Week 6 Addressing and Forwarding Techniques - introduction

CSIT985

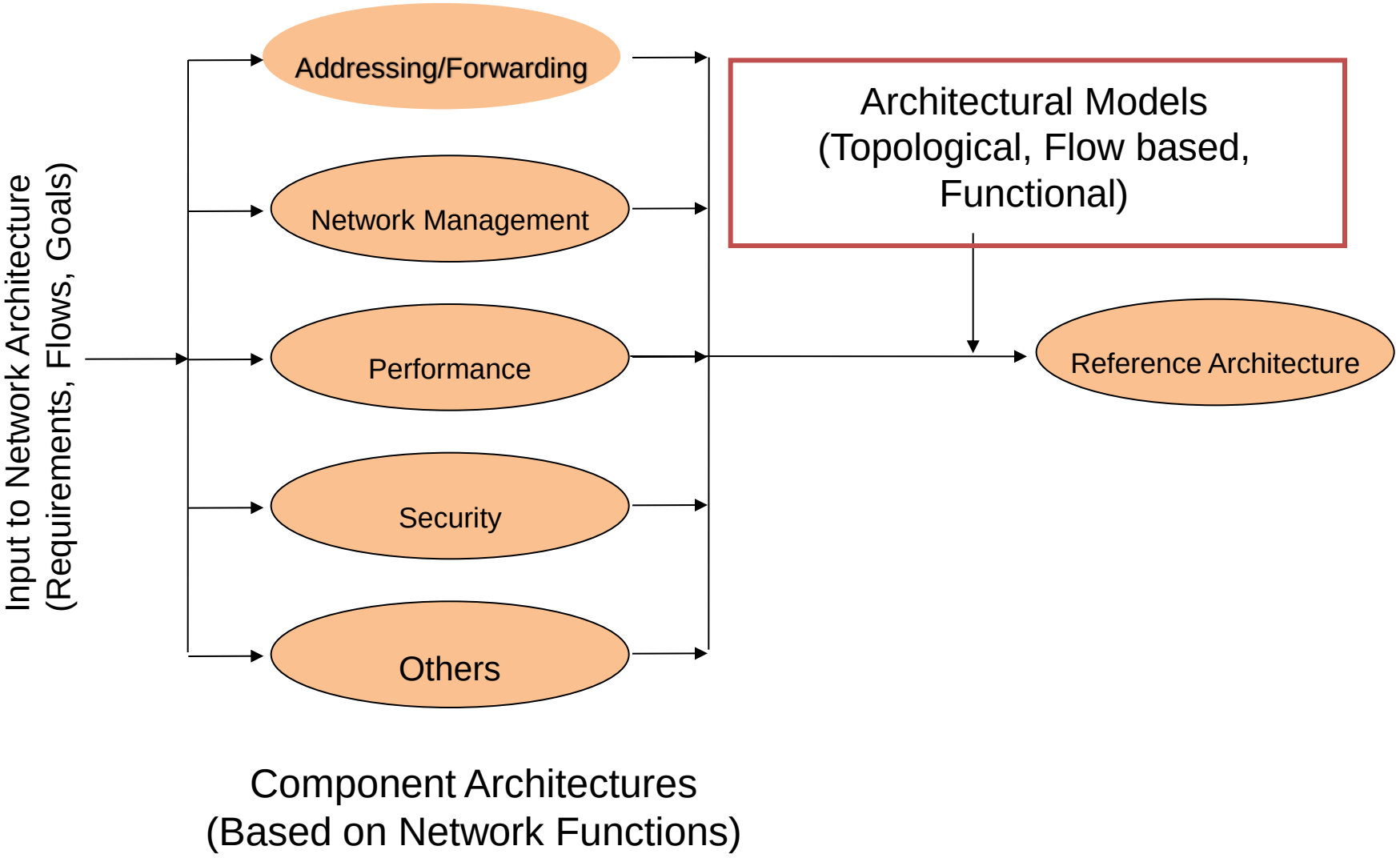
Strategic Network Design


UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Overview

- Definitions
- Addressing Fundamentals
- Routing Fundamentals
- LAN Primer (separate slides)

Component Architecture Approach (from last week)



IP Addresses

The IP addresses are used to identify systems on a TCP/IP network. The IP address is an absolute identifier of both the individual machine and the network on which it resides.

Every IP datagram packet transmitted over a TCP/IP network contains the IP addresses of the source system that generated it and the destination system for which it's intended in its IP header.

IP Addresses

To send a packet across an internet, the sender places the destination's protocol address in the packet and passes the packet to protocol software for delivery.

To provide uniform addressing in an internet, protocol software defines an abstract **addressing scheme** that assigns **each host a unique protocol address**. Users, application programs, and higher layers of protocol software use the abstract protocol addresses to communicate.

IP Addresses

In the TCP/IP protocol stack, addressing is specified by the Internet Protocol (IP).

The IP standard specifies that each host is assigned a unique **32-bit number** known as the host's **Internet Protocol address**, which is often abbreviated **IP address**, or **Internet address**.

Each packet sent across an internet contains the 32-bit IP address of the sender (source) as well as the intended recipient (destination). Thus, to transmit information across a TCP/IP internet, a computer must know the IP address of the remote computer to which the information is being sent.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Addressing Fundamentals

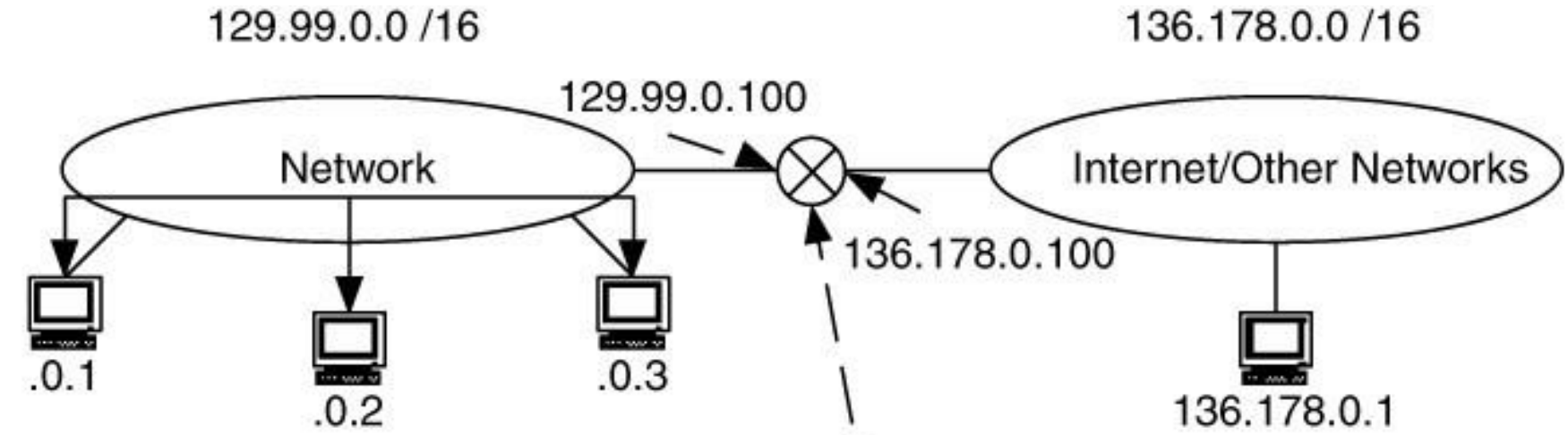
Address Type	Meaning
Local addresses	Addresses that are recognised locally, at the LAN or subnet. Usually at the data link layer (MAC)
Global addresses	Addresses that are recognised worldwide. Usually at the network (IP) layer

Private addresses	Network-layer addresses that are not routed through the public internet. Used in Network Address Translation
Public addresses	Network-layer addresses that are routed through the public internet.

Temporary addresses	Addresses that are assigned for a short duration. Usually through Dynamic Host Configuration Protocol (DHCP)
Persistent addresses	Addresses that are assigned for a long duration of time or permanently configured

Addressing Fundamentals

- We need to make distinction between local and remote addresses.



