Networking Basics

The **Cisco Certified Network Associate** Curriculum

ROUTING FUNDAMENTALS AND SUBNETS

CISCO SYSTEMS
NETWORKING ACADEMY

Version 3.0
Cisco Regional Networking Academy

CCNP CISCO CERTIFIED
CCDP CISCO CERTIFIED

Objectives

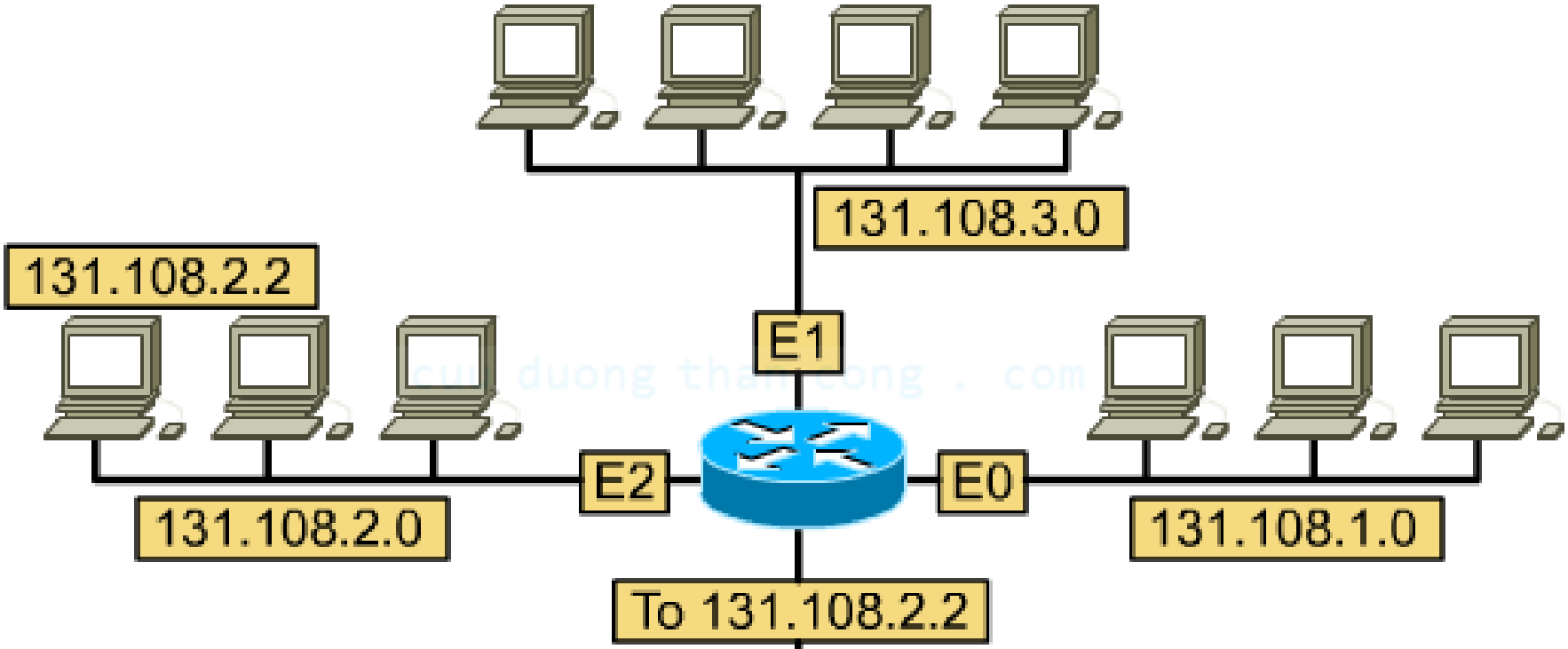
- *Describe routed (routable) protocols.*
- *List the steps of data encapsulation in an internetwork as data is routed to one or more Layer 3 devices.*
- *Describe connectionless and connection-oriented delivery.*
- *Name the IP packet fields.*
- *Describe process of routing.*
- *Compare and contrast different types of routing protocols.*
- *List and describe several metrics used by routing protocols.*
- *List several uses for subnetting.*
- *Determine the subnet mask for a given situation.*
- *Use a subnet mask to determine the subnet ID.*

Table of Content

cuu duong than cong . com

INTERNET PROTOCOL - ROUTED

Routable and routed protocols



131.108.2.2	10000011	01101100	00000010	00000010
AND			AND	
255.255.255.0	11111111	11111111	11111111	00000000
	10000011	01101100	00000010	00000000

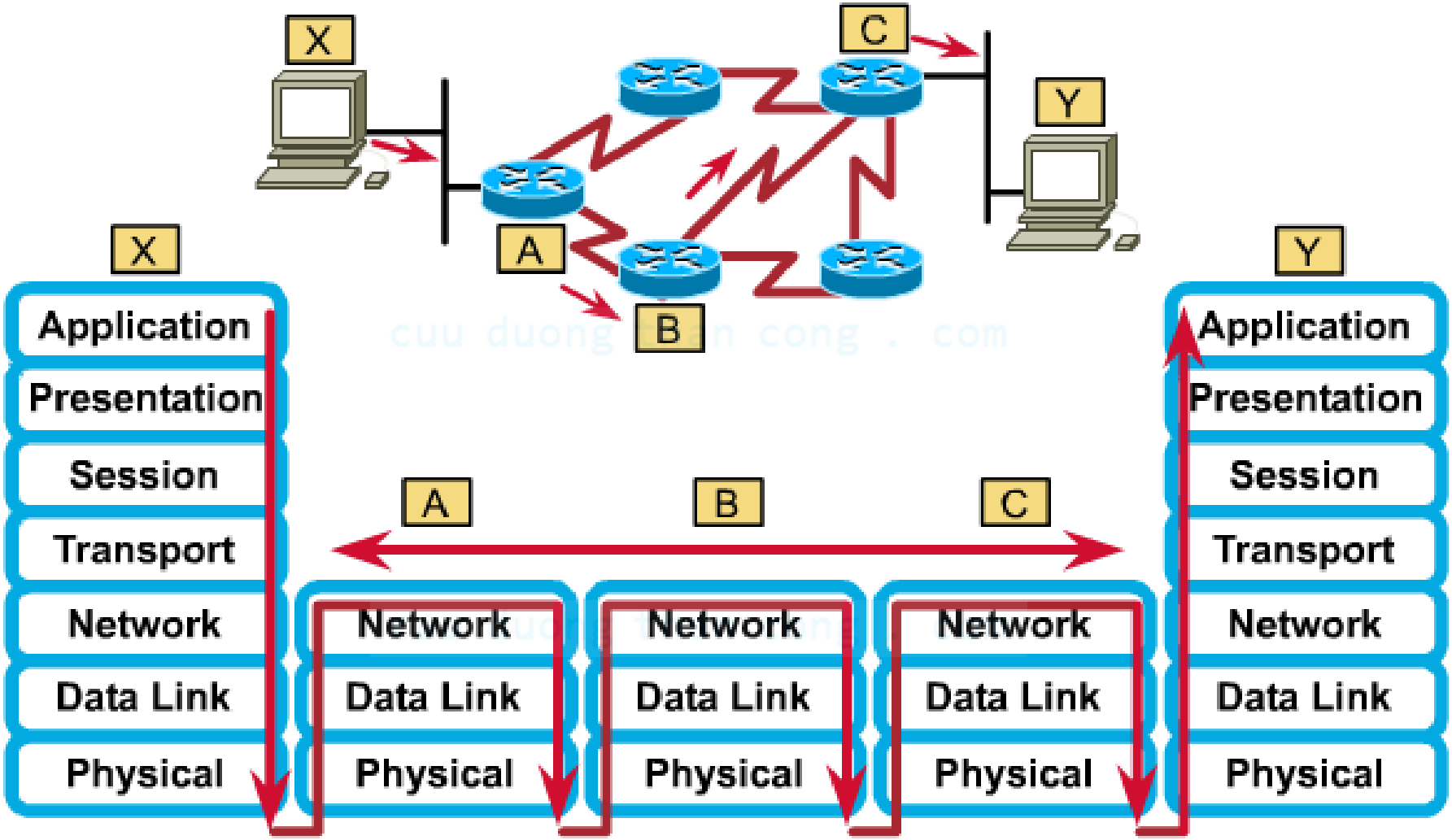
Routable and routed protocols

- A protocol is a set of rules that determines how computers communicate with each other across networks.
- A routed protocol allows the router to forward data between nodes on different networks.
- In order for a protocol to be routable, it must provide the ability to assign a network number and a host number to each individual device.

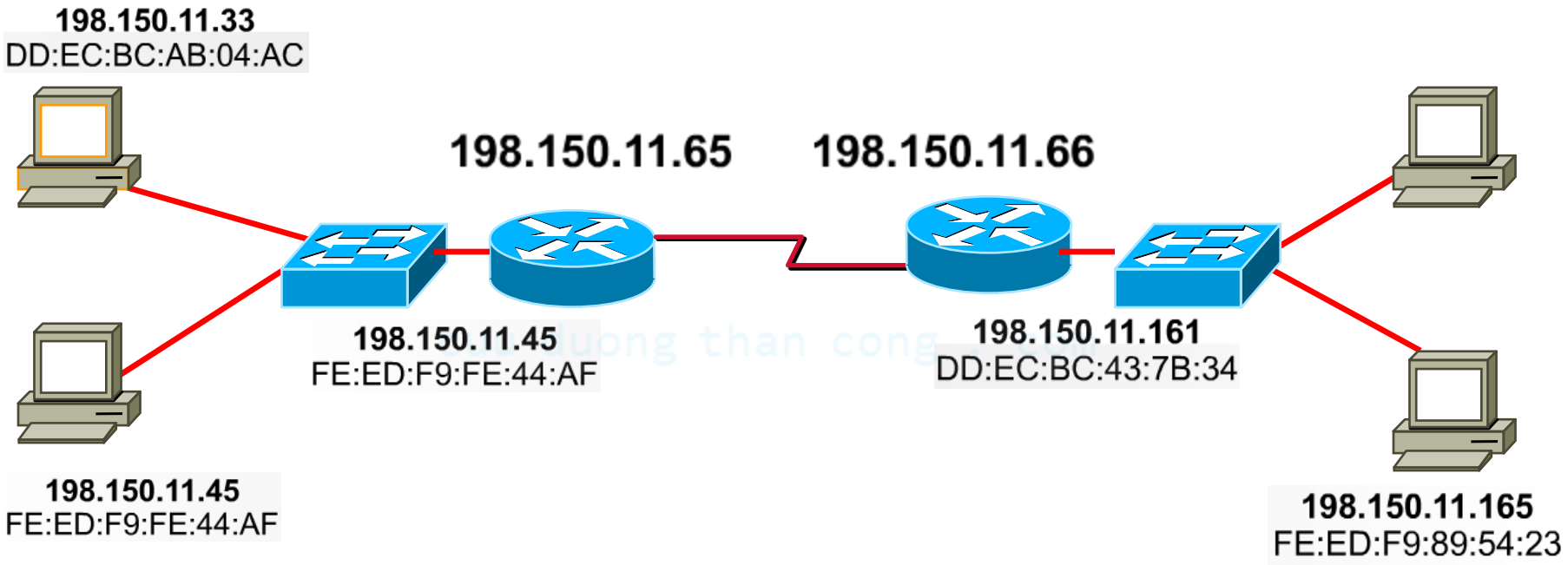
IP as a routed protocol

- The Internet Protocol (IP) is the most widely used implementation of a hierarchical network-addressing scheme.
- IP is a connectionless, unreliable, best-effort delivery protocol.
- At the network layer, the data is encapsulated within packets (also known as datagrams).
- Packet includes header - addressing and other control information + actual data - whatever is passed down from the higher layers.

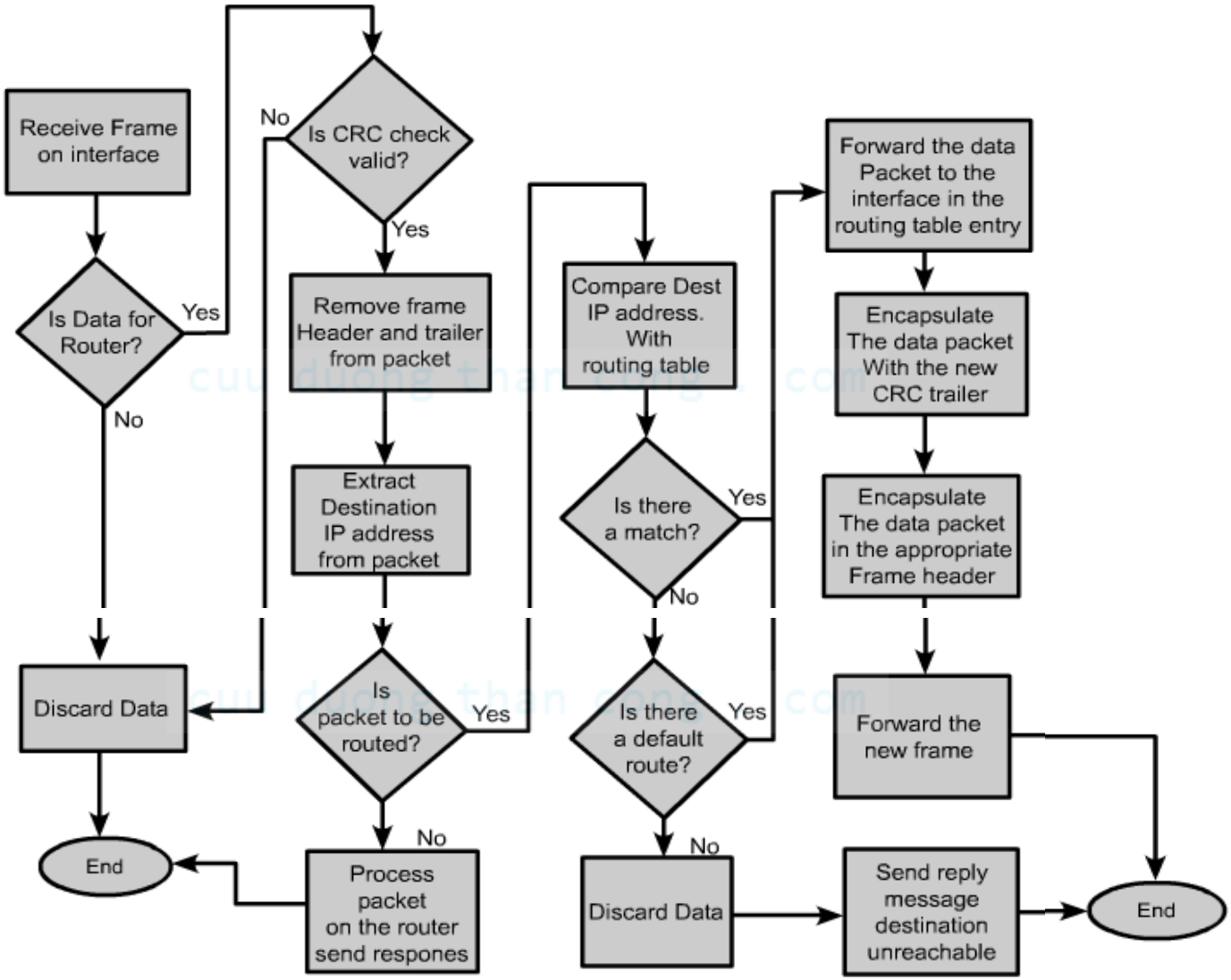
Packet propagation and switching within a router



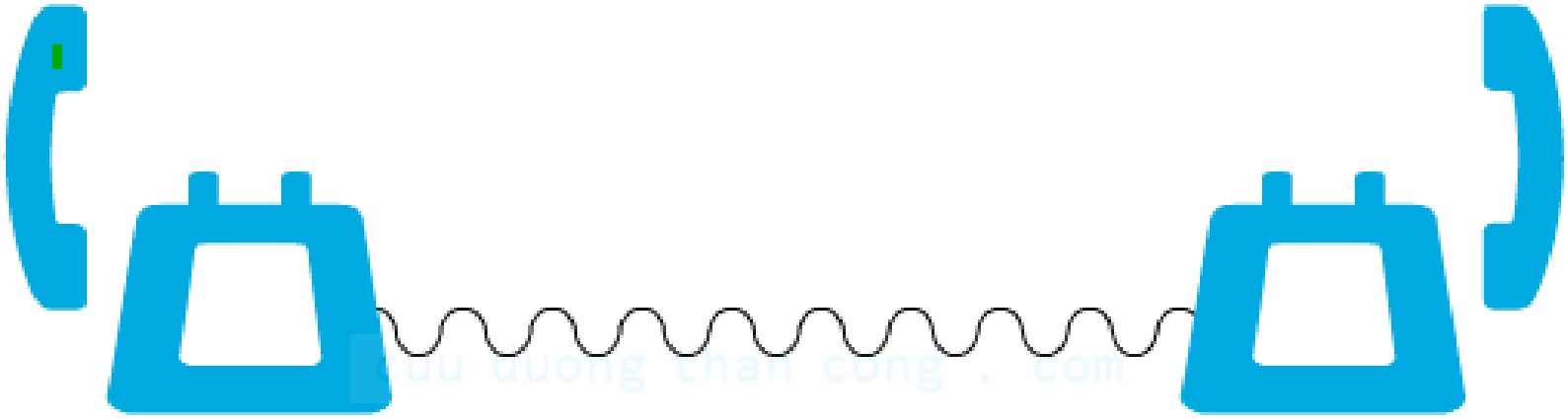
Router protocol stripping



Router protocol stripping (cont.)



