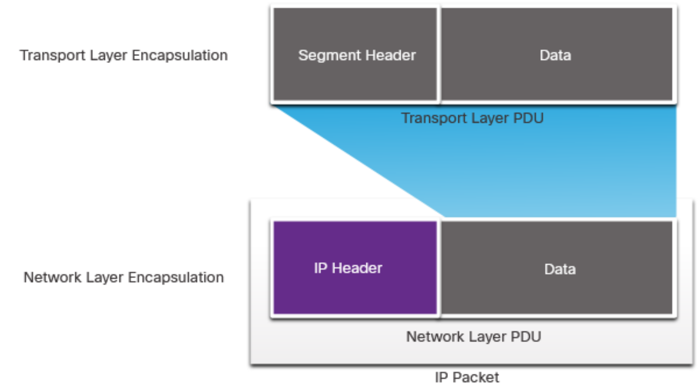
Network layer (L3): a network-level (i.e., end-to-end) communication between source and destination– in contrast to DL layer scope is no longer per link; **IPv4** and **IPv6** are two principal L3 protocols!

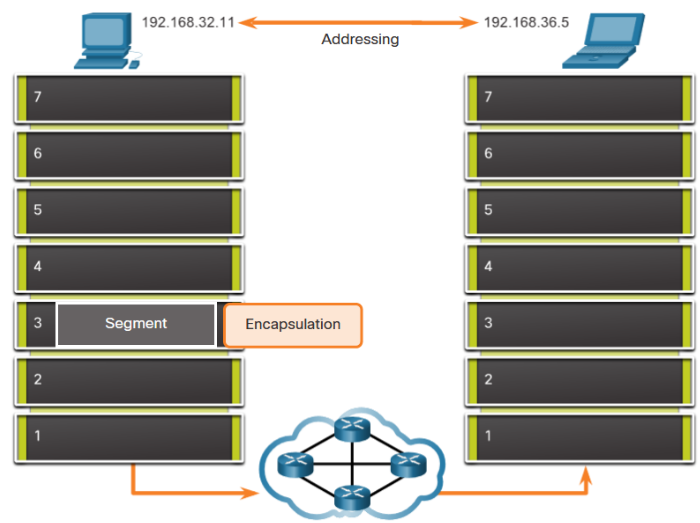
- **Basic operations**: **addressing**, **encapsulation**, **decapsulation**, **routing**

- IP encapsulates transport layer PDU (i.e., segment/datagram for TCP/ UDP)

- IP can be understood by all L3 devices along the network path (e.g., routers or L3 switches)

- **IP addressing** does not change along the end-to-end path (except with NAT)





Network layer protocols forward transport layer PDUs between hosts.

Internet Protocol (IP)

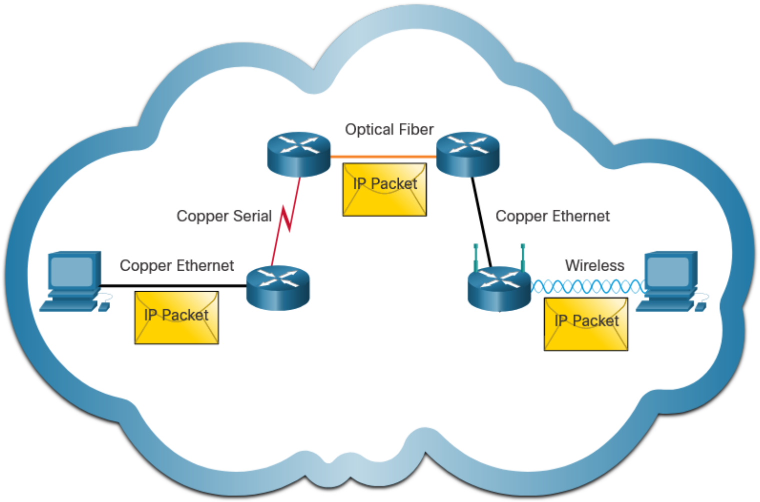
IP is **connectionless**, **best-effort (BE)** and **media-independent**

– No control info (sync, ack packets); connections have to be implemented by an L4 proto

– **BE:** no packet delivery guarantee, losses may occur, no retry, no acks (unreliable!)

– Packets may arrive out-of-sequence, with error/corrupted so; IP relies on L4 to implement these fixes!

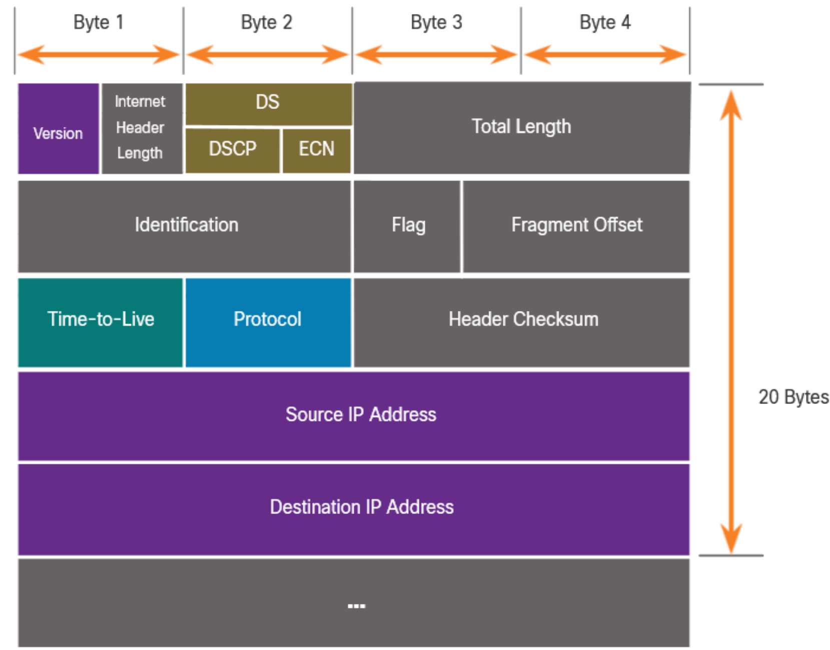
– IP functions irrespective of DLL protocol or media (PHY) – can be sent over fiber, copper, wireless, etc.



