1985
جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

Computer Networks

Lecture 4 : Network Layer

By : Prof. Lamri SAYAD

2026

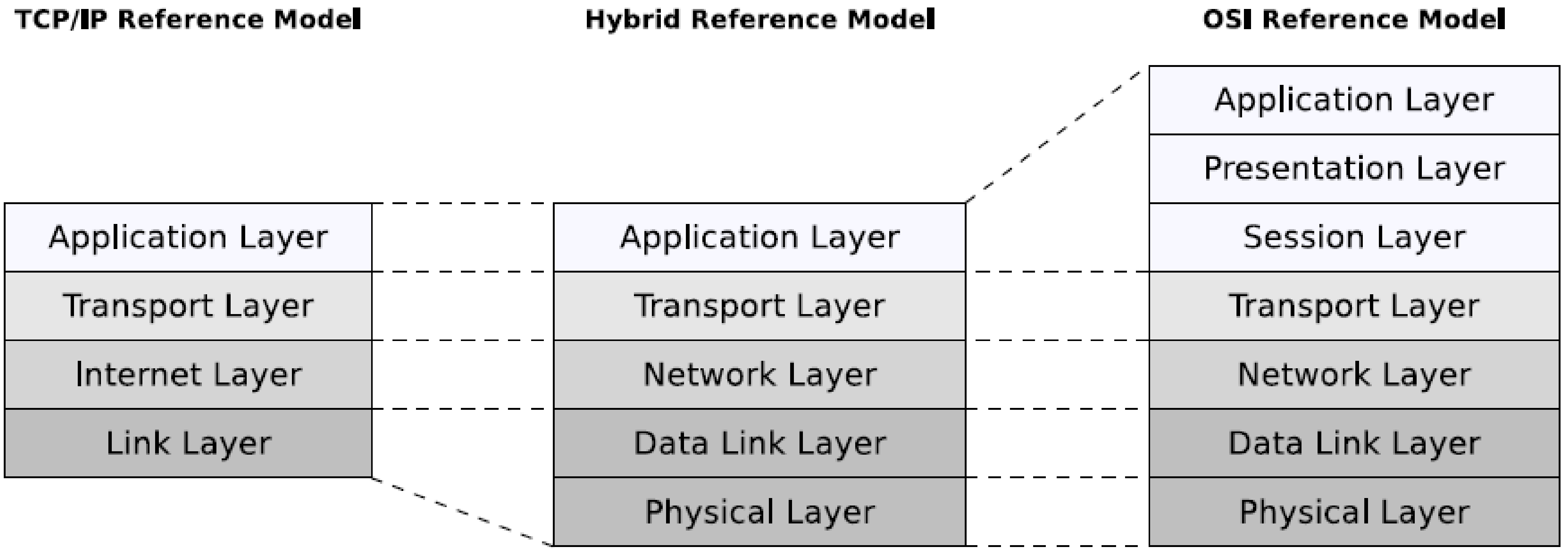
Agenda

- Network layer
  - Functions of Network layer
- Addressing in the Network Layer
  - What is logical addressing
  - Format of IP addresses
  - Classful addressing
- Subnetting
  - FLSM
  - VLSM
- Format of IP packets
- Routing
  - What is routing
  - Components of routing
  - Types of routing
  - Routing algorithms
  - Forwarding vs Routing

Agenda

- **Network layer**
  - Functions of Network layer
- Addressing in the Network Layer
  - What is logical addressing
  - Format of IP addresses
  - Classful addressing
- Subnetting
  - FLSM
  - VLSM
- Format of IP packets
- Routing
  - What is routing
  - Components of routing
  - Types of routing
  - Routing algorithms
  - Forwarding vs Routing

Network Layer in the Reference Models



Functions of Network Layer

- **Logical Addressing (IP Addressing)** : Assigns **unique logical addresses** to devices (independent of hardware).
- **Routing** : Determine the best path from source to the destination
- **Packet Forwarding (Switching) :** Moves packets from **one router to the next** along the selected path.
- **Fragmentation and Reassembly :**
  - Breaks large packets into smaller ones to match the **Maximum Transmission Unit (MTU)** of a network.
  - Reassembles them at the destination.
- **Internetworking :**
  - Connects **multiple heterogeneous networks** (LANs, WANs, etc.).
- **Congestion Control (limited in IP)** : Prevents network collapse due to excessive packets.
- **Quality of Service (QoS) Support :** Provides mechanisms to prioritize certain traffic. (Voice, Video..)

Agenda

- Network layer
  - Functions of Network layer
- **Addressing in the Network Layer**
  - What is logical addressing
  - Format of IP addresses
  - Classful addressing
- Subnetting
  - FLSM
  - VLSM
- Format of IP packets
- Routing
  - What is routing
  - Components of routing
  - Types of routing
  - Routing algorithms
  - Forwarding vs Routing

What is Logical Addressing ?

- **Definition:** Logical addressing is the assignment of **software-based, hierarchical addresses** to devices so they can be uniquely identified and reached across interconnected networks.

- **Implemented by**: Internet Protocol

- **Examples**:
  - IPv4: 192.168.1.10
  - IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Why do we need Logical Addressing ?

- Logical addressing solves key problems that **physical (MAC) addressing cannot**:

✓**Scalability**
- Supports billions of devices using hierarchical structure

✓**Routing Capability**
- Enables routers to determine paths using **network prefixes**

