Information Security Operations Center

Prepared by
Dr. Ibrahim Gomaa

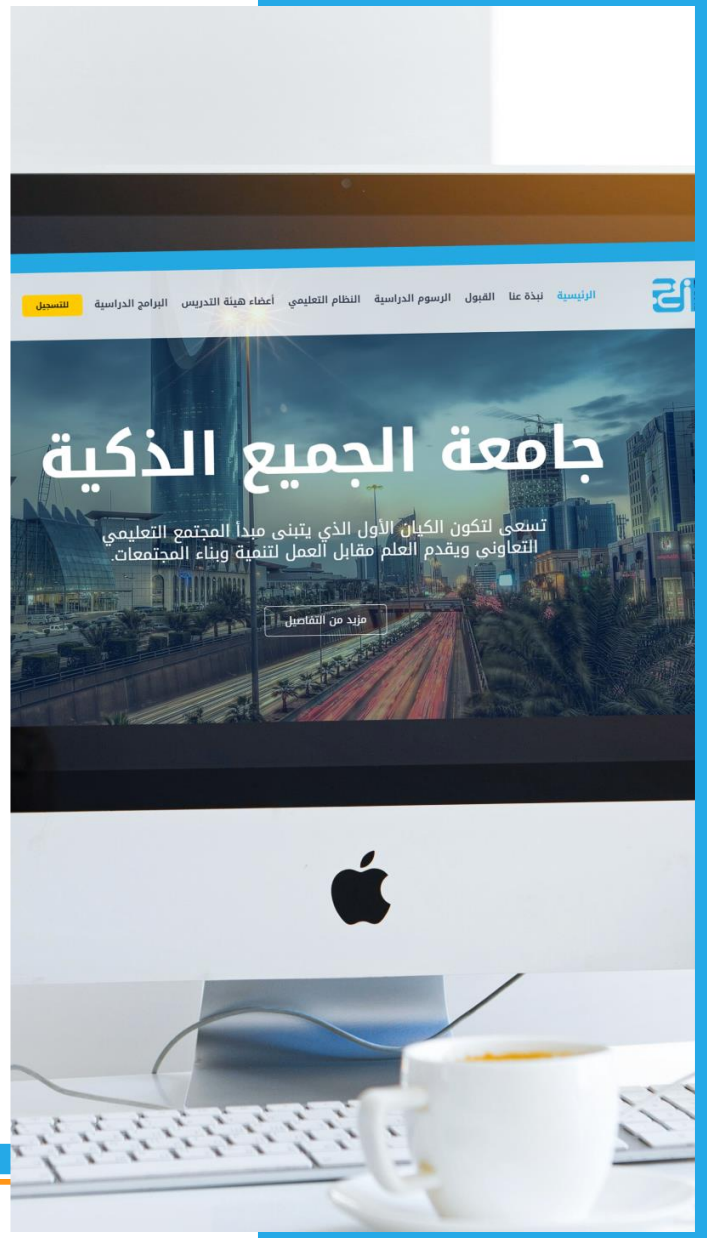
Lecture 3: Network protocols and services analysis

جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

Lecture – 3

Contents

Topic Title	Topic Objective
IPv4 and IPv6	Explain how the IP protocol supports network communications.
ICMP	Explain how ICMP is used to test network connectivity
ARP and ARP Issues	Explain how ARP requests impact network and host performance as well as potential security risks.
DHCP	Explain how DHCP services enable network Functionality
DNS	Explain how DNS services enable network Functionality
NAT	Explain how NAT services enable network Functionality
Email and HTTP	Explain how Email and HTTP services enable network Functionality

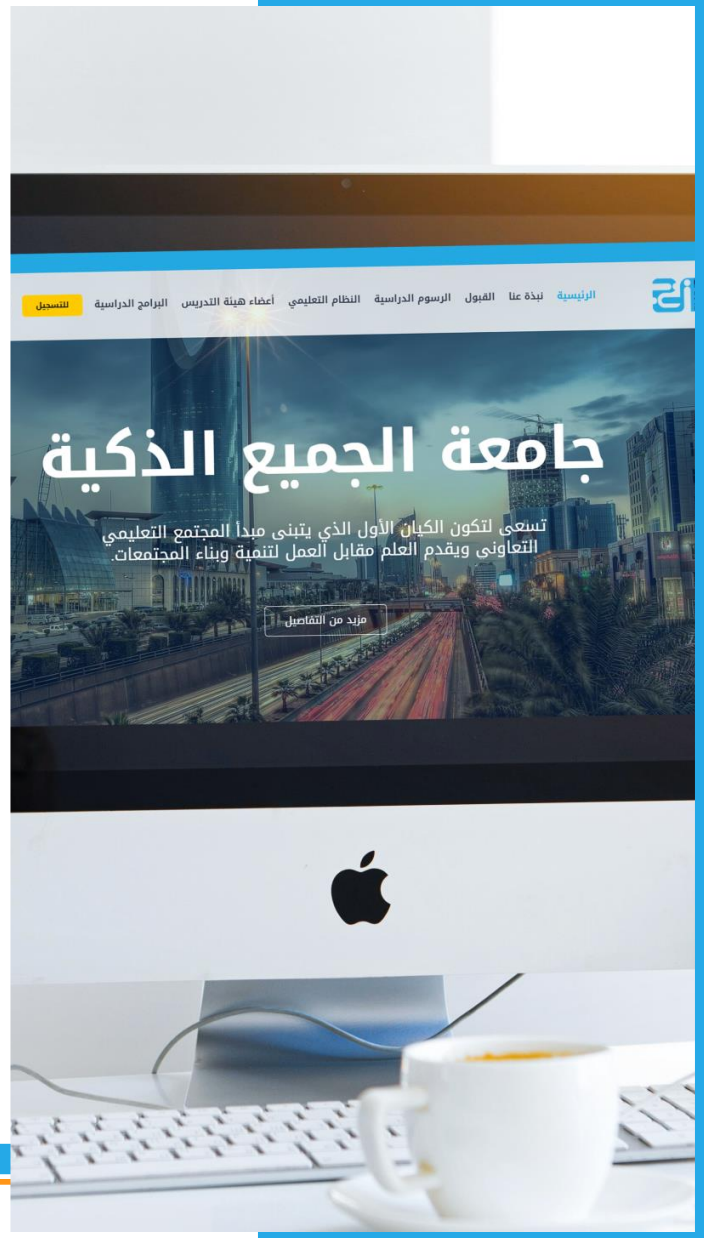


جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

Lecture – 3

Network protocols and services analysis

IPv4 and IPv6

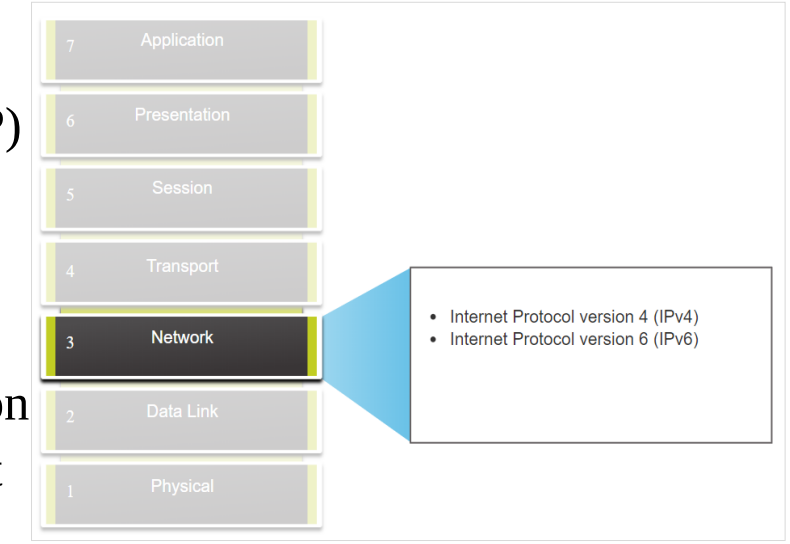


جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

Lecture – 3

The Network Layer

- The network layer provides services to allow end devices to exchange data across networks.
- IPv4 and IPv6 are the principle network layer communication protocols.
- Open Shortest Path First (OSPF) and Internet Control Message Protocol (ICMP) are other network layer protocols



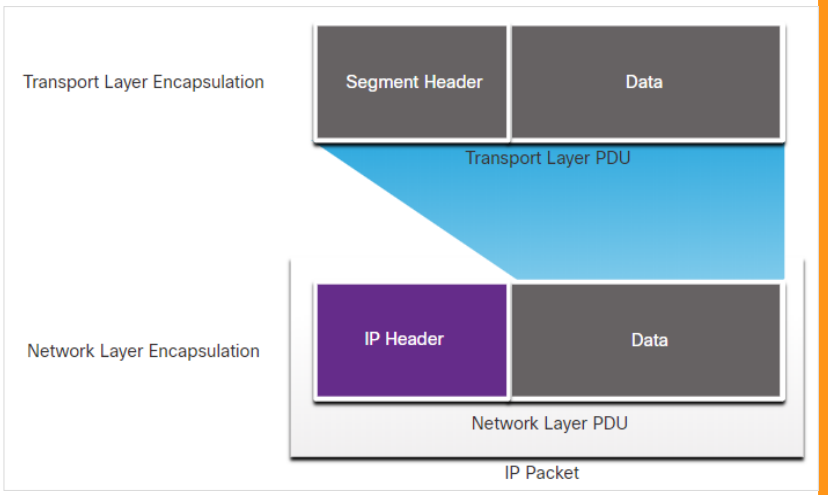
Basic operations of network layer protocol:

- **Addressing end devices -** Configured with a unique IP address for identification
- **Encapsulation -** Encapsulates the Protocol Data Unit (PDU) from the transport layer into a packet.
- **Routing -** Select the best path and direct packets towards destination host.
- **De-encapsulation** – Performed by the destination host.

جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

IP Encapsulation

- IP encapsulates the transport layer segment or other data by adding an IP header.
- IP Header is used to deliver the packet to the destination host. It is examined by Layer 3 devices.
- The process of encapsulating data layer by layer enables the services at the different layers to develop and scale without affecting the other layers.
- IP addressing information remains the same from the time the packet leaves the source host until it arrives at the destination host, except when translated by the device performing Network Address Translation (NAT) for IPv4.
- The encapsulated transport layer PDU or other data, remains unchanged during the network layer processes.



Characteristics of IP

IP was designed as a protocol with low overhead.

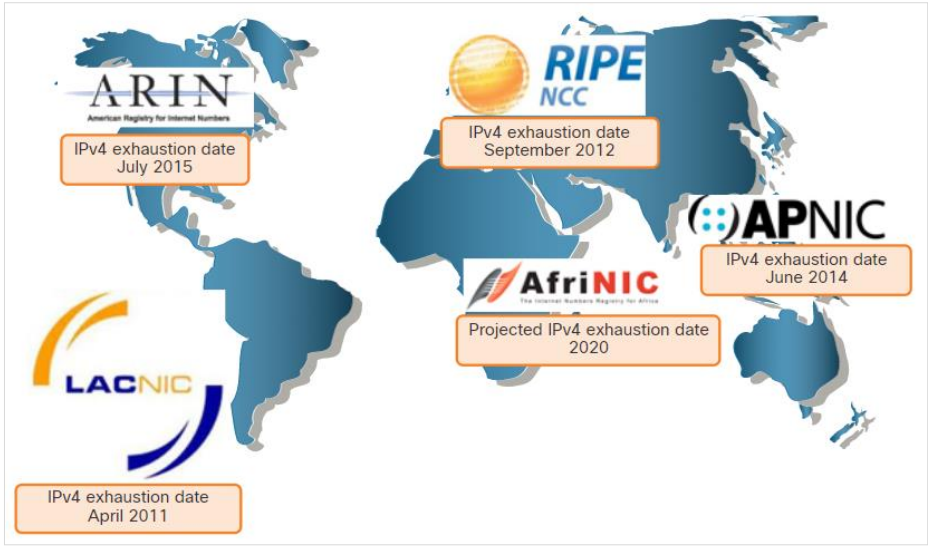
IP provides the functions that are necessary to deliver a packet from a source to a destination over an interconnected system of networks.

The basic characteristics of IP are as follows**:**

- **Connectionless -** There is no connection with the destination established before sending data packets.
- **Best Effort -** IP is inherently unreliable because packet delivery is not guaranteed.
- **Media Independent -** Operation is independent of the medium (for example, copper, fiber-optic, or wireless) carrying the data.