IPv4 Packet Header

IPv4 packet header: in binary, with most important info about the packet (e.g., src/dst IP address); three major limitations

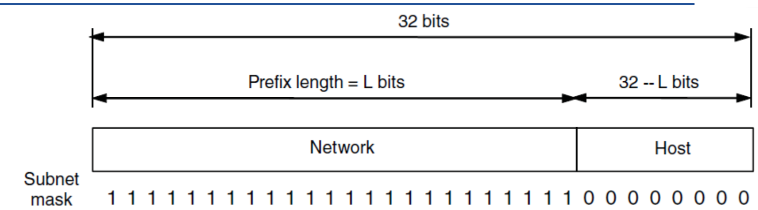
- **IPv4 address depletion:** not much left from IPv4 address space
- **Lack of end-to-end connectivity:** private addressing & NAT was created to extend the IPv4 address space at the cost of losing direct communication and public IP addressing
- **Increased network complexity:** NAT originally meant as a temporary solution, but it now creates issues with header manipulation and causing additional latency



Function	Description
Version	This will be for **v4**, as opposed to **v6**, a 4-bit field= **0100**
Differentiated Services	Used for QoS: **DiffServ** – **DS** field or the older IntServ – **ToS** or Type of Service
Header Checksum	Detect corruption in the IPv4 header
Time to Live (TTL)	Layer 3 hop count. When it becomes zero the router will discard the packet.
Protocol	I.D.s next level protocol: ICMP, TCP, UDP, etc.
Source IPv4 Address	32-bit source address
Destination IPV4 Address	32-bit destination address

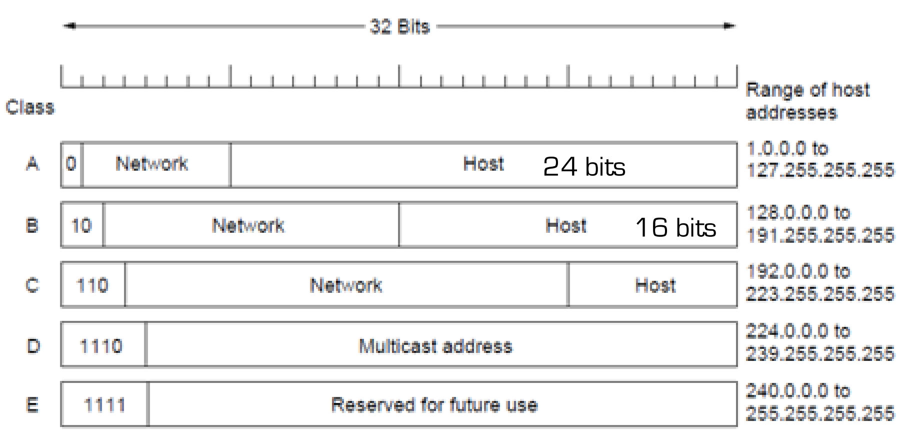
IPv4 Addressing (#1)

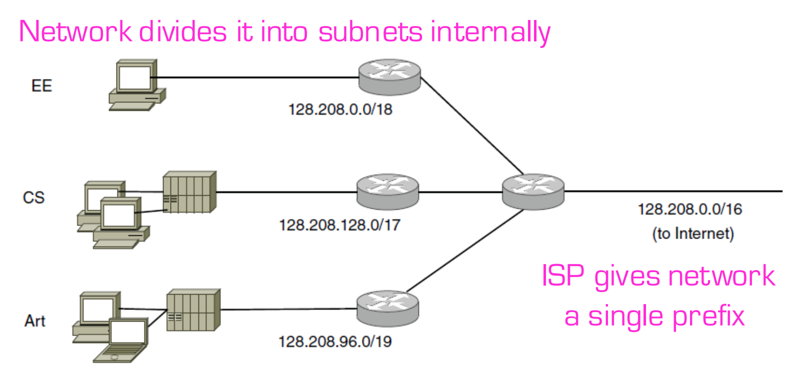
- Addresses are allocated in **blocks** called <u>prefixes</u>!
  - Determined by **network portion**
  - Network addr/**length** -- e.g., 18.0.31.0/**24**



- **<u>Classful addressing</u>:** old addresses came in blocks of fixed size (A, B, C)
  - **Carries size as part of address; inflexible! E.g. class B allocated address has 65K hosts even though net might have 2K hosts only.**
  - Called classful (vs. classless) addressing

- **<u>Sub-netting</u>** splits up IP prefix to help with management of network – known to local routers but looks like a single prefix from outside (routers)!





Figures: CN5E by Tanenbaum & Wetherall, © Pearson Education-Prentice Hall and D. Wetherall, 2011

IPv4 Addressing (#2)

- **Classless InterDomain Routing (CIDR):** more efficient use of IPv4 address space than classful method

- **CIDR network portion** can be of arbitrary length; within the allocated portion of ISP's address space

network part **host part**

11001000 00010111 00010000 00000000

200.23.16.0/23

Assigned by ICANN

ISP's block	11001000 00010111 00010000 00000000	**200.23.16.0/20**
Organization #0	**11001000 00010111 0001000**0 00000000	**200.23.16.0/23**
Organization #1	**11001000 00010111 0001001**0 00000000	**200.23.18.0/23**
Organization #2	**11001000 00010111 0001010**0 00000000	**200.23.20.0/23**
…		
Organization #7	**11001000 00010111 0001111**0 00000000	**200.23.30.0/23**

