OSI Layer 3: Network Layer

Routing and Addressing

Layer3: Network Layer

- Overview of the Network Layer
- IP Addresses and Subnets
- Layer 3 Devices
- ARP Protocol
- Network Layer Services
- Routed and Routing Protocols
- VLSM
- ICMP

Layer 3 Responsibilities

- Move data through networks
- Use a *hierarchical* addressingscheme
  (opposed to MAC addressing, which is flat)
- Segment network and control flow of traffic
- Reduce congestion
- Talk to other networks

Layer 3 Devices

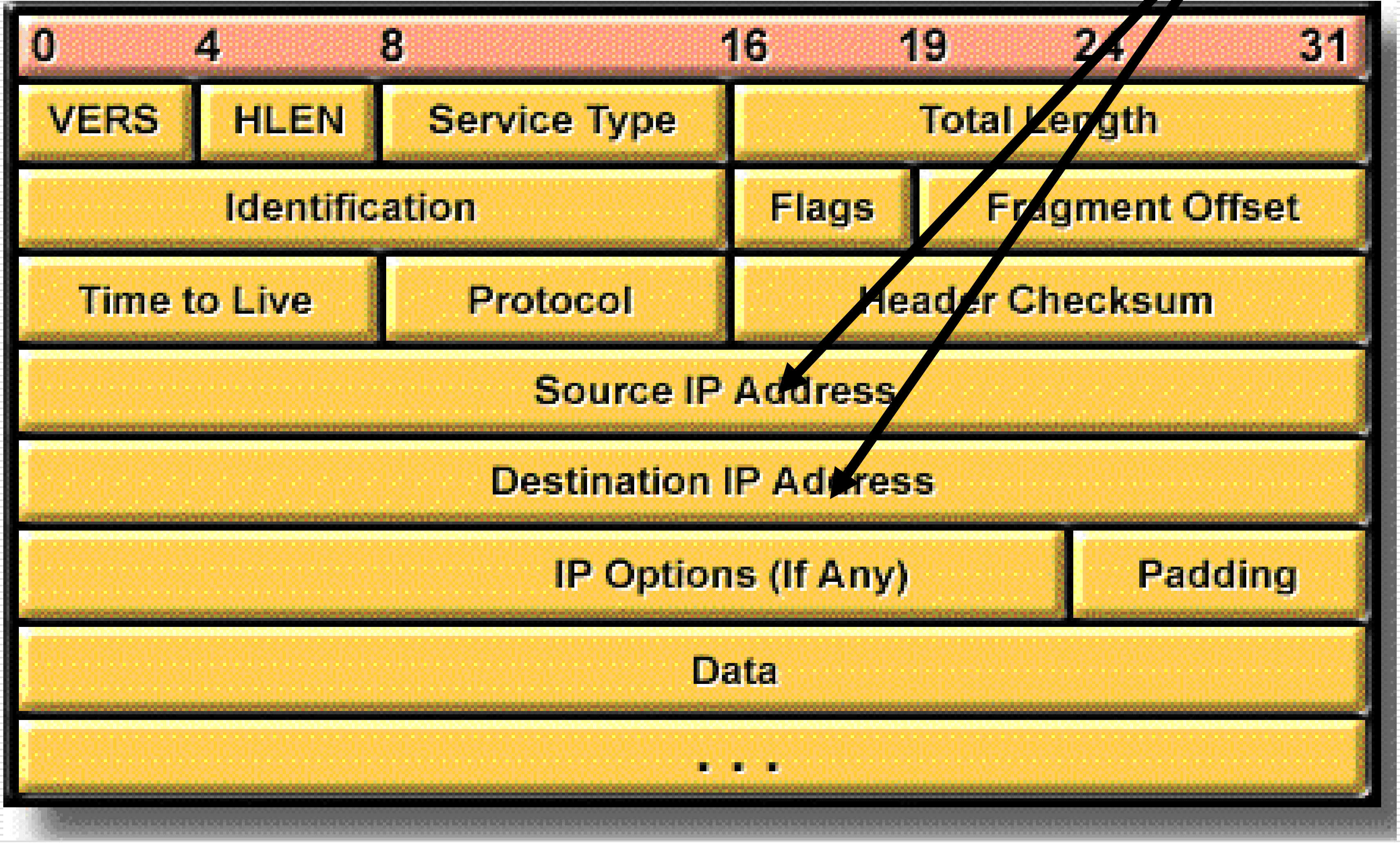
- Routers
  - Interconnect network segments *or* networks
  - Make logical decisions based on IP addresses
  - Determine best path
  - Switch packets from incoming ports to outgoing ports

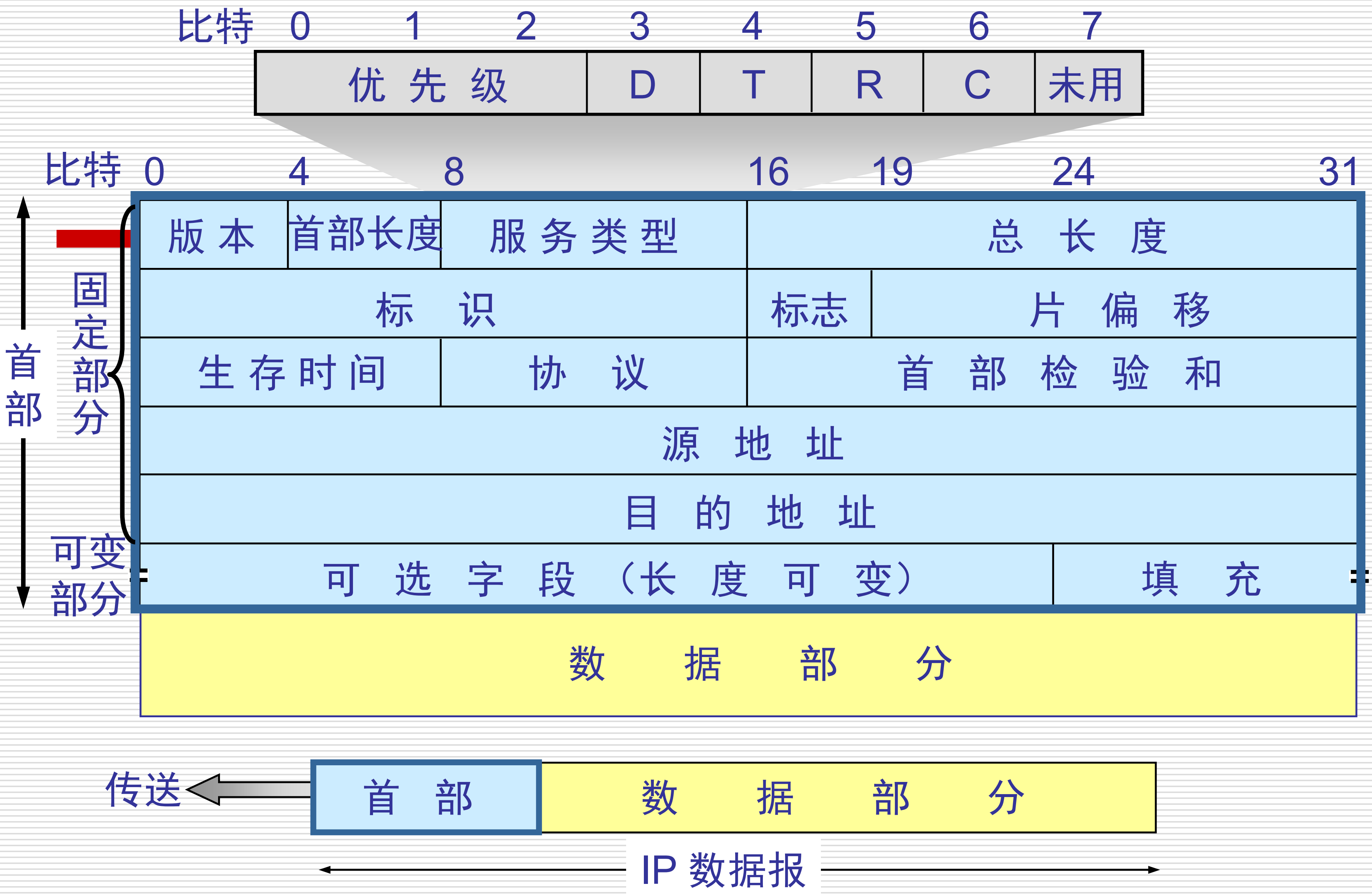
Layer3: Network Layer

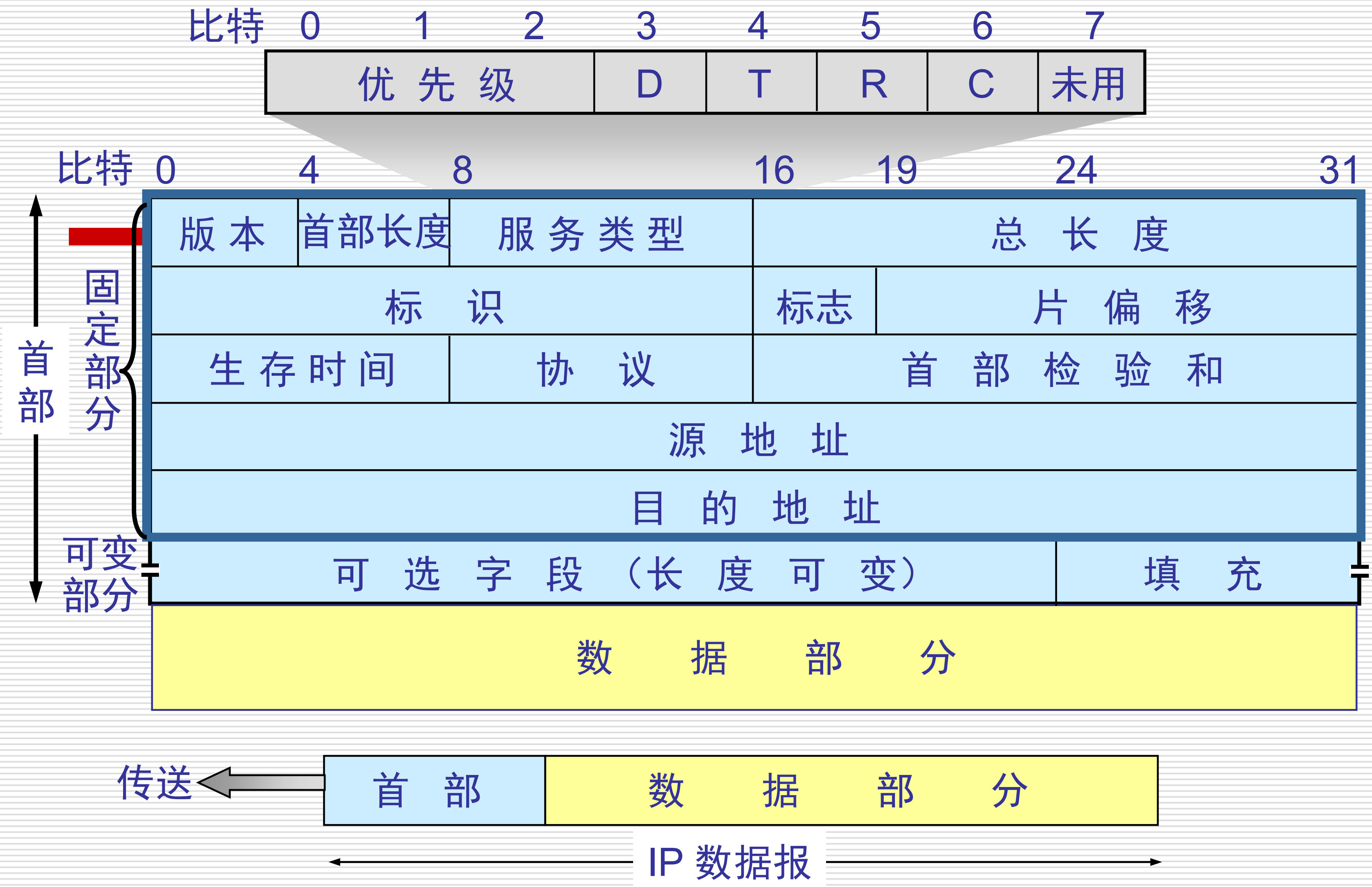
- Overview of the Network Layer
- IP Addresses and Subnets
- Layer 3 Devices
- ARP Protocol
- Network Layer Services
- Routed and Routing Protocols
- VLSM
- ICMP

Layer 3 Packet/Datagram

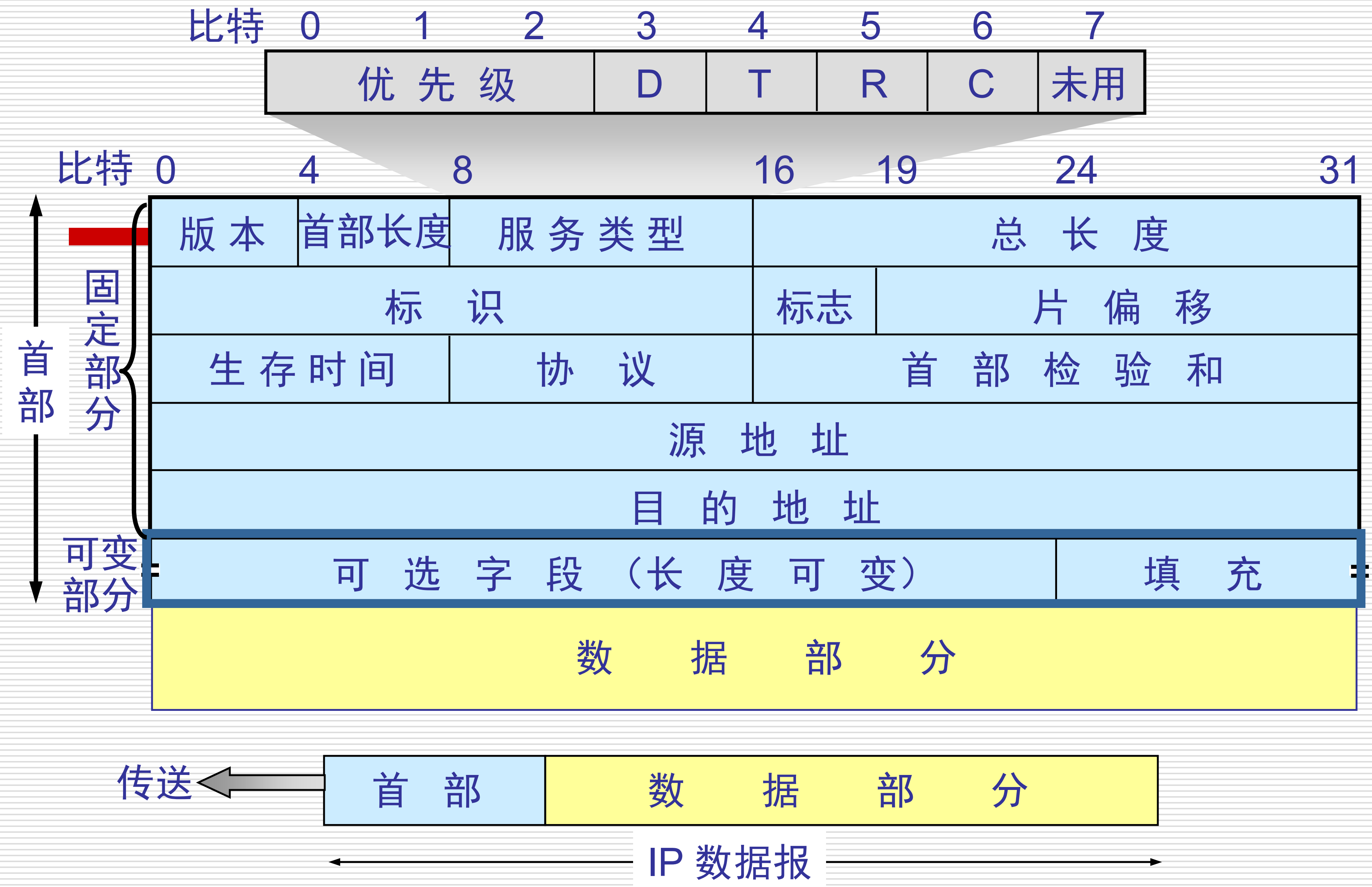
Header includes source AND destination addresses




比特 0 1 2 3 4 5 6 7
优 先 级
D
T
R
C
未用
比特 0 4 8 16 19 24 31
版 本
首部长度
服 务 类 型
总 长 度
标 识
标志
片 偏 移
生 存 时 间
协 议
首 部 检 验 和
源 地 址
目 的 地 址
可 选 字 段 （长 度 可 变）
填 充
数 据 部 分
首部
固定部分
可变部分
传送
首 部
数 据 部 分
IP 数据报



比特 0 1 2 3 4 5 6 7
优 先 级
D
T
R
C
未用
比特 0 4 8 16 19 24 31
版 本
首部长度
服 务 类 型
总 长 度
标 识
标志
片 偏 移
生 存 时 间
协 议
首 部 检 验 和
源 地 址
目 的 地 址
可 选 字 段 （长 度 可 变）
填 充
数 据 部 分
首部
固定部分
可变部分
传送
首 部
数 据 部 分
IP 数据报

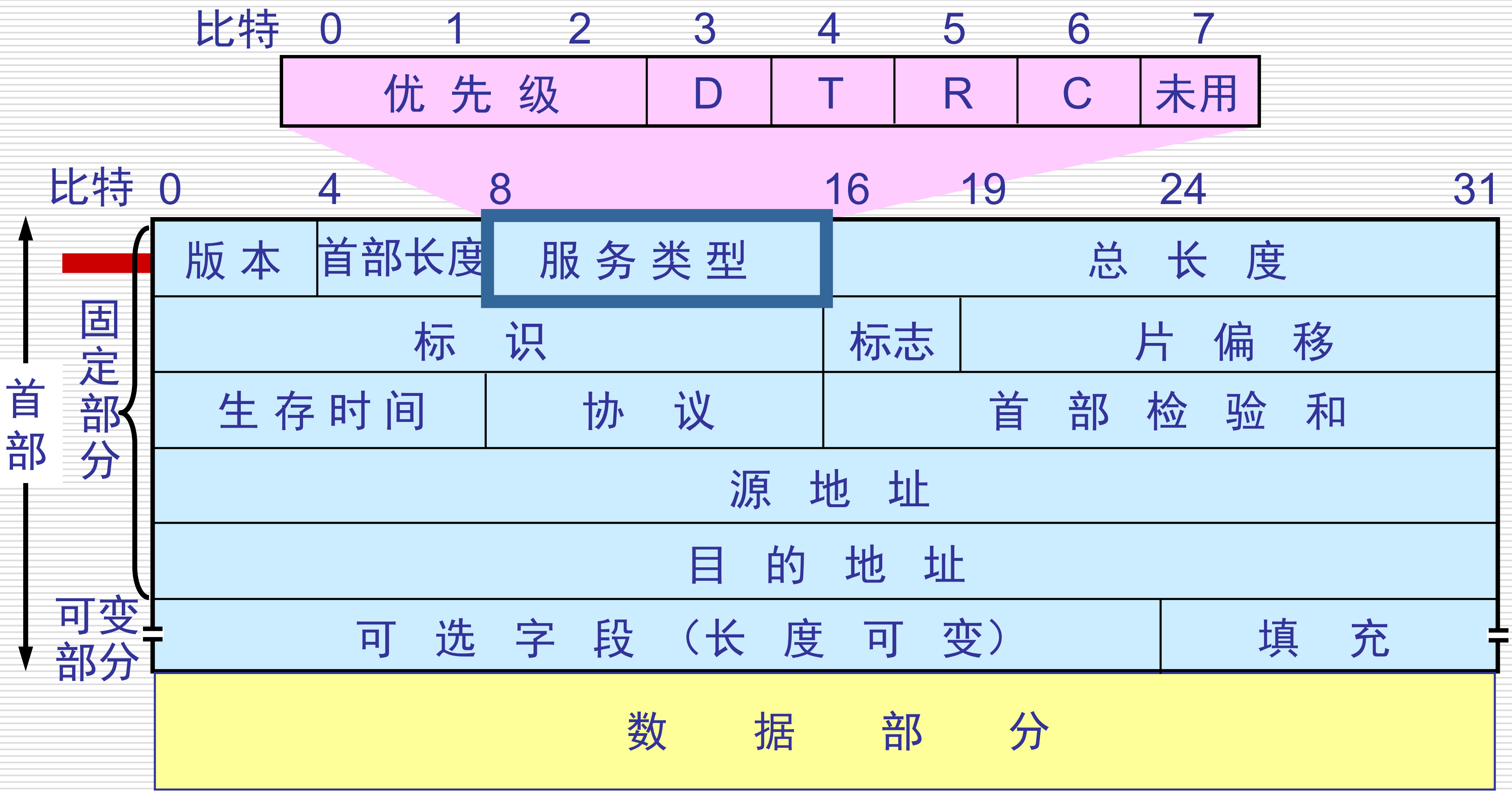


比特 0 1 2 3 4 5 6 7
优 先 级
D
T
R
C
未用
比特 0 4 8 16 19 24 31
版 本
首部长度
服 务 类 型
总 长 度
标 识
标志
片 偏 移
生 存 时 间
协 议
首 部 检 验 和
源 地 址
目 的 地 址
可 选 字 段（长 度 可 变）
填 充
数 据 部 分
首部
固定部分
可变部分
传送
首 部
数 据 部 分
IP 数据报

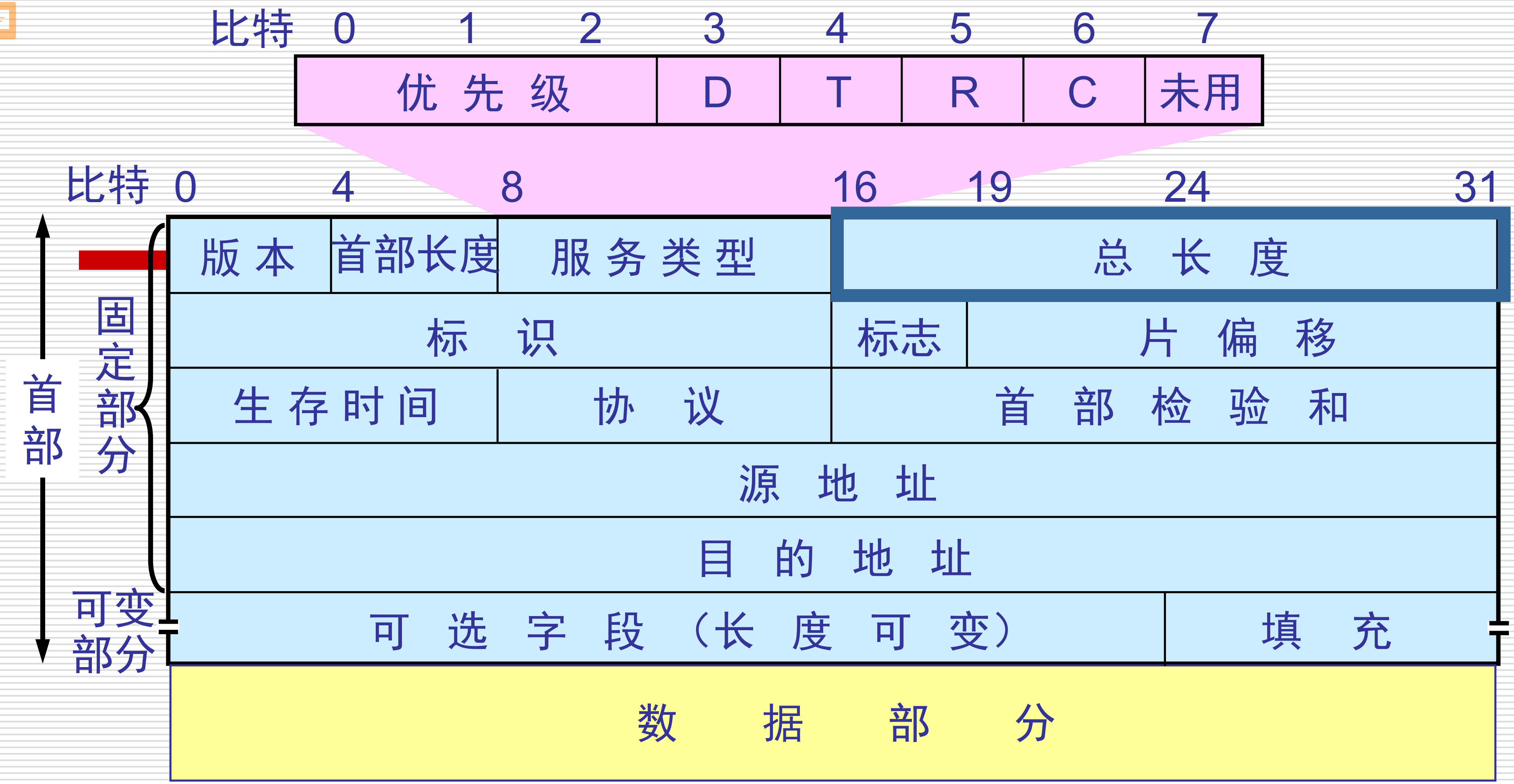
版本——占 4 bit，指IP协议的版本
目前的 IP 协议版本号为 4 (即 IPv4)

首部长度——占 4 bit，可表示的最大数值是 15 个单位(一个单位为 4 字节)