Need for IPv6

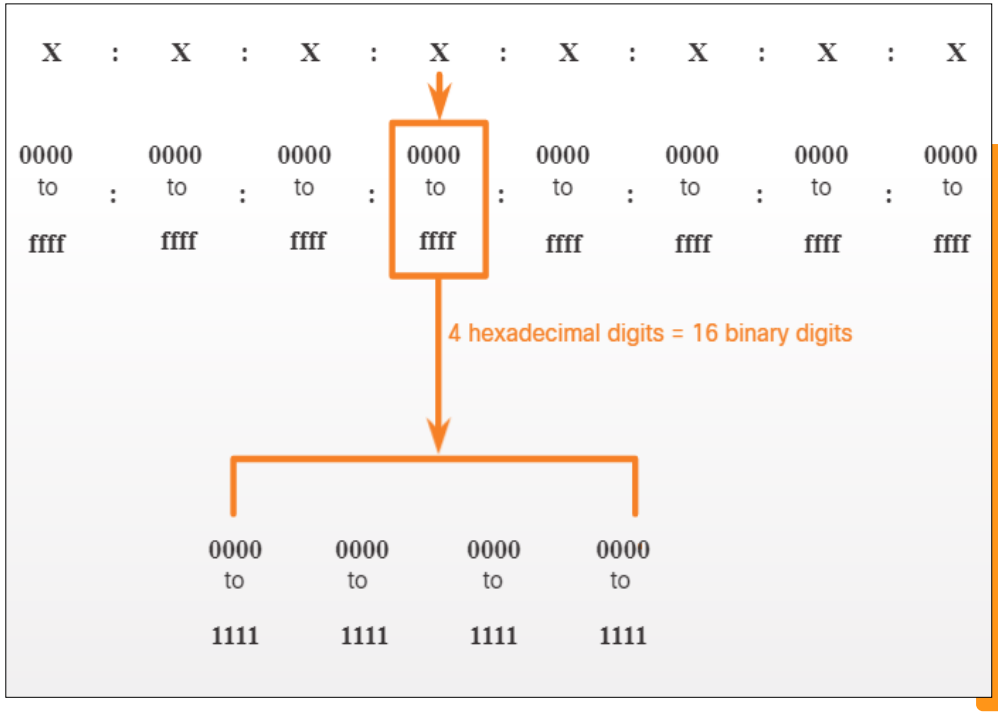
- IPv6 is designed to be the successor to IPv4.
- IPv6 has a larger 128-bit address space, providing 340 undecillion possible addresses.
- Mobile providers have been leading the way with the transition to IPv6.
- Most top ISPs and content providers such as YouTube, Facebook, and Netflix, have also made the transition.
- Many companies like Microsoft, Facebook, and LinkedIn are transitioning to IPv6-only internally.
- The depletion of IPv4 address space has been the motivating factor for moving to IPv6.



RIR IPv4 Exhaustion Dates

IPv6 Addressing Formats

- IPv6 addresses are 128 bits in length and written as a string of hexadecimal values.
- Every four bits is represented by a single hexadecimal digit for a total of 32 hexadecimal values.
- IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.



16-bit Segments or Hextets

IPv6 Addressing Formats (Contd.)

Preferred Format

- The preferred format for writing an IPv6 address is x:x:x:x:x:x:x:x, with each “x” consisting of four hexadecimal values.
- Each “x” is a single hextet which is 16 bits or four hexadecimal digits.

Examples of IPv6 addresses in the preferred format

```
2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000: 0200
2001 : 0db8 : 0000 : 00a3 : abcd : 0000 : 0000: 1234
2001 : 0db8 : 000a : 0001 : c012 : 9aff : fe9a: 19ac
2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000: 0000
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef
fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001
fe80 : 0000 : 0000 : 0000 : c012 : 9aff : fe9a: 19ac
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0000
```

Rule 1 - Omit Leading Zeros

- **Rule 1:** Omit any leading 0s (zeros) in any hextet.
- The four examples of ways to omit leading zeros:
  - 01ab can be represented as 1ab
    - 09f0 can be represented as 9f0
    - 0a00 can be represented as a00
    - 00ab can be represented as ab
- This rule only applies to leading 0s, NOT to trailing 0s, otherwise the address would be ambiguous. 01ab. For example, refer to the below table.

Type	Format
Preferred	2001 : **0**db8 : **000**0 : 1111 : **000**0 : **000**0 : **000**0 : **0**200
No leading 0s	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200

Rule 2 - Double Colon

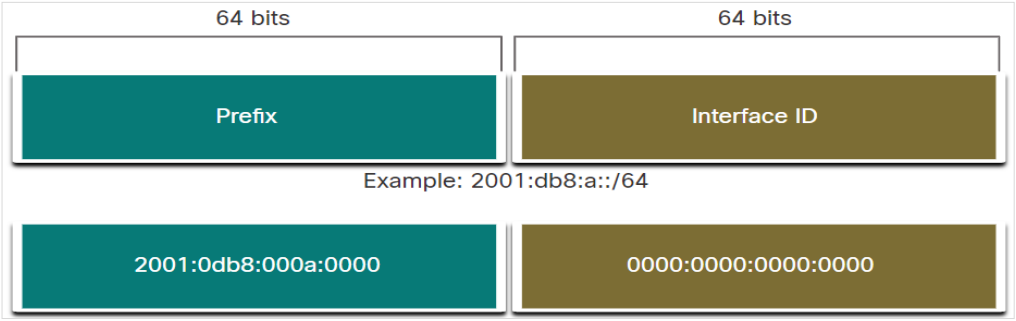
Rule 2: Double colon (::) can replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros.

- **Example:** 2001:db8:cafe:1:0:0:0:1 could be represented as 2001:db8:cafe:1::1.
- The double colon (::) is used in place of the three all-0 hextets (0:0:0).
- The double colon (::) can only be used once within an address.
- When used with the omitting leading 0s technique, the notation of IPv6 address can often be greatly reduced. This is commonly known as the compressed format.
- **Example of incorrect use of the double colon:** 2001:db8::abcd::1234.

Type	Format
Preferred	2001 : **0**db8 : **000**0 : 1111 : **0000** : **0000** : **0000** : **0**200
Compressed/spaces	2001 : db8 : 0 : 1111 : : 200
Compressed	2001:db8:0:1111::200

IPv6 Prefix Length

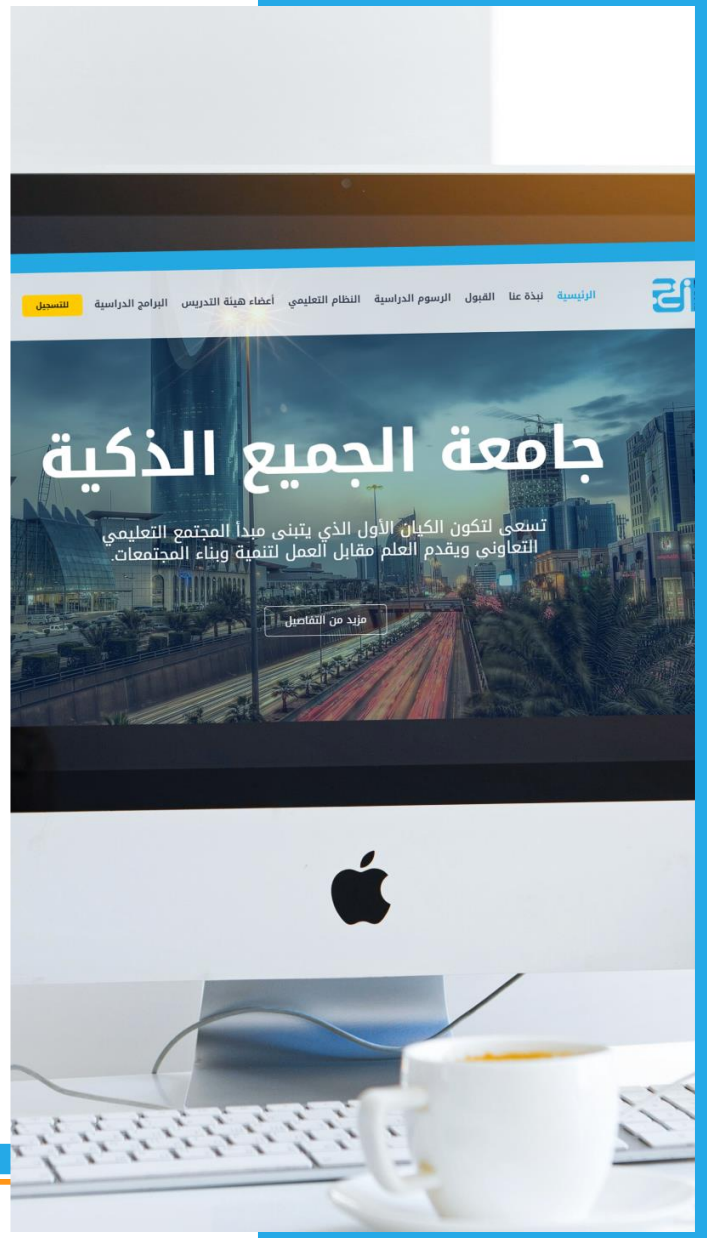
- The prefix can be identified by a dotted-decimal subnet mask or prefix length (slash notation).
- For example, an IPv4 address of 192.168.1.10 with dotted-decimal subnet mask 255.255.255.0 is equivalent to 192.168.1.10/24.
- In IPv4 the /24 is called the prefix, whereas in Pv6 it is called the prefix length.
- Similar to IPv4, the prefix length is represented in slash notation and is used to indicate the network portion of an IPv6 address. It can range from 0 to128.
- It is strongly recommended to use a 64-bit Interface ID for most networks.



Lecture – 3

Network protocols and services analysis

ICMP



جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

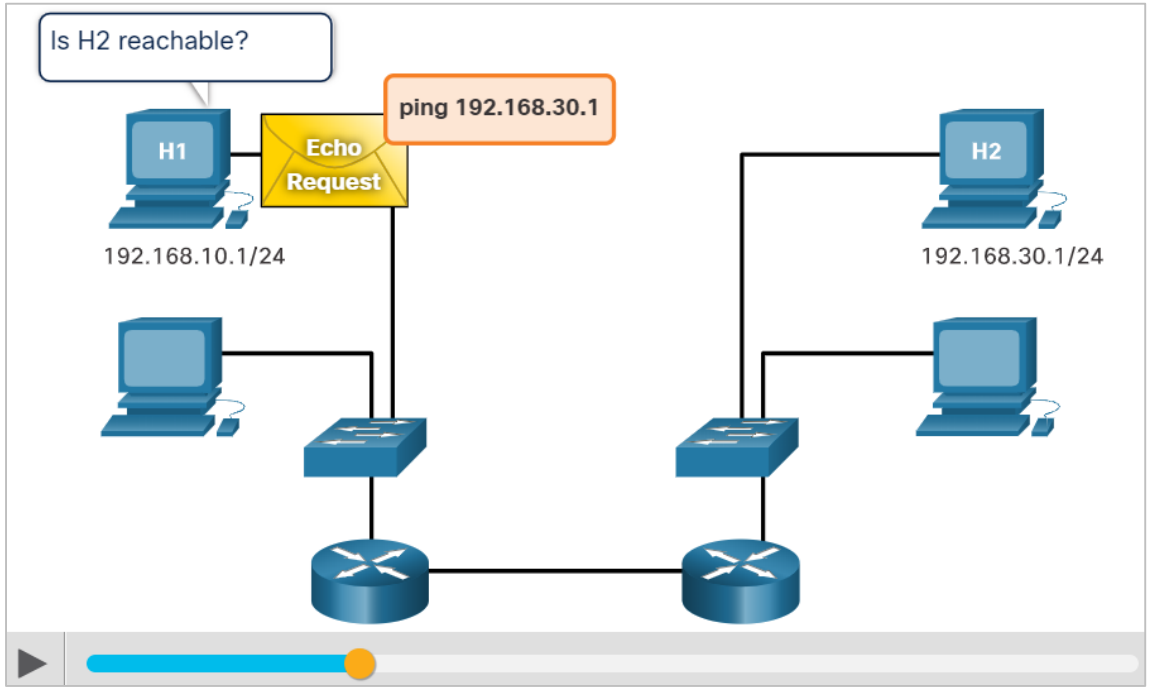
ICMPv4 Messages

- The TCP/IP suite provide messages to be sent in the event of certain errors. These messages are sent using the services of ICMP.
- The purpose of these messages is to provide feedback about issues related to the processing of IP packets under certain conditions.
- ICMP messages are not required and are often not allowed within a network for security reasons.
- ICMP is available for both IPv4 and IPv6. ICMPv4 is the messaging protocol for IPv4. ICMPv6 provides the same services for IPv6 but includes additional functionality.
- ICMP messages common to both ICMPv4 and ICMPv6 include host confirmation, destination or service unreachable, time exceeded and route redirection.

ICMPv4 Messages (Contd.)

Host Confirmation

- An ICMP Echo Message can be used to determine if a host is operational.
- The local host sends an ICMP Echo Request to a host. If the host is available, the destination host responds with an Echo Reply.
- This use of the ICMP Echo messages is the basis of the ping utility.



ICMPv4 Messages (Contd.)

Destination or Service Unreachable

- When a host or gateway receives a packet that it cannot deliver, it can use an ICMP Destination Unreachable message to notify the source that the destination or service is unreachable.
- The message will include a code that indicates why the packet could not be delivered. The Destination Unreachable codes for ICMPv4 includes the following:
  - **0 -** Net unreachable
  - **1 -** Host unreachable
  - **2 -** Protocol unreachable
  - **3 -** Port unreachable

ICMPv4 Messages (Contd.)