Connection oriented network services

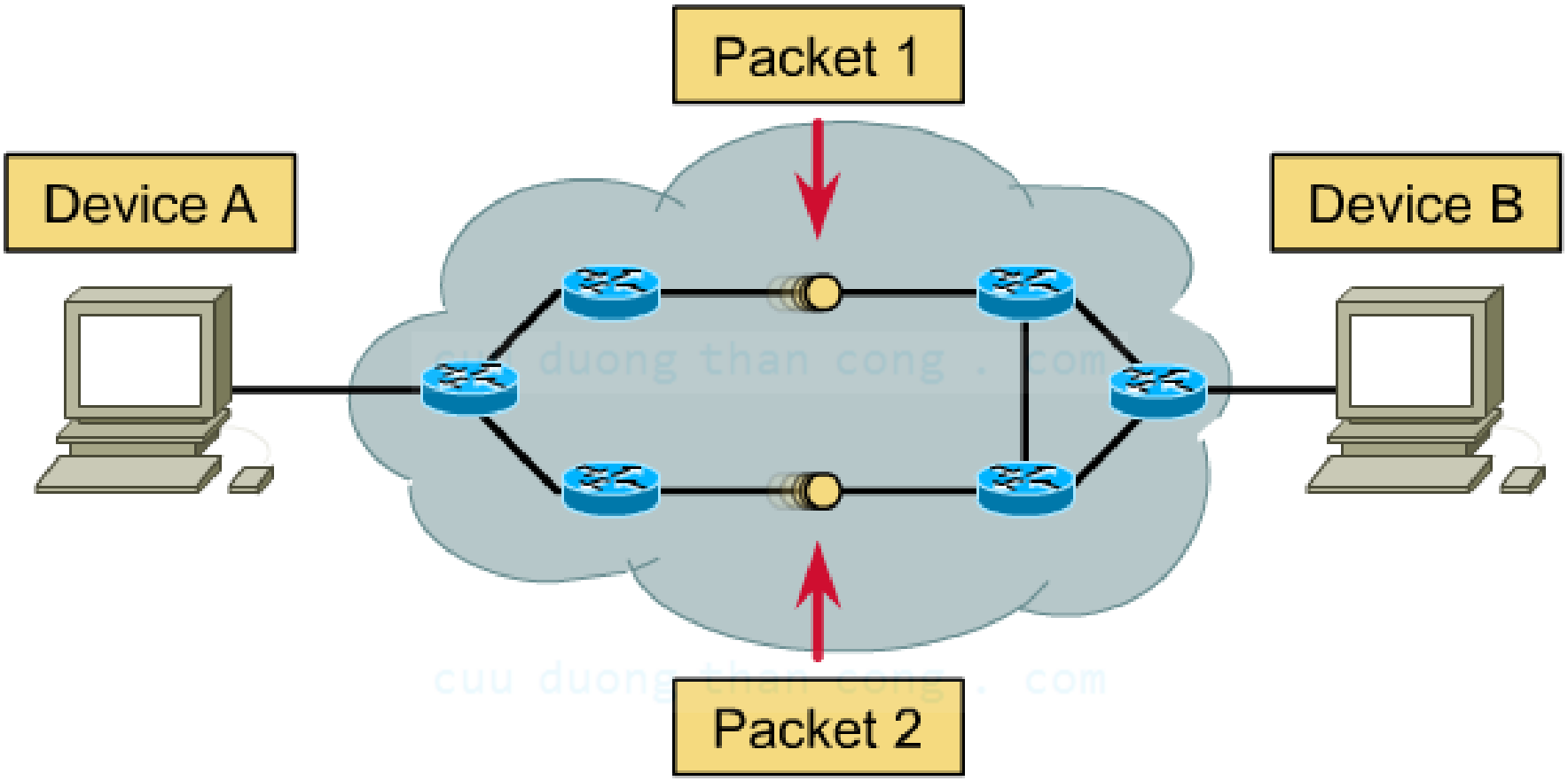


- A connection is established between the sender and the recipient before any data is transferred.

Circuit switched

- Connection-oriented network processes are often referred to as circuit switched.
- These processes establish a connection with the recipient, first, and then begin the data transfer.
- All packets travel sequentially across the same physical circuit, or more commonly, across the same virtual circuit.

Connectionless network services



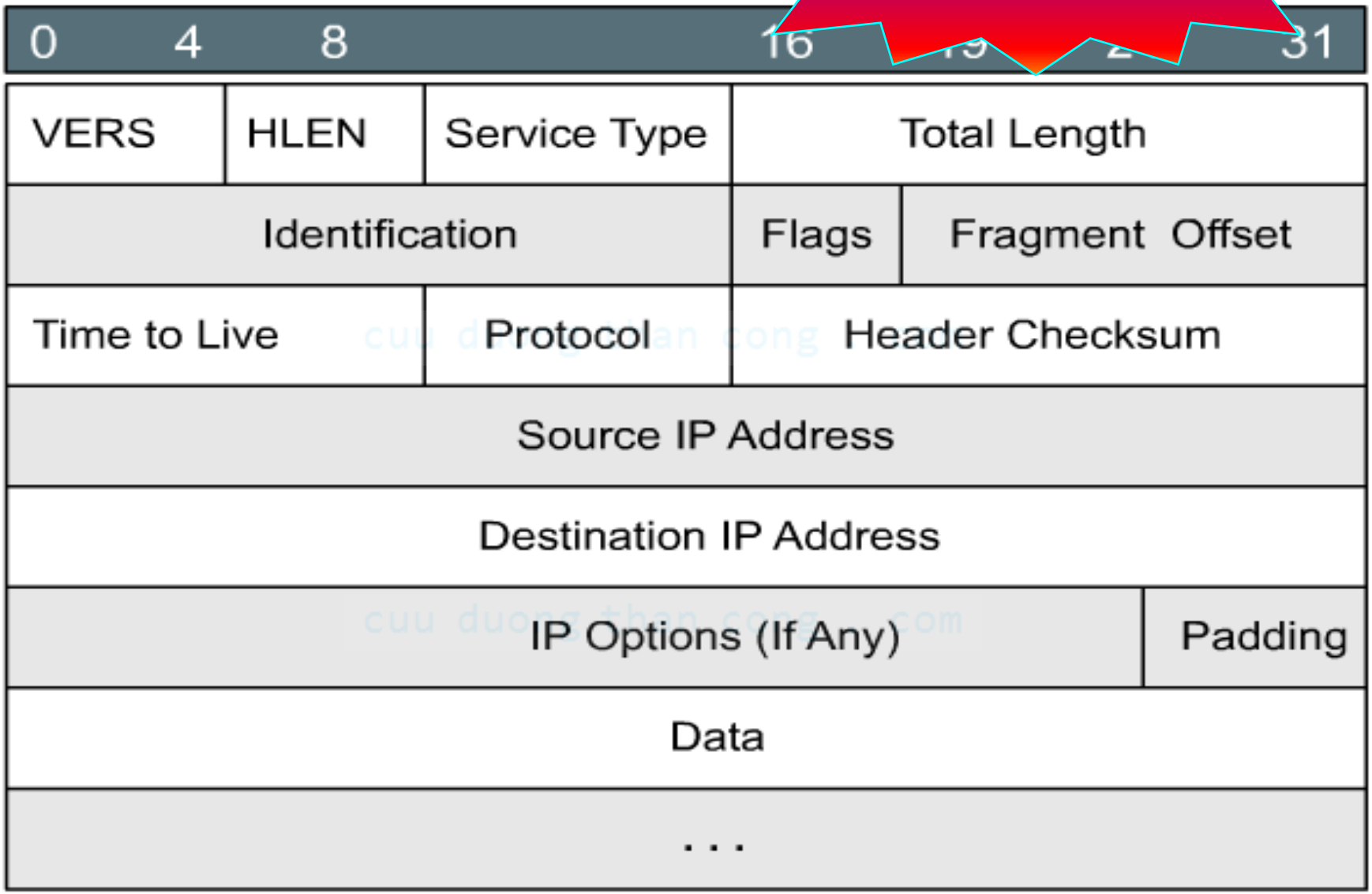
- They treat each packet separately.
- IP is a connectionless system.

Packet switched

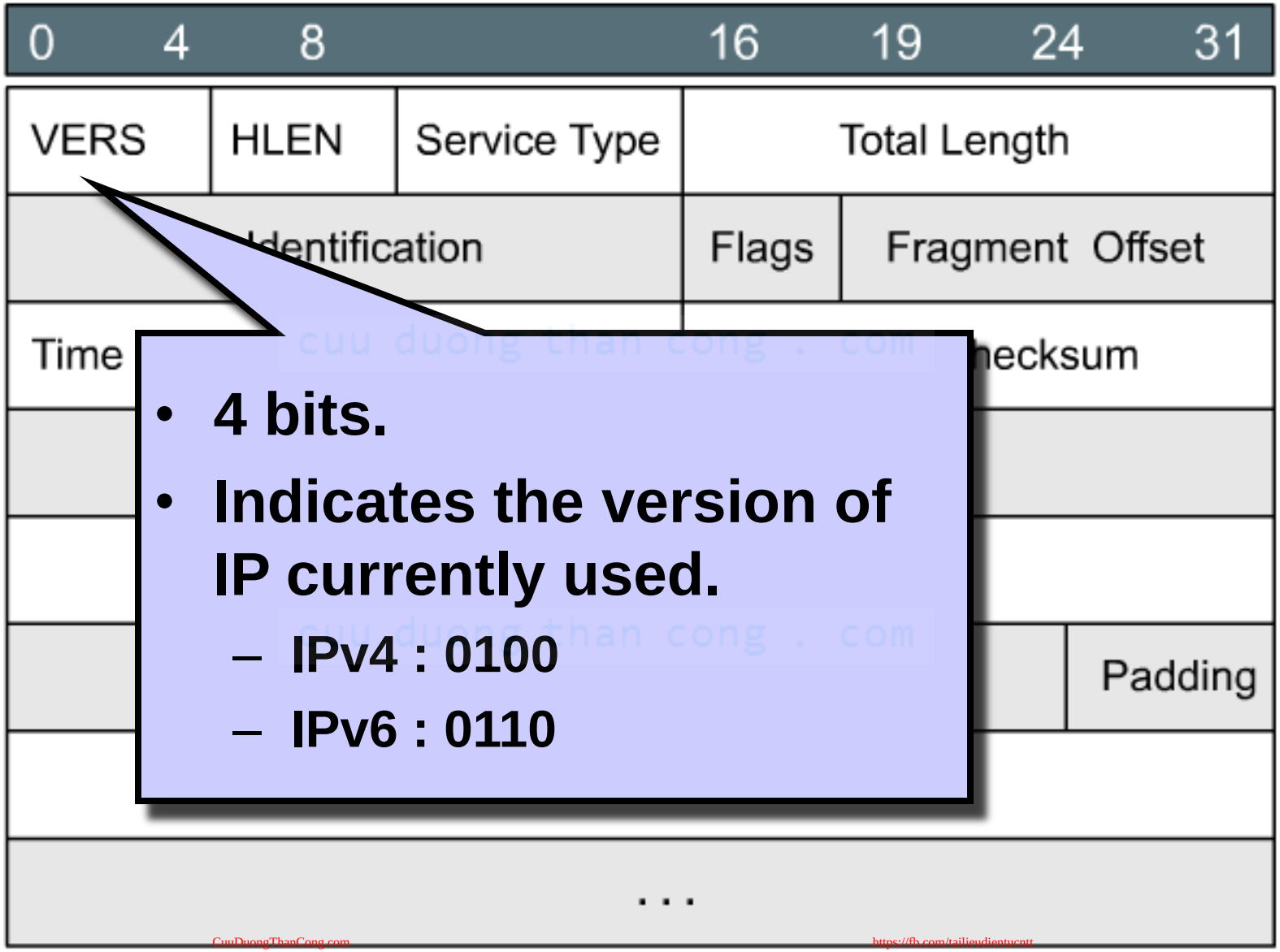
- Connectionless network processes are often referred to as packet switched.
- When the packets pass from source to destination, they can:
  - Switch to different paths.
  - Arrive out of order.
- Devices make the path determination for each packet based on a variety of criteria. Some of the criteria may differ from packet to packet.

