CCNA Semester 01

Chapter 02

OSI MODEL

Objective

- ✓ *Explains how standards ensure greater compatibility and interoperability between various types of network technologies.*
- ✓ *Learn how the OSI reference model networking scheme supports networking standards.*
- ✓ *Learn about the basic functions that occur at each layer of the OSI model, which will serve as a foundation as you begin to design, build and troubleshoot networks.*

Table of Content

NETWORK TRAINING CENTER

MODEL OF COMMUNICATION

Networking History

- Standalone Device.
  - Duplication of equipments and resources.
  - Inability to communicate efficiently.
  - Lack of networking management.
- LAN.
  - Connects devices that are close together.
- WAN.
  - Interconnects LANs across a large area.

Analyzing network in layers

NETWORK TRAINING CENTER

What is flowing ?
Data

What different forms flow ?
Text, Graphic, Video ...

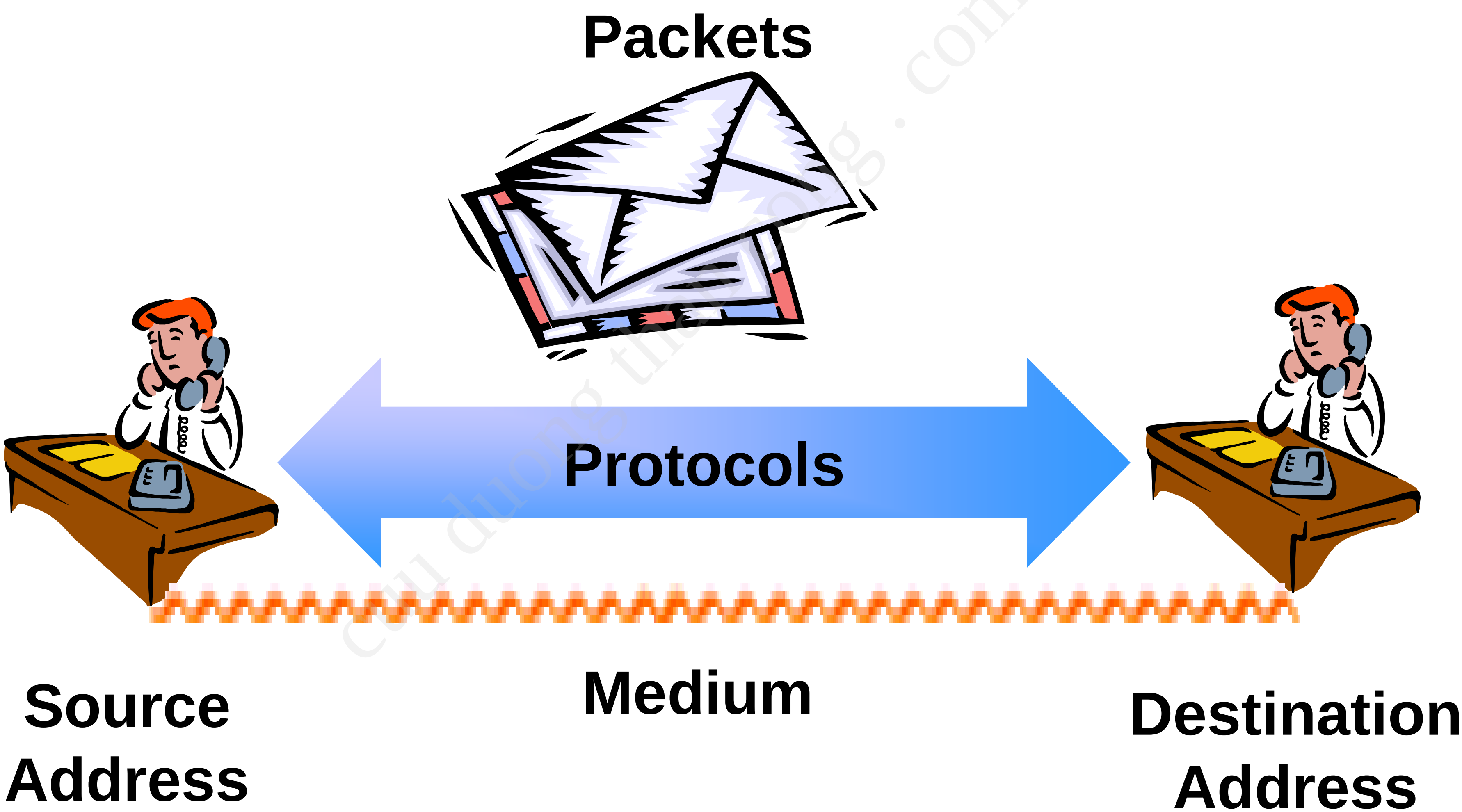
What rules govern flow ?
Standard, Protocol ...

Where does the flow occur ?
Cable, Atmosphere ...

Communication

- Transmission of information.
- Examples:
  - Speaking.
  - Smoke signal.
  - Body language.
  - Morse.
  - Telephone.
  - Broadcast systems (radio, television).
  - Internet

Communication process



Communication characteristics

- Addresses
  - Who are the source and the destination of a communication process?
- Media
  - Where is the communication take place?
- Protocols
  - How to make the communication process effectively?

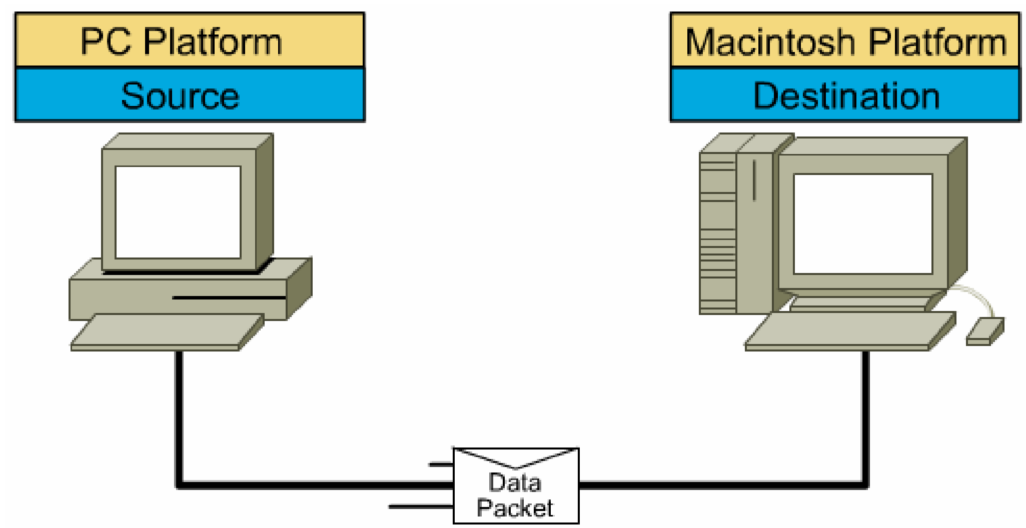
Communication: Human conversation

NETWORK TRAINING CENTER

- Address
  - Hello Mr.A, I am B
- Media
  - Atmosphere
- Protocol
  - Language
  - Speed
  - Handshaking

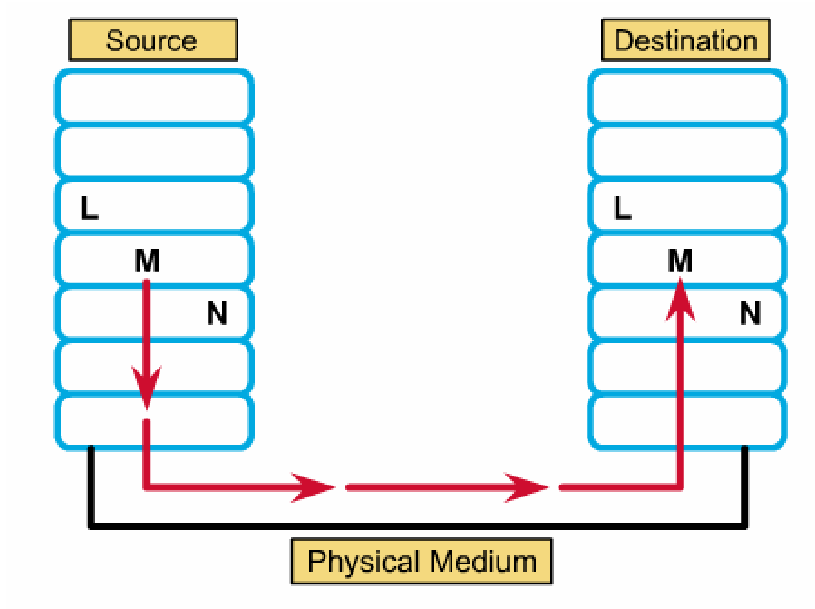
Data Communication

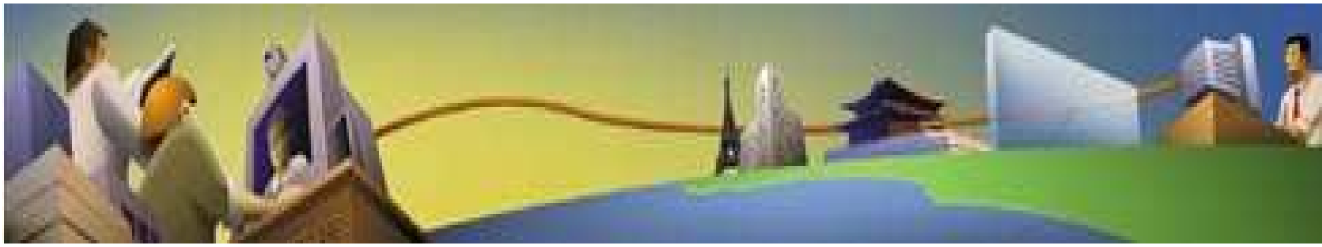
- Address
  - Source address, Destination address
- Media
  - Cable, Fiber, Atmosphere
- Protocol
  - Format
  - Procedure



Protocol

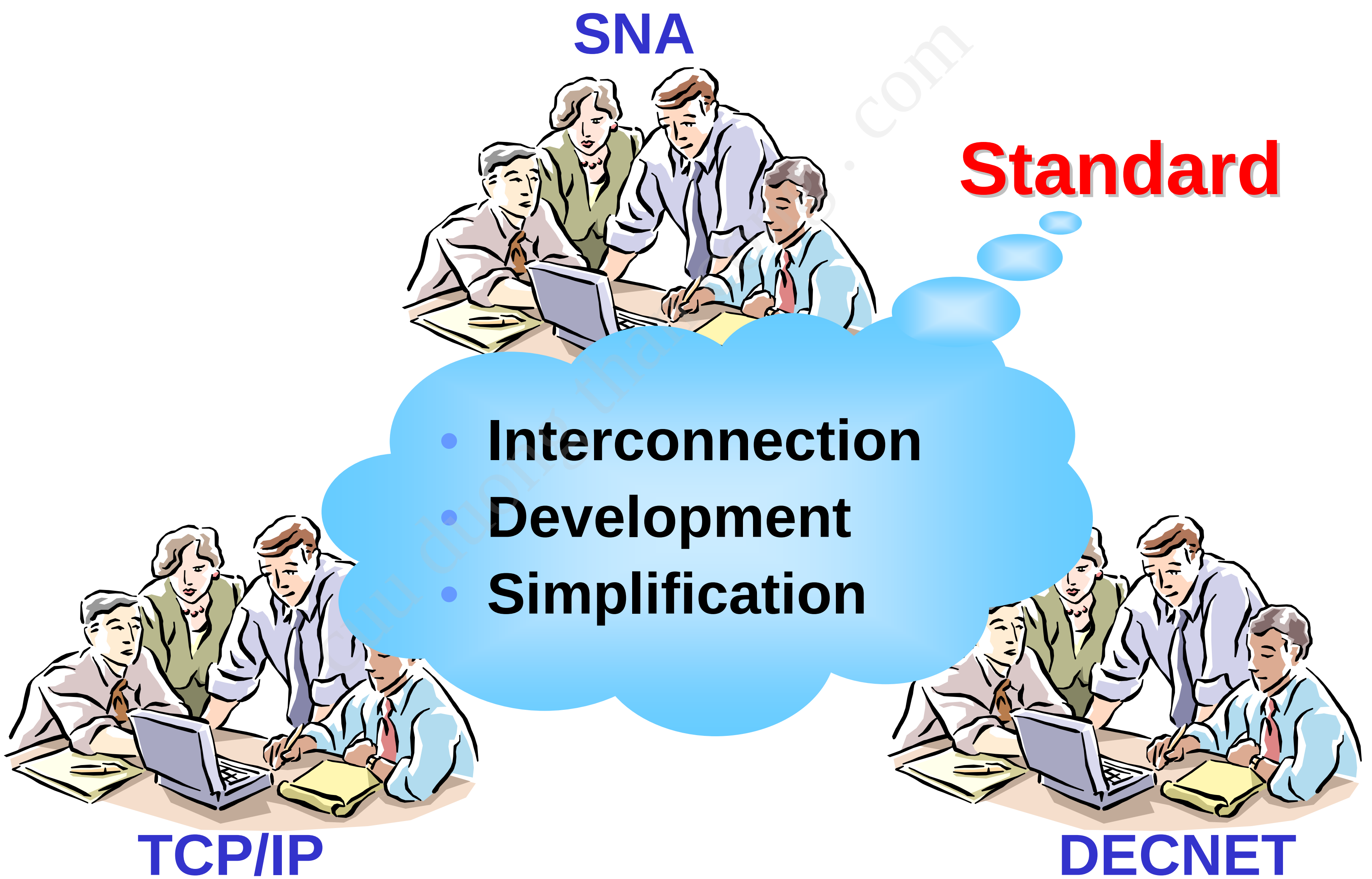
- Protocol is a set of rules, or an agreement, that determines the format and transmission of data that make communication on a network more efficient.





OSI MODEL

Evolution of networking standards



OSI model development

- Researched and developed by the ISO - *International Organization for Standardizations.*
- 1977: establish a subcommittee to develop a communications architecture.
- 1984: publish ISO-7498, the Open System Interconnection (OSI) **reference model**.

OSI model

- The OSI model: a framework within which networking standards can be developed.
  - *It provided vendors with a set of standards that ensured greater compatibility and interoperability between the various types of network technologies that were produced by the many companies around the world.*

Proprietary vs. Open

A layered model

- The communications functions are partitioned into a hierarchical set of layers.
- Each layer performs a related subset of the functions required to communicate.
- Each layer relies on the next lower layer to perform more primitive functions and provides services to the next higher layer.

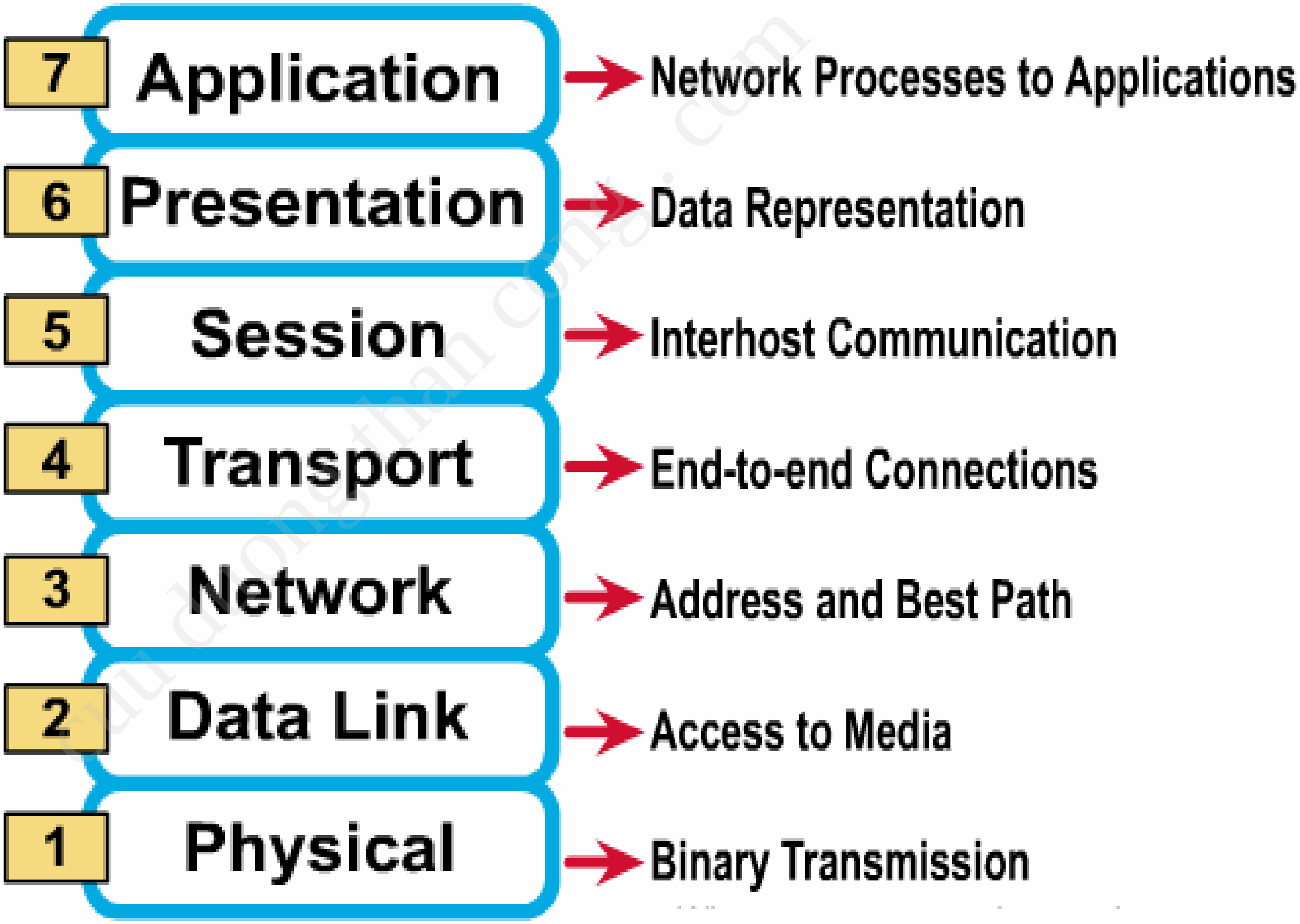
→ *The OSI Model define a set of layers and the services performed by each layer*

Why a layered model?

- Reduces complexity.
- Standardizes interfaces.
- Facilitates modular engineering.
- Ensures interoperable technology.
- Accelerates evolution.
- Simplifies teaching and learning.

7 layers of the OSI reference model

- Layer 7:
- Layer 6:
- Layer 5:
- Layer 4:
- Layer 3:
- Layer 2:
- Layer 1:



- *All People Seem To Need Data Processing*

The physical layer

- Transmission of an unstructured bit stream over a physical link between end systems.
  - Electrical, mechanical, procedural and functional specifications
  - Physical data rate
  - Distances
  - Physical connector

The data-link layer

- Provides for the reliable transfer of data cross a physical link.
  - Frames
  - Physical address
  - Network topology
  - Synchronization
  - Error control
  - Flow control

The network layer

- Provides connectivity and path selection between two host systems that may be located on geographically separated networks.
  - Packets
  - Route, routing table, routing protocol
  - Logical address
  - Fragmentation

The transport layer

NETWORK TRAINING CENTER

- Provides reliable, transparent transfer of data over networks.
  - Segments, data stream, datagram
  - Connection oriented and connectionless
  - End-to-end flow control
  - Error detection and recovery
  - Segmentation & reassembly

The session layer

- Establishes, manages, and terminates sessions between two communicating hosts.
  - Sessions
  - Dialog
  - Conversations
  - Data exchange

The presentation layer

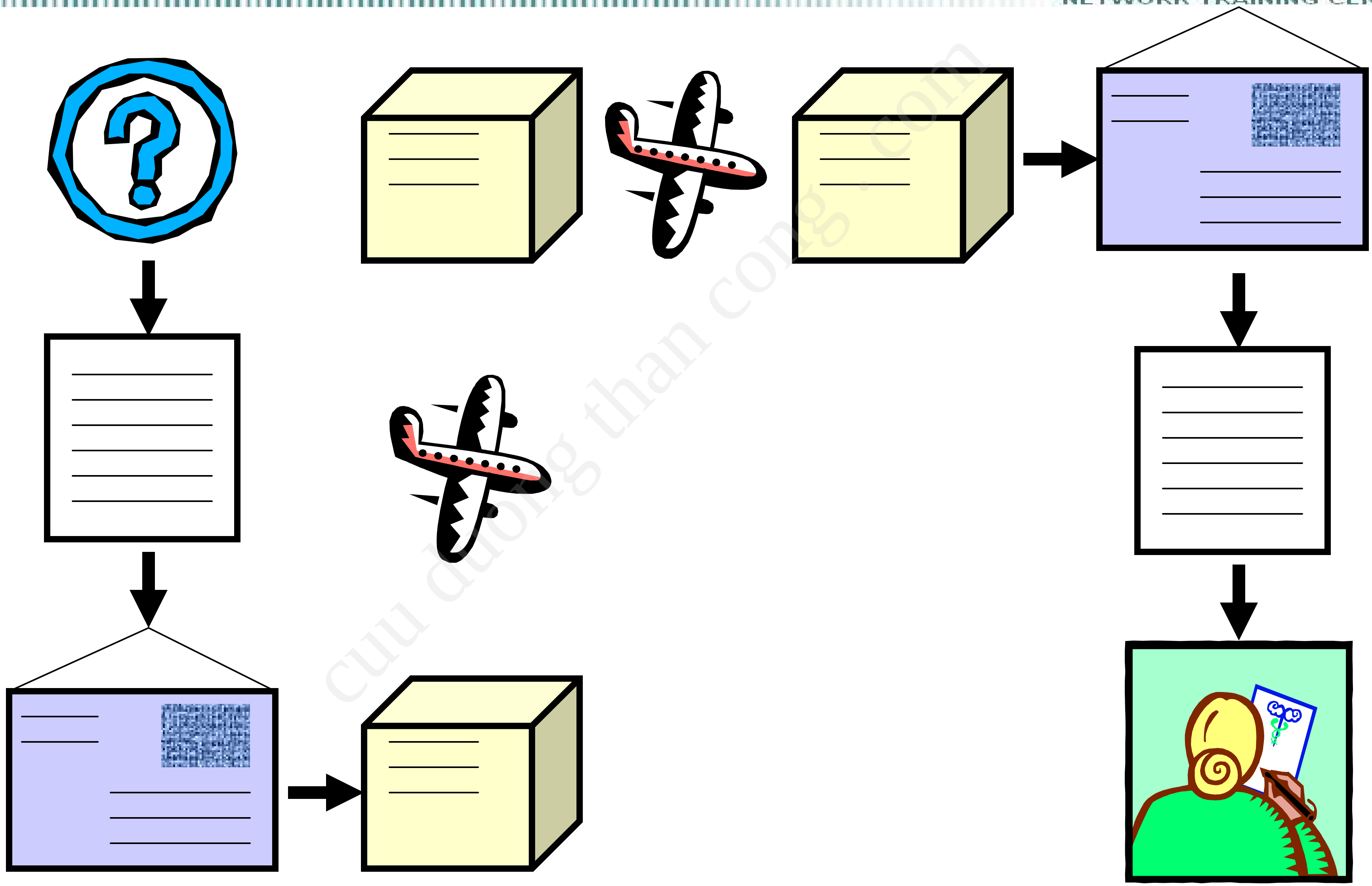
NETWORK TRAINING CENTER

- Ensures that the information that the application layer of one system sends out is readable by the application layer of another system.
  - Format of data
  - Data structure
  - Data conversion
  - Data compression
  - Data encryption

The application layer

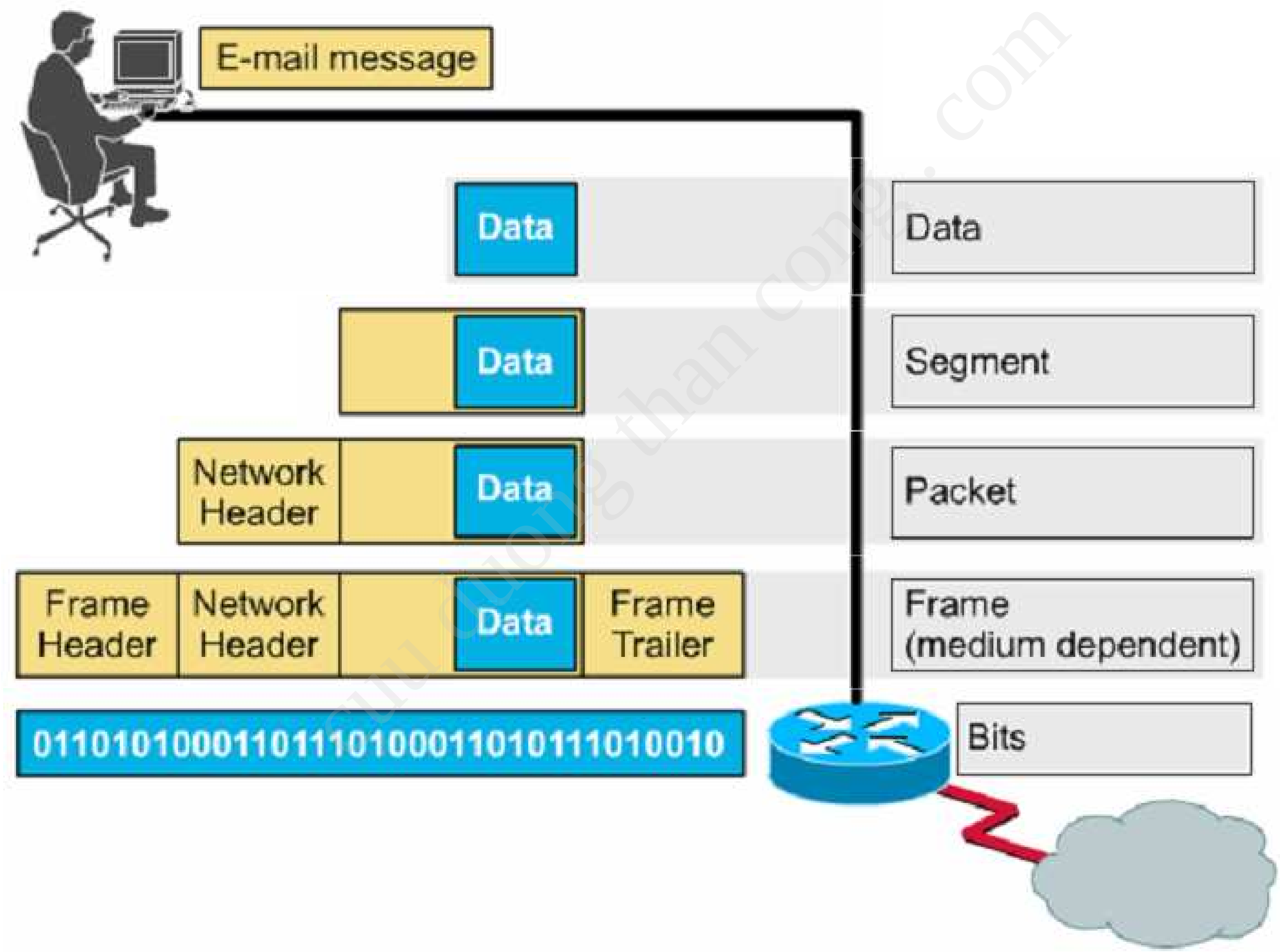
- Is the OSI layer that is closest to the user; it provides network services to the user’s applications.
  - File transfer
  - Electronic mail
  - Terminal access
  - Word processing
  - Intended communication partners

Encapsulation example: Air-mail



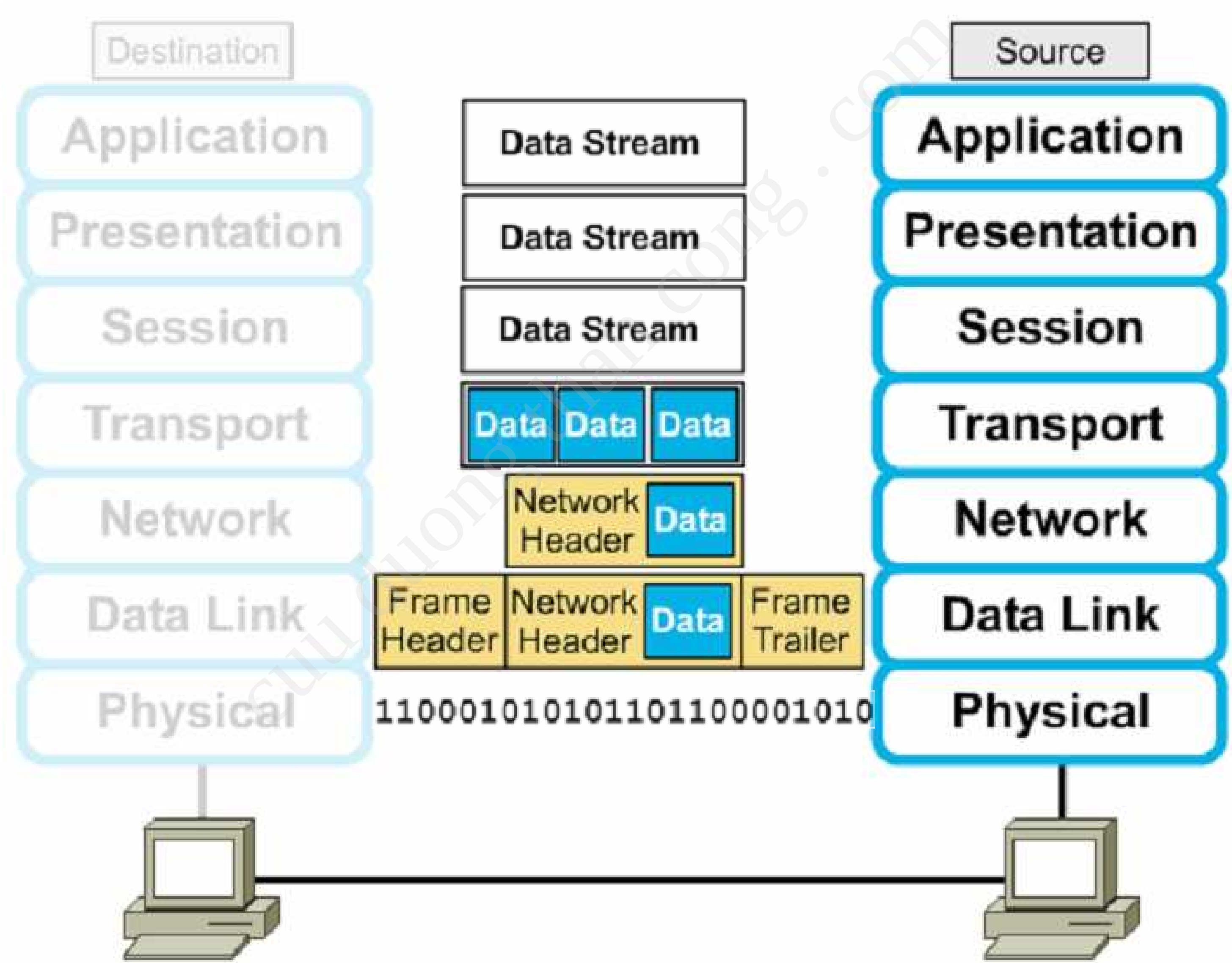
Encapsulation example: E-mail

NETWORK TRAINING CENTER

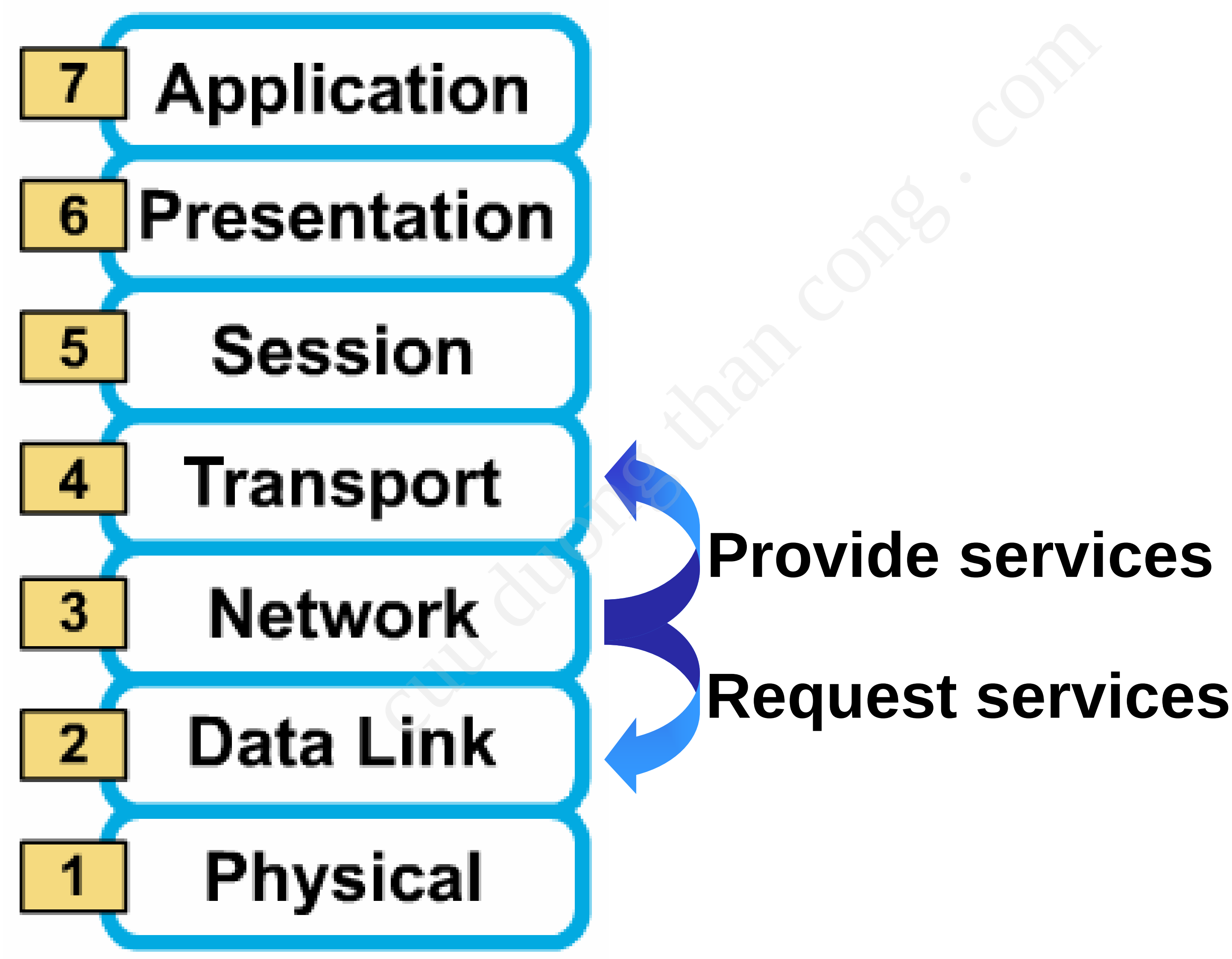


Encapsulation

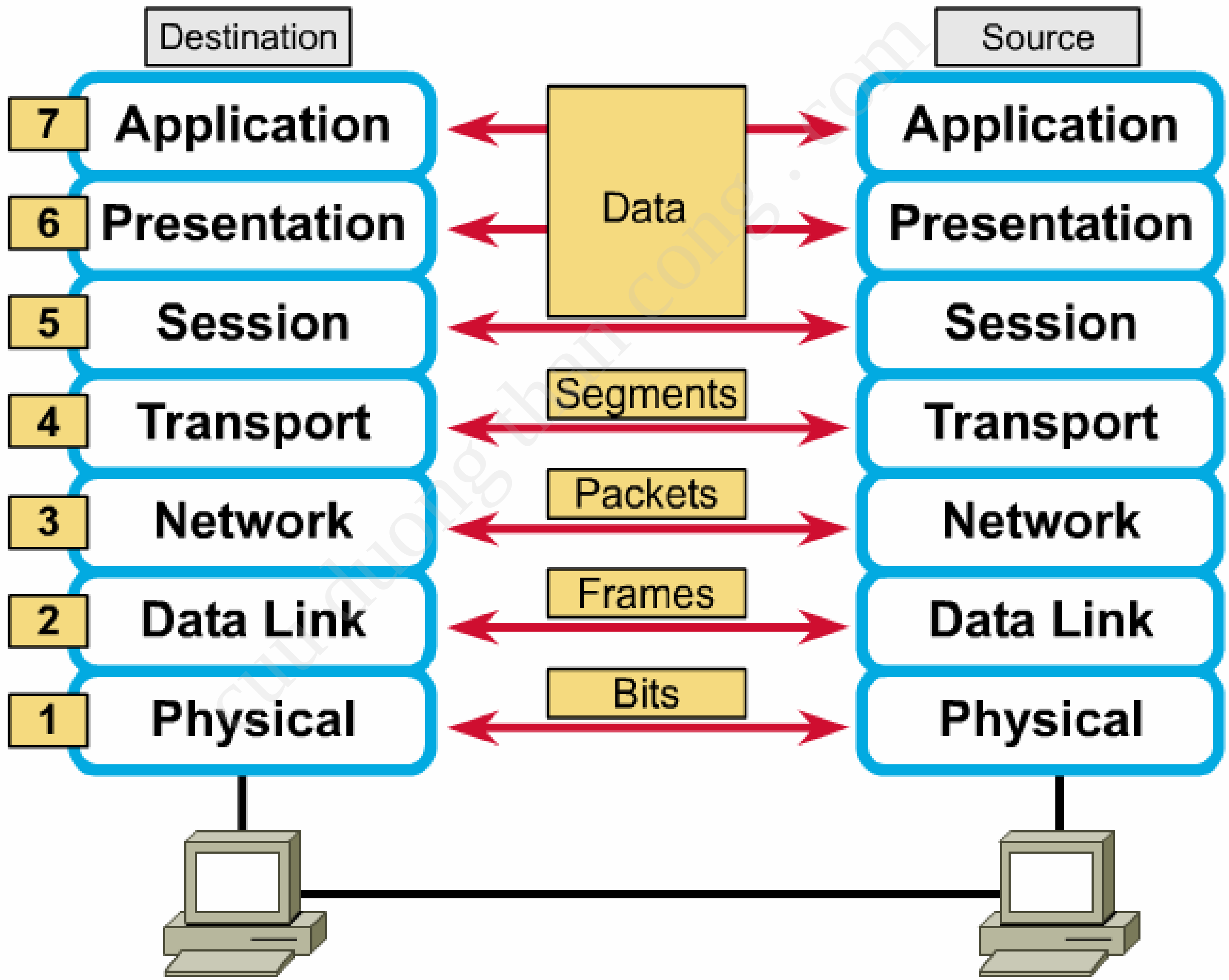
NETWORK TRAINING CENTER



Layer-to-layer communications



Peer-to-peer communications



Protocols

- Is a formal set of rules and conventions that governs how computers exchange information over a network medium.
- Implements the functions of one or more of the OSI layers.
- A communication protocol is concerned with exchanging data between two peer layers.
- Protocol Data Units (PDUs) : Block of data that a protocol exchange.

TCP/IP MODEL

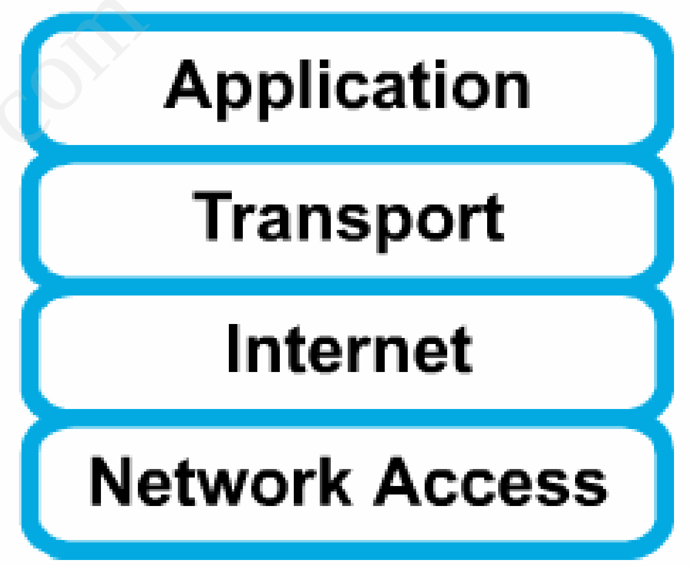
TCP/IP model development

NETWORK TRAINING CENTER

- The late-60s The Defense Advance Research Projects Agency (DARPA) originally developed Transmission Control Protocol/Internet Protocol (TCP/IP) to interconnect various defense department computer networks.
- The Internet, an International Wide Area Network, uses TCP/IP to connect networks across the world.

4 layers of the TCP/IP model

- Layer 4: Application
- Layer 3: Transport
- Layer 2: Internet
- Layer 1: Network access



It is important to note that some of the layers in the TCP/IP model have the same name as layers in the OSI model.
Do not confuse the layers of the two models.

The network access layer

- Concerned with all of the issues that an IP packet requires to actually make the physical link. All the details in the OSI physical and data link layers.
  - Electrical, mechanical, procedural and functional specifications.
  - Data rate, Distances, Physical connector.
  - Frames, physical addressing.
  - Synchronization, flow control, error control.

The internet layer

- Send source packets from any network on the internetwork and have them arrive at the destination independent of the path and networks they took to get there.
  - Packets, Logical addressing.
  - Internet Protocol (IP).
  - Route , routing table, routing protocol.

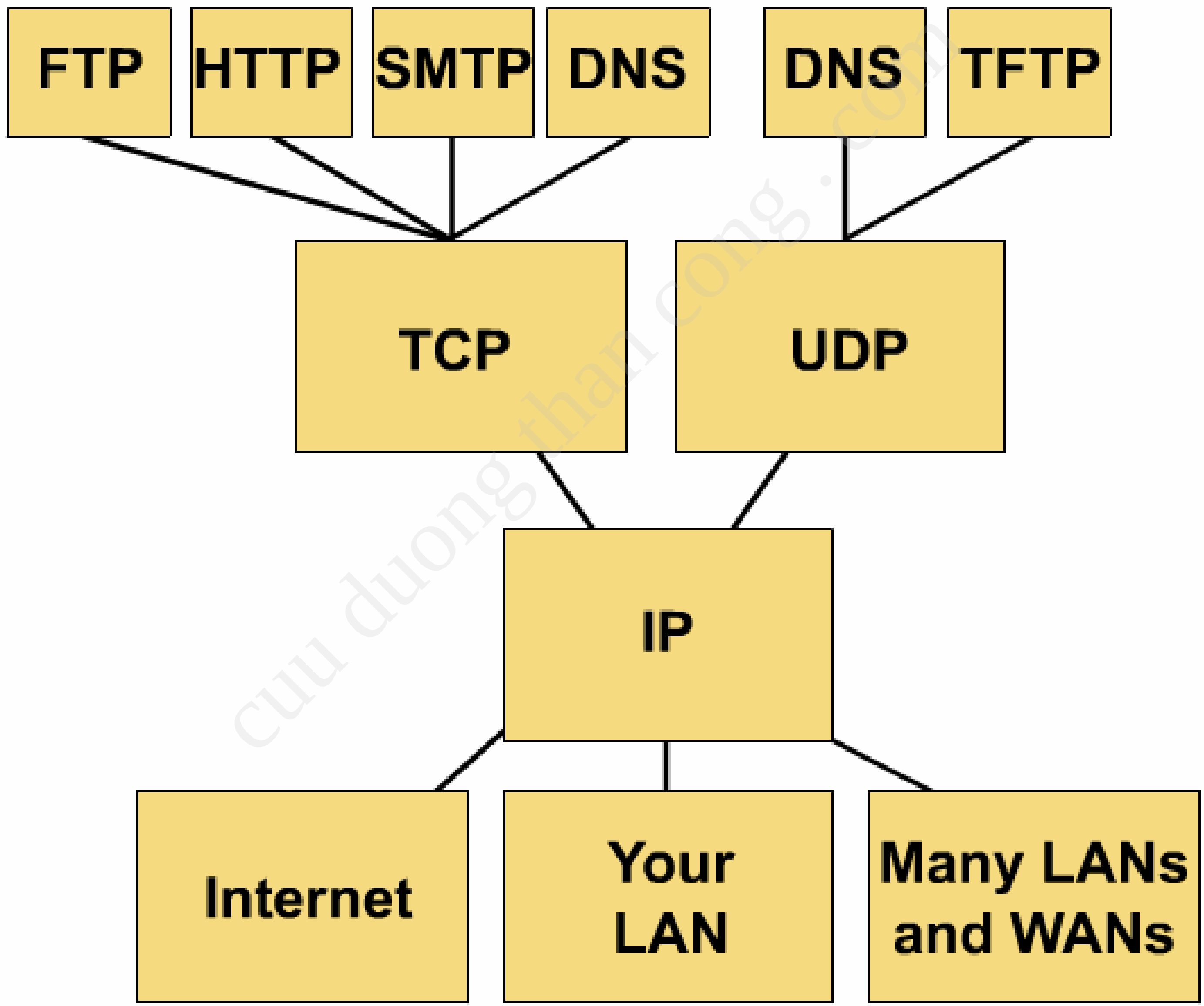
The transport layer

- The transport layer deals with the quality-of-service issues of reliability, flow control, and error correction.
  - Segments, data stream, datagram.
  - Connection oriented and connectionless.
  - Transmission control protocol (TCP).
  - User datagram protocol (UDP).
  - End-to-end flow control.
  - Error detection and recovery.

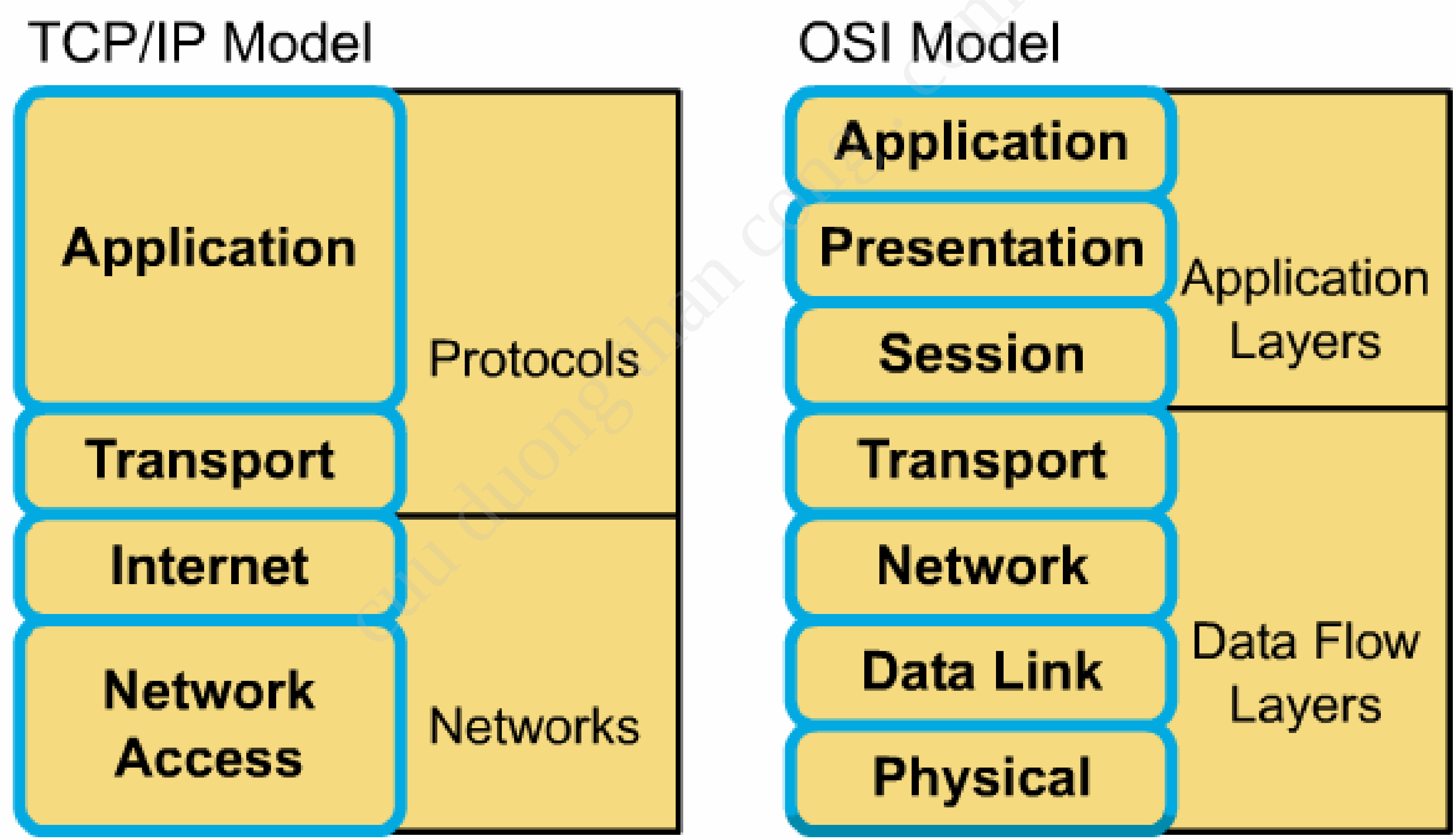
The application layer

- Handles high-level protocols, issues of representation, encoding, and dialog control.
- The TCP/IP combines all application-related issues into one layer, and assures this data is properly packaged for the next layer.
  - FTP, HTTP, SMNP, DNS ...
  - Format of data, data structure, encode …
  - Dialog control, session management …

TCP/IP protocol stack



Comparing TCP/IP with OSI



Comparing TCP/IP with OSI (cont.)

Similarities:

- Both have layers.
- Both have application layers, though they include very different services.
- Both have comparable transport and network layers
- Packet-switched technology is assumed.
- Networking professionals need to know both.

Comparing TCP/IP with OSI (cont.)

Differences:

- TCP/IP combines the presentation and session layer issues into its application layer.
- TCP/IP combines the OSI data link and physical layers into one layer.
- TCP/IP appears simpler because it has fewer layers.
- Typically networks aren't built on the OSI protocol, even though the OSI model is used as a guide.

Focus of the CCNA curriculum

The OSI Model

7	Application	FTP, TFTP, HTTP, SMTP, DNS, TELNET, SNMP
6	Presentation	Very little focus
5	Session	
4	Transport	TCP (the Internet)
3	Network	IP (the Internet)
2	Data Link	Ethernet (common LAN technology)
1	Physical	

Q&A

CCNA Semester 01

The **Cisco Certified Network Associate** Curriculum

Chapter 03

LAN – WAN

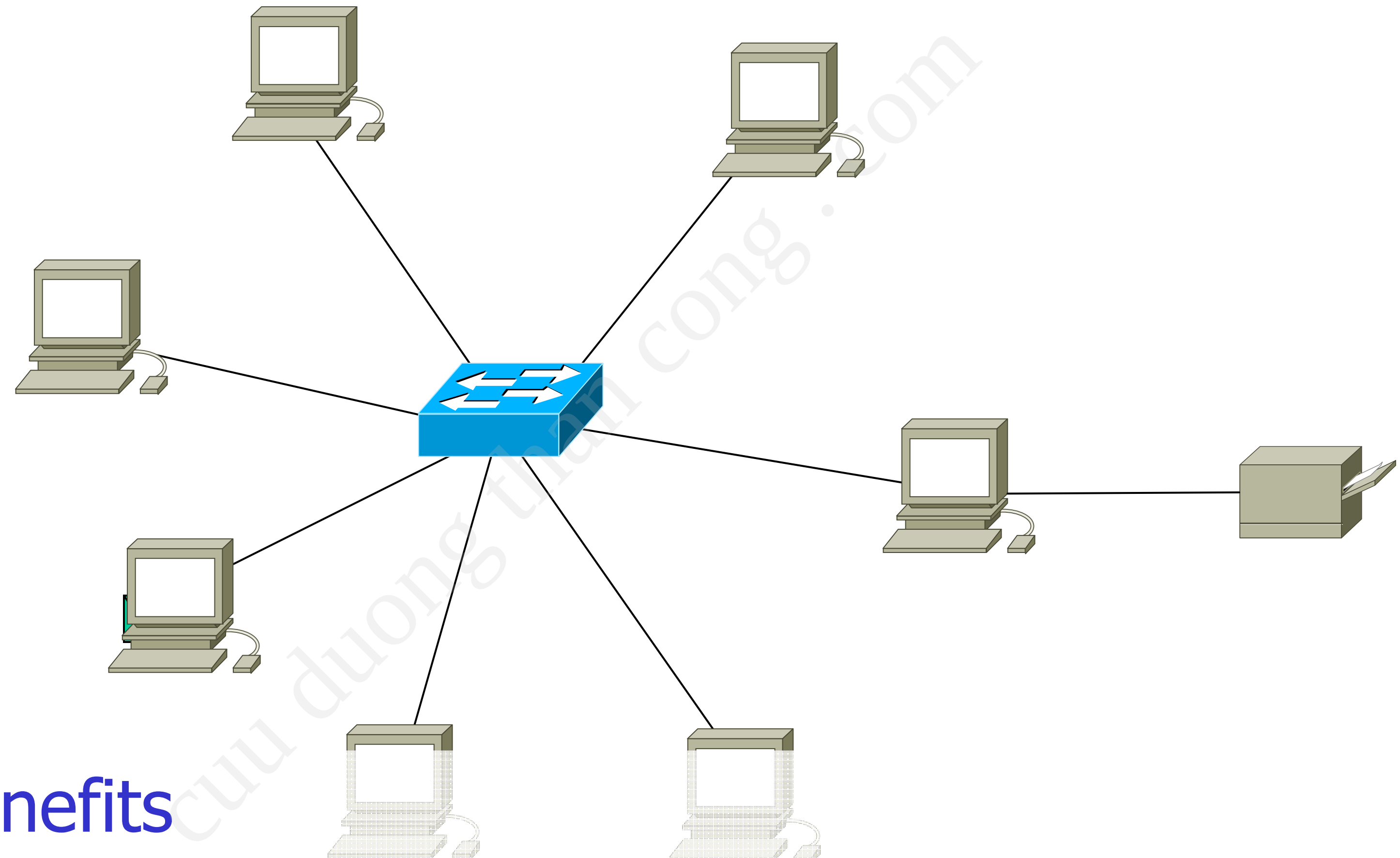
Objectives

- ✓ *Learn about basic LAN devices and the evolution of networking devices.*
- ✓ *Learn about the networking devices that operate at each layer of the OSI model and how packets flow through each device as they go through the layers of the OSI model.*
- ✓ *Define LAN, WAN, MAN, and SAN*
- ✓ *Explain VPNs and their advantages*
- ✓ *Describe the differences between intranets and extranets*
- ✓ *Bandwidth*

Table of Content

NETWORK TRAINING CENTER

Local Area Network



LAN benefits

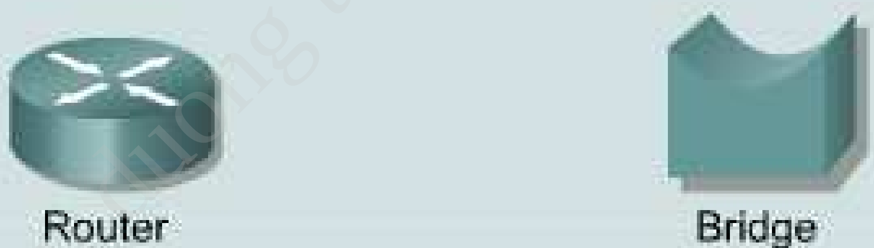
- Avoid duplication of equipment and resources
- Allow user in the department quickly transfer files
- Increase productivity while saving money

Local-area Networks (LANs)

LANS are designed to:

- Operate within a limited geographic area
- Allow multi-access to high-bandwidth media
- Control the network privately under local administration
- Provide full-time connectivity to local services
- Connect physically adjacent devices

Using:



Some common LAN technologies are:

- Ethernet
- Token Ring
- FDDI

Wide-area Networks (WANs)

NETWORK TRAINING CENTER

WANS are designed to:

- Operate over a large geographical area
- Allow access over serial interfaces operating at lower speeds
- Provide full-time and part-time connectivity
- Connect devices separated over wide, even global areas

Using:

Router

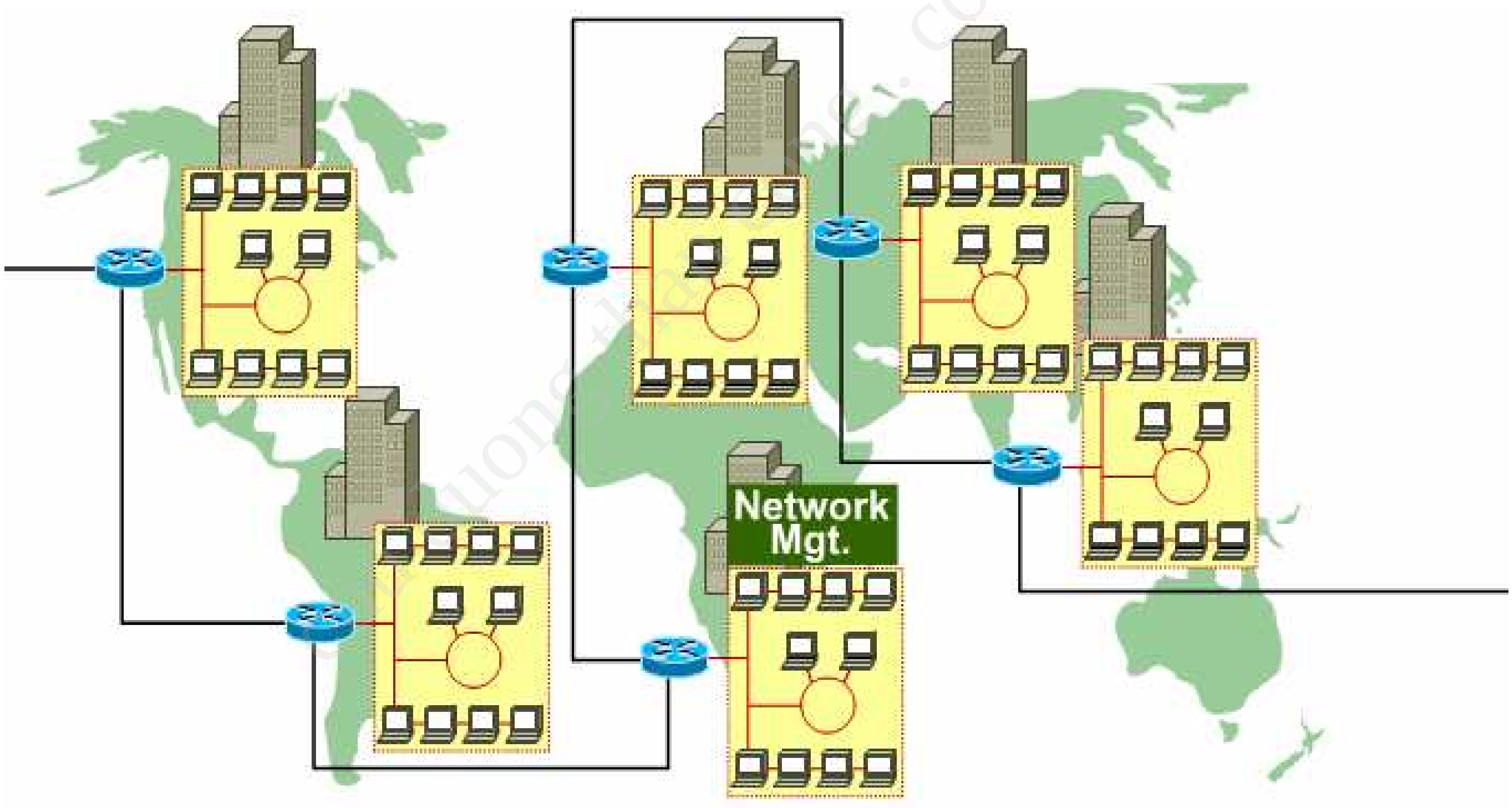
Communication Server

Modem CSU/DSU TA/NT1

Some common WAN technologies are:

- Modems
- Digital Subscriber Line (DSL)
- Frame Relay
- Integrated Services Digital Network (ISDN)
- T1 (1.544 Mbps), E1 (2.048 Mbps)

WAN: Wide Area Network



Examples of Data Networks

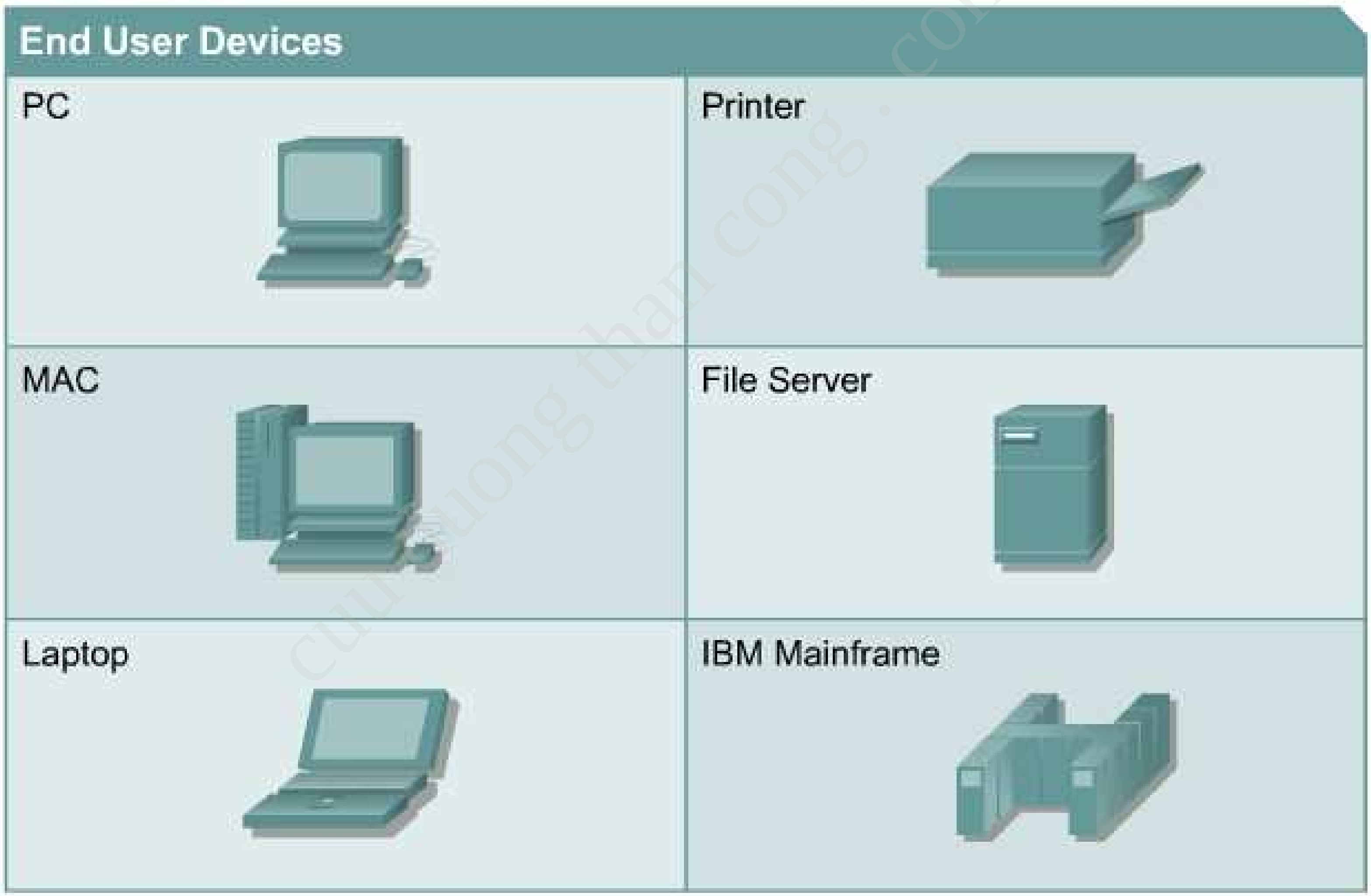
NETWORK TRAINING CENTER

Distance Between CPUs	Location of CPUs	Name
0.1 m	Printed circuit board Personal data asst.	Motherboard Personal area network (PAN)
1.0 m	Millimeter Mainframe	Computer systems network
10 m	Room	Local area network (LAN) Your classroom
100 m	Building	Local area network (LAN) Your school
1000 m = 1 km	Campus	Local area network (LAN) Stanford University
100,000 m = 100 km	Country	Wide area network (WAN) Cisco Systems, Inc.
1,000,000 m = 1,000 km	Continent	Wide area network (WAN) Africa
10,000,000 m = 10,000 km	Planet	Wide area network (WAN) The Internet
100,000,000 m = 100,000 km	Earth-moon system	Wide area network (WAN) Earth and artificial satellites

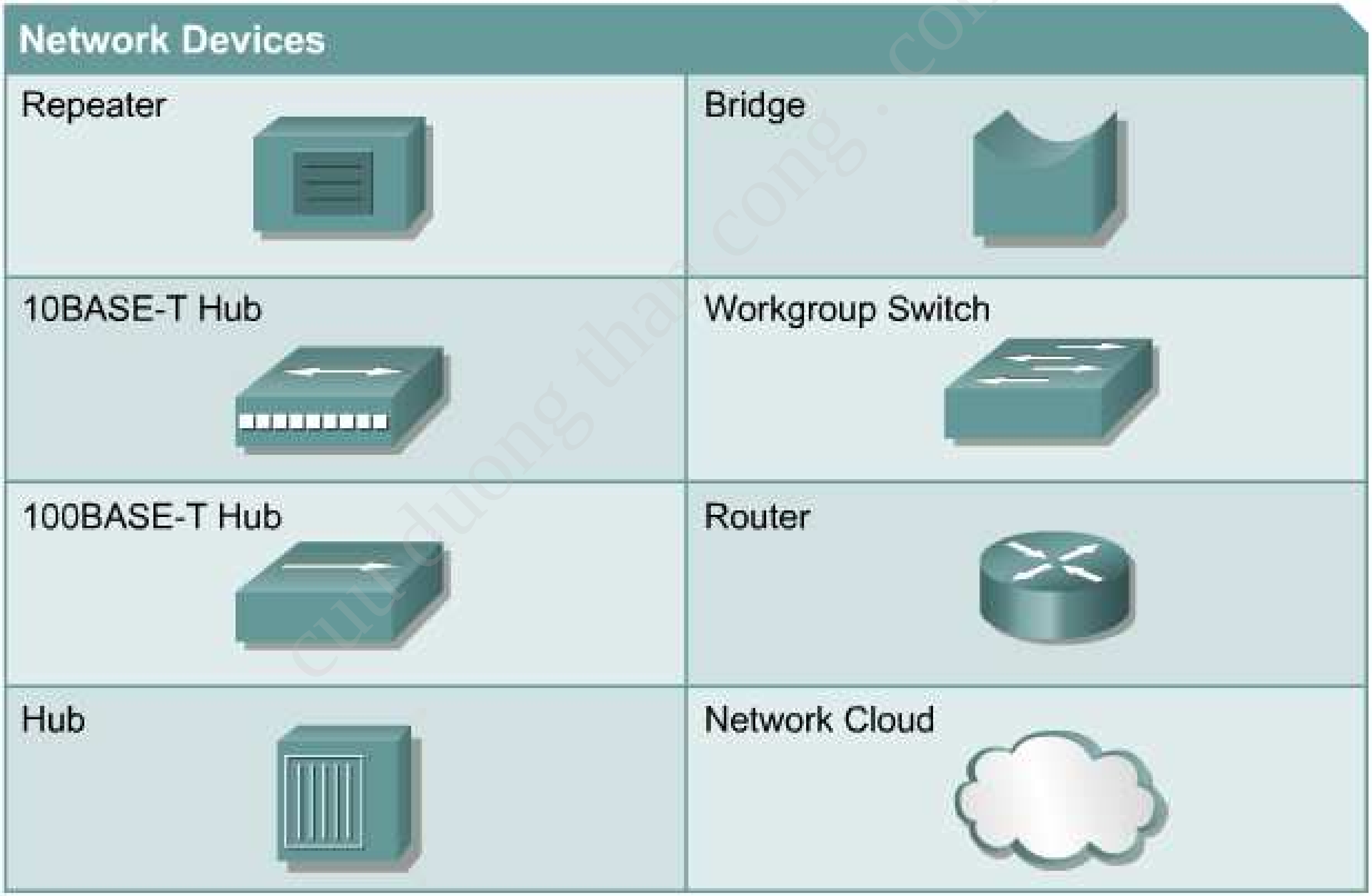
Networking Devices

- Equipment that connects to a network segment is called a **device**
- These devices are broken into two classifications
  - **End user devices**—Includes computers, printers, scanners
  - **Network devices**—Includes devices that connect the end-user devices to allow them to communicate

End User Devices



Network Devices

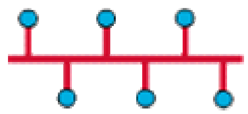


BASIC LAN DEVICES

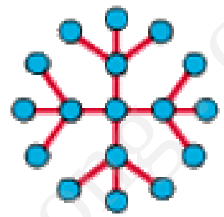
Physical & Logical Topologies

- Physical topologies
  - Define the actual layout of the wire (media)
- Logical topologies
  - Define how the media is accessed by the hosts

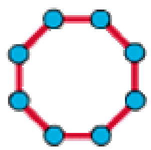
Physical Topologies



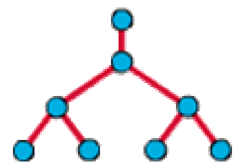
Bus



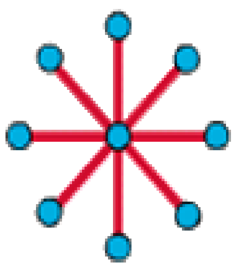
Extended Star



Ring



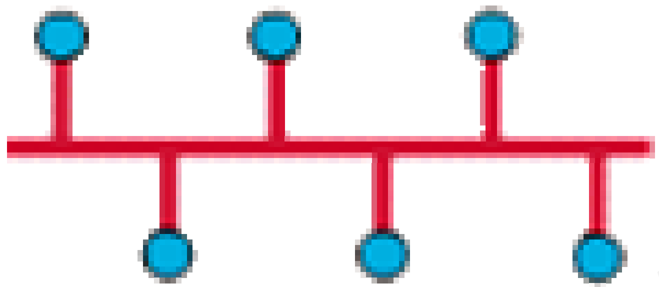
Hierarchical



Star

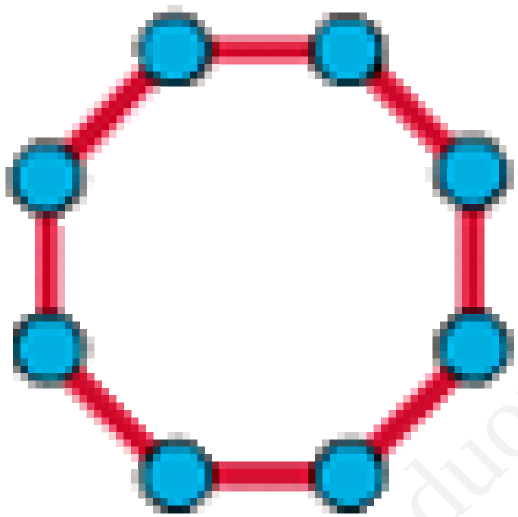
Mesh

Physical Topology: Bus



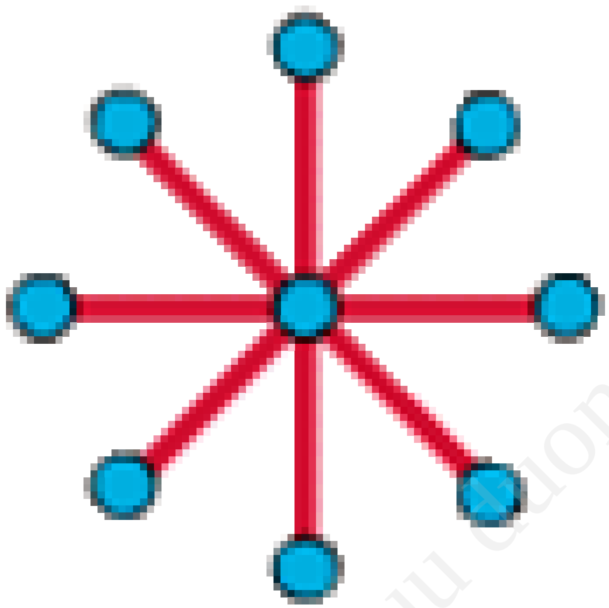
- Single backbone
- All hosts directly connected to backbone
- Each end of the bus must be properly terminated

Physical Topology: Ring



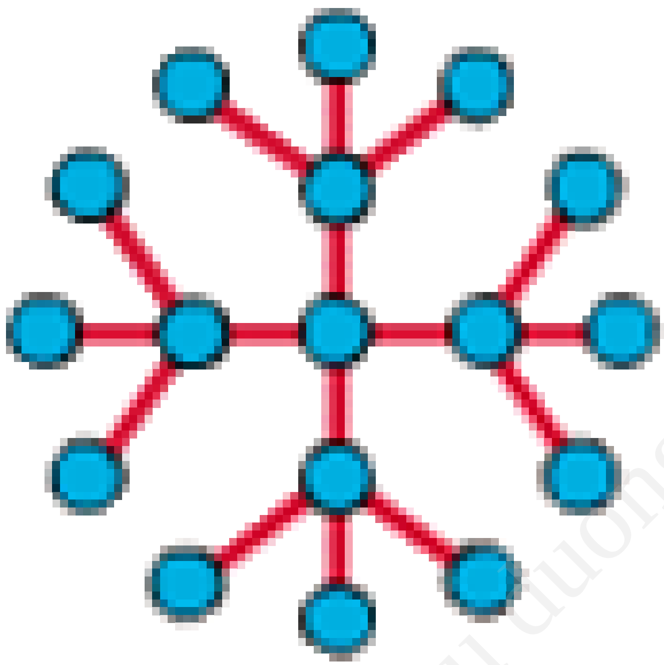
- No backbone
- A host is directly connected to each of its neighbors

Physical Topology: Star



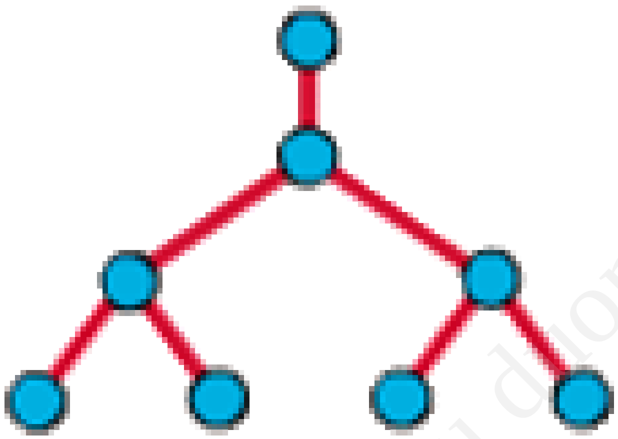
- All devices connected to a central point
- Center of star is usually a hub or a switch

Physical Topology: Extended Star



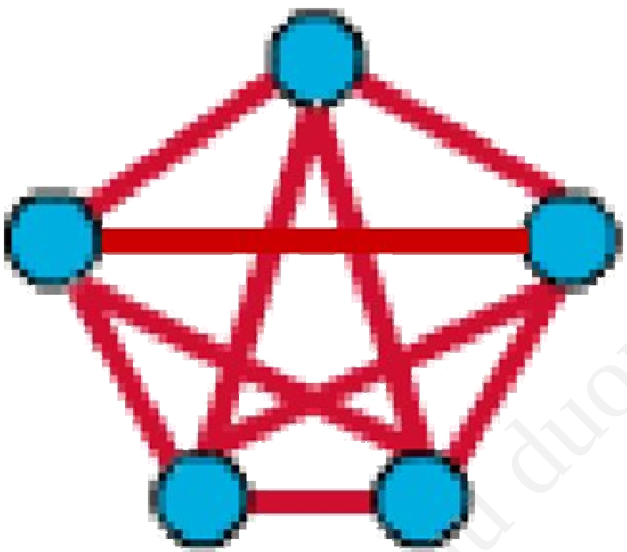
- Connects individual star topologies together.
- At the center of the star is a hub or a switch.
- Extends the length and size of the network.

Physical Topology: Hierarchical



- Like the extended star except a computer controls traffic (not a hub or a switch).

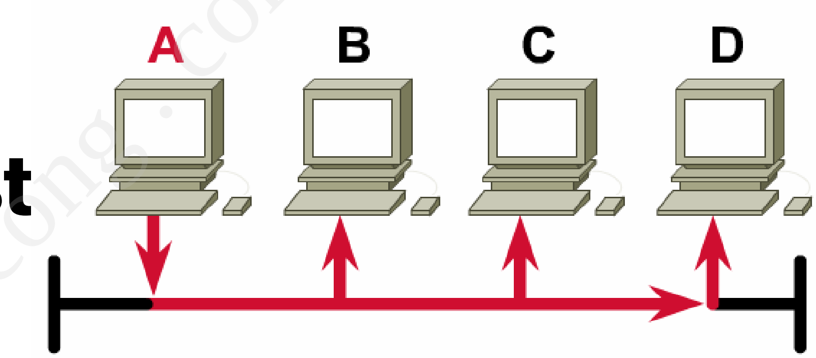
Physical Topology: Mesh

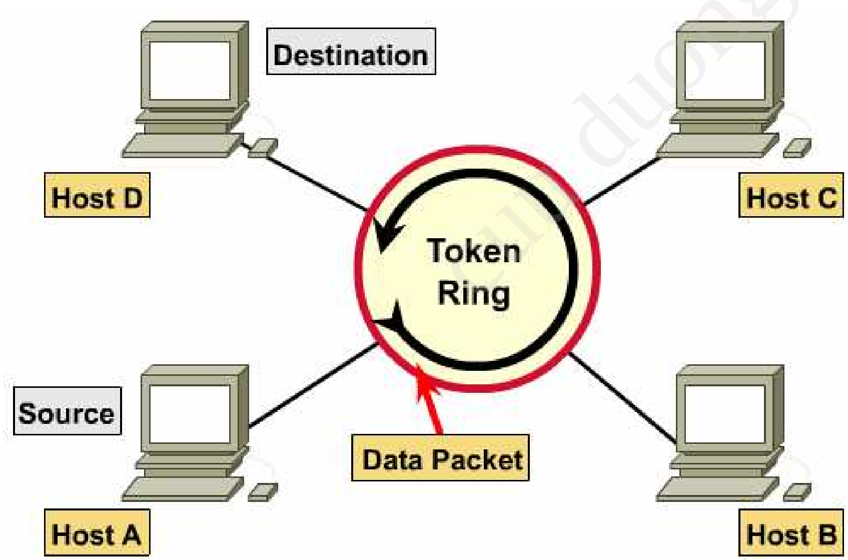


- Each host has its own connection to every other host.
- Used in situations where communication must not be interrupted.

Logical Topologies

Broadcast

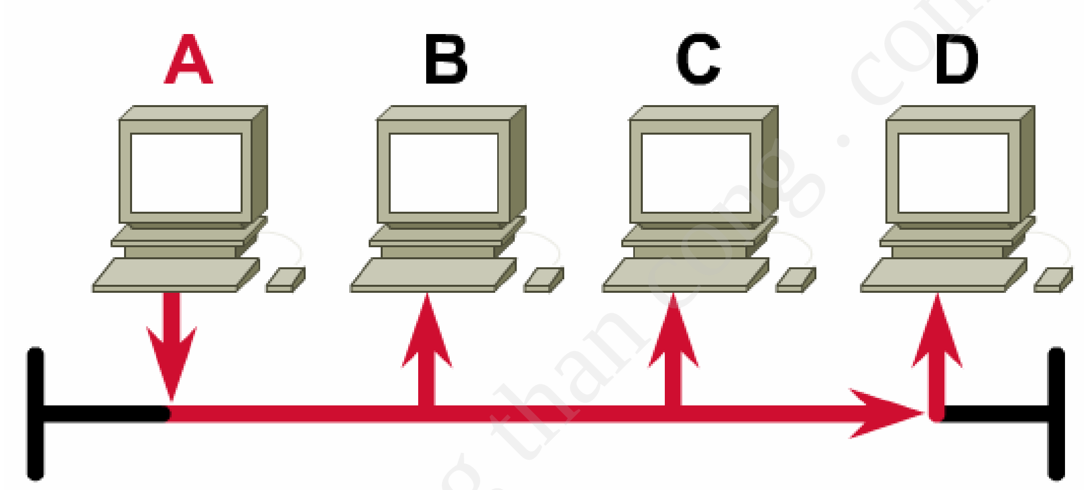




Token Passing

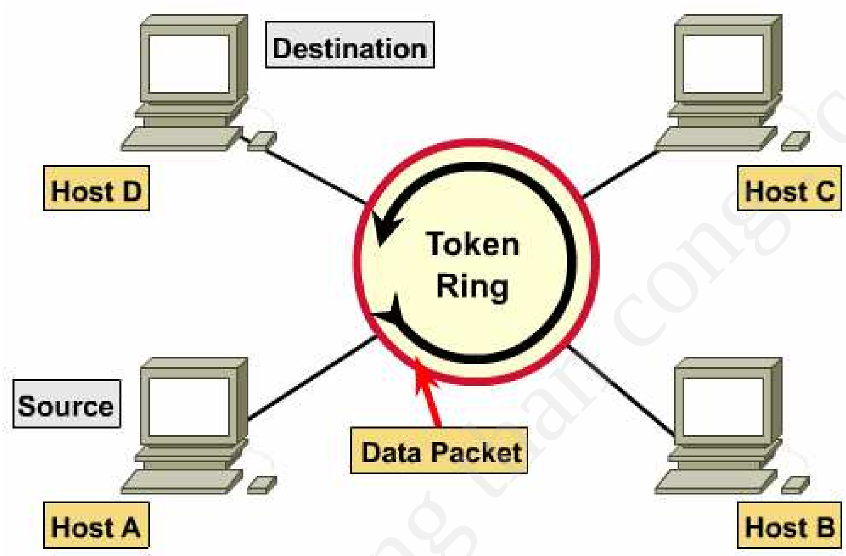
Logical Topology: Broadcast

NETWORK TRAINING CENTER



- Each host on the LAN sends its data (or broadcasts its data) to every other host.
- First-come, first-serve.

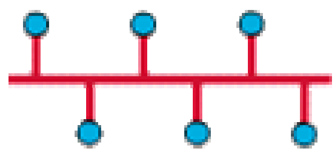
Logical Topology: Token Passing

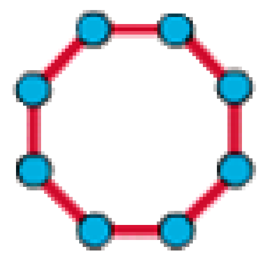


- Access to media is controlled by an electronic token.
- Possession of the token gives the host the right to pass data to its destination.

Technologies

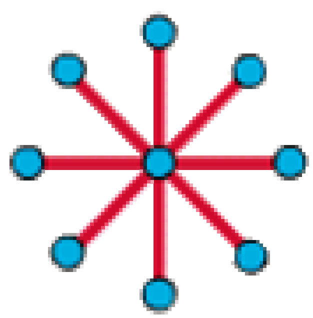
Ethernet



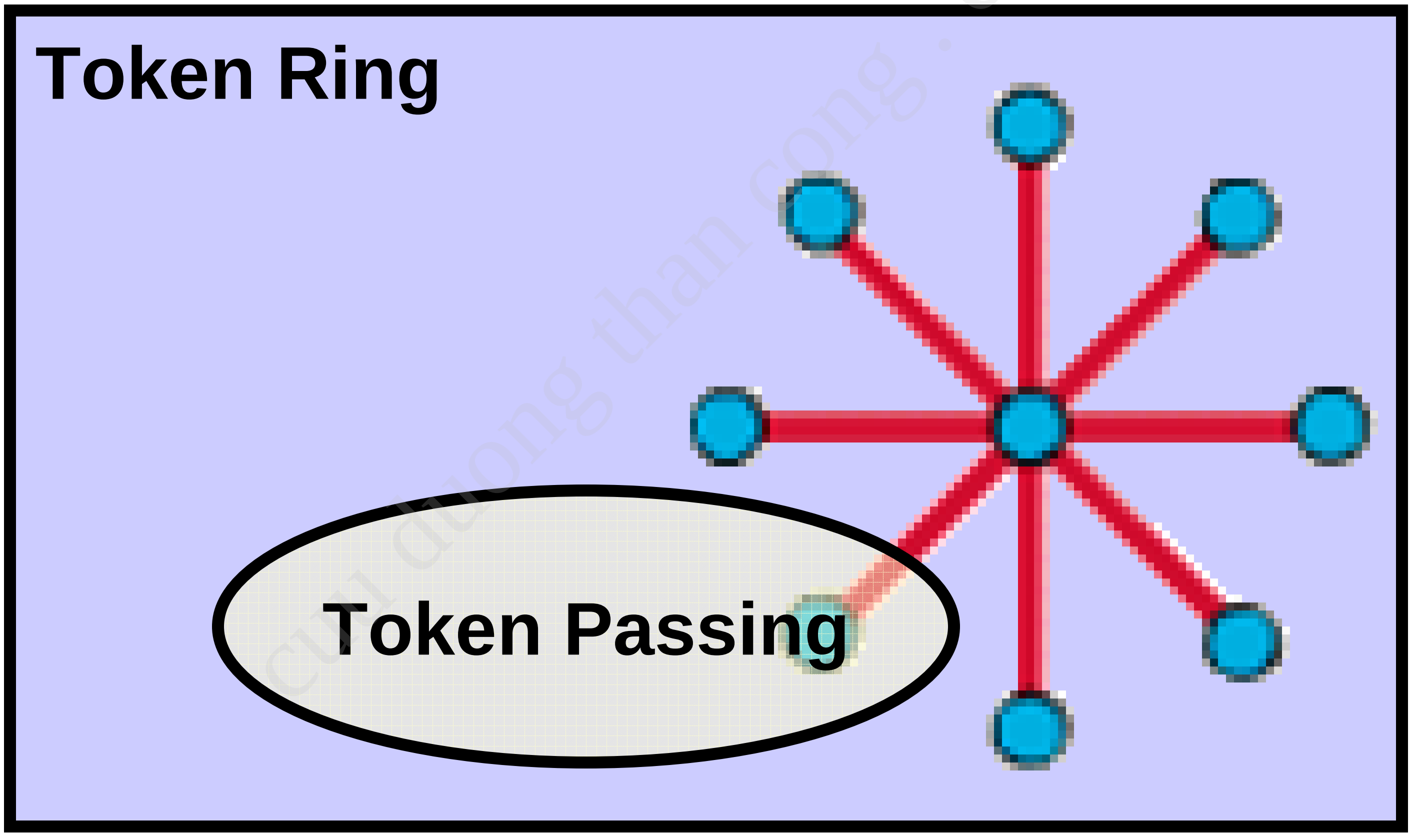


FDDI

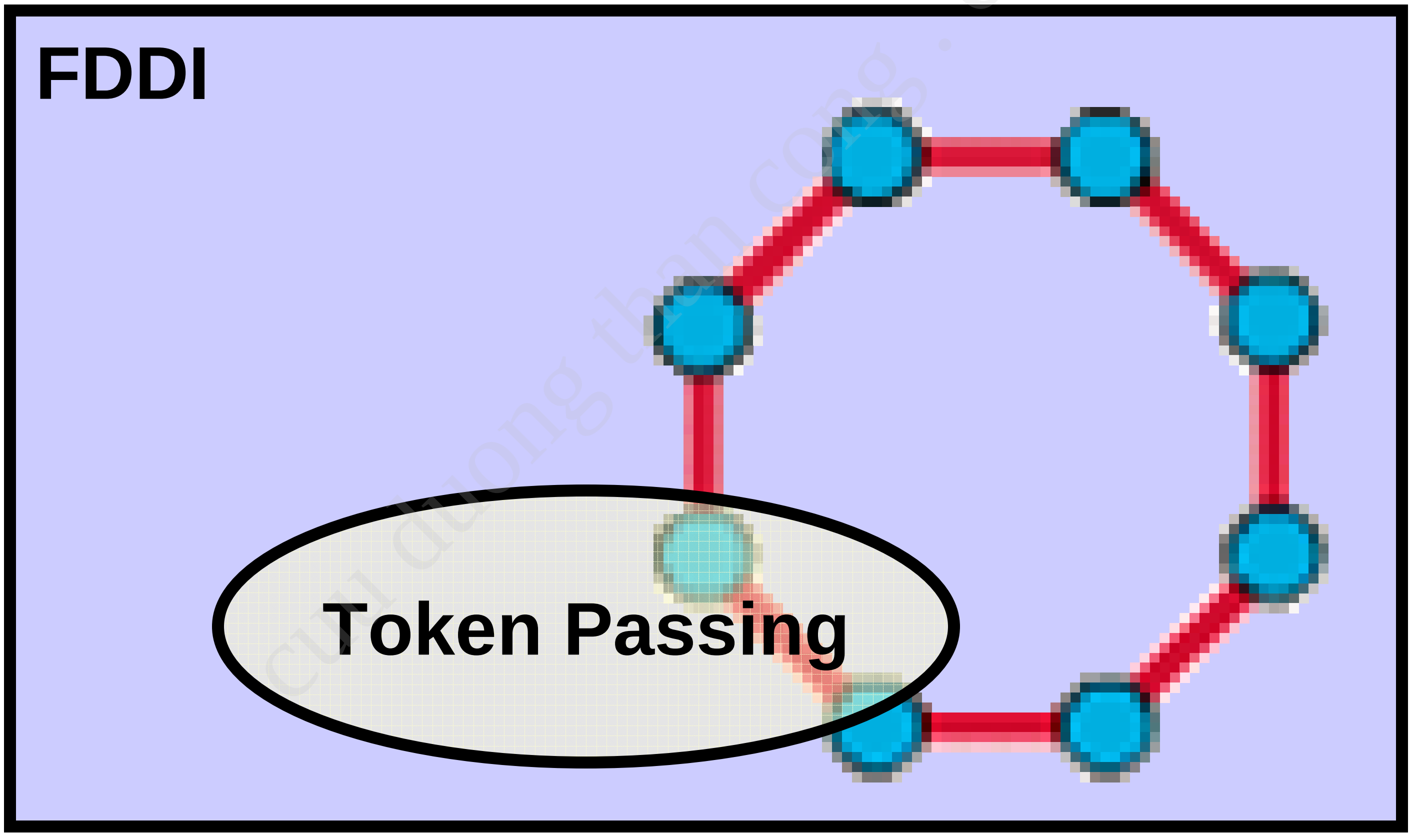
Token Ring



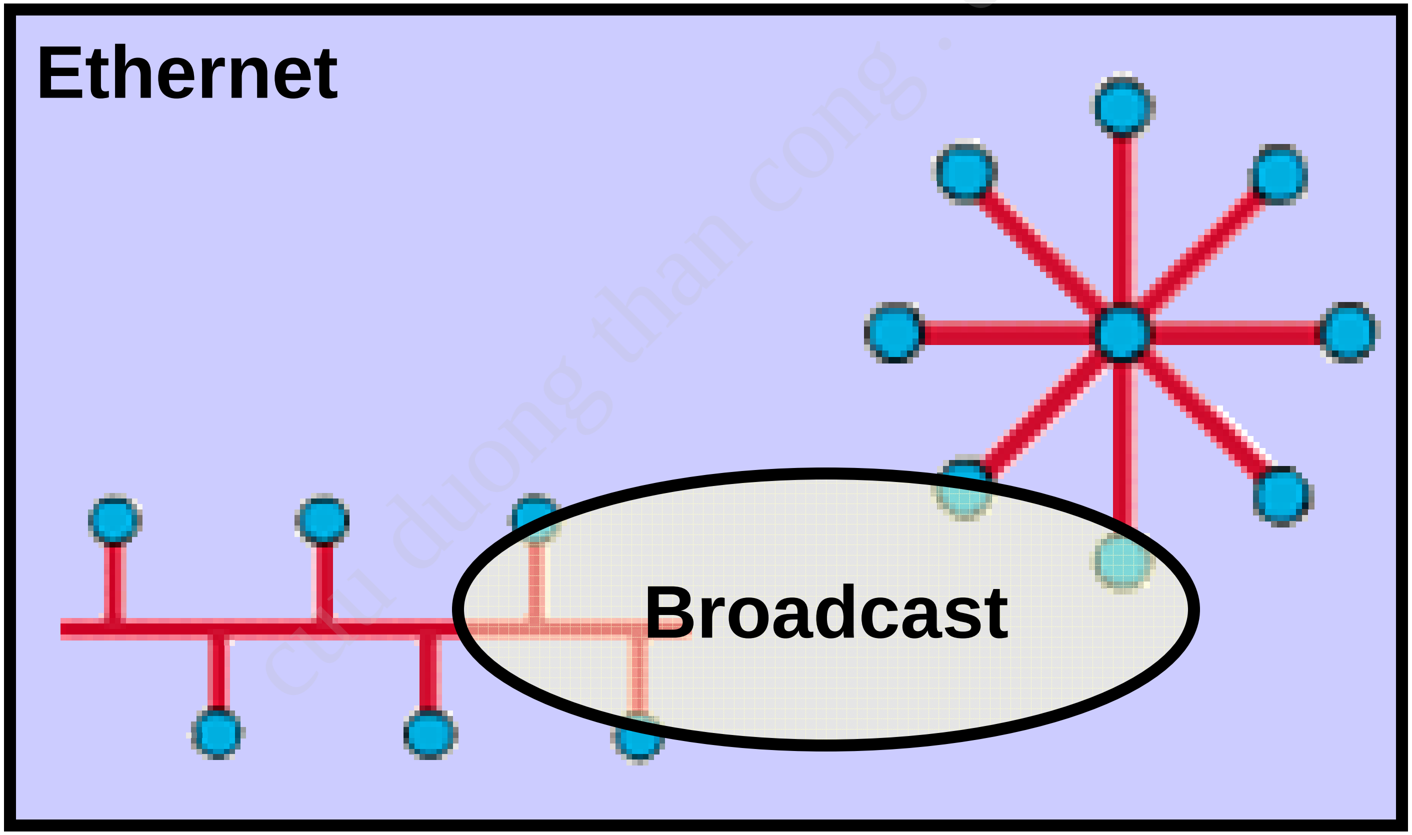
Technology: Token Ring



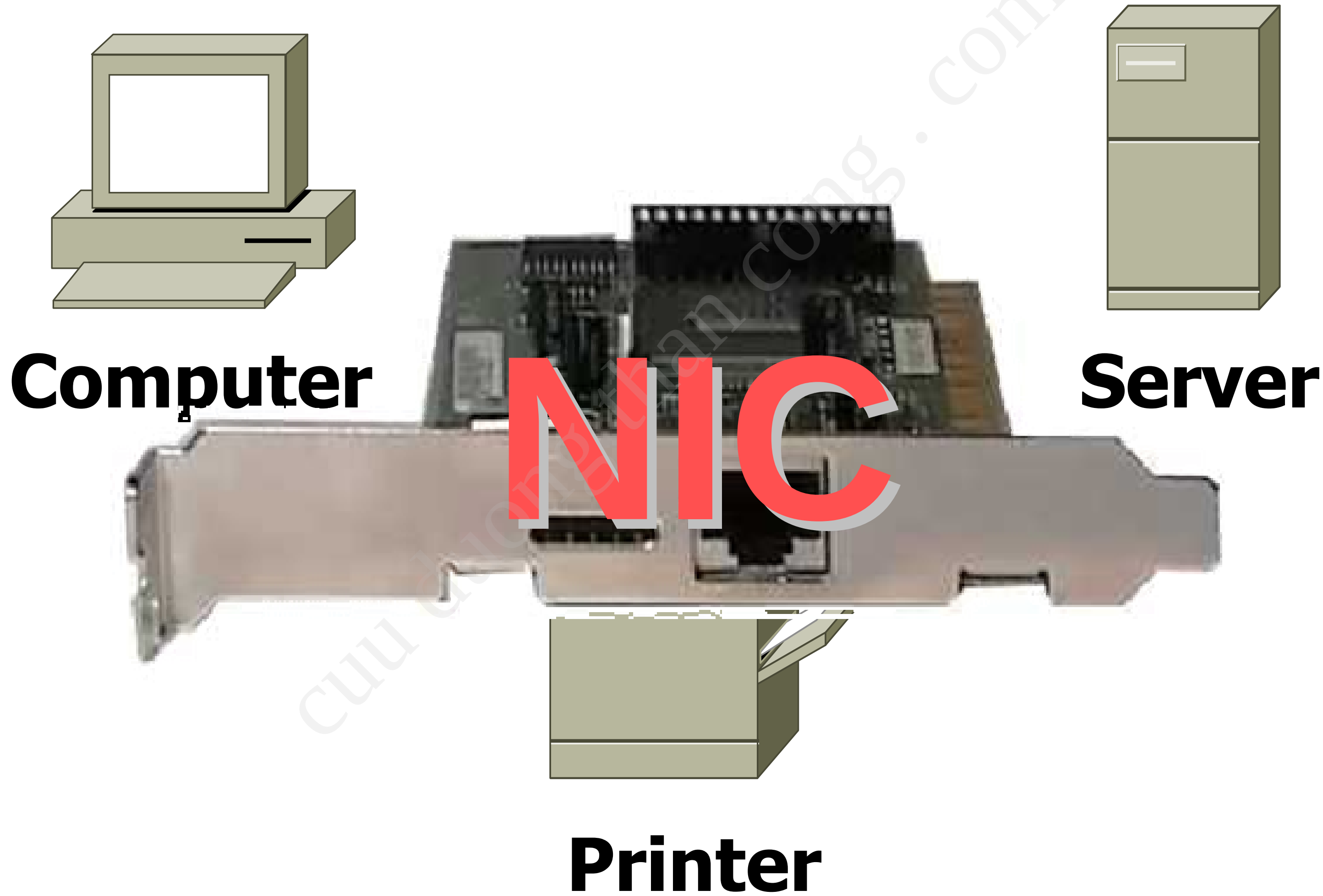
Technology: FDDI



Technology: Ethernet

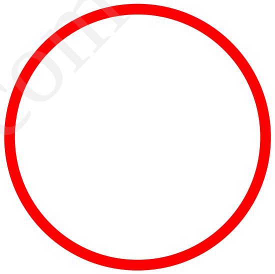


Hosts



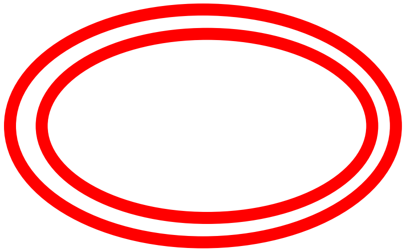
LAN Media Symbols

Ethernet Line



Token Ring

Serial Line

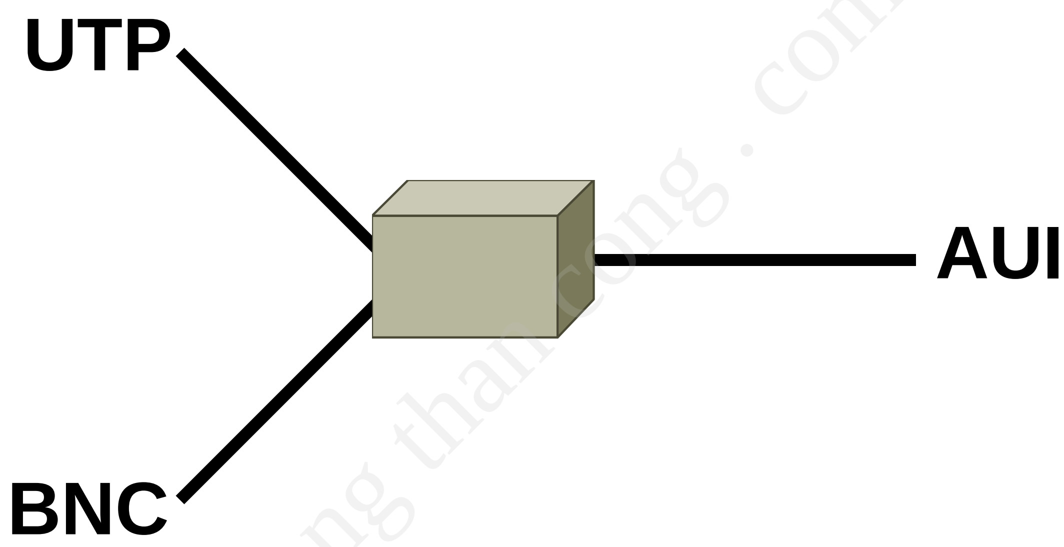


FDDI Ring

OSI Review: Layer 1

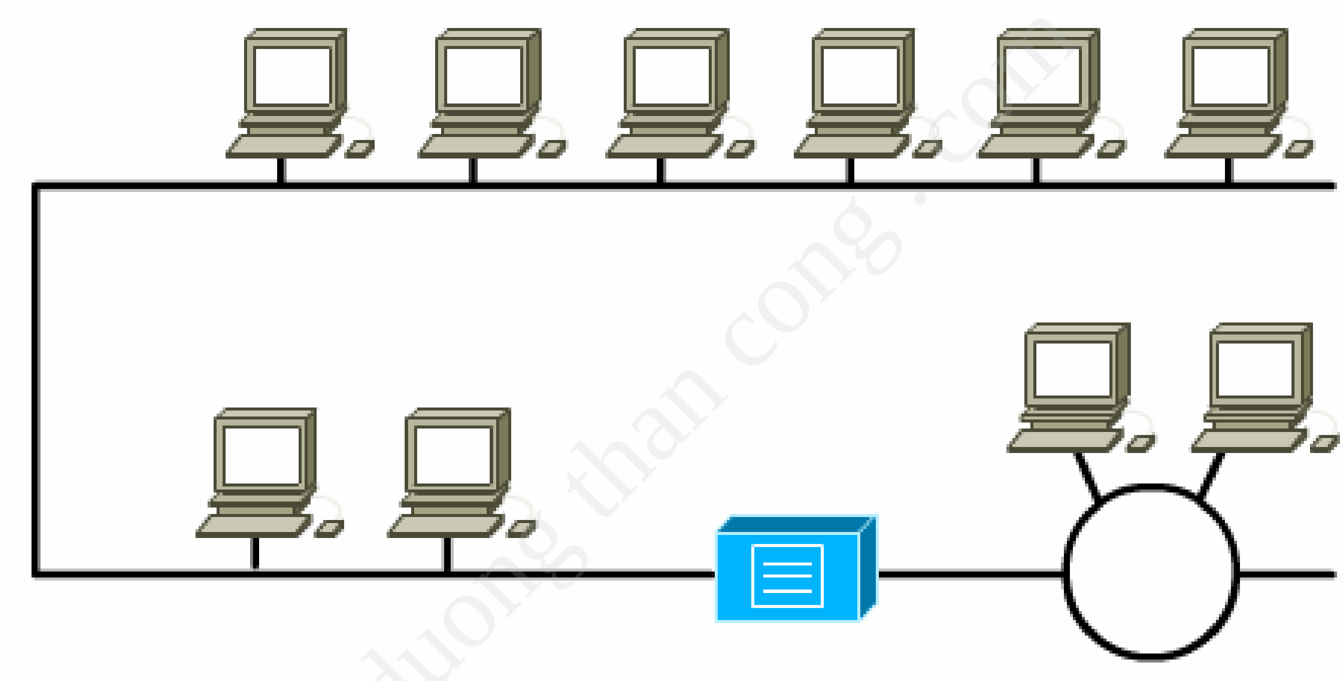
- Responsibility:
  - Transmission of an unstructured bit stream over a physical link between end systems.
- Concerned:
  - Bits.
  - Electrical specifications.
  - Physical data rate.
  - Distances.
  - Physical connector.

LAN Device: Transceiver



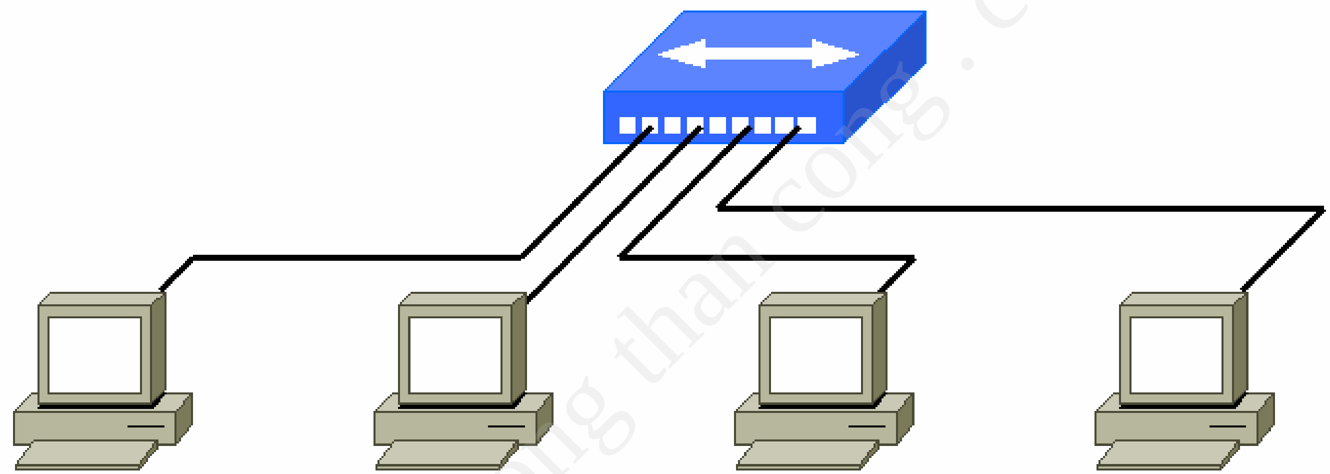
- Connect different media technologies.
- Layer 1 device.