Time Exceeded

- An ICMPv4 Time Exceeded message is used by a router to indicate that a packet cannot be forwarded because the Time to Live (TTL) field of the packet was decremented to 0.
- If a router receives a packet and decrements the TTL field in the IPv4 packet to zero, it discards the packet and sends a Time Exceeded message to the source host.
- ICMPv6 also sends a Time Exceeded message if the router cannot forward an IPv6 packet because the packet has expired.
- IPv6 does not have a TTL field. It uses the hop limit field to determine if the packet has expired.

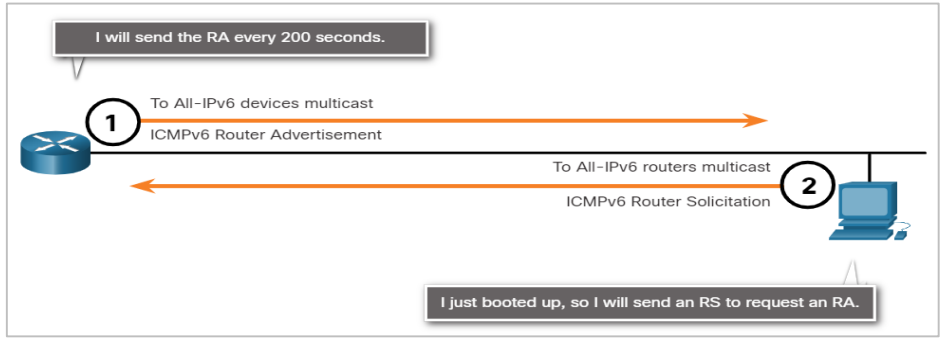
ICMPv6 RS and RA Messages

- ICMPv6 has new features and improved functionality not found in ICMPv4. ICMPv6 messages are encapsulated in IPv6.
- It has four new protocols as part of the Neighbor Discovery Protocol (ND or NDP).
- Messaging between an IPv6 router and an IPv6 device:
  - Router Solicitation (RS) message
  - Router Advertisement (RA) message
- Messaging between IPv6 devices:
  - Neighbour Solicitation (NS) message
  - Neighbour Advertisement (NA) message

ICMPv6 RS and RA Messages (Contd.)

Router Solicitation: Messaging Between an IPv6 Router and an IPv6 Device

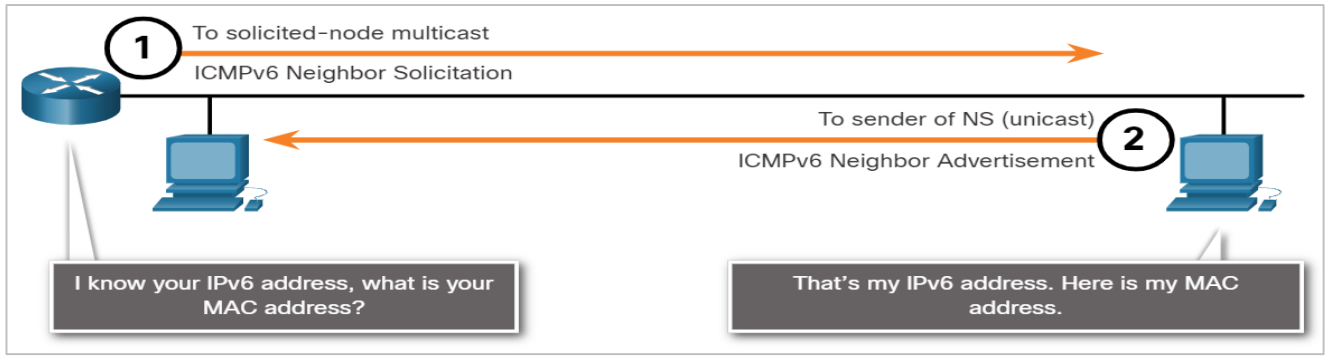
- RA messages are sent by routers to provide addressing information to hosts using Stateless Address Auto Configuration (SLAAC).
- A router will send an RA message periodically or in response to an RS message. A host using SLAAC will set its default gateway to the link-local address of the router that sent the RA.
- When a host is configured to obtain its addressing information automatically using SLAAC, the host will send an RS message to the router requesting an RA message.



ICMPv6 RS and RA Messages (Contd.)

Address Resolution: Messaging Between IPv6 Devices

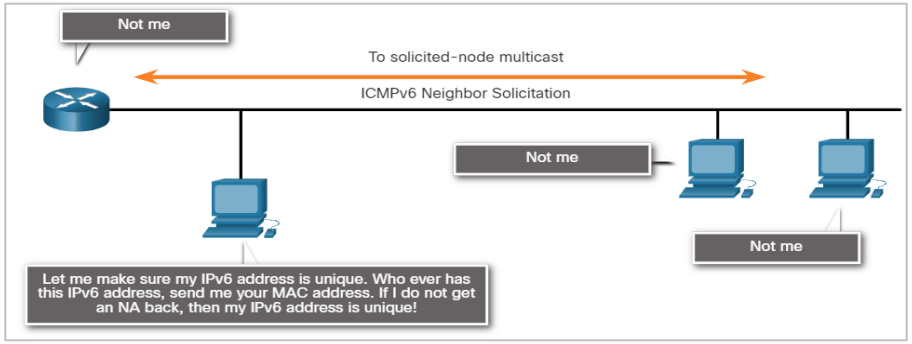
- NA messages are sent when a device knows the IPv6 address of a device but does not know its MAC address. This is equivalent to an ARP Request for IPv4.
- NA messages are sent in response to an NS message and match the target IPv6 address in the NS. The NA message includes the device's Ethernet MAC address. This is equivalent to an ARP Reply in IPv4.



ICMPv6 RS and RA Messages (Contd.)

Duplicate Address Detection (DAD)

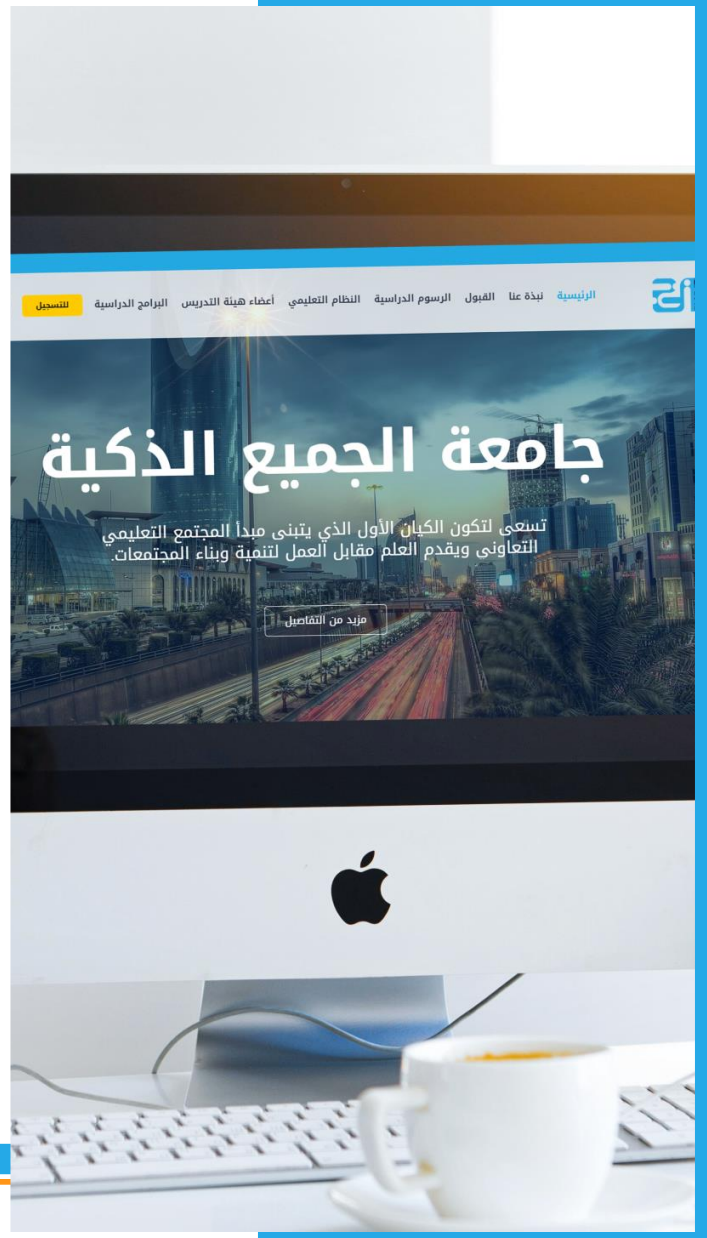
- When a device is assigned a global unicast or link-local unicast address, the DAD is performed on the address to ensure that it is unique.
- To check the uniqueness of an address, the device will send an NS message with its own IPv6 address.
- If another device on the network has this address, it will respond with an NA message which will notify the sending device that the address is in use. If a corresponding NA message is not returned within a certain period of time, the unicast address is unique and acceptable for use.



Lecture – 3

Network protocols and services analysis

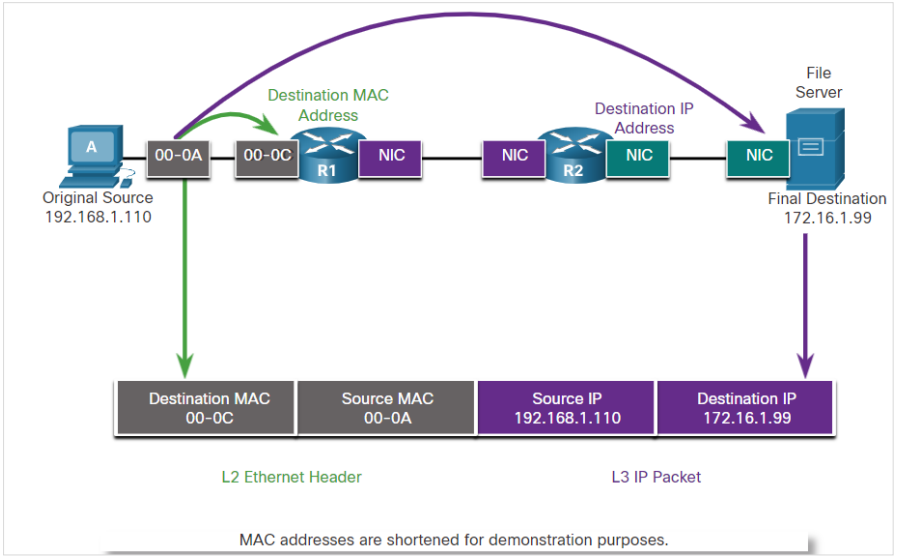
ARP and ARP Issues



جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

Destination on Remote Network

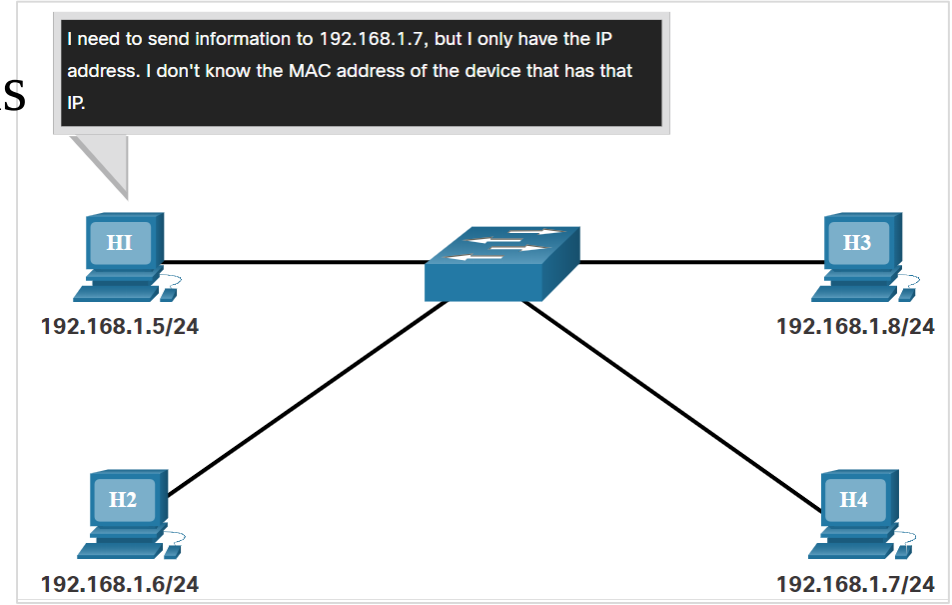
- When the destination IP address is on a remote network, the destination MAC address will be the address of the host's default gateway. The process in the figure is as below:
  - Routers examine the destination IPv4 address.
  - When the router receives the Ethernet frame, it de-encapsulates the Layer 2 information.
  - Using the destination IP address, the router determines the next-hop device, and then encapsulates the IP packet in a new data link frame for the outgoing interface.
  - If the next-hop device is the final destination, the destination MAC address will be that of the device's Ethernet NIC.



