

NETWORK MANAGEMENT AND ADMINISTRATION

Chapter 3

Network Connection and Printing Services

3.1 Dynamic Host Configuration Protocol (DHCP)

3.2 Introduction to Domain Name System (DNS)

3.3 Understand Network Printing Concepts

Study Notes for Engineering Students

Detailed notes | Diagrams | 15 MCQs with Answer Key | 10 Broad Questions

Contents

3.1 Dynamic Host Configuration Protocol (DHCP)	3
3.1.1 DHCP Origins	3
3.1.2 DHCP Objectives	5
3.1.3 IP Address Assignment	5
3.1.4 DHCP Architecture	8
3.2 Introduction to Domain Name System (DNS)	11
3.2.1 DNS Objectives	11
3.2.2 Domain Naming	11
3.2.3 Top Level Domains	12
3.2.4 Second Level Domains	13
3.2.5 Subdomains	13
3.2.6 DNS Functions	13
3.2.7 Resource Records	14
3.2.8 DNS Name Resolution	15
3.2.9 DNS Name Registration	17
3.3 Understand Network Printing Concepts	18
3.3.1 Network Printing Concepts	18
3.3.2 Locally Connected Print Devices	19
3.3.3 Setting up Local Print Devices	19
3.3.4 Shared Print Devices	20
3.3.5 Sharing Locally Attached Print Devices	21
3.3.6 Windows Network Printing	22
3.3.7 Add Printer Wizard	23
Multiple Choice Questions (15)	25
Answer Key - MCQs	27
Broad Questions (10)	28

3.1 Dynamic Host Configuration Protocol (DHCP)

Every device that communicates on a TCP/IP network must be configured with a few essential parameters before it can work: a unique **IP address**, a **subnet mask**, a **default gateway** and the address of a **DNS server**. In a small network these values can be typed in by hand (static configuration), but in a college, company or ISP network with hundreds or thousands of computers, manual configuration is slow, boring and very error-prone. A single typing mistake can create a duplicate IP address and bring down a computer. The **Dynamic Host Configuration Protocol (DHCP)** was created to solve this problem by automating the whole process.

DHCP is an application-layer, client-server protocol that automatically supplies IP addresses and other TCP/IP configuration information to hosts on a network. It works over UDP (server port 67, client port 68) and is defined in RFC 2131 and RFC 2132.

3.1.1 DHCP Origins

DHCP did not appear suddenly; it is the result of three generations of protocols, each trying to remove the limitations of the previous one. A computer that boots up knows only its own hardware (MAC) address, so early protocols were designed to let a machine ask the network, "Who am I and what is my IP address?"

Evolution of automatic configuration

Generation	Protocol	RFC / Year	Main idea
Manual	Static configuration	-	Administrator types IP, mask, gateway on each host.
1st	RARP	RFC 903 / 1984	Maps a MAC address to an IP address.
2nd	BOOTP	RFC 951 / 1985	Supplies IP address plus boot information; works across routers.
3rd	DHCP	RFC 1531 (1993), RFC 2131 (1997)	Dynamic allocation with leases; reuses addresses.

A. Reverse Address Resolution Protocol (RARP)

RARP is the opposite of ARP. ARP finds the MAC address when the IP address is known; RARP finds the **IP address when the MAC address is known**. It was designed for diskless workstations that had no disk to store an IP address and therefore had to learn it from the network at start-up.

Working of RARP

1. The diskless client boots and knows only its own MAC address.
2. It broadcasts a **RARP request** frame on the local network asking "My MAC address is X; what is my IP address?"
3. A **RARP server** that holds a table of MAC-to-IP mappings receives the request.
4. The server sends a **RARP reply** containing the IP address assigned to that MAC address.
5. The client configures itself with this IP address.

Limitations of RARP

- Works at the **data-link layer** (its own Ethernet type, 0x8035), so requests are not forwarded by routers; a RARP server is needed on **every physical network**.
- Supplies only the IP address - no subnet mask, default gateway or DNS server.
- Mapping table is entered **manually** by the administrator; no dynamic allocation.
- Wasteful: one fixed IP address is reserved for each MAC address even when the host is switched off.

B. The Bootstrap Protocol (BOOTP)

BOOTP (Bootstrap Protocol) improved on RARP. It runs on top of **UDP/IP** (server port 67, client port 68), so it works at the application layer and can pass through routers with the help of a **relay agent**. A BOOTP reply carries much more than an IP address: the subnet mask, default gateway, DNS server, the name of a **boot file** and the address of a TFTP server from which a diskless computer downloads its operating system.

BOOTP message field	Meaning
op	Message type: 1 = request (BOOTREQUEST), 2 = reply (BOOTREPLY).
htype / hlen	Hardware type (e.g. Ethernet) and hardware address length.
xid	Transaction ID used to match replies with requests.
ciaddr	Client IP address (filled only if the client already has one).
yiaddr	"Your" IP address - the address offered to the client.
siaddr	IP address of the server (e.g. the TFTP boot server).
giaddr	Gateway (relay agent) IP address used for forwarding across routers.
chaddr	Client hardware (MAC) address.
sname / file	Server host name and boot file name.
vend (options)	Vendor-specific information; subnet mask, gateway, DNS etc.

Limitation of BOOTP: addresses are allocated **statically**. The administrator must create an entry for every client in advance, and the address stays reserved forever, whether the computer is in use or not. BOOTP has no concept of a **lease**, so addresses cannot be reused. DHCP was developed as an extension of BOOTP and is backward compatible with it, so a BOOTP client can still talk to a DHCP server.

Comparison: RARP vs BOOTP vs DHCP

Feature	RARP	BOOTP	DHCP
Layer / transport	Data link layer	Application, UDP	Application, UDP
Information supplied	IP address only	IP, mask, gateway, boot file	IP, mask, gateway, DNS, lease and many options
Allocation	Static table	Static table	Dynamic, automatic or manual
Crosses routers	No	Yes (relay agent)	Yes (relay agent)
Address reuse (lease)	No	No	Yes
Server needed per network	Yes	No	No

3.1.2 DHCP Objectives

The design goals of DHCP, as stated in its specification, are given below.

- **Automatic configuration** - hosts obtain IP address, mask, gateway and DNS information without manual work.
- **Centralised management** - all settings are stored on a DHCP server, so a change (for example a new DNS server) is made in one place only.
- **Avoid duplicate addresses** - the server keeps a record of every address it has given out, so two hosts never receive the same IP address.
- **Efficient use of addresses** - addresses are leased for a limited time and returned to the pool when no longer needed, so a small pool can serve many computers (laptops, mobiles, visitors).
- **Support for mobile users** - a laptop moved to another subnet automatically receives a suitable address.
- **Reduce administrative effort and errors** in medium and large networks.
- **Scalability and reliability** - one server can serve many subnets using relay agents; two servers can be used for fault tolerance.
- **Backward compatibility** with BOOTP clients and relay agents.

3.1.3 IP Address Assignment

A DHCP server can hand out IP addresses in three different ways. A network administrator may use all three on the same network.

