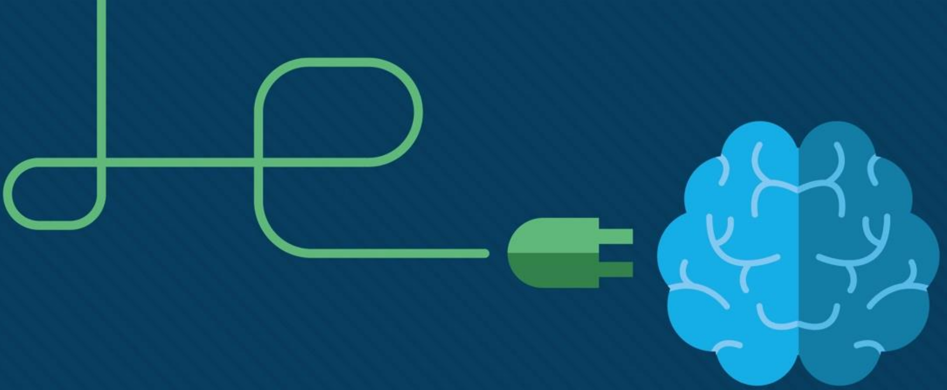


Module 5:Network Protocols

CyberOps Associates v1.0

Module Objectives

Module Title: Network Protocols

Module Objective: Explain how protocols enable network operations.

Topic Title	Topic Objective
Network Communications Process	Explain the basic operation of data networked communications.
Communications Protocols	Explain how protocols enable network operations.
Data Encapsulation	Explain how data encapsulation allows data to be transported across the network.

5.1 Network Communications Process

Network Components

Host Roles

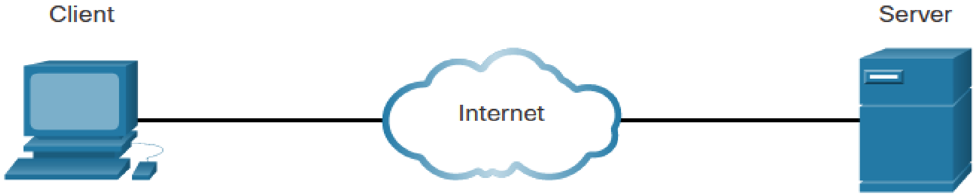
Every computer on a network is called a **host** or **end device**.

Servers are computers that provide information to end devices:

- email servers
- web servers
- file server

Clients are computers that send requests to the servers to retrieve information:

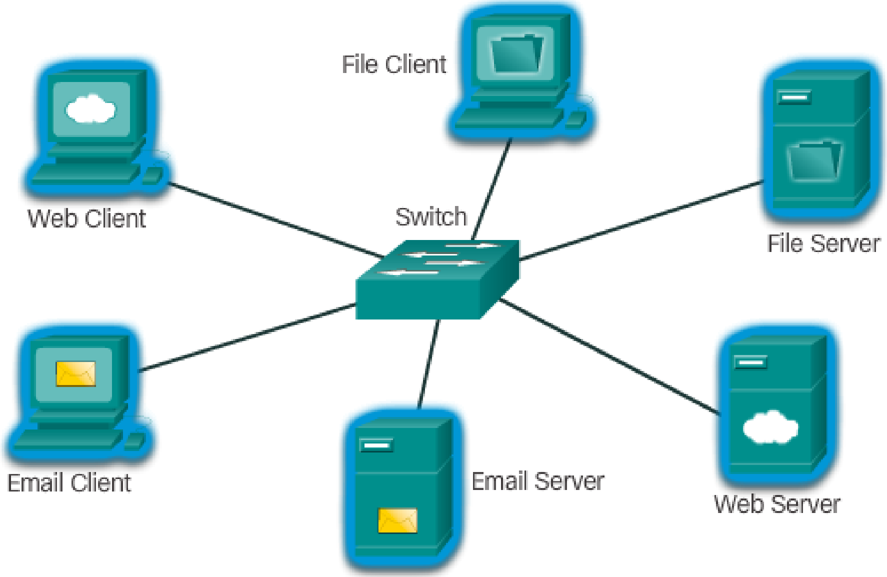
- web page from a web server
- email from an email server



Server Type	**Description**
Email	Email server runs email server software. Clients use client software to access email.
Web	Web server runs web server software. Clients use browser software to access web pages.
File	File server stores corporate and user files. The client devices access these files.

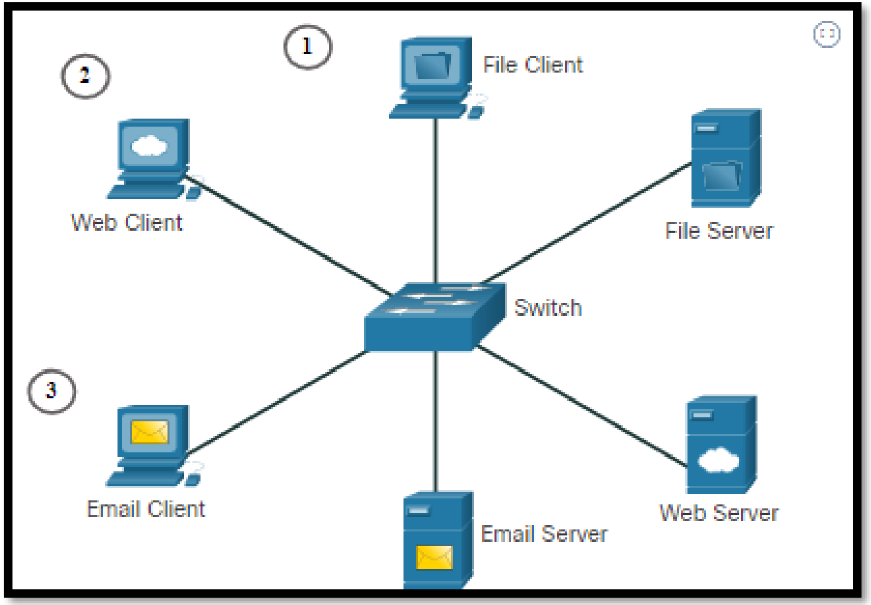
Client-Server Communications

- All computers that are connected to a network and that participate directly in network communication are classified as hosts. Hosts are also called end devices, endpoints, or nodes.
- Servers are simply computers with specialized software that enables servers to provide information to other end devices on the network.
- A server can be single-purpose, providing only one service, such as web pages or it can be multipurpose, providing a variety of services such as web pages, email, and file transfers.
- Client computers have software installed that enables them to request and display the information obtained from the server. A single computer can run multiple types of client software.



Client-Server Communications (Contd.)

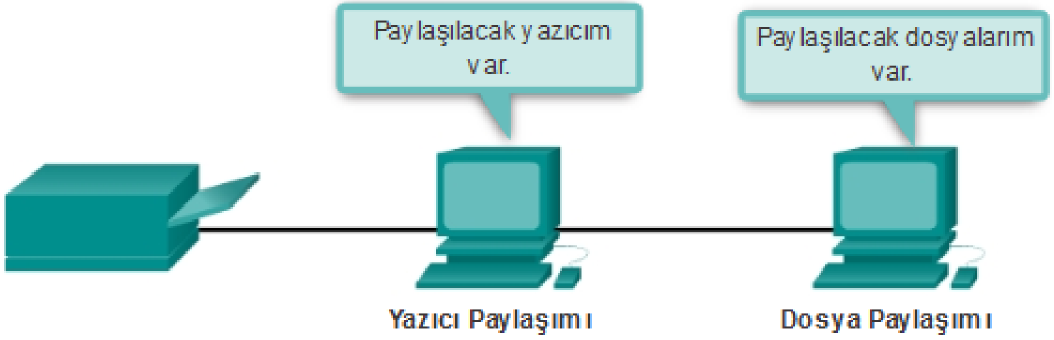
- The File Server stores corporate and user files in a central location. The client devices access these files with client software such as Windows Explorer.
- The Web Server runs web server software and clients use their browser software, such as Windows Internet Explorer, to access web pages on the server.
- The Email Server runs email server software and clients use their mail client software, such as Microsoft Outlook, to access email on the server.



Network Protocols

Peer to Peer (P2P) Communications

Peer-to-peer network: In small businesses and homes, many computers function as both the servers and clients on the network. This type of network is called a peer-to-peer network.

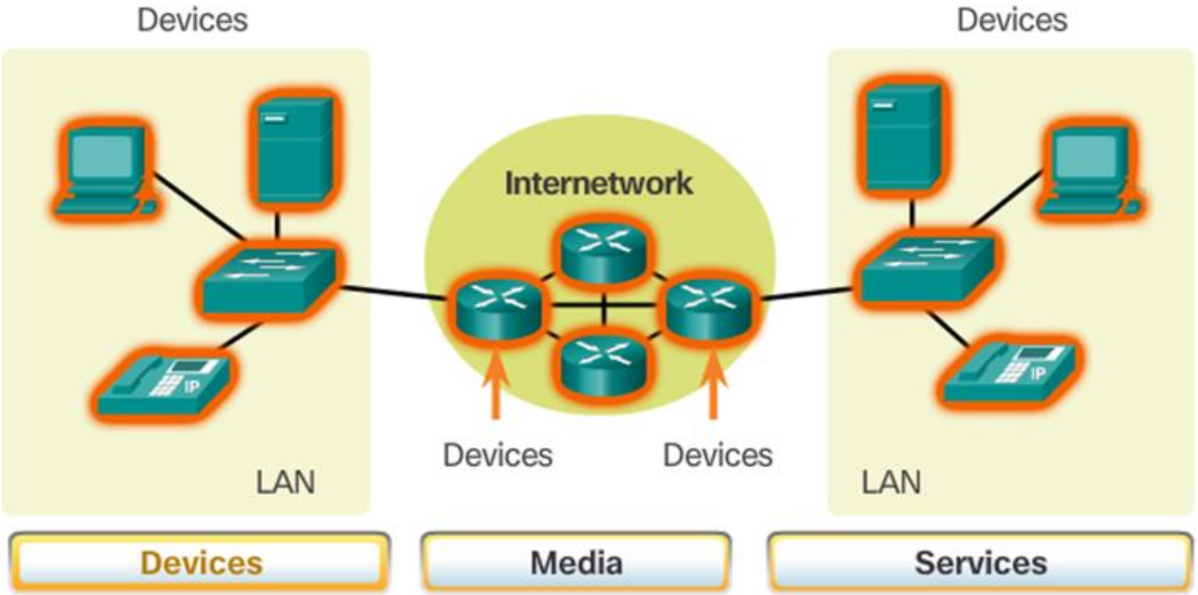


Advantages	Disadvantages
Easy to set up	No centralized administration
Less complex	Not as secure
Lower cost	Not scalable
Used for simple tasks: transferring files and sharing printers	Slower performance

Network Components

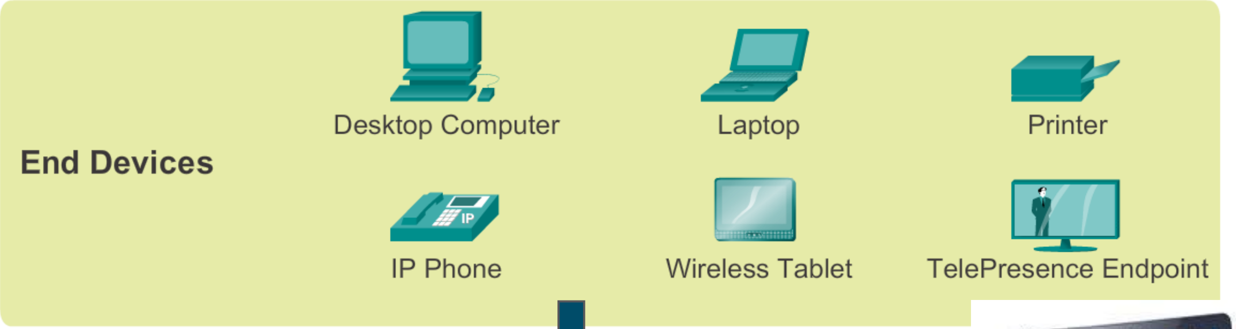
Üç ağ bileşeni kategorisi bulunmaktadır:

- **End Devices** (Uç Cihazlar) and **Intermediary Network Devices** (Ara Ağ Cihazları)
- **Networking Media** (İletim Ortamı)
- **Services** (Servis/ Sunucular)



Network Components

End Devices – (Hosts)
Uç Cihazlar (Son Kullanıcı Cihazları)



End Devices

Desktop Computer

Laptop

Printer

IP Phone

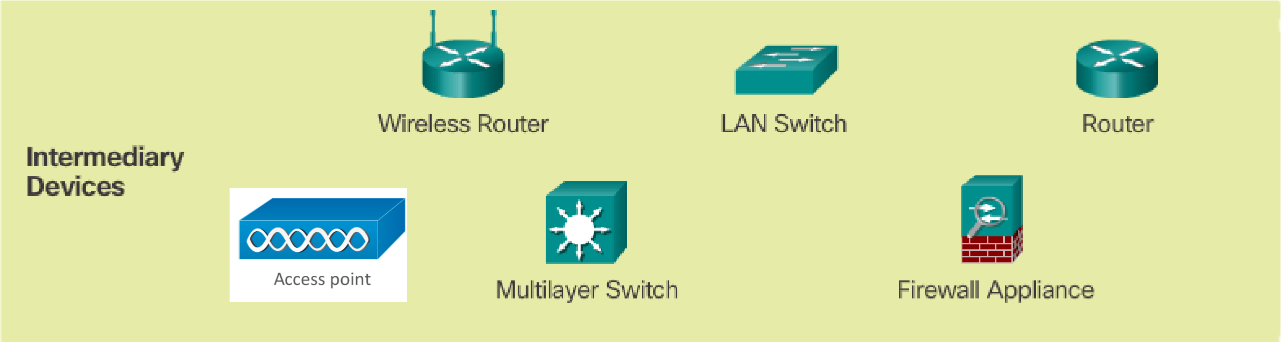
Wireless Tablet

TelePresence Endpoint

Network Interface Card (NIC)

Ağ Arayüz Kartı

Intermediary Network Devices (Ara Ağ Cihazları)



An intermediary device interconnects end devices. Examples include switches, wireless access points, routers, and firewalls.

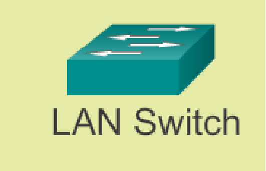
Management of data as it flows through a network is also the role of an intermediary device, including:

- Regenerate and retransmit data signals.
- Maintain information about what pathways exist in the network.
- Notify other devices of errors and communication failures.

Intermediary Network Devices
(Ara Ağ Cihazları)

Ara ağ cihazlarına örnek olarak aşağıdakiler verilebilir:

- Ağ Erişim Cihazları
  - **Anahtarlar (Switch)**



  - **Kablosuz Erişim Noktaları(Access Point)**

Access point

Intermediary Network Devices
(Ara Ağ Cihazları)

Ara ağ cihazlarına örnek olarak aşağıdakiler verilebilir:

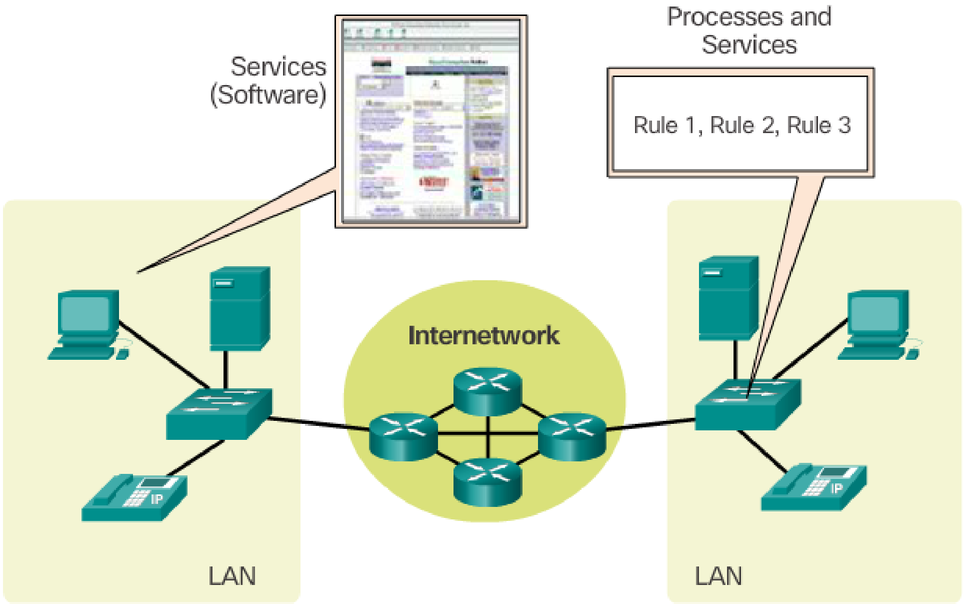
- Ağlar Arası Cihazlar: **Yönlendiriciler (Router)**

  path selection (networkler arası yol seçimi)

- Güvenlik Cihazları: **Güvenlik Duvarları (Firewall)**

Network Components

Services (Servisler /Sunucular)