Communicating on a remote network

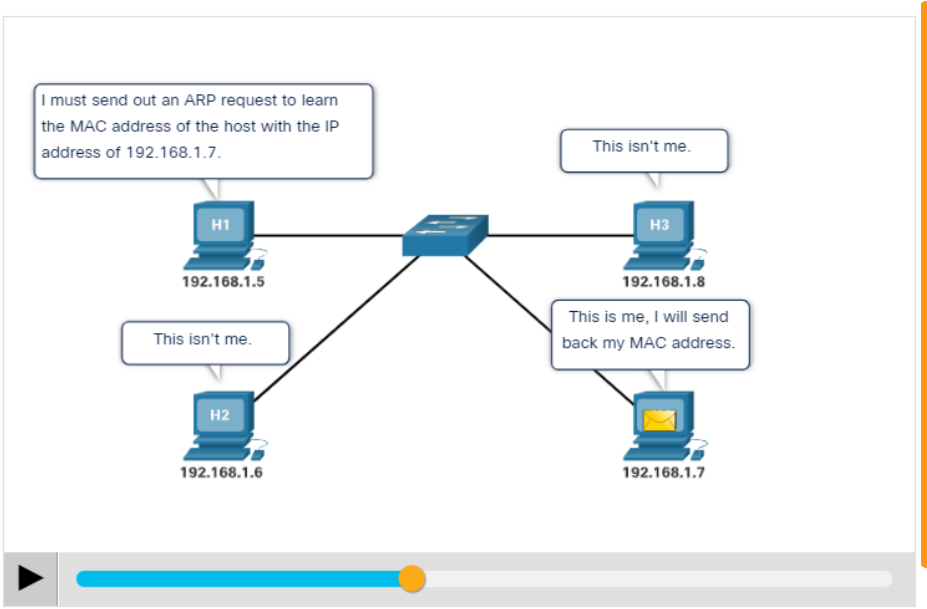
ARP Overview

- The figure illustrates a problem while sending a packet to another host on the same local IPv4 network because the IP address is known but the MAC address of the device is unknown.
- A device uses Address Resolution Protocol (ARP) to determine the destination MAC address of a local device when it knows its IPv4 address.
- ARP provides two basic functions:
  - Resolving IPv4 addresses to MAC addresses
  - Maintaining a table of IPv4 to MAC address mappings



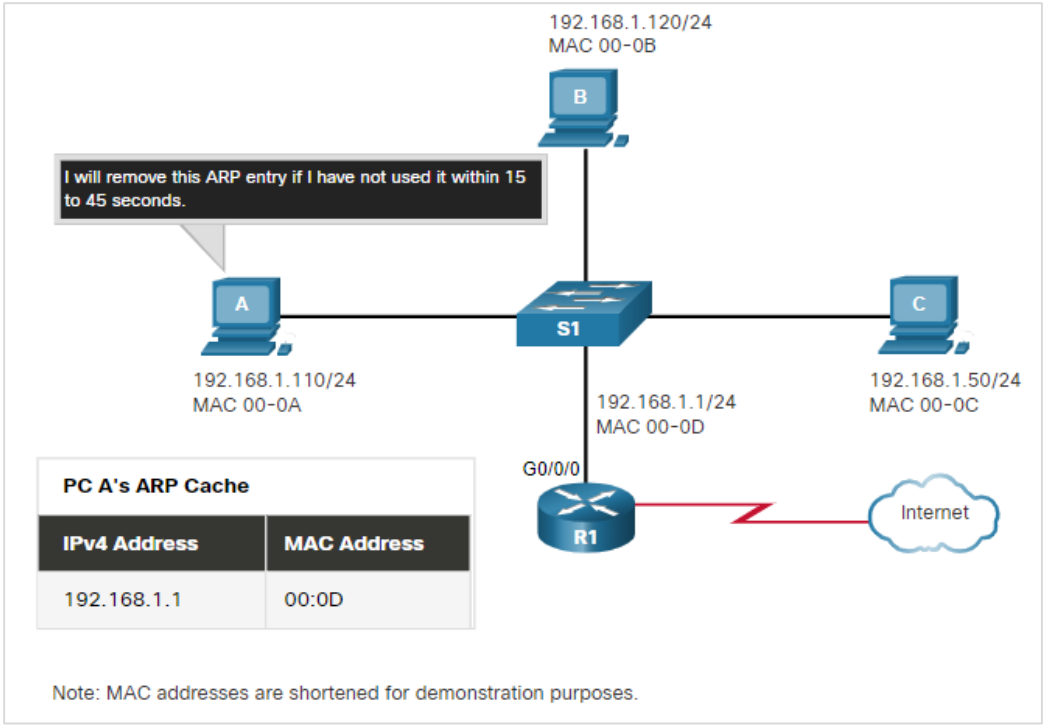
ARP Functions

- When a packet is sent to the data link layer to be encapsulated into an Ethernet frame, the device refers to a table called **ARP table** or ARP cache in its RAM memory to find the MAC address that is mapped to the IPv4 address.
- The sending device will search its ARP table for a destination IPv4 address and a corresponding MAC address, if the packet's destination IPv4 address is on the same network as the source IPv4 address.
- If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame.



Removing Entries from an ARP Table

- For each device, an ARP cache timer removes the ARP entries that have not been used for a specified period of time.
- The times differ depending on the operating system of the device.
- Commands may also be used to manually remove some or all of the entries in the ARP table.
- After an entry has been removed, the process for sending an ARP request and receiving an ARP reply must occur again to enter the map in the ARP table.



ARP Tables on Networking Devices

On a Cisco router, the **show ip arp** command is used to display the ARP table.

