

# Module 15: Uygulama Katmanı (Application Layer)

CCNA1

Introduction to  
Networks v7.0 (ITN)



Gökhan AKIN - CCIE  
[gokhan@agyoneticileri.org](mailto:gokhan@agyoneticileri.org)

Ozan BÜK - CCIE  
[ozan@agyoneticileri.org](mailto:ozan@agyoneticileri.org)



# Module Objectives

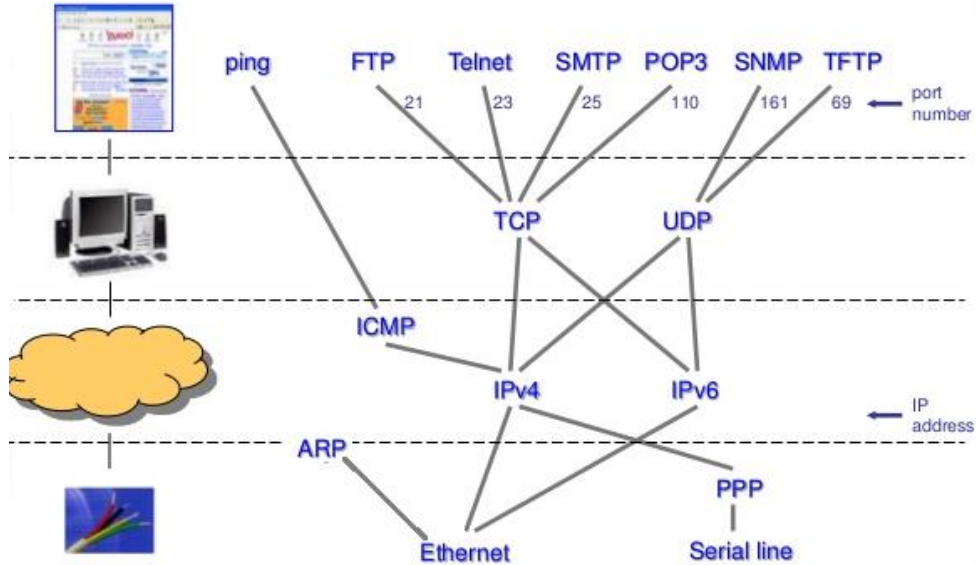
- **Module Title:** Application Layer
- **Module Objective:** Explain the operation of application layer protocols in providing support to end-user applications.

Topic Title	Topic Objective
Application, Presentation, and Session	Explain how the functions of the application layer, presentation layer, and session layer work together to provide network services to end user applications.
Peer-to-Peer	Explain how end user applications operate in a peer-to-peer network.
Web and Email Protocols	Explain how web and email protocols operate.
IP Addressing Services	Explain how DNS and DHCP operate.
File Sharing Services	Explain how file transfer protocols operate.

# 15.1 Application, Presentation, and Session

# Application, Presentation, and Session

## Application Layer

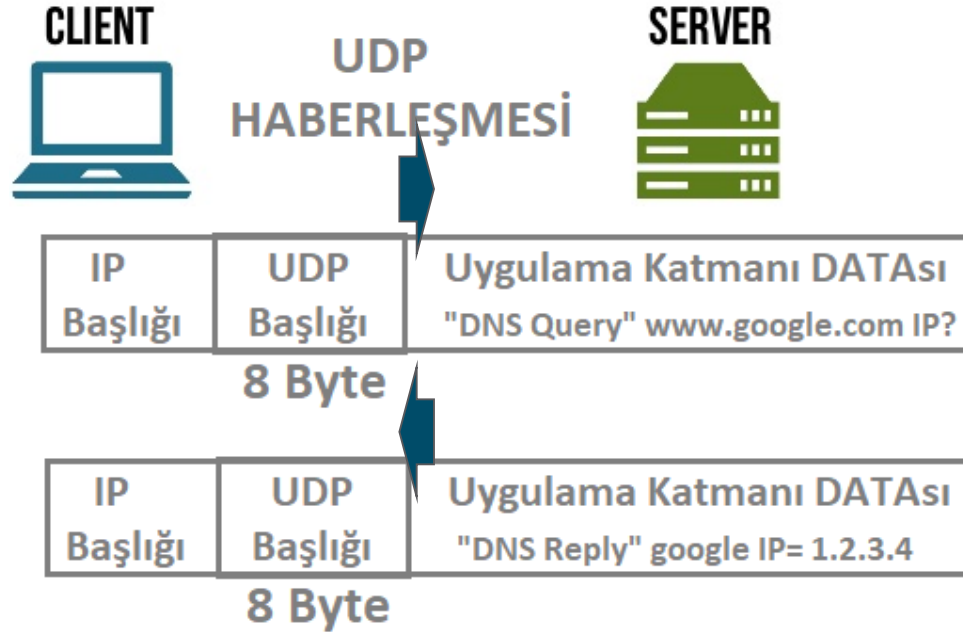


### OSI Referans Modeli

APPLICATION	L7
PRESENTATION	L6
SESSION	L5
TRANSPORT LAYER	L4
NETWORK LAYER	L3
DATA LINK LAYER	L2
PHYSICAL LAYER	L1

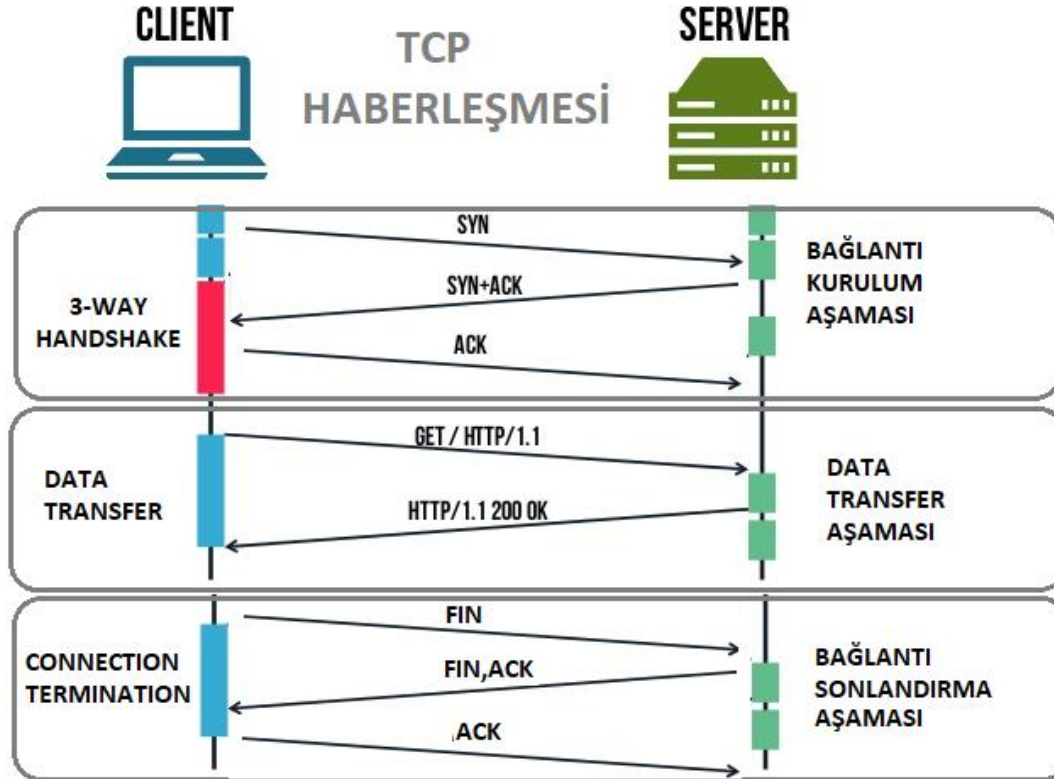
# Application, Presentation, and Session