因此 IP 的首部长度的最大值是60字节。



服务类型——占 8 bit，用来获得更好的服务
这个字段以前一直没有被人们使用

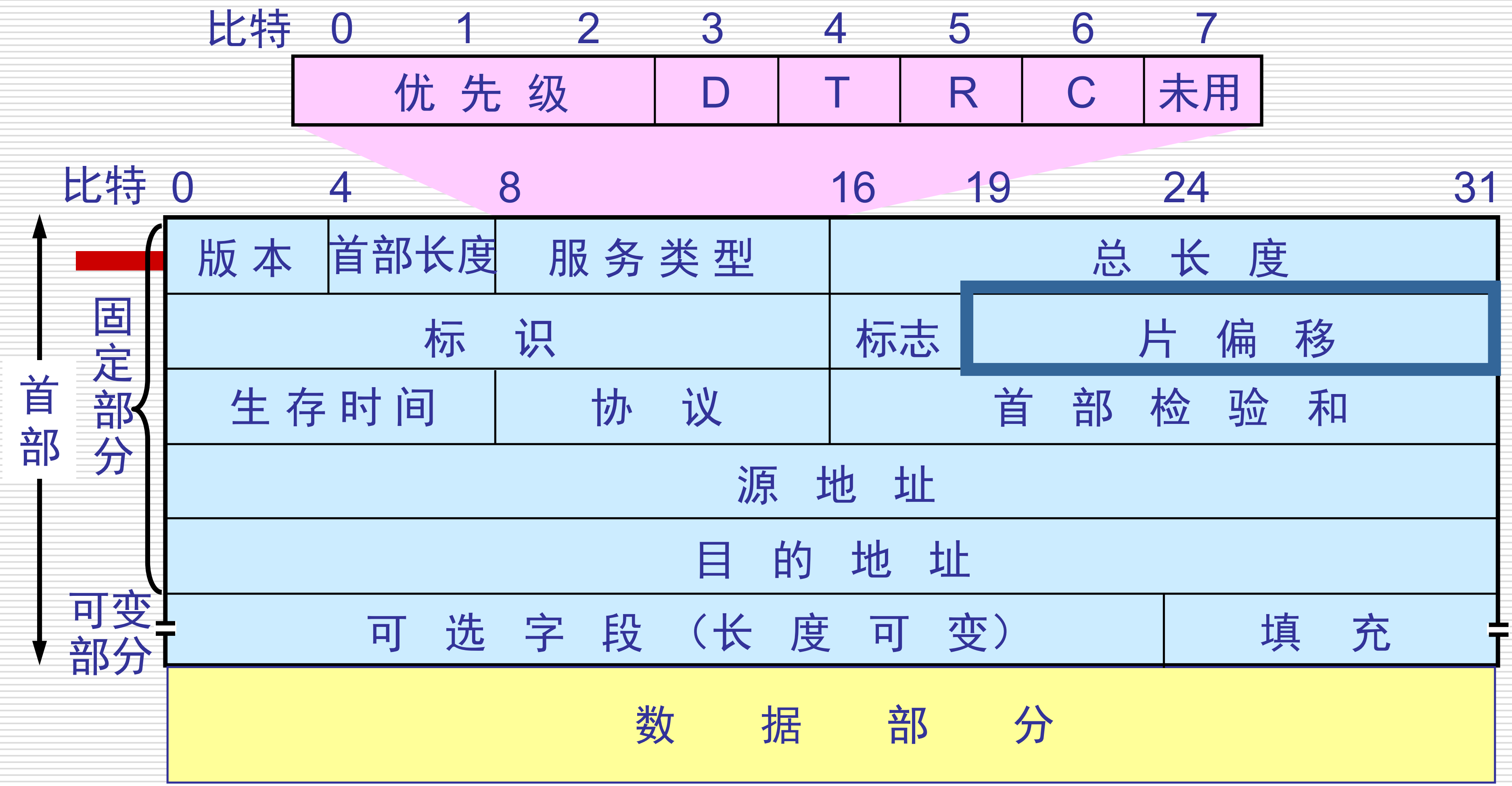


总长度——占 16 bit，指首部和数据之和的长度，
单位为字节，因此数据报的最大长度为 65535 字节。
总长度必须不超过最大传送单元 MTU。

标识(identification) 占 16 bit，

它是一个计数器，用来产生数据报的标识。

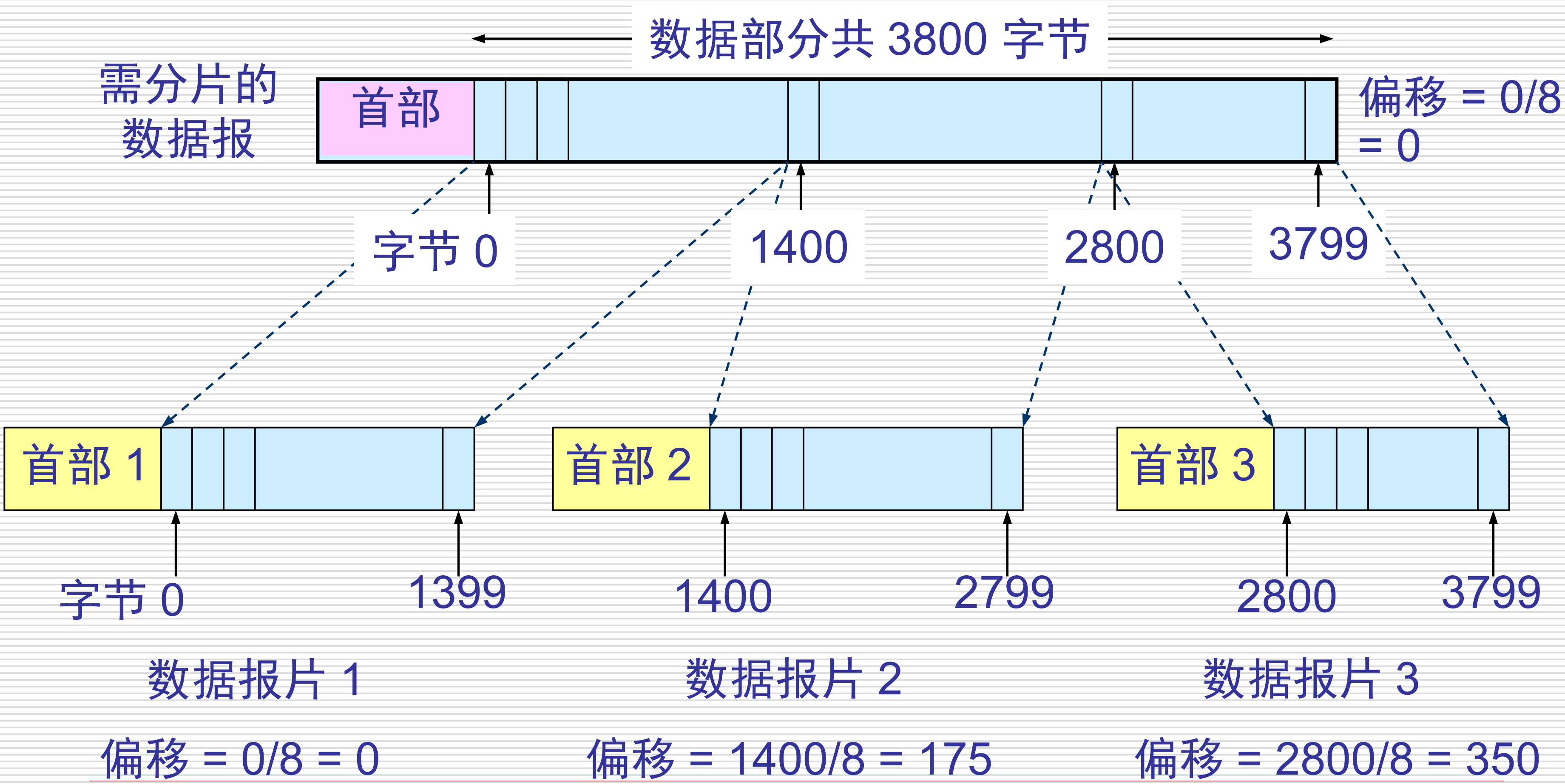
标志占 3 bit，最高位为0
MF为0表示最后一个分片



片偏移(12 bit)指出：较长的分组在分片后某片在原分组中的相对位置。

片偏移以 8 个字节为偏移单位。

IP 数据报分片的举例

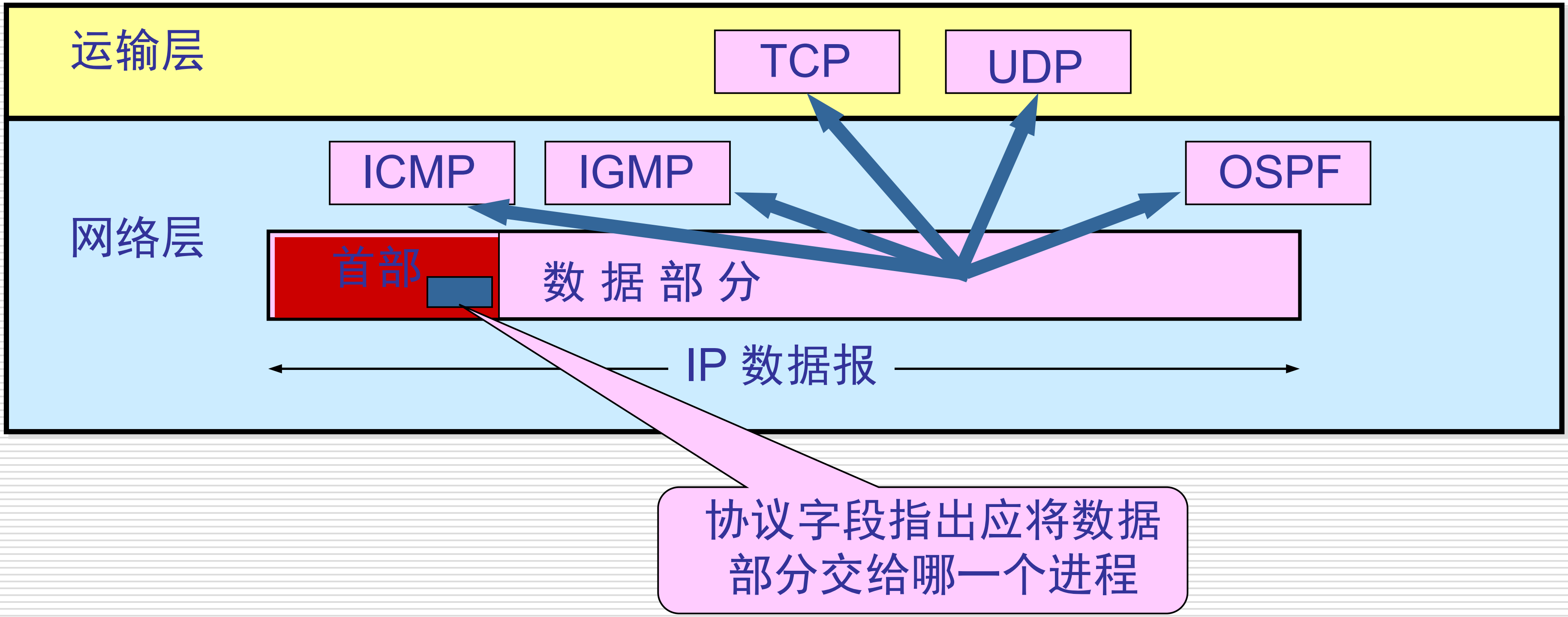


数据部分共 3800 字节
需分片的
数据报
首部
偏移 = 0/8
= 0
字节 0
1400
2800
3799
首部 1
首部 2
首部 3
字节 0
1399
1400
2799
2800
3799
数据报片 1
数据报片 2
数据报片 3
偏移 = 0/8 = 0
偏移 = 1400/8 = 175
偏移 = 2800/8 = 350

生存时间(8 bit)记为 TTL (Time To Live)

数据报在网络中可通过的路由器数的最大值。

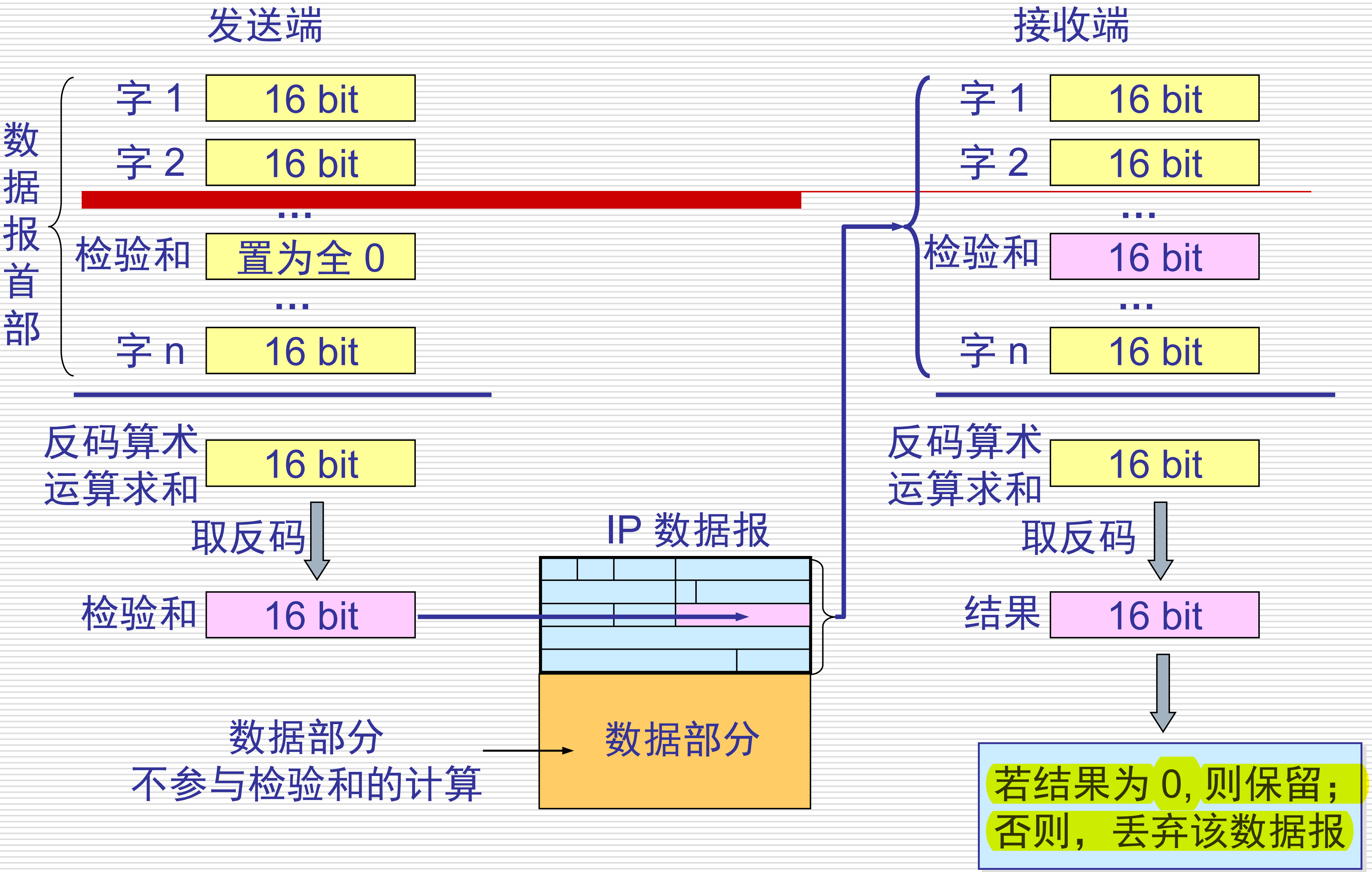
协议(8 bit)字段指出此数据报携带的数据使用何种协议
以便目的主机的 IP 层将数据部分上交给哪个处理过程


运输层
TCP
UDP
网络层
ICMP
IGMP
OSPF
首部
数 据 部 分
IP 数据报
协议字段指出应将数据
部分交给哪一个进程

首部检验和(16 bit)字段只检验数据报的首部

不包括数据部分。

这里不采用 CRC 检验码而采用简单的计算方法。


发送端
接收端
数据报首部
字 1
16 bit
字 2
16 bit
…
检验和
置为全 0
…
字 n
16 bit
反码算术运算求和
16 bit
取反码
检验和
16 bit
IP 数据报
数据部分
数据部分不参与检验和的计算
字 1
16 bit
字 2
16 bit
…
检验和
16 bit
…
字 n
16 bit
反码算术运算求和
16 bit
取反码
结果
16 bit
若结果为 0，则保留；
否则，丢弃该数据报

源地址和目的地址都各占 4 字节

Network Layer Addresses

- IP addresses are 32 bits long
- They are represented as four octets in dotted decimal format

133.14.17.0

- The IP address has two components:
  - The network ID
  - The host ID

Layer 3 Addresses

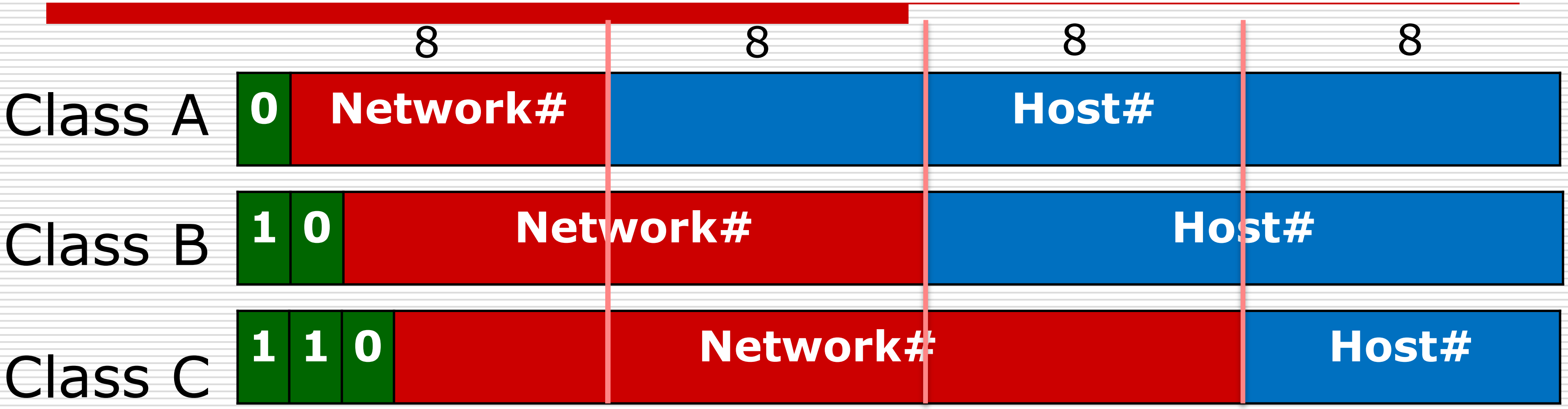
- Network ID
  - assigned by ARIN (American Registry for Internet Numbers, www.arin.net)
  - identifies the network to which a device is attached
  - may be identified by one, two, or three of the first three octets
- Host ID
  - assigned by a network administrator
  - identifies the specific device on that network
  - may be identified by one, two, or three of the last three octets

IP Addresses

- Different class addresses reserve different amounts of bits for the network and host portions of the address

Class A	N	H	H	H
Class B	N	N	H	H
Class C	N	N	N	H

Classes



0–127 Class A address

128-191 Class B address

192–223 Class C address

224–239 Class D – Multicast

240–255 Class E - Research

Number of Hosts

- The maximum number of hosts vary for each class.
  - Class A has 16,777,214 available hosts ($2^{24} - 2$)
  - Class B has 65,534 available hosts ($2^{16} - 2$)
  - Class C has 254 available hosts ($2^{8} - 2$)
- The first address in each network is reserved for the network address
- The last address is reserved for the broadcast address.

Reserved Addresses

- Network Address
  - An IP address that ends with binary 0s in the **host** part of the address
- Class A network address example:
  - 113.0.0.0
- Hosts on a network can only communicate *directly* with other hosts if they have the same network ID.

Reserved Addresses

- Broadcast Address
  - is used to send data to all of the devices on a network.
- Broadcast IP addresses end with binary 1s in the host part of the address.
- Class B broadcast address example:
  - 176.10.255.255
    (decimal 255 = binary 11111111)

IP Addressing

- **Class A**
  - **99.0.0.0:** a reserved *network number*
  - **99.255.255.255:** a *broadcast number*
- **Class B**
  - **156.1.0.0:** a reserved *network number*
  - **156.1.255.255:** a *broadcast number*
- **Class C**
  - **203.1.17.0:** a reserved *network number*
  - **203.1.17.255:**a *broadcast number*

Private Address Space

10.0.0.0 - 10.255.255.255

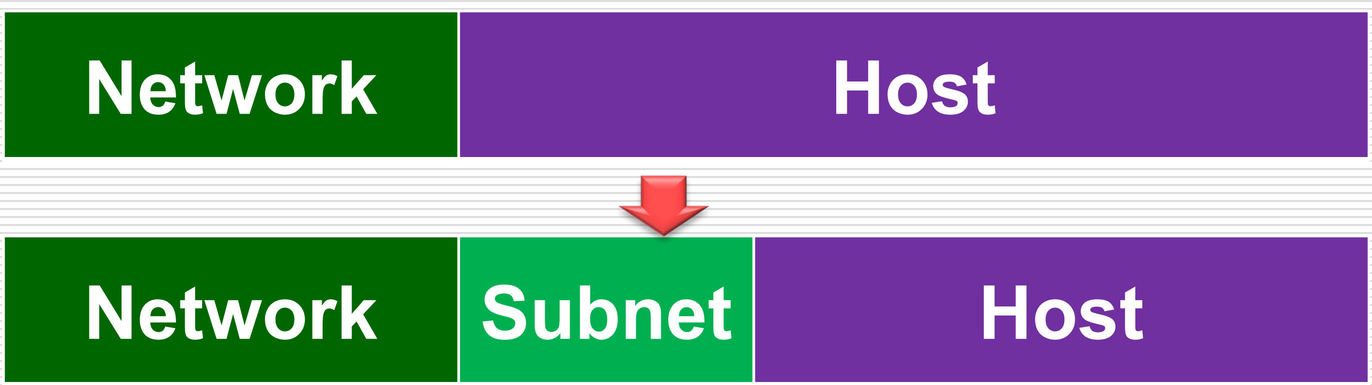
172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

- There are certain IP address ranges reserved for private IP addressing schemes.
- IP address depletion and its solutions:
  - NAT
  - CIDR
  - IPv6

Subnet

- Network administrators sometimes need to divide networks into smaller networks, called *subnets*, in order to provide extra flexibility
- Bits are borrowed from the host field and are designated as the subnet field



Basics of Subnetting

- Subnets are smaller divisions of networks
  - provide addressing flexibility.
- Subnet addresses are assigned locally, usually by a network administrator.
- Subnets reduce a broadcast domain.

How many bits can I borrow?

The minimum number of bits you can borrow is **two**

	Size of Host Field	Maximum # of borrowed bits
Class A	24	<u>22</u>
Class B	16	<u>14</u>
Class C	8	<u>6</u>

How many bits can I borrow?

- The minimum number of bits borrowed is 2,WHY?
  - If you were to borrow only 1 bit, to create a subnet, then you would only have a network number - the .0 network - and the broadcast number - the .1 network
- The maximum number of bits that can be borrowed can be any number that leaves at least 2 bits, remaining, for the host number

Byproduct: Waste Addresses

- We must strike a balance between the number of subnets required, the hosts per subnet that is acceptable, and the resulting waste of addresses.

Number of Bits Borrowed	Number of Subnets Created	Number of Hosts Per Subnet	Total Number of Hosts	Percent Used
2	2	62	124	49%
3	6	30	180	71%
4	14	14	196	77%
5	30	6	180	71%
6	62	2	124	49%

Class C

Subnet Mask

- Subnet mask
  - Alias: extended network prefix
  - define how many bits we use to construct the network, and how many bits to describe the host addresses

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

Calculating a Subnet

- We will subnet the IP address:
  - 223.14.17.0
- Need:
  - 13 subnets
  - 10 hosts on each subnet

Step #1

- Determine the default subnet mask
- What class IP address is this?
  - Class C
- Class C default subnet mask:
  - 255.255.255.0

Step #2

- Figure the actual number of subnets and hosts by borrowing bits from host ID
- Let's see how many subnets and hosts
  - 13 subnets
  - 10 hosts on each subnet
- Borrow 4 bits from the host

Step #3

223.14.17.0

X X X X H H H H

16 possible subnets

16 possible hosts for each subnet

Step #3 continued…

- We get 16 *possible* subnets and 16 *possible* hosts for each subnet because:
  - For the 4 bits borrowed each bit can be a 1 or a 0 leaving you with 2^4 or 16 possible combinations.
  - The same goes for the 4 leftover host bits.
- Important: There are only 14 *available* subnets and hosts on each subnet. Why?

Step #3 continued…

- Because you cannot use the first and last subnet.
- Because you cannot use the first and last address within each subnet.
- For each, one is the broadcast address and one is the network address.

Step #4

- Determine the subnet mask.

223.14.17.0

X X X X H H H H

- Where X represents the borrowed bits for subnetting.

Step #4 continued…

- Add the place values of X together to get the last octet decimal value of the subnet mask.

$$128 + 64 + 32 + 16 = \boxed{240}$$

- The subnet mask is: 255.255.255.240
- The subnet mask is used to reveal the subnet and host address fields in IP addresses.

Step 5

- Determine the ranges of host addresses

Subnet #	Subnet Bits	Host Bits	In Decimal
1	0000	0000-1111	.0 -.15
2	0001	0000-1111	.16 - .31
3	0010	0000-1111	.32 - .47
4	0011	0000-1111	.48 - .63
5	0100	0000-1111	.64 - .79
6	0101	0000-1111	.80 - .95
7	0110	0000-1111	.96 - .111
8	0111	0000-1111	.112 - .127

Step 5 continued…

Subnet #	Subnet Bits	Host Bits	In Decimal
9	1000	0000-1111	.128 -.143
10	1001	0000-1111	.144 - .159
11	1010	0000-1111	.160 - .175
12	1011	0000-1111	.176 - .191
13	1100	0000-1111	.192 - .207
14	1101	0000-1111	.208 - .223
15	1110	0000-1111	.224 - .239
16	1111	0000-1111	.240 - .255

Step 5 continued…

- 16 *possible* subnets.
- 16 *possible* hosts on each subnet
- 14 *available* subnets
- 14 *available* hosts on each subnet

Figuring Subnet Network Addresses

- Step #1: Change the IP host address to binary.
- Step #2: Change the subnet mask to binary.
- Step #3: Use the boolean operator AND to combine the two.
- Step #4: Convert the network binary address to dotted decimal.