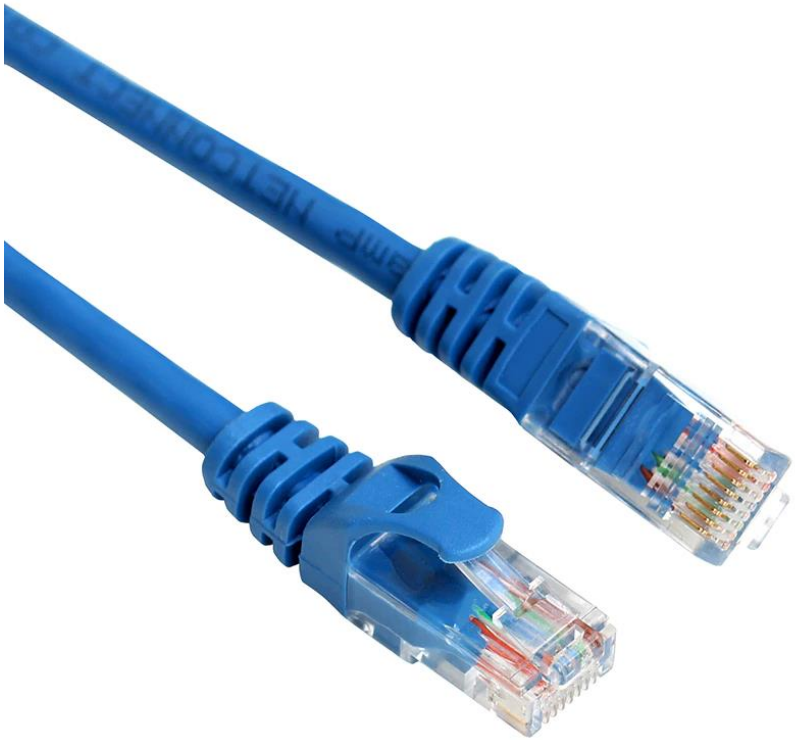
Media Access Control (MAC)

UNIVERSITY OF WOLLONGONG AUSTRALIA

Let's begin at the beginning of your network

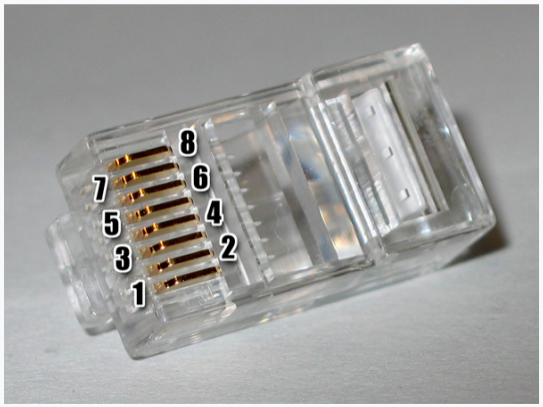
The humble RJ45 connector

- uses UTP (unshielded twisted pair) cable



UNIVERSITY OF WOLLONGONG AUSTRALIA

How is a RJ45 connector wired?

Pin	T568A pair	T568B pair	10BASE-T / 100BASE-TX[11]	1000BASE-T signal ID[12]	Wire	T568A color	T568B color	Pins on plug face
1	3	2	TX+	DA+	tip	white/green stripe	white/orange stripe	
2			TX−	DA−	ring	green solid	orange solid	
3	2	3	RX+	DB+	tip	white/orange stripe	white/green stripe	
4	1		not used	DC+	ring	blue solid		
5			not used	DC−	tip	white/blue stripe		
6	2	3	RX−	DB−	ring	orange solid	green solid	
7	4		not used	DD+	tip	white/brown stripe		
8			not used	DD−	ring	brown solid		

The pin numbering on the plug. Connected pins on the plug and jack have the same number.

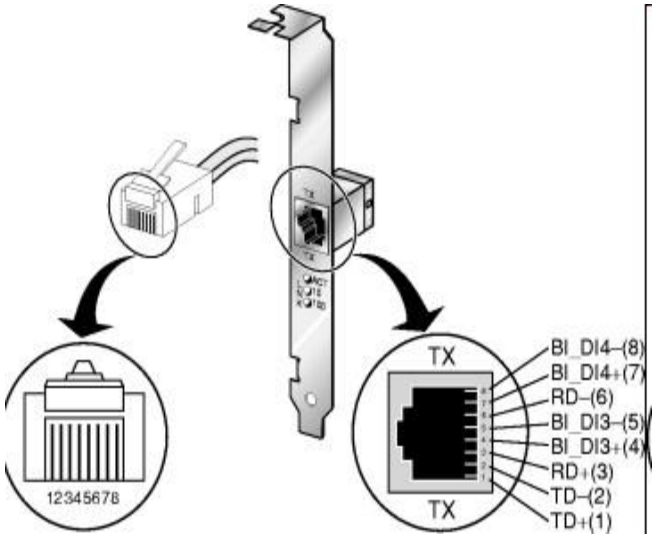
http://en.wikipedia.org/wiki/TIA/EIA-568

How is a RJ45 connector wired?

The only difference between T568A and T568B is that pairs 2 and 3 (orange and green, respectively) are swapped.

The RJ45 is connected to

- NIC – Network Interface Card of your computer



http://support.3com.com/

UNIVERSITY OF WOLLONGONG AUSTRALIA

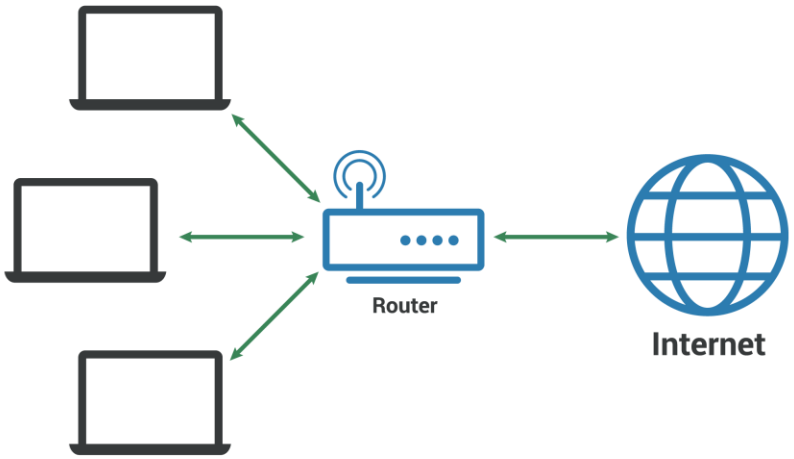
Addressing Fundamentals

- In the local context (LANs) addressing occurs not at the IP-Network layer but at the MAC-Datalink layer using Ethernet
- If the destination is outside the LAN (remote), the PC will send to the default gateway (router)
- The router recognises this address as not being local so uses the IP address to dispatch this information on the WAN (Wide area network)

Addressing (and Routing) Fundamentals

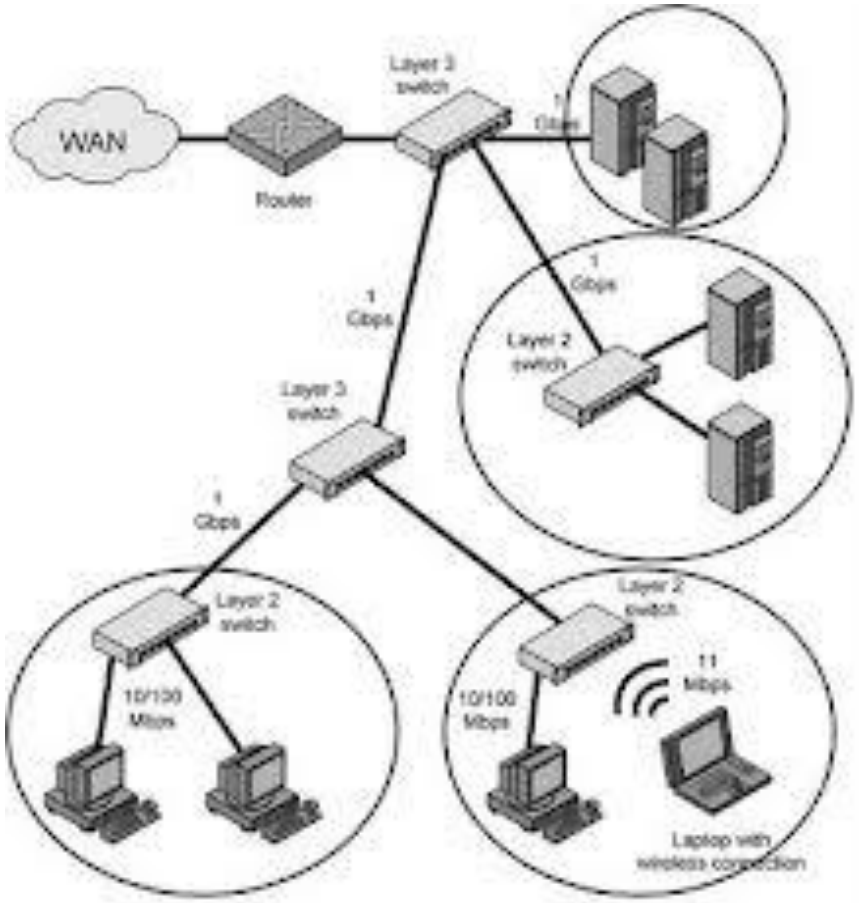
- Packets are forwarded by the router by comparing the destination address to an entry in (typically) a routing table.
- A routing table is stored in a router's memory (or other internetworking device) that keeps a record of routes to particular destinations and metrics associated with that route.
- A routing table can be updated manually or dynamically using a "routing protocol"

Typical LANs



Logical or physical topology?