LAN Device: Repeater



- Regenerates and repeats the signal.
- Layer 1 device.

LAN Device: Hub



- A multi-port repeater.
- Layer 1 device.

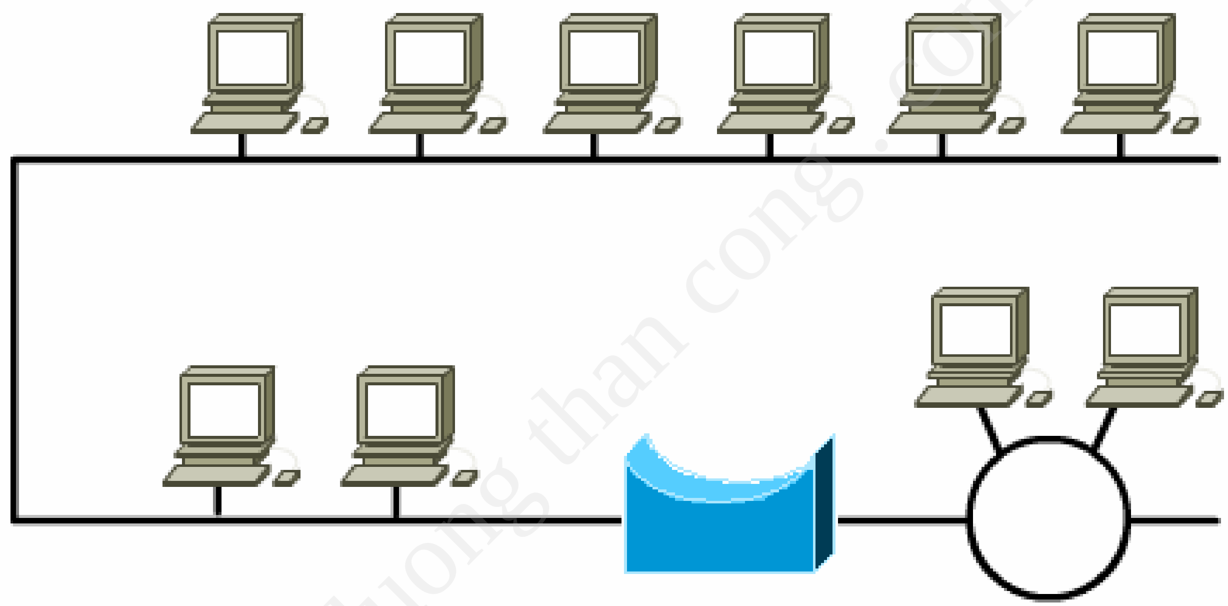
OSI Review: Layer 2

- Responsibility:
  - Provides for the reliable transfer of data cross a physical link.
- Concerned:
  - Frames.
  - Physical address (HW or MAC): Flat.
  - Error and flow control.
  - "Segment".

LAN Device: NIC

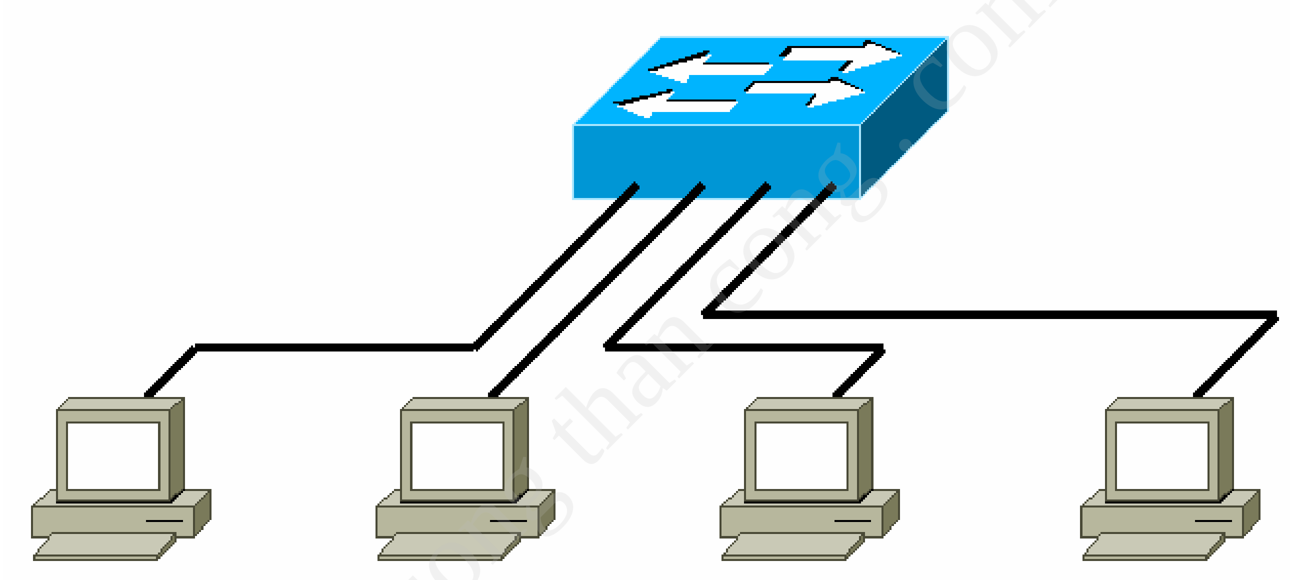
- Network interface of hosts.
- Build-in physical address.
- Layer 2 device.

LAN Device: Bridge



- Keeps traffic local by filtering traffic based on physical addresses.
- Layer 2 device.

LAN Device: Switch



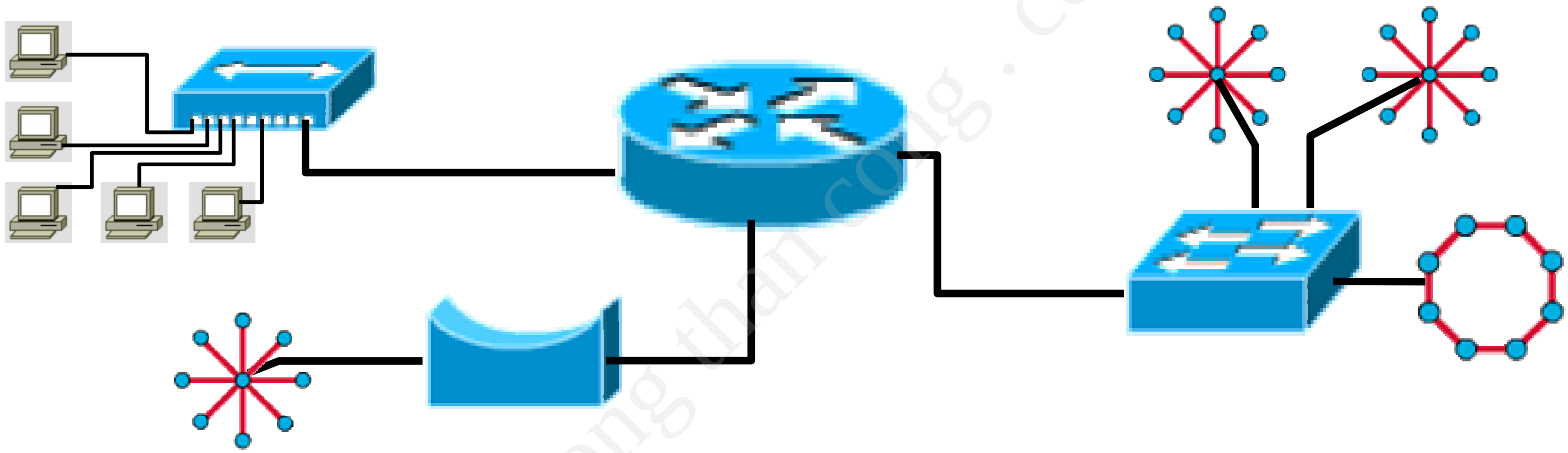
- A multi-port bridge.
- Layer 2 device.

OSI Review: Layer 3

- Responsibility:
  - Connection and path selection between two end system across networks.
- Concerned:
  - Packets.
  - Logical address: Hierarchical.
    - Networks and Hosts addressing.
  - Route , Routing table, Routing protocol.
  - "Network".

LAN Device: Router

NETWORK TRAINING CENTER



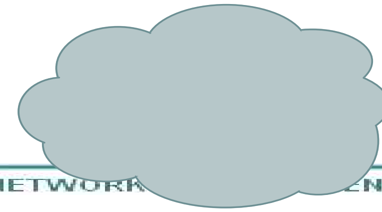
- Makes decisions based on network addresses (logical addresses).
- Layer 3 device.

LAN Device: Router Functions

NETWORK TRAINING CENTER

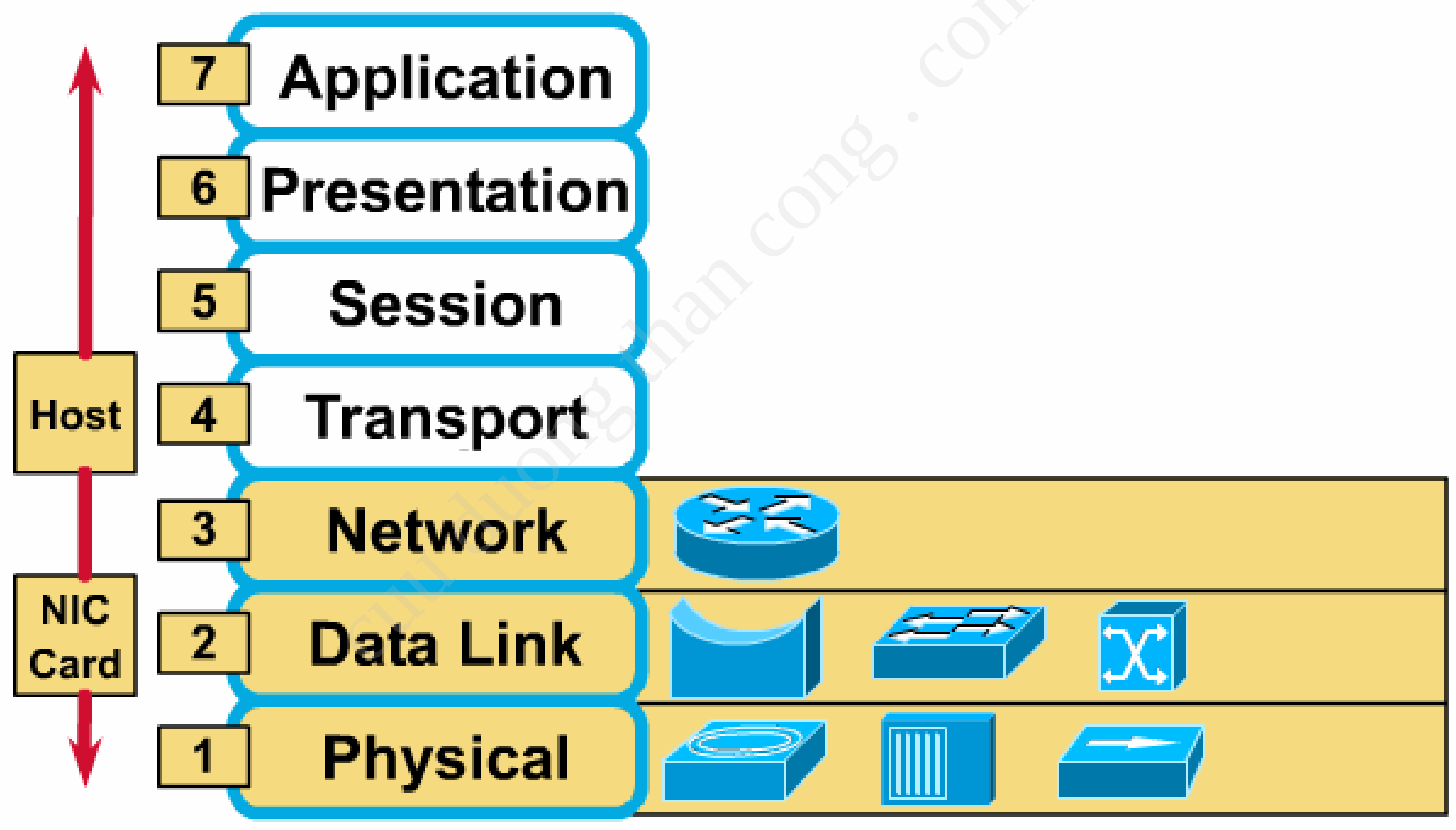
- Path determination:
  - The process of evaluating a packet's destination IP address so that the router can decide which port to send out the packet.
- Packet switching:
  - The router re-encapsulates the packet in the protocol needed for the specified port and then switches the packet out that port.

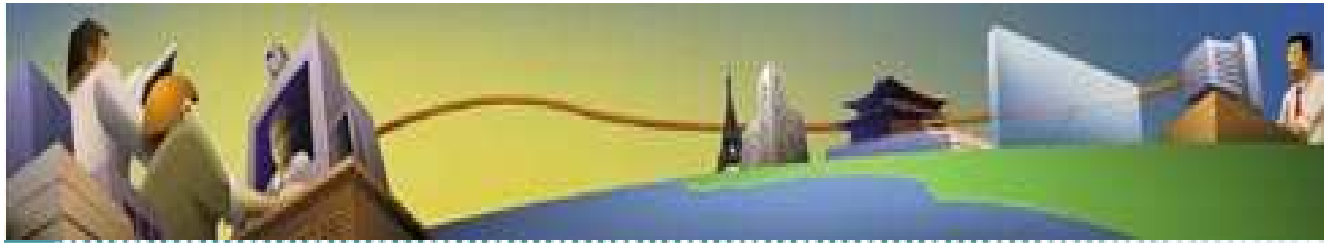
LAN Device: Cloud



- Another network
- Include layer 1 – 7 devices

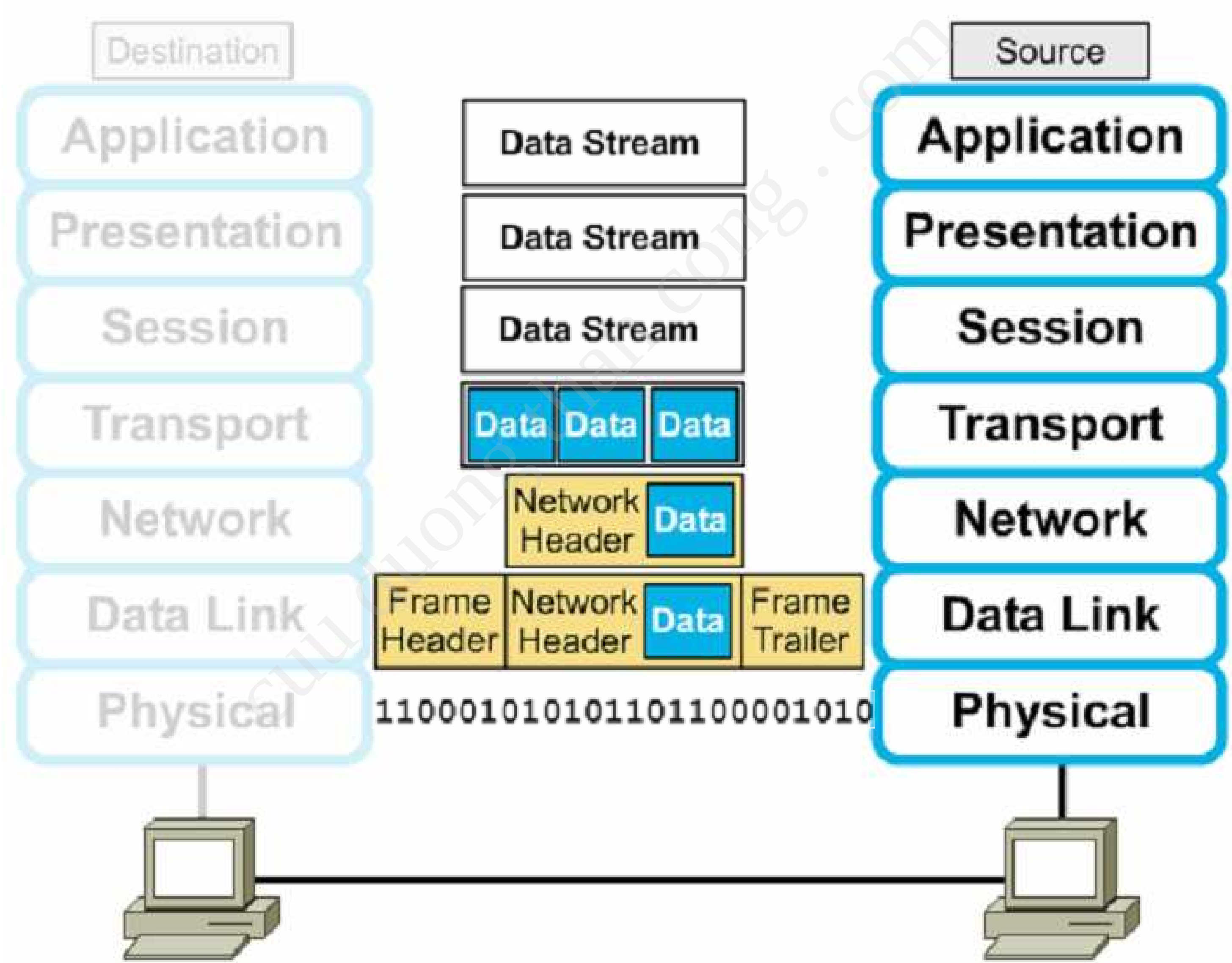
Devices function at Layers



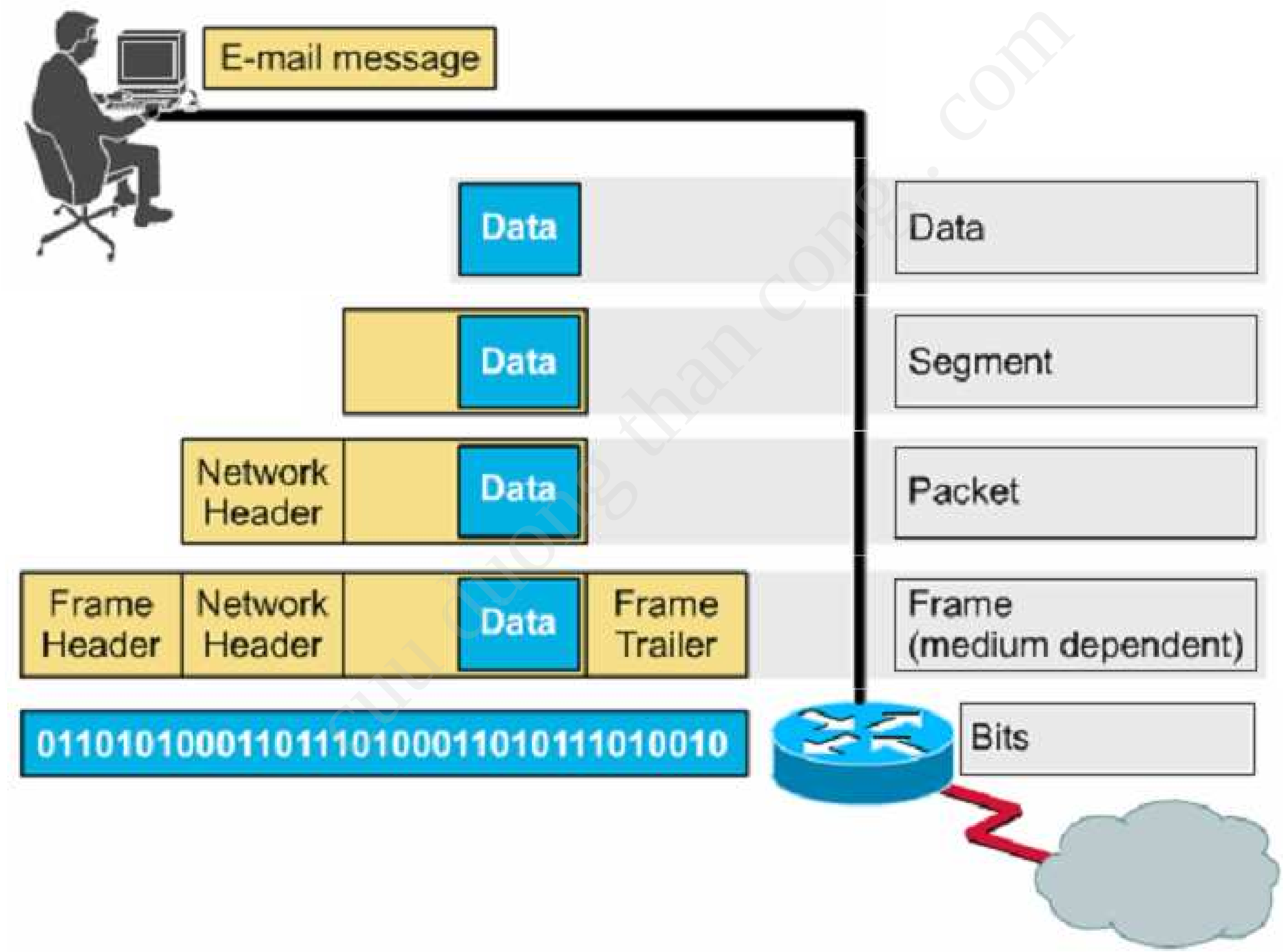


DATA FLOW THROUGH LANs

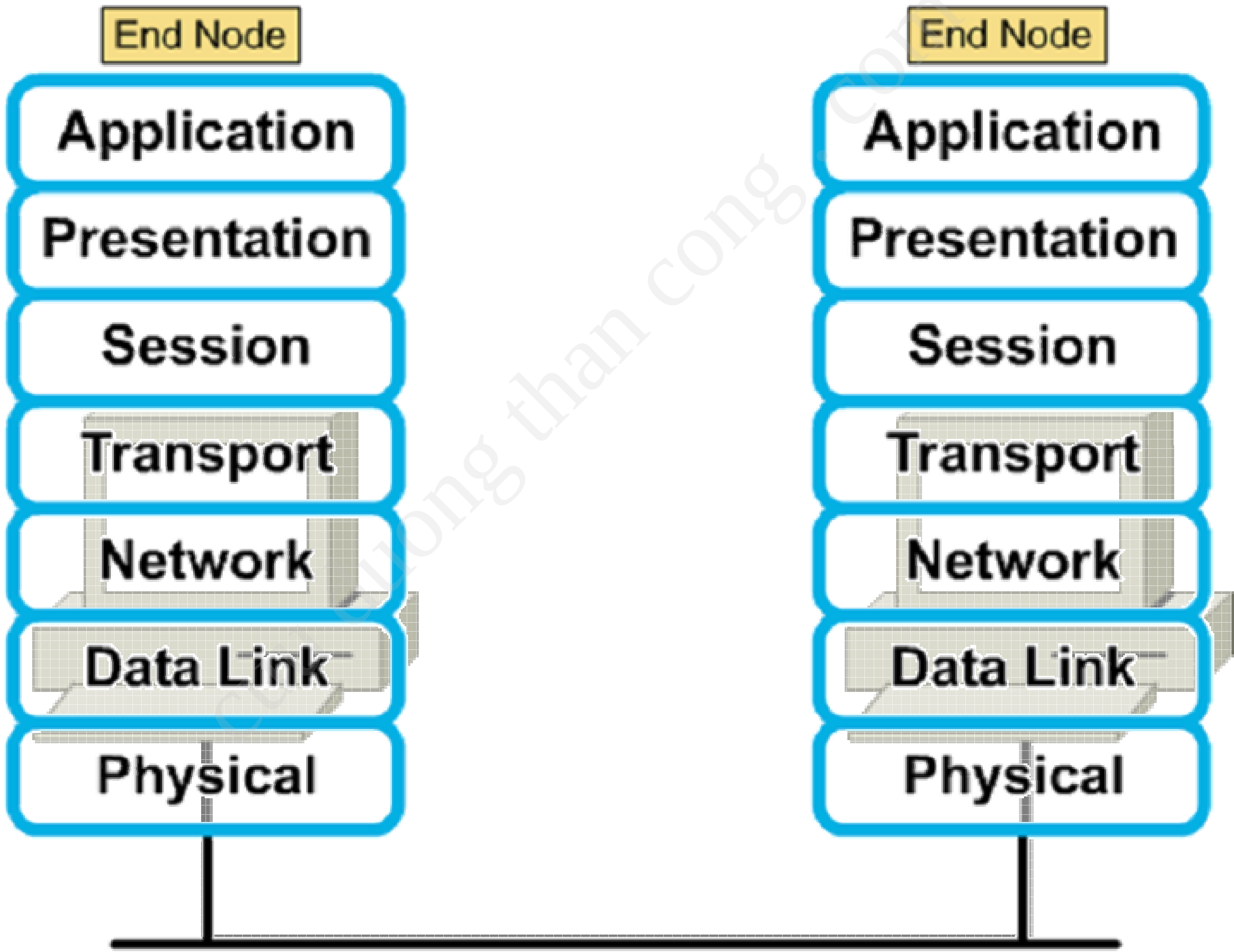
Encapsulation



Encapsulation: Example

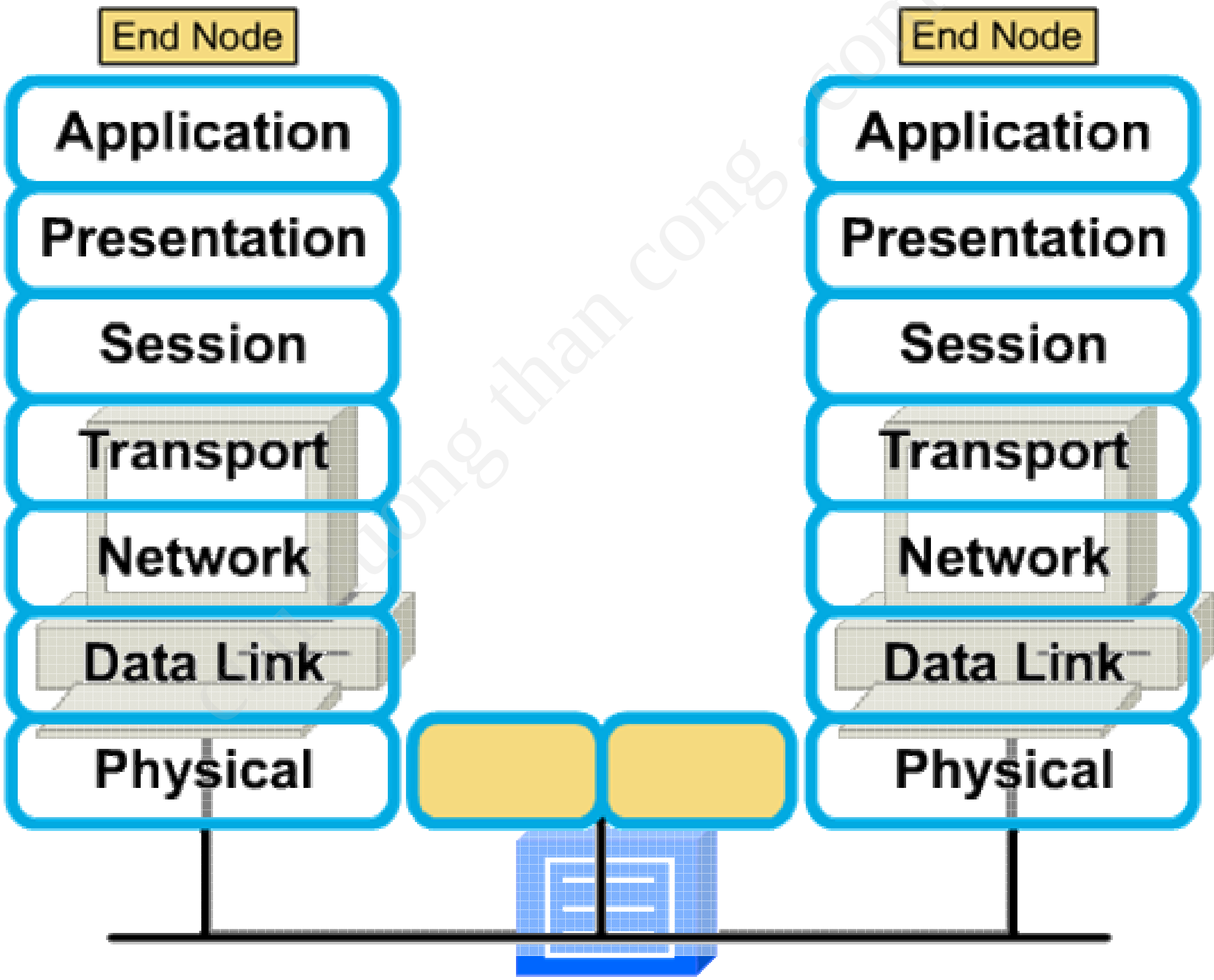


Host to host communication

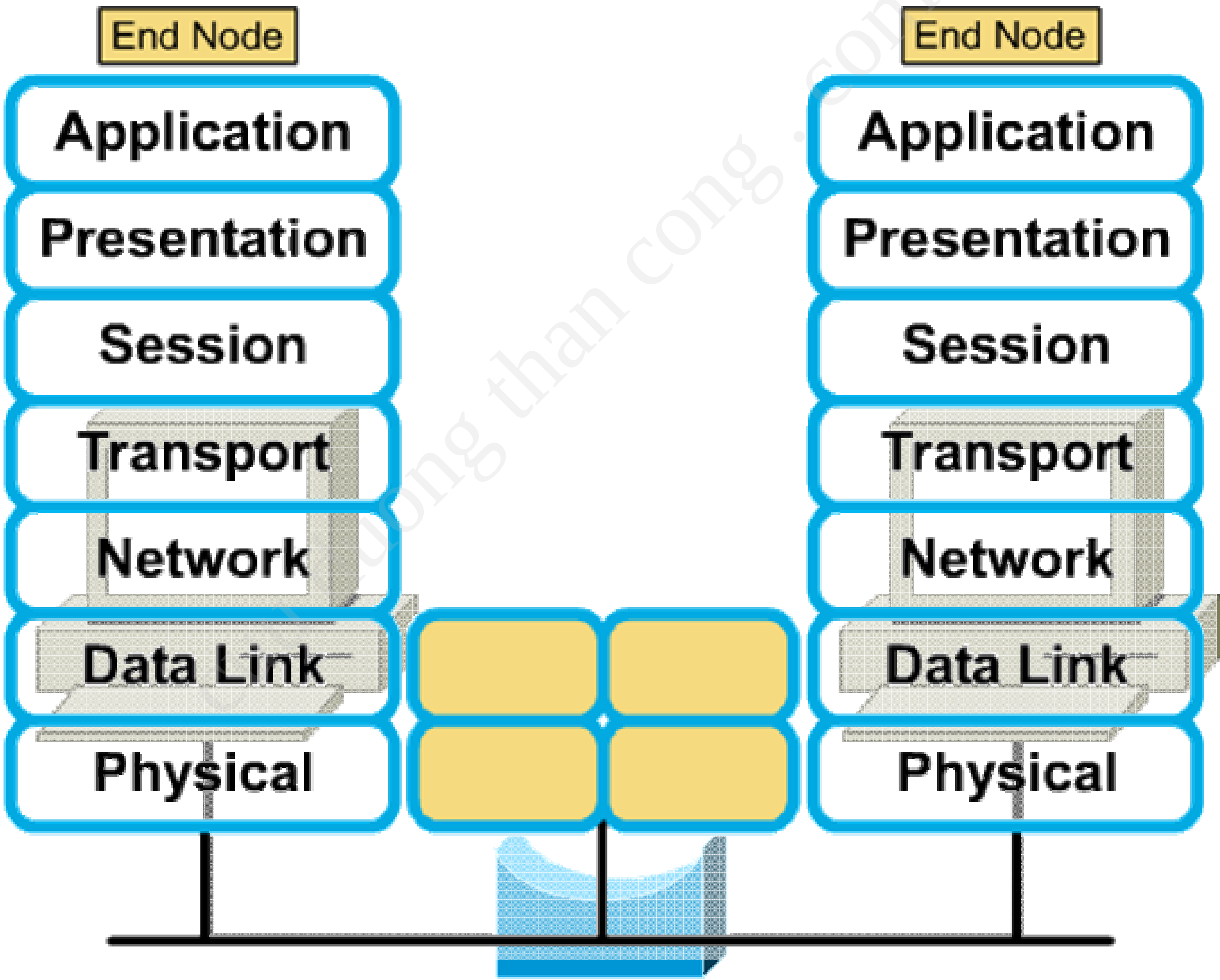


Packet Flow: Layer 1 Device

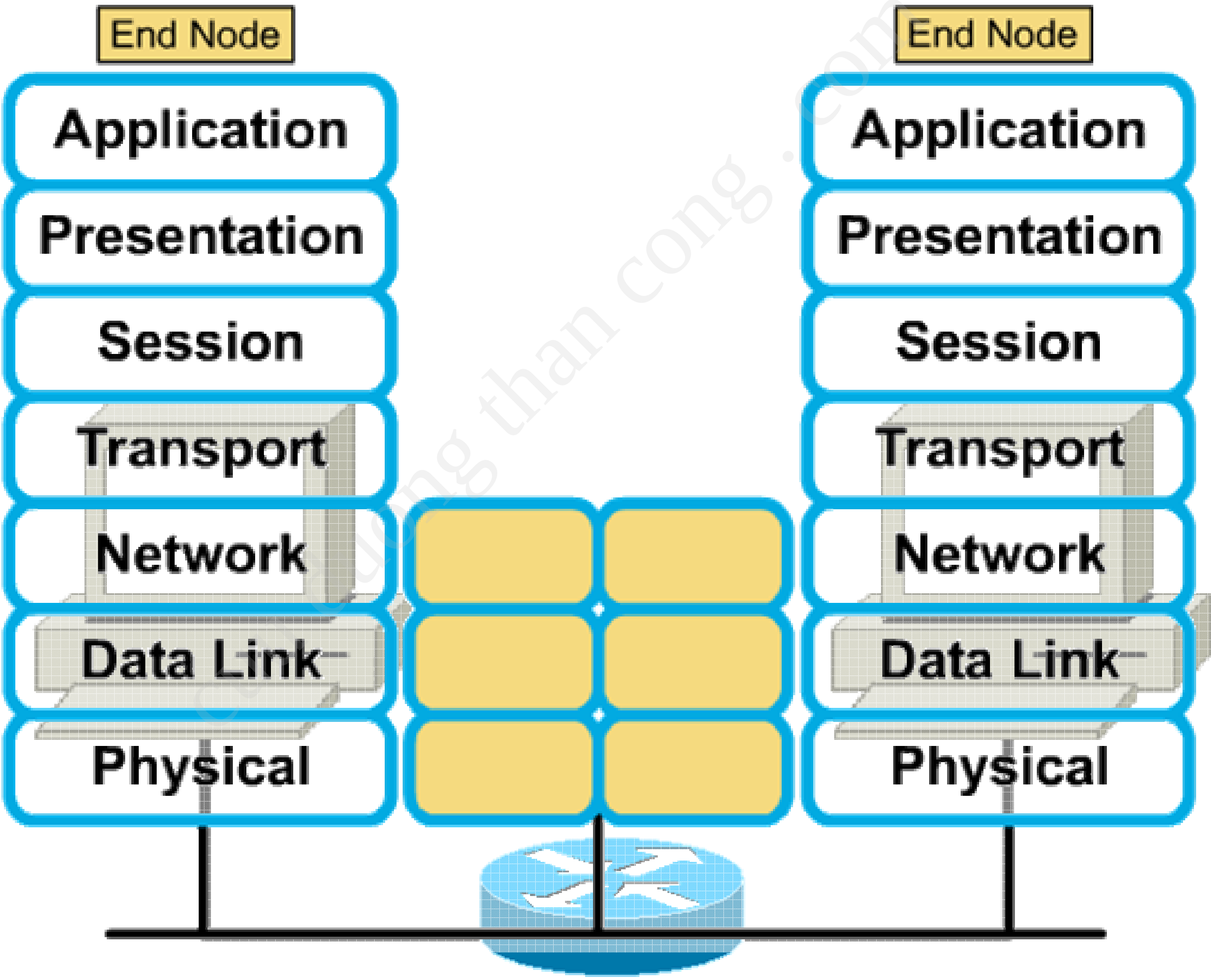
NETWORK TRAINING CENTER



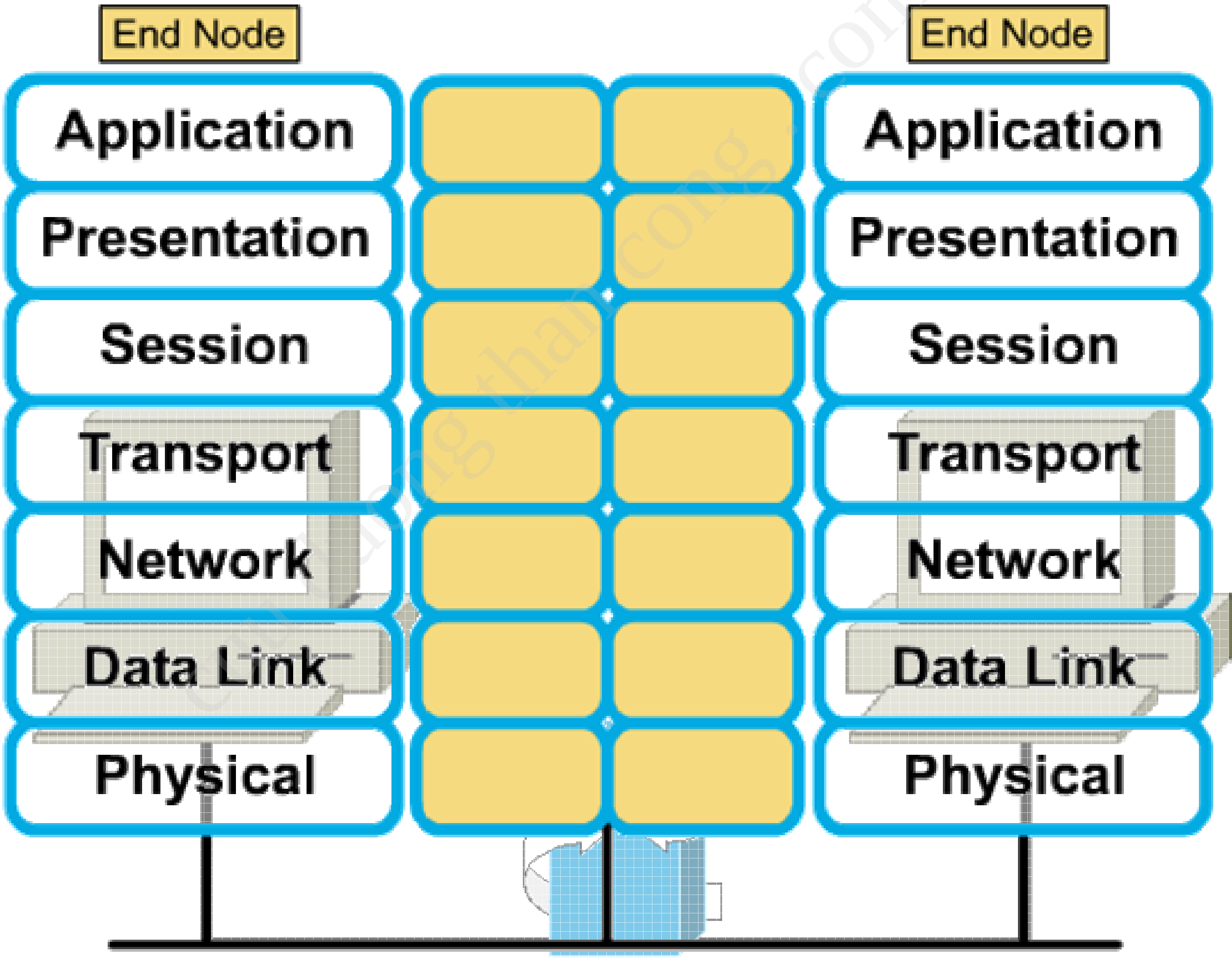
Packet Flow: Layer 2 Device

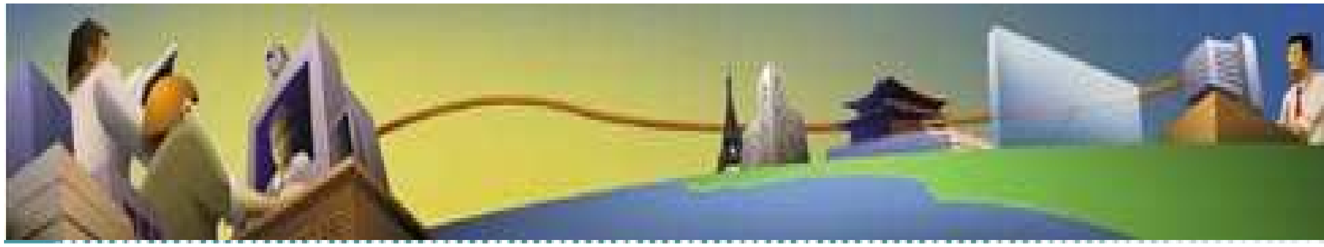


Packet Flow: Layer 3 Device



Packet Flow: Layer 1-7 Device





NETWORKING TERMINOLOGY

Wide-Area Networks (WANs)

NETWORK TRAINING CENTER

WANs are designed to:

- Operate over a large geographical area
- Allow access over serial interfaces operating at lower speeds
- Provide full-time and part-time connectivity
- Connect devices separated over wide, even global areas

Using:

Wide-Area Networks (WANs)

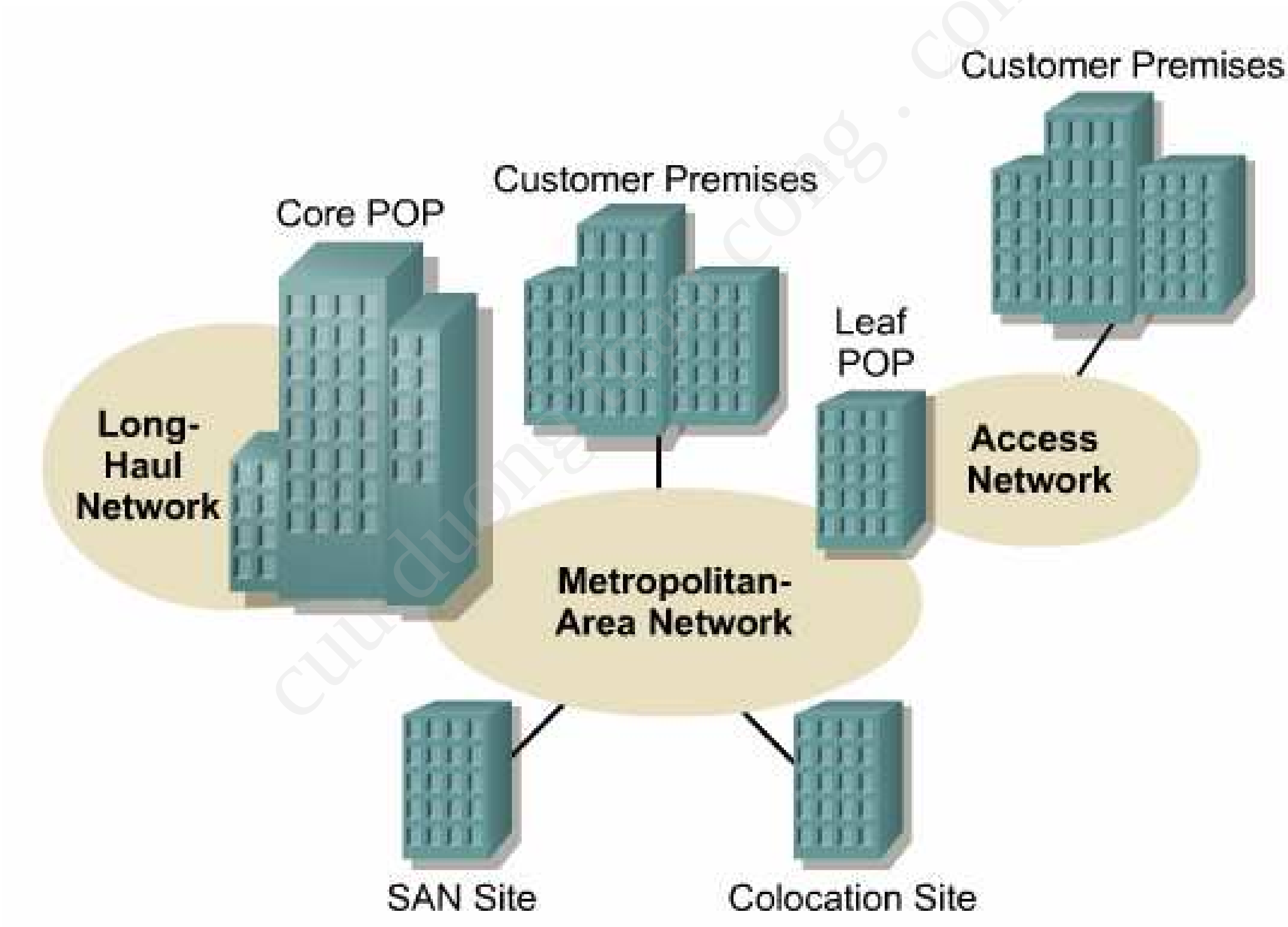
- **WANs** interconnect LANs, which then provide access to computers or file servers in other locations.
- **WANs** make it possible for businesses to communicate across great distances.
- **WANs** allow computers, printers, and other devices on a LAN to be shared with distant locations. WANs provide instant communications across large geographic areas.
- **Collaboration software** provides access to real-time information and resources and allows meetings to be held remotely.

Wide-Area Networks (WANs)

- **WANs** are designed to do the following:
  - Operate over a large and geographically separated area
  - Allow users to have real-time communication capabilities with other users
  - Provide full-time remote resources connected to local services
  - Provide e-mail, Internet, file transfer, and e-commerce services

Metropolitan-Area Networks (MANs)

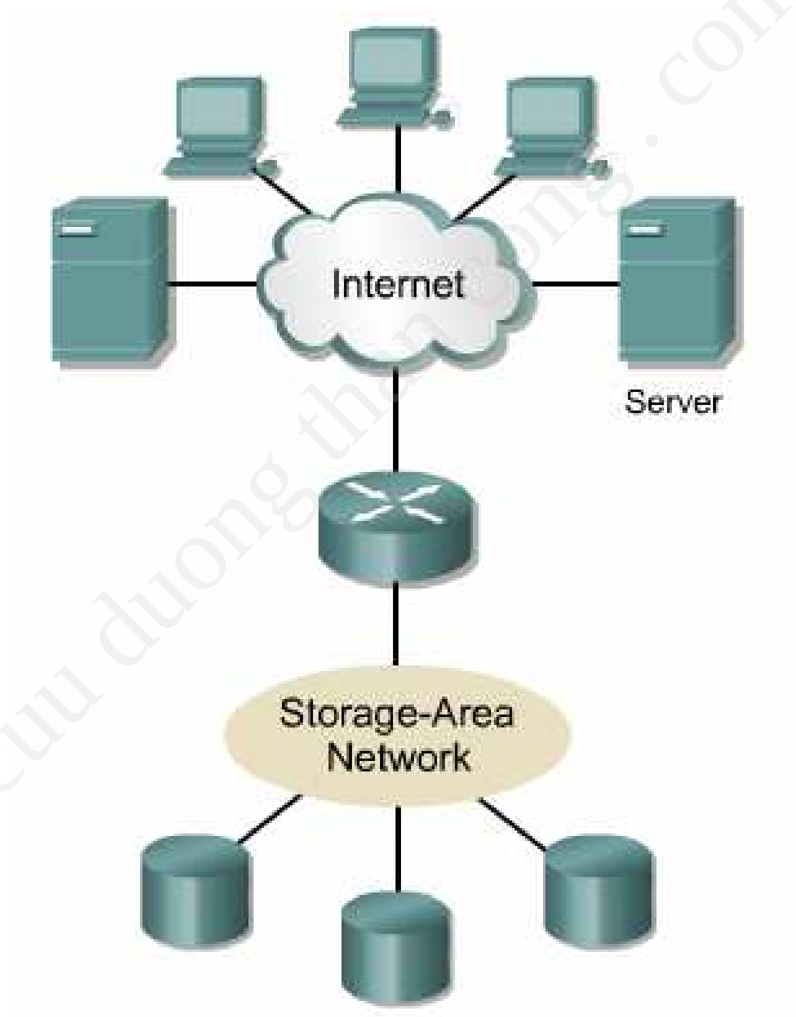
NETWORK TRAINING CENTER



Metropolitan-Area Networks (MANs)

- **Wireless bridge technologies** that send signals across public areas can also be used to create a **MAN**.
- A **MAN** usually consists of two or more LANs in a common geographic area.
- Typically, a service provider is used to connect two or more LAN sites using private communication lines or optical services.
- A MAN can also be created using wireless bridge technology by beaming signals across public areas.

Storage-Area Networks (SANs)



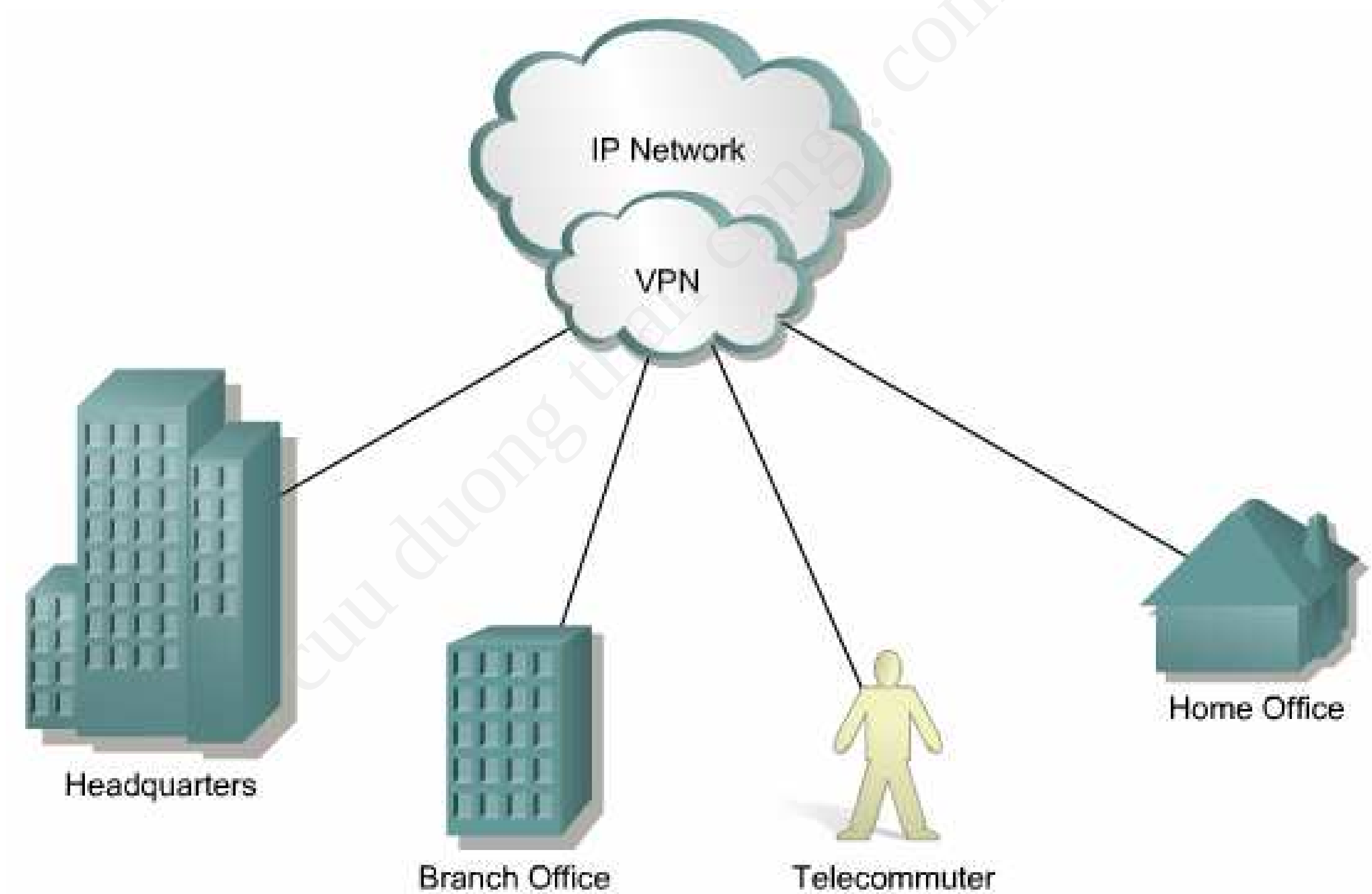
Storage-Area Networks (SANs)

- A **storage-area network (SAN)** is a dedicated, high-performance network used to move data between servers and storage resources; because it is a separate, dedicated network, it avoids any traffic conflict between clients and servers
- **SAN technology** allows high-speed server-to-storage, storage-to-storage, or server-to-server connectivity; this method uses a separate network infrastructure that relieves any problems associated with existing network connectivity

Storage-Area Networks (SANs)

- **SANs** offer the following features:
  - **Performance** – SANs allow concurrent access of disk or tape arrays by two or more servers at high speeds. This provides enhanced system performance.
  - **Availability** – SANs have built-in disaster tolerance. Data can be duplicated on a SAN up to 10 km (6.2 miles) away.
  - **Scalability** – A SAN can use a variety of technologies. This allows easy relocation of backup data, operations, file migration, and data replication between systems.

Virtual Private Network (VPN)



Virtual Private Network (VPN)

- A **vitual private network (VPN)** is a private network that is constructed within a public network infrastructure such as the global Internet
- Using VPN, a **telecommuter** can remotely access the network of the company headquarters
- Through the Internet, a secure tunnel can be built between the PC of the telecommuter and a VPN router at the company headquarters

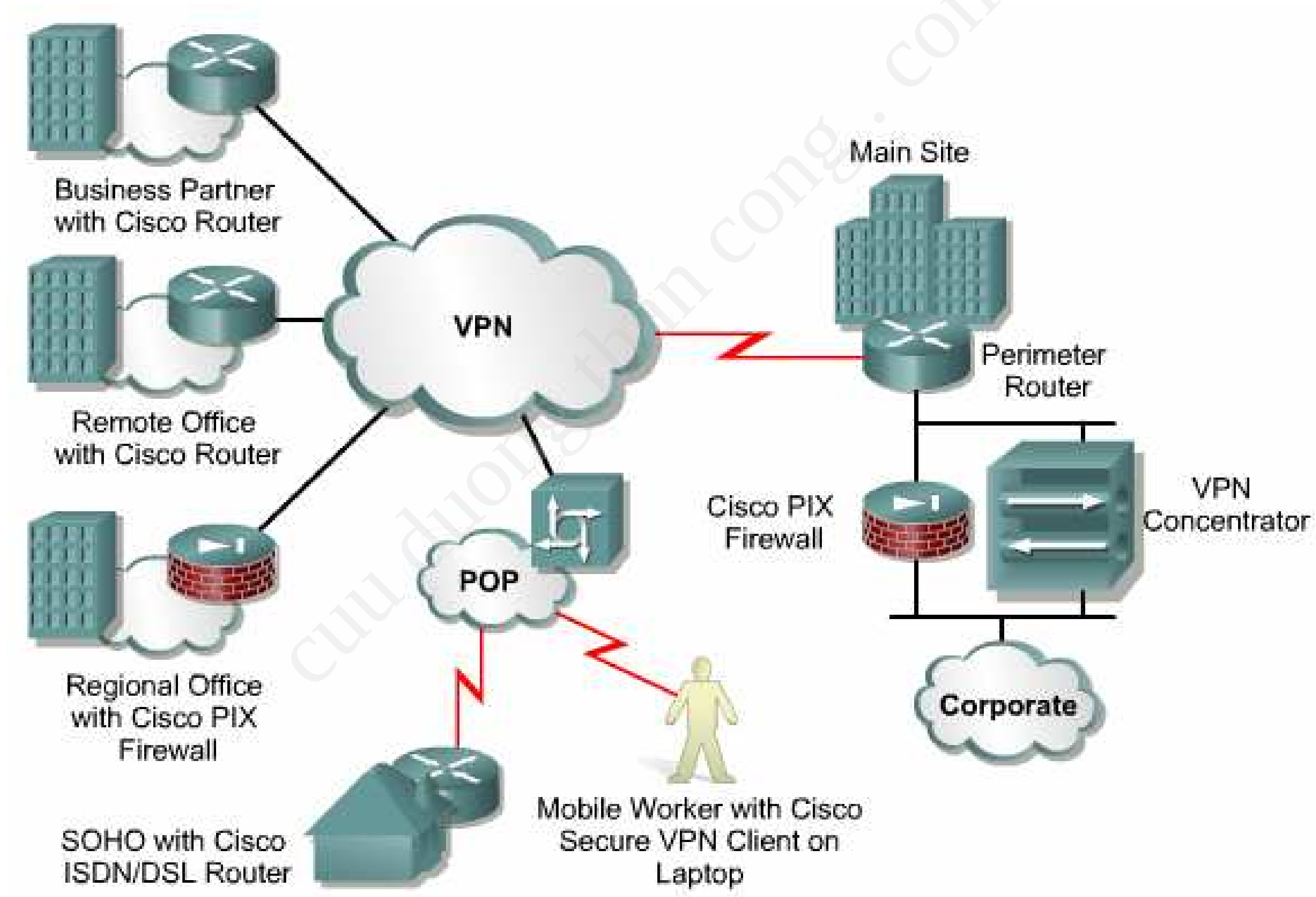
Benefits of VPNs

- A **VPN** is a service that offers secure, reliable connectivity over a shared public network infrastructure such as the Internet. VPNs maintain the same security and management policies as a private network.
- The use of a VPN is the most **cost-effective way** to establish a point-to-point connection between remote users and an enterprise network.

Benefits of VPNs

- The three main types of VPNs:
  - **Access VPNs** provide remote access for mobile and small office, home office (SOHO) users to an Intranet or Extranet over a shared infrastructure. Access VPNs use analog, dialup, ISDN, DSL, mobile IP, and cable technologies to securely connect mobile users, telecommuters, and branch offices.
  - **Intranet VPNs** use dedicated connections to link regional and remote offices to an internal network over a shared infrastructure. Intranet VPNs differ from Extranet VPNs in that they allow access only to the employees of the enterprise.
  - **Extranet VPNs** use dedicated connections to link business partners to an internal network over a shared infrastructure. Extranet VPNs differ from Intranet VPNs in that they allow access to users outside the enterprise.

Benefits of VPNs



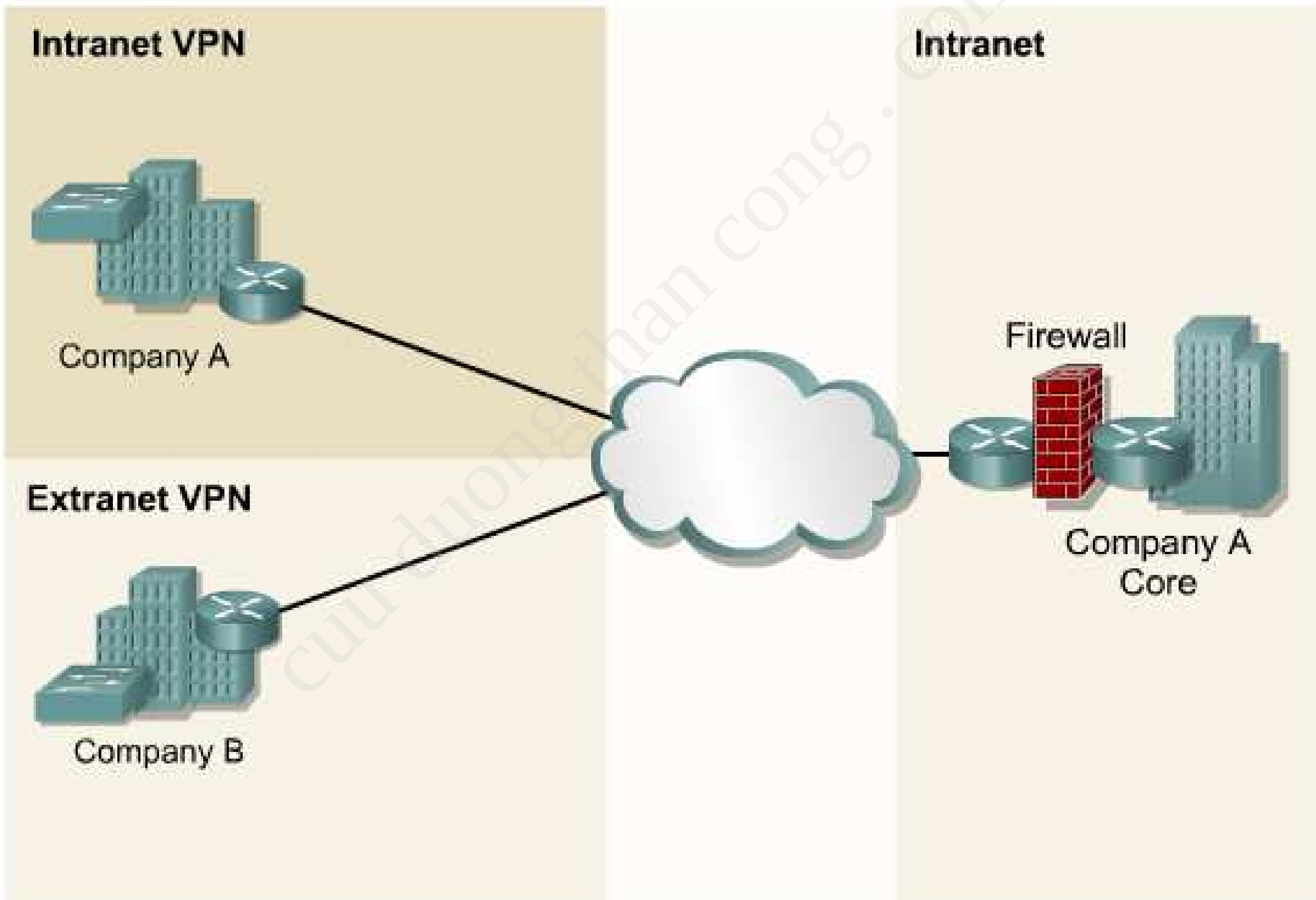
Intranets and Extranets

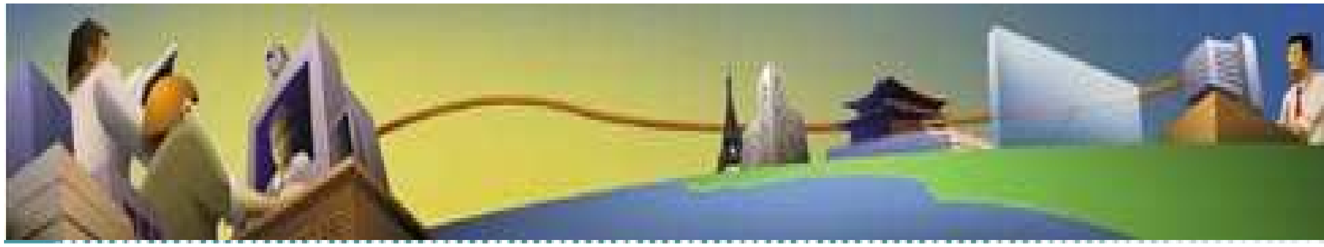
- **Intranet Web servers** differ from public Web servers in that the public must have the proper permissions and passwords to access the intranet of an organization.
- **Intranets** are designed to permit users who have access privileges to the internal LAN of the organization.
- Within an intranet, Web servers are installed in the network.
- **Browser technology** is used as the common front end to access information on servers such as financial, graphical, or text-based data.

Intranets and Extranets

- **Extranets** refer to applications and services that are Intranet based, and use extended, secure access to external users or enterprises.
- This access is usually accomplished through passwords, user IDs, and other application-level security.
- An extranet is the extension of two or more intranet strategies with a secure interaction between participant enterprises and their respective intranets.

Intranets and Extranets





BANDWIDTH

Bandwidth

- **Bandwidth** is defined as the amount of information that can flow through a network connection in a given period of time.

Importance of Bandwidth

Why bandwidth is important:

- Bandwidth is limited by physics and technology
- Bandwidth is not free
- Bandwidth requirements are growing at a rapid rate
- Bandwidth is critical to network performance

Importance of Bandwidth

- **Bandwidth is finite.** Regardless of the media used to build a network, there are limits on the network capacity to carry information. Bandwidth is limited by the laws of physics and by the technologies used to place information on the media.
- **Bandwidth is not free.** It is possible to buy equipment for a LAN that will provide nearly unlimited bandwidth over a long period of time. For WAN connections, it is usually necessary to buy bandwidth from a service provider. In either case, individual users and businesses can save a lot of money if they understand bandwidth and how the demand will change over time.

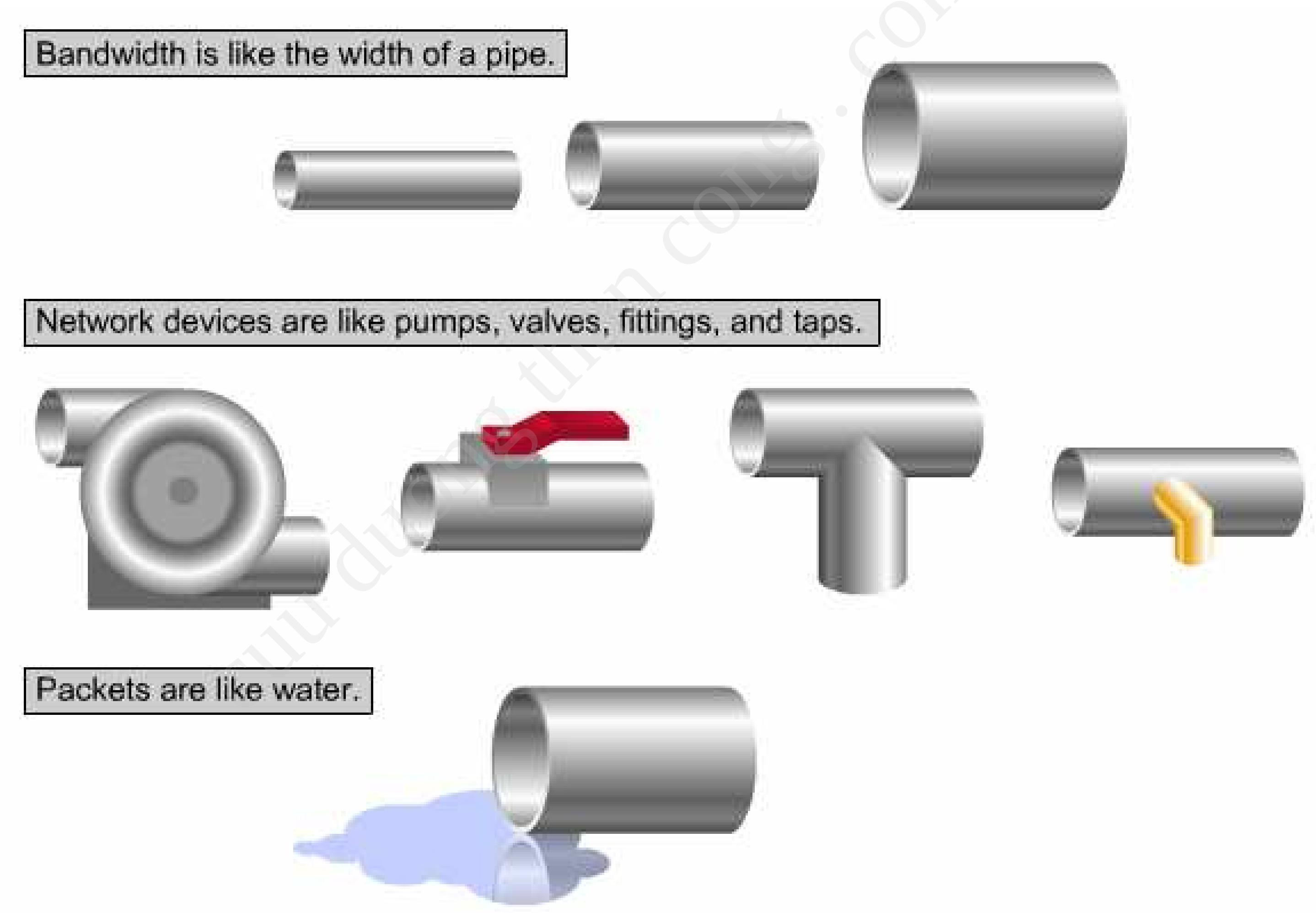
Importance of Bandwidth

- **Bandwidth is an important factor that is used to analyze network performance, design new networks, and understand the Internet.** A networking professional must understand the tremendous impact of bandwidth and throughput on network performance and design.
- **The demand for bandwidth continues to grow.** As soon as new network technologies and infrastructures are built to provide greater bandwidth, new applications are created to take advantage of the greater capacity.

Analogies (of Bandwidth)

- **Bandwidth** has been defined as the amount of information that can flow through a network in a given time.
- **Bandwidth is like the width of a pipe**. A network of pipes brings fresh water to homes and businesses and carries waste water away. This water network is made up of pipes of different diameters.
- Many networking experts say that they need to put in bigger pipes when they wish to add more information-carrying capacity.

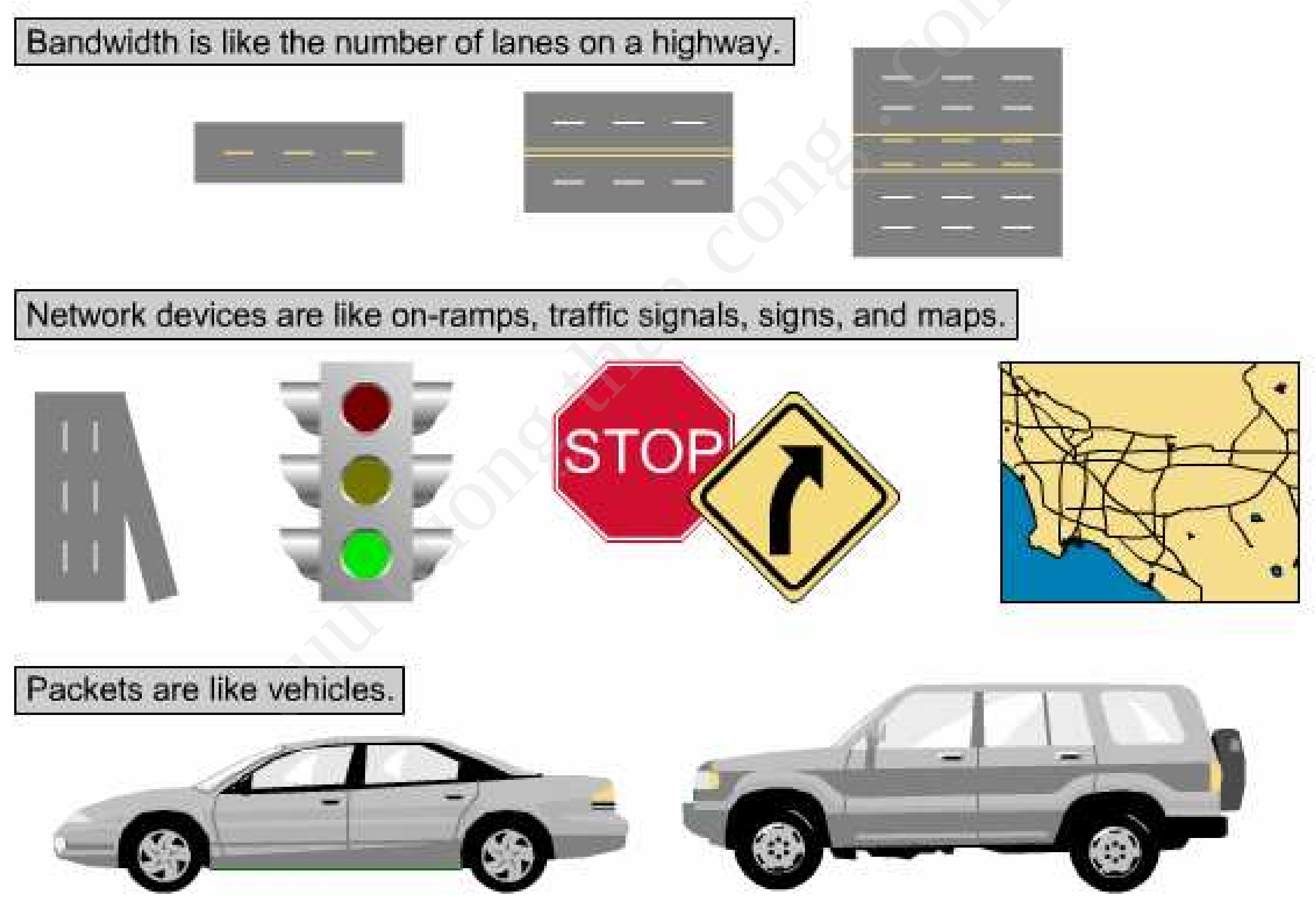
Analogies (of Bandwidth)



Analogies (of Bandwidth)

- **Bandwidth is like the number of lanes on a highway**. A network of roads serves every city or town. A data network is much like the highway system. The data packets are comparable to automobiles, and the bandwidth is comparable to the number of lanes on the highway. When a data network is viewed as a system of highways, it is easy to see how low bandwidth connections can cause traffic to become congested all over the network.

Analogies (of Bandwidth)



Measurement

- In digital systems, the basic unit of bandwidth is **bits per second (bps)**
- Bandwidth is the measure of how many bits of information can flow from one place to another in a given amount of time
- Although bandwidth can be described in bps, a larger unit of measurement is generally used
- Network bandwidth is typically described as **thousands of bits per second (kbps), millions of bits per second (Mbps), billions of bits per second (Gbps), and trillions of bits per second (Tbps)**

Measurement

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	kbps	1 kbps = 1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps = 1,000,000,000 bps = 10^9 bps
Terabits per second	Tbps	1 Tbps = 1,000,000,000,000 bps = 10^{12} bps

Measurement

- Although the terms **bandwidth** and **speed** are often used interchangeably, they are not exactly the **same thing**
  - For example, a T3 connection at 45 Mbps operates at a higher speed than a T1 connection at 1.544 Mbps.
  - However, if only a small amount of their data-carrying capacity is being used, each of these connection types will carry data at roughly the same speed

Limitations

- Bandwidth varies depending upon the type of media as well as the LAN and WAN technologies used
- The physics of the media account for some of the difference; signals travel through twisted-pair copper wire, coaxial cable, optical fiber, and air
- The physical differences in the ways signals travel result in fundamental limitations on the information-carrying capacity of a given medium

Limitations

- However, the actual bandwidth of a network is determined by a combination of the physical media and the technologies chosen for signaling and detecting network signals

Maximum Bandwidth and Length Limitation

Some Typical Media	Bandwidth	Max. Physical Distance
50-Ohm Coaxial Cable (Ethernet 10BASE2, ThinNet)	10-100 Mbps	185m
50-Ohm Coaxial Cable (Ethernet 10BASE5, ThickNet)	10-100 Mbps	500m
Category 5 Unshielded Twisted Pair (UTP) (Ethernet 10BASE-T)	10 Mbps	100m
Category 5 Unshielded Twisted Pair (UTP) (Ethernet 100BASE-TX)(Fast Ethernet)	100 Mbps	100m
Multimode (62.5/125µm) Optical Fiber 100BASE-FX	100 Mbps	2000m
Singlemode (9/125µm core) Optical Fiber 1000BASE-LX	1000 Mbps (1.000 Gbps)	3000m
Wireless	11 Mbps	a few 100meters

WAN Services and Bandwidth

Type of WAN service	Typical User	Bandwidth
Modem	Individuals	56 Kbps = 0.056 Mbps
ISDN	Telecommuters, Small businesses	128 Kbps = 0.128 Mbps
Frame-Relay	Small institutions (schools); reliable WANs	56 Kbps - 1544Kbps = 0.056 Mbps - 1.544 Mbps
T1	Larger entities	1.544 Mbps
T3	Larger entities	44.736 Mbps
E1	Larger entities	2.048 Mbps
E3	Larger entities	34.368 Mbps

Throughput

- **Throughput** refers to actual measured bandwidth, at a specific time of day, using specific Internet routes, and while a specific set of data is transmitted on the network. Unfortunately, for many reasons, throughput is often far less than the maximum possible digital bandwidth of the medium that is being used.

Throughput

- The following are some of the factors that determine throughput:
  - Internetworking devices
  - Type of data being transferred
  - Network topology
  - Number of users on the network
  - User computer
  - Server computer
  - Power conditions

Throughput Variables

NETWORK TRAINING CENTER

Throughput ≤ Digital Bandwidth of a Medium

- PC (client)
- Server
- Other users on the LAN
- Routing within the "Cloud"
- Design, or topology, of all networks involved
- Type of data being transferred
- Time of day

Data Transfer Calculation

- Decisions regarding bandwidth:
  - One decision might be whether to **increase the size of the WAN connection**
  - Another decision might be whether the **current LAN backbone is of sufficient bandwidth**
- The answers to problems like these are not always easy to find, but one place to start is with a simple data transfer calculation.

Data Transfer Calculation

Best Download

$$T = \frac{S}{BW}$$

Typical Download

$$T = \frac{S}{P}$$

BW	Maximum theoretical bandwidth of the "slowest link" between the source host and the destination host (measured in bits per second)
P	Actual throughput at the moment of transfer (measured in bits per second)
T	Time for file transfer to occur (measured in seconds)
S	File size in bits

Digital Versus Analog

- **Analog bandwidth** is measured by how much of the electromagnetic spectrum is occupied by each signal; the basic unit of analog bandwidth is **hertz (Hz)**, or cycles per second.
- While analog signals are capable of carrying a variety of information, they have some significant disadvantages in comparison to digital transmissions.
- The analog video signal that requires a wide frequency range for transmission cannot be squeezed into a smaller band; therefore, if the necessary analog bandwidth is not available, the signal cannot be sent.

Digital Versus Analog

- In **digital signaling** all information is sent as bits, regardless of the kind of information it is
- Voice, video, and data all become streams of bits when they are prepared for transmission over digital media
- This type of transmission gives digital bandwidth an important advantage over analog bandwidth
- Unlimited amounts of information can be sent over the smallest or lowest bandwidth digital channel

Digital Versus Analog

Bandwidth (digital) is like analog bandwidth.

Network devices are like phones, AM/FM radios, and CD ROM players.

Packets are like music.

Q&A

CCNA Semester 1

NETWORK TRAINING CENTER

The **Cisco Certified Network Associate** Curriculum

Chapter 04

NETWORKING MEDIA

Objectives

- *Describe coaxial cable and its advantages and disadvantages over other types of cable.*
- *Describe shielded twisted-pair (STP) cable and its uses.*
- *Describe unshielded twisted-pair cable (UTP) and its uses.*
- *Discuss the characteristics of straight-through, crossover, and rollover cables and where each is used.*
- *Explain the basics of fiber-optic cable.*
- *Describe the type of connectors and equipment used with fiber-optic cable*

Objectives

- *Compare and contrast noise levels on various types of cabling.*
- *Define and describe the affects of attenuation and impedance mismatch.*
- *Define crosstalk, near-end crosstalk, far-end crosstalk, and power sum near-end crosstalk.*
- *Describe how crosstalk and twisted pairs help reduce noise.*
- *Describe the ten copper cable tests defined in TIA/EIA-568-B.*
- *Describe the difference between Category 5 and Category 6 cable.*

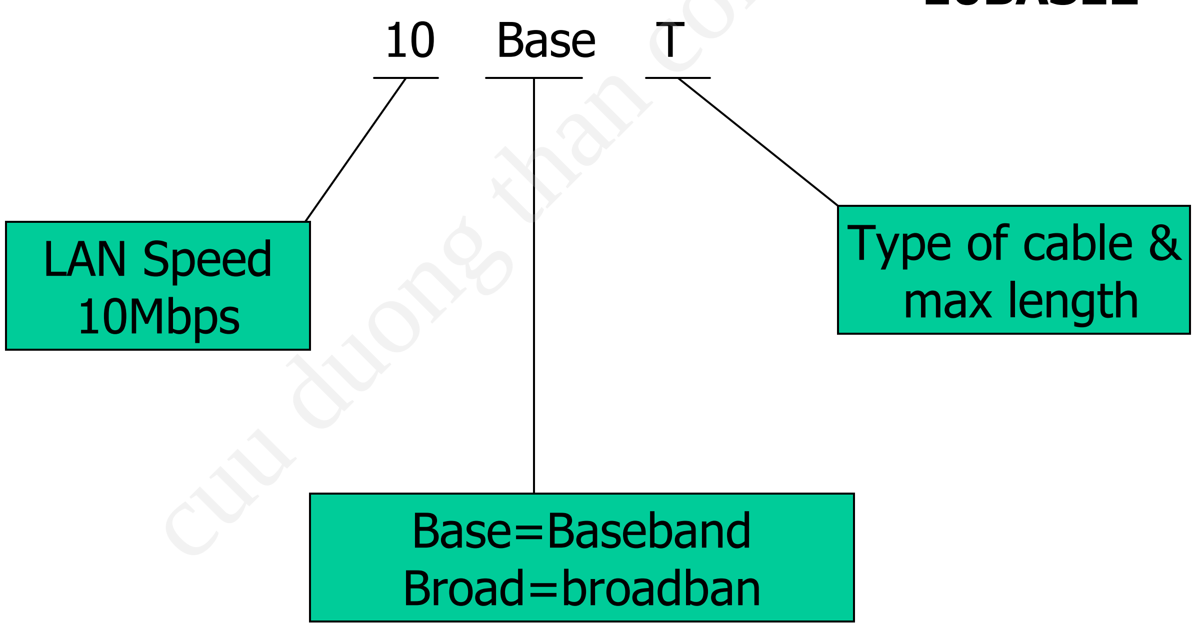
Table of Content

COPPER MEDIA

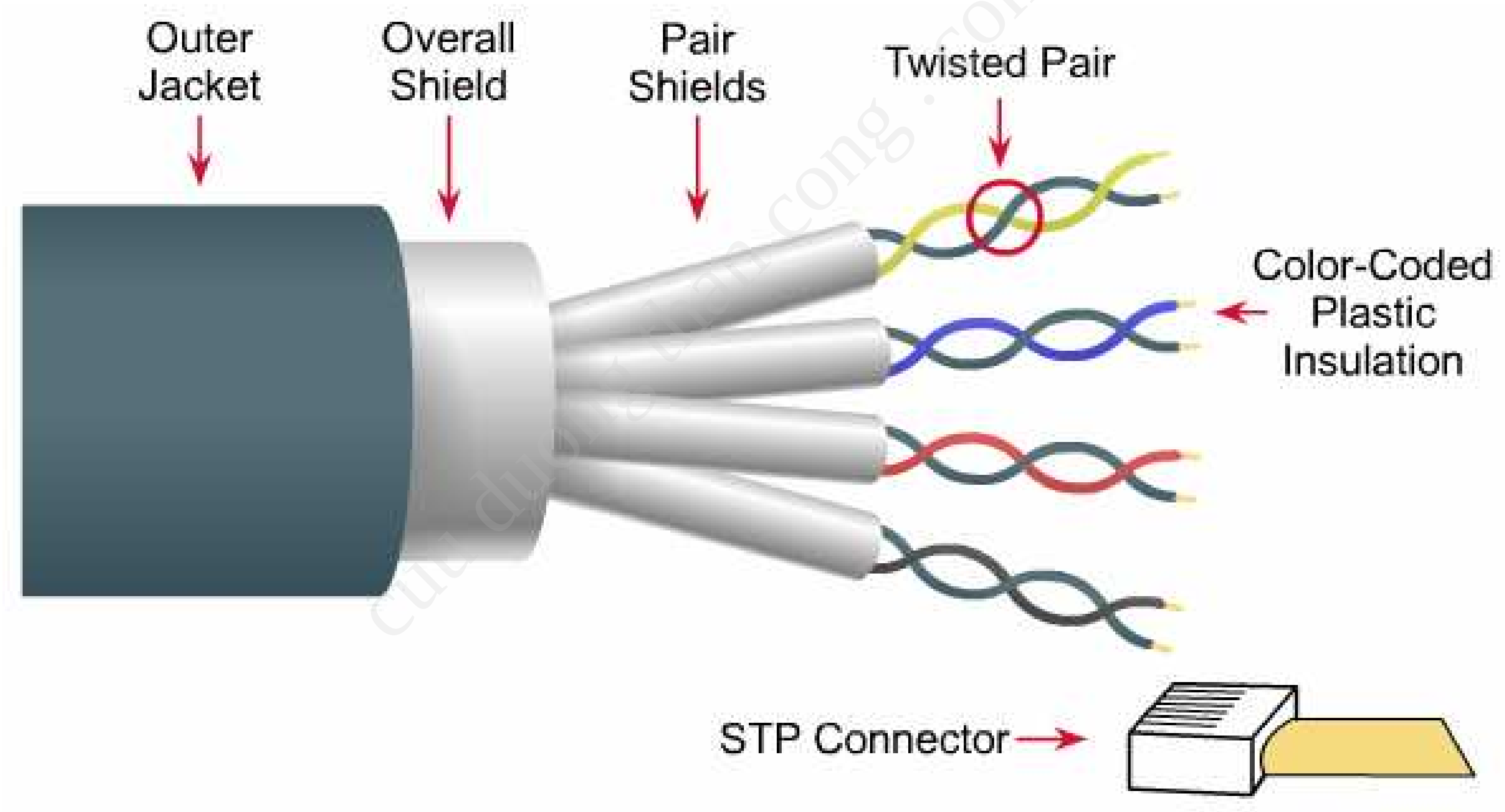
Cable Specifications

NETWORK TRAINING CENTER

e.g.
10BASE-T
10BASE5
10BASE2



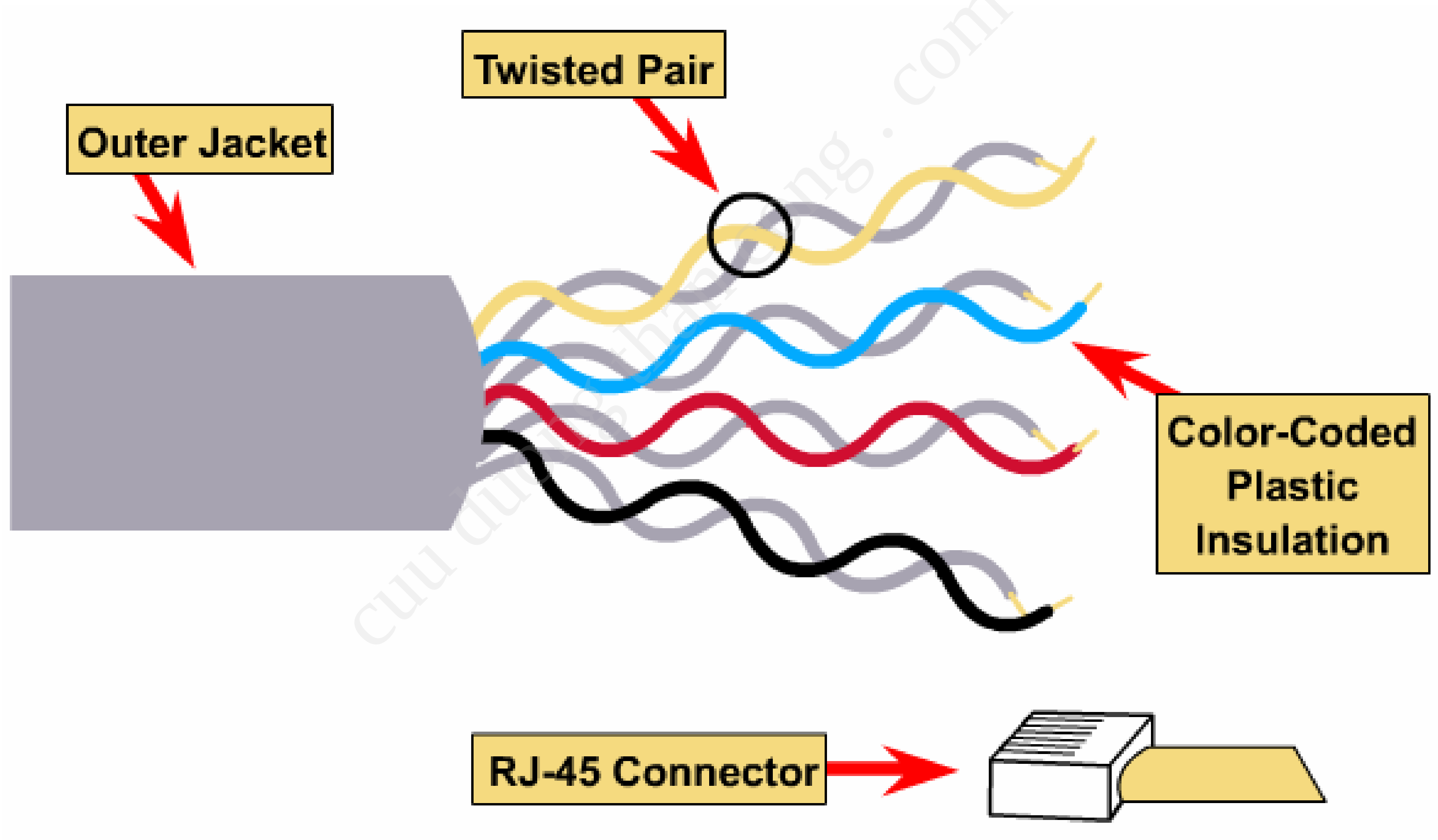
Shielded twisted-pair (STP)



Shielded twisted-pair (STP)

- Protection from all types of external interference, include EMI and RFI.
- Cancellation: twisting of wires.
- Shielding.
- More expensive.
- Maximum cable length 100m.
- 150Ω for Token ring.

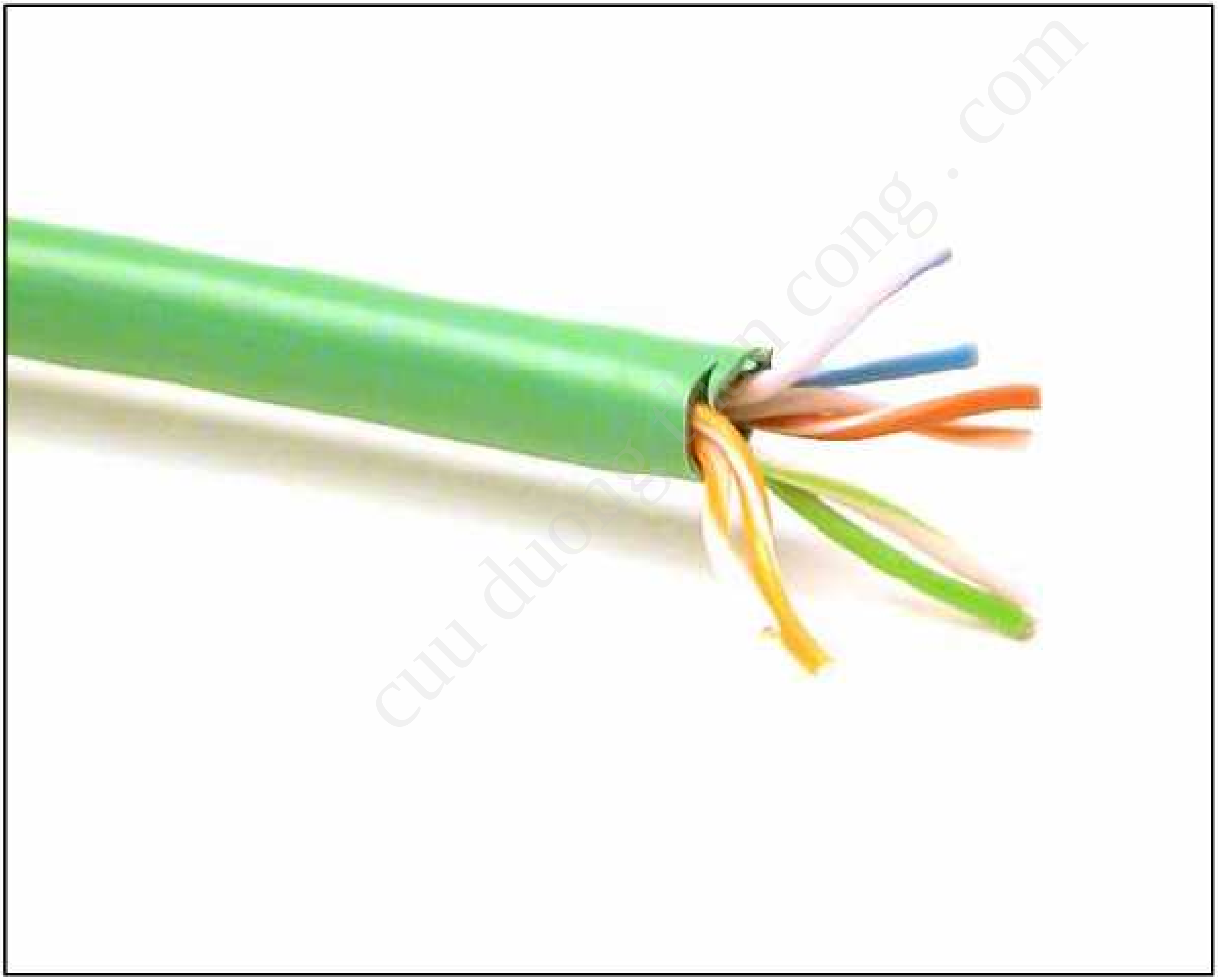
Unshielded twisted-pair (UTP)



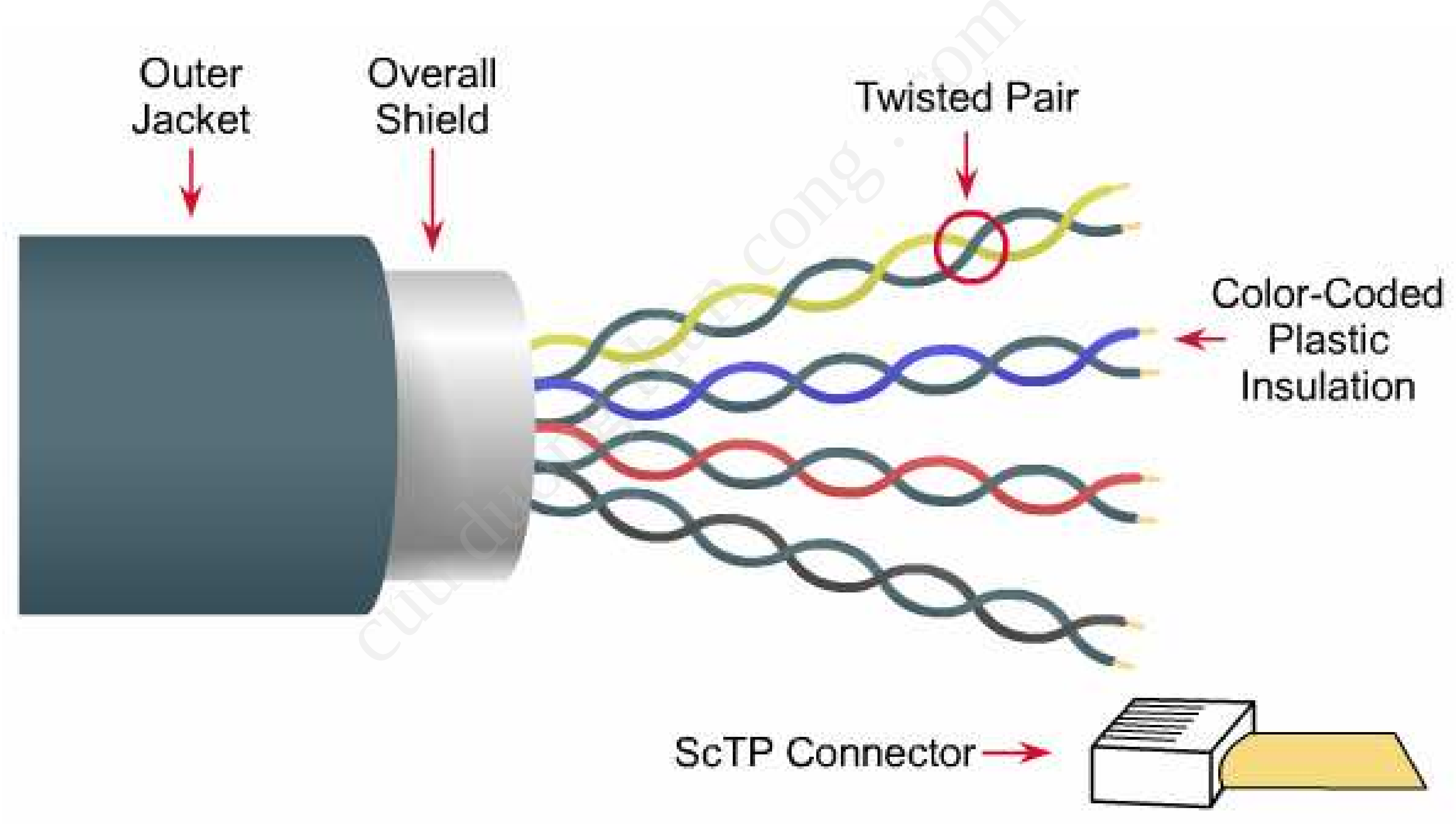
Unshielded twisted-pair (UTP)

- Cancellation: twisted wire pairs.
- More prone to EMI (*electromagnetic interference*) /RFI (*radio frequency interference.*) than any other cable.
- Least expensive of all media, small diameter of cable, easy to install.
- Maximum cable length 100m.
- 100Ω for Ethernet.

Unshielded twisted-pair (UTP)



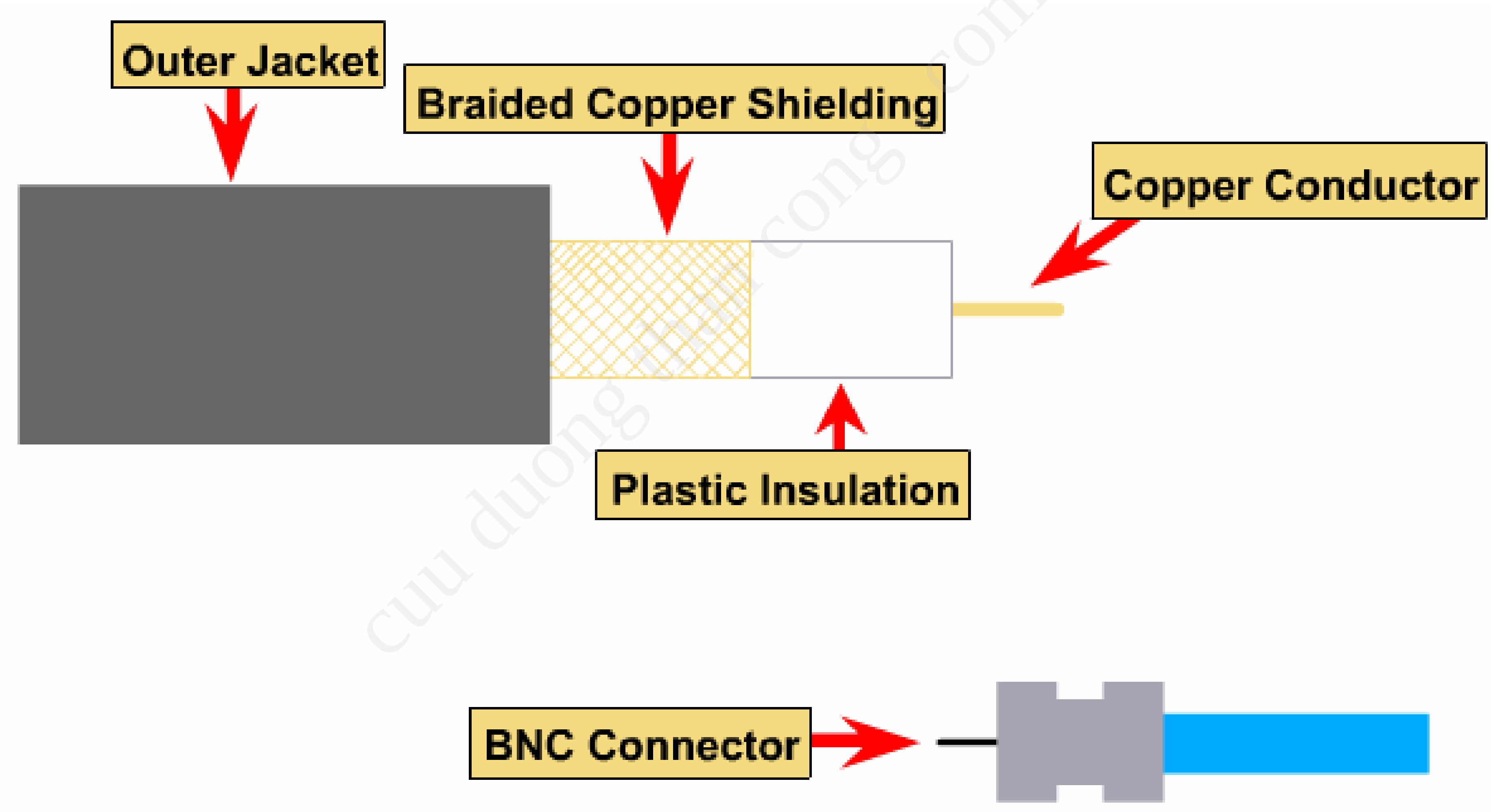
Screened Twisted-pair (ScTP – FTP)



Screened Twisted-pair (ScTP – FTP)

- Hybrid of UTP with STP.
- Maximum cable length 100m.
- 100Ω for Ethernet.

Coaxial Cable



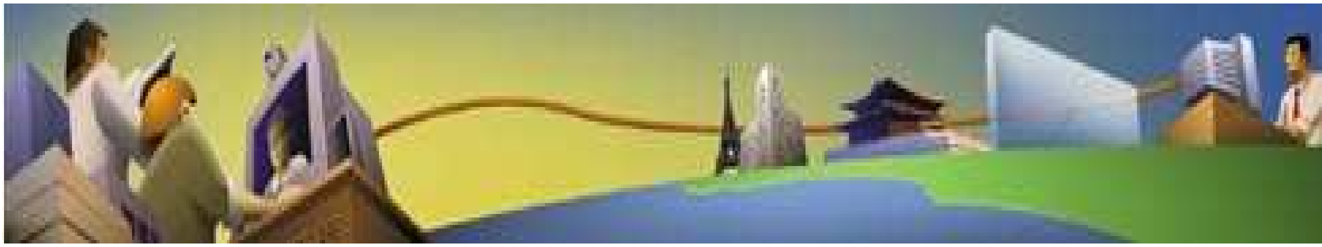
Coaxial Cable

- Technology is well known (Cable TV).
- The shield can help reduce the amount of outside interference.
- Longer cable runs than UTP & STP.
- Maximum cable length :
  - Thin cable : 185 m.
  - Thick cable : 500 m.
- 50Ω for Ethernet.