Anatomy of an IP packet

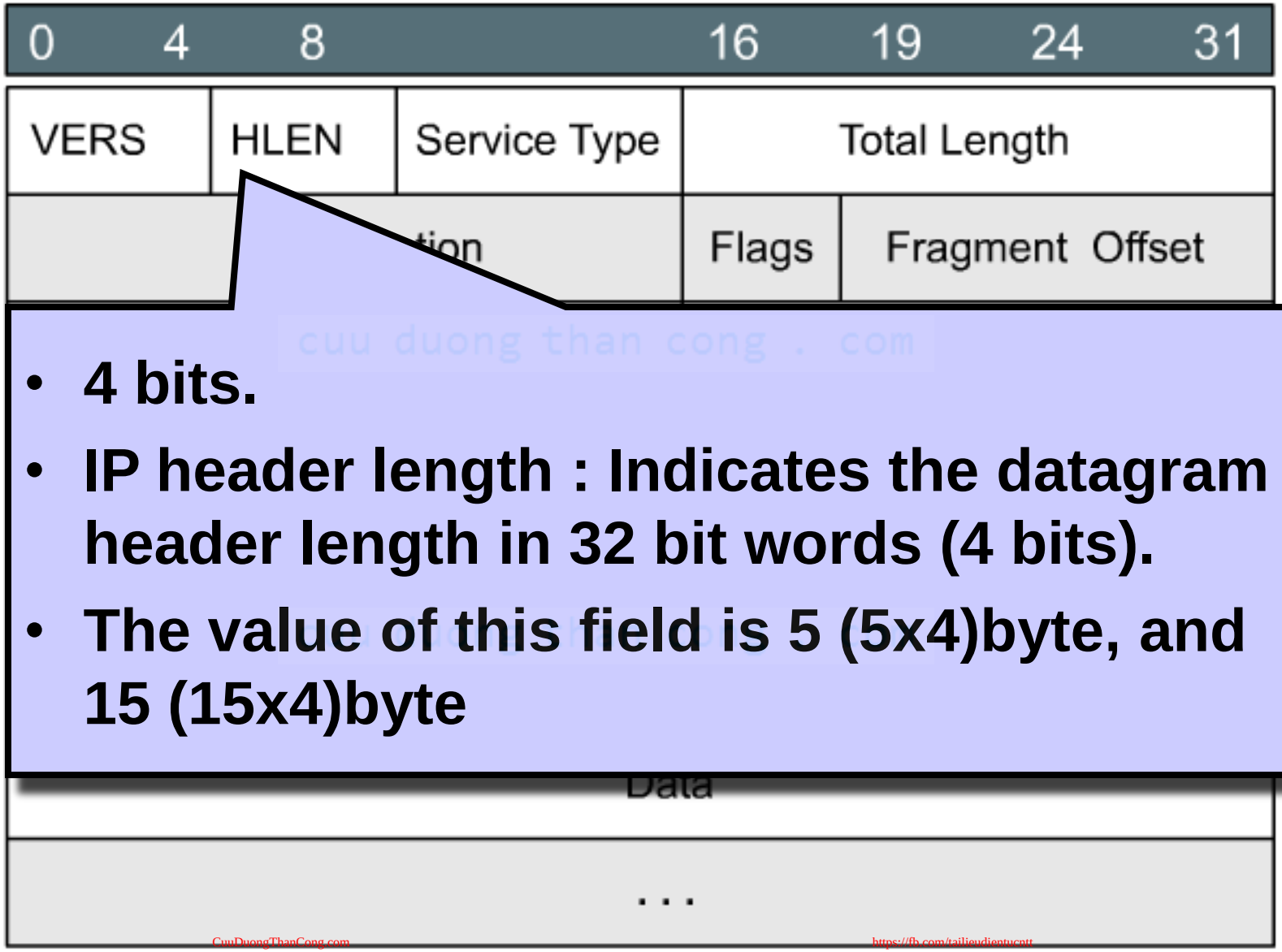
- www.ietf.org and RFC-760



IP header format: Version

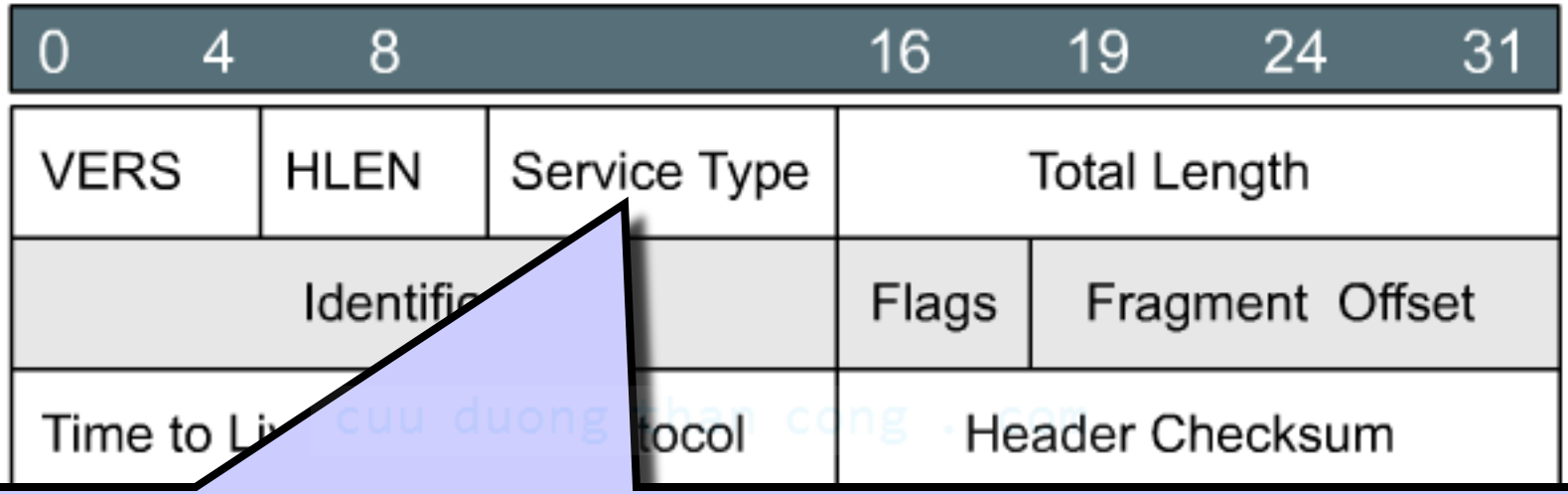


IP header format: Header length



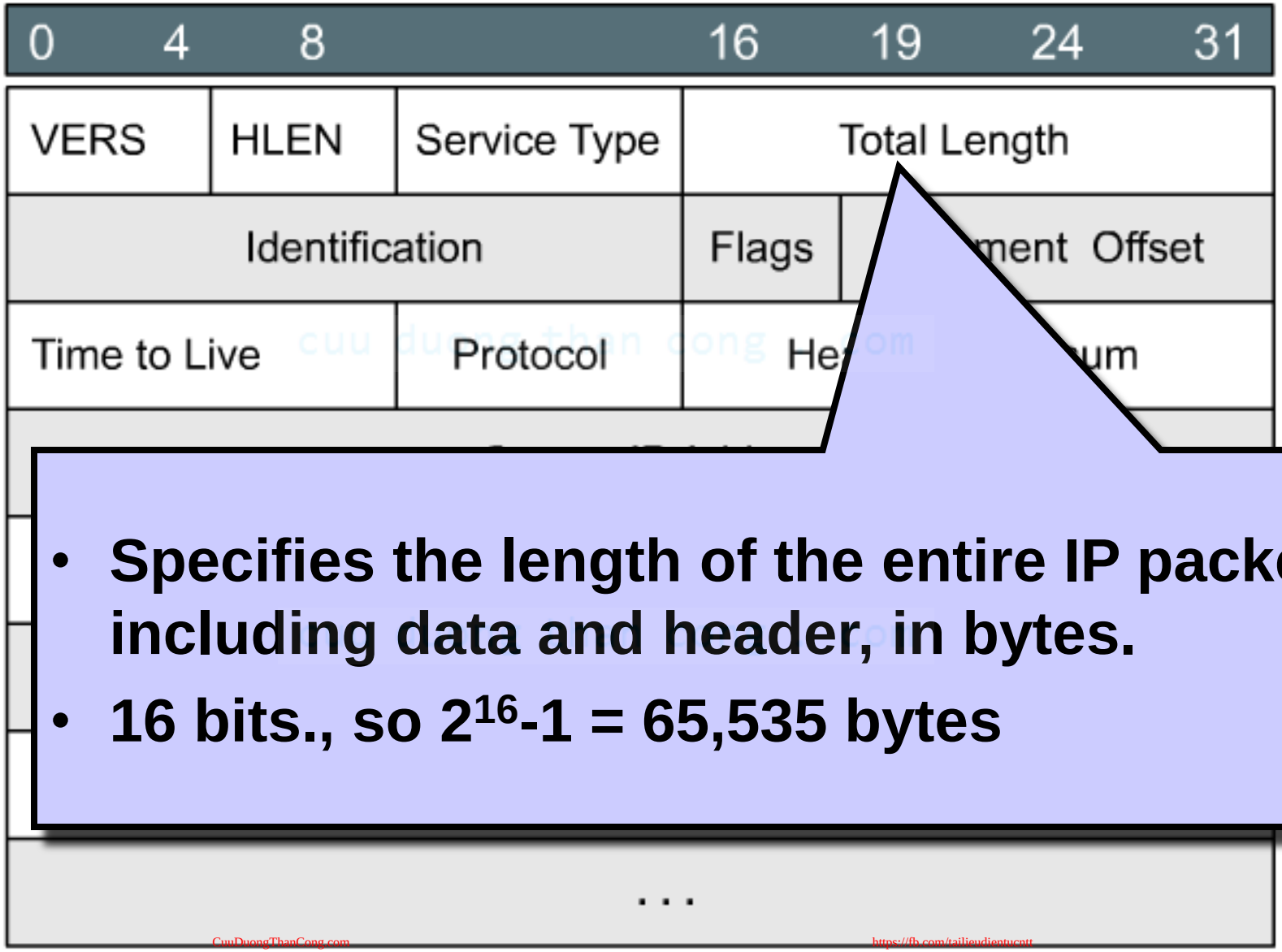
- **4 bits.**
- **IP header length : Indicates the datagram header length in 32 bit words (4 bits).**
- **The value of this field is 5 (5x4)byte, and 15 (15x4)byte**

IP header format: Service type



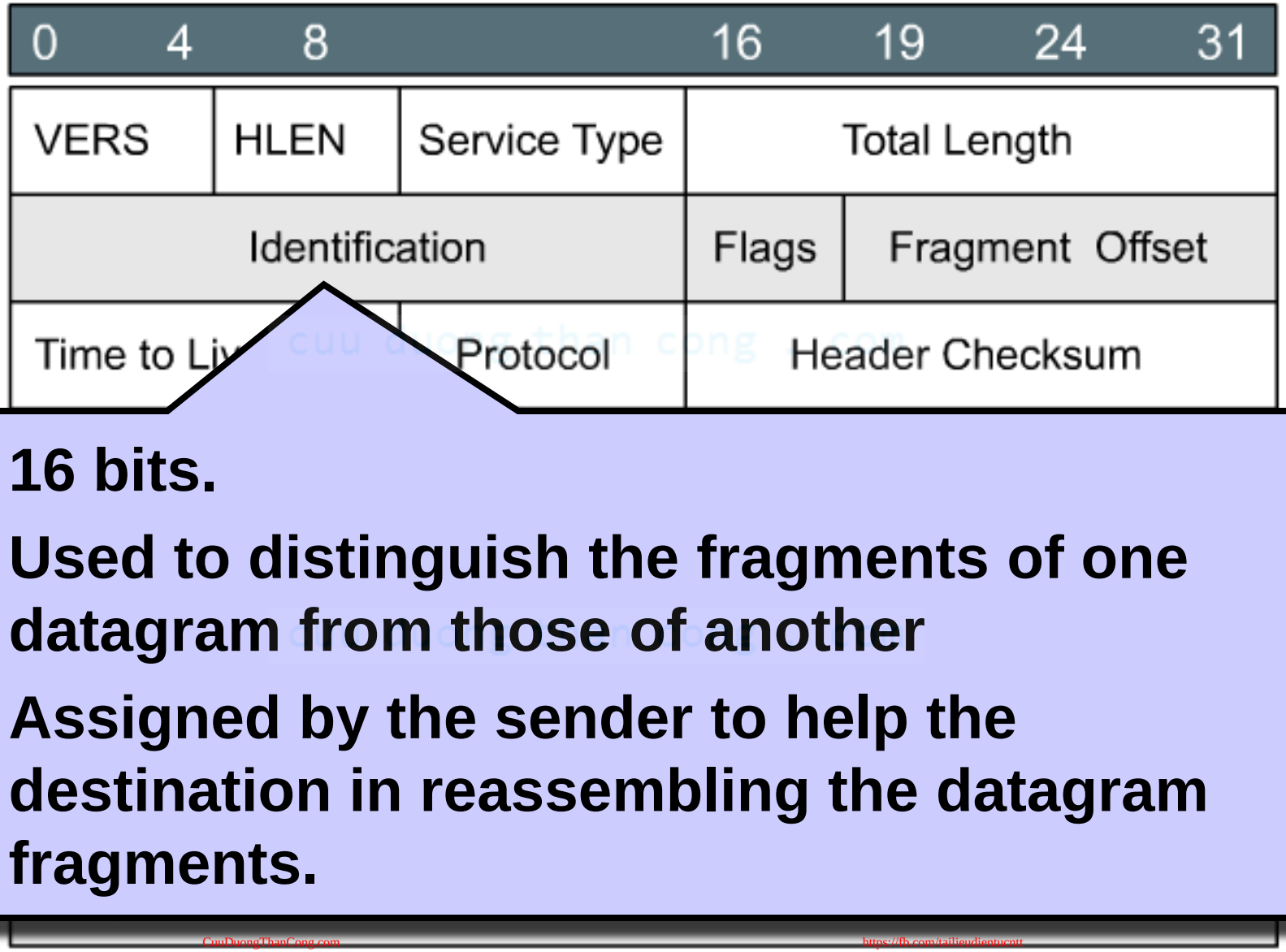
- How the datagram should be handled by the routers.
- Specifies the level of importance that has been assigned by a particular upper-layer protocol.
- 8 bits:
  - Precedence (3 bits) not use in version 4
  - Service Type (4 bits) (Link to TOS)
  - Unused (1 bit)

IP header format: Total length



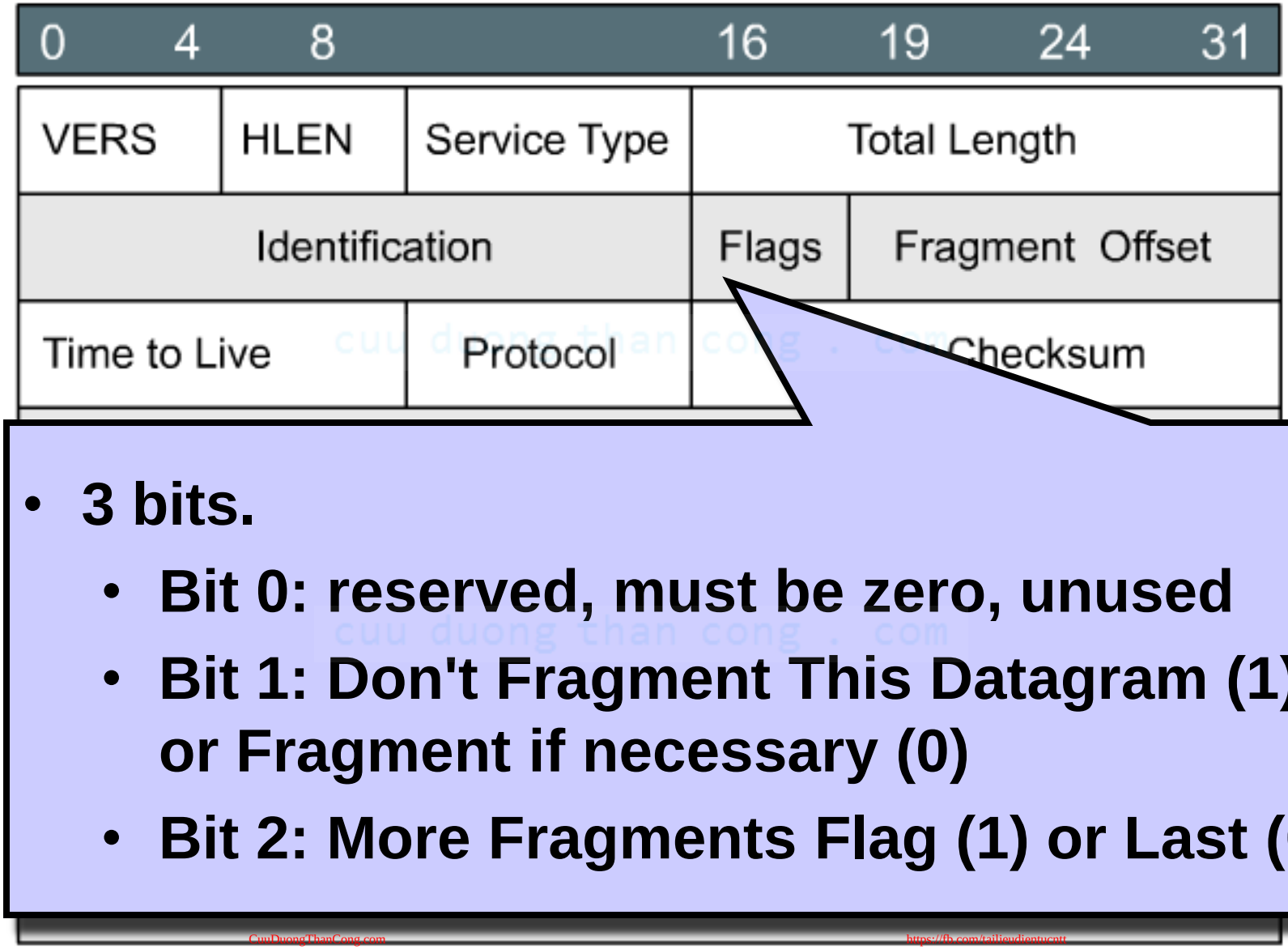
- **Specifies the length of the entire IP packet, including data and header, in bytes.**
- **16 bits., so 2^{16}-1 = 65,535 bytes**

IP header format: Identification



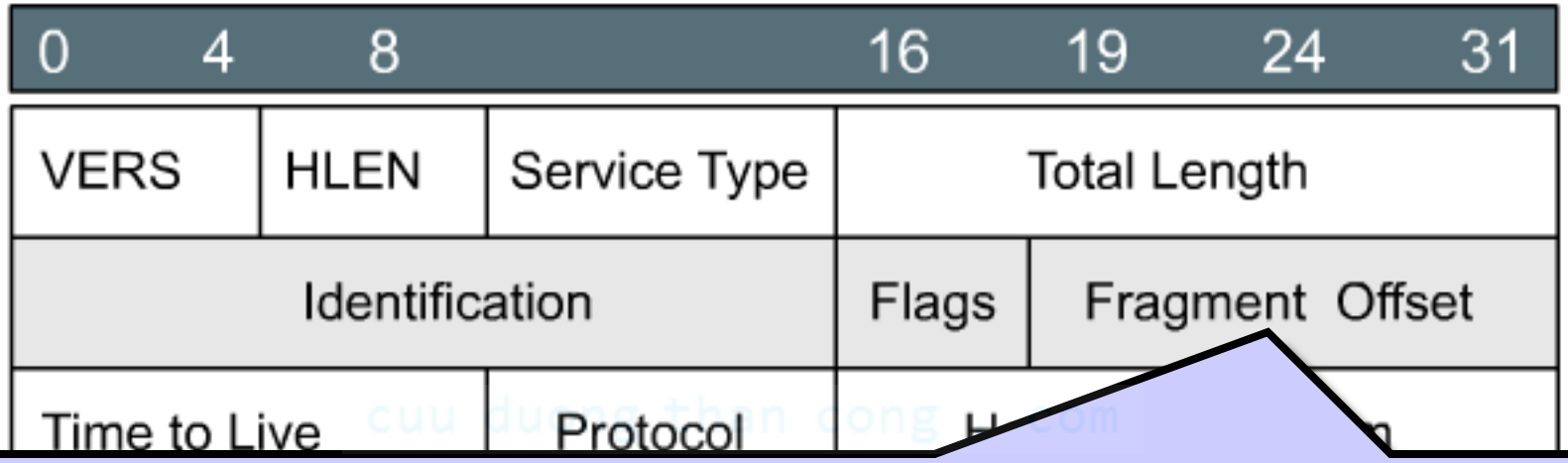
- **16 bits.**
- **Used to distinguish the fragments of one datagram from those of another**
- **Assigned by the sender to help the destination in reassembling the datagram fragments.**

IP header format: Flags



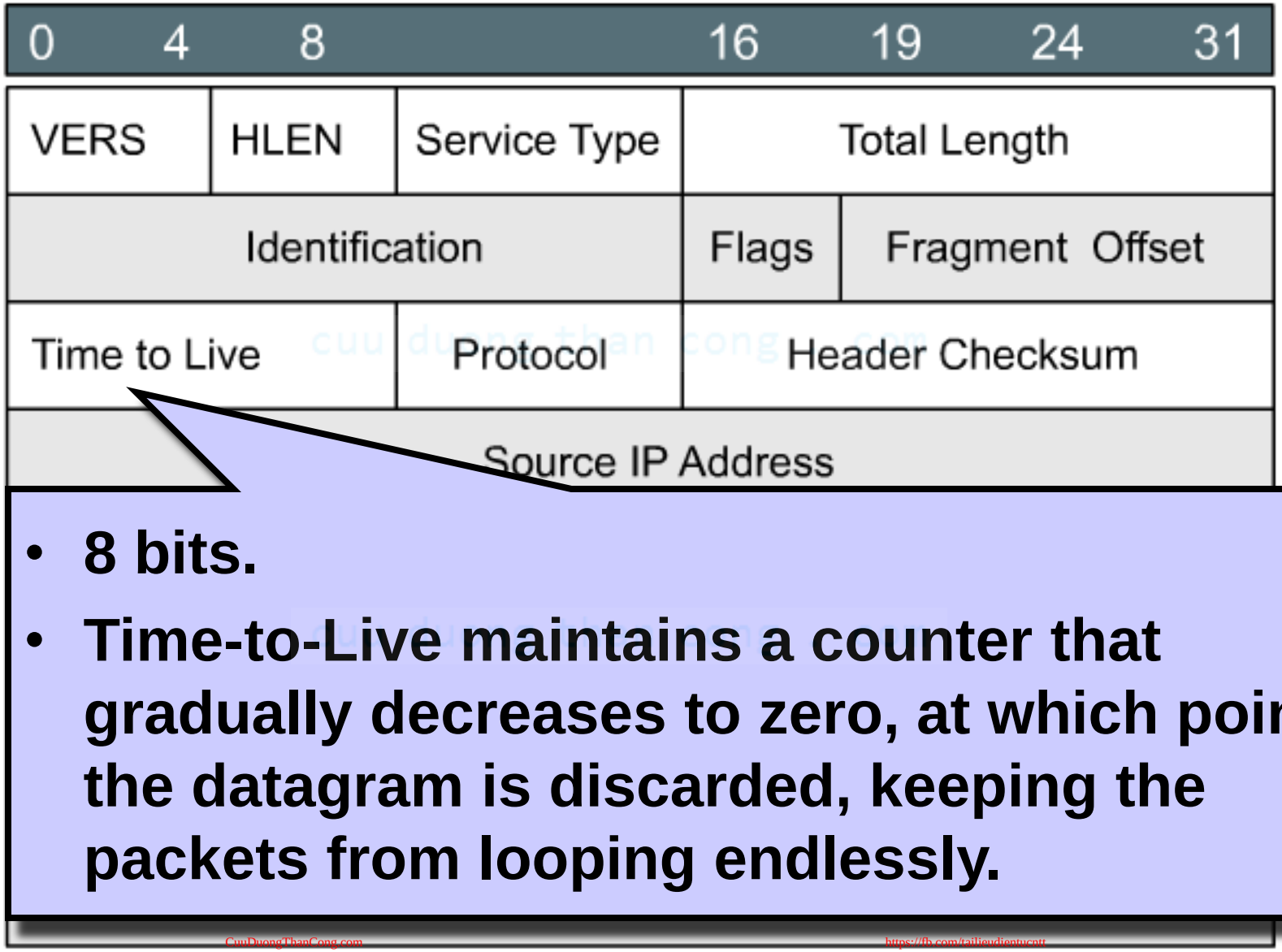
- **3 bits.**
  - **Bit 0: reserved, must be zero, unused**
  - **Bit 1: Don't Fragment This Datagram (1) or Fragment if necessary (0)**
  - **Bit 2: More Fragments Flag (1) or Last (0)**