Devices

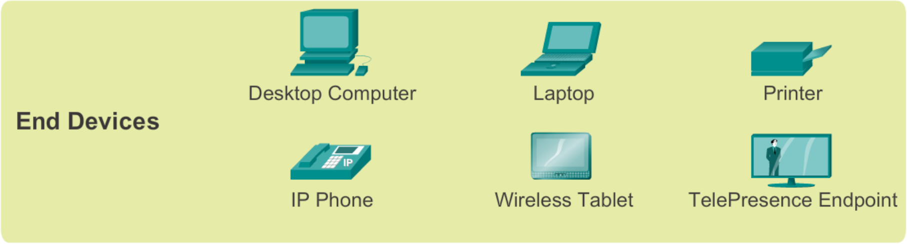
Media

Services

Ağ Bileşenleri

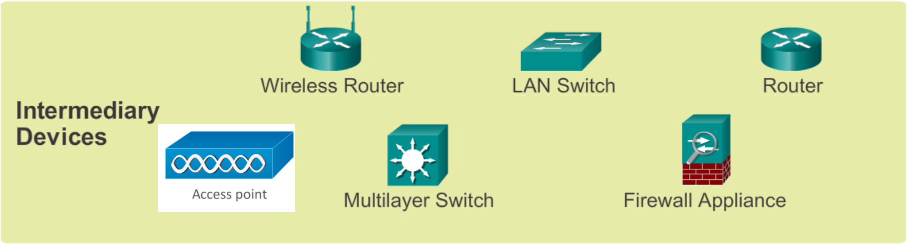
Ağ Temsilleri

Son Cihazlar



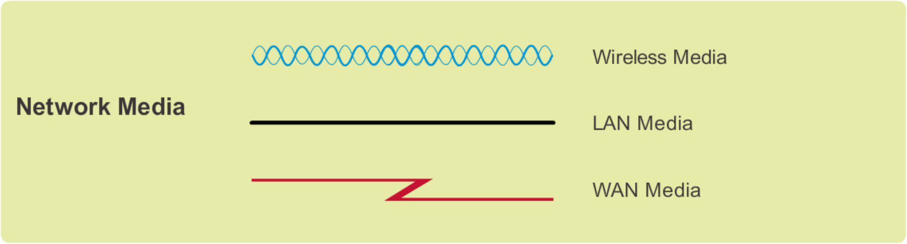
End Devices

Ara Cihazlar



Intermediary Devices

Ağ Medyası
(Ağ İletim Ortamı)



Network Media

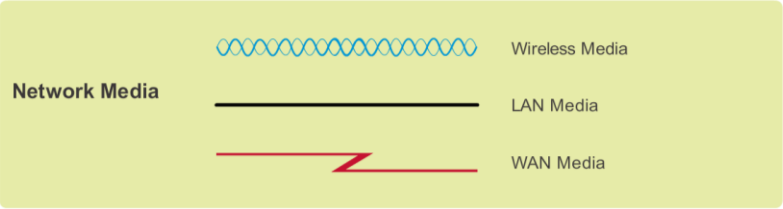
Ağın Bileşenleri

Network Media (Ağ Medyası)

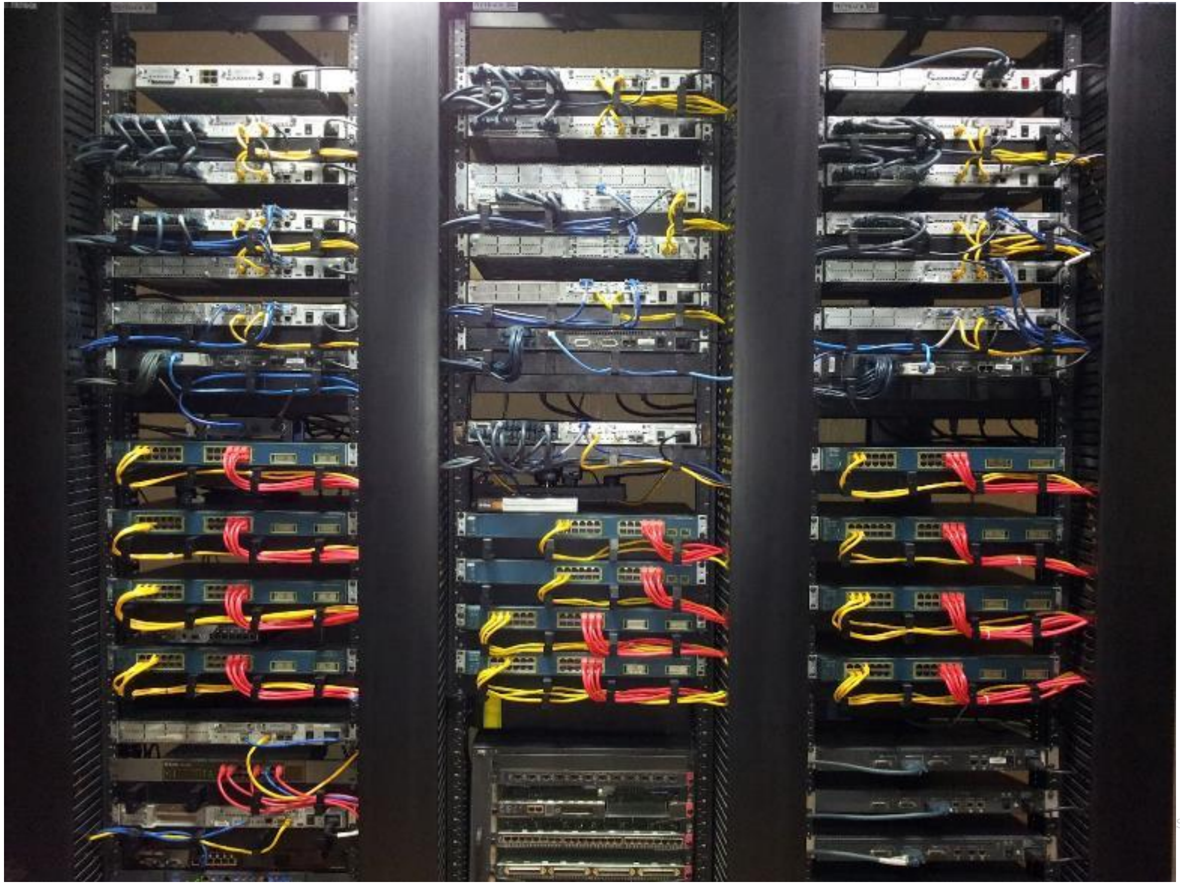
Bakır Kablolar:
- elektriksel iletim
  - UTP Kablo

Fiber Optik Kablolar
- Işık ile iletim
  - Single Mode Fiber
  - Multi Mode Fiber

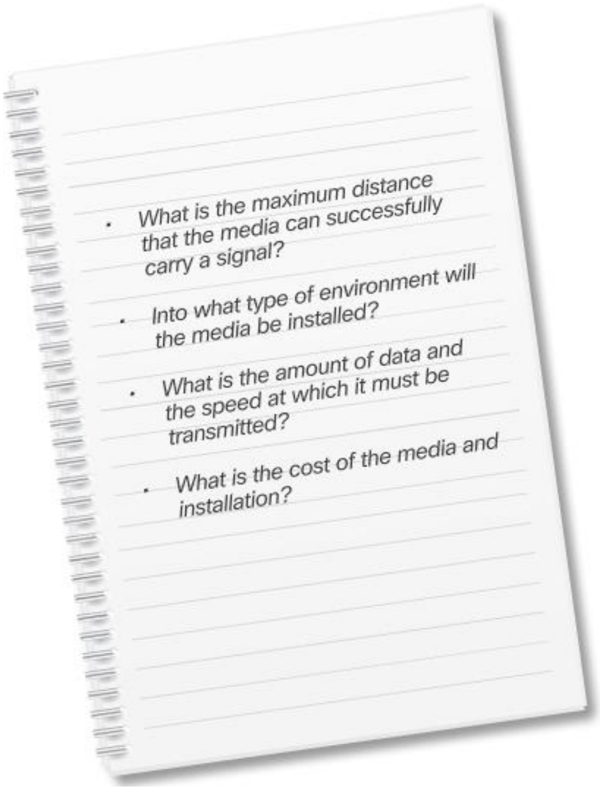
Kablosuz İletim:
- Elektromanyetik dalgalar ile iletim



Kabinet içerisinde Ağ Cihazları ve Kablolama



Network Media (Ağ Medyası) seçimi….



- What is the maximum distance that the media can successfully carry a signal?
- Into what type of environment will the media be installed?
- What is the amount of data and the speed at which it must be transmitted?
- What is the cost of the media and installation?

İletim Ortamının maksimum sinyal taşıma mesafesi nedir?

Medya ne tür bir ortama kurulacak?

İletilmesi istenen veri miktarı ve hızı nedir?

Medya ve Kurulum maliyetleri nedir?

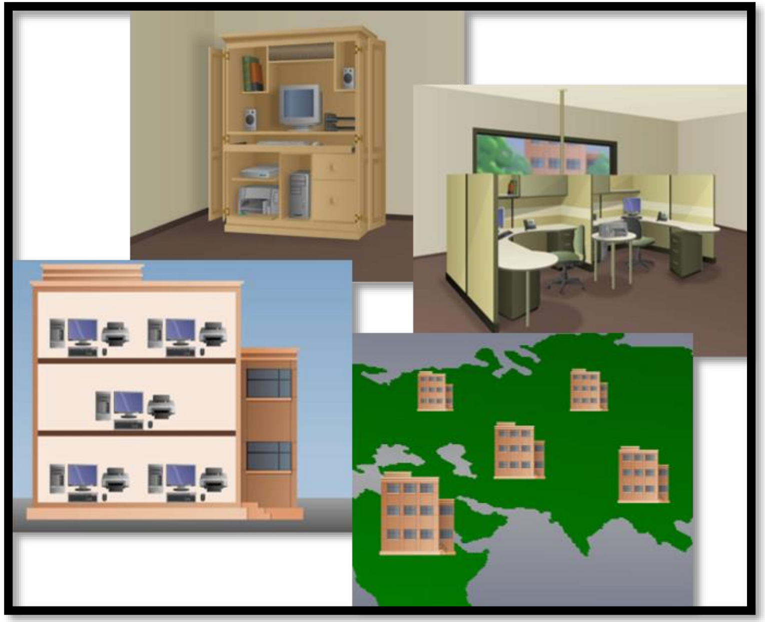
Common Types of Networks (Yaygın Ağ Türleri)

Networks of Many Sizes

- Networks vary in size. They range from simple networks consisting of two computers, to networks connecting millions of devices.
- Businesses and large organizations use networks to provide consolidation, storage, and access to information on network servers. Networks provide email, instant messaging, and collaboration among employees. Many organizations use their network’s connection to the internet to provide products and services to customers.

Networks of Many Sizes (Contd.)

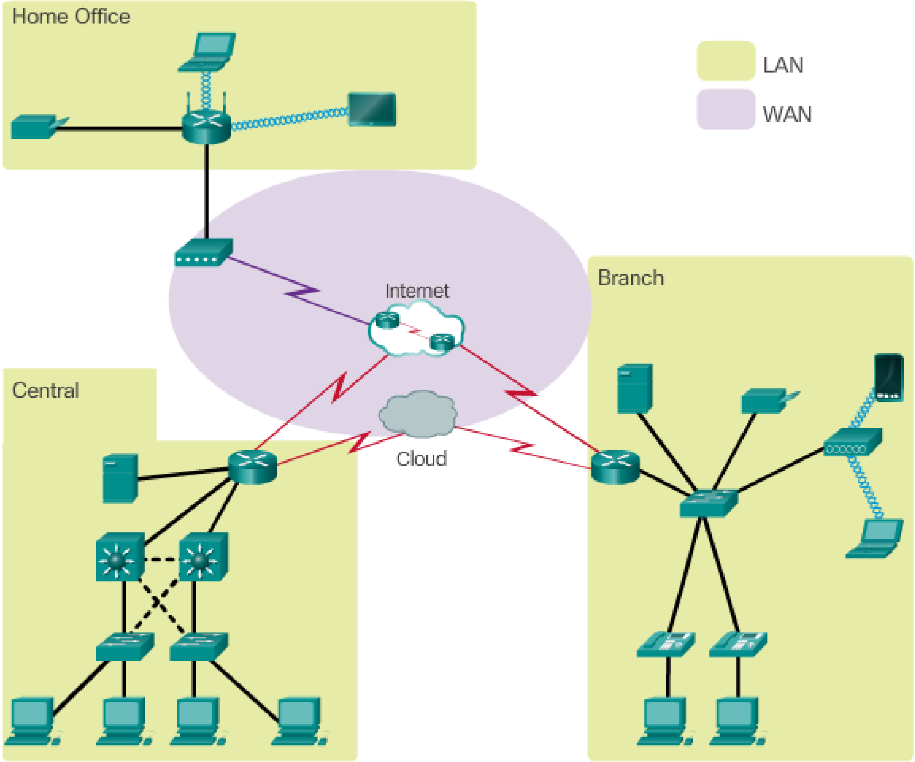
- **Small Home networks:** Small home networks connect a few computers to each other and to the internet.
- **Small Office and Home Office (SOHO) networks:** The SOHO network allows a home office or a remote office to connect to a corporate network, or access centralized, shared resources.
- **Medium to Large networks**: These are used by corporations and schools and can have many locations with hundreds or thousands of interconnected hosts.
- **World Wide networks**: The internet is a network of networks that connects hundreds of millions of computers world-wide.



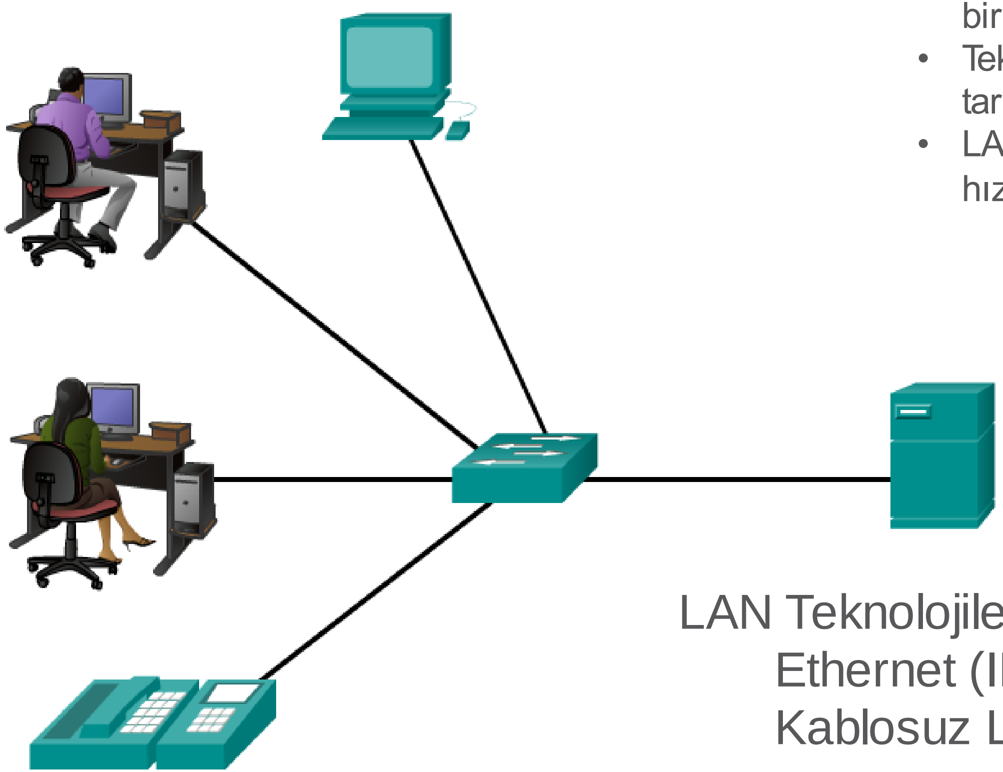
Types of Networks

Ağ türleri

- **Local Area Network (LAN)** *- Yerel Alan Ağı*
- **Wide Area Network (WAN)** *- Geniş Alan Ağı*



Local Area Networks (LAN)



- Sınırlı bir alanda uç cihazları birbirine bağlar
- Tek bir kuruluş veya kişi tarafından yönetilir
- LAN içi haberleşmede yüksek hızlı bant genişliği sağlar

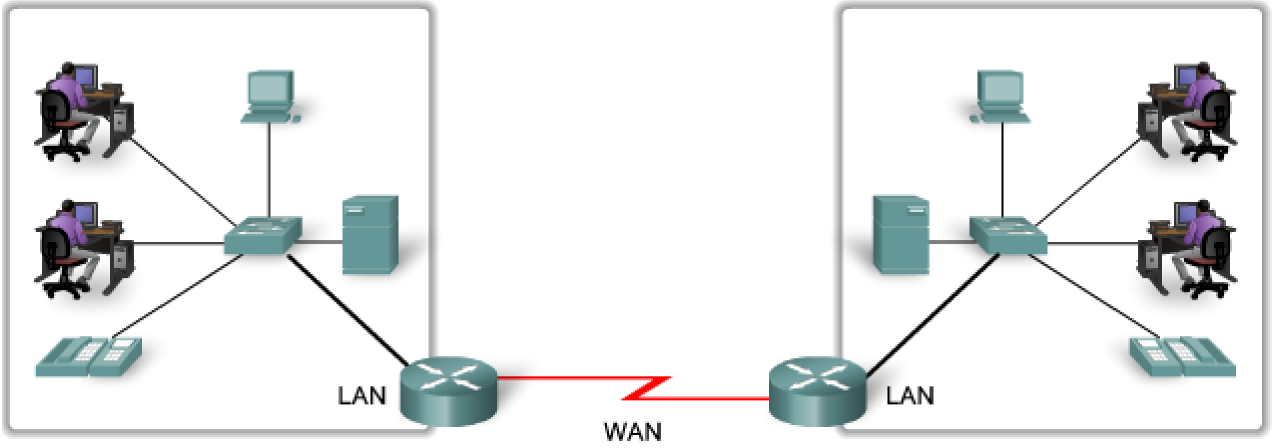
LAN Teknolojileri:

Ethernet (IEEE 802.3)

Kablosuz LAN (IEEE 802.11)

Wide Area Networks (WAN)

LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN).



- Geniş coğrafi bölgelerde LAN'ları birbirine bağlar
- Genellikle bir veya daha fazla servis sağlayıcı tarafından yönetilir.
- Genellikle LAN'lar arasında daha düşük hız bağlantıları sağlar.