Figuring Subnet Network Addresses

IP Host	172.16.2.120
Subnet Mask	255.255.255.0

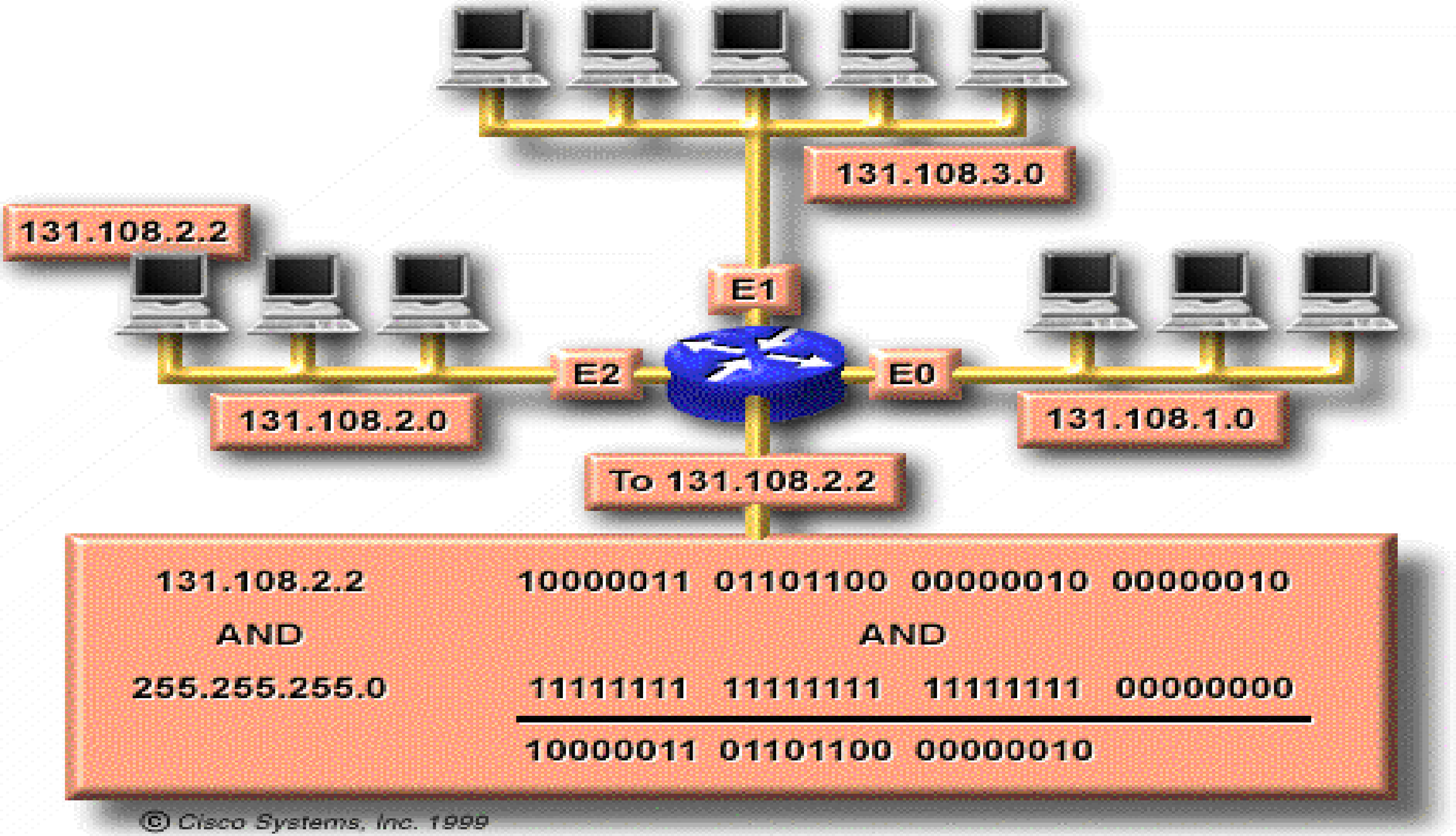
10101100.00010000.00000010.01111000

AND 11111111.11111111.11111111.00000000

10101100.00010000.00000010.00000000

172.16.2.0

- This is the subnet network address
- It can help determine path.



- In order to find the network ID of a subnet, the router must take the IP address, and the subnet mask, and logically, AND them together

Practice: IP Addressing Problems

Given 195.137.92.0 and needing 8 usable subnets, find the subnetwork numbers, the ranges of host numbers, and subnetwork broadcast numbers.

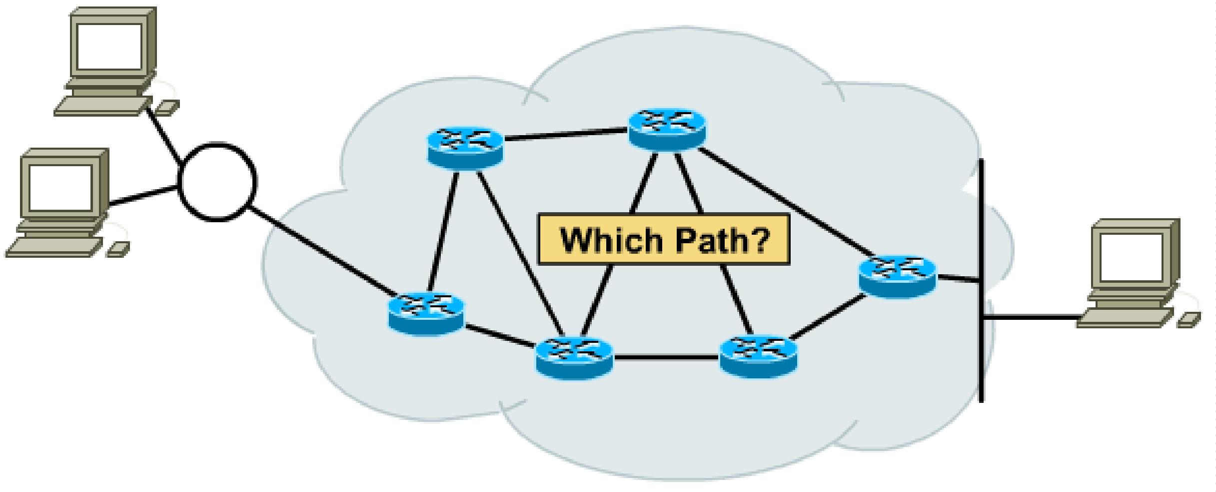
Solution

- IP Address is a class C. Default subnet mask is 255.255.255.0. We need to extend the network number by enough bits to give 8 usable subnets.
- Stealing 2 bits yields 2 usable subnets, stealing 3 bits yields 6 usable subnets, so we must steal 4 bits to get 14 usable subnets, of which we needed 8.
- This makes the subnet mask 255.255.255.240. So the Network number is 195.137.92.NNNN HHHH where Ns stand for network extension bits (subnets) and Hs stand for host numbers.
- Next we must number the subnets; there are 16 combinations of 4 bit binary numbers but they retain their place value within the last octet.

Layer3: Network Layer

- Overview of the Network Layer
- IP addresses and Subnets
- Layer 3 Devices
- ARP Protocol
- Network Layer Services
- Routed and Routing Protocols
- VLSM
- ICMP

Path determination

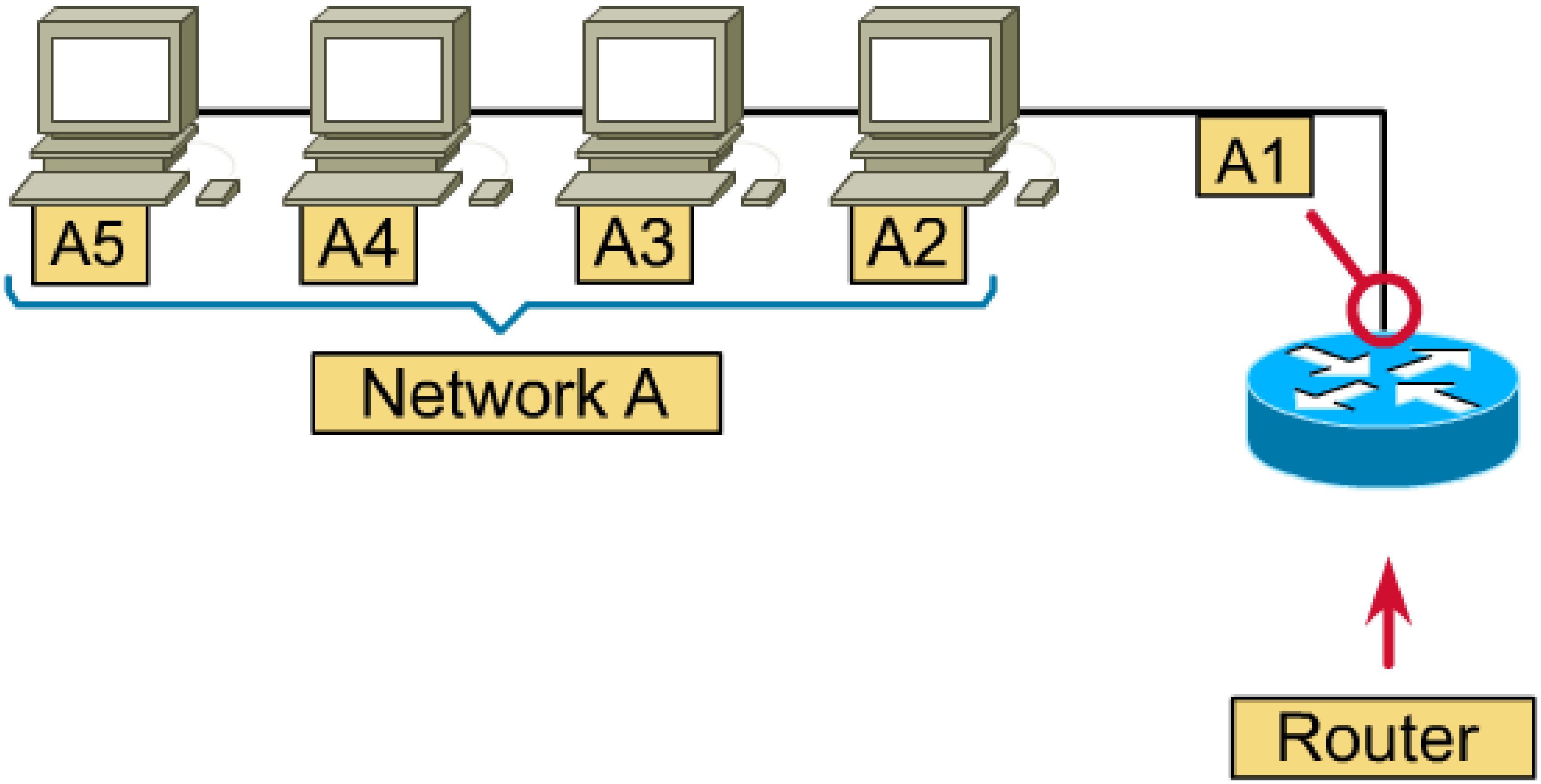


- Path determination
  - The router uses to choose the next hop in the path for the packet to travel to its destination based on the link bandwidth, hop, delay …

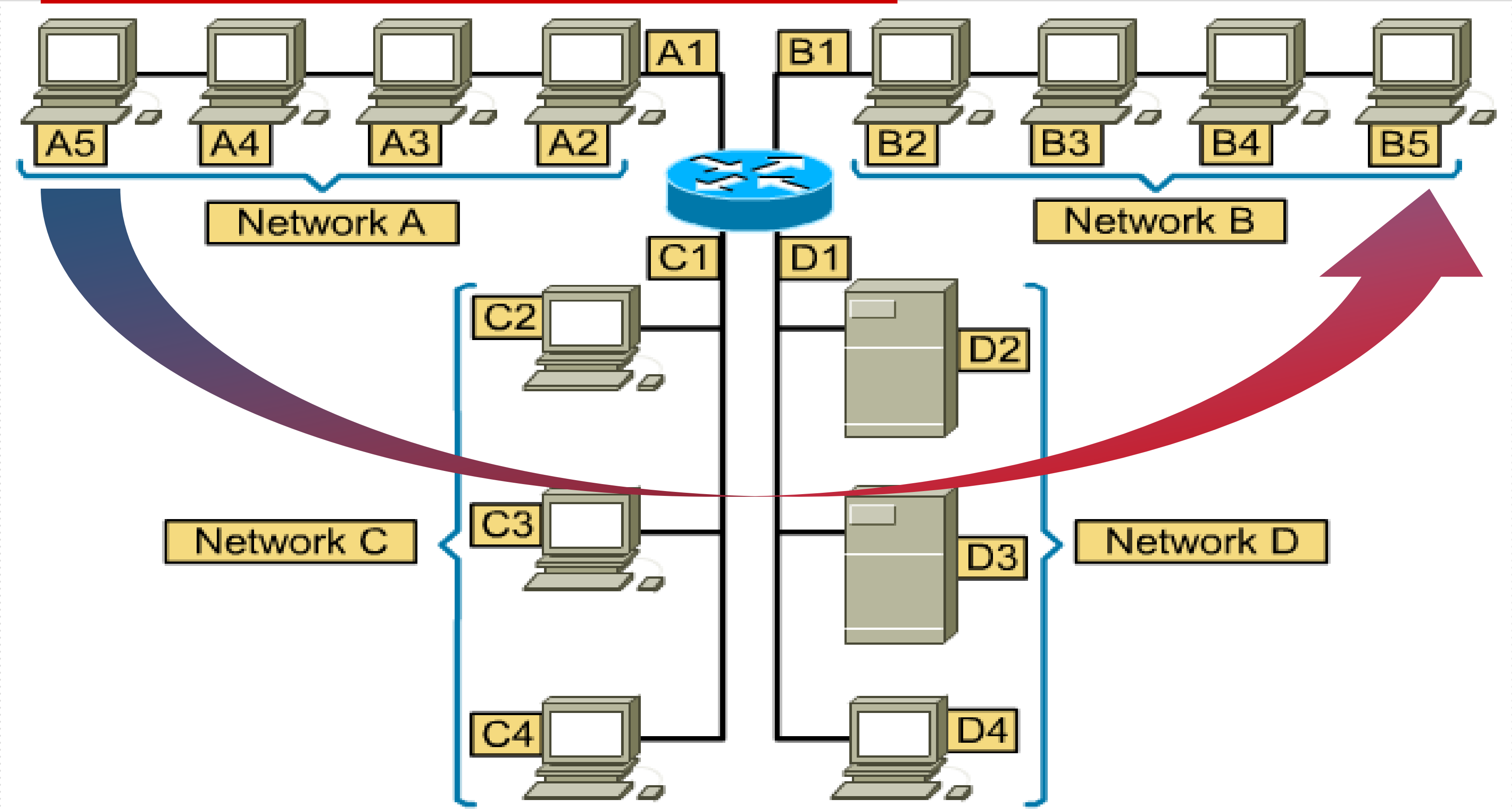
IP addresses

- IP addresses are implemented in software, and refer to the network on which a device is located.
- Routers connect networks, each of which must have a unique network number in order for routing to be successful.
- The unique network number is incorporated into the IP address that is assigned to each device attached to that network

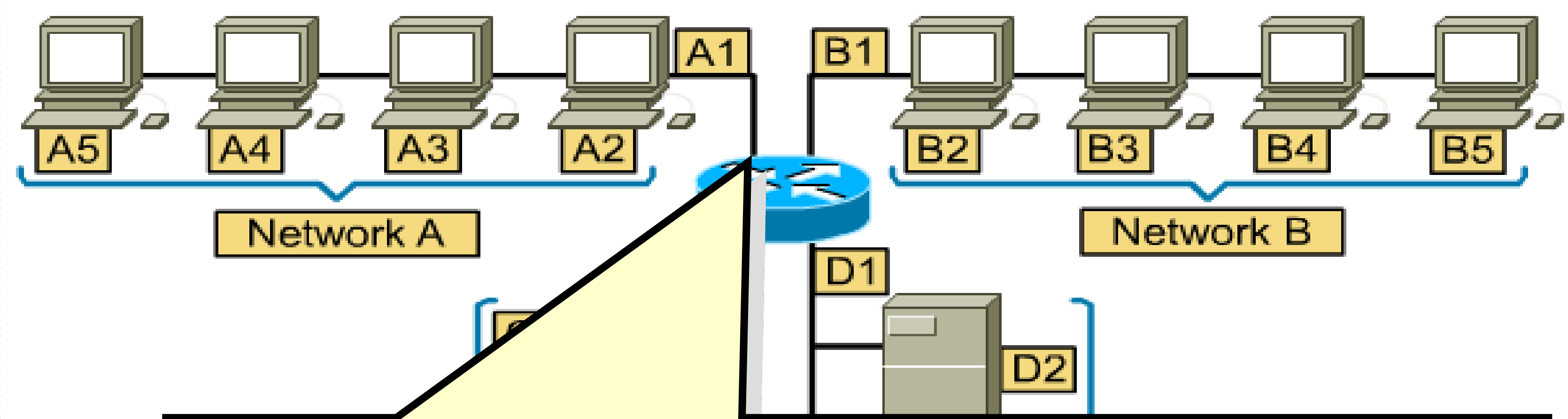
Router Interface



Router function



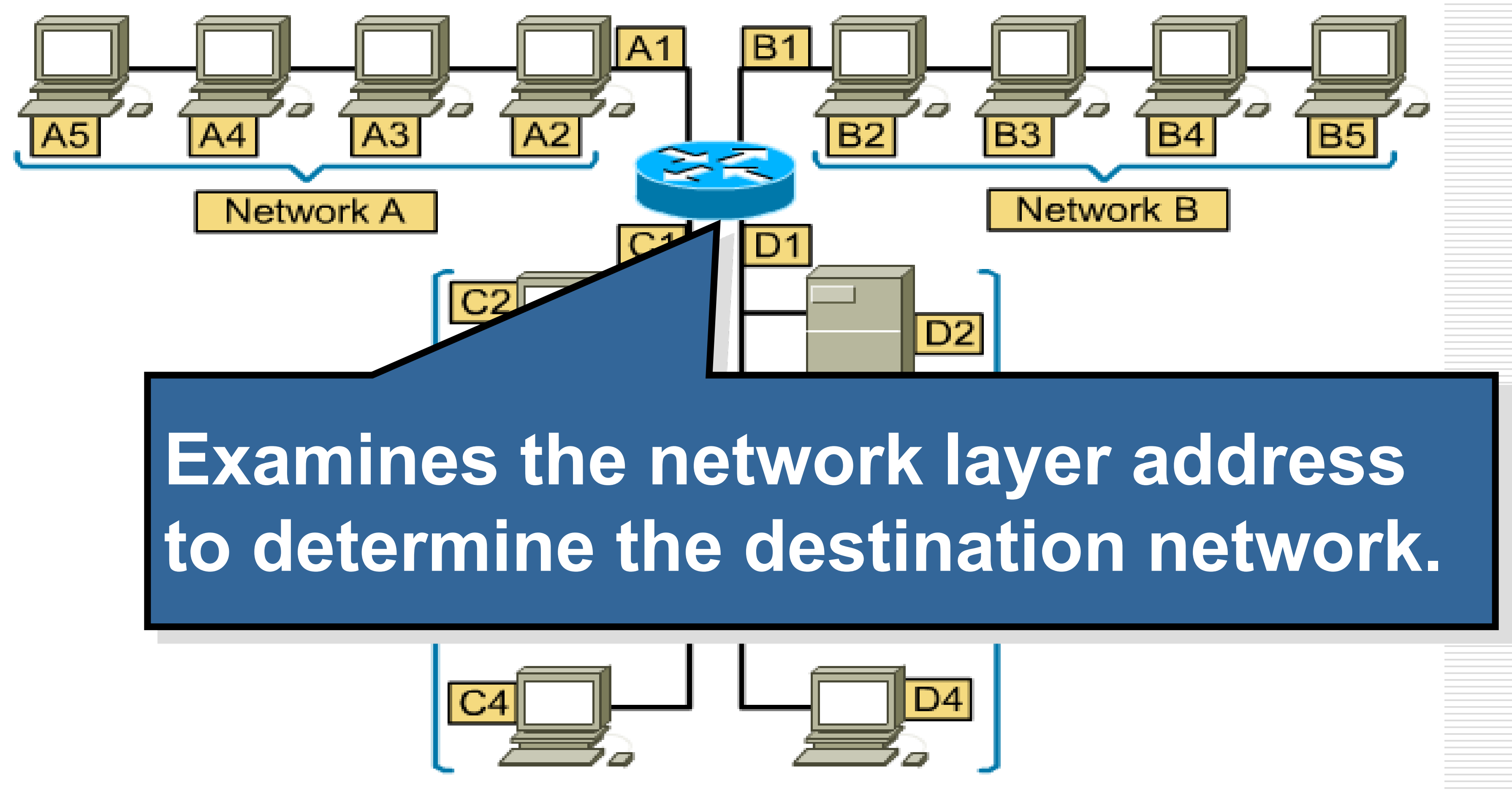
Router function (cont.1)



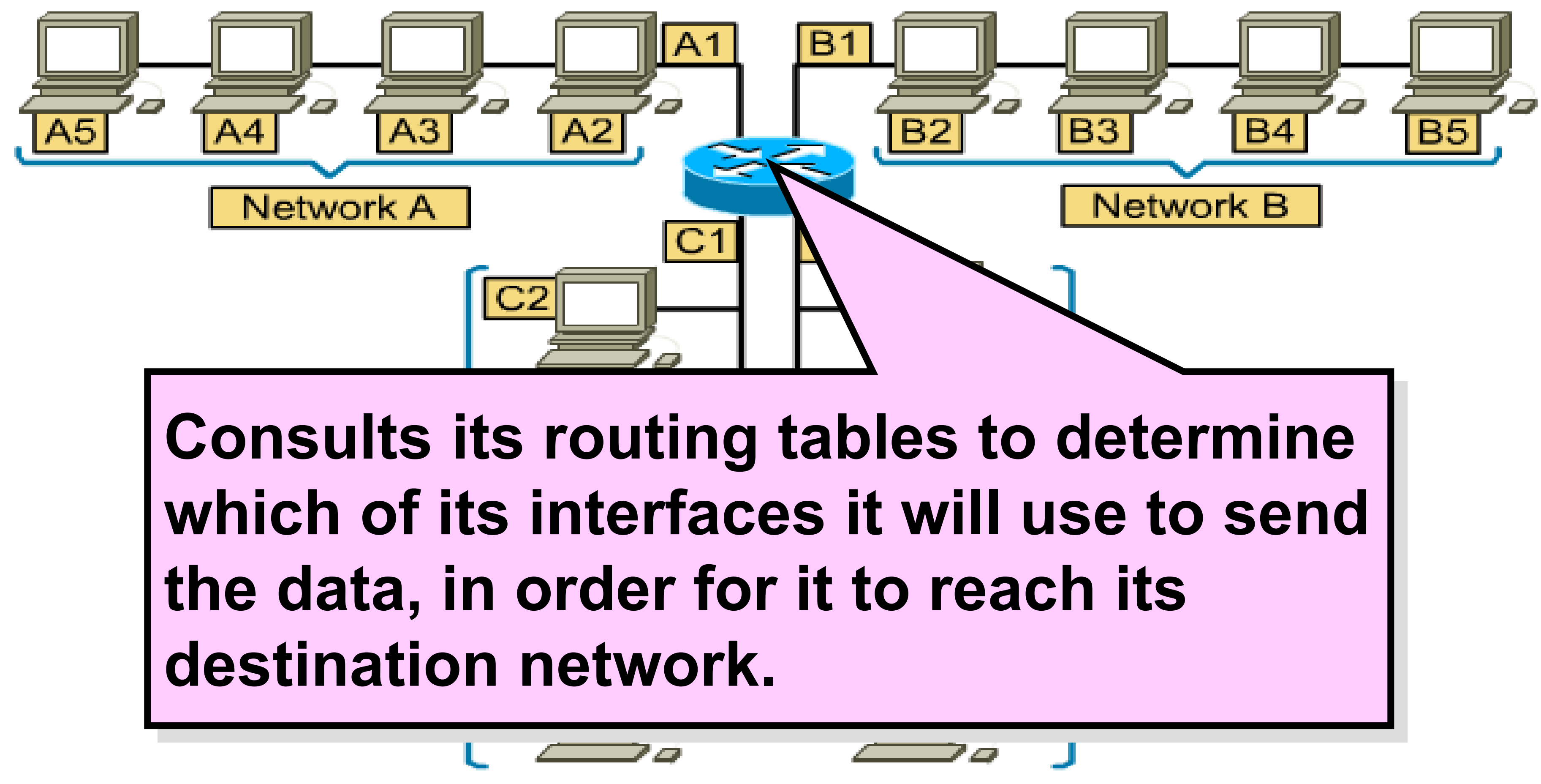
Strips off the data link header, carried by the frame.

(The data link header contains the MAC addresses of the source and destination.)