IPv4 Address Space Limitation

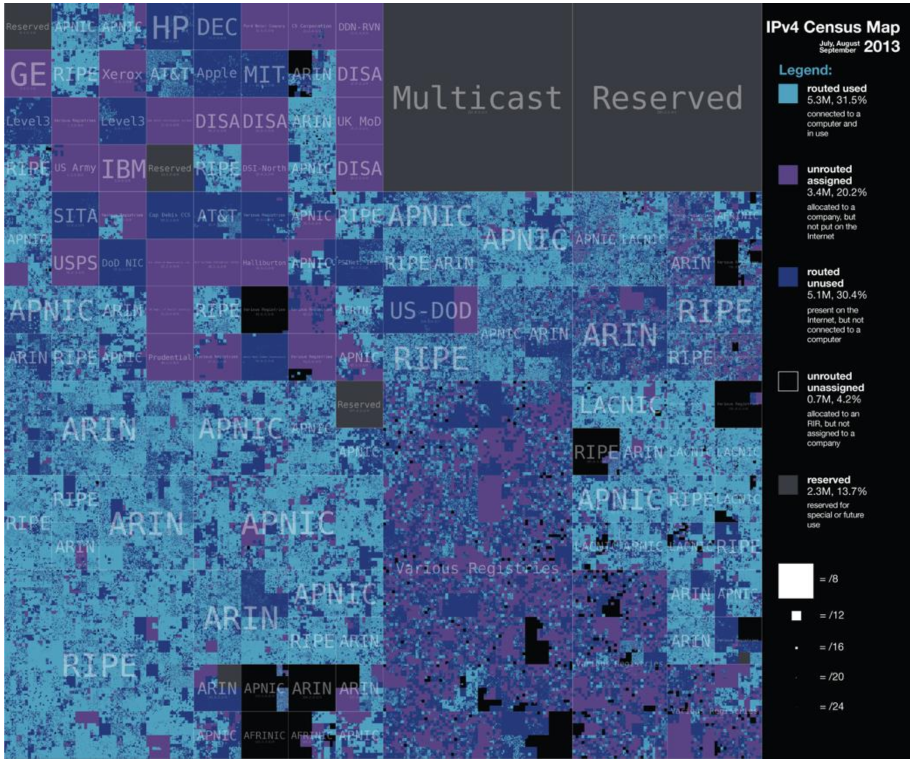
Network Address Translation (NAT): allows an organization to use a smaller number of **public IP addresses** with the use of **private IP addresses**

- Maps one external IP address to many internal IP addresses
- Uses TCP/UDP port to tell connections apart (PAT)
- Violates layering; very common in homes, etc.
- With special config, servers cannot be behind a NAT since clients don't know the server's local address to establish a connection to!

Private IPv4 addresses per RFC1918

Class	Address Range	Net. Prefix
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

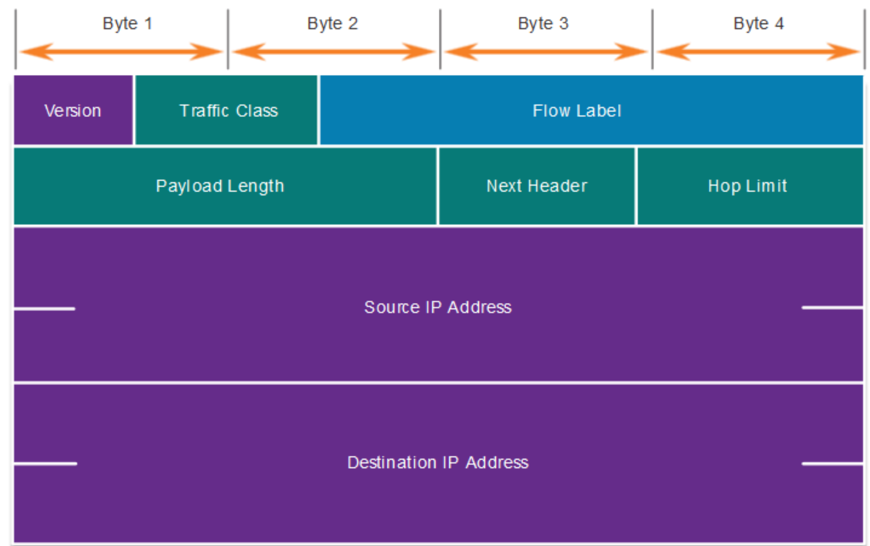
IPv4 address assignment and census map in 2013 by CAIDA

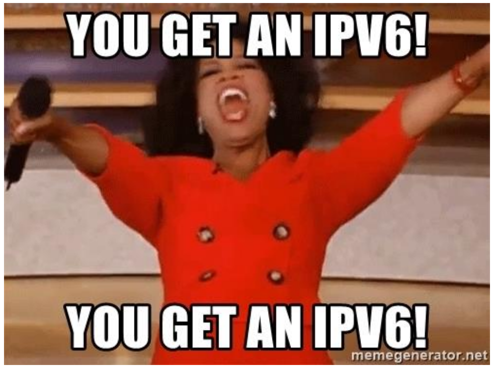


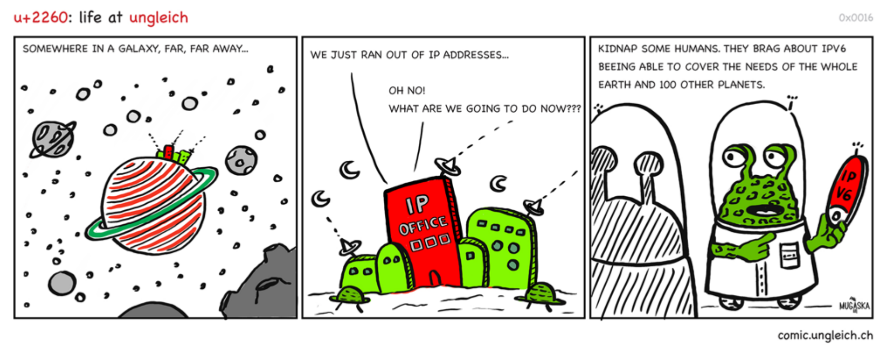
IPv6

IPv6: developed by the IETF to overcome the limitations of IPv4

- Introduced in 1995 (RFC1883) yet we're still using IPv4!!
- **Increased address space:** 4 billion IPv4 address (2^{32}) vs 340 trillion trillion trillion IPv6 addresses (2^{128})!
- **Improved packet handling:** simpler headers with fewer fields! 40 bytes long header; IPv4 "flag", "fragment offset", "header checksum" removed!
- **Eliminates the need of NATs** i.e., "everybody gets an IPv6 address"