WAN Teknolojileri:

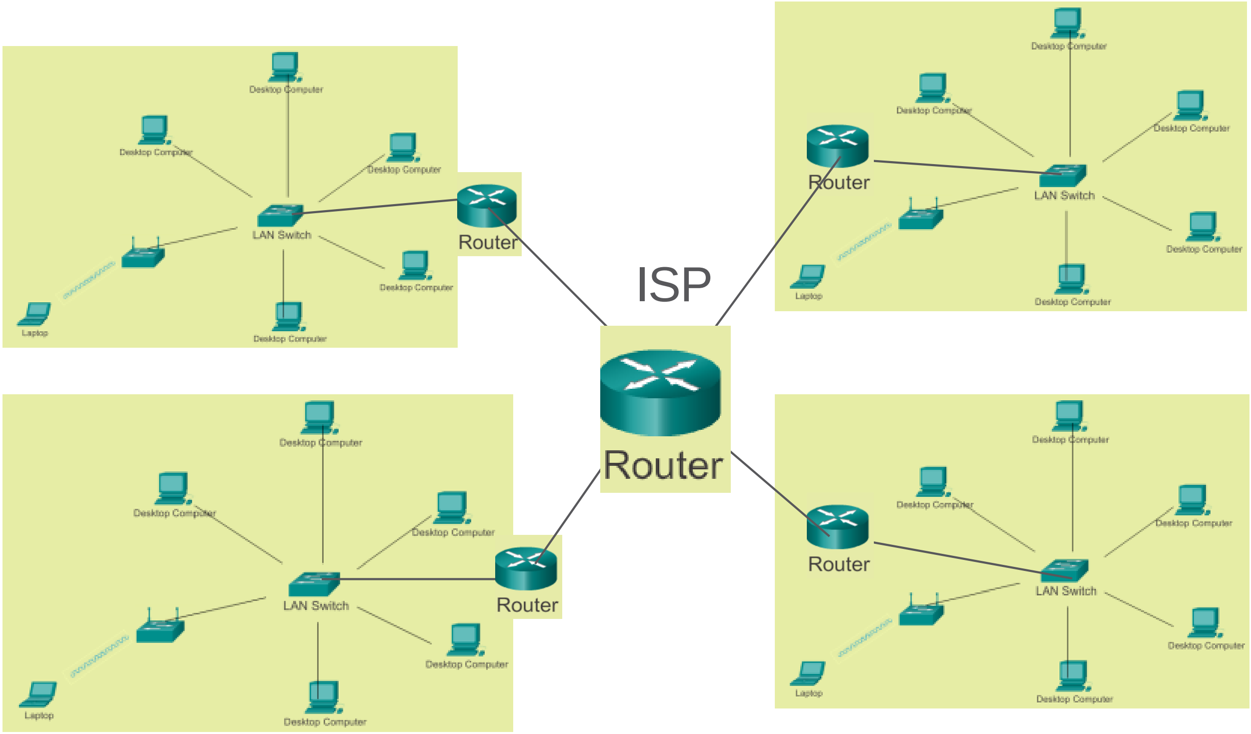
ADSL (PPPoE)

Kablo Net (DOCSIS)

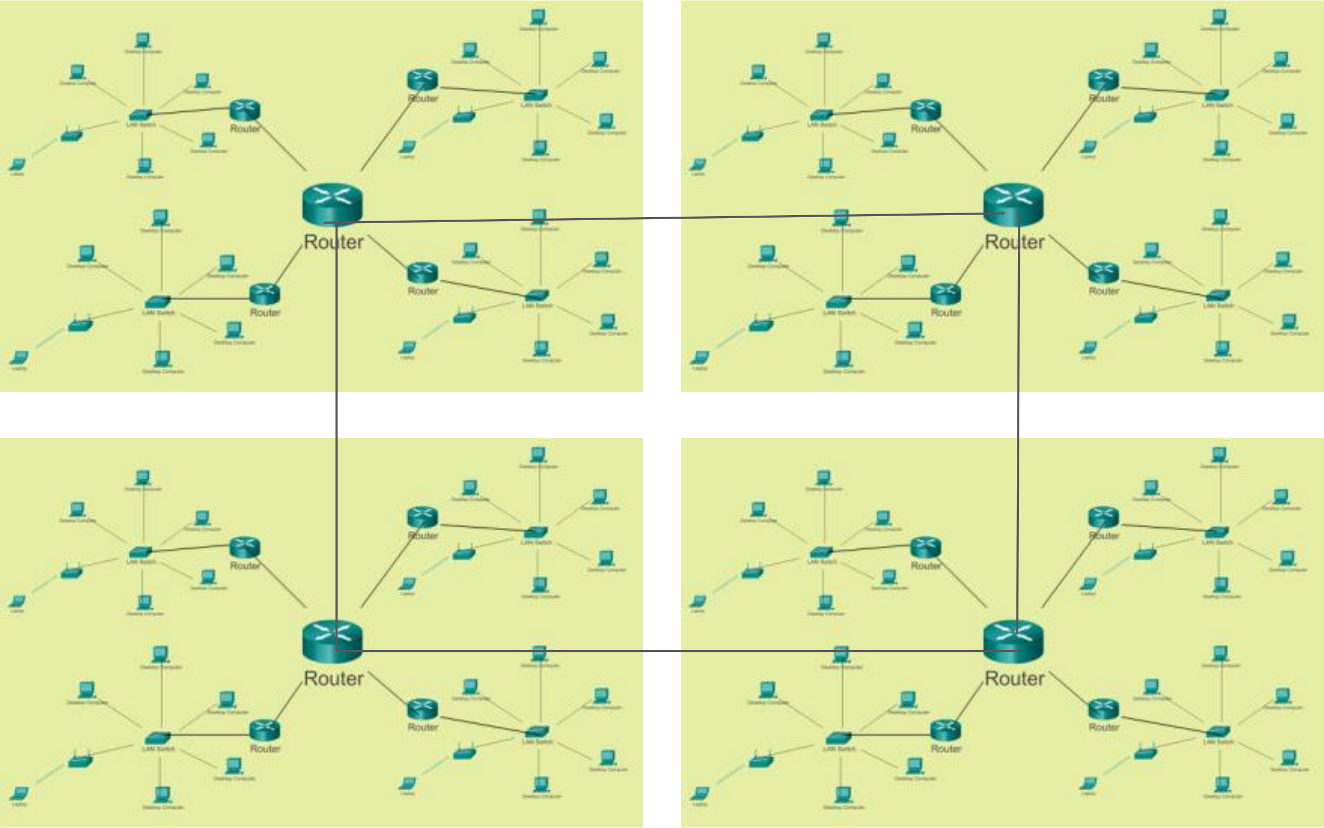
Dial Up (PPP)

Fiber Internet (Metro Ethernet), ATM vs.

Yerel Ağların Birleşmesi

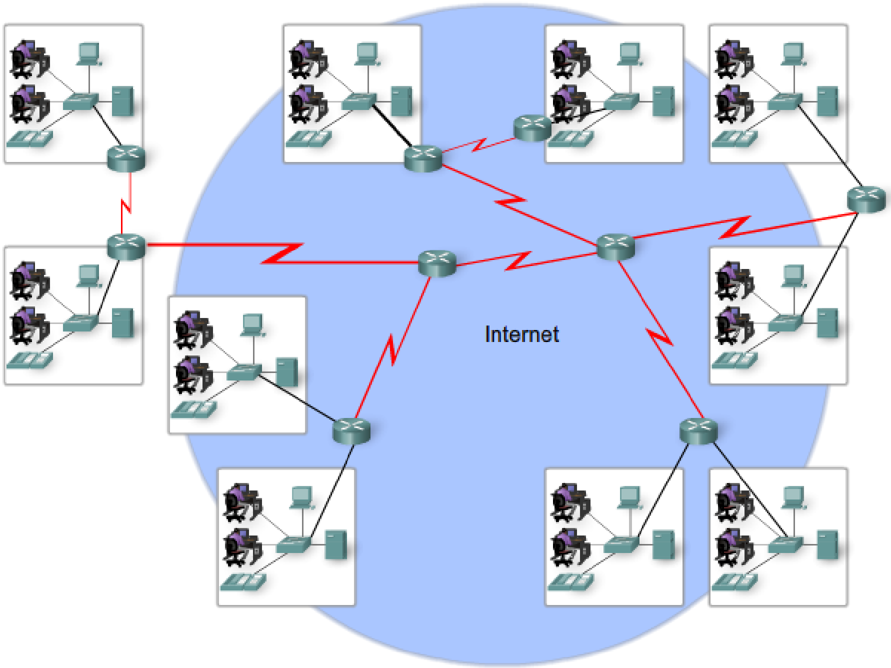


ISP Ağların Birleşmesi



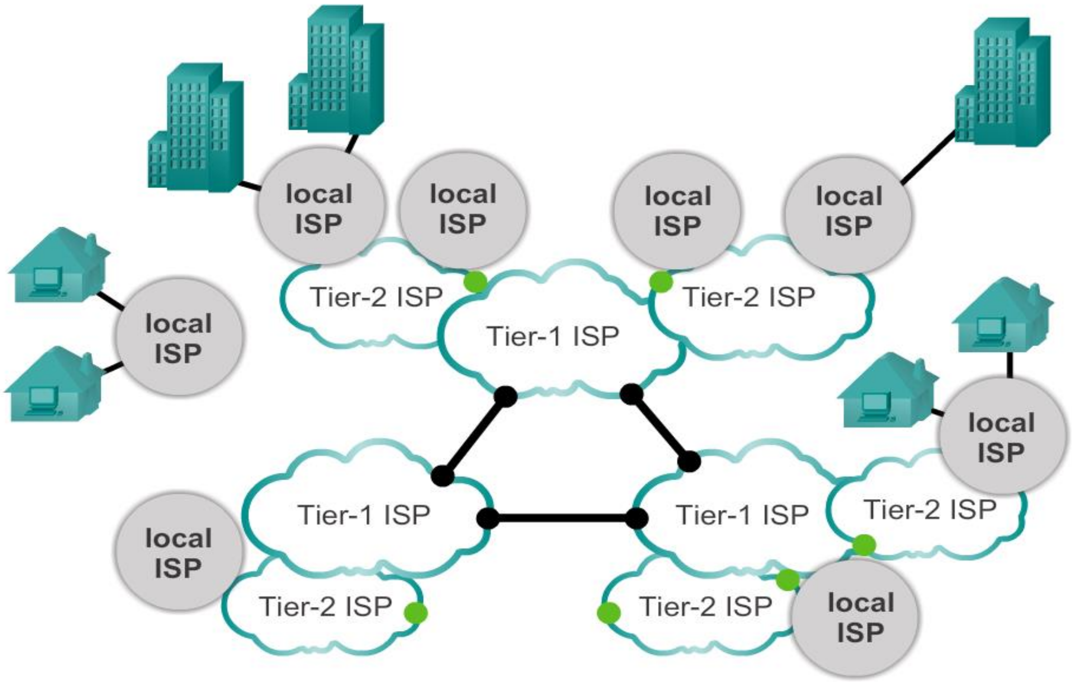
LAN’lar WAN’lar ve Internet

LANs and WANs may be connected into internetworks.



Internet

Tier 3



Tier-3 ISPs are the local providers of service directly to end users. Tier-3 ISPs are usually connected to Tier 2 ISPs and pay Tier 2 providers for Internet access.

5.2 Communications Protocols

Mesaj Biçimlendirme ve Kapsülleme

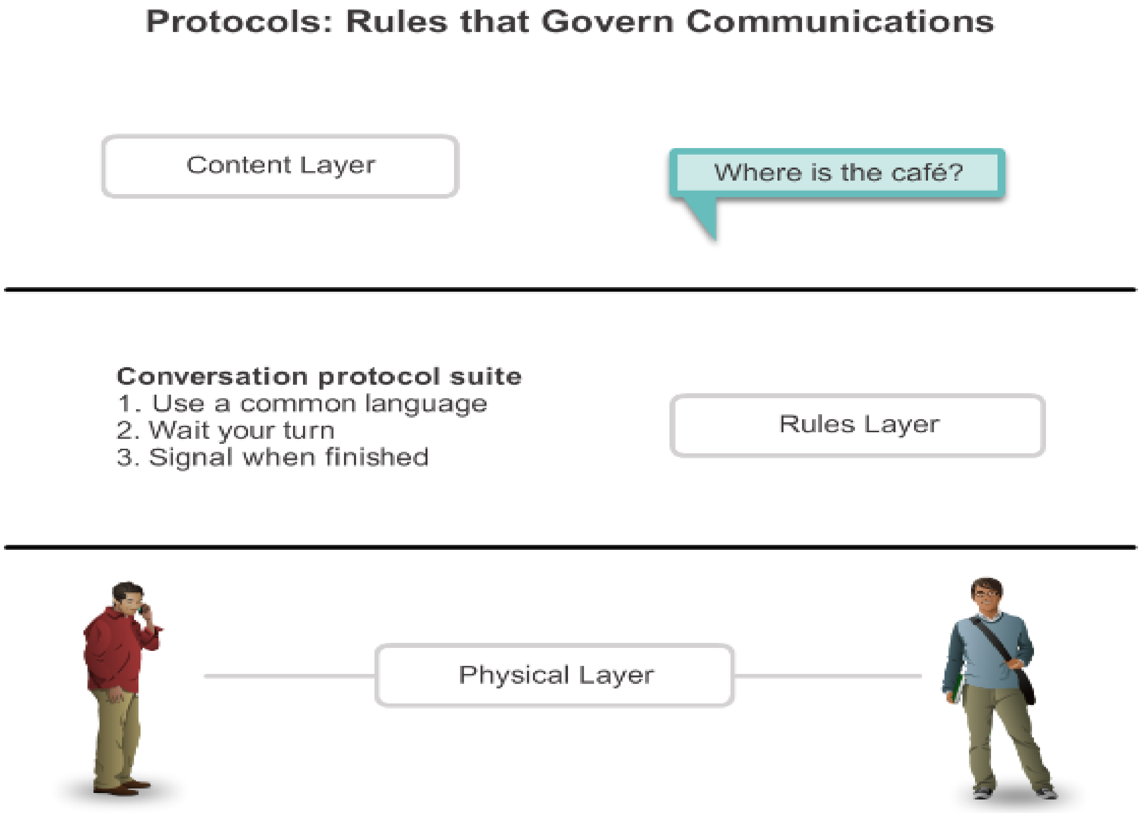
Örnek: Kişisel mektuplar aşağıdaki öğeleri içerir:

- Alıcının bir tanımlayıcısı
- Selamlama veya karşılama
- Mesaj içeriği
- Kapanış ifadesi
- Gönderenin bir tanımlayıcısı

Sender
4085 SE Pine Street
Ocala, Florida 34471
Recipient
1400 Main Street
Canton, Ohio 44203

Protokoller

İletişimle İlgili Kurallar

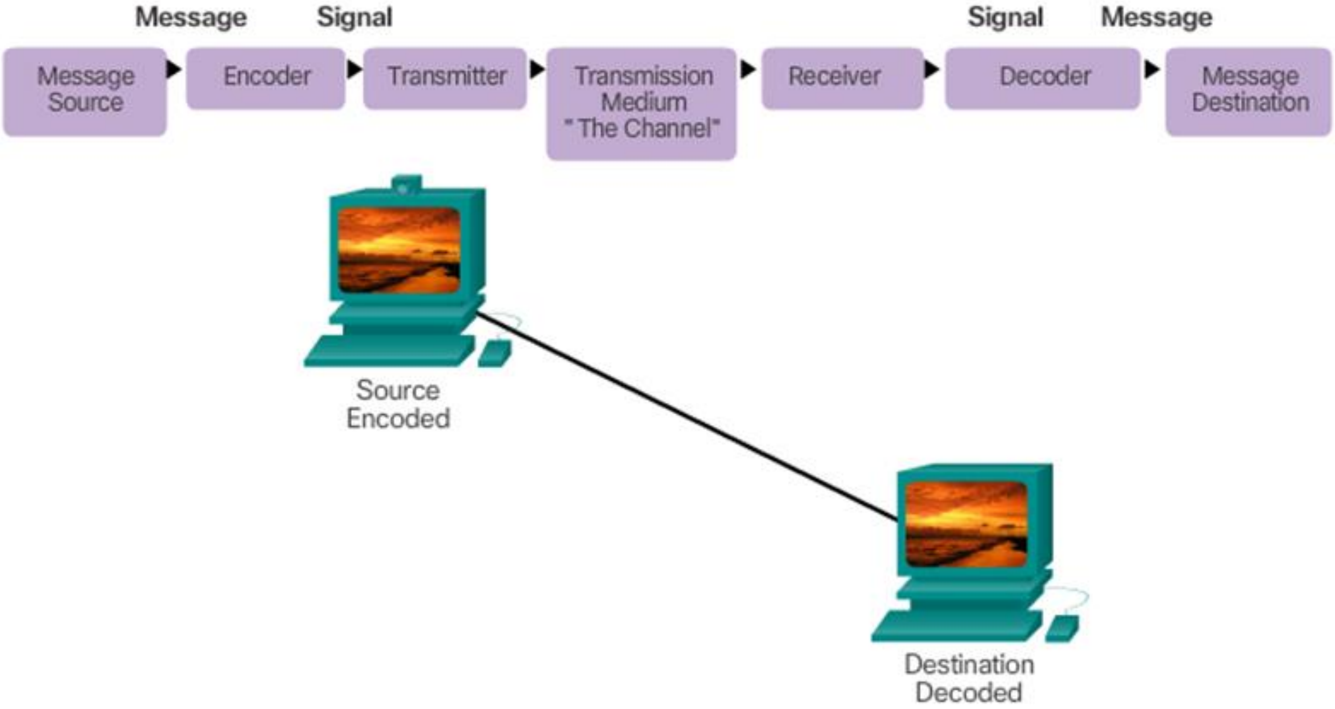


Conversation protocol suite

1. Use a common language
2. Wait your turn
3. Signal when finished

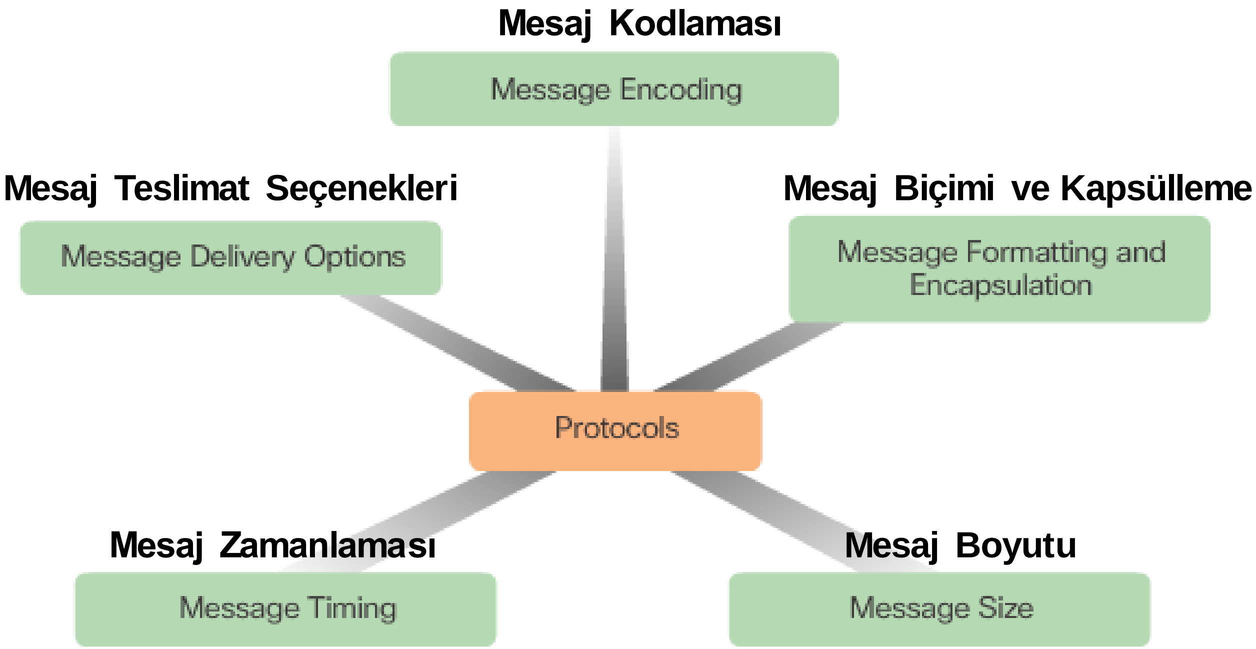
Protocol suites are sets of rules that work together to help solve a problem.