Method	Description	Typical use
Automatic allocation	The server assigns a permanent IP address to the client from the pool. The address is never returned.	Small stable network where hosts rarely change.
Dynamic allocation	The server leases an IP address for a limited period. The client must renew it; when the lease ends the address returns to the pool.	Most common; laptops, wireless users, large networks.

Method	Description	Typical use
Manual allocation (reservation)	The administrator ties a specific IP address to the MAC address of a device; DHCP only delivers it.	Servers, printers, routers that need a fixed address but central control.

Important DHCP terms

Term	Meaning
Scope	The complete range of IP addresses (with subnet mask) that the server can lease on one subnet.
Address pool	The addresses of the scope that remain available after exclusions are removed.
Exclusion range	Addresses inside the scope that the server must never lease (kept for static devices).
Reservation	A permanent mapping of one IP address to one MAC address.
Lease	The length of time a client may use an assigned IP address (Windows server default is 8 days).
DHCP options	Extra settings delivered with the address: 003 router, 006 DNS server, 015 domain name, 051 lease time.
Relay agent	Router or host that forwards DHCP broadcasts to a server on another subnet.

The DHCP lease process (DORA)

When a client starts, it does not yet have an IP address, so it uses the source address 0.0.0.0 and the broadcast address 255.255.255.255. The exchange consists of four messages, remembered by the word **DORA**: **D**iscover, **O**ffer, **R**quest, **A**cknowledge.

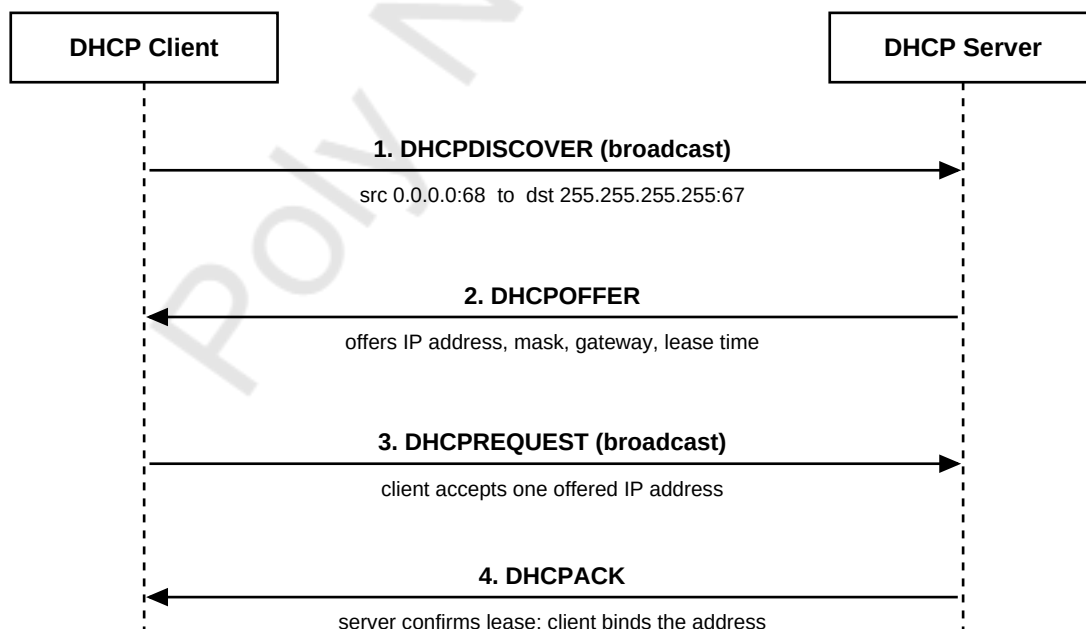


Fig. 3.1 DHCP lease process (Discover - Offer - Request - Acknowledge)

1. **DHCPDISCOVER** - the client broadcasts a message to find any available DHCP server.

2. **DHCPOFFER** - each server that has a free address replies with an offer (IP address, mask, lease time, server ID). The offered address is temporarily held for the client.
3. **DHCPREQUEST** - the client chooses one offer (normally the first received) and broadcasts a request for it. Because it is a broadcast, the other servers know their offers were rejected and release those addresses.
4. **DHCPACK** - the selected server confirms the lease and sends the complete configuration. The client binds the address and starts using it.

DHCP message types

Message	Sent by	Purpose
DHCPDISCOVER	Client	Locate DHCP servers (broadcast).
DHCPOFFER	Server	Offer an IP address and configuration to the client.
DHCPREQUEST	Client	Accept an offer, renew a lease, or confirm a previous address.
DHCPACK	Server	Confirm the lease and deliver the options.
DHCPNAK	Server	Refuse the request (address invalid or already used); client restarts the process.
DHCPDECLINE	Client	Tell the server the offered address is already in use on the network.
DHCPRELEASE	Client	Give the address back before the lease ends (e.g. on shutdown).
DHCPINFORM	Client	Ask for configuration options only; client already has an IP address.

Lease renewal and expiry

A lease is not permanent, so the client must renew it before it expires. Two timers control the process.

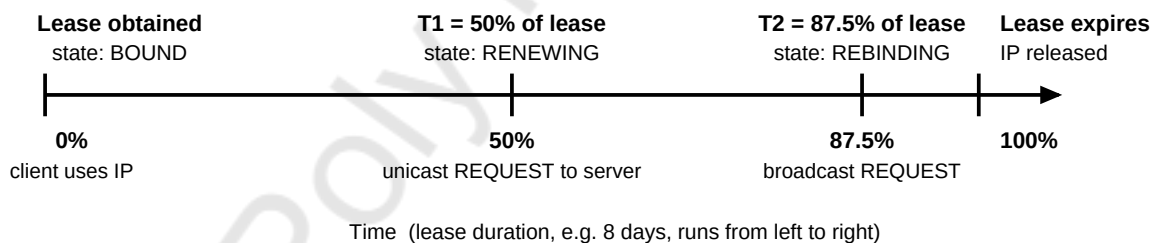


Fig. 3.2 DHCP lease timeline: renewal (T1) and rebinding (T2)

- At **T1 (50% of the lease time)** the client enters the RENEWING state and sends a unicast DHCPREQUEST to the server that gave the lease. If the server replies with DHCPACK, the lease starts again.
- If there is no reply, at **T2 (87.5% of the lease time)** the client enters the REBINDING state and broadcasts a DHCPREQUEST to any DHCP server.
- If no server answers before the lease expires, the client must stop using the address and restart with DHCPDISCOVER.

APIPA - when no DHCP server is found

If a Windows client cannot contact any DHCP server it assigns itself an address from the range **169.254.0.0/16** using **Automatic Private IP Addressing (APIPA)**. This allows communication with other APIPA hosts on the same local network only, and is a common sign that the DHCP server is unreachable.