✓**Flexibility**
- IP addresses can change depending on the network

✓**Network Organization**
- Allows subnetting and structured design

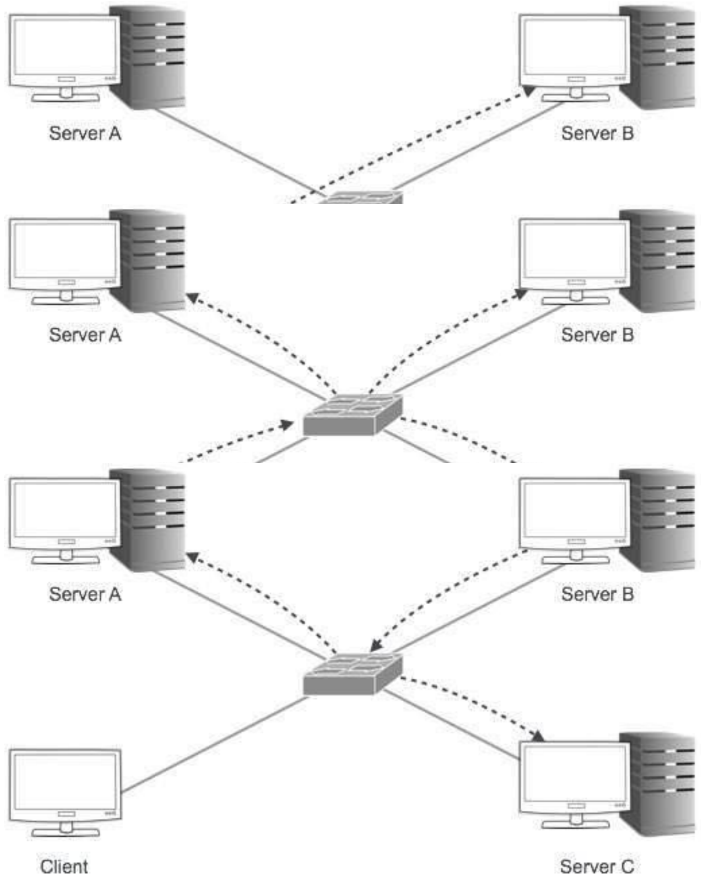
IPv4 Logical Addressing

- **Characteristics**
  - Unique numerical identifier
  - Assigned to every device connected to a network that uses the Internet Protocol (IP)
  - Written in **dotted decimal notation**
  - 32 bits or 4 bytes (the address space contains $2^{32} = 4\ 294\ 967\ 296$ possible addresses)
  - The 4 bytes are written as decimal integers in the range from 0 to 255

- **Example**: 141.52.166.25

Types Of Addressing Modes

- IPv4 supports three different types of addressing modes:
  - Unicast Addressing (one-to-one)
  - Broadcast Addressing (one-to-all)
    - The Destination Address field contains a special broadcast address, i.e. 255.255.255.255
  - Multicast Addressing (one-to-many)
    - The Destination Address contains a special address in the range 224.0.0.0 to 239.255.255.255 (class D)



Reserved IP Addresses

Some IPv4 addresses are reserved for specific uses:

- **Loopback IPs :**
  - It is reserved for looping back (when a host sends a network request to itself).
  - The IPv4 address range 127.0.0.0 to 127.255.255.255
- **Private IPs** (Non-routable on the Internet) :
  - Reserved for internal networks (LANs).
  - they cannot connect directly to internet.
  - IP Ranges:
    - 10.0.0.0 — 10.255.255.255
    - 172.16.0.0 — 172.31.255.255
    - 192.168.0.0 — 192.168.255.255
- **Public IPs**:
  - Assigned by ISPs, globally unique.
  - All other IP addresses are public. Public addresses are used to connect directly to internet.

Structure of an IP address :
Network prefix and Host number

- An IP address is divided into two parts:
- The network prefix identifies a network and the host number identifies a specific device within that network.

network prefix	host number
[Network Part]	[Host Part]

- How do we know how long the network prefix is?
  - The network prefix is implicitly defined (see class-based addressing)
  - The network prefix is indicated by a Subnet mask.

Mask (Subnet Mask)

- A **subnet mask** (or simply **mask**) is a 32-bit number used in IPv4 networking to split an IP address into :
  - **Network portion** (identifies the network)
  - **Host portion** (identifies devices on that network)
- The mask is written in dotted-decimal notation (like an IP address) or CIDR notation (e.g., /24).
- The mask "hides" (masks) the host part of the IP address, leaving only the network identifier.
- A 1 in the mask means "this bit belongs to the network."
- A 0 means "this bit belongs to the host."
- Hosts per networ $k = 2^h - 2$ (***h*** = number of host bits)

- **Why Use a Mask?**
  - **Routing Efficiency:** Helps routers determine if a destination is on the same network or needs forwarding.
  - **Network Segmentation:** Splits large networks into smaller subnets (e.g., VLANs).
  - **Security:** Isolates traffic between subnets (e.g., separating guest Wi-Fi from internal LANs).

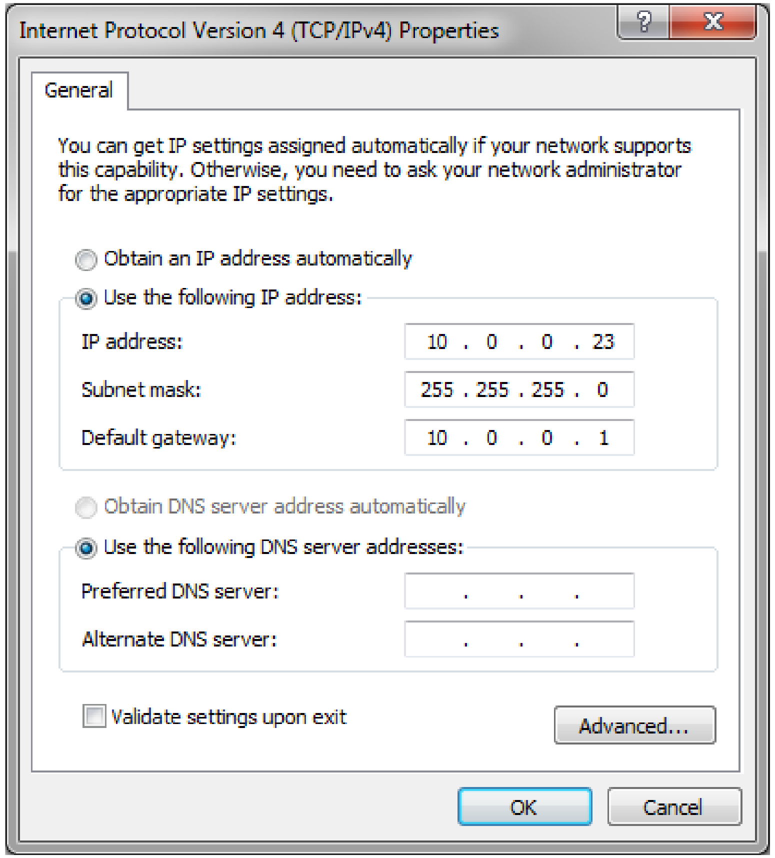
Mask (Subnet Mask)

- **Example**:
  - IP Address: 192.168.1.100
  - Subnet Mask: 255.255.255.0 (/24 in CIDR)

  - In binary:

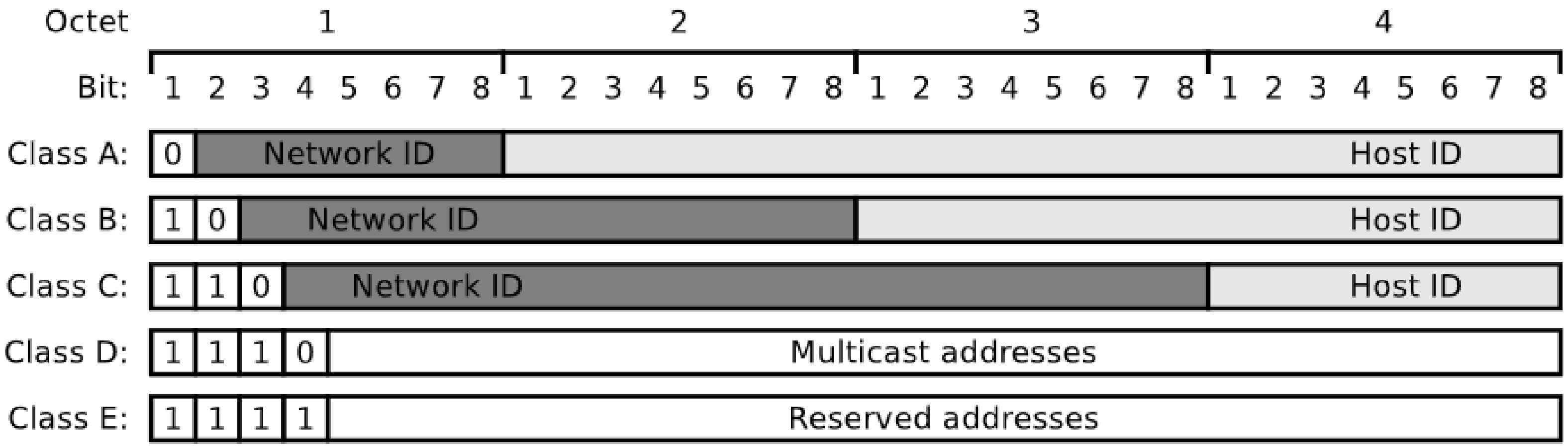
    IP: 11000000 . 10101000 . 00000001 . 01100100
    Mask: 11111111 . 11111111 . 11111111 . 00000000

  - The first 24 bits (255.255.255) define the network (192.168.1.0).
  - The last 8 bits (0) define hosts (.100 in this case).


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
10 . 0 . 0 . 23
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
10 . 0 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

Classful Addressing (1/5)

- Before CIDR, IPv4 used a **class-based system** to divide address space into fixed categories called **classes**.
- Each class defines:
  - The **default division** between network and host parts
  - The **size of the network**
- IPv4 addresses are categorized into 5 classes from A to E, but only the classes A, B and C are relevant in practice.
- Address classes
  - Class A: 7 bits for the network ID and 24 bits for the host ID
  - Class B: 14 bits for the network ID and 16 bits for the host ID
  - Class C: 21 bits for the network ID and 8 bits for the host ID



Classful Addressing (2/5)

- The prefixes specify the address classes and their address ranges

Class	Prefix	Address Range	Default Subnet Mask	Purpose
A	0	0.0.0.0 – 127.255.255.255	255.0.0.0 (/8)	Large networks (e.g., ISPs)
B	10	128.0.0.0 – 191.255.255.255	255.255.0.0 (/16)	Medium networks (e.g., enterprises)
C	110	192.0.0.0 – 223.255.255.255	255.255.255.0 (/24)	Small networks (e.g., LANs)
D	1110	224.0.0.0 – 239.255.255.255	**No subnet mask**	**Multicast** (not for hosts)
E	1111	240.0.0.0 – 255.255.255.255	**Reserved/Experimental**	Never used publicly

- 2^7 = 128 class A networks with a maximum of 2^{24} = 16 777 216 host addresses each
- 2^{14} = 16 384 class B networks with a maximum of 2^{16} = 65 536 host addresses each
- 2^{21} = 2 097 152 class C networks with a maximum of 2^8 = 256 host addresses each
- Class D contains multicast addresses (e.g. for IPTV)
- Class E is reserved for future purposes and experiment

Classful Addressing (3/5)

Reserved IP Addresses

- Some IPv4 addresses are reserved for specific uses:
  - **Loopback IPs**: The IPv4 address range 127.0.0.0 to 127.255.255.255 is reserved for looping back, which is when a host sends a network request to itself.
  - **Private IPs**: The IP ranges 10.0.0.0 — 10.255.255.255 , 172.16.0.0 — 172.31.255.255 , and 192.168.0.0 — 192.168.255.255 are designated private network addresses, meaning they cannot connect directly to internet.
  - **Public IPs**: All other IP addresses are public. Public addresses are used to connect directly to internet.

Classful Addressing (4/5)

- This approach causes some drawbacks
- **Problems of Classful Addressing**:
  - **Problem 1**. Too few network addresses for large networks
    - Class A and Class B addresses are gone
  - **Problem 2**. Two-layer hierarchy is not appropriate for large networks with Class A and Class B addresses.
    - **Fix #1: Subnetting :** Logical networks are divided into subnets
  - **Problem 3**. Inflexible. Assume a company requires 2,000 addresses
    - Class A and B addresses are overkill
    - Class C address is insufficient (requires 8 Class C addresses)
    - Fix #2: Classless Interdomain Routing (CIDR)

Classful Addressing (5/5)

- **Problem 4**: Exploding Routing Tables: Routing on the backbone Internet needs to have an entry for each network address. In 1993, the size of the routing tables started to outgrow the capacity of routers.
  - Fix #2: Classless Interdomain Routing (CIDR)
- **Problem 5**. The Internet is going to outgrow the 32-bit addresses
  - Fix #3: IP Version 6

Transition to CIDR

- Because of these limitations:

☞ Classful addressing was replaced by:

- **CIDR (Classless Inter-Domain Routing)**

  CIDR is a method of IP addressing that **removes the concept of fixed classes (A, B, C)** and allows **flexible allocation of IP addresses using variable-length prefixes**.