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1            -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.225          -   a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.226          1   a03d.6fe1.9d91  ARPA   GigabitEthernet0/0/1
R1#
```

On a Windows 10 PC, the **arp –a** command is used to display the ARP table.

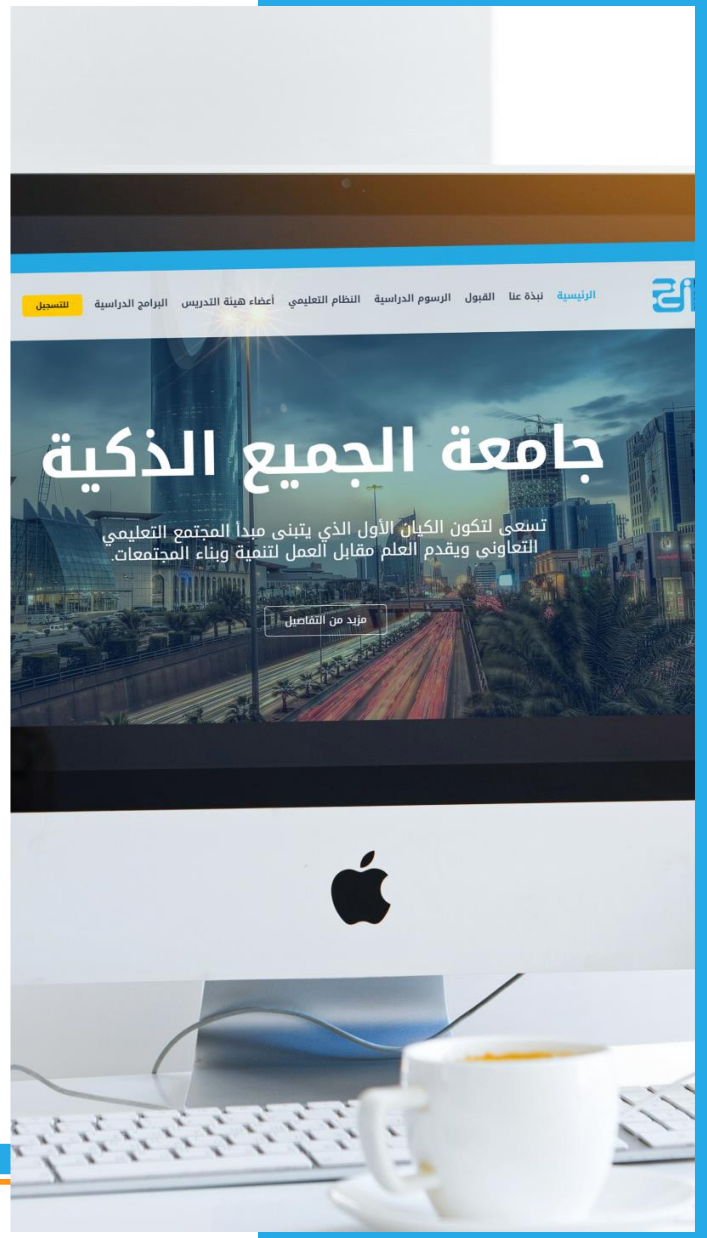
```
C:\Users\PC> arp -a
Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
  192.168.1.110         08-3e-0c-f5-f7-56     dynamic
  192.168.1.112         ac-b3-13-4a-bd-d0     dynamic
  192.168.1.117         08-3e-0c-f5-f7-5c     dynamic
  192.168.1.126         24-77-03-45-5d-c4     dynamic
  192.168.1.146         94-57-a5-0c-5b-02     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\Users\PC>
```

Lecture – 3
Activity 1

Wireshark to Examine Ethernet Frames

In this lab, you will do the following:

- Use Wireshark to capture and view Ethernet Frames in order to investigate ARP and IP and MAC addressing.
- Capture and analyze ICMP frames.

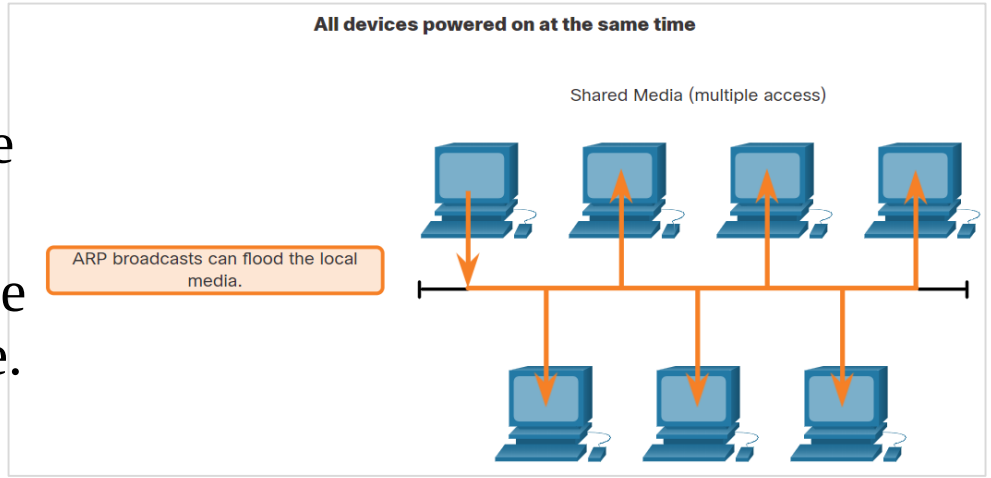


جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

ARP Issues - ARP Broadcasts and ARP Spoofing

ARP Broadcasts

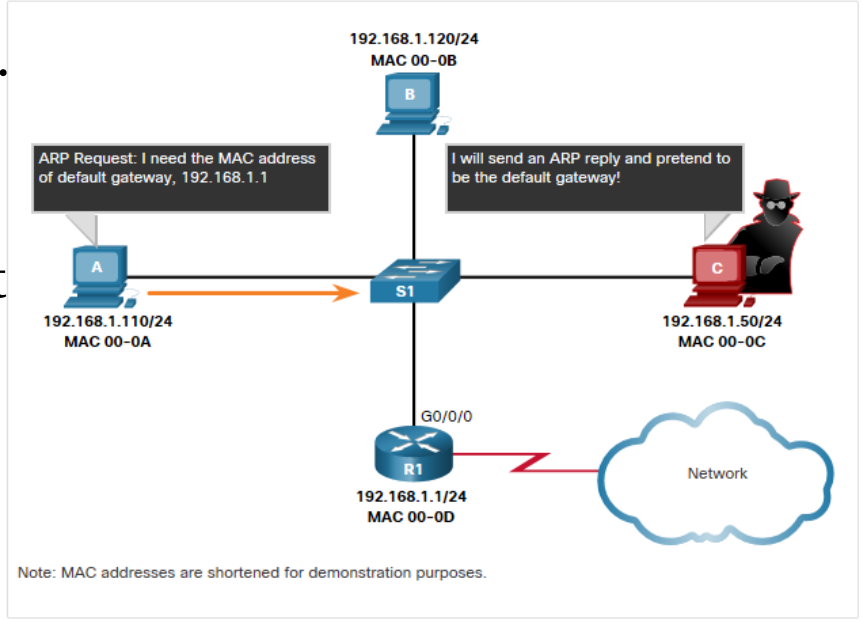
- As a broadcast frame, an ARP request is received and processed by every device on the local network.
- On a typical business network, these broadcasts would have minimal impact on network performance.
- If many devices start accessing network services at the same time, there can be reduction in performance for a short time.
- After the devices send out the initial ARP broadcasts and have learned the necessary MAC addresses, any impact on the network will be minimized.



ARP Issues - ARP Broadcasts and ARP Spoofing (Contd.)

ARP Spoofing

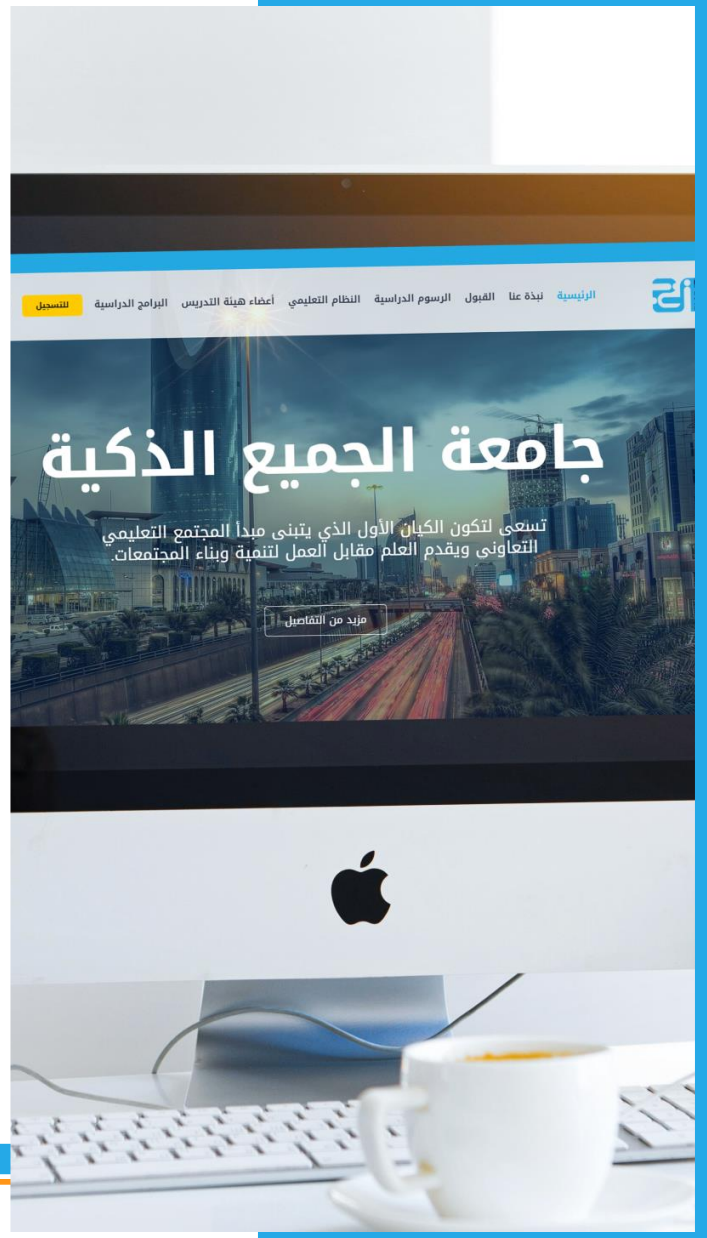
- The use of ARP can lead to a potential security risk in some cases.
- A threat actor uses ARP spoofing to perform an ARP poisoning attack.
  - It is a technique used by a threat actor to reply to an ARP request for an IPv4 address belonging to another device, such as the default gateway.
  - The threat actor sends an ARP reply with its own MAC address.The receiver of the ARP reply will add the wrong MAC address to its ARP table and send these packets to the threat actor.



Lecture – 3

Network protocols and services analysis

DHCP

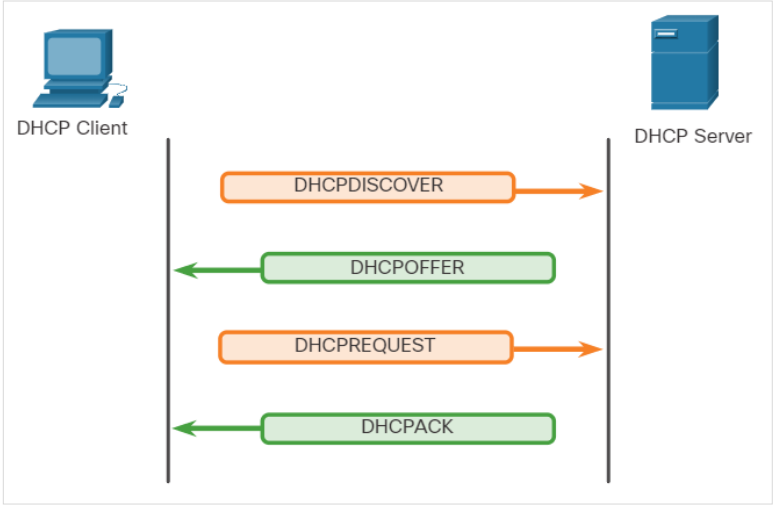


جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

DHCP Operation

- DHCP operation includes: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK, and DHCPNAK.

- When DHCP-configured device connects to the network, the client broadcasts a **DHCPDISCOVER** message to identify any available DHCP servers on the network.
- A DHCP server replies with a **DHCPOFFER** message, which offers a lease to the client.
- The client sends a **DHCPREQUEST** message that identifies the explicit server and lease offer that the client is accepting.

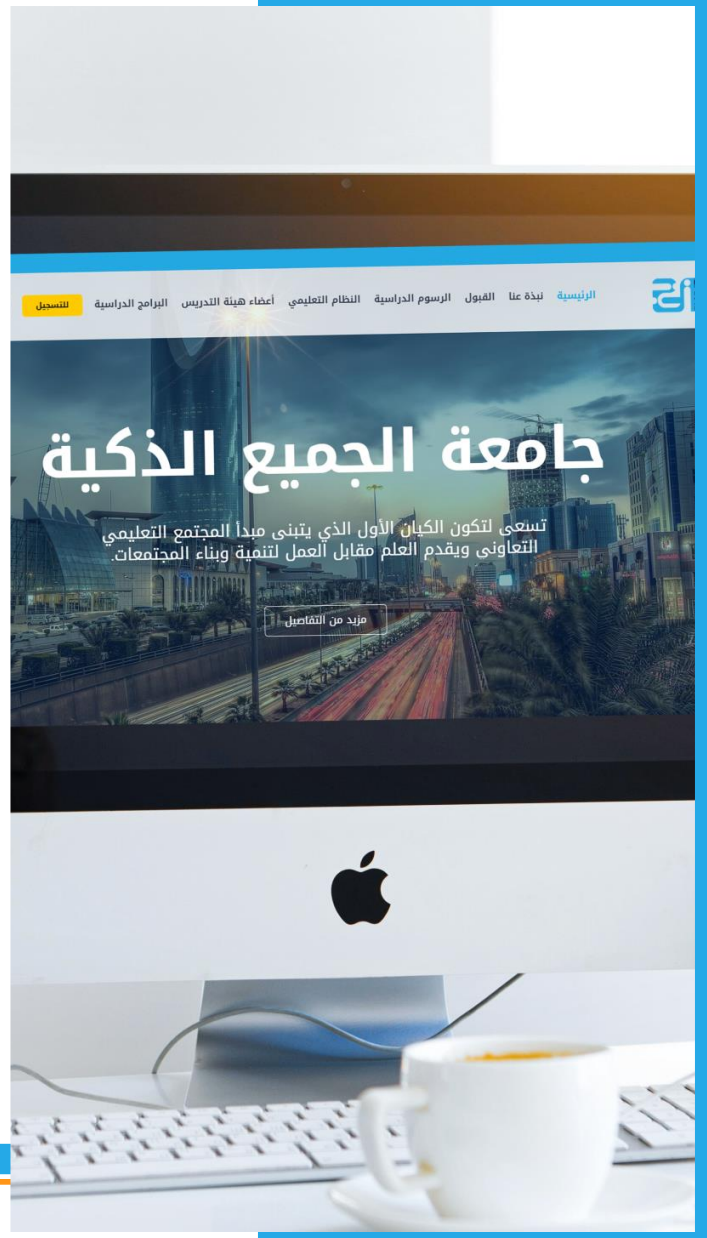