Example DHCP scope configuration

Parameter	Example value
Scope name	Computer Lab
Address range	192.168.10.10 to 192.168.10.200
Subnet mask	255.255.255.0
Exclusion range	192.168.10.10 to 192.168.10.20 (servers, printers)
Reservation	192.168.10.50 reserved for MAC 00-1A-2B-3C-4D-5E (network printer)
Router (option 003)	192.168.10.1
DNS server (option 006)	192.168.10.2
Lease duration	8 days

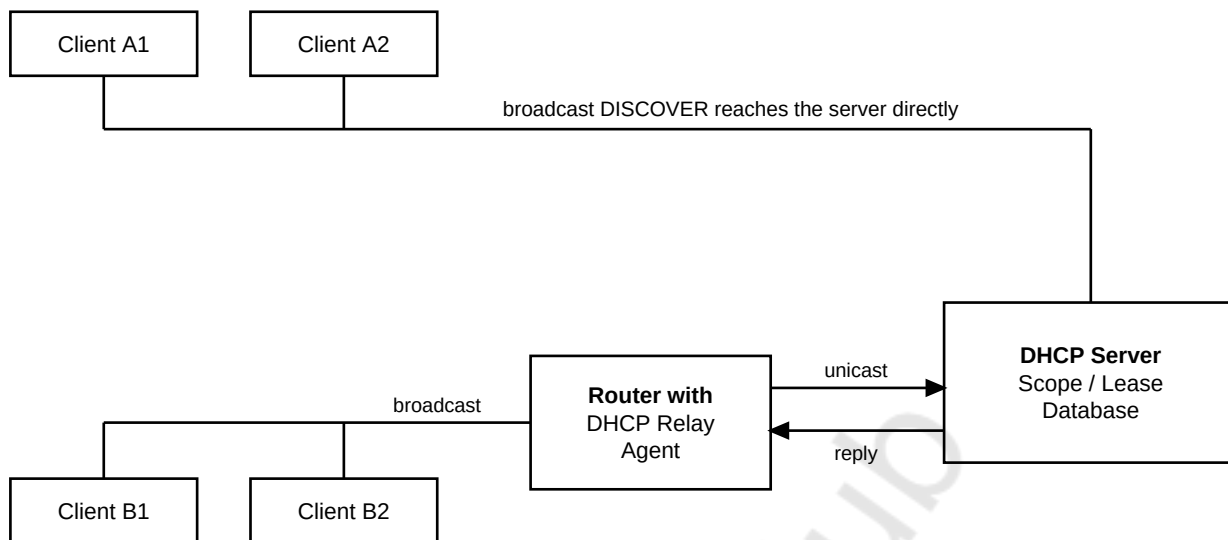
3.1.4 DHCP Architecture

DHCP follows the **client-server model**. The main components of the DHCP architecture are listed below.

Component	Role
DHCP client	Any host (computer, laptop, phone, printer) configured to "obtain an IP address automatically".
DHCP server	Computer or router running the DHCP service; stores scopes, options and the lease database and answers client requests.
DHCP relay agent	Forwards DHCP messages between clients and a server located on a different subnet, so one server can serve many subnets.
Scope / address pool	Range of IP addresses available for leasing on a subnet.
Lease database	Record of leased addresses, MAC addresses of clients, and lease expiry times.
DHCP options	Additional configuration parameters delivered with the IP address.

Because the first DHCPDISCOVER is a **broadcast**, and routers do not forward broadcasts, a DHCP server would normally be needed on every subnet. A **DHCP relay agent** (configured on the router as an "IP helper address") removes this need. The relay agent receives the broadcast, inserts its own interface address into the **giaddr** field, and forwards the message as a unicast packet to the DHCP server. The server uses giaddr to decide from which scope the address must be chosen, and sends the reply back to the relay agent, which then delivers it to the client.

Subnet A (same subnet as the DHCP server)



Subnet B (remote subnet - no DHCP server)

Fig. 3.3 DHCP architecture with a relay agent serving a remote subnet

Client states in the DHCP process

State	Meaning
INIT	Client has no address and starts the process by sending DHCPDISCOVER.
SELECTING	Client is waiting for offers and chooses one.
REQUESTING	Client has sent DHCPREQUEST and waits for DHCPACK.
BOUND	Lease confirmed; the client uses the IP address.
RENEWING	Timer T1 expired; client asks the original server to extend the lease.
REBINDING	Timer T2 expired; client asks any server to extend the lease.
INIT-REBOOT	Client restarts with a previously leased address and tries to confirm it.

Advantages and disadvantages of DHCP

Advantages	Disadvantages
Automatic, quick configuration; no typing errors.	If the DHCP server fails, new clients cannot get addresses (needs a backup server).
Central control of IP settings.	Addresses of devices can change, which is inconvenient for servers unless reservations are used.
Efficient reuse of limited IP addresses.	A rogue (unauthorised) DHCP server can give wrong settings and disturb the network.
Easy support for mobile and wireless users.	DHCP traffic is not authenticated by default, so it can be misused.

Useful DHCP commands on a Windows client

ipconfig /all	Show full IP configuration, DHCP server and lease times
ipconfig /release	Release the current DHCP lease
ipconfig /renew	Request a new / renewed lease from the DHCP server

In Windows Server networks, the DHCP server must be **authorised in Active Directory** before it can answer clients; this protects the network against rogue DHCP servers. For reliability, two servers can be configured with **DHCP failover** or a split scope (for example 80:20).

Key points - DHCP

- RARP: MAC to IP, data-link layer; BOOTP: UDP 67/68, static; DHCP: dynamic, lease based.
- DHCP uses UDP port 67 (server) and 68 (client).
- DORA = Discover, Offer, Request, Acknowledge. T1 = 50%, T2 = 87.5% of lease.
- Three allocation methods: automatic, dynamic, manual. APIPA range: 169.254.0.0/16.
- Relay agents let one DHCP server serve many subnets.

3.2 Introduction to Domain Name System (DNS)

Computers find each other using numeric IP addresses such as 142.250.183.4, but people find it easier to remember names such as *www.google.com*. The **Domain Name System (DNS)** is the distributed, hierarchical database and service that translates human-friendly domain names into IP addresses (and the reverse). It is often called the "phone book of the Internet".

In the early ARPANET days, every host name was listed in one file called **HOSTS.TXT**, maintained by SRI-NIC and downloaded by every site. As the network grew, this single file became too large, changed too fast and caused name conflicts. In 1983 **Paul Mockapetris** proposed DNS (RFC 882 and 883, later replaced by **RFC 1034 and RFC 1035**), which distributes the database across many servers worldwide. On a Windows or Linux computer the old idea still exists as the local *hosts* file, which is checked before DNS.

3.2.1 DNS Objectives

- **Name-to-address translation** - convert a domain name to an IP address (forward lookup) and an IP address to a name (reverse lookup).
- **Hierarchical naming** - a tree structure that avoids name conflicts and gives every host a unique name.
- **Distributed database** - no single server holds all names; responsibility is divided among many servers (delegation).
- **Decentralised administration** - each organisation manages its own part (zone) of the name space.
- **Scalability** - works for billions of names through caching and replication.
- **Reliability and fault tolerance** - every zone is served by at least two name servers.
- **Fast response** - caching of answers reduces delay and network traffic.
- **Support for other services** - mail routing (MX), service location (SRV), text data (TXT) and more.

