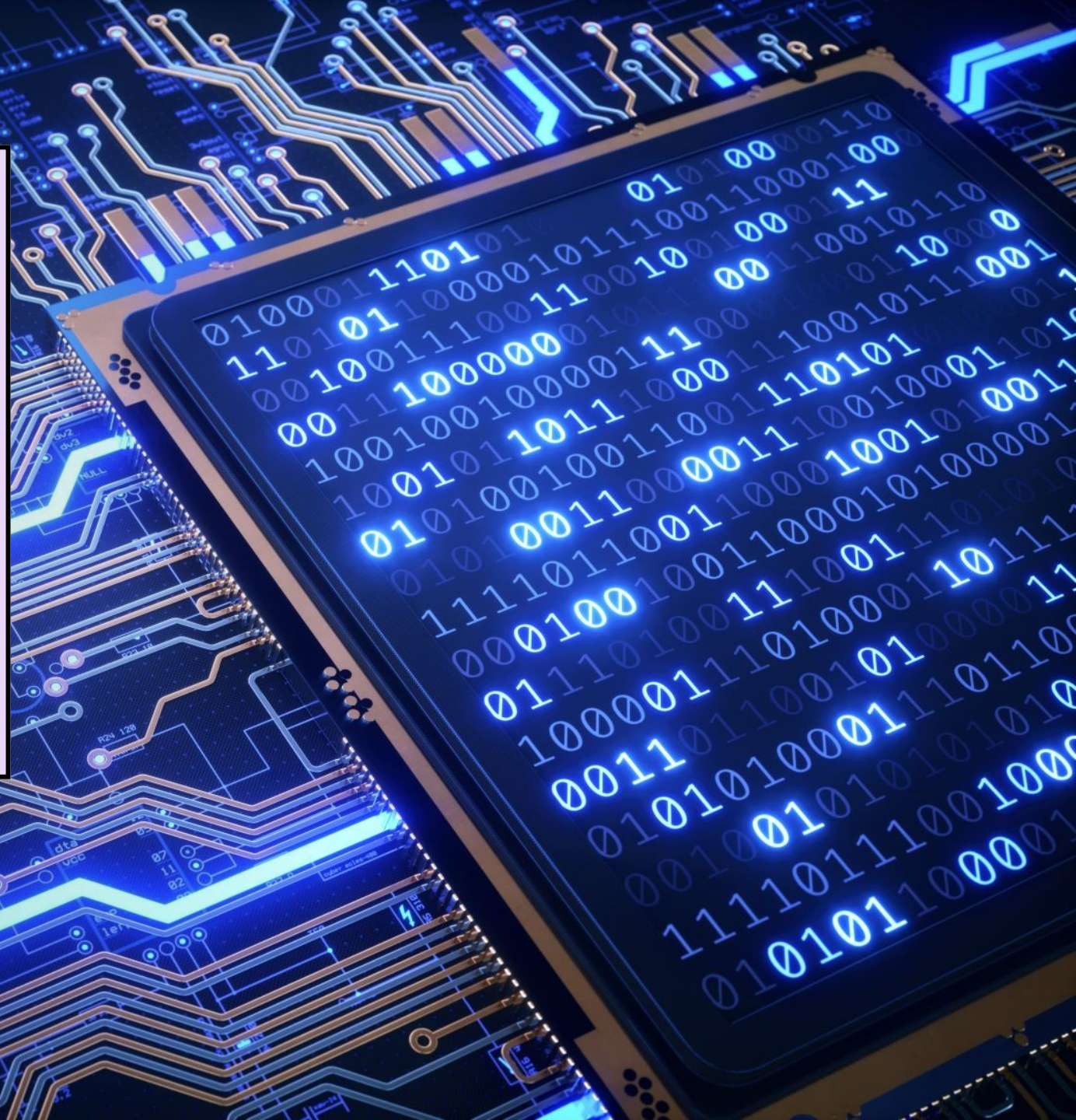


COMPUTER NETWORKS

APPLICATION LAYER



○ Topic of the day

- IP Addressing Protocols
 - Domain Name System - DNS
- Network Management Protocol
 - Dynamic Host Configuration Protocol - DHCP
- MIME Quiz