IP header format: Fragment offset



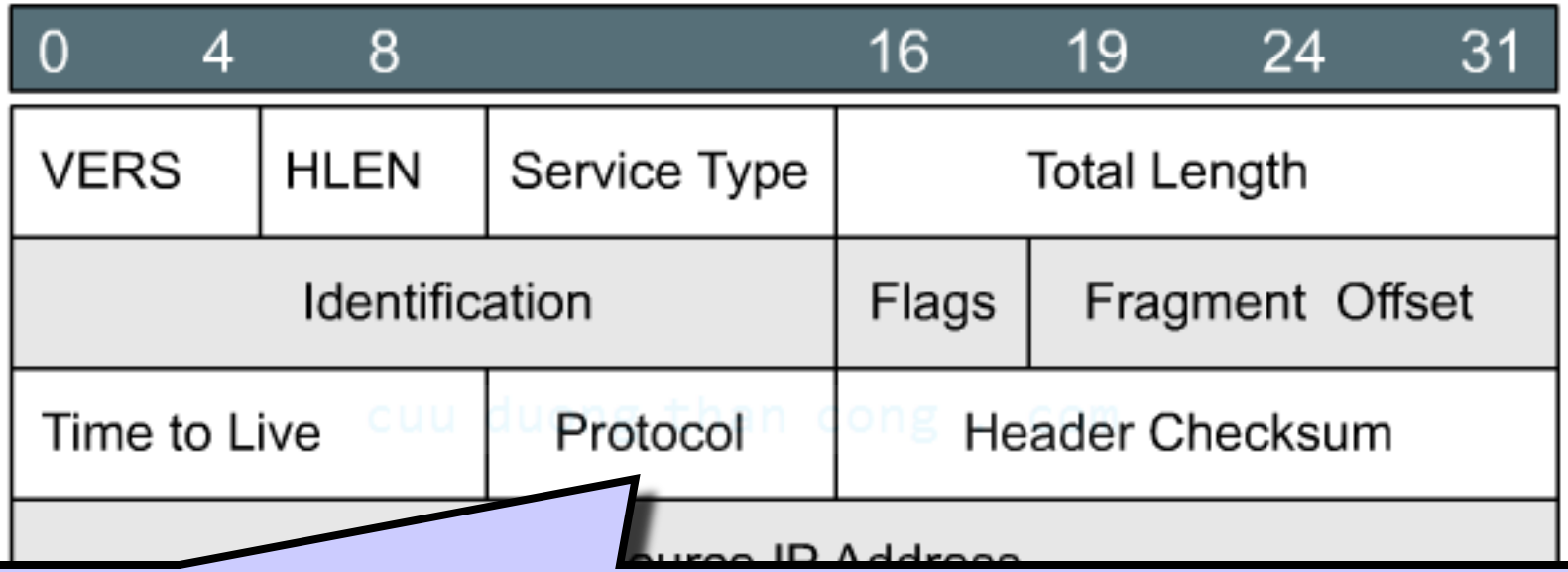
- 13 bits
- Tells the receiver the position of a fragment in the original datagram
- The fragment offset is measured in units of 8 bytes (Position number / 8)
- The first fragment has offset zero.
- The last fragment has flags zero.

IP header format: Time to Live



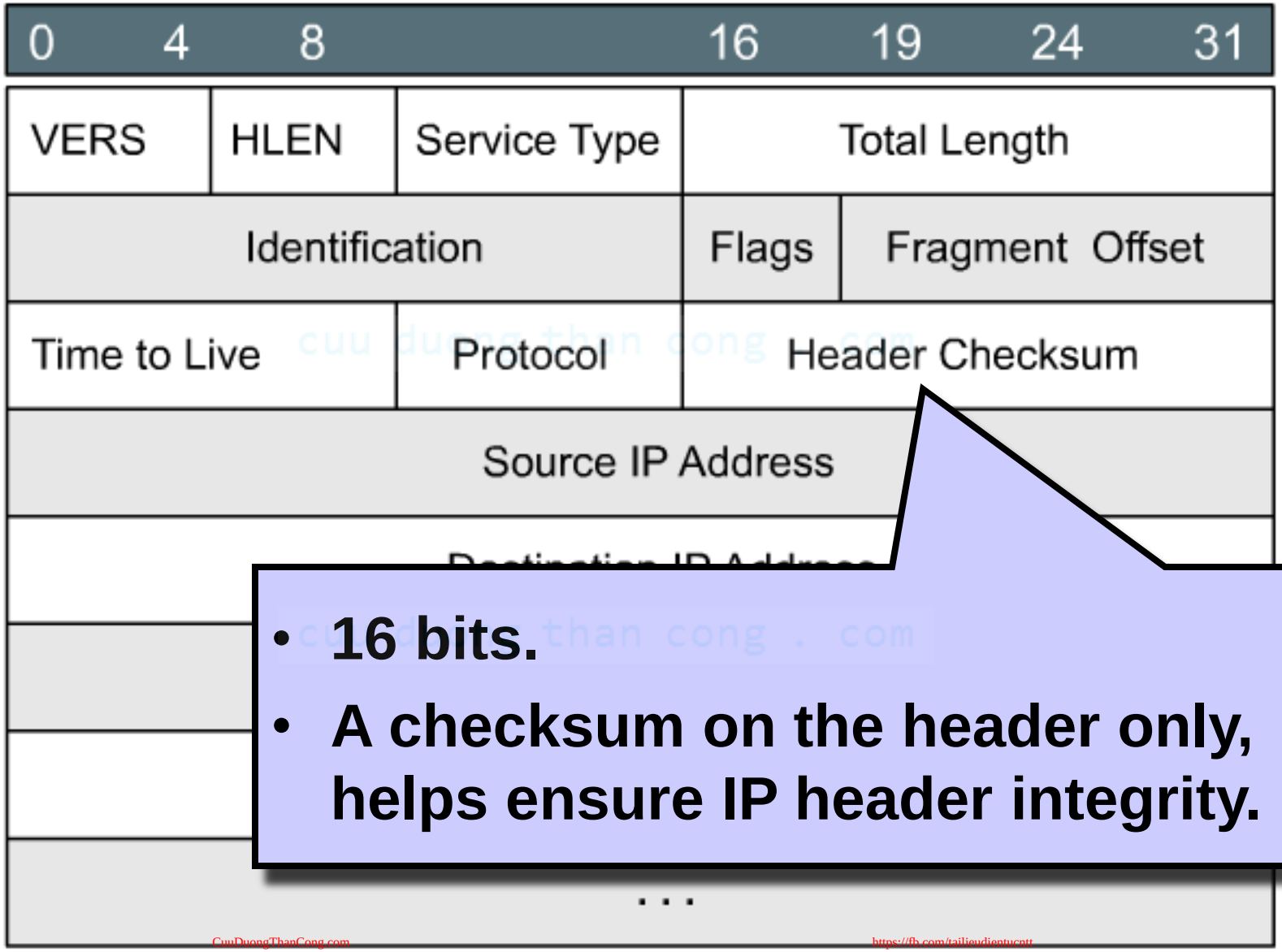
- **8 bits.**
- **Time-to-Live maintains a counter that gradually decreases to zero, at which point the datagram is discarded, keeping the packets from looping endlessly.**

IP header format: Protocol



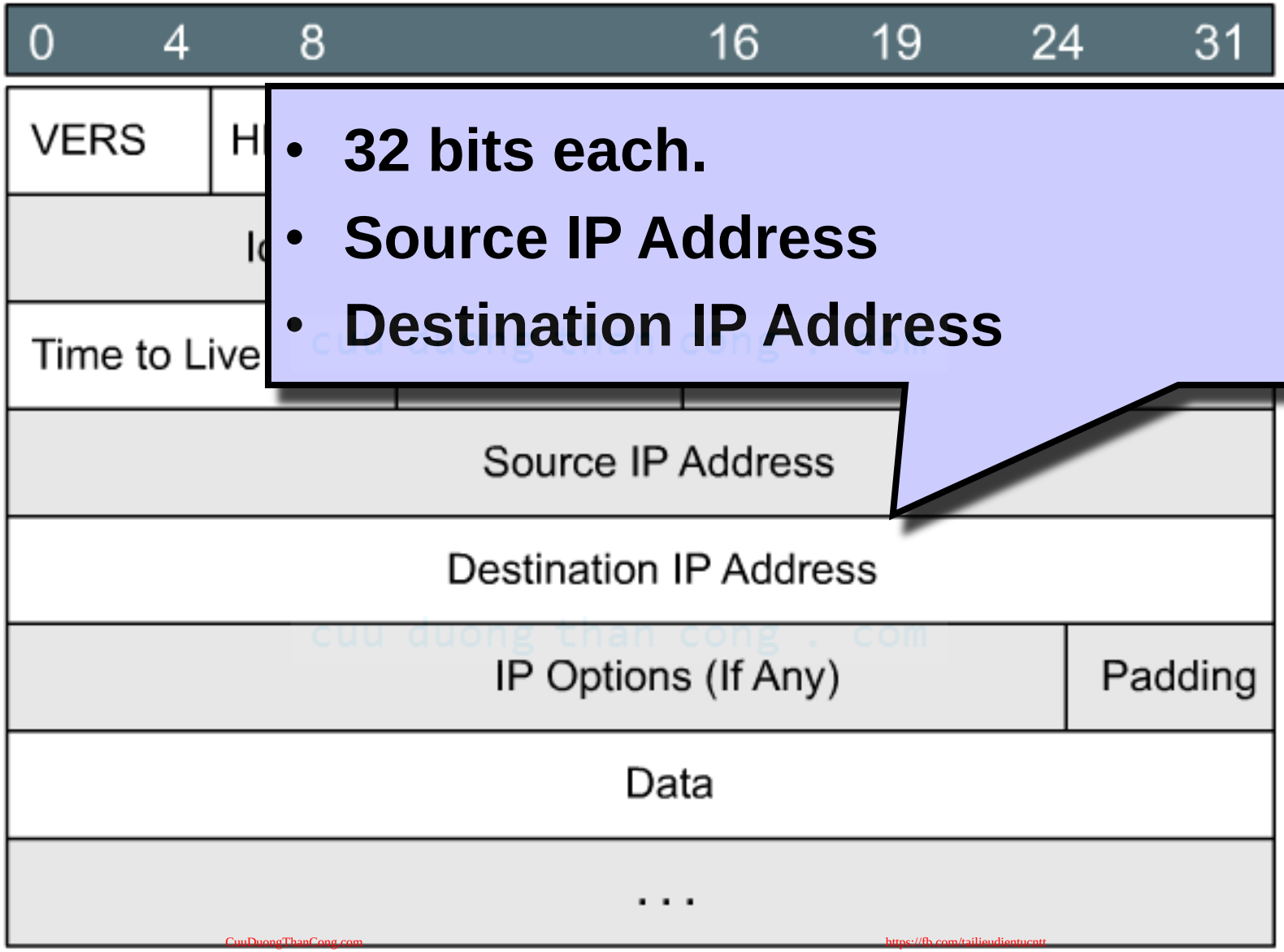
- 8 bits.
- Indicates which upper-layer protocol receives incoming packets after IP processing has been completed
  - 06 : TCP 01 : ICMP
  - 17 : UDP 08 : EGP

IP header format: Header checksum

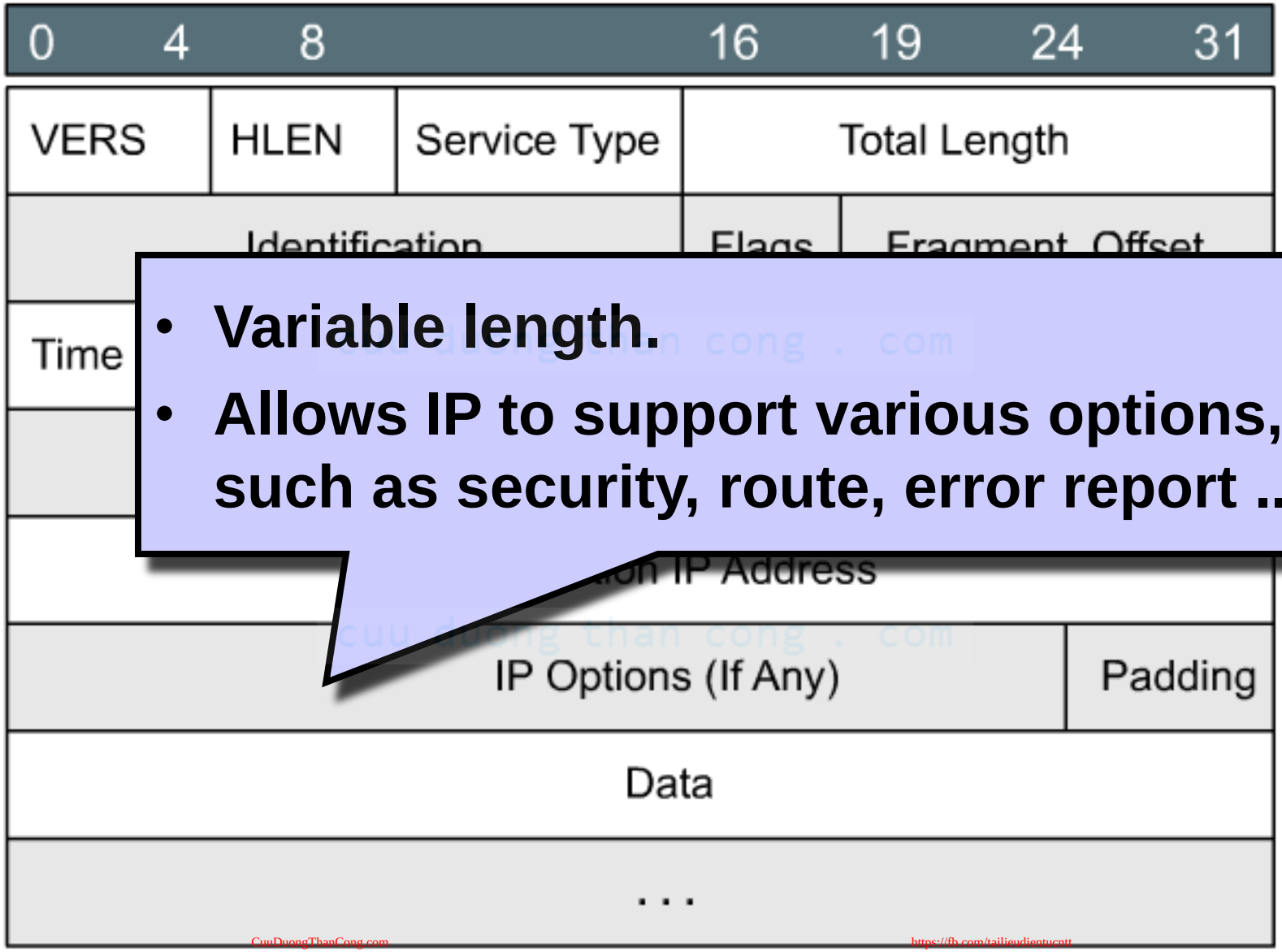


- **16 bits.**
- **A checksum on the header only, helps ensure IP header integrity.**