Message Encoding



Communications Protocols

Protokoller: Kurallar Dizisi



Mesaj Kodlaması

Mesaj Teslimat Seçenekleri

Mesaj Biçimi ve Kapsülleme

Mesaj Zamanlaması

Mesaj Boyutu

Standartlar Kuruluşları

IEEE

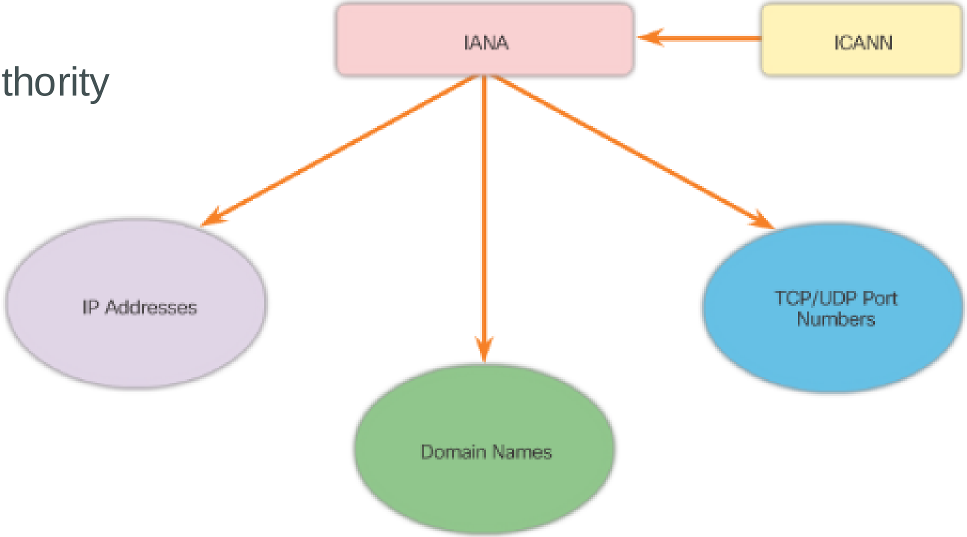
- 38 topluluk
- 130 dergi
- her yıl 1.300 konferans
- 1.300 standart ve proje
- 400.000 üye
- 160 ülke
- IEEE 802.3
- IEEE 802.11

Internet Standards (cont.)

IETF: Internet Engineering Task Force

ICANN:
Internet Corporation for Assigned Names & Numbers
(İnternetin kararlılığını ve bütünlüğünü desteklemek için birlikte çalışan küresel İnternet topluluğu)

IANA:
Internet Assigned Numbers Authority

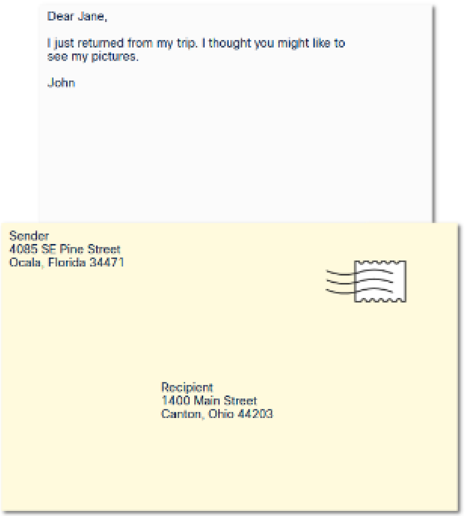


The Rules

Message Formatting and Encapsulation

- Birileri kuralları koymalı!

•When a message is sent from source to destination, it must use a specific format or structure.
•Message formats depend on the type of message and the channel that is used to deliver the message.



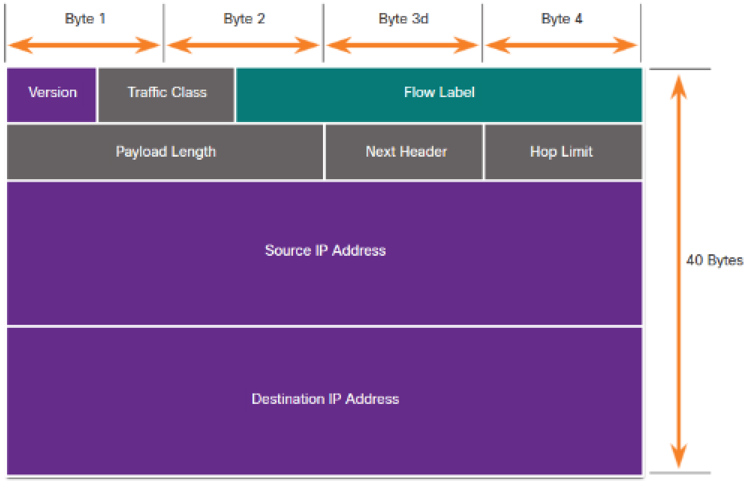
Dear Jane,

I just returned from my trip. I thought you might like to see my pictures.

John

Sender
4085 SE Pine Street
Ocala, Florida 34471

Recipient
1400 Main Street
Canton, Ohio 44203



Byte 1 | Byte 2 | Byte 3d | Byte 4

Version | Traffic Class | Flow Label

Payload Length | Next Header | Hop Limit

Source IP Address

Destination IP Address

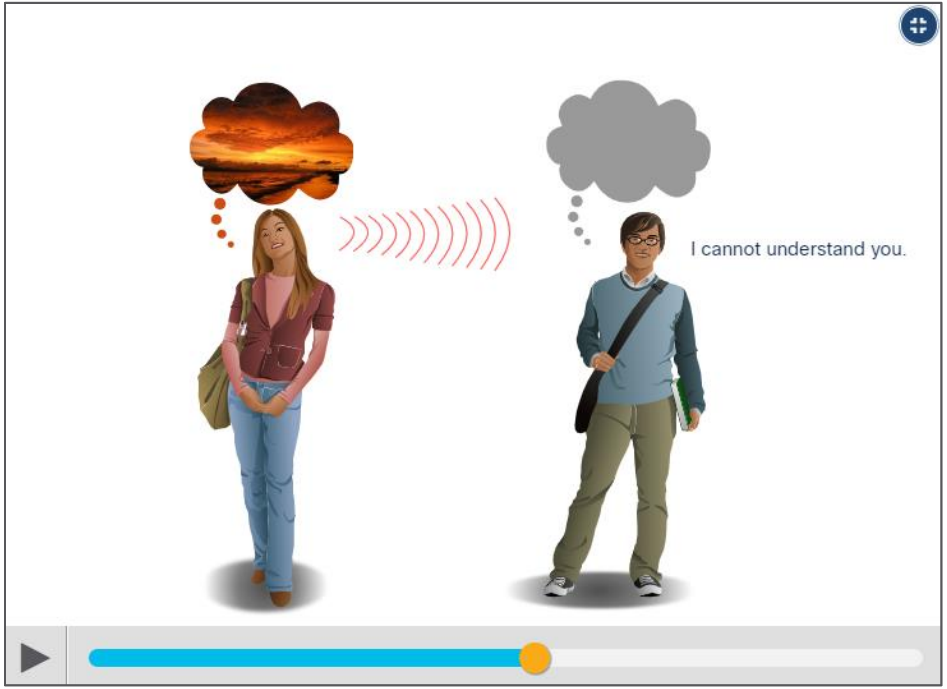
40 Bytes

Message Size

Another rule of communication is message size.

Analogy:

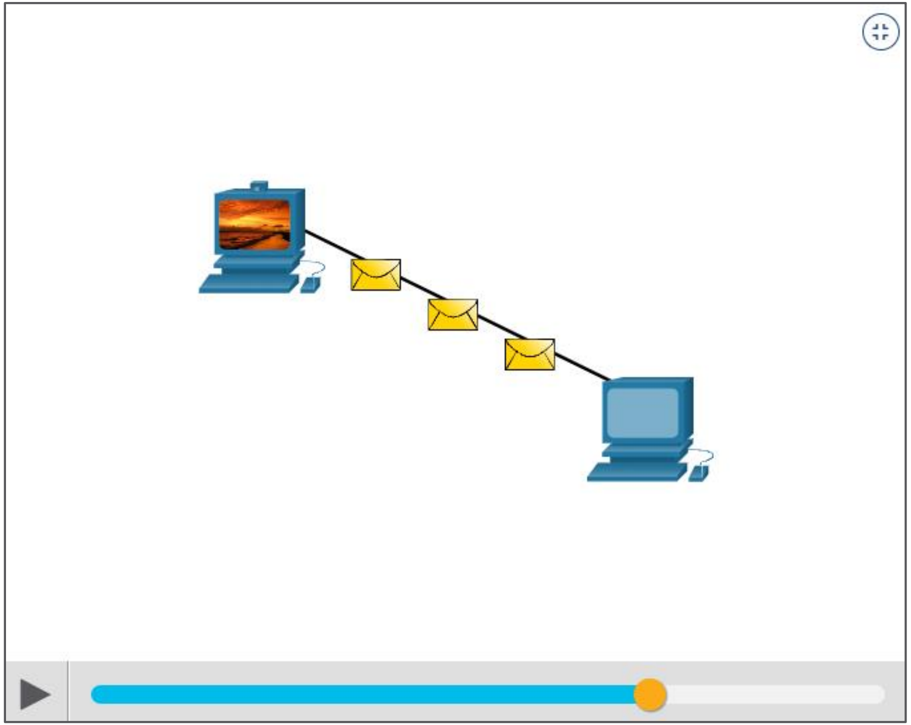
- When people communicate with each other, the messages that they send are usually broken into smaller parts or sentences.
- These sentences are limited in size to what the receiving person can process at one time. It also makes it easier for the receiver to read and comprehend.



Message Size (Contd.)

Network:

- Encoding between hosts must be in an appropriate format for the medium.
- Messages sent across the network are first converted into bits by the sending host
- Each bit is encoded into a pattern of sounds, light waves, or electrical impulses depending on the network media over which the bits are transmitted.
- The destination host receives and decodes the signals to interpret the message.

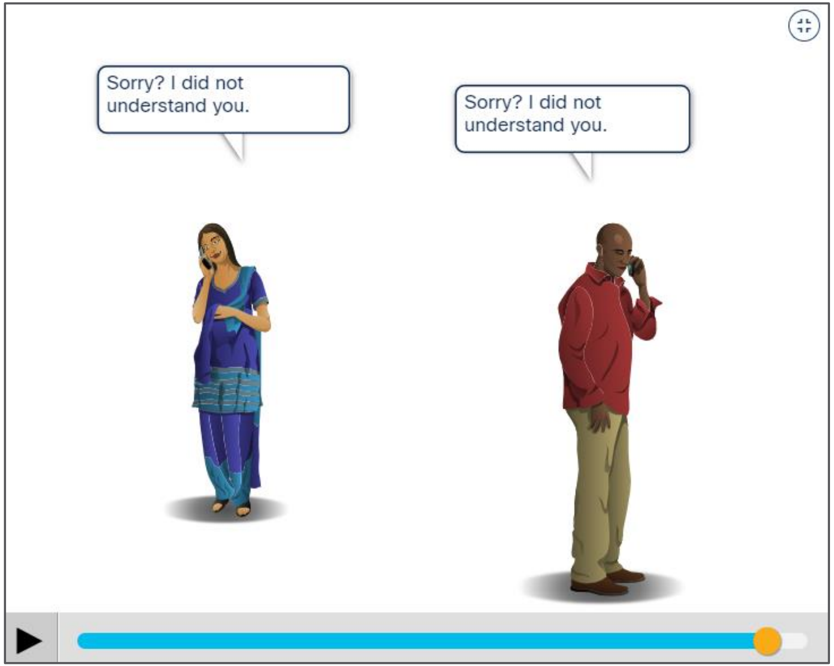


Communications Protocols

Message Timing

Message timing includes the following:

- **Flow Control – (Akış Kontrolü)** Flow control defines how much information can be sent and the speed at which it can be delivered.
- **Response Timeout (Yanıt Zaman Aşımı)-** Hosts on the network use network protocols that specify how long to wait for responses and what action to take if a response timeout occurs.
- **Access method (Erişim Metodu)-** This determines when someone can send a message. When a device wants to transmit on a wireless LAN, it is necessary for the WLAN NIC to determine whether the wireless medium is available.


Sorry? I did not understand you.
Sorry? I did not understand you.

Mesaj İletim Seçenekleri

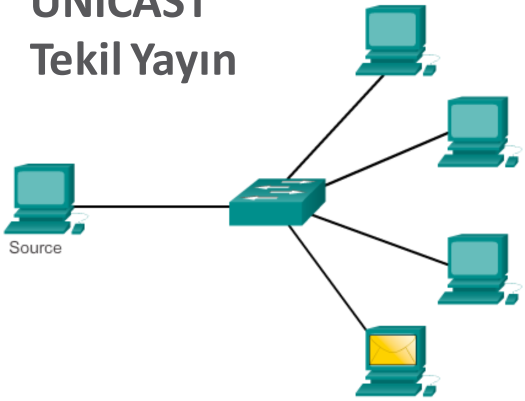
Hosts on a network has various delivery options to communicate. The different methods of communication are called as unicast, multicast, and broadcast.

Unicast: Aone-to-one delivery option means there is only a single destination for the message.

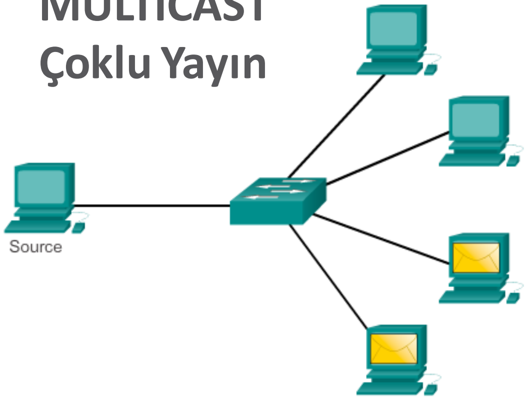
Multicast: When a host needs to send messages using a one-to many delivery option.

Broadcast: If all hosts on the network need to receive the message at the same time, a broadcast may be used. Broadcasting represents a one-to-all message delivery option.

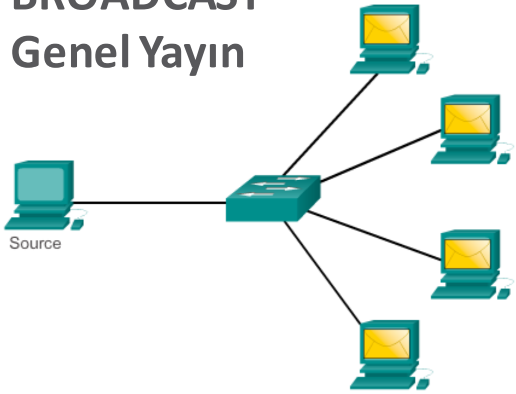
UNICAST
Tekil Yayın



MULTICAST
Çoklu Yayın



BROADCAST
Genel Yayın



Communications Protocols

Network Protocols

- Network protocols provide the means for computers to communicate on networks.
- Network protocols dictate the message encoding, formatting, encapsulation, size, timing, and delivery options.
- Networking protocols define a common format and set of rules for exchanging messages between devices.
- Some common networking protocols are Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP), and Internet Protocol (IP).