## Application Layer



# Application, Presentation, and Session

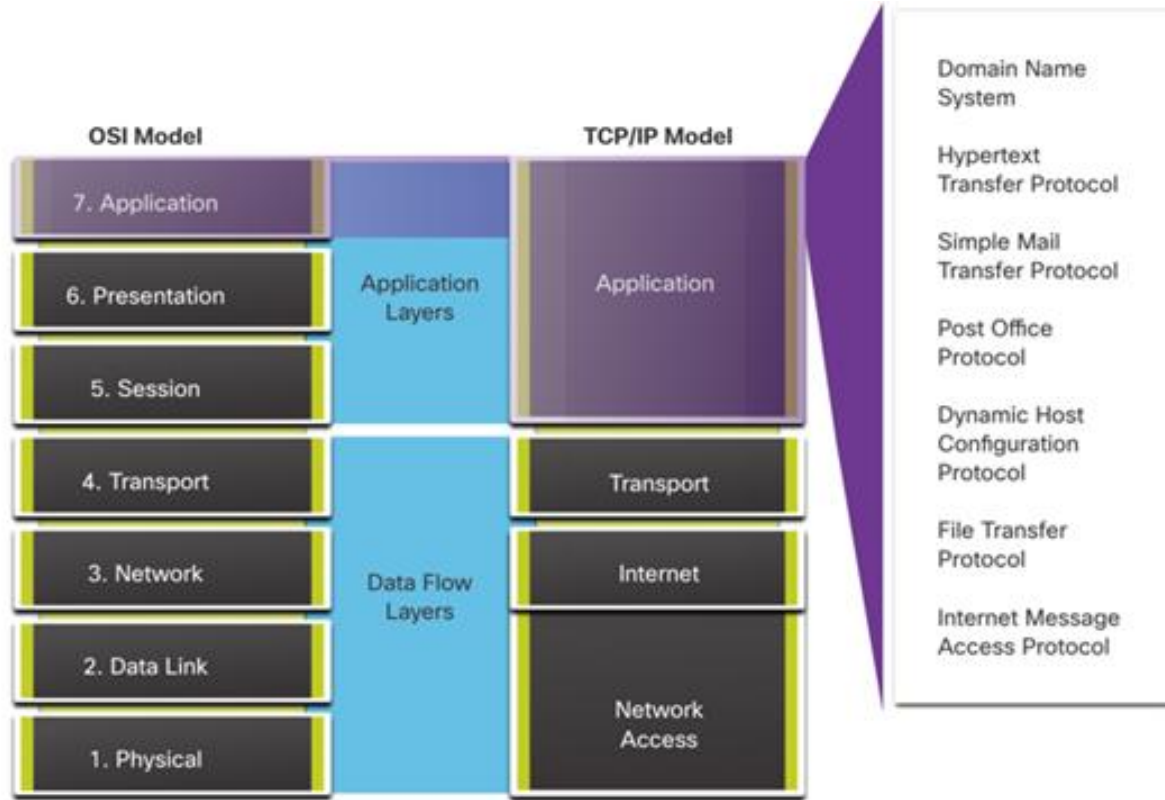
## Application Layer



# Application, Presentation, and Session

## Application Layer

- The upper three layers of the OSI model (application, presentation, and session) define functions of the TCP/IP application layer.
- The application layer provides the interface between the applications used to communicate, and the underlying network over which messages are transmitted.
- Some of the most widely known application layer protocols include HTTP, FTP, TFTP, IMAP and DNS.



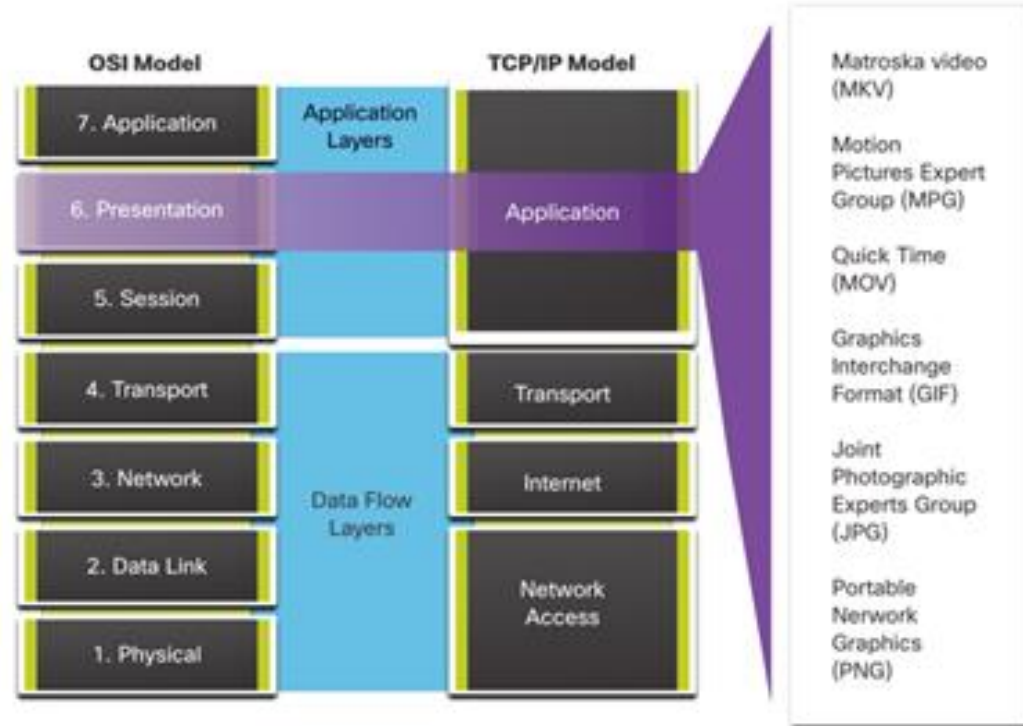
# Presentation and Session Layer *(Sunum Katmanı ve Oturum Katmanı)*

The **presentation layer** has three primary functions:

- Formatting, or presenting, data at the source device into a compatible format for receipt by the destination device
- Compressing data in a way that can be decompressed by the destination device
- Encrypting data for transmission and decrypting data upon receipt

The **session layer** functions:

- It creates and maintains dialogs between source and destination applications.
- It handles the exchange of information to initiate dialogs, keep them active, and to restart sessions that are disrupted or idle for a long period of time.





# TCP/IP Application Layer Protocols

- The TCP/IP application protocols specify the format and control information necessary for many common internet communication functions.
- Application layer protocols are used by both the source and destination devices during a communication session.
- For the communications to be successful, the application layer protocols that are implemented on the source and destination host must be compatible.

## **Name System**

### **DNS - Domain Name System (or Service)**

- TCP, UDP 53
- Translates domain names, such as cisco.com, into IP addresses.

## **Host Config**

### **DHCP - Dynamic Host Configuration Protocol**

- UDP client 68, server 67
- Dynamically assigns IP addresses to be re-used when no longer needed