Router function (cont.2)

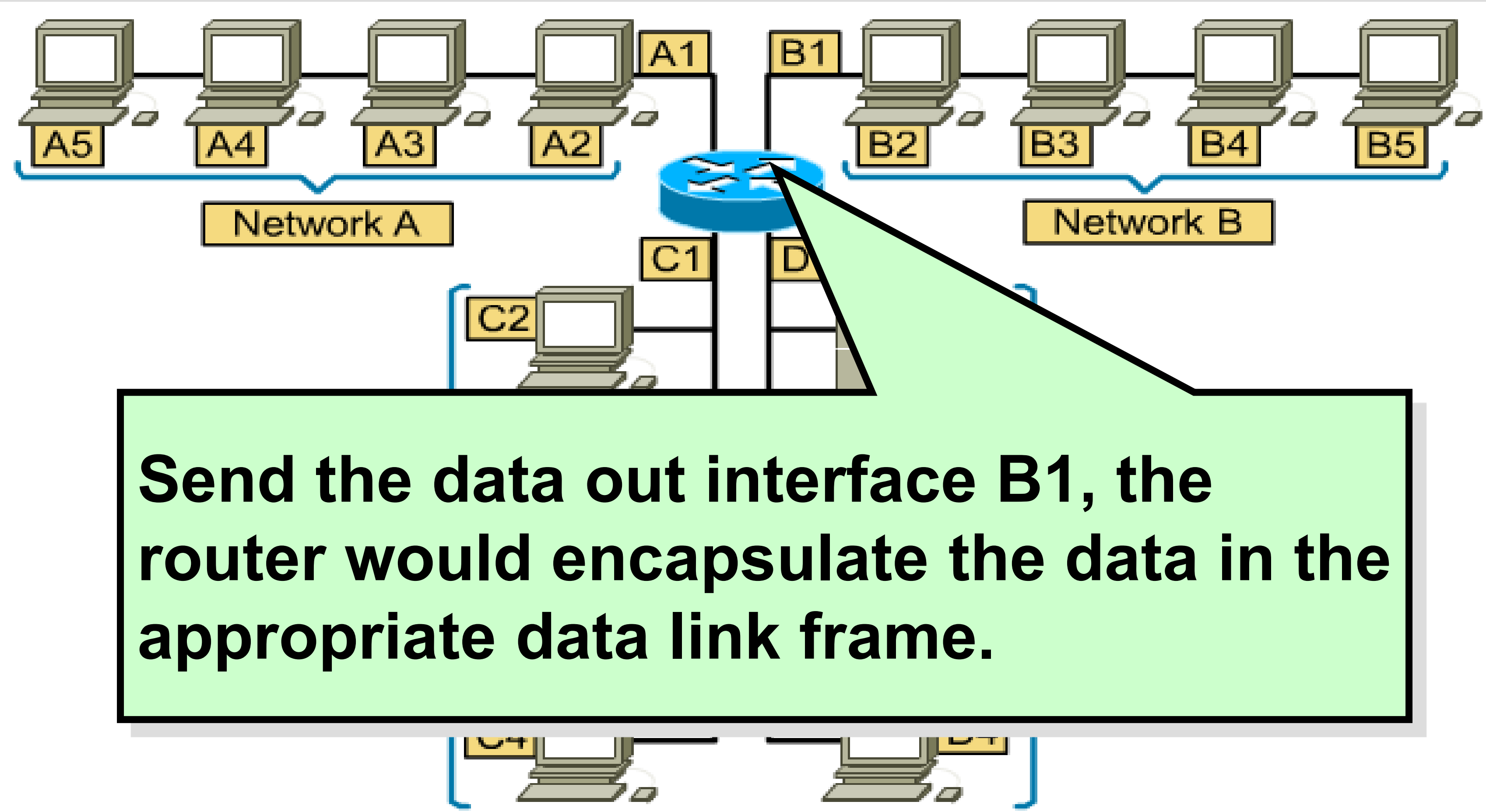


Router function (cont.3)



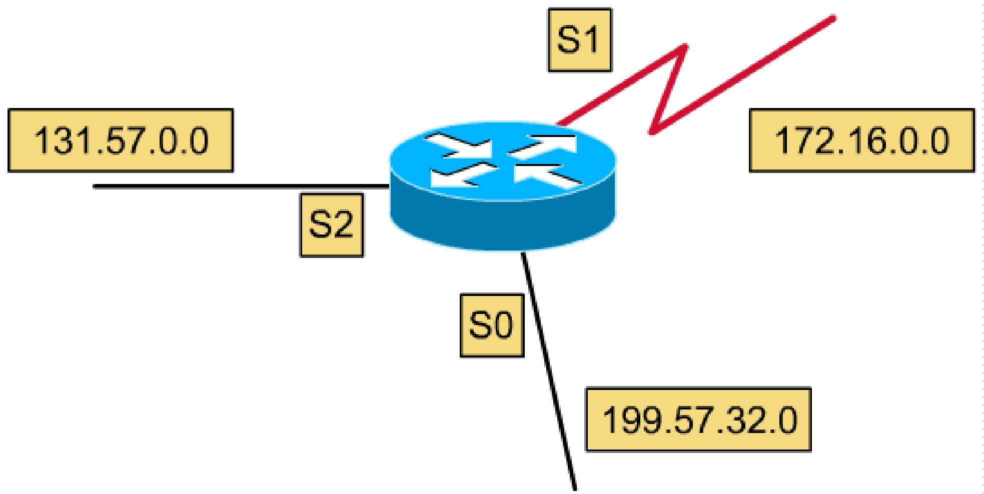
Consults its routing tables to determine which of its interfaces it will use to send the data, in order for it to reach its destination network.

Router function (cont.4)



Send the data out interface B1, the router would encapsulate the data in the appropriate data link frame.

Router Interface example



- Interface is a router's attachment to a network, it may also be referred to as a port in IP routing.
- Each interface must have a separate, unique network address.

IP address assignment

- Static addressing
  - Configure each individual device with an IP address
  - You should keep very meticulous records, because problems can occur if you use duplicate IP addresses.
- Dynamic addressing
  - There are a few different methods can be used to assign IP addresses dynamically:
    - RARP: Reverse Address Resolution Protocol.
    - BOOTP: BOOTstrap Protocol.
    - DHCP: Dynamic Host Configuration Protocol.

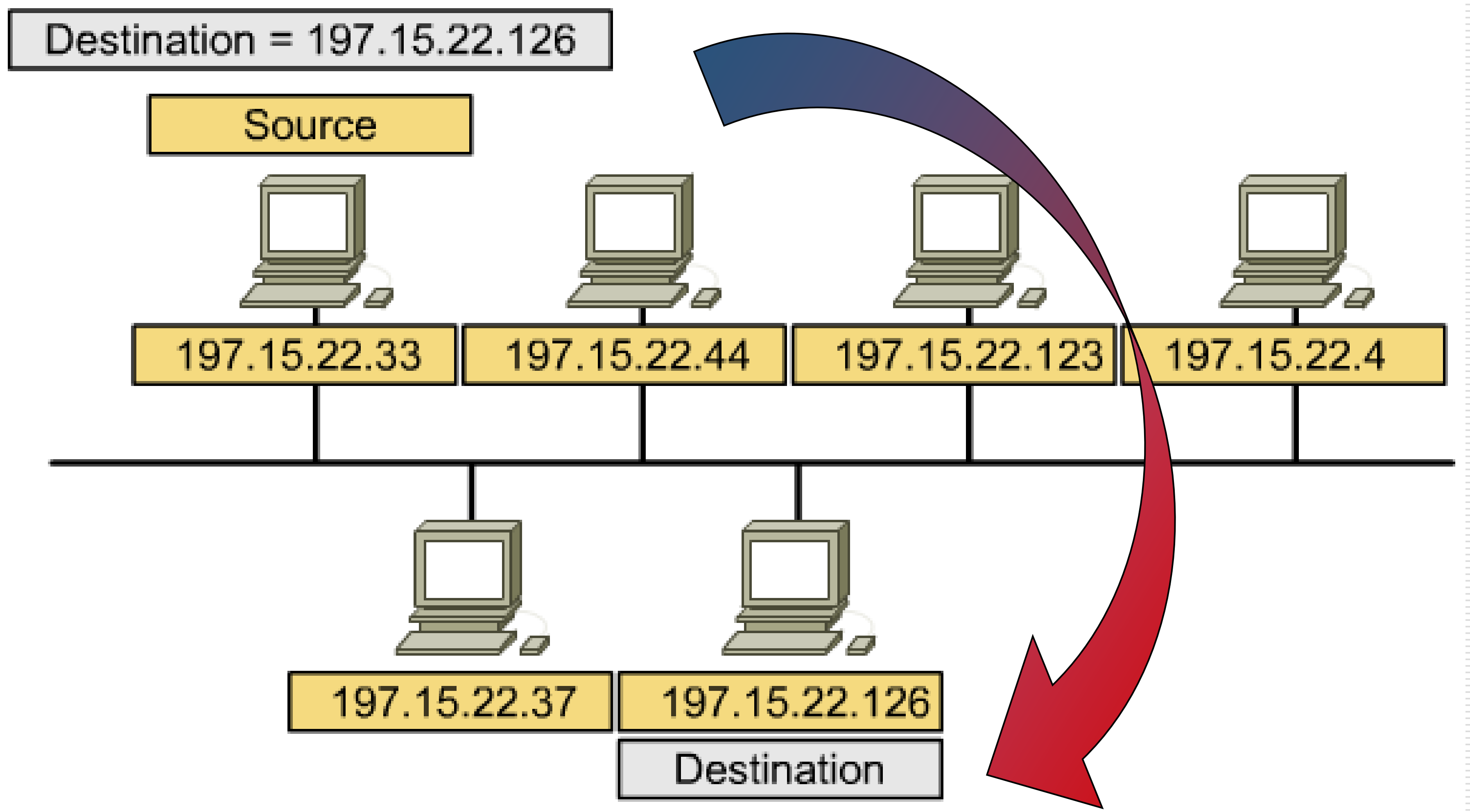
Layer3: Network Layer

- Overview of the Network Layer
- IP addresses and Subnets
- Layer 3 Devices
- ARP Protocol
- Network Layer Services
- Routed and Routing Protocols
- VLSM
- ICMP

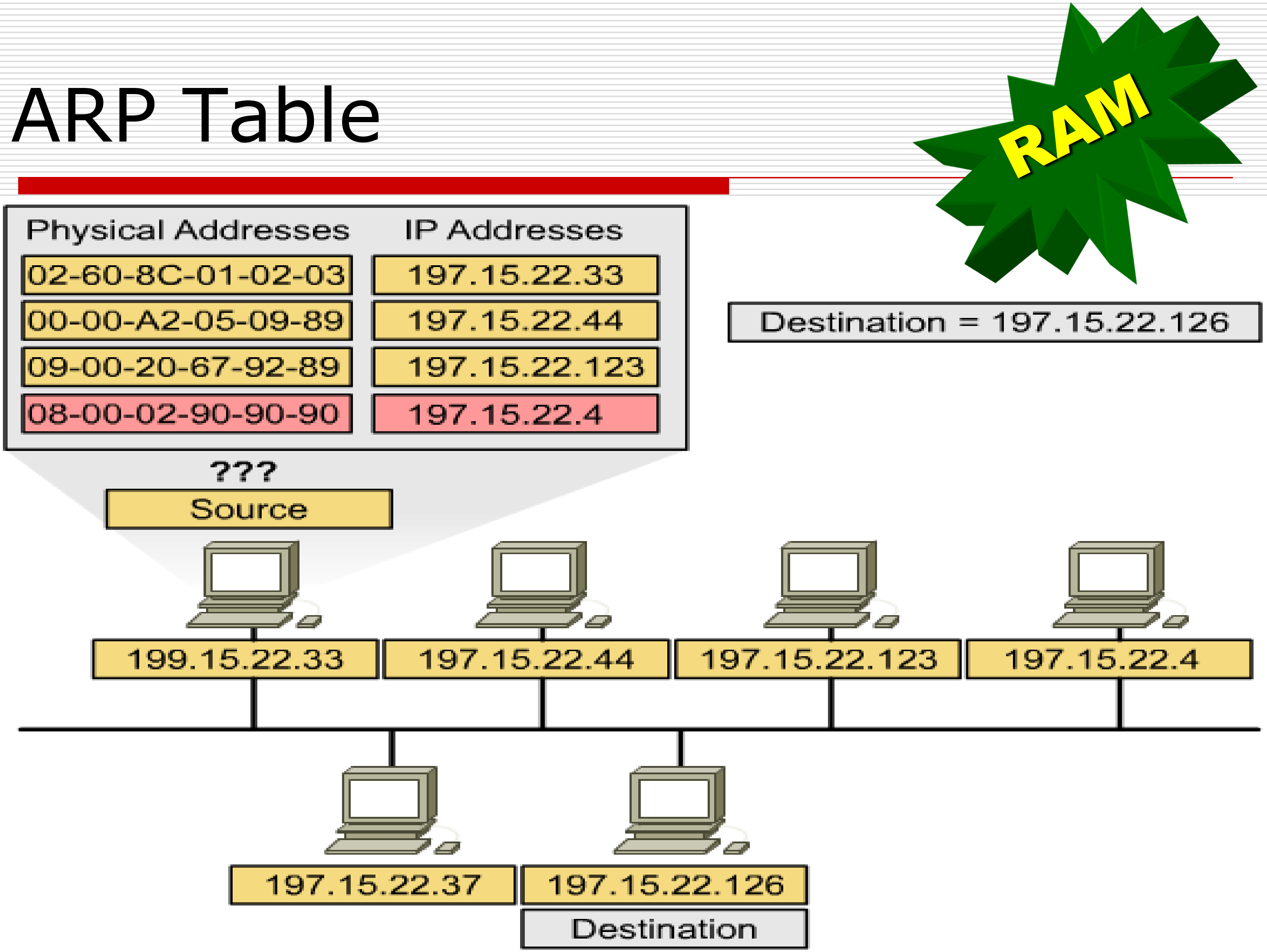
Address Resolution Protocol

- In order for devices to communicate, the sending devices need both the IP addresses and the MAC addresses of the destination devices.
- ARP enables a computer to find the MAC address of the computer that is associated with an IP address.

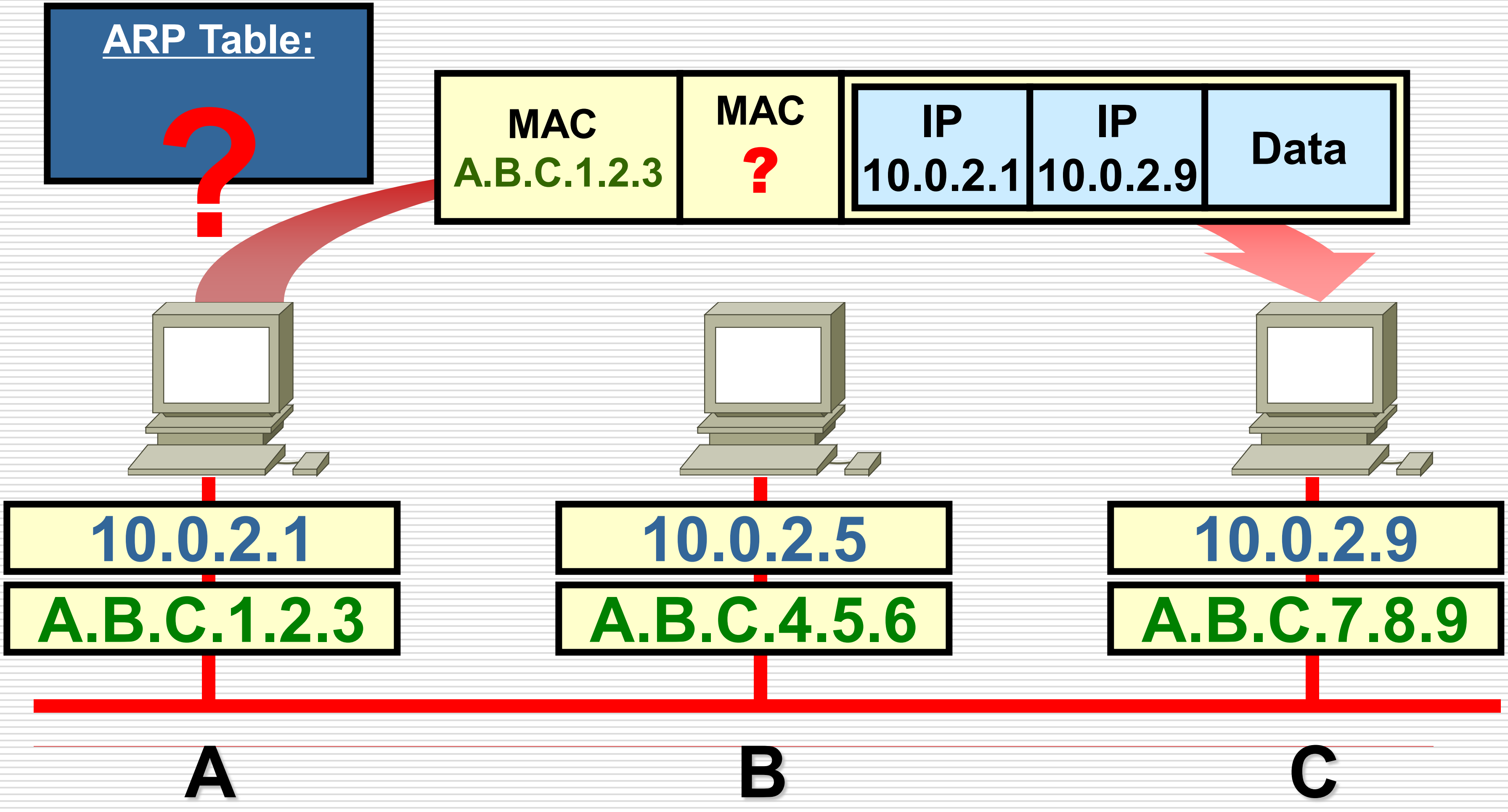
Address Resolution Protocol



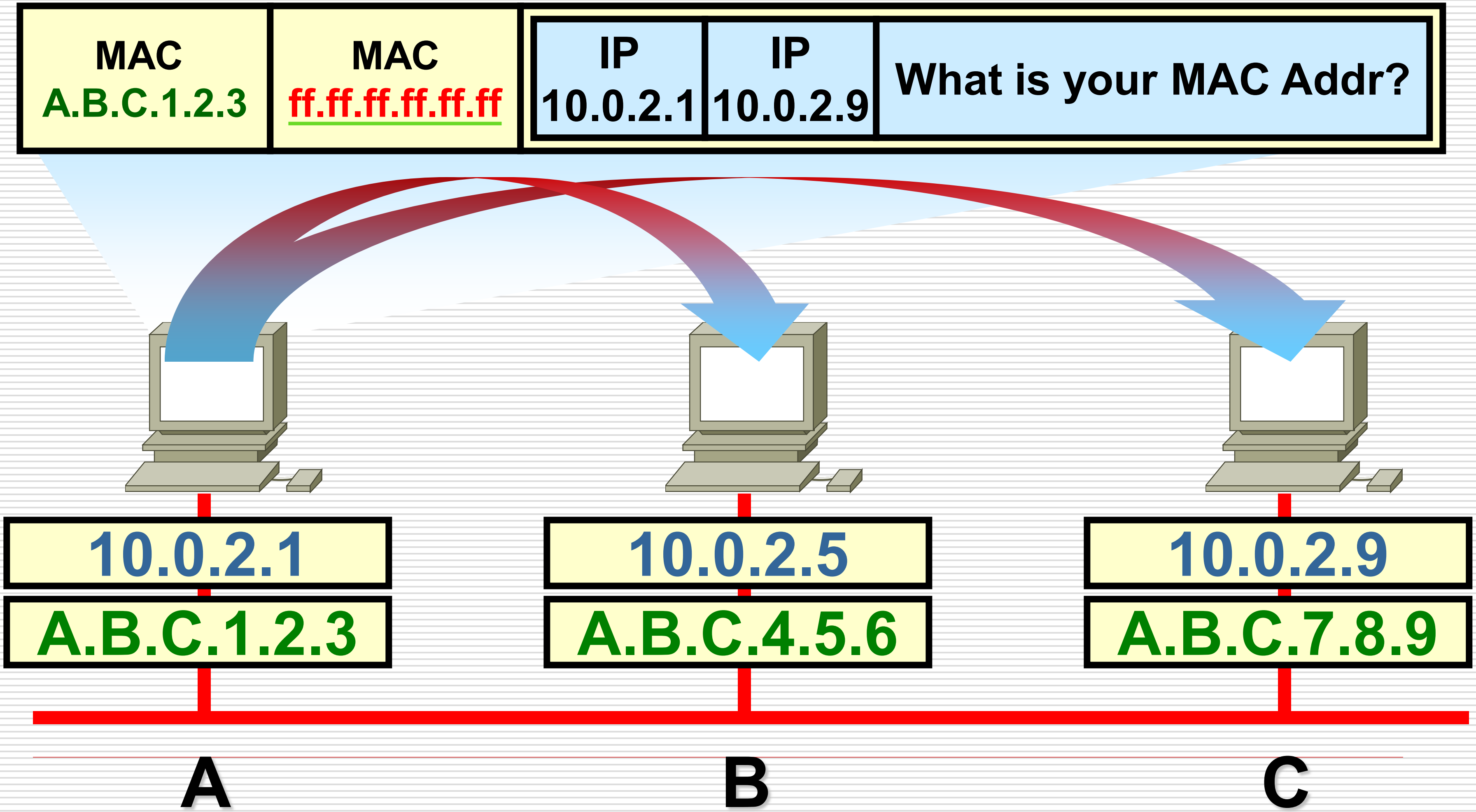
ARP Table


RAM
Physical Addresses
IP Addresses
02-60-8C-01-02-03
197.15.22.33
00-00-A2-05-09-89
197.15.22.44
09-00-20-67-92-89
197.15.22.123
08-00-02-90-90-90
197.15.22.4
Destination = 197.15.22.126
???
Source
199.15.22.33
197.15.22.44
197.15.22.123
197.15.22.4
197.15.22.37
197.15.22.126
Destination