- If the IPv4 address requested by the client, or offered by the server, is still available, the server returns the **DHCPACK** message. If the offer is no longer valid, then the selected server responds with a **DHCPNAK** message. If a **DHCPNAK** message is returned, then the selection process begins again with a new **DHCPDISCOVER** message being transmitted.

Lecture – 3

Network protocols and services analysis

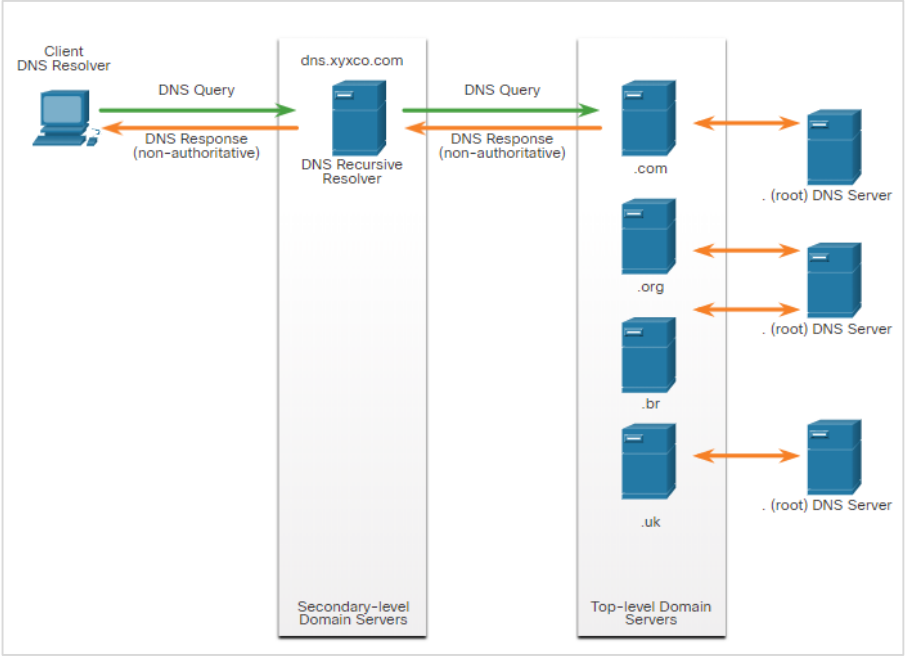
DNS



جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

The DNS Lookup Process

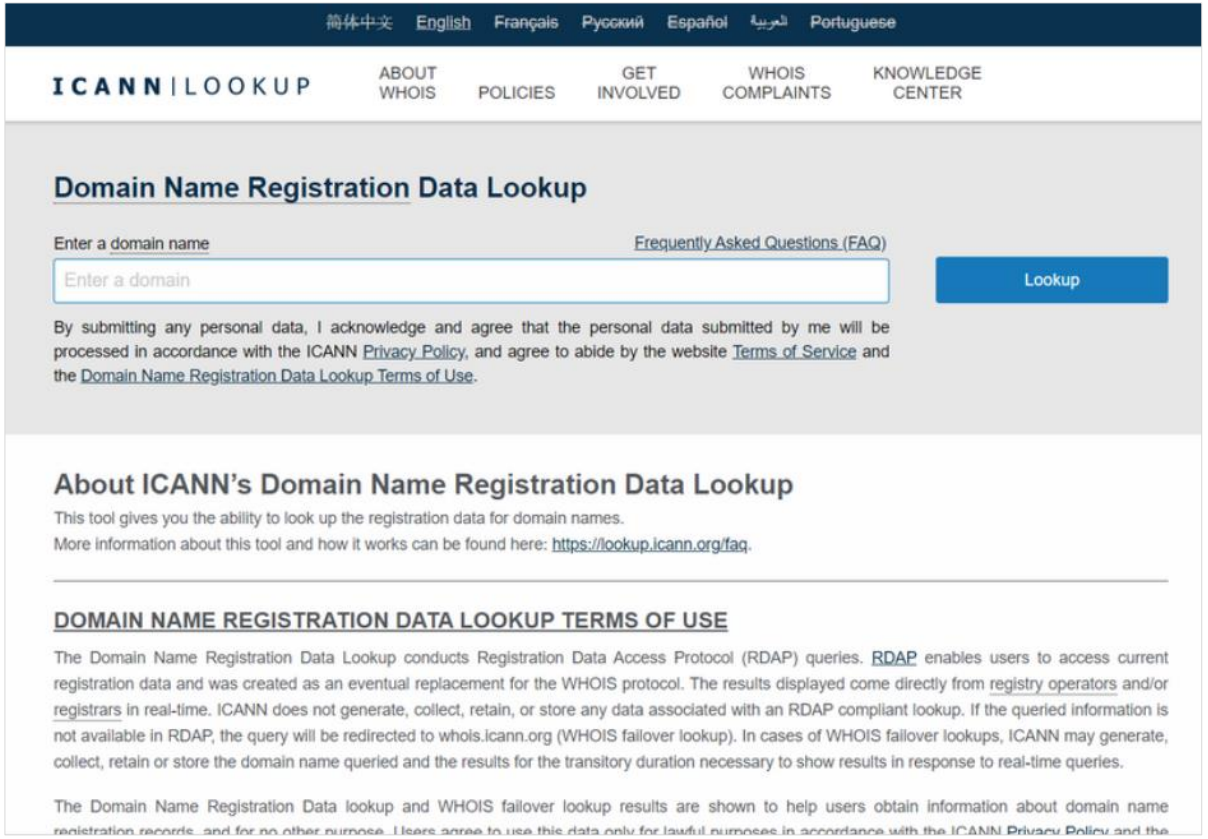
- To resolve a name to an IP address, the resolver, will first check its local DNS cache. If the mapping is not found, a query will be issued to the DNS server .
- If the mapping is not found there, the DNS server will query other higher-level DNS servers that are authoritative for the top-level domain in order to find the mapping. These are known as **recursive queries**.
- The caching DNS servers can resolve recursive queries without forwarding the queries to higher level servers.



- If a server requires data for a zone, it will request a transfer of that data from an authoritative server for that zone. The process of transferring DNS data between servers is known as zone transfer.

The WHOIS Protocol

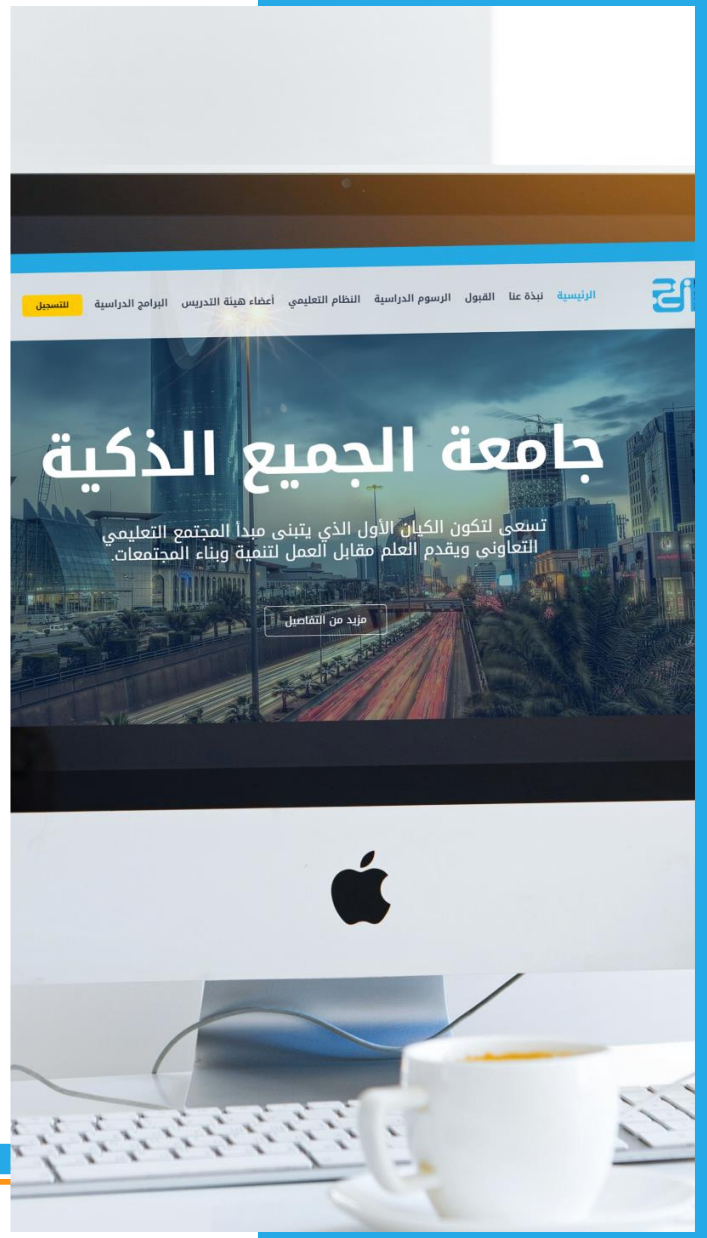
- WHOIS is a TCP-based protocol that is used to identify the owners of internet domains through the DNS system.
- The WHOIS application uses a query, in the form of a FQDN.
- WHOIS is a starting point for identifying potentially dangerous internet locations that may have been reached through the network.
- ICANN Lookup, an internet-based WHOIS tool, is used to obtain the registration record a URL.



Lecture – 3

Network protocols and services analysis

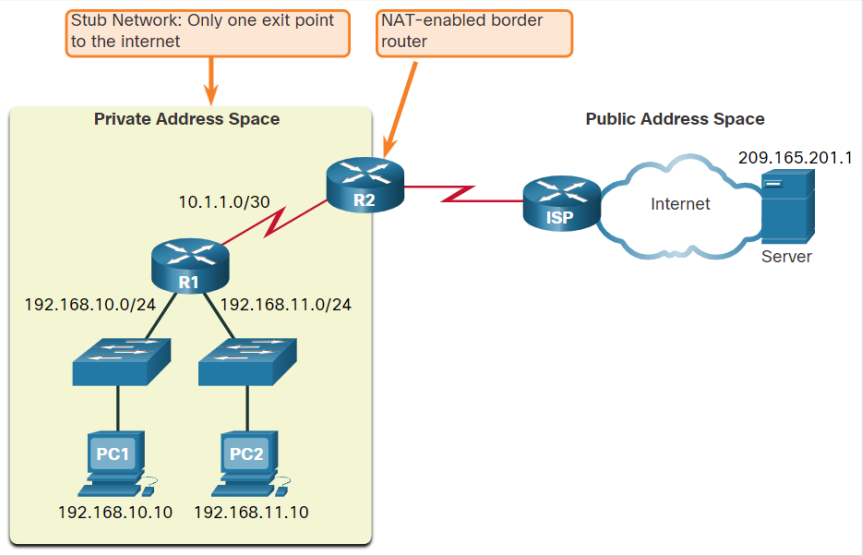
NAT



جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

What is NAT?

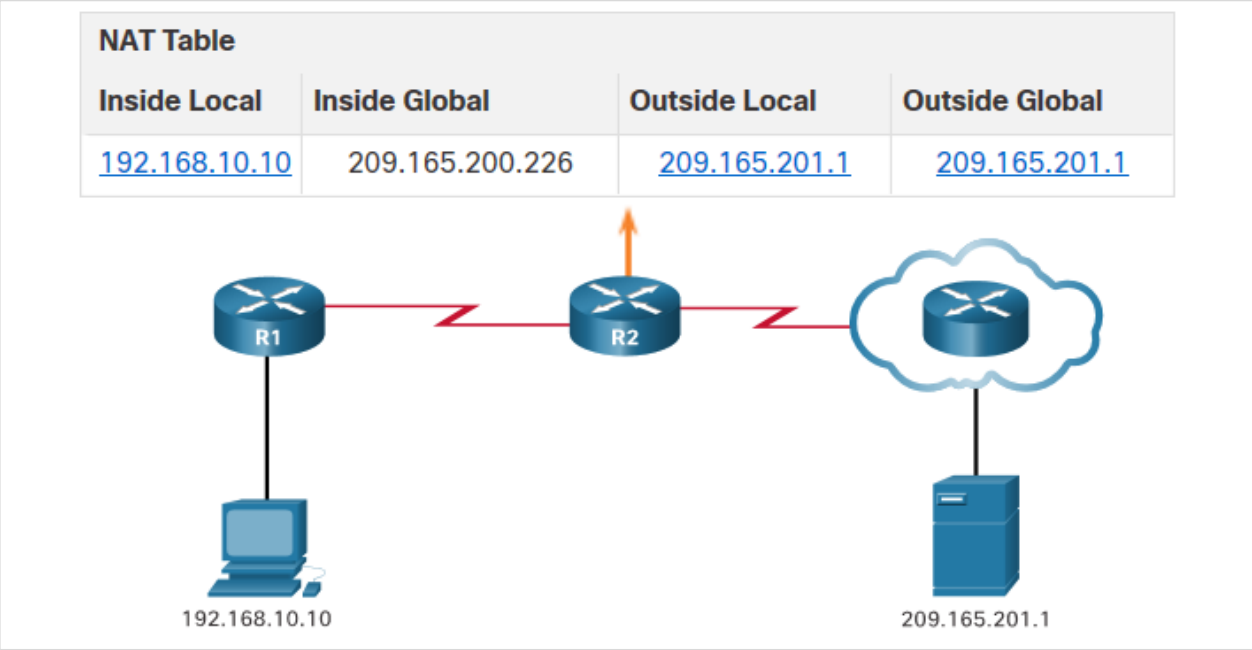
- NAT is used to conserve public IPv4 addresses.
- NAT-enabled routers can be configured with one or more valid public IPv4 addresses which are known as the **NAT pool**.
- A NAT router typically operates at the border of a stub network.
- When a device inside the stub network wants to communicate with a device outside its network, the packet is forwarded to the border router and the router performs the NAT process.



***Note**: The connection to the ISP may use a private address or a public address that is shared among customers. For the purposes of this module, a public address is shown.*

How NAT works?

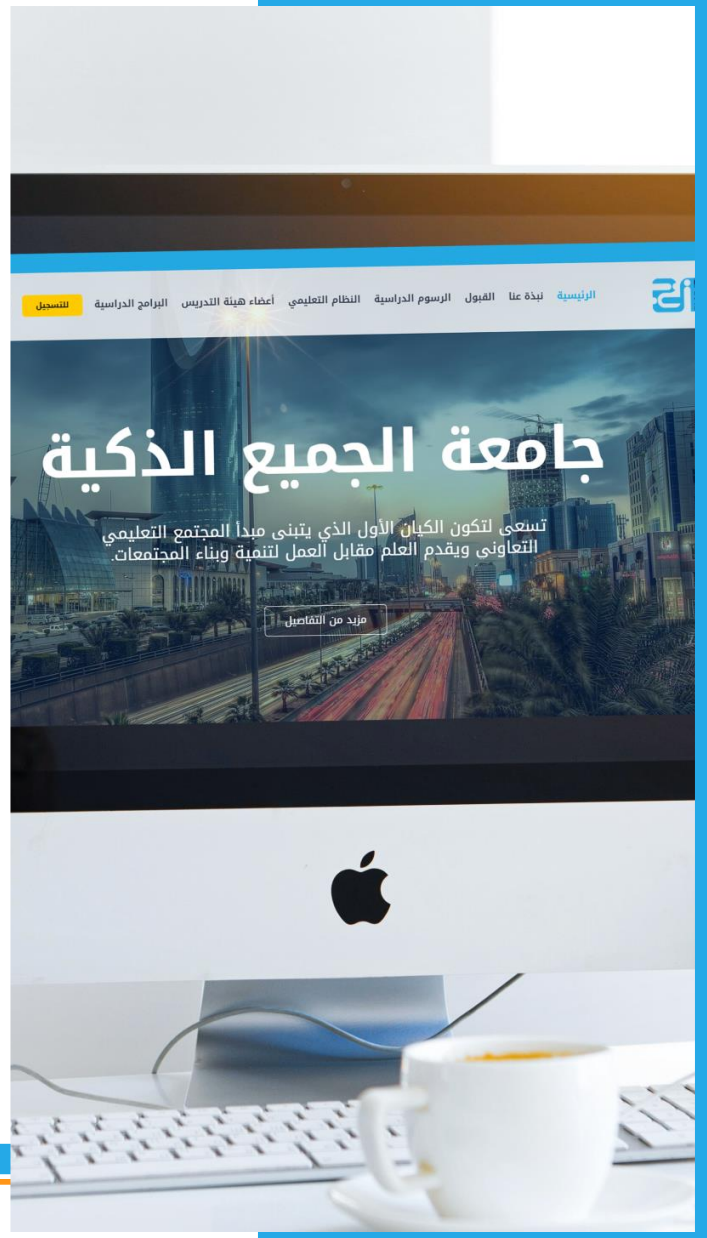
- In this example, PC1 with private address 192.168.10.10 wants to communicate with an outside web server with public address 209.165.201.1.



Lecture – 3

Network protocols and services analysis

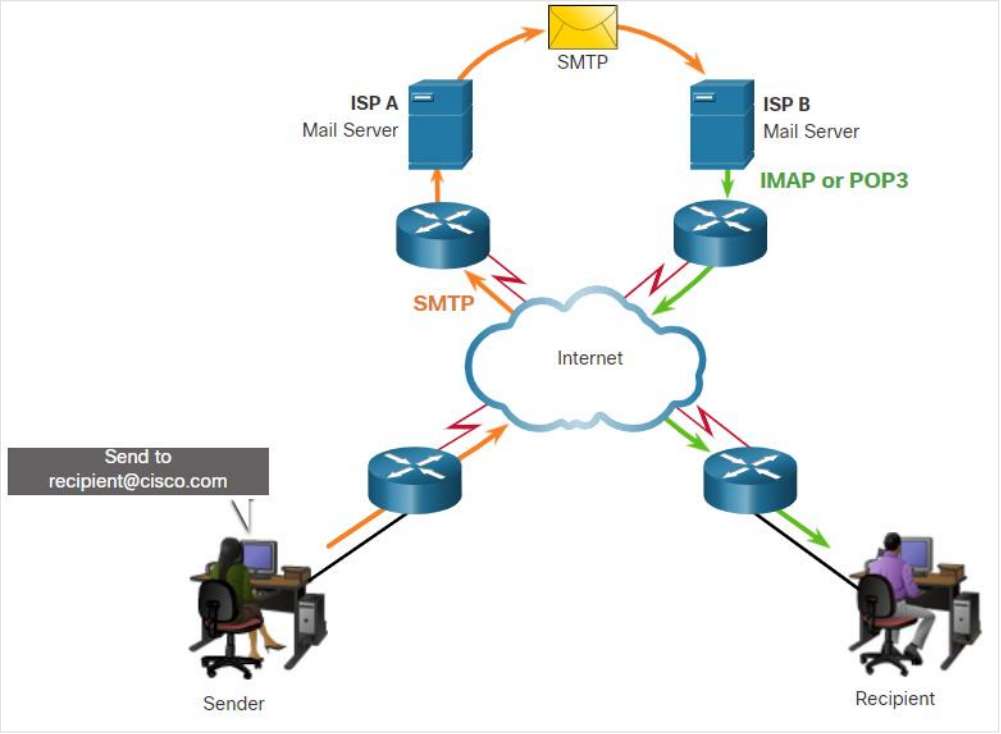
Email and HTTP



جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

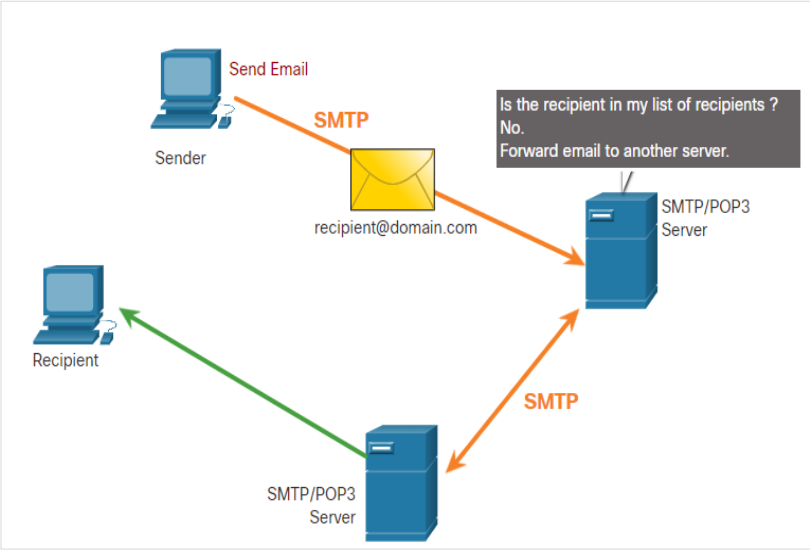
Email protocols

- Email is a store-and-forward method of sending, storing, and retrieving electronic messages across a network.
- Email clients communicate with mail servers to send and receive email.
- Email supports three separate protocols for operation: Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and IMAP.