- Enables:
  - Flexible subnetting
  - Efficient IP allocation
  - Smaller routing tables

Transition to CIDR

- **CIDR Notation**

CIDR represents an IP address with a **prefix length**:

192.168.1.0/26

☞ Meaning:

- First **26 bits** → network part
- Remaining bits → host part

CIDR vs Classful Addressing

Feature	Classful	CIDR
Structure	Fixed classes	Flexible
Masks	/8, /16, /24	Any (/0 to /32)
Efficiency	Low	High
Used today	✗ No	✓ Yes

CIDR is what **enables modern subnetting**

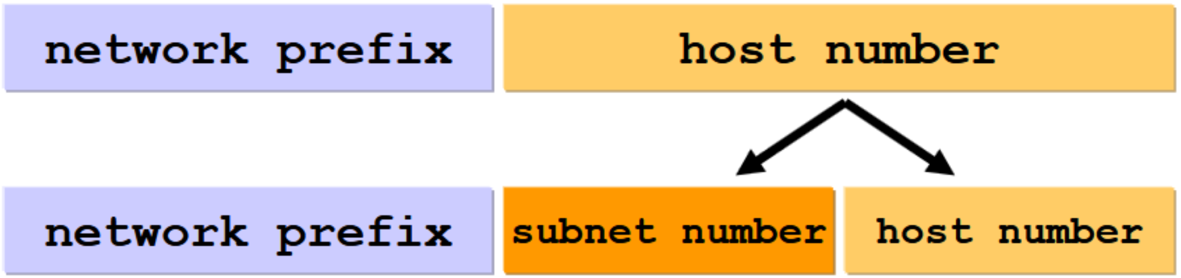
Agenda

- Network layer
  - Functions of Network layer
- Addressing in the Network Layer
  - What is logical addressing
  - Format of IP addresses
  - Classful addressing
- **Subnetting**
  - FLSM
  - VLSM
- Format of IP packets
- Routing
  - What is routing
  - Components of routing
  - Types of routing
  - Routing algorithms
  - Forwarding vs Routing

Subnetting (1/2)

- **What is Subnetting**
  - **Subnetting** is the process of dividing a **large IP network** into **smaller, more manageable subnetworks** (called *subnets*). Each subnet functions as its own smaller network, allowing better **organization, security, and efficient IP address usage**.

- **How Subnetting Works**
  - Subnetting works by **"borrowing" bits from the host portion** to create more network IDs (subnets).



Subnetting (2/2)

Key Formulas

- Number of Subnets

$$2^n$$

- Number of Hosts per Subnet

$$2^h - 2$$

Where:

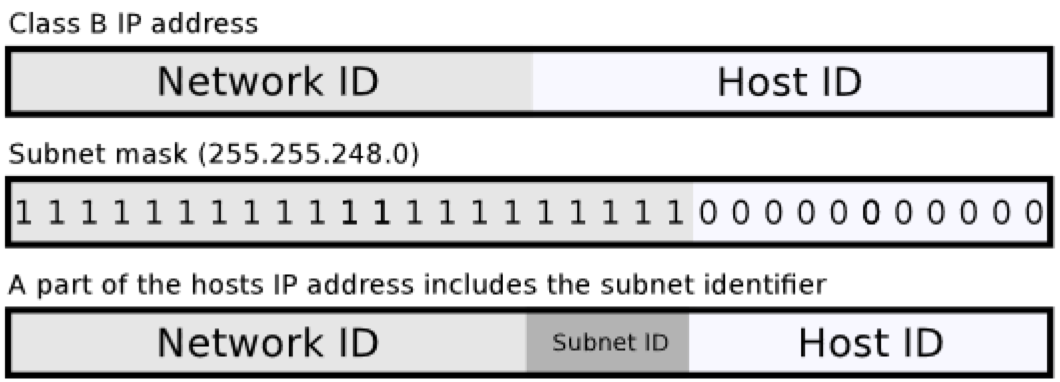
- ***n*** = number of borrowed bits
- ***h*** = remaining host bits

Subnet Mask (1/2)

- For creating subnets, a **(sub-)netmask** is required
  - All hosts in a network have a subnet mask assigned
    - Length: 32 bits (4 bytes)
    - It is used to specify the number of subnets and hosts
- The subnet mask splits the host ID of an IP address into **subnet ID** and **host ID**
  - The network ID remains unchanged
  - The network mask adds another level of hierarchy into the IP address

Subnet Mask (2/2)

- Structure of the subnet mask:
  - 1-bits indicate, which part of the address space is used for subnet IDs
  - 0-bits indicate, which part of the address space is used for host IDs
- **Example**: Splitting a class B network into 20 subnets requires 5 bits
  - Each subnet requires its own subnet ID and it must be represented in binary form
  - If 5 bits are used for the representation of the subnet IDs, 11 bits remain for host IDs



Subnetting Methods

- The most common Subnetting approaches:
  - **Fixed-Length Subnet Mask (FLSM)**
  - **Variable-Length Subnet Mask (VLSM)**
  - **Classless Inter-Domain Routing (CIDR)**

FLSM

- **Definition:** is a subnetting method where **all subnets within a network have the same size** (i.e., the same number of host addresses). This means every subnet uses an **identical subnet mask**, making it simple but sometimes inefficient for IP allocation.

- **Use Case**:
  - When all subnets require an equal number of hosts (e.g., branch offices with similar sizes).

✓ **Pros:** Simple to implement.
❌ **Cons:** Wastes IPs if subnets don’t need equal hosts.

FLSM

- Algorithm (steps) :
  1. Step 1: Identify Requirements (Number of subnets OR hosts)
  2. Step 2: Determine Borrowed Bits ($2^n \geq$ required subnets)
  3. Step 3: Calculate New Mask (Add borrowed bits to original prefix)
  4. Step 4: Determine Hosts per Subnet ($2^h - 2$)
  5. Step 5: Determine Subnet Increment (Magic Number)
     - 256 – subnet mask value (in the interesting octet)

  6. Step 6: List All Subnets
     - Generate network addresses
     - Identify:
       - ✓ First host
       - ✓ Last host
       - ✓ Broadcast

FLSM

- **Example**:
  - Given:
    - Network: 192.168.1.0/24
    - Subnet Mask: 255.255.255.0
    - Total IPs: 256 (254 usable hosts).
  - Goal:
    - Split into 4 equal subnets (FLSM).
- **Solution**:
  - Step 1: Determine New Subnet Mask
    - To create 4 subnets, we need 2 extra bits (since $2^2 = 4$).
    - Original mask: /24 (255.255.255.0)
    - New mask: /26 (255.255.255.192)
  - Step 2: Calculate Subnet Ranges

Subnet	Network Address	Subnet Mask	Usable Host Range	Broadcast Address
Subnet 1	192.168.1.0	255.255.255.192 or /26	192.168.1.1 – 192.168.1.62	192.168.1.63
Subnet 2	192.168.1.64	255.255.255.192 or /26	192.168.1.65 – 192.168.1.126	192.168.1.127
Subnet 3	192.168.1.128	255.255.255.192 or /26	192.168.1.129 – 192.168.1.190	192.168.1.191
Subnet 4	192.168.1.192	255.255.255.192 or /26	192.168.1.193 – 192.168.1.254	192.168.1.255

VLSM

- **Definition:** is an advanced subnetting technique that allows different subnets within the same network to use **different subnet masks**. Unlike FLSM, VLSM creates **custom-sized subnets** based on actual host requirements, minimizing IP wastage.