Typical LANs



Logical or physical topology?

Difference between Physical and Logical Topology

What is Physical Topology?

- It indicates the arrangement of different elements of a network, and reflects the physical layout of devices and cables to form a connected network.
- It is concerned with the essentials of the network ignoring minute details like transfer of data and device type.
- The pattern of arrangement of nodes (computers) and network cables depends on the ease of installation and setup of the network.
- It affects cost and bandwidth capacity based on a solution of devices. It takes into account the placement of nodes and the distance between them.
- Devices can be arranged to form a ring (Ring Topology) or linearly connected in a line called Bus Topology.

Difference between Physical and Logical Topology

Types of Physical Topology

- The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **Network Topology**.
- On the basis of arrangements, Physical Topology has several types:
  ① Mesh Topology
  ② Star Topology
  ③ Bus Topology
  ④ Ring Topology
  ⑤ Hybrid Topology

Difference between Physical and Logical Topology

Types of Physical Topology

- The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **Network Topology**.
- On the basis of arrangements, Physical Topology has several types:
  ① Mesh Topology
  ② Star Topology
  ③ Bus Topology
  ④ Ring Topology
  ⑤ Hybrid Topology

Difference between Physical and Logical Topology

What is Logical Topology?

- It reflects the arrangement of devices and their communication.
- It is the transmission of data over physical topology. It is independent of physical topology, irrespective of the arrangements of nodes.
- It is concerned with intricate details of network like type of devices (switches, routers) chosen and their quality, which affects rate and speed of data packets delivery.
- The logical topology ensures optimal flow control that can be regulated within network.
- The data can either flow in a linear pattern called Logical bus or in form of a circle Logical ring.

Difference between Physical and Logical Topology

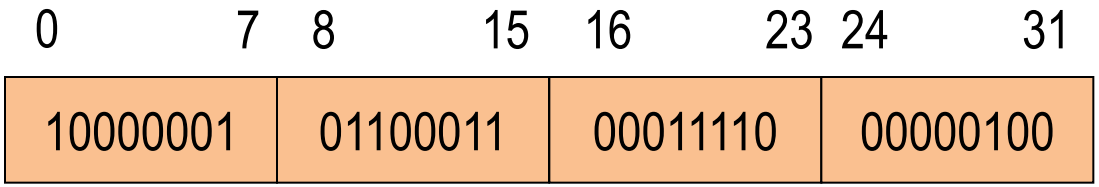
- Logical topology refers to the manner in which the data is transported and the network device structure is displayed.
- On the basis of data transfer, logical topology have below mentioned types:
  ① Ethernet
  ② TCP/IP (Transmission Control Protocol/Internet Protocol)
  ③ OSI (Open Systems Interconnection)

Difference between Physical and Logical Topology

Physical Topology	Logical Topology
Depicts physical layout of network.	Depicts logistics of network concerned with transmission of data.
The layout can be modified based on needs.	There is no interference and manipulation involved here.
This has major impact on cost, scalability and bandwidth capacity of network based on selection and availability of devices.	This has major impact on speed and delivery of data packets. It also handles flow control and ordered delivery of data packets.
It is actual route concerned with transmission.	It is a high level representation of data flow.
Physical connection of the network.	Data path followed of the network.

Addressing Fundamentals

- For IP, addressing consists of an address identifier and an associated mask (bit mask)
  - Usually presented in dotted-decimal notation
- Address mask determines which parts of the address belong to the network and which part belongs to the device (or host)
  - This allows the address to be separated into network and host portions



Addressing Fundamentals

The total size of the IP address is 32 bits and the IP address is divided into four octets each of size is 8 bits. And further, divide into NID (Internet) and HID (Host). Let’s discuss each class in detail.

Addressing Fundamentals

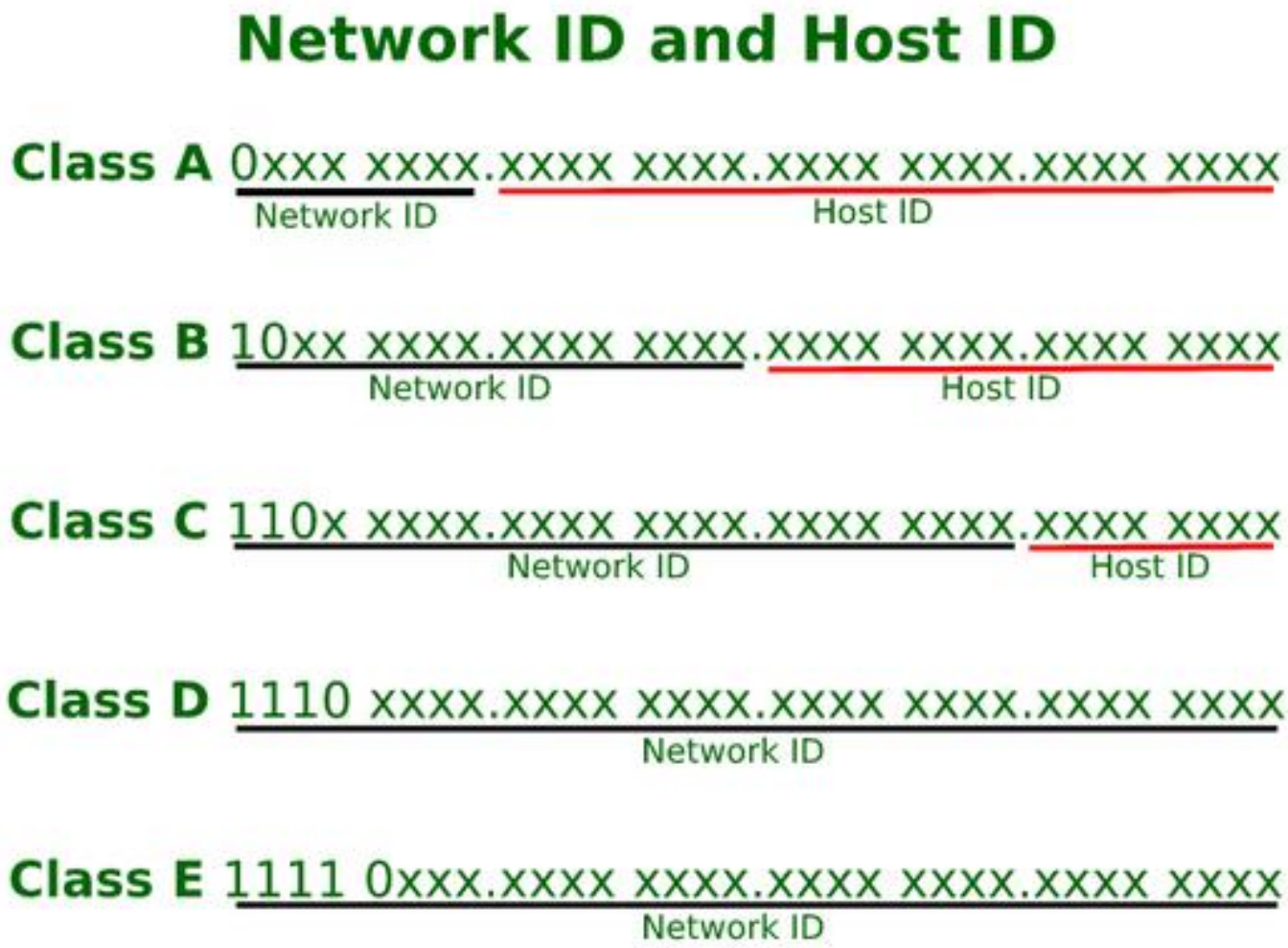
IP addresses are divided into 5 classes:

- Class A is used for big networks such as ISP networks.
- Class B is used by big organizations.
- Class C is used by small organizations.
- Class D no NID and HID all 28 bits are used to define the multicast address.
- Class E is reserved for research and future purchases.