IP header format: Addresses

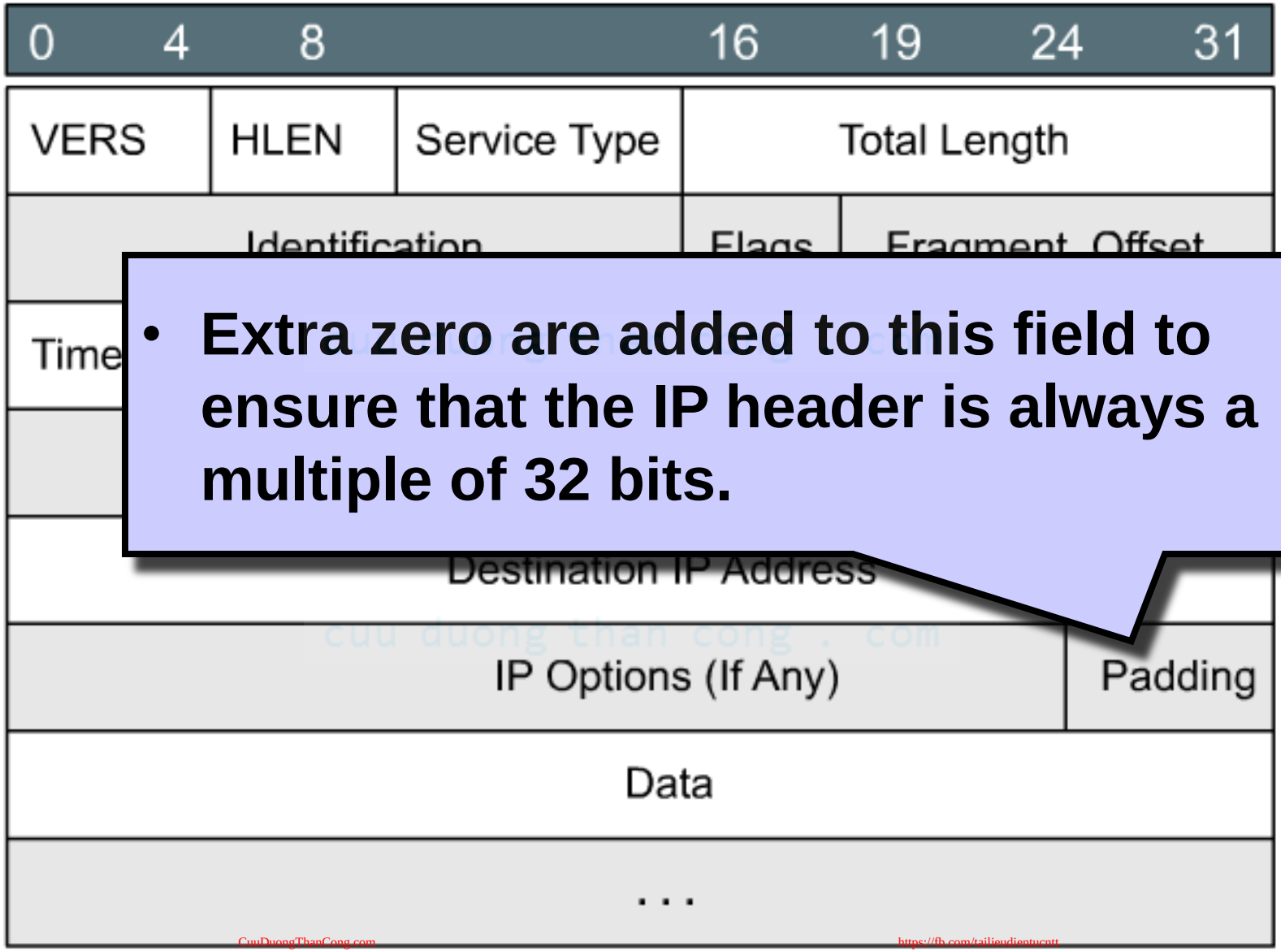


IP header format: Options (Homework)



- **Variable length.**
- **Allows IP to support various options, such as security, route, error report ...**

IP header format: Padding



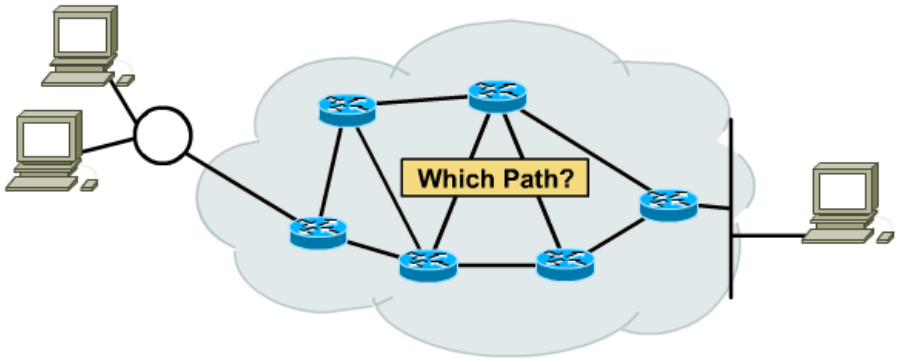
- **Extra zero are added to this field to ensure that the IP header is always a multiple of 32 bits.**

IP ROUTING PROTOCOLS

Routing overview

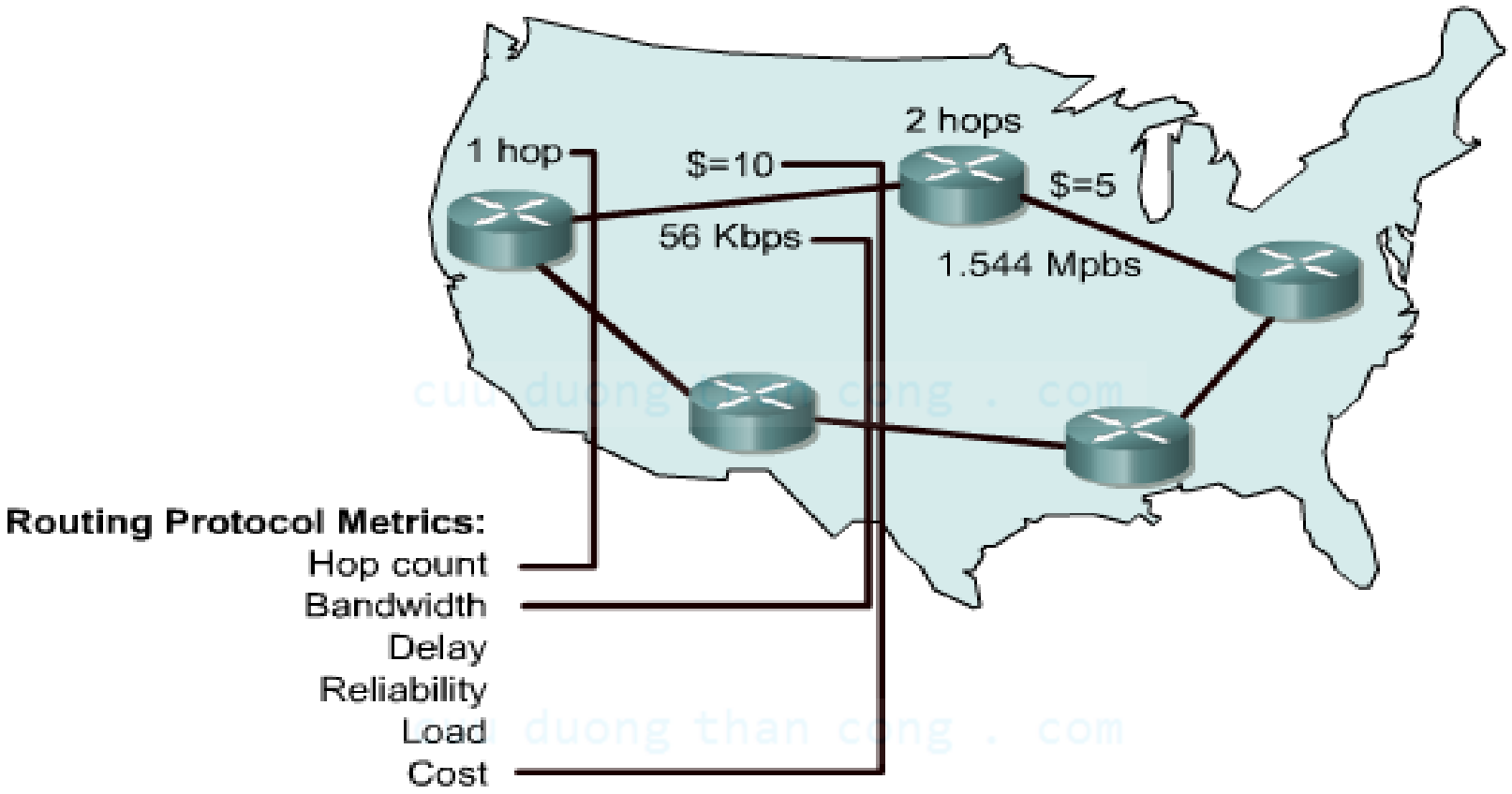
- Routing is an OSI Layer 3 function.
- Routing is the process of finding the most efficient path from one device to another.
- The primary device that performs the routing process is the router.
  - Routers must maintain routing tables and make sure other routers know of changes in the network topology.
  - The router switches the packets to the appropriate interface, adds the necessary framing information for the interface, and then transmits the frame.

Router Two basic functions



- Path determination:
  - Path determination is the process that 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, load, cost ...
- Packet switching:
  - The router re-encapsulates the packet in the protocol needed for the specified port and then switches the packet out that port.

Routing metrics

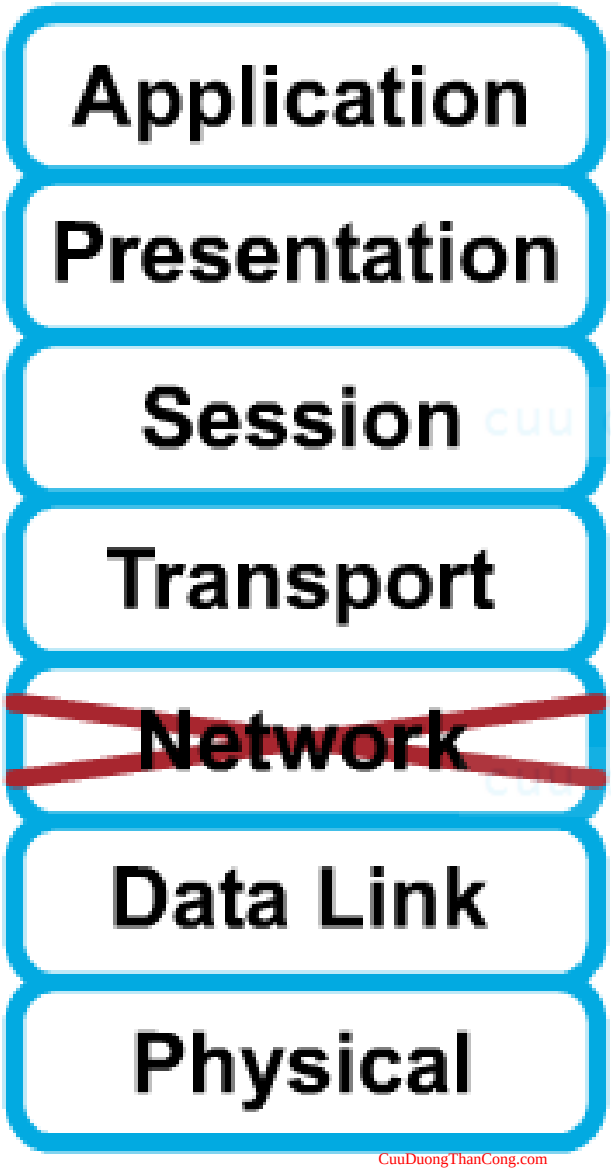


- Routing metrics are values used in determining the advantage of one route over another, which used by router.

Router

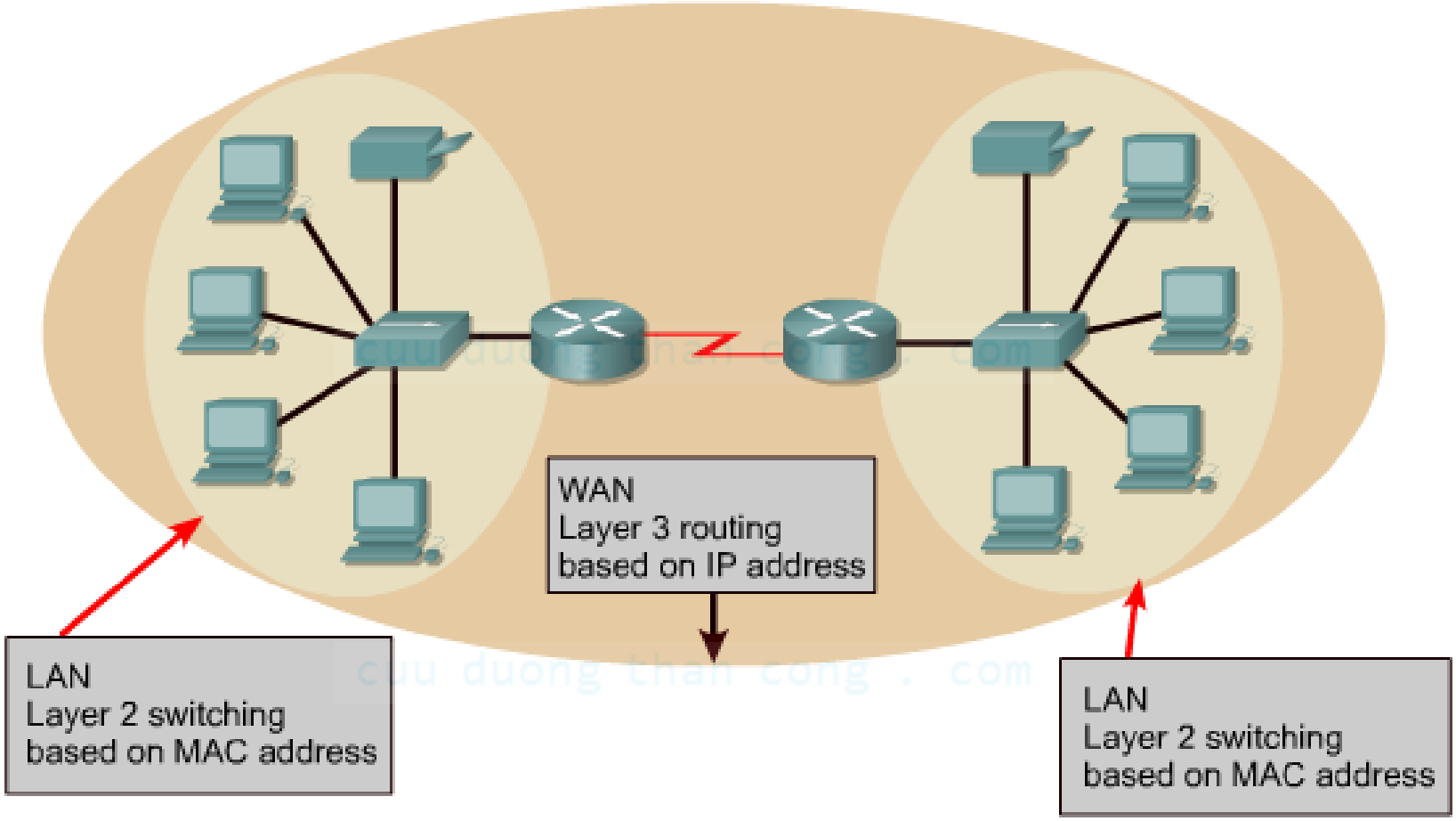
- A router is a type of internetworking device that passes data packets between networks, based on Layer 3 addresses.
- A router has the ability to make intelligent decisions regarding the best path for delivery of data on the network.
- Routers connect two or more networks, each of which must have a 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.

Non-routable protocol



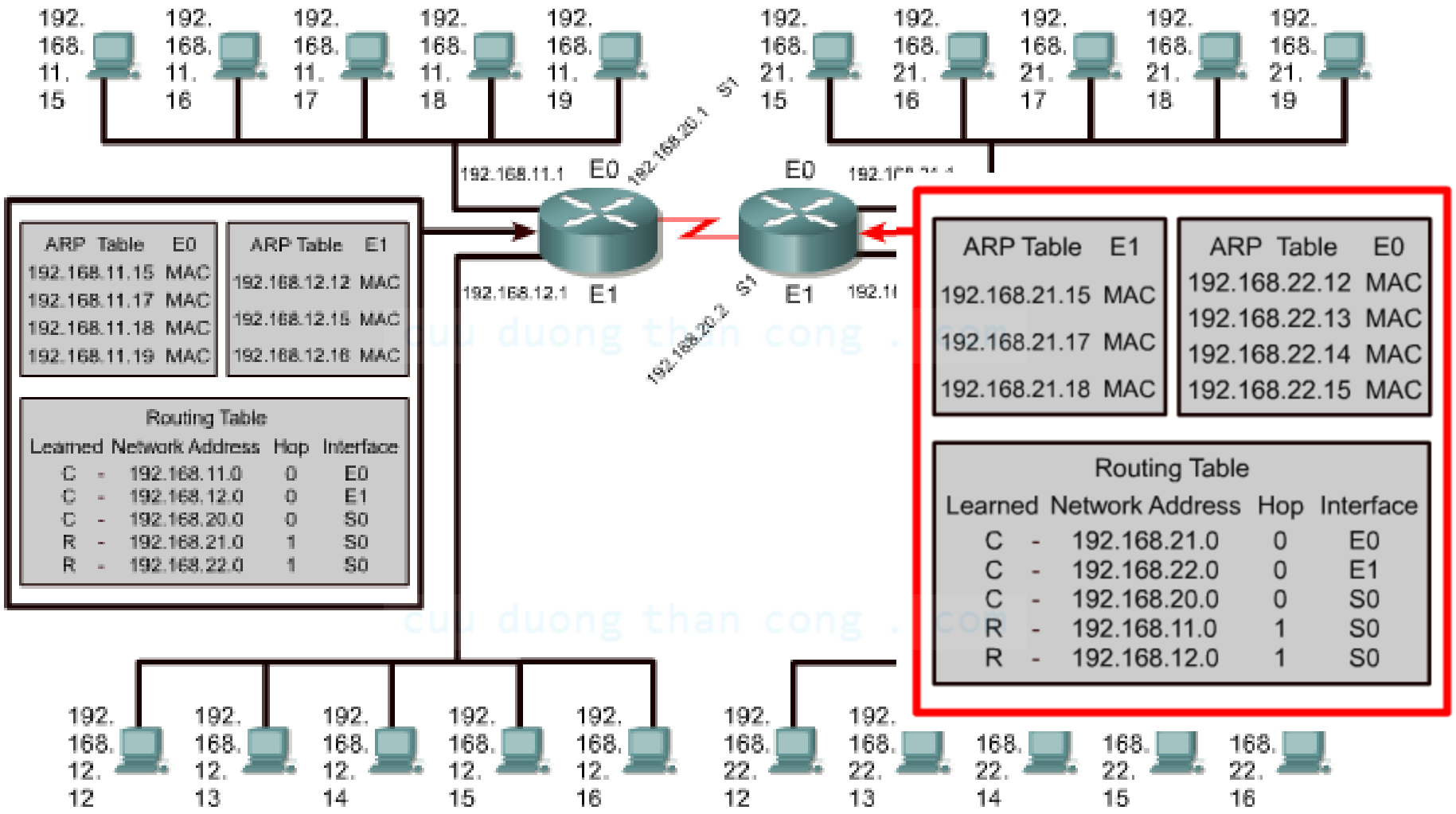
- This course focuses on the most common routable protocol
- Non-routable protocols are protocols that do not support Layer 3.
- The most common of these non-routable protocols is NetBEUI.
- NetBEUI is a small, fast, and efficient protocol that is limited to running on one segment.