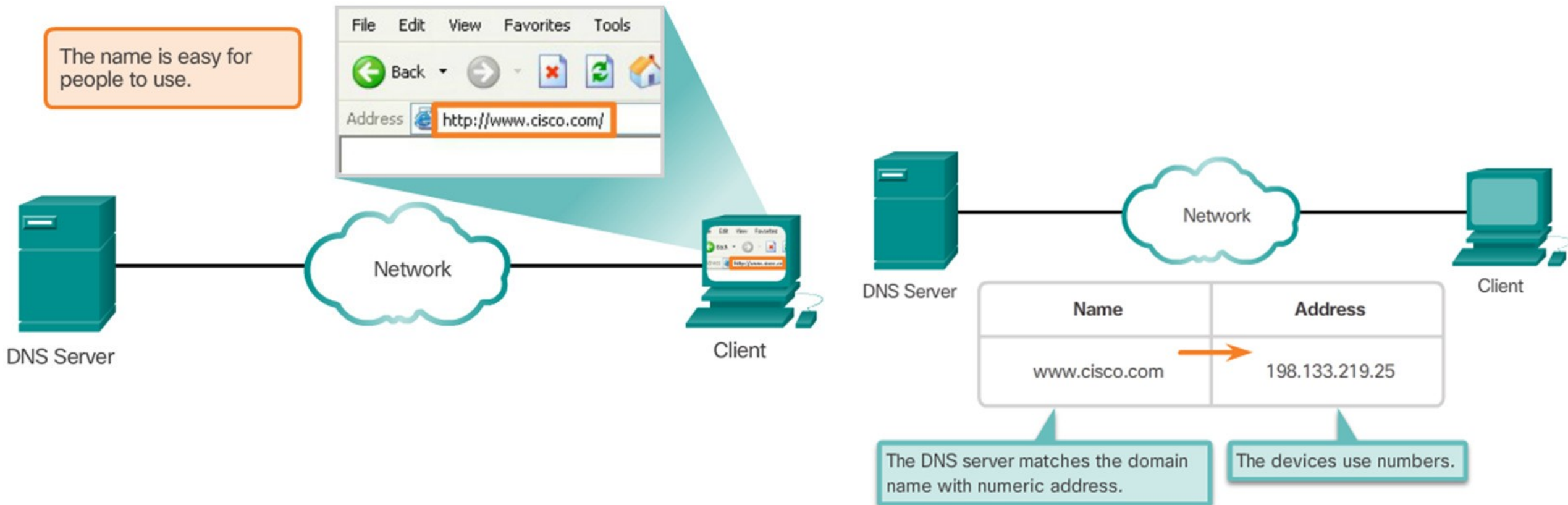
○ IP Addressing Protocols - DNS

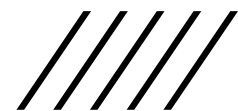
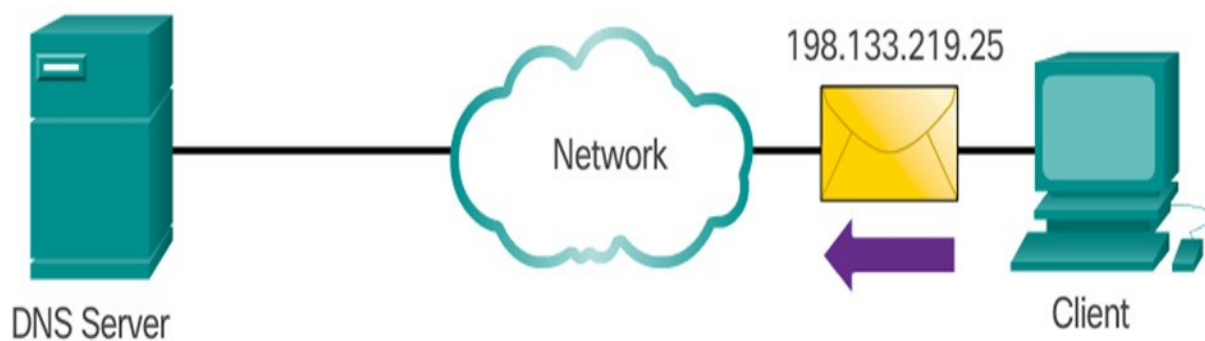
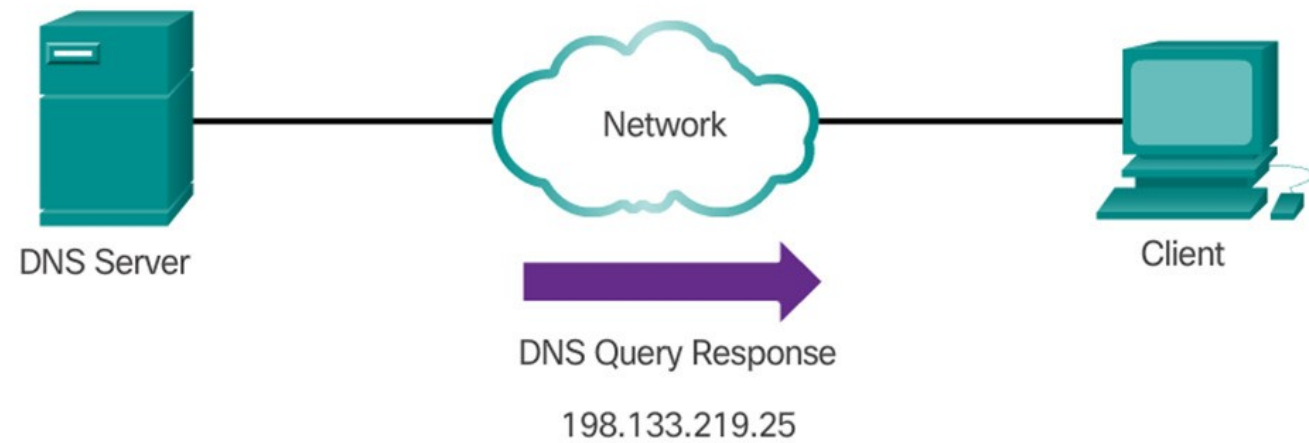
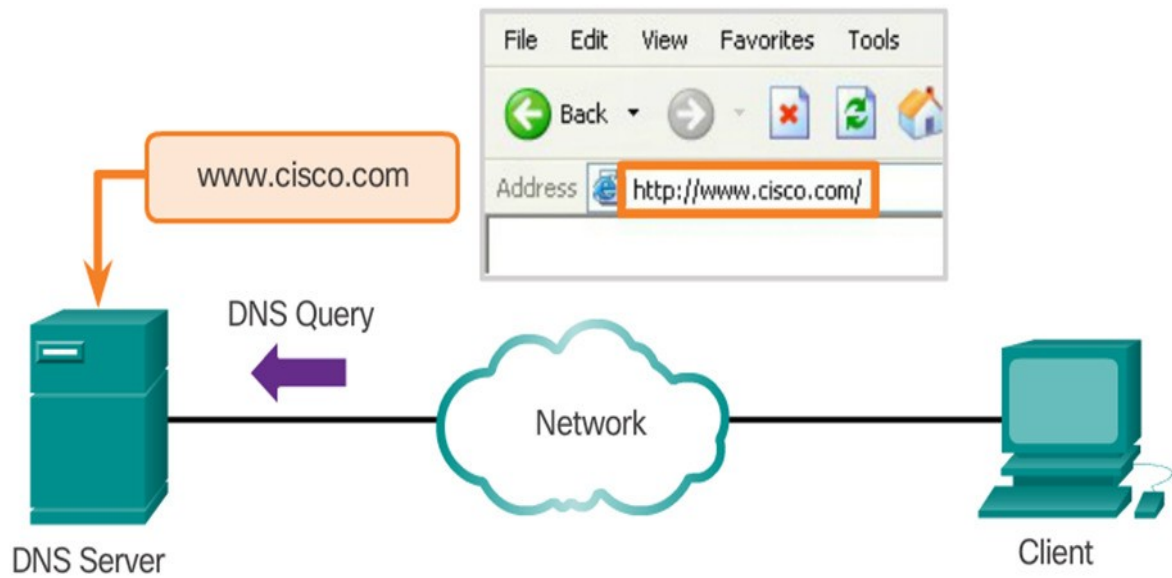
- Domain Name System
- While IP addresses are crucial for network communication, they are not easy to memorize.
- Domain names are created to make server addresses more user-friendly.
- Domain names such as <http://www.cisco.com> are user-friendly addresses associated with the IP address of a specific server.
- However, computers still need the actual numeric address before they can communicate.



Domain Name System

- The DNS protocol allows for the dynamic translation of a domain name into the correct IP address.
- The DNS protocol communications using a single format called a message.