Universitetet i Stavanger

Need for IPv6

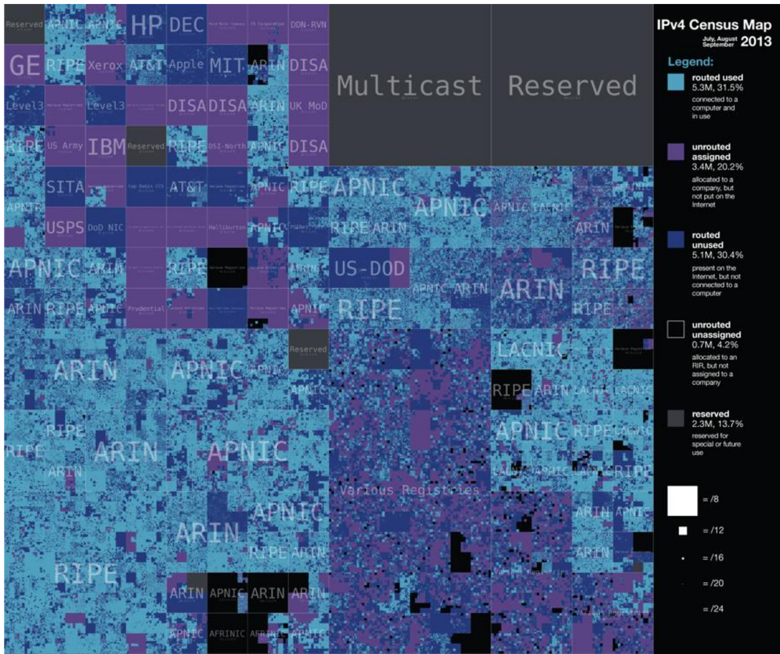
- **IPv6:** 128—bits address; lots of fixes to IPv4 limitations, and enhancements

- NAT, IoT, mobility and increase in Internet population; IPv6 is quite old, introduced in 1995 (RFC1883) but not widely used! IPv4 and v6 will continue to **co-exist** for a while!

- **Transition from IPv4 to v6** will involve the following migration techniques by IETF:
  - **Dual stack:** devices run both IPv4 and IPv6 protocol stacks simultaneously.
  - **Tunneling:** transporting an IPv6 packet over an IPv4 network. v6 packet is encapsulated inside a v4 packet.
  - **Translation: NAT64** allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique like IPv4 NAT.

- Native IPv6 use is preferred and is the ultimate goal! Tunneling and translations are only for transition period!

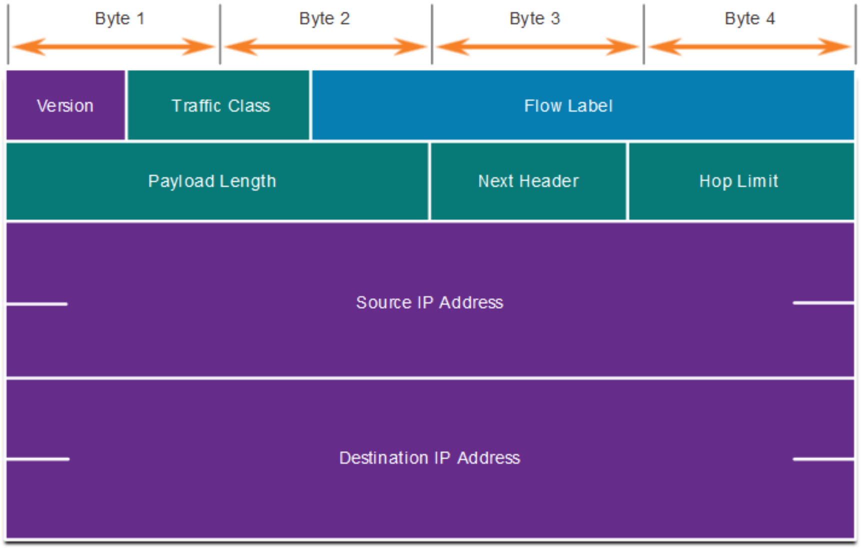
IPv4 address assignment and census map in 2013 by CAIDA



IPv6 Packet Header

- May contain **extension headers (EH)**
  - Provide optional network layer info
  - Are optional
  - Placed between IPv6 header and payload
  - May be used for fragmentation, security, mobility support, etc.

- Unlike IPv4, routers don't fragment IPv6 packets



Function	Description
Version	This will be for **v6**, as opposed to v4, a 4-bit field= **0110**
Traffic Class	Used for QoS: Equivalent to **DiffServ** – DS field
Flow Label	Informs device to handle **identical flow labels** the same way, 20-bit field **Support for resource allocation and specialized traffic!**
Payload Length	This 16-bit field indicates the length of the data portion or payload of the IPv6 packet
Next Header	I.D.s next level protocol: ICMP, TCP, UDP, etc. **Improved options mechanisms and speeding up router processing**
Hop Limit	Replaces TTL field Layer 3 hop count
Source IPv6 Address	128-bit source address
Destination IPV6 Address	128-bit destination address

IPv6 Address Format

- **IPv6 Address:** 128—bits address written in HEX; not case-sensitive; **x:x:x:x:x:x:x:x** with x (aka hextet) being 4 HEX values

```
2001:0db8:0000:1111:0000:0000:0000:0200
2001:0db8:0000:00a3:abcd:0000:0000:1234
```

- **Rule #1**: omit leading zeros -- **01ab** as **1ab**; **0a00** as **a00**; **00ab** as **ab**

Type	Format
Preferred	2001 : **0**db8 : **000**0 : 1111 : **000**0 : **000**0 : **000**0 : **0**200
No leading zeros	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200

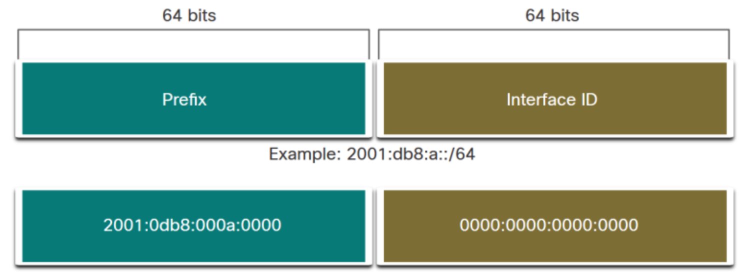
- **Rule #2**: double colon **(::)** can replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros; can only be used once within an address else ambigious!

```
2001:db8:cafe:1:0:0:0:1
2001:db8:cafe:1::1
```