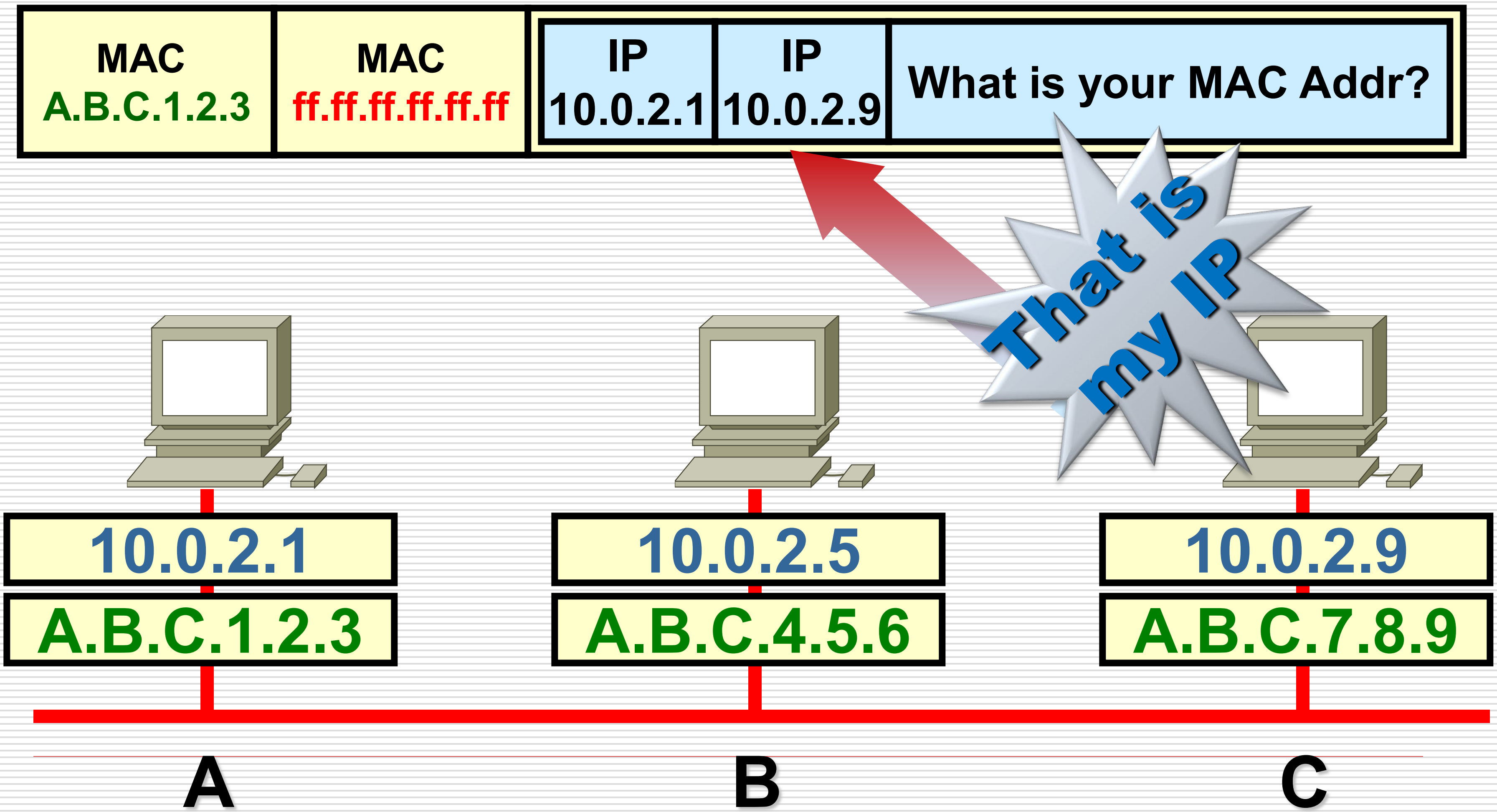
ARP operation



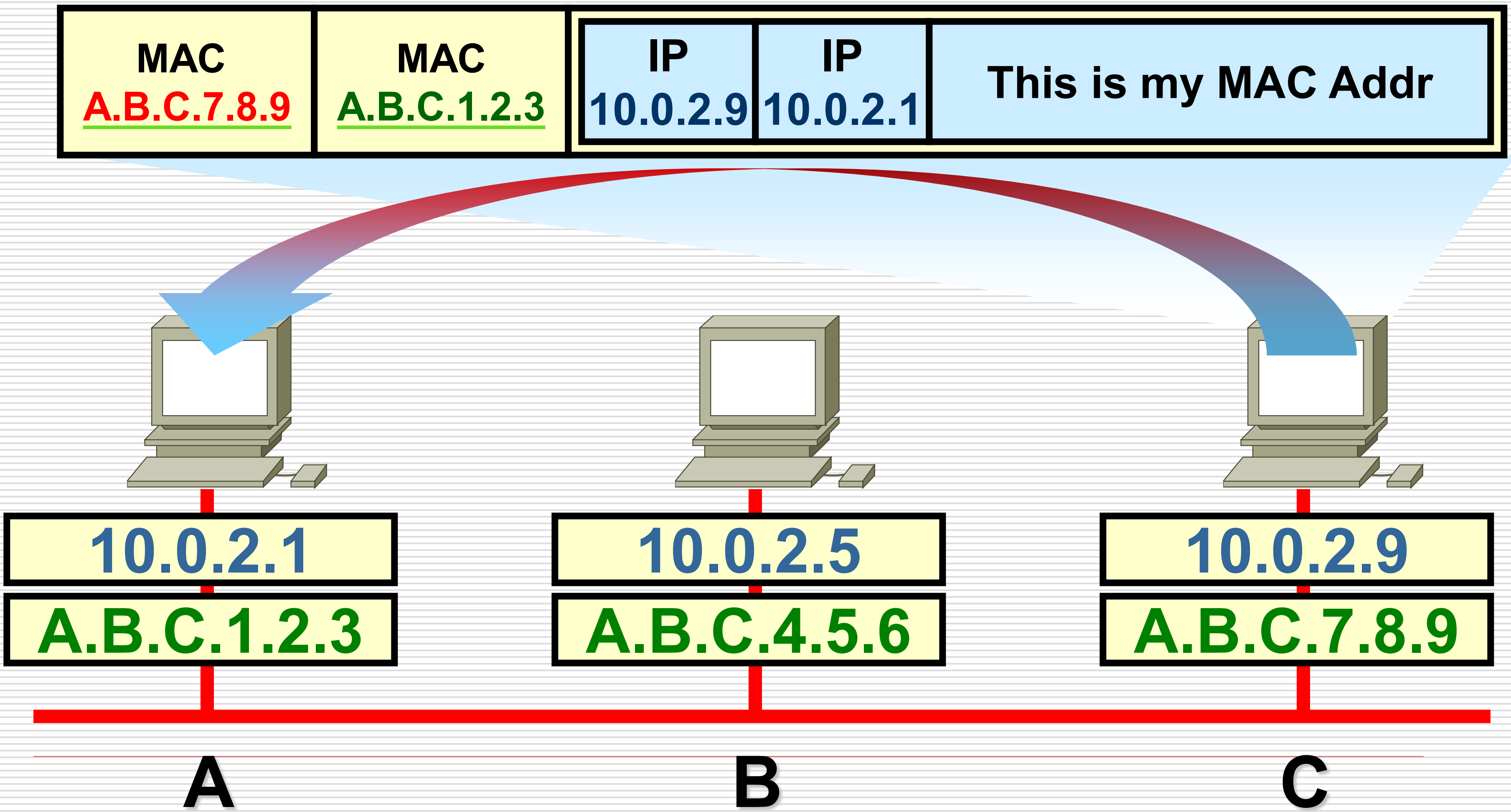
ARP operation: ARP request



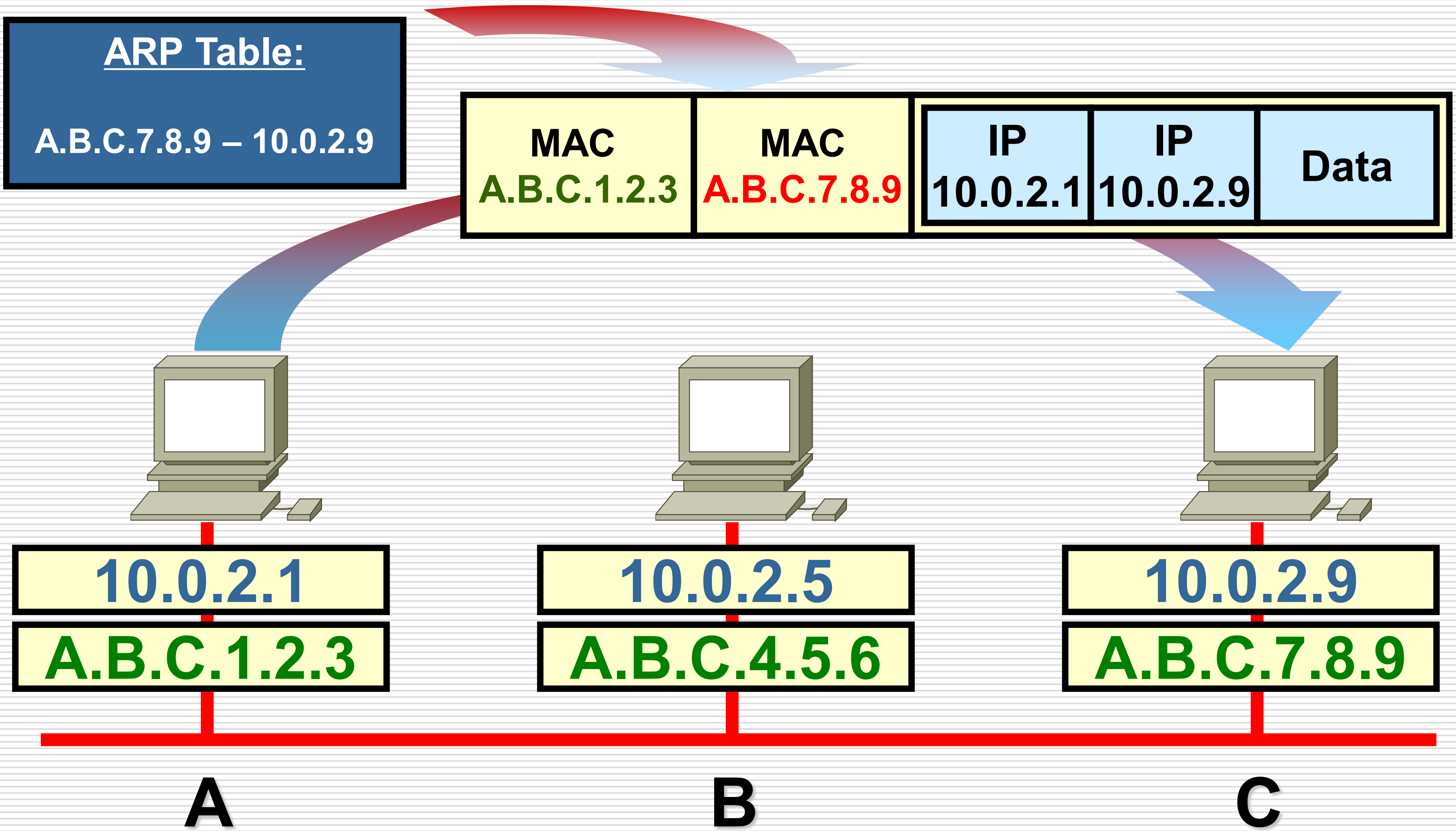
ARP operation: Checking



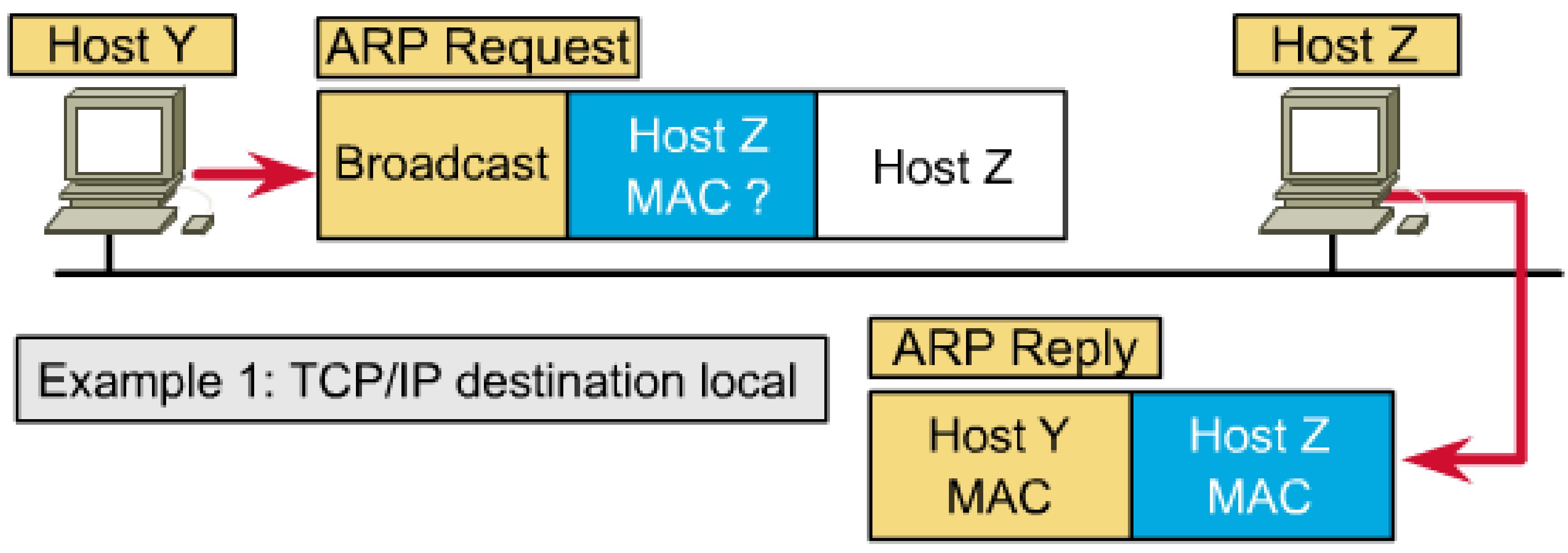
ARP operation: ARP reply



ARP operation: Caching



ARP: Destination local



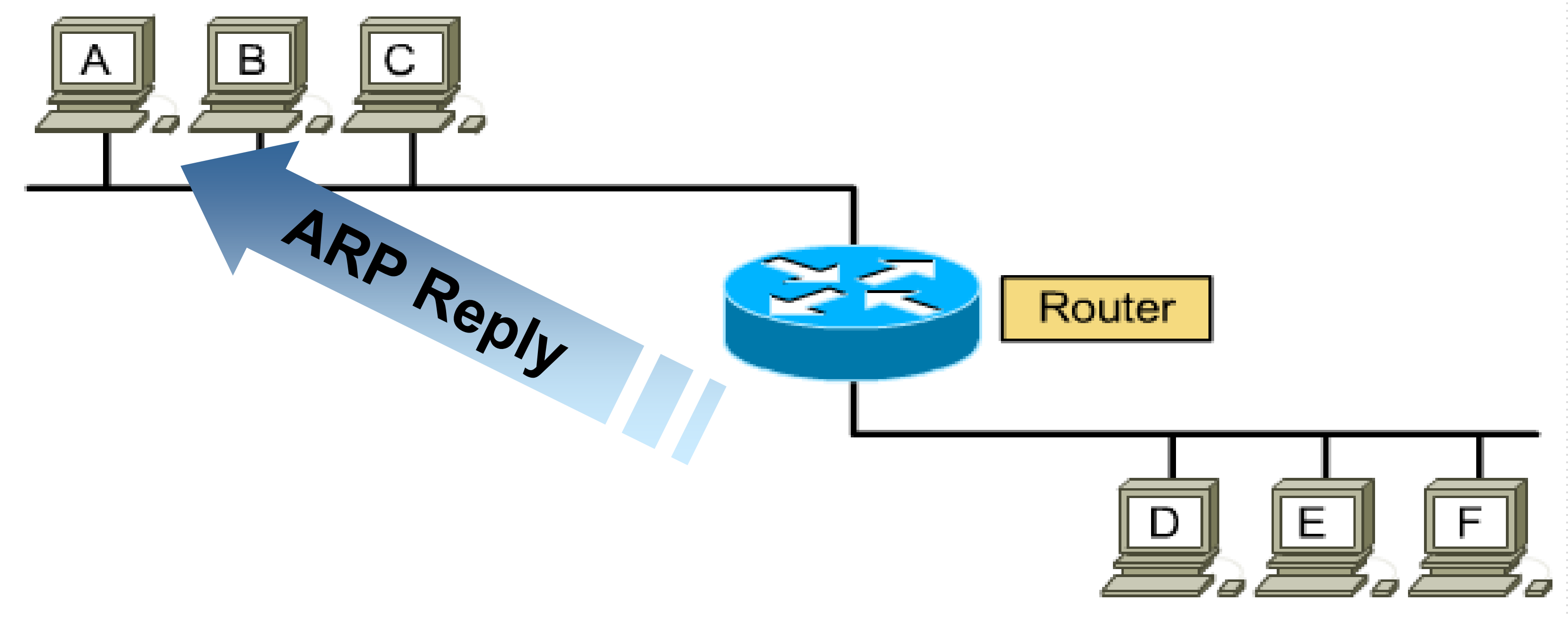
ARP: Internetwork Communication

- How to communicate with devices that are not on the same physical network segment?
  - Default gateway
  - Proxy ARP

Default gateway

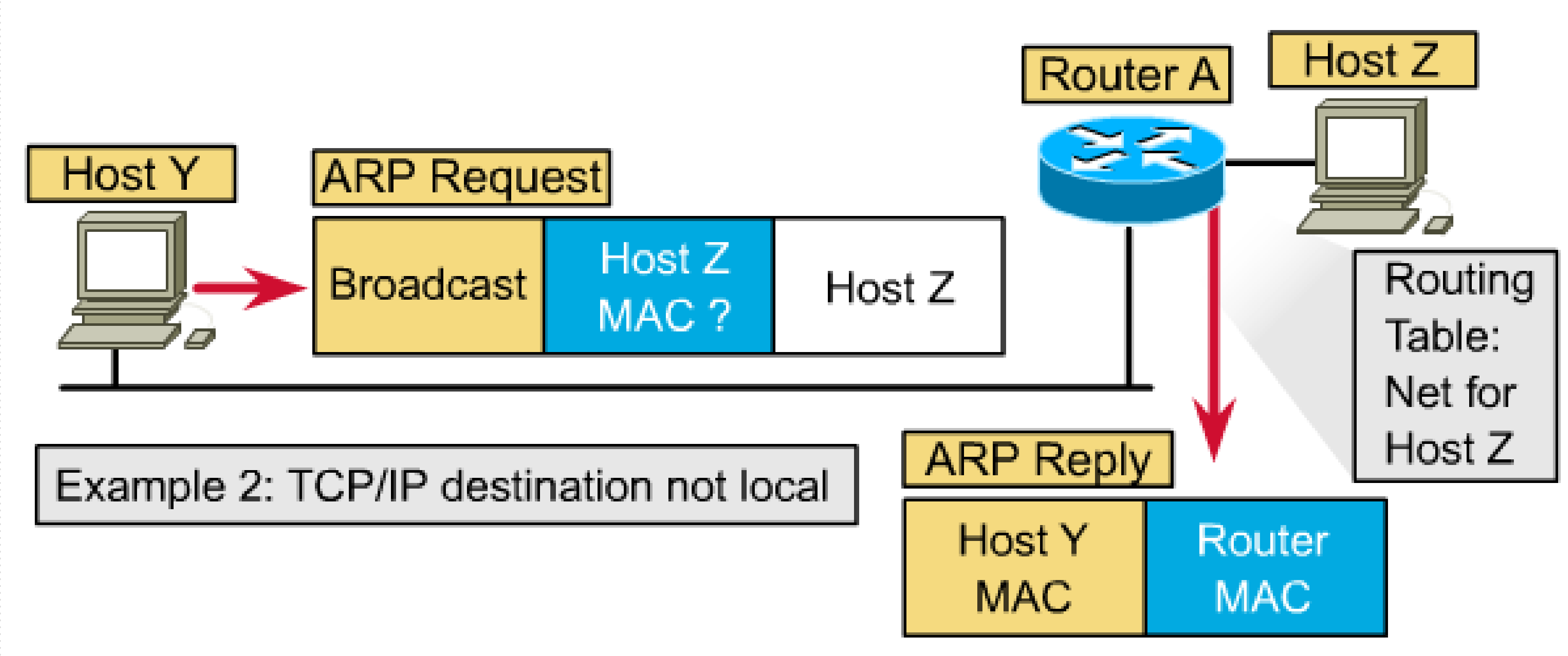
- In order for a device to communicate with another device on another network, you must supply it with a default gateway.
- A default gateway is the IP address of the interface on the router that connects to the network segment on which the source host is located.
- In order for a device to send data to the address of a device that is on another network segment, the source device sends the data to a default gateway.

Proxy ARP

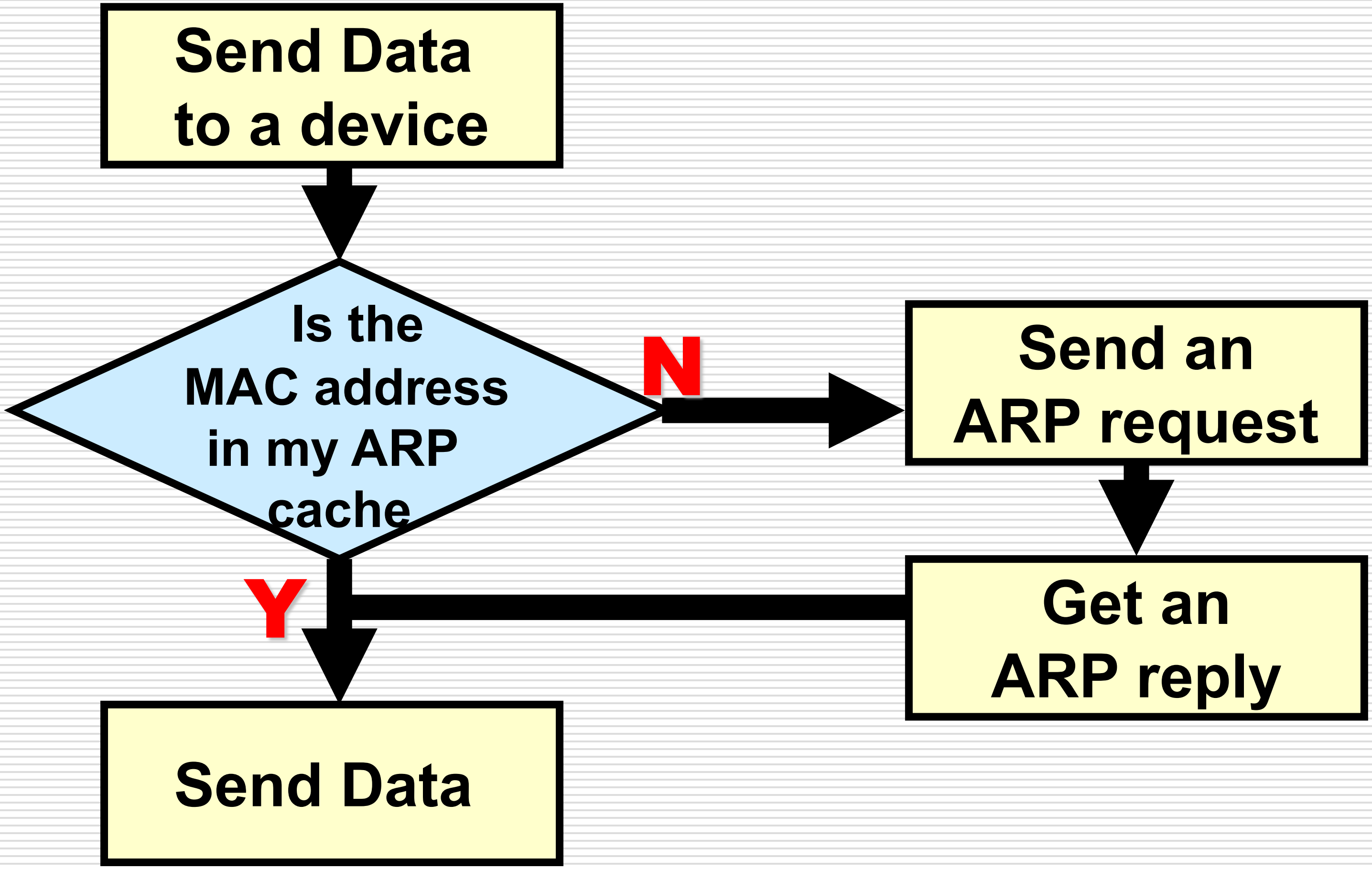


- Proxy ARP is a variation of the ARP.
- In the case the source host does not have a default gateway configured.

ARP: Destination not local



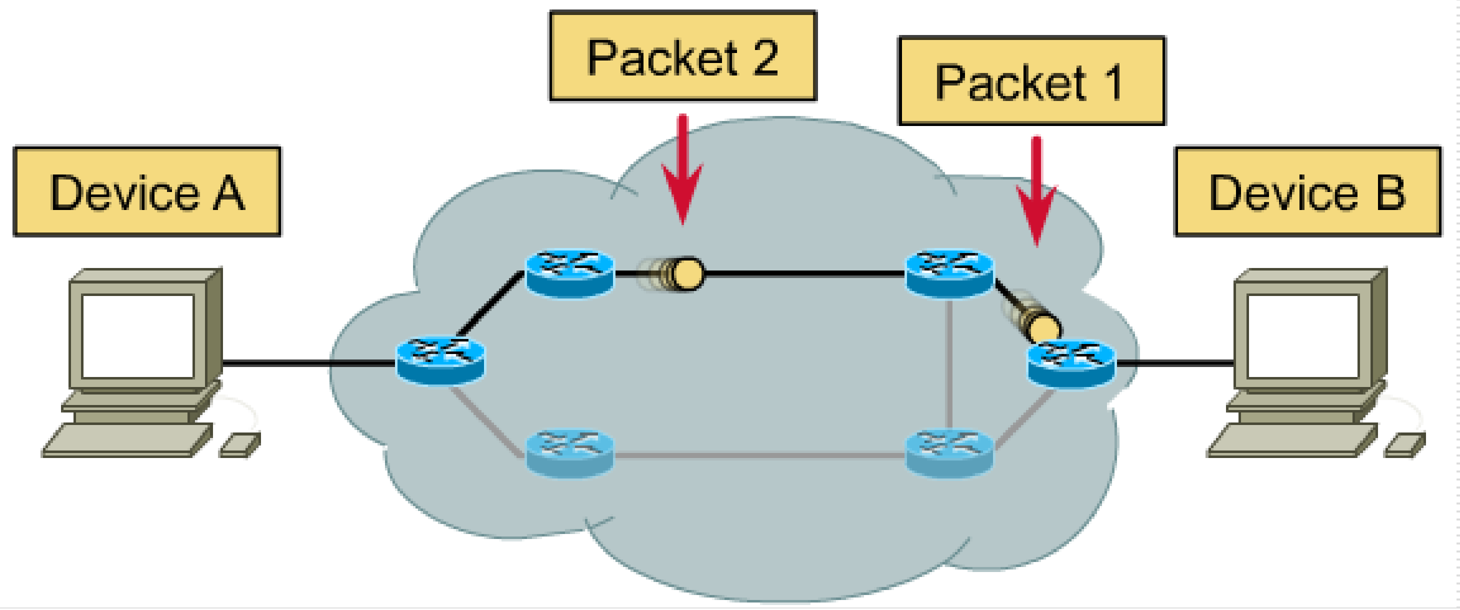
ARP Flowchart



Layer3: Network Layer

- Overview of the Network Layer
- IP addresses and Subnets
- Layer 3 Devices
- ARP Protocol
- Network Layer Services
- Routed and Routing Protocols
- VLSM
- ICMP

Connection oriented network services

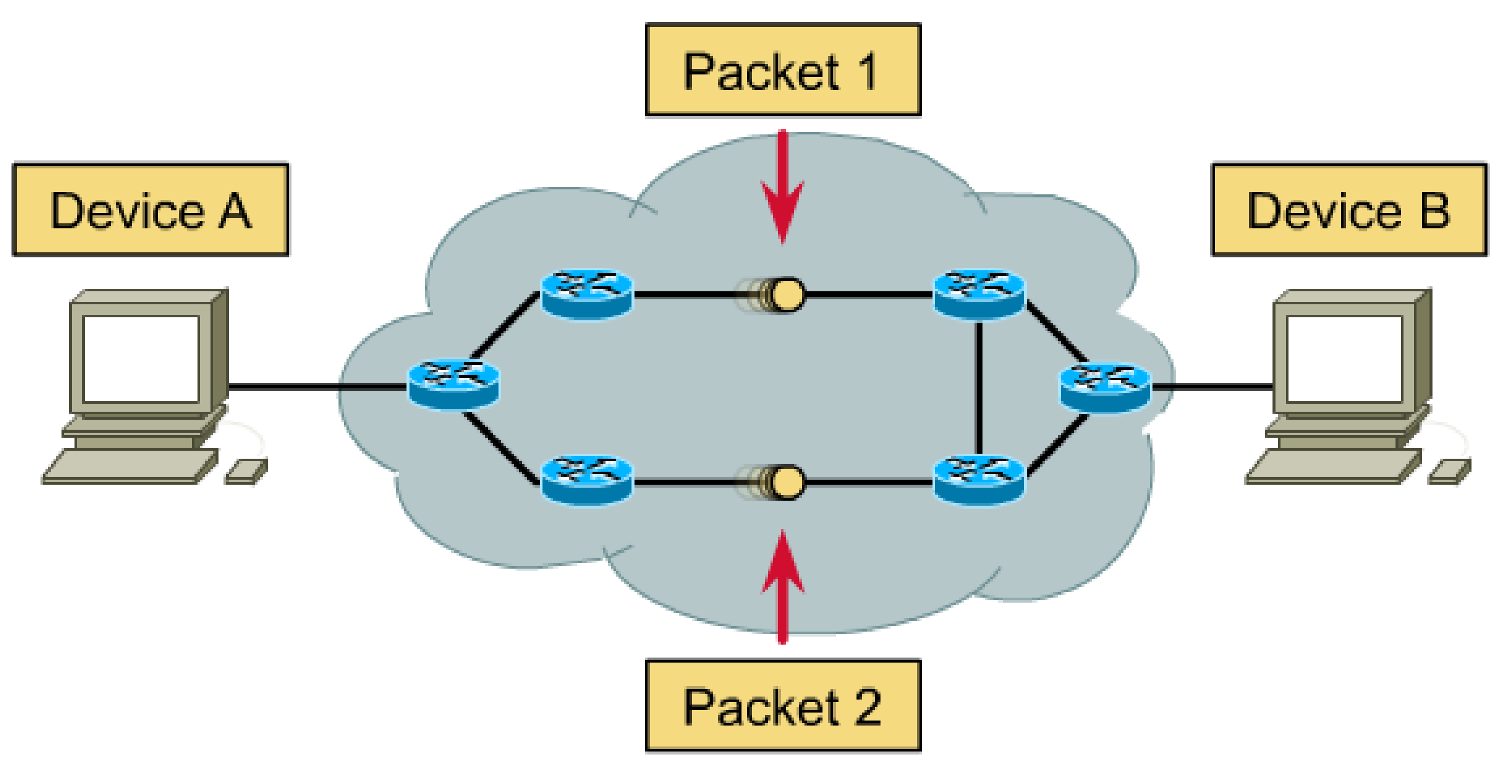


- A connection is established between the sender and the recipient before any data is transferred.