○ DNS Message Format

- DNS supports different types of records. Some of these record types are:
 - **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
- DNS servers will first look at its own records to resolve the name. If the server is unable to resolve the name using its locally stored records, it relays the query to other servers.
- The response is then forwarded to the requesting client.
- The DNS Client service on Windows PCs also stores previously resolved names in memory.
- **ipconfig /displaydns** displays all of the cached DNS entries on



DNS uses the same message format for:

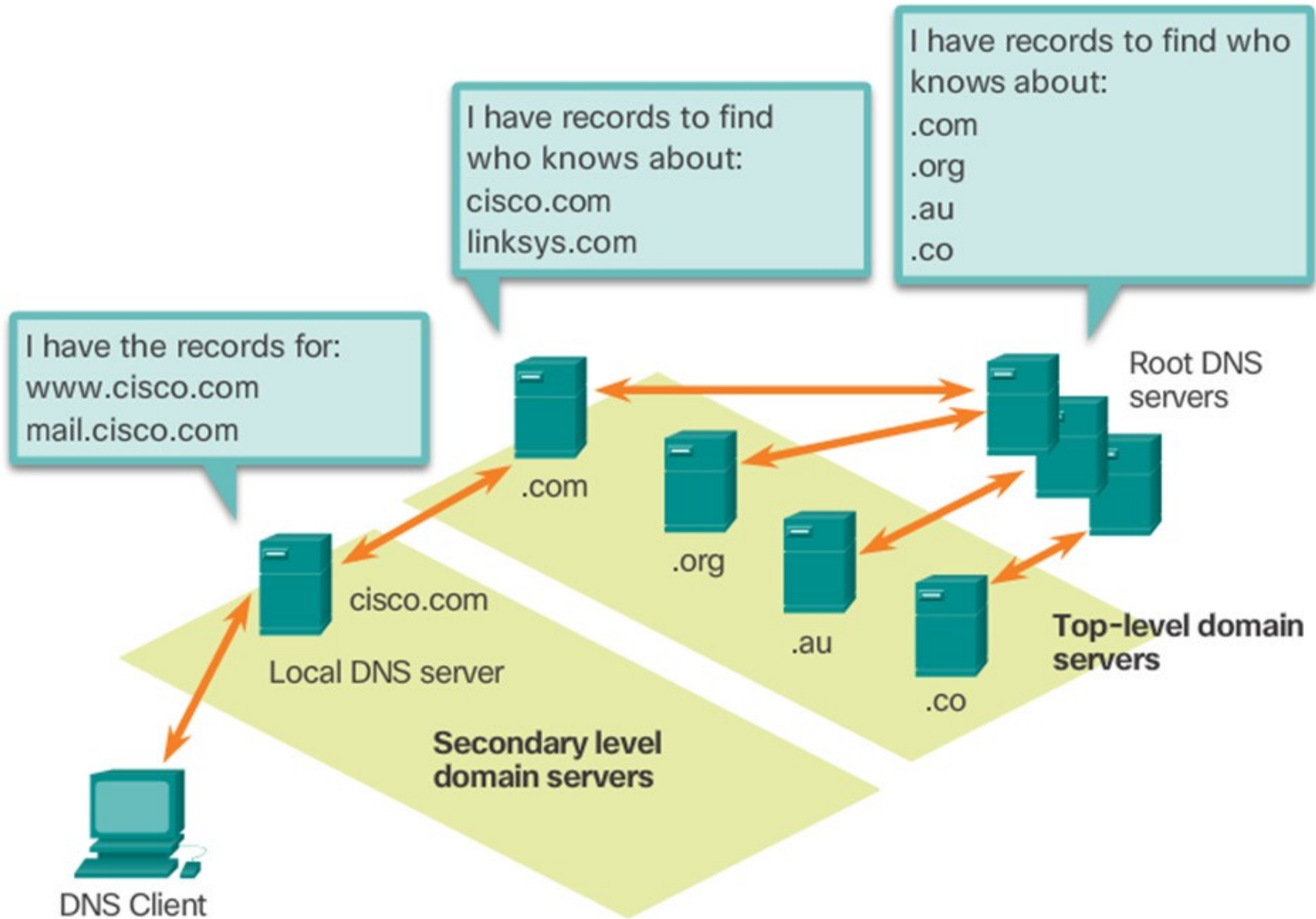
- all types of client queries and server responses
- error messages
- the transfer of resource record information between servers