Routing versus switching



Layer 2 switching takes place within the LAN. Layer 3 routing moves traffic between broadcast domains. This requires the hierarchical addressing format that a Layer 3 addressing scheme like IP provides.

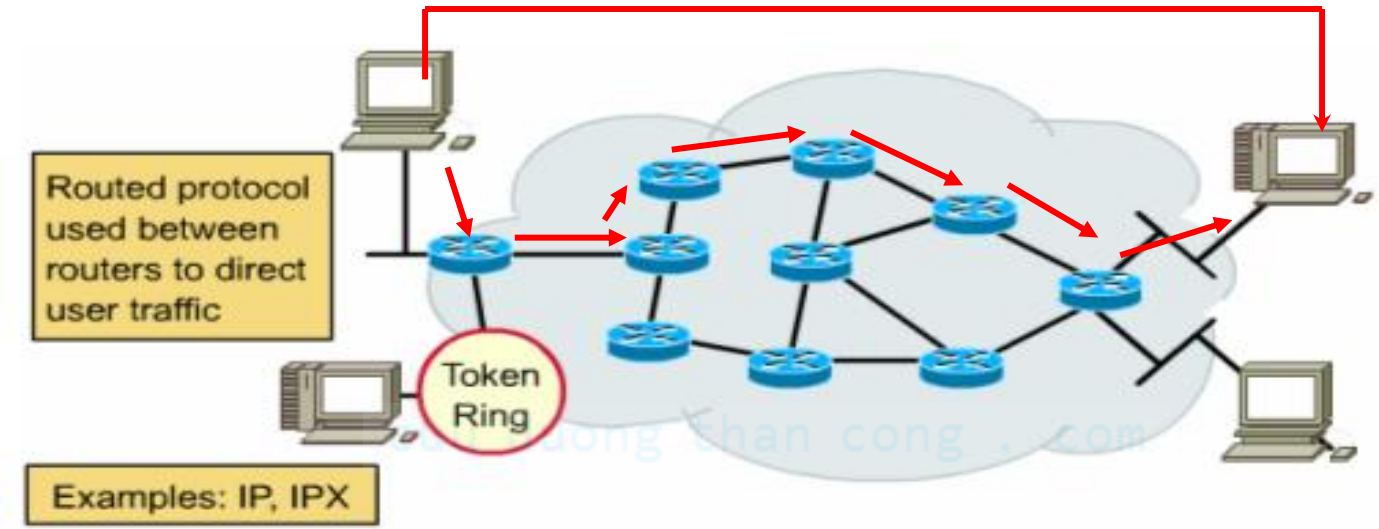
ARP tables and Routing tables



Router and Switch feature comparison

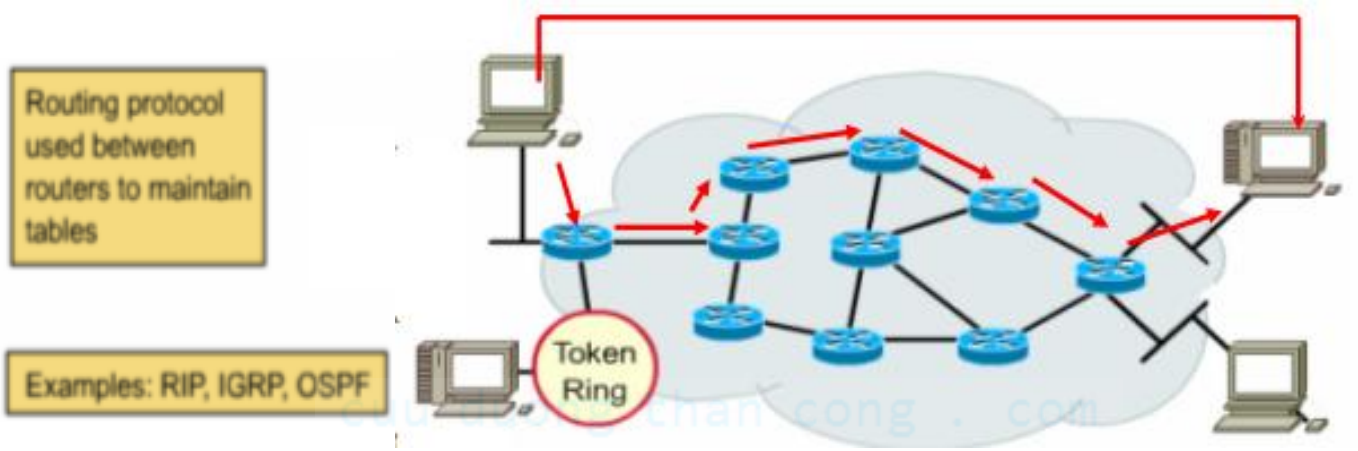
Features	Router	Switch
Speed	Slower	Faster
IOS layer	Layer 3	Layer 2
Addressing used	IP	MAC
Broadcasts	Blocks	Forwards
security	Higher	Lower

Routed Protocol



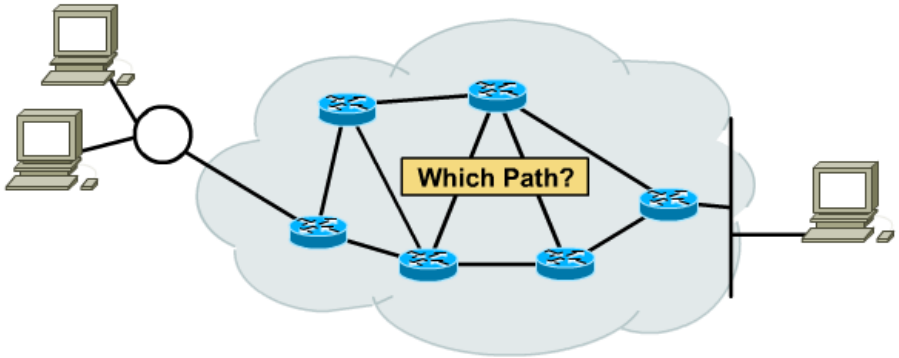
- Protocols used at the network layer that transfer data from one host to another across a router are called routed or routable protocols.
- Functions include the following:
  - Provides network layer address.
  - Defines the format and use of the fields within a packet.

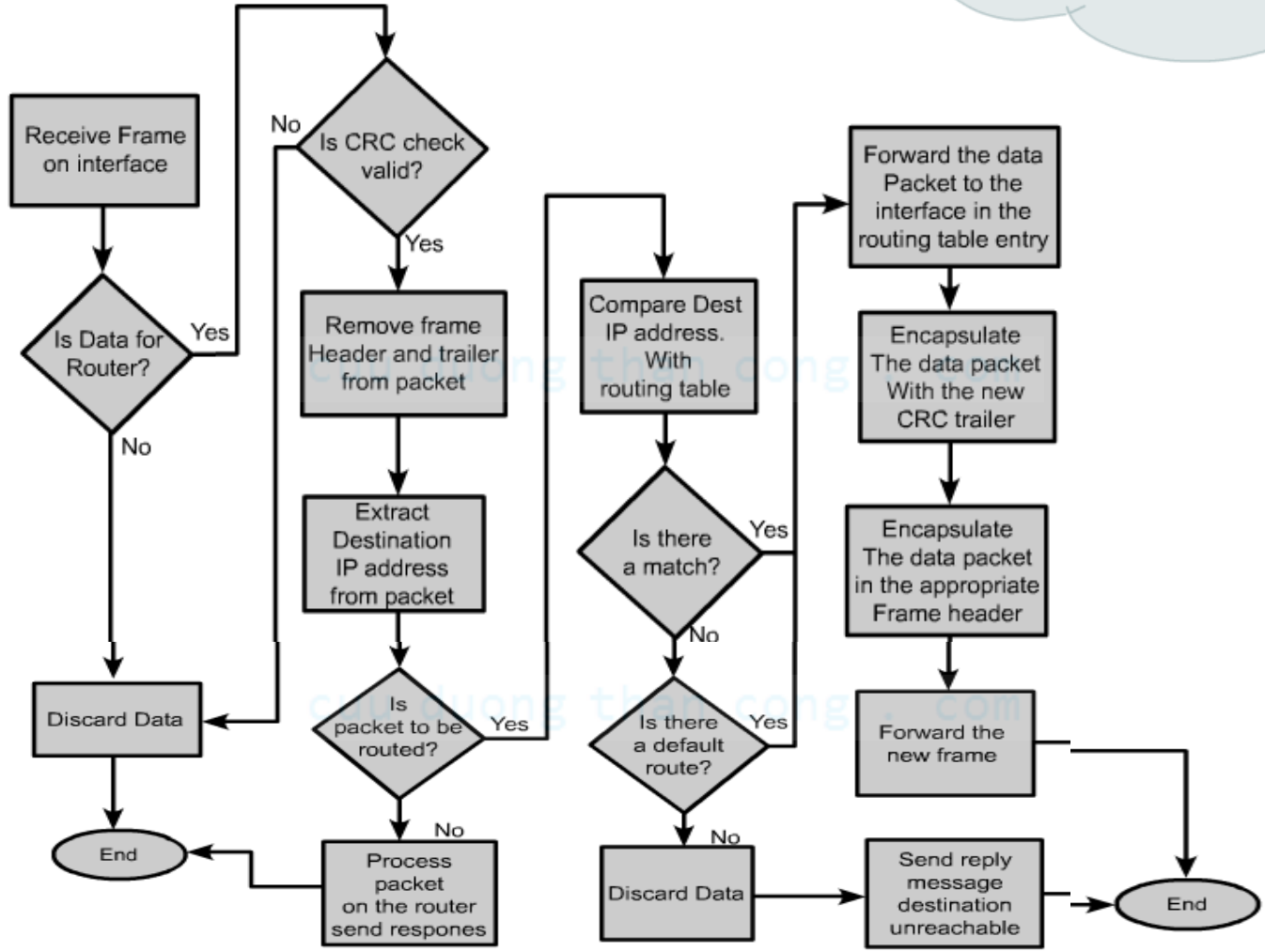
Routing Protocol



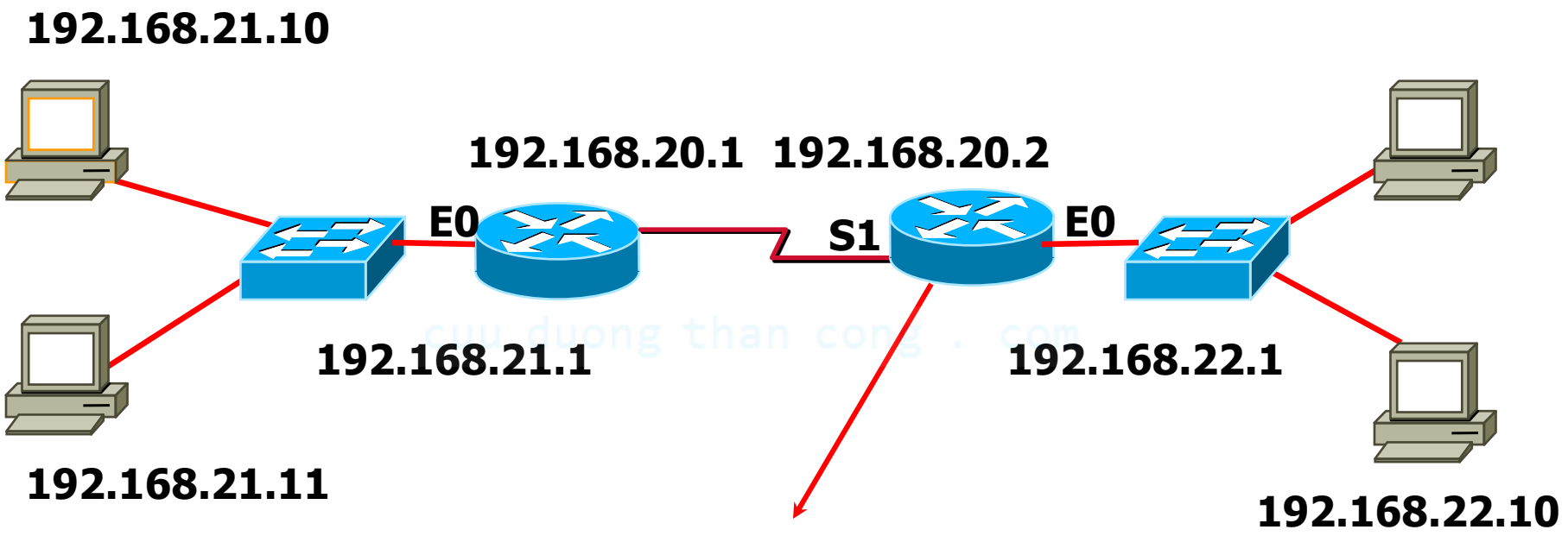
- Routing protocols allow routers to choose the best path for data from source to destination.
- Functions includes the following:
  - Provides processes for sharing route information.
  - Allows routers to communicate with other routers to update and maintain the routing tables

Path Determination





Routing Table



Routing Table

Learned		Network Address	Hop	Interface
C	-	192.168.20.0	0	E0
C	-	192.168.22.0	0	S1
R	-	192.168.21.0	1	S1

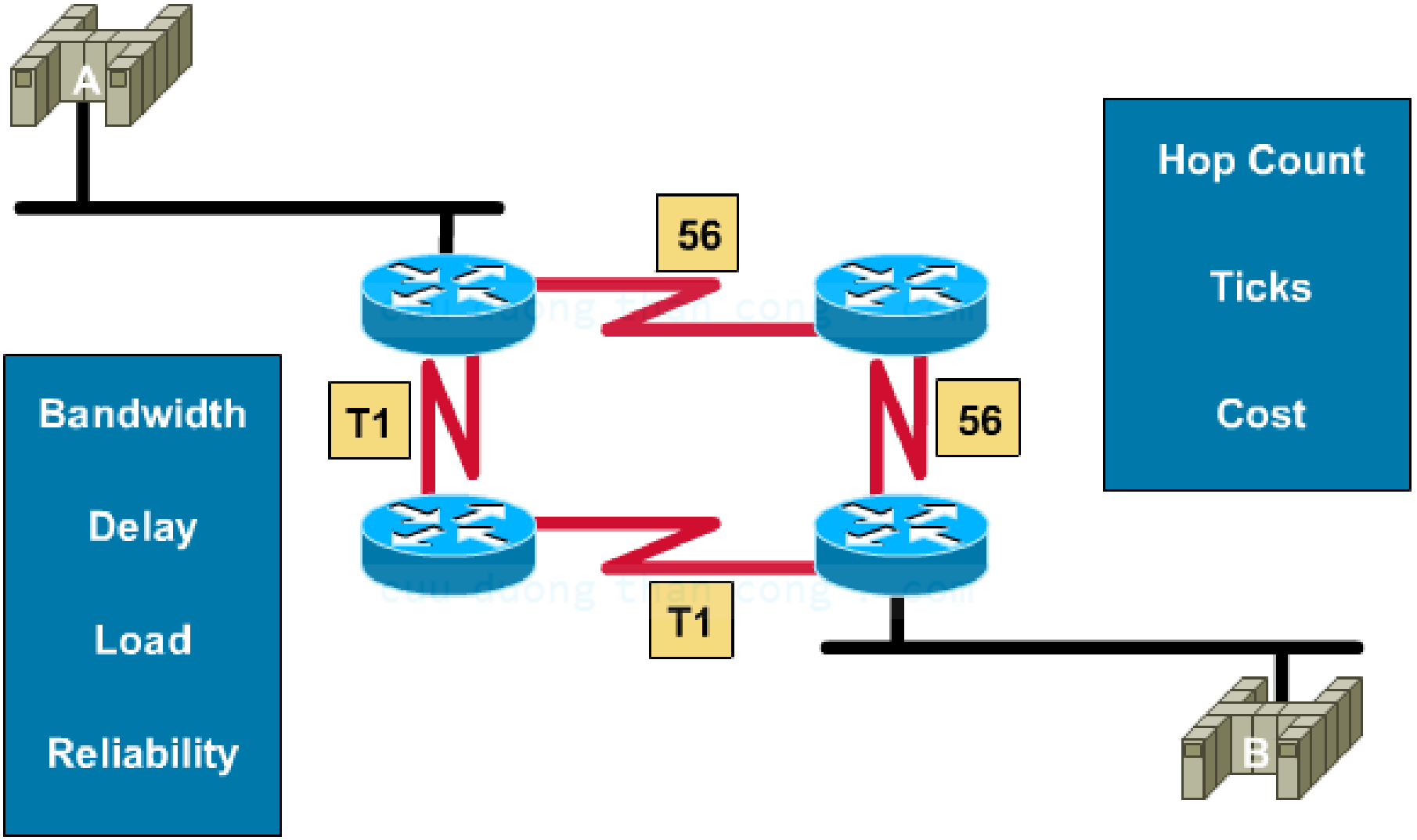
Routing algorithms and metrics

- Different routing protocols use different algorithms .
- Routing algorithms depend on metrics to make these decisions.
- Routing protocol design goals:
  - Optimization
  - Simplicity and low overhead
  - Robustness and stability
  - Flexibility
  - Rapid convergence

How the metric is calculated

- Each routing algorithm interprets what is best in its own way.
- Routing algorithm generates a number, called the **metric value**, for each path through the network.
- Typically, The smaller the metric number, the better the path.
- Metrics can be calculated based on:
  - A single characteristic of a path.
  - A combination of several characteristics.