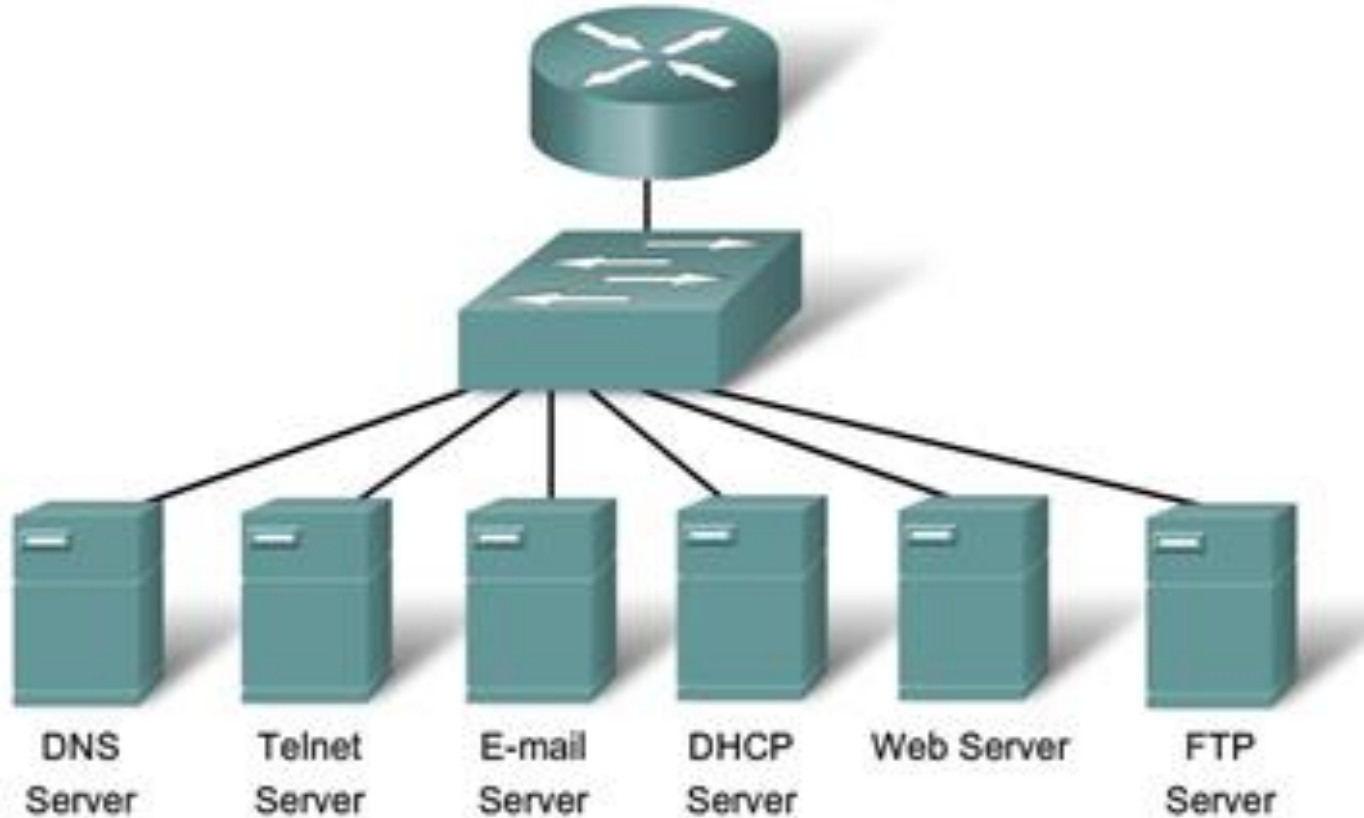
## **Web**

### **HTTP - Hypertext Transfer Protocol**

- TCP 80, 8080
- A set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web

# Application, Presentation, and Session

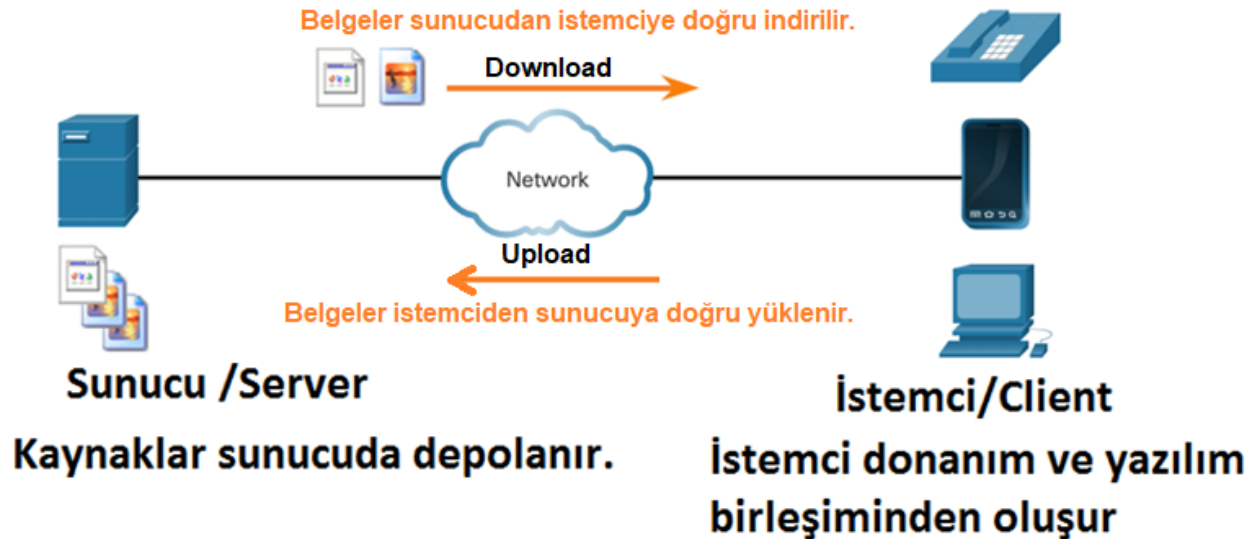
## TCP/IP Application Layer Protocols



# 15.2 Peer-to-Peer

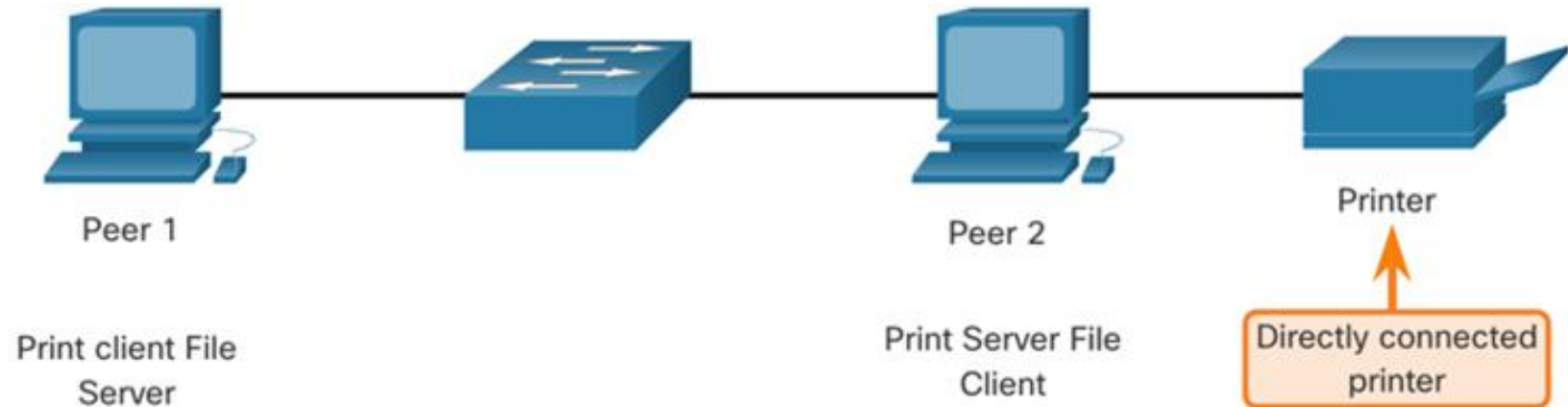
# Client-Server Model

- Client and server processes are considered to be in the application layer.
- In the client/server model, the device requesting the information is called a client and the device responding to the request is called a server.
- Application layer protocols describe the format of the requests and responses between clients and servers.



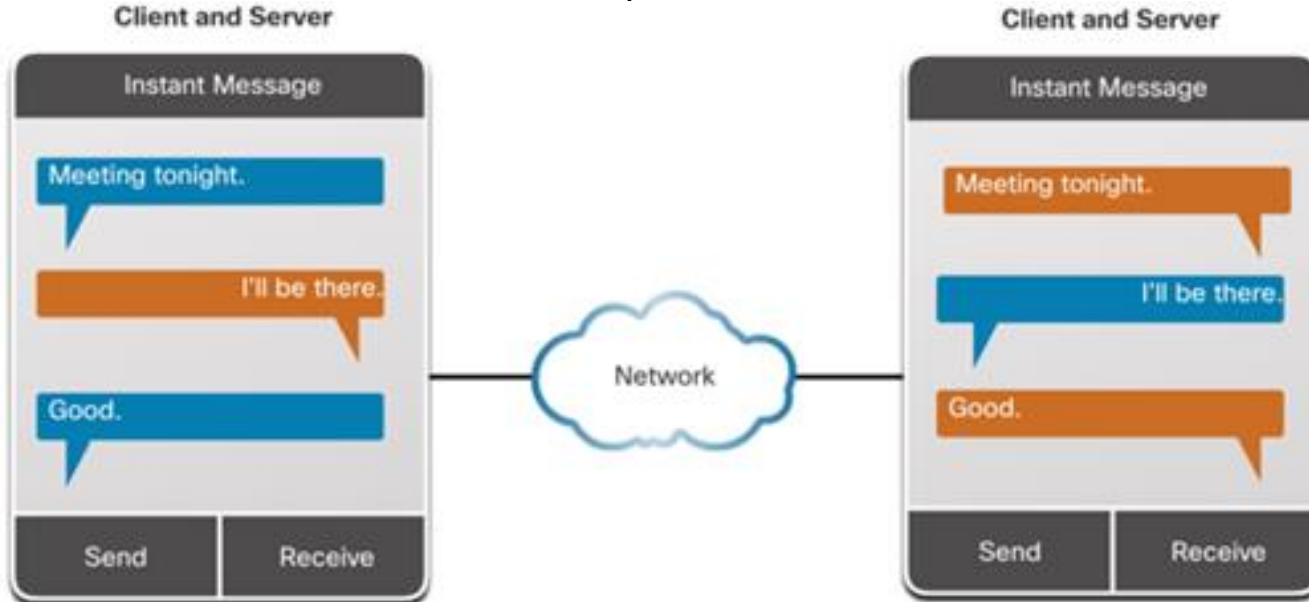
# Peer-to-Peer Networks

- In a peer-to-peer (P2P) network, two or more computers are connected via a network and can share resources (such as printers and files) without having a dedicated server.
- Every connected end device (known as a peer) can function as both a server and a client.
- One computer might assume the role of server for one transaction while simultaneously serving as a client for another. The roles of client and server are set on a per request basis.



# Peer-to-Peer Applications

- A P2P application allows a device to act as both a client and a server within the same communication.
- Some P2P applications use a hybrid system where each peer accesses an index server to get the location of a resource stored on another peer.

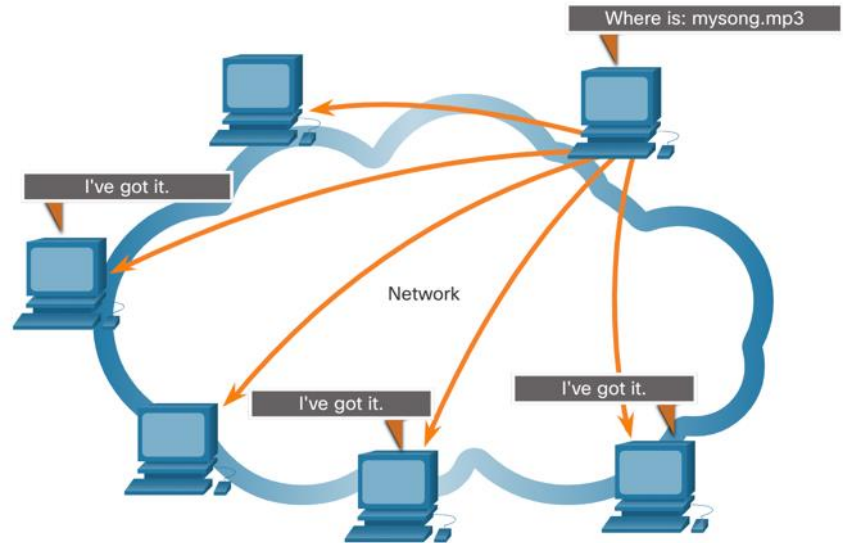


# Common P2P Applications

With P2P applications, each computer in the network that is running the application can act as a client or a server for the other computers in the network that are also running the application.

Common P2P networks include the following:

- BitTorrent
- Direct Connect
- eDonkey
- Freenet



# 15.3 Web and Email Protocols



# Hypertext Transfer Protocol and Hypertext Markup Language

When a web address or Uniform Resource Locator (URL) is typed into a web browser, the web browser establishes a connection to the web service. The web service is running on the server that is using the HTTP protocol.

To better understand how the web browser and web server interact, examine how a web page is opened in a browser.