- **Key Characteristics of VLSM**
  - Different Subnet Masks in the Same Network
  - Optimized IP Usage
  - Supports Hierarchical Networking

- **When to Use VLSM?**
  - **Networks with varying host requirements** (e.g., data centers + small branch offices).
  - **ISP allocations** (to assign blocks efficiently to customers).
  - **Large enterprises** (where IP conservation is critical).

VLSM

- **Algorithm (steps)**
  1. Step 1: Sort Requirements (Arrange subnets by **largest to smallest**)
  2. Step 2: Allocate Largest Subnet First
     - Apply formula : $2^h - 2 \geq$ required hosts ☞ Find smallest subnet that fits
  3. Step 3: Assign Address Block
     - Start from beginning of network
     - Reserve required address range
  4. Step 4: Move to Next Subnet
     - Continue from **next available address**
  5. Step 5: Repeat Until Done

VLSM

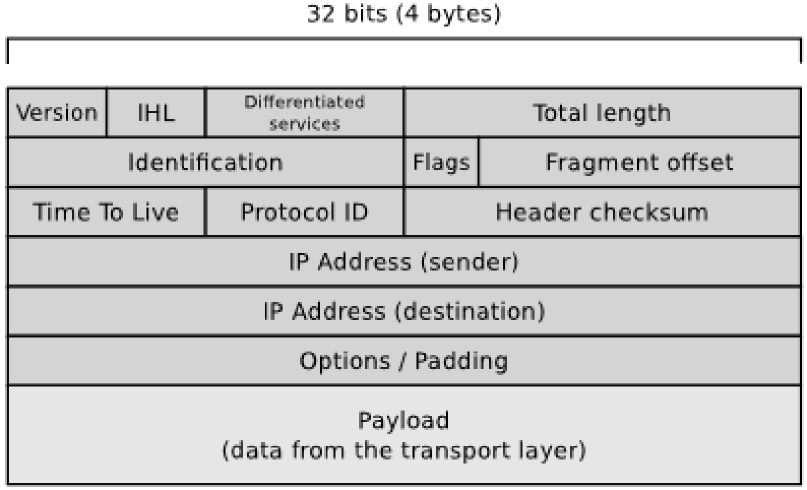
- **Example**:
  - Network: 192.168.1.0/24
  - Requirements:
    - Subnet A: 60 hosts
    - Subnet B: 30 hosts
    - Subnet C: 10 hosts
    - Subnet D: 2 hosts (for a router-to-router link).
- **Solution**:
  - **Step 1: Sort Requirements from Largest to Smallest**
    - Subnet A (60 hosts)
    - Subnet B (30 hosts)
    - Subnet C (10 hosts)
    - Subnet D (2 hosts)
  - **Step 2: Assign Subnets Based on Host Needs**

Subnet	Hosts Needed	Subnet Mask	Usable Hosts	Network Range
A	60	/26 (255.255.255.192)	62	192.168.1.0/26 (1-62)
B	30	/27 (255.255.255.224)	30	192.168.1.64/27 (65-94)
C	10	/28 (255.255.255.240)	14	192.168.1.96/28 (97-110)
D	2	/30 (255.255.255.252)	2	192.168.1.112/30 (113-114)

Agenda

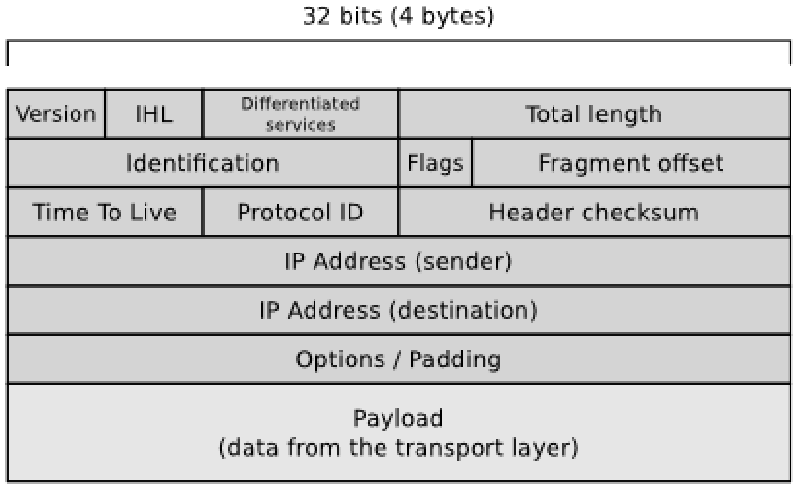
- Network layer
  - Functions of Network layer
- Addressing in the Network Layer
  - What is logical addressing
  - Format of IP addresses
  - Classful addressing
- Subnetting
  - FLSM
  - VLSM
- **Format of IP packets**
- Routing
  - What is routing
  - Components of routing
  - Types of routing
  - Routing algorithms
  - Forwarding vs Routing

Structure of IPv4 Packets (1/6)



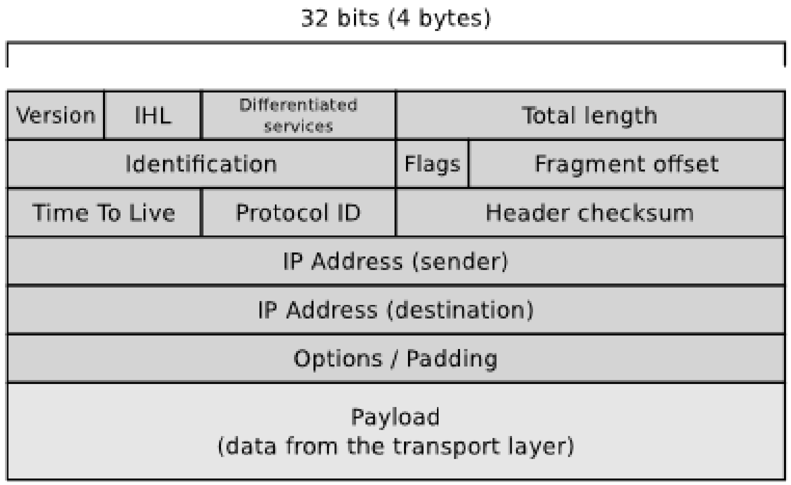
- **Version** = (4 bits)
  - Protocol version
    - Version = 4 ==⇒ IPv4
    - Version = 6 ==⇒ IPv6
- **IHL** = IP Header Length (4 bits)
  - Header length, represented as the number of 4 byte words
    - Example: IHL = 5 ==⇒ 5 ∗ 4 bytes = 20 bytes
  - Indicates where the payload begins
- **Differentiated services** (8 bits)
  - Prioritization of IP packets is possible with this field (Quality of Service)
  - The field slightly changed over the years (RFC 791, RFC 2474, RFC 3168