- A client retrieves email using one of the two application layer protocols: POP or IMAP.



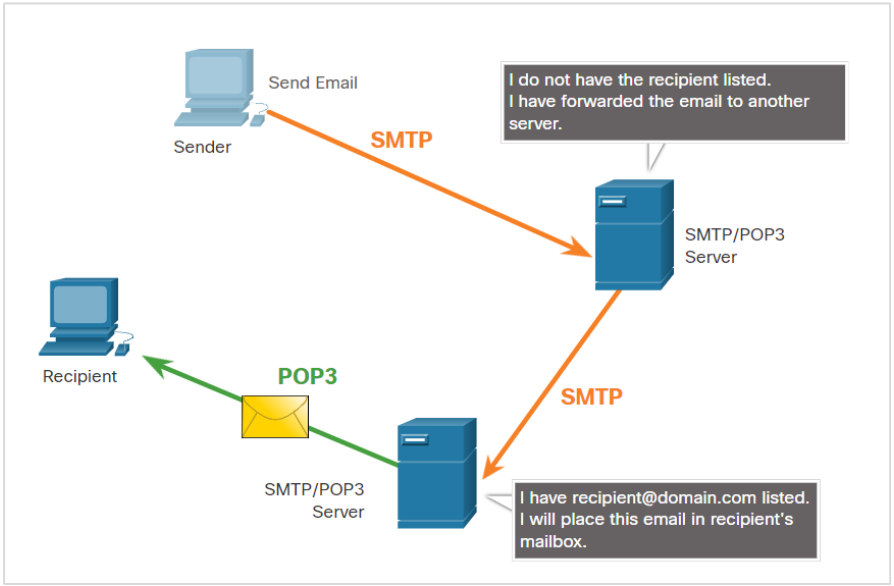
SMTP

- SMTP message formats require a message header and a message body.
- When a client sends an email, the client SMTP process connects with a server SMTP process on a well-known port 25.
- 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.
- Periodically, the server checks the queue for messages and attempts to send them again. If the message is still not delivered after a predetermined expiration time, it is returned to the sender as undeliverable.



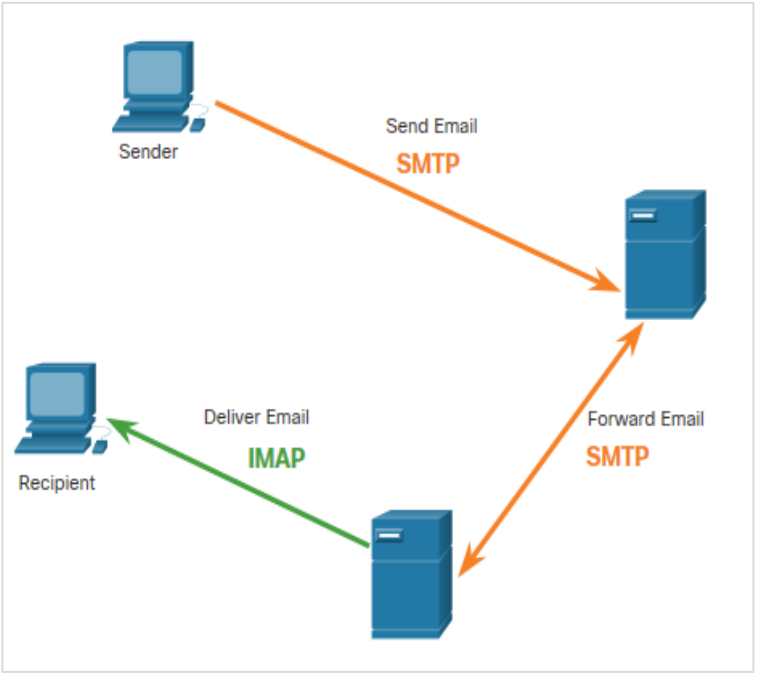
POP3

- POP3 is used by an application to retrieve a mail from a mail server.
- With POP3, email messages are downloaded to the client and removed from the server.
- The server starts the POP3 service by passively listening on TCP port 110 for client connection requests.
- The client sends a request to establish a TCP connection with the server.
- Once the connection is established, the POP3 server sends a greeting. The client and POP3 server then exchange commands and responses until the connection is closed or aborted.



IMAP

- IMAP is the protocol that describes a method to retrieve email messages.
- When the user connects to an IMAP-capable server, copies of the messages are downloaded to the client application. The original messages are kept on the server until manually deleted.
- Users view copies of the messages in their email client software.
- Users can create a file hierarchy on the server to organize and store mail.
- When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.



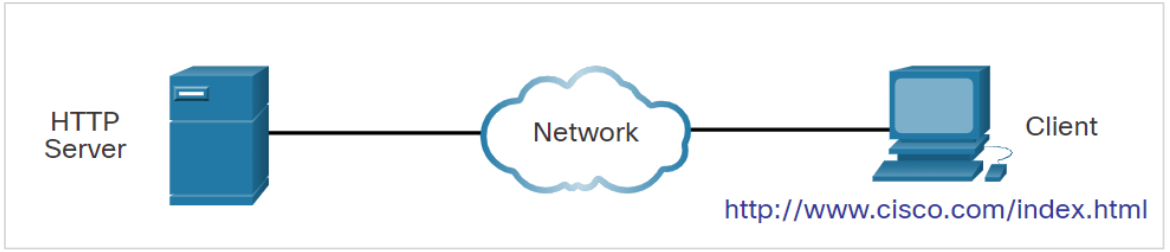
Lecture – 3

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 with the web service that is using the HTTP protocol.
- Lets take a look on how a web page is opened in a browser.
  Example: http://www.cisco.com/index.html

Step 1: The browser interprets the three parts of the URL:

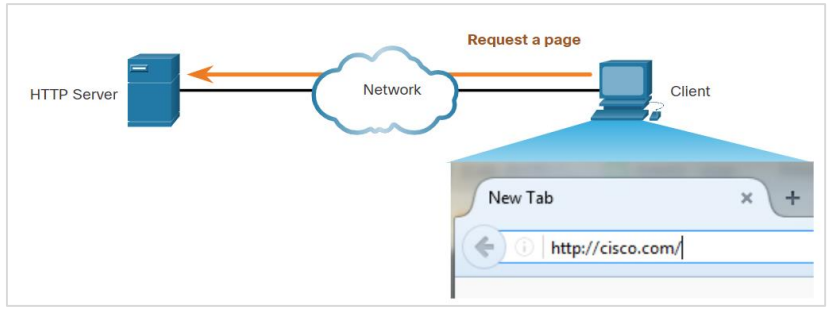
- http (the protocol or scheme)
- www.cisco.com (the server name)
- index.html (the specific filename requested)



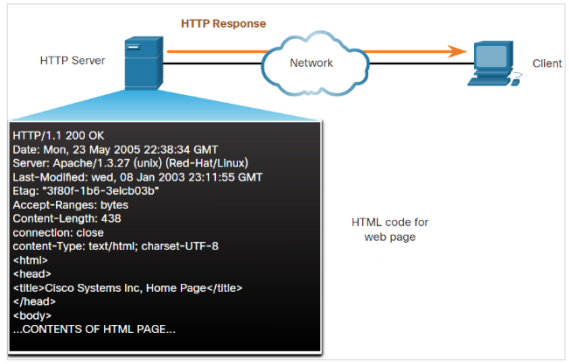
جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

Hypertext Transfer Protocol and Hypertext Markup Language (Contd.)

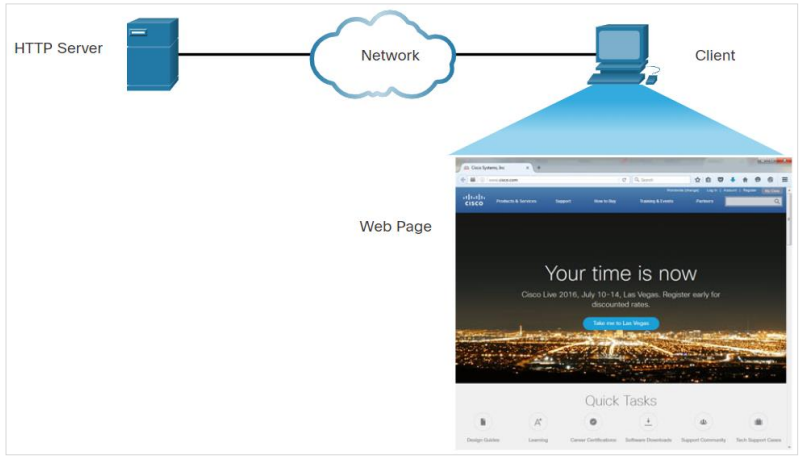
- **Step 2:** The client initiates an HTTP request to a server by sending a GET request to the server and asks for the index.html file.



- **Step 3:** In response to the request, the server sends the HTML code for this web page to the browser.



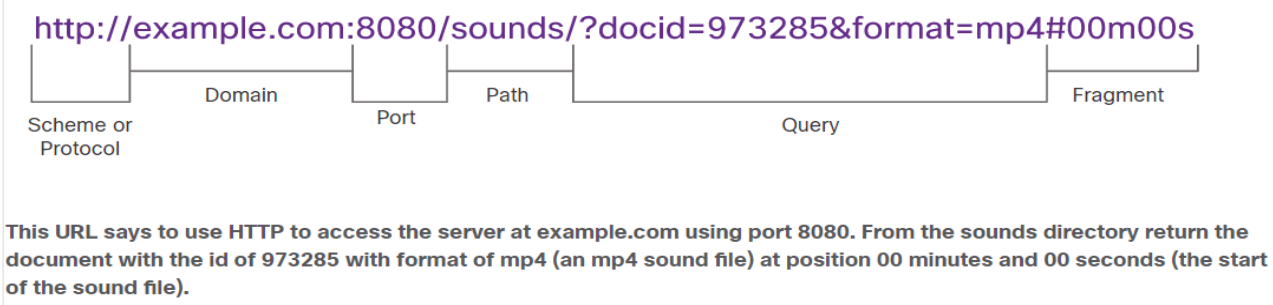
- **Step 4:** The browser deciphers the HTML code and formats the page for the browser window.



جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

The HTTP URL

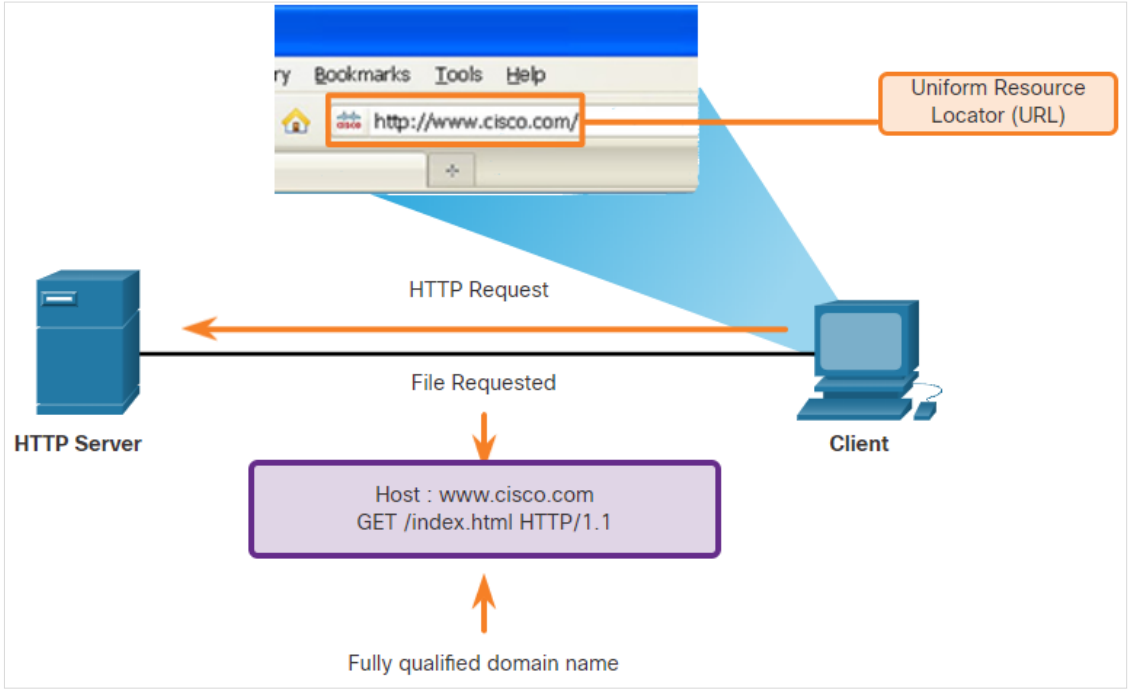
- HTTP URLs can specify the port on the server that should handle the HTTP methods.
- It can specify a query string and fragment.
- Query strings are preceded by a "?" character and typically consist of a series of name and value pairs.
- A fragment is preceded by a "#" character. It refers to a subordinate part of the resource that is requested in the URL.