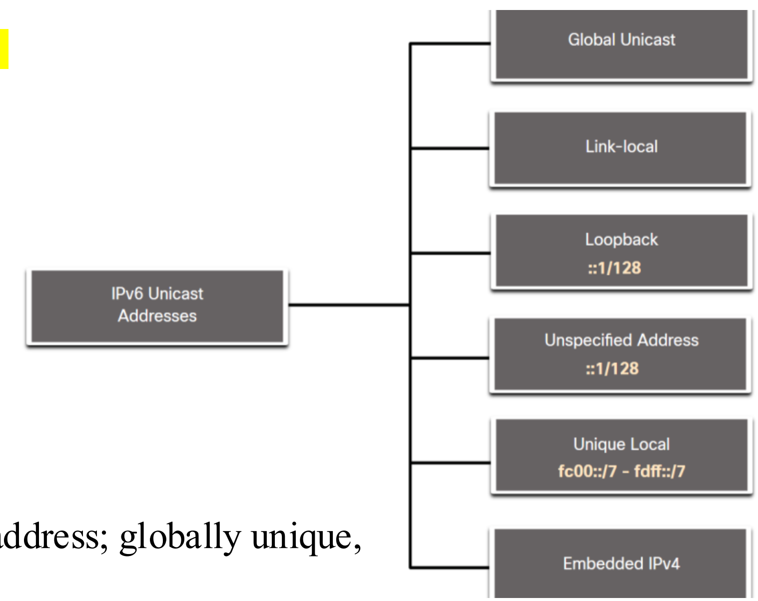
Type	Format
Preferred	2001 : **0**db8 : **000**0 : 1111 : **0000** : **0000** : **0000** : **0**200
Compressed	2001:db8:0:1111::200

IPv6 Address Types

- **IPv6 Address types:**
  - **Unicast:** uniquely identifies an IPv6-enabled device interface
  - **Multicast:** single IPv6 packet to multiple destinations.
  - **Anycast:** any IPv6 unicast address that can be assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device having that address.
  - No broadcast in IPv6 but IPv6 all-nodes multicast address works the same as broadcast!



- Prefix length can be 0-128; recommended value is /64 for LAN and most nets.
  - Because SLAAC uses /64
- Unlike IPv4, IPv6 typically has two unicast addresses



  - **Global Unicast Address (GUA):** like a public IPv4 address; globally unique, internet-routable addresses.
  - **Link-local Address (LLA):** required for every IPv6-enabled device and used to communicate with other devices on the same local link. LLAs are not routable and are confined to a single link – e.g., for automatic address config or net discovery

IP Routing

- Packets created at the *src*; each host devices creates their own **routing table**
- **Local traffic** to host interface; **remote traffic** to the **DGW** on the LAN (router or L3 switch)
- **Default Gateway (DGW) router:**
  - Same IP address range as the rest of the LAN
  - Can accept data from LAN and forward it off the LAN (i.e., another outgoing interface)
  - Can route to other networks
  - Either set statically by the host or determined through DHCP protocol in IPv4
  - IPv6 uses either router solicitation (RS) or manual config.

IPv4 Routing Table for PC1

```
C:\Users\PC1> netstat -r

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1   192.168.10.10     25
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    306
     192.168.10.0    255.255.255.0         On-link    192.168.10.10    281
    192.168.10.10  255.255.255.255         On-link    192.168.10.10    281
   192.168.10.255  255.255.255.255         On-link    192.168.10.10    281
        224.0.0.0        240.0.0.0         On-link        127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10    281
  255.255.255.255  255.255.255.255         On-link        127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10    281
```

Basic information fields in **routing table**:

- **network ID**: destination subnet
- **metric**: cost to each available route
- **next hop**: next hop, or gateway, is the address of the next station to which the packet is to be sent on the way to its final destination
- **interface**: outgoing network interface the device should use when forwarding the packet to the next hop or final destination

Routing & Route Types

Route types in IP routing table:

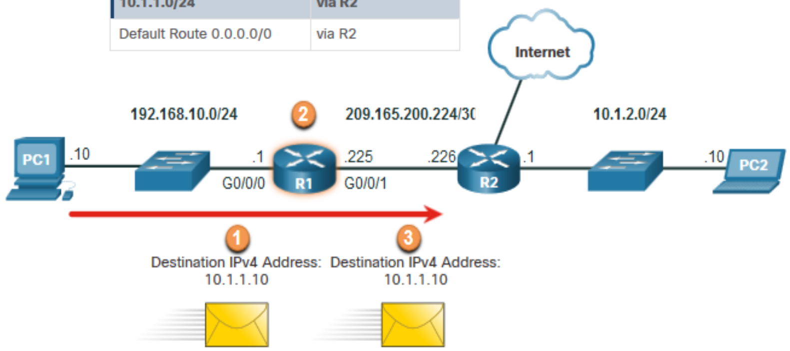
I. **Directly Connected:** automatically added by the router, with active interface with an address.

II. **Remote:** router does not have a direct connection and may be learned:
   - **Manually:** with a static route
     - Must be adjusted manually by net admin when there's a change in topo
     - Good for small networks
   - **Dynamically:** using a routing protocol

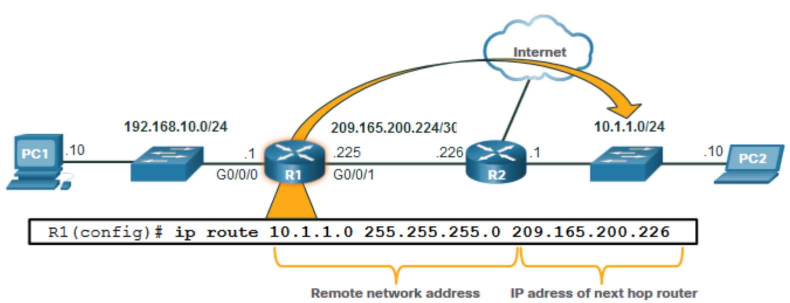
III. **Default Route:** forwards all traffic to a specific direction if no match in routing table