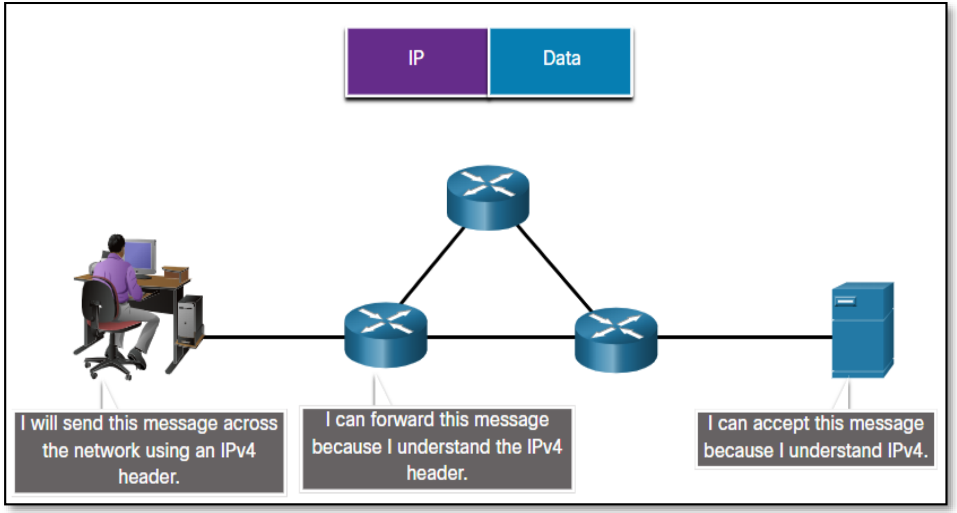
Note: *IP in this course refers to both the IPv4 and IPv6 protocols. IPv6 is the most recent version of IP and will eventually replace the more common IPv4.*

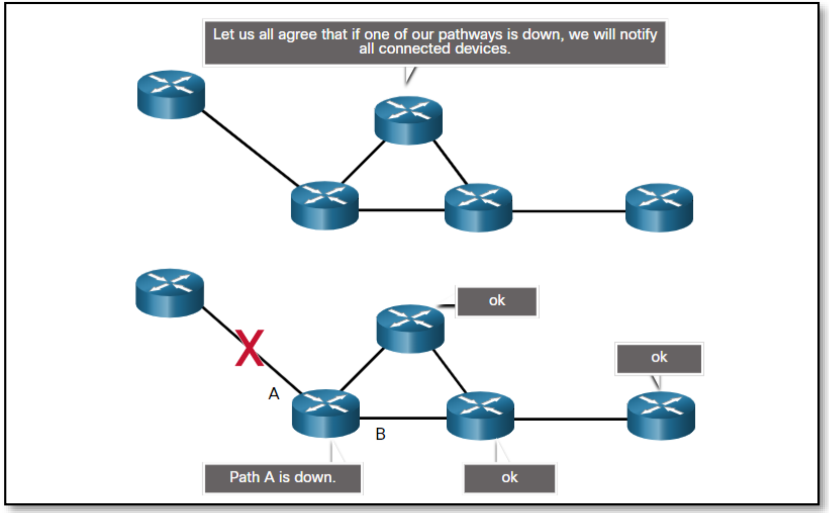
Communications Protocols

Network Protocols (Contd.)

Message Structure specifies how the message is formatted or structured.

Path Sharing specifies the process by which networking devices share information about pathways with other networks.


IP
Data
I will send this message across the network using an IPv4 header.
I can forward this message because I understand the IPv4 header.
I can accept this message because I understand IPv4.

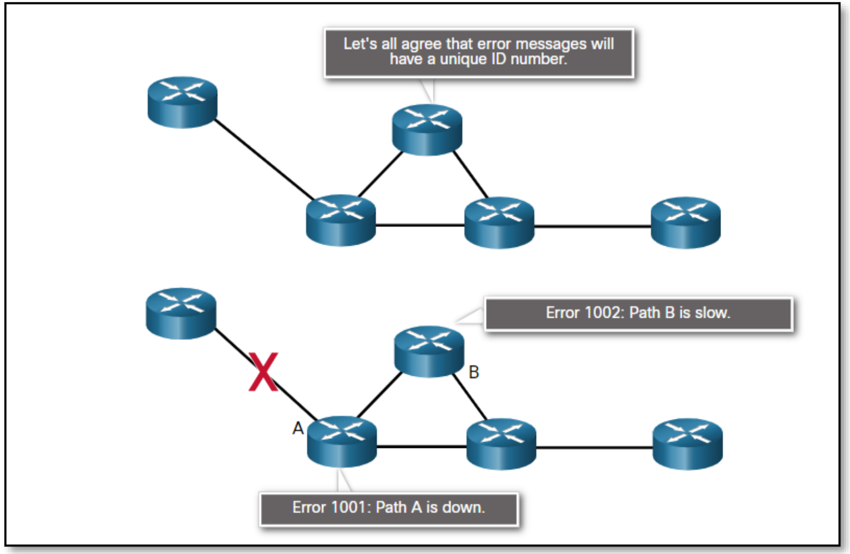

Let us all agree that if one of our pathways is down, we will notify all connected devices.
ok
X
A
ok
B
Path A is down.
ok

Communications Protocols

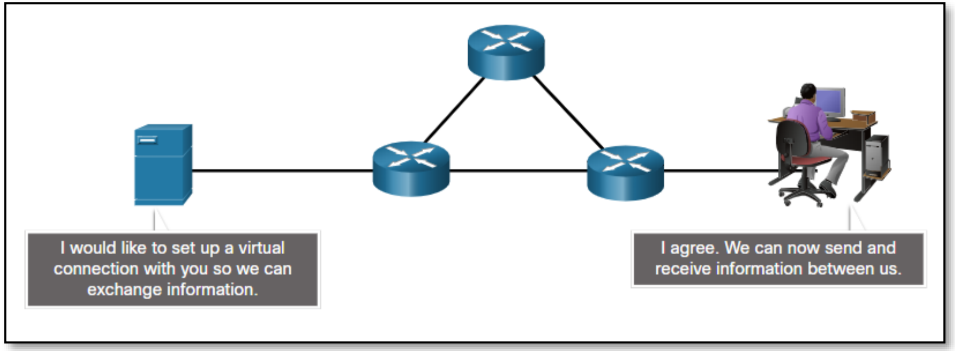
Network Protocols (Contd.)

Information Sharing specifies how and when error and system messages are passed between devices.

Session Management manages the setup and termination of data transfer sessions.



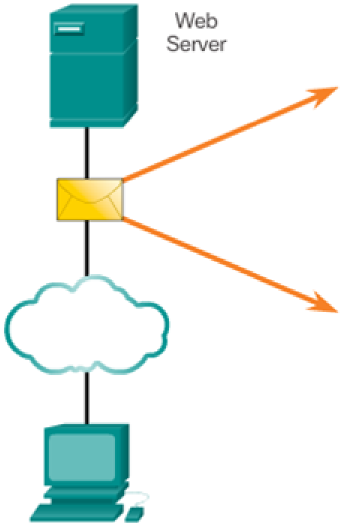
Let's all agree that error messages will have a unique ID number.
Error 1002: Path B is slow.
B
A
Error 1001: Path A is down.



I would like to set up a virtual connection with you so we can exchange information.
I agree. We can now send and receive information between us.

Protokollerin Etkileşimi

- Uygulama Protokolü – Hypertext Transfer Protocol (HTTP)
- Taşıma Protokolü – Geçiş Kontrol Protokolü (TCP)
- İnternet Protokolü – İnternet Protokolü (IP)
- Ağ Erişim Protokolleri – Veri Bağlantısı katmanı ve Fiziksel katman



Layer Name	Protocol Stack
Application	Hypertext Transfer Protocol (HTTP)
Transport	Transmission Control Protocol (TCP)
Internet	Internet Protocol (IP)
Network Access	Ethernet

Reference Models

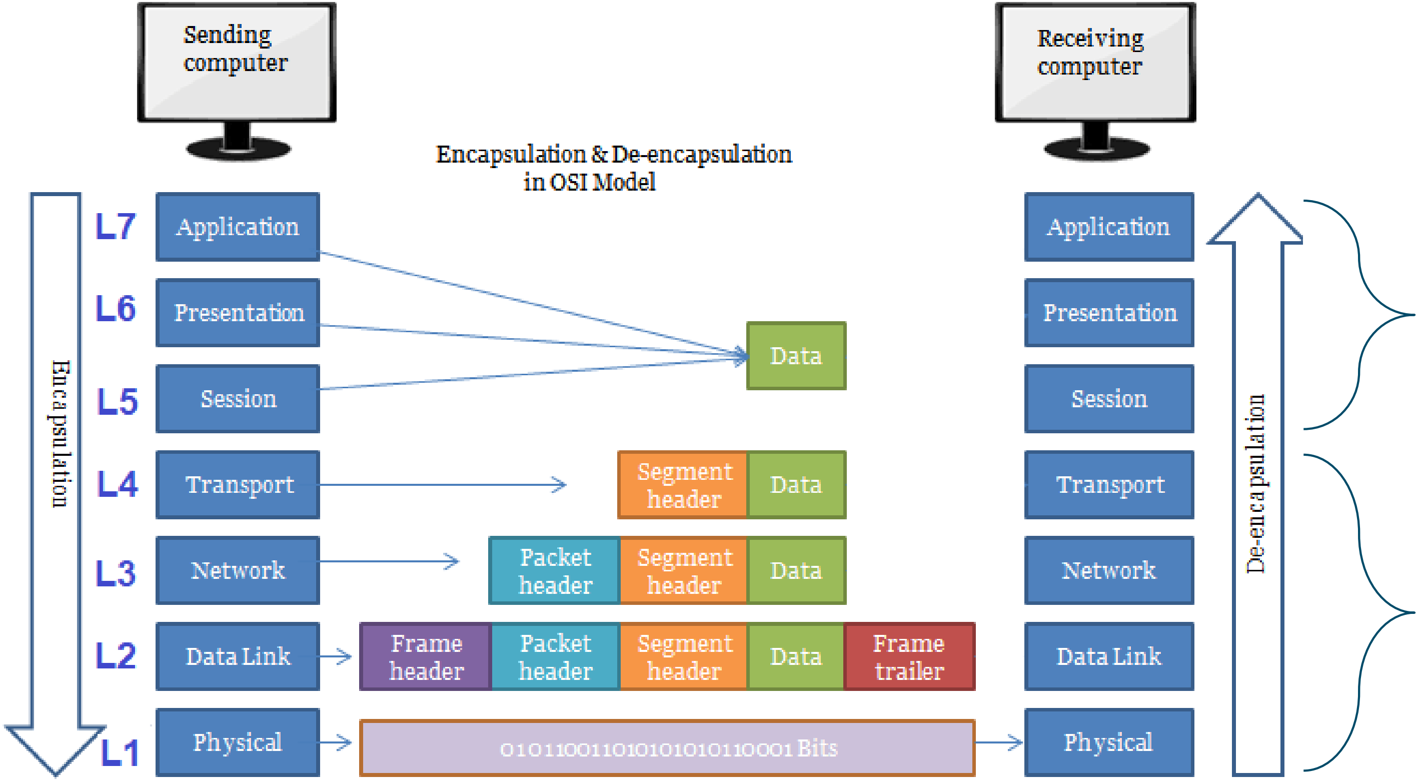
Communications Protocols

The OSI Reference Model (Contd.)

OSI Model Layer	Description
7 - Application	Contains protocols used for process-to-process communications
6 - Presentation	Provides representation of the data transferred between application layer services
5 - Session	Provides services to the presentation layer to organize its dialogue and to manage data exchange
4 - Transport	Defines services to segment, transfer, and reassemble the data for individual communications between the end devices
3 - Network	Provides services to exchange the individual pieces of data over the network
2 - Data Link	Describe methods for exchanging data frames between devices over a common media
1 - Physical	Describe the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical connections for a bit transmission between devices

Referans Modelleri

OSI Referans Modeli

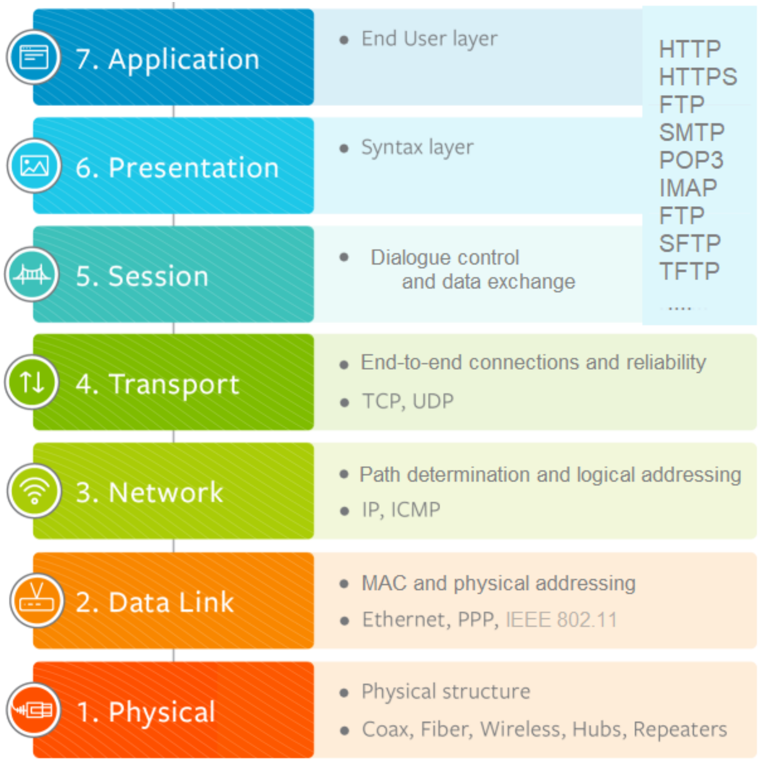


UYGULAMA KATMANLARI

DATA İLETİMİ İLE İLGİLİ KATMANLARI

Referans Modelleri

OSI Referans Modeli



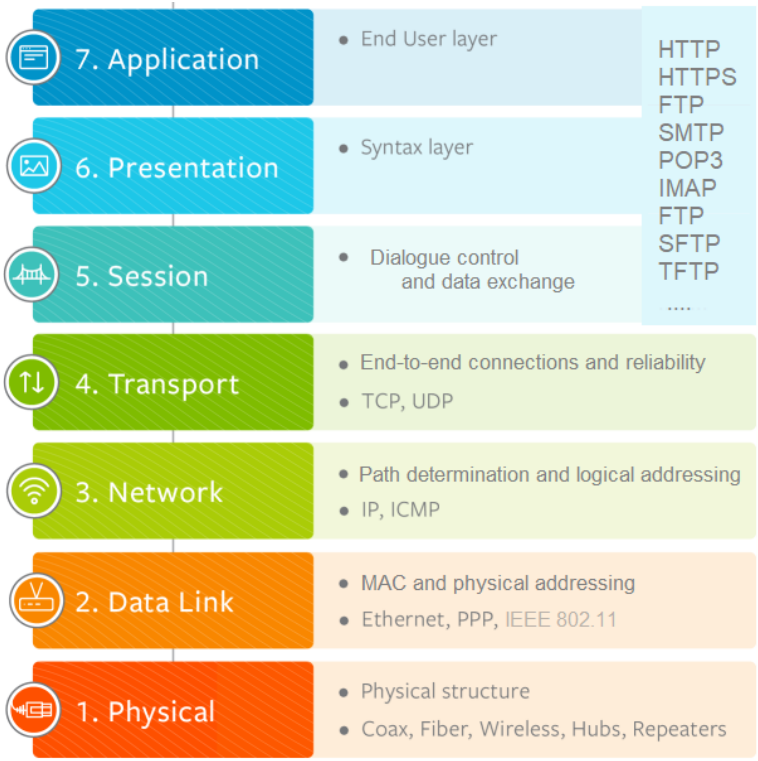
7. Application	End User layer	HTTP HTTPS FTP SMTP POP3 IMAP FTP SFTP TFTP ....
6. Presentation	Syntax layer	
5. Session	Dialogue control and data exchange	
4. Transport	End-to-end connections and reliability TCP, UDP	
3. Network	Path determination and logical addressing IP, ICMP	
2. Data Link	MAC and physical addressing Ethernet, PPP, IEEE 802.11	
1. Physical	Physical structure Coax, Fiber, Wireless, Hubs, Repeaters	

UYGULAMA
KATMANLARI

DATA
İLETİMİ İLE İLGİLİ
KATMANLARI

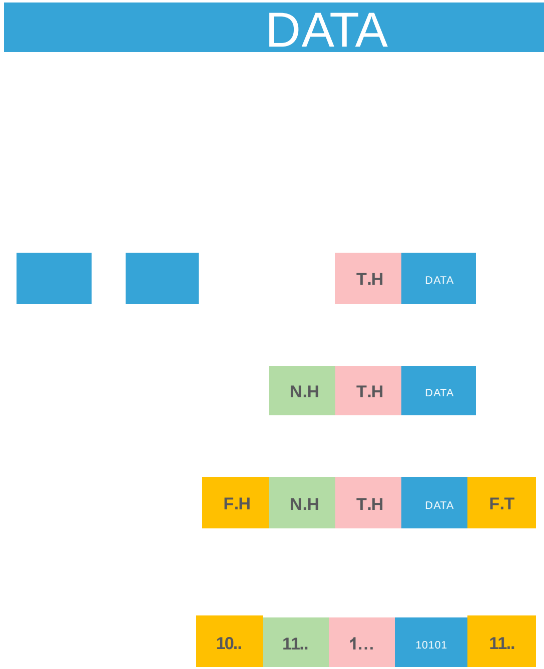
Referans Modelleri

OSI Referans Modeli



7. Application	End User layer
6. Presentation	Syntax layer
5. Session	Dialogue control and data exchange
4. Transport	End-to-end connections and reliability TCP, UDP
3. Network	Path determination and logical addressing IP, ICMP
2. Data Link	MAC and physical addressing Ethernet, PPP, IEEE 802.11
1. Physical	Physical structure Coax, Fiber, Wireless, Hubs, Repeaters

HTTP
HTTPS
FTP
SMTP
POP3
IMAP
FTP
SFTP
TFTP
....