Structure of IPv4 Packets (2/6)



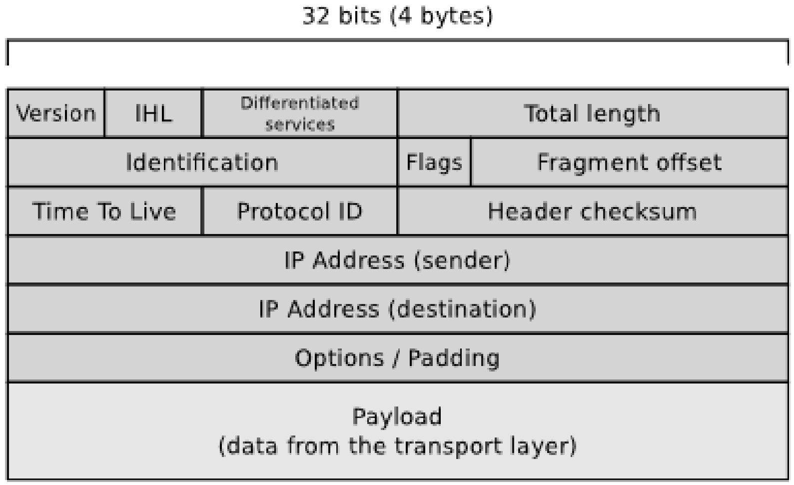
- **Total length** (16 bits)
  - This field defines the entire packet size (header and payload)
  - This length of the field is 16 bits and therefore the maximum possible IPv4 packet length is 65 535 bytes

Structure of IPv4 Packets (3/6)



- The fields **Identification, Flags** and **Fragment Offset** control the assembly of fragmented IP packets
- **Identification** (16 bits)
  - Contains a unique identifier of the IP packet
- **Flags** (3 bits)
  - Here the sender informs whether the packet can be fragmented and the receiver is informed whether more fragments follow
- **Fragment Offset** (13 bits)
  - Contains a number which states for fragmented packets, from which position of the unfragmented packet the fragment begins

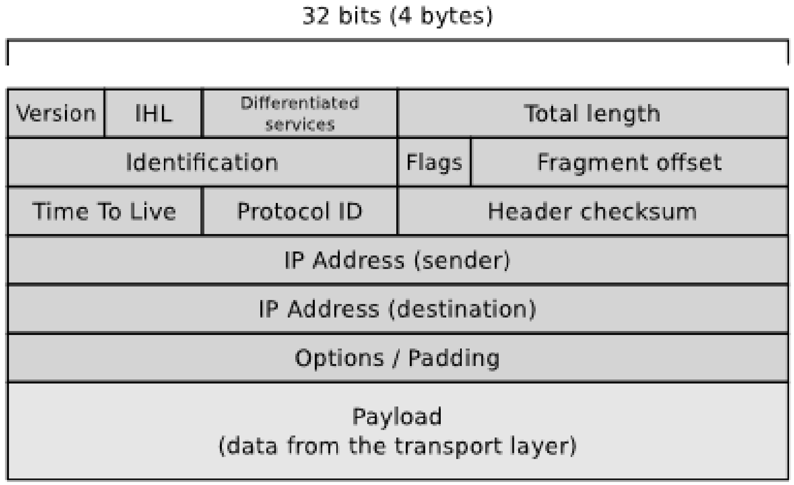
Structure of IPv4 Packets (4/6)



- **Time To Live** (8 bits)
  - Contains the maximum number of hops
    - Each Router on the route to the destination decrements the value by one
  - Prevents that undeliverable IP packets endlessly go in cycles in the network

Structure of IPv4 Packets (5/6)

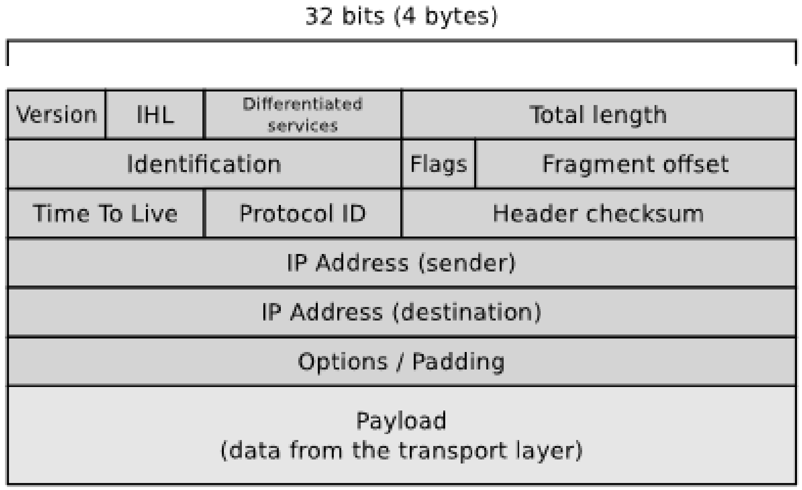
- **Protocol ID** (8 bits)
  - Contains the number of the Transport Layer protocol used
  - TCP segments ==⇒ 6
  - UDP segments ==⇒ 17
  - ICMP message ==⇒ 1
  - OSPF message==⇒ 89



- Each IPv4 packet contains a checksum (16 bits) of the header
  - Because at each Router on the way to the destination, the content of the field Time To Live changes, each Router needs to verify the checksum, recalculate and insert it into the header

Structure of IPv4 Packets (6/6)

- The field **IP address (sender)** (32 bits) contains the source address and **IP address (destination)** contains the destination address
- The field **Options / Padding** can contain additional information such as a time stamp
  - This last field before the payload area is filled with padding bits (0 bits) if necessary, to ensure that the header size is an integer number of 32 bit words
  - The last field contains the data from the Transport Layer



Agenda

- Network layer
  - Functions of Network layer
- Addressing in the Network Layer
  - What is logical addressing
  - Format of IP addresses
  - Classful addressing
- Subnetting
  - FLSM
  - VLSM
- Format of IP packets
- **Routing**
  - What is routing
  - Components of routing
  - Types of routing
  - Routing algorithms
  - Forwarding vs Routing

What is routing?

- **Routing** is the process of selecting the **best path** to send a packet from the **source** to the **destination** across one or more networks.