Header	
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

○ DNS Hierarchy

- The DNS protocol uses a hierarchical system, with the root at the top and branches below. The naming structure is broken down into small, manageable zones.
- Each DNS server is only responsible for managing name-to-IP mappings for that small portion of the DNS structure.
- Requests for zones not stored in a specific DNS server are forwarded to other servers for translation.
- Top-level domains represent either the type of domain or the country of origin.
- Examples of top-level domains are:
 - o **.com** - a business or industry
 - o **.org** - a non-profit organization
 - o **.au** - Australia
 - o **.co** - Colombia





● Nslookup Command

- Allows the user to manually place DNS queries.
- It can also be used to troubleshoot name resolution issues.
- Has many options available for extensive testing and verification of the DNS process.
- DDNS: Dynamic Domain Name System
- DNS Caching

Command Prompt - nslookup

```
Microsoft Windows [Version 10.0.19041.508]  
(c) 2020 Microsoft Corporation. All rights reserved.
```


```
C:\Users\DELL>nslookup  
Default Server:  csp3.zte.com.cn.home  
Address:  192.168.10.1
```

```
> flex.nu.edu.pk  
Server:  csp3.zte.com.cn.home  
Address:  192.168.10.1
```

```
Non-authoritative answer:  
Name:      flex.nu.edu.pk  
Address:  210.56.9.83
```

```
> slate.nu.edu.pk  
Server:  csp3.zte.com.cn.home  
Address:  192.168.10.1
```

```
Non-authoritative answer:  
Name:      slate.nu.edu.pk  
Address:  210.56.27.170
```



```
C:\Users\DELL>nslookup -type=a www.gmail.com
Server:  www.huaweimobilewifi.com
Address: 192.168.8.1
```

```
DNS request timed out.
    timeout was 2 seconds.
```

```
Non-authoritative answer:
```

```
Name:     www.gmail.com
Address:   172.217.19.5
```

```
C:\Users\DELL>nslookup -type=mx www.gmail.com
Server:  www.huaweimobilewifi.com
Address: 192.168.8.1
```


```
DNS request timed out.
    timeout was 2 seconds.
```

```
Non-authoritative answer:
```

```
www.gmail.com  canonical name = mail.google.com
mail.google.com canonical name = googlemail.l.google.com
```

```
l.google.com
```

```
    primary name server = ns1.google.com
    responsible mail addr = dns-admin.google.com
    serial  = 333996677
    refresh = 900 (15 mins)
    retry   = 900 (15 mins)
    expire  = 1800 (30 mins)
    default TTL = 60 (1 min)
```



○ DNS Security Issues

- Major attacks:
- DNS Hijacking
- Cache Poisoning/ DNS Spoofing
- DNS DOS attack

- DNS SEC



○ Additional Topics

- Types of DNS
 - Iterative DNS
 - Reverse DNS
 - Recursive DNS



```
C:\Users\DELL>tracert www.gmail.com
```