3.2.2 Domain Naming

The DNS name space is organised as an **inverted tree**. The top of the tree is the **root**, written as a single dot. Each node in the tree is called a **label**; the full path from a node up to the root is its **domain name**. Labels are separated by dots and are read from **right (most general) to left (most specific)**.

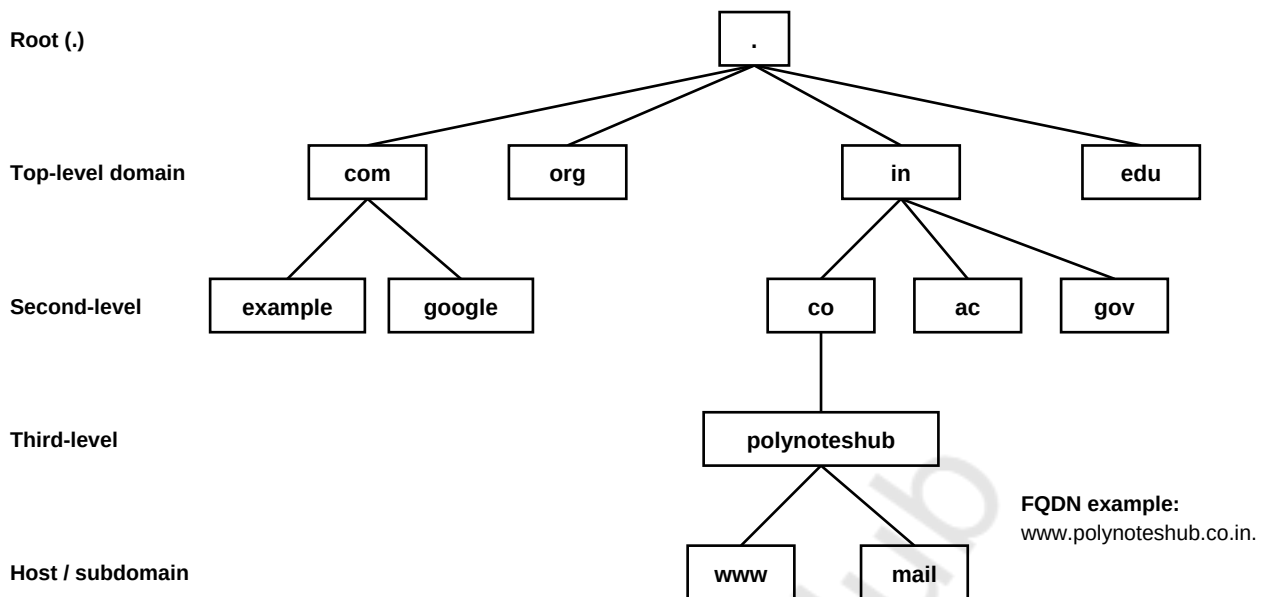


Fig. 3.4 The DNS domain name space (hierarchy)

Rules for domain names

- Each label may be at most **63 characters** long.
- A complete name (FQDN) may be at most 255 bytes in wire format (about 253 characters as text).
- Names are **not case sensitive**: *WWW.Example.COM* and *www.example.com* are the same.
- Allowed characters: letters (a-z), digits (0-9) and hyphen (-); a label cannot start or end with a hyphen.
- A **Fully Qualified Domain Name (FQDN)** gives the complete path to the root and ends with a dot, e.g. *www.example.com.*
- A **Partially Qualified Domain Name (PQDN)** is only a part of the name, such as *www*, and is completed by the resolver using a default suffix.

Domain and zone: A *domain* is a whole branch of the tree. A *zone* is the part of that branch that is administered by one set of name servers. A domain owner may delegate a sub-branch to another zone.

3.2.3 Top Level Domains

The labels immediately below the root are the **Top Level Domains (TLDs)**. They are managed under the supervision of ICANN/IANA. In the name *www.example.com* the TLD is **com**.

Type	Meaning	Examples
Generic TLD (gTLD)	Open or purpose-based domains	.com (commercial), .org (organisation), .net (network), .info
Restricted / sponsored	Limited to a particular group	.edu (US education), .gov (US government), .mil (US military), .int (treaty organisations)
Country code TLD (ccTLD)	Two-letter code for a country or territory	.in (India), .uk, .us, .jp, .au
New gTLDs	Introduced from 2012 onwards	.online, .app, .tech, .shop

Type	Meaning	Examples
Infrastructure TLD	Technical use only	.arpa (reverse DNS lookups)

3.2.4 Second Level Domains

A **Second Level Domain (SLD)** is the label directly to the left of the TLD. It is normally the name that an organisation or individual registers, for example **example** in *example.com* or **google** in *google.com*. The owner of a second level domain controls everything below it and may create any number of subdomains.

Many country code TLDs, including India, reserve second level labels for categories of users and the registrant registers a third level name under them.

Second level domain (India)	Used for	Example
co.in	Companies / commercial	example.co.in
ac.in	Academic institutions	college.ac.in
gov.in / nic.in	Government bodies	india.gov.in
org.in	Organisations	ngo.org.in
net.in	Network providers	isp.net.in
edu.in / res.in	Education and research	school.edu.in

3.2.5 Subdomains

A **subdomain** is a domain that is part of a larger domain. Any label placed to the left of a registered domain creates a subdomain. The owner of *example.com* can create *mail.example.com*, *www.example.com* or *cs.college.example.com* without asking any outside authority. Subdomains are used to divide a large organisation into departments, to separate services (web, mail, FTP), and to delegate administration.

Name	Level / part	Description
www.polynotesHub.co.in	Full name (FQDN)	Complete name of a host.
in	Top Level Domain	Country code of India.
co.in	Second Level Domain	Commercial category under .in.
polynotesHub.co.in	Registered domain	Name registered by the owner.
www	Host / subdomain	Name of the web server inside the domain.

3.2.6 DNS Functions

- **Forward lookup** - name to IP address (uses A and AAAA records).
- **Reverse lookup** - IP address to name, using PTR records in the special *in-addr.arpa* domain (IPv4) or *ip6.arpa* (IPv6).
- **Mail routing** - MX records tell mail servers which host receives mail for a domain.

- **Aliasing** - CNAME records give a second name to a host (e.g. *www* pointing to *web01*).
- **Load distribution** - several A records for one name allow round-robin sharing of traffic between servers.
- **Service location** - SRV records locate services such as Active Directory domain controllers.
- **Caching** - servers store answers for the time given by TTL to speed up later queries.
- **Zone transfer** - a secondary (slave) server copies the zone data from the primary (master) server for redundancy.

3.2.7 Resource Records

DNS data is stored on name servers in the form of **Resource Records (RRs)**. All records of a zone are kept in a **zone file**. Each resource record has the format: **Name, TTL, Class, Type, Data**. The class is almost always **IN** (Internet), and the TTL is the time in seconds for which the record may be cached.