R1 Routing Table

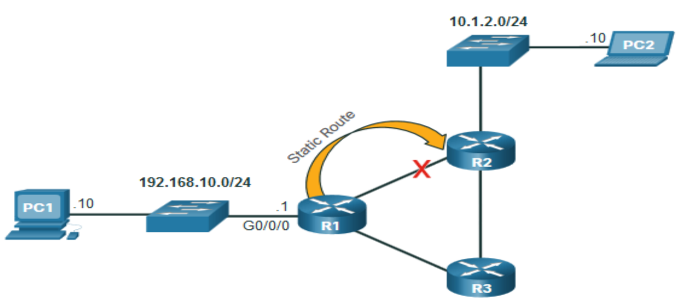
Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	**via R2**
Default Route 0.0.0.0/0	via R2



1. Packet arrives on the Gigabit Ethernet 0/0/0 interface of router R1. R1 de-encapsulates the Layer 2 Ethernet header and trailer.
2. Router R1 examines the destination IPv4 address of the packet and searches for the best match in its IPv4 routing table. The route entry indicates that this packet is to be forwarded to router R2.
3. Router R1 encapsulates the packet into a new Ethernet header and trailer, and forwards the packet to the next hop router R2.



R1 is manually configured with a static route to reach the 10.1.1.0/24 network. If this path changes, R1 will require a new static route.



If the route from R1 via R2 is no longer available, a new static route via R3 would need to be configured. A static route does not automatically adjust for topology changes.

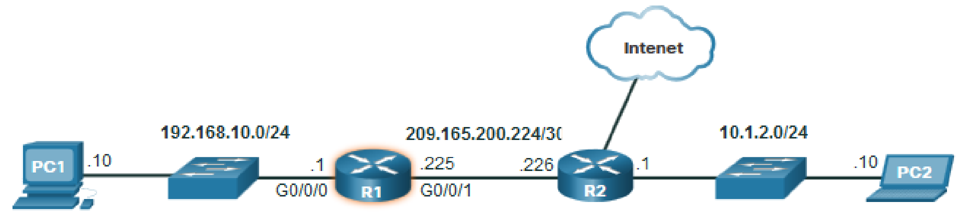
Dynamic Routing

Universitetet i Stavanger

Dynamic routing:

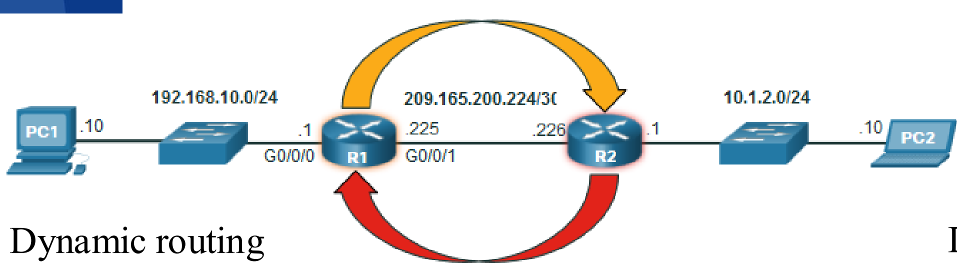
- Remote network discovery
- Maintain up-to-date info
- Select best path to destination
- Find new best path when topology changes
- Can share static default router with other routers
- DR protocols: OSPF, EIGRP,…

L – Directly connected local interface IP address
C – Directly connected network
S – Static route was manually configured by an administrator
O – OSPF (remote, dynamic)
D – EIGRP (remote, dynamic)

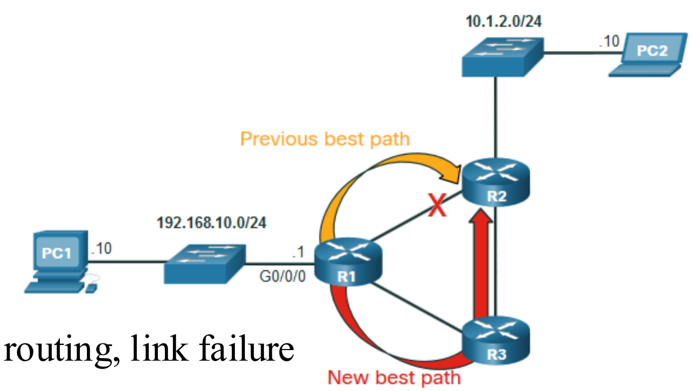


Routing table

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```



Dynamic routing



Dynamic routing, link failure

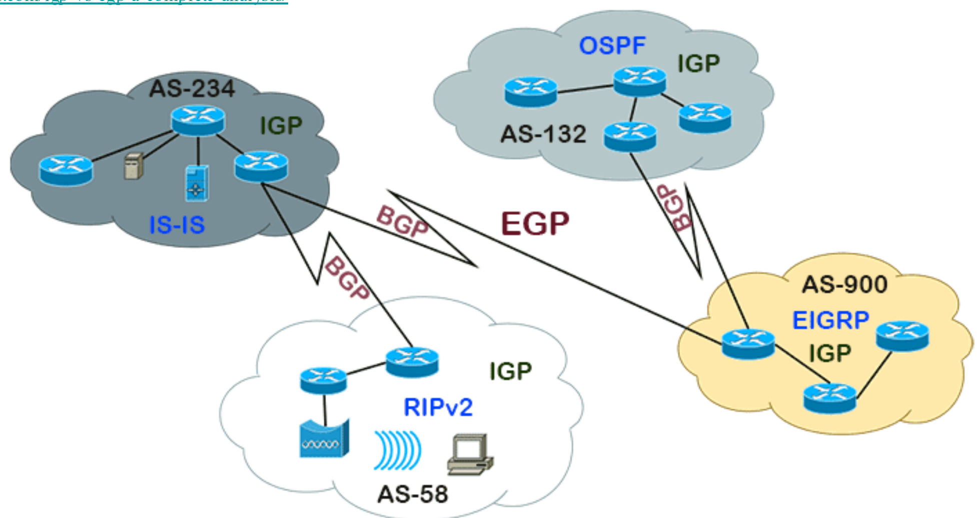
- R1 is using the routing protocol OSPF to let R2 know about the 192.168.10.0/24 network.
- R2 is using the routing protocol OSPF to let R1 know about the 10.1.1.0/24 network.