- **Key points:**
  - Occurs at **Layer 3 (Network Layer)**
  - Works with **IP addresses** (logical addressing)
  - Uses **routing tables** to make forwarding decisions

Components of routing

Routing involves several components:

1. **Routing Table**
   - Stores network destinations and associated next-hop information
2. **Routing Algorithm / Protocol**
   - Determines how to build and maintain routing tables
   - Examples:
     - Static routing (manually configured)
     - Dynamic routing (learned via protocols)
3. **Forwarding Function**
   - Actual process of sending the packet to the next hop

Routing table

- Typical entries in a routing table include:

Field	Description
Destination Network	IP network address (e.g., 192.168.2.0/24)
Subnet Mask	Defines network portion
Next Hop	IP of next router
Interface	Router interface to send packet
Metric / Cost	Determines preference (lower = better)

- Example Table:

Destination	Mask	Next Hop	Interface	Metric
192.168.1.0	255.255.255.0	–	FastEthernet0/0	0
10.0.0.0	255.0.0.0	192.168.1.1	FastEthernet0/1	1

Types of routing

- **Static Routing**
  - Routes are **manually configured** by the network administrator
  - Simple, predictable
  - Not suitable for large/dynamic networks
  - **Example** : ip route 10.0.0.0 255.0.0.0 192.168.1.1

- **Dynamic Routing**
  - Routes are **automatically learned** via routing protocols
  - Responds to **network changes**
  - Common protocols:
    - **RIP** (Routing Information Protocol) → Distance-vector
    - **OSPF** (Open Shortest Path First) → Link-state
    - **EIGRP** (Enhanced Interior Gateway Routing Protocol) → Hybrid

Forwarding

- Primary task of Routers: **Forwarding** IP packets
  - To carry out this task, Routers must determine for each incoming packet, the correct port
- Each Router maintains a local **routing table**
  - The routing table contains. . .
    - the **logical networks**, a Router knows about
    - the information, which logical network can be accessed via which **port**
- A Router transmits the IP packets in the direction, which is specified in the routing table

Path Determination (Routing)

- The **path determination (routing)** is the process of creating **routing tables** by using **routing protocols**
  - The routing tables are necessary for calculating the best path, which allows to reach the destination at the lowest cost possible
  - The routing protocols are carried out between the Routers
  - Routing protocols base on distributed algorithms
    - Reason: scalability

- 2 major classes of routing protocols exist:
  - **Distance-vector routing protocols** (implement the Bellman-Ford algorithm)
    - Example: Routing Information Protocol (RIP)
  - **Link-state routing protocols** (implement the Dijkstra algorithm) Example: Open Shortest Path First (OSPF)

Routing tables

- Each router and each host keeps a routing table which tells the router how to process an outgoing packet
- Main columns:
  1. Destination address: where is the packet going to?
  2. Next hop or interface: how to send the packet?
- Routing tables are set so that a packet gets closer to the its destination every hop

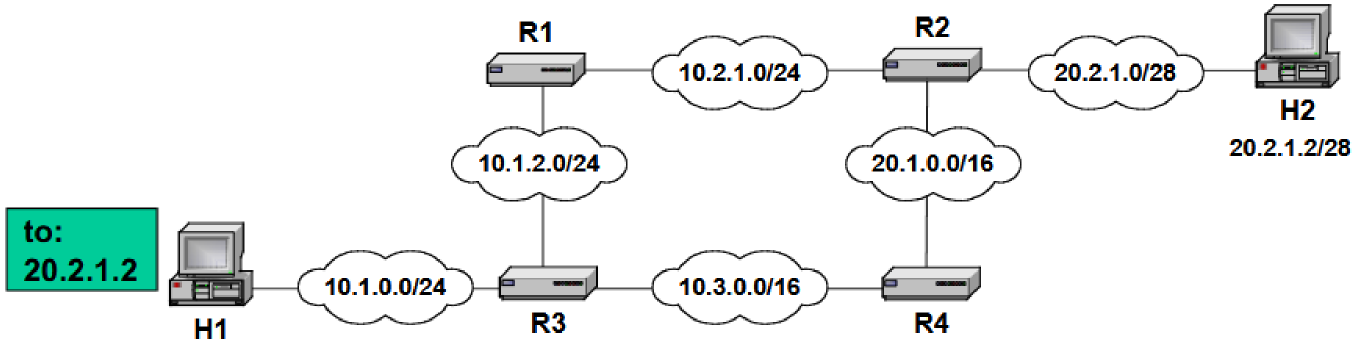
Destination	**Next Hop**
10.1.0.0/24	direct
10.1.2.0/24	direct
10.2.1.0/24	R4
10.3.1.0/24	direct
20.1.0.0/16	R4
20.2.1.0/28	R4

Example

Destination	Next Hop
10.1.0.0/24	R3
10.1.2.0/24	direct
10.2.1.0/24	direct
10.3.1.0/24	R3
20.2.0.0/16	R2
30.1.1.0/28	R2

Destination	Next Hop
10.1.0.0/24	R1
10.1.2.0/24	R1
10.2.1.0/24	direct
10.3.1.0/24	R4
20.1.0.0/16	direct
20.2.1.0/28	direct

Destination	Next Hop
10.1.0.0/24	R2
10.1.2.0/24	R2
10.2.1.0/24	R2
10.3.1.0/24	R2
20.1.0.0/16	R2
20.2.1.0/28	direct



Destination	Next Hop
10.1.0.0/24	direct
10.1.2.0/24	R3
10.2.1.0/24	R3
10.3.1.0/24	R3
20.1.0.0/16	R3
20.2.1.0/28	R3

Destination	Next Hop
10.1.0.0/24	direct
10.1.2.0/24	direct
10.2.1.0/24	R4
10.3.1.0/24	direct
20.1.0.0/16	R4
20.2.1.0/28	R4

Destination	Next Hop
10.1.0.0/24	R3
10.1.2.0/24	R3
10.2.1.0/24	R2
10.3.1.0/24	direct
20.1.0.0/16	direct
20.2.1.0/28	R2

Longest Prefix Match

- **Longest Prefix Match:** Search for the routing table entry that has the longest match with the prefix of the destination IP address

1. Search for a match on all 32 bits
2. Search for a match for 31 bits

   …..