Range of All Classes

```
Class A: 1.0.0.0 to 127.255.255.255
Class B: 128.0.0.0 to 191.255.255.255
Class C: 192.0.0.0 to 223.255.255.255
Class D: 224.0.0.0 to 239.255.255.255
Class E: 240.0.0.0 to 255.255.255.255
```

Addressing Fundamentals



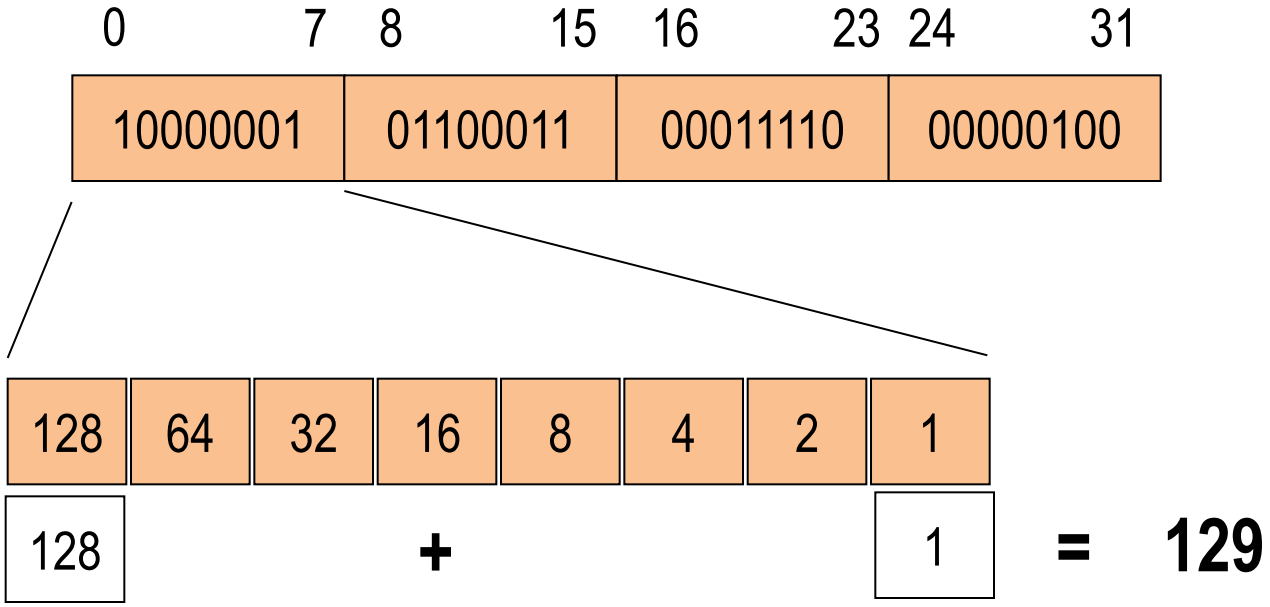
Addressing Fundamentals

Address Identifier

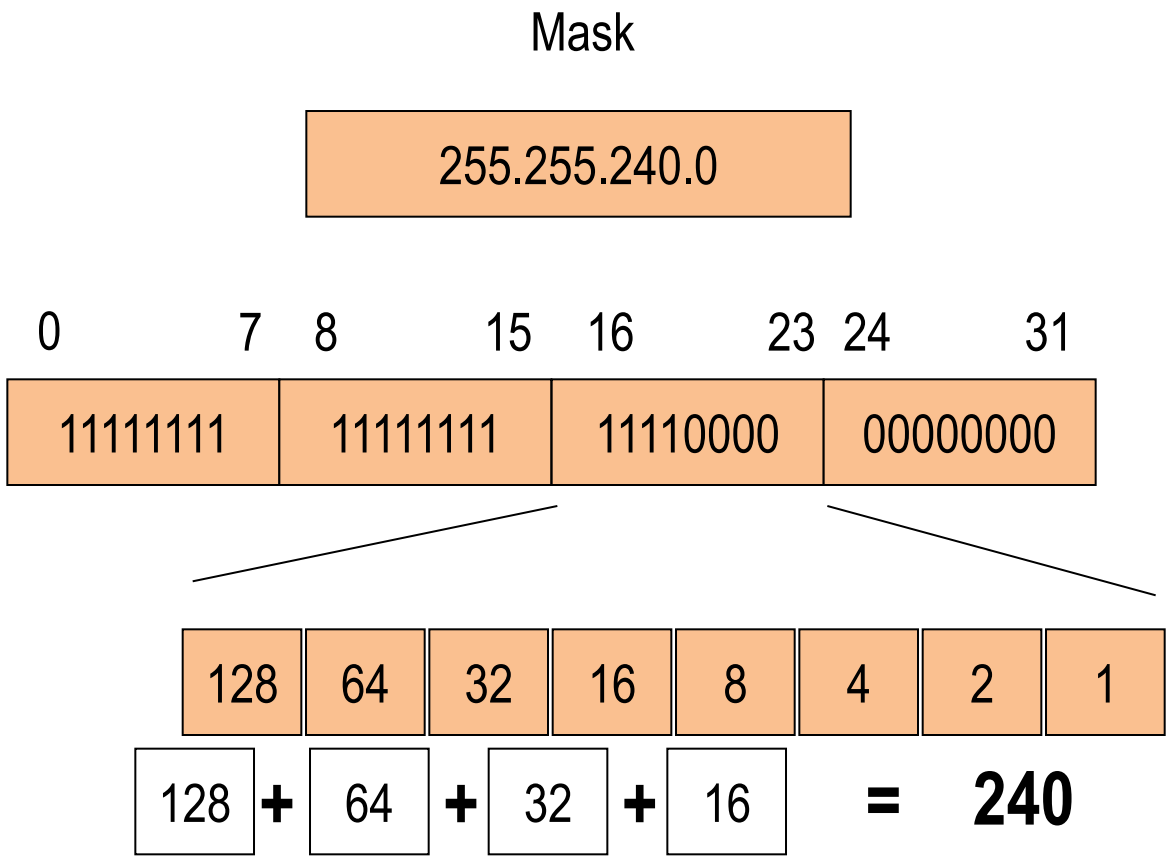
129.99.30.4

Mask

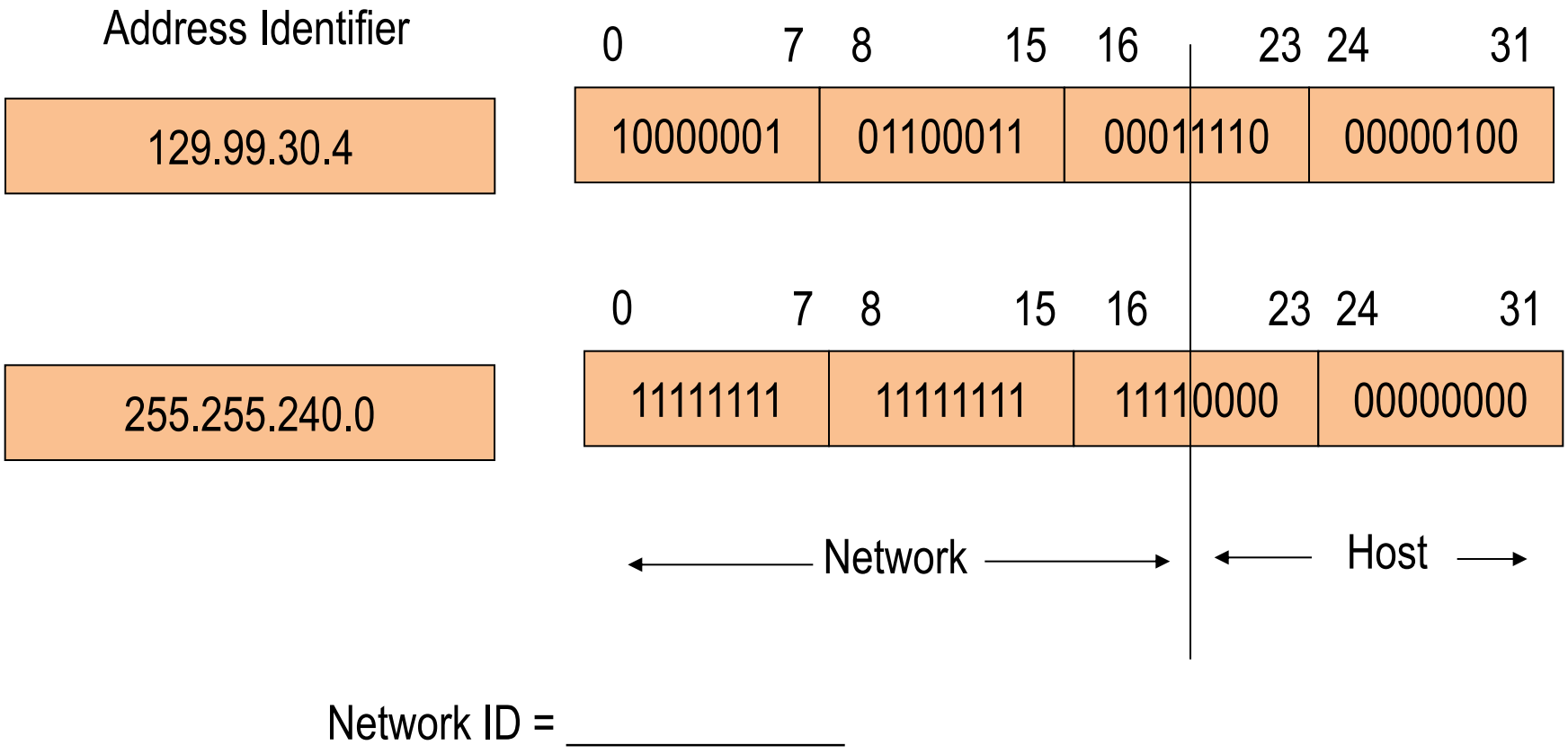
255.255.240.0



Addressing Fundamentals



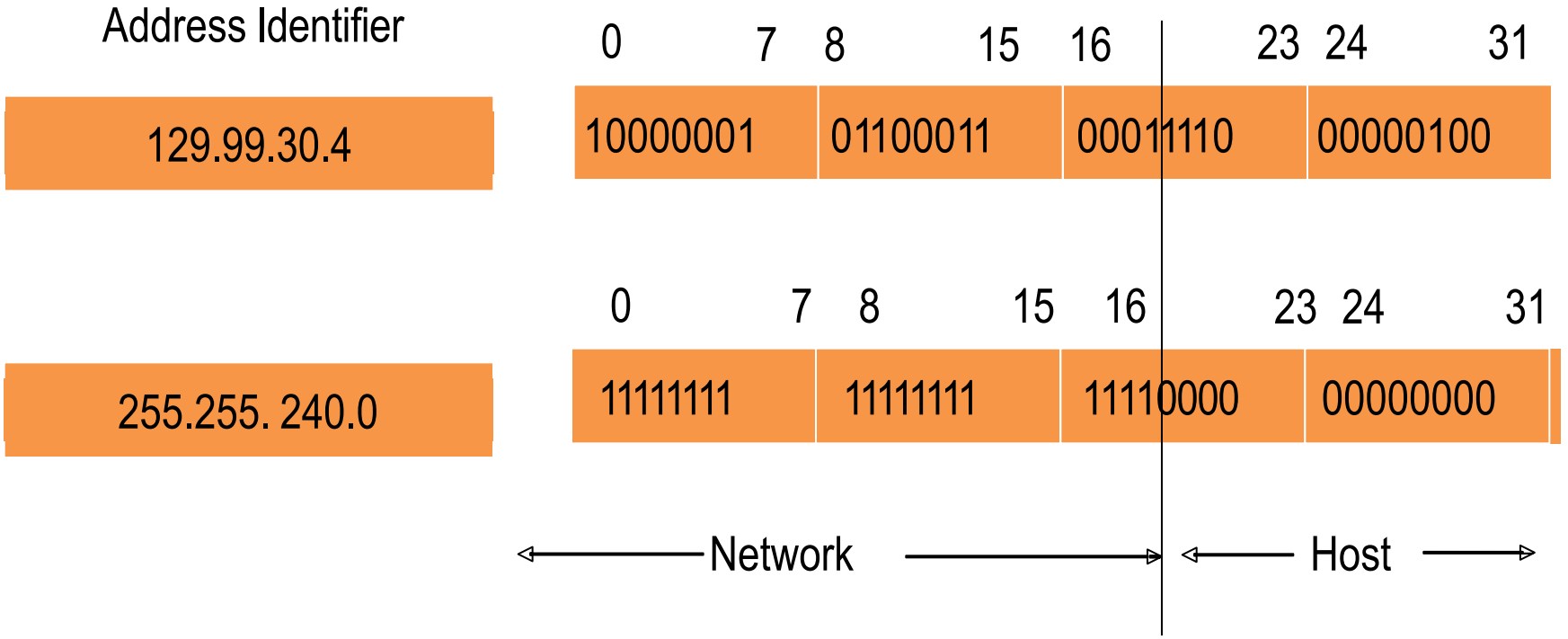
Addressing Fundamentals



Network ID = _____

UNIVERSITY OF WOLLONGONG AUSTRALIA

Addressing Fundamentals



Network ID = 129.99.16.0

Addressing Mechanisms: Classful addressing

- Classful Addressing
  - Predetermined mask lengths
  - Set of classes of address
    - A,B,C,D,E
    - Differ in maximum network size
  - Class identifier in the first octet of address determines class
    - Classful addressing has been superseded but has legacy implications requiring us to cover this topic in order to understand current practice

Addressing: Classful addressing

Class	Identifier	Network Address Range	Number of Networks	Addresses / Network	Natural Mask
A	1st bit = 0	1-127	127	Over 16M	255.0.0.0
B	1st bit = 1 2nd bit = 0	128-191	16,000	64K	255.255.0.0
C	1st bit = 1 2nd bit = 1 3rd bit = 0	192-223	2M	254	255.255.255.0
D	Multicast	224-239			
E	Reserved	240-247			

Private addresses	• Network-layer addresses that are not routed through the public internet. Used in Network Address Translation.
Public addresses	• Network-layer addresses that are routed through the public internet.

What is Network Address Translation(NAT)?

- It is a process in which one or more local (private) IP addresses are translated into one or more Global (public) IP addresses and vice versa to provide Internet access to the local hosts.

- It also does the translation of port numbers, i.e., masks the port number of the host with another port number in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

Working of Network Address Translation (NAT)

- The border router is configured for NAT, i.e., the router which has one interface in the local (inside) network and one interface in the global (outside) network.
- When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address.
- When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