Record	Name	Purpose	Example data
A	Address	Host name to IPv4 address	www IN A 203.0.113.10
AAAA	IPv6 address	Host name to IPv6 address	www IN AAAA 2001:db8::10
NS	Name server	Lists authoritative name servers of a zone	example.com. IN NS ns1.example.com.
CNAME	Canonical name	Alias for another name	ftp IN CNAME www
MX	Mail exchanger	Mail server with priority	example.com. IN MX 10 mail.example.com.
PTR	Pointer	IP address to name (reverse)	10.113.0.203.in-addr.arpa. IN PTR www.example.com.
SOA	Start of authority	Zone administration data (serial, refresh, retry, expire, minimum TTL)	One per zone
TXT	Text	Free text, used for SPF, domain verification	"v=spf1 mx -all"
SRV	Service	Host and port of a service	_ldap._tcp IN SRV 0 5 389 dc1

Sample zone file

\$TTL 86400	
example.com.	IN SOA ns1.example.com. admin.example.com. (
	2026102201 ; serial
	3600 ; refresh
	900 ; retry
	604800 ; expire
	86400) ; minimum TTL
example.com.	IN NS ns1.example.com.
example.com.	IN MX 10 mail.example.com.
ns1	IN A 203.0.113.2
www	IN A 203.0.113.10
ftp	IN CNAME www

3.2.8 DNS Name Resolution

Name resolution is the process of finding the IP address that belongs to a domain name. Several types of DNS servers and software take part in it.

Resolvers

A **resolver** is the client-side software (the *stub resolver* built into the operating system) that creates DNS queries on behalf of applications such as a web browser. The resolver first checks its own **local cache** and the **hosts file**; if the answer is not there it sends a query to its configured DNS server, which is usually a **recursive resolver** operated by the ISP or organisation (or a public one such as 8.8.8.8).

Types of name servers

Server type	Function
Authoritative server	Holds the original zone data and gives definite answers for its zone. Can be primary (master) or secondary (slave).
Recursive resolver	Receives queries from clients and does all the work of finding the answer, then caches it.
Caching-only server	Does not own any zone; only stores answers obtained from other servers.
Forwarder	Passes queries it cannot answer to another designated DNS server.
Root server	Top of the hierarchy; knows the servers of every TLD.

DNS requests

DNS clients and servers exchange simple **query and response messages**. They normally travel in **UDP packets on port 53**; **TCP port 53** is used for zone transfers and for responses too large for one UDP packet. A DNS message contains five sections: Header, Question, Answer, Authority and Additional.

Query type	Description
Recursive query	The client asks the server to return the final answer or an error. The server must do all the searching. Used between client and its resolver.
Iterative query	The server returns the best answer it has, usually a referral to another server that is closer to the answer. The asker continues the search. Used between a recursive resolver and other name servers.
Inverse / reverse query	Asks for the name that belongs to a given IP address (PTR lookup).

Root name servers

The **root name servers** are the starting point of every full DNS search. They do not know the final IP address of a website but they know which servers are responsible for each **top level domain**. There are **13 logical root servers** named **A to M** (a.root-servers.net to m.root-servers.net), operated by 12 independent organisations. Using **anycast** routing, each of the 13 addresses is actually served by many physical machines located worldwide, which gives high speed and strong protection against failure and attack. Every recursive resolver has a built-in **root hints** file listing the addresses of the root servers.

Resolving a domain name - step by step

Suppose a user types *www.example.com* in a browser and the recursive resolver has nothing in its cache.

Query: www.example.com ?

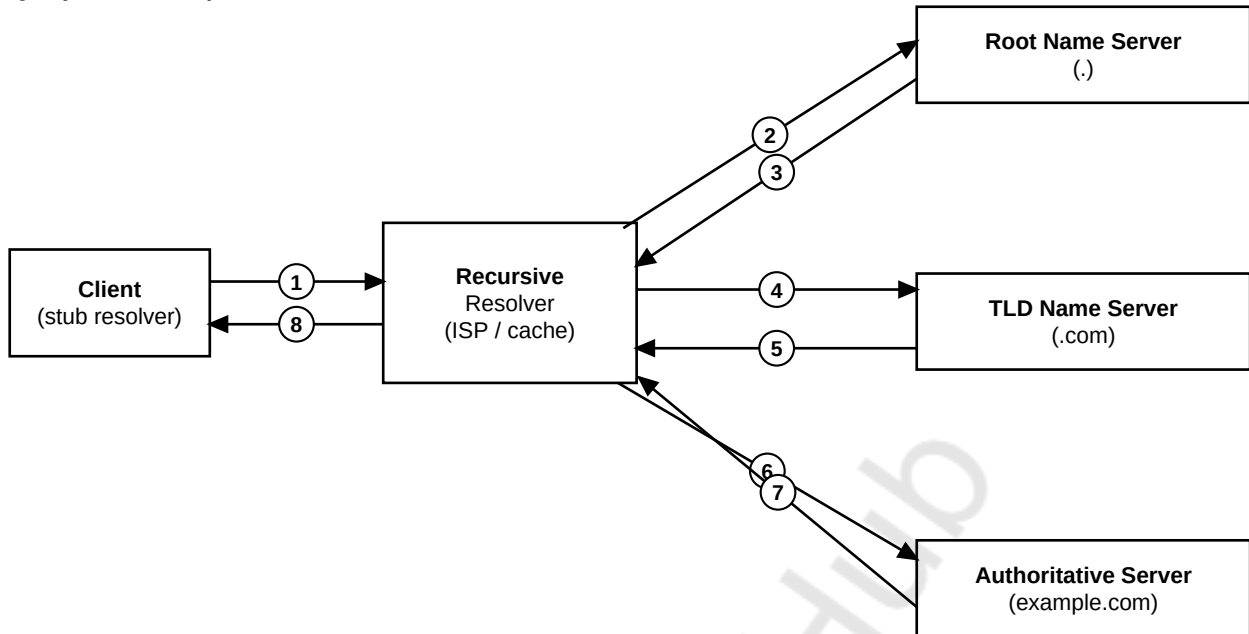


Fig. 3.5 Recursive resolver finding www.example.com using iterative queries

Step	Action
1	The client (stub resolver) sends a recursive query for www.example.com to its recursive resolver.
2	The resolver, finding no cached answer, sends an iterative query to a root server .
3	The root server replies with a referral: the addresses of the name servers for .com .
4	The resolver asks a .com TLD server for www.example.com.
5	The TLD server replies with a referral to the authoritative name servers of example.com .
6	The resolver asks the authoritative server of example.com.
7	The authoritative server returns the A record (the IP address) of www.example.com.
8	The resolver caches the answer for the TTL period and sends the IP address to the client, which connects to the website.