Distance in Metrics



Routing metrics – Path length

- Tick - Measures delay on a link using IBM PC clock tick (~ 55 millisecs)
- Hop count:
  - A hop = an intermediate systems (such as routers) through which a packet must pass to travel from the source to the destination
  - Hop count = accumulative sum of hops between source and destination
- *Path length does not discriminate between fast and slow links*

Routing metrics – Cost

- A value associated with a given route
- Chosen and configured by administrator
- Can be based on: bandwidth, monetary value, and so on

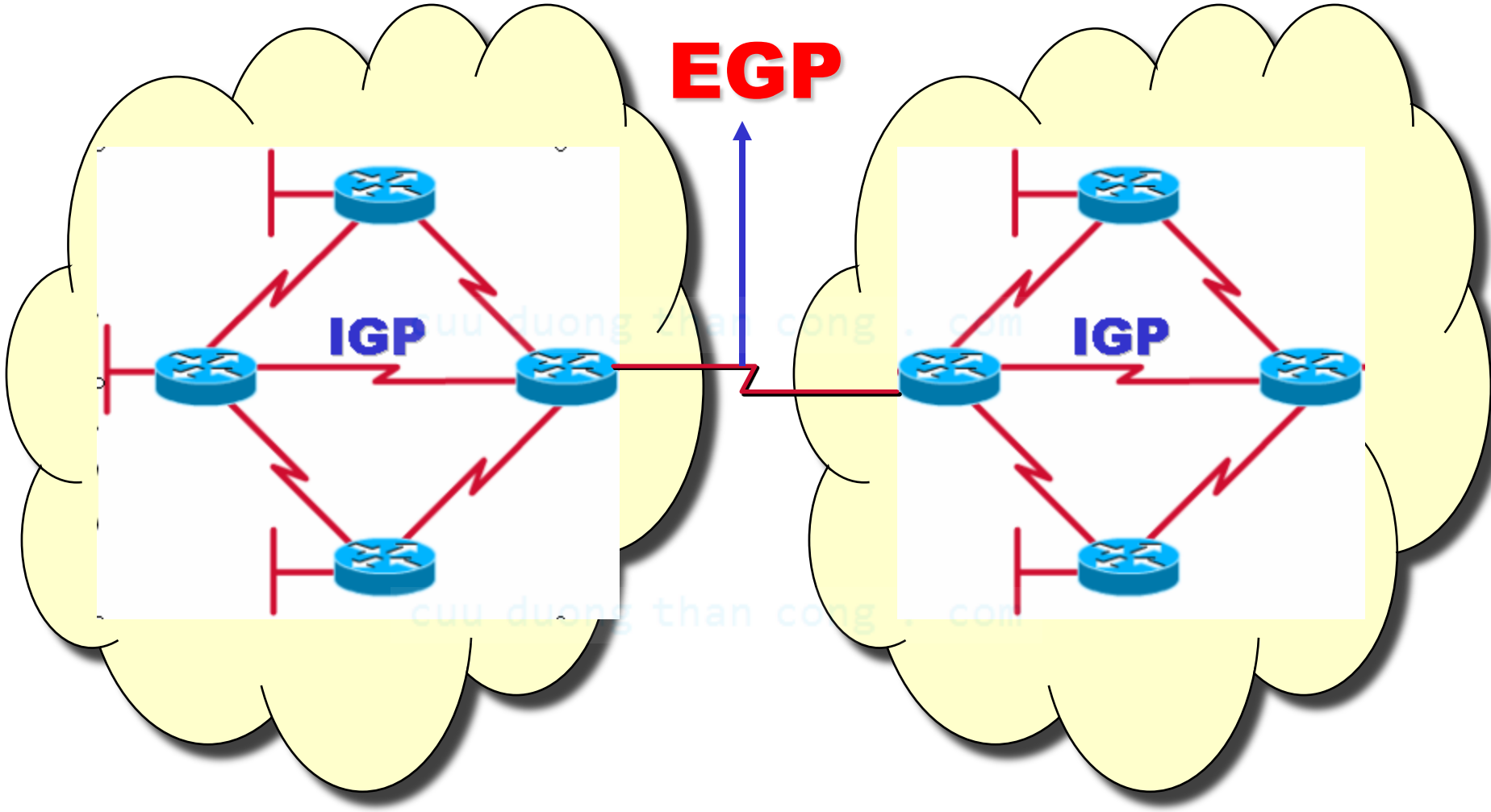
Routing metrics – Composite

- **Bandwidth** – The data capacity of a link.
- **Delay** – The length of time required to move a packet along each link from source to destination.
- **Load** – The amount of activity on a network resource such as a router or a link.
- **Reliability** – Usually a reference to the error rate of each network link.

IGP and EGP (classification #1)

- An autonomous system is a network or set of networks under common administrative control, consists of routers that present a consistent view of routing to the external world, such as cisco.com
- Interior Gateway Protocols (RIP, IGRP, EIGRP, OSPF):
  - Be used within an autonomous system
- Exterior Gateway Protocols (EGP, BGP):
  - Be used to route packets between autonomous systems.

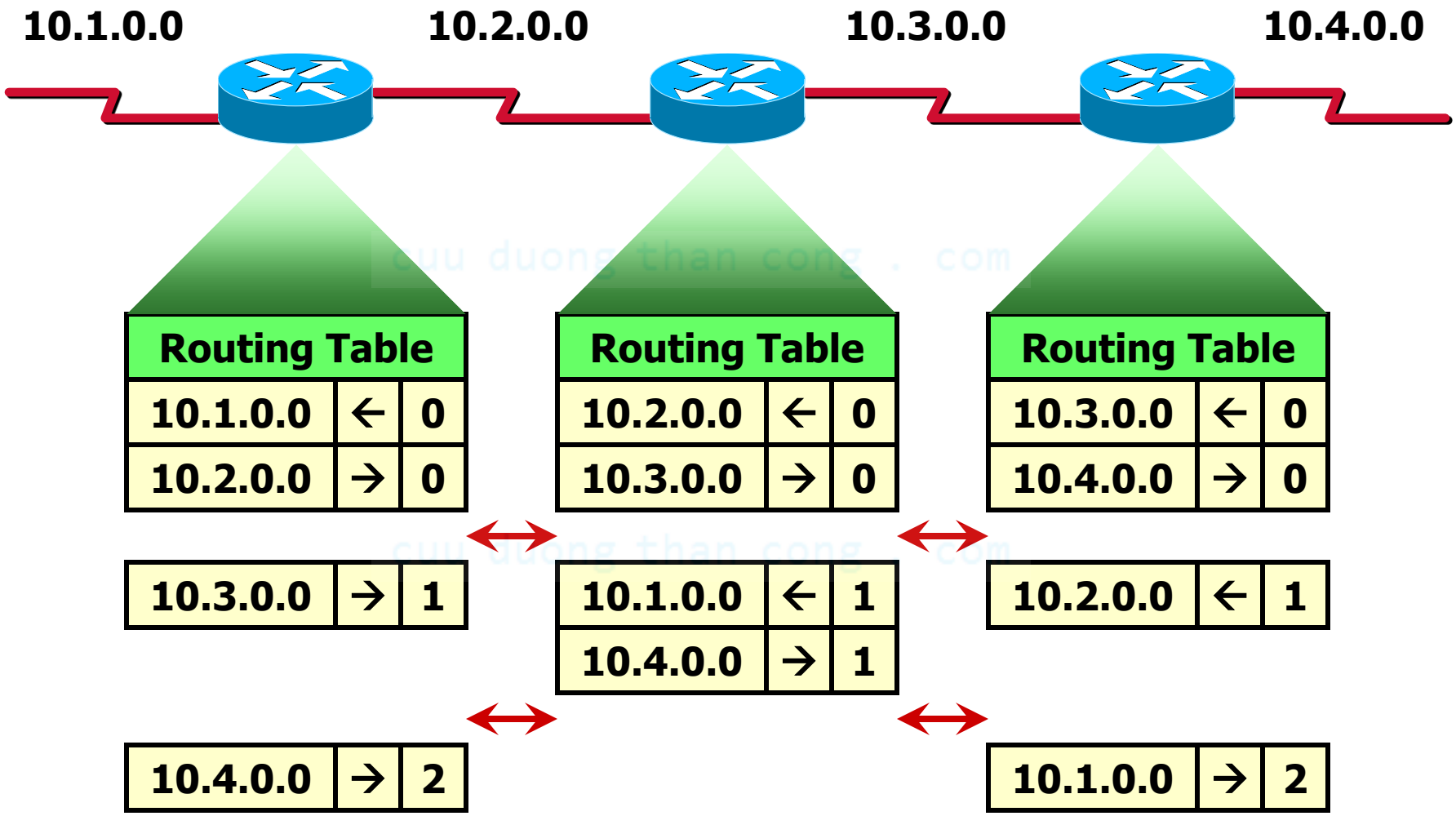
IGP vs. EGP



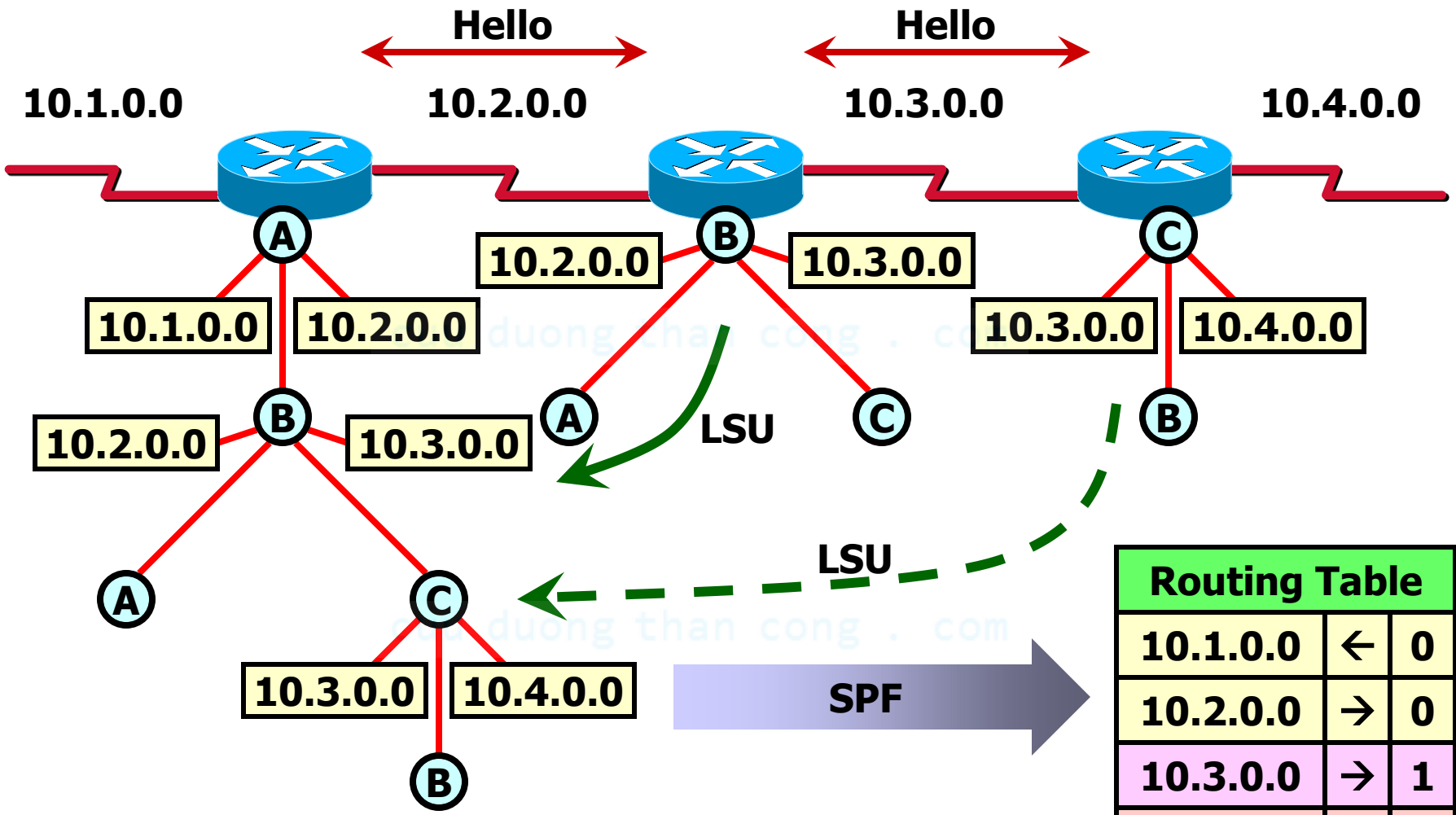
Link state and distance vector (classification #2)

- Most routing algorithms can be classified into one of two categories:
  - The distance vector routing approach determines the direction (vector) and distance to any link in the internetwork.
  - The link-state approach, also called shortest path first, recreates the exact topology of the entire internetwork.

Distance vector Routing Protocol



Link-state Routing Protocol Features



RIP

- 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.
- RIP Version 1 (RIPv1) requires that all devices in the network use the same subnet mask, is also known as classful routing.
- RIP Version 2 (RIPv2) is classless routing

IGRP and EIGRP

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

IS-IS

- Intermediate System-to-Intermediate System (IS-IS) is a link-state routing protocol used for routed protocols other than IP.
- Integrated IS-IS is an expanded implementation of IS-IS that supports multiple routed protocols including IP.

IS-IS

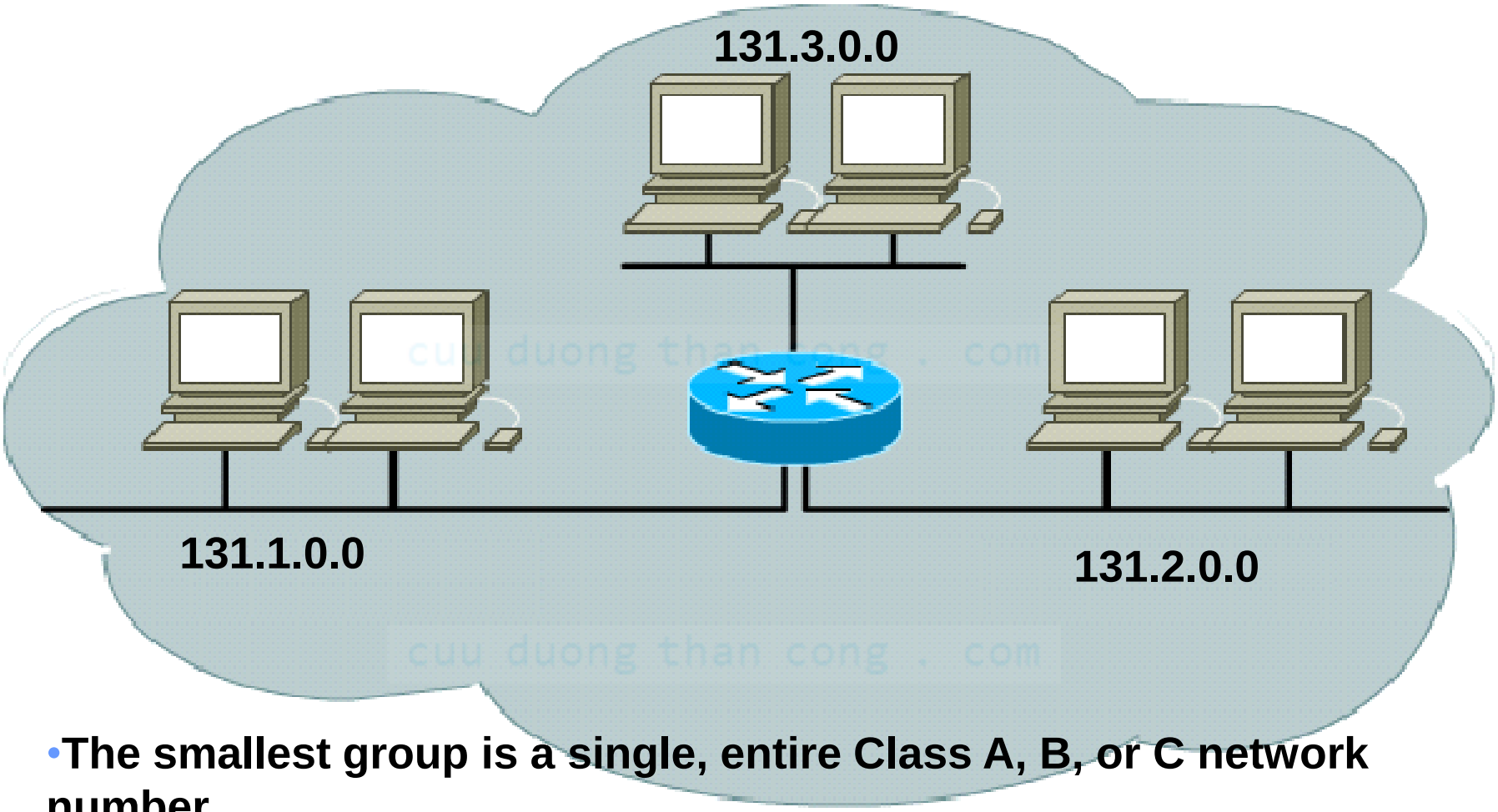
- Border Gateway Protocol (BGP)
  - is an EGP, exchanges routing information between autonomous systems while guaranteeing loop-free path selection.
  - BGP is the principal route advertising protocol used by major companies and ISPs on the Internet.
  - Unlike common IGPs, BGP does not use metrics. Instead, BGP makes routing decisions based on network policies, or rules using various BGP path attributes.