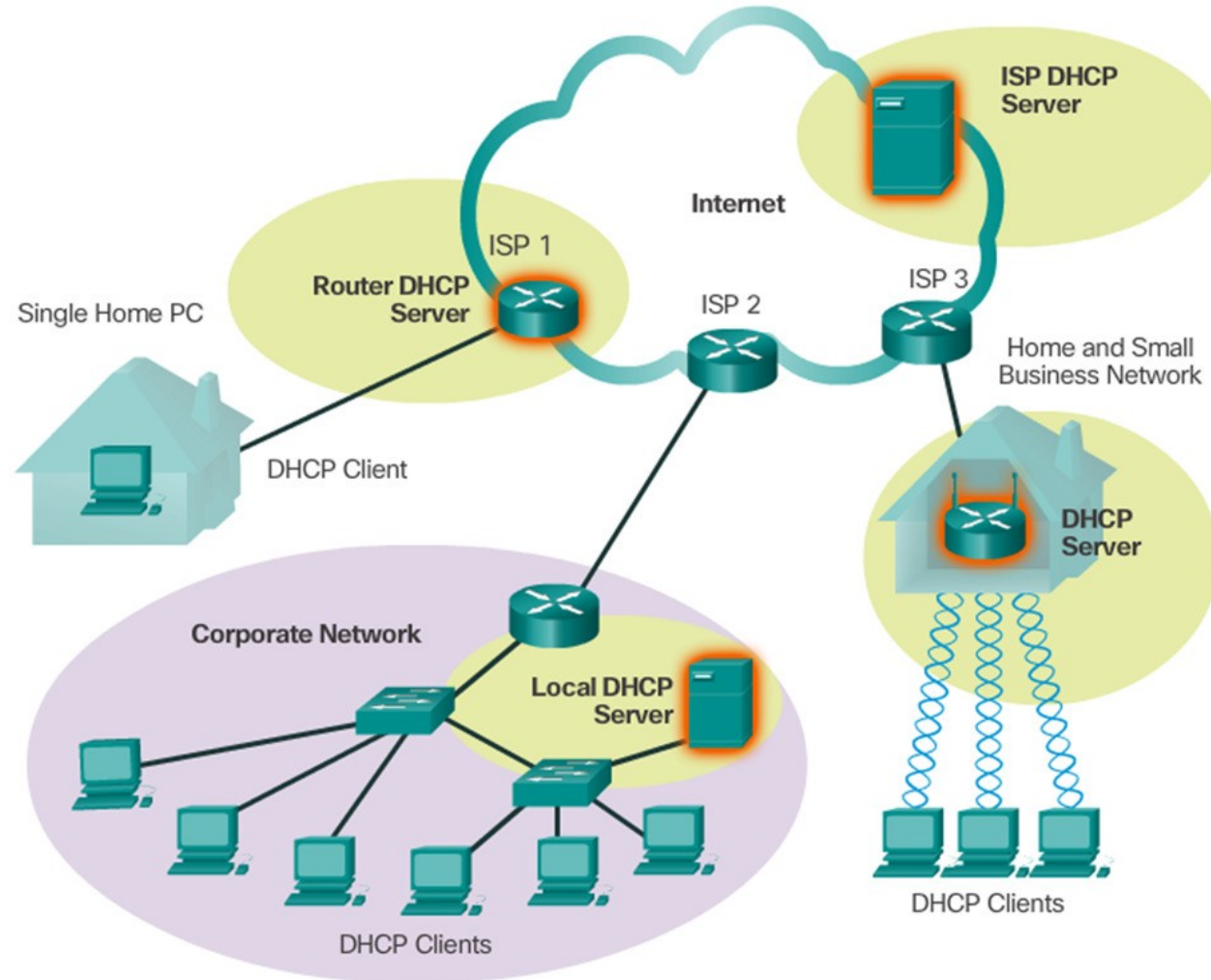
```
Tracing route to googlemail.l.google.com [172.217.19.165]  
over a maximum of 30 hops:
```

1	12 ms	17 ms	17 ms	www.huaweimobilewifi.com [192.168.8.1]
2	*	*	*	Request timed out.
3	48 ms	87 ms	57 ms	10.81.84.161
4	67 ms	67 ms	67 ms	10.81.195.198
5	82 ms	76 ms	87 ms	10.81.91.21
6	83 ms	57 ms	56 ms	59.103.253.25
7	77 ms	56 ms	96 ms	10.253.12.42
8	812 ms	267 ms	77 ms	10.253.4.38
9	106 ms	108 ms	98 ms	172.253.51.205
10	99 ms	97 ms	*	209.85.250.17
11	500 ms	557 ms	373 ms	zrh04s07-in-f5.1e100.net [172.217.19.165]

```
Trace complete.
```

Dynamic Host Configuration Protocol

- Computers need network addresses to communicate over a network.
- Additional crucial information includes gateway address, subnet mask, and DNS server.
- Manually configuring end devices is not scalable. DHCP allows for automated distribution of network information.
- DHCP-distributed addresses are leased for a set period of time.
- Addresses are returned to the pool for reuse when no longer in use.
- DHCP supports IPv4 and DHCPv6 supports IPv6.



/////



- DHCP (Dynamic Host Configuration Protocol)
- Network management protocol
- Used to dynamically assign an Internet Protocol ([IP](#)) address.
- Allocates TCP/IP configuration information to DHCP clients.
- DHCP automates and centrally manages these configurations assigning IP addresses to all network devices.
- DHCP can be implemented on small local networks, as well as large enterprise networks.
- Versions of DHCP are available for use in IP version 4 ([IPv4](#)) and IP version 6 ([IPv6](#)).



Configuration information includes

Subnet mask information,
Default gateway IP addresses and
Domain name system (DNS) addresses.



DHCP is a client-server protocol



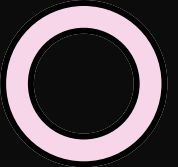
Servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.