Circuit switched

- Connection-oriented vs. circuit switched.
  - However, the two terms are not the same
- Connection-oriented: establish a connection with the recipient, first, and then begin the data transfer.
- All packets travel sequentially across the same channel, or more commonly, across the same virtual circuit.

Connectionless network services



- They treat each packet separately.
- IP is a connectionless system.

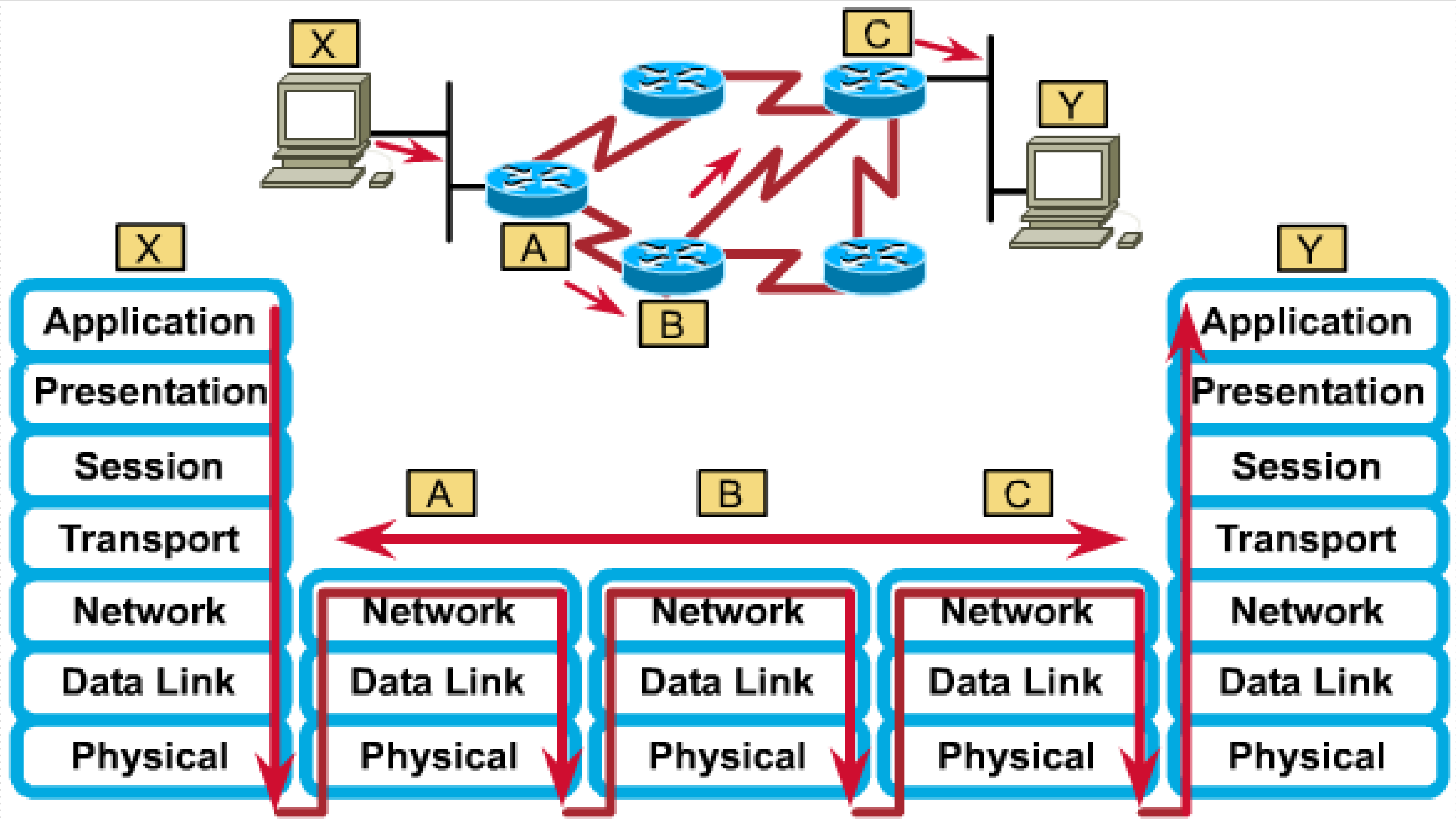
Packet switched

- Connectionless network vs. packet switched.
  - The two terms are not the same, either
- When the packets pass from source to destination, they can:
  - Switch to different paths.
  - Arrive out of order.
- Devices make the path determination for each packet based on a variety of criteria. Some of the criteria may differ from packet to packet.

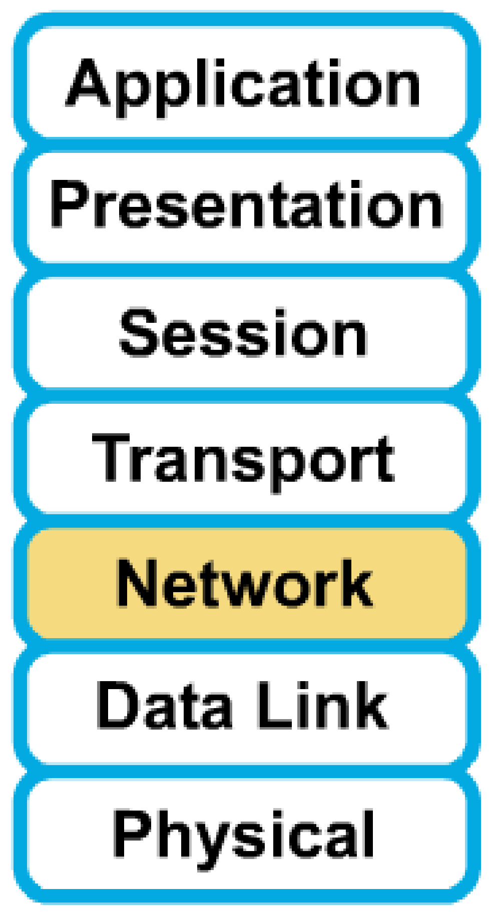
Layer3: Network Layer

- Overview of the Network Layer
- IP addresses and Subnets
- Layer 3 Devices
- ARP Protocol
- Network Layer Services
- Routed and Routing Protocols
- VLSM
- ICMP

Network protocol operation

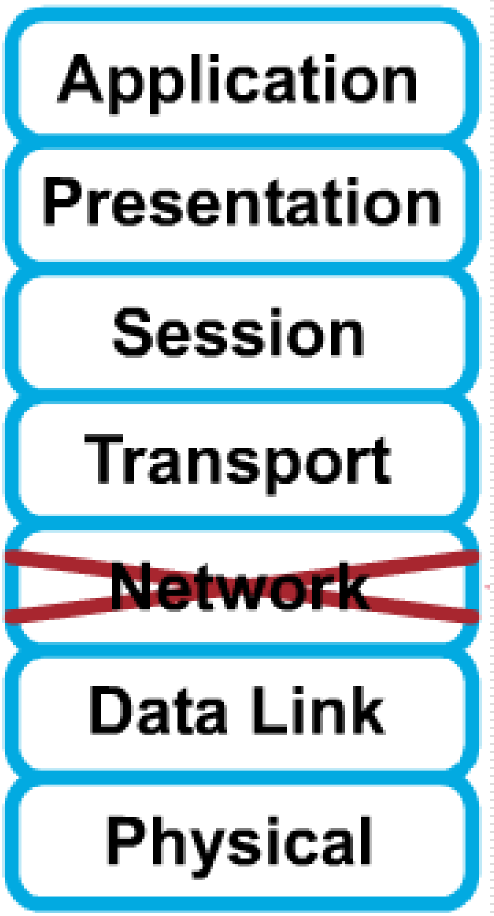


Routed protocol



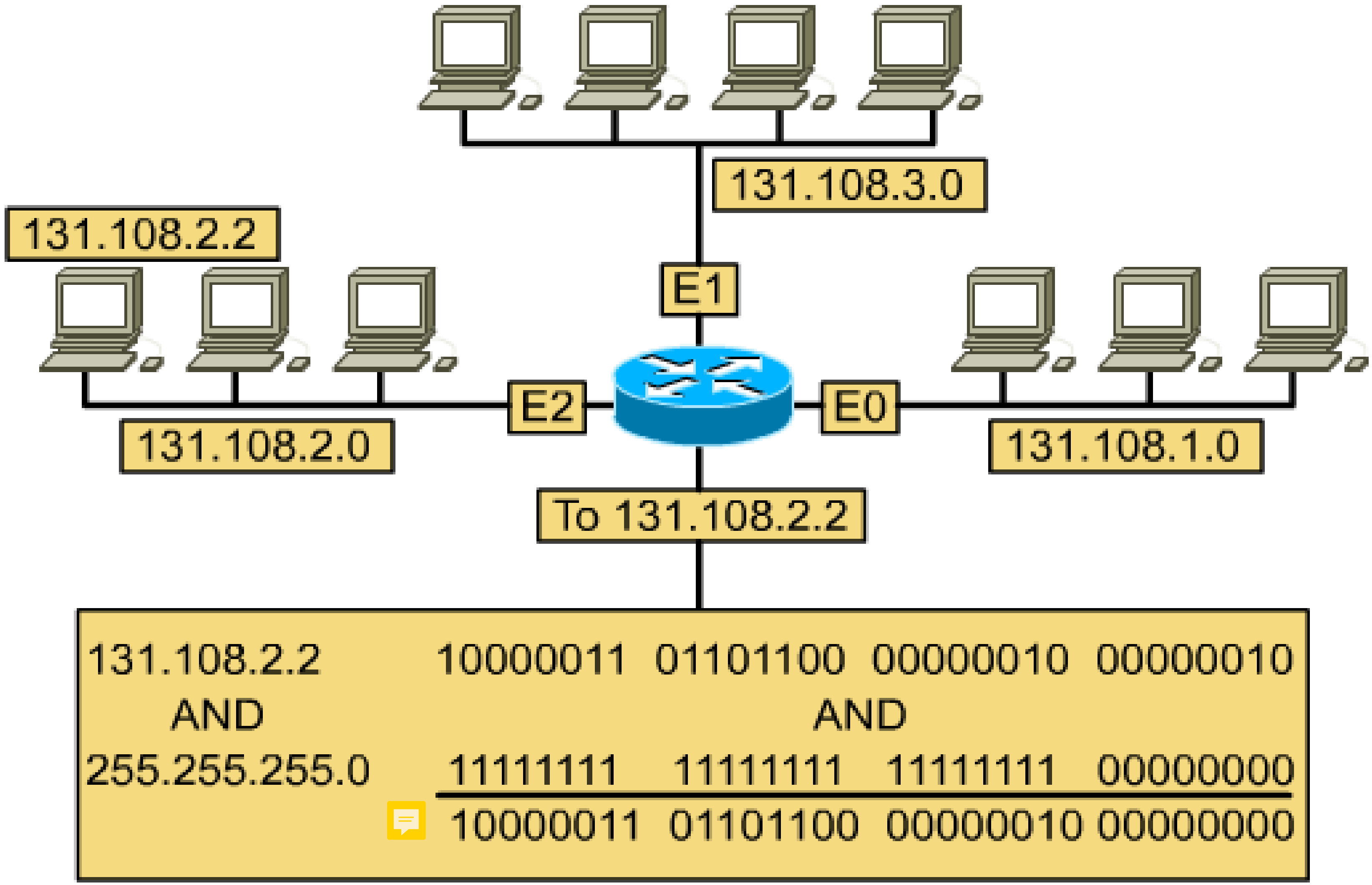
- Protocols that provide support for the network layer are called routed or routable protocols.
- IP is a network layer protocol, and because of that, it can be routed over an internetwork.

Non-routable protocol

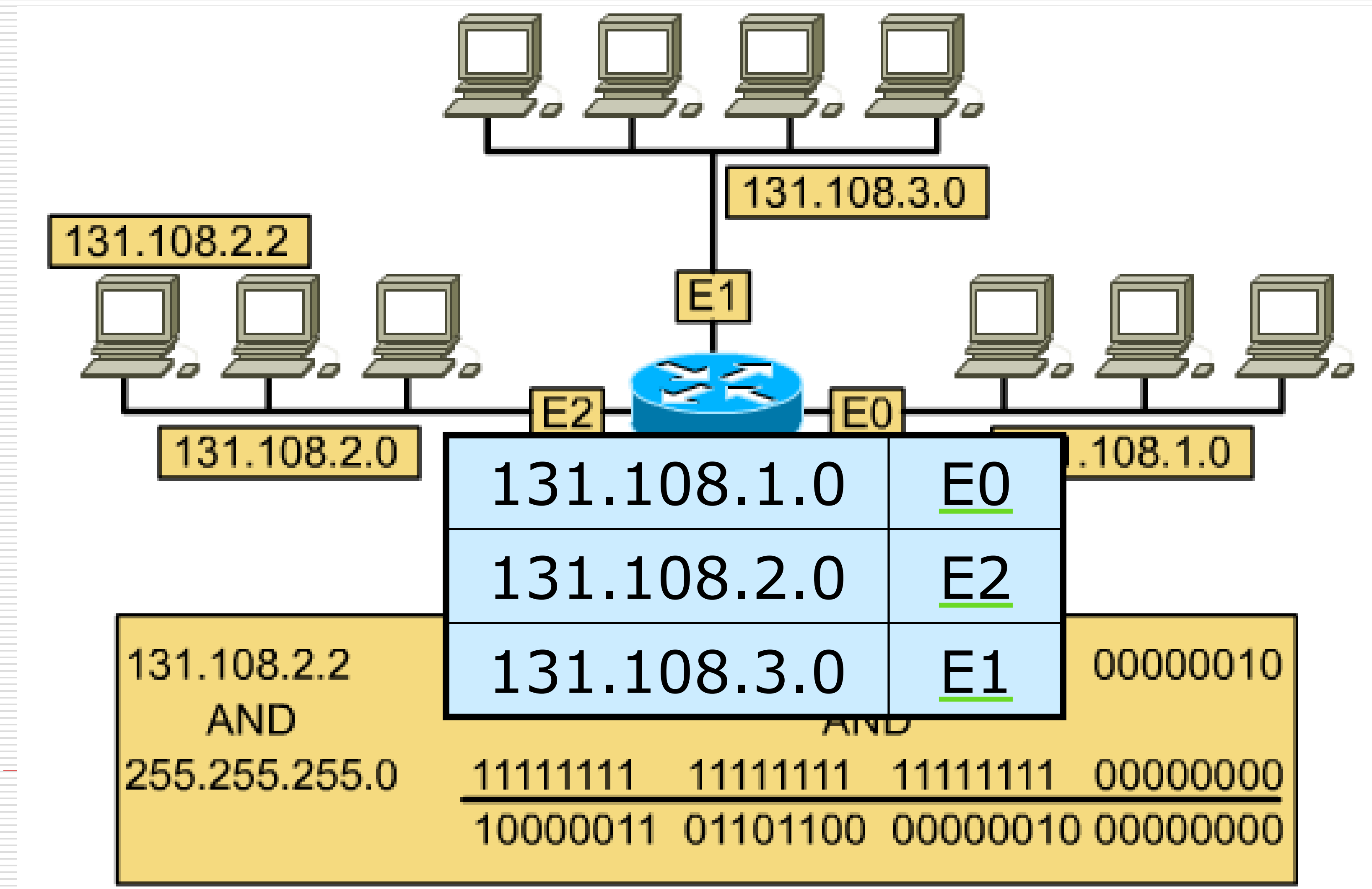


- Non-routable protocols are protocols that do not support Layer 3.
- The most common of these non-routable protocols is NetBEUI.
- NetBEUI is a small, fast, and efficient protocol that is limited to running on one segment.

Addressing of a routable protocol



Routing table



131.108.1.0	E0
131.108.2.0	E2
131.108.3.0	E1

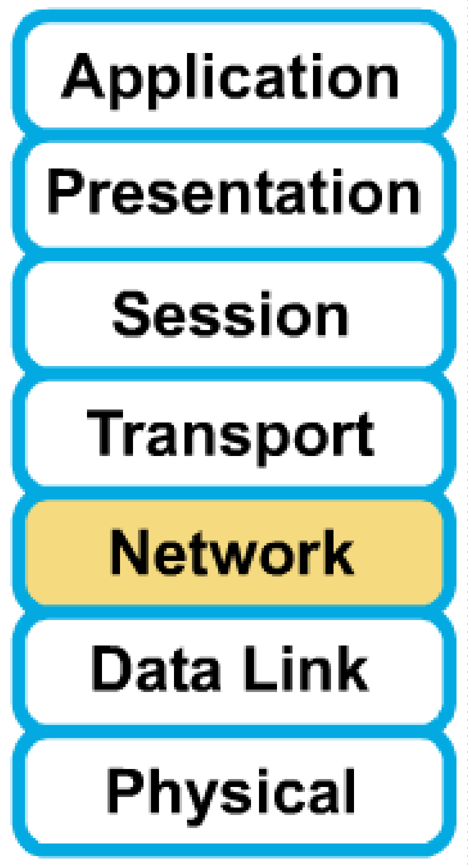
Classification #1: Static and Dynamic

- Static routes:
  - The network administrator manually enter the routing information in the router.
- Dynamic routes:
  - Routers can learn the information from each other on the fly.
  - Using routing protocol to update routing information.
  - RIP, IGRP, EIGRP, OSPF …

Static vs. dynamic routes

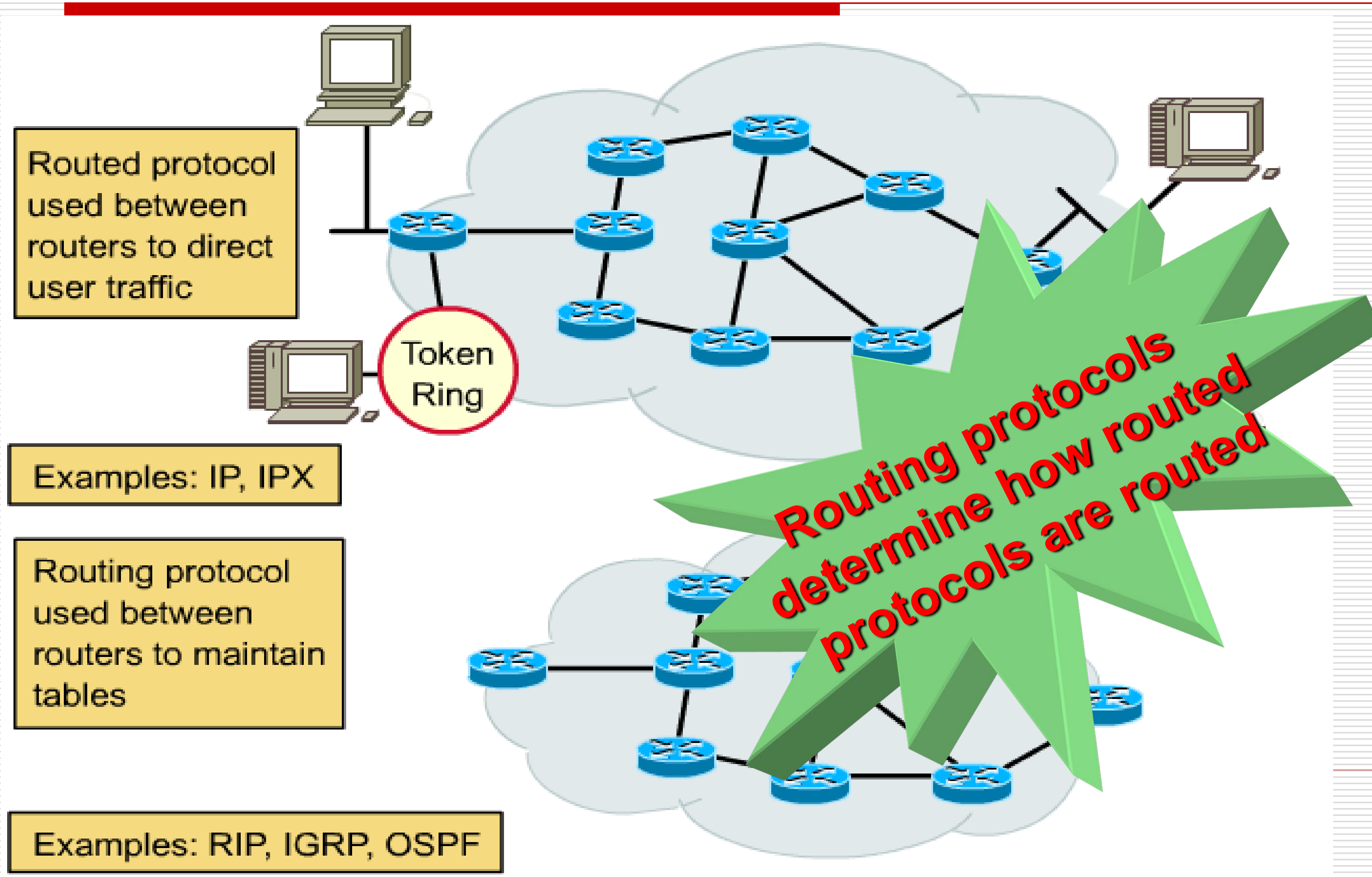
- Static routes:
  - For hiding parts of an internetwork.
  - To test a particular link in a network.
  - For maintaining routing tables whenever there is only one path to a destination network.
- Dynamic routes:
  - Maintenance of routing table.
  - Timely distribution of information in the form of routing updates.
  - Relies on routing protocol to share knowledge.
  - Routers can adjust to changing network conditions.

Routing protocol



- Routing protocols determine the paths that routed protocols follow to their destinations.

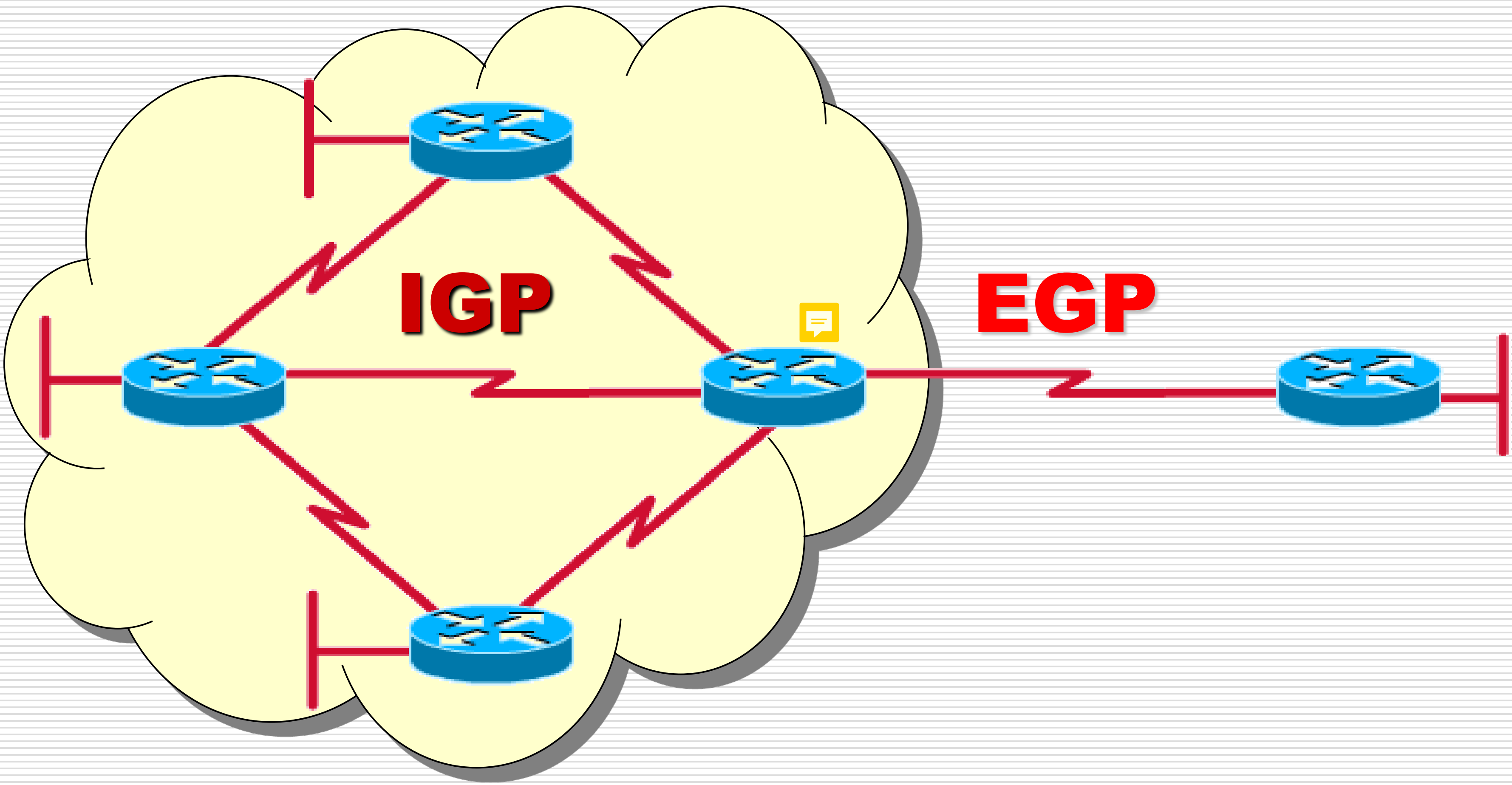
Routed vs. Routing protocol



Classification #2: IGP and EGP

- Dynamic routes.
- Interior Gateway Protocols (RIP, IGRP, EIGRP, OSPF):
  - Be used within an autonomous system, a network of routers under one administration, like a corporate network, a school district's network, or a government agency's network.
- Exterior Gateway Protocols (EGP, BGP):
  - Be used to route packets between autonomous systems.