32. Search for a mach on 0 bits

128.143.71.21

↓

Destination address	Next hop
10.0.0.0/8	R1
128.143.0.0/16	R2
128.143.64.0/20	R3
128.143.192.0/20	R3
128.143.71.0/24	R4
128.143.71.55/32	R3
default	R5

↓

The longest prefix match for 128.143.71.21 is for 24 bits with entry 128.143.71.0/24

Datagram will be sent to R4

Routing table of Windows workstation

```
C:\Users\DELL>route print
===========================================================================
Liste d'Interfaces
  7...e4 b9 7a 4c 84 e9 ......Intel(R) Ethernet Connection (4) I219-LM
 16...18 1d ea 6b b1 98 ......Microsoft Wi-Fi Direct Virtual Adapter
 11...1a 1d ea 6b b1 97 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  5...18 1d ea 6b b1 97 ......Intel(R) Dual Band Wireless-AC 8265
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Table de routage
===========================================================================
Itinéraires actifs :
Destination réseau    Masque réseau  Adr. passerelle   Adr. interface Métrique
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.110     50
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.0.0    255.255.255.0         On-link     192.168.0.110    306
    192.168.0.110  255.255.255.255         On-link     192.168.0.110    306
    192.168.0.255  255.255.255.255         On-link     192.168.0.110    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     192.168.0.110    306
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link     192.168.0.110    306
===========================================================================
```

Routing protocols

- **Routing protocol**— is a network protocol used by routers (routers) for the purpose of determining data transmission routes in a computer network
- Routing protocols are divided into two types depending on the area of application:
  - **Interior Gateway Protocol(IGP)** - intra-domain routing (RIP,OSPF);
  - **External Gateway Protocol(EGP)** - interdomain routing (EGP,BGP).
- Also, routing protocols are divided into three types depending on the types of algorithms that build routes in the network:
  - **Source or Policy Based Algorithm**– source routing algorithms (IPAndACL).
  - **Distance Vector Algorithm(DVA)** - distance vector protocols (RIP, EGP, IGRP,BGP);
  - **Link State Algorithm(LSA)** - link state protocols (OSPF).

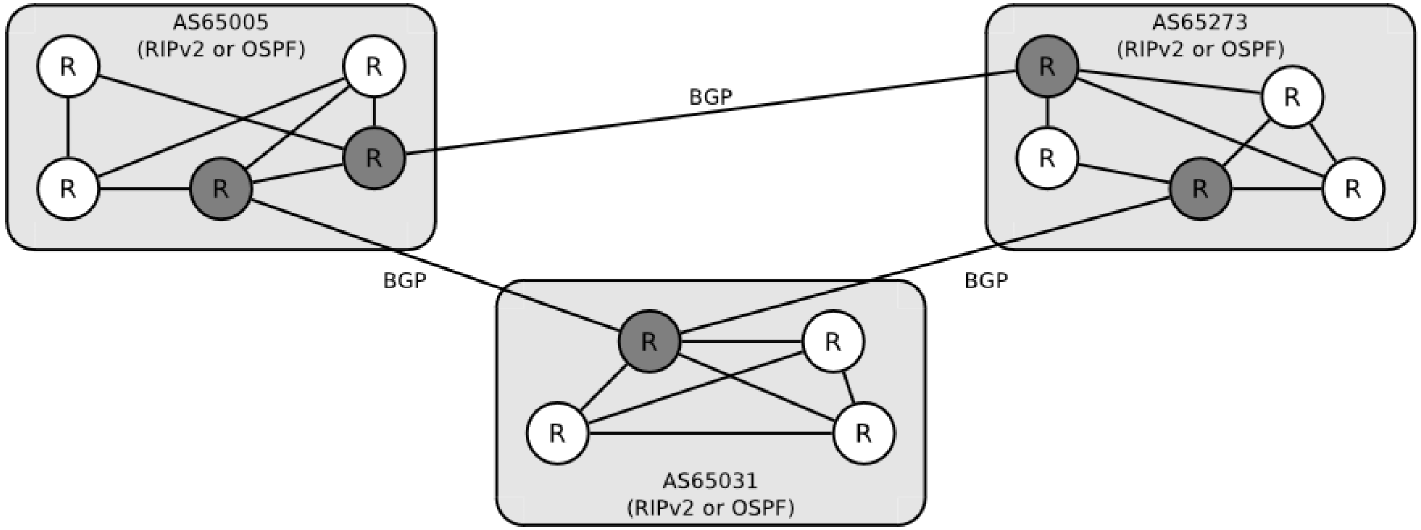
Autonomous Systems

- Routers are organized in Autonomous Systems (AS)
  - Each AS consists of a group of logical networks, which. . .
    - use the Internet Protocol (IP)
    - are operated and managed by the same organization (e.g. an Internet Service Provider, a corporation or university)
    - use the same routing protocol
  - The interconnected AS in their totality form the internet

- Each AS has a unique Autonomous System Number (ASN)
  - The ASNs are assigned by the Internet Assigned Numbers Authority (IANA) in blocks to the Regional Internet Registries
  - The Regional Internet Registries assign ASNs to entities inside their areas

Intra-AS-Routing and Inter-AS-Routing

- For the routing inside AS (⇒ Intra-AS routing), the operators of the AS themselves are responsible
  - Protocols for intra-AS routing are e.g. RIP and OSPF
- For the routing between AS (⇒ inter-AS routing), the BGP is used



Distance-Vector Routing Protocols (1/3)

- Implement the Bellman-Ford algorithm
- Example: **Routing Information Protocol** (RIP)
  - RIP allows routing inside autonomous systems (**Intra-AS-Routing**)
- Functioning of RIP:
  - Every Router sends during initialization via all its ports a RIP request via broadcast
    - This way, the new Router requests all neighboring (accessible) Routers to transmit their routing tables
  - With the routing information from the incoming RIP responses, the Router fills its local routing table with entries

Distance-Vector Routing Protocols (2/3)

- Functioning of RIP (continuation):
  - Every 30 seconds, each Router sends its routing table via the connectionless Transport Layer protocol UDP to its direct neighbors
    - This periodic message is called advertisement
  - If a Router receives an advertisement, it checks whether the message contains entries, which are better than the entries in the routing table
    - If the received advertisement contains better routes, the Router updates the appropriate entries in its local routing table
  - In addition to the periodic advertisements, a Router sends an advertisement to its direct neighbors, whenever it made a change to a metric in its local routing table ($\Rightarrow$ triggered updates)

Distance-Vector Routing Protocols (3/3)

- Functioning of RIP (continuation):
  - If the Internet Protocol (IP) is used, the cost to reach a network depends only on the number of Routers, which must be passed on the way
    - The number of Routers is counted in hops
  - Each Router increments the hop count by 1
  - If RIP is used, each Router only knows the content of its own routing table
    - No Router has an overview of the complete network

- Because no Router has an overview of the entire network, the protocol implements a **distributed algorithm**
  - This is the only way to achieve good scalability