seq.number
ack.number
source port
dest.port

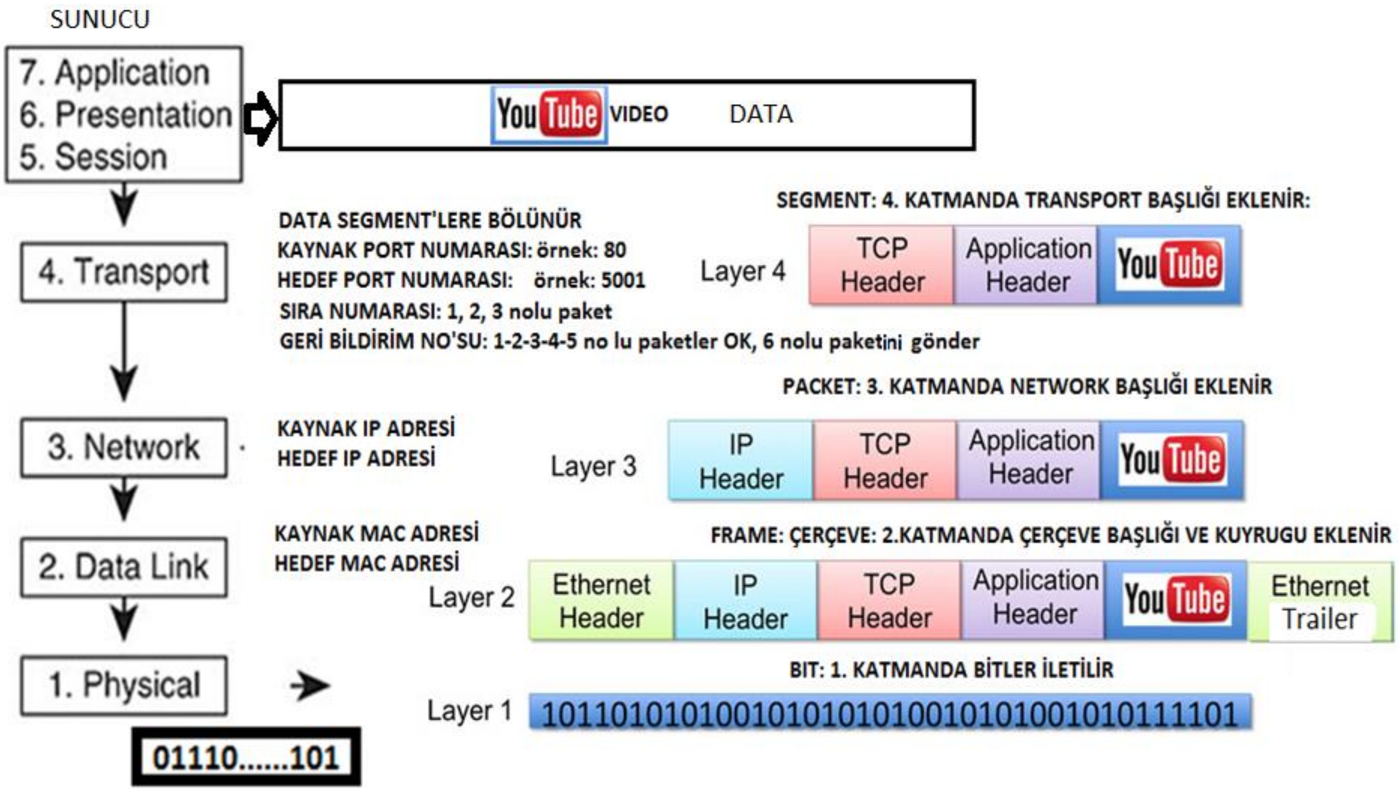
source IP
dest. IP

source MAC
dest. MAC
+
Kuyruk:hata kontrolü

bitlerin iletimi

Referans Modelleri

OSI Referans Modeli



SUNUCU

7. Application
6. Presentation
5. Session

You Tube VIDEO DATA

4. Transport

DATA SEGMENT'LERE BÖLÜNÜR
KAYNAK PORT NUMARASI: örnek: 80
HEDEF PORT NUMARASI: örnek: 5001
SIRA NUMARASI: 1, 2, 3 nolu paket
GERİ BİLDİRİM NO'SU: 1-2-3-4-5 no lu paketler OK, 6 nolu paketini gönder

SEGMENT: 4. KATMANDA TRANSPORT BAŞLIĞI EKLENİR:

Layer 4 | TCP Header | Application Header | You Tube

3. Network

KAYNAK IP ADRESİ
HEDEF IP ADRESİ

PACKET: 3. KATMANDA NETWORK BAŞLIĞI EKLENİR

Layer 3 | IP Header | TCP Header | Application Header | You Tube

2. Data Link

KAYNAK MAC ADRESİ
HEDEF MAC ADRESİ

FRAME: ÇERÇEVE: 2.KATMANDA ÇERÇEVE BAŞLIĞI VE KUYRUGU EKLENİR

Layer 2 | Ethernet Header | IP Header | TCP Header | Application Header | You Tube | Ethernet Trailer

1. Physical

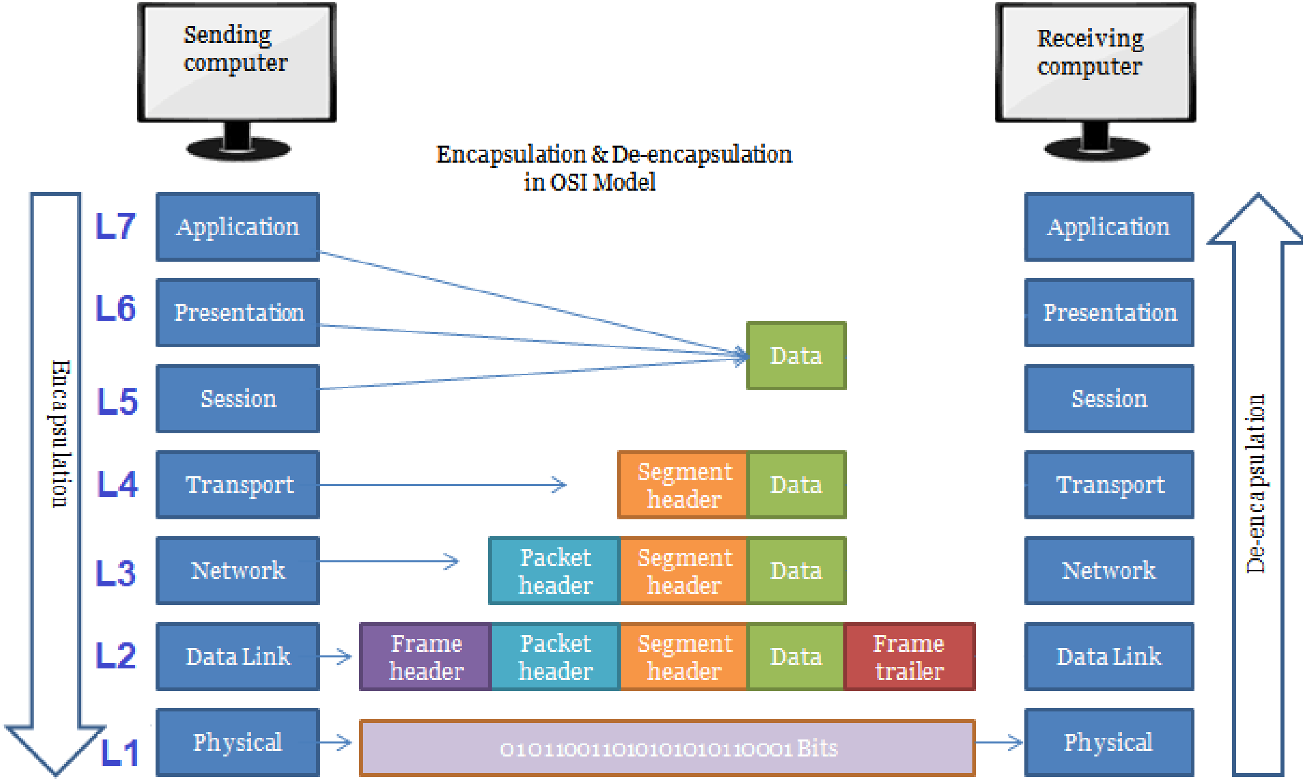
01110......101

BIT: 1. KATMANDA BİTLER İLETİLİR

Layer 1 | 1011010101001010101010010101001010111101

Referans Modelleri

OSI Referans Modeli



Akşam

Pazarından

Sonra

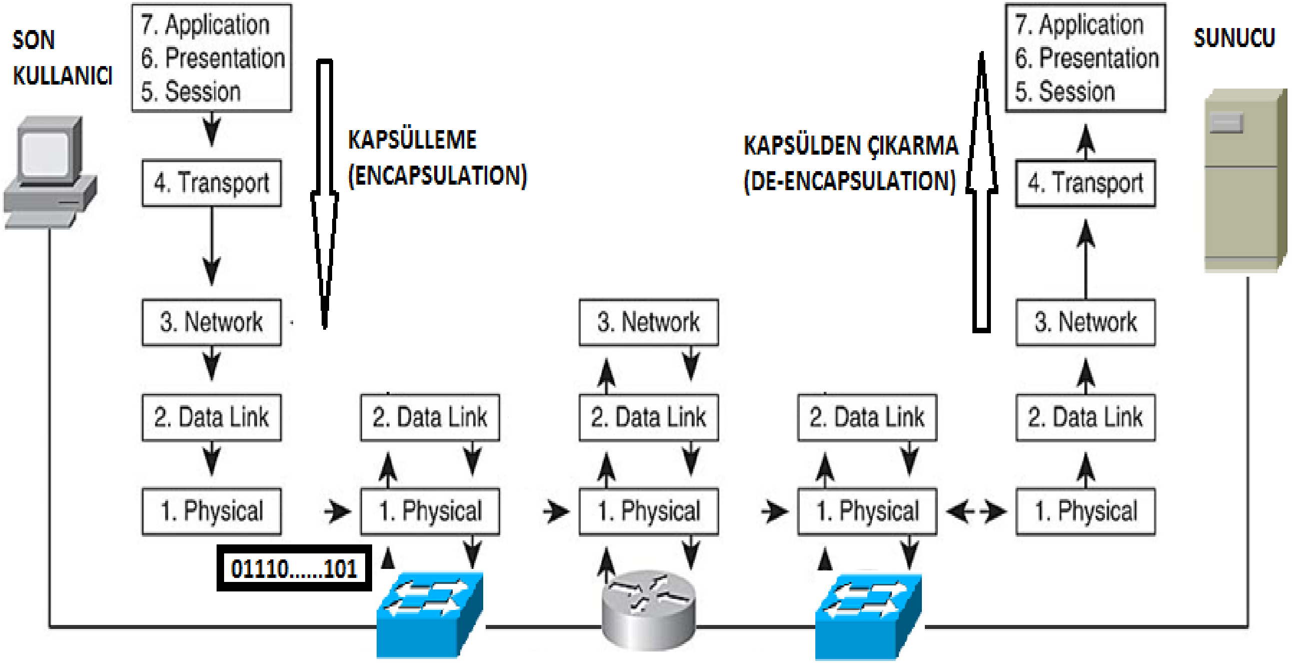
Tüm

Niğde

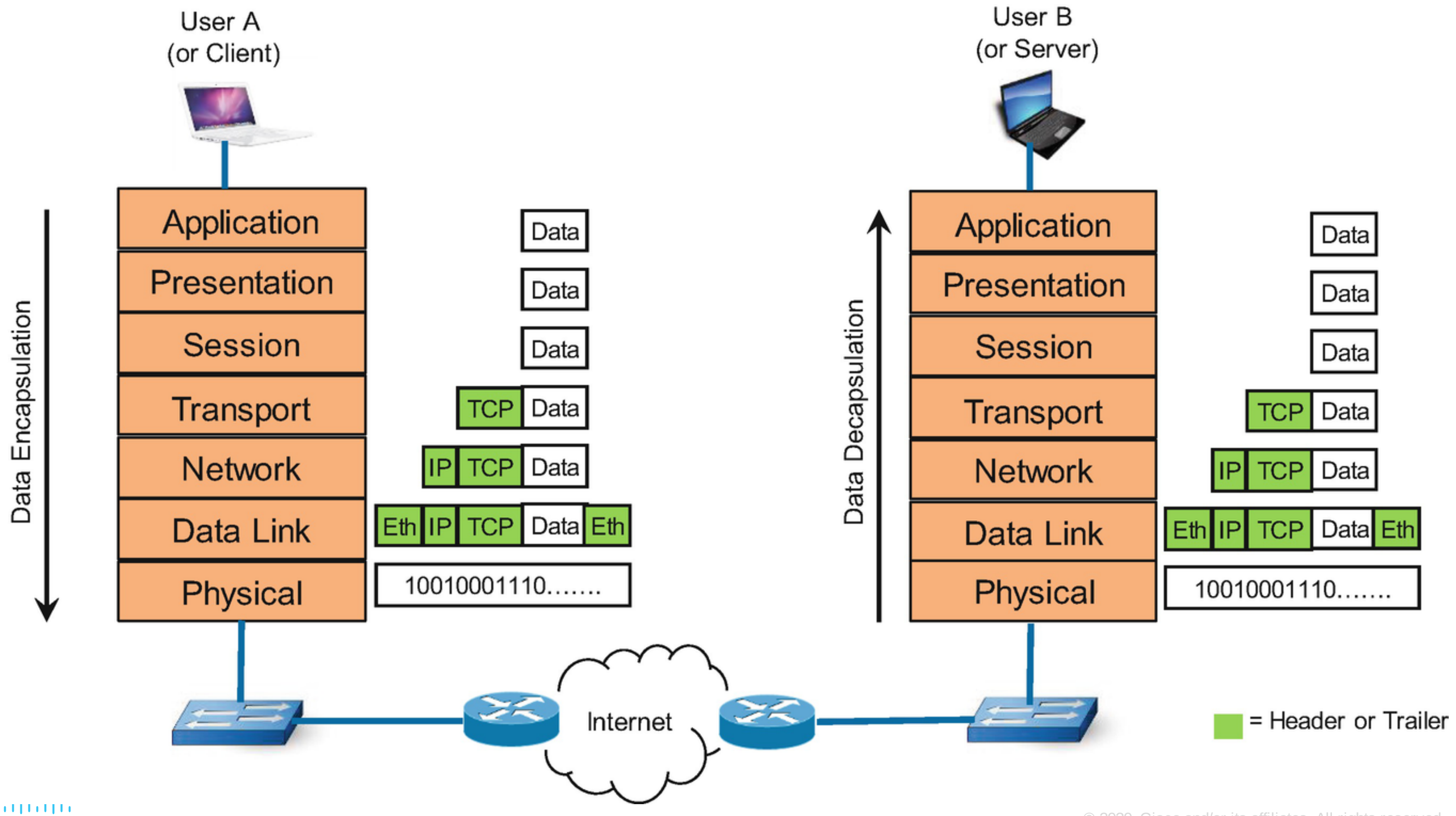
Domatesleri

Patlaktır

OSI Referans Modeli



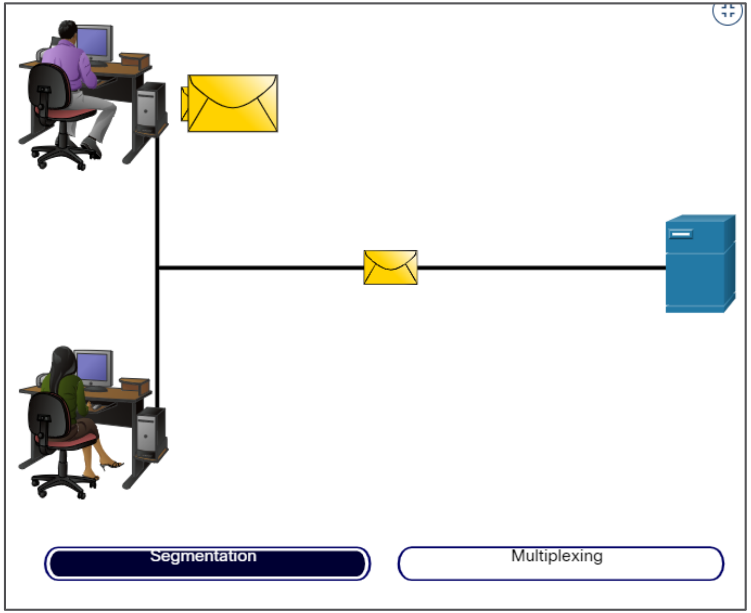
OSI Referans Modeli



5.3 Data Encapsulation

Segmenting Messages

- If large streams of data is sent across a network, it would result in delays. If any link in the interconnected network failed during the transmission, it will result in lost of complete message.
- Segmentation is the process of dividing a stream of data into smaller units for transmissions over the network.
- Segmentation is necessary as networks use the TCP/IP protocol to send data in individual IP packets. Each packet is sent separately and the packets containing segments for the same destination can be sent over different paths.

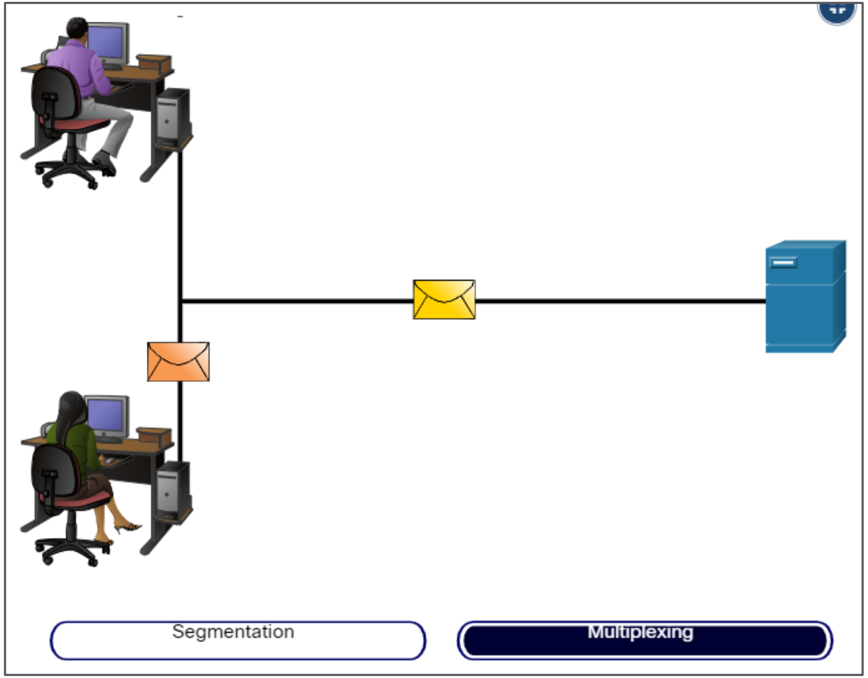


Data Encapsulation

Segmenting Messages (Contd.)