Coaxial Cable

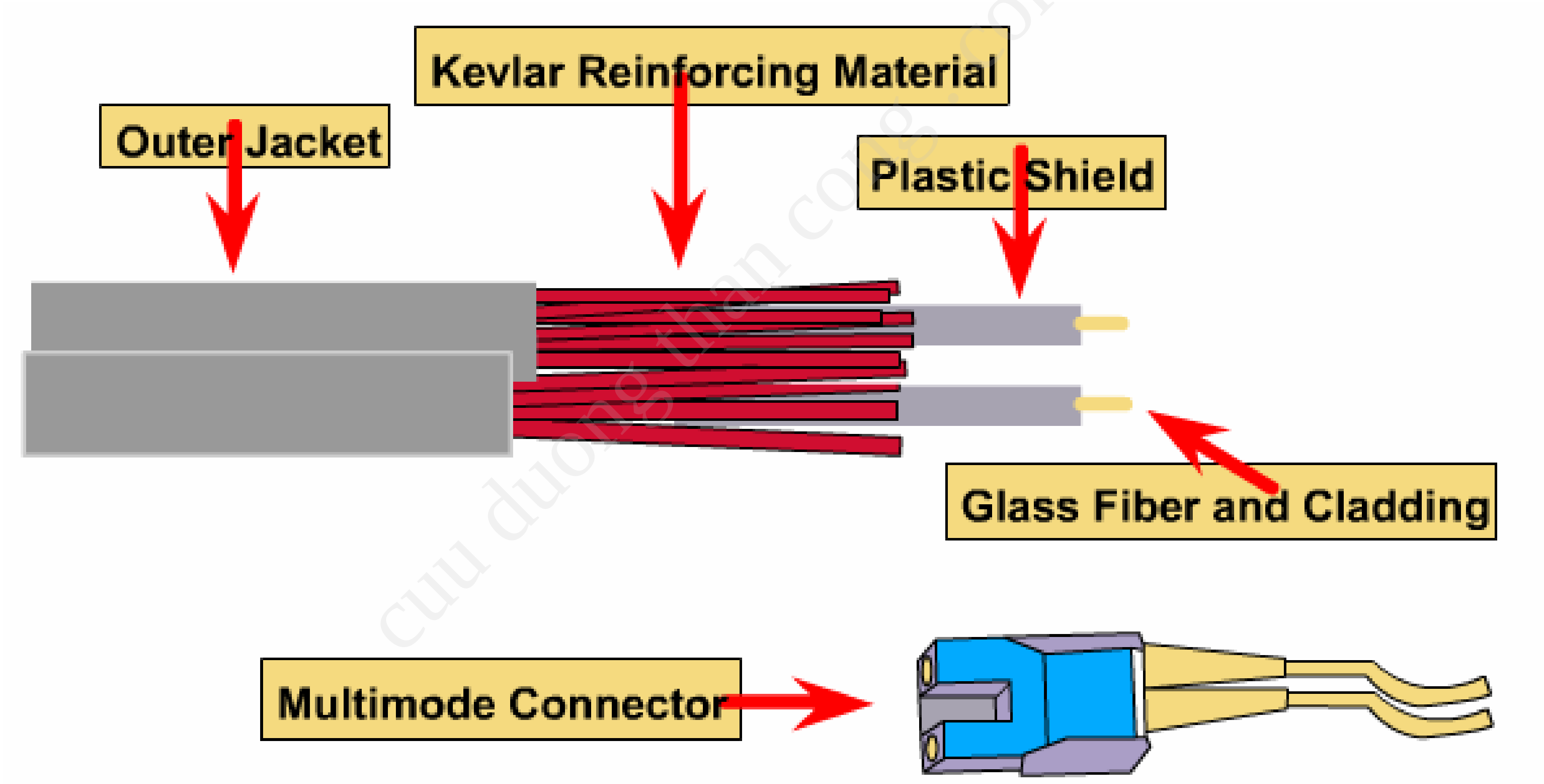
Coaxial Cable

NETWORK TRAINING CENTER



OPTICAL CABLE

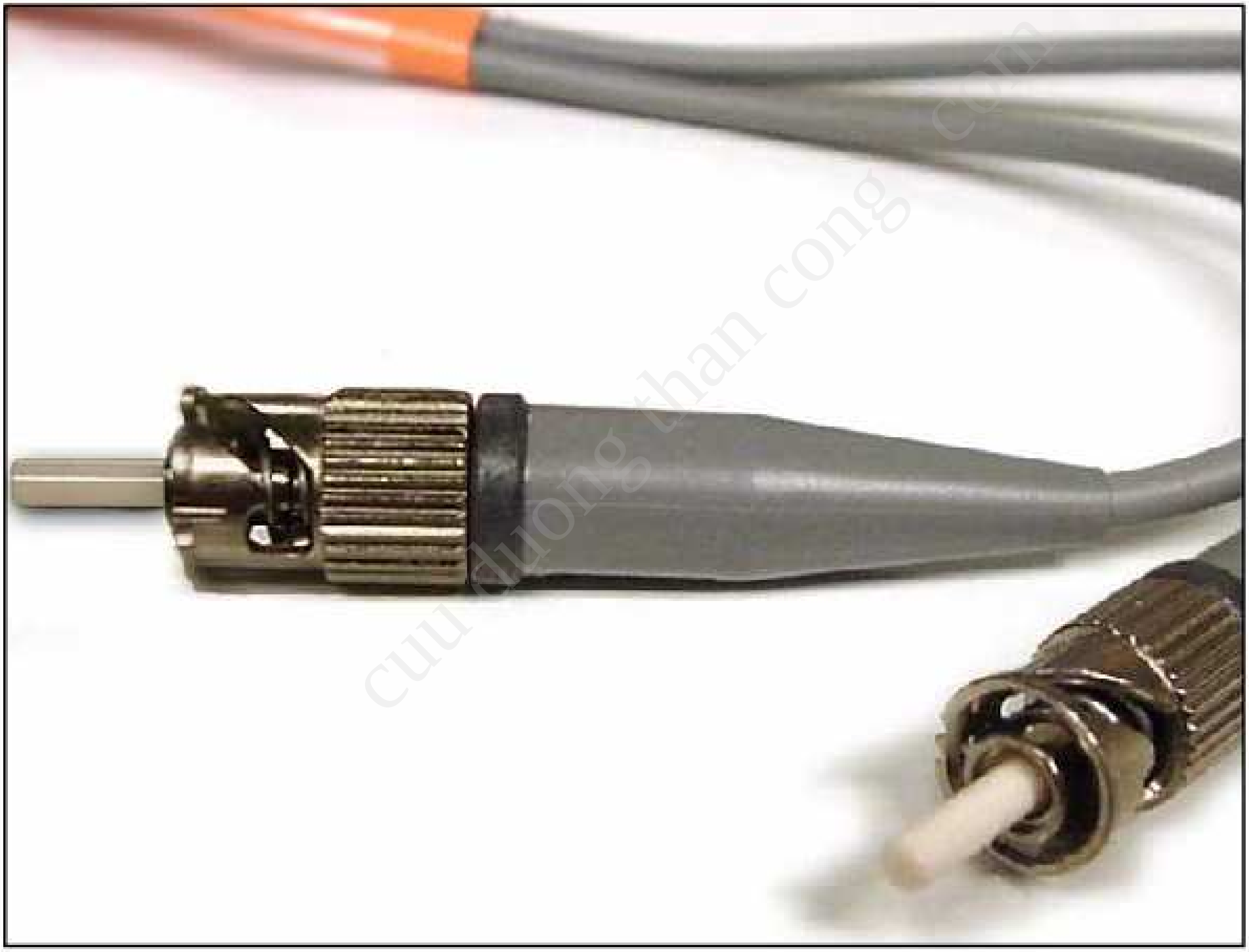
Fiber Optic Cable



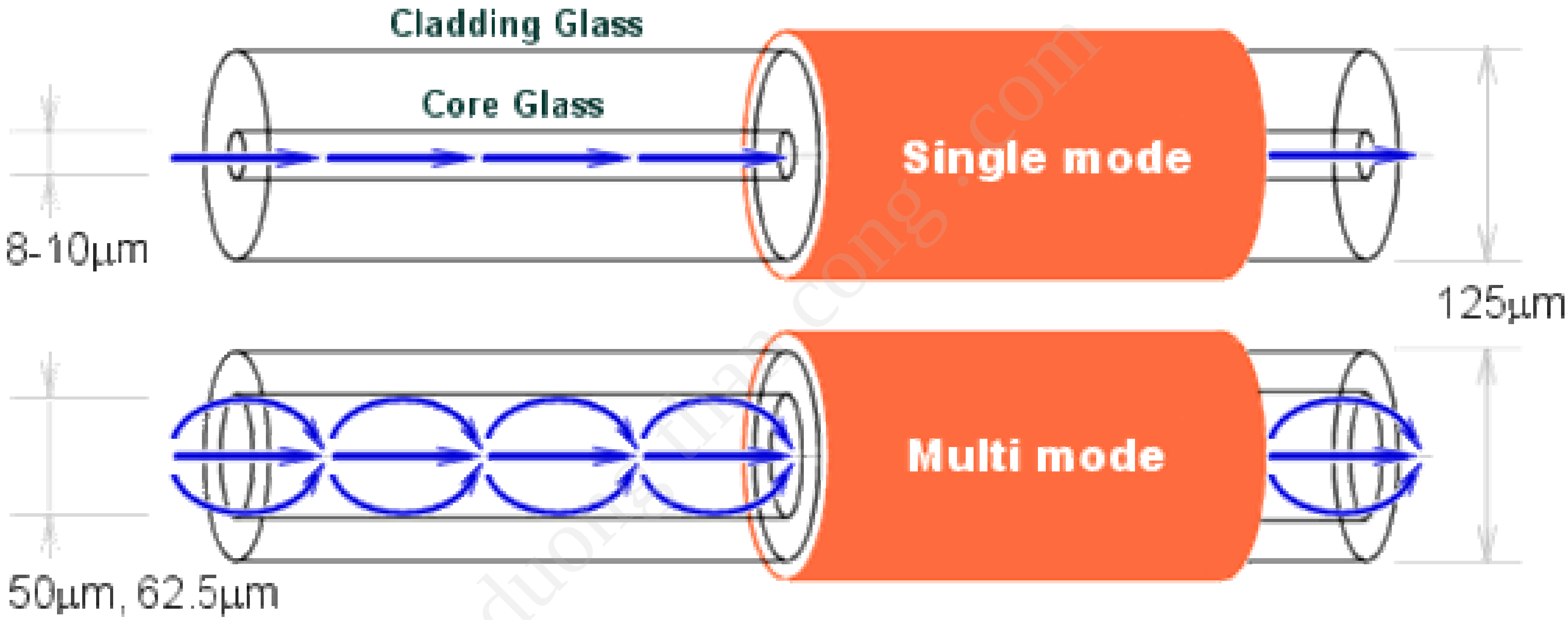
Fiber Optic Cable

- Medium capable of light transmissions.
- Higher data rates (>100Mbps).
- NO EMI and RFI.
- Very expensive.
- Difficult to install.
- Maximum cable length :
  - Single Mode : 3000 m.
  - Multi Mode : 2000 m.

Fiber Optic Cable



Single mode and multi mode



- Single: Light to travel in a straight line.
- Multi: Light to travel multiple paths.

WIRELESS MEDIA

Wireless LAN Organizations And Standards

- A key technology contained within the 802.11 standard is Direct Sequence Spread Spectrum (DSSS).
- DSSS applies to wireless devices operating within a 1 to 2 Mbps range.
- 802.11b increased transmission capabilities to 11 Mbps.
- 802.11a covers WLAN devices operating in the 5 GHZ transmission band
- 802.11g provides the same throughout as 802.11a but with backwards compatibility for 802.11b devices using Othogonal Frequency Division Multiplexing (OFDM) modulation technology.

Wireless Devices And Topologies

- Nodes could simply be hosts equipped with wireless NICs
- An access point installed to act as a central hub
- APs are equipped with antennae and provide wireless connectivity over a specified area referred to as a cell.

How Wireless Lans Communicate

- A node will pass frames in the same manner as on any other 802.x network.
- There are three types of frames: control, management, and data.
- A wireless frame could be as large as 2346 bytes.
- Collisions can occur just as they do on wired shared medium.
- WLANs use Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). This is somewhat like Ethernet CSMA/CD.
- When a source node sends a frame, the receiving node returns a positive acknowledgment (ACK).

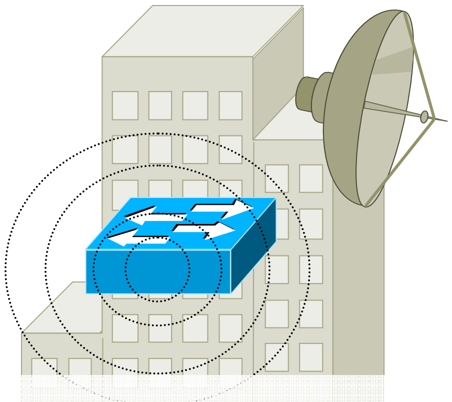
Authentication and Association

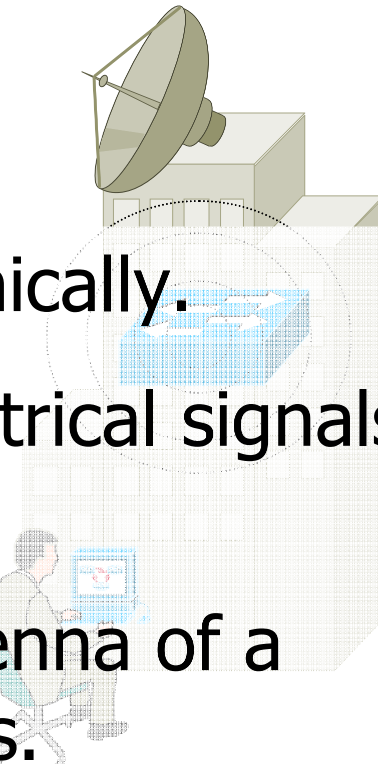
- WLAN authentication, occurring at Layer 2 is the process of authenticating the device not the user.
- Association is the state that permits a client to use the services of the AP to transfer data

Authentication and Association Types

- Unauthenticated and unassociated
  - The node is disconnected from the network and not associated to an access point.
- Authenticated and unassociated
  - The node has been authenticated on the network but has not yet associated with the access point.
- Authenticated and associated
  - The node is connected to the network and able to transmit and receive data through the access point.
- The first authentication process is the open system.
- The second process is the shared key.

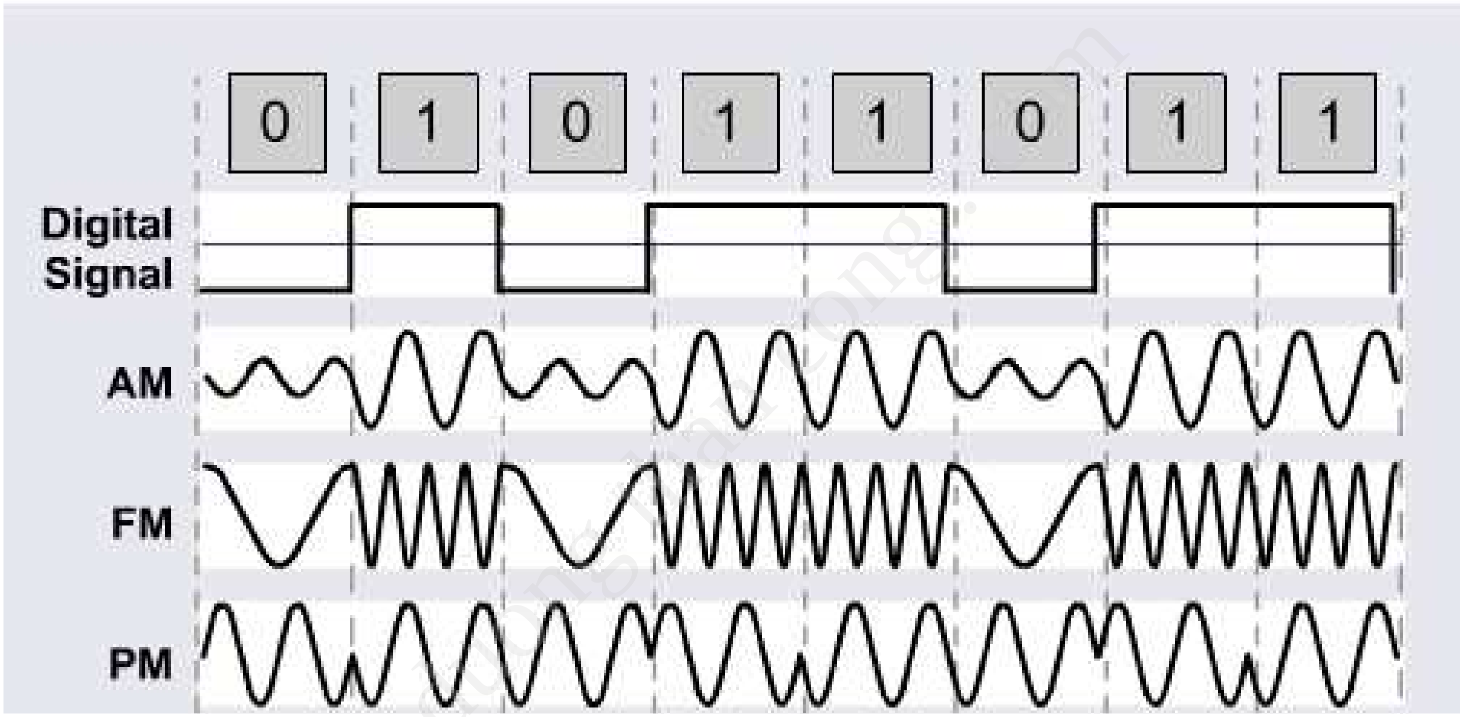
The Radio Wave And Microwave Spectrums



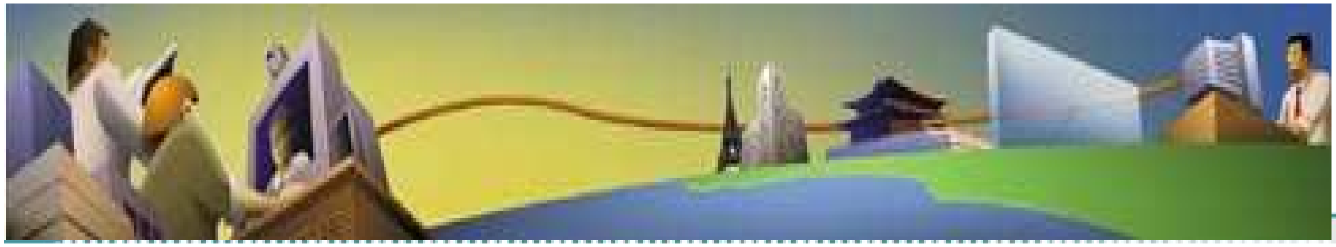


- Computers send data signals electronically.
- Radio transmitters convert these electrical signals to radio waves.
- Changing electric currents in the antenna of a transmitter generates the radio waves.
- These radio waves radiate out in straight lines from the antenna

Modulation



- The process of altering the carrier signal that will enter the antenna of the transmitter is called modulation.
- Amplitude Modulated, Frequency Modulated, Phase modulation



MAKING CABLE - LAB

TIA/EIA-568-A: Twisted-pair cables

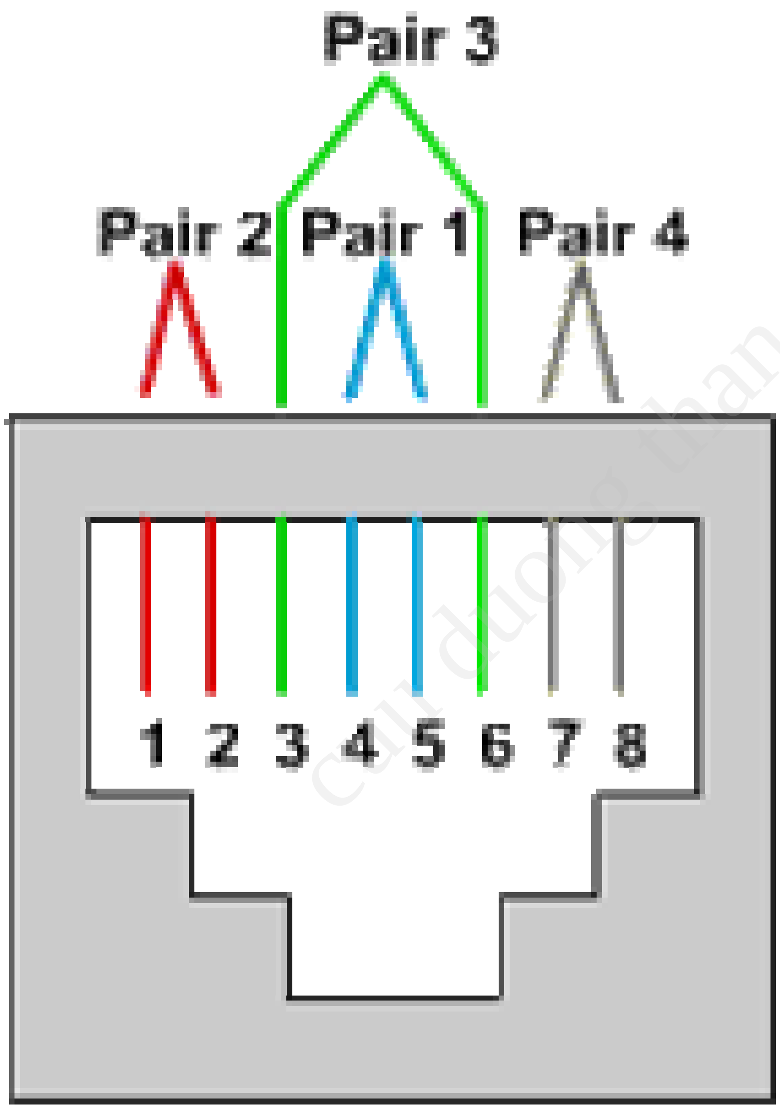
- Category 1 is used for telephone and is not suitable for transmitting data.
- Category 2 is capable of transmitting data at speeds up to 4 Mbps.
- Category 3 is used in Ethernet, and can transmit data at speeds up to 10 Mbps.
- Category 4 is used in Token Ring, and can transmit data at speeds up to 16 Mbps.
- Category 5 can transmit data at speeds up to 100 Mbps.

Making cables

- Making Ethernet 100Base-T cables:
  - Straight-thru cable: PC-to-HUB.
  - Crossover cable: PC-to-PC.

- Making console cables:
  - Rollover cable:
    - Serial port-to-console port of Cisco equipments.

100Base-T: NIC network port



1: Transmit

2: Transmit

3: Receive

4: Not used

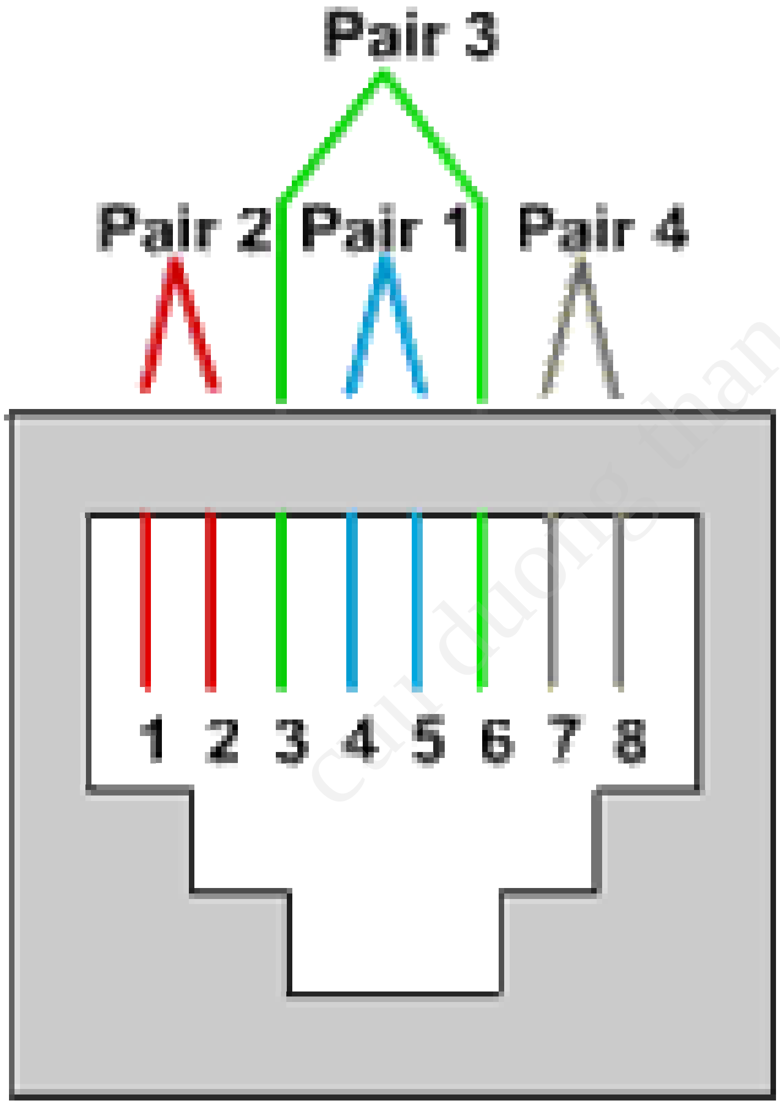
5: Not used

6: Receive

7: Not used

8: Not used

100Base-T: HUB network port



1: Receive

2: Receive

3: Transmit

4: Not used

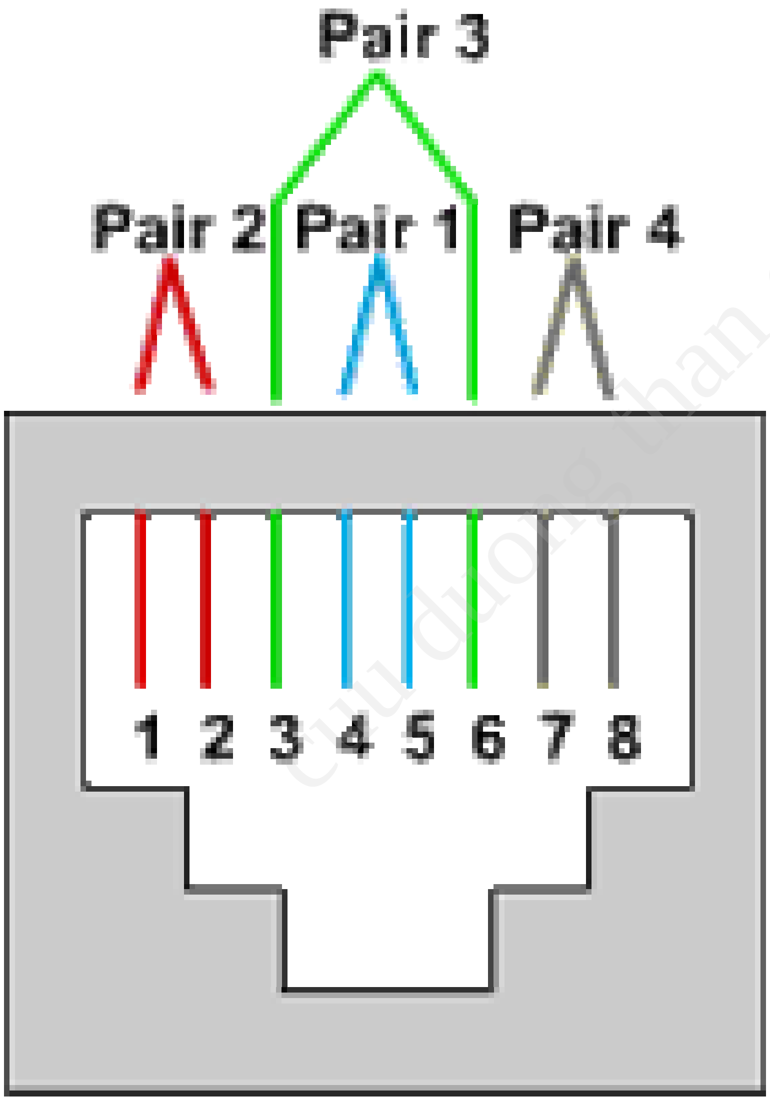
5: Not used

6: Transmit

7: Not used

8: Not used

100Base-T: T568-B



1: White Orange

2: Orange

3: White Green

4: Blue

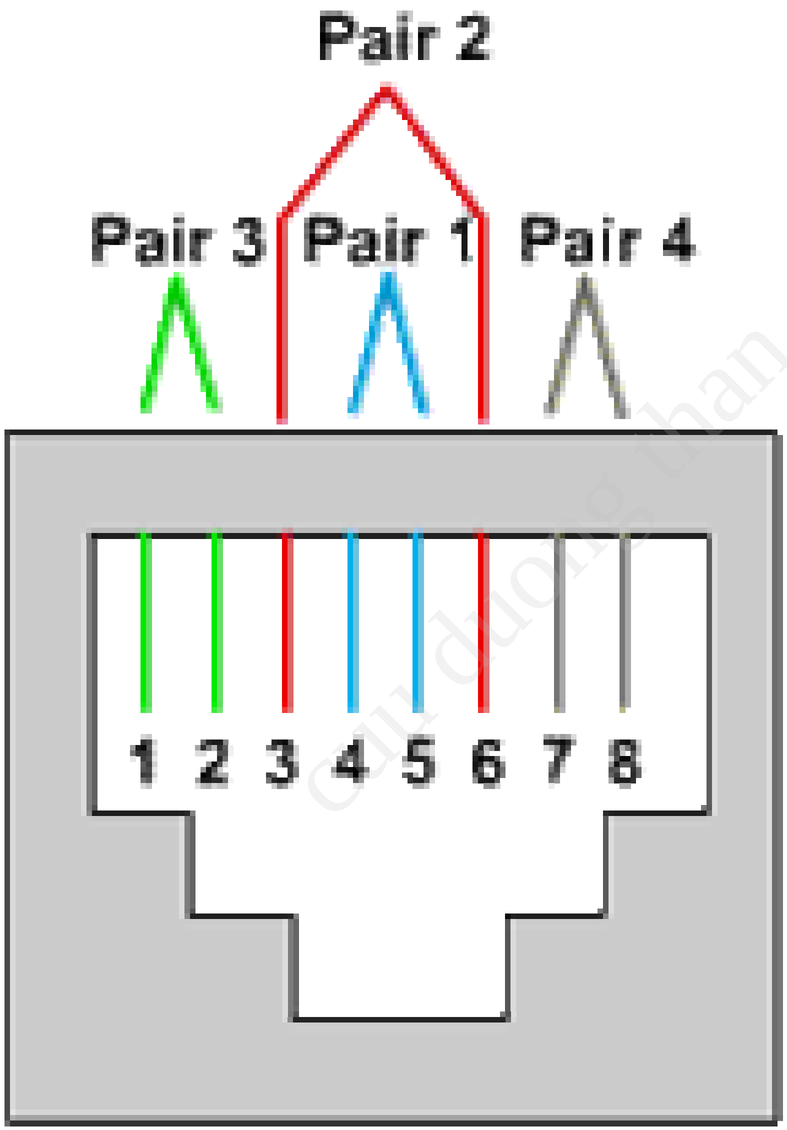
5: White Blue

6: Green

7: White Brown

8: Brown

100Base-T: T568-A



1: White Green
2: Green
3: White Orange
4: Blue
5: White Blue
6: Orange
7: White Brown
8: Brown

Straight-through Cable

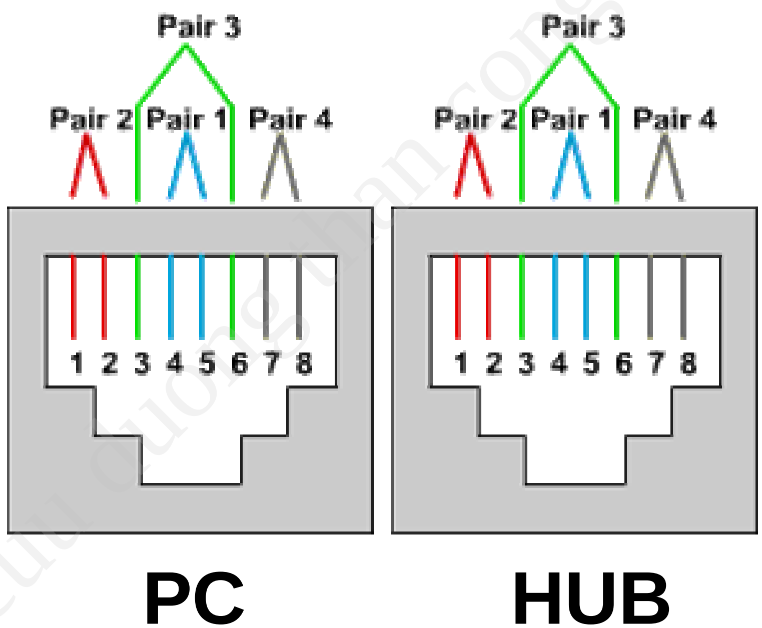
NETWORK TRAINING CENTER

Pin 1	Pin 1
Pin 2	Pin 2
Pin 3	Pin 3
Pin 4	Pin 4
Pin 5	Pin 5
Pin 6	Pin 6
Pin 7	Pin 7
Pin 8	Pin 8

100Base-T: Straight-thru cable

NETWORK TRAINING CENTER

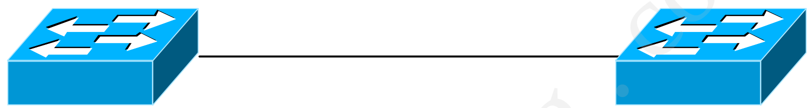
1: White Orange
2: Orange
3: White Green
4: Blue
5: White Blue
6: Green
7: White Brown
8: Brown



1: White Orange
2: Orange
3: White Green
4: Blue
5: White Blue
6: Green
7: White Brown
8: Brown

Crossover Cable

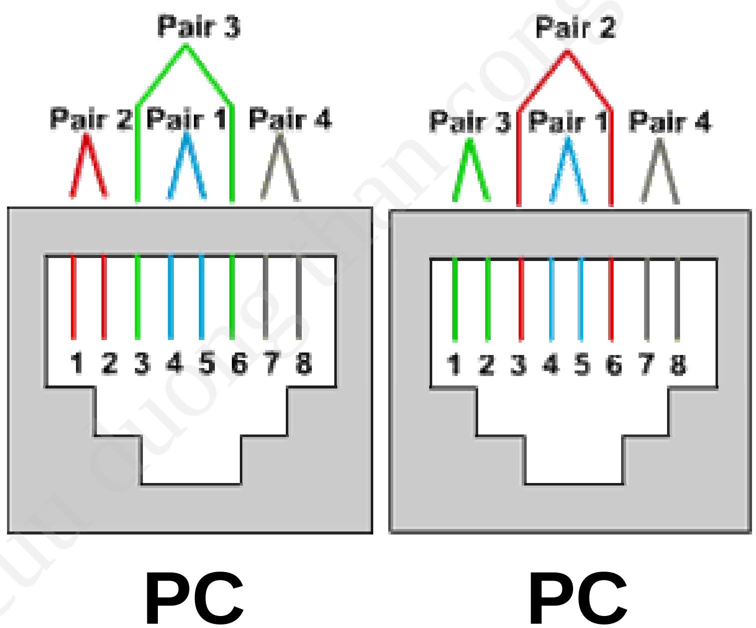
NETWORK TRAINING CENTER



Pin 1	Pin 3
Pin 2	Pin 6
Pin 3	Pin 1
Pin 4	Pin 4
Pin 5	Pin 5
Pin 6	Pin 2
Pin 7	Pin 7
Pin 8	Pin 8

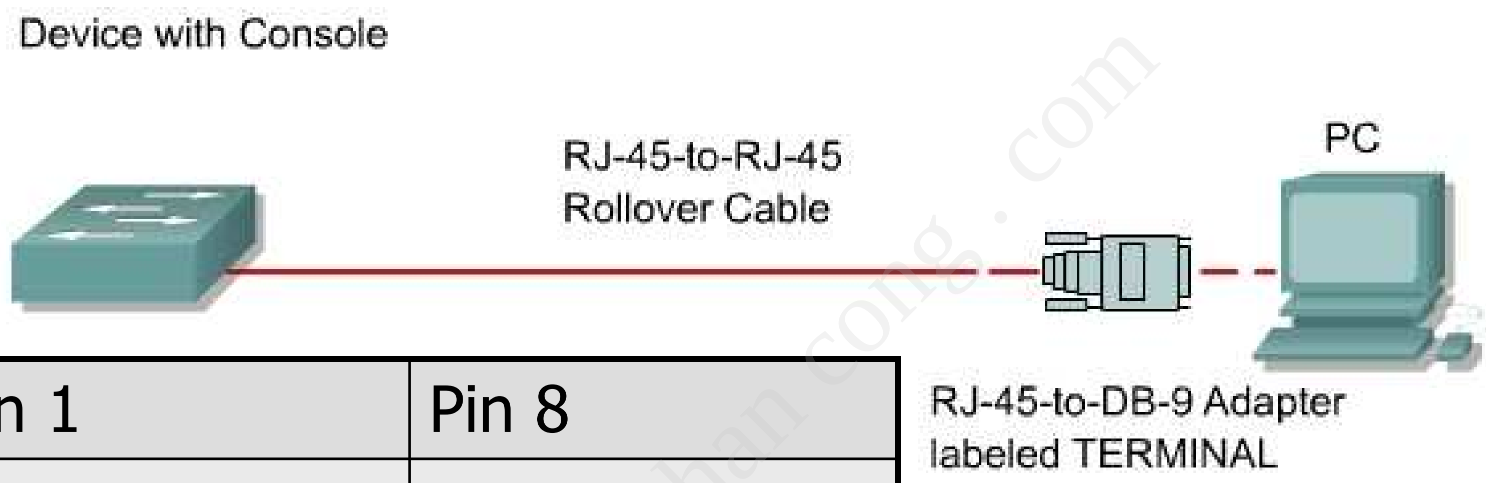
100Base-T: Crossover cable

1: White Orange
2: Orange
3: White Green
4: Blue
5: White Blue
6: Green
7: White Brown
8: Brown



1: White Green
2: Green
3: White Orange
4: Blue
5: White Blue
6: Orange
7: White Brown
8: Brown

Rollover Cable



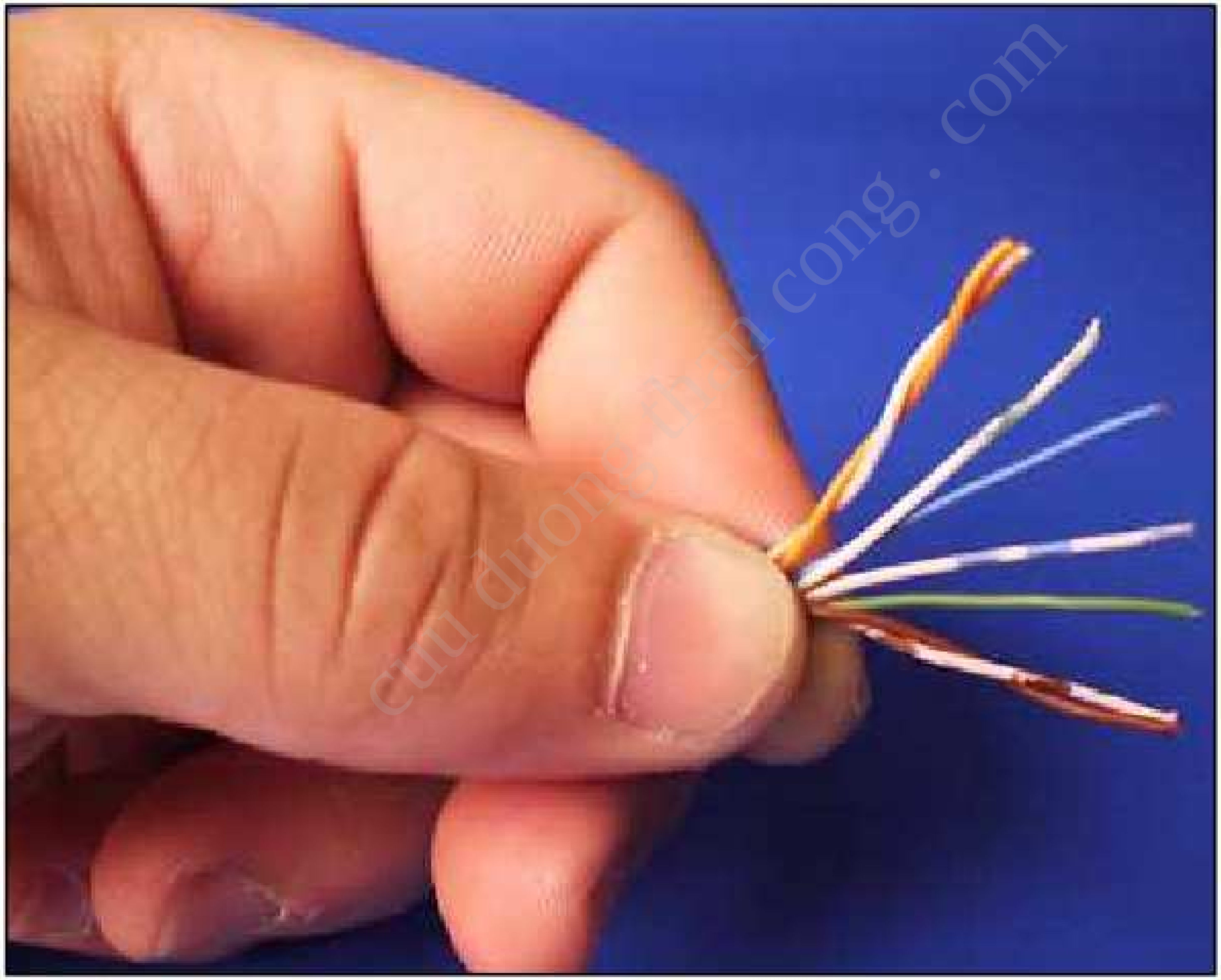
Pin 1	Pin 8
Pin 2	Pin 7
Pin 3	Pin 6
Pin 4	Pin 5
Pin 5	Pin 4
Pin 6	Pin 3
Pin 7	Pin 2
Pin 8	Pin 1

100Base-T: Cut a length of cable

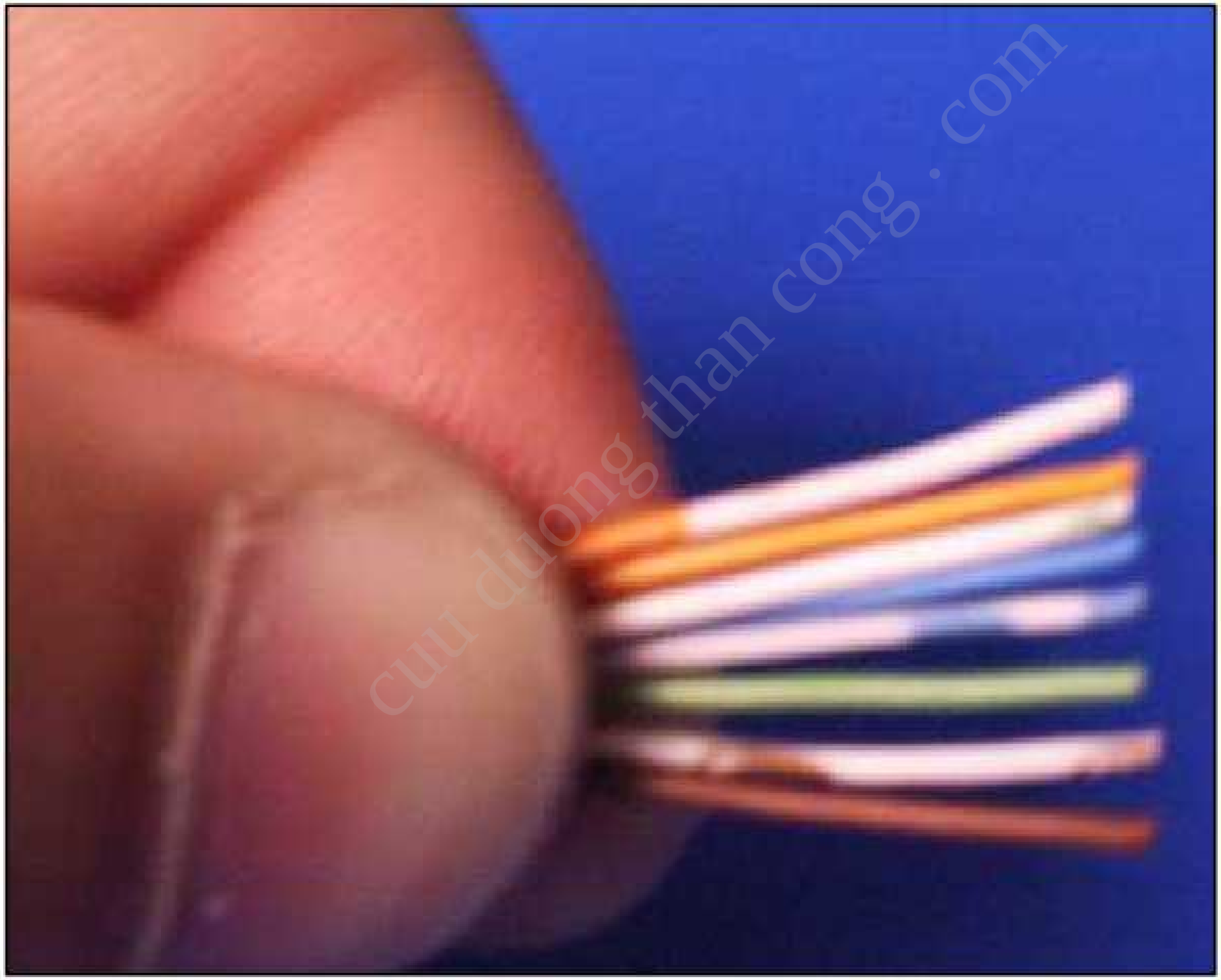
100Base-T: Strip off the jacket

100Base-T: Separate the wires

100Base-T: Untwist the wires

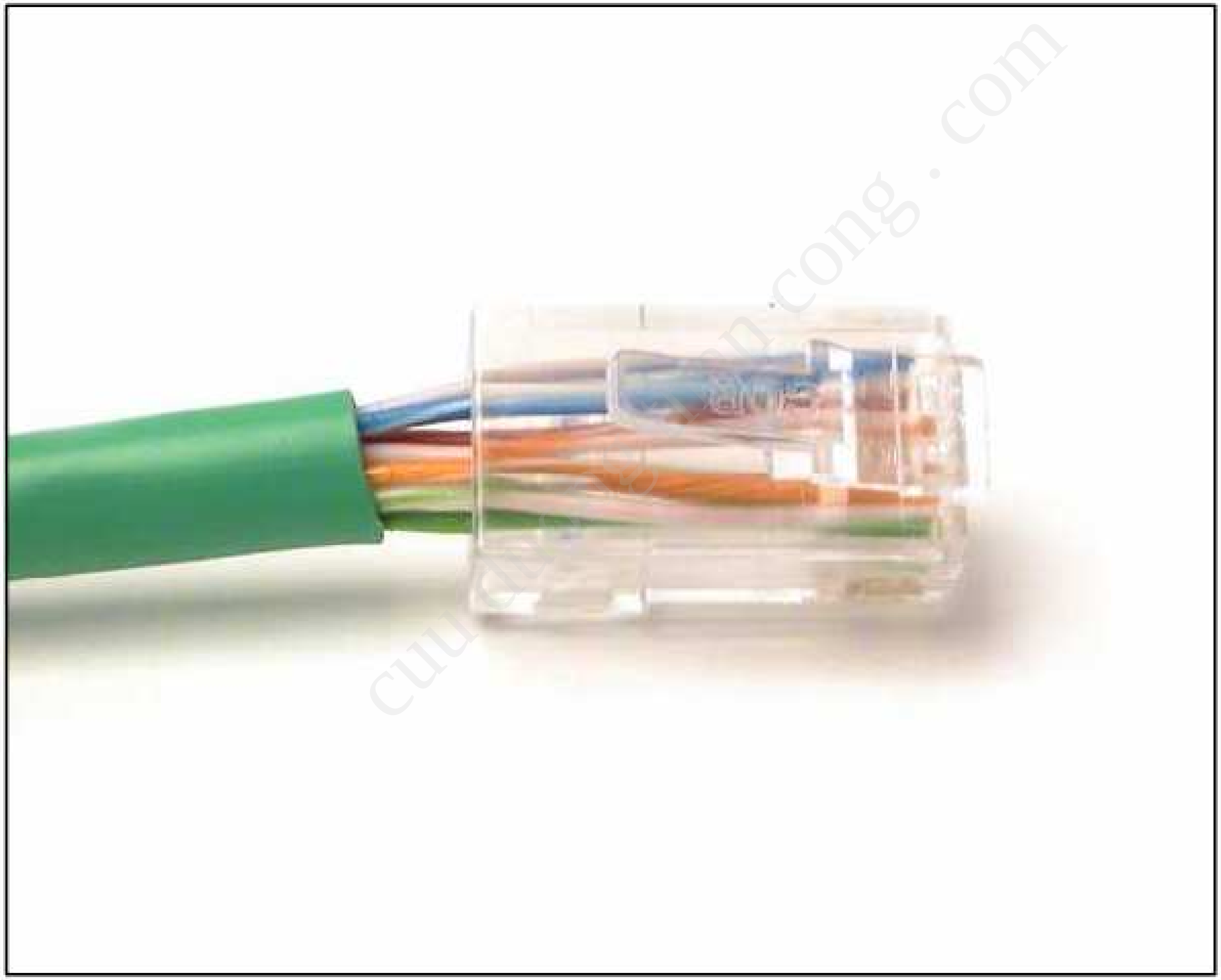


100Base-T: Organize and flatten wires

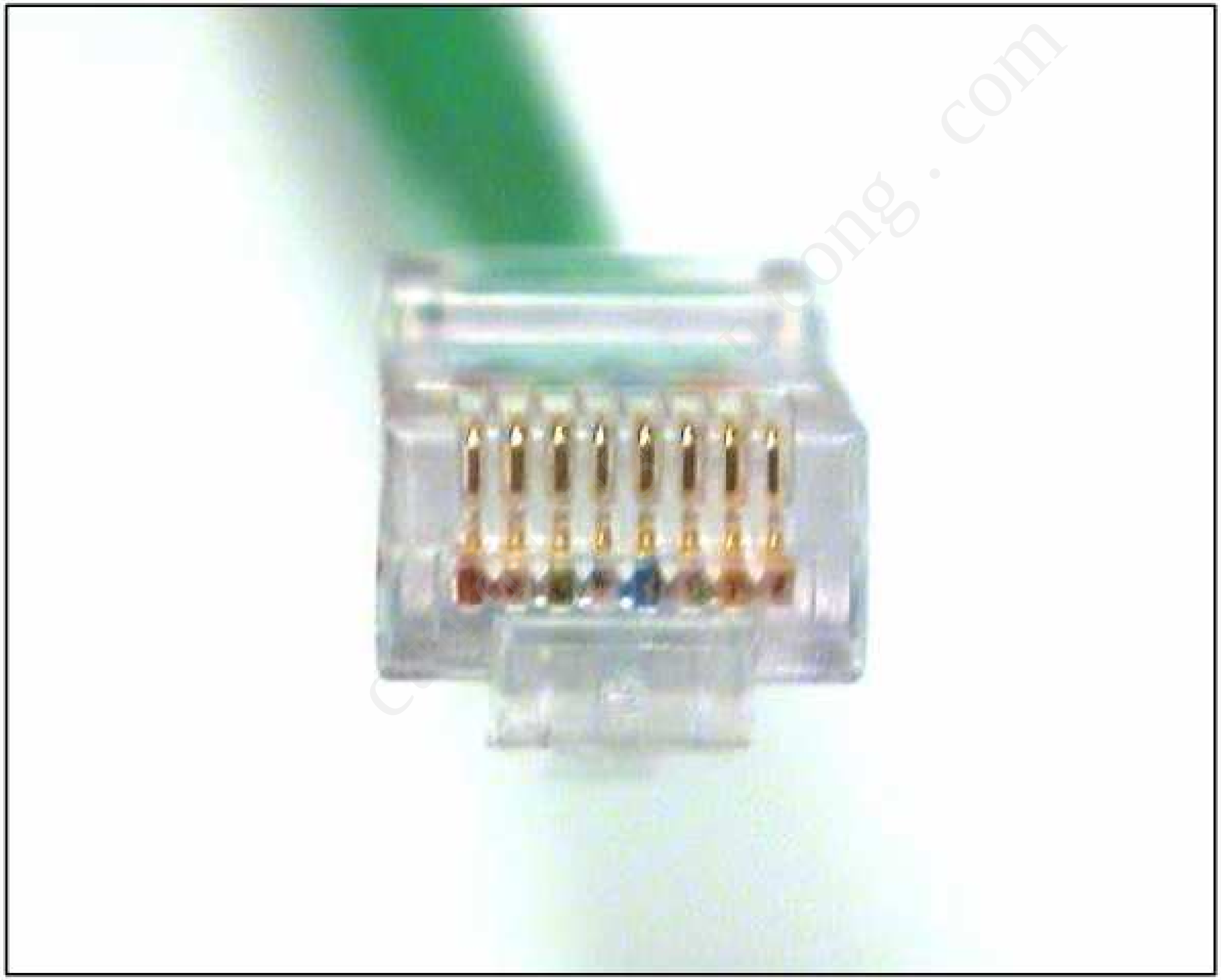


100Base-T: Clip the wires

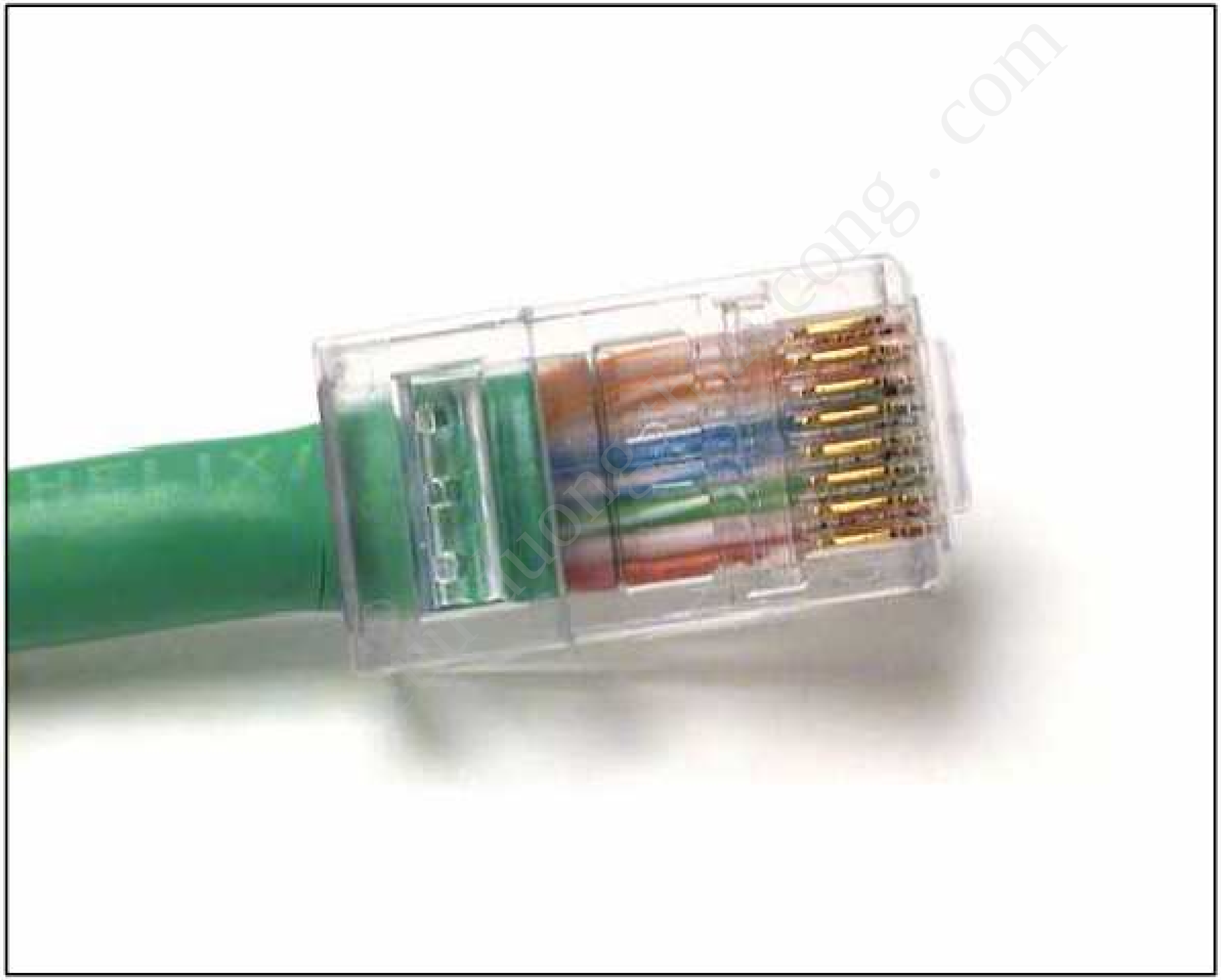
100Base-T: Insert wires into RJ-45 plug



100Base-T: Push the wires in



100Base-T: Inspect the color code



100Base-T: Crimp down the wires

100Base-T: Inspect both ends

100Base-T: Test the quality of cable

Preparation for LAB

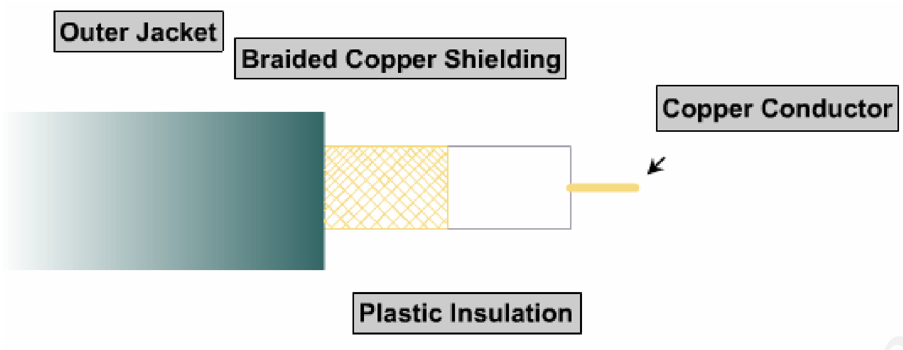
- Lab:
  - Straight-through cable.
  - Crossover cable.
  - Cable tester – wire map.

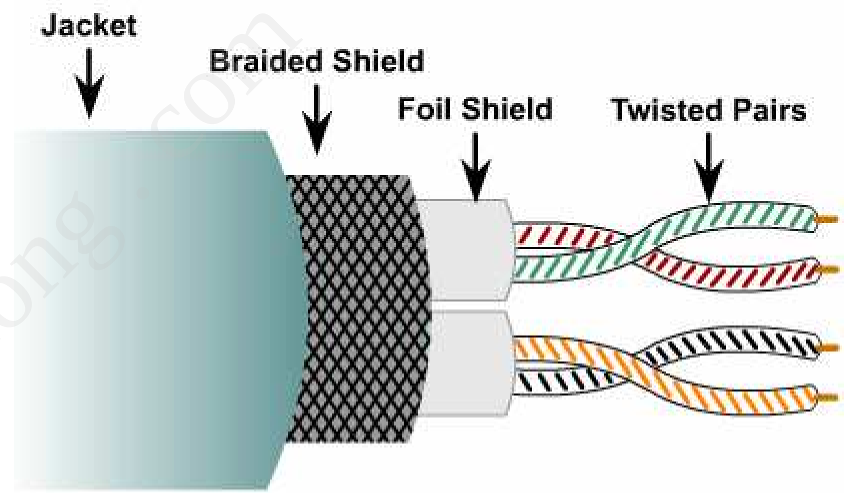
SIGNALS AND NOISE

Signaling Over Copper

- On copper cable, data signals are represented by voltage levels that represent binary ones and zeros.
- It is important for devices that transmit and receive data to have the same 0-volt reference point (signal ground)

Signaling Over Copper (cont.)





- In shielded cable, shielding material protects the data signal from external sources of noise and from noise generated by electrical signals within the cable.
- In LAN applications, the braided shielding is electrically grounded to protect the inner conductor from external electrical noise

Signaling Over Fiber Optic Cabling

- Fiber optic cable is used to transmit data signals by increasing and decreasing the intensity of light to represent binary ones and zeros.
- Not affected by electrical noise, and does not need to be grounded.
- Therefore, optical fiber is often used between buildings and between floors within the building.

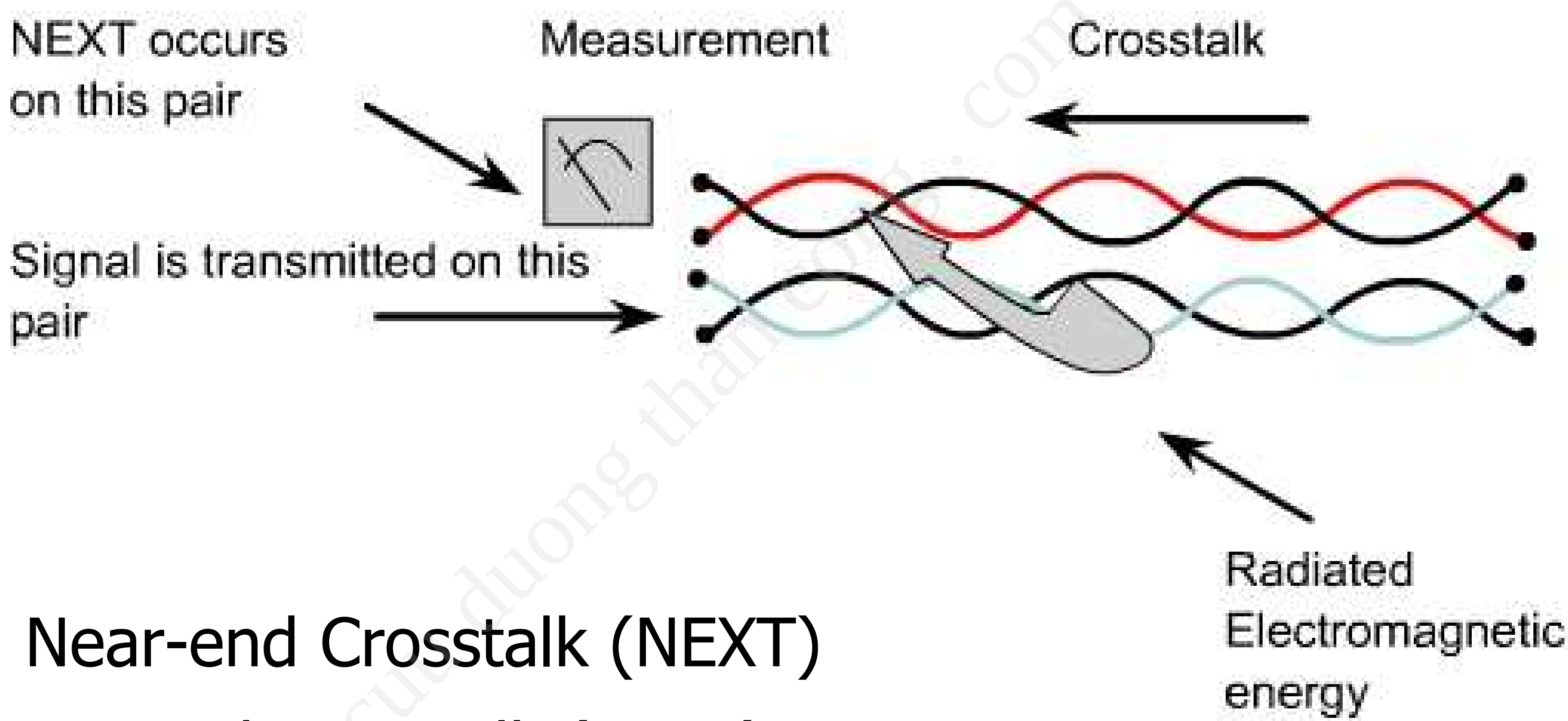
Attenuation And Insertion Loss On Copper Media

- Attenuation is the decrease in signal amplitude over the length of a link
- There are several factors that contribute to attn.
  - Signal energy is also lost when it leaks through the insulation of the cable.
  - By impedance caused by defective connectors.
- Impedance discontinuities cause transmitted signal will be reflected back to the transmitting device
- The combination of the effects of signal attenuation and impedance discontinuities on a communications link is called insertion loss

Sources Of Noise On Copper Media

- Noise is any electrical energy on the transmission cable that makes it difficult for a receiver to interpret the data sent from the transmitter
- Crosstalk involves the transmission of signals from one wire to a nearby wire.
- Twisting one pair of wires in a cable also helps to reduce crosstalk of data or noise signals from an adjacent wire pair.
- When attaching connectors to the ends of UTP cable, untwisting of wire pairs must be kept to an absolute minimum

Types of Crosstalk

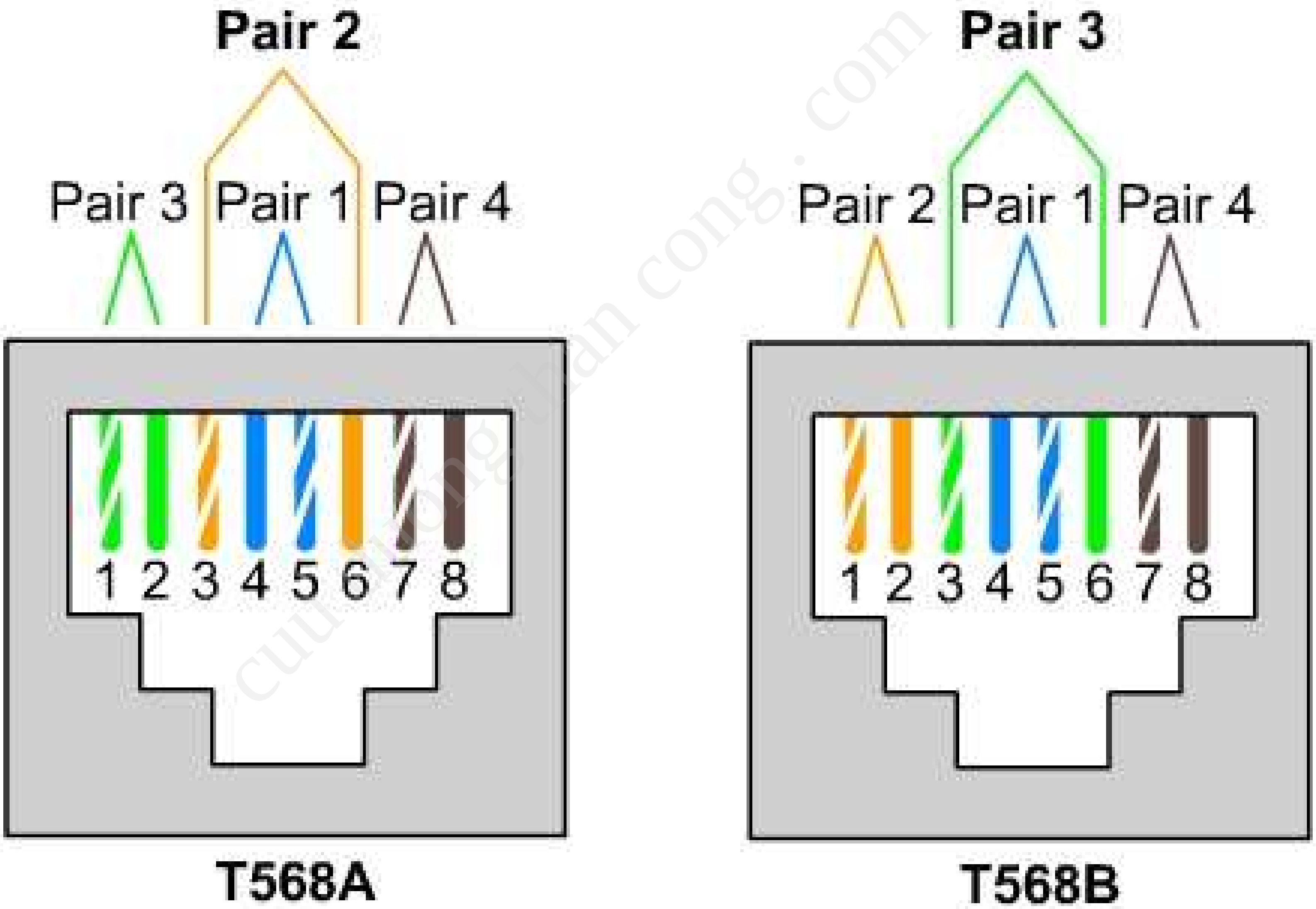


- Near-end Crosstalk (NEXT)
- Far-end Crosstalk (FEXT)
- Power Sum Near-end Crosstalk (PSNEXT)

Cable Testing Standards

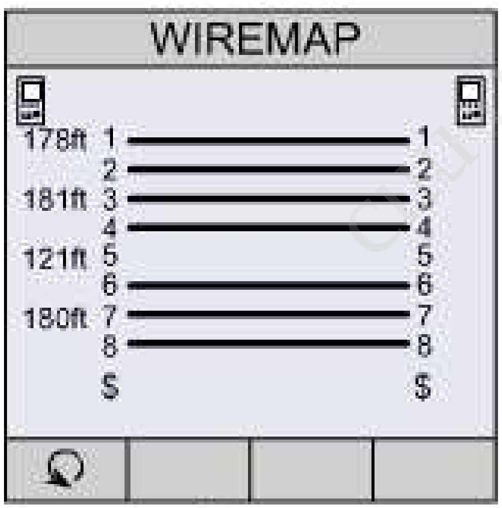
- The ten primary test parameters that must be verified for a cable link to meet TIA/EIA standards are:
  - Wire map
  - Insertion loss
  - Near-end crosstalk (NEXT)
  - Power sum near-end crosstalk (PSNEXT)
  - Equal-level far-end crosstalk (ELFEXT)
  - Power sum equal-level far-end crosstalk (PSELFEXT)
  - Return loss
  - Propagation delay
  - Cable length
  - Delay skew

Ethernet Standards

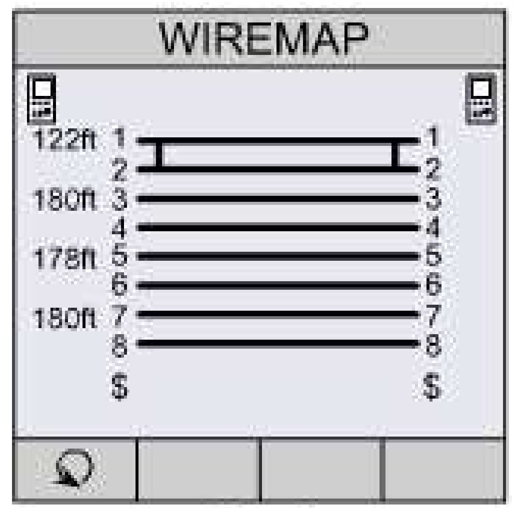


Cable Test Standards

Good Wiremap

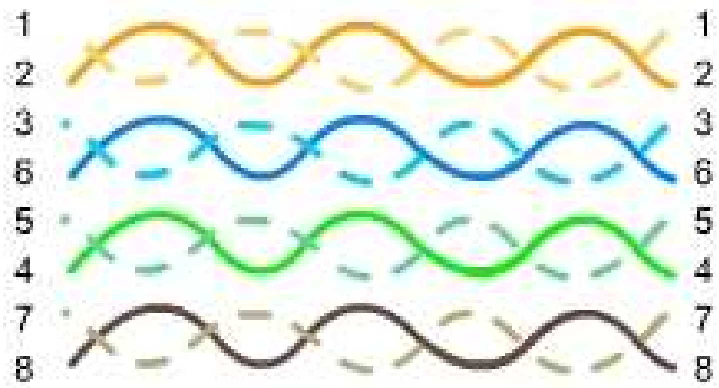


Open

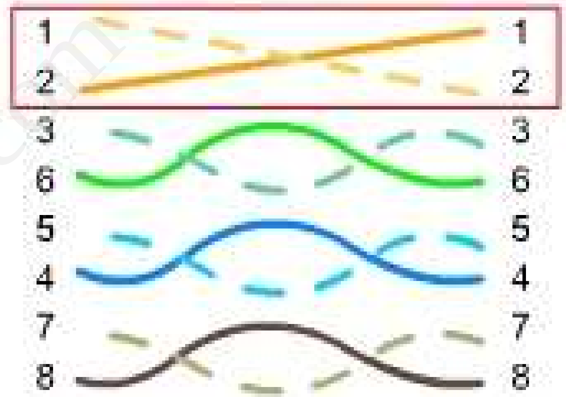


Short

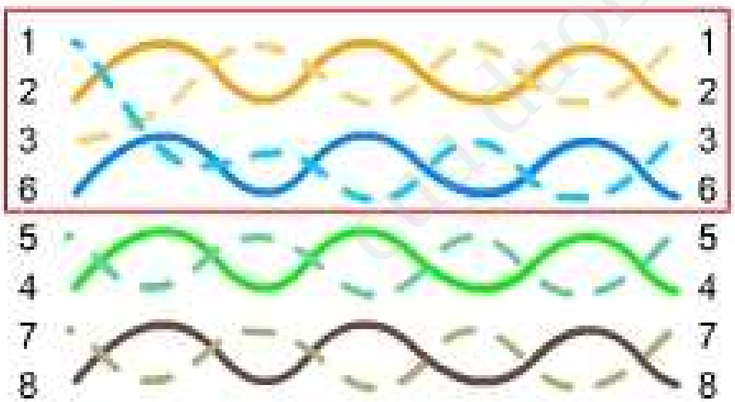
Wiring Fault



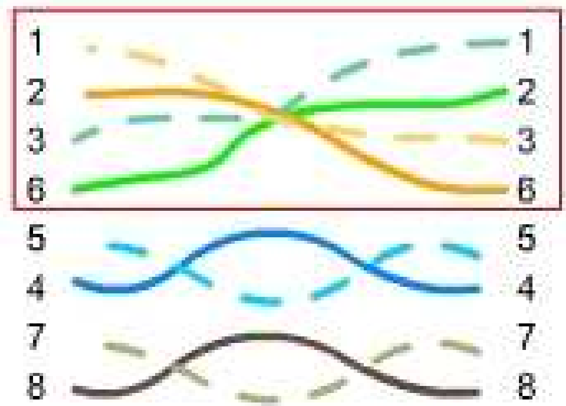
Correct T568B Wiring



Reversed-pair wiring fault



Split-pair Wiring Fault



Transposed-pair Wiring Fault

Other Test Parameters

- The combination of the effects of signal attenuation and impedance discontinuities on a communications link is called insertion loss. Insertion loss is measured in decibels at the far end of the cable
- Crosstalk is measured in four separate tests
- A cable tester measures NEXT by applying a test signal to one cable pair and measuring the amplitude of the crosstalk signals received by the other cable pairs
- The equal-level far-end crosstalk (ELFEXT) test measures FEXT
- Power sum equal-level far-end crosstalk (PSELFEXT) is the combined effect of ELFEXT from all wire pairs.

Time-based Parameters

- Propagation delay is a simple measurement of how long it takes for a signal to travel along the cable being tested. The delay in a wire pair depends on its length, twist rate, and electrical properties
- TIA/EIA-568-B standard sets a limit for propagation delay for the various categories of UTP.
- The delay difference between pairs is called delay skew. The propagation delays of different wire pairs is because of differences in the number of twists and electrical properties of each wire pair.

Q&A

CCNA Semester 1

NETWORK TRAINING CENTER

The **Cisco Certified Network Associate** Curriculum

Chapter 05

CABLING LANS AND WANS

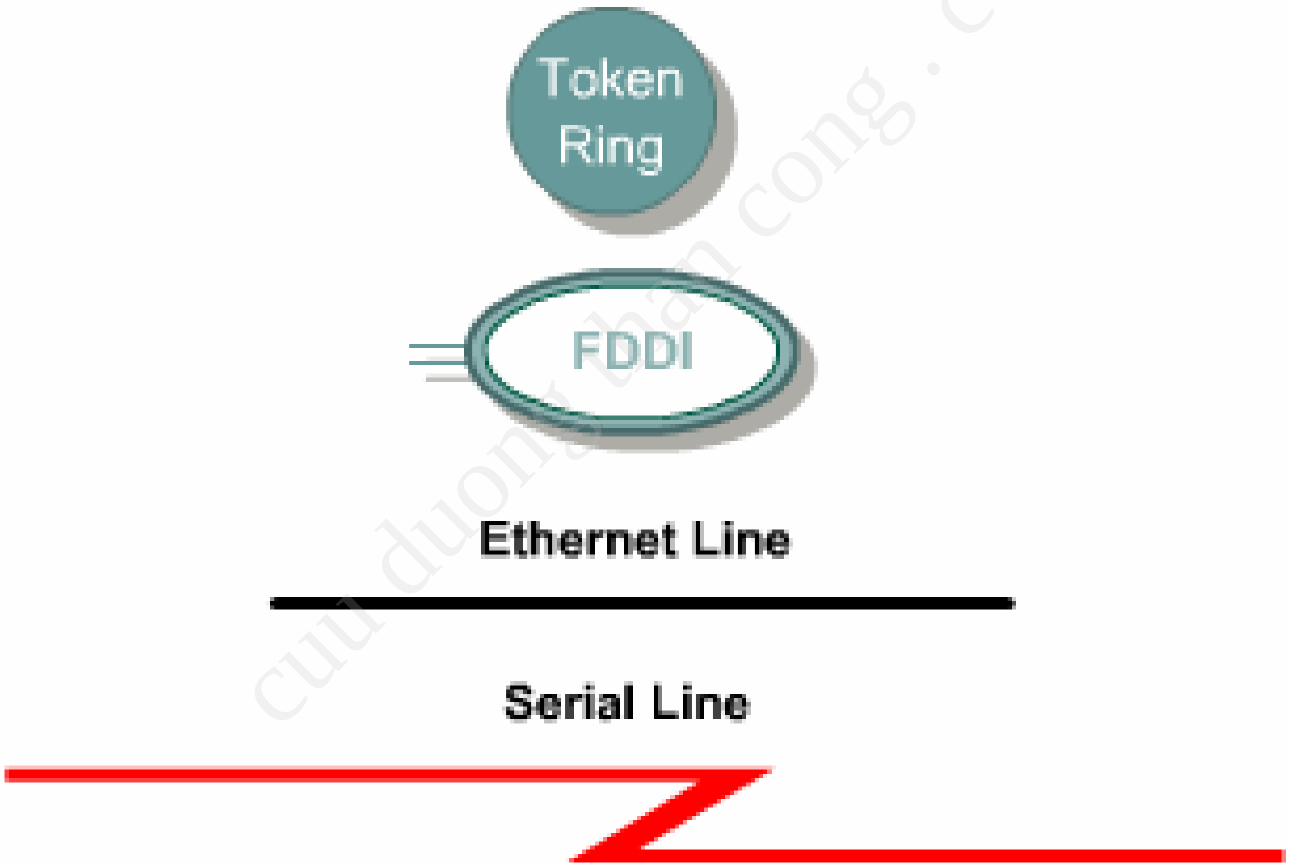
Objectives

- *Identify characteristics of Ethernet networks.*
- *Identify straight-through, crossover, and rollover cables.*
- *Describe the function, advantages, and disadvantages of repeaters, hubs, bridges, switches, and wireless network components.*
- *Describe and differentiate between serial, Integrated Services Digital Network (ISDN), digital subscriber line (DSL), and cable modem WAN connections.*

Table of Content

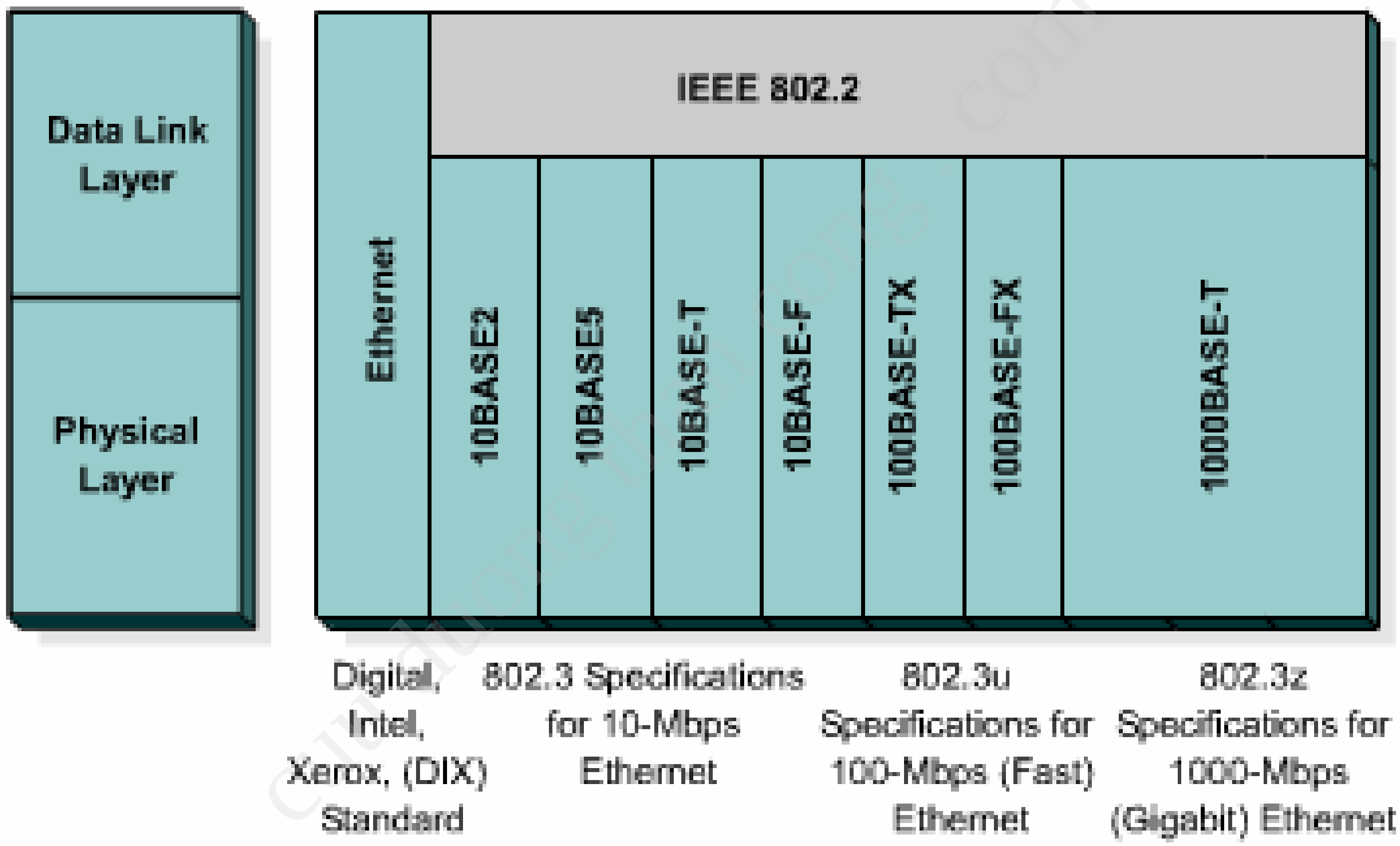
CABLING THE LAN

LAN Physical Layer



LAN Physical Layer

NETWORK TRAINING CENTER



- Physical layer implementations vary.
- Some implementations support multiple physical media.

LAN Physical Layer

- Each type of media has advantages and disadvantages. These are based on the following factors:
  - Cable length
  - Cost
  - Ease of installation
  - Susceptibility to interference

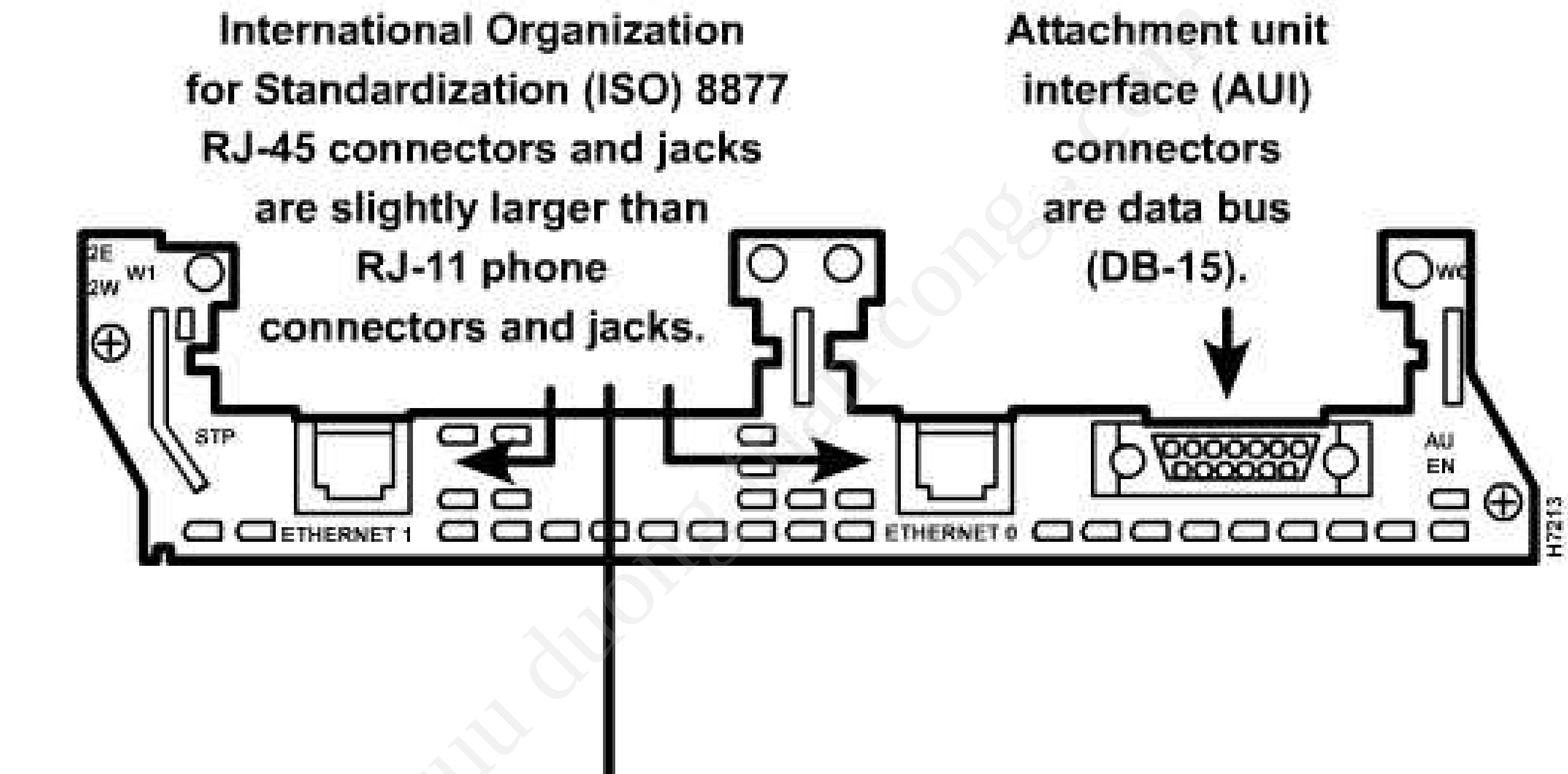
Ethernet In The Campus

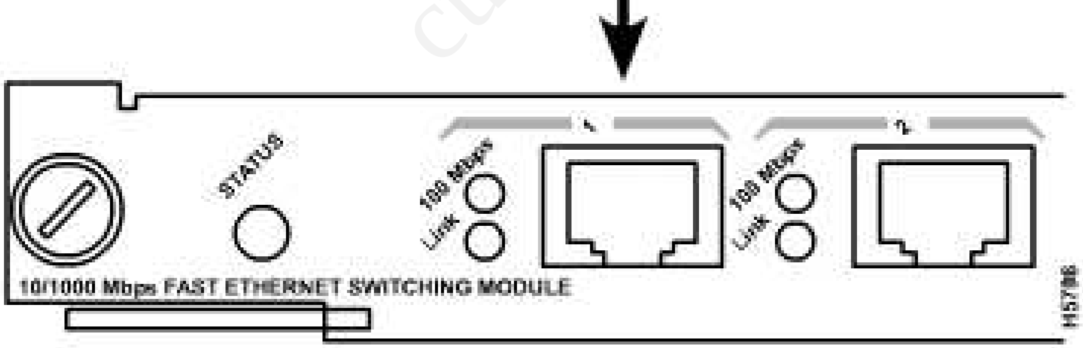
	Ethernet 10BASE-T Implementation	Fast Ethernet Implementation	Gigabit Ethernet Implementation
End-user Level (End-user device to workgroup device)	Provides connectivity for low-to medium-volume applications.	Gives high-performance PC workstations 100-Mbps access to the server.	Not typically used at this level.
Workgroup Level (Workgroup device to backbone)	Not typically used at this level.	Provides connectivity between the end user and workgroups. Provides connectivity from the workgroup to backbone. Provides connectivity from the server block to the backbone layer.	Provides high-performance connectivity to the enterprise server block.
Backbone Level	Not typically used at this level.	Provides connectivity from the workgroup server block to the backbone.	Provides high-speed backbone and network device connectivity.

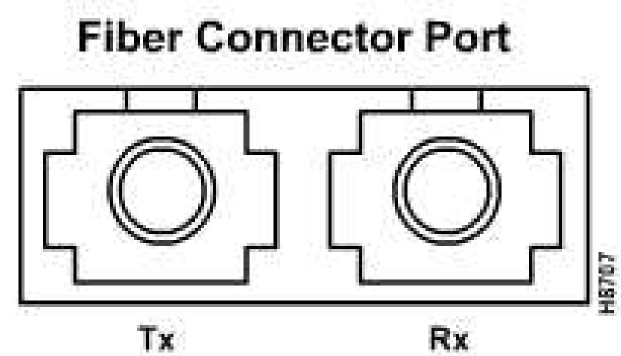
Ethernet Media And Connector Requirements

	10BASE2	10BASE5	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX
Media	50-ohm coaxial (Thinnet)	50-ohm coaxial (Thicknet)	EIA/TIA Category 3, 4, 5 UTP, two pair	EIA/TIA Category 5 UTP, two pair	62.5/125 multimode fiber	STP	EIA/TIA Category 5 UTP, four pair	62.5/50 micro multimode fiber	62.5/50 micro multimode fiber; 9-micron single-mode fiber
Maximum Segment Length	185 m (606.94 feet)	500 m (1640.4 feet)	100 m (328 feet)	100 m (328 feet)	400 m (1312.3 feet)	25 m (82 feet)	100 m (328 feet)	275 m (853 feet) for 62.5 micro fiber; 550 m (1804.5 feet) for 50 micro fiber	440 m (1443.6 feet) for 62.5 micro fiber; 550 m (1804.5 feet) for 50 micro fiber; 3 to 10 km (1.86 to 6.2 miles) on single-mode fiber
Topology	Bus	Bus	Star	Star	Star	Star	Star	Star	Star
Connector	BNC	Attachment unit interface (AUI)	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Duplex media interface connector (MIC) ST or SC connector	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	SC connector	SC connector

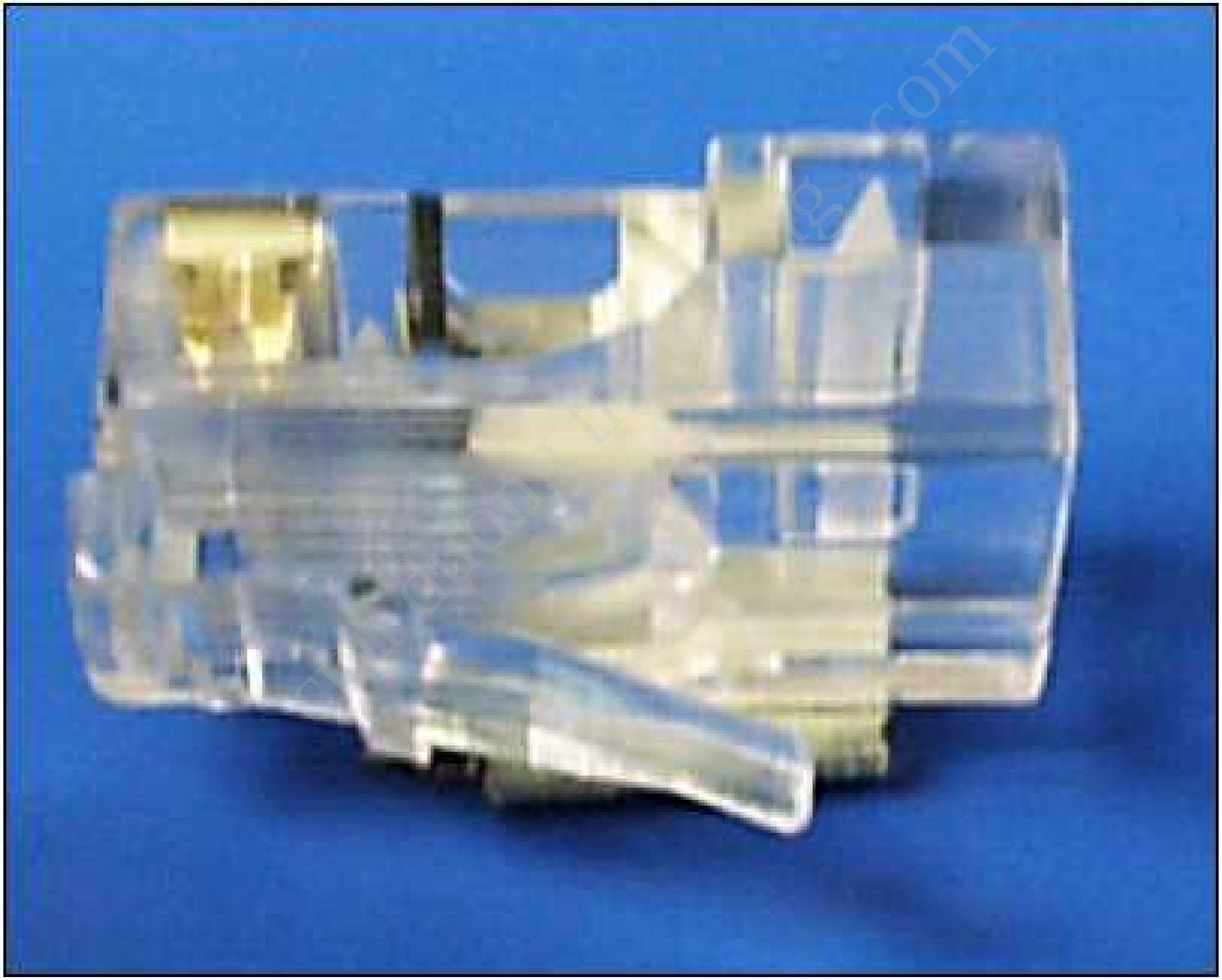
Connection Media



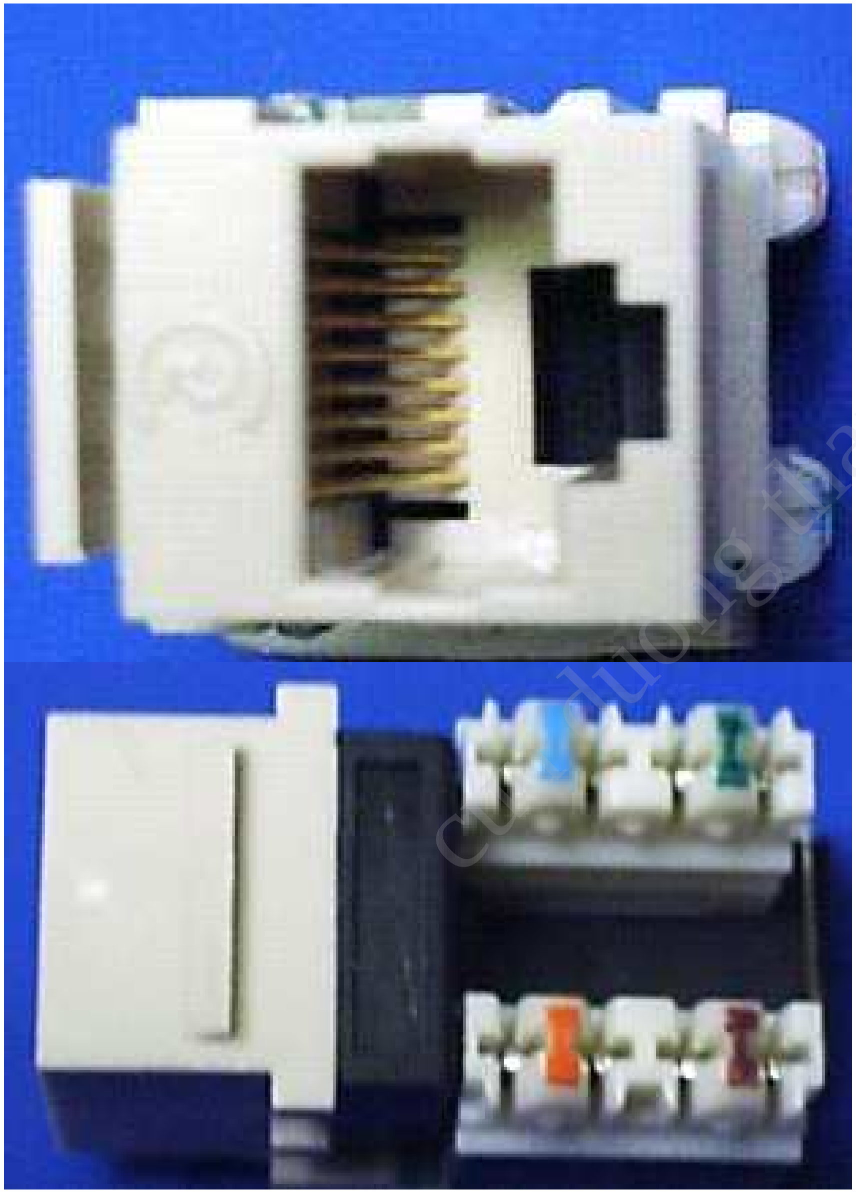




RJ-45 Plug



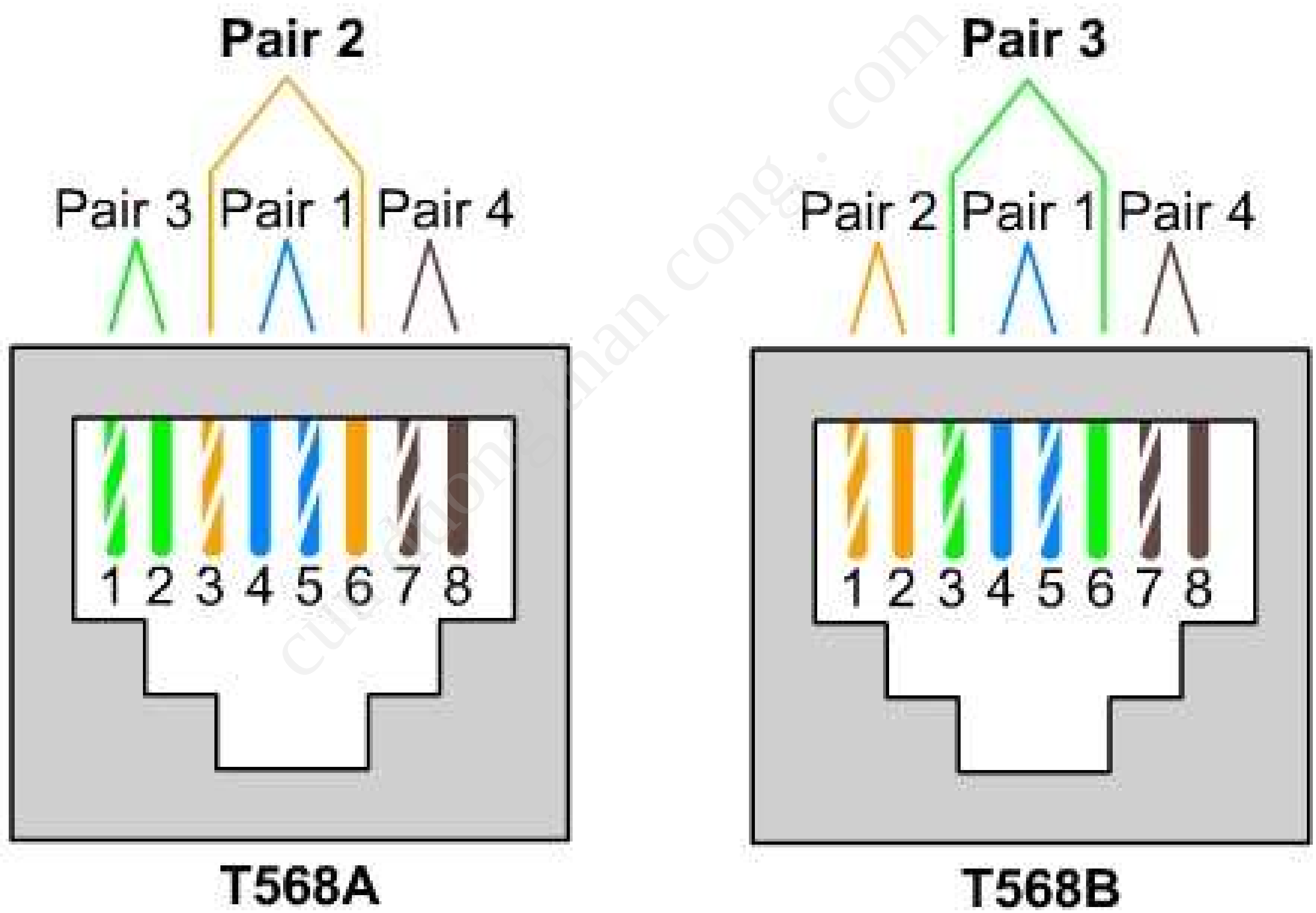
RJ-45 Jack



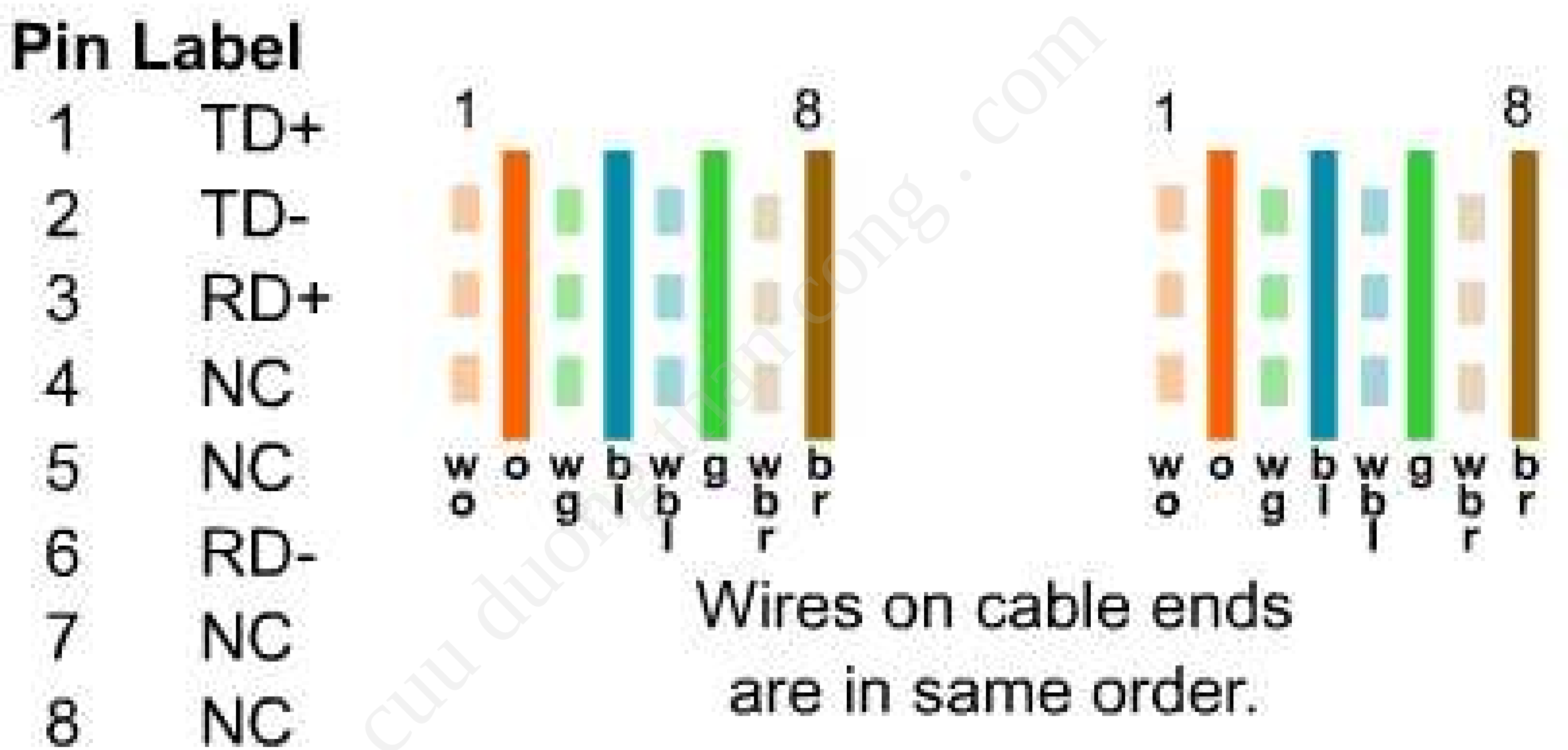
The jack is the female component in a network device, wall outlet, or patch panel

Punch-down connections at the back of the jack where the Ethernet UTP cable connects.