R1, R2, and R3 are using the dynamic routing protocol OSPF. If there is a network topology change, they can automatically adjust to find a new best path.

Routing Algorithms

	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector		Link-State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP

Source: https://tolumichael.com/igp-vs-egp-a-complete-analysis/



Routing algorithm type:

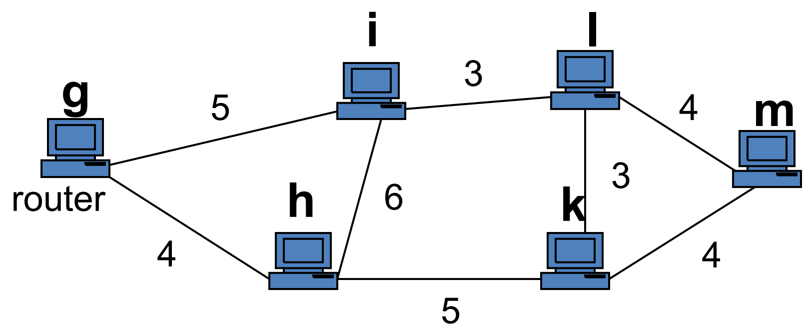
- **Distance Vector (DV):** router knows only the distance and direction – e.g., by asking neighbors.
- **Link State (LS):** router learns the full network topology. Computes the best path.
- **Path Vector (PV):** designed for inter-AS routing router advertises the entire path, instead of distance or link cost.

DV Algorithms

Distance: number of routers a packet has to pass, one router counts as one hop

- Alternative: cost related to the links

Distance Vector: each router shares its routing table with its immediate neighbors – i.e., cost/distance to every destination.



Dest.	Gateway	Cost
h	h	4
i	h	10
I	h	12
k	h	9
m	h	13

Table of g (previous)

Dest.	Gateway	Cost
g	g	5
h	h	6
l	l	3
k	l	6
m	l	7

Table of i (previous)

Dest.	Gateway	Cost
h	h	4
i	**i**	**5**
l	**i**	**8**
k	h	9
m	**i**	**12**

Table of g (modified)

DV Algorithms

DV algorithm's count-to-infinity problem!

A B C D E

A is down at the beginning.

	∞	∞	∞	∞

A comes up.

	1	∞	∞	∞ after 1 exc.
	1	2	∞	∞ after 2 exc.
	1	2	3	∞ after 3 exc.
	1	2	3	4 after 4 exc.

- *Algorithm rapidly reacts to good news.*
- *In N exchanges, everyone knows about the new router where the longest path is N hop.*

A B C D E

A is up at the beginning.

	1	2	3	4

A goes down.

	3	2	3	4 after 1 exc.
	3	4	3	4 after 2 exc.
	5	4	5	4 after 3 exc.
	5	6	5	6 after 4 exc.
	7	6	7	6 after 5 exc.
	7	8	7	8 after 6 exc.
	9	8	9	8 after 6 exc.

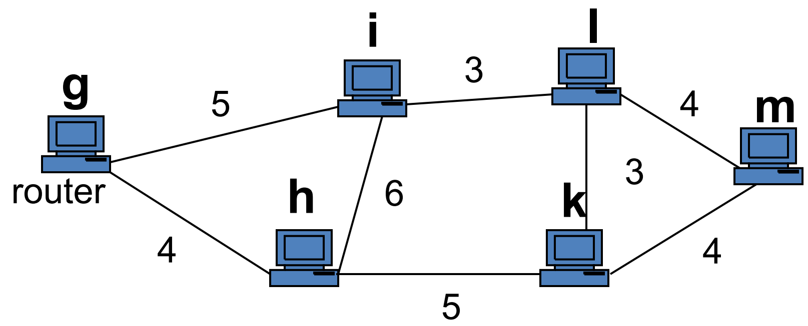
It repeats until

	∞	∞	∞	∞

- *What is infinitive?*
- *It is the highest number of hop plus 1, if the paths are measured according to the number of hops.*
- *What if we use delay?*

LS Algorithms

Link State: each router shares its own link state information with all routers in the group using multicast (e.g., flooding). Each router then computes the network topology and calculates the best path – e.g., using Dijkstra's Shortest Path First (SPF) algorithm.