THE MECHANICS OF SUBNETTING

Why we need to divide network?

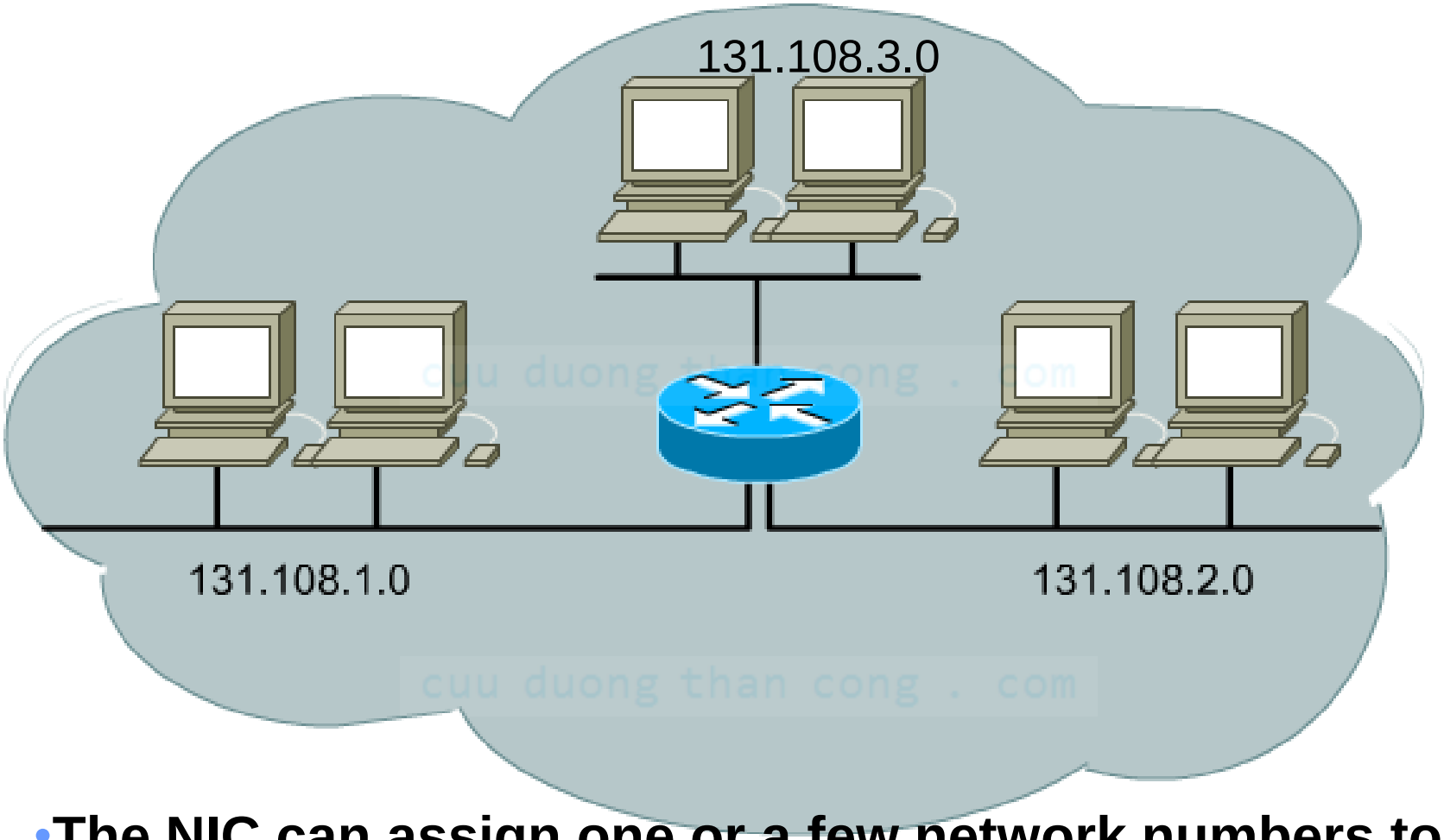
- Network administrators sometimes need to divide networks, especially large ones, into smaller networks:
  - Reduce the size of a broadcast domain.
  - Improve network security.
  - Implement the hierarchical managements.
- *So we need more network addresses for your network. But I want the outside networks see our network as a single network.*

Without subnet



- The smallest group is a single, entire Class A, B, or C network number.
- The NIC would be woefully short of assignable networks and NIC.

Divide network by three



- The NIC can assign one or a few network numbers to an organization, and then the organization can subdivide those networks into subnets of more usable sizes.

Subnetting

- To create a subnet address, a network administrator "borrows" bits from the original host portion and designates them as the subnet field.
- "Borrows" bits is always the leftmost host bit, the one closest to the last network octet.
- Subnet addresses include the Class A, Class B, or Class C network portion, plus a subnet field and a host field.
- Subnet addresses are assigned locally, usually by a network administrator.

Subnetting: Example

Class C Network address: 192.168.10.0			
11000000.	101010000.	00001010.	00000000
N .	N .	N .	H
11000000.	101010000.	00001010.	000**00000**
N .	N .	N .	sN H

Class B Network address: 132.10.0.0			
10000100.	00001010.	00000000.	00000000
N .	N .	N .	H
10000100.	00001010.	**00000**000	00000000
N .	N .	sN H.	H

Class A Network address: 10.0.0.0			
00001010.	00000000.	00000000.	00000000
N .	N .	N .	H
00001010.	**00000000.**	**0000**0000.	00000000
N .	sN .	sN H.	H

Establishing the subnet mask address

- "Extended Network Prefix".
- Give router the information to determines which part of an IP address is the network field and which part is the host field.
- 32 bits long, divided into four octets.
- Network and Subnet portions all 1's.
- Host portions all 0's.

Subnet mask: Example

Class C Network address: 192.168.10.100/255.255.255.0 (or /24)				
IP Address	11000000. N .	101010000. N .	00001010. N .	01100100 H
AND operation				
Default subnet Mask	11111111.	11111111.	11111111.	00000000
Network address	11000000.	101010000.	00001010.	00000000

Class A Network address: 10.0.160.13/255.255.240.0 (or /20)				
IP Address	00001010. N .	00000000. sN .	10100000. sN H.	00001101 H
AND operation				
Subnet Mask	11111111.	11111111.	11111111.	00000000
Network address	00001010.	00000000.	10100000.	00000000

AND operator

1 AND 1 = 1

1 AND 0 = 0

0 AND 1 = 0

0 AND 0 = 0

How many bits can I borrow?

- All of subnet bits are:
  - 0 : reserved for network address.
  - 1 : reserved for broadcast address.
- The minimum bits you can borrow is:
  - 2 bits.
- The maximum bits you can borrow is:
  - A: 22 bits ~ 2^{22} - 2 = 4.194.302 subnets.
  - B: 14 bits ~ 2^{14} - 2 = 16.382 subnets.
  - C: 06 bits ~ 2^{06} - 2 = 62 subnets.

cuu duong than cong . com

Before implement subnetting

you need to determine your current requirements and plan for future conditions. Follow these steps:

- 1. Determine the number of required subnet IDs.
  - A. One for each broadcast domain
  - B. One for each wide area network connection
- 2. Determine the number of required host IDs per subnet.
  - A. One for each TCP/IP host (pc, server, printer)
  - B. One for each router interface

Subnetting example

- Given network 172.16.0.0.
- We need 6 usable subnets and up to 8100 hosts on each subnet.

Calculating a subnet

1. Determine the subnet mask based on how many bits must to borrow.
2. Determine the subnets ID.
3. Determine the ranges of host address for each subnet. Choose the subnets that you want to use.
4. Determine the broadcast address for each subnet.

STEP 1a: subnet mask?

- Determine the Class of network
- → Class B
- Determine the default subnet mask
- → 255.255.0.0

STEP 1b: subnet mask?

- Number of subnets <= 2^n - 2 with n is number of bits that are borrowed.
- Number of hosts <= 2^m - 2 with m is number of bits that are remained.
- Determine how many bits to borrow from the host portion from requirement:
  - 8 subnets.
  - 1000 hosts on each subnet.

STEP 1c: subnet mask?

- Choose n = 4:
  - Number of possible subnets is:

$$2^4 - 2 = 14$$

  - Number of possible hosts on each subnet is:

$$2^{(16-4)} - 2 = 4094$$

- *Other choice n = 5 , n = 6 ?*

STEP 1d: subnet mask?

128	64	32	16	8	4	2	1	
1	0	0	0	0	0	0	0	= 128
1	1	0	0	0	0	0	0	= 192
1	1	1	0	0	0	0	0	= 224
1	1	1	1	0	0	0	0	= 240
1	1	1	1	1	0	0	0	= 248
1	1	1	1	1	1	0	0	= 252
1	1	1	1	1	1	1	0	= 254
1	1	1	1	1	1	1	1	= 255

- The subnet mask: 255.255.224.0.

STEP 2: Determine subnet ID usable?

- Determine the subnets from 3 borrowed bits from the host portion (last 2 bytes):
- 0 subnet: .000**00000**.00000000
- 1st subnet: .001**00000**.00000000(32=2^5)
- 2nd subnet: .010**00000**.00000000
- 3rd subnet: .011**0000**.00000000
- 4th subnet: .100**00000**.00000000
- 5th subnet: .101**00000**.00000000
- 6th subnet: .110**00000**.00000000(6x2^5)
- subnet: .111**00000**.00000000

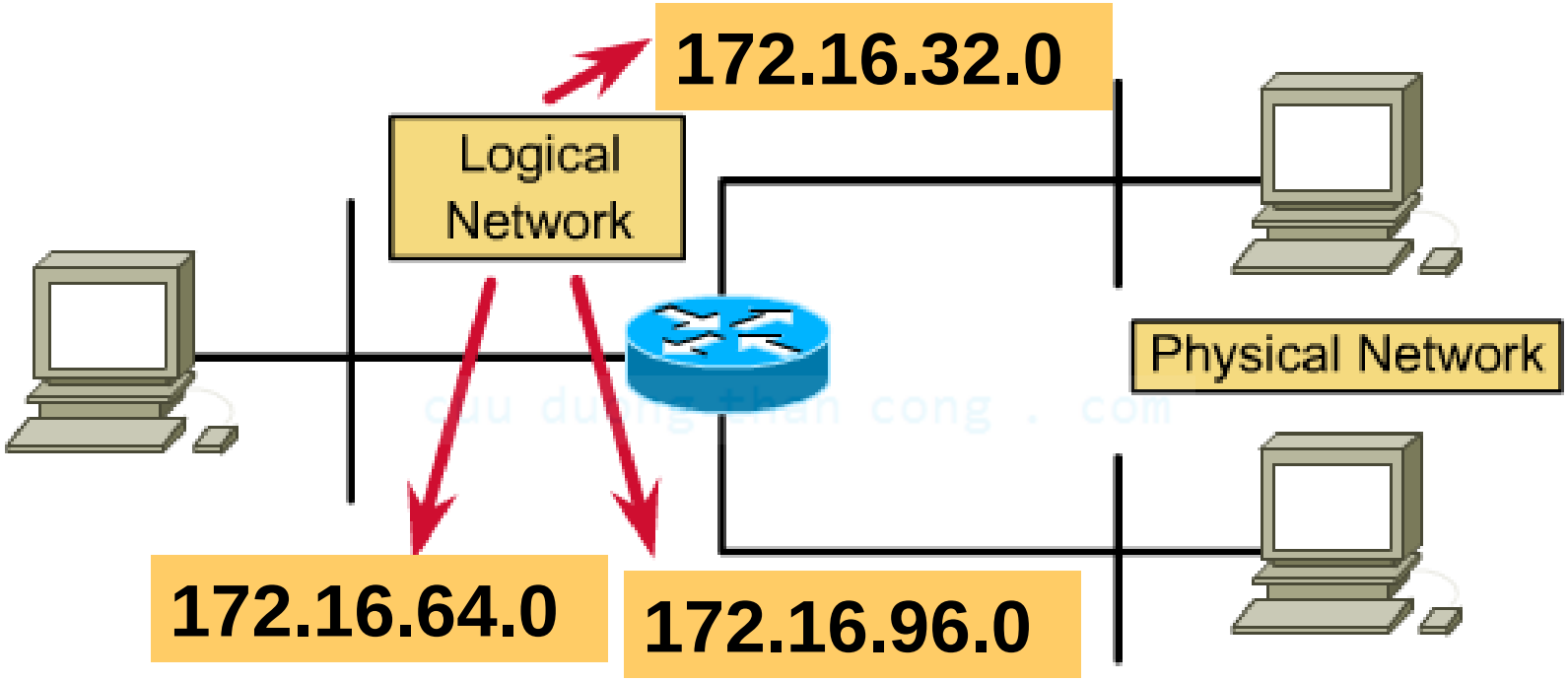
STEP 3: Determine range of host address

No	Sub-network address	Possible host address	Broadcast address	Use ?
0	172.16.0.0	.0.1 – .15.254	.31.255	N
1	172.16.32.0	.32.1 – .63.254	.63.255	Y
2	172.16.64.0	.64.1 –.95.254	.95.255	Y
3	172.16.96.0	.96.1 –.127.254	.127.255	Y
4	172.16.128.0	.128.1 –.159.254	.159.255	Y
5	172.16.160.0	.160.1 –.191.254	.191.255	Y
6	172.16.192.0	.192 –.223.254	.223.255	Y
7	172.16.224.0	.224.1 –.255.254	.255.255	N

STEP 4: Determine broadcast address?

- 1st = 32.0 63.255
- 2nd = 64.0 95.255
- 3rd = 96.0 127.255
- 4th = 128.0 159.255
- 5th = 160.0 191.255
- 6th = 192.0 223.255

Assign IP addresses



- Using subnets No.1 to No.6.
- Assign IP addresses to hosts and interfaces on each network. IP address configuration.

Addresses are loose by subnetting.

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%

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

Conclusion

- 1 Determine the subnet mask?
  - How many bits to borrow?
  - Number of subnets <= 2^n - 2 with n is number of "1" bits that are borrowed.
  - Number of hosts <= 2^m - 2 with m is number of "0" bits that are remained.
  - Fill "1" to borrow bits and convert to decimal.
- 2. Determine subnet ID usable for each segment?
  - $1^{st} = 2^m$
  - $2^{nd} = 2 \times 2^m$; $3^{rd} = ?$
  - Last = number of usable subnet x 2^m
- 3. Determine range of host IDs for each subnet?
  - Between subnet ID and broadcast address
- 4. Determine broadcast address for each subnet?
  - The number right before the next subnet is all host bits turned on

Summary

- An understanding of the following key points should have been achieved:
- Routed or routable protocol characteristics
- The steps of data encapsulation in an internetwork as data is routed to one or more Layer 3 devices
- Connectionless and connection-oriented delivery
- The IP packet fields
- Routers operate at the network layer. Initially, the router receives a Layer 2 frame with a Layer 3 packet encapsulated within it. The router must strip off the Layer 2 frame and examine the Layer 3 packet. When the router is ready to transmit the packet, the router then must encapsulate the Layer 3 packet in a new Layer 2 frame.
- Routed protocols define the format and use of the fields within a packet. Packets generally are conveyed from end system to end system.

Summary

- LAN switching occurs at Layer 2 of the OSI reference model, and routing occurs at Layer 3.
- Routing protocols are used between routers to determine paths and maintain routing tables. Routed protocols are used to direct user traffic.
- Routing involves two basic activities: determining the best routing paths and transporting packets through an internetwork.
- Routing algorithms process routing updates and populate the routing table with the best routes.
- Routing tables contain the best routes to all known networks. These routes can be either static routes, which are entered manually, or dynamic routes, which are learned through routing protocols.
- Convergence describes the speed at which all routers agree on a change in the network.

Summary

- Interior routing protocols route data within autonomous systems, while exterior routing protocols route data between autonomous systems.
- Routers using distance-vector routing protocols periodically send routing updates consisting of all or part of its routing table. Routers using link-state routing protocols use link-state advertisements (LSAs) to send updates only when topological changes occur in the network, and send complete routing tables much less frequently.
- The uses for subnetting
- How to determine the appropriate subnet mask for a given situation
- How to subnet Class A, B, and C networks
- How to use a subnet mask to determine the subnet ID

Q&A

Enjoy the Course