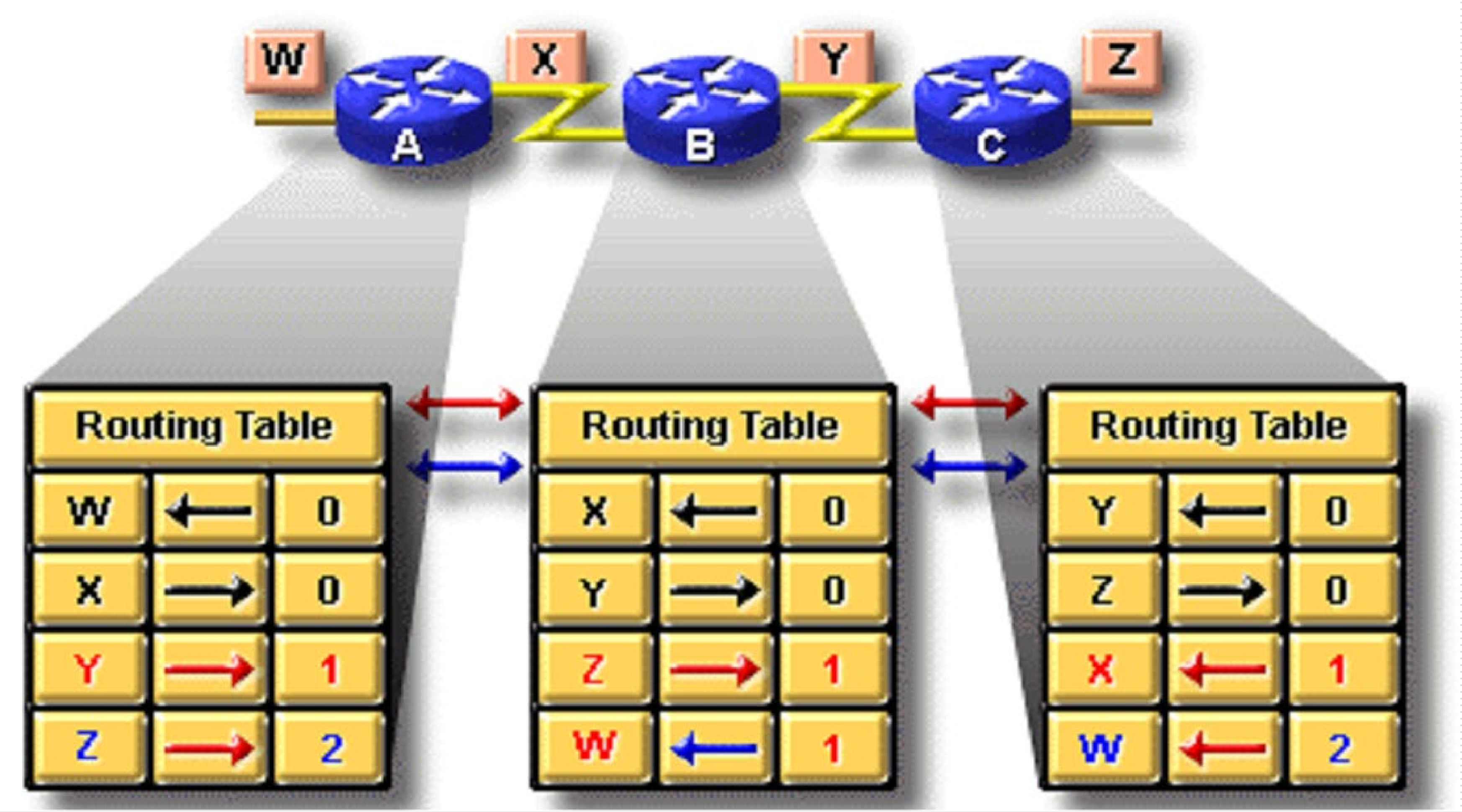
IGP vs. EGP



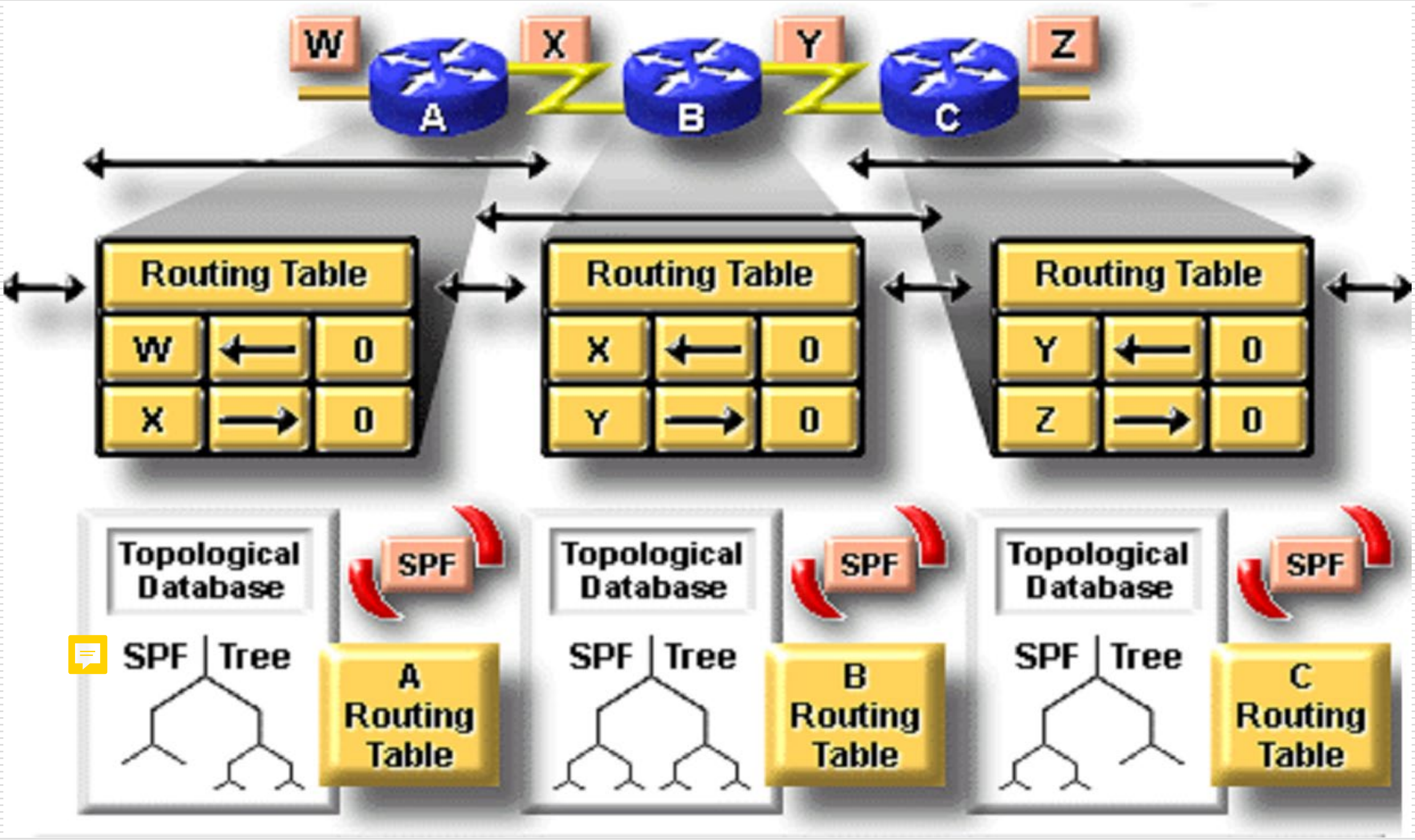
Classification #3: DVP and LSP

- Distance-Vector Protocols (RIP, IGRP):
  - View network topology from neighbor's perspective.
  - Add distance vectors from router to router.
  - Frequent, periodic updates.
  - Pass copy of routing tables to neighbor routers.
- Link State Protocols (OSPF):
  - Gets common view of entire network topology.
  - Calculates the shortest path to other routers.
  - Event-triggered updates.
  - Passes link state routing updates to other routers.

Distance vector routing



Link state routing



RIP(Route Information Protocol)

- Most popular.
- Interior Gateway Protocol.
- Distance Vector Protocol.
- Only metric is number of hops.
- Maximum number of hops is 15.
- Updates every 30 seconds.
- Doesn’t always select fastest path.
- Generates lots of network traffic.
- RIP v2 is an improved version of RIP v1

IGRP (Interior Gateway Route Protocol) and EIGRP (Enhanced IGRP)

- Cisco proprietary.
- Interior Gateway Protocol.
- Distance Vector Protocol.
- Metric is compose of bandwidth, load, delay and reliability.
- Maximum number of hops is 255.
- Updates every 90 seconds.
- EIGRP is an advanced version of IGRP, that is hybrid routing protocol.

OSPF(Open Shortest Path First)

- Open Shortest Path First.
- Interior Gateway Protocol.
- Link State Protocol.
- Metric is compose of cost, speed, traffic, reliability, and security.
- Event-triggered updates.

Layer3: Network Layer

- Overview of the Network Layer
- IP addresses and Subnets
- Layer 3 Devices
- ARP Protocol
- Network Layer Services
- Routed and Routing Protocols
- VLSM
- ICMP

Classful routing & VLSM

- Classful routing
  - Classful routing protocols require that a single network use the same subnet mask.
  - Example: network 192.168.187.0 must use just one subnet mask such as 255.255.255.0.
- VLSM — Variable-Length Subnet Masks
  - VLSM is simply a feature that allows a single autonomous system to have networks with different subnet masks.

VLSM

- With VLSM, a network administrator can use a long mask on networks with few hosts, and a short mask on subnets with many hosts.
- If a routing protocol allows VLSM:
  - use a 30-bit subnet mask on network connections, 255.255.255.252
  - a 24-bit mask for user networks, 255.255.255.0
  - Or, even a 22-bit mask, 255.255.252.0, for networks with up to 1000 users.

Why use the VLSM

- VLSM allows an organization to use more than one subnet mask within the same network address space.
- Implementing VLSM is often referred to as "subnetting a subnet", and can be used to maximize addressing efficiency.
- VLSM is one of the modifications that has helped to bridge the gap between IPv4 and IPv6.

VLSM

- Advantages:
  - Efficient use of IP addresses
  - Better route aggregation
- Support VLSM Routing Protocol:
  - Open Shortest Path First (OSPF)
  - Integrated Intermediate System to Intermediate System (Integrated IS-IS)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
  - RIP v2
  - Static routing.

A Waste of Space

- In the past, it has been recommended that the first and last subnet not be used. But we can used the Subnet 0 from Cisco IOS ver12.0.
- From IOS ver12.0, the Cisco router use subnet zero by default.
- command:
  router(config)#no ip subnet-zero

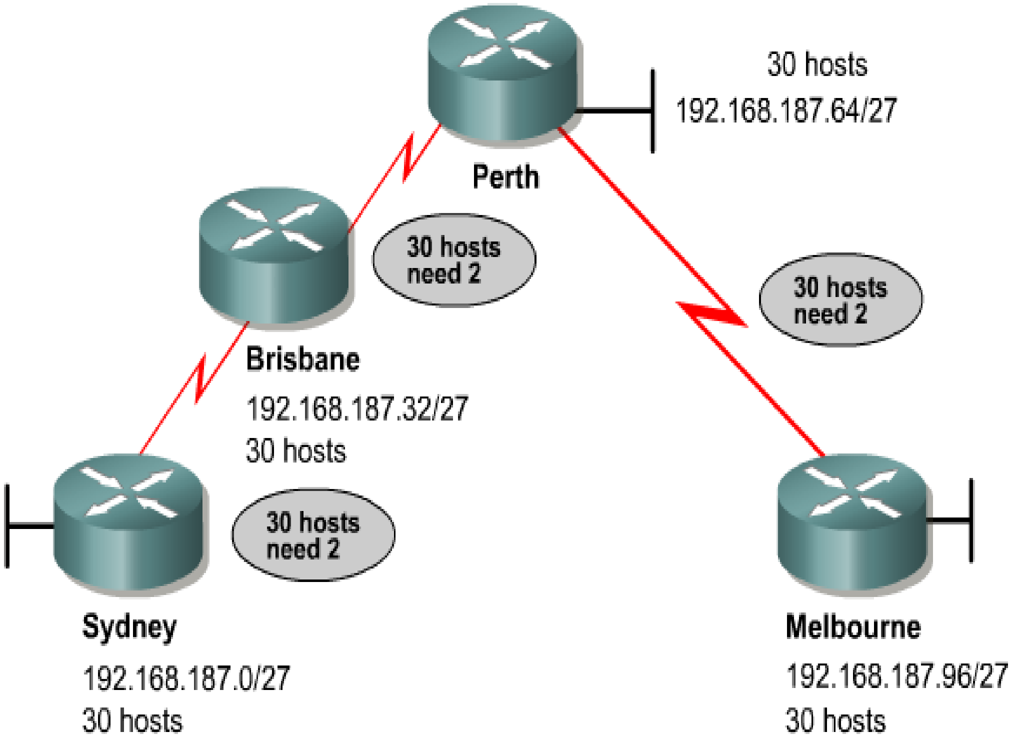
A Waste of Space

- 192.168.187. 000 *****

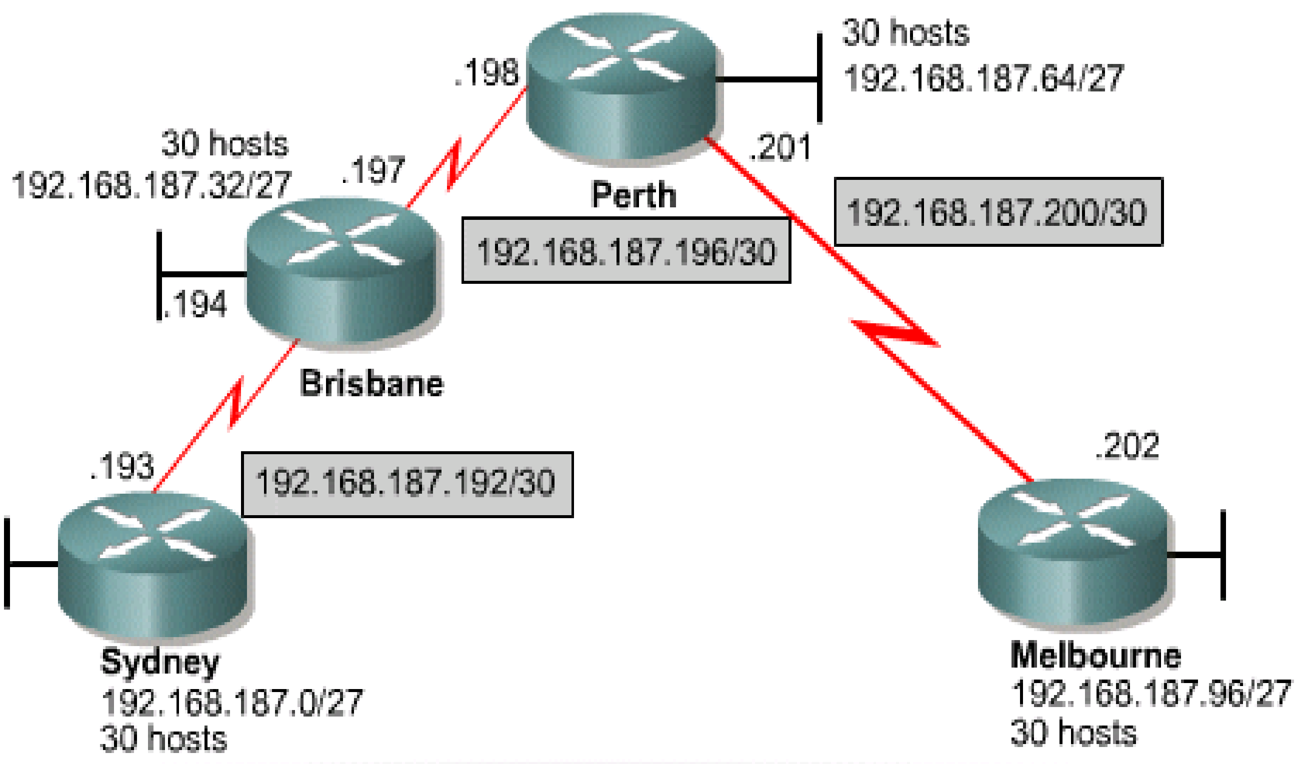
subnet-id Host-id

- 255.255.255.224 (1110 0000)

Subnet Number	Subnet Address	
Subnet 0	192.168.187.0	/27
Subnet 1	192.168.187.32	/27
Subnet 2	192.168.187.64	/27
Subnet 3	192.168.187.96	/27
Subnet 4	192.168.187.128	/27
Subnet 5	192.168.187.160	/27
Subnet 6	192.168.187.192	/27
Subnet 7	192.168.187.224	/27

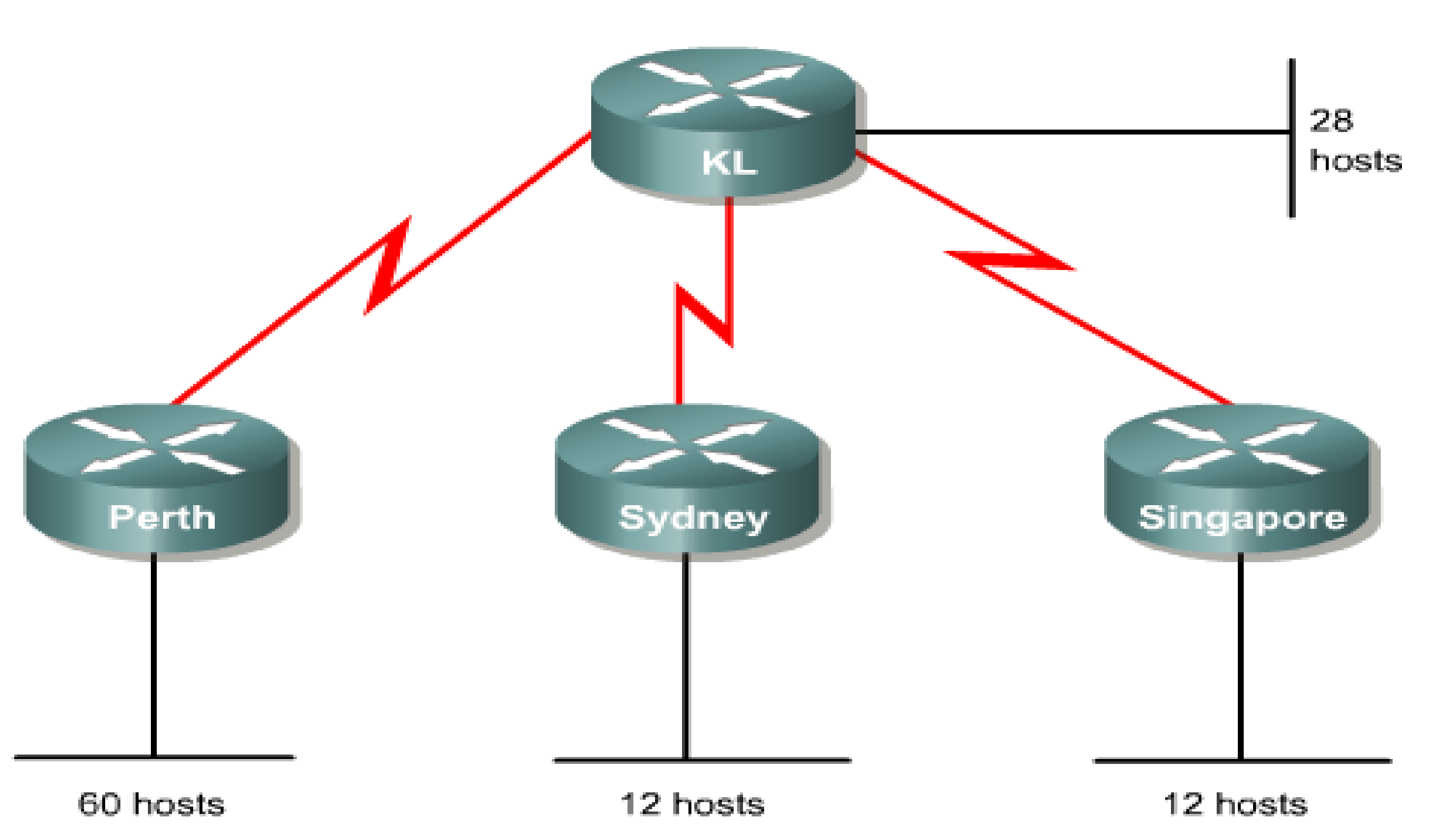


How to use the VLSM



Notice the /27 bit masks for the LANs, and the /30 for the serial links

VLSM: An Example



VLSM: An Example

- A class C address of 192.168.10.0/24 has been allocated.
  - Perth, Sydney, and Singapore have a WAN connection to Kuala Lumpur (KL).
  - Perth requires 60 hosts.
  - KL requires 28 hosts.
  - Sydney and Singapore each require 12 hosts.
- To calculate VLSM subnets and the respective hosts allocate the largest requirements first from the address range. Requirements levels should be listed from the largest to the smallest.

VLSM: An Example

- **Step 1**
  - In this example Perth requires 60 hosts.
  - Use 6 bits since $2^6 - 2 = 62$ usable host addresses. Thus 2 bits will be used from the 4th Octet to represent the extended-network-prefix of /26 and the remaining 6 bits will be used for host addresses.
- Applying VLSM on address 192.168.10.0/24 gives:
  - 192.168.10.<u>00</u> hh hhhh /26
  - 255.255.255.192 (1100 0000)

192.168.10.0/24 （Subnetted）	192.168.10.0/26 (0000 0000)	Perth (60 hosts) □192.168.10.0/26 (Network Address) □192.168.10.1/26 □192.168.10.2/26 □…… □192.168.10.61/26 □192.168.10.62/26 □192.168.10.63/26(Broadcast Address)
	192.168.10.64/26 (0100 0000)	Unused （Subnetted） See next slide
	192.168.10.128/26 (1000 0000)	Unused
	192.168.10.192/26 (1100 0000)	Unused

VLSM: An Example

- **Step 2**
  - KL requires 28 hosts. The next available address after 192.168.10.63/26 is 192.168.10.64/26.
  - Since 28 hosts are required, 5 bits will be needed for the host addresses, $2^5 - 2 = 30$ usable host addresses.
  - Thus 5 bits will be required to represent the hosts and 3 bits will be used to represent the extended-network prefix of /27.
- Applying VLSM on address 192.168.10.64/26 gives:
  - 192.168.10.<u>010</u> hhhhh /27
  - 255.255.255.224 (1110 0000)

From 192.168.10.64/26	192.168.10.64/27 (0100 0000)	KL (28 hosts) ● 192.168.10.64/27 (Network Address) ● 192.168.10.65/27 ● 192.168.10.66/27 ● …… ● 192.168.10.94/27 ● 192.168.10.95/27 ● 192.168.10.96/27 (Broadcast Address)
	192.168.10.96/27 (0110 0000)	Unused （Subnetted） See next slide
	192.168.10.128/27 (1000 0000)	Unused
	192.168.10.160/27 (1010 0000)	Unused
	192.168.10.192/27 (1100 0000)	Unused
	192.168.10.224/27 (1110 0000)	Unused

VLSM: An Example

- **Step 3**
  - Now Sydney and Singapore require 12 hosts each. The next available address starts from192.168.10.96/27.
  - Since 12 hosts are required, 4 bits will be needed for the host addresses, $2^4 = 16$, $16 – 2 = 14$ usable addresses.
  - Thus 4 bits are required to represent the hosts and 4 bits for the extended-network-prefix of /28.
- Applying VLSM on address 192.168.10.96/27 gives:
  - 192.168.10.<u>0110</u> hhhh /28
  - 255.255.255.240 (1111 0000)