g's link state

Neighbor	Cost
h	4
i	5

i's link state

Neighbor	Cost
h	6
g	5
l	3

h's link state

Neighbor	Cost
i	6
g	4
k	5

l's link state

Neighbor	Cost
i	3
m	4
k	3

k's link state

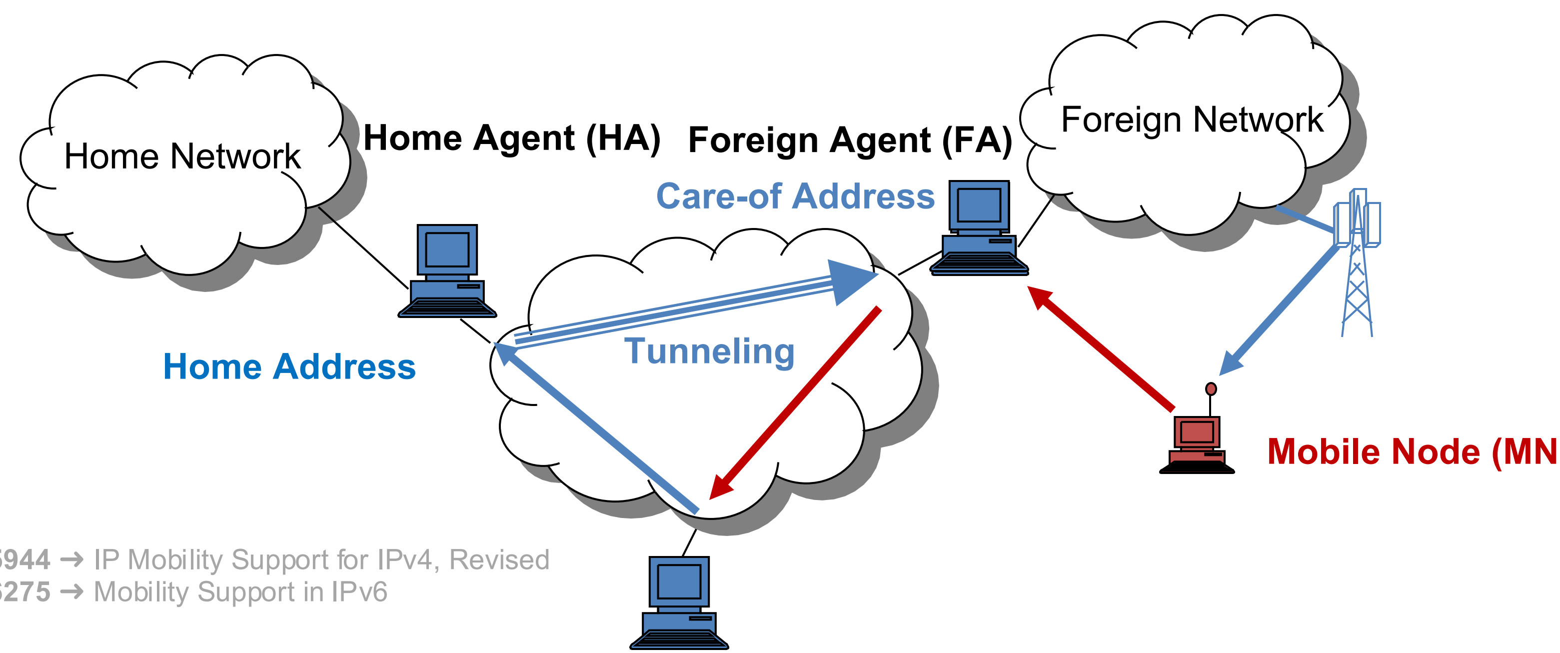
Neighbor	Cost
l	3
m	4
h	5

Mobile IP

Three basic capabilities:

1. **Discovery**: identify *home agent* and *foreign agent*
2. **Registration**: inform *home agent* of *care-of address;* MN sends a registration request to the HA
3. **Tunneling**: forward from *home address* to *care-of address* via tunnelling

- Agents periodically broadcast **agent advertisements**.
- MN can also send **Agent Solicitation message** for discovery of agent immediately
- MN learns of Care-of-Address (CoA)



RFC 5944 → IP Mobility Support for IPv4, Revised
RFC 6275 → Mobility Support in IPv6

Quality of Service Requirements

QoS requirements: different applications have different requirements – e.g., audio: low BW but OWD<150ms; MMO gaming a couple of 10s of ms; interactive video: high BW yet low latency.

QoS Techniques:

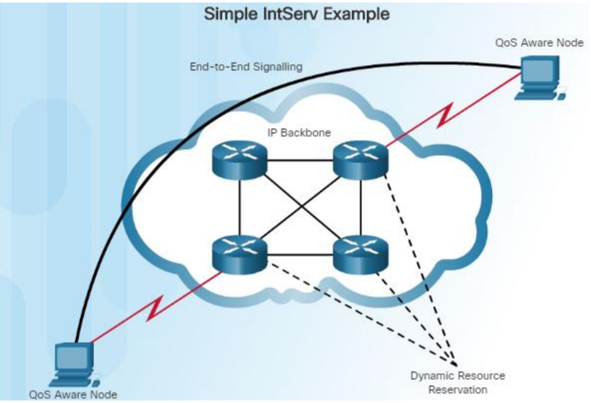
- Overprovisioning
- Buffering
- Traffic shaping
  - Leaky bucket
  - Token bucket
- Resource reservation (RSVP)
- Admission control
- Proportional routing
- Packet scheduling

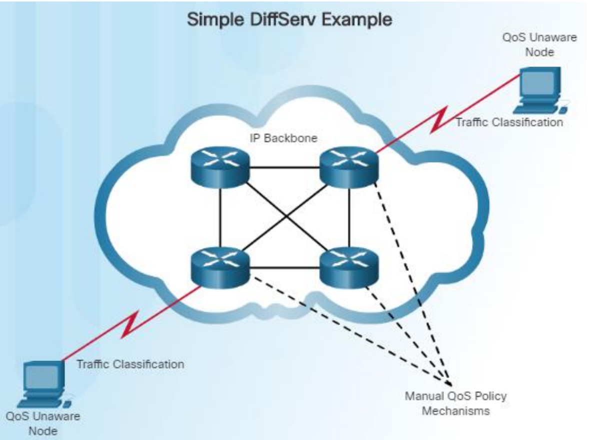
Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

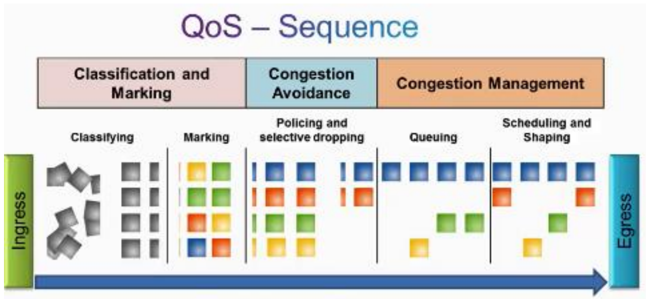
QoS Models

QoS Architectures:

1) **Best Effort (BE) – No QoS**
2) **Integrated Services (IntServ)**
   - Resource Reservation Protocol (RSVP)
   - Requires full cooperation between endpoints as well as all middleboxes along the path
3) **Differentiated Services (DiffServ)**
   - Priority-based – e.g., using DSCP codepoints in the IP packet header.
   - Shoot the packet and forget. Let the "network" decide locally on how to treat the packet.







QoS – Traffic Marking

QoS Tools	Layer	Marking Field	Width in Bits
Ethernet (802.1Q, 802.1p)	2	Class of Service (CoS)	3
802.11 (Wi-Fi)	2	Wi-Fi Traffic Identifier (TID)	3
MPLS	2	Experimental (EXP)	3
IPv4 and IPv6	3	IP Precedence	3
IPv4 and IPv6	3	Differentiated Services Code Point (DSCP)	6