### Step 1

The browser interprets the three parts of the URL:

- **http** (the protocol or scheme)
- **www.cisco.com** (the server name)
- **index.html** (the specific filename requested)



# Hypertext Transfer Protocol and Hypertext Markup Language (Cont.)

### Step 2

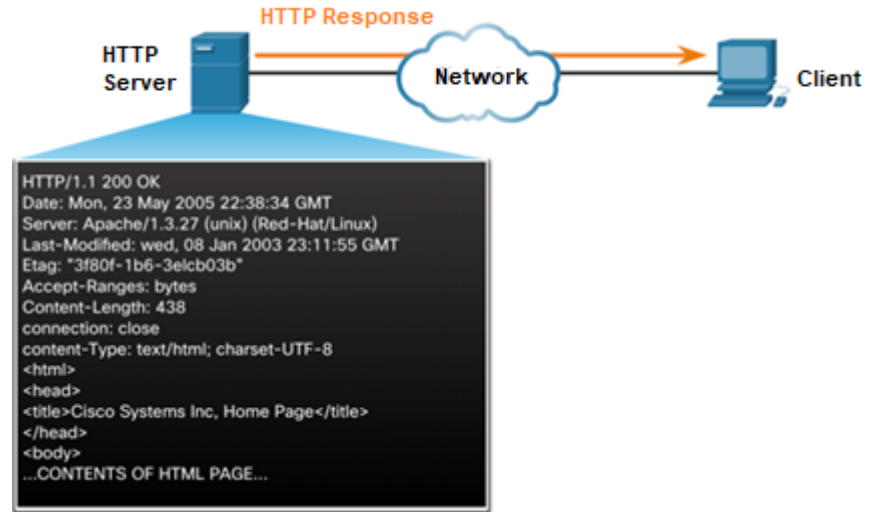
The browser then checks with a name server to convert `www.cisco.com` into a numeric IP address, which it uses to connect to the server.

The client initiates an HTTP request to a server by sending a GET request to the server and asks for the `index.html` file.



### Step 3

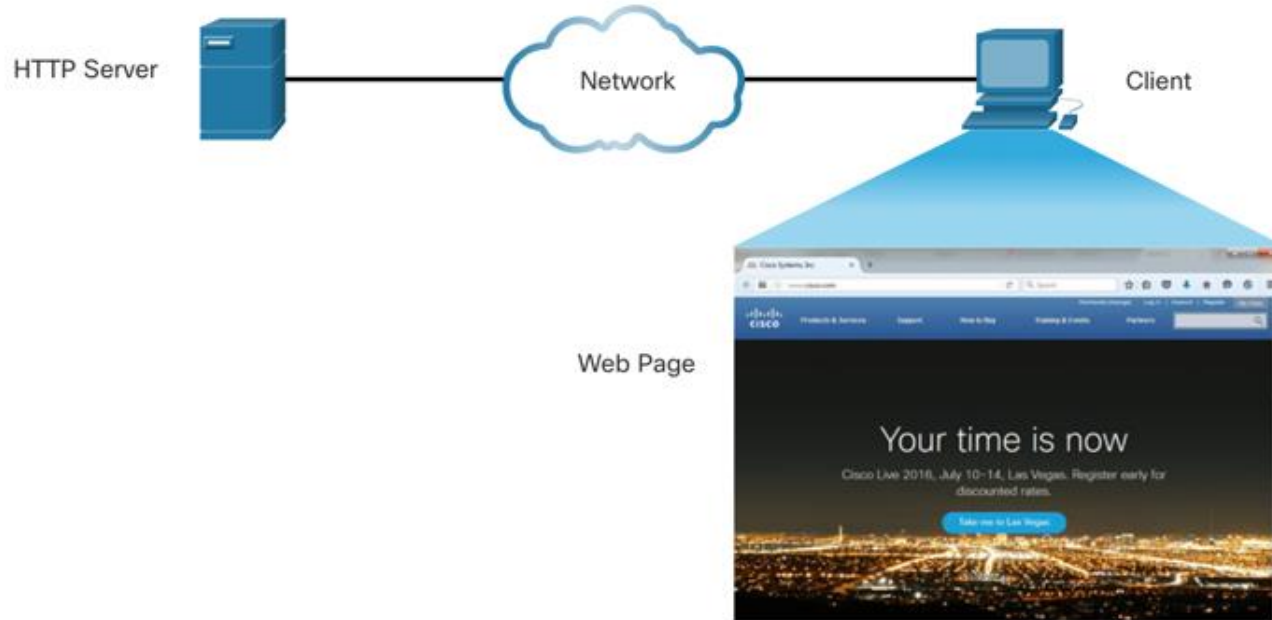
In response to the request, the server sends the HTML code for this web page to the browser.



# Hypertext Transfer Protocol and Hypertext Markup Language (Cont.)

### Step 4

The browser deciphers the HTML code and formats the page for the browser window.

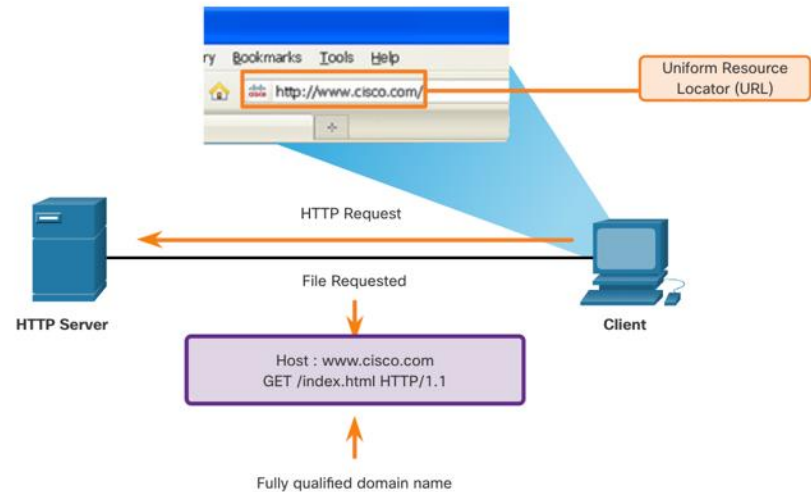


# HTTP (tcp 80) and HTTPS (tcp 443)

HTTP is a request/response protocol that specifies the message types used for that communication.

The three common message types are GET, POST, and PUT:

- **GET** - This is a client request for data. A client (web browser) sends the GET message to the web server to request HTML pages.
- **POST** - This uploads data files to the web server, such as form data.
- **PUT** - This uploads resources or content to the web server, such as an image.



**Note:** HTTP is not a secure protocol. For secure communications sent across the internet, HTTPS should be used.

Taşıyın!

# HTTP GET Mesajı ve Cevabı

## GET / HTTP/1.1

Host: www.mit.edu

User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:39.0) Gecko/20100101  
Firefox/39.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: keep-alive

## HTTP/1.1 200 OK

Server: Apache/1.3.41 (Unix) mod\_ssl/2.8.31

OpenSSL/0.9.8j

Last-Modified: Mon, 10 Aug 2015 04:01:04 GMT

ETag: "10e863f8-4844-55c82200"

Accept-Ranges: bytes

X-Cnection: close

Content-Type: text/html

Vary: Accept-Encoding

Content-Encoding: gzip

Date: Mon, 10 Aug 2015 08:56:19 GMT

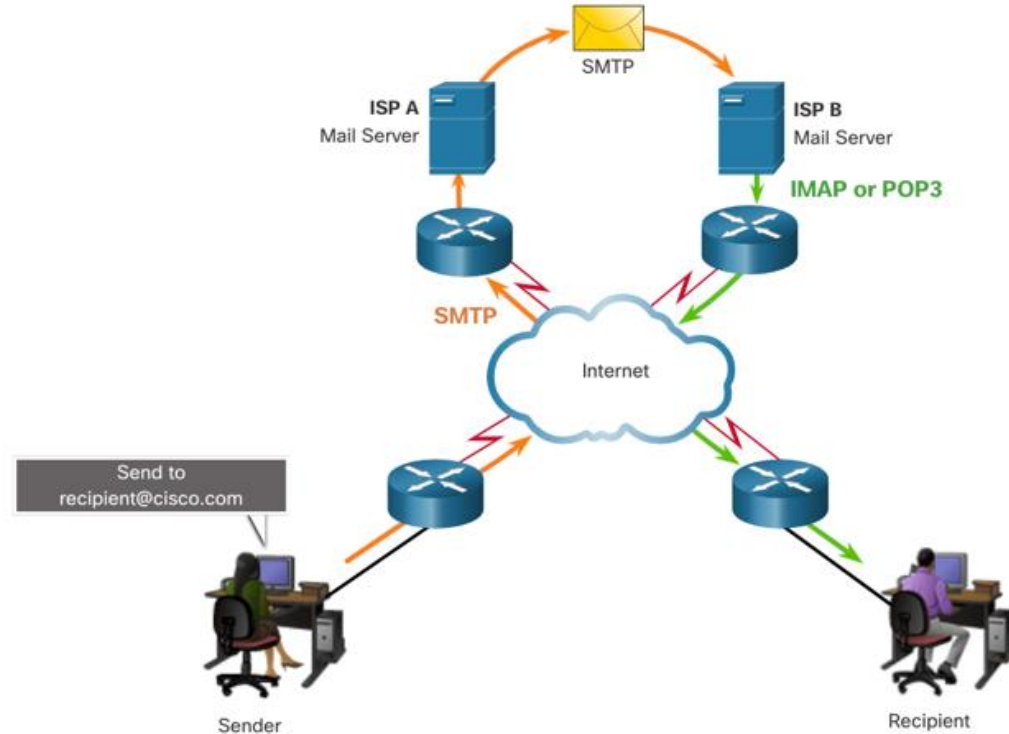
## Web and Email Protocols

# Email Protocols

Email is a store-and-forward method of sending, storing, and retrieving electronic messages across a network. Email messages are stored in databases on mail servers. Email clients communicate with mail servers to send and receive email.