Benefits of segmenting messages:

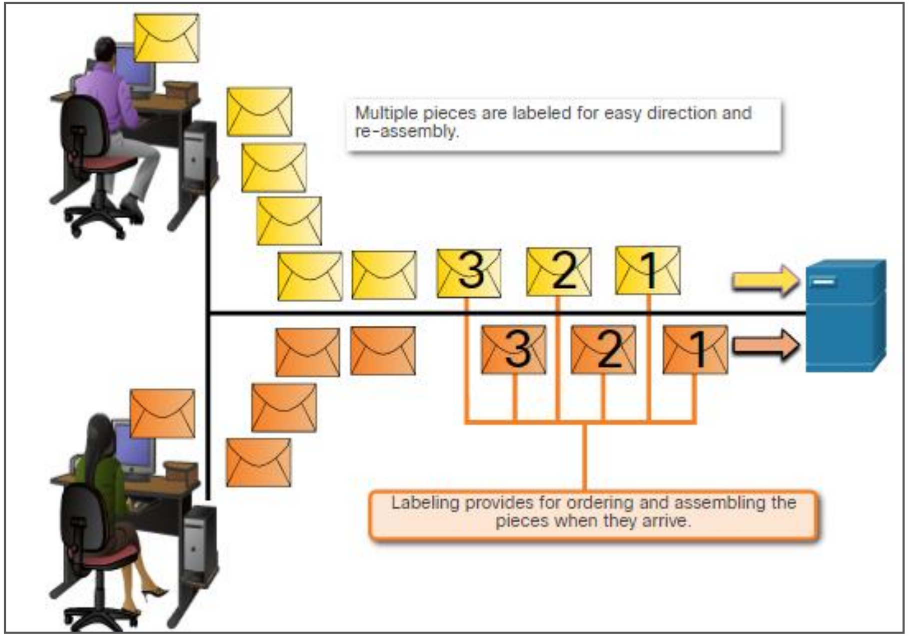
- **Increases speed** - As a large data stream is segmented into packets, more data can be sent over the network without tying up a communications link. This allows many different conversations to be interleaved on the network called *multiplexing*.
- **Increases efficiency** - If a single segment fails to reach its destination, only that segment needs to be retransmitted instead of resending the entire data stream.



Data Encapsulation

Sequencing

- While transmitting messages using segmentation and multiplexing, there is a possibility of data to reach the destination in a collapsed order.
- Each segment of the message must go through a sequencing process to ensure that it gets to the correct destination and can be reassembled similar to the content of the original message.
- TCP is responsible for sequencing the individual segments


Multiple pieces are labeled for easy direction and re-assembly.
3
2
1
3
2
1
Labeling provides for ordering and assembling the pieces when they arrive.

Data Encapsulation

Protocol Data Units

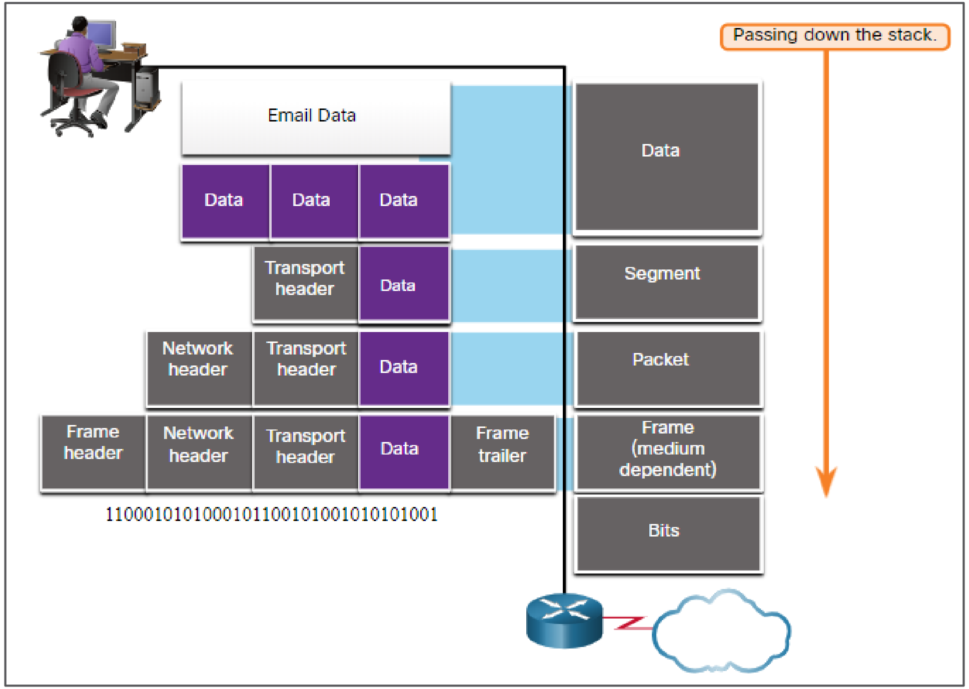
- As application data is passed down the protocol stack on its way to be transmitted across the network media, various protocol information is added at each level. This is known as the encapsulation process.
- The form that a piece of data takes at any layer is called a Protocol Data Unit (PDU).
- During encapsulation, each succeeding layer encapsulates the PDU that it receives from the layer above in accordance with the protocol being used.
- At each stage of the process, a PDU has a different name to reflect its new functions.

***Note**: Although the UDP PDU is called datagram, IP packets are sometimes also referred to as IP datagrams.*

Data Encapsulation

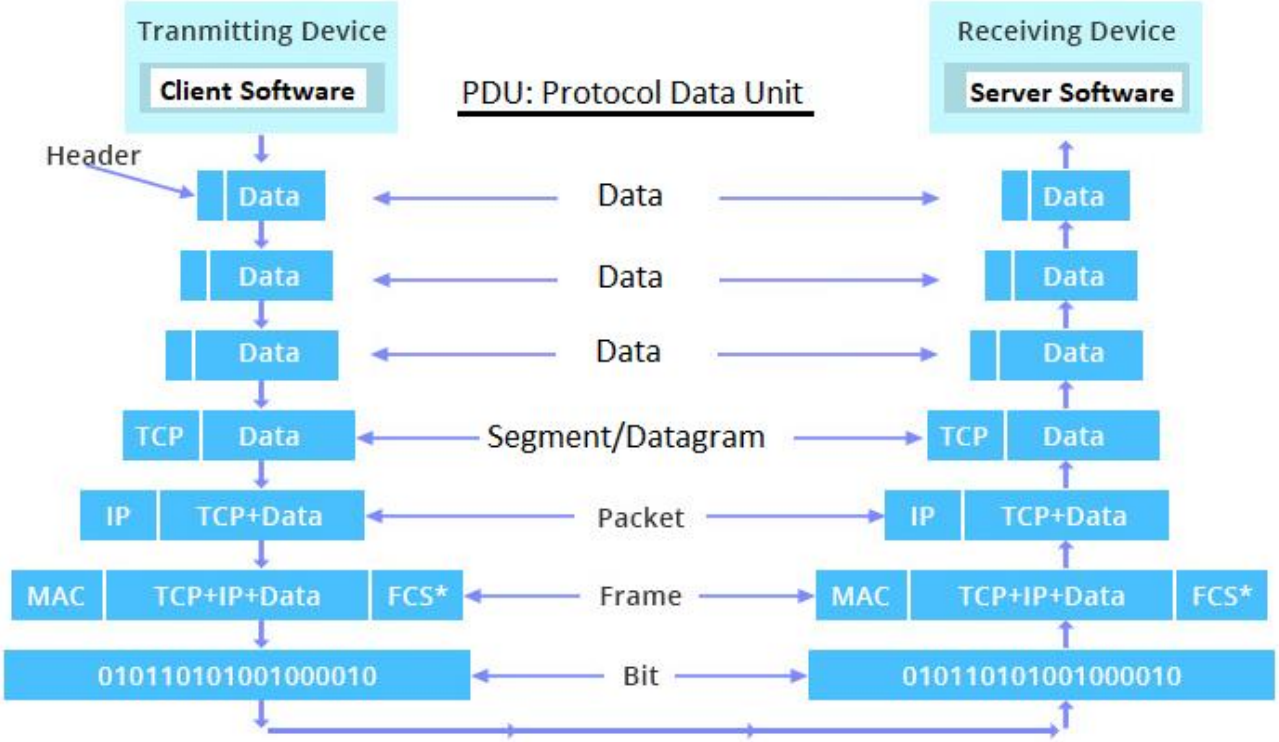
Protocol Data Units (Contd.)

- The PDUs for each form of data are:
  - **Data** - The general term for the PDU used at the application layer
  - **Segment** - Transport layer PDU
  - **Packet** - Network layer PDU
  - **Frame** - Data Link layer PDU
  - **Bits** - Physical layer PDU used when physically transmitting data over the medium



***Note**: If the Transport header is TCP, then it is a segment. If the Transport header is UDP then it is a datagram.*

OSI Referans Modeli

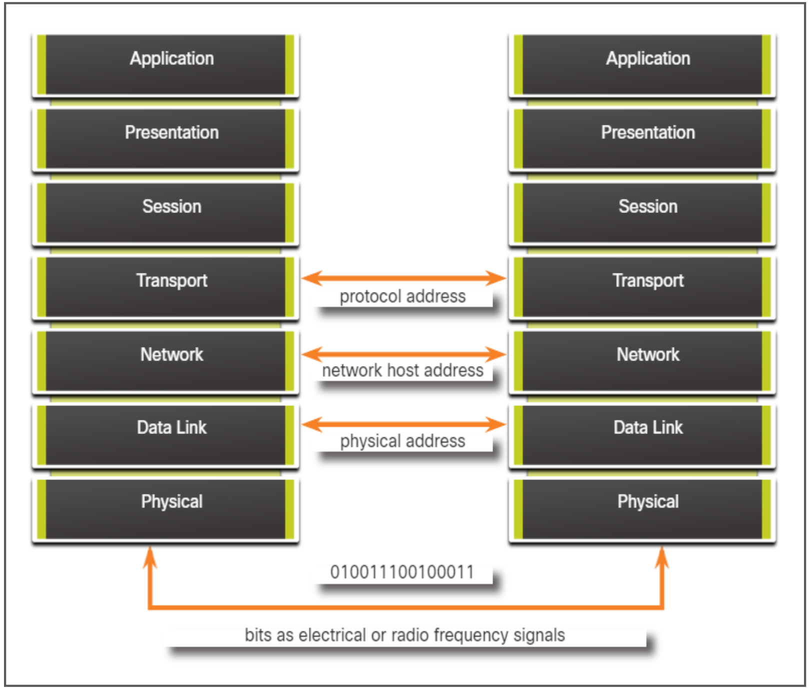


FCS＊: Frame Check Sequence

Data Encapsulation

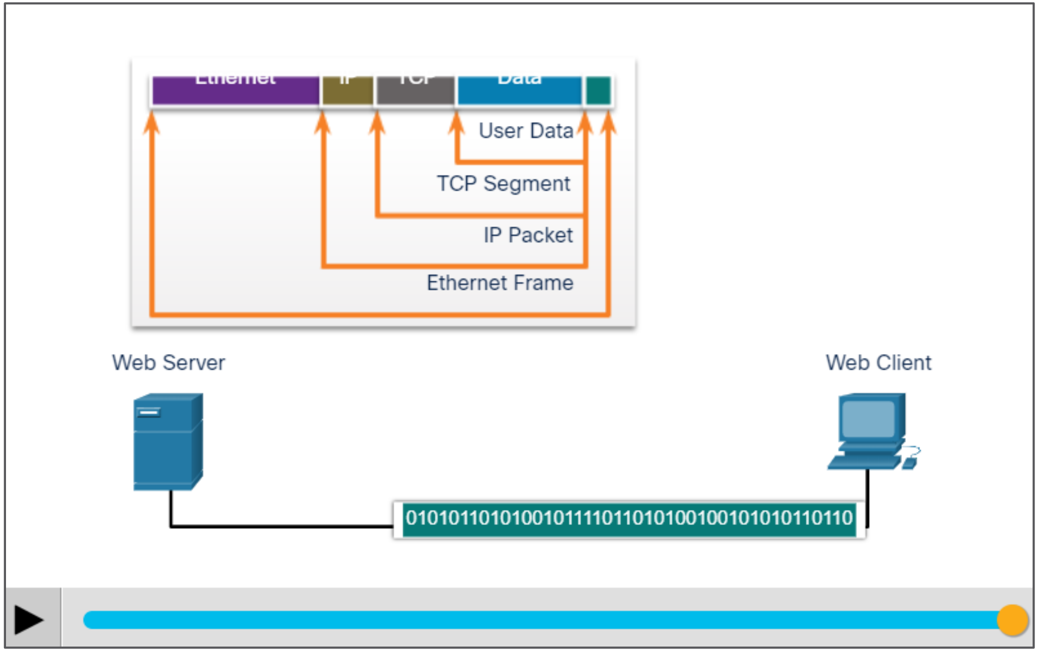
Three Addresses

- Network protocols require addresses to be used for network communication.
- The OSI transport, network, and data link layers use addressing in some form.
- The transport layer uses protocol addresses in the form of port numbers to identify network applications.
- The network layer specifies addresses that identify the networks that clients and servers are attached to.
- Data link layer specifies the devices on the local LAN that should handle data frames.
- All three addresses are required for client-server communication.



Encapsulation Example

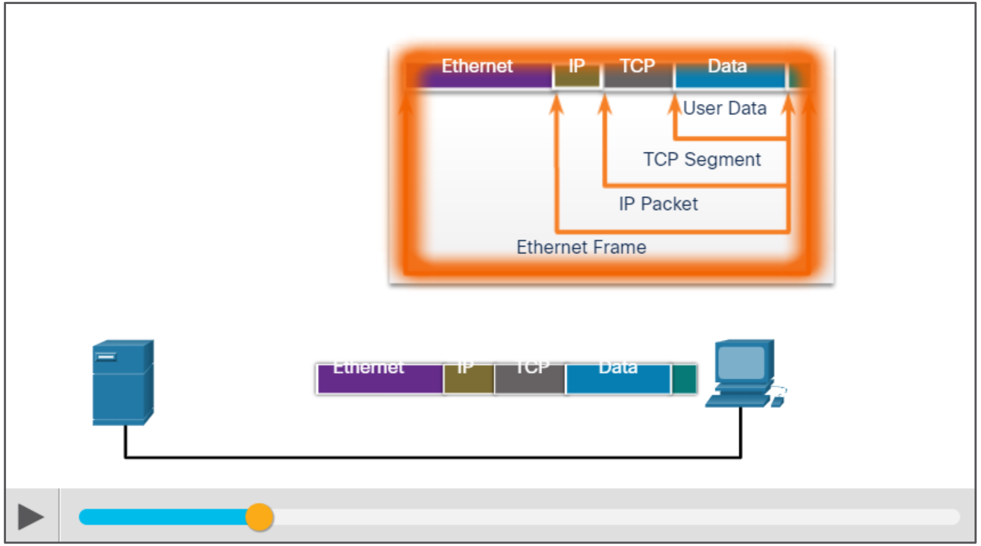
- When messages are being sent on a network, the encapsulation process works from top to bottom.
- At each layer, the upper layer information is considered data within the encapsulated protocol. For example, the TCP segment is considered data within the IP packet.



Data Encapsulation

De-encapsulation Example

- This process is reversed at the receiving host and is known as de-encapsulation.
- De-encapsulation is the process used by a receiving device to remove one or more of the protocol headers.
- The data is de-encapsulated as it moves up the stack toward the end-user application.



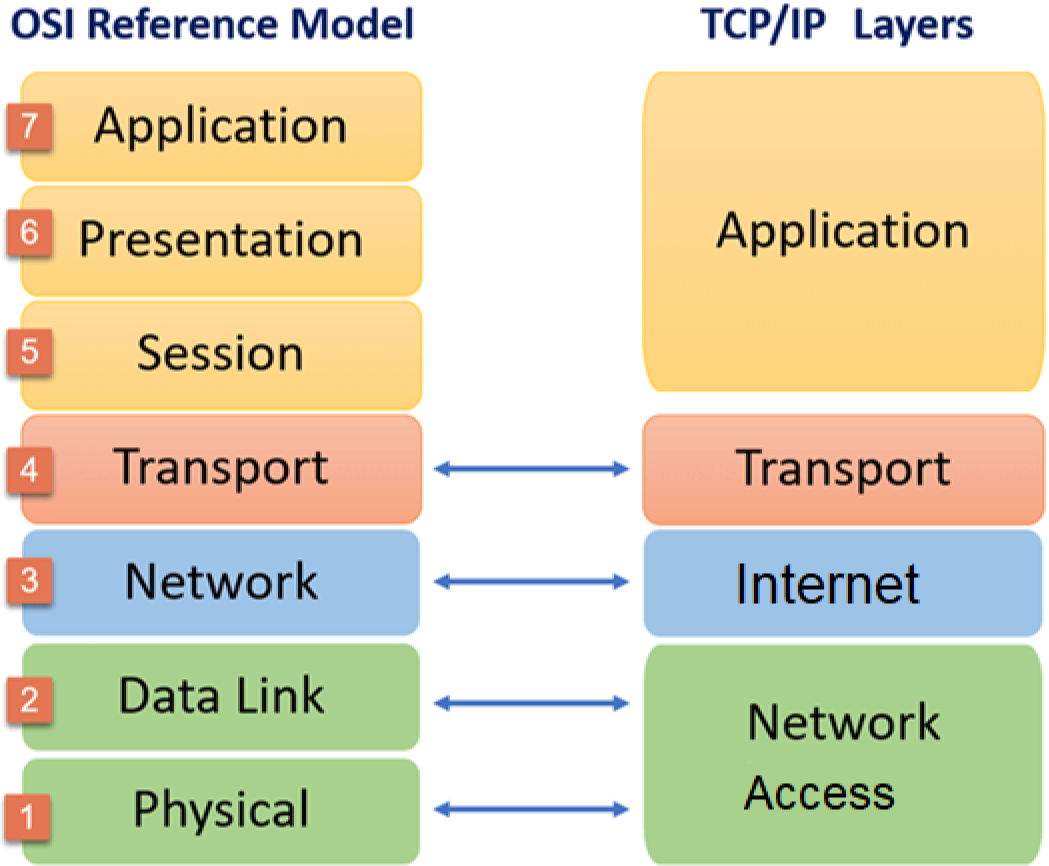
TCP/ IP Protocol Suite

The OSI Reference Model

- The OSI reference model provides list of functions and services that can occur at each layer.
- This type of model provides consistency within all types of network protocols and services by describing what must be done at a particular layer, but not prescribing how it should be accomplished.
- It also describes the interaction of each layer with the layers directly above and below.
- Note that while the TCP/IP model layers are referred only by name but the seven OSI model layers are more often referred by number rather than by name.