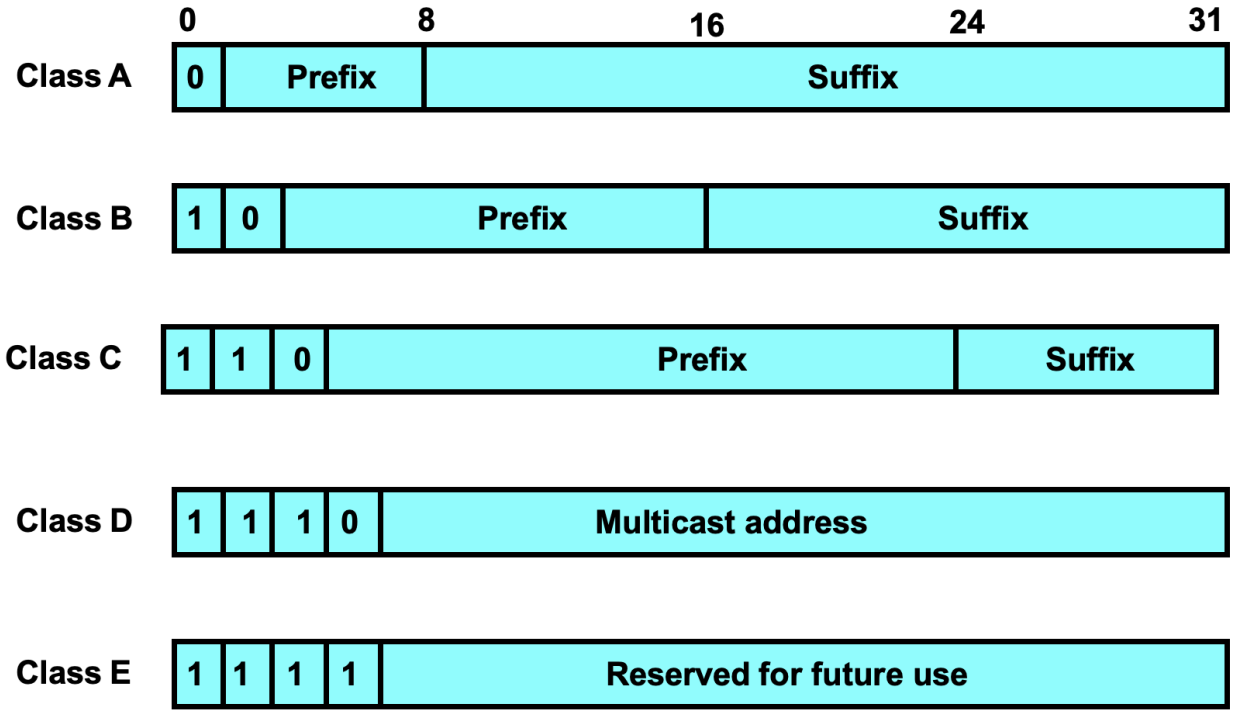
IP Addresses

Every 32-bit address is divided into two parts**: a prefix and suffix**.

The address **prefix** identifies the physical network to which the computer is attached, while the **suffix** identifies an individual computer on that network. That is, each physical network in an internet is assigned a unique value known as a **network number.** The network number appears as a **prefix** in the address of each computer attached to the network.

No two networks can be assigned the same network number and no two computers on the same network can be assigned the same suffix.

Classes of IP Addresses



UNIVERSITY OF WOLLONGONG AUSTRALIA

Private addressing

- Private addresses as defined by RFC 1918
- Original motivation was the prospect of **running out of IP addresses**
  - 10.0.0.0 - 10.255.255.255
    - (10/8 prefix)
  - 172.16.0.0 - 172.31.255.255
    - (172.16/12 prefix)
  - 192.168.0.0 - 192.168.255.255
    - (192.168/16 prefix)

UNIVERSITY OF WOLLONGONG AUSTRALIA

Routing Fundamentals

- For routers to forward IP packets they need to know
  ① What other routers they are connected to
  ② If networks connected by these routers are available
- This is called “reachability”

Routing Fundamentals

Reachability can be:

- Programmed
  - Statically: Programmed by network personnel
- Learnt
  - Dynamically: Learnt through the use of a routing protocol, e.g.,
    - RIP/RIP v2 – Routing Information Protocol
    - OSPF – Open Shortest Path First
    - EIGRP – Enhanced Interior Gateway Protocol
    - BGP4 – Borader gateway Protocol

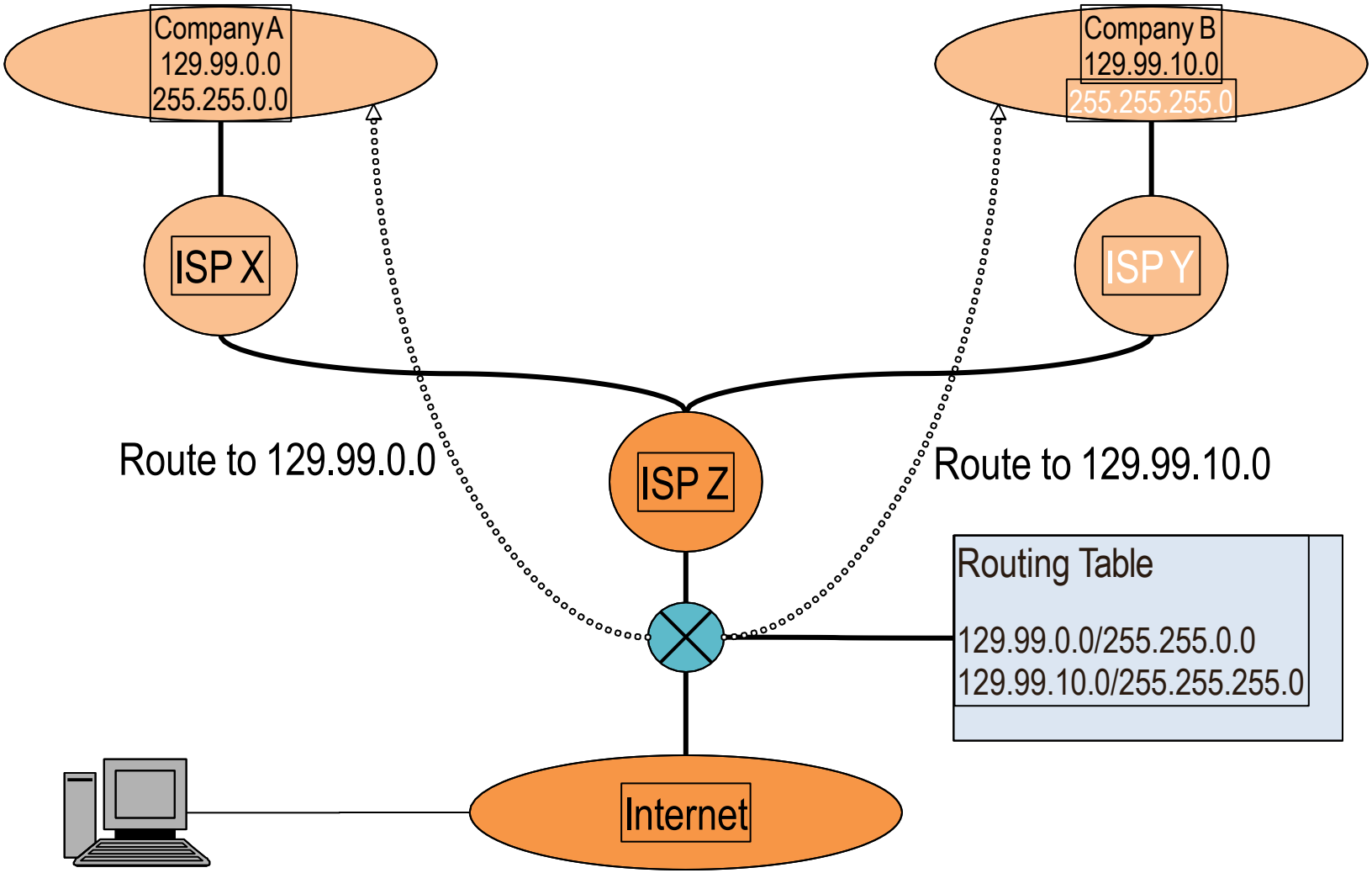

Routing Fundamentals

- Packets are forwarded by comparing the destination address to an entry in (typically) a routing table

- When routers compare destination addresses to entries, the longest match to the destination address is selected