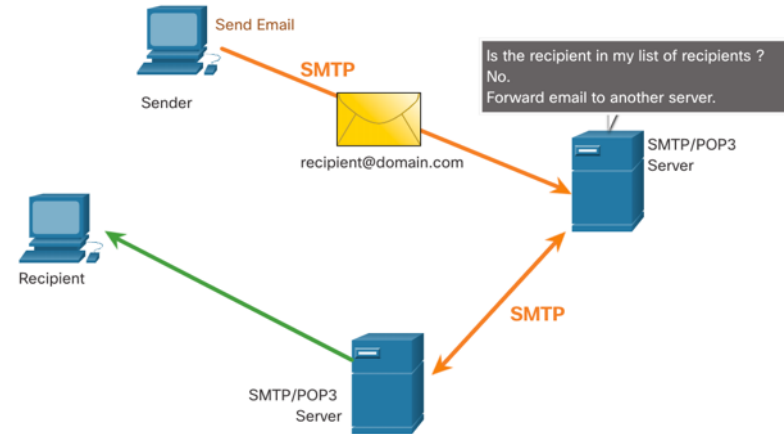
The email protocols used for operation are:

- Simple Mail Transfer Protocol (SMTP) – used to send mail.
- Post Office Protocol (POP) & IMAP – used for clients to receive mail.



# SMTP, POP and IMAP

- When a client sends email, the client SMTP process connects with a server SMTP process on well-known port 25.
- After the connection is made, the client attempts to send the email to the server across the connection.
- When the server receives the message, it either places the message in a local account, if the recipient is local, or forwards the message to another mail server for delivery.
- The destination email server may not be online or may be busy. If so, SMTP spools messages to be sent at a later time.

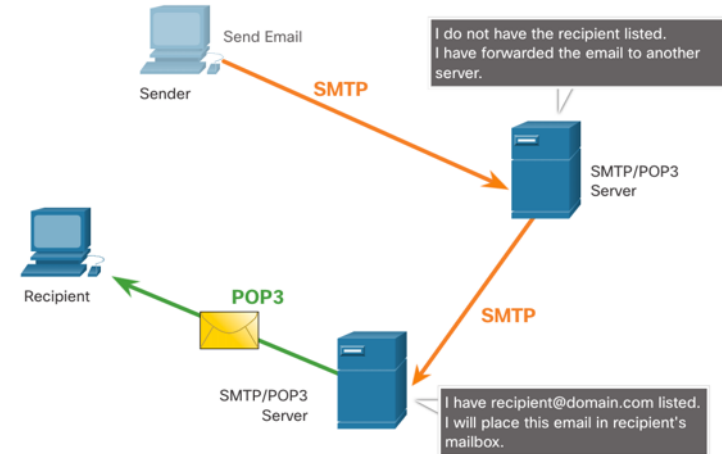


**Note:** SMTP message formats require a message header (recipient email address & sender email address) and a message body.

# SMTP, POP and IMAP (Cont.)

POP is used by an application to retrieve mail from a mail server. When mail is downloaded from the server to the client using POP the messages are then deleted on the server.

- The server starts the POP service by passively listening on TCP port 110 for client connection requests.
- When a client wants to make use of the service, it sends a request to establish a TCP connection with the server.
- When the connection is established, the POP server sends a greeting.
- The client and POP server then exchange commands and responses until the connection is closed or aborted.



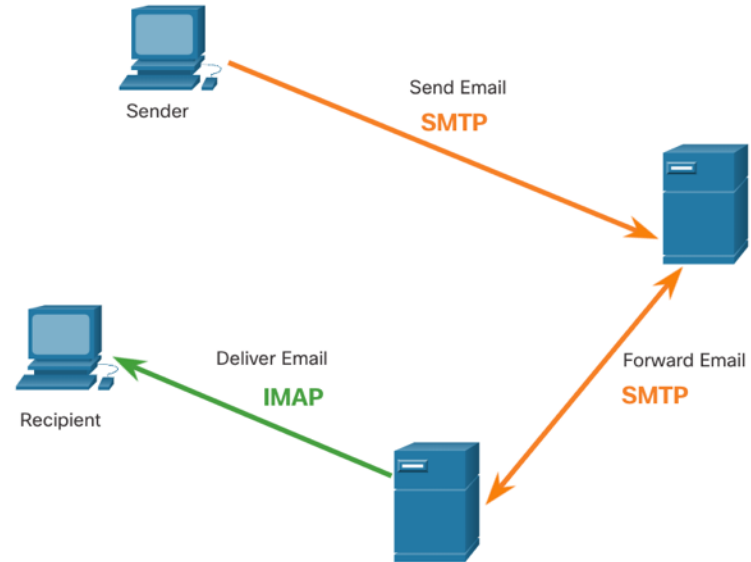
Note: Since POP does not store messages, it is not recommended for small businesses that need a centralized backup solution.



# SMTP, POP and IMAP (Cont.)

IMAP is another protocol that describes a method to retrieve email messages.

- Unlike POP, when a user connects to an IMAP server, copies of the messages are downloaded to the client application. The original messages are kept on the server until manually deleted.
- When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.



# Yaygın Uygulama Katmanı Protokolleri

## SMTP, POP ve IMAP (Devamı)

Change Account

POP and IMAP Account Settings

Enter the mail server settings for your account.

User Information

Your Name: Clint Eastwood

Email Address: agyoneticileri@gmail.com

Server Information

Account Type: IMAP

Incoming mail server: imap.gmail.com

Outgoing mail server (SMTP): smtp.gmail.com

Logon Information

User Name: agyoneticileri

Password: \*\*\*\*\*

☒ Remember password

☐ Require logon using Secure Password Authentication (SPA)

Test Account Settings

We recommend that you test your account to ensure that the entries are correct.

Test Account Settings ...

☒ Automatically test account settings when Next is clicked

Mail to keep offline: All

More Settings ...

< Back

Next >

Cancel

## Yaygın Uygulama Katmanı Protokolleri

# SMTP, POP ve IMAP (Devamı)

Internet E-mail Settings ✕

General **Outgoing Server** Advanced

Server Port Numbers

Incoming server (IMAP):

Use the following type of encrypted connection: SSL

Outgoing server (SMTP):

Use the following type of encrypted connection: TLS

Server Timeouts

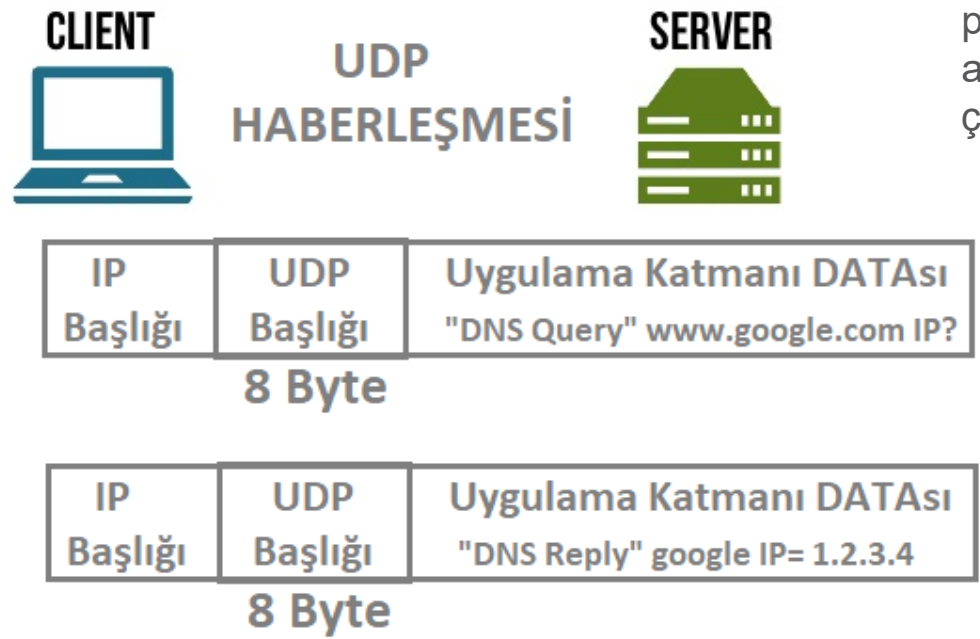
Short  Long 1 minute

# 15.4 IP Addressing Services

# IP Addressing Services

## Domain Name Service

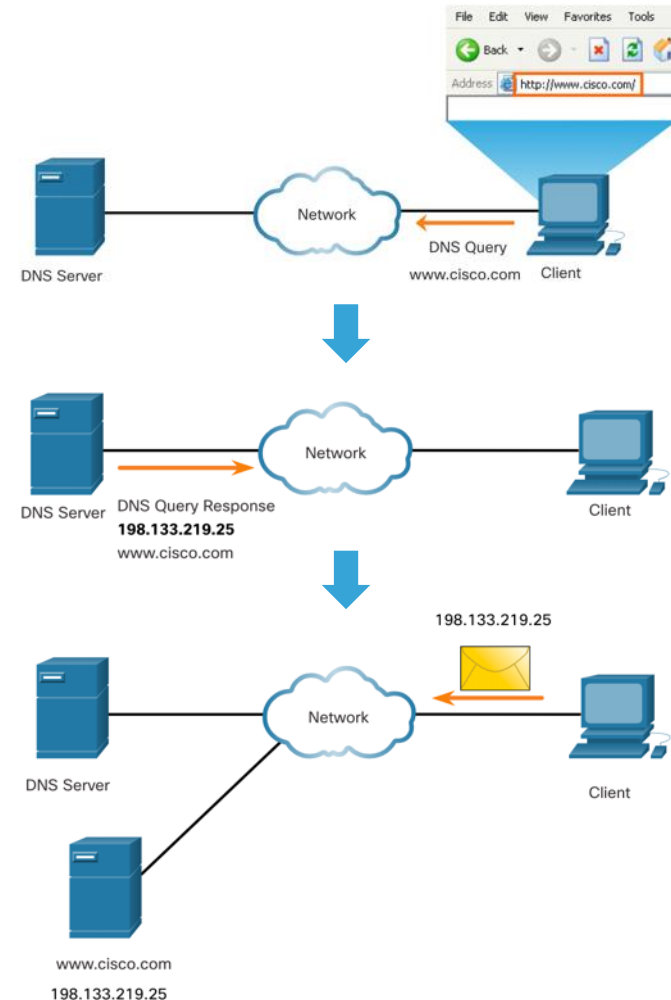
İnsanlar tarafından okunabilen bir ad, DNS protokolü tarafından sayısal ağ cihaz adresine çözümlenir



# IP Addressing Services

## Domain Name Service

- Domain names were created to convert the numeric IP addresses into a simple, recognizable name.
- Fully-qualified domain names (FQDNs), such as `http://www.cisco.com`, are much easier for people to remember than `198.133.219.25`.
- The DNS protocol defines an automated service that matches resource names with the required numeric network address. It includes the format for queries, responses, and data.