UTP Implementation

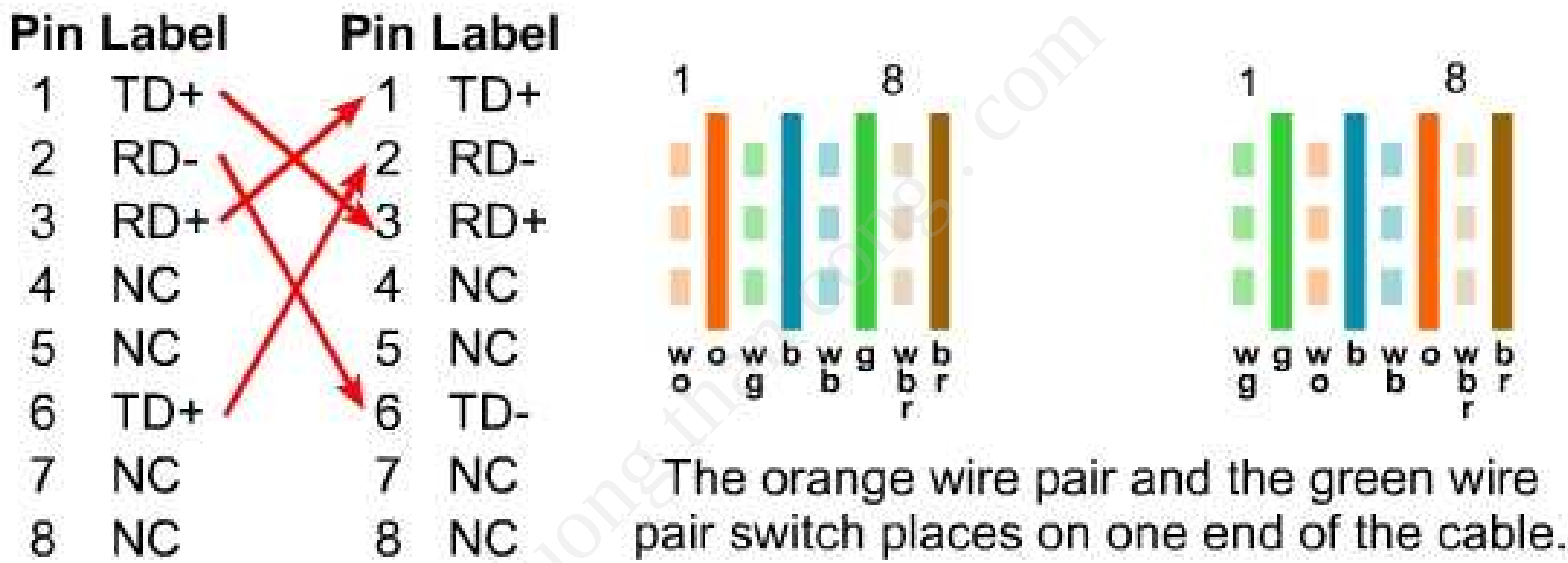


Straight-through Cable



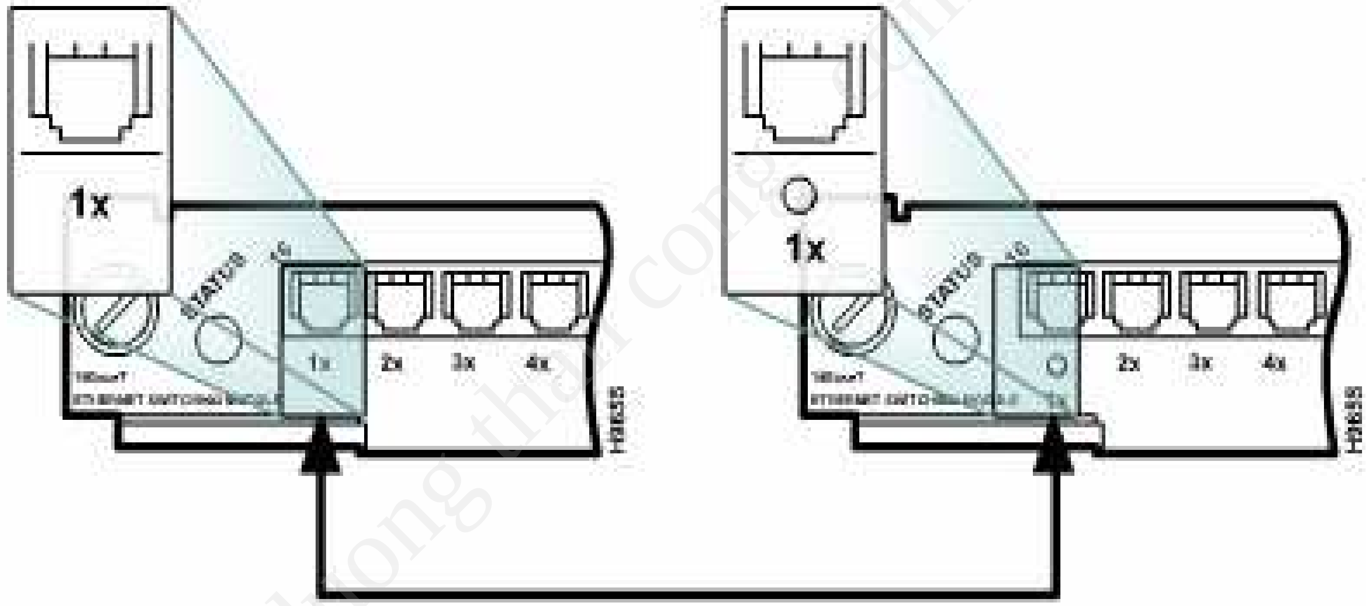
- Switch to router
- Switch to PC or server
- Hub to PC or server

Cross-over Cable



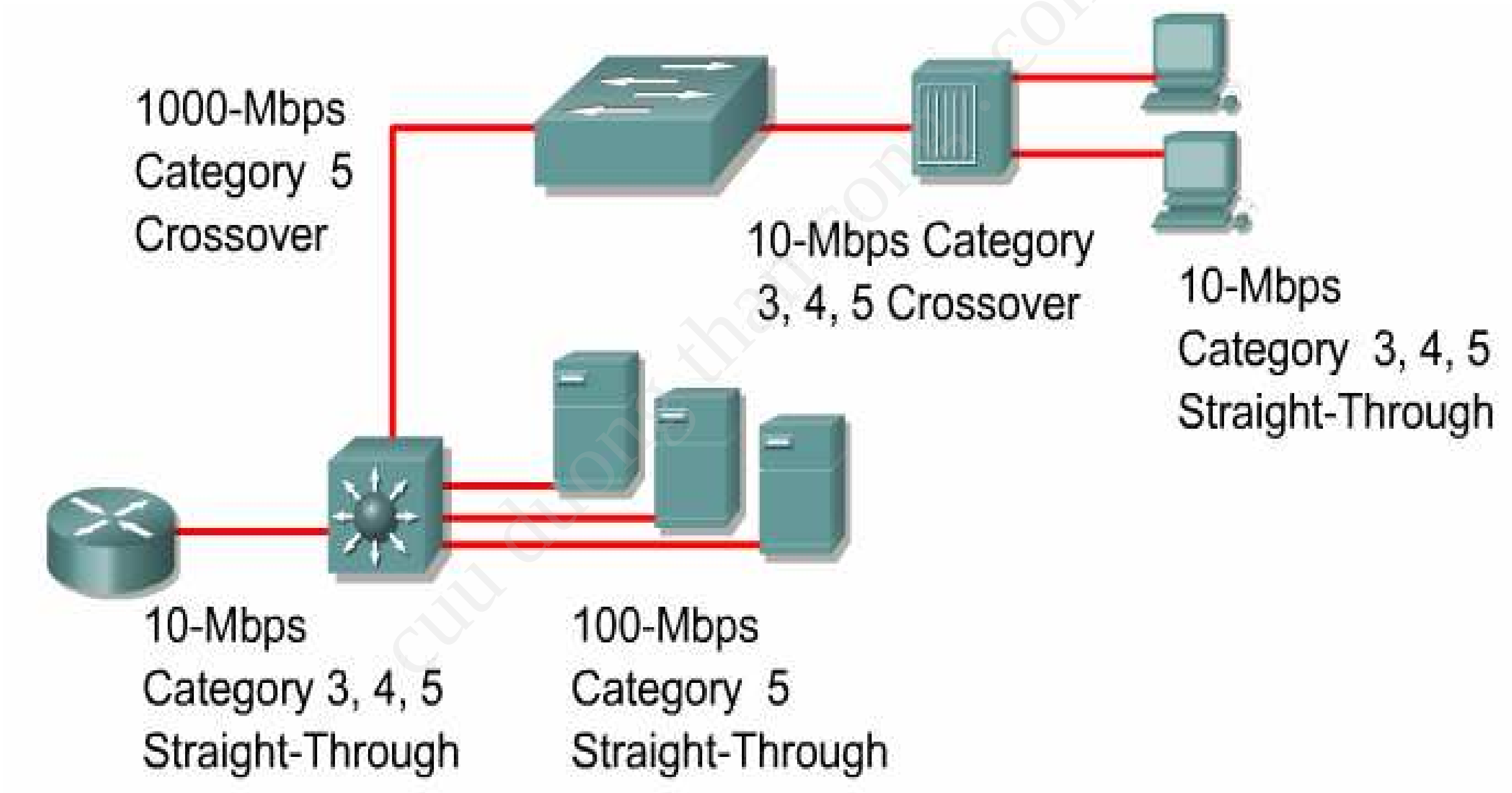
- Switch to switch
- Switch to hub
- Hub to hub
- Router to router
- PC to PC
- Router to PC

UTP Crossover Cable



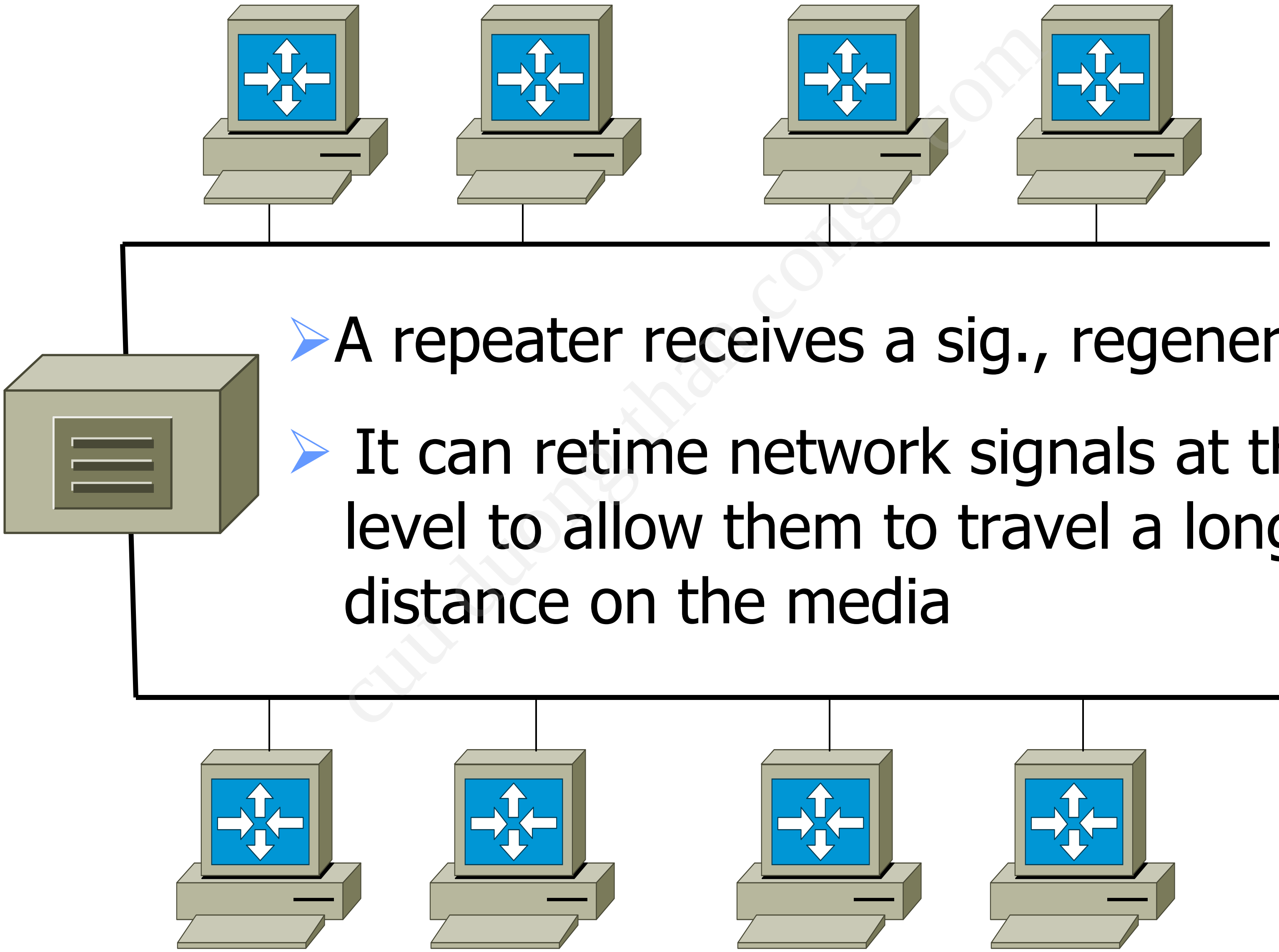
Use crossover cable when BOTH ports are designated with an "x"or neither port is designated with an "x".

UTP Usage


1000-Mbps
Category 5
Crossover
10-Mbps Category
3, 4, 5 Crossover
10-Mbps
Category 3, 4, 5
Straight-Through
10-Mbps
Category 3, 4, 5
Straight-Through
100-Mbps
Category 5
Straight-Through

Repeaters

NETWORK TRAINING CENTER



- A repeater receives a sig., regenerates it
- It can retime network signals at the bit level to allow them to travel a longer distance on the media

Hubs

Hubs

- **Passive**
  - A passive hub serves as a physical connection point only.
  - It does not manipulate or view the traffic that crosses it.
  - It does not boost or clean the signal.
- **Active**
  - It needs power to amplify the incoming signal before passing it out to the other ports.
- **Intelligent**
  - These devices basically function as active hubs
  - It also includes a microprocessor chip and diagnostic capabilities.

Wireless Media

- **Wireless signals** are electromagnetic waves that travel through the air
- Wireless networks use **radio frequency (RF)**, **laser**, **infrared (IR)**, **satellite**, or **microwaves** to carry signals between computers without a permanent cable connection.
- **No need for cabling** to the hosts; the only permanent cabling can be to the access points for the network
- A common application of wireless data communication is for **mobile use**

Wireless Media

- At the core of wireless communication are devices called **transmitters** and **receivers**
  - The transmitter converts source data to electromagnetic waves that are sent to the receiver
  - The receiver then converts these electromagnetic waves back into data for the destination
- For two-way communication, each device requires a transmitter and a receiver

Wireless Media

- Many networking device manufacturers build the transmitter and receiver into a single unit called a **transceiver** or **wireless network card**
- All devices in a WLAN must have the correct wireless network card installed

Wireless Media

- The two most common wireless technologies used for networking are **IR** and **RF**
- **IR** technology has its weaknesses - must be in the **line of sight** of the transmitter to work correctly
- **IR** networking technology can be installed quickly
- New **IR** technologies will be able to work out of sight

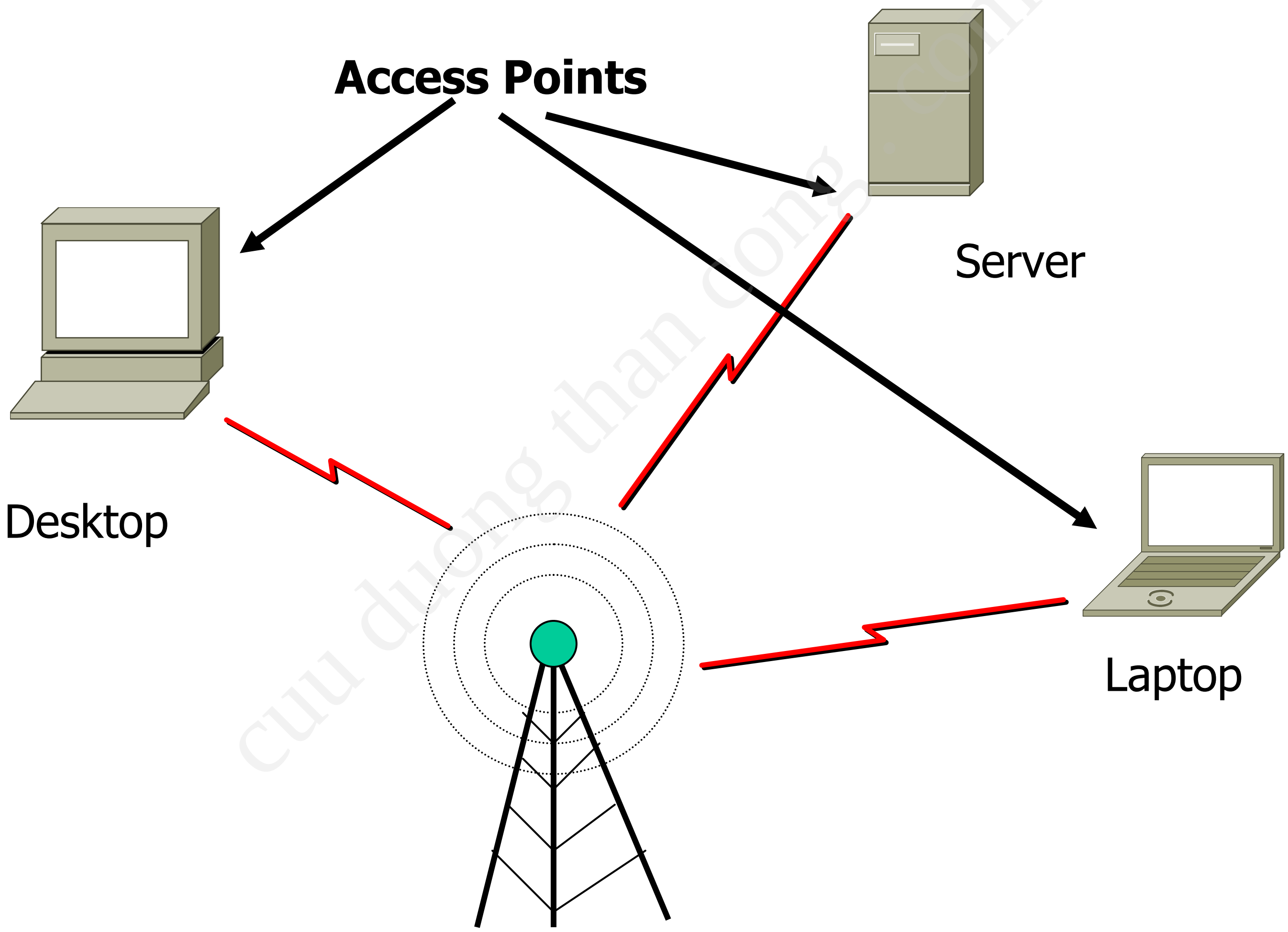
Wireless Media

- **RF** technology allows devices to be in different rooms or buildings
- The **limited range of radio signals** restricts the use of this kind of network
- RF technology can be on single or multiple frequencies
- A single radio frequency is subject to outside interference and geographic obstructions

Wireless Media

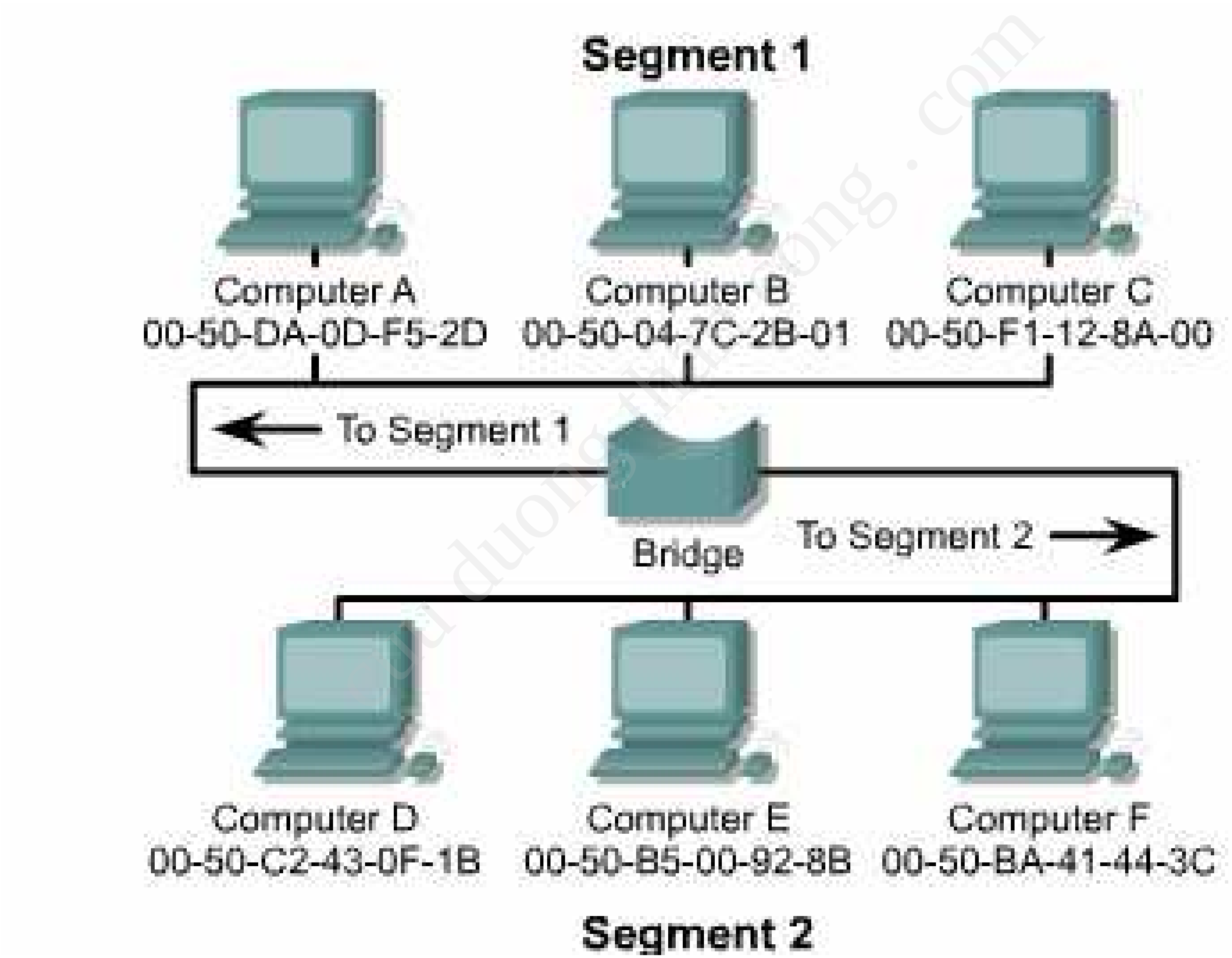
- It is also easily monitored by others, which makes the transmissions of data **insecure**
- **Spread spectrum** uses multiple frequencies to increase the immunity to noise and to make it difficult for outsiders to intercept data transmissions
- Two forms of spread spectrum for WLAN transmissions are **Frequency Hopping Spread Spectrum (FHSS)** and **Direct Sequence Spread Spectrum (DSSS)**

Wireless

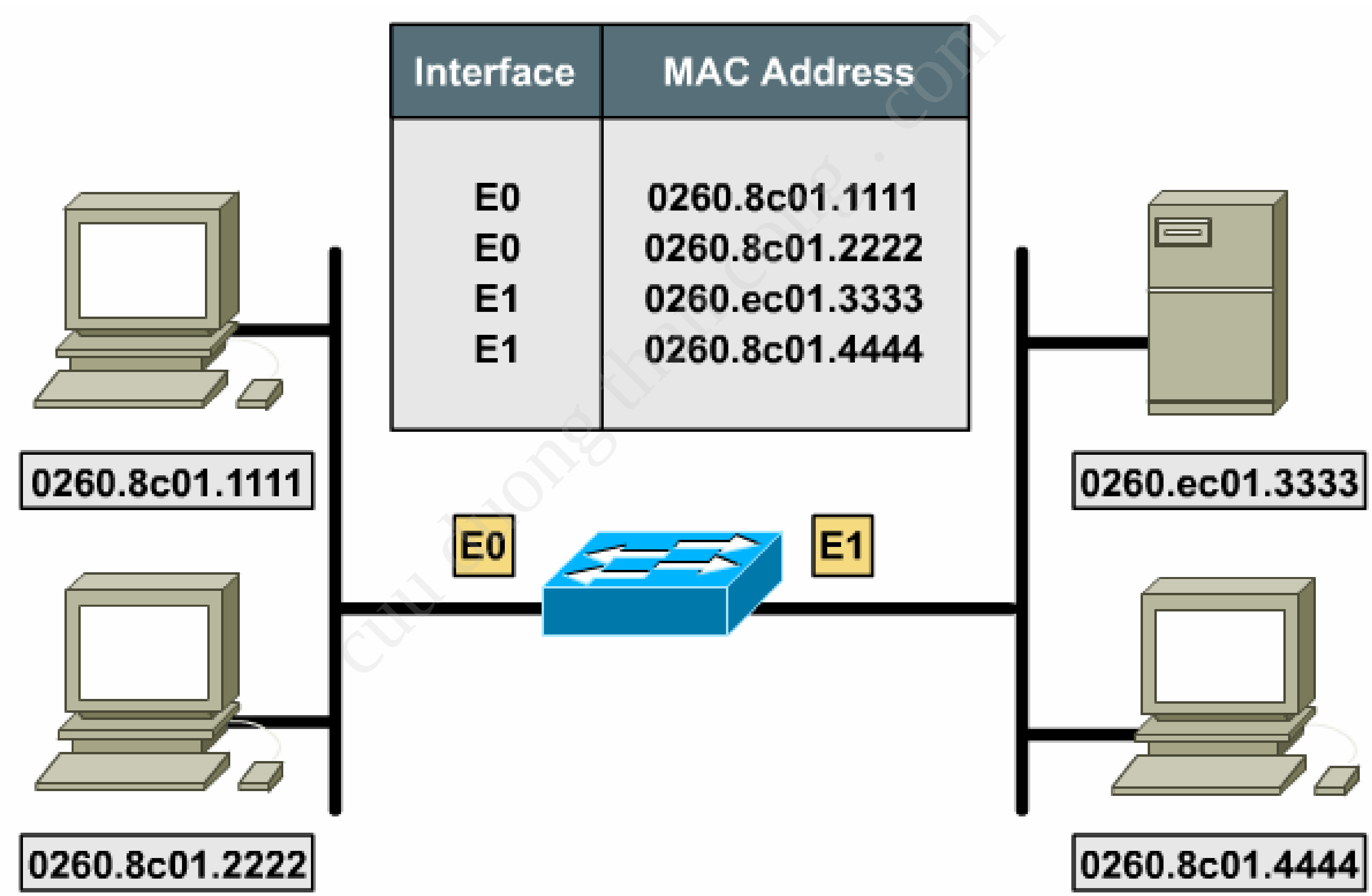


Bridges

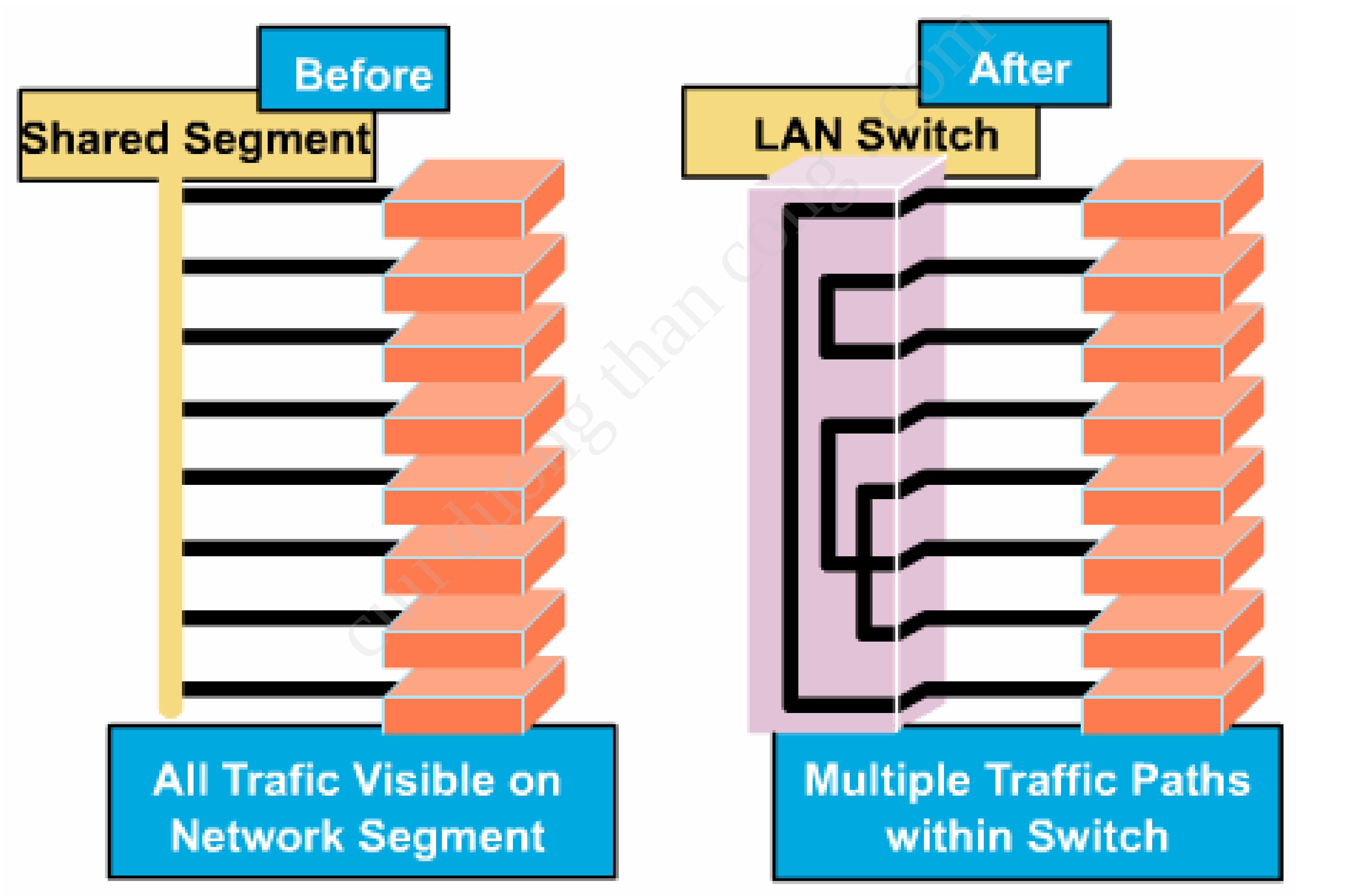
NETWORK TRAINING CENTER



Switches


Interface
MAC Address
E0
E0
E1
E1
0260.8c01.1111
0260.8c01.2222
0260.ec01.3333
0260.8c01.4444
0260.8c01.1111
0260.8c01.2222
E0
E1
0260.ec01.3333
0260.8c01.4444

Micro-segmentation



Host Connectivity: NIC

- The function of a NIC is to connect a host device to the network medium
- A NIC is a printed circuit board that fits into the expansion slot on the motherboard or peripheral device of a computer
- The NIC is also referred to as a network adapter

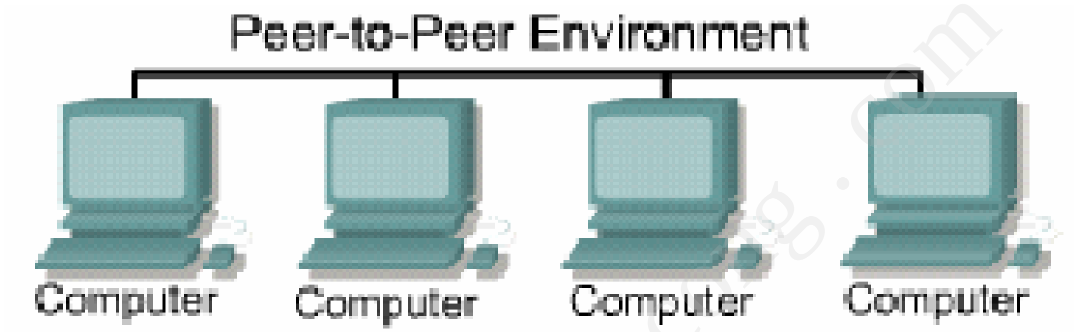
Host Connectivity: NIC

- NICs are classified as **Data Link Layer (Layer 2) devices** because each NIC carries a unique code called a MAC address
- This address is used to control data communication for the host on the network
- NICs control host access to the medium.

Host Connectivity: NIC

Host Connectivity: NIC

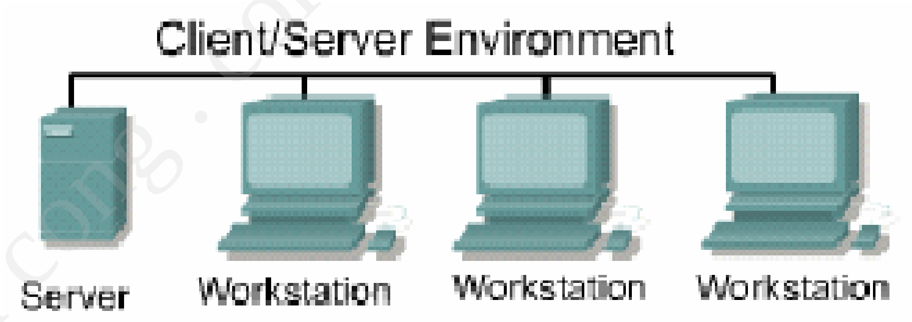
Peer-to-peer

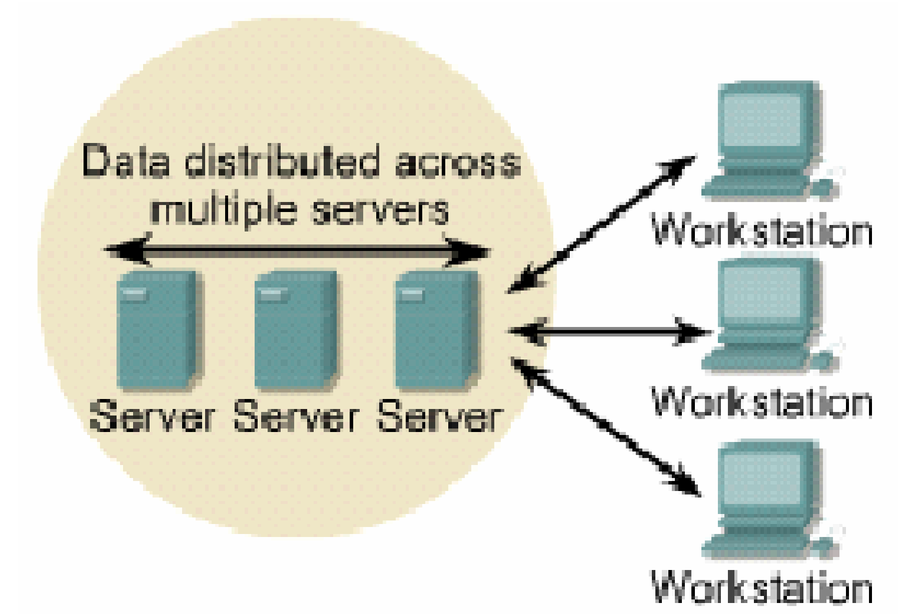


- In a peer-to-peer network, networked computers act as equal partners, or peers
- Individual users control their own resources
- Peer-to-peer networks are relatively easy to install and operate
- As networks grow, peer-to-peer relationships become increasingly difficult to coordinate

Client/server

- network services are located on a dedicated computer called a server
- Servers are designed to handle requests from many clients simultaneously
- Data generated is easier to back-up and maintain





Client/server

NETWORK TRAINING CENTER

Advantages of a Peer-to-Peer Network	Advantages of a Client/Server Network
Less expensive to implement.	Provides for better security.
Does not require additional specialized network administration software	Easier to administer when the network is large because administration is centralized.
Does not require a dedicated network administrator.	All data can be backed up on one central location.

Disadvantages of a Peer-to-Peer Network	Disadvantages of a Client/Server Network
Does not scale well to large networks and administration becomes unmanageable.	Requires expensive specialized network administrative and operational software
Each user must be trained to perform administrative tasks.	Requires expensive, more powerful hardware for the server machine.
Less secure.	Requires a professional administrator.
All machines sharing the resources negatively impact the performance.	Has a single point of failure. User data is unavailable if the server is down.

CABLING THE WAN

WAN Physical Layer

NETWORK TRAINING CENTER

Cisco HDLC	PPP	Frame Relay	ISDN BRI (with PPP)	DSL Modem	Cable Modem
EIA/TIA-232 EIA/TIA-449 X.21 V.24 V.35 High Speed Serial Interface (HSSI)			RJ-45 Note: ISDN BRI cable pinouts are different than the pinouts for Ethernet	RJ-11 Note: Works over telephone line	BNC Note: Works over Cable TV line

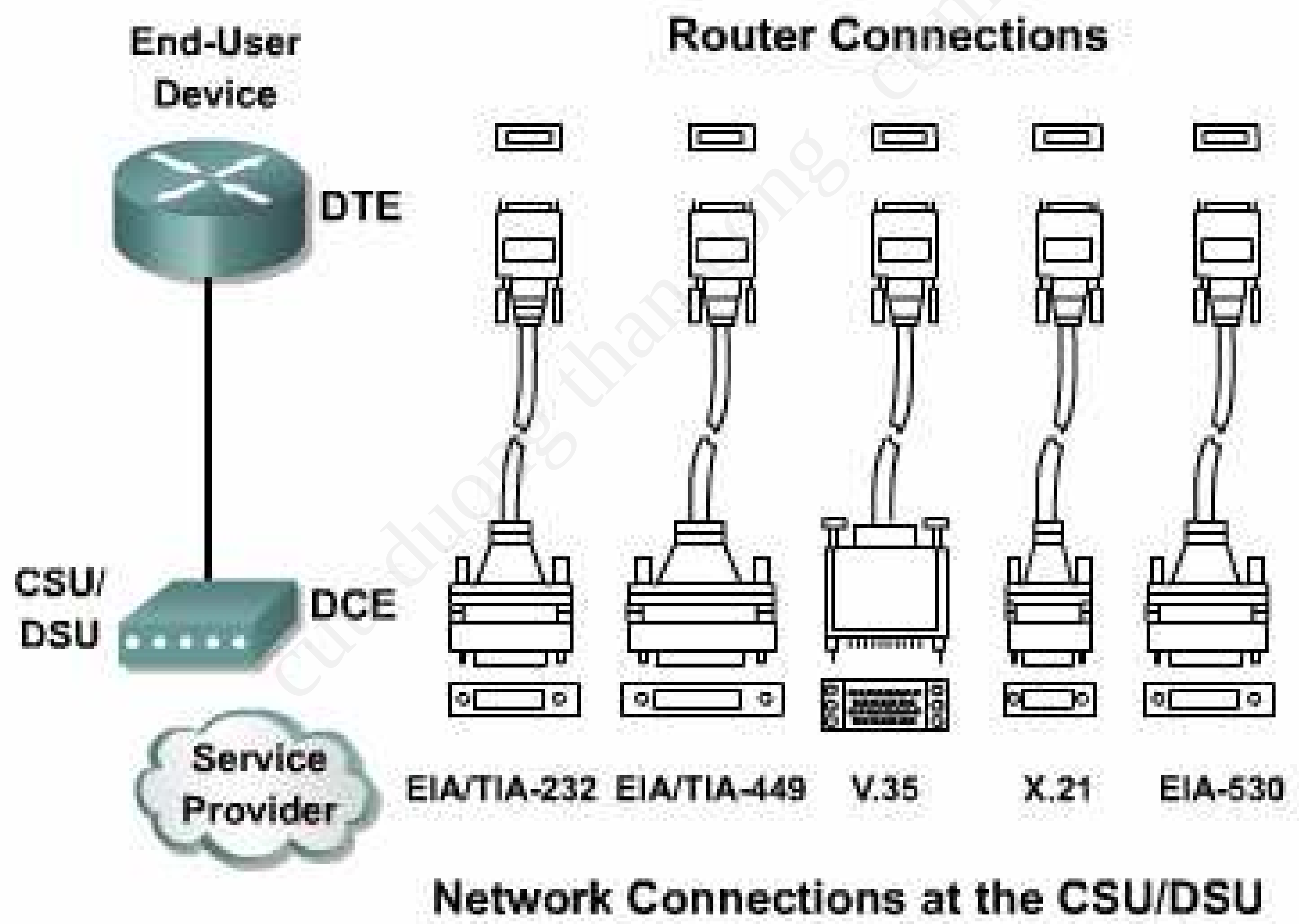
- Physical Layer implementation vary
- Cable specifications define speed of link

WAN Serial Connections

Data (bps)	Distance (Meters) EIA/TIA-232	Distance (Meters) EIA/TIA-449
2400	60	1250
4800	30	625
6900	15	312
19,200	15	156
38,400	15	78
115,200	3.7	—
T1 (1.544 Mbps)	—	15

WAN Serial Connections

NETWORK TRAINING CENTER

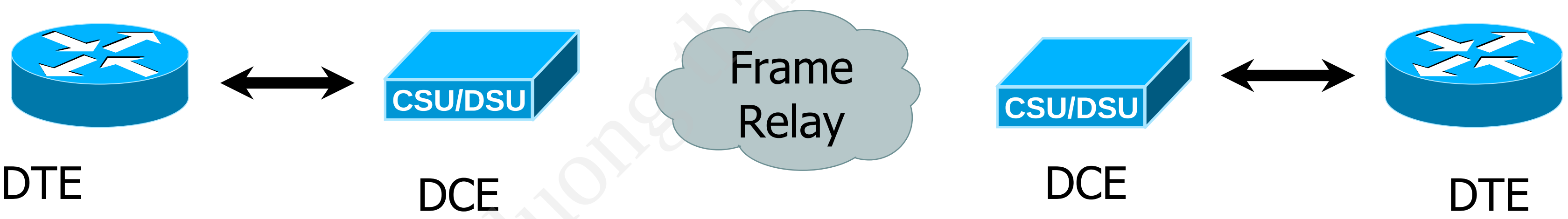


41

Routers and Serial Connections

Data Terminal Equipment
End of user's device
on the WAN link

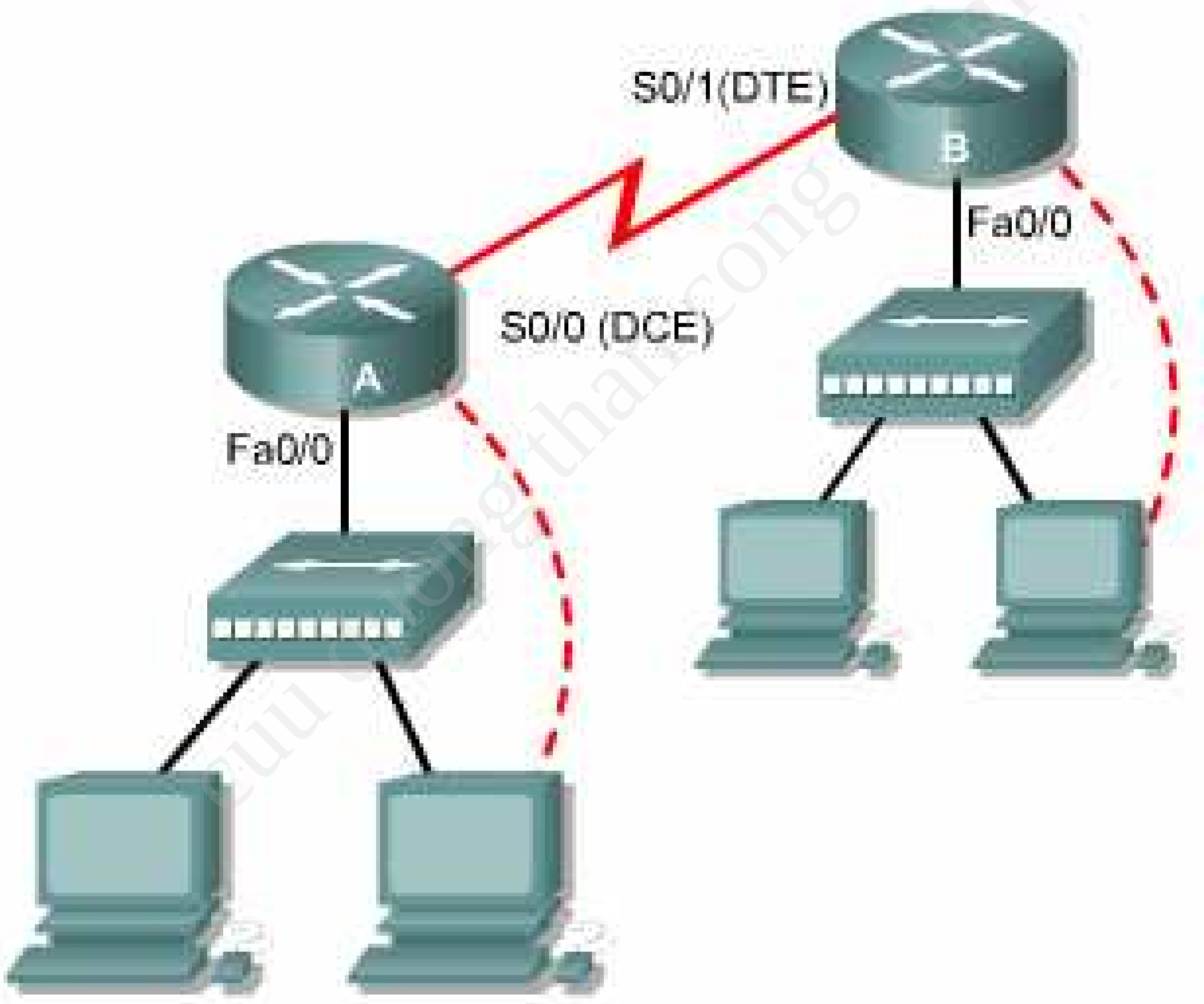
Data Communications Equipment
- End of provider's site
  Of communication facility
- Responsible for clocking



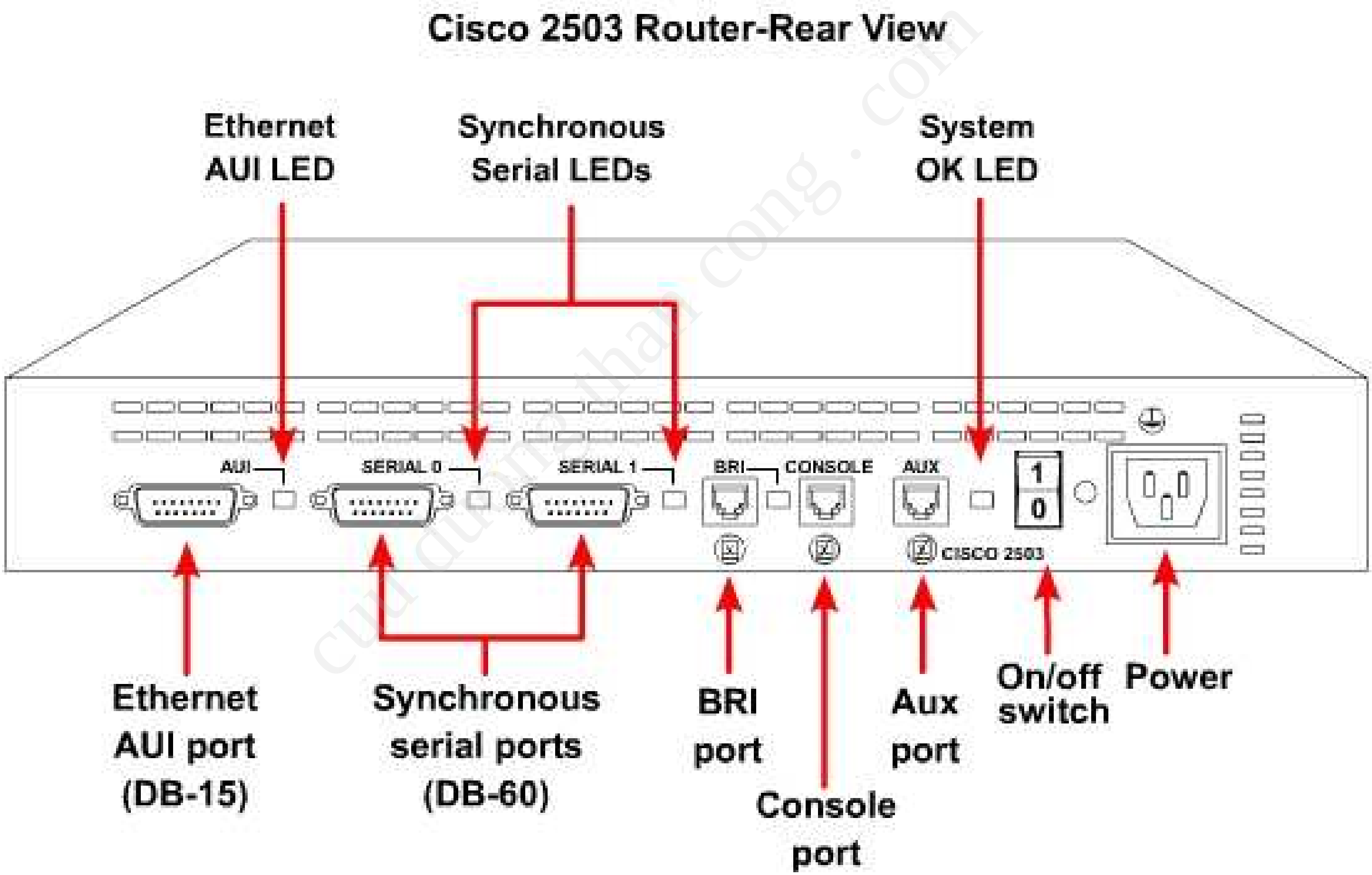
it is necessary to determine whether DTE or DCE connectors are required.

DCE like CSU/DSU will perform signal clocking

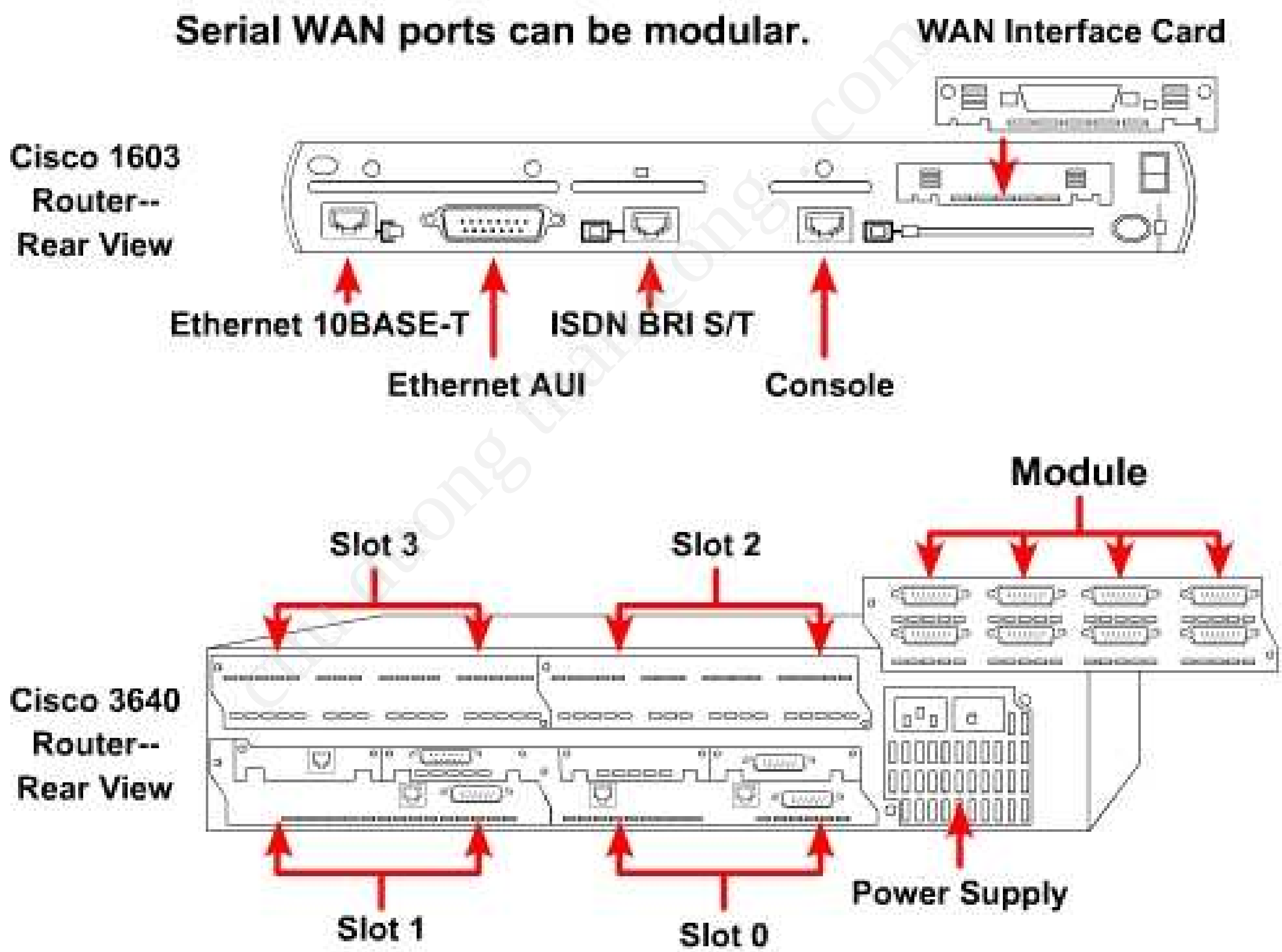
Routers and Serial Connections



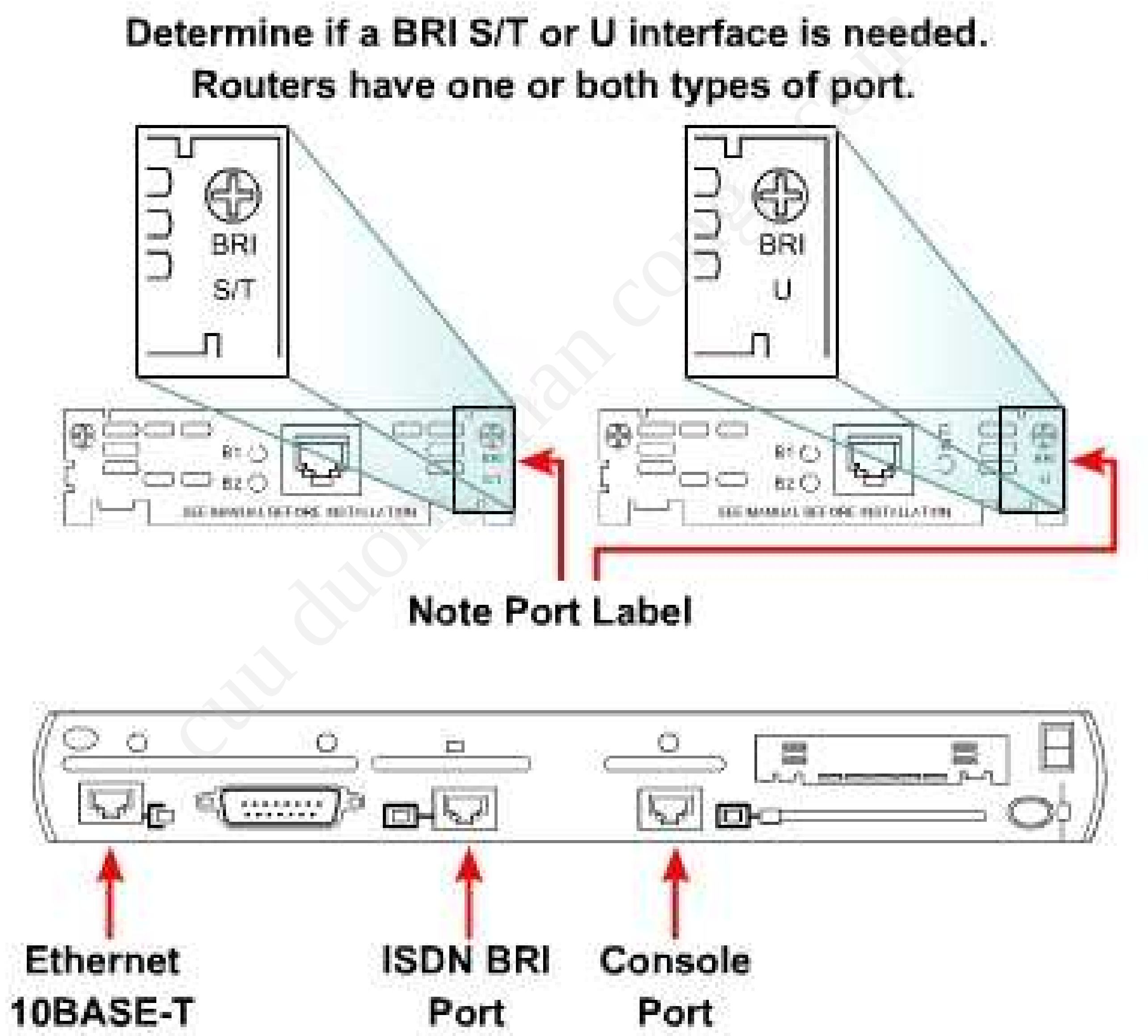
Fixed Module Router



Module Router

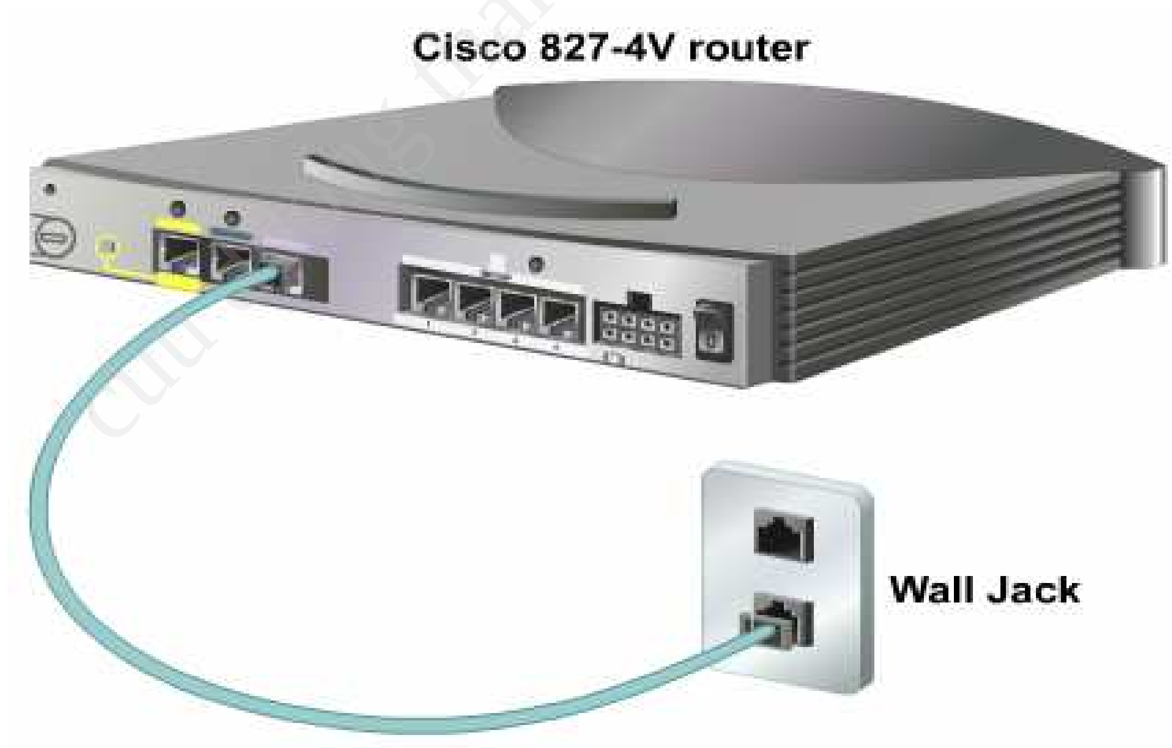


Routers and ISDN BRI Connections



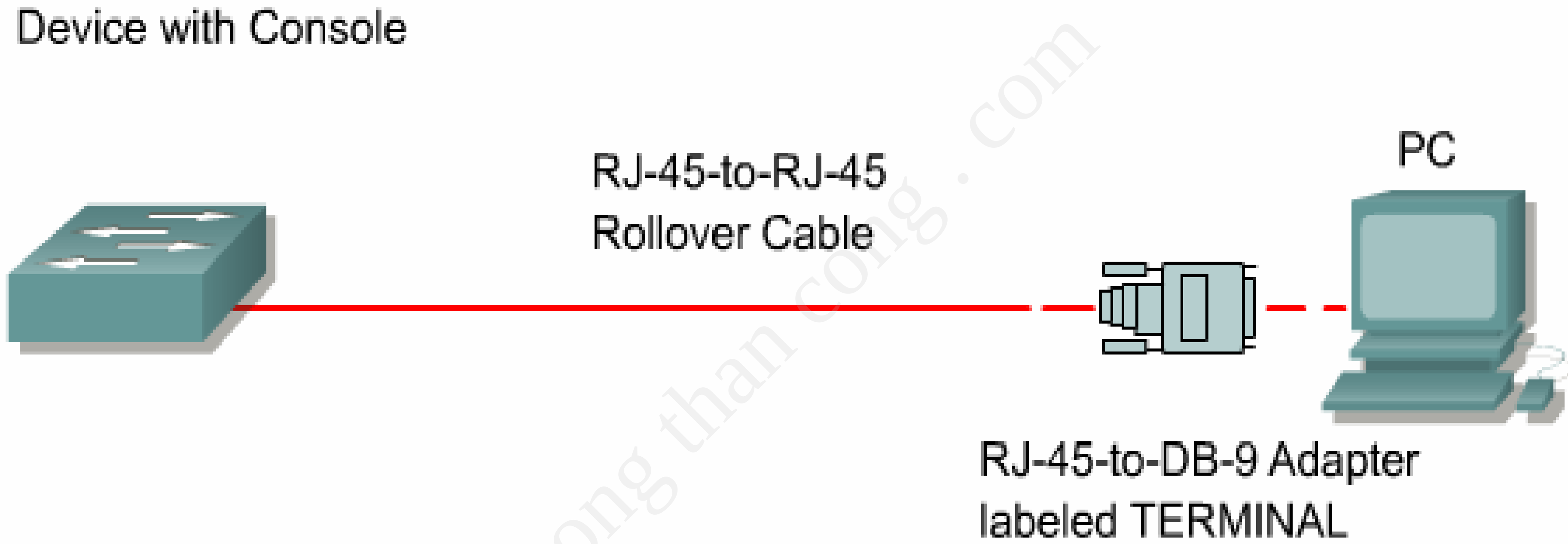
Routers and DSL Connections

- The Cisco 827 ADSL router has one asymmetric digital subscriber line (ADSL) interface.
- To connect an ADSL line to the ADSL port on a router



Setting up Console Connections

NETWORK TRAINING CENTER



- PCs require an RJ-45 to DB-9 or RJ-45 to DB-25 adapter.
- COM port settings are 9600 bps, 8 data bits, no parity, 1 stop bit, no flow control.
- This provides out-of-band console access.
- AUX switch port may be used for a modem-connected console.

Summary

- Use a crossover cable to connect between two similar devices, such as switches, routers, PCs, and hubs.
- Use a straight-through cable to connect between different devices.
- WANs use serial data transmission. WAN connection types include ISDN, DSL, and cable modems.
- A router is usually the DTE and needs a serial cable to connect to a DCE device like a CSU/DSU.
- The ISDN BRI has two types of interfaces, S/T and U interfaces
- Rollover cable is used to connect a terminal and the console port of an internetworking device

Q&A

CCNA Semester 1

NETWORK TRAINING CENTER

The **Cisco Certified Network Associate** Curriculum

Chapter 06

ETHERNET FUNDAMENTALS

Objectives

- Describe the basics of Ethernet technology.
- Explain naming rules of Ethernet technology.
- Define how Ethernet and the OSI model interact.
- Describe the Ethernet framing process and frame structure.
- List Ethernet frame field names and purposes.
- Identify the characteristics of CSMA/CD.
- Describe the key aspects of Ethernet timing, interframe spacing and backoff time after a collision.
- Define Ethernet errors and collisions.
- Explain the concept of auto-negotiation in relation to speed and duplex.

Table of Content

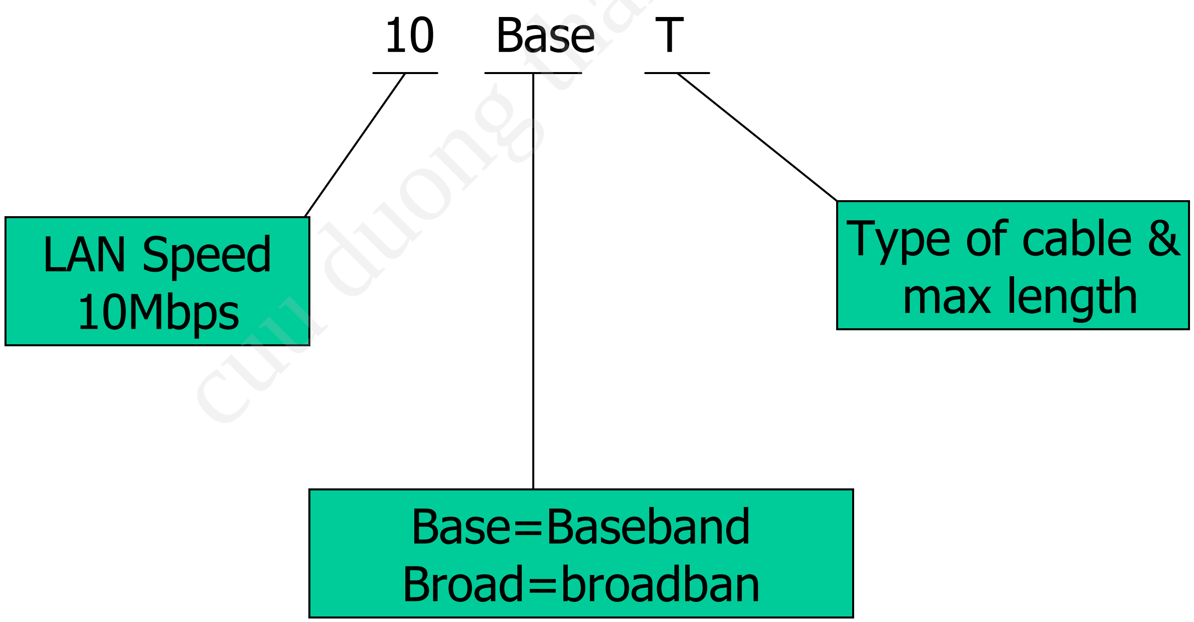
ETHERNET FUNDAMENTALS

Introduction to Ethernet

- In 1970's
  - CSMA/CD developed at the University of Hawaii
- In 1980's
  - First Ethernet standard was published by DIX
- In 1985
  - IEEE 802.3 released. It was based on Ethernet.
  - Ethernet and IEEE 802.3 are the same standards
- In 1995, IEEE announced a standard for a 100-Mbps Ethernet.
- In 1998, IEEE released 1Gbps
- In 2002, IEEE approved 10Gbps

IEEE Ethernet naming rules

- The term Ethernet refers to a family of networking technologies that include original Ethernet, Fast Ethernet, Gigabit Ethernet and 10 Gigabit Ethernet

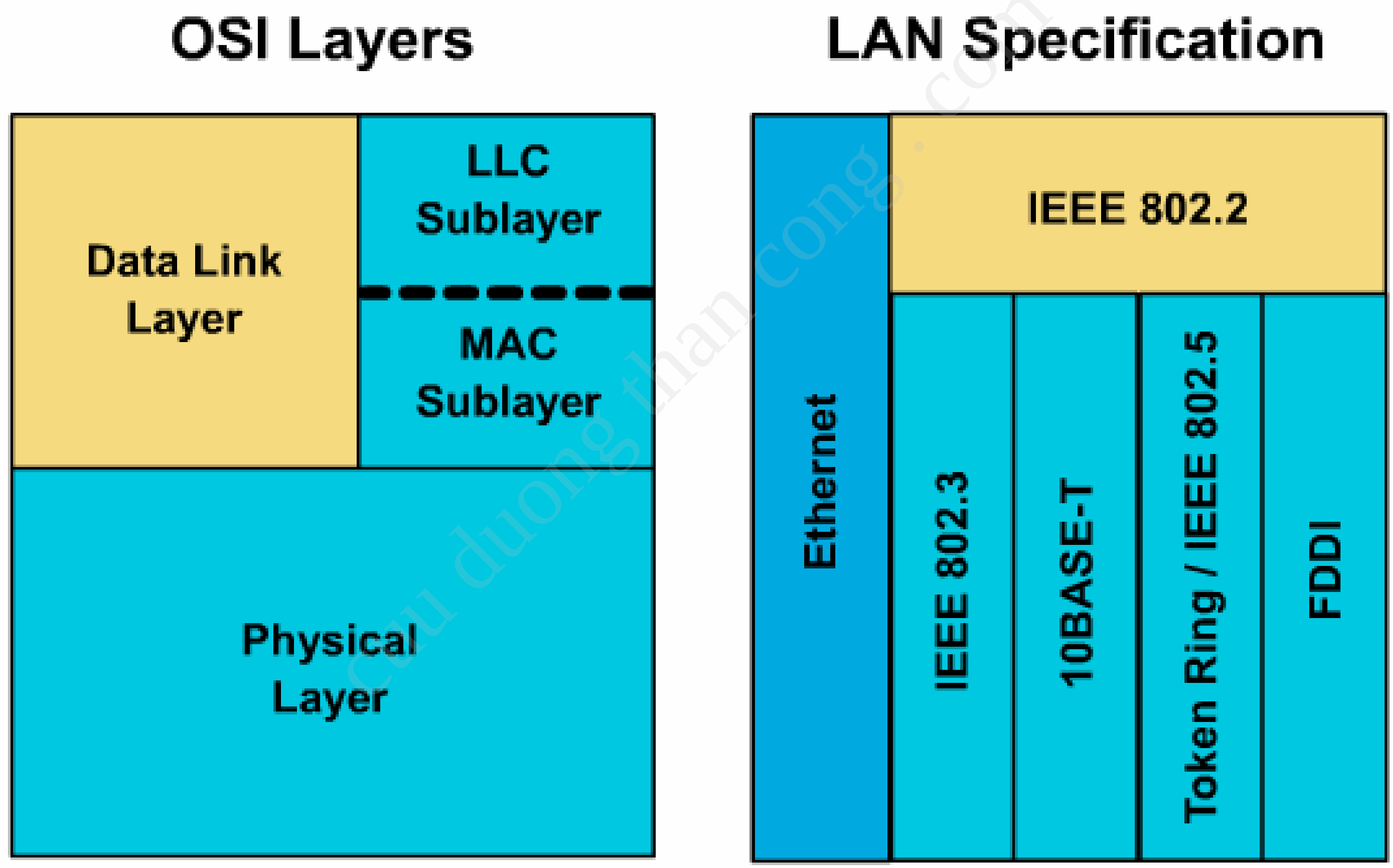


- Baseband verus Broadband

IEEE Ethernet naming rules

		IEEE 802.3 Values				
Characteristic	Ethernet Value	10Base5	10Base2	10BaseT	10BaseFL	100BaseT
Data rate (Mbps)	10	10	10	10	10	100
Signaling method	Baseband	Baseband	Baseband	Baseband	Baseband	Baseband
Maximum segment length (m)	500	500	185	100	2,000	100
Media	50-ohm coax (thick)	50-ohm coax (thick)	50-ohm coax (thin)	Unshielded twisted-pair cable	Fiber-optic	Unshielded twisted-pair cable
Topology	Bus	Bus	Bus	Star	Point-to-point	Bus

Ethernet and the OSI model



Layer 1 vs Layer 2

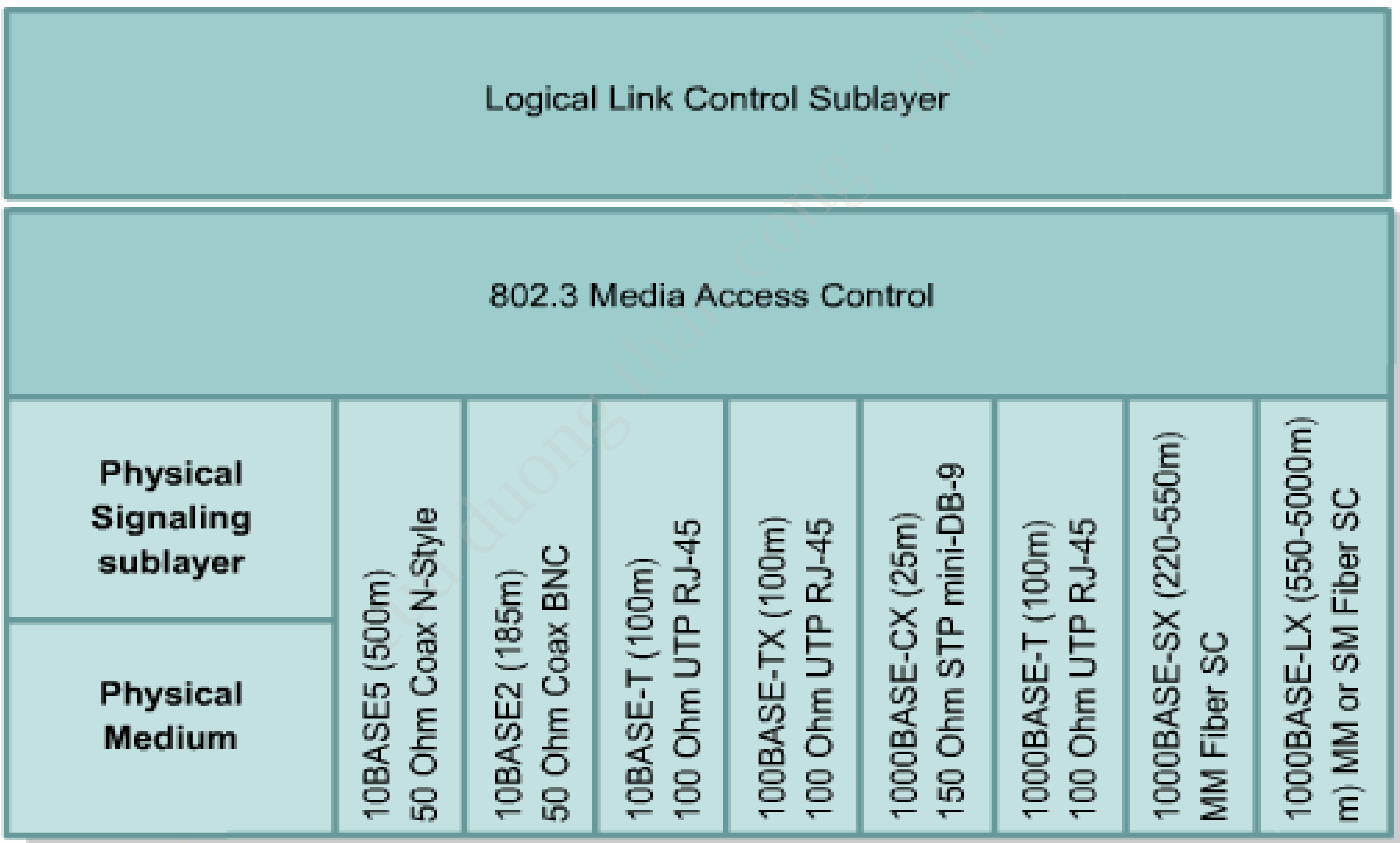
- Layer 1 can only describe streams of bits.
- Layer 2 uses *framing* to organize or group the bits.

- Layer 1 cannot name or identify computers.
- Layer 2 uses an *addressing* process to identify computers.

- Layer 1 cannot communicate with the upper-level layers.
- Layer 2 uses *Logical Link Control* (*LLC*) to communicate with the upper-level layers.

- Layer 1 cannot decide which computer will transmit binary data.
- Layer 2 uses *Media Access Control* (*MAC*) to decide which computer will transmit.

Ethernet and the OSI mode



Naming

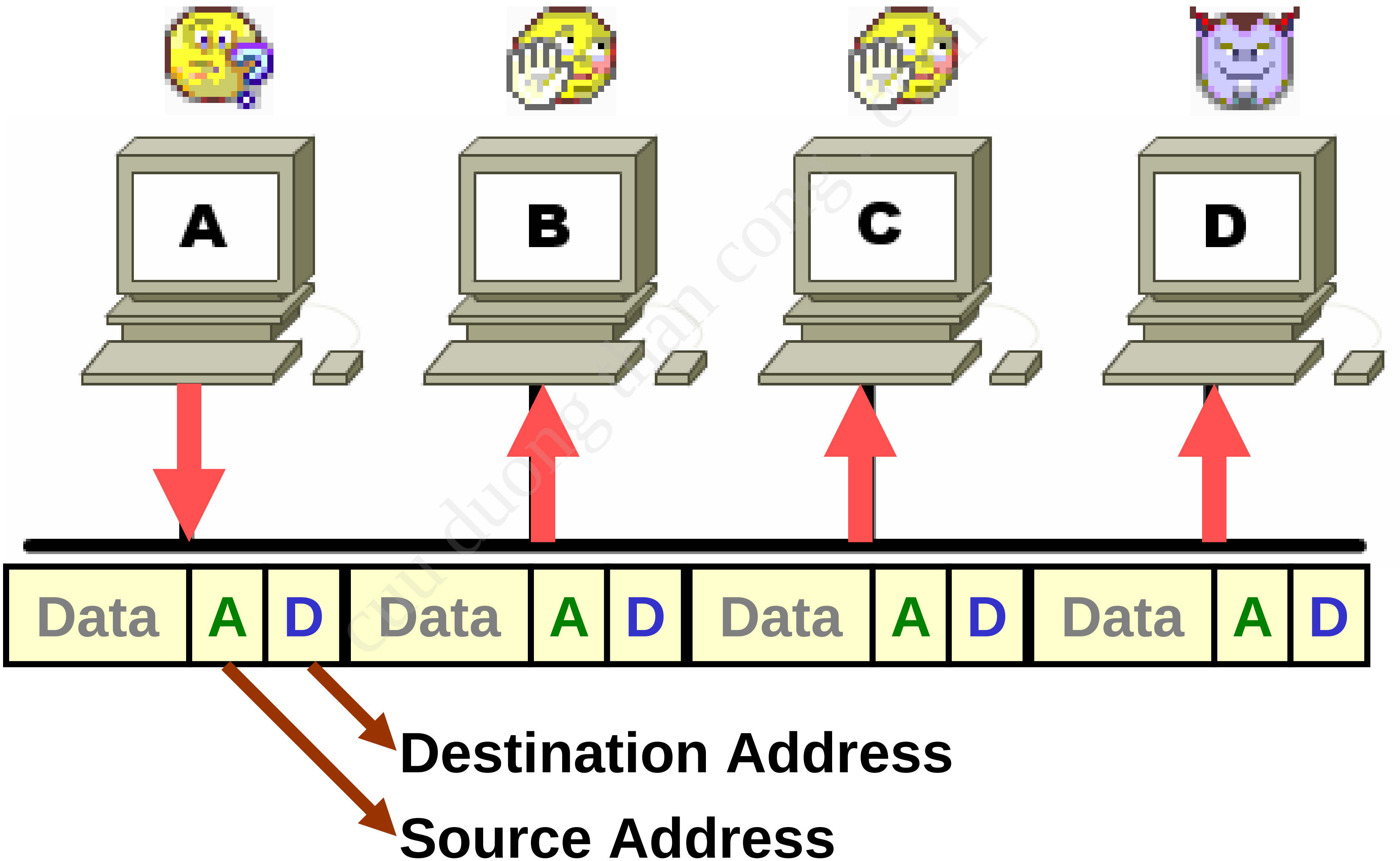
- Every computer has a unique way of identifying itself : MAC address or physical address.
- The physical address is located on the Network Interface Card (NIC).
- MAC addresses have no structure, and are considered flat address spaces. MAC addresses are sometimes referred to as *burned-in addresses* (*BIAs*) because they are burned into read-only memory (ROM) and are copied into random-access memory (RAM) when the NIC initializes.
- 0000.0c12.3456 or 00-00-0c-12-34-56.

MAC address format

The remaining six hexadecimal digits comprise the interface serial number.

...decimal ...ministered ...ntify the vendor.

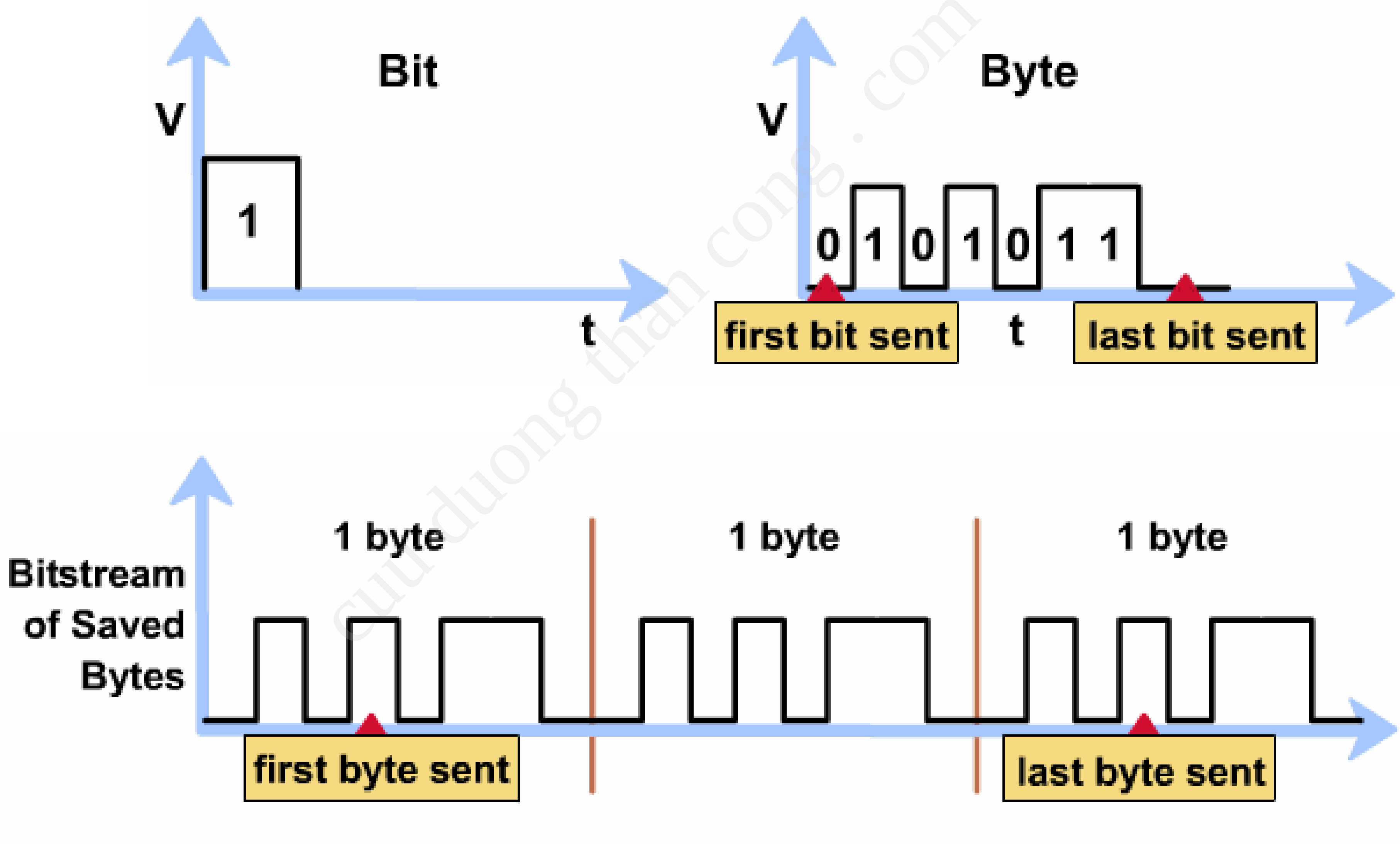
Using MAC addresses



Layer 2 framing : Why framing is necessary?

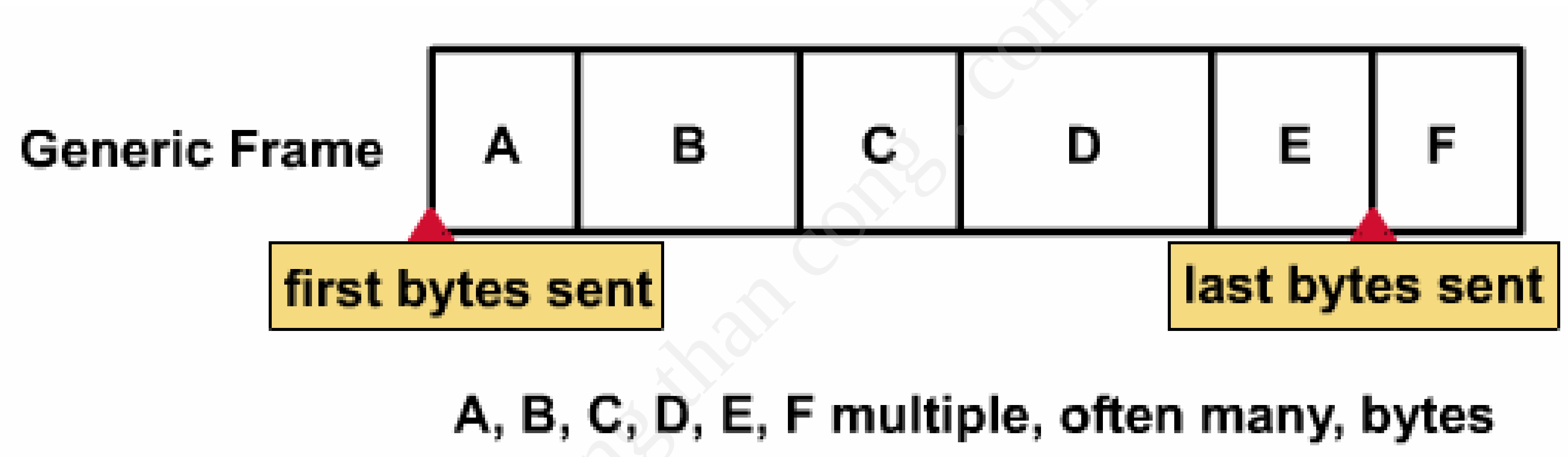
- Which computers are communicating with one another.
- When communication between individual computers begins and when it terminates.
- A record of errors that occurred during the communication.
- Whose turn it is to "talk" in a computer "conversation".

Frame format diagram



Frame format diagram

NETWORK TRAINING CENTER



- The frame format diagram shows different groupings of bits (*fields*) that perform other functions.
- Read them from left to right.

Generic frame format

Field Names					
A	B	C	D	E	F
Start Frame Field	Address Field	Type/ Length Field	Data Field	FCS Field	Stop Frame Field

- There are many different types of frames described by various standards.

Start frame field

Field Names					
A	B	C	D	E	F
Start Frame Field	Address Field	Type/ Length Field	Data Field	FCS Field	Stop Frame Field

- The **Start Frame field** tells other devices on the network that a frame is coming down the wire.

Address field

Field Names					
A	B	C	D	E	F
Start Frame Field	Address Field	Type/ Length Field	Data Field	FCS Field	Stop Frame Field

- The **Address field** stores the source and destination MAC addresses.

Length/Type field

NETWORK TRAINING CENTER

Field Names					
A	B	C	D	E	F
Start Frame Field	Address Field	Type/ Length Field	Data Field	FCS Field	Stop Frame Field

- The Type/Length field is an optional field
- Exact length of frame, or
- Layer 3 protocol making the sending request, or
- Not used

Data field

Field Names					
A	B	C	D	E	F
Start Frame Field	Address Field	Type/ Length Field	Data Field	FCS Field	Stop Frame Field

- The **Data field** is the actual information being sent by the upper layer protocols. Therefore, it will be all upper layer data.

FCS field

Field Names					
A	B	C	D	E	F
Start Frame Field	Address Field	Type/ Length Field	Data Field	FCS Field	Stop Frame Field

- *Cyclic Redundancy Check (CRC) - performs polynomial calculations on the data*
- *Two-dimensional parity - adds an 8th bit that makes an 8 bit sequence have an odd or even number of binary 1's*
- *Internet checksum - adds the values of all of the data bits to arrive at a sum*

Stop frame field

Field Names					
A	B	C	D	E	F
Start Frame Field	Address Field	Type/ Length Field	Data Field	FCS Field	Stop Frame Field

- The **Stop Frame** field, also called the Frame Trailer, is an optional field that is used when the length of the frame was not specified in the Type/Length field.

Ethernet frame structure

Ethernet-II(DIX 2.0)

7+1	6	6	2	46-1500	4
Preamble	Dest. Address	Source Address	Type	Data	FCS

IEEE 802.3

7	1	6	6	2	64-1500	4
Preamble	Start Frame Delimiter	Dest. Address	Source Address	Length	802.2 Header & Data	FCS

Preamble Field

IEEE 802.3

7	1	6	6	2	64-1500	4
Preamble	Start Frame Delimiter	Dest. Address	Source Address	Length	802.2 Header & Data	FCS

- Preamble
  - Alternating patterns of 1s and 0s, ended by 2 bits **11**
  - Tells receiving stations whether frame is Ethernet or IEEE 802.3
    - Preamble + SOF(101010**11**) =Ethernet frame

Start of Frame

IEEE 802.3						
7	1	6	6	2	64-1500	4
Preamble	Start Frame Delimiter	Dest. Address	Source Address	Length	802.2 Header & Data	FCS

- Start of Frame
  - IEEE 802.3 only
  - Delimiter byte ends with 2 consecutive 1 bits
    - **Synchronize the frame-reception, ready to receive**
  - Explicitly specified in Ethernet

Address

IEEE 802.3						
7	1	6	6	2	64-1500	4
Preambl e	Start Frame Delimiter	Dest. Address	Source Address	Length	802.2 Header & Data	FCS

- Destination and source addresses
  - 1st 3 bytes are vendor-specific
    - **Specified by IEEE**
  - Last 3 bytes are specified by vendor
    - **Ethernet or IEEE 802.3 vendor**
  - Source address is always unicast
  - Destination can be unicast, multicast, or broadcast

Type/Length

IEEE 802.3						
7	1	6	6	2	64-1500	4
Preambl e	Start Frame Delimiter	Dest. Address	Source Address	Length	802.2 Header & Data	FCS

- **Type:** DIX versions of Ethernet used, Specifies the upper-layer protocol to receive the data
- **Length:** Early IEEE Ethernet versions used
- If => 0x600 (hexadecimal), then the frame is interpreted according to the Ethernet II type code indicated.

Data - Ethernet

NETWORK TRAINING CENTER

Ethernet-II(DIX 2.0)

7+1	6	6	2	46-1500	4
Preamble	Dest. Address	Source Address	Type	Data	FCS

- Data—Ethernet
  - At least 46 bytes of data
  - Padding bytes inserted as needed

Data IEEE 802.3

IEEE 802.3						
7	1	6	6	2	64-1500	4
Preamble	Start Frame Delimiter	Dest. Address	Source Address	Length	802.2 Header & Data	FCS

- Data—IEEE 802.3
  - Upper-layer protocol destination is defined within the data portion of the frame (DSAP, SSAP, Control)
  - At least 64 bytes
  - Padding bytes inserted as needed

FCS

NETWORK TRAINING CENTER

Ethernet-II(DIX 2.0)					
7+1	6	6	2	46-1500	4
Preamble	Dest. Address	Source Address	Type	Data	FCS

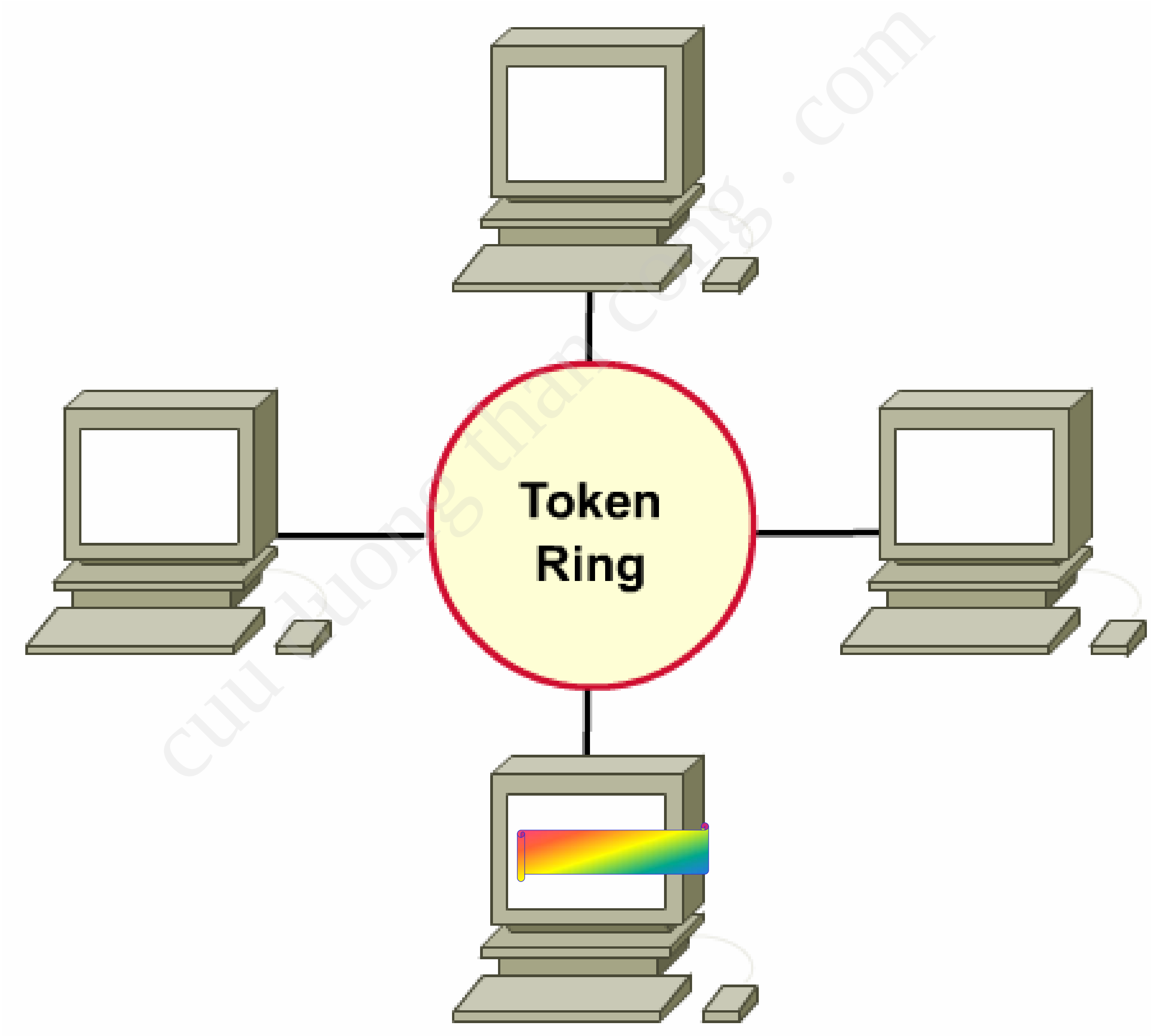
- Frame Check Sequence
  - 4 byte CRC value

ETHERNET OPERATION

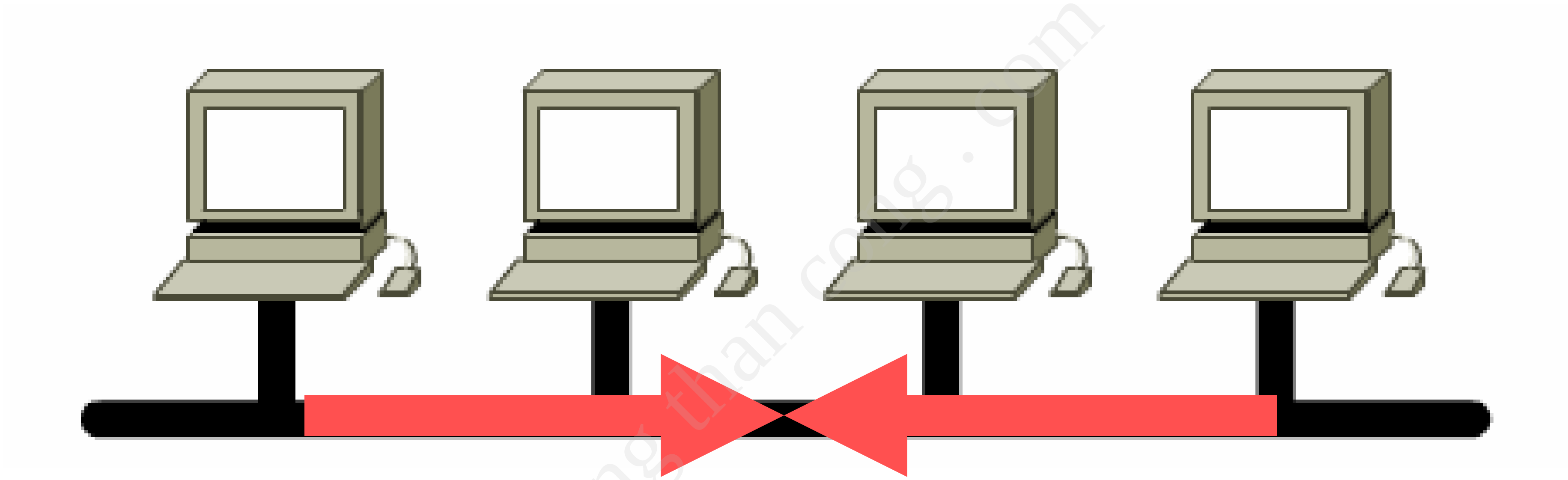
Media Access Control (MAC)

- Determine who can transmit in a shared-media environment
- MAC is a sublayer Layer 2
- Two types:
  - **Deterministic**: "Let's take turns".
    - *Token-Ring, FDDI.*
  - **Non-deterministic**: "First come, first serve".
    - *Ethernet : CSMA/CD.*

Deterministic MAC protocol

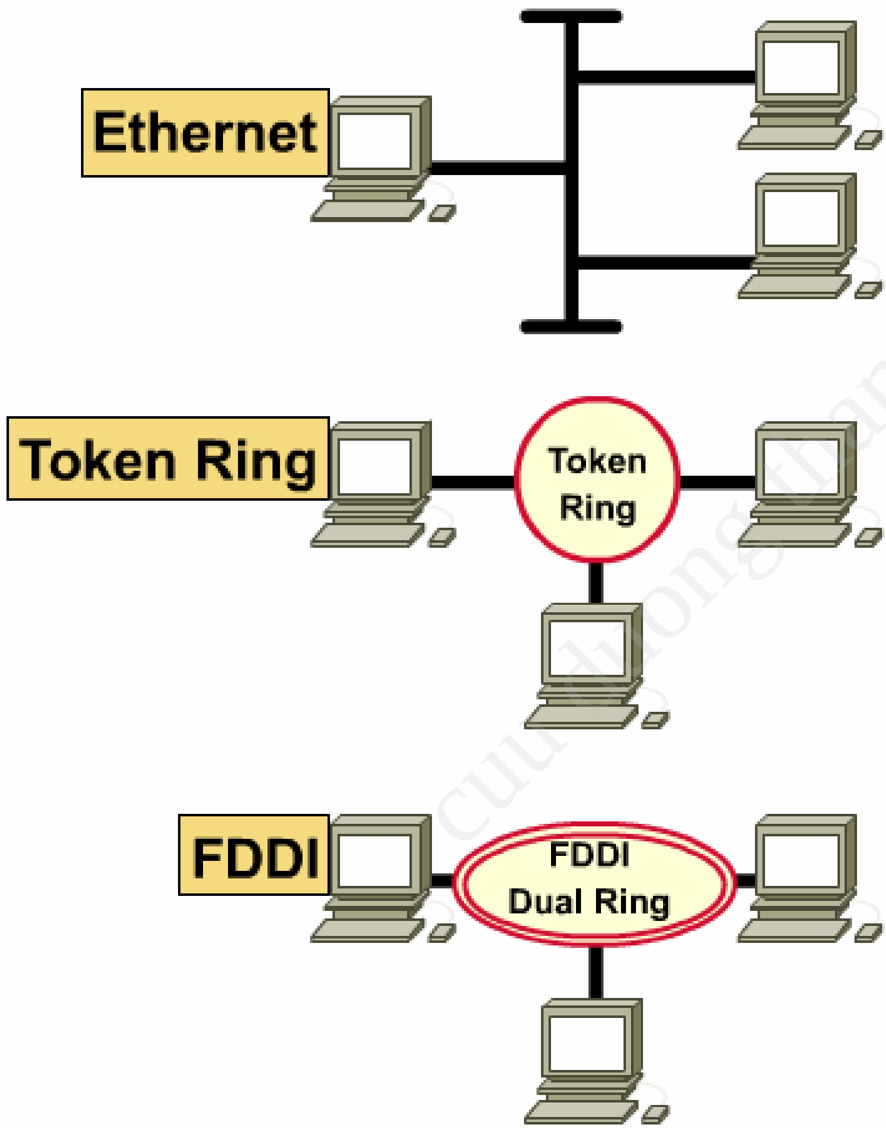


Non-deterministic MAC protocol



- Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

Three common Layer 2 technologies



- Ethernet: logical broadcast topology
- Token Ring: logical token ring topology
- FDDI: logical token ring topology

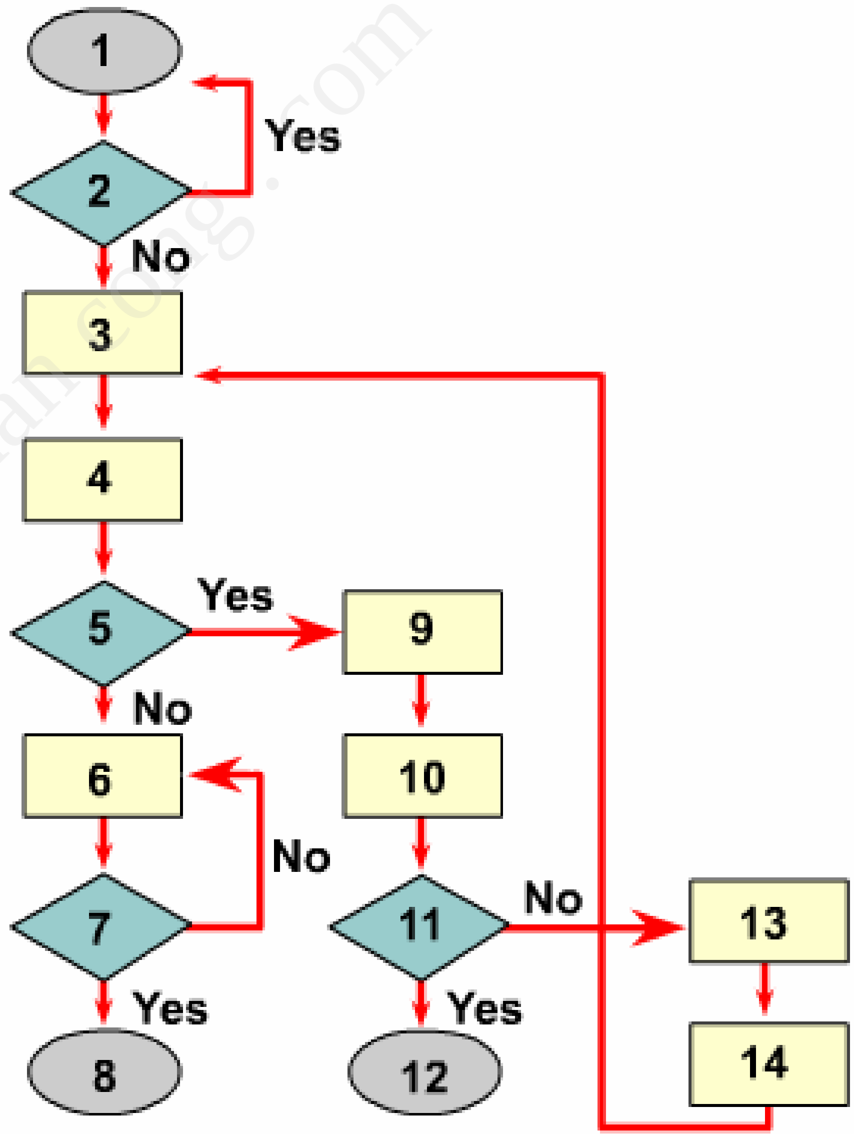
MAC rules and collision detection/backoff

- Ethernet is a shared-media broadcast technology. The access method CSMA/CD used in Ethernet performs three functions:
  - Transmitting and receiving data packets
  - Decoding data packets and checking them for valid addresses before passing them to the upper layers of the OSI model
  - Detecting errors within data packets or on the network

1

CSMA/CD Process

1. Host wants to transmit
2. Is carrier sensed?
3. Assemble frame
4. Start transmitting
5. Is a collision detected?
6. Keep transmitting
7. Is the transmission done?
8. Transmission completed
9. Broadcast jam signal
10. Attempts = Attempts + 1
11. Attempts > Too many?
12. Too many collisions; abort transmission
13. Algorithm calculates backoff
14. Wait for t microseconds



Ethernet timing

- The electrical signal takes time to travel down the cable (delay), and each subsequent repeater.
- Because of the **delay** and **latency**, it is possible for more than one station to begin transmitting at or near the same time. This results in a **collision**.
- In **full duplex** collisions should not occur

→ eliminates the concept of slot time.