UNIVERSITY OF WOLLONGONG AUSTRALIA

Routing Fundamentals

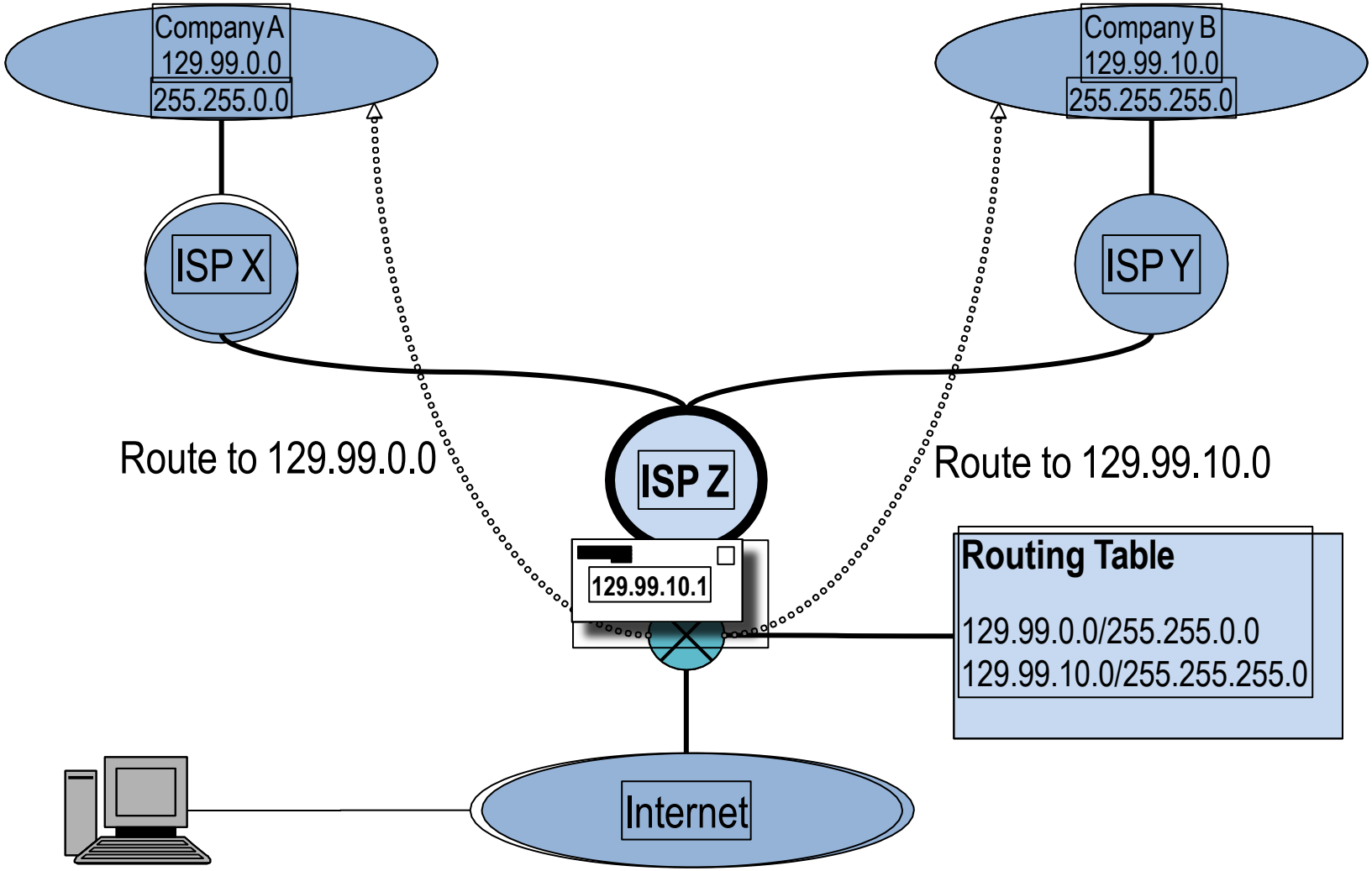


Routing Fundamentals

- Packets are forwarded by comparing the destination address to an entry in (typically) a routing table
  - If an IP packet with a destination address of 129.99.10.1 arrived at ISP Z

UNIVERSITY OF WOLLONGONG AUSTRALIA

Routing Fundamentals

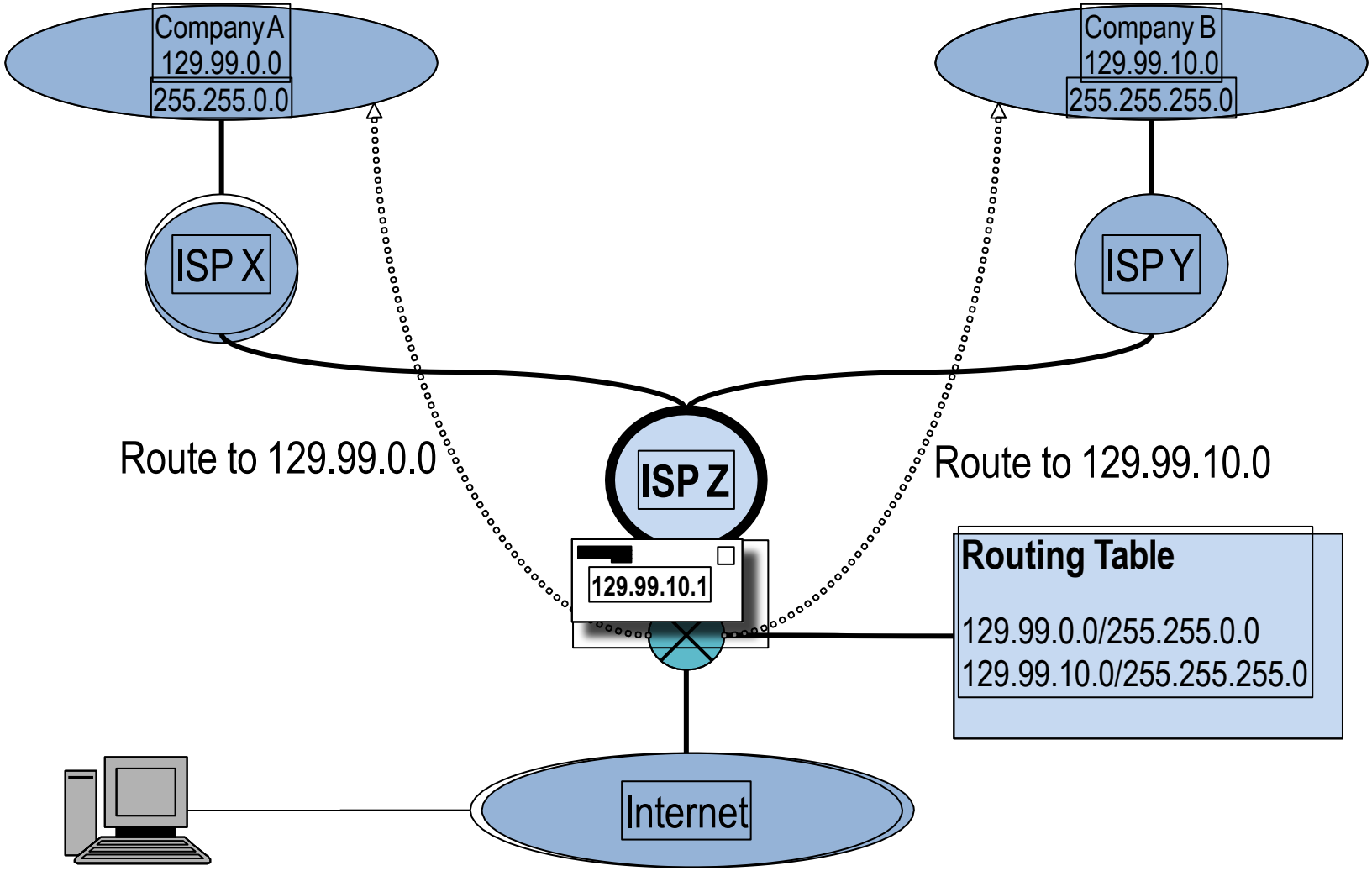


Routing Fundamentals

- Packets are forwarded by comparing the destination address to an entry in (typically) a routing table
  - If an IP packet with a destination address of 129.99.10.1 arrived at ISP Z
  - On the surface, this would match both entries in the routing table

UNIVERSITY OF WOLLONGONG AUSTRALIA

Routing Fundamentals



Routing Fundamentals

- Packets are forwarded by comparing the destination address to an entry in (typically) a routing table
  - If an IP packet with a destination address of 129.99.10.1 arrived at ISP Z
  - This would match both entries in the routing table (assuming Class B convention)
  - If we apply the first mask of 255.255.0.0 to 129.99.10.1, we get 129.99 as the network
    - Matches first two octets
  - If we apply the second mask of 255.255.255.0 to 129.99.10.1
    - We get 129.99.10 as the network
    - Matches first three octets

Routing Fundamentals

- In this example the packet would be forwarded to Company B because applying the mask of 255.255.255.0 would result in a three octet match – a more explicit match – meaning that the packet would be forwarded to ISP Y.

Routing Fundamentals

Acronyms

- RIP – Routing Information Protocol
- OSPF – Open Shortest Path First
- IGRP – Interior Gateway Routing Protocol
- EIGRP – Enhanced Interior Gateway Routing Protocol
- BGP – Border Gateway Protocol

Routing Fundamentals

- Dynamic Routing protocols at a glance – Open Source
  - RIP/RIP v2 – Routing Information Protocol
  - OSPF – Open Shortest Path First
- Cisco proprietary
  - EIGRP is Cisco proprietary protocols that are most closely related to RIP;
  - IGRP is another Cisco protocol but is now extinct

UNIVERSITY OF WOLLONGONG AUSTRALIA

IGP, EGP/BGP

- These “routing protocols” fall into two groups…
  - Interior Gateway Protocol
  - Exterior Gateway Protocol (see p. 270)
- IGP – routing protocol within an Autonomous System.
  - RIP, OSPF, EIGRP
- EGP – routing protocol between AS.
  - EGP is extinct.
  - BGP is the common standard

UNIVERSITY OF WOLLONGONG AUSTRALIA

Autonomous Systems

- An **autonomous system** (**AS**) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy (RFC 1930)
- AS numbers are issued by ICANN or its delegated local authority called Regional Internet Registries (APNIC in Australia) and cost money

IP Routing

‘Routing’ refers to the process of choosing a path over which to send packets and router refers to a computer making the choice.