DHCP-enabled clients send a request to the DHCP server whenever they connect to a network.



Ethernet adapter Ethernet 2:



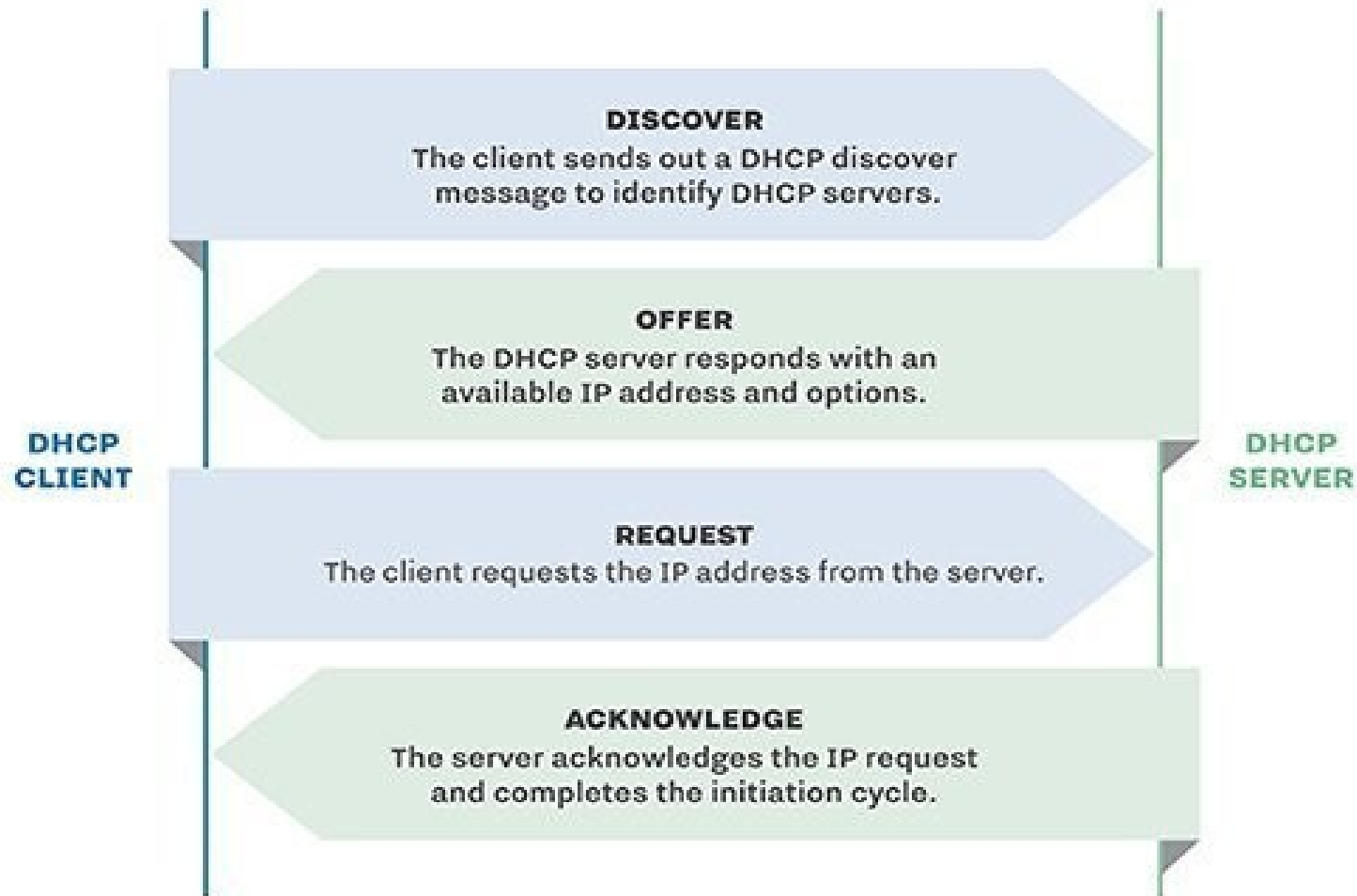
Connection-specific DNS Suffix . :
Description : Remote NDIS based Internet Sharing De
Physical Address. : 00-1E-10-1F-00-00
DHCP Enabled. : Yes
Autoconfiguration Enabled : Yes
Link-local IPv6 Address : fe80::a433:8533:2d88:524c%9(Preferred
IPv4 Address. : 192.168.8.100(Preferred)
Subnet Mask : 255.255.255.0
Lease Obtained. : Monday, September 28, 2020 9:31:07 PM
Lease Expires : Tuesday, September 29, 2020 9:31:07 P
Default Gateway : 192.168.8.1
DHCP Server : 192.168.8.1
DHCPv6 IAID : 704650768
IPv6 Client DUID. : 00-01-00-01-26-A4-A4-B0-A4-4C-C8-1B-D
DNS Servers : 192.168.8.1
 192.168.8.1
NetBIOS over Tcpip. : Enabled