- The parts of an HTTP URL are shown in the below figure:



This URL says to use HTTP to access the server at example.com using port 8080. From the sounds directory return the document with the id of 973285 with format of mp4 (an mp4 sound file) at position 00 minutes and 00 seconds (the start of the sound file).

HTTP Operation

- HTTP is a request/response protocol that uses TCP port 80.It is flexible but not a secure protocol.
- When a client sends a request to a web server, it will use one of the six methods specified by HTTP:
  - GET
  - POST
  - PUT
  - DELETE
  - OPTIONS
  - CONNECT



HTTP Status Codes

- The HTTP Status codes are numeric, with the first number in the code indicating the type of message.
- The five status code groups are **1xx** - Informational, **2xx** - Success, **3xx** - Redirection , **4xx** - Client Error and **5xx** - Server Error
- The below table explains some common status codes:

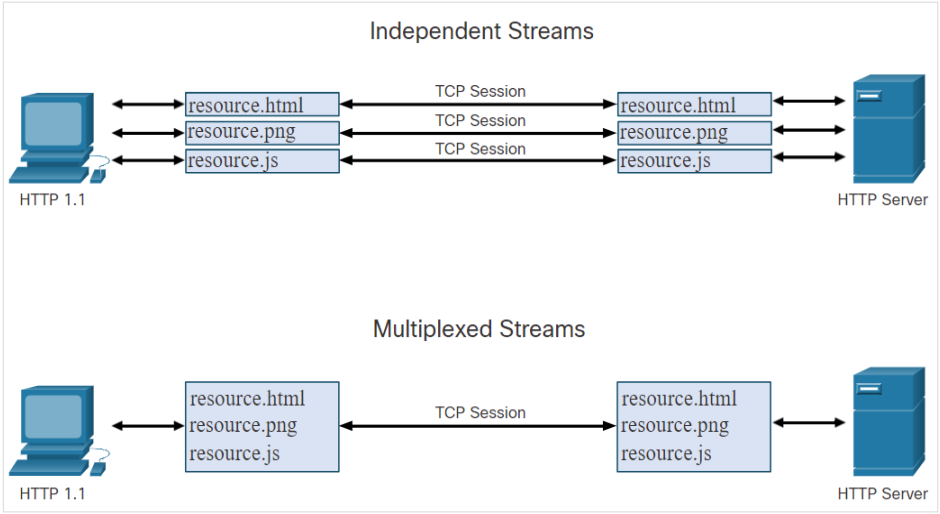
Code	Status	Meaning
1xx - Informational		
100	Continue	The client should continue with the request. The Server has verified that the request can be fulfilled.
2xx - Success		
200	OK	The request completed successfully.
202	Accepted	The request has been accepted for processing, but processing is not completed.

HTTP Status Codes (Contd.)

Code	Status	Meaning
4xx – Client Error		
403	Forbidden	The request is understood by the server, but the resource will not be fulfilled. This is possibly because the requester is not authorized to view the resource.
404	Not Found	The server could not find the requested resource. This can be caused by an out-of-date or incorrect URL.

HTTP/2

- The purpose of HTTP/2 is to improve HTTP performance by addressing latency issues that existed in the HTTP 1.1 version of the protocol.
- HTTP/2 uses the same header format as HTTP 1.1 and uses the same status codes.
- Few important features of HTTP/2 that a cybersecurity analyst must be aware of:
  - Multiplexing
  - Server PUSH
  - A binary protocol
  - Header compression



جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

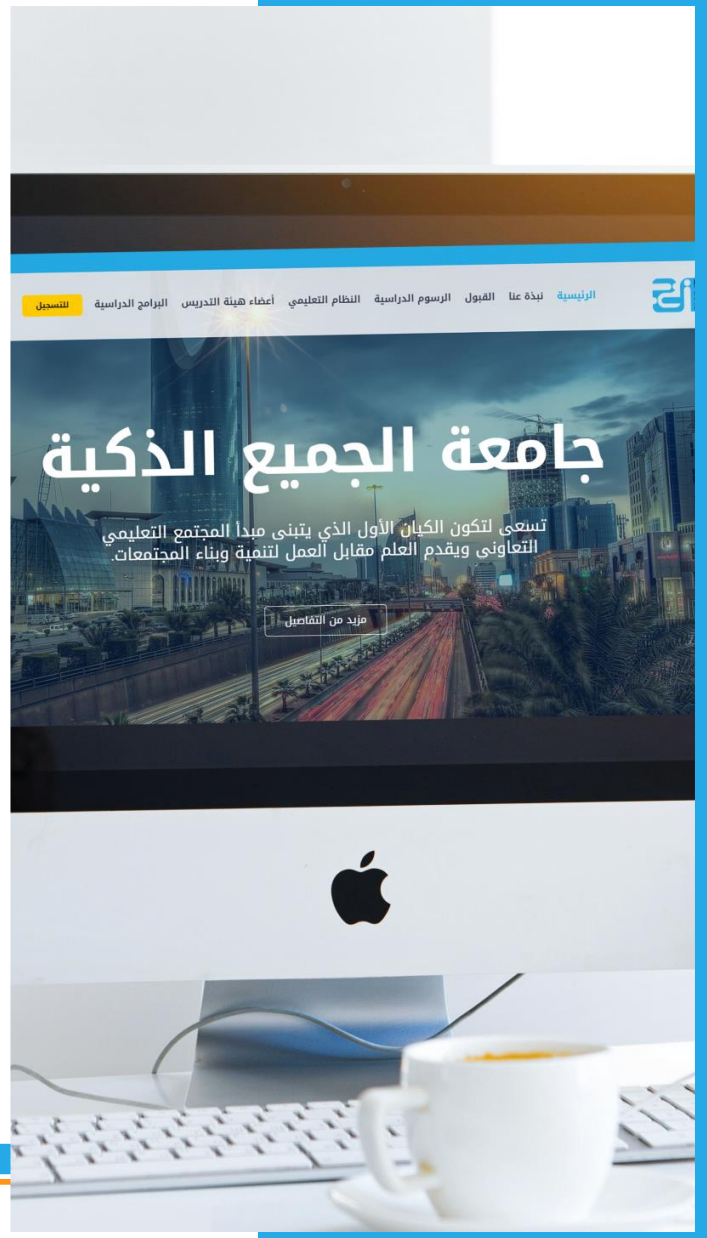
Securing HTTP – HTTPS

- For secure communication across the internet, the HTTP Secure (HTTPS) protocol is used.
- HTTPS uses authentication and encryption to secure data as it travels between the client and the server.
- HTTPS uses the same client request-server response process as HTTP, but the data stream is encrypted with Secure Socket Layer (SSL), or Transport Layer Security (TLS), before being transported across the network.
- HTTPS/2 is specified to use HTTPS over TLS with the Application-Layer Protocol Negotiation (ALPN) extension for TLS 1.2 or newer.
- Confidential information is transmitted over the Internet using HTTPS.

Lecture – 3
Activity 2

Using Wireshark to Examine HTTP and HTTPS Traffic

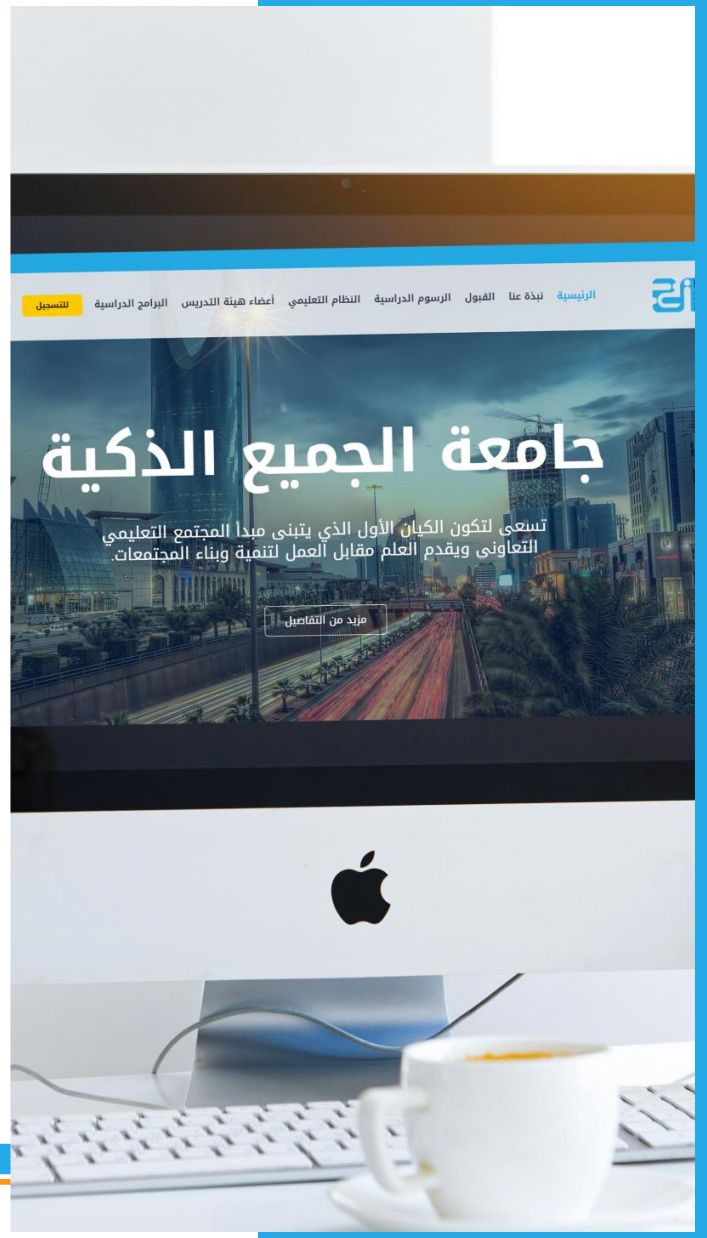
- In this lab, you will complete the following objectives:
  - Capture and view HTTP traffic
  - Capture and view HTTPS traffic



جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY

Network protocols and services analysis

Thanks



جامعة الجميع الذكية
EVERYONE`S SMART UNIVERSITY