The goal of IP is to provide a virtual network that encompasses multiple physical networks and offers a connectionless datagram delivery service. Thus, we will focus on IP forwarding, which is also called **Internet routing or IP routing.**

IP Routing

A router forwards each packet from one network to another. A source host creates a packet, places the destination address in the packet header, and then sends packet to near to router.

When a router receives a packet, the router uses the destination address to select the next router on the path to the destination, and then transmit the packet. Eventually, the packet reaches a router that can deliver the packet to its final destination.

IP Routing

TCP/IP Protocol uses the name IP datagram to refer to an internet packet.

The datagram begins with a header followed by a data area.

A Packet sent across a TCP/IP internet is called an IP datagram. Each datagram consists of a header followed by data. Source and destination address in the datagram header are IP address.

Forwarding An IP Datagram

Datagram traverses an internet by following a path from their initial source through routers to the final destination.

Each router along the path receives the datagram, extracts the destination address from the header, and uses the destination address to determine a next hop to which the datagram should be sent.

The router then forwards the datagram to the next hop (**hop**- A measure of distance between two points in an internet. A hop count of *n* means that *n* routers separate the source and destination), either the final destination or another router.

IP Routing

To make the selection of a next hop efficient and to make it possible for humans to understand the computation, each IP router keeps information in a ‘routing table.’

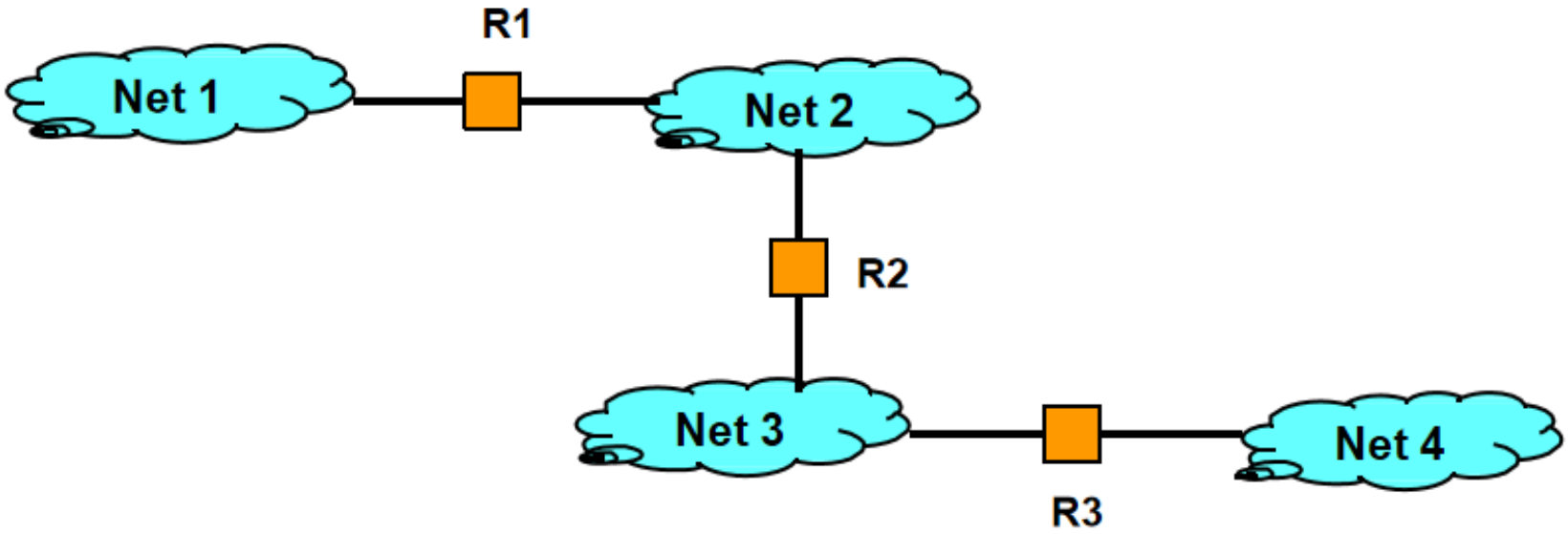
The router forwards packets by maintaining a list of networks and hosts, called ‘routing table.’

Routing table stores information about possible destinations and how to reach them. Because both hosts and routers route datagrams, both have IP routing tables. Whenever the IP routing software in a host or router needs to transmit a datagram, it consults the routing table to decide where to send the datagram.

IP Routing

The routing table contains a set of entries that each specifies a destination and next hop used to reach that destination.

The figure shows the contents of a routing table in one of three routers that are used to interconnect four networks in a small internet.



The Conceptual Routing Table found in R2

Destination	Next Hop
Net 1	R1
Net 2	Deliver direct
Net 3	Deliver direct
Net 4	R3

IP Routing

As the above figure shows, router R2 connects directly to the networks labeled Net 2 and Net 3. Therefore R2 can deliver a datagram to any destination attached to those networks. When a datagram is destined for network 4, R2 sends the datagram to router R3.

Each destination listed in a routing table is a network, not an individual host. The distinction is important because an internet can contain over 1000 times as many hosts as networks. Thus using networks as destinations keeps routing table small.

Because each destination in a routing table corresponds to a network, the number of entries in a routing table is proportional to the network of networks in an internet.

IP address & Routing Table Entries

In practice, an IP routing table is slightly more complex than shows previously.

First, the destination field in each entry contains the network prefix of the destination network.

Second, an additional field in each entry contains an address mask that specifies which bits of the destination correspond to the network prefix.

Third, an IP address is used when the Next hop field denotes a router.

IP Routing

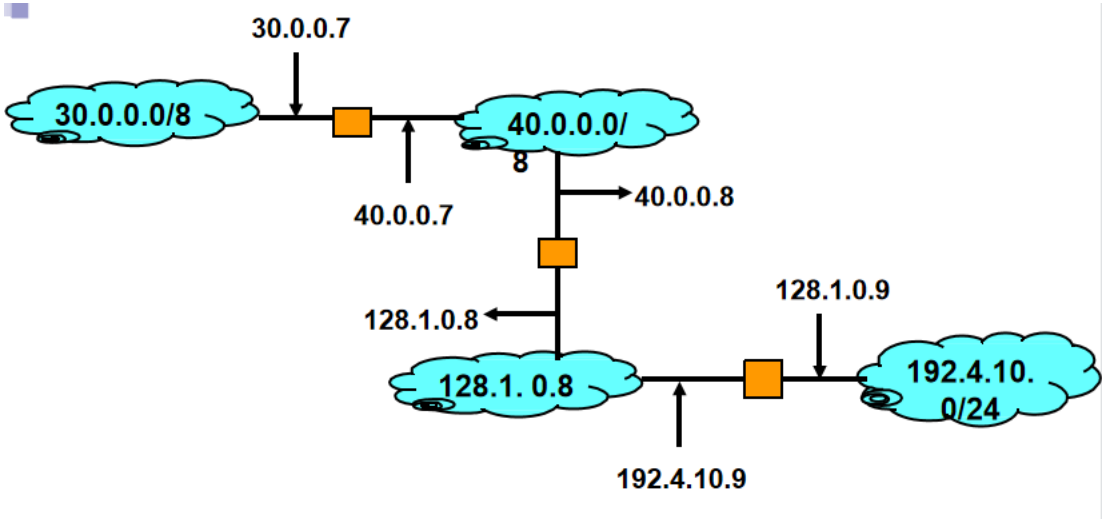


Fig. – An internet of four networks and three routers with an IP address assigned to each router interface

IP Routing

Destination	Mask	Next Hop
30.0.0.0	255.0.0.0	40.0.0.7
40.0.0.0	255.0.0.0	Deliver direct
128.1.0.0.	255.255.0.0	Deliver direct
192.4.10.0	255.255.255.0	128.1.0.9

Fig – Routing table found in the center router. Each entry in the table lists a destination, a mask, and the next hop used to reach the destination.