Because of **caching**, later requests for the same name (or for other names under .com) are answered much faster, often without contacting the root or TLD servers at all. The **TTL** in each record controls how long an answer is kept; the answer from a cache is called a *non-authoritative* answer. The command **nslookup** (or **dig**) can be used to test DNS.

```
C:\> nslookup www.example.com
Server:      dns.isp.local
Address:     192.168.10.2
Non-authoritative answer:
Name:        www.example.com
Address:     203.0.113.10
```

3.2.9 DNS Name Registration

A domain name cannot be used until it is **registered**. Registration gives the registrant the exclusive right to use a name for a fixed period (typically 1 to 10 years) which can be renewed. Names are unique across the whole Internet, so registration works on a first-come, first-served basis.

Organisations involved

Entity	Role
ICANN / IANA	Coordinates the DNS root zone, TLDs and global policy.
Registry	Organisation that manages a TLD and its master database (e.g. Verisign for .com; NIXI manages the .IN registry for India).
Registrar	Accredited company that sells domain names to the public and updates the registry.
Registrant	Person or organisation that registers and owns (leases) the domain name.

Steps in domain name registration

1. Choose a suitable name and TLD, and check its **availability** through a registrar (WHOIS search).
2. Select a registrar and fill in the **registrant details** (name, address, e-mail, phone) and the registration period.
3. Pay the registration fee. The registrar sends the request to the **registry**, which adds the name to the TLD zone.
4. Provide (or choose) the **name servers** that will host the zone. NS records are placed in the TLD zone.
5. Create resource records (A, MX, CNAME, etc.) in the zone. Changes spread across the Internet as caches expire (**propagation**).
6. Renew the registration before it expires; otherwise the name is suspended and later released for others.

Key points - DNS

- DNS is a distributed hierarchical database; names are read right to left (root, TLD, SLD, subdomain, host).
- Label maximum 63 characters; DNS uses port 53 (UDP for queries, TCP for zone transfer).
- Important records: A, AAAA, NS, CNAME, MX, PTR, SOA, TXT, SRV.
- Resolution: client - recursive resolver - root - TLD - authoritative server; answers are cached for the TTL.
- 13 logical root servers (A to M); reverse lookup uses in-addr.arpa.

3.3 Understand Network Printing Concepts

Printing is one of the most common shared services in an office or computer lab. Instead of buying one printer for every computer, an organisation connects a few good printers and lets many users share them over the network. This reduces cost, simplifies maintenance and gives the administrator central control over who can print and how much.

3.3.1 Network Printing Concepts

Windows uses its own printing vocabulary. It is very important to understand these terms because they are asked often in examinations.

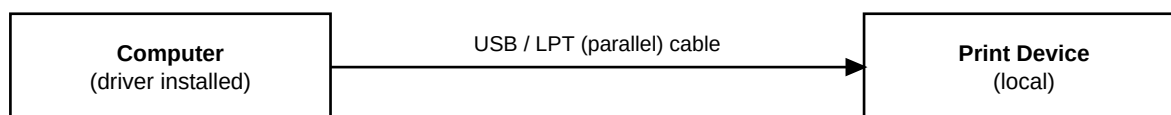
Term	Meaning
Print device	The physical hardware that produces the paper output (laser, inkjet, dot-matrix printer).
Printer	The software interface (logical printer) between the operating system and the print device; it is created by installing a driver and is shown in the Printers folder.
Print driver	Software that converts the document into the language the print device understands (PCL, PostScript).
Print server	A computer (or device) that hosts shared printers, manages print queues and sends jobs to print devices.
Print queue	List of documents (jobs) waiting to be printed on a printer.
Print spooler	Service that stores print jobs on disk (spooling) and sends them to the print device one by one.
Print job	A document that has been submitted for printing.
Port	The connection point used to reach the print device: LPT1, USB001, or a TCP/IP port.

Why spooling? A printer is much slower than a computer. With spooling, the application "prints" the document to a file on disk quickly and is free again, while the spooler sends the data to the printer in the background.

Types of print devices

Type	Description
Locally attached print device	Connected directly to a computer through a USB, parallel (LPT) or serial cable.
Network-attached print device	Has its own network interface card (wired or Wi-Fi) and IP address; connected directly to the network.

(a) Locally attached print device



(b) Shared / network printing

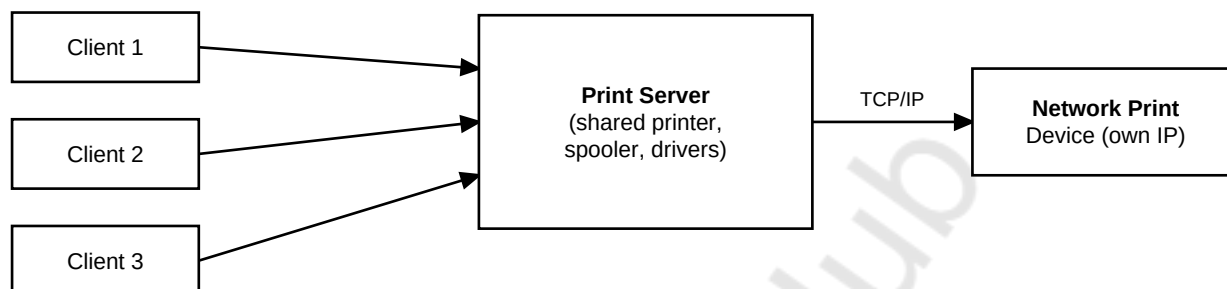


Fig. 3.6 (a) Locally attached printing and (b) shared network printing through a print server

3.3.2 Locally Connected Print Devices

A **locally connected print device** is attached to one computer by a cable. That computer owns the printer: the driver is installed on it and the print jobs are spooled on it. This is the simplest form of printing and is common in homes and small offices.

Common interfaces

Interface	Features
USB	Most common today; plug and play, hot-pluggable, fast.
Parallel (LPT1)	Old 25-pin interface; mainly for older printers.
Serial (COM)	Rarely used; slow.

Advantages and disadvantages

Advantages	Disadvantages
Simple and inexpensive to set up.	Only the connected computer can print unless the printer is shared.
No network configuration needed.	The host computer must be switched on for others to print.
Full control by the local user.	Difficult to manage when there are many printers.

3.3.3 Setting up Local Print Devices

Modern Windows detects most local printers automatically through **Plug and Play (PnP)**. The setup can also be done manually with the Add Printer Wizard.

Automatic installation

1. Connect the printer cable (USB) to the computer and connect the power cable.
2. Switch on the printer. Windows detects the new hardware.
3. Windows searches for a suitable **driver** (built-in, Windows Update or the manufacturer disc) and installs it.
4. The printer appears in **Devices and Printers**. Print a test page to confirm that it works.

Manual installation (when PnP does not detect the printer)

1. Open **Control Panel > Devices and Printers > Add a printer**.
2. Choose **Add a local printer**.
3. Select the **port** (for example LPT1 or USB001) or create a new port.
4. Select the **manufacturer and model** from the list, or use **Have Disk** to install the driver supplied by the manufacturer.
5. Type a **printer name** and choose whether to make it the **default printer**.
6. Choose whether to **share** the printer (and give it a share name).
7. Click **Print a test page** and then Finish.