- In **half duplex**, assuming that a collision does not occur, the 64 bits of preamble must be sent for timing synchronization first.

Ethernet timing

- 10 Mbps and slower versions of Ethernet are asynchronous.
- 100 Mbps and higher speed implementations of Ethernet are synchronous.
- The slot time defines Ethernet's maximum network diameter which limits its collision domain

Speed	Slot Time	Time Interval
10 Mbps	512 bit-times	51.2 μs
100 Mbps	512 bit-times	5.12 μs
1 Gbps	4096 bit-times	4.096 μs
10 Gbps	not applicable	not applicable

Ethernet timing

Ethernet Speed	Bit time
10 Mbps	100 ns
100 Mbps	10 ns
1000 Mbps = 1 Gbps	1 ns
10,000 Mbps = 10 Gbps	.1 ns

Interframe spacing

- The minimum spacing between two non-colliding frames is also called the interframe spacing.
- Spacing gap.

Speed	Interframe Spacing	Time required
10 Mbps	96 bit-times	9.6 µs
100 Mbps	96 bit-times	0.96 µs
1 Gbps	96 bit-times	0.096 µs
10 Gbps	96 bit-times	0.0096 µs

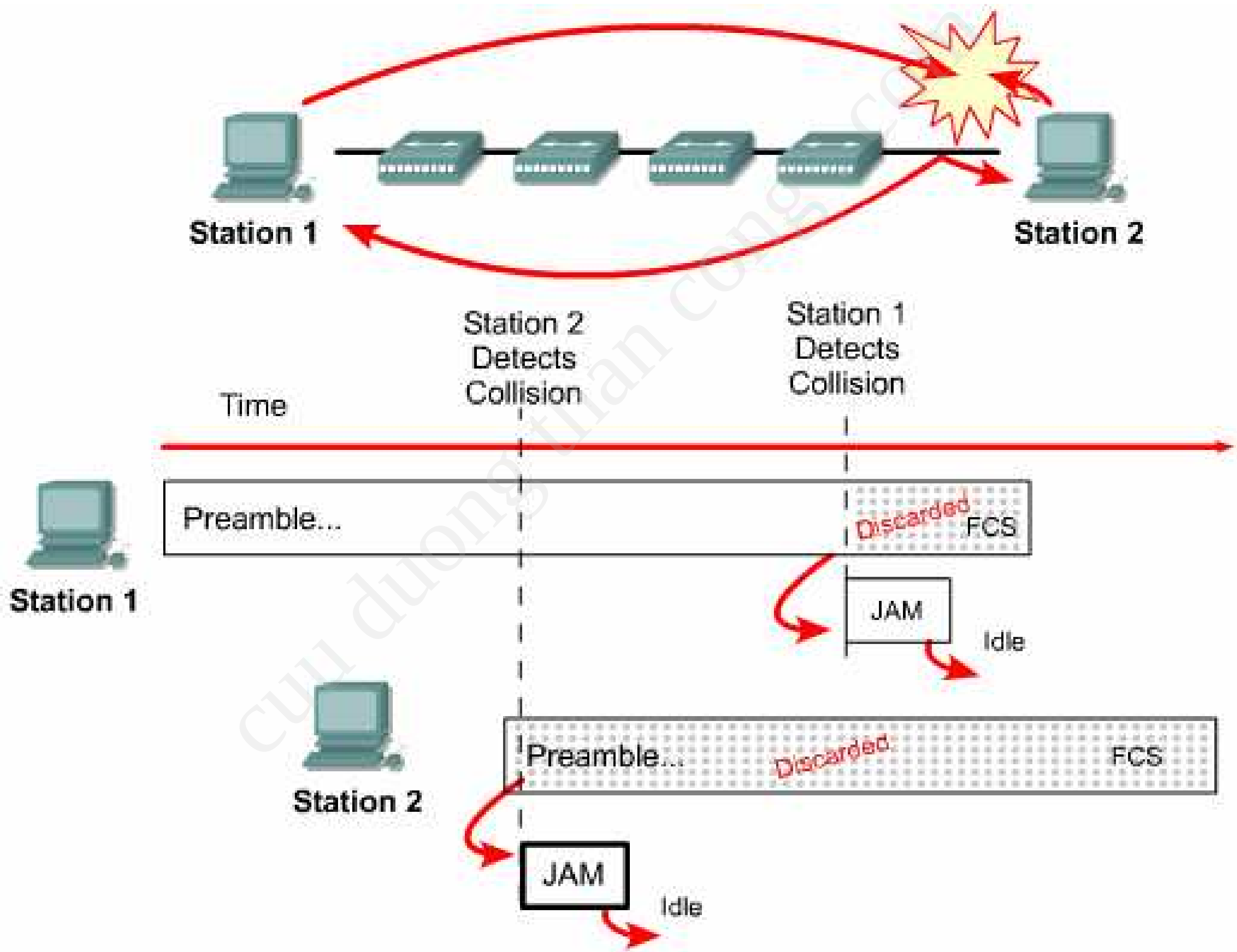
Backoff algorithm

NETWORK TRAINING CENTER

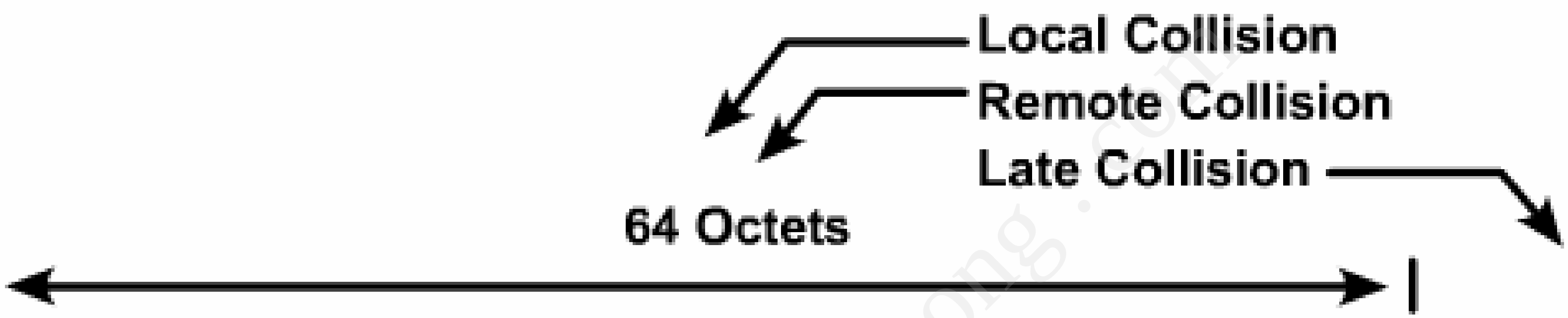
Speed	Slot Time	Time Interval
10 Mbps	512 bit-times	51.2 µs
100 Mbps	512 bit-times	5.12 µs
1 Gbps	4096 bit-times	4.096 µs
10 Gbps	not applicable	not applicable

- Backoff is the process by which a transmitting interface determines how long to wait following a collision before attempting to retransmit the frame.
- All transmitting interface then stop sending for a backoff time (randomly 0 .. 2n - 1 of 51.2ms).
- The range continues to expand until after 10 attempts it reaches 0 to 1023.
- unsuccessful after 16 attempts, the MAC function reports an **excessive collision error**.

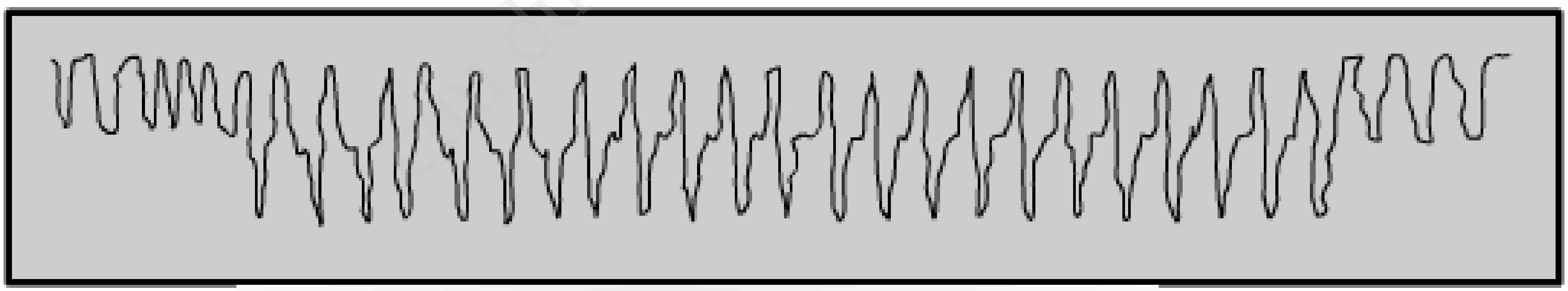
Error handling: Collision



Types of collisions



8	6	6	2	46 to 1500	4
Preamble	Destination Address	Source Address	Type	Data	Frame Check Sequence



Midframe 10BASE2 /10BASE5 collision captured by a digital storage oscilloscope.

Collisions

- **Local Collision**
  - Signal travels down the cable until it encounters a signal from the other station
  - The waveforms then overlap, the doubling of the signal pushes the voltage level of the signal beyond the allowed maximum
  - This over-voltage condition is then sensed by all of the stations on the local cable segment as a collision
  - Detected in first 64 octets

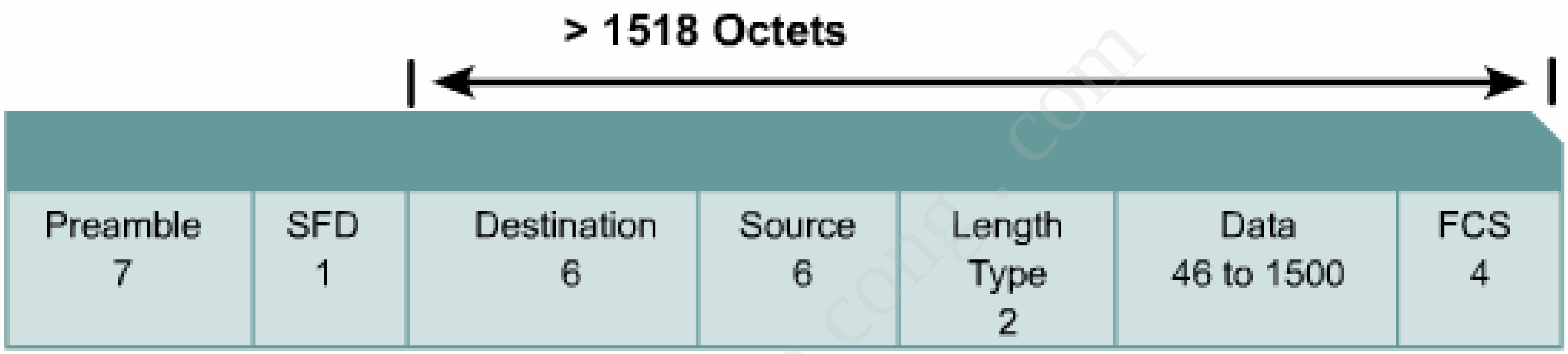
Collisions

- **Remote Collision**
  - Frame that is less than the minimum length
  - Has an invalid FCS checksum
  - Does not exhibit over voltage or simultaneous transmission activity
  - On UTP networks this is the most common sort of collision observed

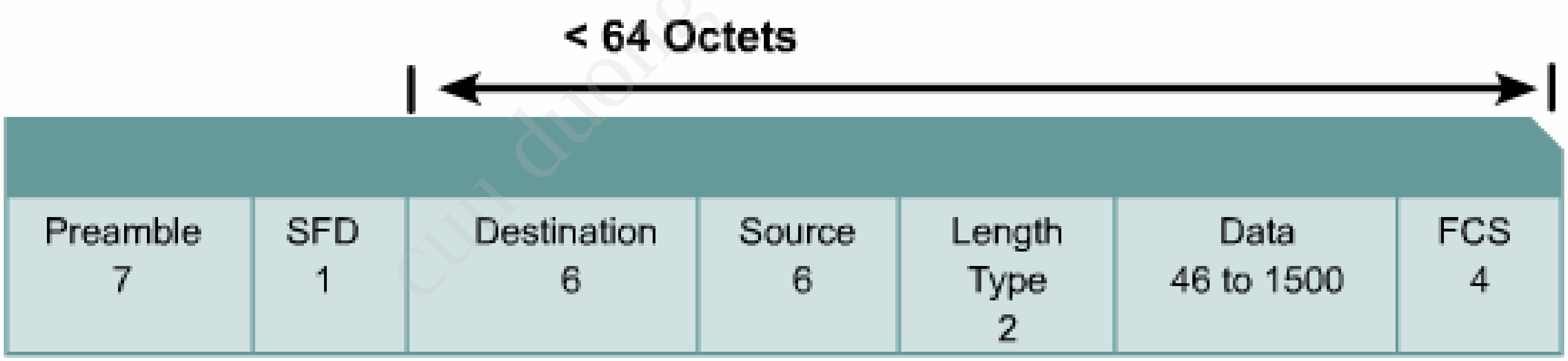
Collisions

- **Late Collision**
  - No possibility remaining for a normal or legal collision after the first 64 octets of data has been transmitted by the sending stations
  - Collisions occurring after the first 64 octets are called **late collisions**
  - Ethernet NIC will not automatically retransmit a frame that was collided late

Ethernet errors



Jabber and Long Frames are both in excess of the maximum frame size. Jabber is significantly larger.



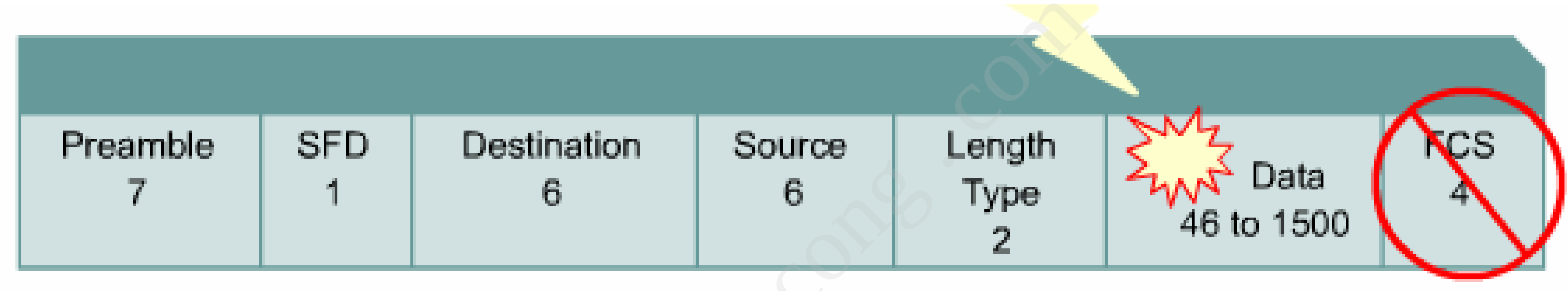
Short frames are properly formed in all but one aspect and have valid FCS checksums, but are less than the minimum frame size (64 octets).

Ethernet errors

The following are the sources of Ethernet error:

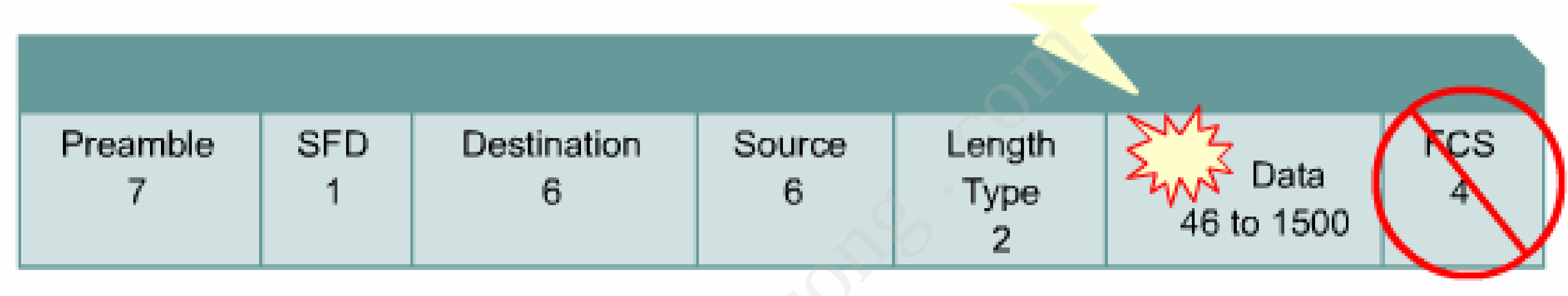
- **Collision or runt** – Simultaneous transmission occurring before slot time has elapsed
- **Late collision** – Simultaneous transmission occurring after slot time has elapsed
- **Jabber, long frame and range errors** – Excessively or illegally long transmission
- **Short frame, collision fragment or runt** – Illegally short transmission
- **FCS error** – Corrupted transmission
- **Alignment error** – Insufficient or excessive number of bits transmitted
- **Range error** – Actual and reported number of octets in frame do not match
- **Ghost or jabber** – Unusually long Preamble or Jam event

FCS and beyond



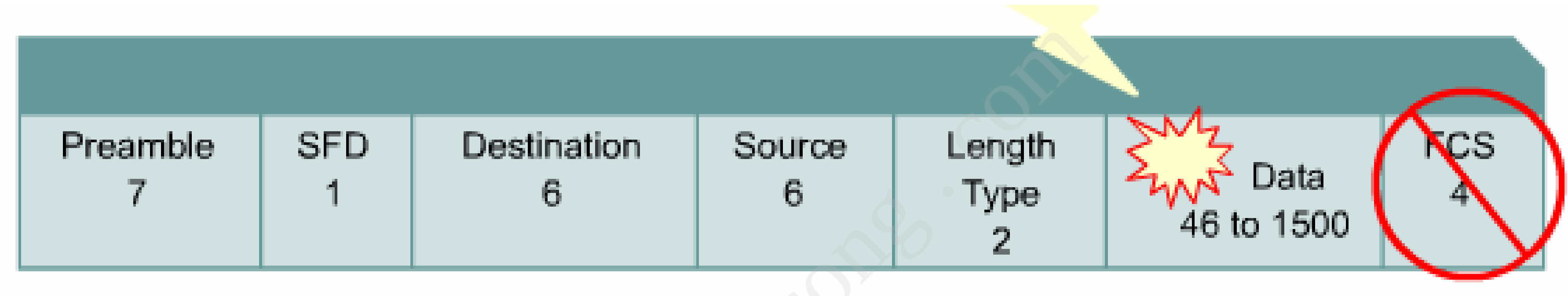
- High numbers of FCS errors from a single station usually indicates a faulty NIC and/or faulty or corrupted software drivers, or a bad cable connecting that station to the network.
- If FCS errors are associated with many stations, they are generally traceable to bad cabling, a faulty version of the NIC driver, a faulty hub port, or induced noise in the cable system.

FCS and beyond: Alignment error



- A message that does not end on an octet boundary is known as an alignment error.
- Such a frame is truncated to the nearest octet boundary, and if the FCS checksum fails, then an alignment error is reported.
- This is often caused by bad software drivers, or a collision, and is frequently accompanied by a failure of the FCS checksum.

FCS and beyond: Range error

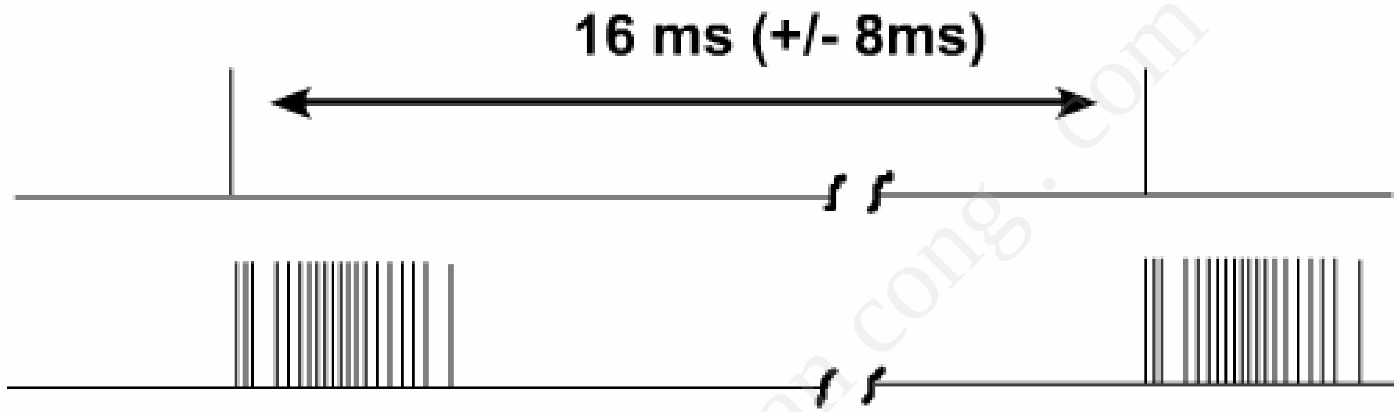


- A frame with a valid value in the Length field but did not match the actual number of octets counted in the data field of the received frame is known as a range error.
- This error also appears when the length field value is less than the minimum legal unpadded size of the data field. A similar error, Out of Range, is reported when the value in the Length field indicates a data size that is too large to be legal.

FCS and beyond: Ghost

- Term ghost to mean energy (noise) detected on the cable that appears to be a frame, but is lacking a valid SFD.
- To qualify as a ghost, the frame must be at least 72 octets long, including the preamble. Otherwise, it is classified as a remote collision.
- Ground loops and other wiring problems are usually the cause of ghosting.
- Most network monitoring tools do not recognize the existence of ghosts for the same reason that they do not recognize preamble collisions.

Ethernet auto-negotiation



- A process called Auto-Negotiation of speeds at half or full duplex was developed to make each technology interoperable
- Defines how two link partners may automatically negotiate a configuration offering the best common performance level.

Link establishment and full and half duplex

- 1000BASE-T full duplex ←→ 1000BASE-T full duplex
- 1000BASE-T half duplex ←→ 1000BASE-T half duplex
- 100BASE-TX full duplex ←→ 100BASE-TX full duplex
- 100BASE-TX half duplex ←→ 100BASE-TX half duplex
- 10BASE-T full duplex ←→ 10BASE-T full duplex
- 10BASE-T half duplex ←→ 10BASE-T half duplex

Summary

- *The basics of Ethernet technology*
- *The naming rules of Ethernet technology*
- *How Ethernet and the OSI model interact*
- *Ethernet framing process and frame structure*
- *Ethernet frame field names and purposes*
- *The characteristics and function of CSMA/CD*
- *Ethernet timing*
- *Interframe spacing*
- *The backoff algorithm and time after a collision*
- *Ethernet errors and collisions*
- *Auto-negotiation in relation to speed and duplex*

Q&A

CCNA Semester 1

The **Cisco Certified Network Associate** Curriculum

Chapter 07

ETHERNET TECHNOLOGIES

Objectives

- *Describe the differences and similarities among Ethernet, Fast Ethernet, Giga Ethernet and 10Giga Ethernet.*

Table of Content

10Mbps and 100Mbps Ethernet

10Mbps Ethernet: Parameters

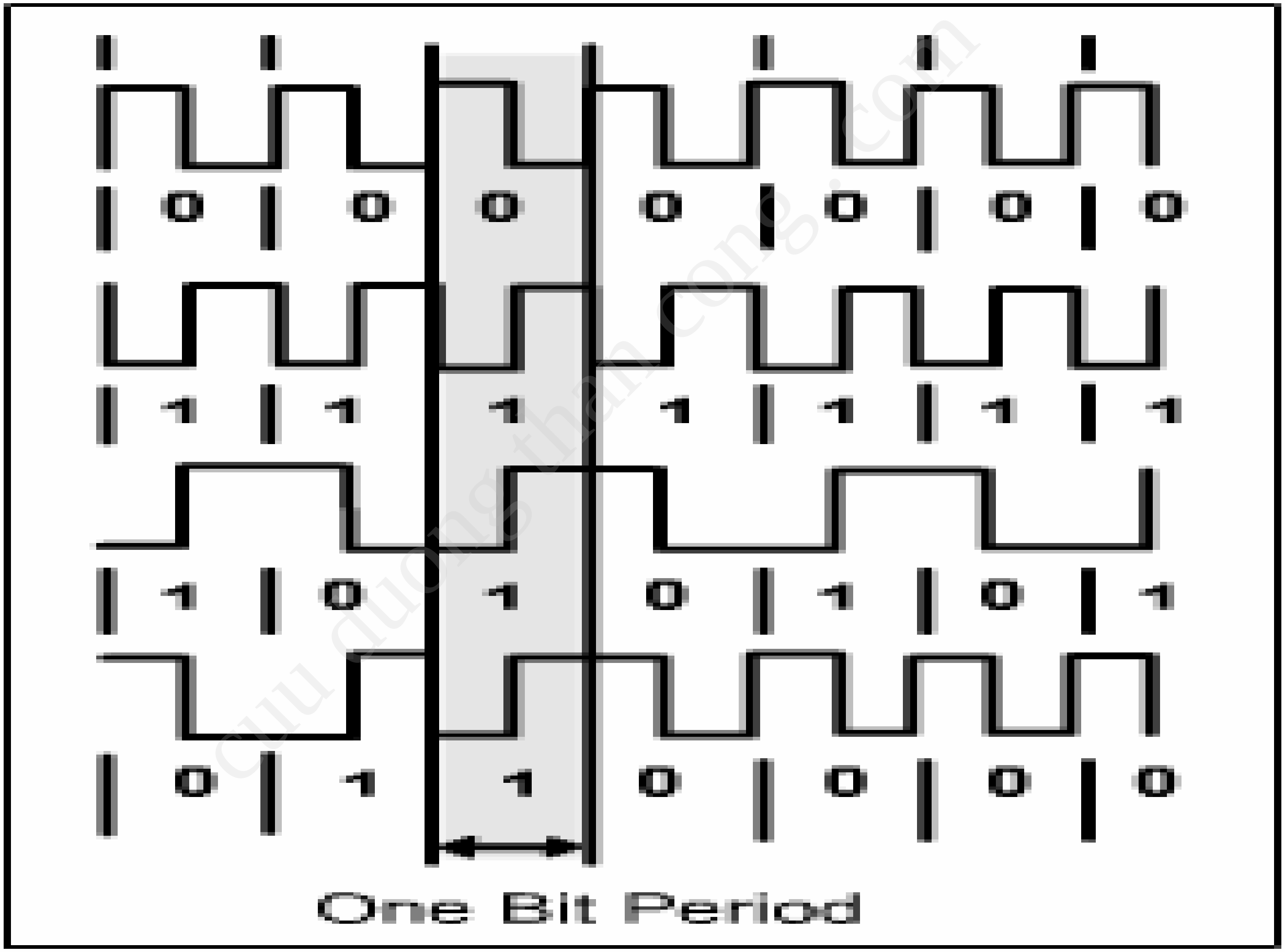
Parameter	Value
Bit Time	100 nanoseconds (ns)
Slot Time	512 bit times (64 octets)
Interframe Spacing	96 bits *
Collision Attempt Limit	16
Collision Backoff Limit	10
Collision Jam Size	32 bits
Maximum Untagged Frame Size	1518 octets
Minimum Frame Size	512 bits (64 octets)

10Mbps Ethernet: Frame Ethernet

Ethernet Frame

Preamble	SFD	Destination	Source	Length Type	Data : Pad	FCS
7	1	6	6	2	46 to 1500	4

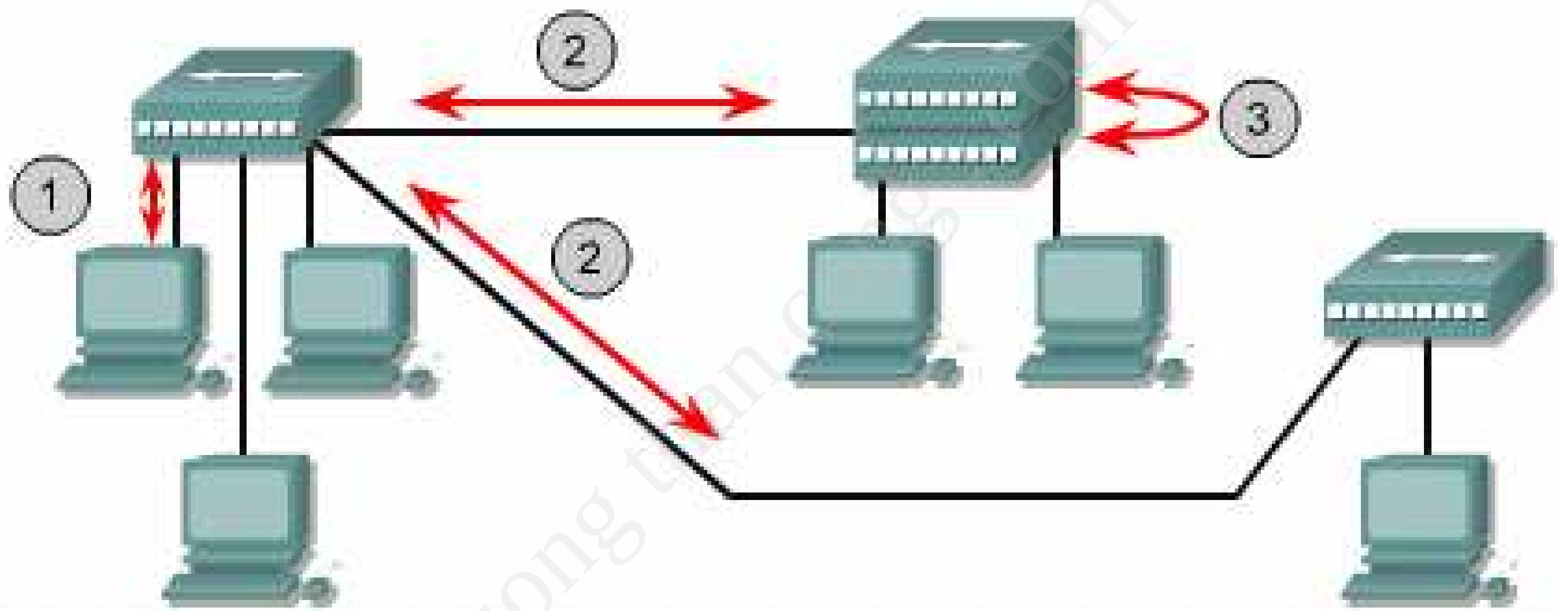
10Mbps Ethernet :Manchester encoding example



10Mbps Ethernet (cont.)

Standard	Topology	Medium	Maximum cable length	Transport
10BASE5	Bus	Thick coaxial cable	500m	Half-duplex
10BASE2	Bus	Thin coaxial cable	185m	Half-duplex
10BASE-T	Star	CAT3 UTP	100m	Half or Full-duplex

10Mbps Ethernet: Architecture



1. The UTP Link Segment cable length is normally 1 to 100 m between the workstation and the hub, and between the hubs.

2. Each hub is a multi-port repeater, so links between hubs count toward the repeater limit.

3. These two "stackable" hubs with interconnected backplanes count as only one hub, or repeater.

100Mbps Ethernet

- 100BASE-TX, 100BASE-FX
- Bit time: 10ns
- Slot time: 512 bit times.
- Frame format is the same as the 10-Mbps frame
- Encoding: 4B/5B
- Topology: star
- Half or Full - duplex

100BASE-TX and 100BASE-FX

Standard	Medium	Maximum cable length	Encoding
100BASE-TX	CAT5 UTP	100m	MLT-3
100BASE-FX	Multi-mode fibre (MMF) **62.5/125**	412m	NRZI

Fast Ethernet architecture

NETWORK TRAINING CENTER

Architecture	100BASE-TX	100BASE-FX	100BASE-TX and FX
Station/switch to station/switch	100m	412m	N/A
One Class I Repeater	200m	272m	100m (TX) 160,8m (FX)
One Class II repeater	200m	320m	100m (TX) 208m (FX)
Two Class II repeaters	205m	228m	105m (TX) 211,2m (FX)

Gigabit and 10-Gigabit Ethernet

1000-Mbps Ethernet

- Bit time: 1ns
- Slot time: 4096 bit times.
- Frame has the same format as is used for 10 and 100-Mbps Ethernet.
- *The differences between standard Ethernet, Fast Ethernet and Gigabit Ethernet occur at the physical layer!*

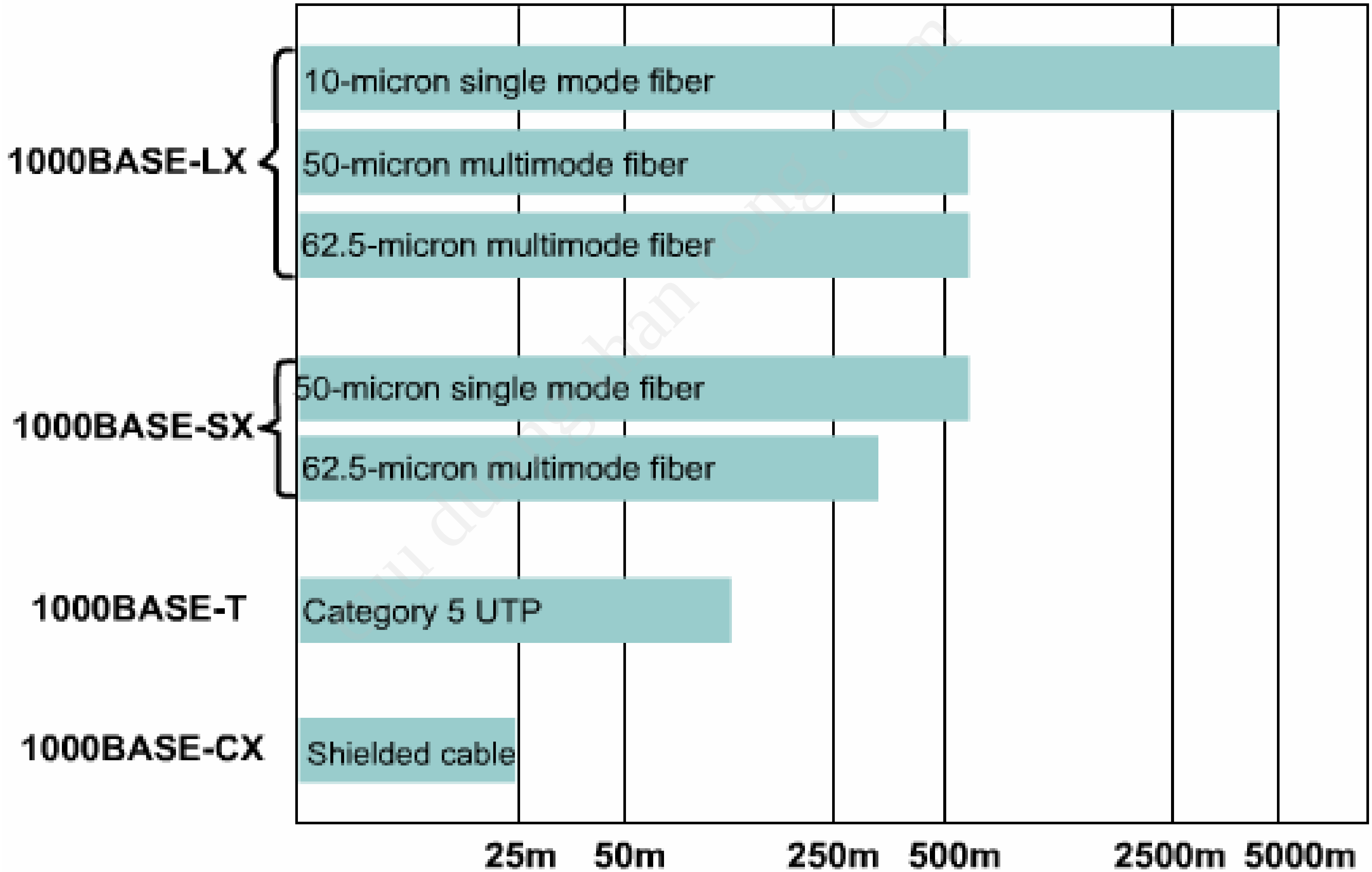
1000BASE - T

- Medium: CAT5 UTP.
- 4D-PAM5 line encoding.
- 1000BASE-T supports both half-duplex as well as full-duplex operation.

1000BASE-SX and LX

- Medium:
  - 1000BASE – SX: short-wavelength 850nm laser.
  - 1000BASE – LX: long-wavelength 1310nm laser.
- Uses 8B/10B encoding converted to non-return to zero (NRZ) line encoding.
- Full duplex

Gigabit Ethernet architecture



10GbE compare to other varieties of Ethernet

- Frame format is the same
- Only full-duplex fiber connections are used, CSMA/CD is not necessary
- The IEEE 802.3 sublayers within OSI Layers 1 and 2 are mostly preserved, with a few additions to accommodate 40 km fiber links and interoperability with SONET/SDH technologies.
- Flexible, efficient, reliable, relatively low cost end-to-end Ethernet networks become possible.
- TCP/IP can run over LANs, MANs, and WANs with one Layer 2 Transport method.

10GbE family

- **10GBASE-SR**
- **10GBASE-LX4**
- **10GBASE-LR and 10GBASE-ER**
- **10GBASE-SW, 10GBASE-LW, 10GBASE-EW**

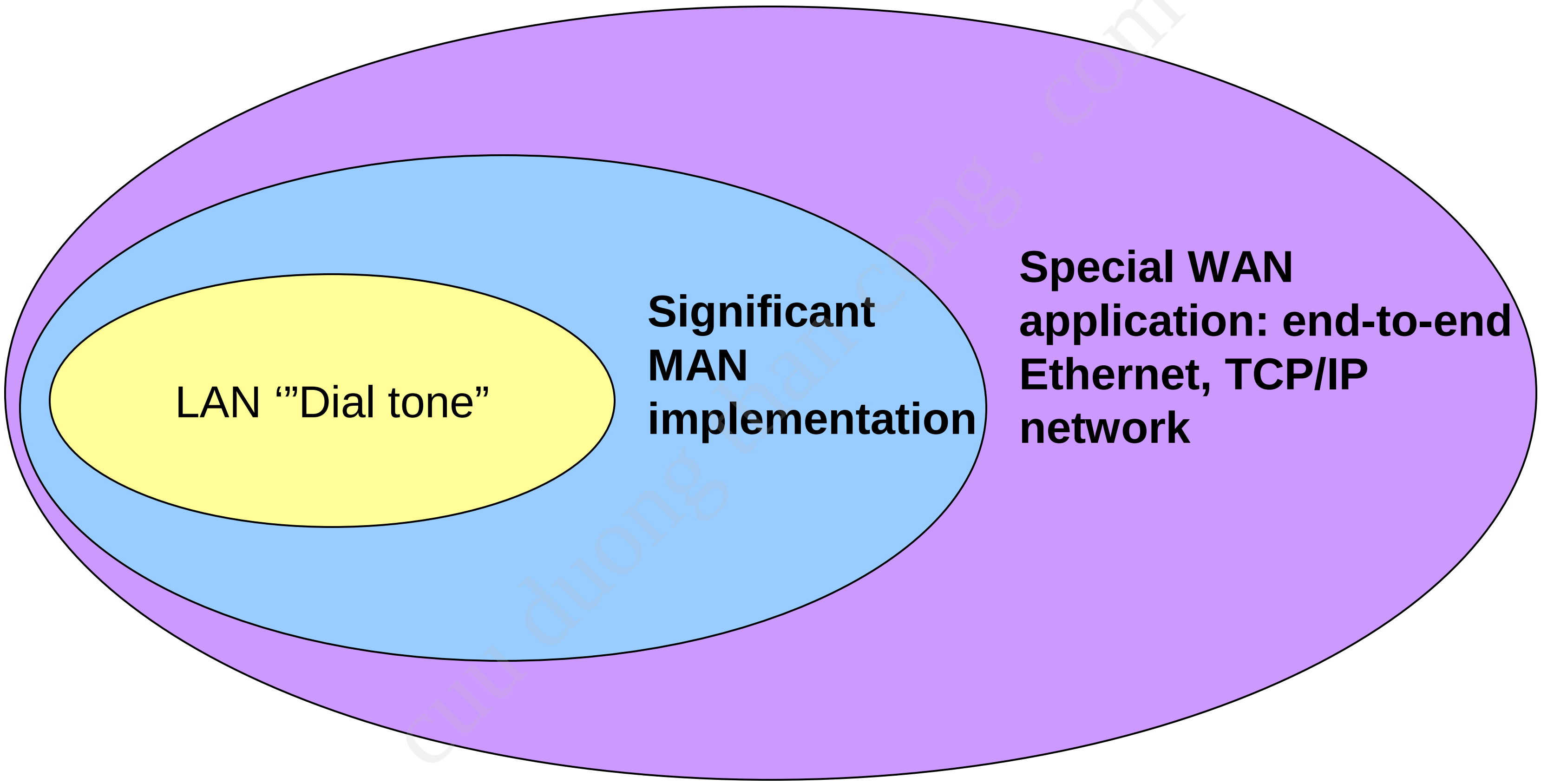
☞ ***The IEEE 802.3ae Task force and the 10-Gigabit Ethernet Alliance (10 GEA) are working to standardize these emerging technologies.***

10-Gigabit Ethernet architectures

IMPLEMENTATION	WAVE LENGTH	MEDIUM	MINIMUM MODAL BANDWIDTH	OPERATION DISTANCE
10GBASE-LX4	1310nm	62,5µm MMF	500Mhz/km	2-300m
10GBASE-LX4	1310nm	50um MMF	400Mhz/km	2-240m
10GBASE-LX4	1310nm	50um MMF	500Mhz/km	2-300m
10GBASE-LX4	1310nm	10um MMF	N/A	2-10Km
10GBASE-S	850nm	62,5um MMF	160Mhz/km	2-26m
10GBASE-S	850nm	50um MMF	200Mhz/km	2-33m
10GBASE-S	850nm	50um MMF	400Mhz/km	2-66m
10GBASE-S	850nm	50um MMF	500Mhz/km	2-82m
10GBASE-S	850nm	50um MMF	2000Mhz/km	2-300m
10GBASE-L	1310nm	10um SMF	N/A	2-10km
10GBASE-E	1550nm	10um SMF	N/A	2-30km

Future of Ethernet

NETWORK TRAINING CENTER



Summary

- The differences and similarities among 10BASE5, 10BASE2, and 10BASE-T Ethernet
- The key characteristics and varieties of 100-Mbps Ethernet
- The uses of specific media and encoding with Gigabit Ethernet
- The similarities and differences between Gigabit and 10-Gigabit Ethernet

Q&A

CCNA Semester 1

NETWORK TRAINING CENTER

The Cisco Certified Network Associate Curriculum

Chapter 08

ETHERNET SWITCHING

Objectives

NETWORK TRAINING CENTER

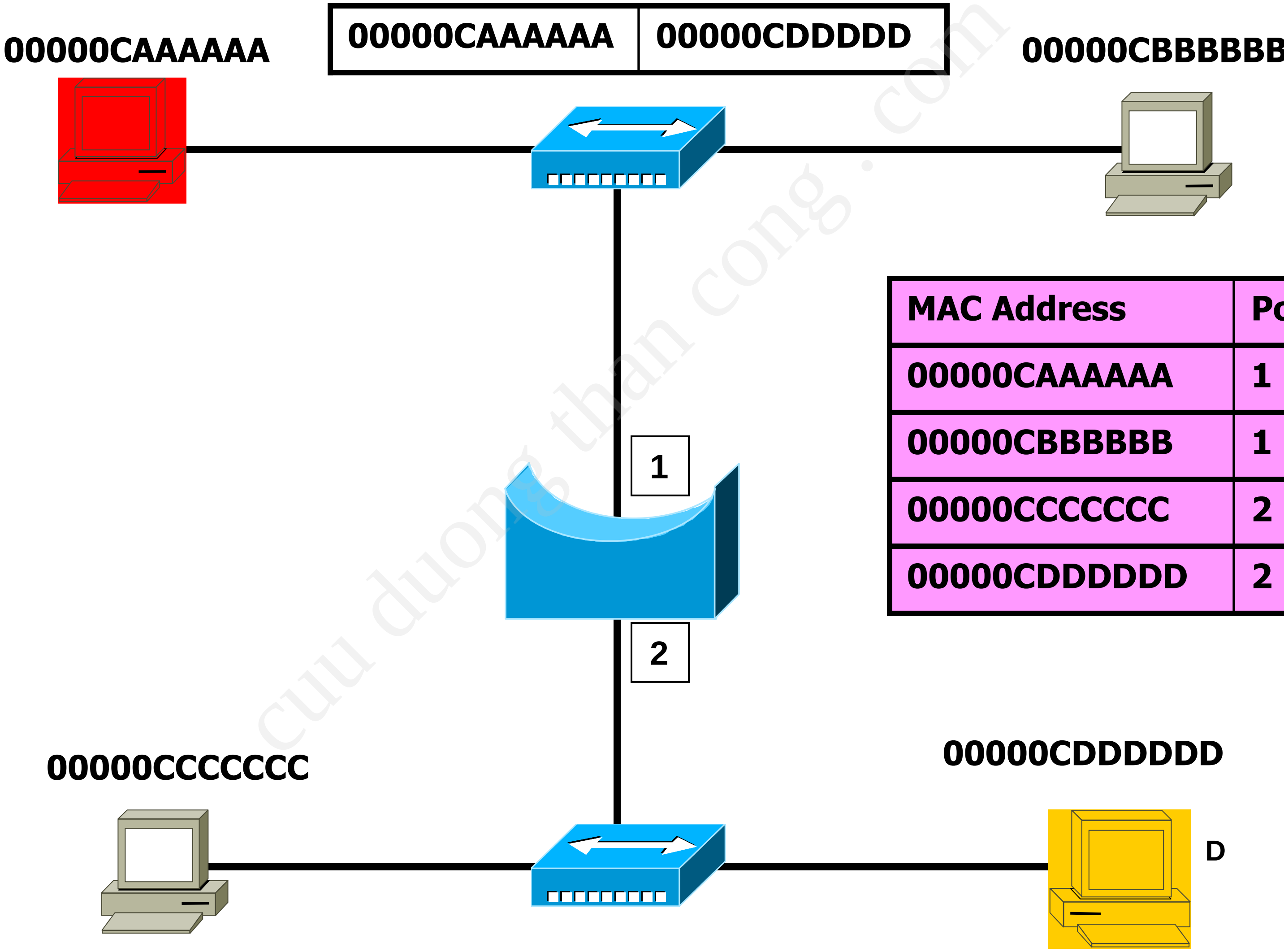
- Define bridging and switching
- Define and describe the content-addressable memory (CAM) table
- Define latency
- Describe store-and-forward and cut-through packet switching modes
- Explain Spanning-Tree Protocol (STP)
- Define collisions, broadcasts, collision domains, and broadcast domains
- Identify the Layers 1, 2, and 3 devices used to create collision domains and broadcast domains
- Discuss data flow and problems with broadcasts
- Explain network segmentation and list the devices used to create segments

Table of Content

NETWORK TRAINING CENTER

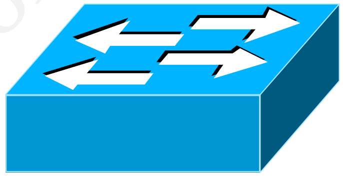
Ethernet Switching

Layer 2 bridging



MAC Address	Port
00000CAAAAAA	1
00000CBBBBBB	1
00000CCCCCCC	2
00000CDDDDDD	2

Switch operation

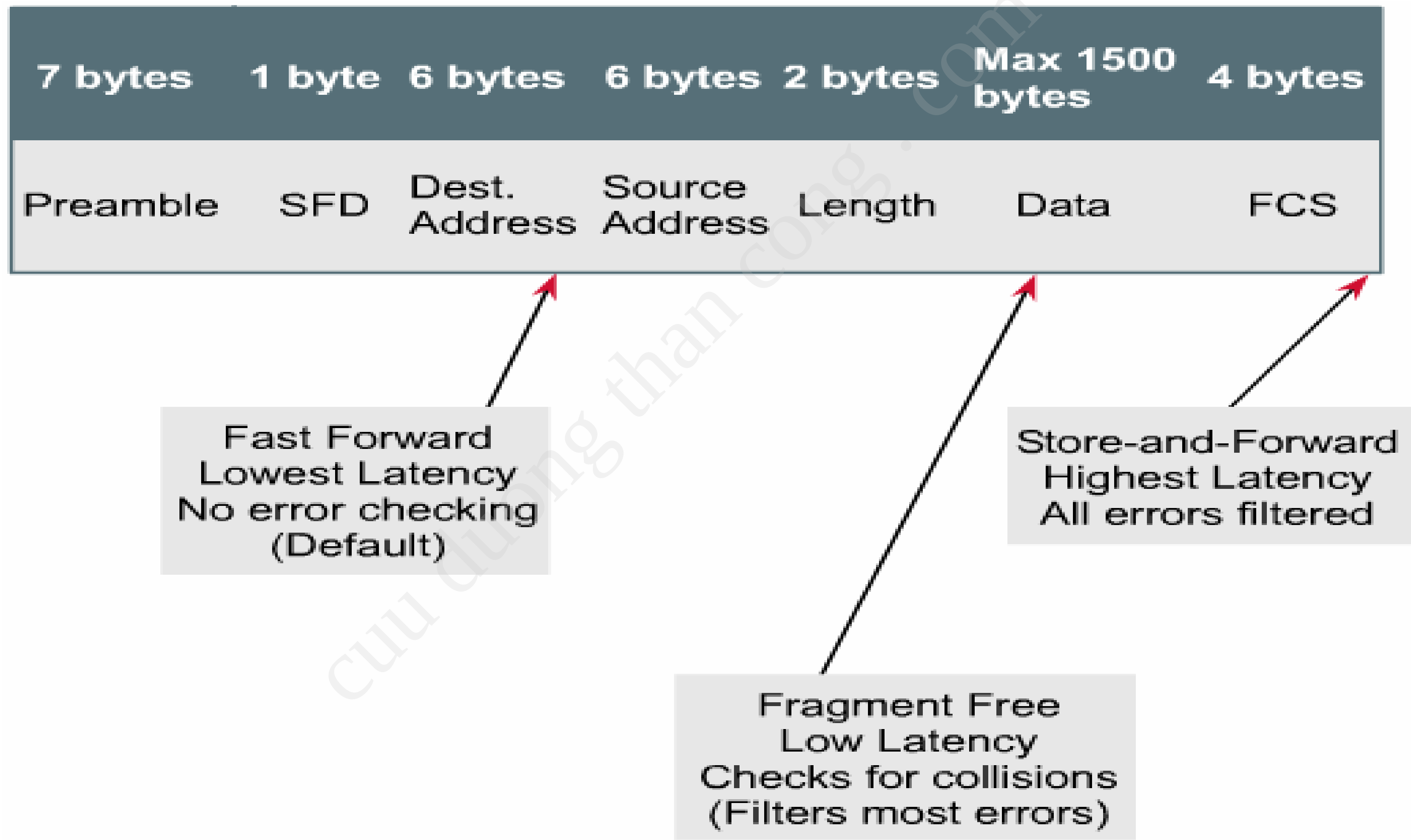


- A multi port bridge.
- Micro-segment
- Support full duplex.
- Dynamically builds and maintains a Content-Addressable Memory (CAM) table.

Latency

- Media delays caused by the finite speed that signals can travel through the physical media.
- Circuit delays caused by the electronics that process the signal along the path.
- Software delays caused by the decisions that software must make to implement switching and protocols.
- Delays caused by the content of the frame and where in the frame switching decisions can be made.

Switching modes



Switch modes

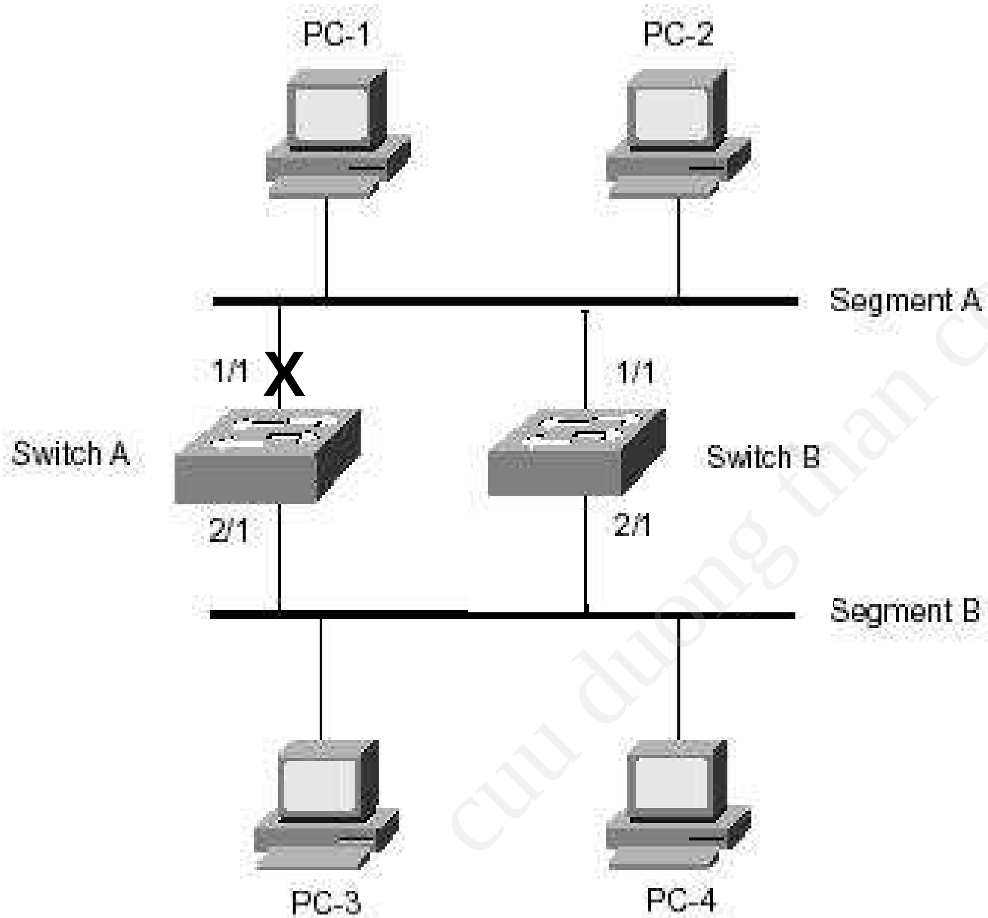
NETWORK TRAINING CENTER

- Store-and-forward:
  - The entire frame is received before forward.
  - The latency is greater with larger frames.
  - Error detection is high.
  - Must be used for asymmetric switching.
- Cut-through (Fast Forward):
  - Transfer the frame as soon as the destination MAC address is received
  - Lowest latency
  - No error checking
  - Must be used for symmetric switching

Switch modes (cont)

- Fragment-free
  - Reads the first 64 bytes (frame header) and starts to send out the packet before the entire data field and checksum are read
  - Verifies the reliability of the addresses and LLC protocol information

Spanning-Tree Protocol

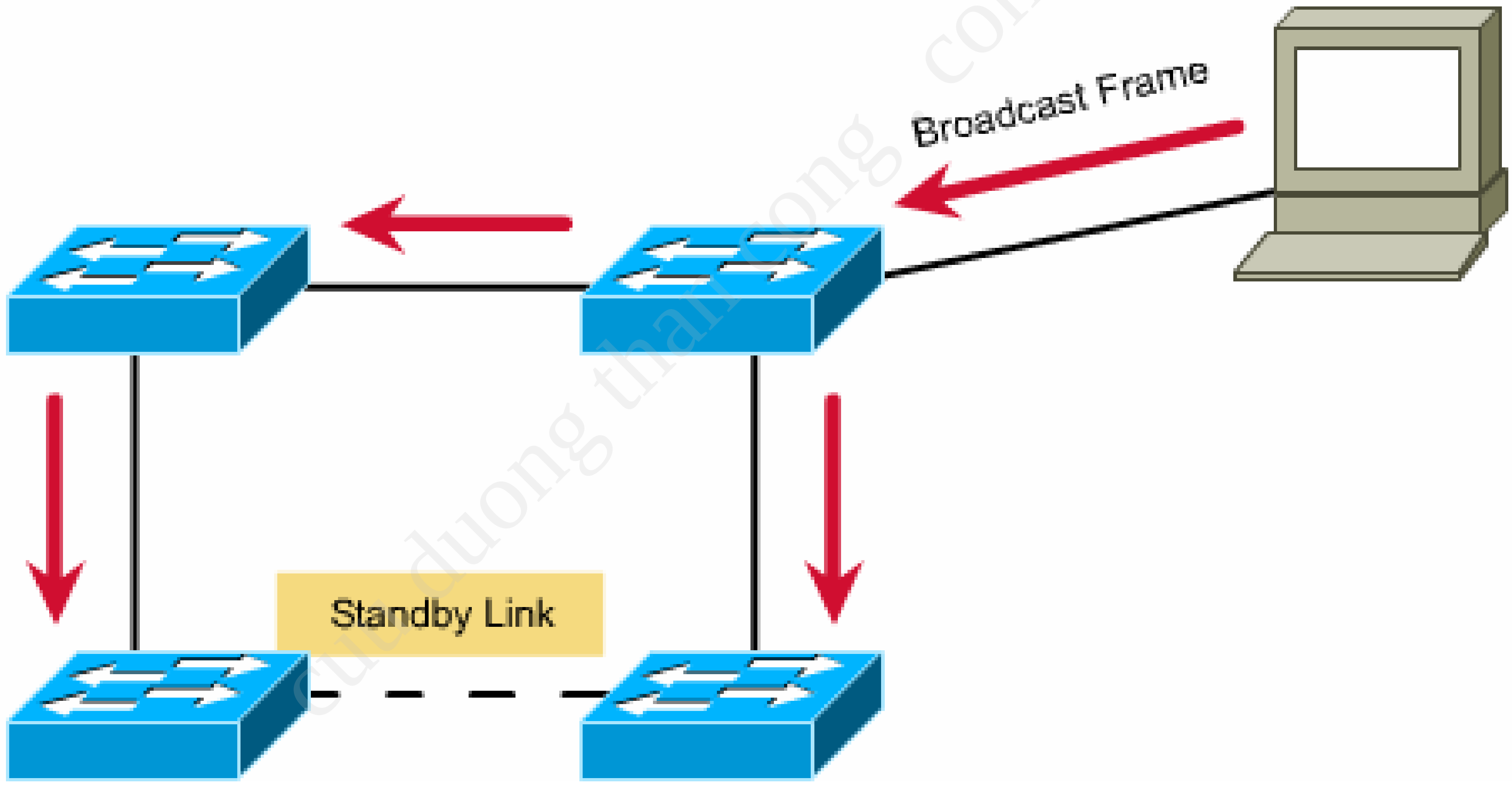


- Broadcast storms
- Multiple frame transmissions
- MAC database instability

Spanning-Tree Protocol (Cont)

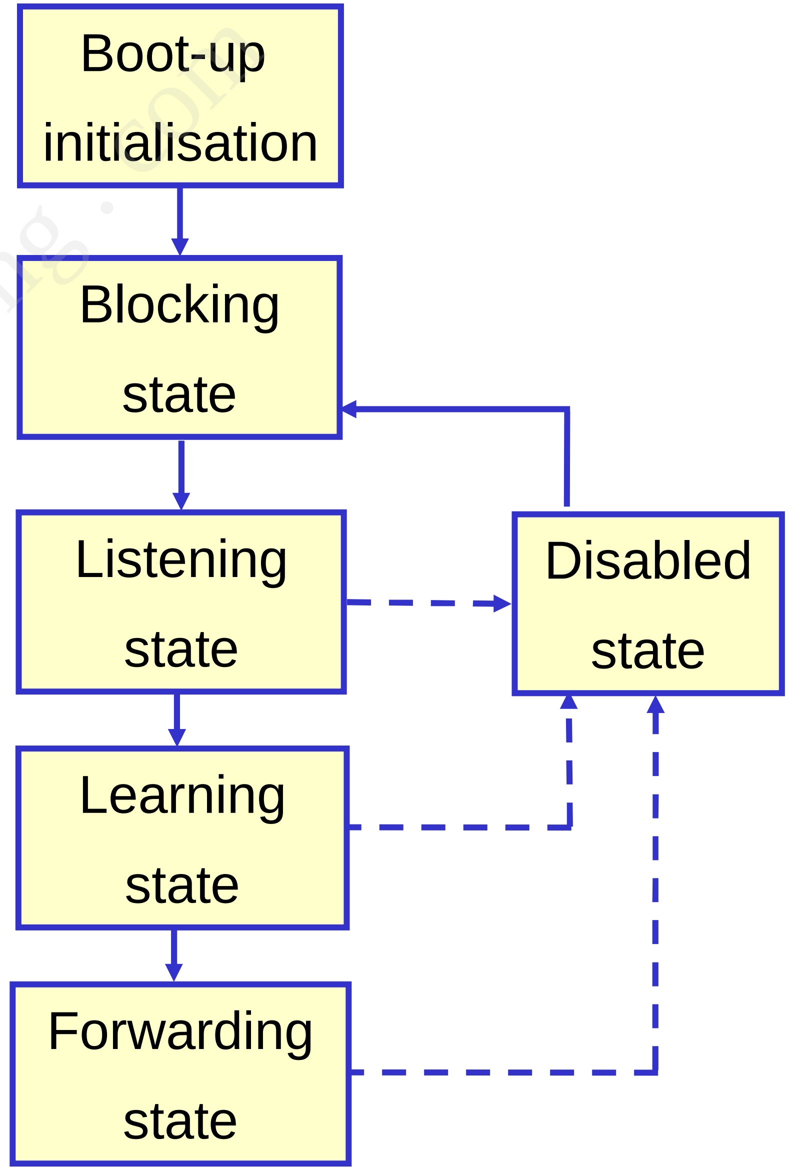
- STP is a standards-based routing protocol that is used to create a logical hierarchical tree with no loops
- Bridge Protocol Data Units (BPDUs)
- The switches use the spanning-tree algorithm (STA) to resolve and shut down the redundant paths.

Spanning-Tree Protocol (Cont)



Spanning-Tree Protocol (Cont) : STP port status

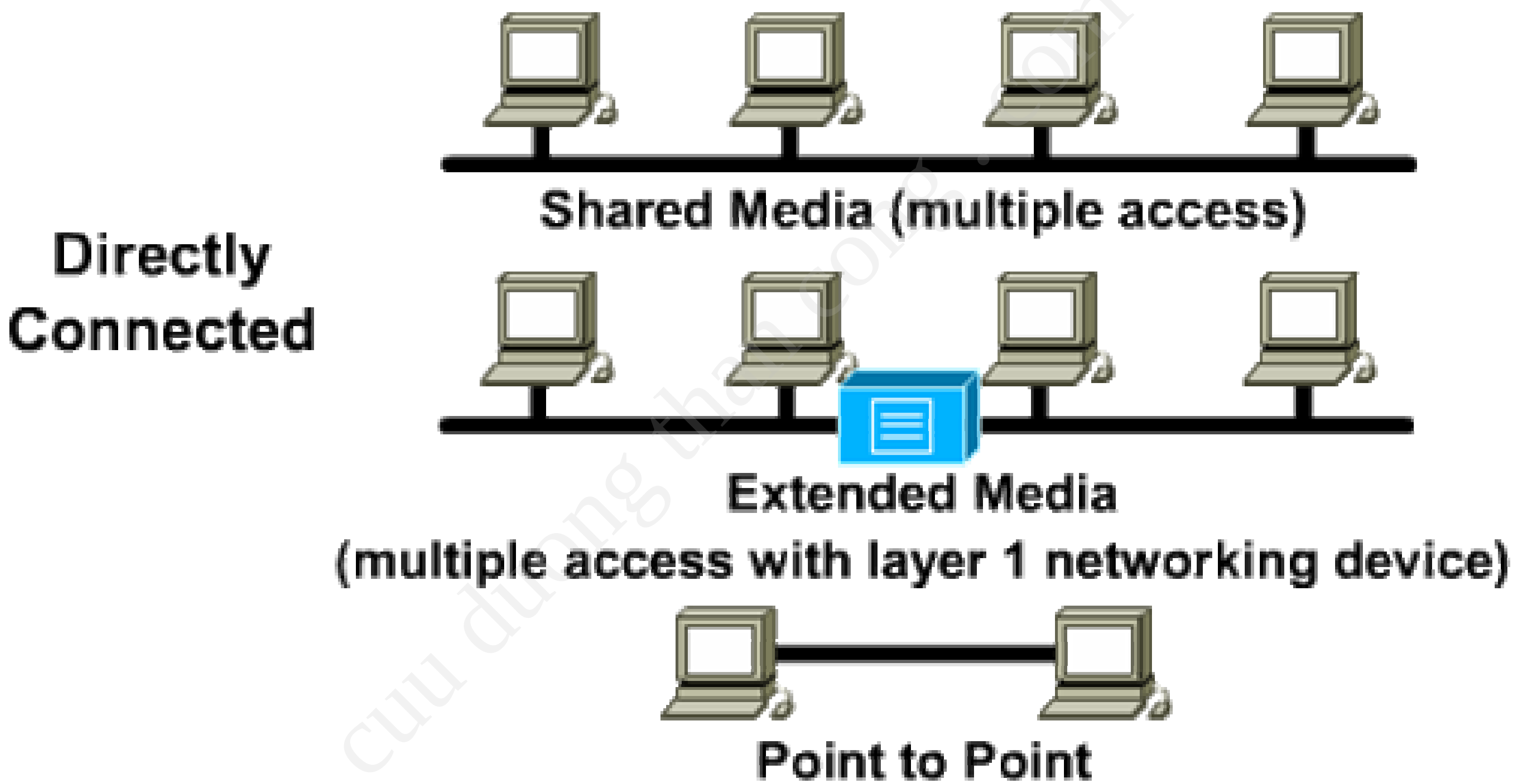
- Blocking: no frames forwarded, BPDUs heard
- Listening: no frames forwarded, listening for frames
- Learning: no frames forwarded, learning addresses
- Forwarding: frames forwarded, learning addresses
- Disabled: no frames forwarded, no BPDUs heard



Collision Domains and Broadcast Domains

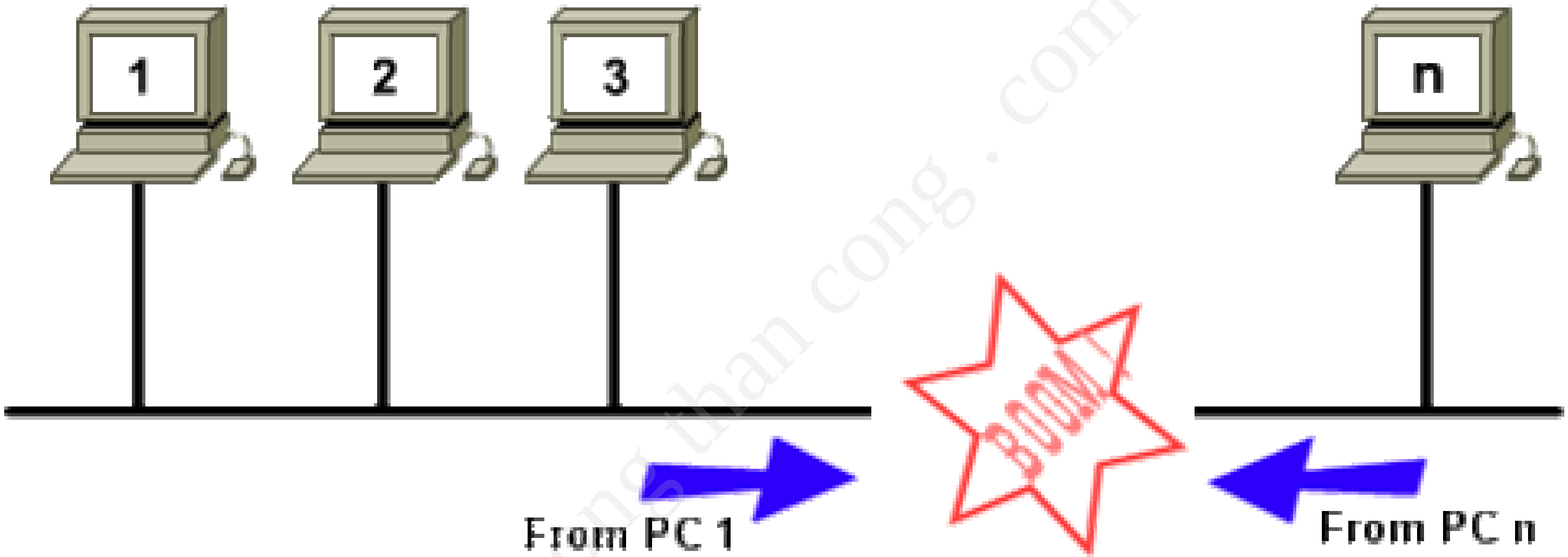
Shared media environments

NETWORK TRAINING CENTER



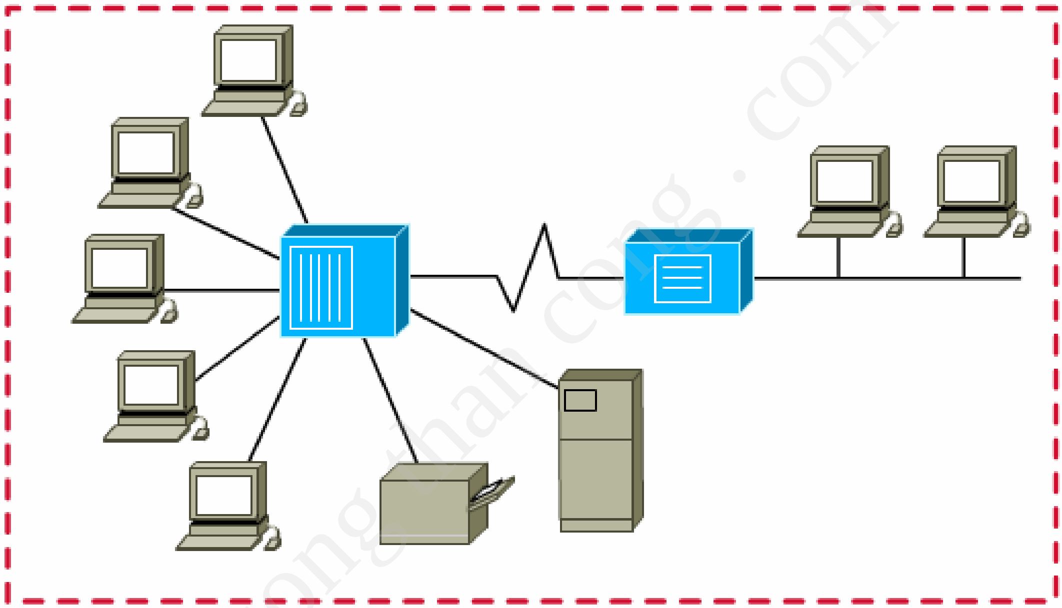
Collisions only occur in a shared environment

Collisions



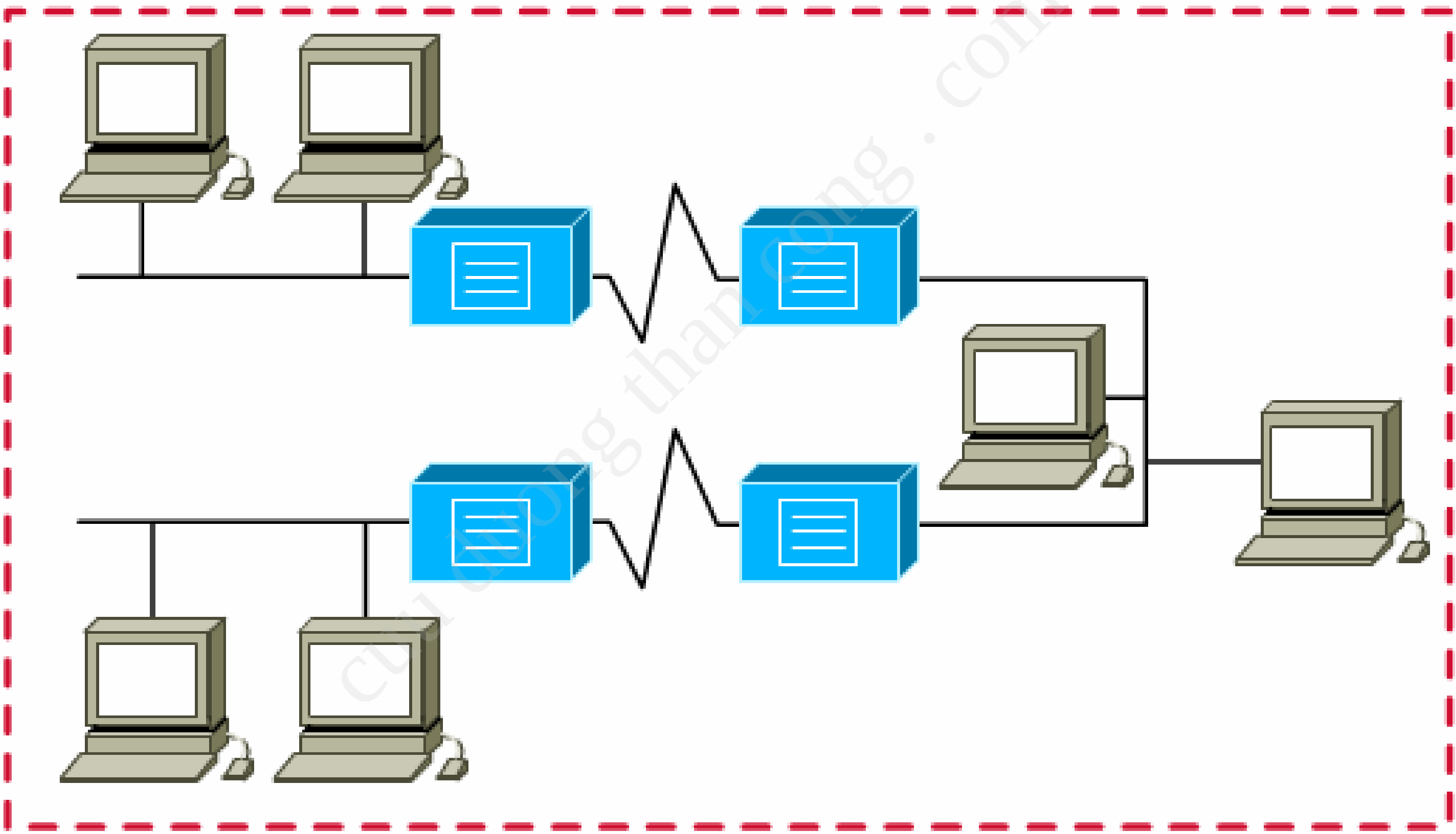
- More than one node attempts to transmit at the same time.
- Collisions occur in broadcast topology:
  - Ethernet LAN technology.

Collisions domain



- Collision Domains are the area where collisions occur.
- All of layer 1 interconnections are part of the collision domain.
- Extending a network with a repeater or a hub, results in a larger collision domain.

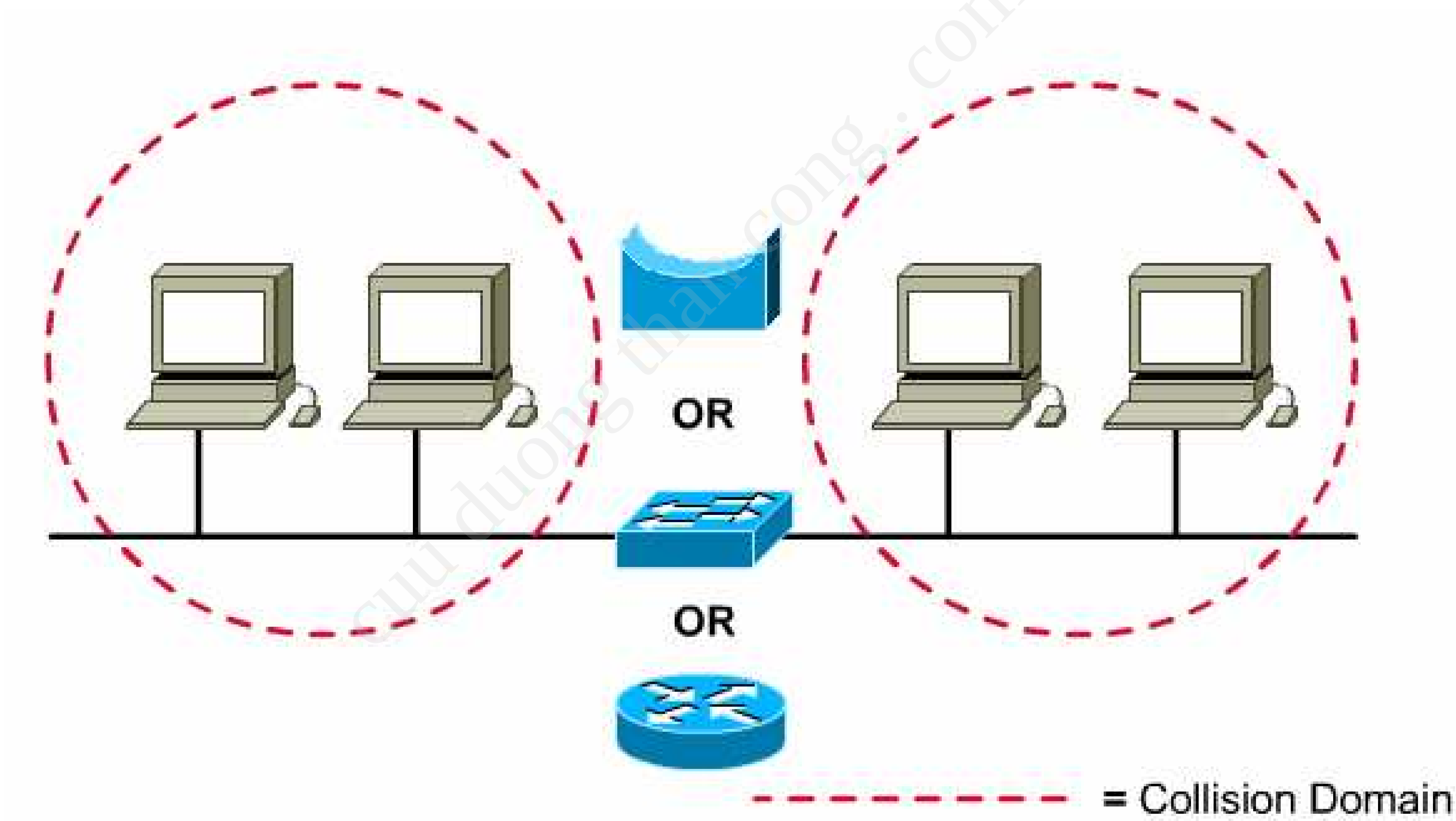
5-4-3-2-1 rule



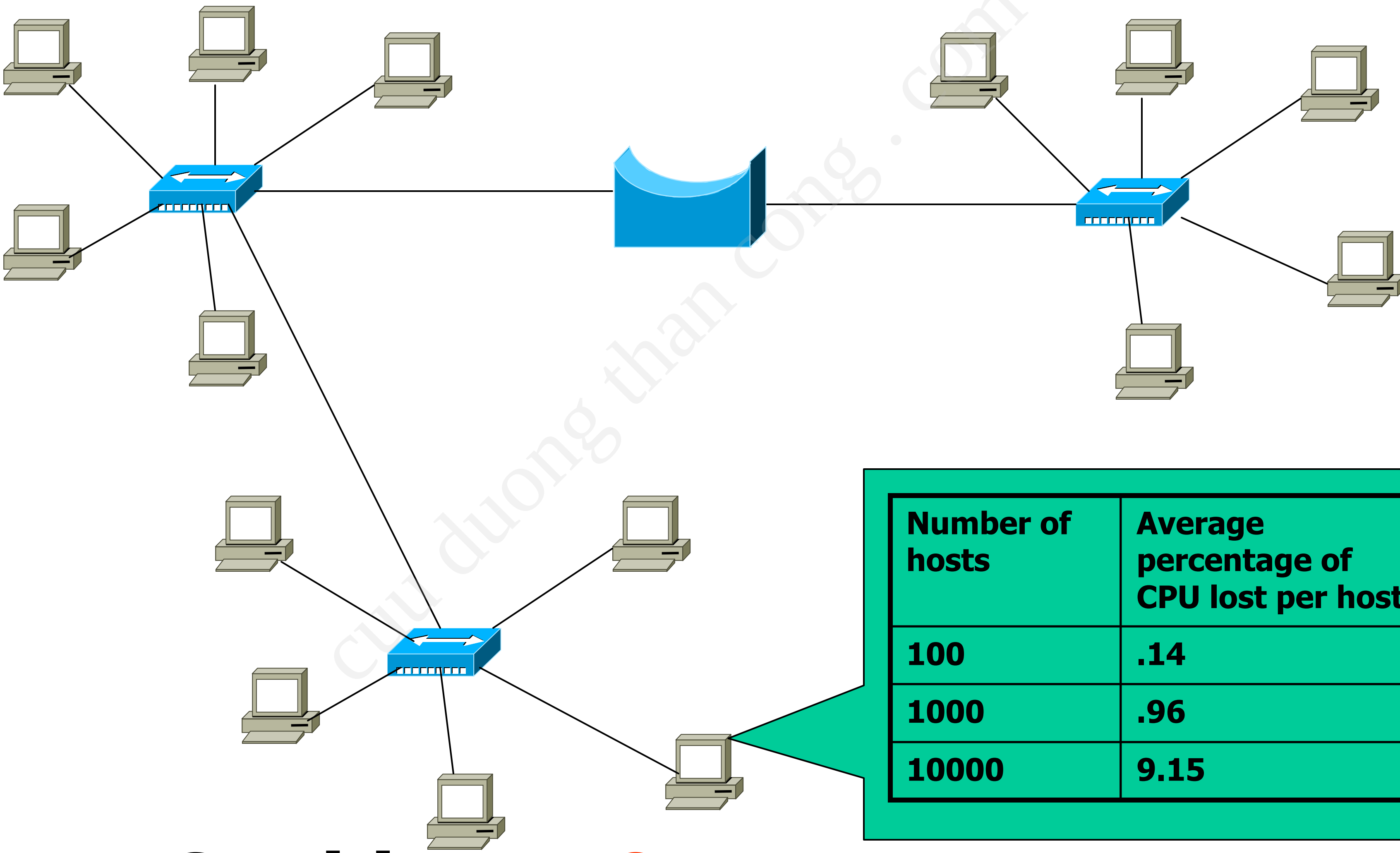
5-4-3-2-1 rule

- 5 sections of the network.
- 4 repeaters or hubs.
- 3 sections of the network are "mixing" sections (with hosts).
- 2 sections are link sections (for link purposes).
- 1 large collision domain.

Segmenting Collision Domain



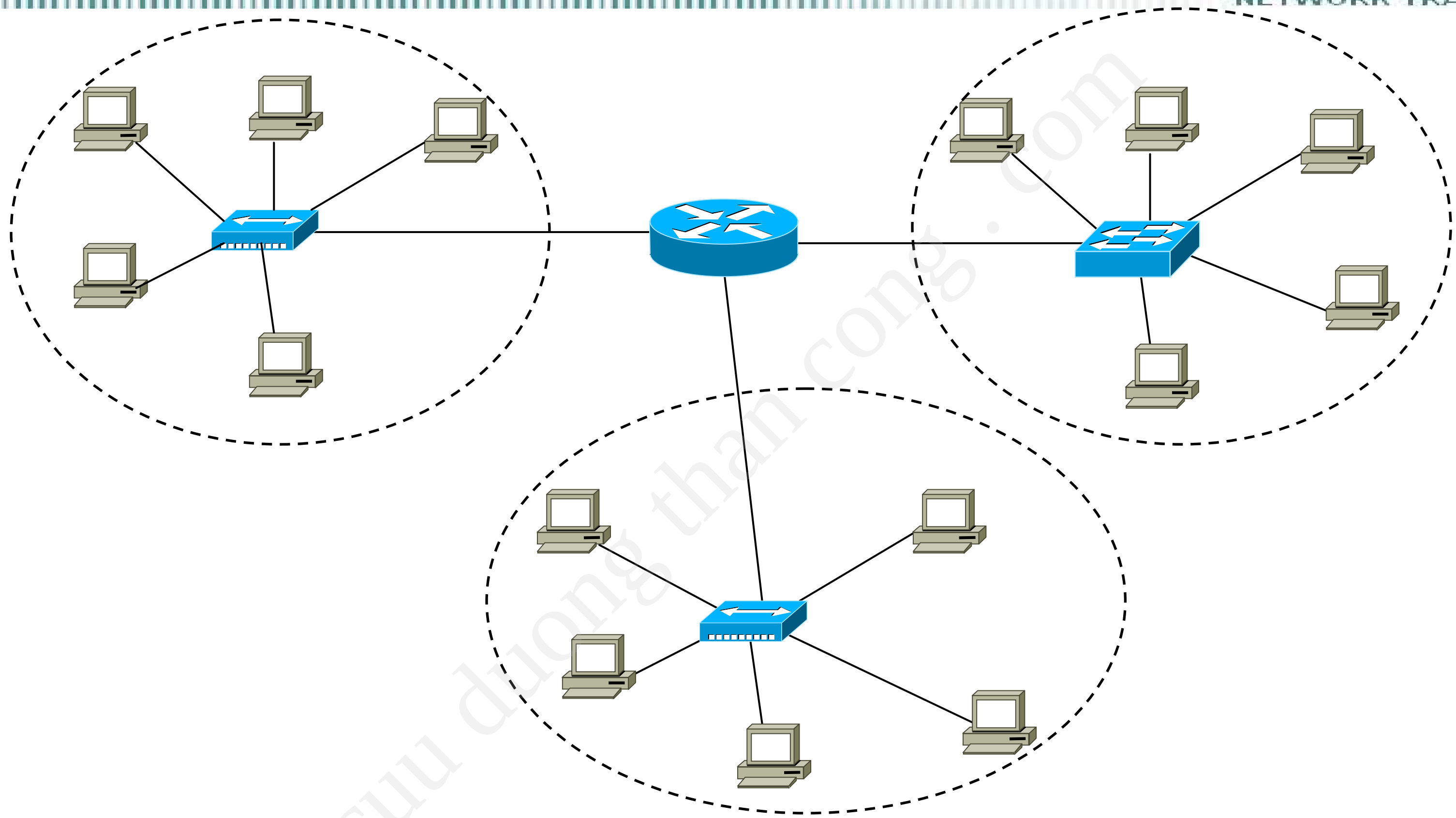
Layer 2 broadcasts



Number of hosts	Average percentage of CPU lost per host
100	.14
1000	.96
10000	9.15

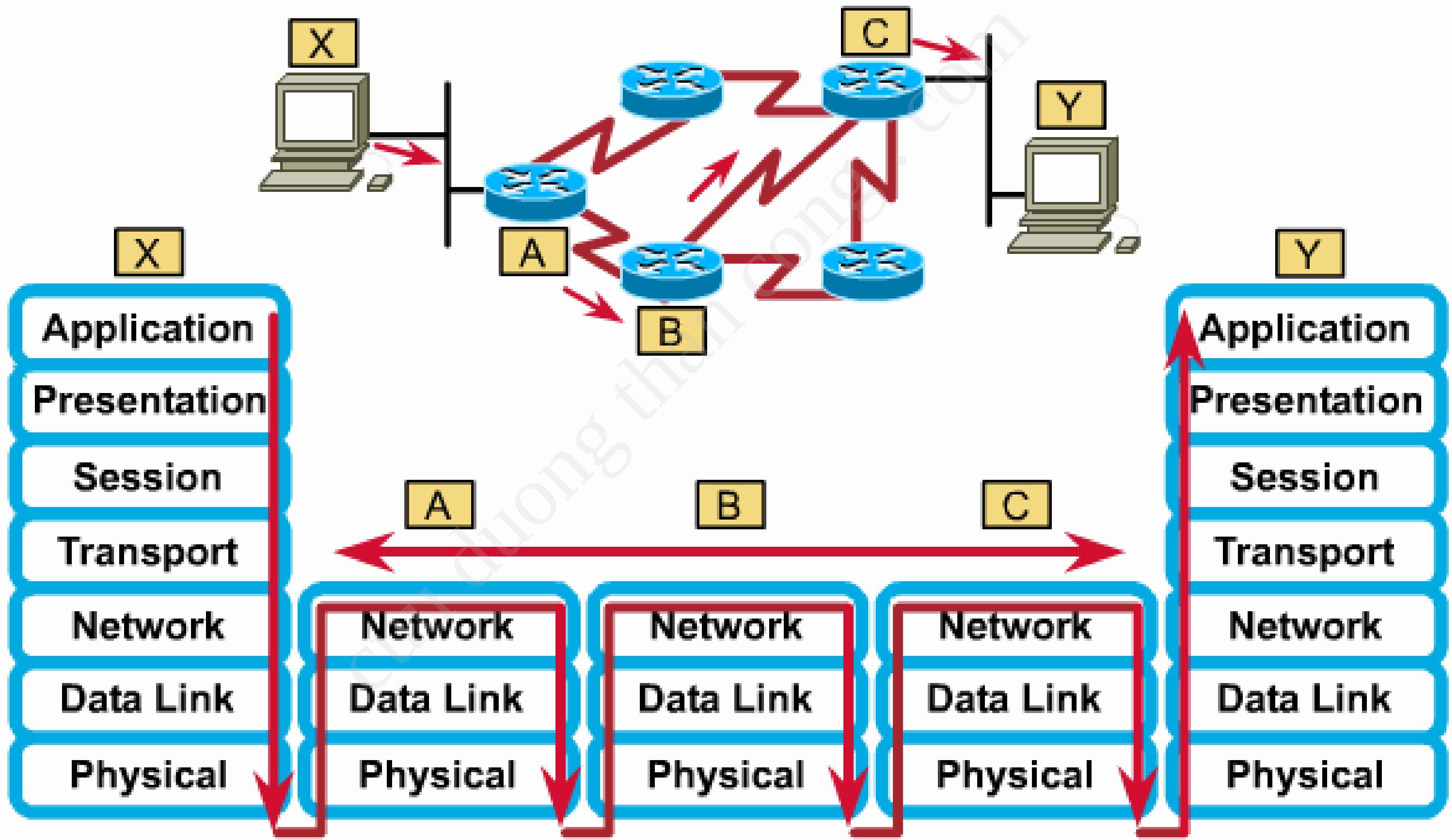
- **MAC Address: 0xFFFFFFFFFFFF**

Broadcast domains



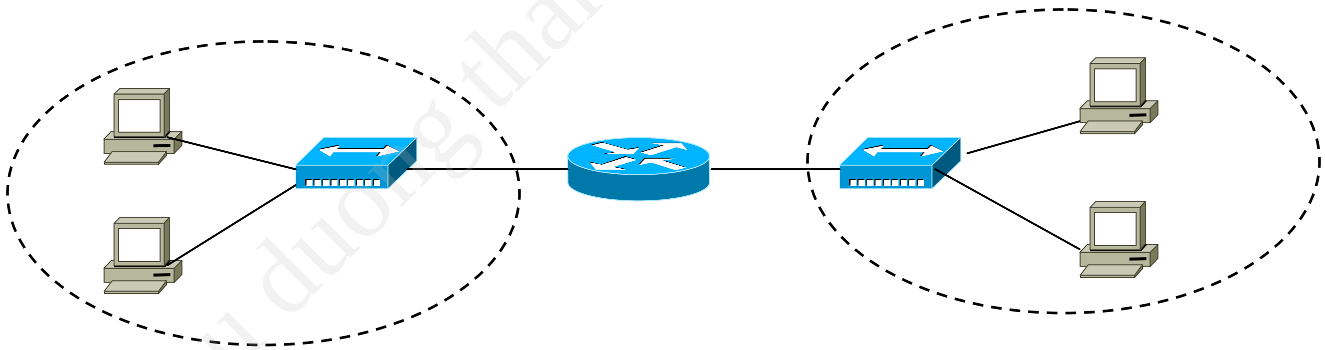
- A broadcast domain is a grouping of collision domains that are connected by Layer 2 devices
- Broadcast domains are controlled at Layer 3 because routers do not forward broadcasts.

Data flow through a Network

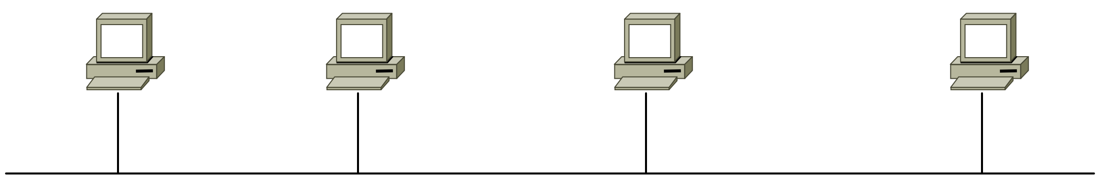


What is a network segment?

Data stream segments



Two network segments



Wire segment

Summary

- Bridging and switching evolution
- Store-and-forward and cut-through switching modes
- Spanning-Tree Protocol (STP)
- Collisions, broadcasts, collision domains, and broadcast domains
- The Layer 1, 2, and 3 devices used to create collision domains and broadcast domains
- Data flow and problems with broadcasts

Q&A

CCNA Semester 1

NETWORK TRAINING CENTER

Chapter 09

ROUTING & ADDRESSING

Objective

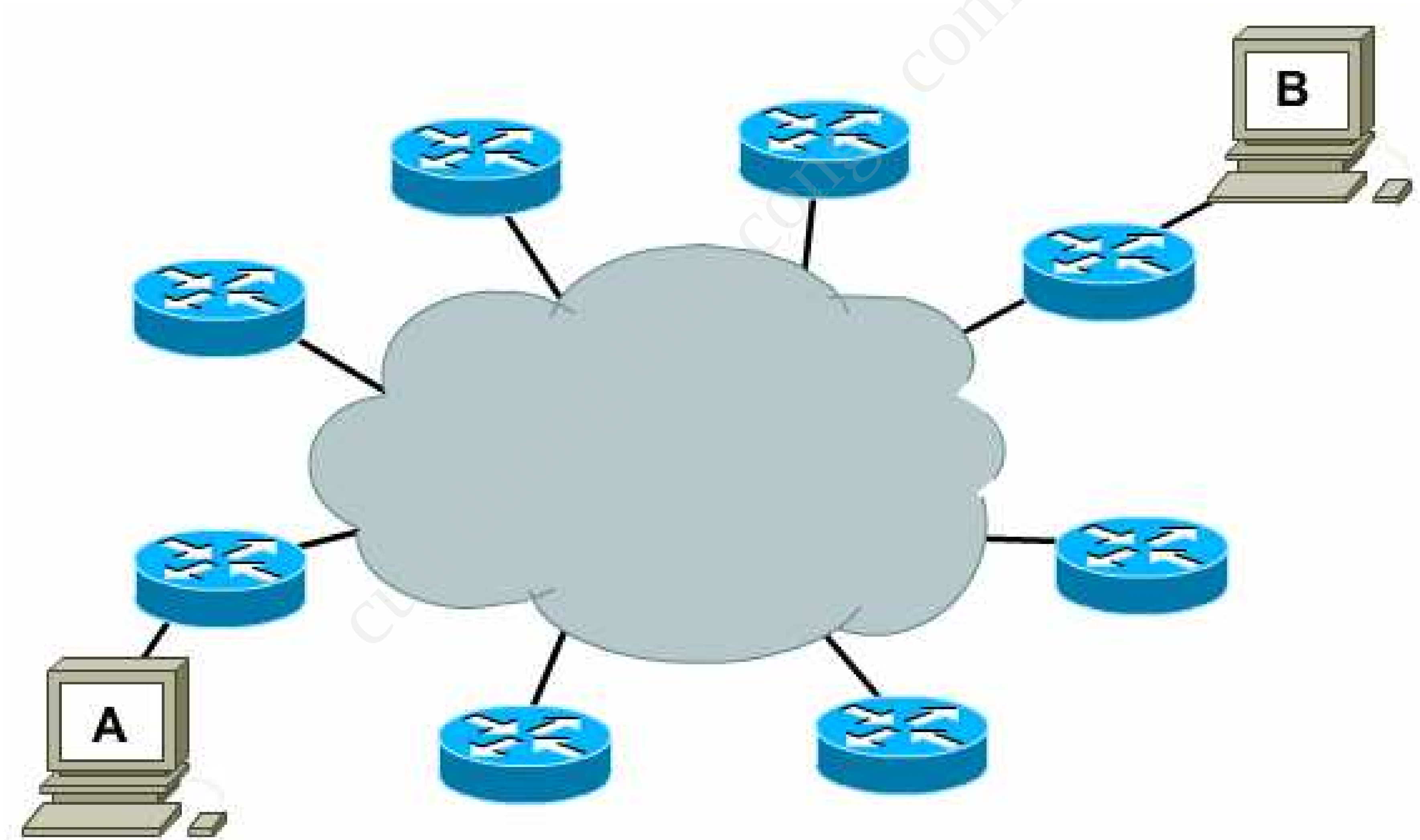
- ✓ *Learn about the router's use and operations in performing the key internetworking function of the Open System Interconnection (OSI) reference model's network layer, Layer 3.*
- ✓ *Learn about IP addressing and the three classes of networks in IP addressing schemes.*
- ✓ *Learn that some IP addresses have been set aside by the ARIN and cannot be assigned to any network.*
- ✓ *Learn about subnetworks and subnet masks and their IP addressing schemes.*

NETWORK LAYER

AND

PATH DETERMINATION

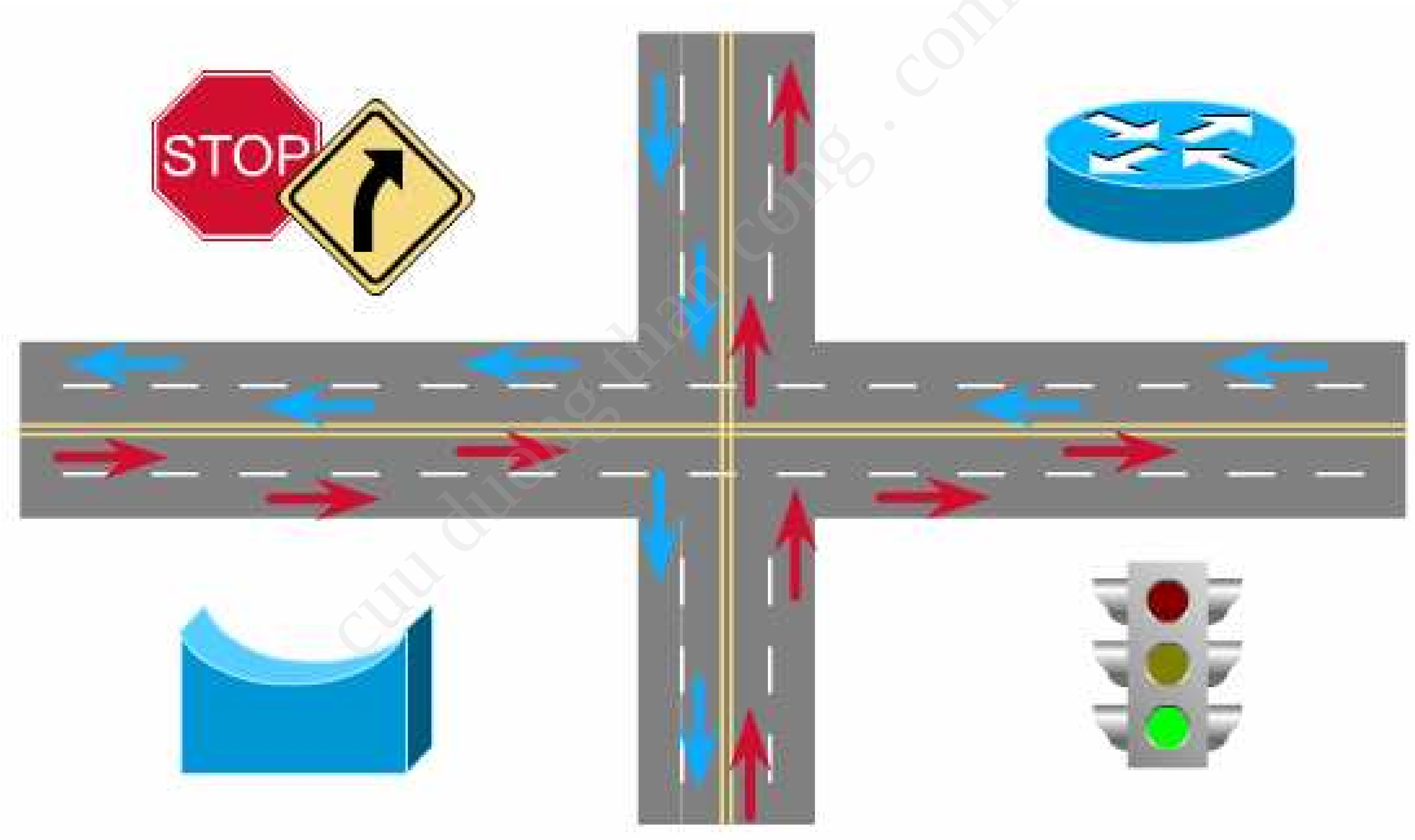
A network layer. Why?



Network layer

- Segment network and control flow of traffic.
- Move data through a set of networks.
- Logical Addressing, use a hierarchical addressing scheme.

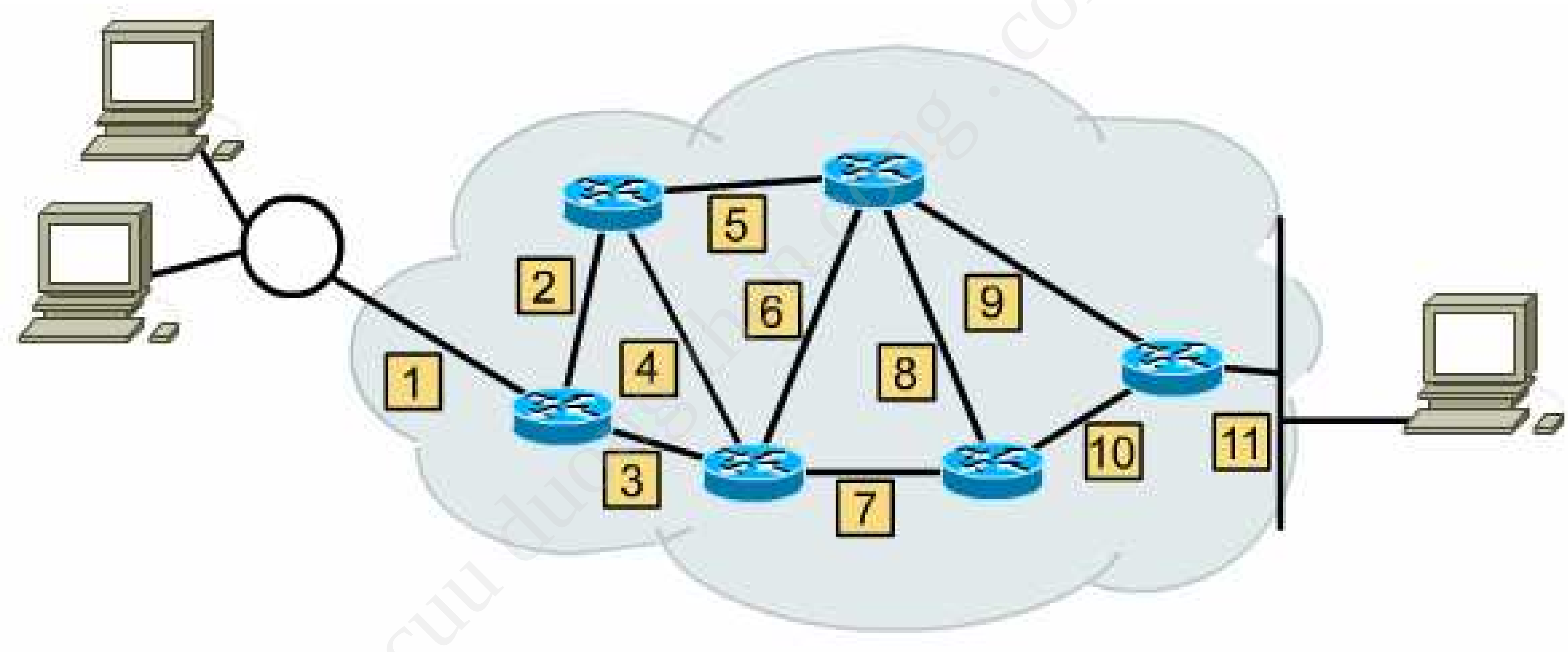
Network segmentation. Why?