# DNS Message Format

The DNS server stores different types of resource records that are used to resolve names. These records contain the name, address, and type of record.

Some of these record types are as follows:

- **A** - An end device IPv4 address
- **NS** - An authoritative name server
- **AAAA** - An end device IPv6 address (pronounced quad-A)
- **MX** - A mail exchange record

When a client makes a query, the server DNS process first looks at its own records to resolve the name. If it is unable to resolve the name by using its stored records, it contacts other servers to resolve the name.

After a match is found and returned to the original requesting server, the server temporarily stores the numbered address in the event that the same name is requested again.

# DNS Message Format (Cont.)

DNS uses the same message format between servers, consisting of a question, answer, authority, and additional information for all types of client queries and server responses, error messages, and transfer of resource record information.

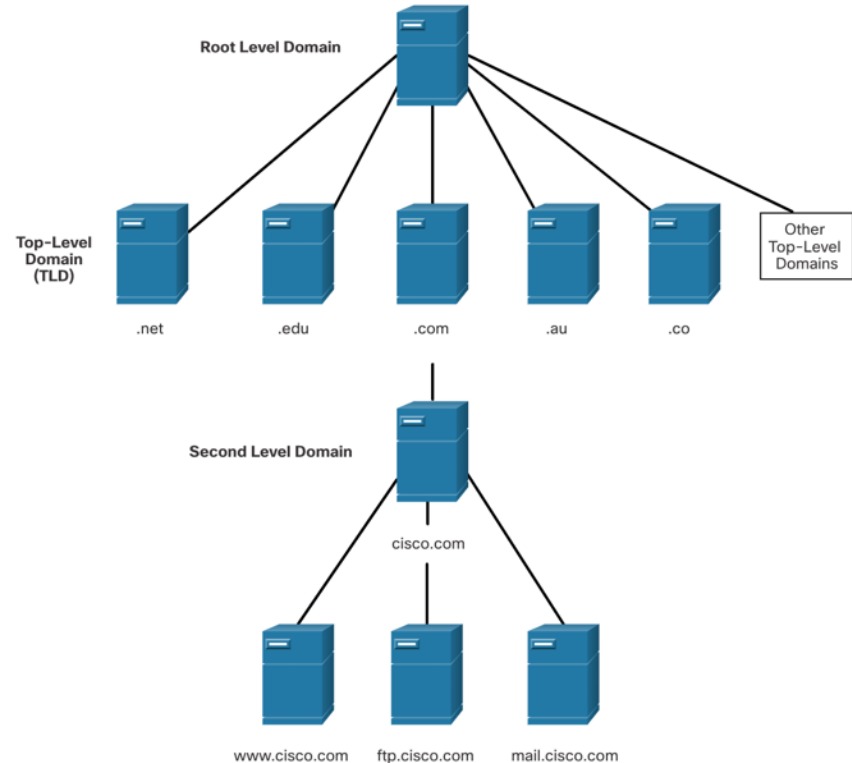
DNS message section	Description
Question	The question for the name server
Answer	Resource Records answering the question
Authority	Resource Records pointing toward an authority
Additional	Resource Records holding additional information



# IP Addressing Services

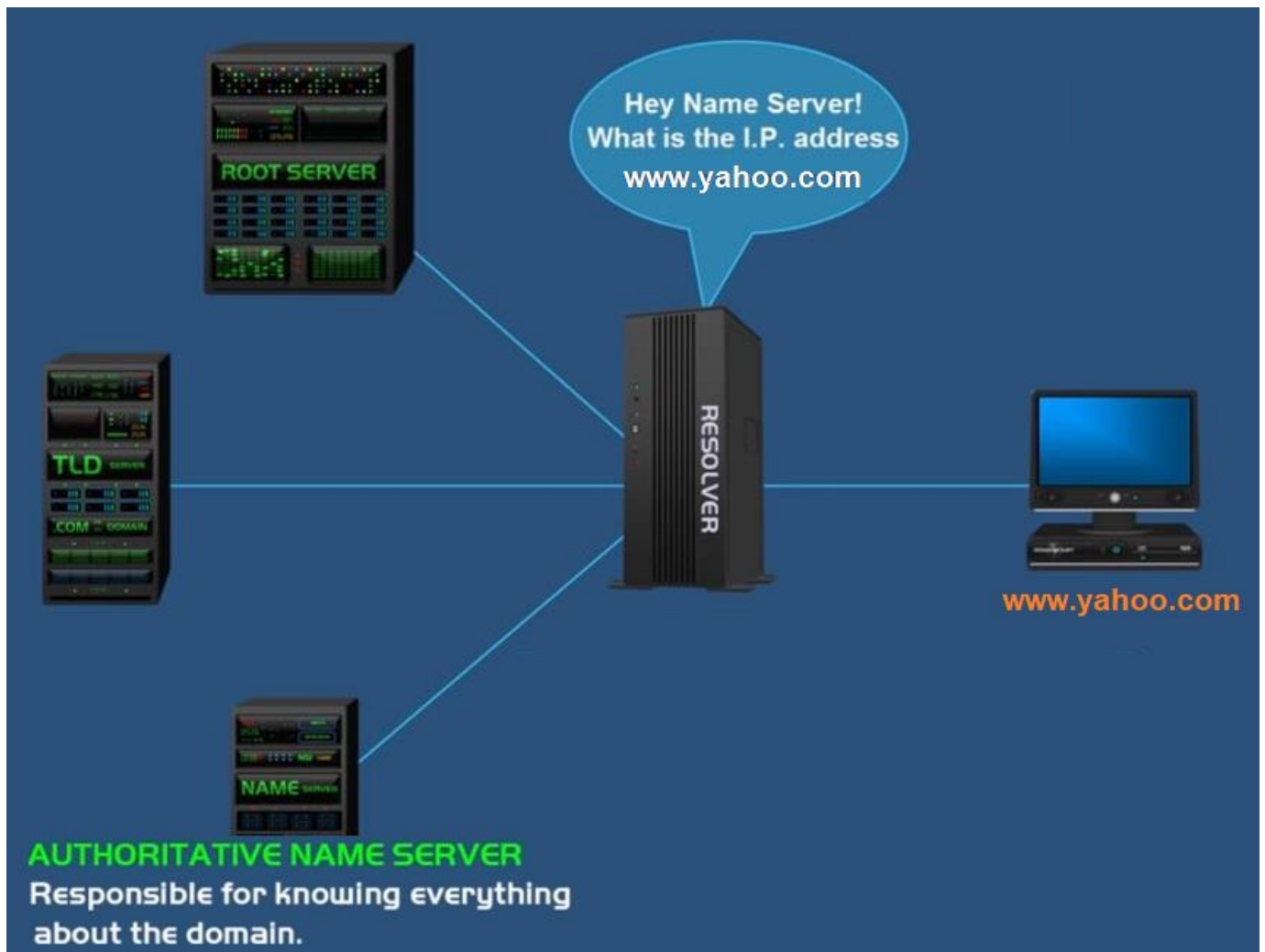
## DNS Hierarchy

- DNS uses a hierarchical system to create a database to provide name resolution.
- Each DNS server maintains a specific database file and is only responsible for managing name-to-IP mappings for that small portion of the entire DNS structure.
- When a DNS server receives a request for a name translation that is not within its DNS zone, the DNS server forwards the request to another DNS server within the proper zone for translation.
- Examples of top-level domains:
  - **.com** - a business or industry
  - **.org** - a non-profit organization
  - **.au** - Australia