○ Components

- DHCP is made up of numerous components, such as the
 - DHCP server,
 - client and
 - relay.
- The DHCP server:
 - typically either a server or router, is a networked device that runs on the DHCP service.
 - The DHCP server holds IP addresses, as well as related information pertaining to configuration.
- The DHCP client:
 - is a device -- such as a computer or phone -- that can connect to a network and communicate with a DHCP server.
- The DHCP relay:
 - will manage requests between DHCP clients and servers.
 - Typically, relays are used when an organization has to handle large or complex networks.
- Other components include the
 - IP address pool,
 - subnet,
 - lease and
 - DHCP communications protocol.



DHCP HANDSHAKE



DHCP Operation

- A DHCP client goes through the following basic steps to request an IP:
 - The client broadcasts a DHCPDISCOVER.
 - A DHCP server replies with a DHCPOFFER message
 - The client sends a DHCPREQUEST message to the server it wants to use (in case of multiple offers).
- A client may also choose to request an address that it had previously been allocated by the server.
- The server returns a DHCPACK message to confirm the lease has been finalized.



- The server would respond with a DHCPNAK if the offer is no longer valid
- Leases must be renewed before its expiration through another DHCPREQUEST.
- DHCPv6 has a similar set of messages:
 - o SOLICIT
 - o ADVERTISE
 - o INFORMATION REQ
 - o REPLY





Clients configured with DHCP **broadcast a request** to the DHCP server and request network configuration information for the local network to which they're attached.



Query broadcasted by client immediately after booting up.



The DHCP server responds to the client request by providing IP configuration information previously specified by a network administrator.



This includes a specific IP address, as well as a time period -- also called a **lease** -- for which the allocation is valid.



When refreshing an assignment, a DHCP client requests the same parameters, but the DHCP server may assign a new IP address based on policies set by administrators.

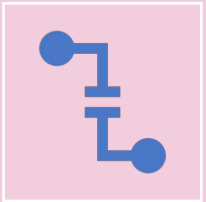


DHCP clients can also be configured on an Ethernet interface.

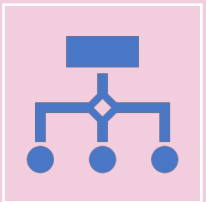




A DHCP server manages a record of all the IP addresses it allocates to network nodes.



If a node is relocated in the network, the server identifies it using its Media Access Control (MAC) address, which prevents the accidental configuration of multiple devices with the same IP address.



Configuring a DHCP server also requires the creation of a configuration file, which stores network information for clients.



- If network administrators want a DHCP server to provide addressing to multiple subnets on a given network, they must configure DHCP **relay** services located on interconnecting routers that DHCP requests have to cross.
- These agents relay messages between DHCP clients and servers located on different subnets.



○ DHCP Security

- DHCP is not a routable protocol, nor is it a secure one.
- DHCP lacks any built-in mechanism that would enable clients and servers to authenticate each other.
- Both are vulnerable to deception -- one computer pretending to be another -- and to attack, where rogue clients can exhaust a DHCP server's IP address pool.
- Man in the Middle Attack
- Memory Corruption Vulnerability





References

- [https://searchnetworking.techtarget.com/definition/DHCP#:~:text=DHCP%20runs%20at%20the%20application,name%20system%20\(DNS\)%20addresses](https://searchnetworking.techtarget.com/definition/DHCP#:~:text=DHCP%20runs%20at%20the%20application,name%20system%20(DNS)%20addresses)
- <https://ns1.com/resources/dns-types-records-servers-and-queries#:~:text=The%20most%20common%20DNS%20record,and%20its%20corresponding%20IPv6%20address>
- [DHCP CLI Commands](#)
- [CVE Database](#)