Network segmentation

- Control network traffics and reduce broadcast traffics.
- Separate computer networks is managed by a single administration - Autonomous systems.

Communication among networks

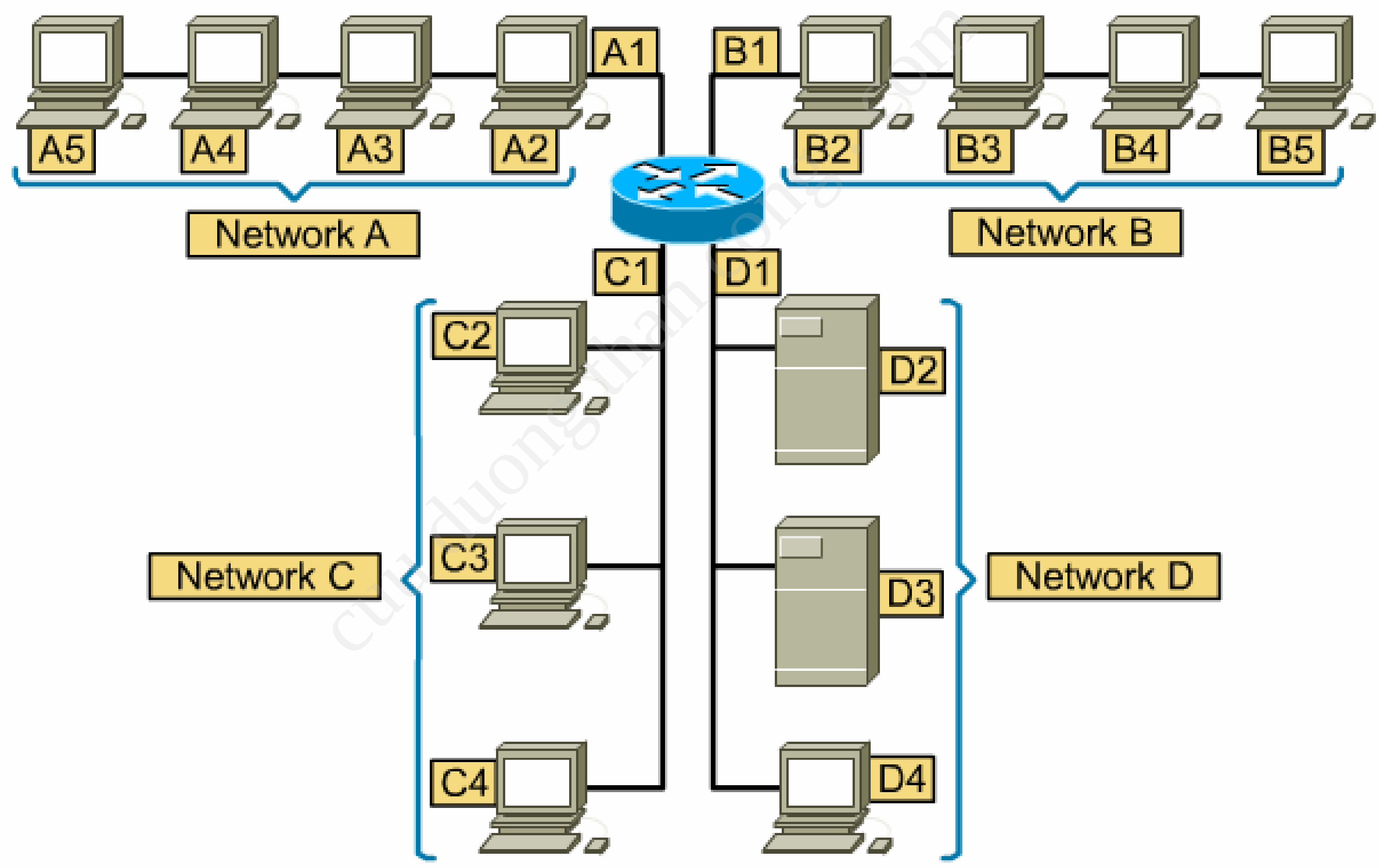


- Networks operate in much the same manner.

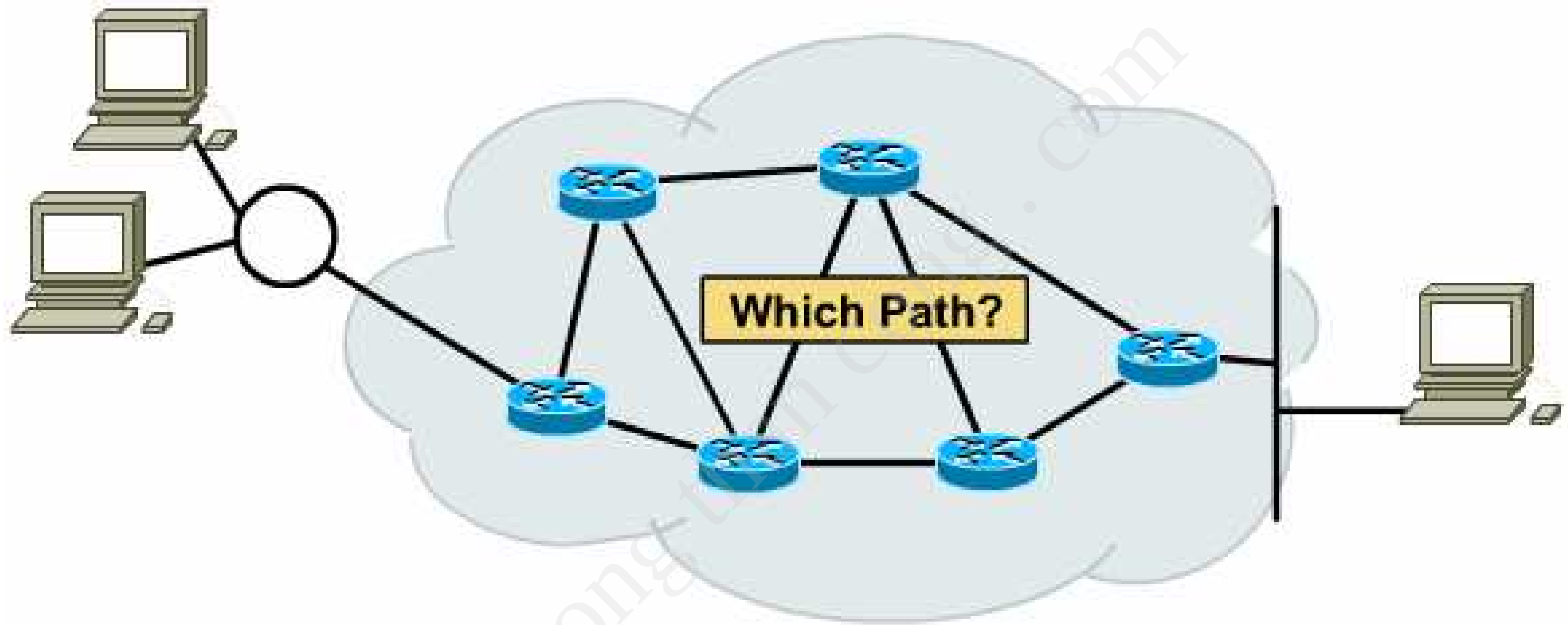
Router

- Routers connect separate networks.
- Routers make best path decisions based on Layer 3 information.
- Routers actually switch packets from incoming ports to appropriate outgoing ports.

Data relaying



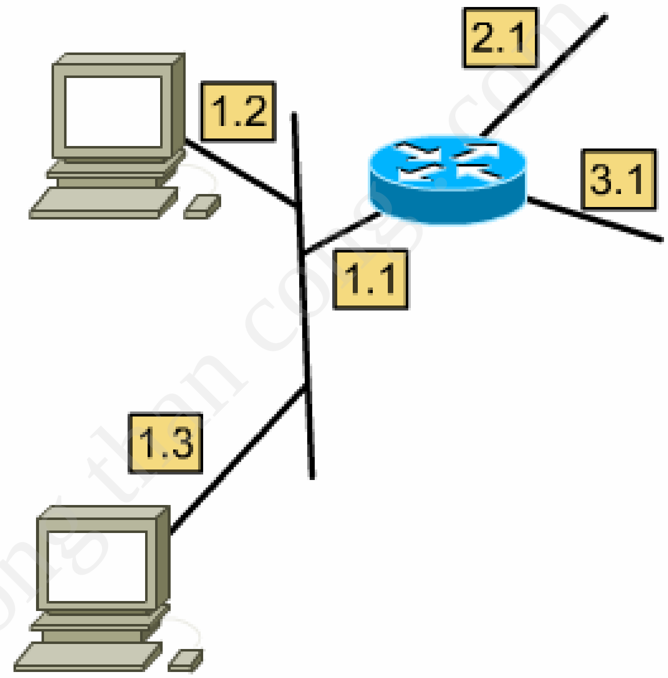
Path determination



- 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 ...

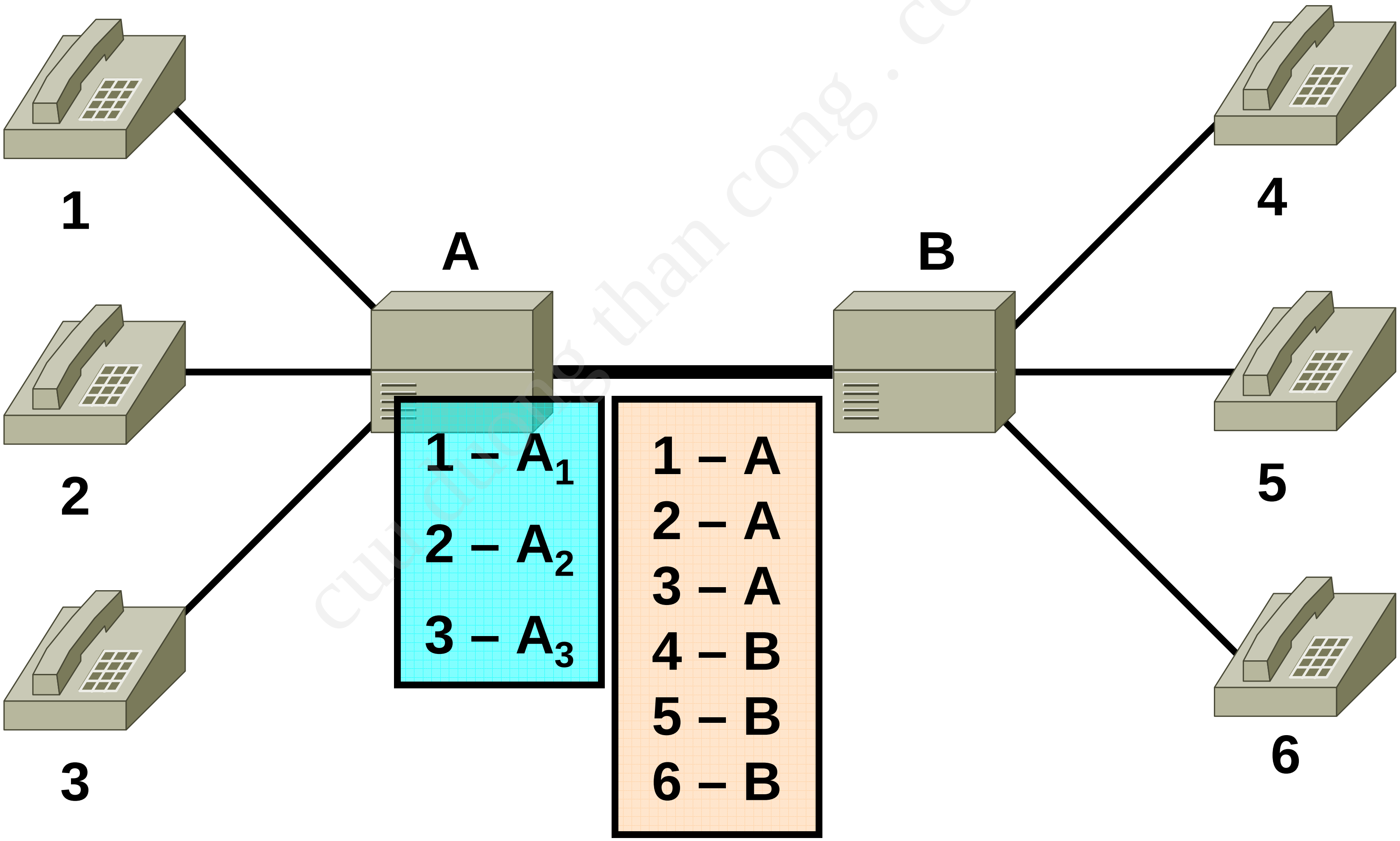
Network layer addressing

Network	Host
1	1
	2
	3
2	1
3	1



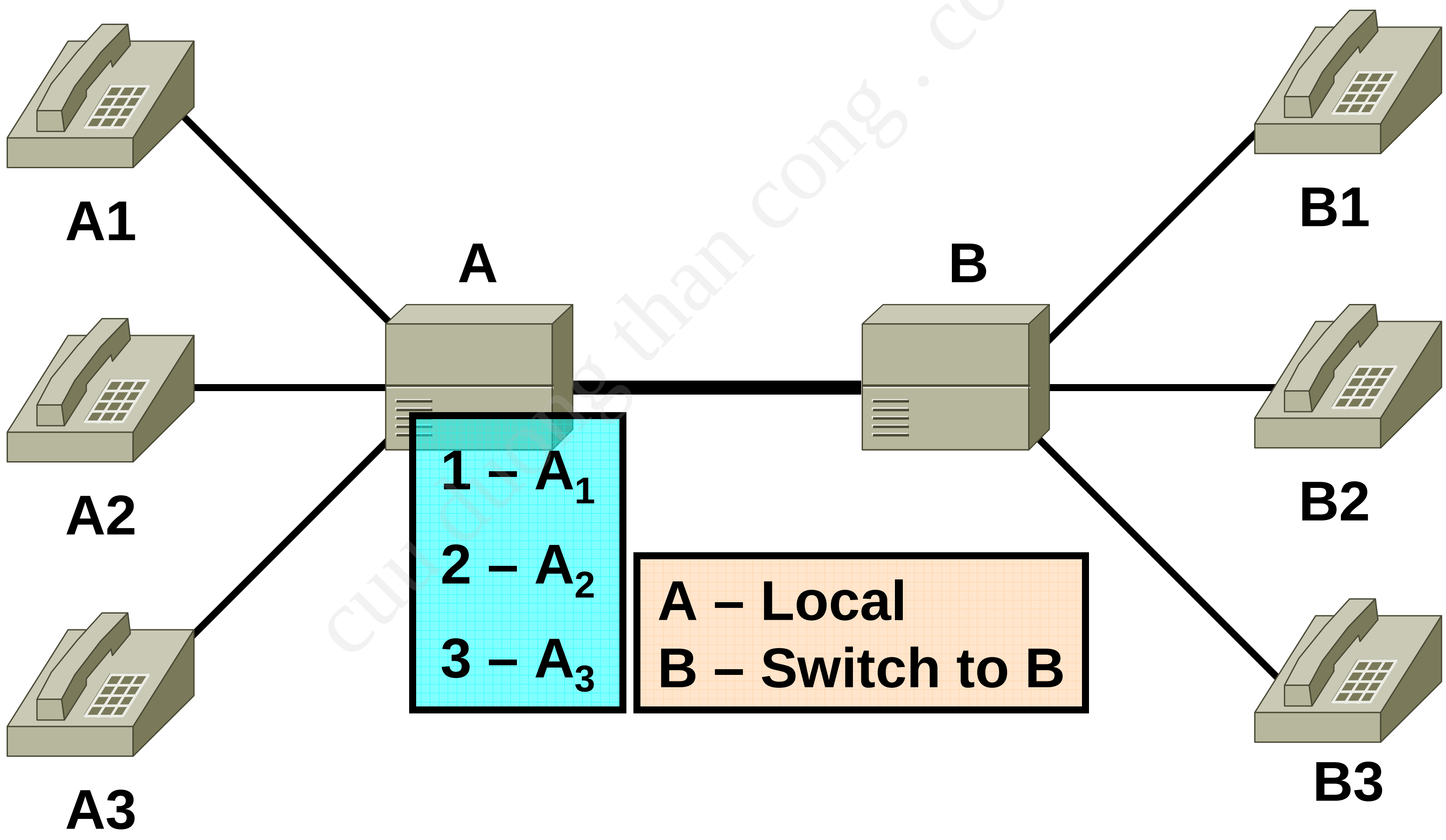
- Network address + Host address: Hierarchical Addressing Schemes.

Flat Addressing Scheme

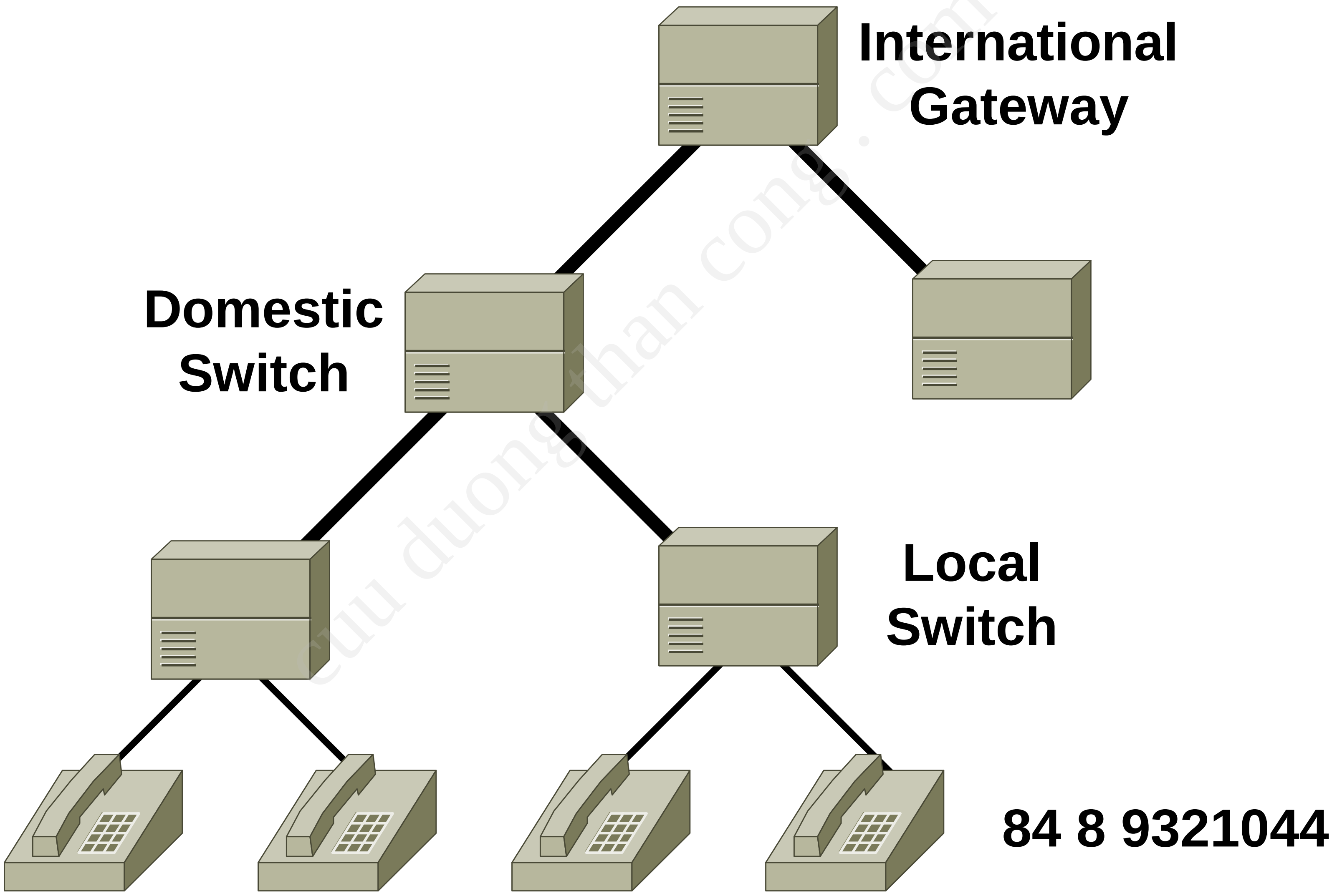


Hierarchical Addressing Scheme

NETWORK TRAINING CENTER

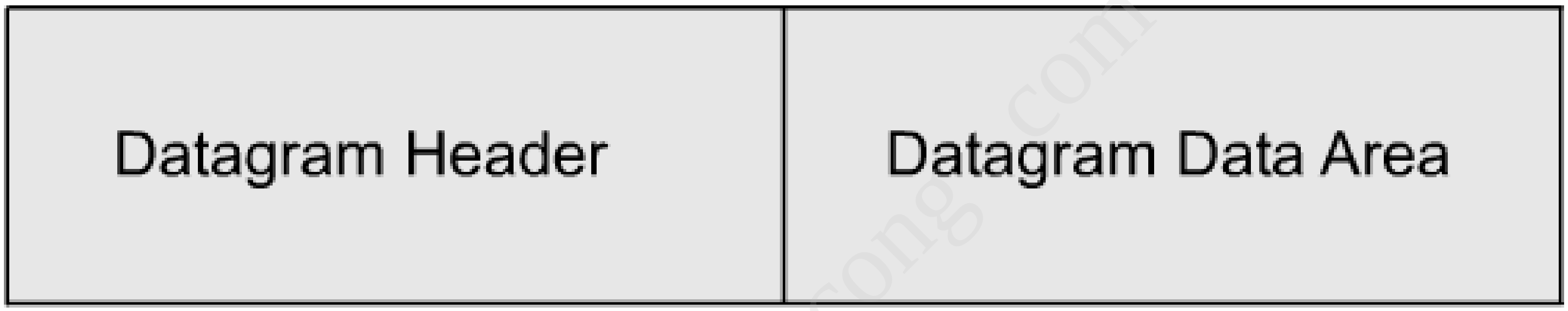


Hierarchical Addressing Scheme



IP ADDRESS WITHIN THE IP HEADER

Network layer datagram



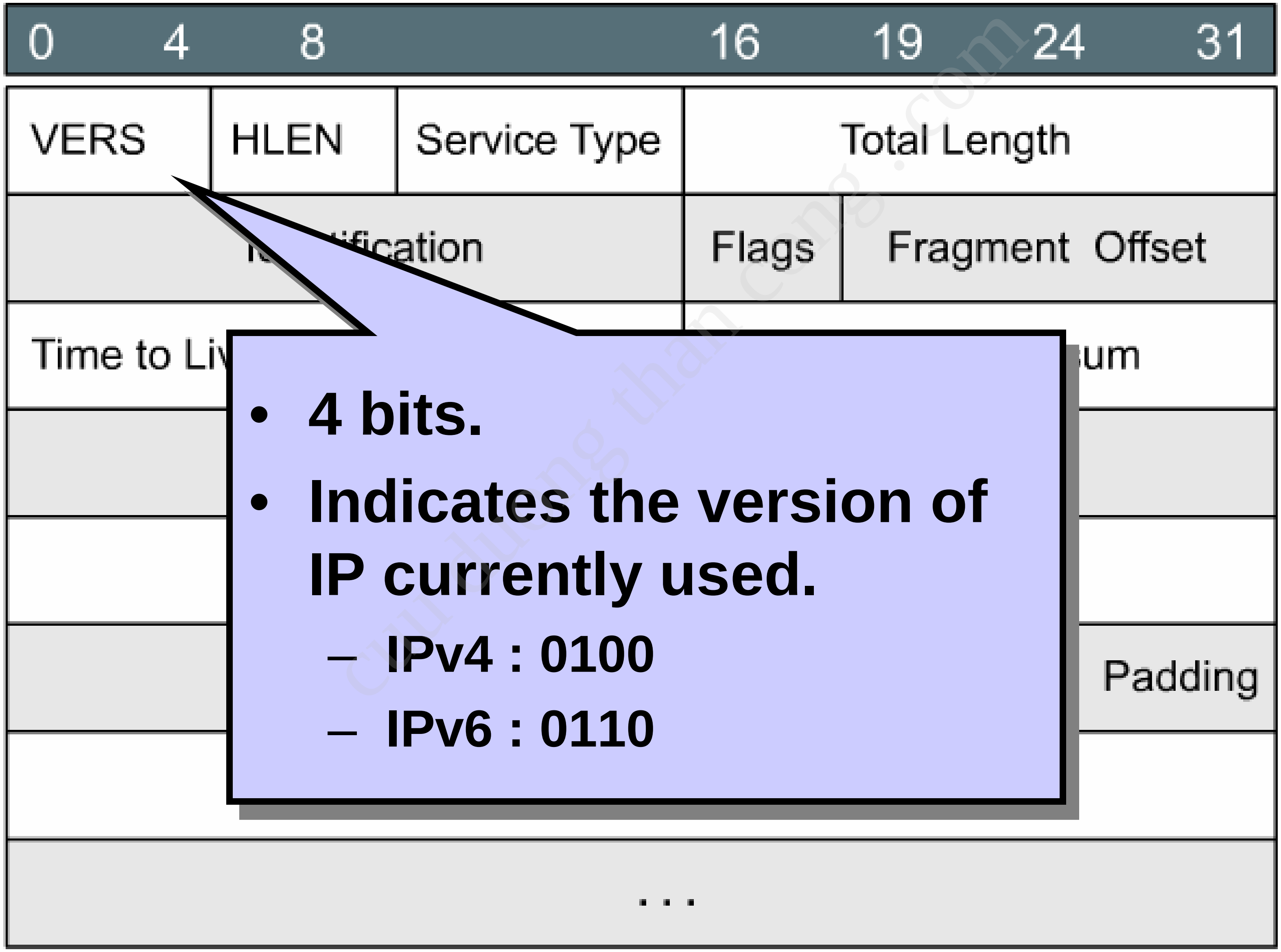
- At the network layer, the data is encapsulated within packets (also known as datagrams).
- Packet includes header - addressing and other control information - and actual data - whatever is passed down from the higher layers.

IP header format

<table>
<tr><th>0</th><th>4</th><th>8</th><th>16</th><th>19</th><th>24</th><th>31</th></tr>
<tr><td>VERS</td><td>HLEN</td><td>Service Type</td><td colspan="4">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td colspan="3">Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="4">Header Checksum</td></tr>
<tr><td colspan="7">Source IP Address</td></tr>
<tr><td colspan="7">Destination IP Address</td></tr>
<tr><td colspan="6">IP Options (If Any)</td><td>Padding</td></tr>
<tr><td colspan="7">Data</td></tr>
<tr><td colspan="7">. . .</td></tr>
</table>

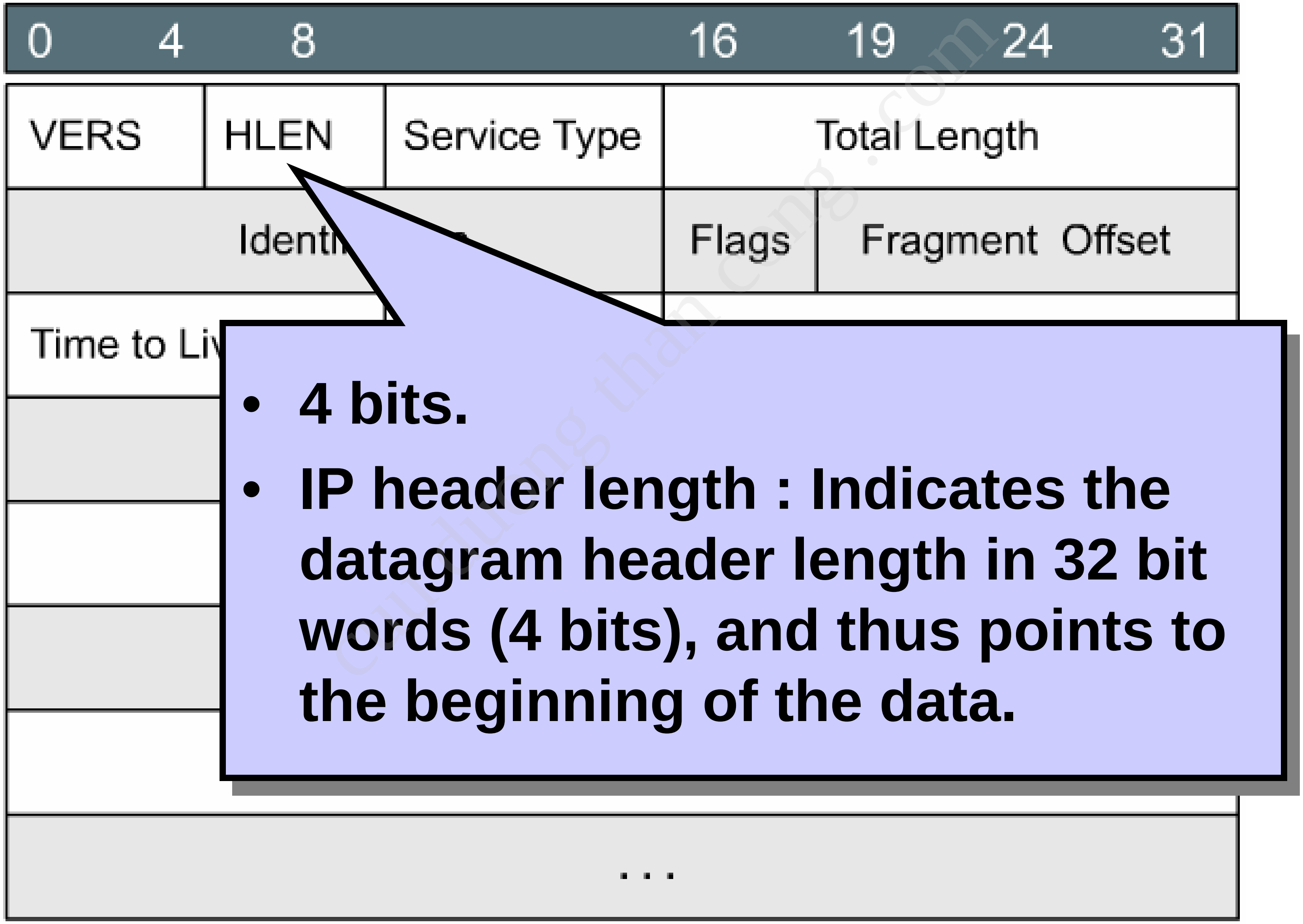
IP header format: Version

NETWORK TRAINING CENTER



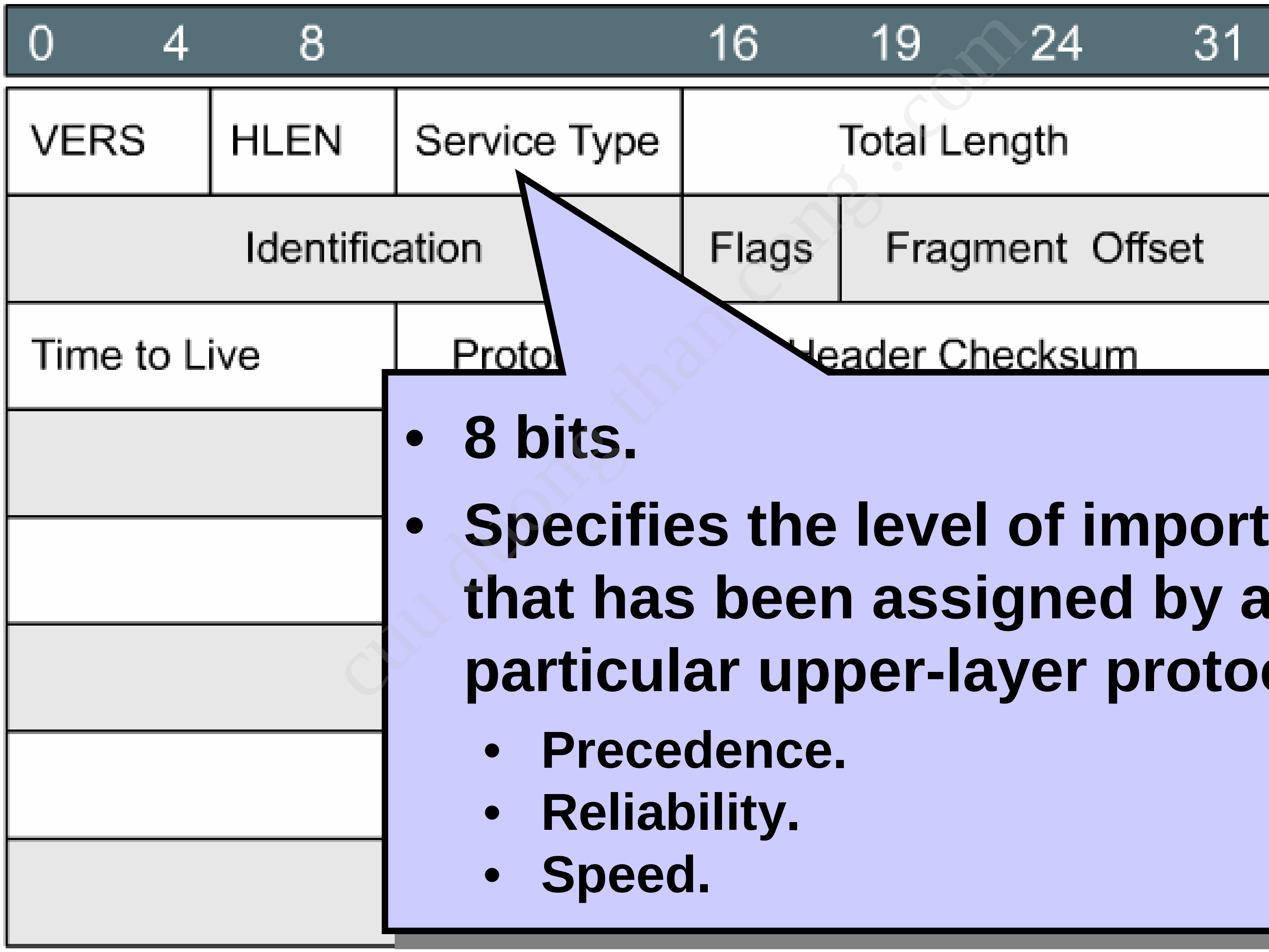
- **4 bits.**
- **Indicates the version of IP currently used.**
  - **IPv4 : 0100**
  - **IPv6 : 0110**

IP header format: Header length



- **4 bits.**
- **IP header length : Indicates the datagram header length in 32 bit words (4 bits), and thus points to the beginning of the data.**

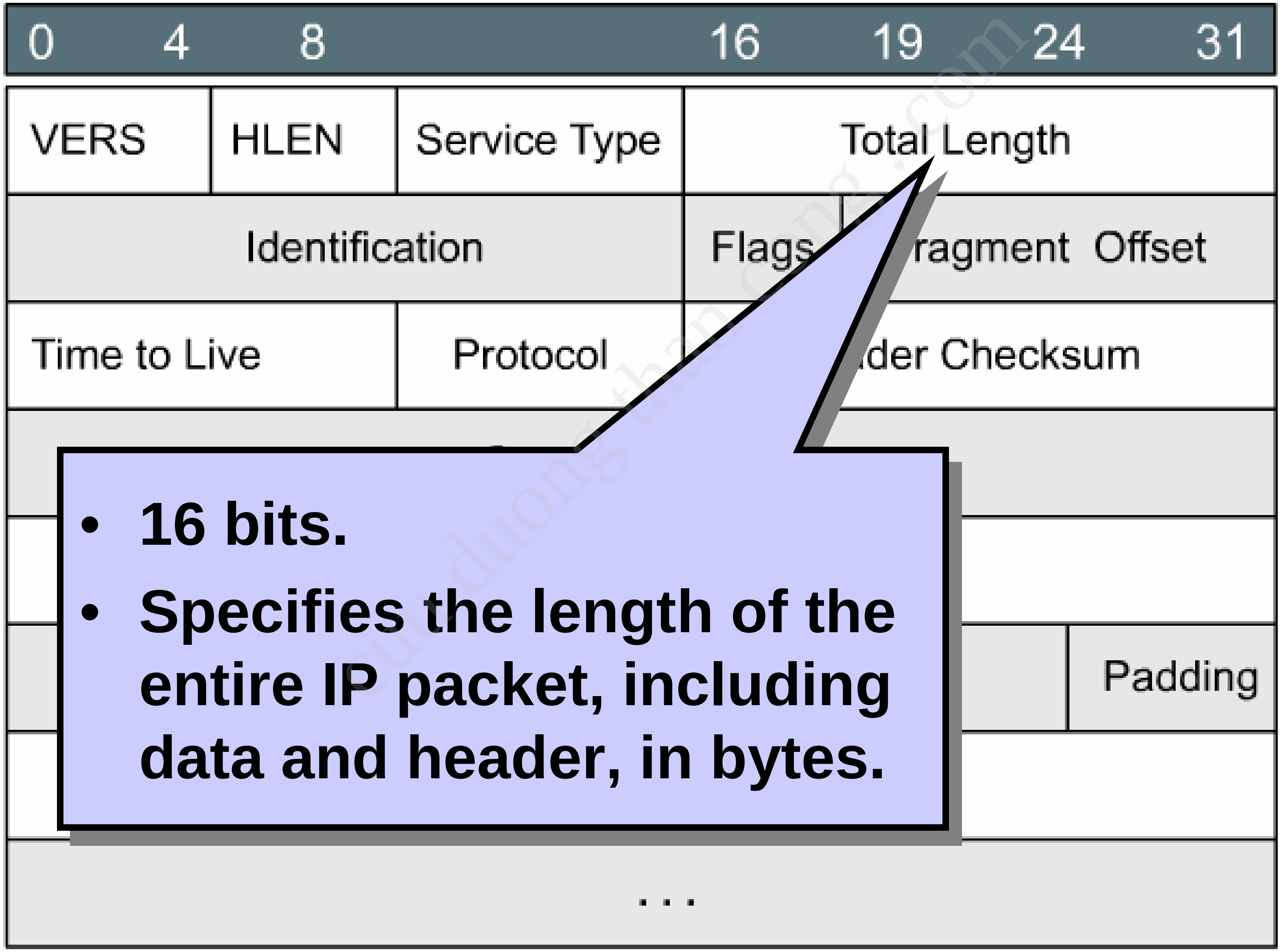
IP header format: Service type



- **8 bits.**
- **Specifies the level of importance that has been assigned by a particular upper-layer protocol.**
  - **Precedence.**
  - **Reliability.**
  - **Speed.**

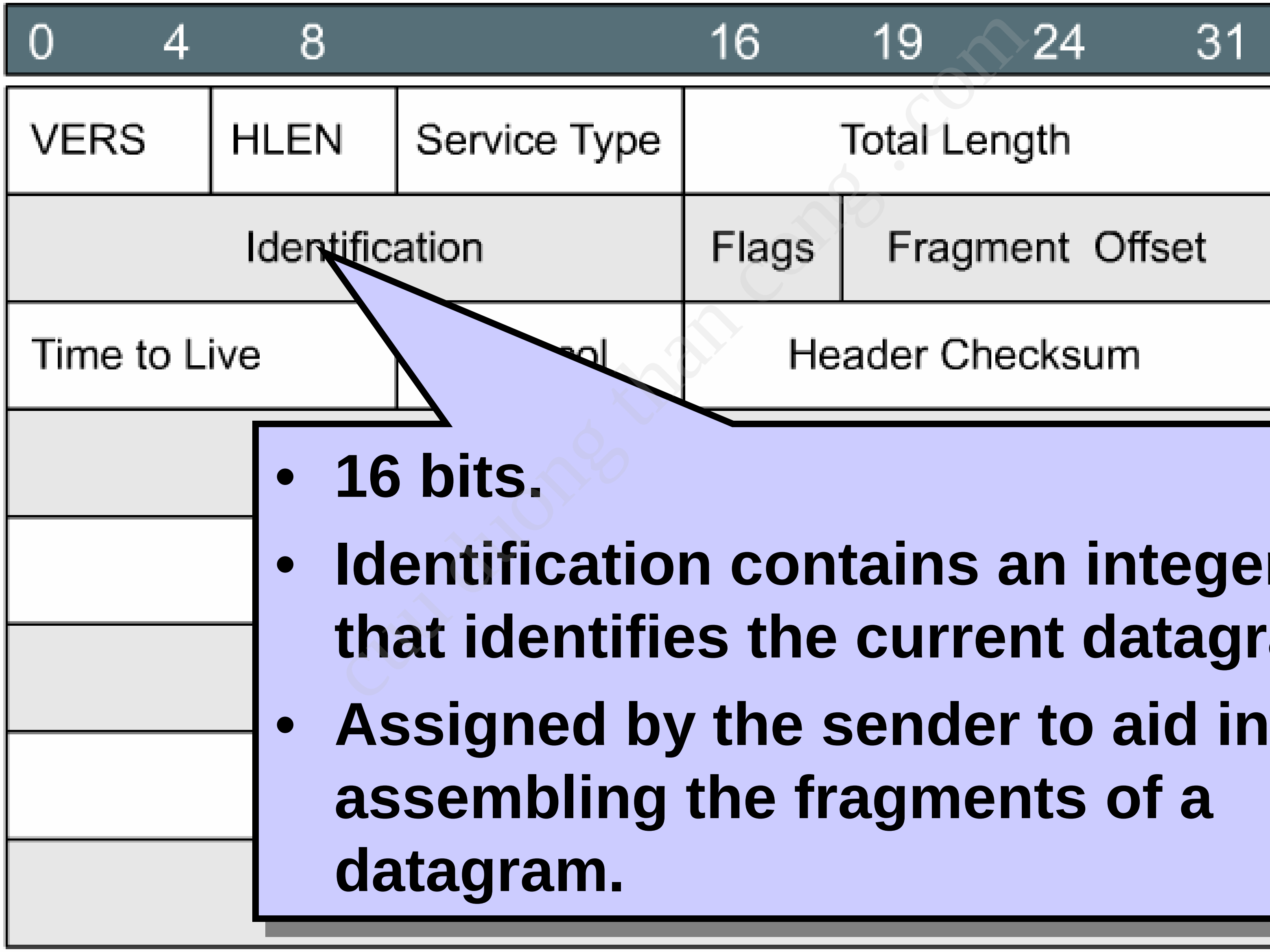
IP header format: Total length

NETWORK TRAINING CENTER



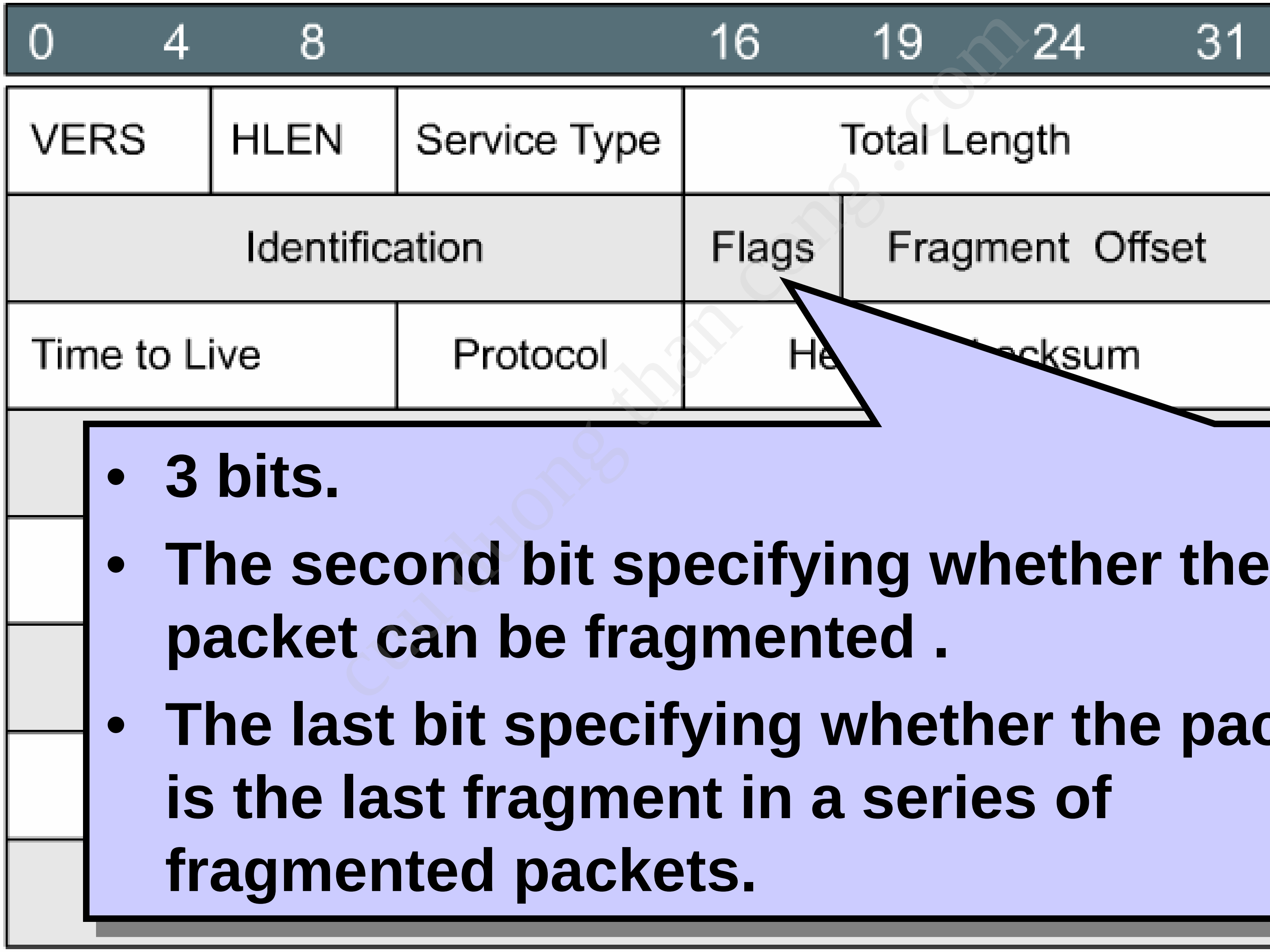
- **16 bits.**
- **Specifies the length of the entire IP packet, including data and header, in bytes.**

IP header format: Identification



- **16 bits.**
- **Identification contains an integer that identifies the current datagram.**
- **Assigned by the sender to aid in assembling the fragments of a datagram.**

IP header format: Flags



- **3 bits.**
- **The second bit specifying whether the packet can be fragmented .**
- **The last bit specifying whether the packet is the last fragment in a series of fragmented packets.**

IP header format: Fragment offset

0	4	8	16	19	24	31
VERS	HLEN	Service Type	Total Length			
Identification			Flags	Fragment Offset		
Time to Live		Protocol	Heade			

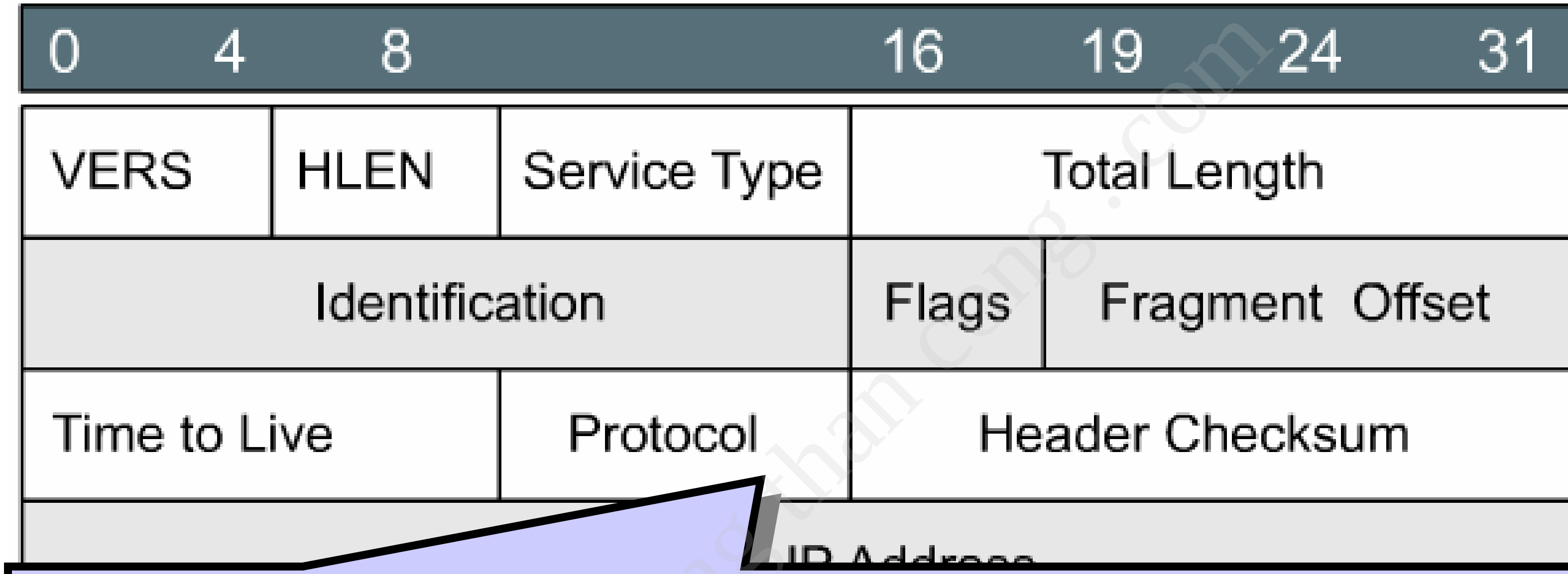
- 13 bits.
- The field that is used to help piece together datagram fragments.
- The fragment offset is measured in units of 8 octets (64 bits).
- The first fragment has offset zero.

IP header format: Time to Live

0 4	8	16 19	24 31
VERS / HLEN	Service Type	Total Length	
Identification		Flags	Fragment Offset
Time to Live	Protocol	Header Checksum	
Source IP Address			

- **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**
  - **17 : UDP**

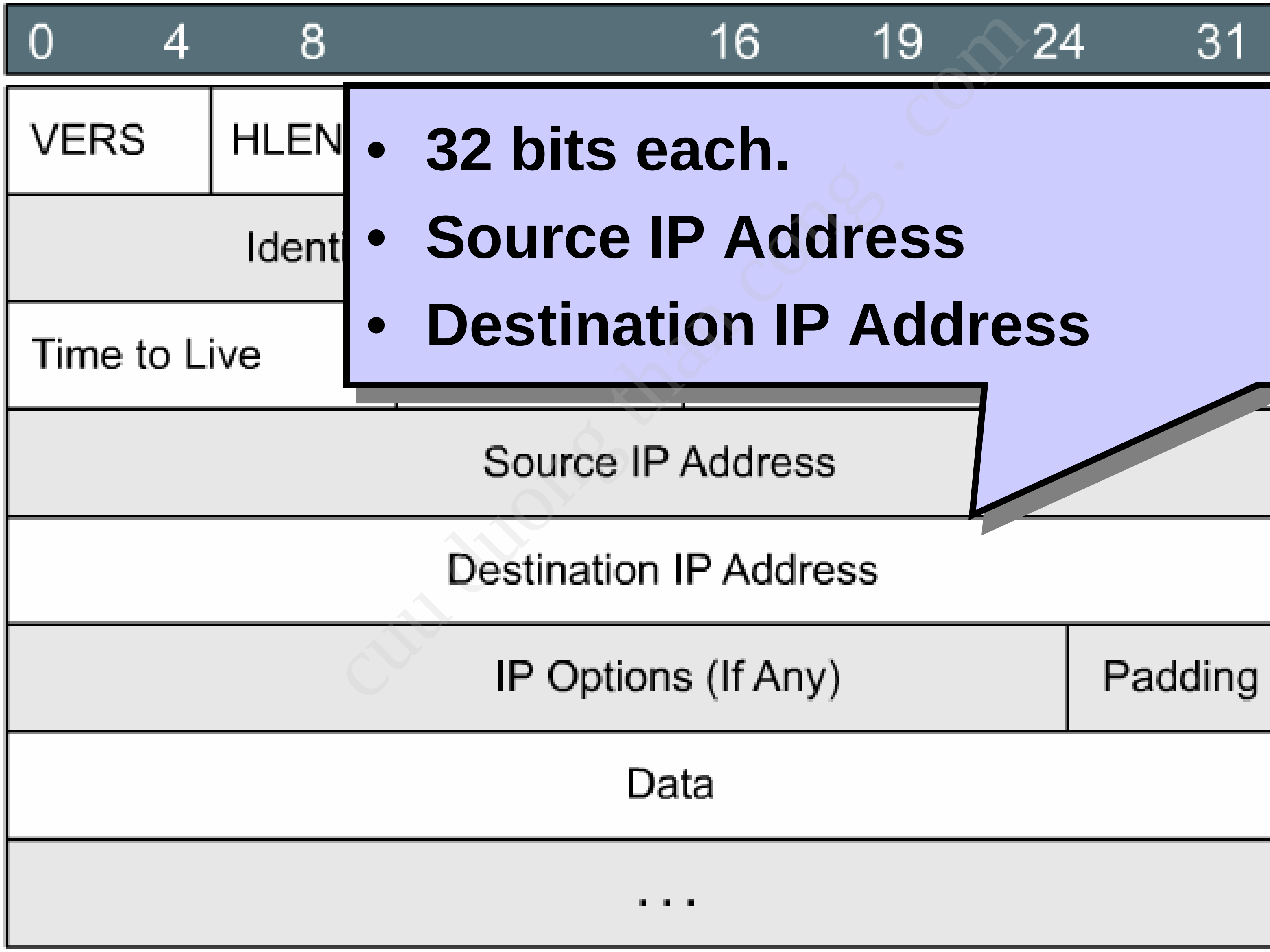
IP header format: Header checksum

0	4	8	16	19	24	31
VERS	HLEN	Service Type	Total Length			
Identification			Flags	Fragment Offset		
Time to Live		Protocol	Header Checksum			
Source IP Address						
Destination IP Address						
. . .						

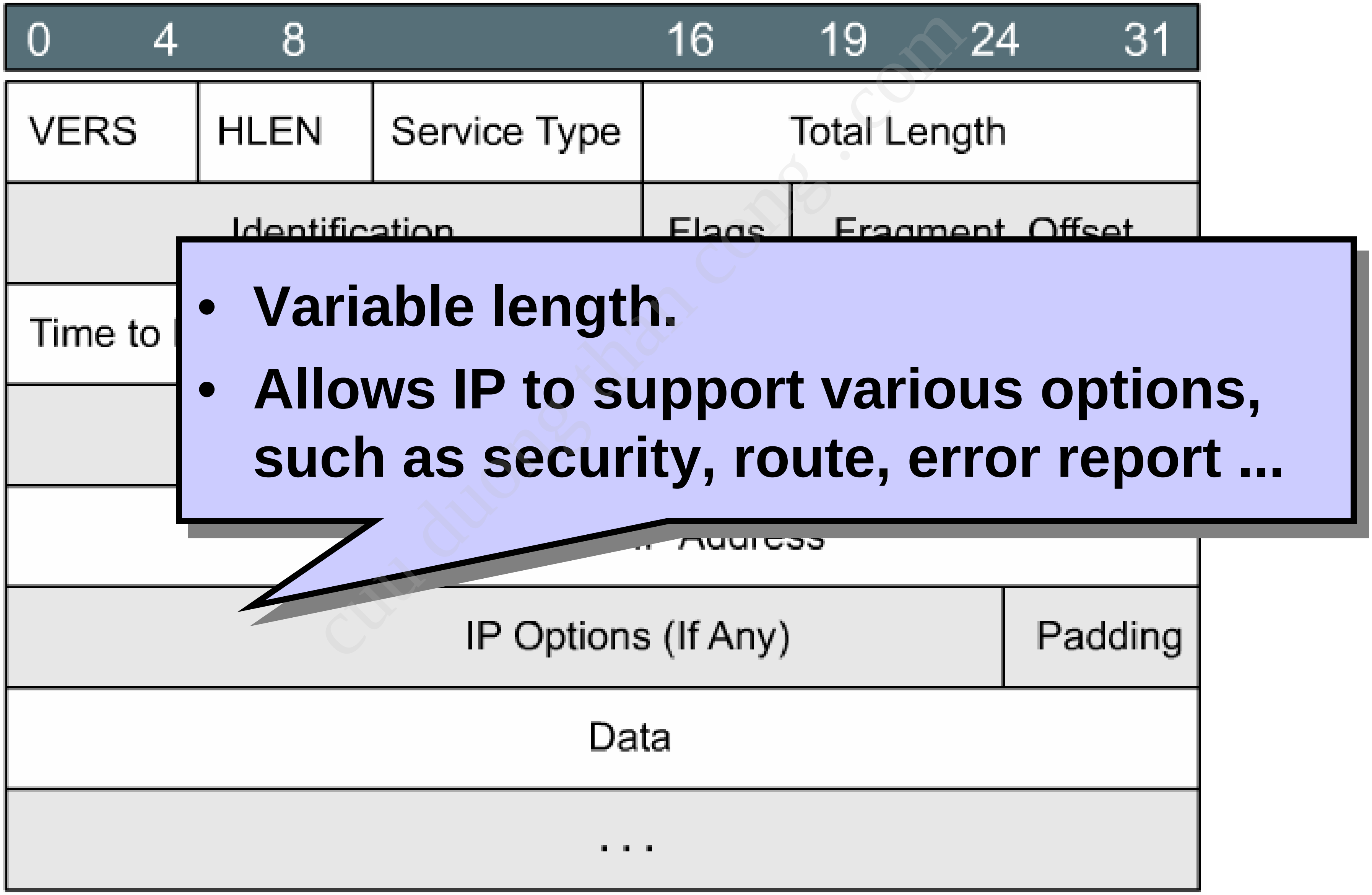
- **16 bits.**
- **A checksum on the header only, helps ensure IP header integrity.**

IP header format: Addresses

- 32 bits each.
- Source IP Address
- Destination IP Address

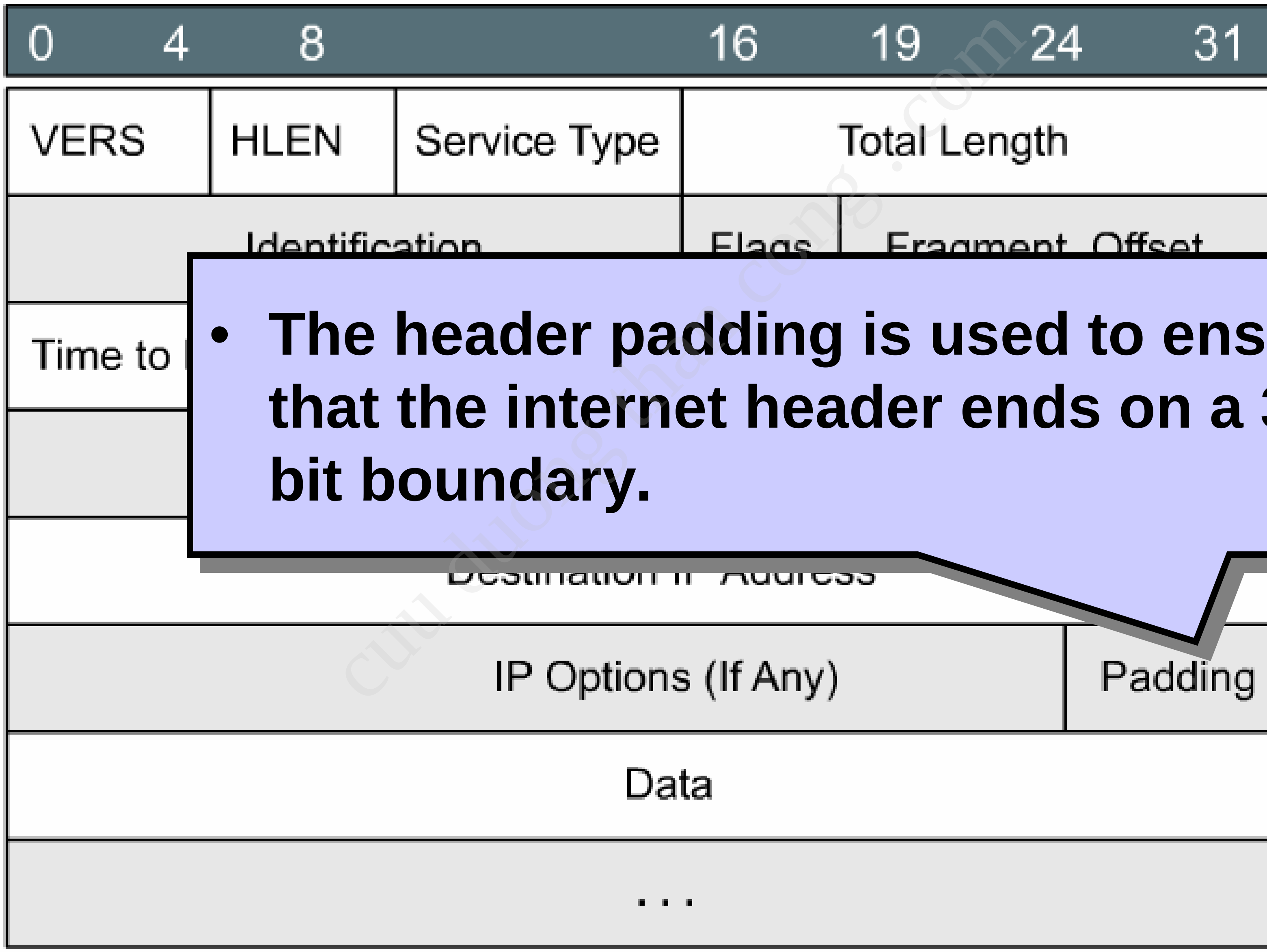


IP header format: Options



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

IP header format: Padding



- **The header padding is used to ensure that the internet header ends on a 32 bit boundary.**

Homework

- www.ietf.org and RFC-760.
- Groups presentations:
  - Internet Protocol Overview.
  - Packet fragment fields.
  - Type of services field.
  - Option field.

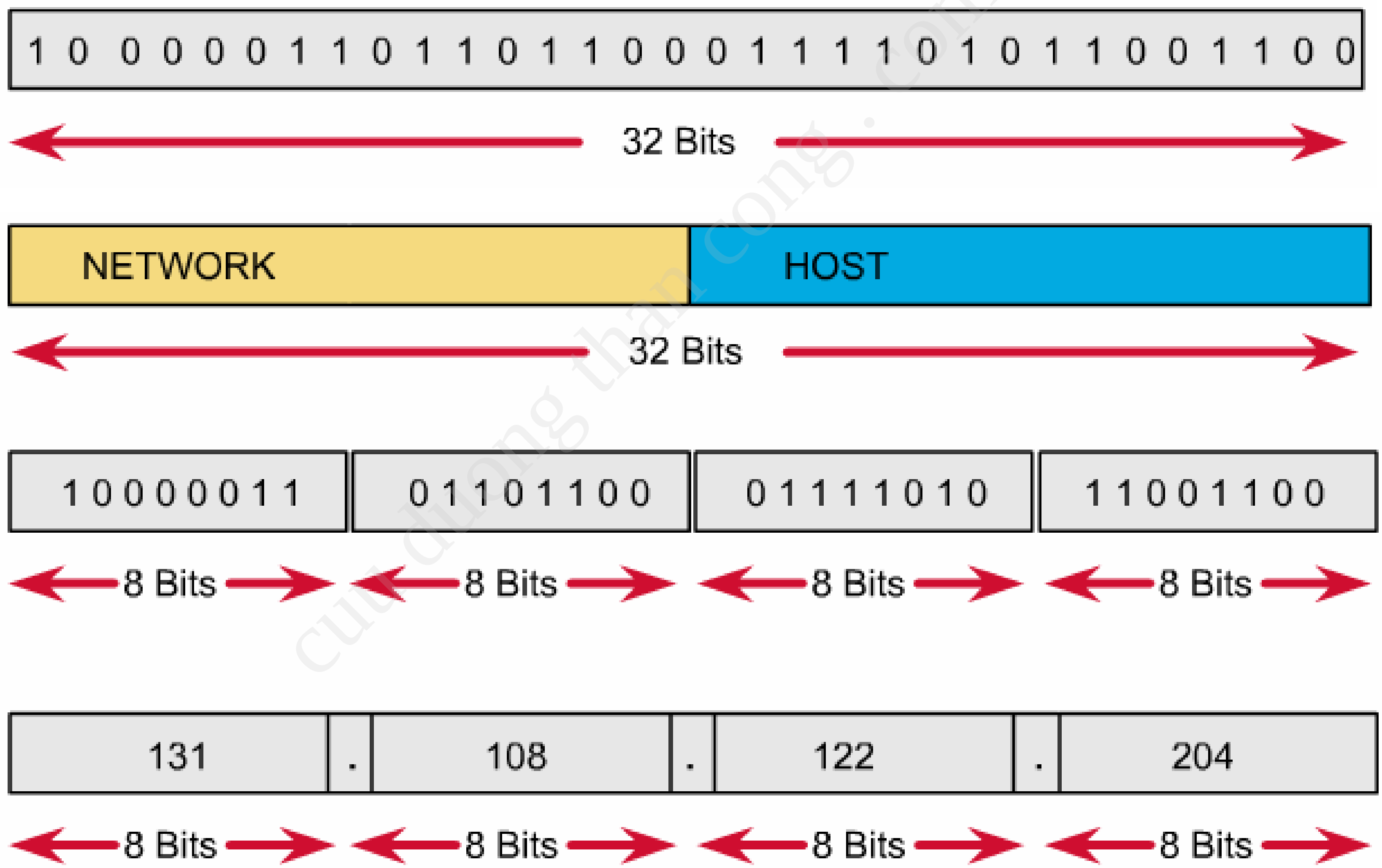
IP ADDRESS CLASSES

IP network address

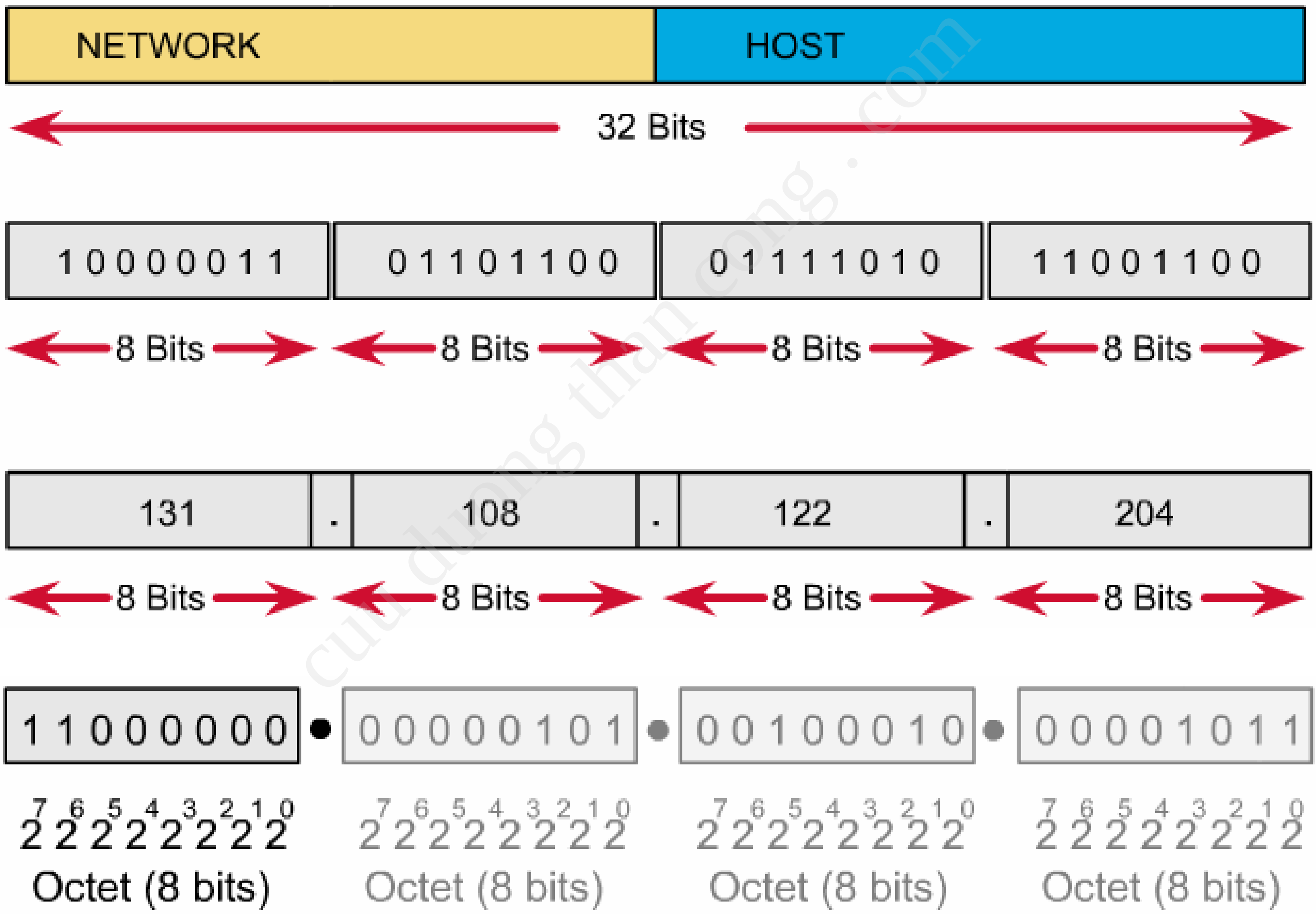
NETWORK TRAINING CENTER

- Network layer addresses are 32 bits long.
- The are presented as four octets in dotted decimal format.
- The IP address has two components: Network ID and Host ID.

IP address format



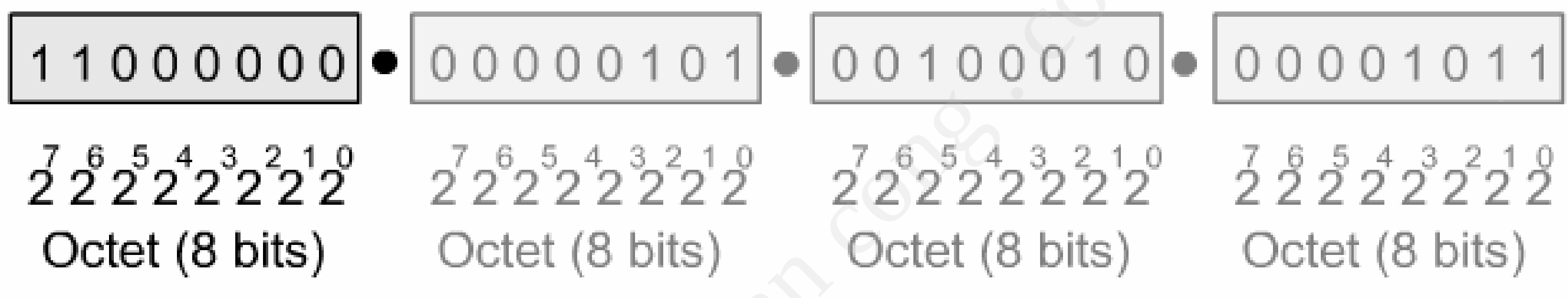
Binary and decimal conversion



Why we need to know B-D conversion

- Use of calculators is discouraged for two reasons :
  - First, practitioners of networking often need to make quick.
  - Second, no calculators are allowed on the CCNA exam.

Fast conversion



$2^{(7)}$	$2^{(6)}$	$2^{(5)}$	$2^{(4)}$	$2^{(3)}$	$2^{(2)}$	$2^{(1)}$	$2^{(0)}$
128	64	32	16	8	4	2	1

Exercise: DEC – BIN

203

↓

11001011

Exercise: BIN – DEC

10100010

↓

162

Network ID and host ID

NETWORK TRAINING CENTER

- Network ID :
  - Assigned by Internet Network Information Center.
  - Assigned by upper organization.
  - Identifies the network to which a devices is attached.
- Host ID :
  - Assigned by a network administrator.
  - Identifies the specific device on that network.

Bits on the IP address

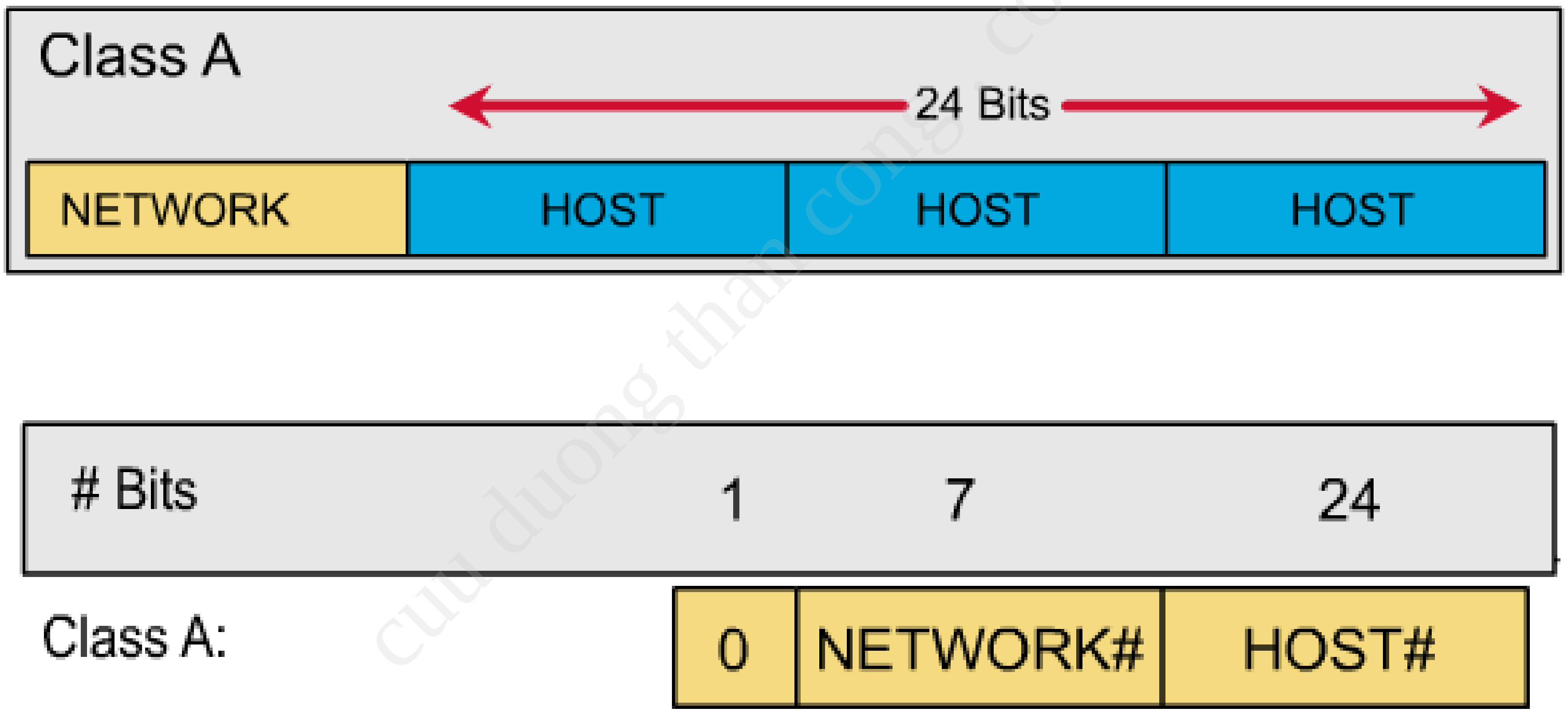
- Network Bits :
  - Identifies network ID
  - Identifies class of the IP address
  - All of bits are 0: not allowed
- Host Bits :
  - Identifies host ID
  - All of bits are 0: reserved for network address
  - All of bits are 1: reserved for broadcast address

IP address classes

	1 Byte 8 Bits	1 Byte 8 Bits	1 Byte 8 Bits	1 Byte 8 Bits
Class A:	N	H	H	H
Class B:	N	N	H	H
Class C:	N	N	N	H

- Different class addresses reserve different amounts of bits for the Network and Host portions of the address
- Provide the flexibility required to support different size networks

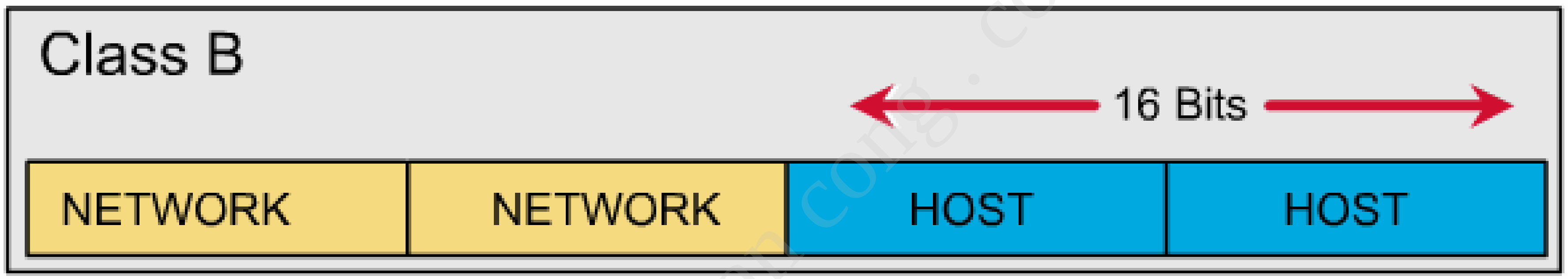
IP address classes: Class A

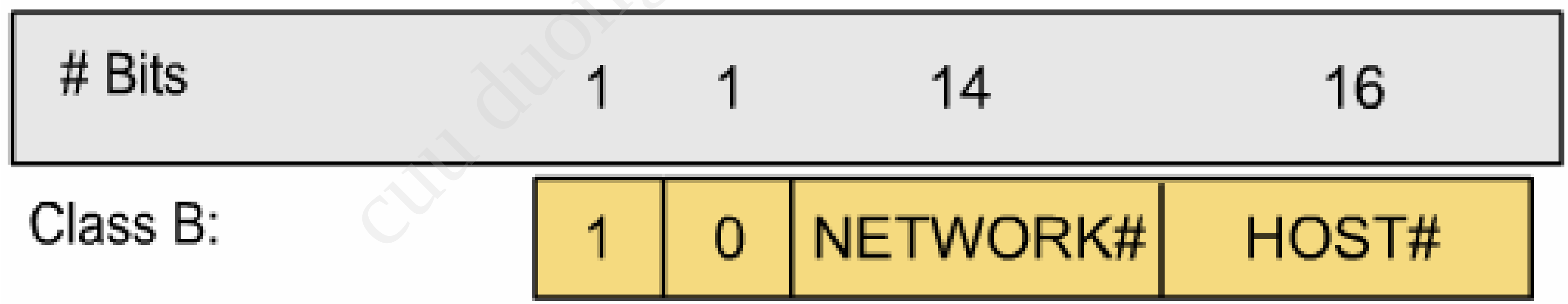


IP address classes: Class A

- The first bit of a Class A address is always 0.
- The first 8 bits to identify the network part of the address.
- Possible network address from 1.0.0.0 to 127.0.0.0.
- The remaining three octets can be used for the host portion of the address.
- Each class A network have up to 16,777,214 possible IP addresses.

IP address classes: Class B

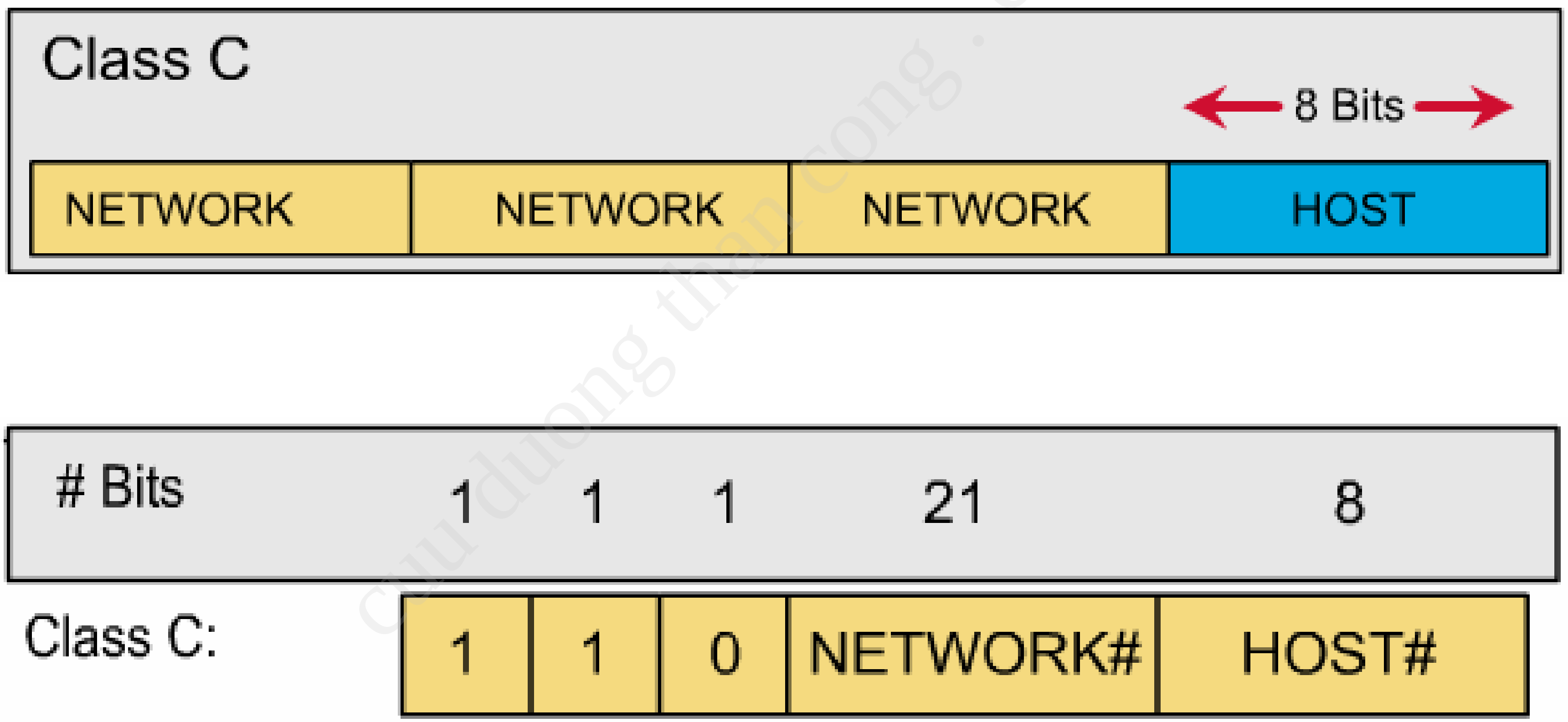




IP address classes: Class B

- The first 2 bits of a Class B address is always 10.
- The first two octets to identify the network part of the address.
- Possible network address from 128.0.0.0 to 191.255.0.0.
- The remaining two octets can be used for the host portion of the address.
- Class B network have up to 65.534 possible IP addresses.

IP address classes: Class C



IP address classes: Class C

- The first 3 bits of a Class C address is always 110.
- The first three octets to identify the network part of the address.
- Possible network address from 192.0.0.0 to 223.255.255.0.
- The remaining last octet can be used for the host portion of the address.
- Class C network have up to 254 possible IP addresses.

IP address classes: Summary

- 1.0.0.0 - 126.0.0.0 : Class A.
- 127.0.0.0 : Loopback network.
- 128.0.0.0 - 191.255.0.0 : Class B.
- 192.0.0.0 - 223.255.255.0 : Class C.
- 224.0.0.0 < 240.0.0.0 : Class D, multicast.
- >= 240.0.0.0 : Class E, reserved.

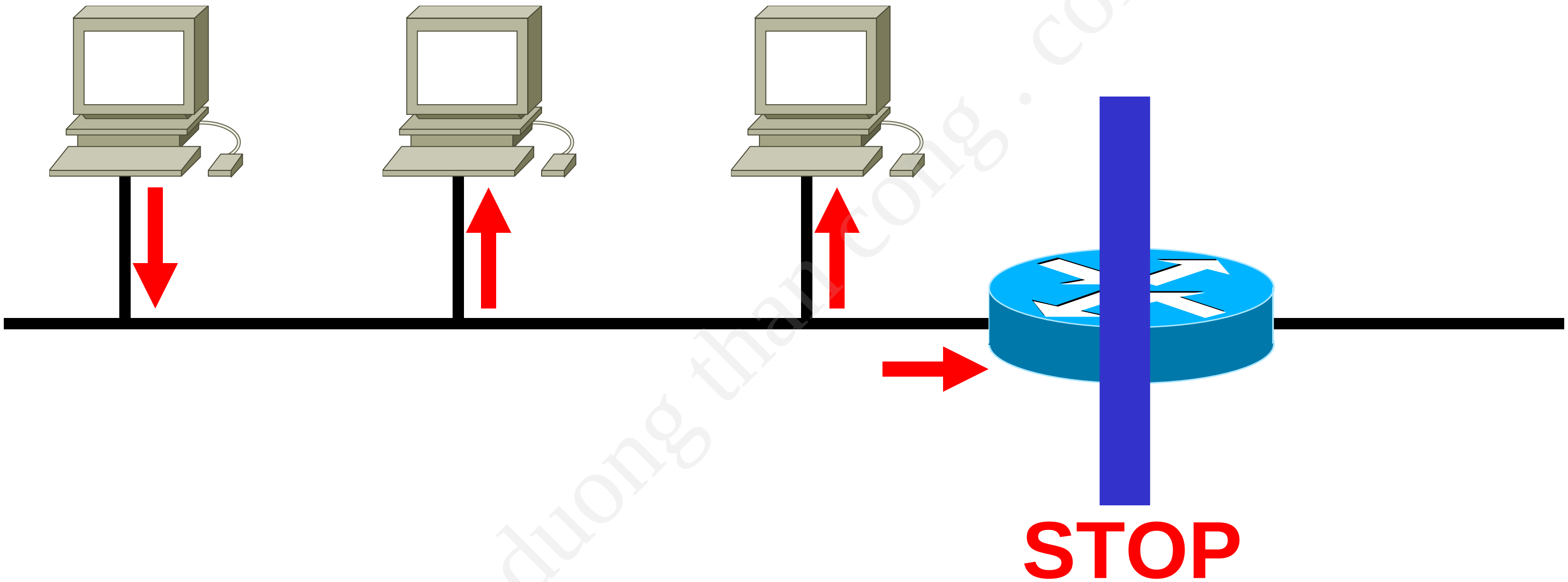
Network address

- Network address provide a convenient way to refer to all of the addresses on a particular network or subnetwork.
- Two hosts with differing network address require a device, typically a router, in order to communicate.
- An IP address that ends with binary 0s in all host bits is reserved for the network address.

Broadcast address

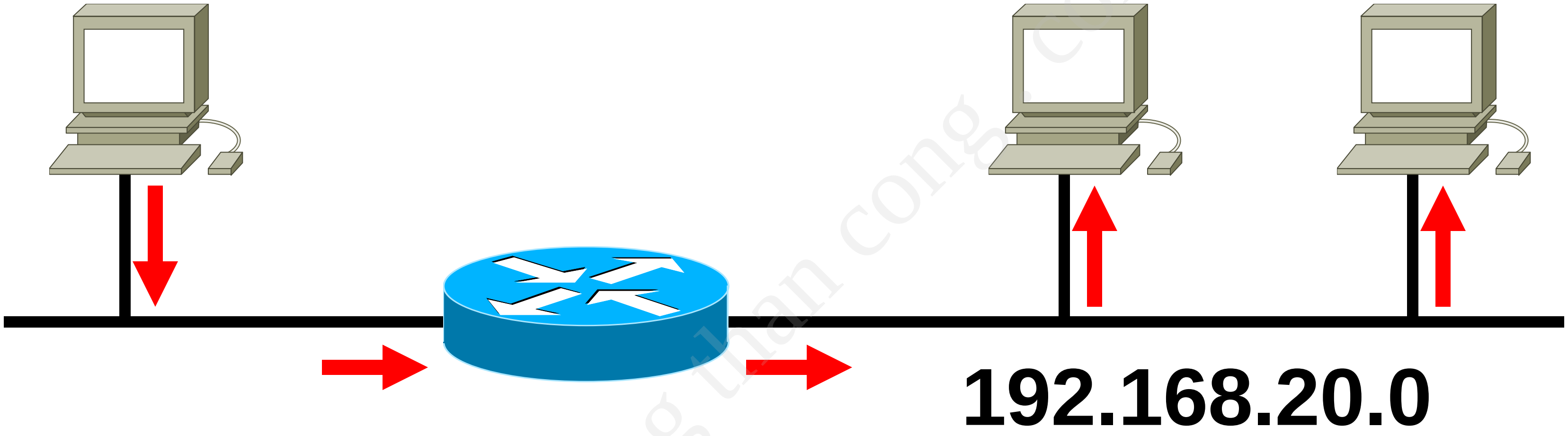
- Broadcast goes to every host with a particular network ID number.
- An IP address that ends with binary 1s in all host bits is reserved for the directed broadcast address.
- An IP address with binary 1s in all network bits and host bits is reserved for the local broadcast address.

Local broadcast address



255.255.255.255

Directed broadcast address



192.168.20.255

Broadcast address

Example: 172.16.20.200

- 172.16.20.200 is Class B address
- Network portion: 172.16
- Host portion: 20.200
- Network address: 172.16.0.0
- Broadcast address: 172.16.255.255

Private addresses

- According to RFC-1918.
- Organizations make use of the private Internet address space for hosts that require IP connectivity within their enterprise network, but do not require external connections to the global Internet.
- Class A: 10.0.0.0.
- Class B: 172.16.0.0 - 172.31.0.0.
- Class C: 192.168.0.0 - 192.168.255.0.

Example : Step 1

- Review IP address classes and their characteristics.

Example : Step 2

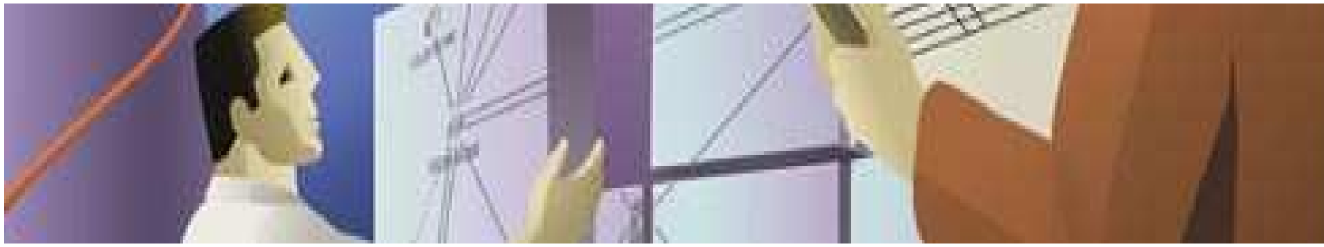
1. What is the decimal and binary range of the first octet of class B IP addresses?
   - Decimal: 128 – 191
   - Binary: 10000000 – 10111111
2. Which octet(s) represent the network portion of a class C IP address?
   - The first three octets
3. Which octet(s) represent the host portion of a class A IP address?
   - The last three octets

Example : Step 3

Host IP Address	Address Class	Network Address	Host Address	Broadcast Address
218.14.55.137	C	218.14.55	137	218.14.55.255
123.1.1.15	A	123	1.1.15	123.255.255.255
150.127.221.244	B	150.127	221.244	150.127.255.255
194.125.35.199	C	194.125.35	199	194.125.35.255
175.12.239.244	B	175.12	239.244	175.12.255.255

Example : Step 4 – Valid address

- 150.100.255.255
- 175.100.255.18
- 195.234.253.0
- 100.0.0.23
- 188.258.221.176
- 127.34.25.189
- 224.156.217.73



SUBNETTING

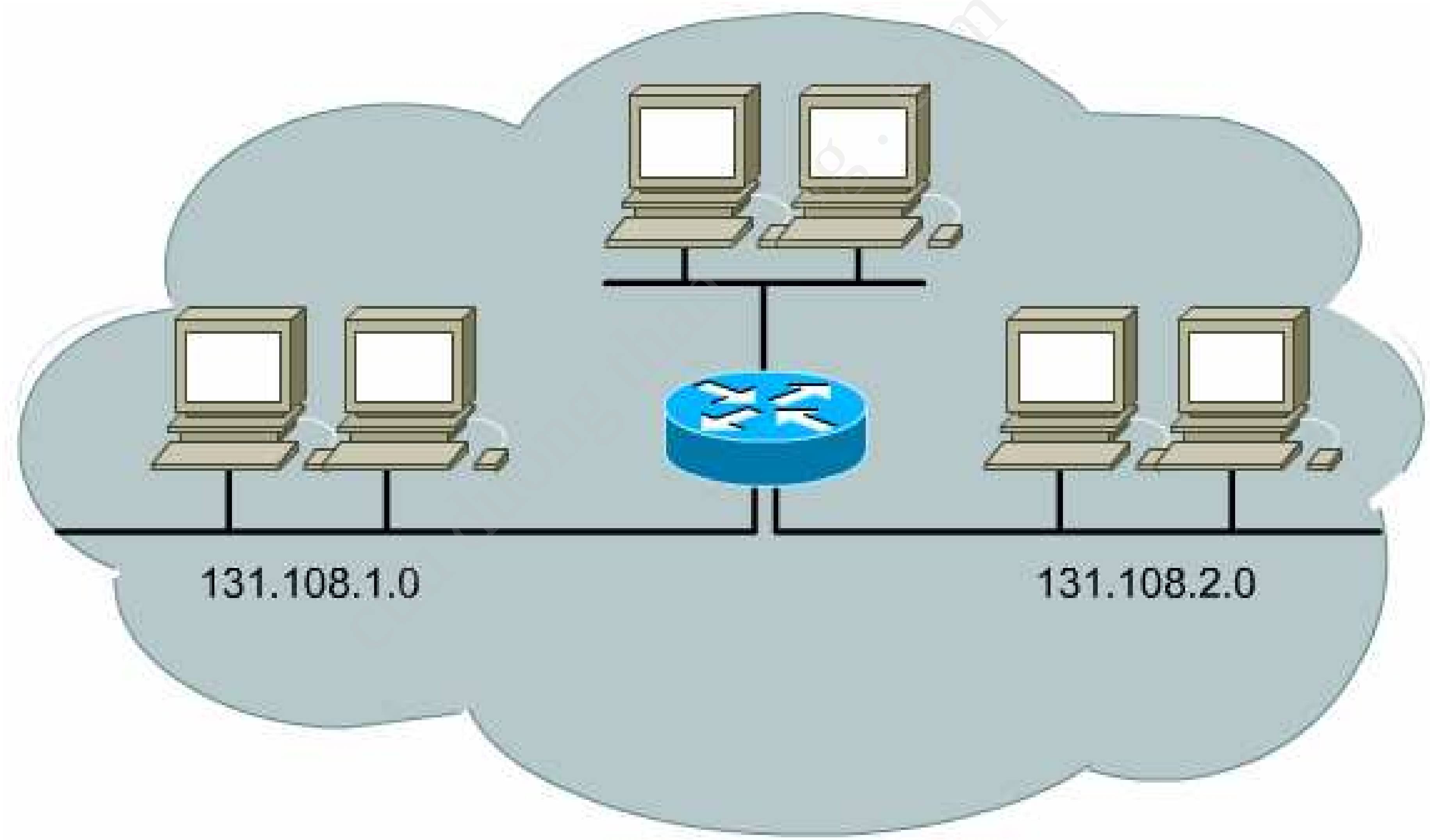
AND

CREATING A SUBNET

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.*

Divide network by three

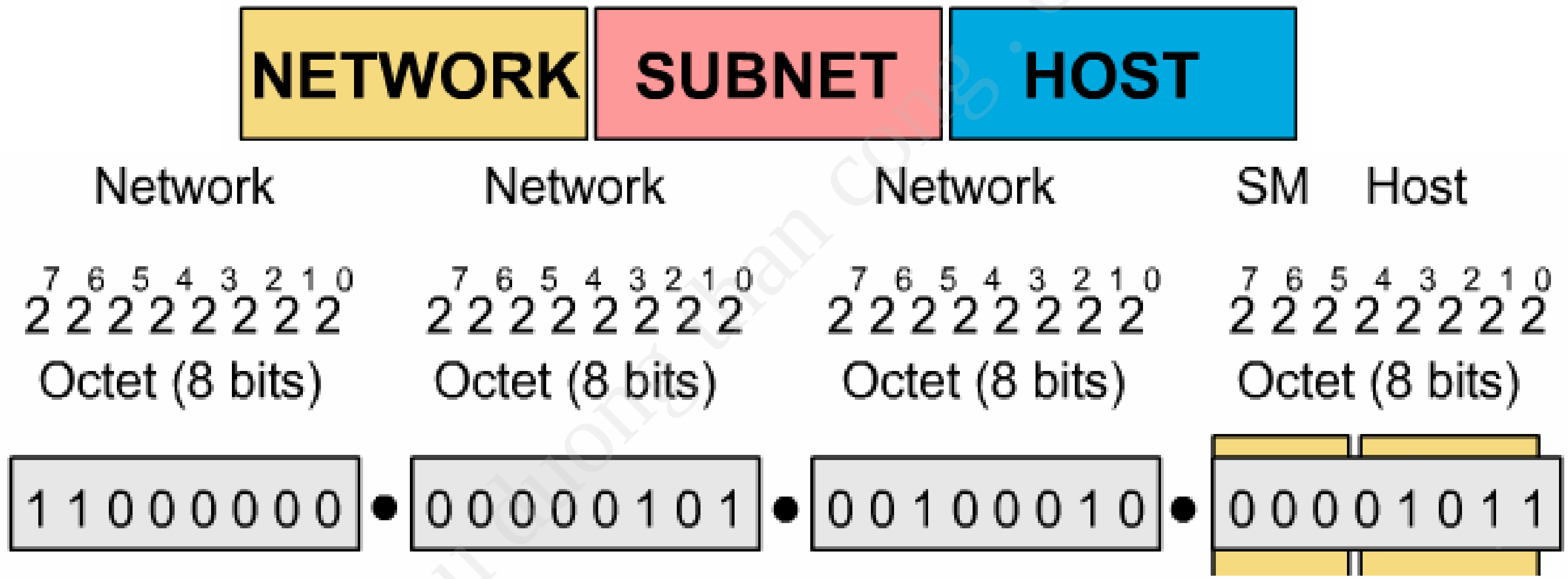


Subnetting

- Subnetworks are smaller divisions of network.
- Subnet addresses include the Class A, Class B, or Class C network portion, plus a subnet field and a host field.
- To create a subnet address, a network administrator borrows bits from the original host portion and designates them as the subnet field.
- Subnet addresses are assigned locally, usually by a network administrator.

Subnetting

SOLUTION: Create another section in the IP address called the subnet.



HOW???

By using a SUBNET MASK

Subnet mask

- "Extended Network Prefix".
- 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.

Default subnet mask: Example

- 192.168.2.100 / 255.255.255.0.
- 11000000.10101000.00000010.01100100.
- 11111111.11111111.11111111.00000000.
- 11000000.10101000.00000010.01100100.
- Class C network:
  - 24 bits for network portion.
  - 0 bits for subnet portion.
  - 8 bits for host portion.
- Subnet address: 192.168.2.0.

Subnet mask: Example

NETWORK TRAINING CENTER

- 172.16.65.100 / 255.255.240.0.
- 10101100.00010000.01000001.01100100.
- 11111111.11111111.11110000.00000000.
- 10101100.00010000.01000001.01100100.
- Class B network:
  - 16 bits for network portion.
  - 4 bits for subnet portion.
  - 12 bits for host portion.
- Subnet address: 172.16.64.0.

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.

Boolean algebra review

- Boolean operators:
  - AND.
  - OR.
  - NOT.

AND operator

NETWORK TRAINING CENTER

1 AND 1 = 1

1 AND 0 = 0

0 AND 1 = 0

0 AND 0 = 0

OR operator

1 OR 1 = 1

1 OR 0 = 1

0 OR 1 = 1

0 OR 0 = 0

NOT operator

NOT 1 = 0

NOT 0 = 1

Boolean algebra examples

1010 AND 0110 = 0010

1010 OR 0110 = 1110

Why we need to know Boolean ops?

NETWORK TRAINING CENTER

IP Address	AND	Subnet Mask	=	Network and Subnet address

- Network layer performs the Boolean operations in order to find the network ID of a subnet
- Example:
  - 172.16.65.100 AND 255.255.240.0
  - Network address: 172.16.64.0

Subnetting example

- Given network 172.16.0.0.
- We need 8 usable subnets and up to 1000 hosts on each subnet.

Calculating a subnet

1. Determine the class of network and default subnet mask.
2. Determine how many bits to borrow. Determine the subnet mask and the actual number of subnets and hosts.
3. Determine the ranges of host address for each subnet. Choose the subnets that you want to use.

Calculating a subnet: STEP 1

- Determine the Class of network

→ Class B

- Determine the default subnet mask

→ 255.255.0.0

Calculating a subnet: STEP 2

- 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.

Calculating a subnet: STEP 2 (Cont.)

- 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 ?*

Calculating a subnet: STEP 2 (Cont.)

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: 255.255.240.0.

Calculating a subnet: STEP 3

- Determine the subnets and the ranges of host address for each subnet. Including:
  - Sub-network addresses
  - Range of usable IP addresses
  - Sub-network broadcast addresses

Calculating a subnet: STEP 3 (Cont.)

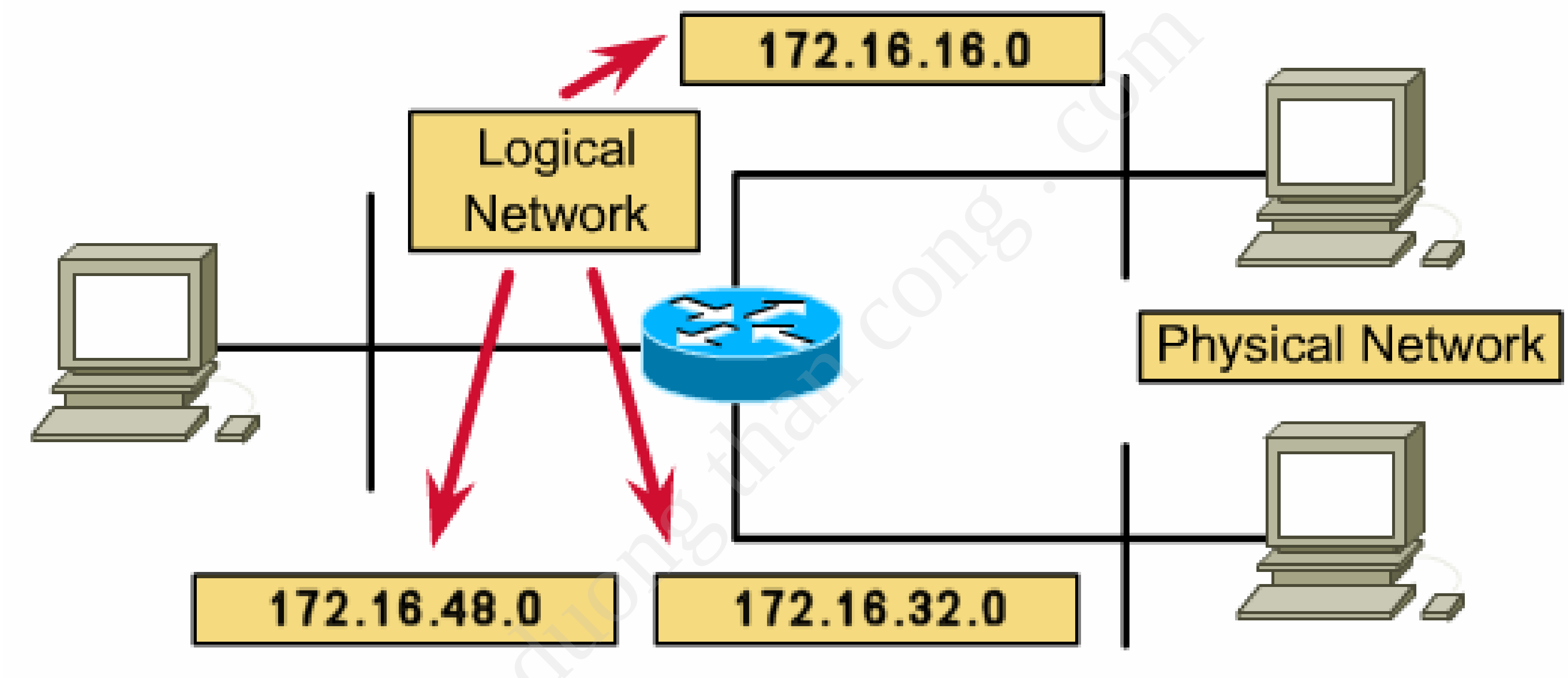
- Determine the subnets from 4 borrowed bits from the host portion (last 2 bytes):

- Subnet zero: .00000000.00000000
- 1st subnet: .00010000.00000000
- 2nd subnet: .00100000.00000000
- 3rd subnet: .00110000.00000000
- …
- 15th subnet: .11110000.00000000

Calculating a subnet: STEP 3 (Cont.)