3.3.4 Shared Print Devices

A **shared print device** is a printer that can be used by many users over the network. There are two common ways to share a printer.

- **Sharing a locally attached printer** - the printer is connected by USB to a computer, which then shares it.
- **Network-attached (TCP/IP) printer shared through a print server** - the print device has its own IP address; the print server connects to it with a Standard TCP/IP port and shares the logical printer to clients.

Common network printing protocols and ports

Protocol	Port	Description
RAW / HP JetDirect	TCP 9100	Sends data directly to the printer; the most widely used for TCP/IP printers.
LPR / LPD	TCP 515	Line Printer Remote / Daemon; used by UNIX and Linux systems.
IPP	TCP 631	Internet Printing Protocol; allows printing over the Internet using HTTP.
SMB	TCP 445	Used when a client prints to a Windows shared printer (\\server\printer).

Local printing vs. shared network printing

Feature	Local printer	Shared network printer
Connection	Cable to one computer	Over LAN through a print server or its own IP address
Number of users	One (unless shared)	Many users
Driver installation	On the local computer	On the print server; clients download it (Point and Print)
Management	Individual, at each computer	Central, from the print server
Cost for many users	High (many printers)	Low (one printer for many users)
Security / auditing	Limited	Permissions and auditing available

Benefits of a print server

- Central management of queues, drivers and settings.
- Automatic driver distribution to clients (**Point and Print**).
- Control of access using **permissions** and auditing of usage.
- Printer pools, priorities and scheduling for better use of devices.
- Publishing of printers in **Active Directory**, so users can search for them.

3.3.5 Sharing Locally Attached Print Devices

Once a printer is installed on a computer, it can be shared with other computers on the network. The sharing computer then acts as a small print server.

Steps to share a locally attached printer

1. Open **Devices and Printers**, right-click the printer and choose **Printer properties**.
2. Go to the **Sharing** tab and select **Share this printer**.
3. Enter a **share name** (keep it short and without spaces, e.g. LabPrinter1).
4. Tick **Render print jobs on client computers** to reduce load on the server (optional).
5. Click **Additional Drivers** and install drivers for other processor types (e.g. x86 and x64) so that every client can download a matching driver.
6. Use the **Security** tab to set **permissions** for users and groups.
7. Optionally tick **List in the directory** (on a domain) so that the printer can be found in Active Directory.

Connecting to the shared printer from a client

A client can connect by browsing the network, searching Active Directory, or typing the path of the shared printer in the form **\\ServerName\ShareName** (UNC path) in the Add Printer Wizard or in the Run box. The first time it connects, the driver is downloaded automatically from the print server.

Printer permissions

Permission	What the user can do
Print	Connect to the printer and send documents; pause, resume or delete own documents.
Manage documents	Control all print jobs of every user (pause, resume, restart, cancel) but cannot change printer settings.
Manage this printer	Change printer properties, share or unshare it, set permissions, delete the printer, and manage all jobs.
Special permissions	Fine-grained rights such as Read permissions and Change permissions.

By default, **Everyone** (or Users) has the *Print* permission, **Administrators** have all permissions, and **Creator Owner** has *Manage documents*.

3.3.6 Windows Network Printing

In Windows network printing, the clients, the print server and the print device cooperate to produce a printout. The flow of a document from the application to the paper is shown below.

Client computer

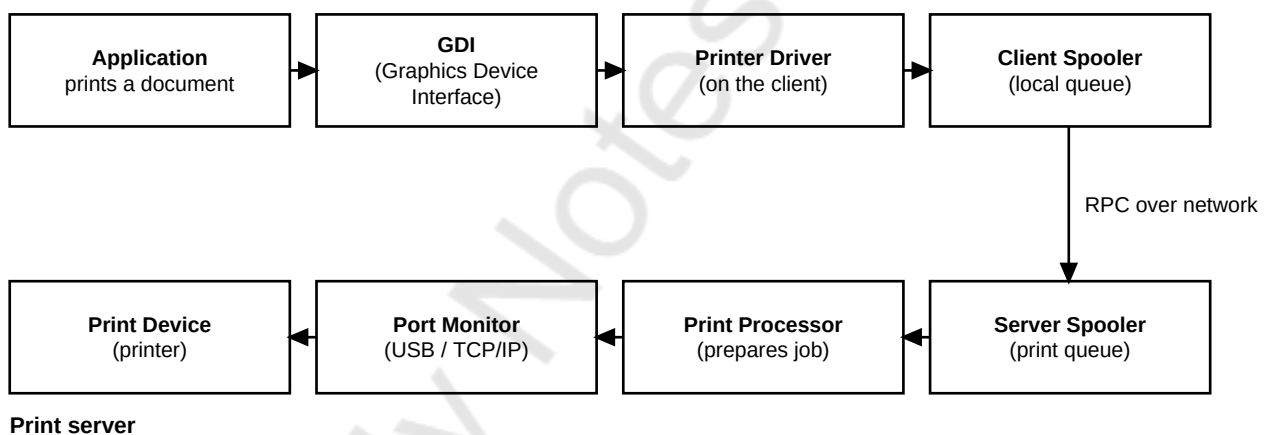


Fig. 3.7 Flow of a print job in Windows network printing

Component	Function
Print driver (GDI)	The application sends the document to the Graphics Device Interface, and the printer driver converts it into a form (print job) that the print device can understand.
Client spooler	Stores the job locally and passes it to the print server using Remote Procedure Call (RPC).
Print server spooler	Receives the job, stores it in the spool folder (%SystemRoot%\System32\spool\PRINTERS) and holds it in the print queue.
Print processor	Changes the job into the final format (e.g. RAW, EMF) required by the print device.
Port monitor	Controls the port (LPT, USB, TCP/IP) and delivers the data to the physical print device.

Component	Function
Print device	Prints the document; the job is then removed from the queue.

Other Windows printing features

- **Printer pooling** - one logical printer is connected to two or more identical print devices through multiple ports. The spooler sends each job to the first free device, which speeds up printing in busy offices.
- **Printer priorities** - two logical printers can point to the same print device with different priorities (1 to 99), so that important users (such as managers) are printed first.
- **Scheduling** - a printer can be made available only at certain hours (for example large jobs at night).
- **Print Management console** - lets the administrator view and manage all printers and drivers of many print servers from one place.
- **Group Policy / Active Directory** - deploys printers to users and computers automatically.

Troubleshooting tip

When the print queue is stuck, restart the **Print Spooler** service (services.msc, or the command **net stop spooler** followed by **net start spooler**) after clearing the files in the spool folder.

3.3.7 Add Printer Wizard

The **Add Printer Wizard** (Add a Printer) is a step-by-step tool in Windows that installs and configures a printer, whether it is local, shared on another computer, or connected directly to the network. It is started from **Control Panel > Devices and Printers > Add a printer** (or **Settings > Devices > Printers and scanners**).