Communications Protocols

The TCP/IP Protocol Suite



Communications Protocols

The TCP/IP Protocol Model

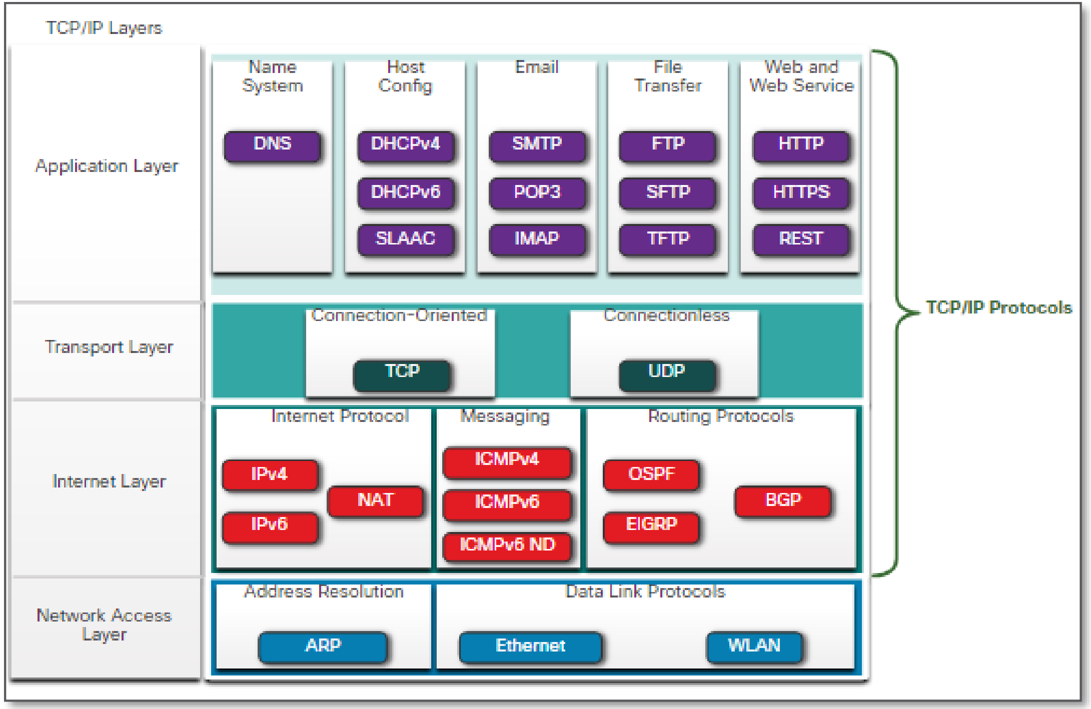
- The TCP/IP protocol model is also referred to as the internet model.
- It describes the functions that occur at each layer of protocols within the TCP/IP suite. TCP/IP is also used as a reference model.

TCP/IP Model Layer	Description
4 - Application	Represents data to the user, plus encoding and dialog control
3 - Transport	Supports communication between various devices across diverse networks
2 - Internet	Determines the best path through the network
1 - Network Access	Controls the hardware devices and media that make up the network

Communications Protocols

The TCP/IP Protocol Suite

- TCP/IP is the protocol suite used by the internet and the networks of today.
- TCP/IP has two important aspects for vendors and manufacturers:
  - **Open standard protocol suite** - This means it is freely available to the public and can be used by any vendor on their hardware or in their software.
  - **Standards-based protocol suite** - This means it has been endorsed by the networking industry and approved by a standards organization.



TCP/IP Layers

TCP/IP Protocols

Application Layer

Name System: DNS

Host Config: DHCPv4, DHCPv6, SLAAC

Email: SMTP, POP3, IMAP

File Transfer: FTP, SFTP, TFTP

Web and Web Service: HTTP, HTTPS, REST

Transport Layer

Connection-Oriented: TCP

Connectionless: UDP

Internet Layer

Internet Protocol: IPv4, IPv6, NAT

Messaging: ICMPv4, ICMPv6, ICMPv6 ND

Routing Protocols: OSPF, EIGRP, BGP

Network Access Layer

Address Resolution: ARP

Data Link Protocols: Ethernet, WLAN

The TCP/IP Protocol Suite (Contd.)

Lets have a look at the brief description of protocols at each layer.

Application Layer

- **Name System - DNS** (Domain Name System): Translates domain names into IP addresses.

Host Config

Protocol	Description
DHCPv4 (Dynamic Host Configuration Protocol for IPv4)	Dynamically assigns IPv4 addressing information to DHCPv4 clients at start-up and allows the addresses to be re-used when no longer needed.
DHCPv6 (Dynamic Host Configuration Protocol for IPv6)	It is similar to DHCPv4. Dynamically assigns IPv6 addressing information to DHCPv6 clients at start-up.
SLAAC (Stateless Address Autoconfiguration)	A method that allows a device to obtain its IPv6 addressing information without using a DHCPv6 server.

The TCP/IP Protocol Suite (Contd.)

Email

Protocol	Description
SMTP (Simple Mail Transfer Protocol)	Enables clients to send email to a mail server and enables servers to send email to other servers.
POP3 (Post Office Protocol version 3)	Enables clients to retrieve email from a mail server and download the email to the client's local mail application.
IMAP (Internet Message Access Protocol)	Enables clients to access email stored on a mail server as well as maintaining email on the server.

File Transfer

Protocol	Description
FTP (File Transfer Protocol)	Sets the rules that enable a user on one host to access and transfer files to and from another host over a network.
SFTP (SSH File Transfer Protocol)	Used to establish a secure file transfer session in which the file transfer is encrypted.
TFTP (Trivial File Transfer Protocol)	A simple and connectionless protocol with best-effort, unrecognized file delivery.

The TCP/IP Protocol Suite (Contd.)

Web and Web Service

Protocol	Description
HTTP (Hypertext Transfer Protocol)	A set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web.
HTTPS (HTTP Secure)	A secure form of HTTP that encrypts the data that is exchanged over the World Wide Web.
REST (Representational State Transfer)	A web service that uses application programming interfaces (APIs) and HTTP requests to create web applications

The TCP/IP Protocol Suite (Contd.)

Transport Layer

- **Connection-Oriented - TCP** (Transmission Control Protocol): Enables *reliable communication* between processes running on separate hosts and provides *reliable transmissions* that confirm successful delivery.
- **Connectionless - UDP** (User Datagram Protocol): Enables a process running on one host to send packets to a process running on another host.

The TCP/IP Protocol Suite (Contd.)

Internet Layer

Internet Protocol

Protocol	Description
IPv4 (Internet Protocol version 4)	Receives message segments from the transport layer, packages messages into packets, and addresses packets for end-to-end delivery over a network. IPv4 uses a 32-bit address.
IPv6 (IP version 6)	Similar to IPv4 but uses a 128-bit address.
NAT (Network Address Translation)	Translates IPv4 addresses from a private network into globally unique public IPv4 addresses.

Communications Protocols

The TCP/IP Protocol Suite (Contd.)

Messaging

Protocol	Description
ICMPv4 (Internet Control Message Protocol for IPv4)	Provides feedback from a destination host to a source host about errors in packet delivery.
ICMPv6 (ICMP for IPv6)	Similar functionality to ICMPv4 but is used for IPv6 packets.
ICMPv6 ND (ICMPv6 Neighbor Discovery)	Includes four protocol messages that are used for address resolution and duplicate address detection.

Routing Protocols

Protocol	Description
OSPF (Open Shortest Path First)	Link-state routing protocol that uses a hierarchical design based on areas. OSPF is an open standard interior routing protocol.
EIGRP (Enhanced Interior Gateway Routing Protocol)	A Cisco proprietary routing protocol that uses a composite metric based on bandwidth, delay, load and reliability.
BGP (Border Gateway Protocol)	An open standard exterior gateway routing protocol used between Internet Service Providers (ISPs).

The TCP/IP Protocol Suite (Contd.)

Network Access Layer

- **Address Resolution - ARP** (Address Resolution Protocol): Provides dynamic address mapping between an IPv4 address and a hardware address.
- **Data Link Protocols -**
  - **Ethernet**: Defines the rules for wiring and signaling standards of the network access layer.
  - **WLAN** (Wireless Local Area Network): Defines the rules for wireless signaling across the 2.4 GHz and 5 GHz radio frequencies.

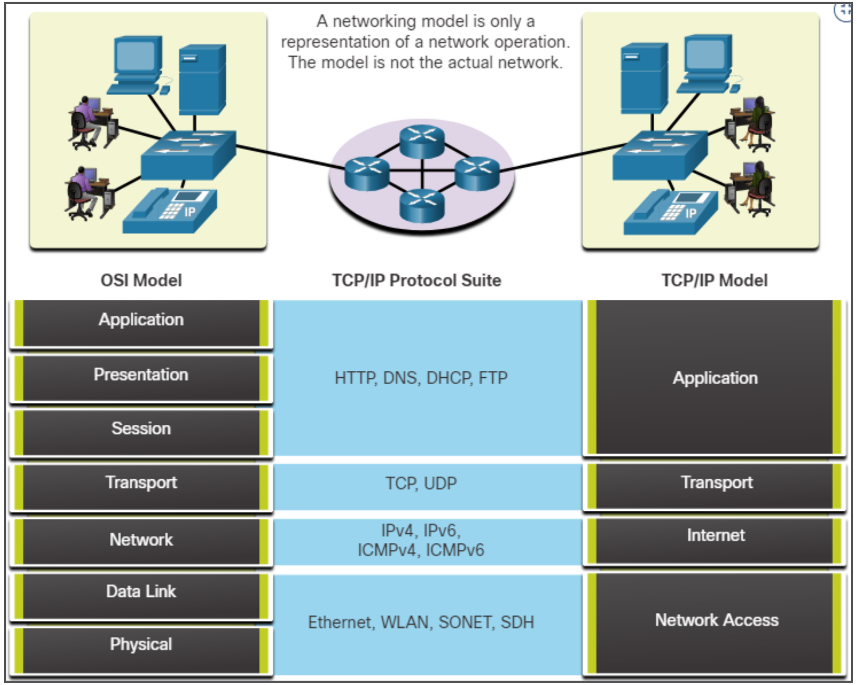
The Benefits of Using a Layered Model

A layered model is used to modularize the operations of a network into manageable layers. These are the benefits of using a layered model:

- Assisting in protocol design
- Fostering competition
- Preventing technology or capability changes
- Providing a common language

Two layered models that are used to describe network operations are:

- Open System Interconnection (OSI) Reference Model
- TCP/IP Reference Model

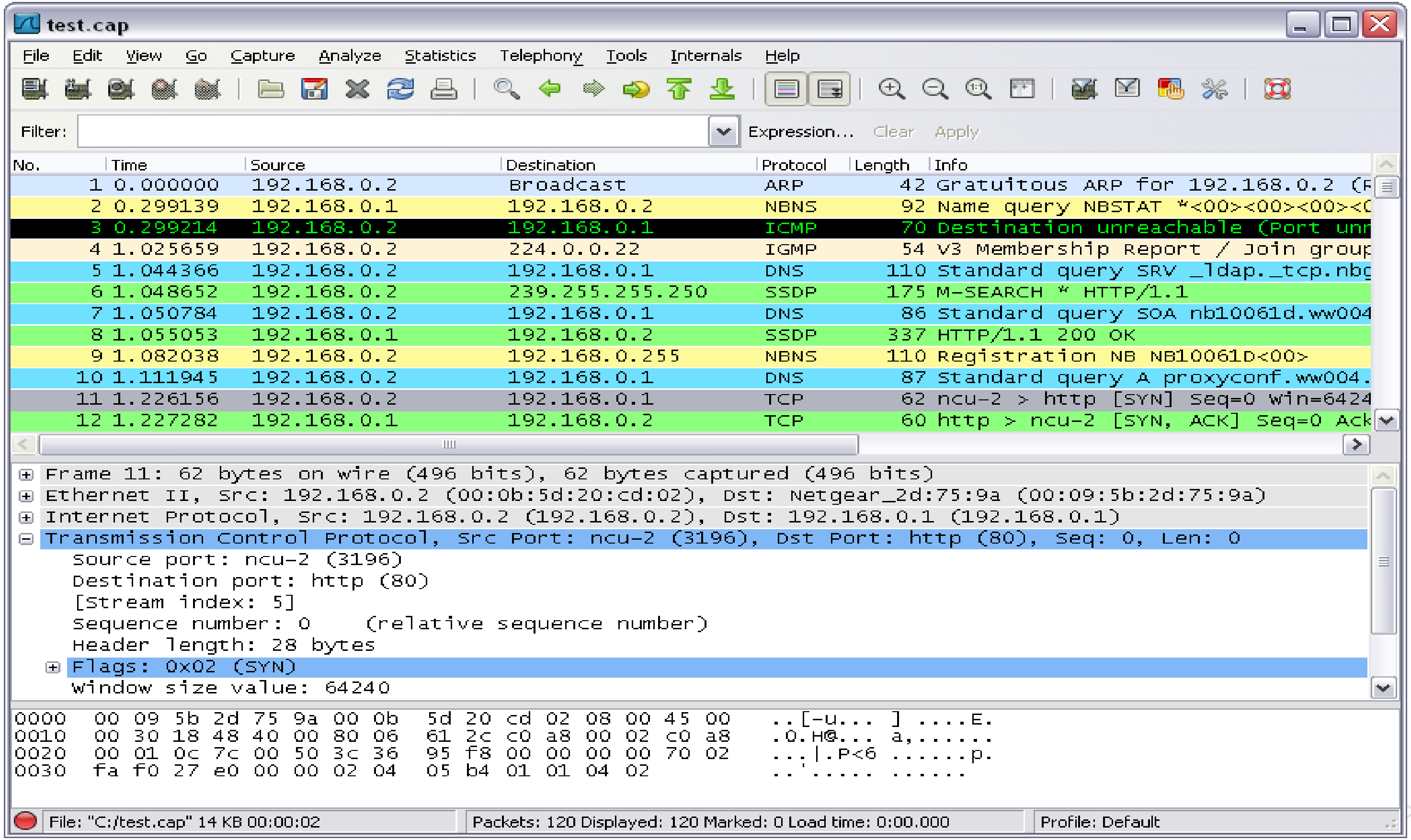


A networking model is only a representation of a network operation. The model is not the actual network.

OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application	HTTP, DNS, DHCP, FTP	Application
Presentation		
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	Ethernet, WLAN, SONET, SDH	Network Access
Physical		

Uzak Kaynaklara Erişme

Ağ Trafiğini Görüntülemek için Wireshark'ı Kullanma


test.cap
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.    Time       Source         Destination       Protocol Length Info
     1 0.000000   192.168.0.2    Broadcast          ARP         42 Gratuitous ARP for 192.168.0.2 (R
     2 0.299139   192.168.0.1    192.168.0.2        NBNS        92 Name query NBSTAT *<00><00><00><0
     3 0.299214   192.168.0.2    192.168.0.1        ICMP        70 Destination unreachable (Port unr
     4 1.025659   192.168.0.2    224.0.0.22         IGMP        54 V3 Membership Report / Join group
     5 1.044366   192.168.0.2    192.168.0.1        DNS        110 Standard query SRV _ldap._tcp.nbg
     6 1.048652   192.168.0.2    239.255.255.250    SSDP       175 M-SEARCH * HTTP/1.1
     7 1.050784   192.168.0.2    192.168.0.1        DNS         86 Standard query SOA nb10061d.ww004
     8 1.055053   192.168.0.1    192.168.0.2        SSDP       337 HTTP/1.1 200 OK
     9 1.082038   192.168.0.2    192.168.0.255      NBNS       110 Registration NB NB10061D<00>
    10 1.111945   192.168.0.2    192.168.0.1        DNS         87 Standard query A proxyconf.ww004.
    11 1.226156   192.168.0.2    192.168.0.1        TCP         62 ncu-2 > http [SYN] Seq=0 Win=6424
    12 1.227282   192.168.0.1    192.168.0.2        TCP         60 http > ncu-2 [SYN, ACK] Seq=0 Ack
```

```
⊞ Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
⊞ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊟ Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0
    Source port: ncu-2 (3196)
    Destination port: http (80)
    [Stream index: 5]
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ⊞ Flags: 0x02 (SYN)
    Window size value: 64240
```

```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] .....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

File: "C:/test.cap" 14 KB 00:00:02 | Packets: 120 Displayed: 120 Marked: 0 Load time: 0:00.000 | Profile: Default

5.4 Network Protocols Summary

What Did I Learn in this Module?

- Networks come in all sizes and can be found in homes, businesses, and other organizations. The internet is the largest network in existence.
- Servers are hosts that use specialized software to enable them to respond to requests for different types of data from clients.
- Clients are hosts that use software applications such as web browsers, email clients, or file transfer applications to request data from servers.
- Larger businesses may connect to Tier 2 ISPs through a Point of Presence (POP).
- Tier 3 ISPs connect homes and businesses to the internet
- Network protocols specify many features of network communication such as message encoding, message formatting and encapsulation, and delivery options.
- Protocols specify how messages are structured and the way that networking devices share information about pathways to other networks.

Network Protocols Summary

What Did I Learn in this Module? (Contd.)

- Common protocols at the application layer of the suite are DNS, DHCP, POP3, and HTTPS.
- The OSI model has seven layers. The TCP/IP model has four layers.
- Data is broken into a series of smaller pieces and sent over the network. This is called segmentation.
- Increased speed is gained because many data conversations can happen at the same time on the network. This is called multiplexing.
- As data is passed down the protocol stack to be sent, different information is added by each layer. This process is called encapsulation.
- The form that data takes at different layer is called a protocol data unit (PDU)
- De-encapsulation is the process used by a receiving device to remove one or more of the protocol headers.