No	Sub-network address	Possible host address	Broadcast address	Use?
0	172.16.0.0	172.16.0.1 – 172.16.15.254	172.16.15.255	N
1	172.16.16.0	172.16.16.1 – 172.16.31.254	172.16.31.255	Y
2	172.16.32.0	172.16.32.1 – 172.16.47.254	172.16.47.255	Y
..	..	..	..	..
..	..	..	..	..
13	172.16.208.0	172.16.208.1 – 172.16.223.254	172.16.223.255	Y
14	172.16.224.0	172.16.224.1 – 172.16.239.254	172.16.239.255	Y
15	172.16.240.0	172.16.240.1 – 172.16.255.254	172.16.255.255	N

Calculating a subnet: STEP 3 (Cont.)



- Using subnets No.1 to No.8.
- 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.

Q&A

CCNA Semester 1

The **Cisco Certified**
Network Associate
Curriculum

Chapter 10

LAYER 3

PROTOCOLS

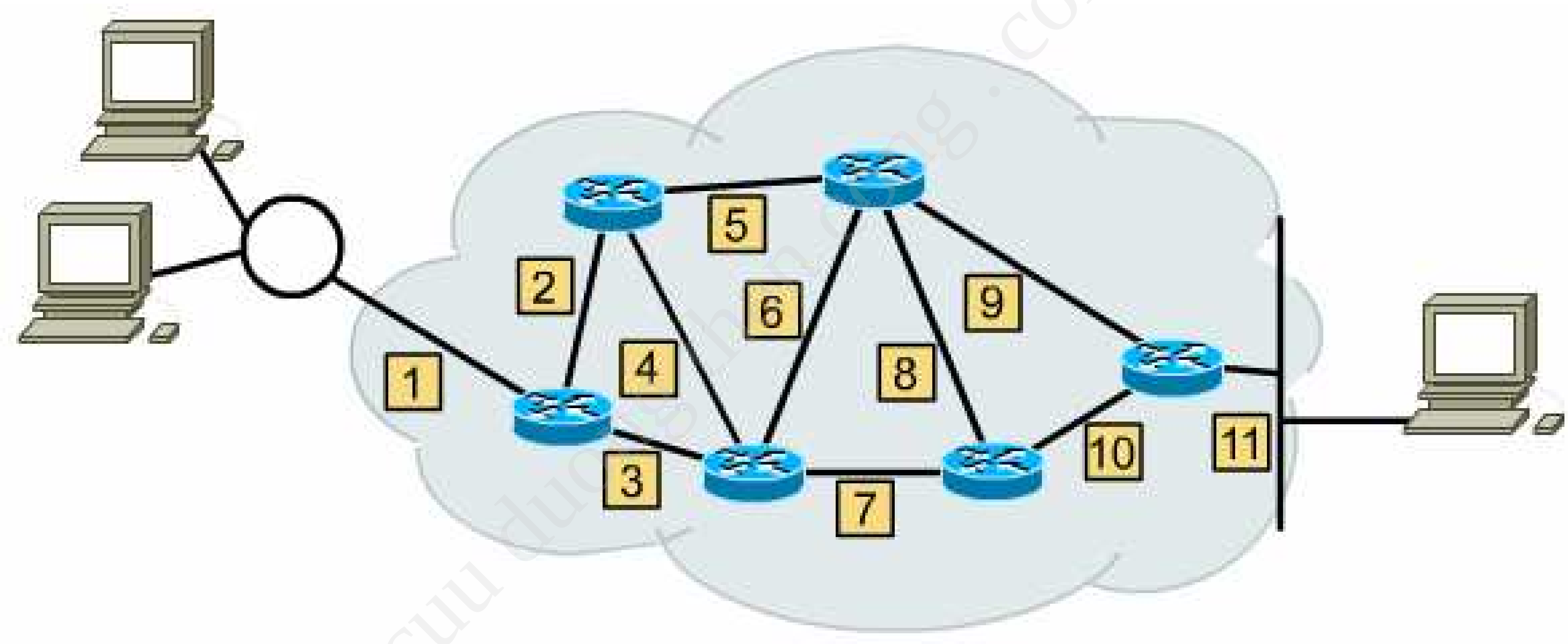
LAYER 3 DEVICES

AND

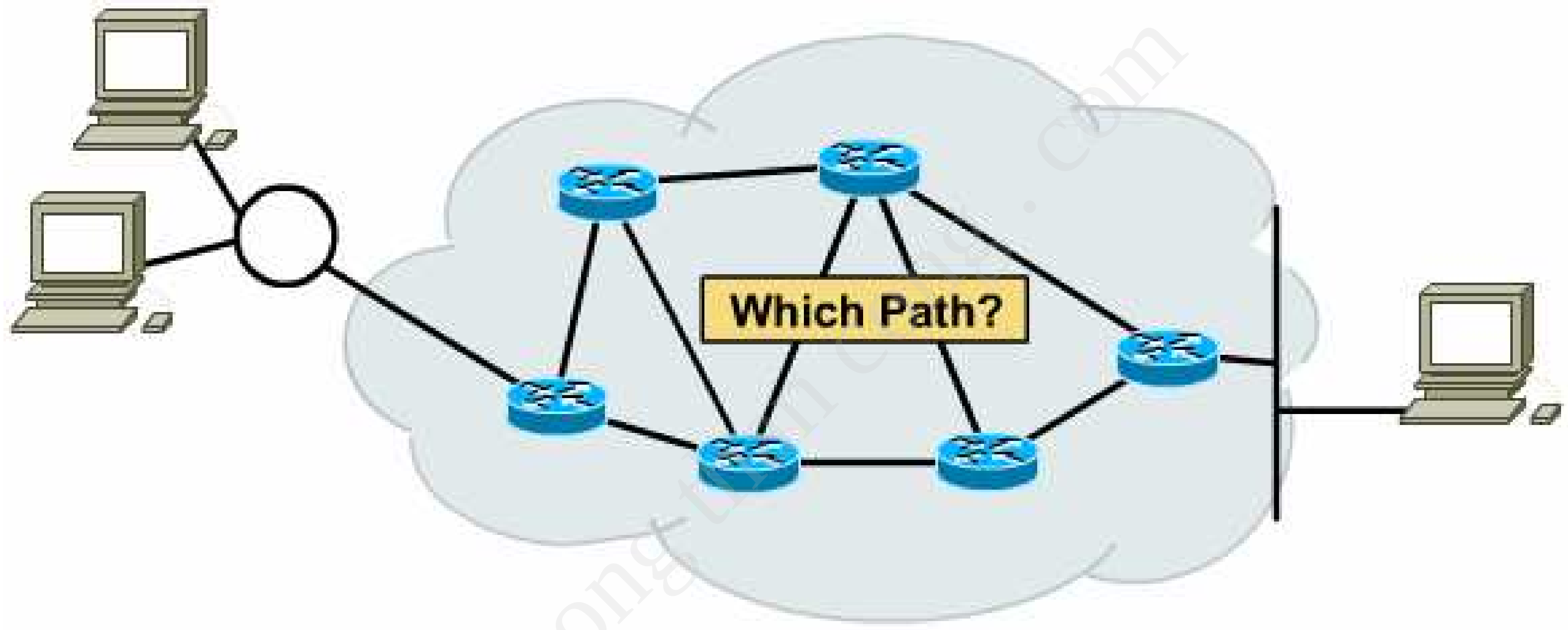
NETWORK TO NETWORK

COMMUNICATION

Internetworking



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 ...

Router

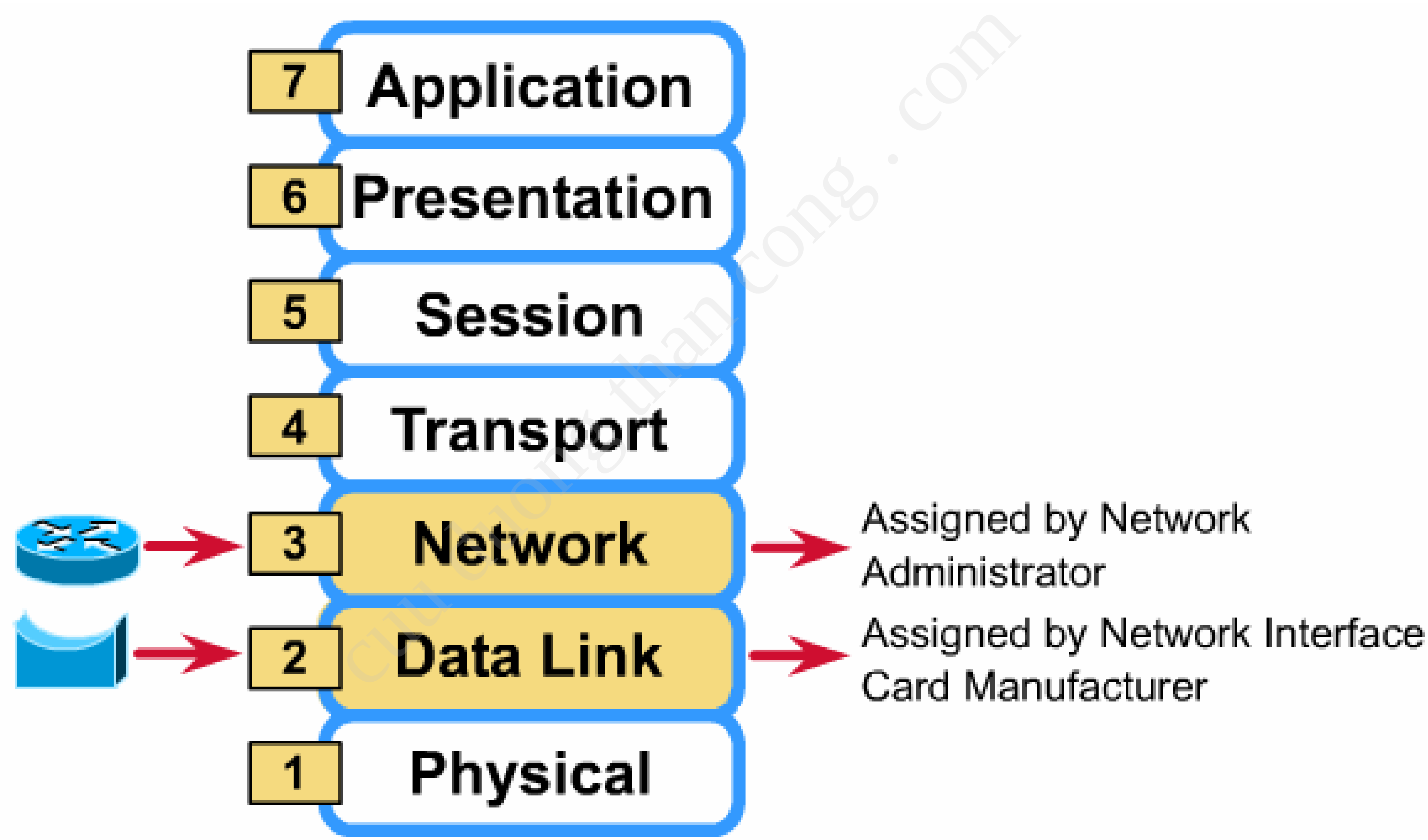
- A router is a type of internetworking device that passes data packets between networks, based on Layer 3 addresses.
- A router has the ability to make intelligent decisions regarding the best path for delivery of data on the network.

IP addresses

- IP addresses are implemented in software, and refer to the network on which a device is located.
- IP addressing scheme, according to their geographical location, department, or floor within a building.
- Because they are implemented in software, IP addresses are fairly easy to change.

Router and Bridge

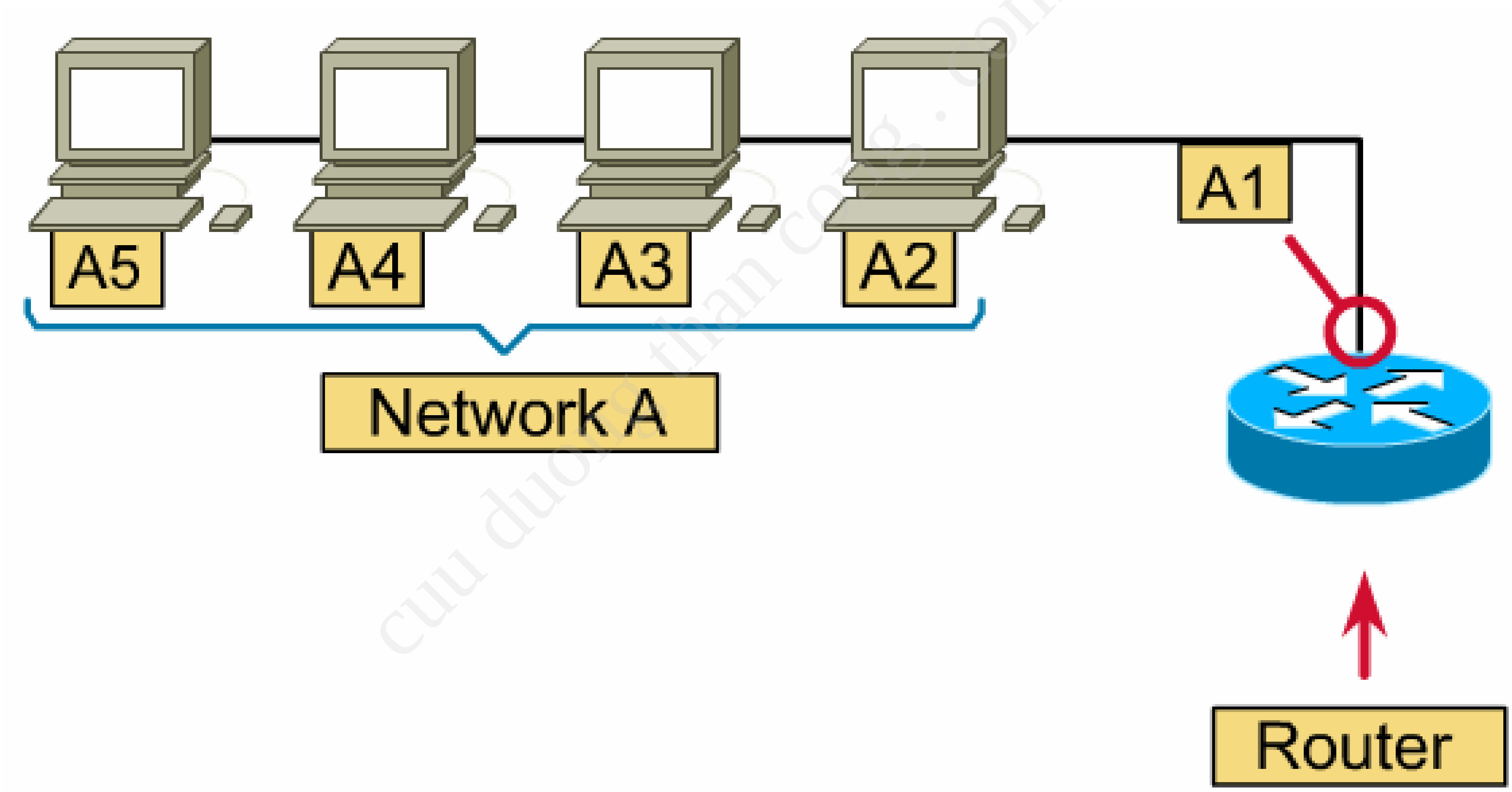
NETWORK TRAINING CENTER



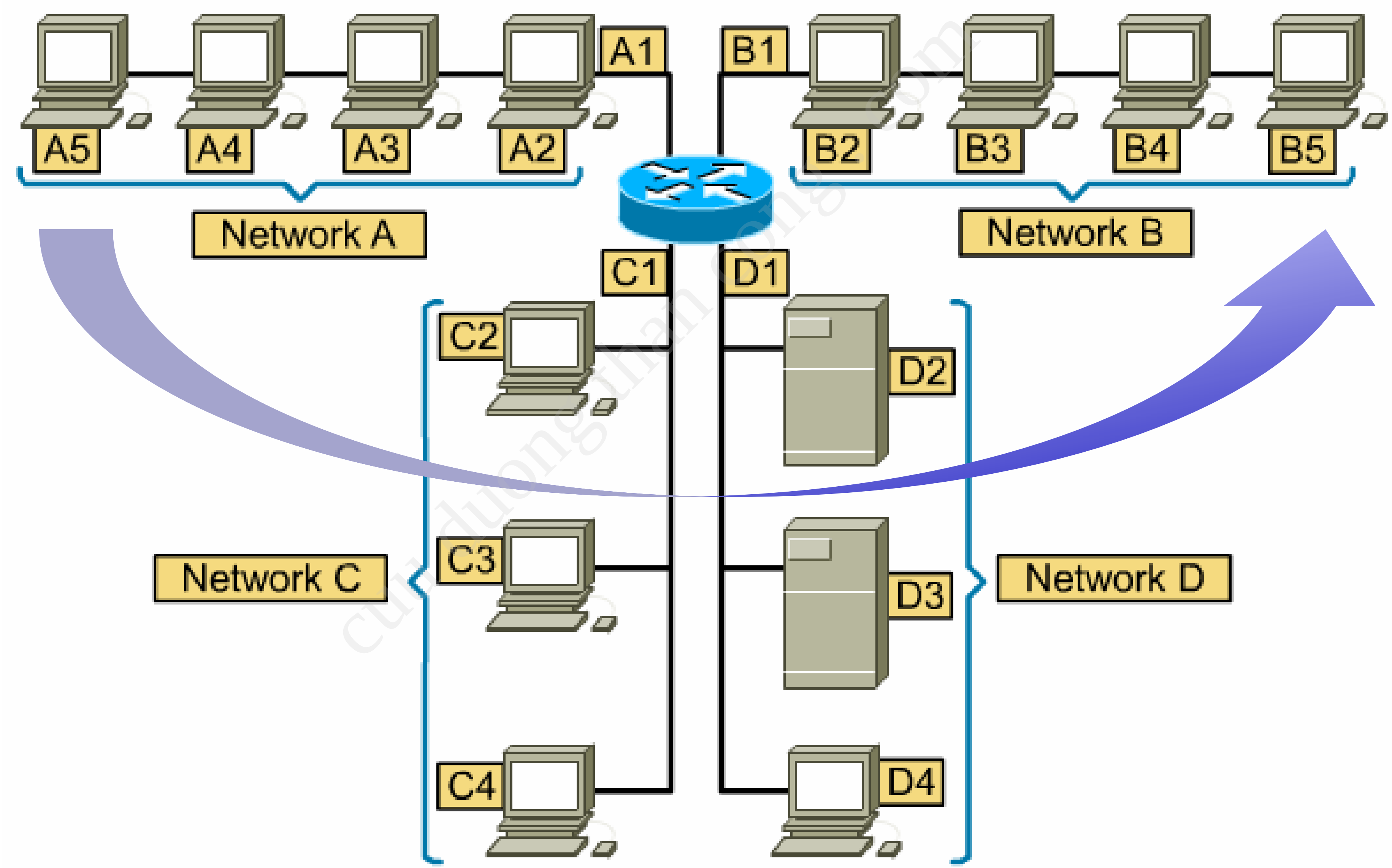
Router connections

- 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.

Router Interface

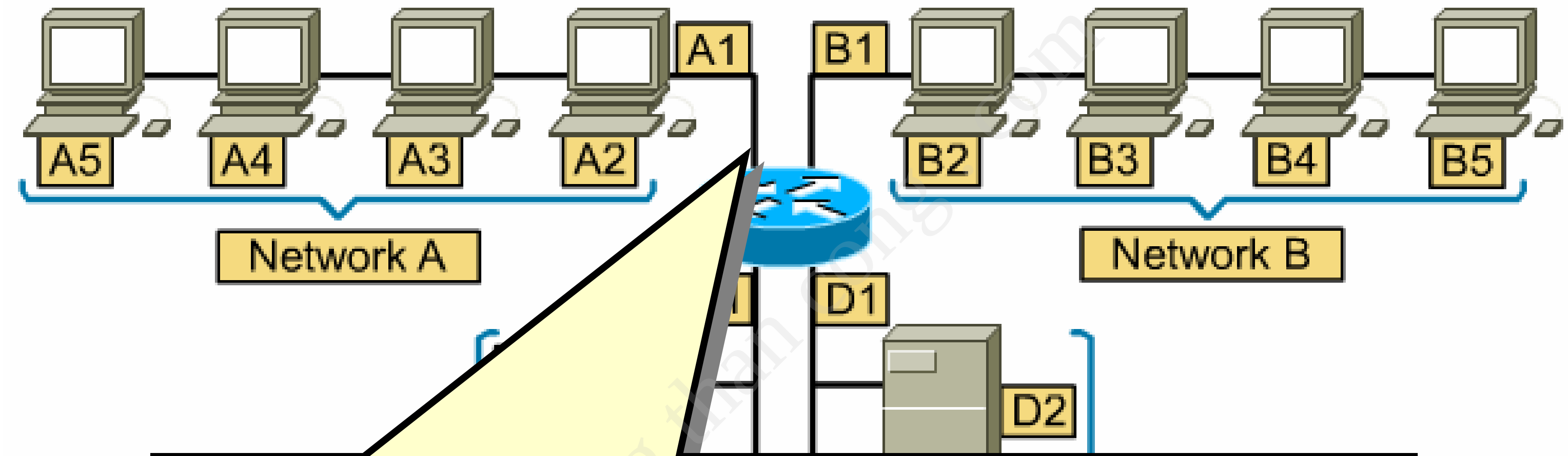


Router function



Router function (cont.1)

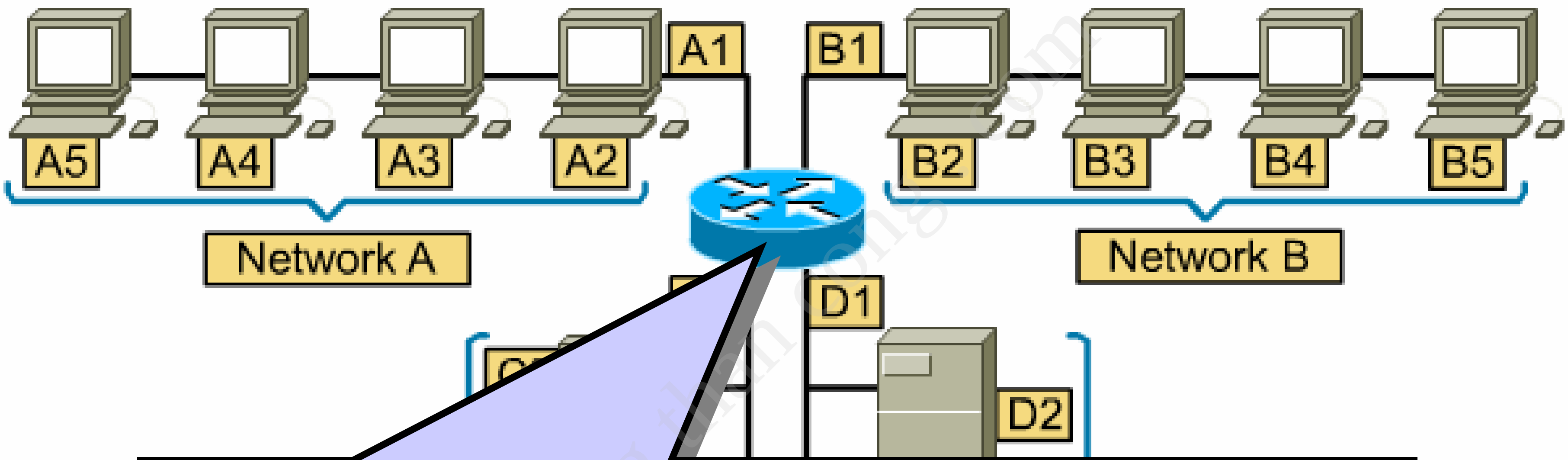
NETWORK TRAINING CENTER



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

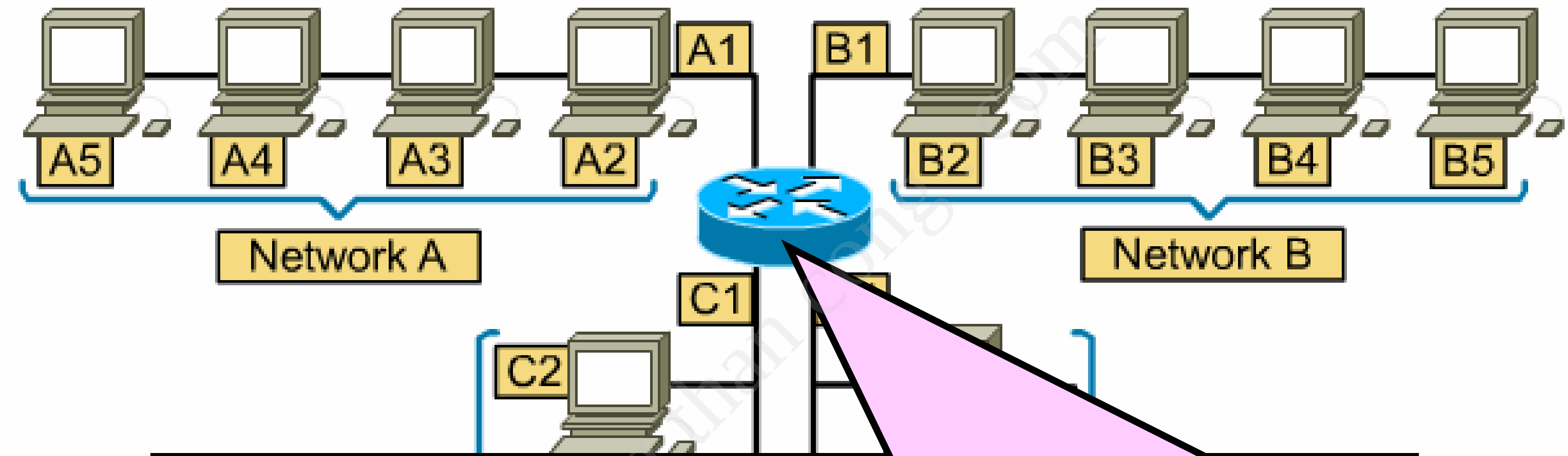
(The data link header contains the MAC addresses of the source and destination.)

Router function (cont.2)



Examines the network layer address to determine the destination network.

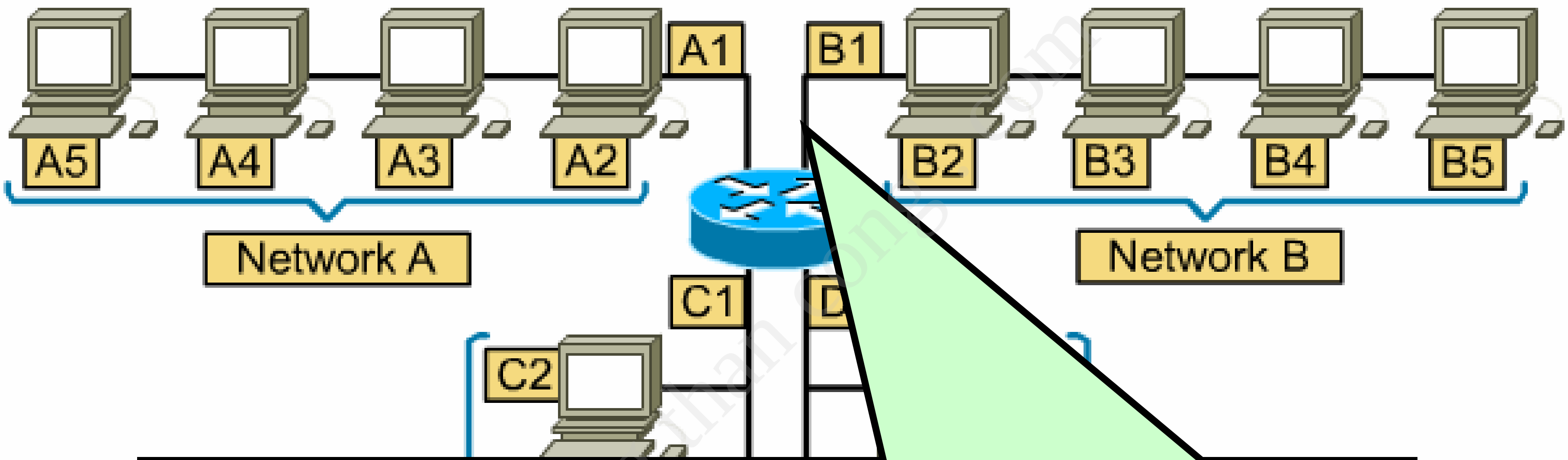
Router function (cont.3)



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.

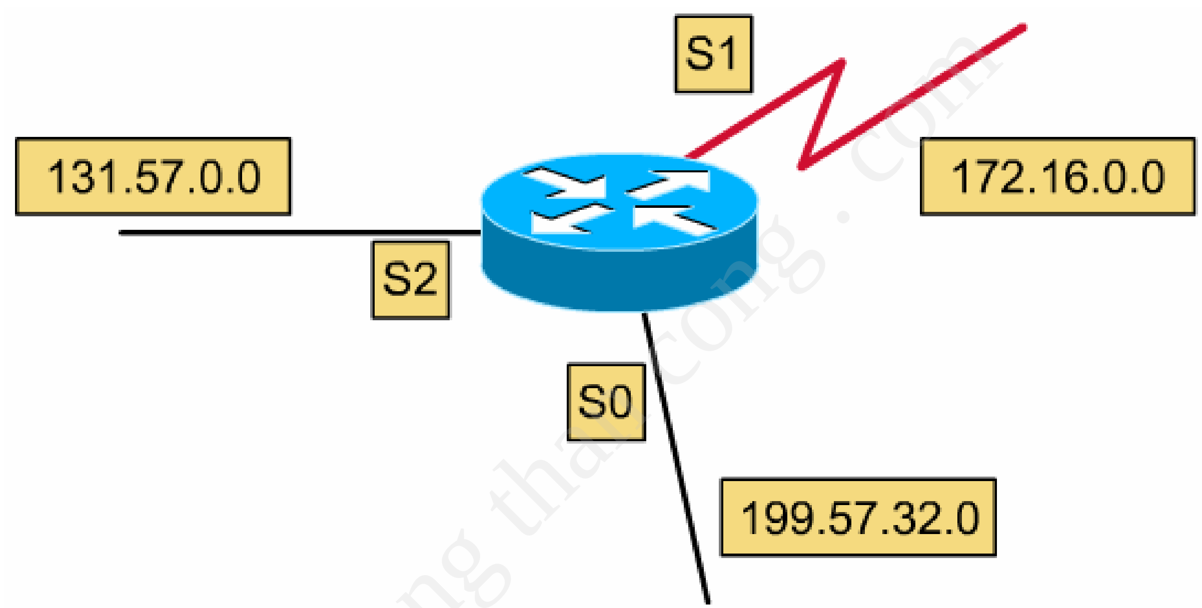
Router function (cont.4)

NETWORK TRAINING CENTER



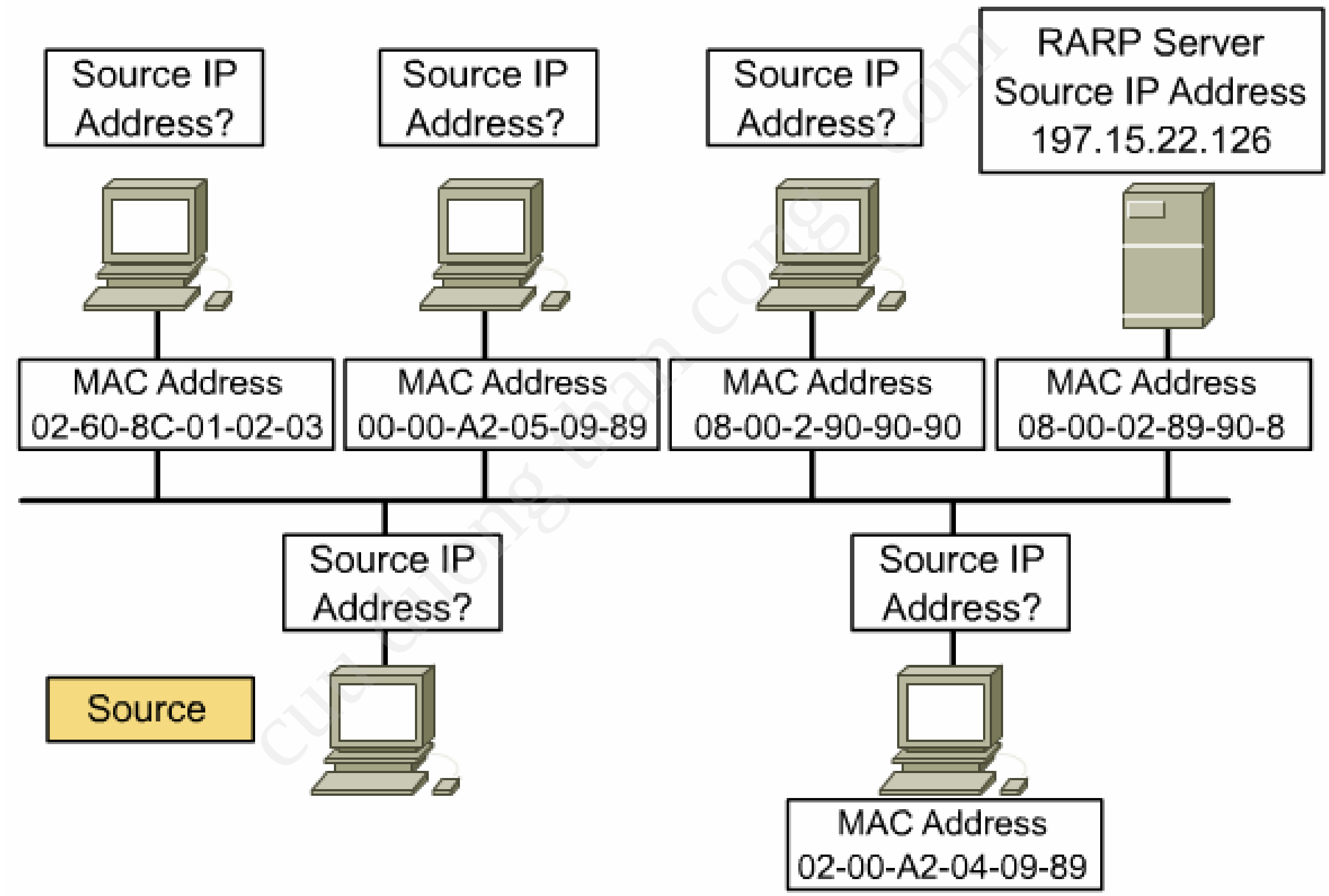
Send the data out interface B1, the router would encapsulate the data in the appropriate data link frame.

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 and dynamic addressing

Static addressing

- You must go to each individual device and configure it with an IP address.
- You should keep very meticulous records, because problems can occur on the network if you use duplicate IP addresses.

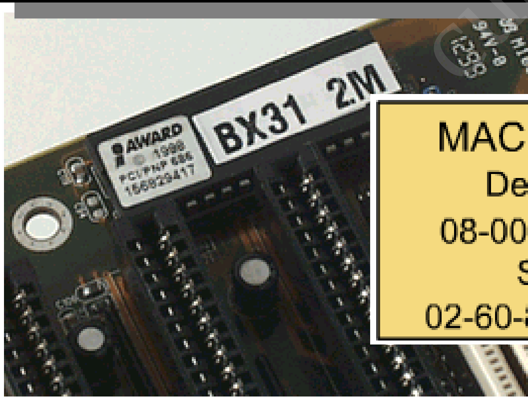
Dynamic addressing

- There are a few different methods that you can use to assign IP addresses dynamically:
  - RARP: Reverse Address Resolution Protocol.
  - BOOTP: BOOTstrap Protocol.
  - DHCP: Dynamic Host Configuration Protocol.

Dynamic addressing: RARP

MAC: Known
IP: Unknown

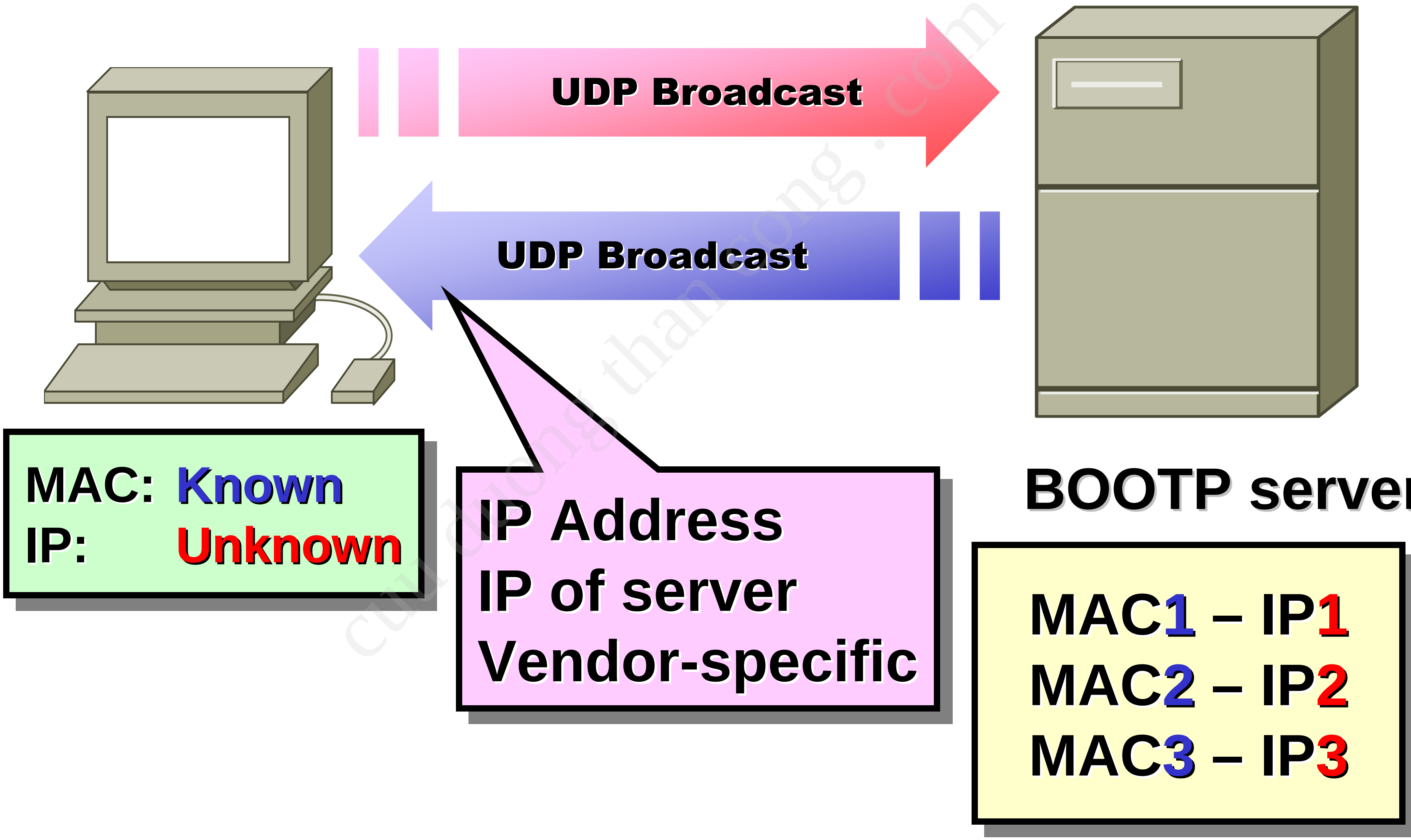
RARP server



MAC HEADER	IP HEADER	RARP REQUEST MESSAGE
Destination 08-00-02-89-90-8 Source 02-60-8C-01-02-03	Destination 11111111 Source ????????	What is my IP address?

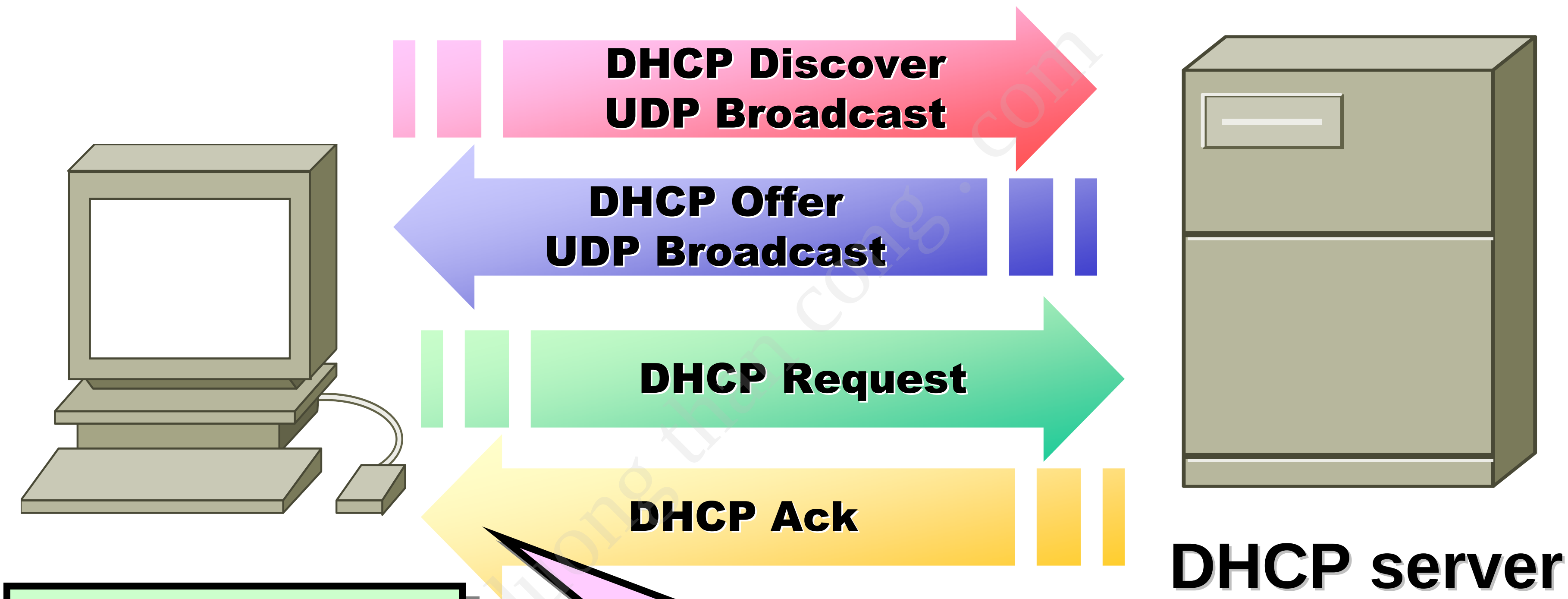
Dynamic addressing: BOOTP

NETWORK TRAINING CENTER



Dynamic addressing: DHCP

NETWORK TRAINING CENTER



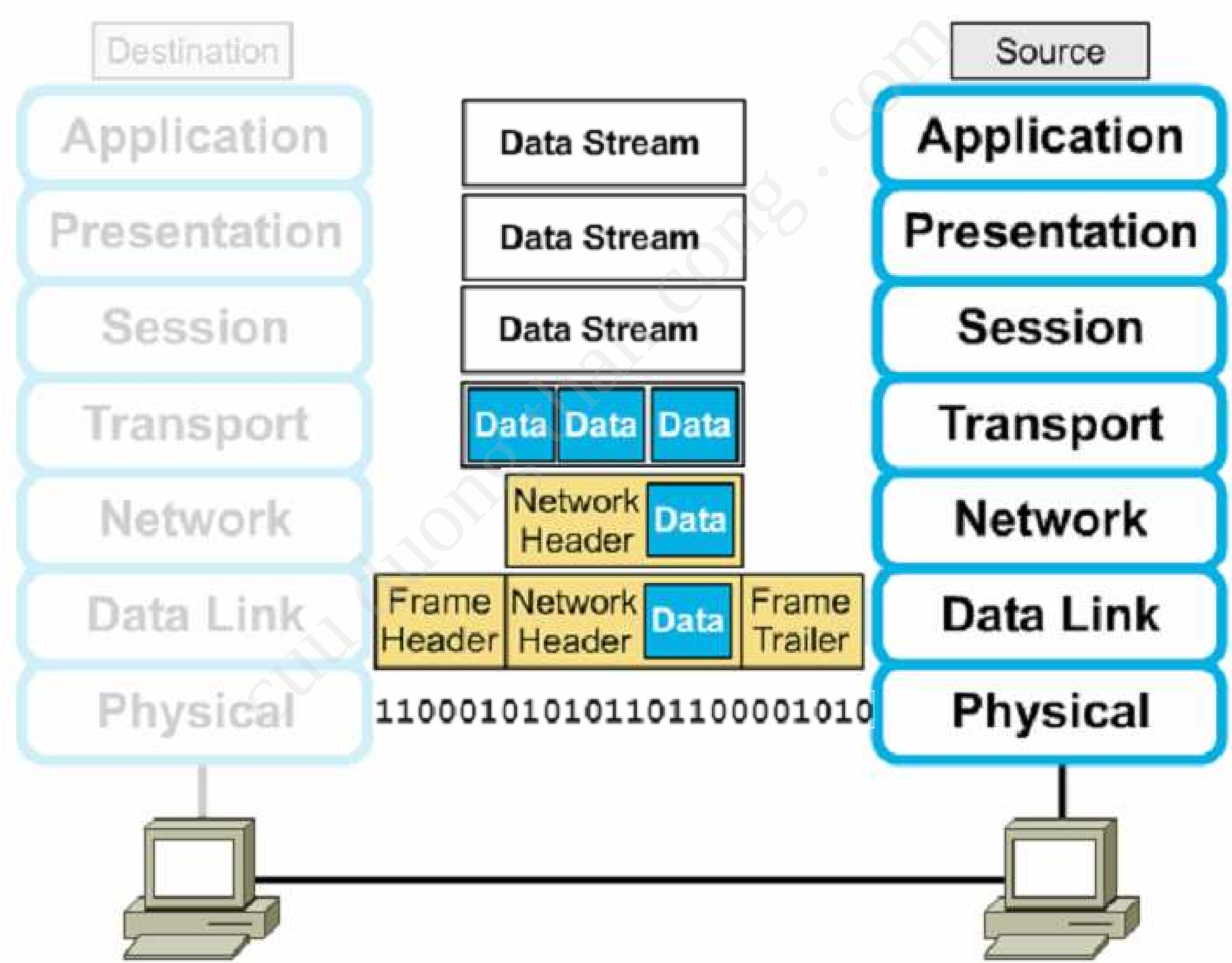
MAC: Known
IP: Unknown

IP Address
Gateway
IP of servers
And more …

IP1
IP2
IP3

ARP CONCEPT

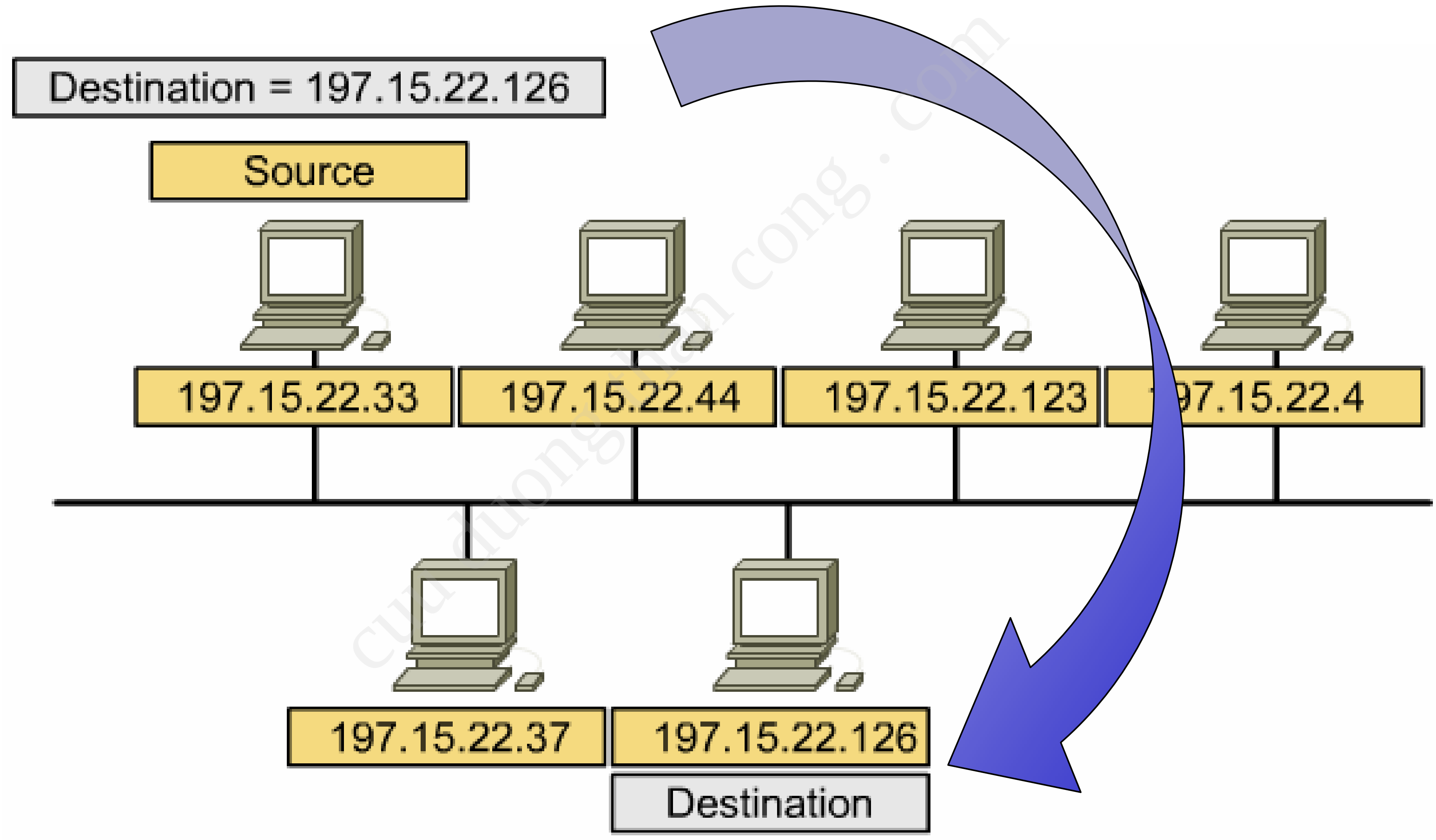
Encapsulation



Address resolution protocol

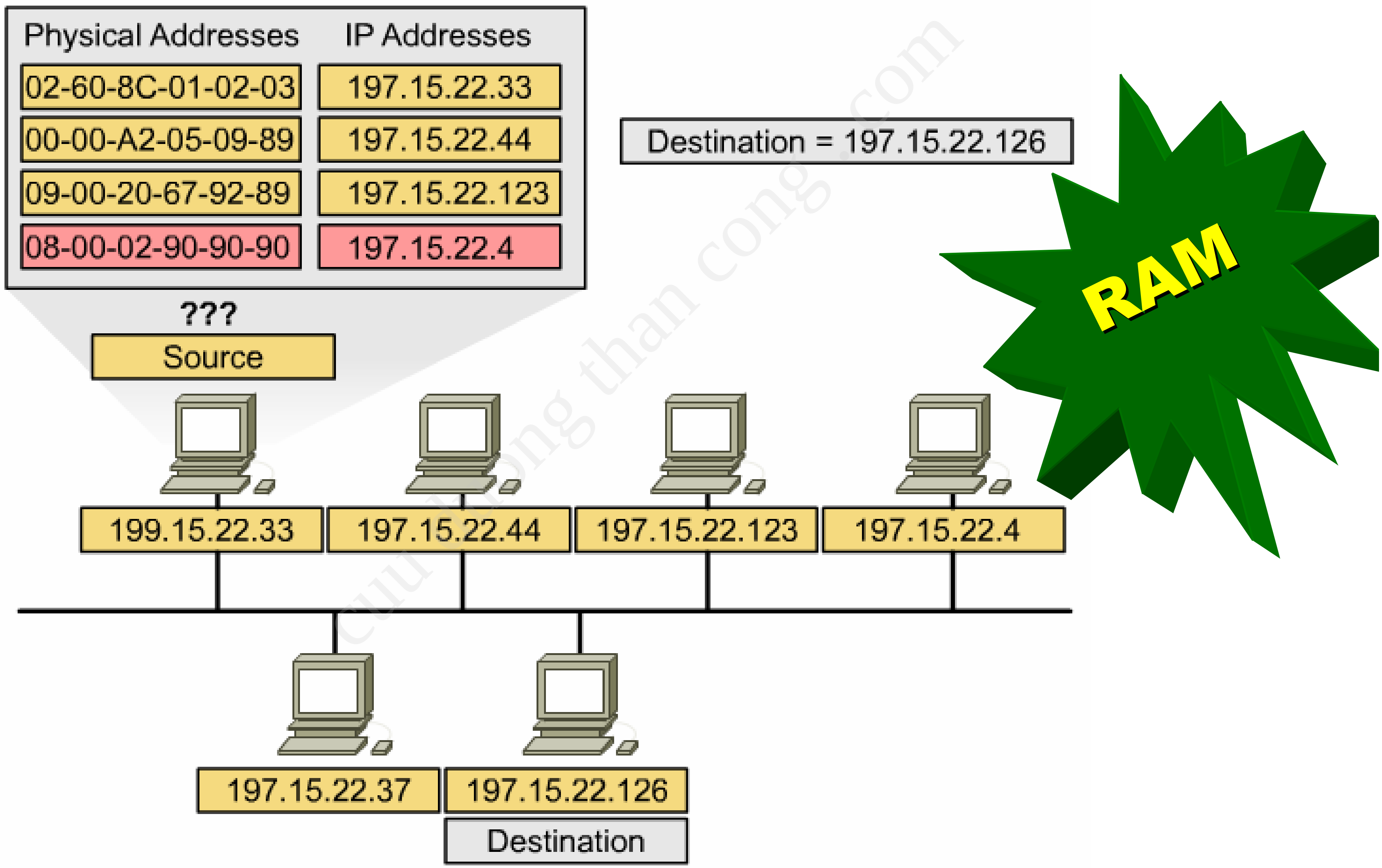
- In order for devices to communicate, the sending devices need both the IP addresses and the MAC addresses of the destination devices.
- When they try to communicate with devices whose IP addresses they know, they must determine the MAC addresses.
- ARP enables a computer to find the MAC address of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

Address resolution protocol

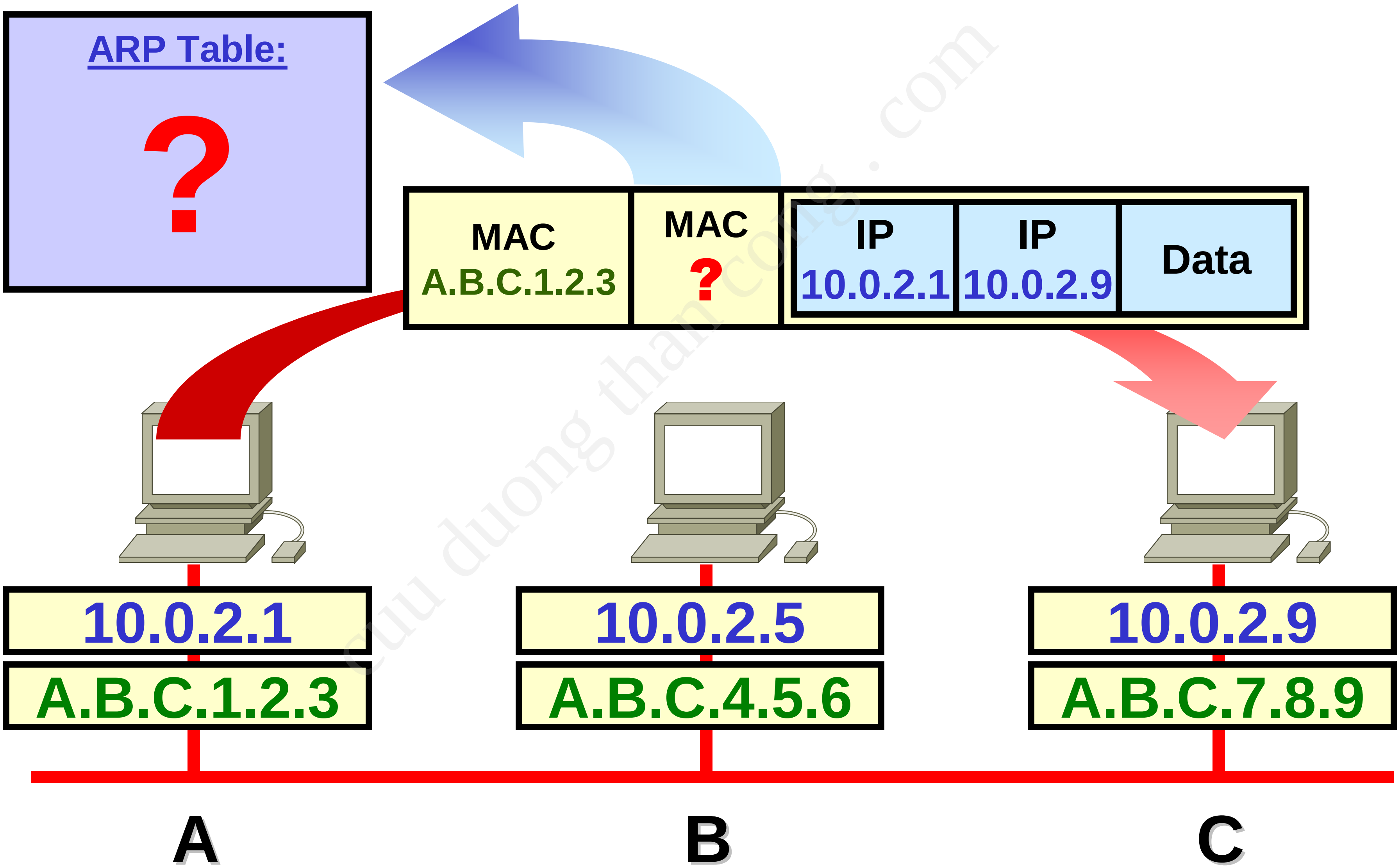


ARP table in host

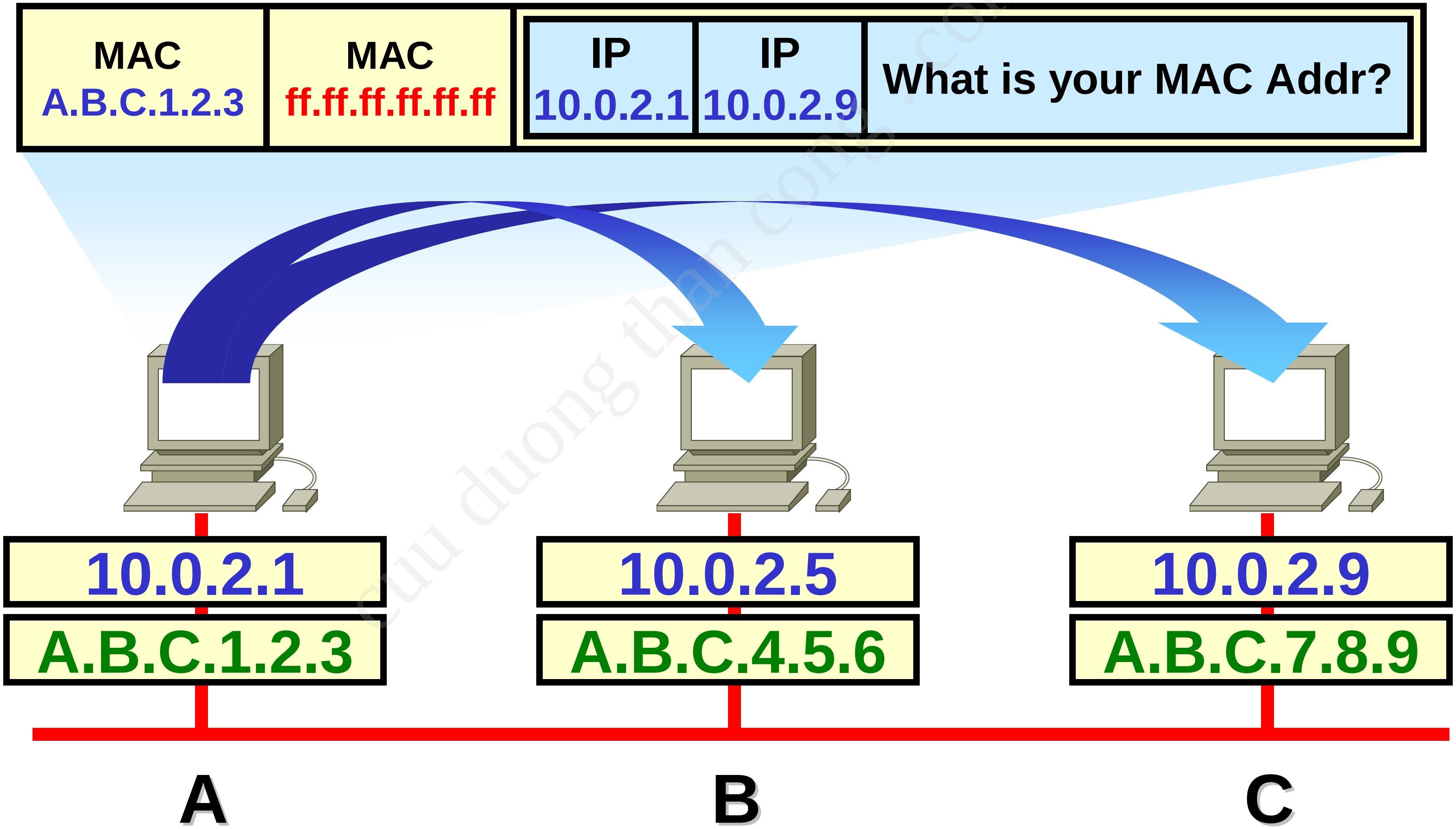
NETWORK TRAINING CENTER



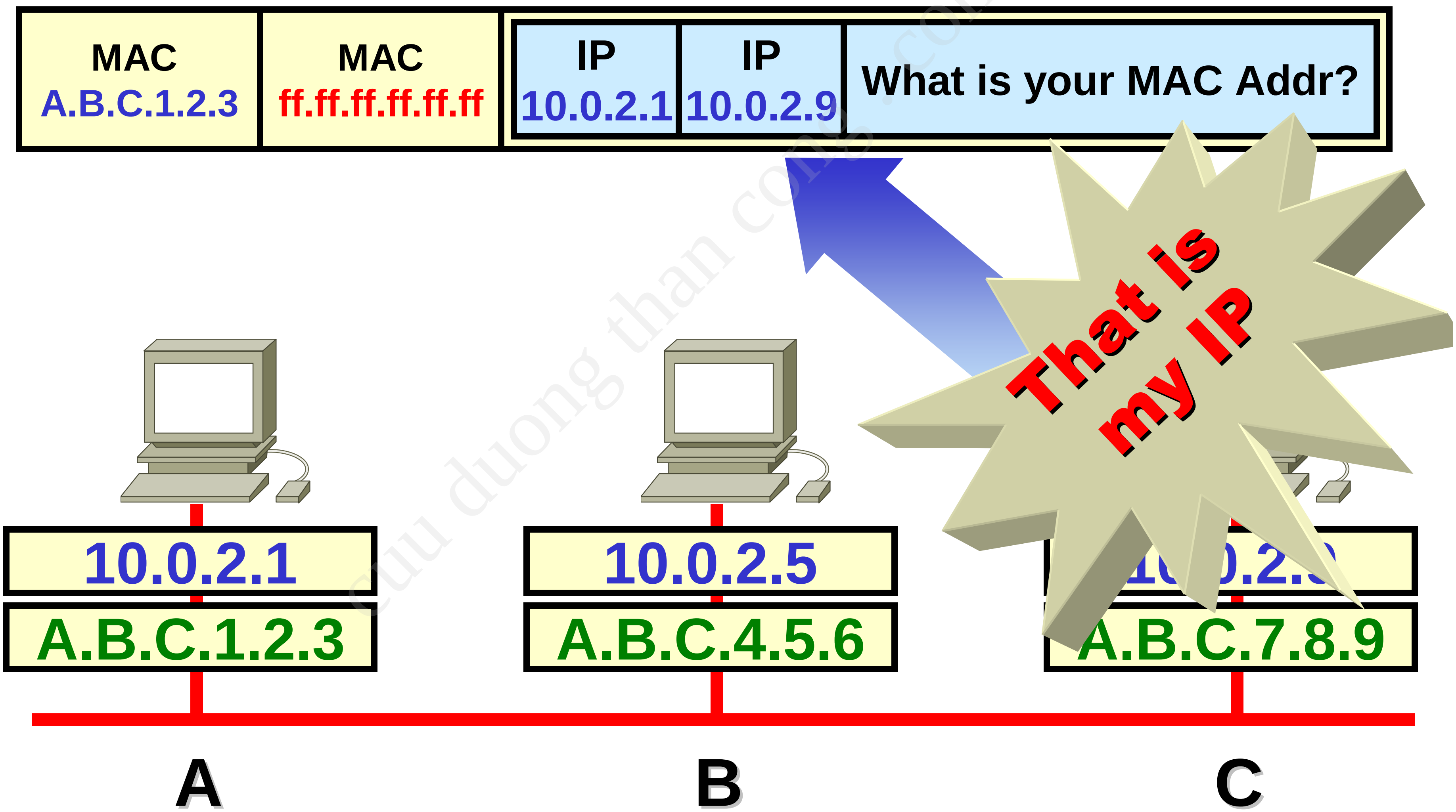
ARP operation



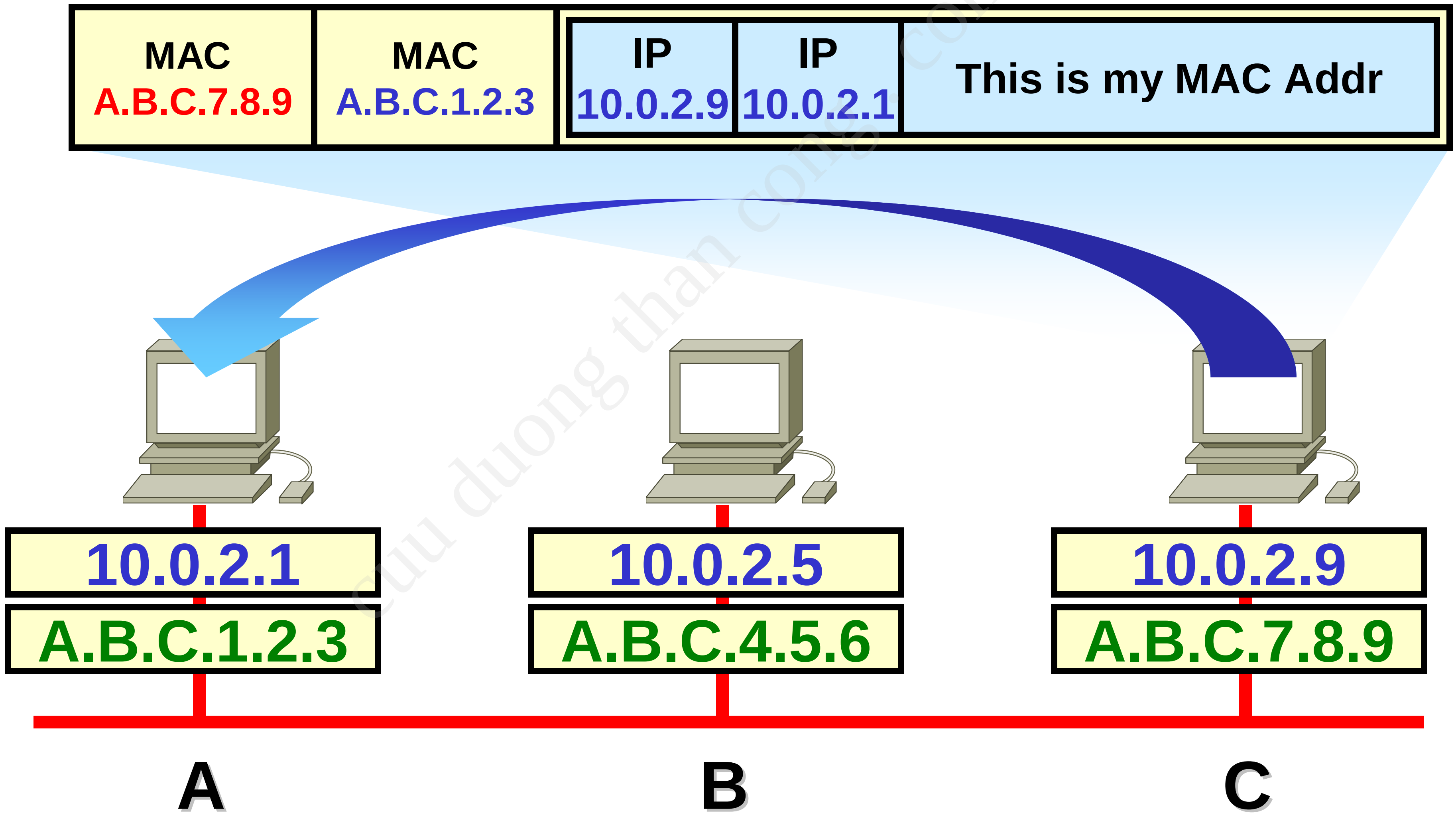
ARP operation: ARP request



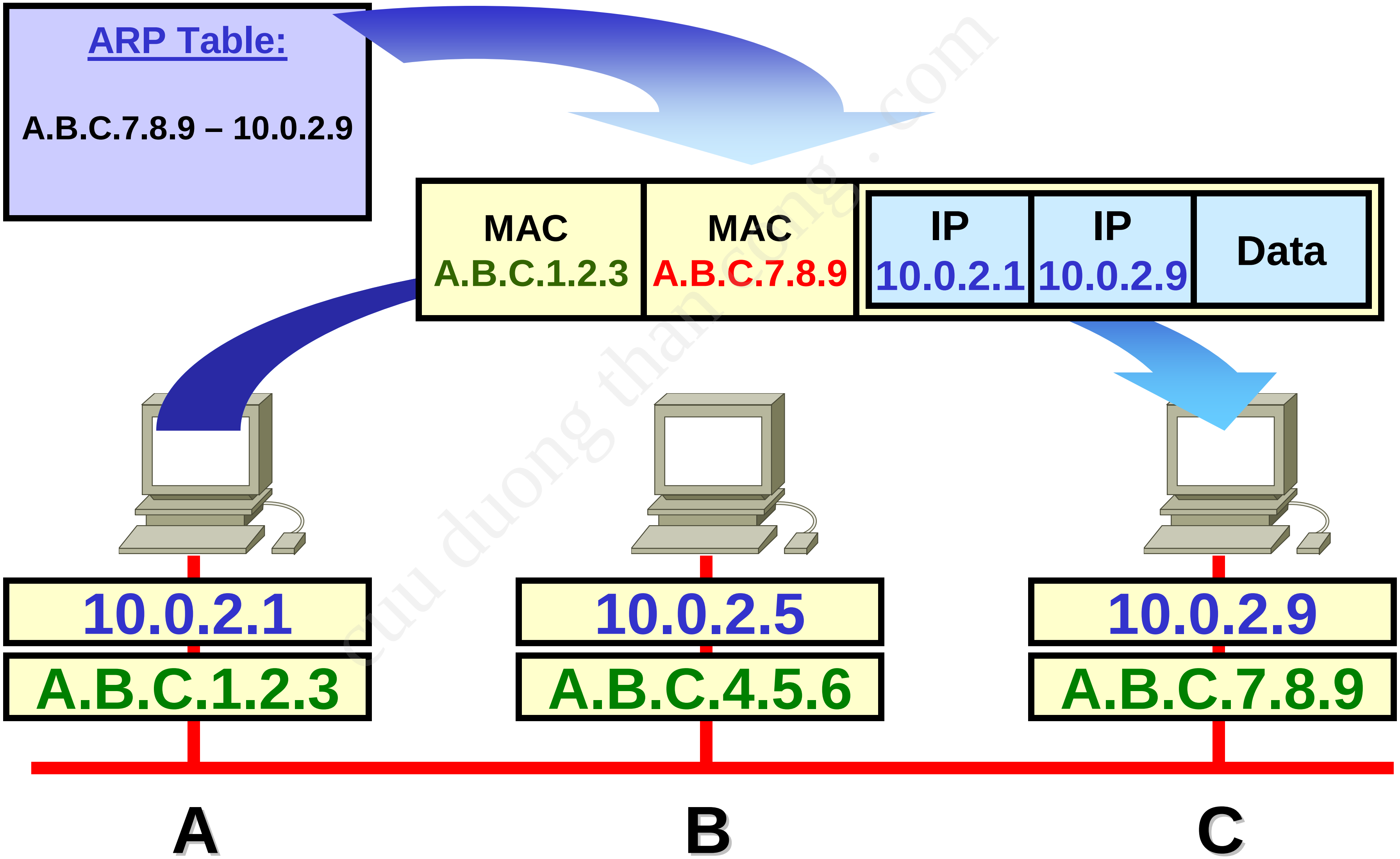
ARP operation: Checking



ARP operation: ARP reply

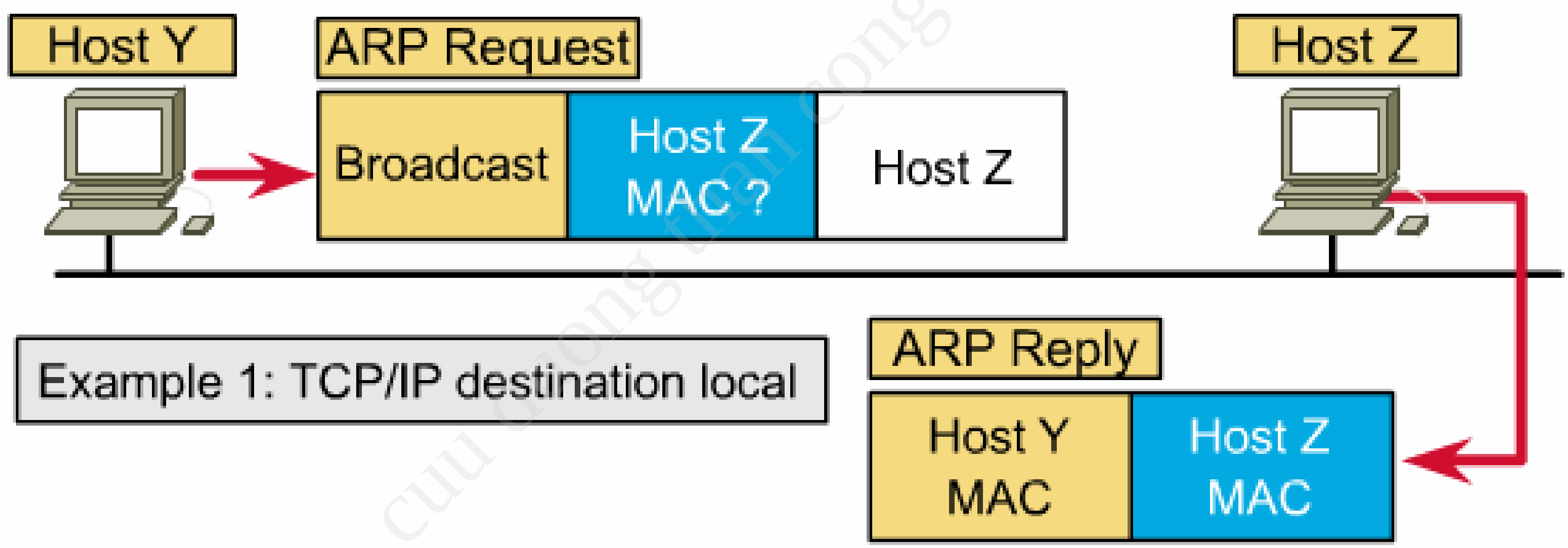


ARP operation: Caching



ARP: Destination local

NETWORK TRAINING CENTER



Internetwork communication

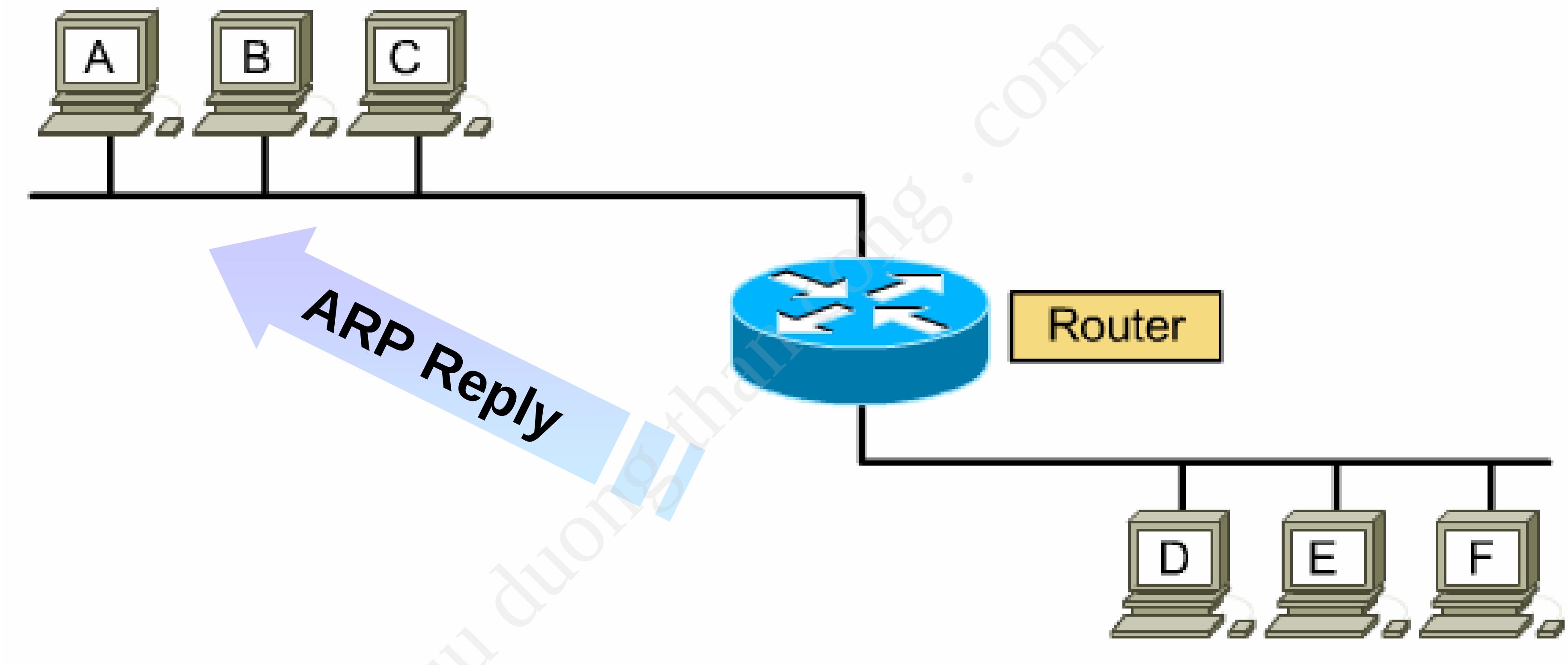
- How to communicate with devices that are not on the same physical network segment.

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.

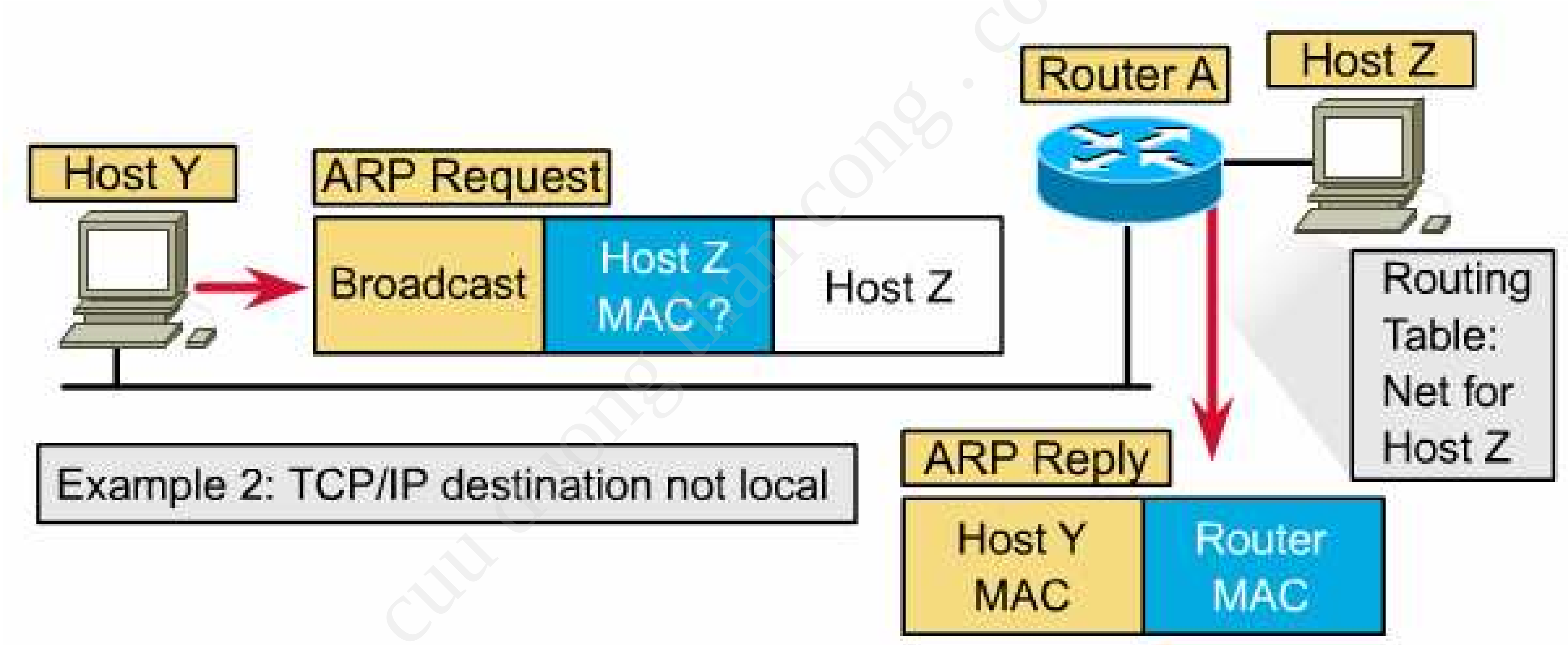
Proxy ARP

NETWORK TRAINING CENTER

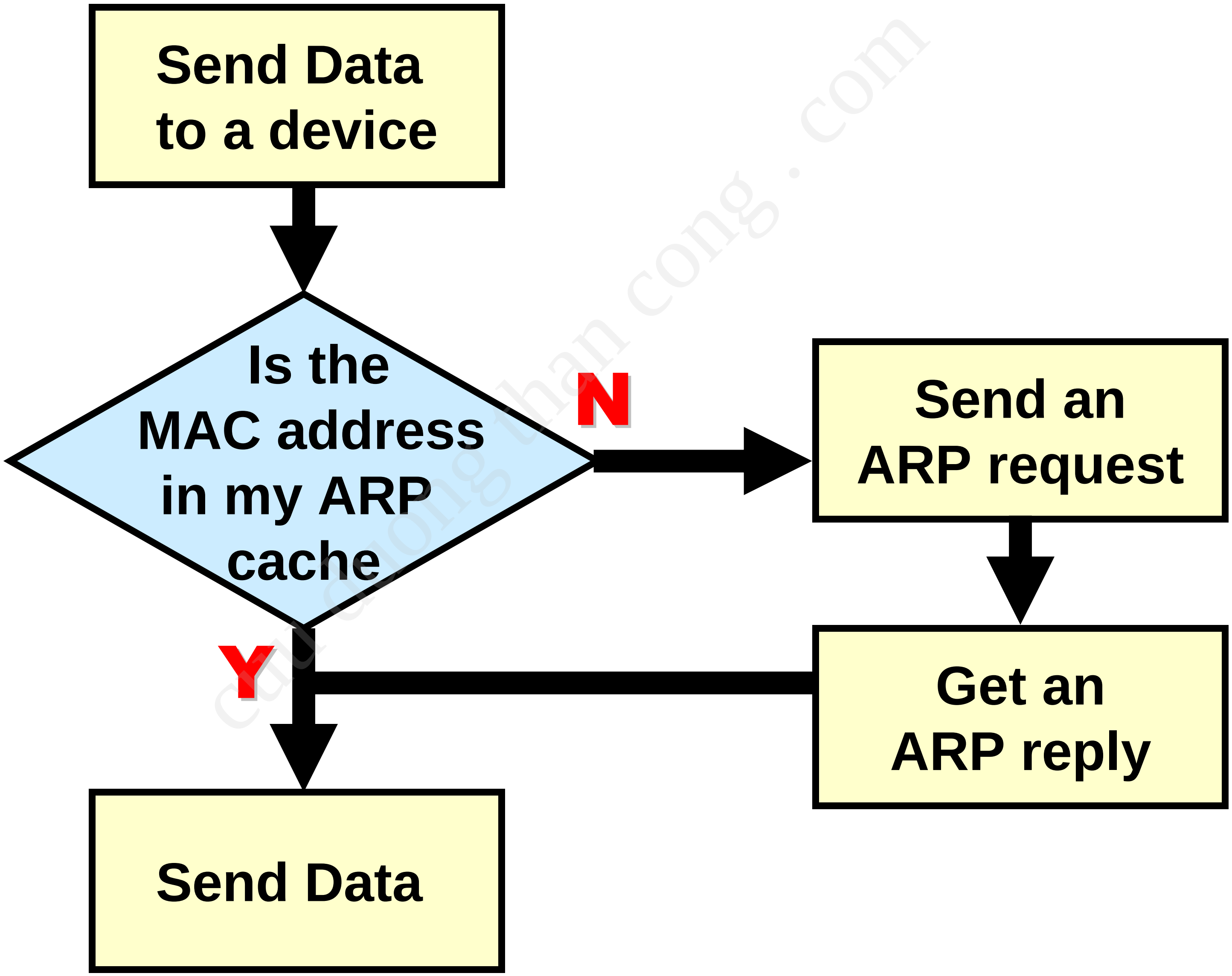


- Proxy ARP is a variation of the ARP.
- In the case the source host does not have a default gateway configured.

ARP: Destination not local



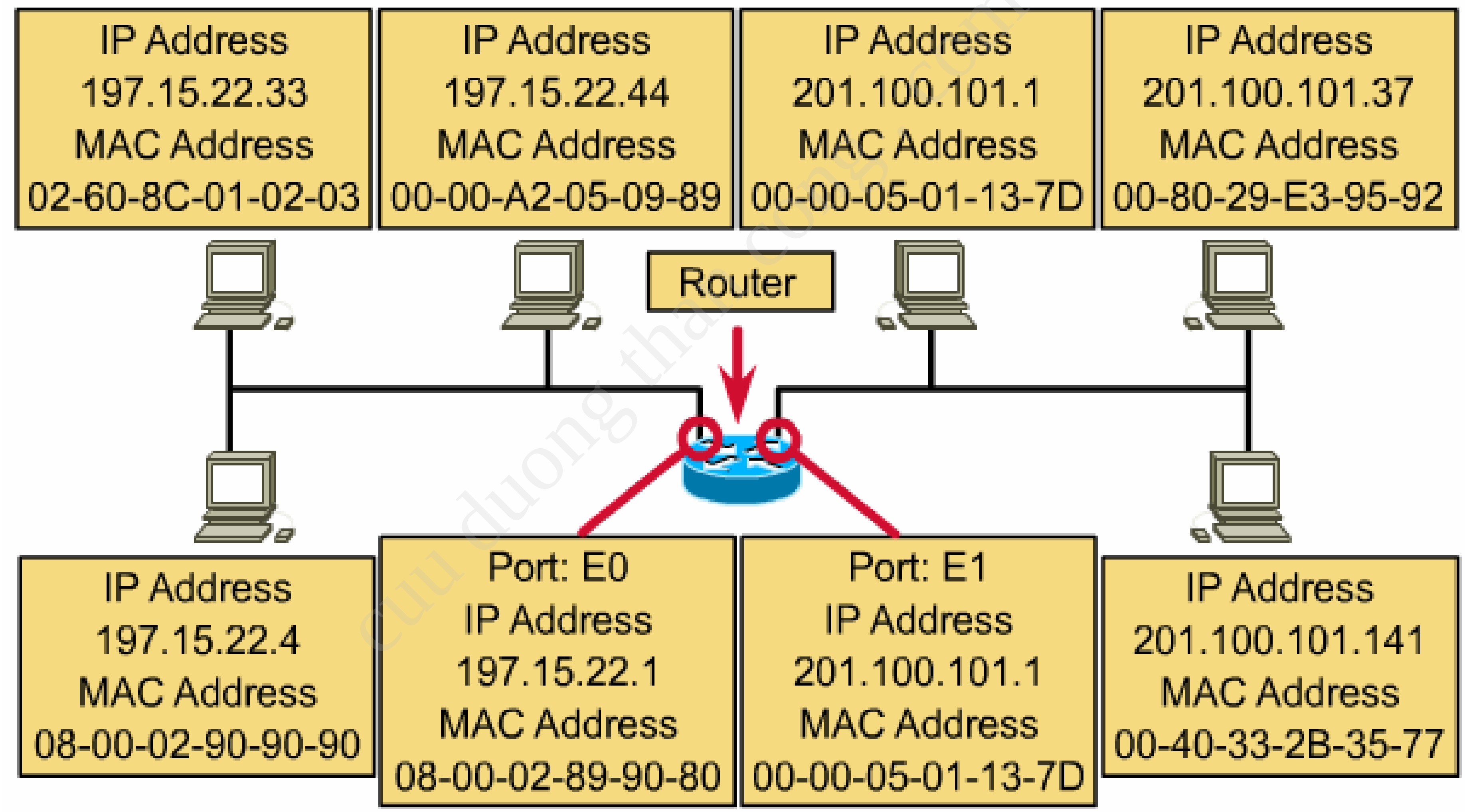
ARP Flowchart



ARP table in router

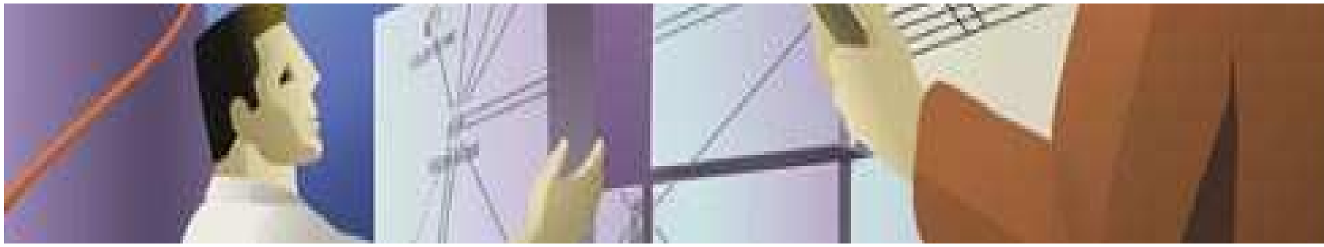
- The router interface connected to the network has an IP address for that network.
- Routers, just like every other device on the network, send and receive data on the network.
- If router connects to a LAN, it builds ARP tables that maps IP addresses to MAC addresses in that interface.

ARP table in routers and in hosts



Preparation for LAB

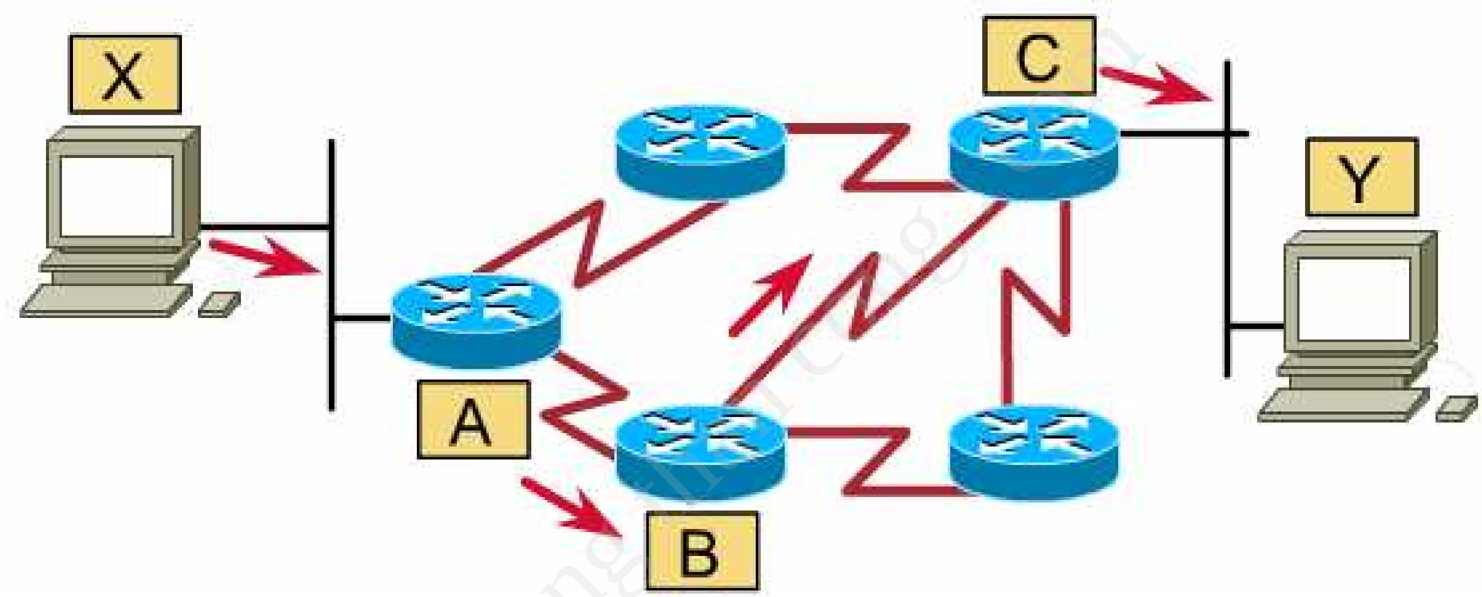
- Lab:
  - ARP and Network Analyzer (Ethereal)



ROUTED AND ROUTING PROTOCOLS

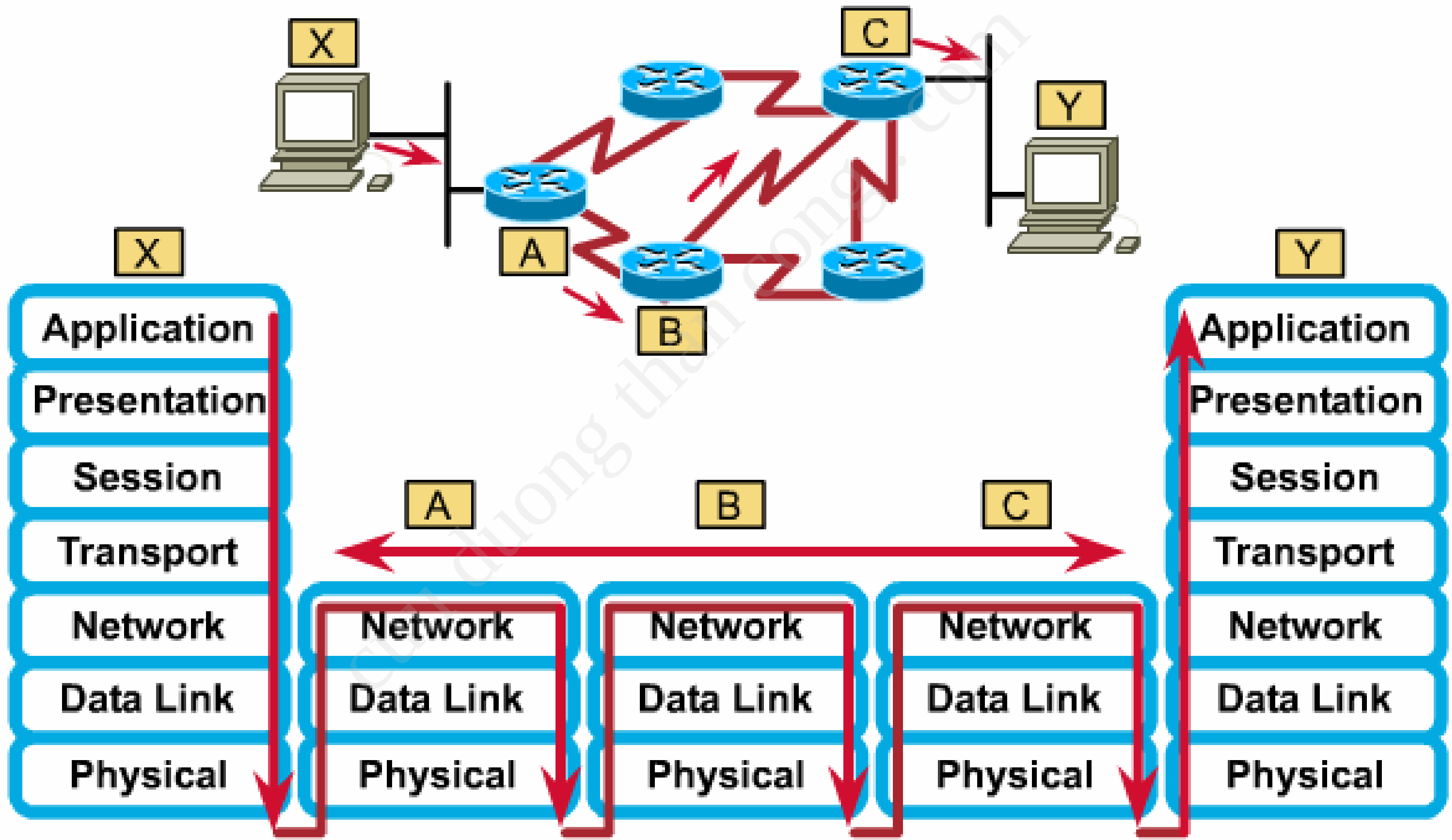
Network protocols

NETWORK TRAINING CENTER

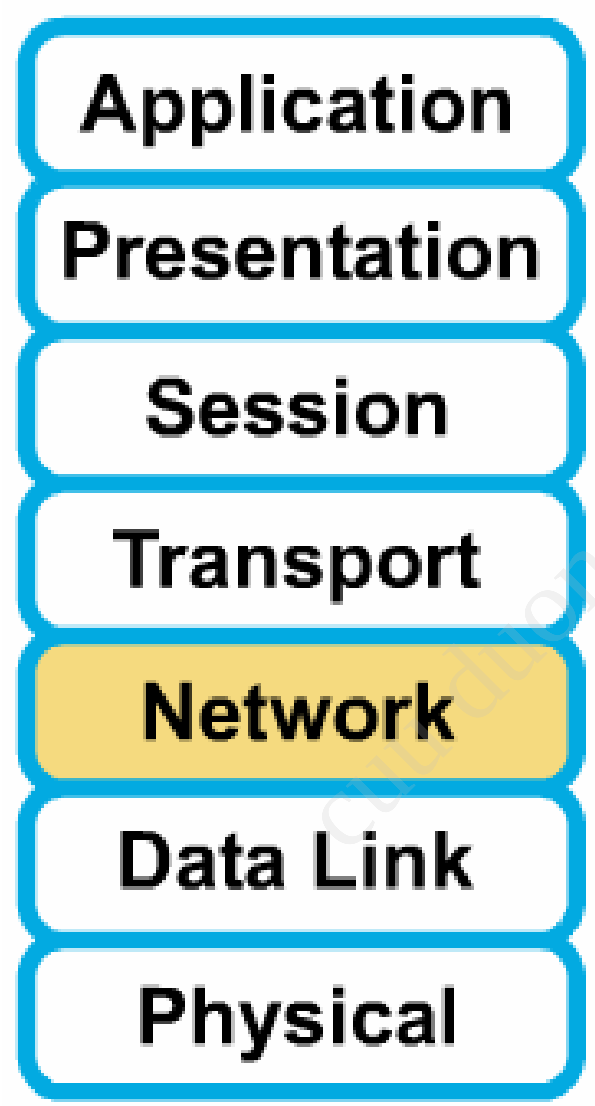


- In order to allow two host communicate together through internetwork, they need a same network protocol.
- Protocols are like languages.
- IP is a network layer protocol.

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.