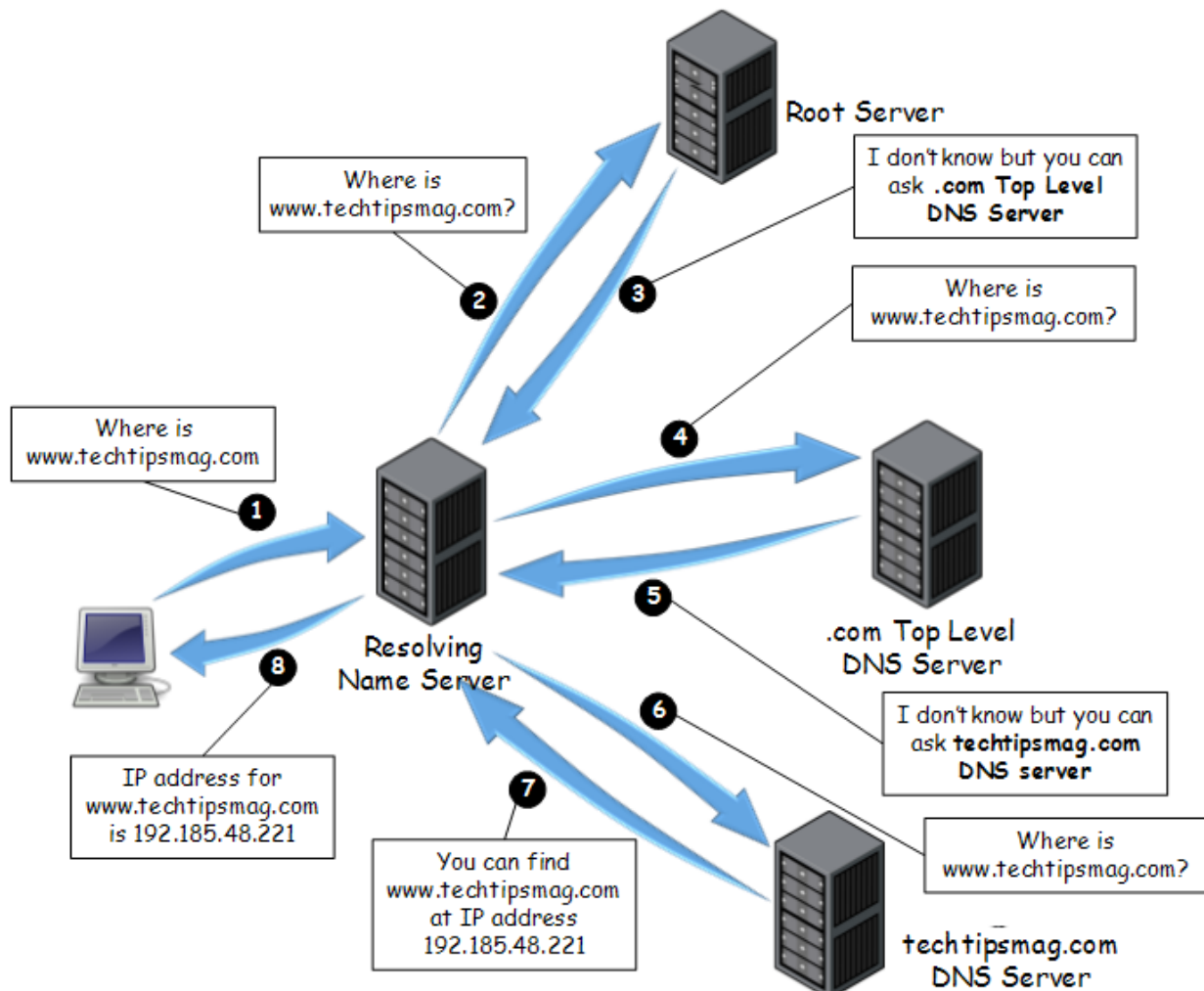
# IP Addressing Services

## DNS Hierarchy



# IP Addressing Services

## DNS Hierarchy




## IP Adresleme Hizmetleri Sağlama

# nslookup

- **nslookup** adındaki işletim sistemi yardımcı programı, belirli bir host adını çözümlmek için kullanıcıya ad sorgulama imkanı tanır
- Yardımcı program, ad çözümü sorunlarını gidermek ve ad sunucularının güncel durumlarını doğrulamak için kullanılabilir

```
C:\>nslookup
```

```
Default Server:  public-dns-a.google.com  
Address:  8.8.8.8
```

  
BİRİNCİL DNS SUNUCUSU

```
> www.cisco.com  
Server:  google-public-dns-a.google.com  
Address:  8.8.8.8
```

```
Addresses:  2a02:26f0:ad:19c::90 ➡ IPv6 Address  
            2a02:26f0:ad:18f::90  
            104.86.251.162 ➡ IPv4 Address
```

```
Aliases:  www.cisco.com
```

```
> set type=a
> www.hotmail.com
Addresses: 157.55.46.242
          157.55.46.243
Aliases:  www.hotmail.com
```

```
> set type=cname
> www.hotmail.com

www.hotmail.com canonical name=dispatch.microsoft.com
```

```
> set type=mx
> hotmail.com

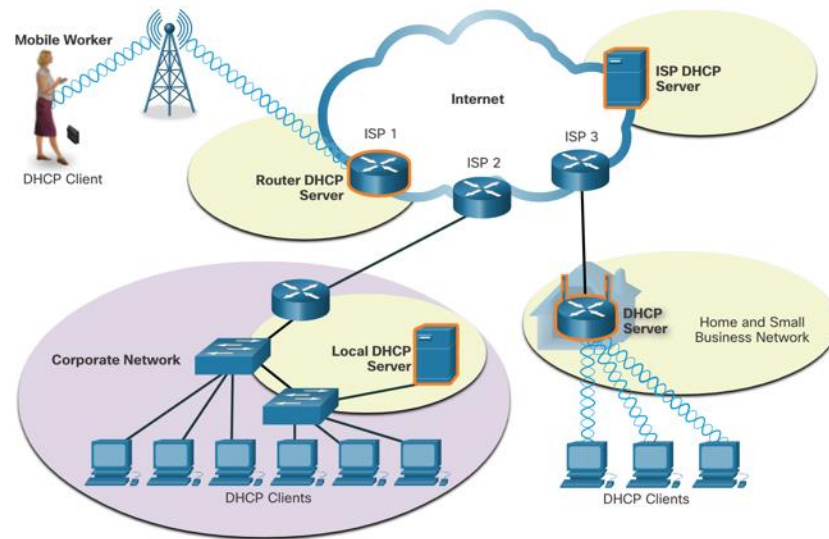
hotmail.com      MX preference = 5, mail exchanger = mx2.hotmail.com
hotmail.com      MX preference = 5, mail exchanger = mx3.hotmail.com
hotmail.com      MX preference = 5, mail exchanger = mx4.hotmail.com
hotmail.com      MX preference = 5, mail exchanger = mx1.hotmail.com
```

```
> set type=ns
> hotmail.com

hotmail.com      nameserver = ns3.msft.net
hotmail.com      nameserver = ns4.msft.net
hotmail.com      nameserver = ns1.msft.net
hotmail.com      nameserver = ns2.msft.net
```

# Dynamic Host Configuration Protocol

- The Dynamic Host Configuration Protocol (DHCP) for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters.
- DHCP is considered dynamic addressing compared to static addressing. Static addressing is manually entering IP address information.
- When a host connects to the network, the DHCP server is contacted, and an address is requested. The DHCP server chooses an address from a configured range of addresses called a pool and assigns (leases) it to the host.
- Many networks use both DHCP and static addressing. DHCP is used for general purpose hosts, such as end user devices. Static addressing is used for network devices, such as gateway routers, switches, servers, and printers.



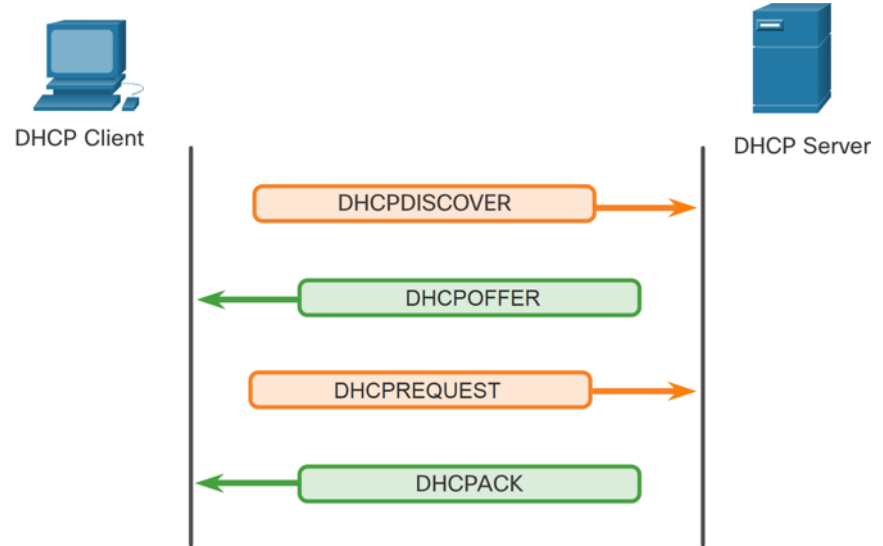
**Note:** DHCP for IPv6 (DHCPv6) provides similar services for IPv6 clients. However, DHCPv6 does not provide a default gateway address. This can only be obtained dynamically from the Router Advertisement message of the router.

# IP Addressing Services

## DHCP Operation

### The DHCP Process:

- When an IPv4, DHCP-configured device boots up or connects to the network, the client broadcasts a DHCP discover (DHCPDISCOVER) message to identify any available DHCP servers on the network.
- A DHCP server replies with a DHCP offer (DHCPOFFER) message, which offers a lease to the client. (If a client receives more than one offer due to multiple DHCP servers on the network, it must choose one.)
- The client sends a DHCP request (DHCPREQUEST) message that identifies the explicit server and lease offer that the client is accepting.
- The server then returns a DHCP acknowledgment (DHCPACK) message that acknowledges to the client that the lease has been finalized.
- If the offer is no longer valid, then the selected server responds with a DHCP negative acknowledgment (DHCPNAK) message and the process must begin with a new DHCPDISCOVER message.