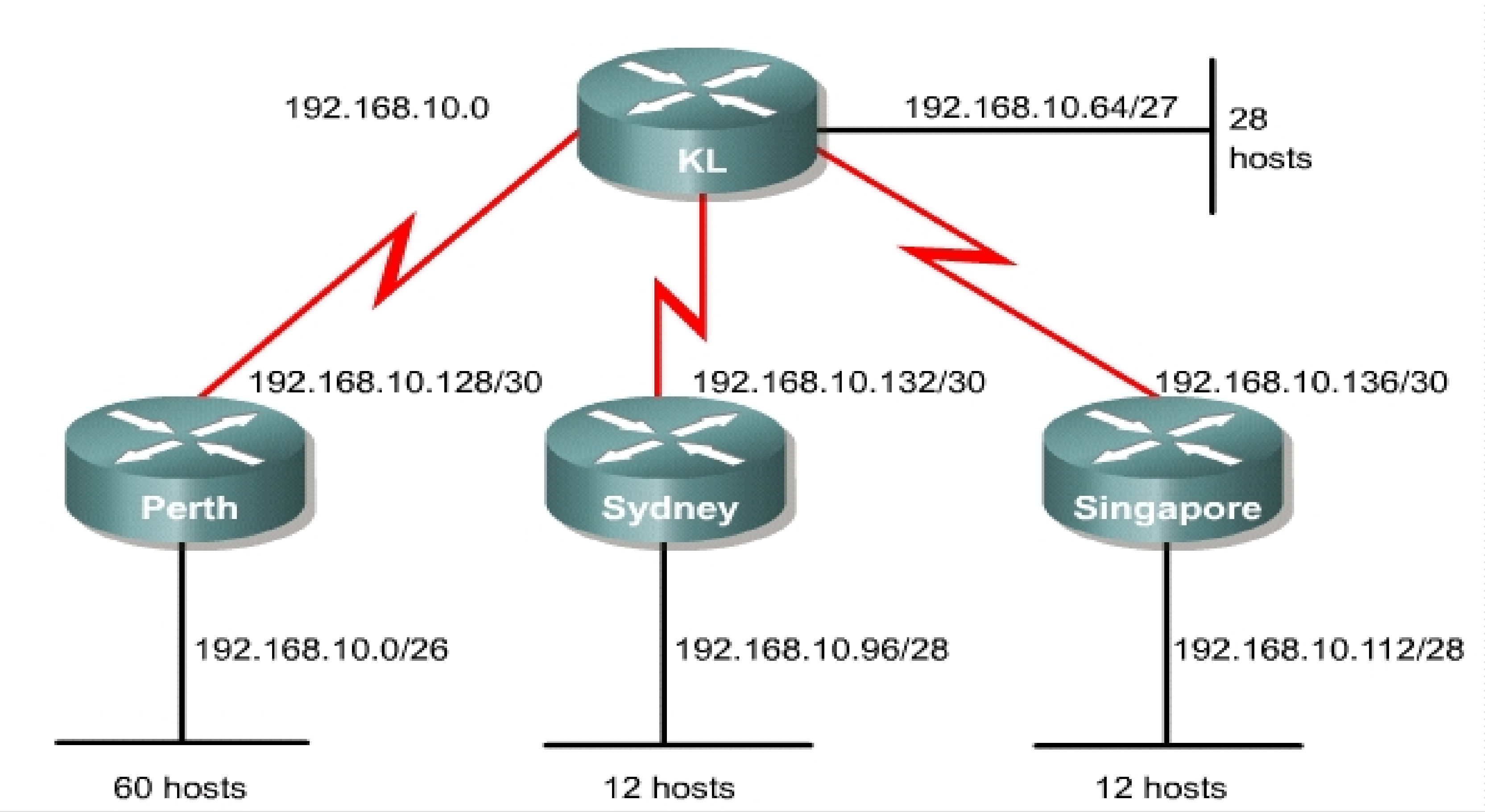
From 192.168.10.96/27	192.168.10.96/28	Sydney(12 hosts) □ 192.168.10.96/28 (Network Address) □ 192.168.10.97/28 □ 192.168.10.98/28 □ …… □ 192.168.10.109/28 □ 192.168.10.110/28 □ 192.168.10.111/28 (Broadcast Address)
	192.168.10.112/28	Singapore (12 hosts) □192.168.10.112/28 (Network Address) □192.168.10.113/28 □192.168.10.114/28 □…… □192.168.10.126/28 □192.168.10.127/28 □192.168.10.128/28(Broadcast Address)
	192.168.10.128/28	Unused （Subnetted） See next slide
	192.168.10.144/28	Unused
	… …	Unused
	192.168.10.240/28	Unused

VLSM: An Example

- **Step 4**
  - Now allocate addresses for the WAN links. Remember that each WAN link will require two IP addresses. The next available subnet is 192.168.10.128/28.
  - Since 2 network addresses are required for each WAN link, 2 bits will be needed for host addresses, $2^2 - 2 = 2$ usable addresses.
  - Thus 2 bits are required to represent the links and 6 bits for the extended-network-prefix of /30.
- Applying VLSM on 192.168.10.128/28 gives:
  - 192.168.10.011000 hh /30
  - 255.255.255.252 (1111 1100)

From 192.168.10.128 /28	192.168.10.128/30	Perth – KL □192.168.10.128/30 (Network Address) □192.168.10.129/30 □192.168.10.130/30 □192.168.10.131/30 (Broadcast Address)
	192.168.10.132/30	Sydney – KL □192.168.10.132/30(Network Address) □192.168.10.133/30 □192.168.10.134/30 □192.168.10.135/30(Broadcast Address)
	192.168.10.136/30	Singapore – KL □192.168.10.136/30 (Network Address) □192.168.10.137/30 □192.168.10.138/30 □192.168.10.139/30 (Broadcast Address)
	192.168.10.140/30	Unused
	192.168.10.144/30	Unused
	… …	Unused

VLSM: An Example

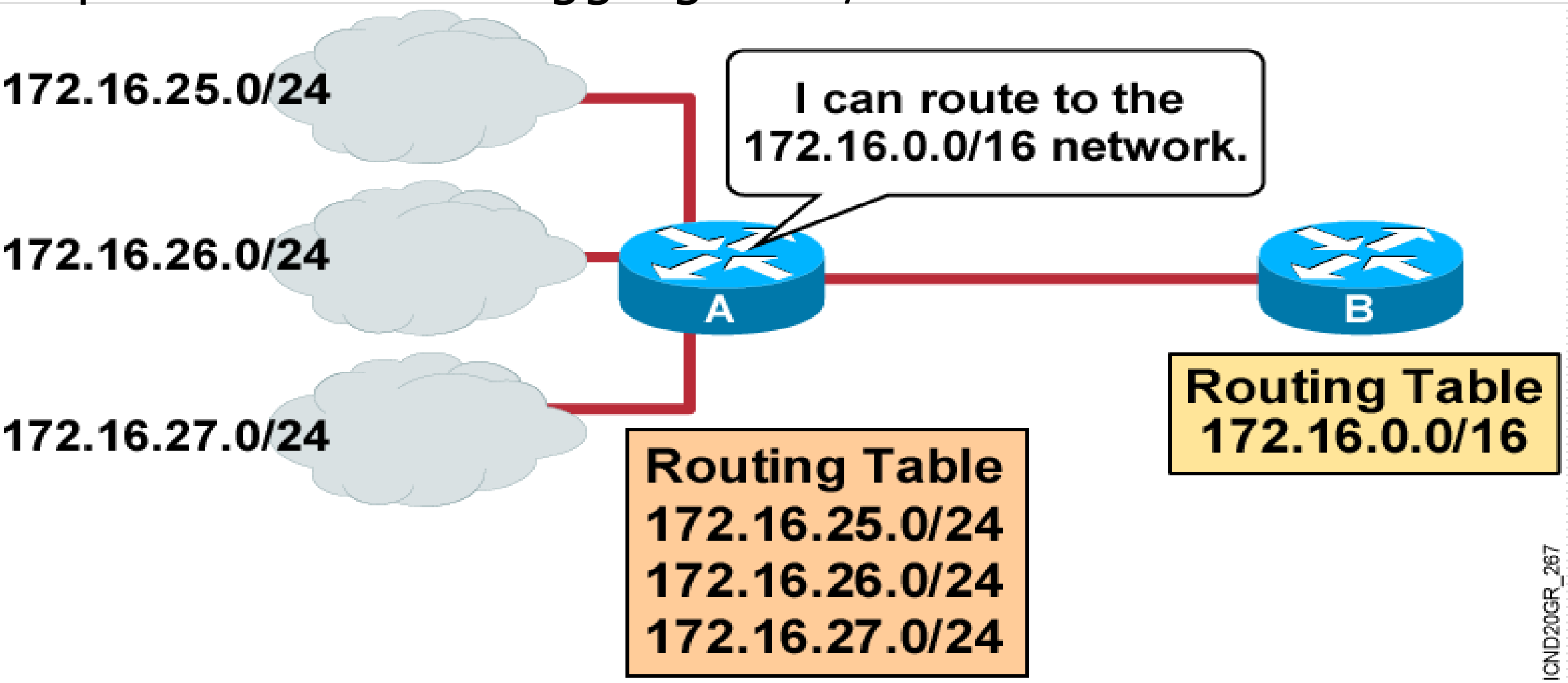


VLSM: An Example

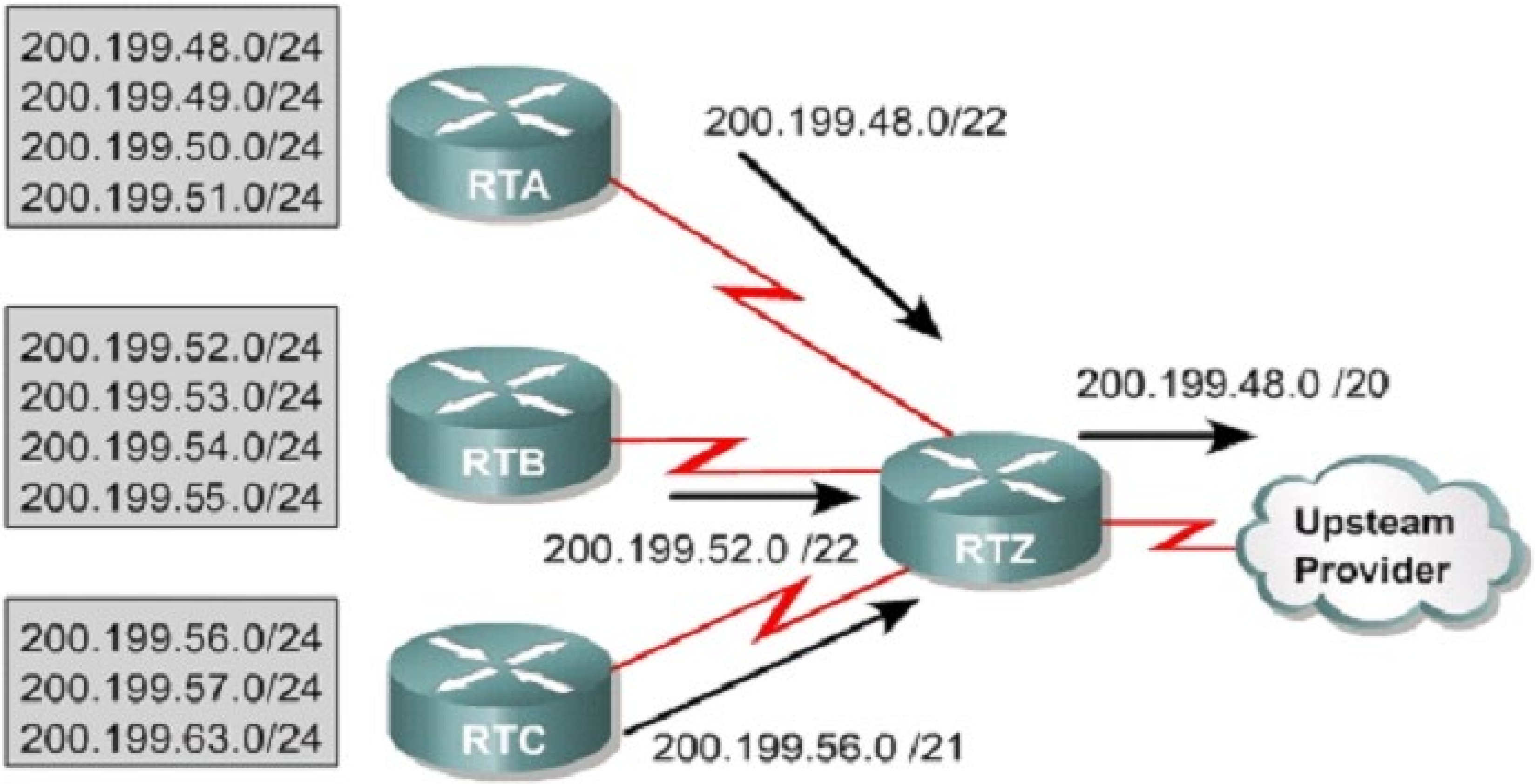
- It is important to remember that only unused subnets can be further subnetted.
- If any address from a subnet is used, that subnet cannot be further subnetted.

Route Aggregation

- The use of Classless InterDomain Routing (CIDR) and VLSM not only prevents address waste, but also promotes route aggregation, or summarization.



Route Summarization Sample



Route summarization reduces routing table size by aggregating routes to multiple networks into one supernet.

Working it out

200.199.48.0 /24	200.199.001100 00.hhhhhhhh
200.199.49.0 /24	200.199.001100 01.hhhhhhhh
200.199.50.0 /24	200.199.001100 10.hhhhhhhh
200.199.51.0 /24	200.199.001100 11.hhhhhhhh
	255.255.111111 00.00000000

Summarized Address 200.199.48.0 / 22

Route Aggregation

- Advantages:
  - Reduction of the number of Routing Table entries.
  - May be used to isolate Topological changes
- For aggregation to work properly, carefully assign addresses in a hierarchical fashion so that summarized addresses will share the same high-order bits.
- VLSM allows for the aggregation of routes and increases flexibly by basing the aggregation entirely on the higher-order bits shared on the left, even if the networks are not contiguous.

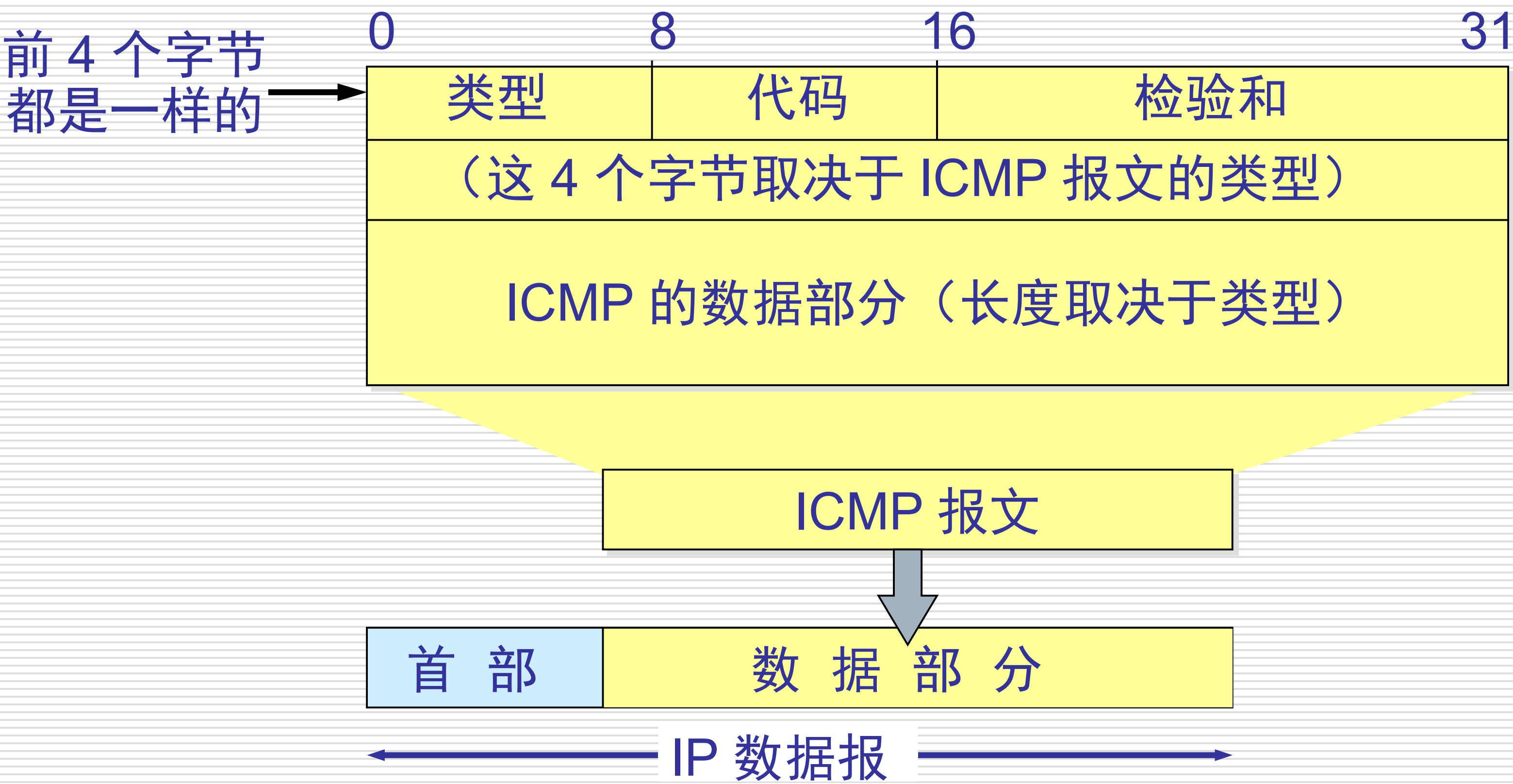
Layer3: Network Layer

- Overview of the Network Layer
- IP Addresses and Subnets
- Layer 3 Devices
- ARP Protocol
- Network Layer Services
- Routed and Routing Protocols
- VLSM
- ICMP

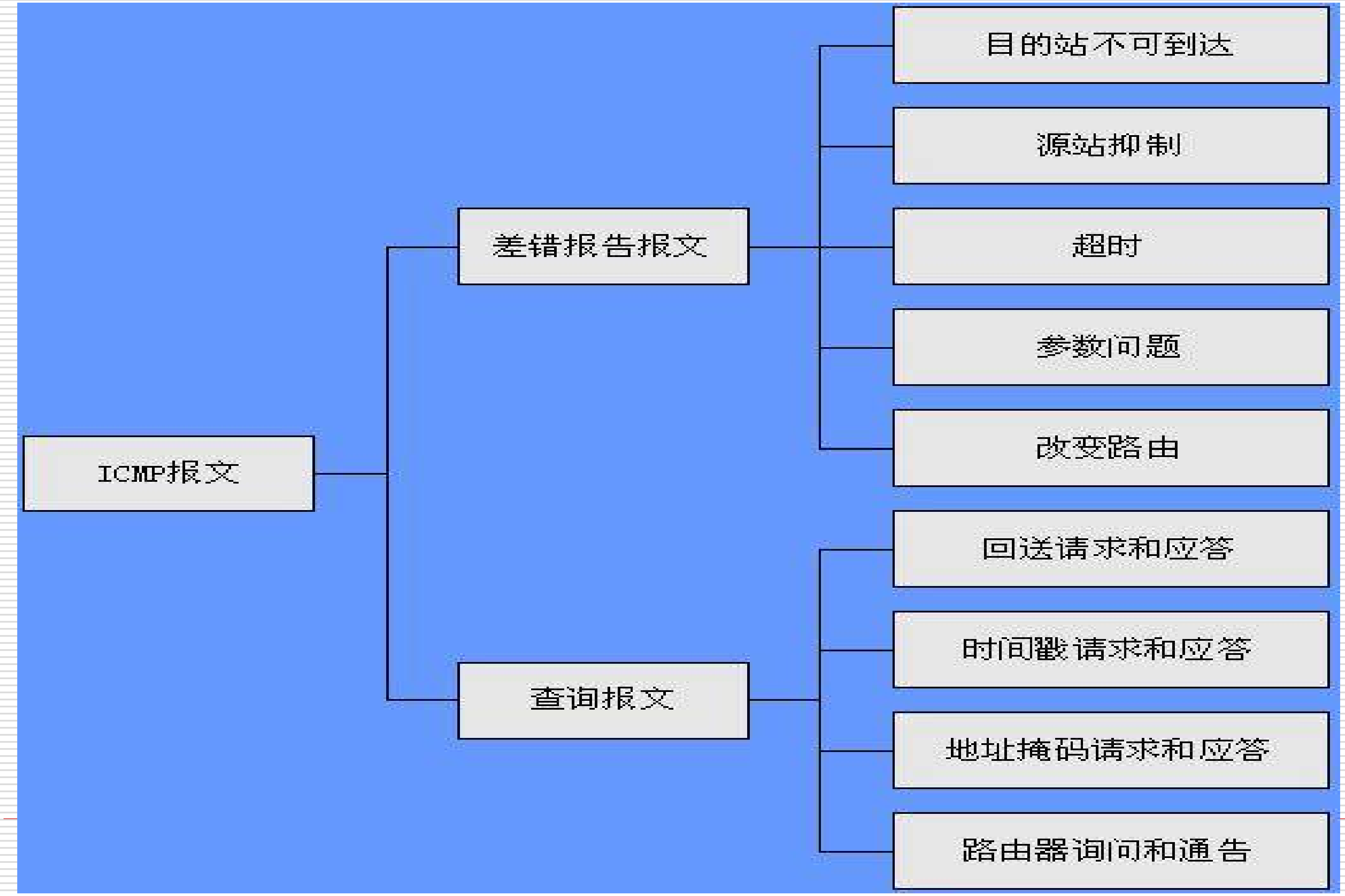
因特网控制报文协议 ICMP

- ICMP (Internet Control Message Protocol)：为了提高 IP 数据报交付成功的机会
- ICMP 允许主机或路由器报告差错情况和提供有关异常情况的报告
- ICMP 只是 IP 层的协议
- ICMP 报文作为 IP 层数据报的数据，加上数据报的首部，组成 IP 数据报发送出去

ICMP 报文的格式


前 4 个字节
都是一样的
0
8
16
31
类型
代码
检验和
（这 4 个字节取决于 ICMP 报文的类型）
ICMP 的数据部分（长度取决于类型）
ICMP 报文
首 部
数 据 部 分
IP 数据报

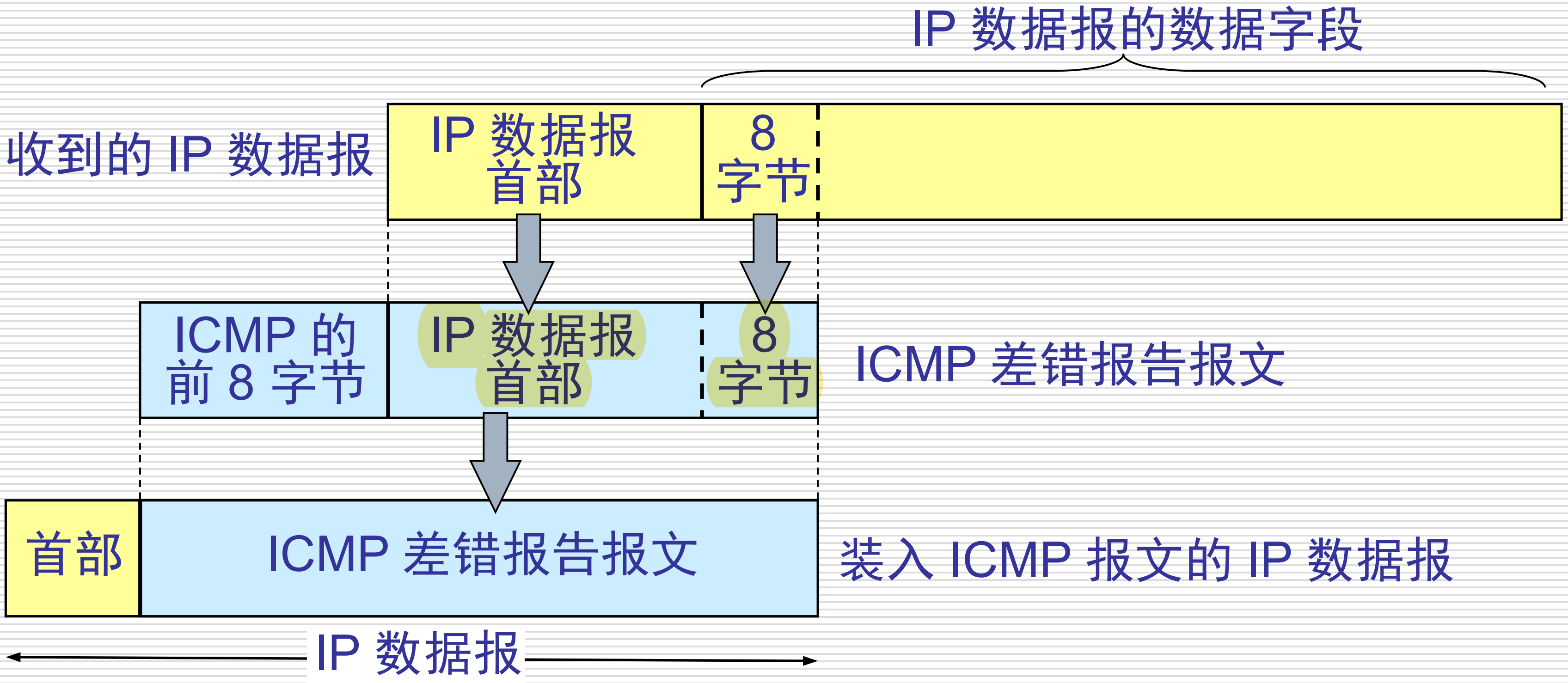
两种ICMP 报文


ICMP报文
差错报告报文
查询报文
目的站不可到达
源站抑制
超时
参数问题
改变路由
回送请求和应答
时间戳请求和应答
地址掩码请求和应答
路由器询问和通告

目的站不可到达

- 网络不可到达（**net unreachable**）
- 主机不可到达（**host unreachable**）
- 协议不可到达（**protocol unreachable**）
- 端口不可到达（**port unreachable**）
- 源路由选择不能完成（**source route failed**）
- 目的网络不可知（**unknown destination network**）
- 目的主机不可知（**unknown destination host**）

ICMP 差错报告报文的数据字段的内容



不应发送 ICMP 差错报告报文的几种情况

- 对 ICMP 差错报告报文不再发送 ICMP 差错报告报文
- 对第一个分片的数据报片的所有后续数据报片都不发送 ICMP 差错报告报文
- 对具有多播地址的数据报都不发送 ICMP 差错报告报文
- 对具有特殊地址（如127.0.0.0或0.0.0.0）的数据报不发送 ICMP 差错报告报文

PING (Packet InterNet Groper)

- PING 是用ICMP的"Echo request"和"Echo reply"消息来实现的
- PING 用来测试两个主机之间的连通性
- PING 使用了 ICMP 回送请求与回送回答报文
- PING 是应用层直接使用网络层 ICMP 的例子，它没有通过运输层的 TCP 或UDP

谢 谢！