Main options in the wizard

Wizard option	Used when
Add a local printer (manual settings)	The printer is attached by USB or LPT cable and was not detected automatically.
Select a shared printer by name	You know the UNC path (\\server\printer) or URL (http://server/printers/name/.printer) of a shared printer.
Add a printer using an IP address or hostname	The printer is a TCP/IP network printer; a Standard TCP/IP port is created automatically.
Add a Bluetooth, wireless or network discoverable printer	Windows searches the network and lists printers it finds.
The printer that I want is not listed	Opens the options above to find the printer manually.

Steps to add a network printer using the wizard

1. Start the **Add Printer Wizard**.
2. Choose **Add a network, wireless or Bluetooth printer** (or wait while Windows searches for printers).
3. If the printer is found, select it and click **Next**. If not, click **The printer that I want isn't listed**.

4. Choose the method: **shared printer by name, TCP/IP address or hostname**, or browse.
5. For a TCP/IP printer, enter the **device type, IP address or host name**, and the port name; Windows detects the printer model.
6. Install the **driver**: choose the manufacturer and model, or use **Windows Update** or **Have Disk**.
7. Type the **printer name**; choose whether to share it and to set it as the **default printer**.
8. Click **Print a test page** to verify, and then click **Finish**.

Key points - Network Printing

- Print device = physical hardware; Printer = logical software interface in Windows.
- Local printers use USB/LPT; network printers have their own IP and use ports such as TCP 9100 (RAW), 515 (LPR), 631 (IPP).
- To share a printer: Printer properties > Sharing tab > Share this printer; set permissions in the Security tab.
- Permissions: Print, Manage documents, Manage this printer.
- Print job flow: Application - GDI - Driver - Client spooler - Server spooler - Print processor - Port monitor - Print device.

Multiple Choice Questions (15)

Choose the correct option for each question. The answer key is given on the next page.

Q1. Which protocol allows a diskless workstation to find its IP address using its MAC address at the data-link layer?

- A) ARP B) RARP C) ICMP D) DNS

Q2. BOOTP and DHCP servers and clients use which pair of UDP ports?

- A) 20 and 21 B) 25 and 110 C) 53 and 53 D) 67 and 68

Q3. Which DHCP message is broadcast by a client to locate available DHCP servers?

- A) DHCPDISCOVER B) DHCPOFFER C) DHCPREQUEST D) DHCPACK

Q4. What is the correct order of the DHCP lease process?

- A) Offer, Discover, Request, Acknowledge B) Discover, Request, Offer, Acknowledge C) Discover, Offer, Request, Acknowledge D) Request, Discover, Offer, Acknowledge

Q5. A DHCP client starts renewing its lease when what fraction of the lease time has passed (timer T1)?

- A) 25% B) 75% C) 50% D) 87.5%

Q6. If no DHCP server is available, a Windows client self-assigns an address from which range (APIPA)?

- A) 169.254.0.0/16 B) 192.168.0.0/16 C) 172.16.0.0/12 D) 127.0.0.0/8

Q7. Which device or service forwards DHCP broadcasts to a DHCP server on another subnet?

- A) Repeater B) Hub C) DNS forwarder D) DHCP relay agent

Q8. What is the maximum length of a single label in a domain name?

- A) 32 characters B) 63 characters C) 127 characters D) 255 characters

Q9. In the domain name www.example.com, the top level domain is:

- A) com B) example C) www D) root

Q10. Which DNS resource record maps a host name to an IPv6 address?

- A) A B) MX C) PTR D) AAAA

Q11. How many logical root name servers exist in the DNS system?

- A) 8 B) 13 C) 26 D) 128

Q12. Which special domain is used for reverse DNS lookups of IPv4 addresses?

- A) ip6.arpa B) root-servers.net C) in-addr.arpa D) local.dns

Q13. In Windows printing terminology, the term "printer" refers to:

- A) The physical machine that prints B) The USB cable C) The print server hardware D) The software interface between the operating system and the print device

Q14. Which printer permission allows a user to change printer properties and share the printer?

- A) Manage this printer B) Print C) Manage documents D) Read

Q15. Which TCP port is commonly used for RAW (HP JetDirect) printing to a network print device?

- A) 80 B) 9100 C) 443 D) 21

Poly Notes Hub

Answer Key - MCQs

Q.	Ans.	Q.	Ans.	Q.	Ans.
1	B) RARP	6	A) 169.254.0.0/16	11	B) 13
2	D) 67 and 68	7	D) DHCP relay agent	12	C) in-addr.arpa
3	A) DHCPDISCOVER	8	B) 63 characters	13	D) The software interface between the operating system and the print device
4	C) Discover, Offer, Request, Acknowledge	9	A) com	14	A) Manage this printer
5	C) 50%	10	D) AAAA	15	B) 9100

Short explanations

1. RARP maps a MAC address to an IP address; ARP does the reverse.
2. BOOTP/DHCP use UDP port 67 for the server and 68 for the client.
3. DHCPDISCOVER is the first message, sent as a broadcast to find servers.
4. DORA: Discover, Offer, Request, Acknowledge.
5. T1 is 50% of the lease duration (T2 is 87.5%).
6. APIPA uses 169.254.0.0/16 when no DHCP server answers.
7. A relay agent forwards broadcasts as unicast to a remote DHCP server.
8. Each DNS label can be up to 63 characters.
9. The TLD is the right-most label (com).
10. AAAA record stores an IPv6 address; A stores IPv4.
11. There are 13 logical root servers, A to M.
12. IPv4 reverse lookup zones are under in-addr.arpa.
13. In Windows, the printer is the logical software; the print device is the hardware.
14. Manage this printer allows changing properties and sharing.
15. Port 9100 is used for RAW/JetDirect printing.

Broad Questions (10)

Answer the following questions in detail. Use neat diagrams and tables wherever necessary.

- Q1.** Explain the origin of DHCP. Describe RARP and BOOTP with their working and limitations, and compare RARP, BOOTP and DHCP.
- Q2.** What are the objectives of DHCP? Explain the three methods of IP address assignment used by a DHCP server.
- Q3.** Describe the DHCP lease process (DORA) with a neat diagram. Explain lease renewal using timers T1 and T2.
- Q4.** Explain the architecture of DHCP. Describe the role of the DHCP server, client, scope and relay agent with a diagram.
- Q5.** What is DNS? Explain the objectives of DNS and the hierarchical structure of the domain name space with a neat diagram.
- Q6.** Explain top level domains, second level domains and subdomains with suitable examples. List the rules for naming a domain.
- Q7.** What are resource records? Explain any six types of DNS resource records with their purpose and examples.
- Q8.** Explain the DNS name resolution process. Differentiate between recursive and iterative queries, and describe the role of root name servers with a diagram.
- Q9.** Explain the process of DNS name registration. Describe the roles of ICANN, registry, registrar and registrant.
- Q10.** Explain network printing concepts in Windows. Differentiate local and shared print devices, explain how a locally attached printer is shared, and describe the steps of the Add Printer Wizard.

- End of Chapter 3 -