**Note:** DHCPv6 has a set of messages that is similar to those for DHCPv4. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.

IP Adresleme Hizmetleri Sağlama

# DHCP İşlemi





IP Adresleme Hizmetleri Sağlama

# DHCP İşlemi

C:\ ipconfig /all

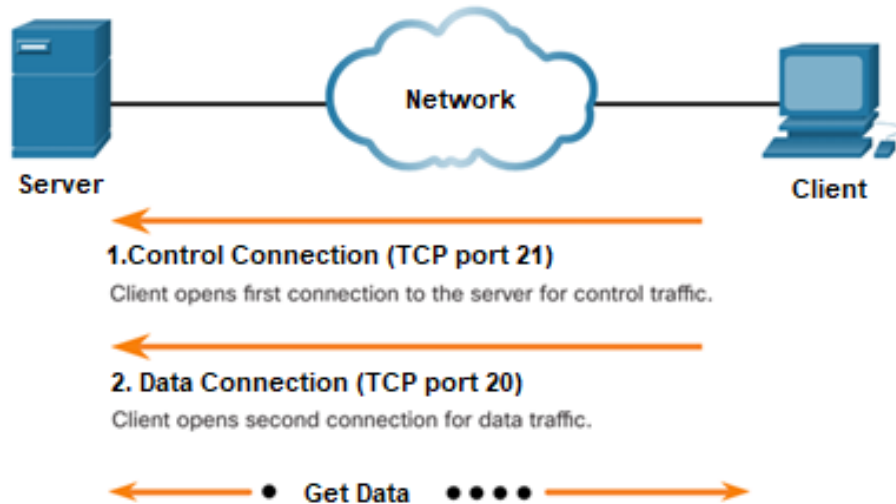
```
Connection-specific DNS Suffix . :  
Description . . . . . : Dell Wireless 1510 Wireless-N  
  
Physical Address. . . . . : 00-24-2C-64-0D-68  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::bc52:e5bd:f6c6:90c%13(Preferred)  
IPv4 Address. . . . . : 10.64.98.119(Preferred)  
Subnet Mask . . . . . : 255.255.240.0  
Lease Obtained. . . . . : 10 Agustos 2015 Pazartesi 10:14:20  
Lease Expires . . . . . : 12 Agustos 2015 Çarşamba 10:14:21  
Default Gateway . . . . . : fe80::ad84:b267:ea1d:9e6c%13  
                             10.64.0.1  
DHCP Server . . . . . : 10.11.0.20  
DHCPv6 IAID . . . . . : 318776364  
DHCPv6 Client DUID. . . . . : 00-01-00-01-19-14-B7-21-00-24-E8-9D-D4-E2  
  
DNS Servers . . . . . : 8.8.8.8  
NetBIOS over Tcpip. . . . . : Enabled
```

Lease Time: Kiralama Süresi ???

# 15.5 File Sharing Services

# File Transfer Protocol

FTP was developed to allow for data transfers between a client and a server. An FTP client is an application which runs on a computer that is being used to push and pull data from an FTP server.



**Step 1** - The client establishes the first connection to the server for control traffic using TCP port 21. The traffic consists of client commands and server replies.

**Step 2** - The client establishes the second connection to the server for the actual data transfer using TCP port 20. This connection is created every time there is data to be transferred.

**Step 3** - The data transfer can happen in either direction. The client can download (pull) data from the server, or the client can upload (push) data to the server.

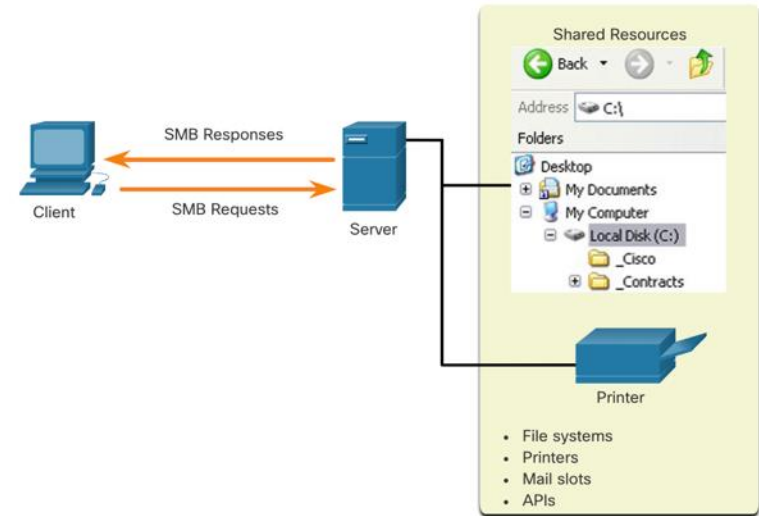
# Server Message Block (TCP port 445)

The Server Message Block (SMB) is a client/server, request-response file sharing protocol. Servers can make their own resources available to clients on the network.

Three functions of SMB messages:

- Start, authenticate, and terminate sessions
- Control file and printer access
- Allow an application to send or receive messages to or from another device

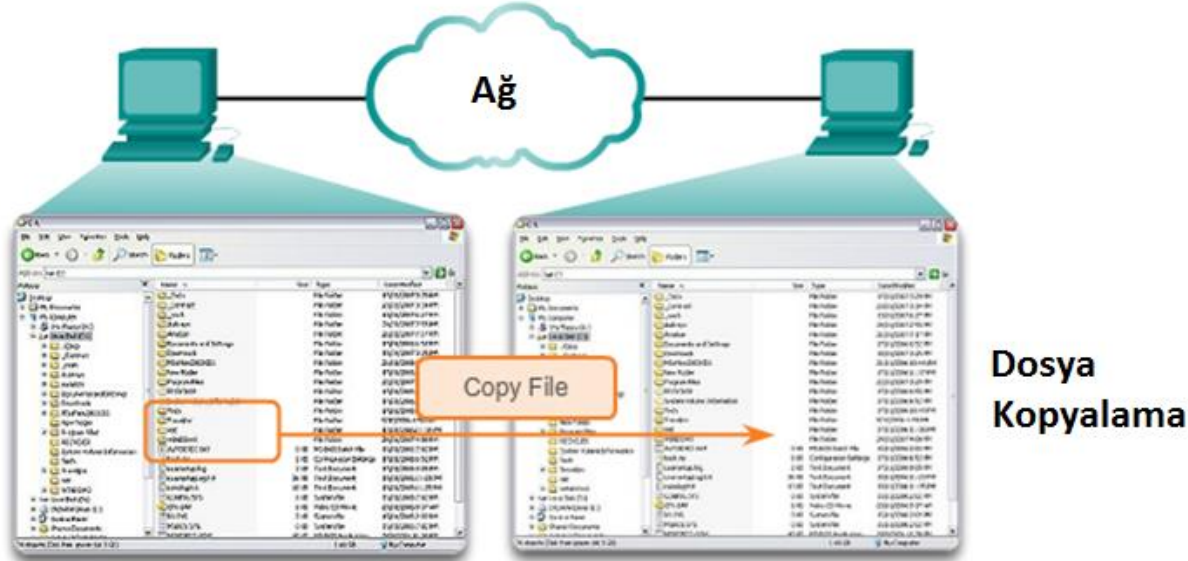
Unlike the file sharing supported by FTP, clients establish a long-term connection to servers. After the connection is established, the user of the client can access the resources on the server as though the resource is local to the client host.



# File Sharing Services

## Server Message Block

### SMB Dosya Paylaşımı



**Windows Explorer'da bir dosya bir PC'den diğer bir PC'ye SMB protokolü kullanılarak paylaşılabilir.**

# EK SLIDE

## Telnet vs SSH

PARAMETER	SSH	Telnet
Security	Highly secured	Less secured than SSH
Port number	Uses TCP port number 22	Uses TCP port number 23
Data format	SSH sends all the data in encrypted format. SSH uses a secure channel to transfer data over the network	Telnet sends the data in plain text.
Authentication	SSH uses public key encryption in order to authenticate the remote users	Telnet uses no authentication mechanisms
Data Privacy	Username and Passwords can be prone to malicious attack	Data sent using this protocol cannot be easily interpreted by the hackers.
Public/Private network recommendation	Suitable for Public networks	Suitable for private networks
Vulnerabilities	Can be considered a replacement of telnet since it has overcome many of the security issues of telnet	Is older than SSH and has many vulnerabilities than SSH.
Bandwidth usage	High bandwidth usage	Low bandwidth usage
Operating system	All popular Operating systems	Used in Linux and Windows Operating system.
RFC	RFC 4253 specifies SSH server	Telnet was developed in 1969 beginning with RFC 15 and extended in RFC 854

# 15.6 Module Practice and Quiz

# What did I learn in this module?

- Application layer protocols are used to exchange data between programs running on the source and destination hosts. The presentation layer has three primary functions: formatting, or presenting data, compressing data, and encrypting data for transmission and decrypting data upon receipt. The session layer creates and maintains dialogs between source and destination applications.
- In the client/server model, the device requesting the information is called a client and the device responding to the request is called a server.
- In a P2P network, two or more computers are connected via a network and can share resources without having a dedicated server.
- The three common HTTP message types are GET, POST, and PUT.
- Email supports three separate protocols for operation: SMTP, POP, and IMAP.
- DNS protocol matches resource names with the required numeric network address.
- DHCP for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.
- An FTP client is an application which runs on a computer that is being used to push and pull data from an FTP server.
- Three functions of SMB messages: start, authenticate, and terminate sessions, control file and printer access, and allow an application to send or receive messages to or from another device.