Protocol addressing variations

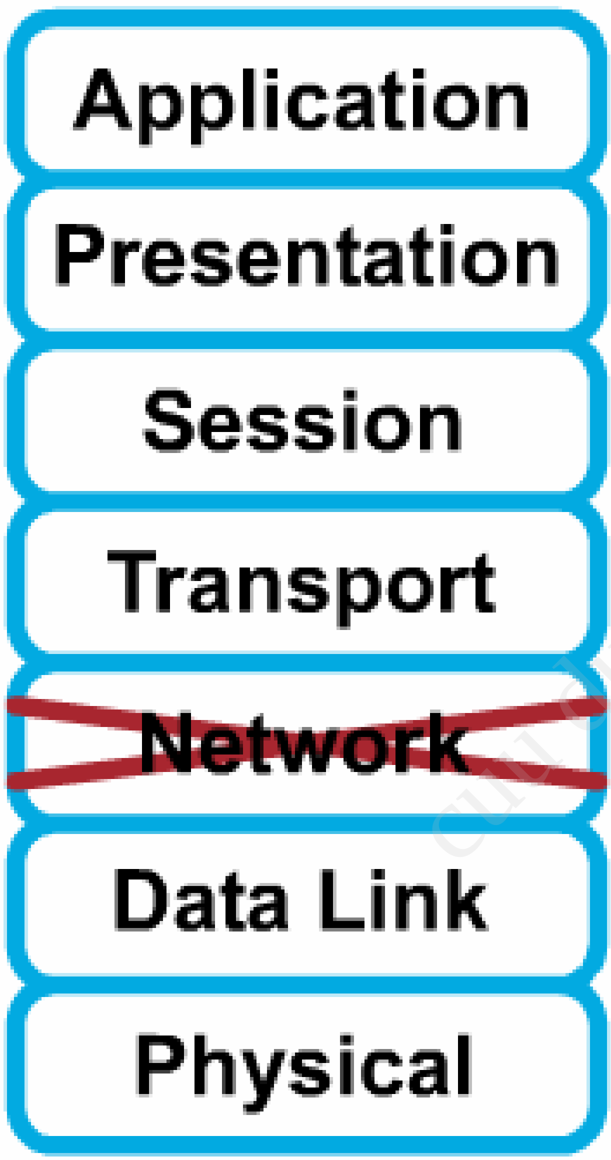
General Example	Network	Node
	1	1
TCP/IP Example	Network	Host
	10.	8.2.48
Novell IPX Example	Network	Node
	1aceb0b.	0000.0c00.6e25

(Mask 255.0.0.0)

Three important routed protocols

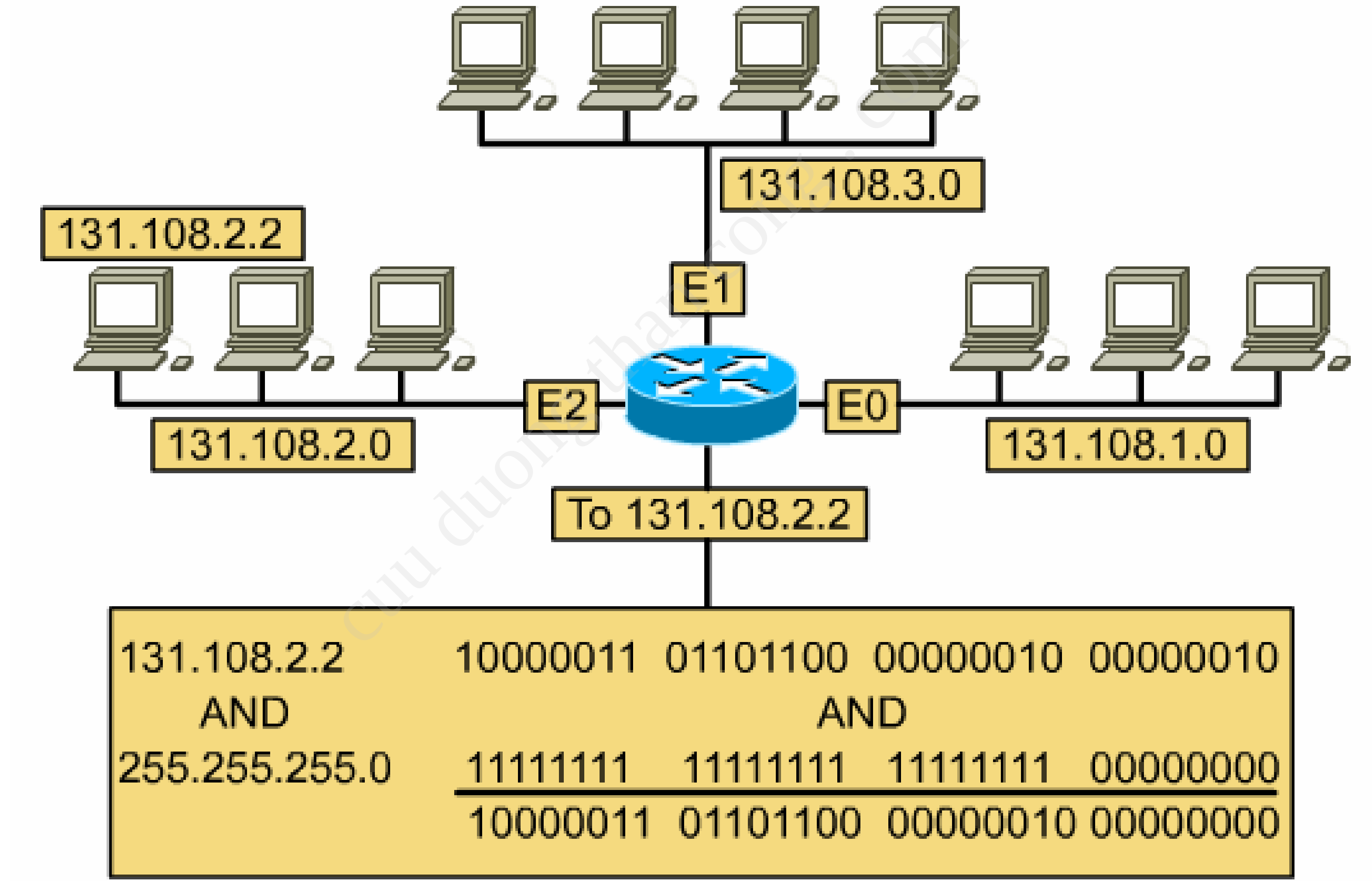
- TCP/IP: 04 bytes
  - Class A: 1 byte network + 3 bytes host
  - Class B: 2 bytes network + 2 bytes host
  - Class C: 3 bytes network + 1 byte host
- IPX/SPX: 10 bytes
  - 4 bytes network + 6 bytes host
- AppleTalk: 03 bytes
  - 2 bytes network + 1 byte host

Non-routable protocol

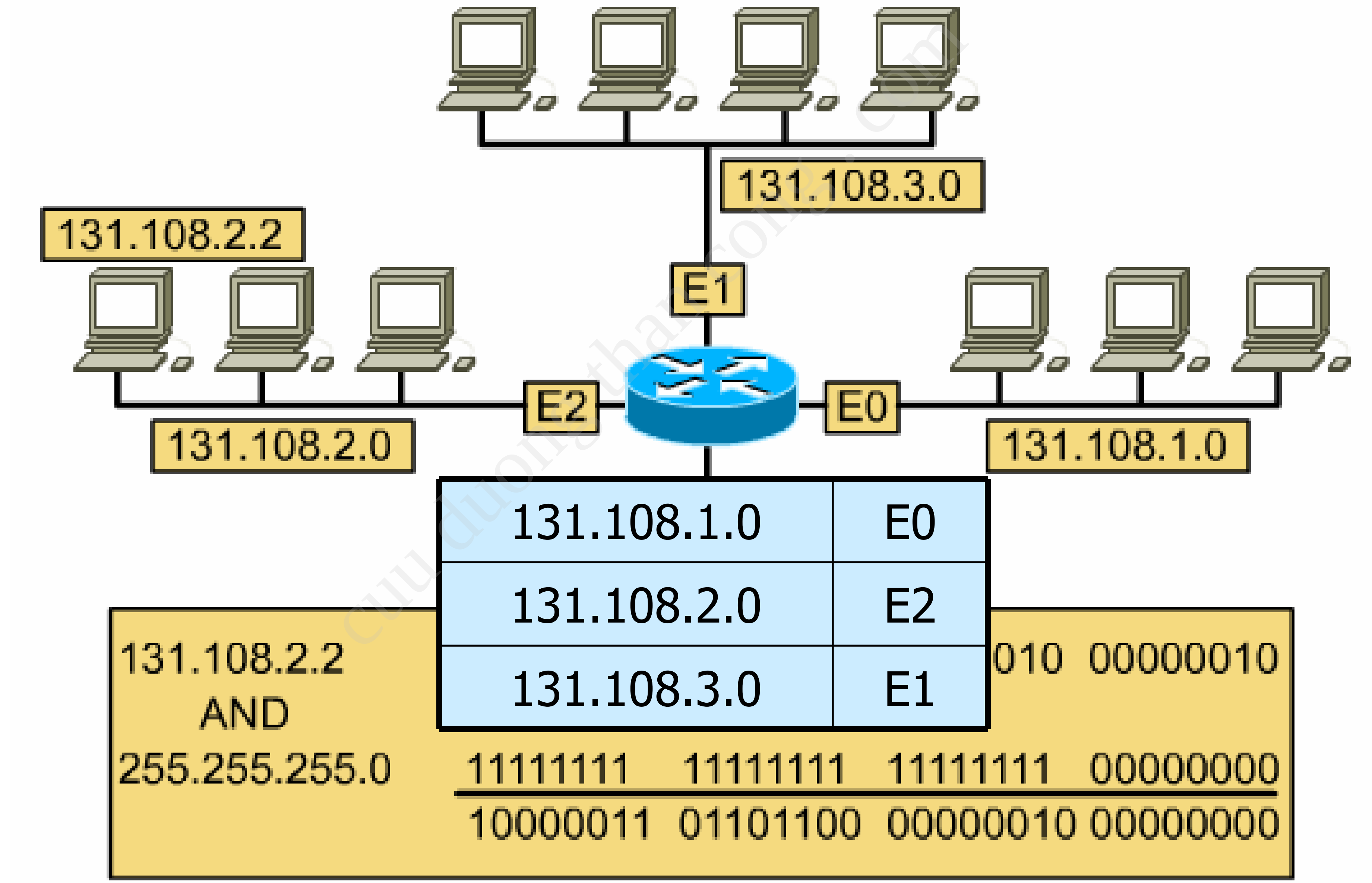


- Non-routable protocols are protocols that do not support Layer 3.
- The most common of these non-routable protocols is NetBEUI.
- NetBEUI is a small, fast, and efficient protocol that is limited to running on one segment.

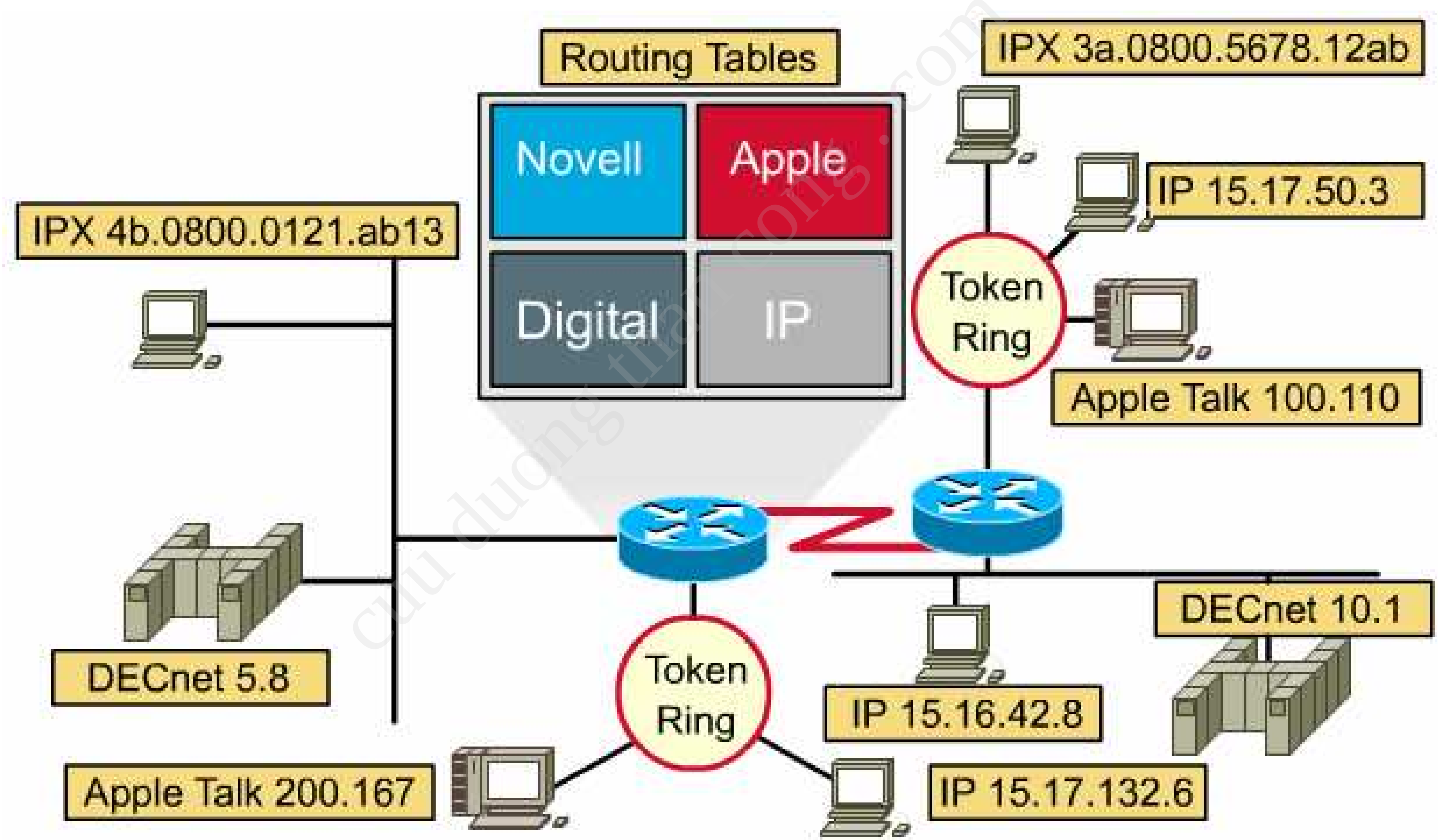
Addressing of a routable protocol



Routing table



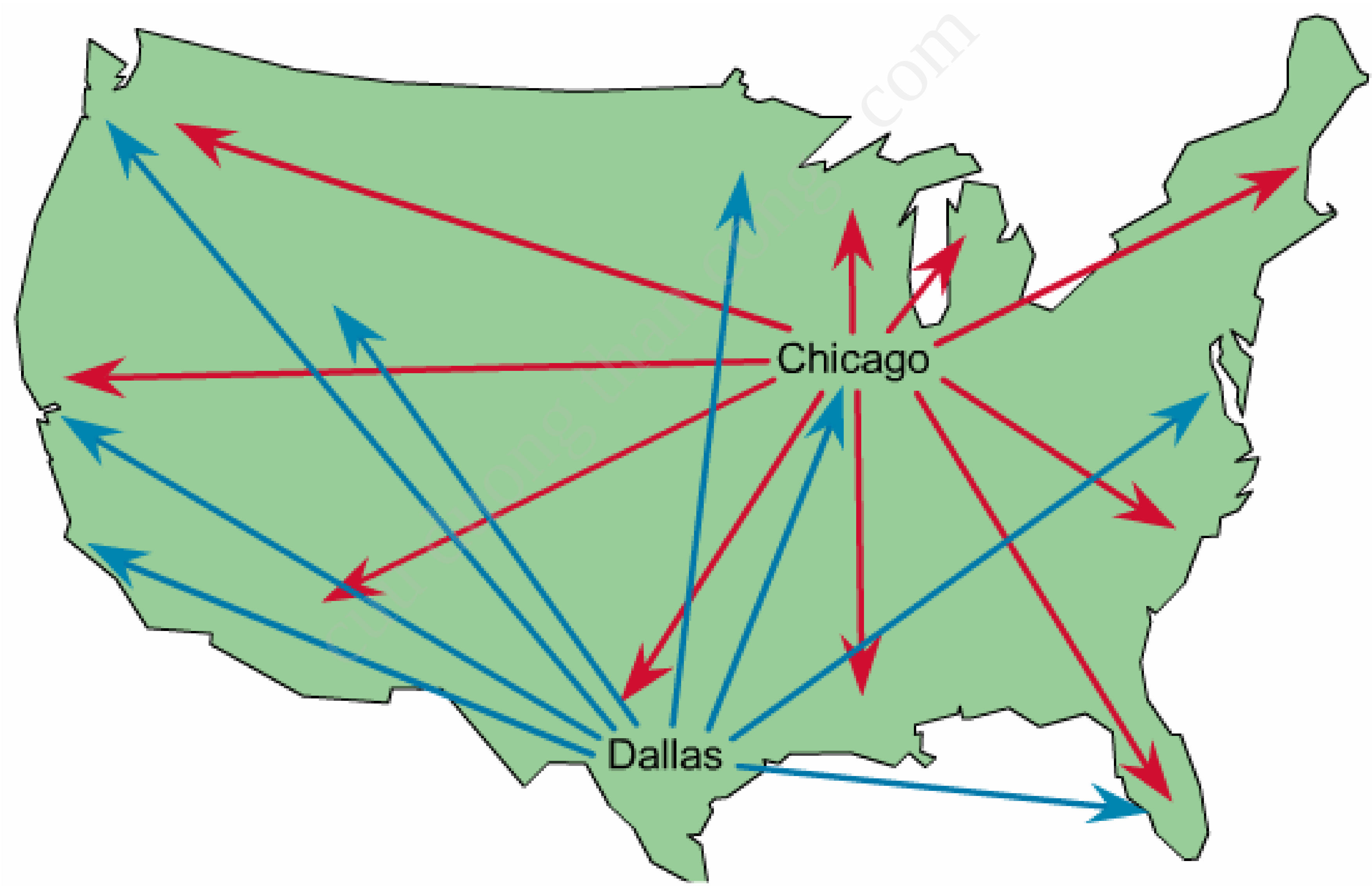
Multi-protocol routing



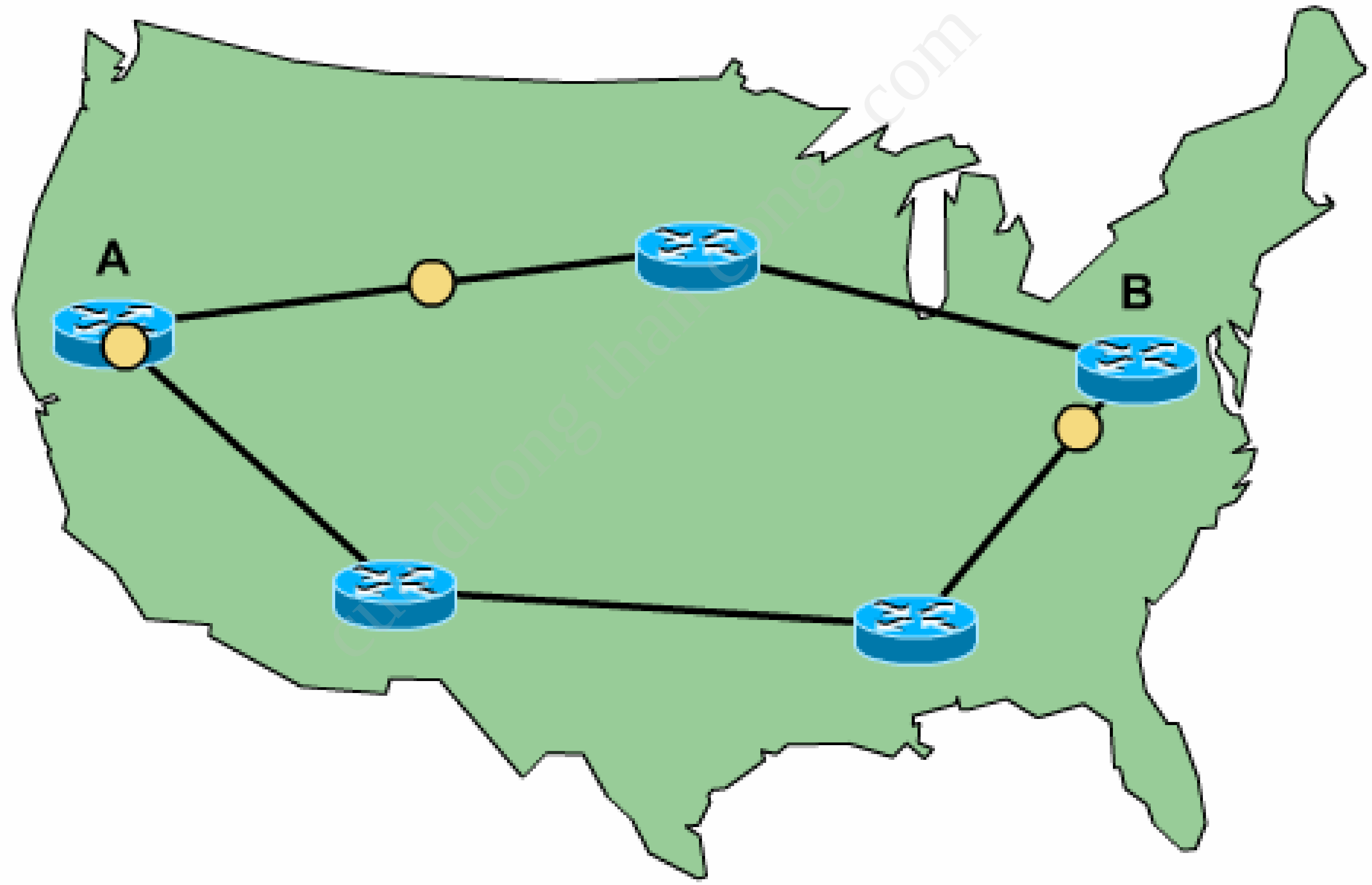
Classification #1: Static and Dynamic

- 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 routes



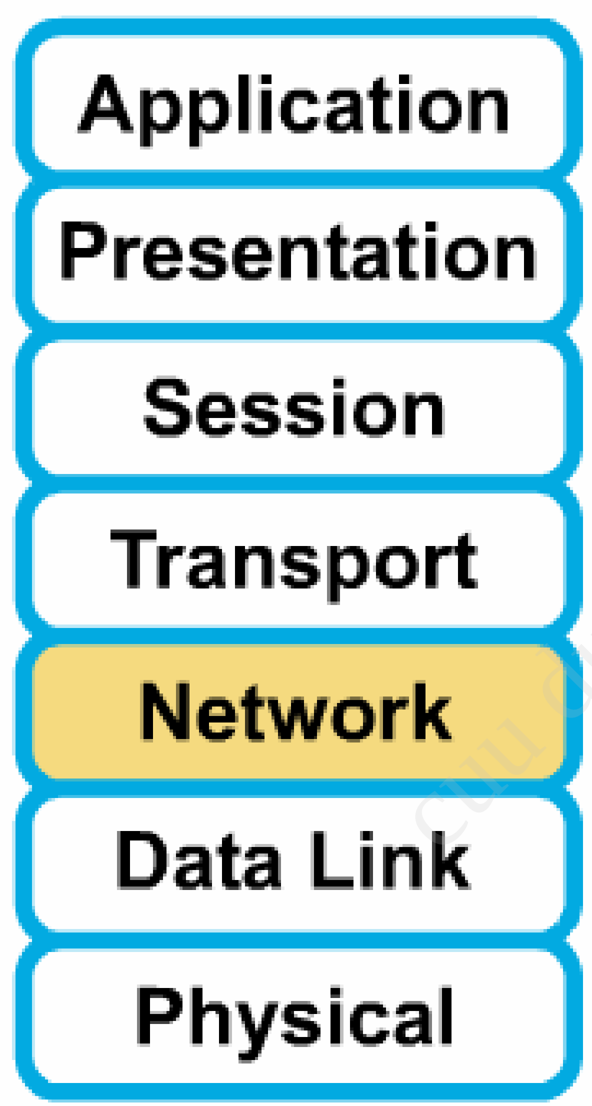
Dynamic routes



Static vs. dynamic routes

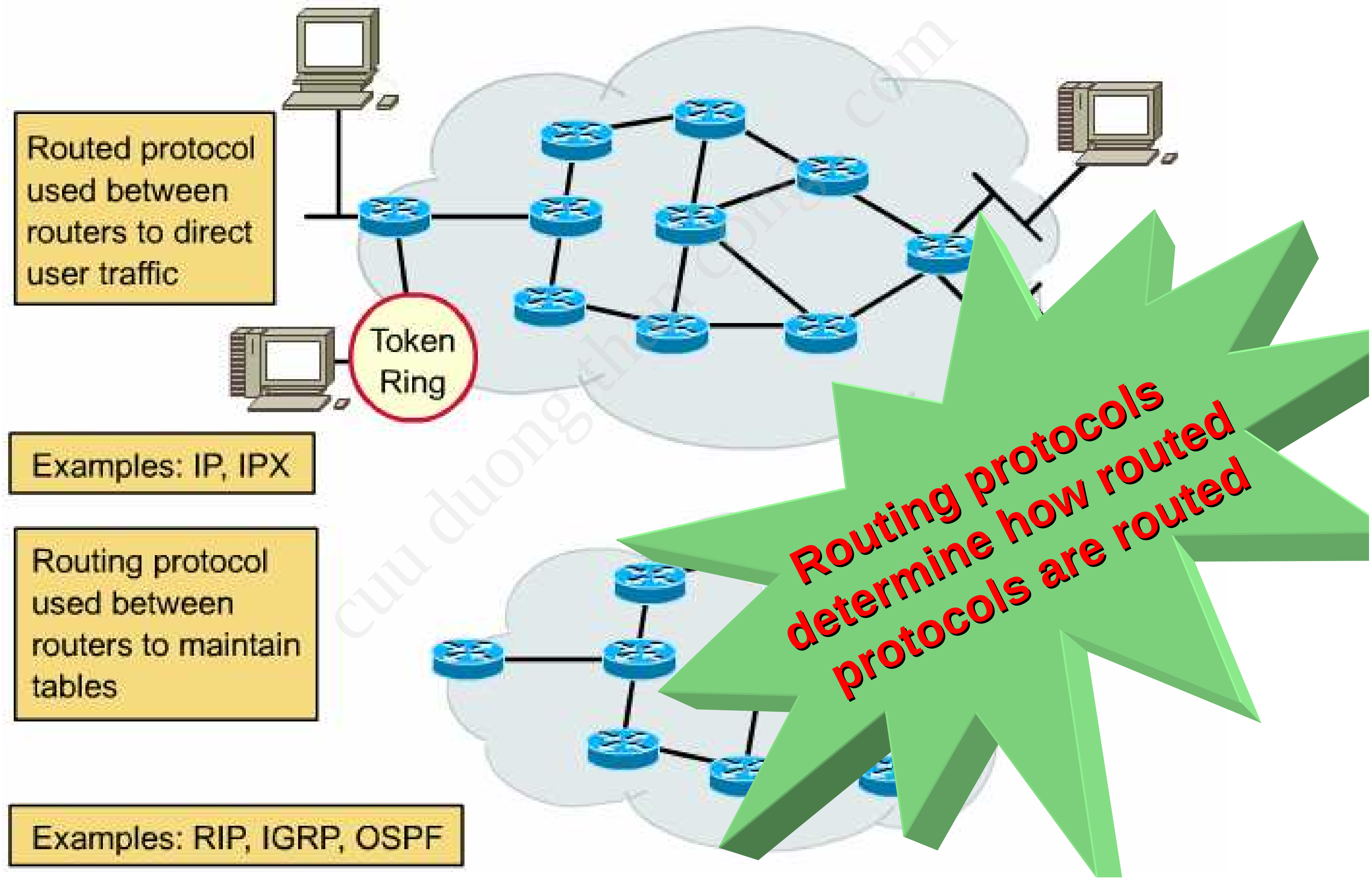
- Static routes:
  - For hiding parts of an internetwork.
  - To test a particular link in a network.
  - For maintaining routing tables whenever there is only one path to a destination network.
- Dynamic routes:
  - Maintenance of routing table.
  - Timely distribution of information in the form of 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.
- Routing protocols enable routers that are connected to create a map, internally, of other routers in the network or on the Internet.

Routed vs. Routing protocol

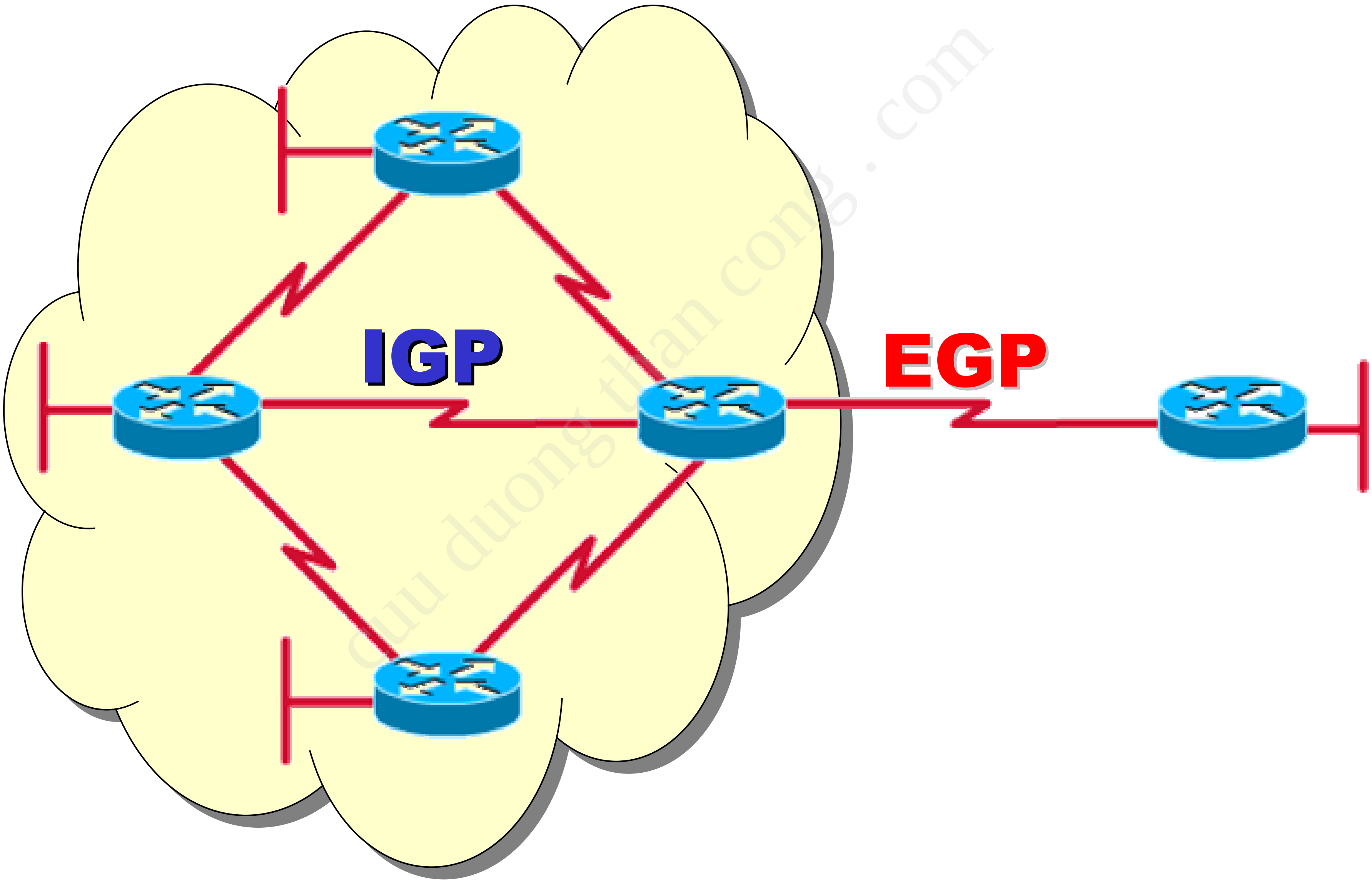


Classification #2: IGP and EGP

- 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

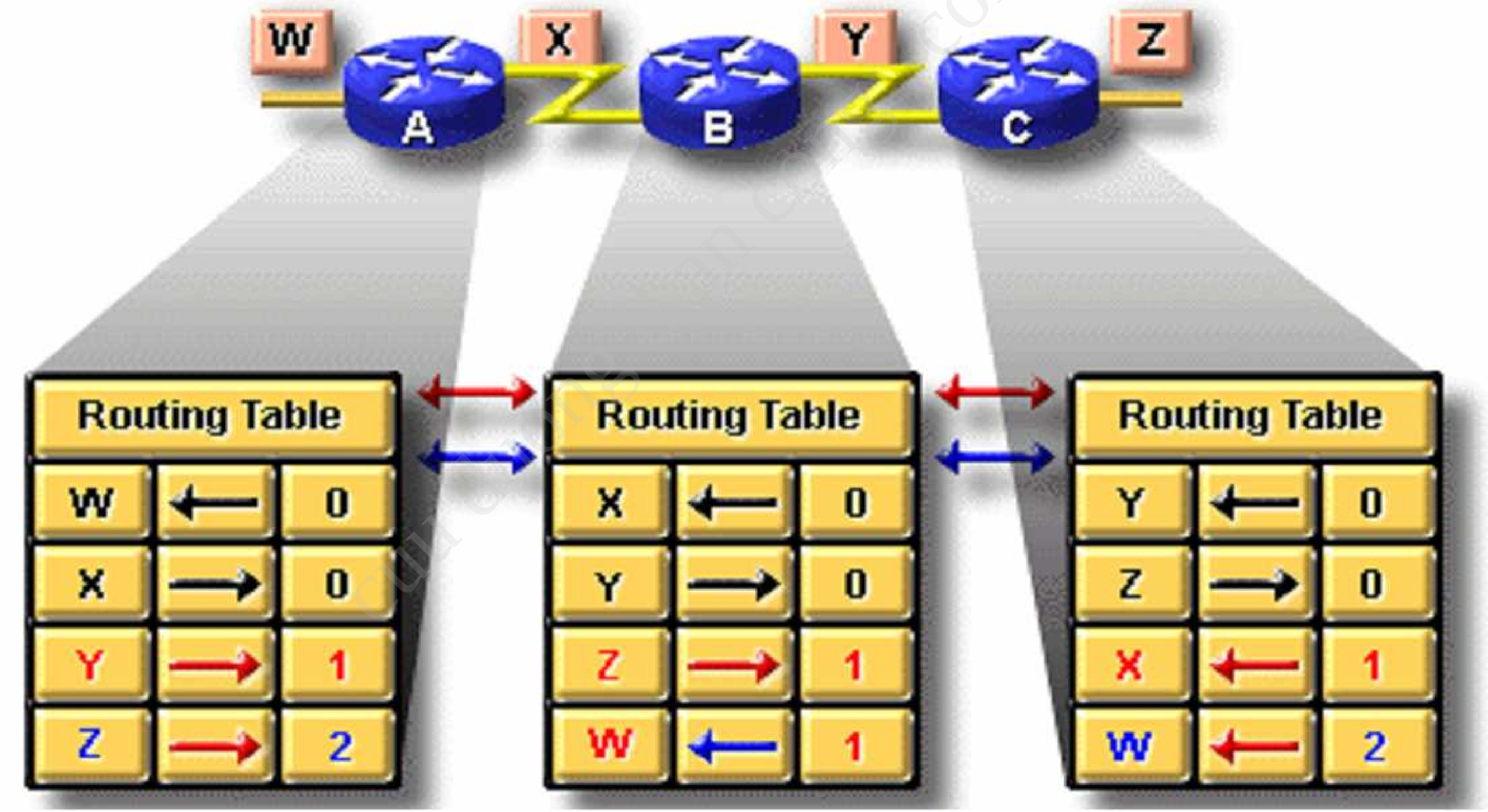
NETWORK TRAINING CENTER



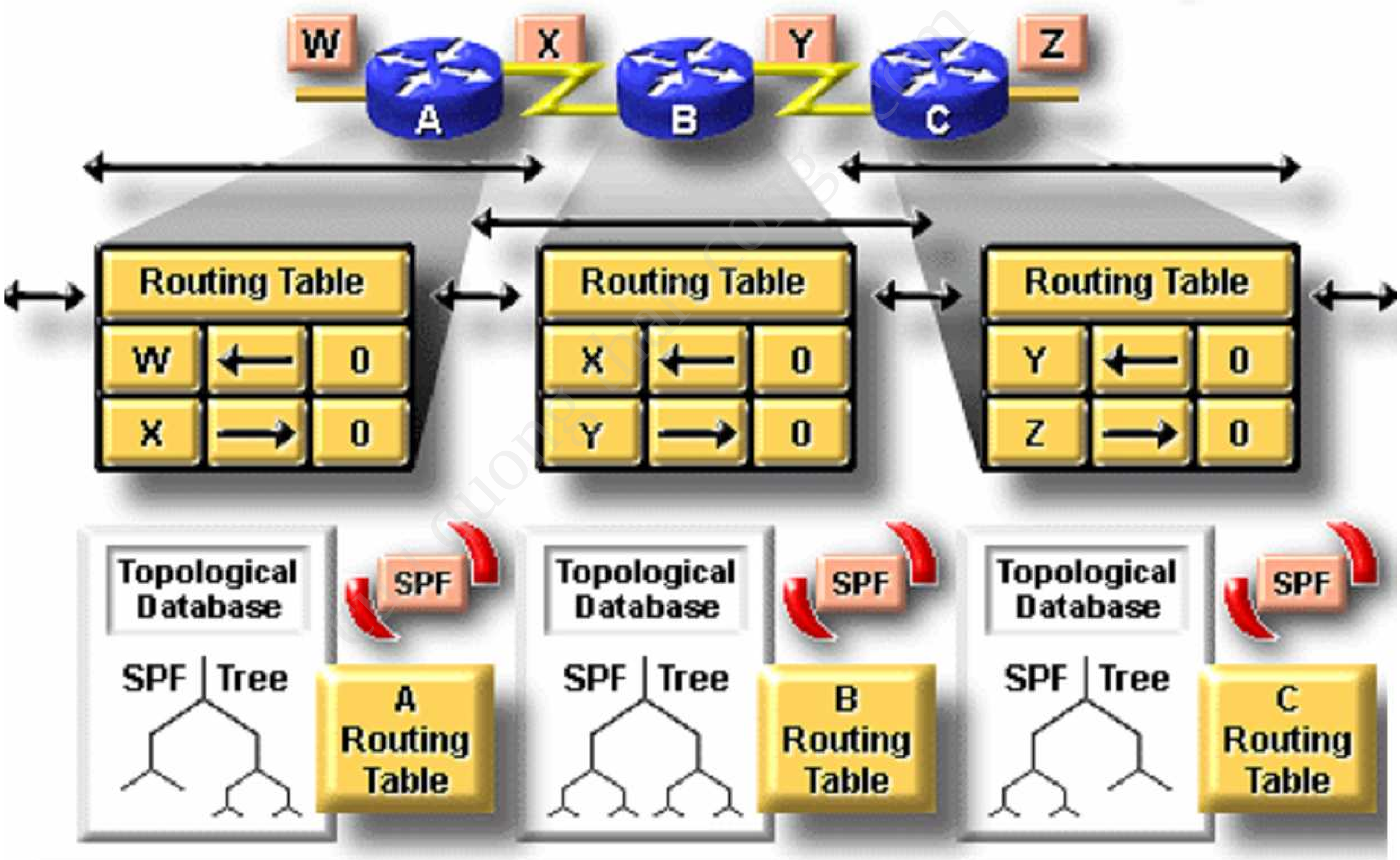
Classification #3: DVP and LSP

- 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

- 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.

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.

Q&A

CCNA Semester 1

NETWORK TRAINING CENTER

The Cisco Certified Network Associate Curriculum

Chapter 11

TCP/IP TRANSPORT and APPLICATION LAYER

Objectives

- *Describe the functions of the TCP/IP transport layer.*
- *Describe the processes of establishing a connection between peer systems.*
- *Describe flow control.*
- *Describe windowing.*
- *Describe acknowledgment.*
- *Identify and describe transport layer protocols.*
- *Describe TCP and UDP header formats.*
- *Describe TCP and UDP port numbers.*
- *List the major protocols of the TCP/IP application layer.*
- *Provide a brief description of the features and operation of well-known TCP/IP applications.*

Table of Content

NETWORK TRAINING CENTER

TCP/IP TRANSPORT LAYER

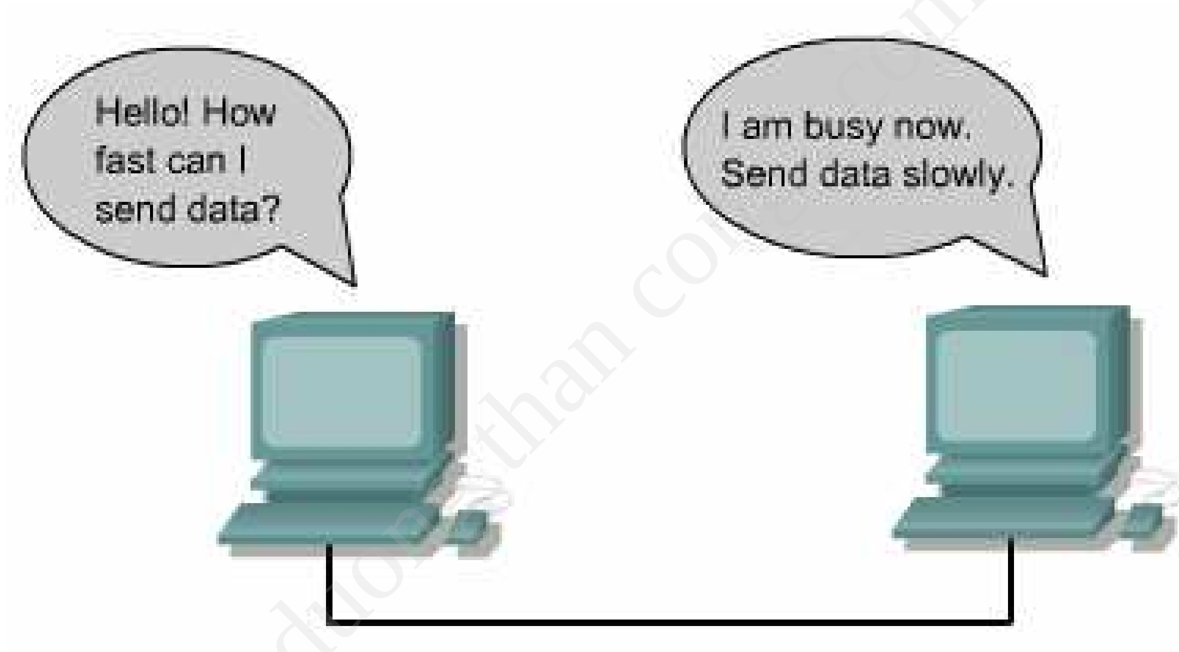
4

Introduction to transport layer

- The primary duties of the transport layer are to transport and regulate the flow of information from the source to the destination, reliably and accurately.
- The Transport layer provides the following basic services:
  - Segmentation of upper-layer application data
  - Establishment of end-to-end operations
  - Transport of segments from one end host to another end host
  - Flow control provided by sliding windows
  - Reliability provided by sequence numbers and acknowledgments
- TCP/IP is combination of two individual protocols, TCP and IP

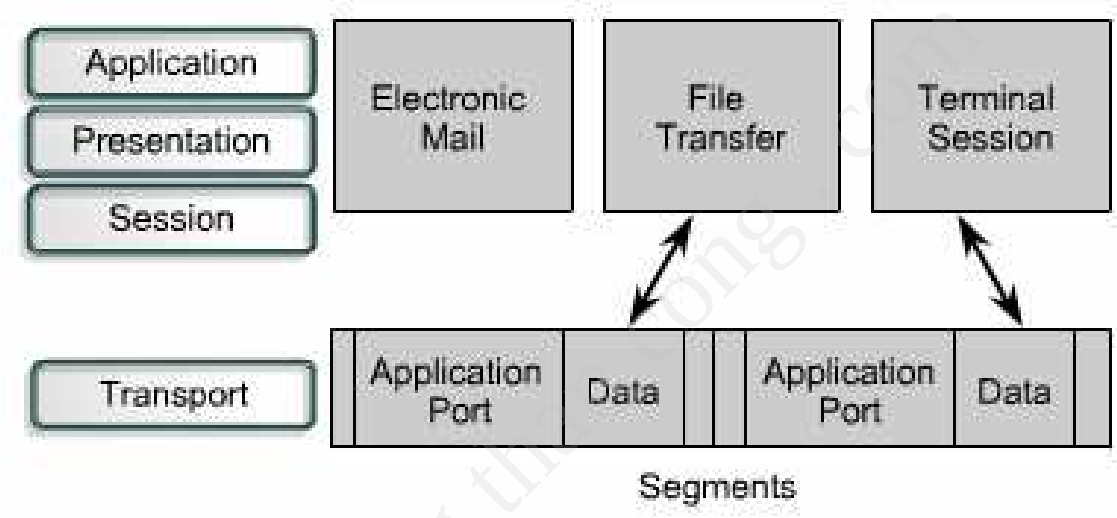
Flow control

NETWORK TRAINING CENTER



- Ensure that segments delivered will be acknowledge to the sender
- Provide for retransmission of any segments that are not acknowledge
- Put segments back into their correct sequence at the destination
- Provide congestion avoidance and control

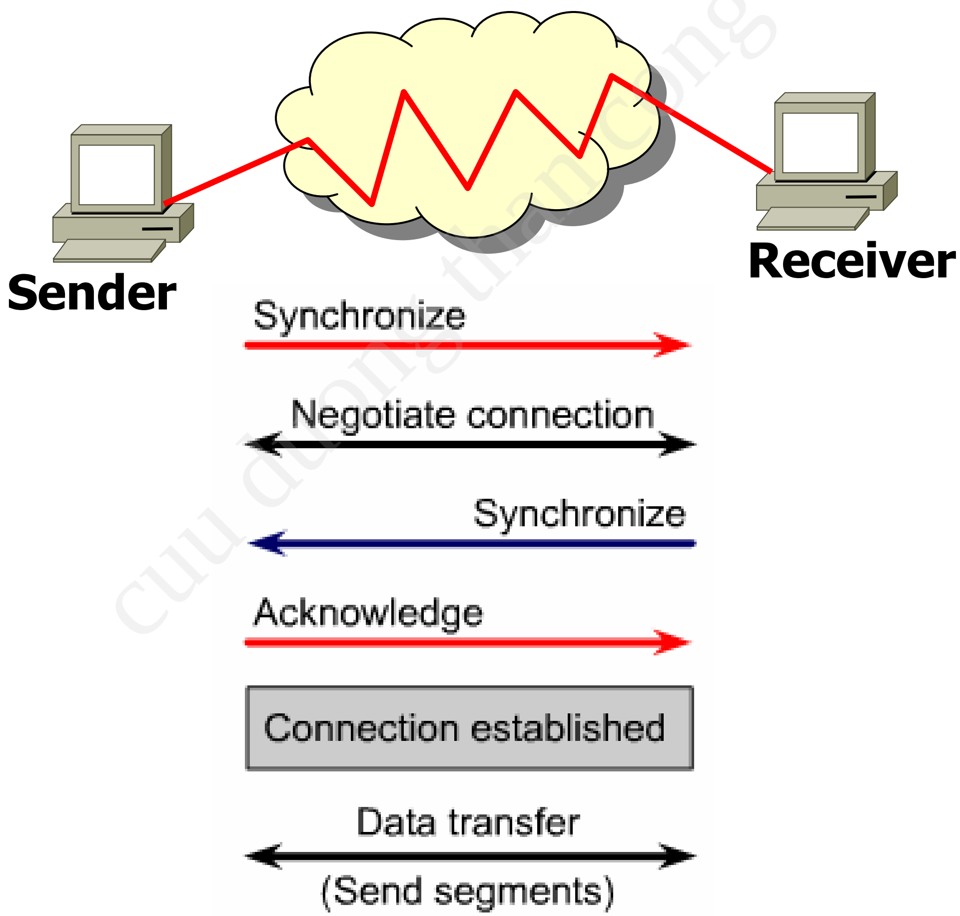
Session establishment, maintenance, and termination overview



Multiple applications can share the same transport connection in the OSI model. This is referred to as the multiplexing of upper layer conversations

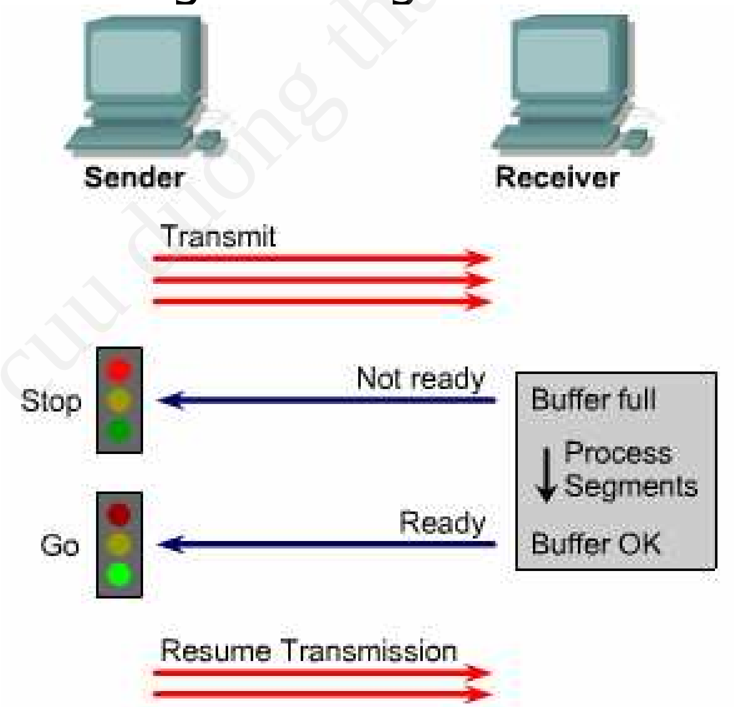
Session establishment, maintenance, and termination overview

- One function of the transport layer is to establish a connection-oriented session with its peer system.

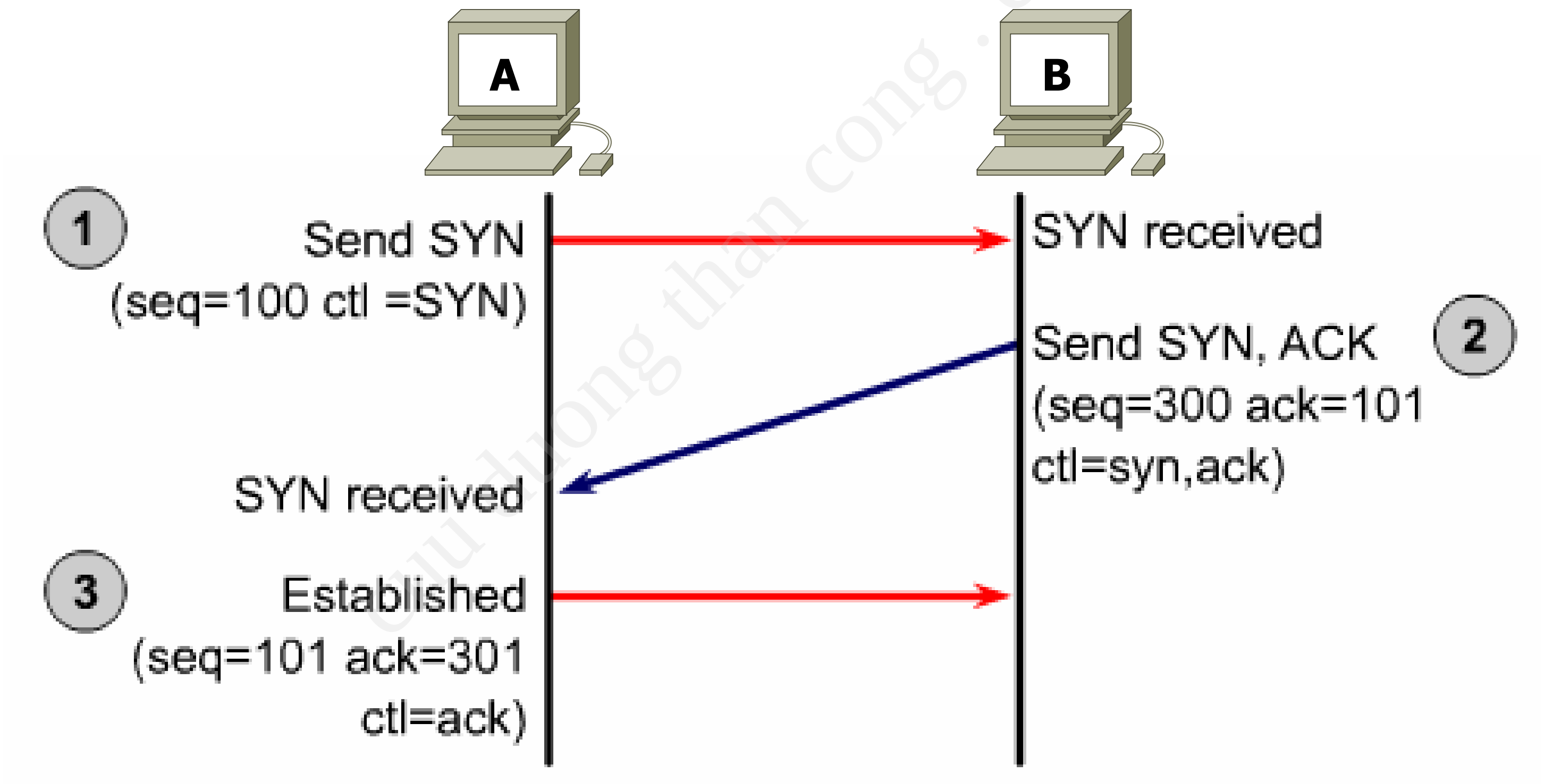


Session establishment, maintenance, and termination overview

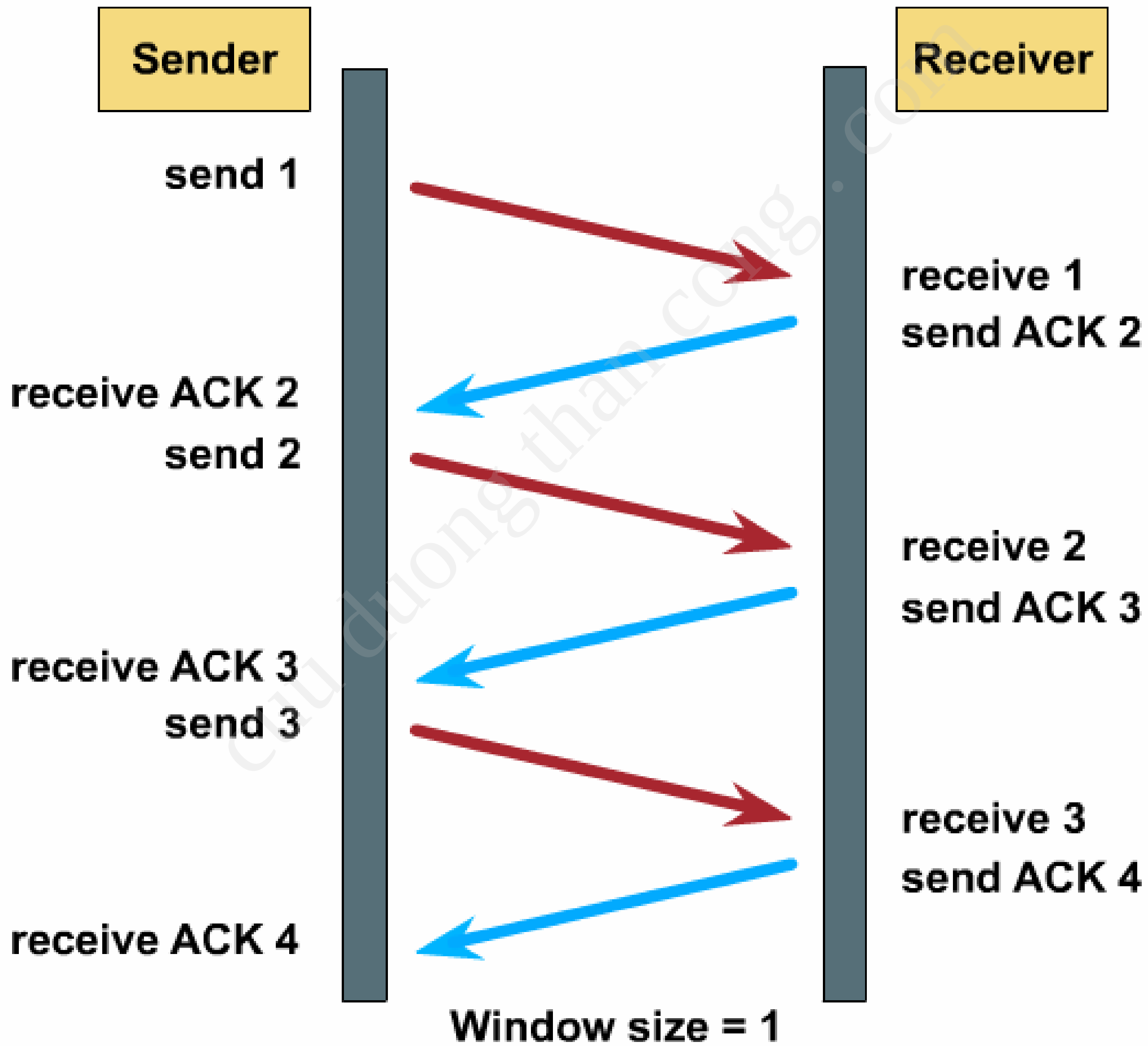
- Congestion can occur for two reasons:
  - First, a high-speed computer might generate traffic faster than a network can transfer it.
  - Second, if many computers simultaneously need to send datagrams to a single destination, that destination can experience congestion, although no single source caused the problem.



TCP: Three way handshaking

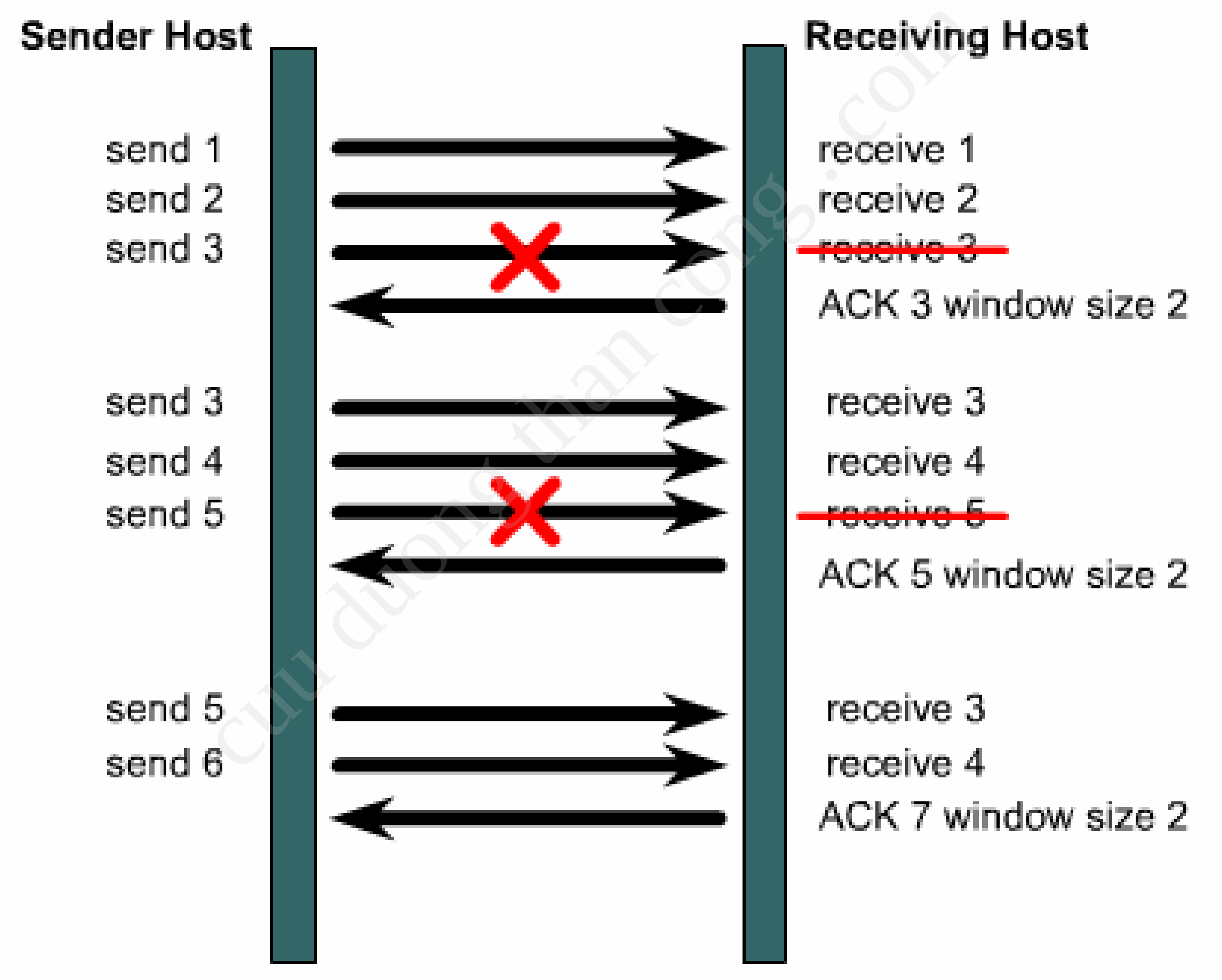


TCP: Window and Acknowledgment

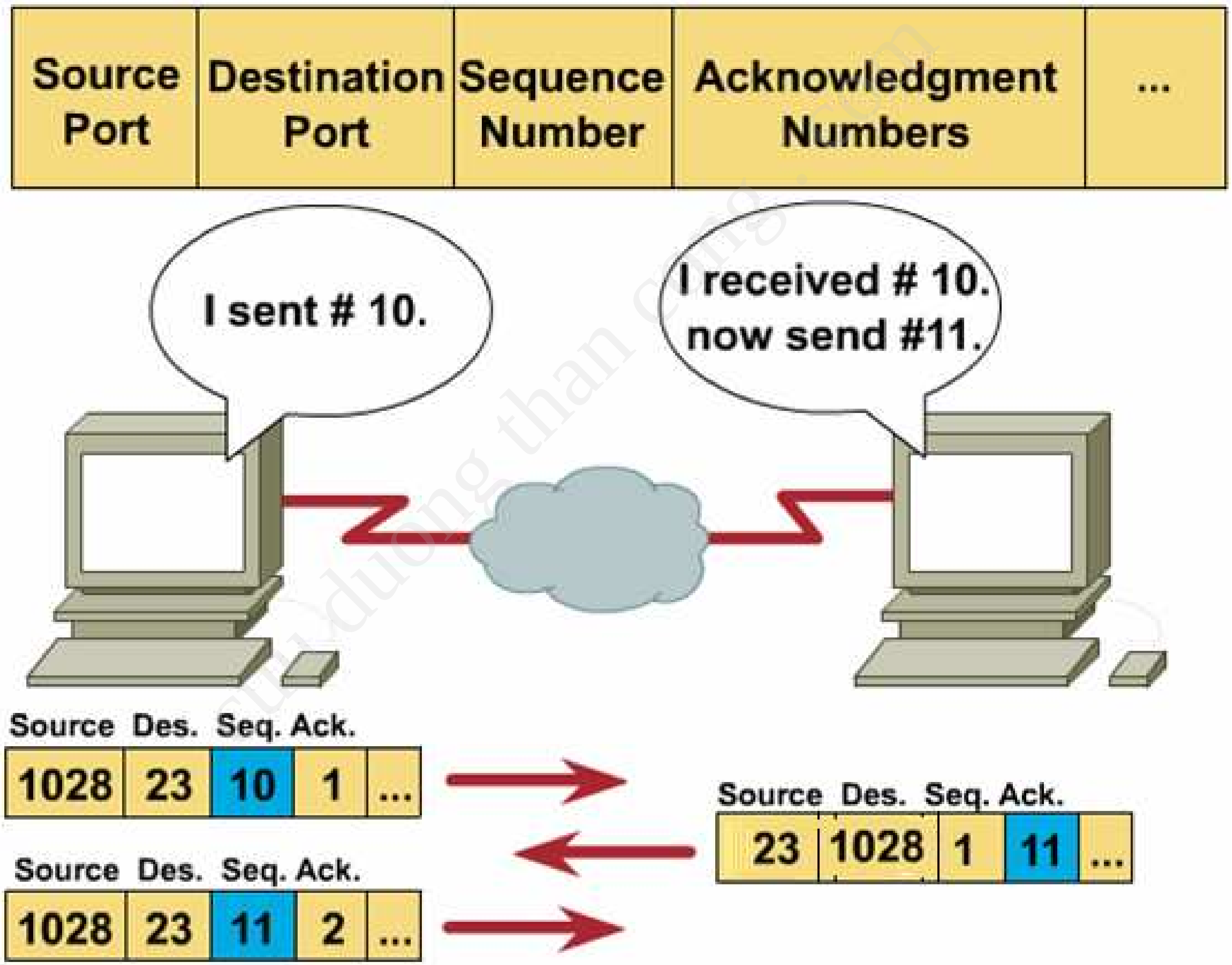


TCP: Sliding window and Acknowledgment

NETWORK TRAINING CENTER



TCP: Sequence and acknowledgment



Transport Layer: TCP

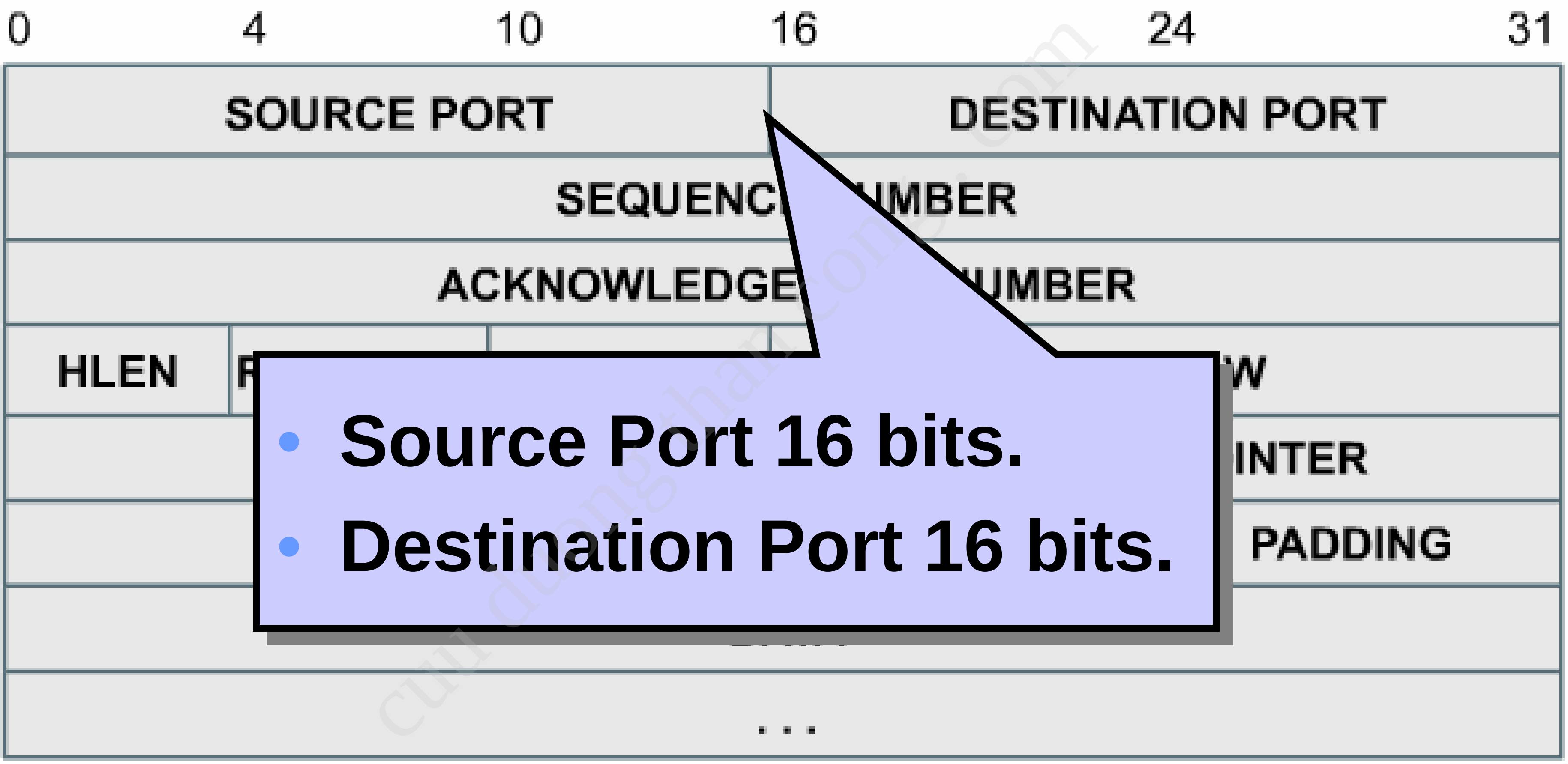
- These are its characteristics:
  - Connection-oriented.
  - Supplies a virtual circuit between both ends
  - Breaking outgoing messages into segments and reassembles messages at the destination.
  - Resends anything not received by acknowledgement.
  - Flow control: Windowing.
- The protocols that use TCP include: FTP, HTTP SMTP, Telnet.

RFC-761

TCP Header format

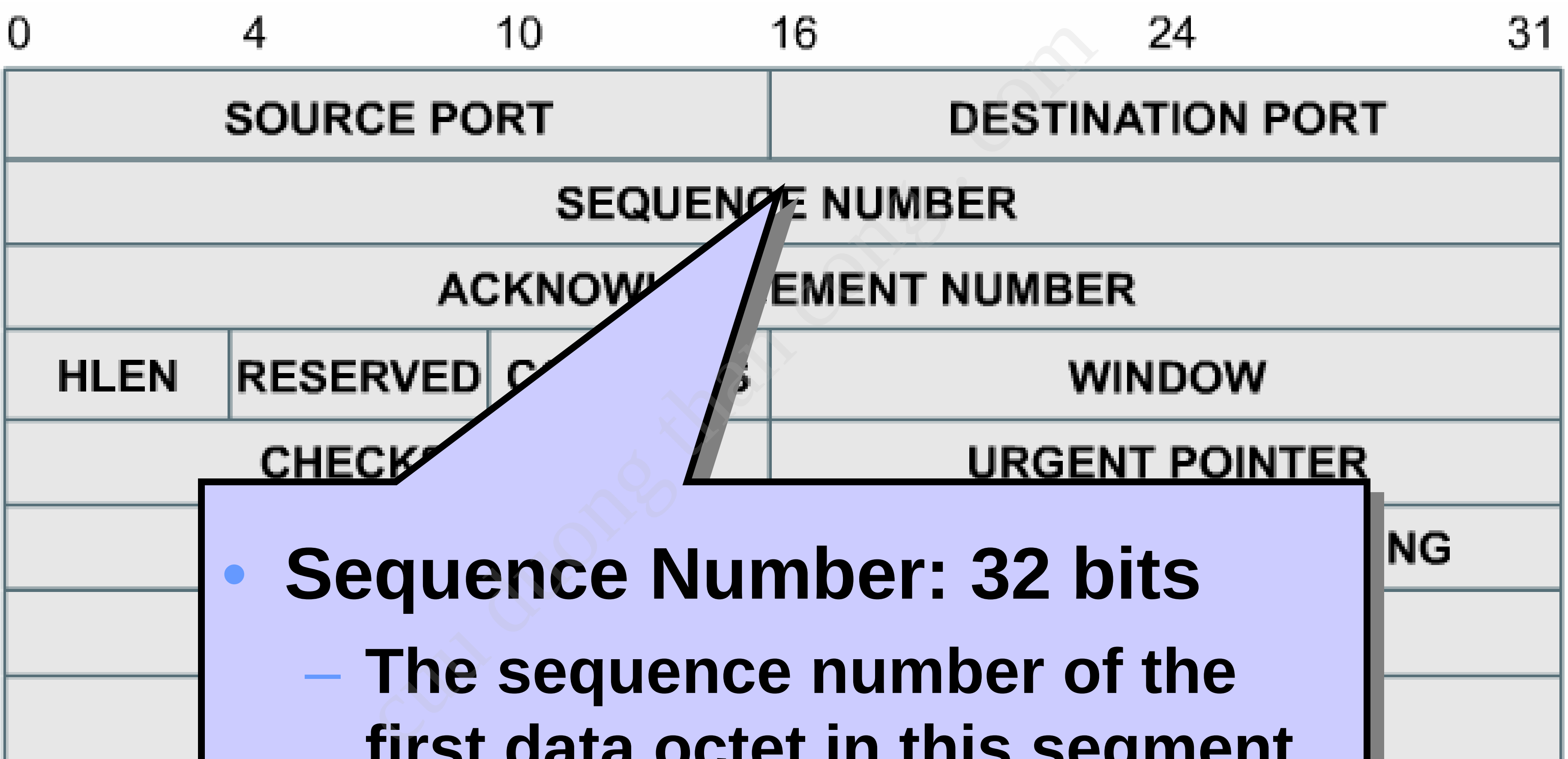
0	4	10	16	24	31
SOURCE PORT			DESTINATION PORT		
SEQUENCE NUMBER					
ACKNOWLEDGEMENT NUMBER					
HLEN	RESERVED	CODE BITS	WINDOW		
CHECKSUM			URGENT POINTER		
OPTIONS (IF ANY)				PADDING	
DATA					
. . .					

TCP Header format: Port number



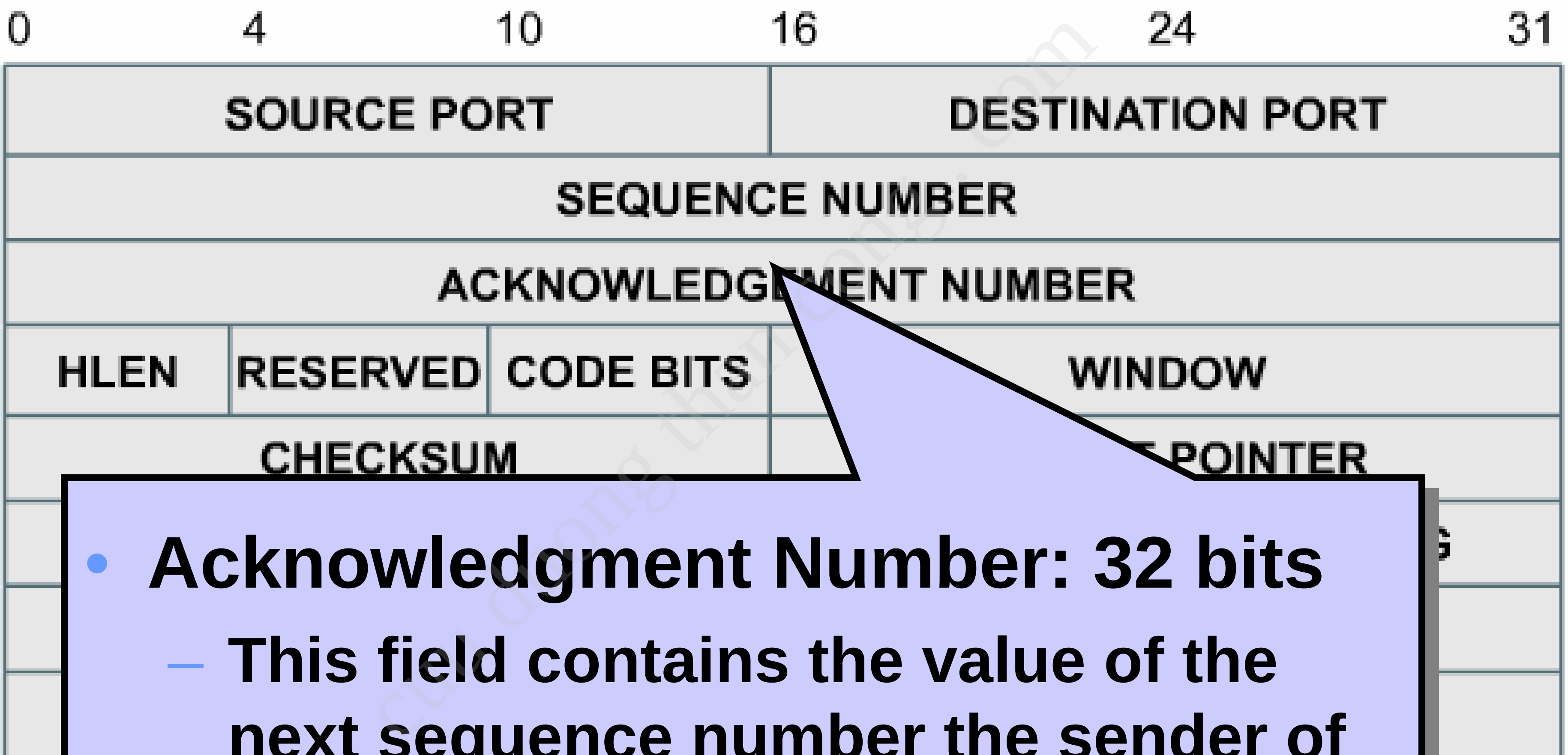
- Source Port 16 bits.
- Destination Port 16 bits.

TCP Header format: Sequence



- **Sequence Number: 32 bits**
  - **The sequence number of the first data octet in this segment (except when SYN is present).**

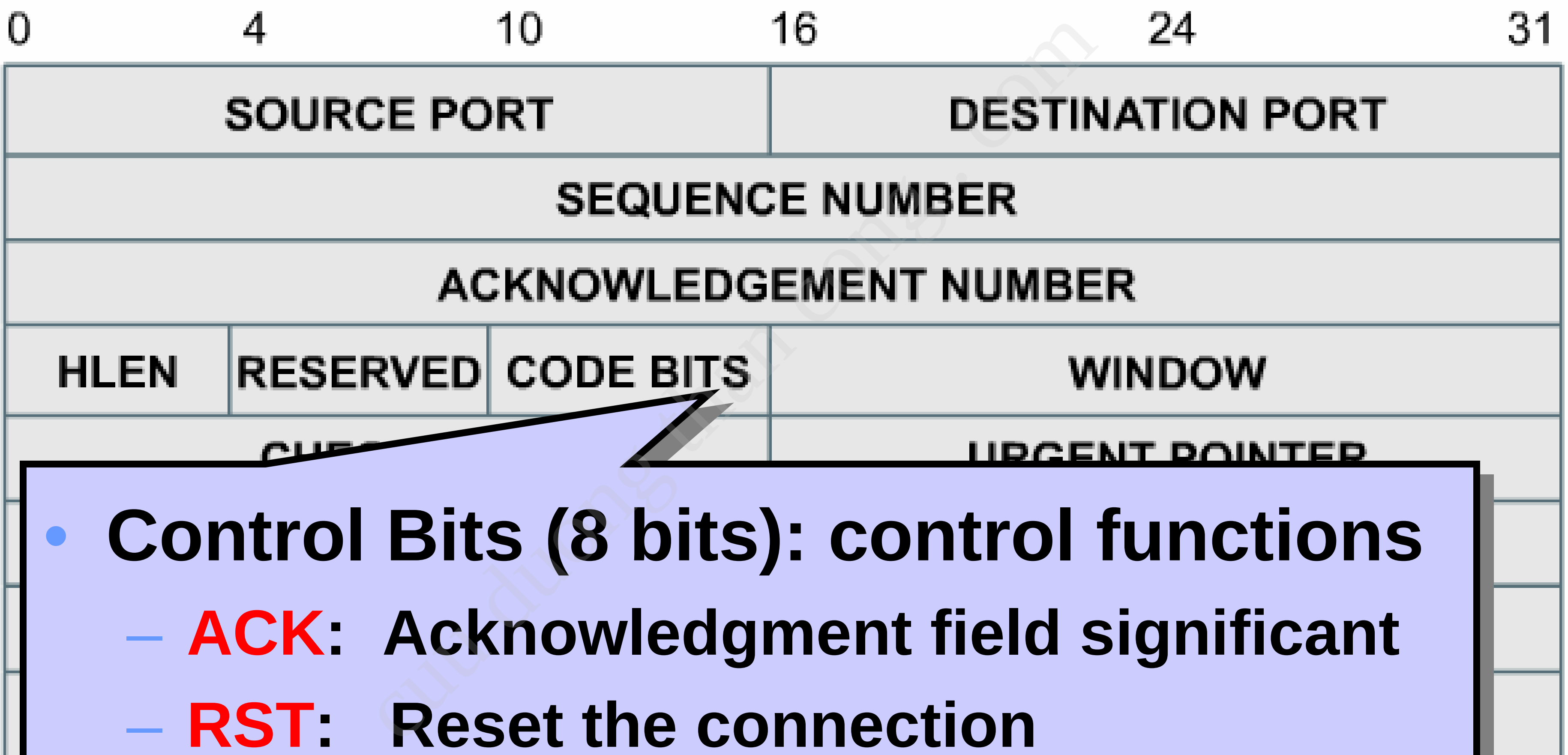
TCP Header format: Acknowledgment



- **Acknowledgment Number: 32 bits**
  - **This field contains the value of the next sequence number the sender of the segment is expecting to receive.**

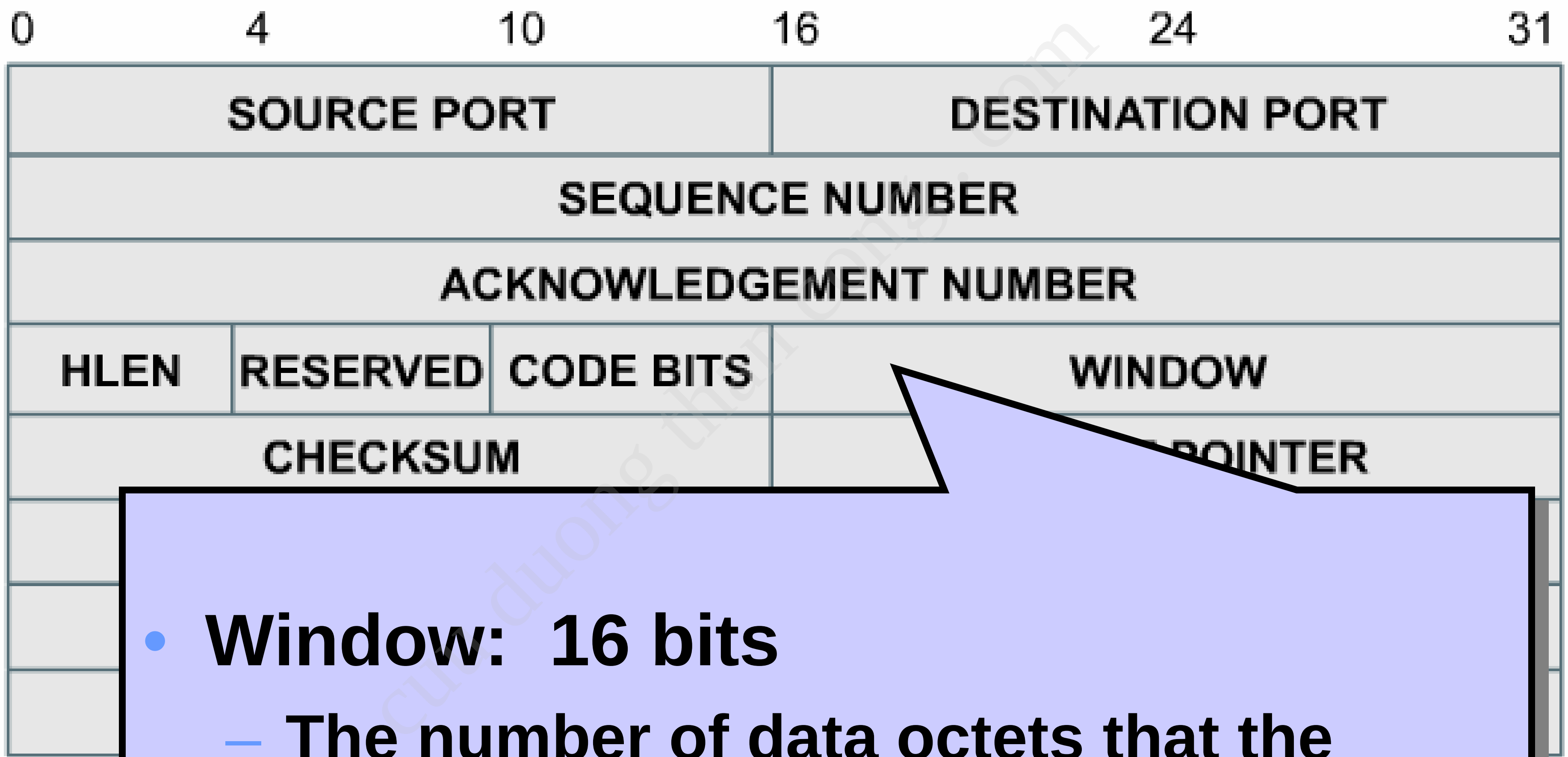
TCP Header format: Code bits

NETWORK TRAINING CENTER



- **Control Bits (8 bits): control functions**
  - **ACK**: Acknowledgment field significant
  - **RST**: Reset the connection
  - **SYN**: Synchronize sequence numbers
  - **FIN**: No more data from sender

TCP Header format: Window



- **Window: 16 bits**
  - **The number of data octets that the sender is willing to accept.**

Transport Layer: UDP

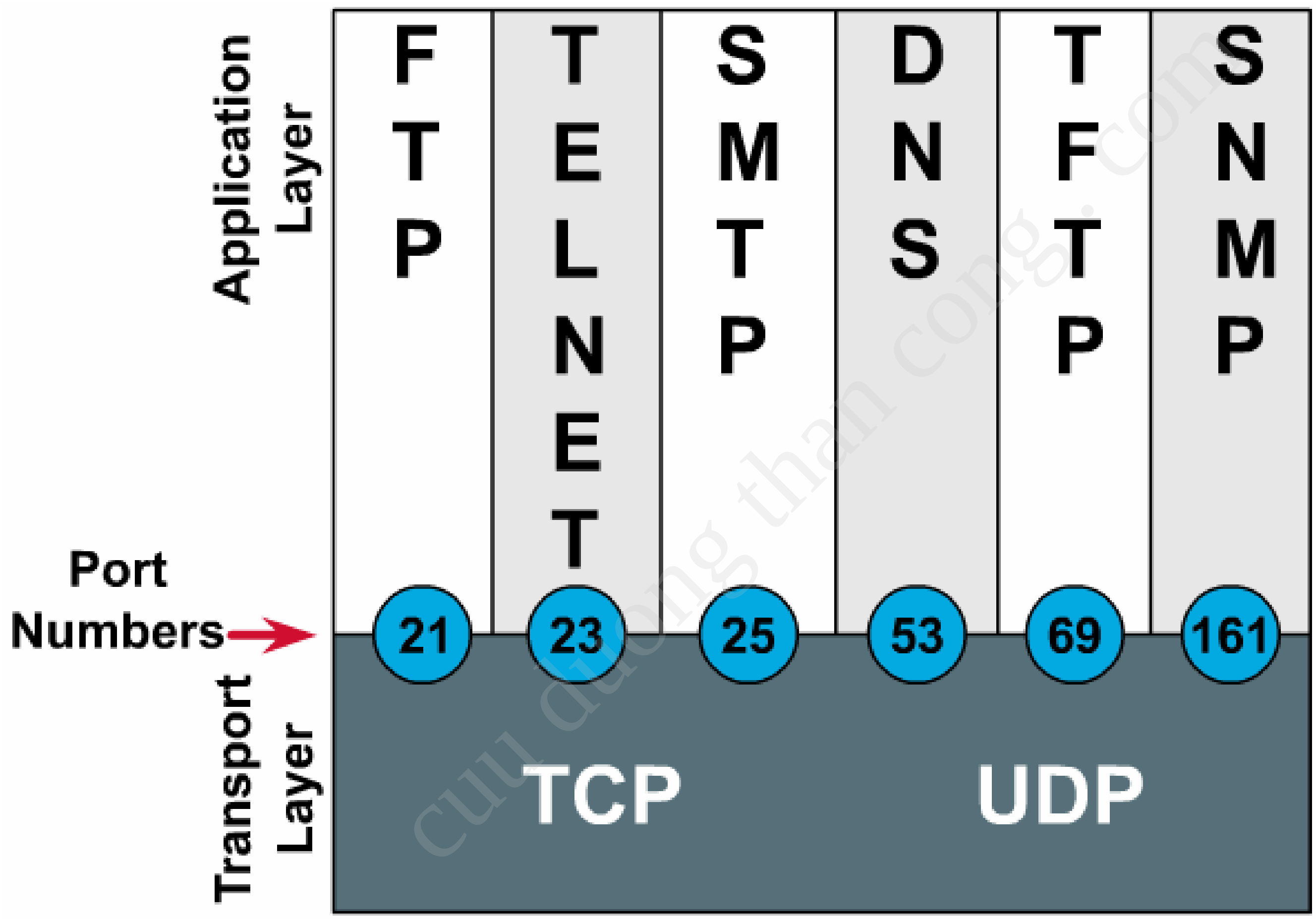
- Following are the characteristics:
  - Connectionless.
  - Unreliable, no software checking for message delivery
  - Transmit messages, does not need reassemble incoming messages.
  - Without acknowledgements.
  - Error processing and retransmission must be handled by higher layer protocols.
- The protocols that use UDP include: TFTP, SNMP , DHCP ,DNS .

UDP Header format

RFC-768

# of Bits	16	16	16	16	
	Source Port	Destination Port	Length	Check Sum	Data...

TCP and UDP port numbers



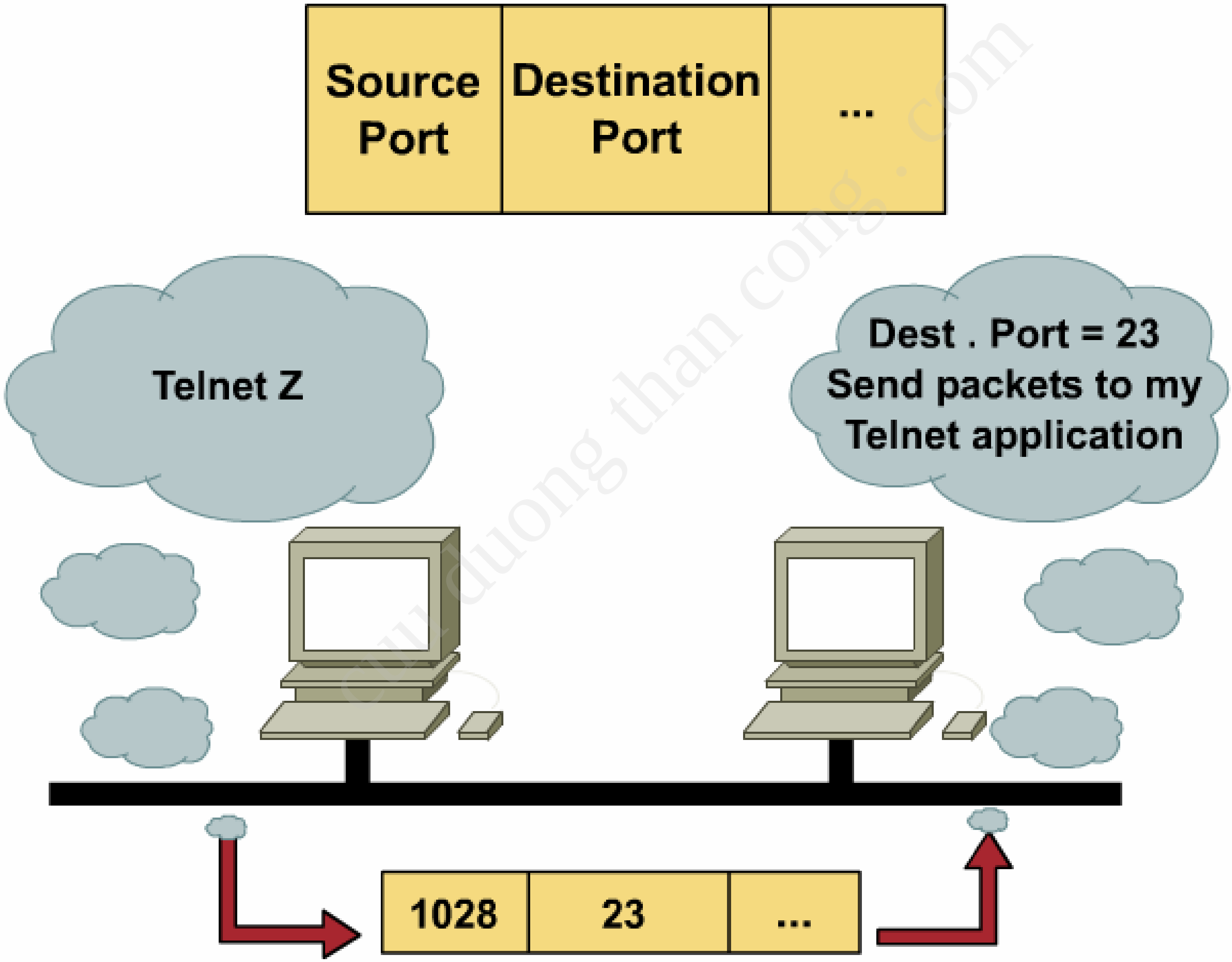
- Both TCP and UDP use port (or socket) numbers to pass information to the upper layers.

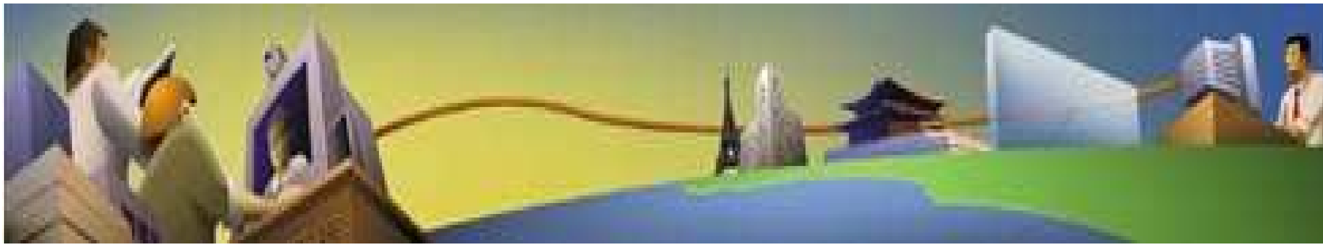
Range of ports

- 2 bytes: 0 – 65535.
  - Numbers below 255 : for public applications.
  - Numbers from 255 - 1023 : assigned to companies for marketable applications.
  - Numbers above 1023 : are unregulated.
- End systems use port numbers to select proper applications.
- Originating source port numbers are dynamically assigned by the source host; usually, it is a number larger than 1023.

Telnet port number

NETWORK TRAINING CENTER





TCP/IP APPLICATIONS

TCP Application layer protocols

- Domain Name System (DNS)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Management Protocol (SNMP)
- Telnet
- ...

DNS: Problems with using IP address

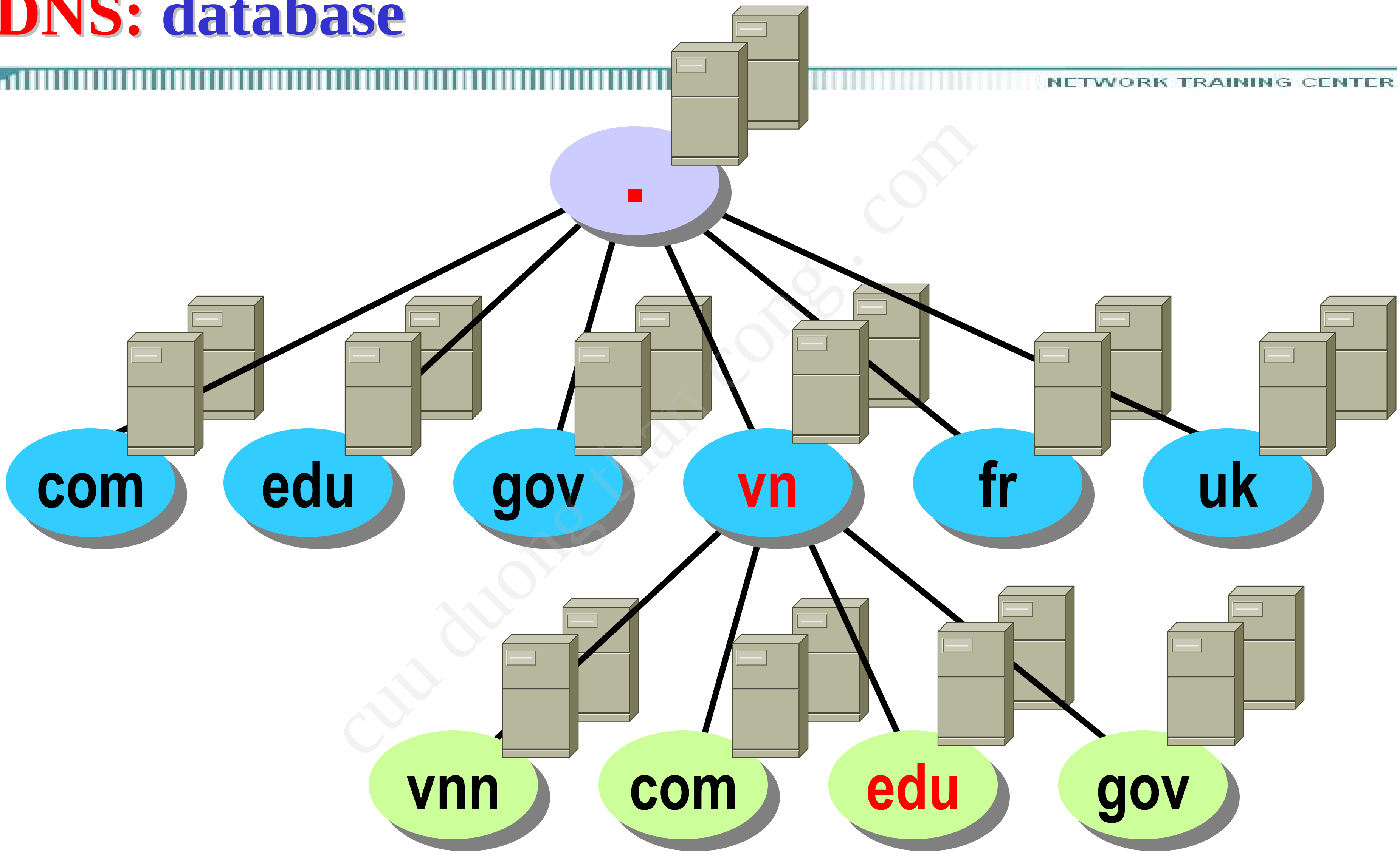
192.31.7.130	CISCO.COM
204.71.177.35	YAHOO.COM
152.163.210.7	AOL.COM
198.150.15.234	MAT-MADISON.COM
207.46.131.15	MICROSOFT.COM
192.233.80.9	NOVELL.COM

DNS

NETWORK TRAINING CENTER

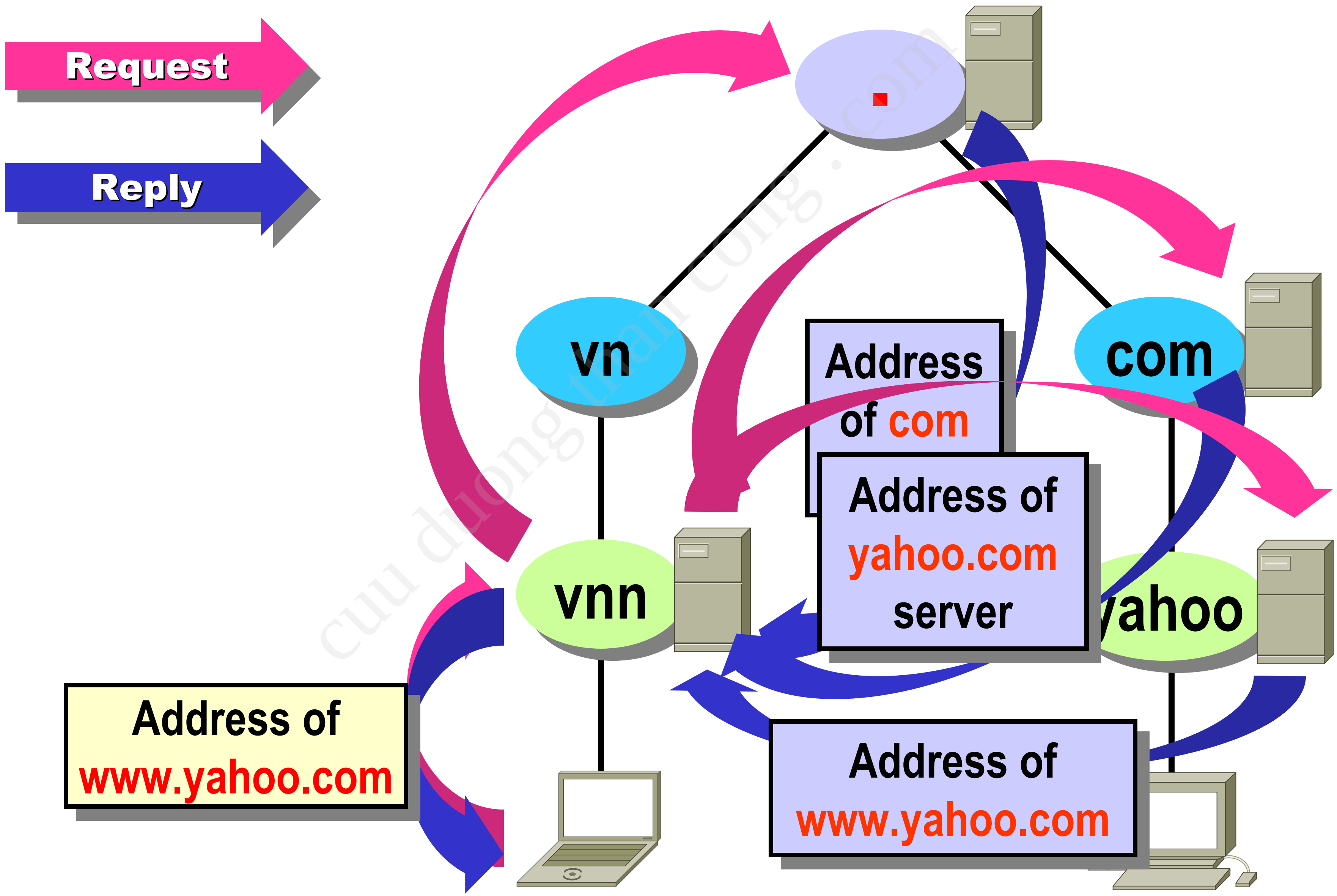
- The DNS server is a device on a network that manages domain names and responds to requests from clients to translate a domain name into the associated IP address.
- The DNS system is set up in a hierarchy that creates different levels of DNS servers.

DNS: database



DNS: Resolve www.yahoo.com

NETWORK TRAINING CENTER



FTP and TFTP

- FTP and TFTP are designed to download files or upload files on the Internet.
- FTP is a reliable, connection-oriented service that use TCP. The FTP session is maintained until the client terminates it, or there is some sort of communication error.
- TFTP is a connectionless sevice that use UDP

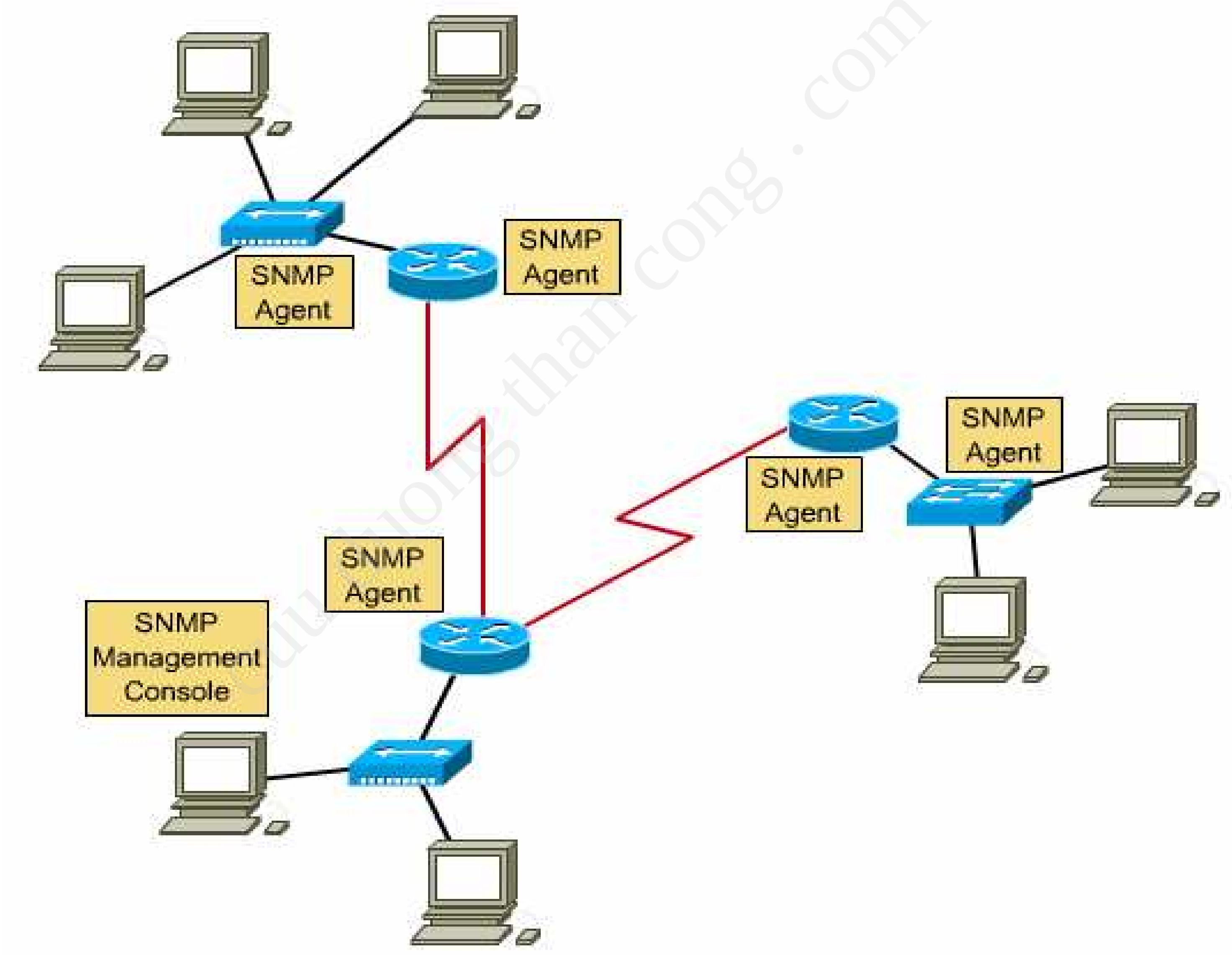
HTTP

- Web pages are created with a format language called Hypertext Markup Language (HTML).
- Hyperlinks make the World Wide Web easy to navigate. A hyperlink is an object on a Web page that, when clicked, transfers you to a new Web page.
- An address location known as a Uniform Resource Locator (URL).
- Example: http://www.cisco.com/edu

SMTP

- Email servers communicate with each other using the SMTP to send and receive mail.
- Email client, work with the POP3 or IMAP4 protocol to access email server.
- Email client, work with the SMTP to send mail.
- For security, when message recipients check their e-mail they are often prompted for a password. The password can also be saved in many e-mail programs.
- An e-mail address consists of the recipient's username and post-office address: abc@yahoo.com.

SNMP


SNMP Agent
SNMP Agent
SNMP Agent
SNMP Agent
SNMP Agent
SNMP Management Console

SNMP

- SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.
- SNMP uses UDP as its transport layer protocol.
- Three key components:
  - Network management system (NMS)
  - Managed devices
  - Agents

Telnet

- Telnet software provides the ability to remotely access another computer.
- The Telnet application works mainly at the application, presentation and session layers of the OSI model.

Summary

- The functions of the TCP/IP transport layer
  - Flow control
  - The processes of establishing a connection between peer systems
  - Windowing
  - Acknowledgment
- Transport layer protocols
  - TCP and UDP header formats
  - TCP and UDP port numbers
- The processes and protocols at the TCP/IP application layer
  - Domain Name Services
  - File Transfer Protocols
  - Simple Mail Transfer Protocol
  - Simple Network Management Protocol
  - Telnet

Q&A