

**GOVERNMENT POLYTECHNIC
AHMEDABAD
PROGRAM: DIPLOMA IN COMPUTER
ENGG**

**NETWORK MANAGEMENT AND
ADMINISTRATION(3360703)**

**UNIT-2
NETWORK PROTOCOLS AND SERVICE**



ARP

- Address resolution Protocol
- Mapping Logical to Physical Address
- If a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver.
- The logical (IP) address is obtained from the DNS.
- DNS :Domain Name System.
- But the IP datagram must be encapsulated in a frame to be able to pass through the physical network.
- This means that the sender needs the physical address of the receiver.



- The host or the router sends an **ARP query packet**.
- The packet includes the physical and IP addresses of the sender and the IP address of the receiver.
- Because the sender does not know the physical address of the receiver and the query is broadcast over the network.


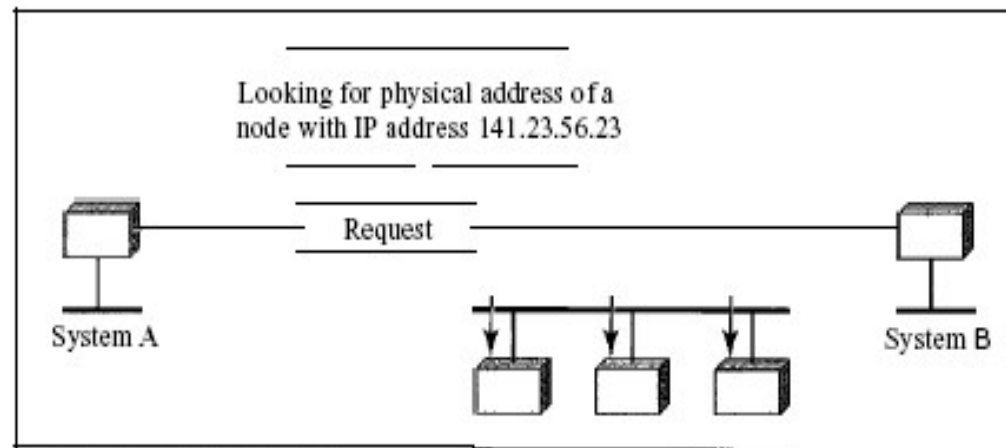
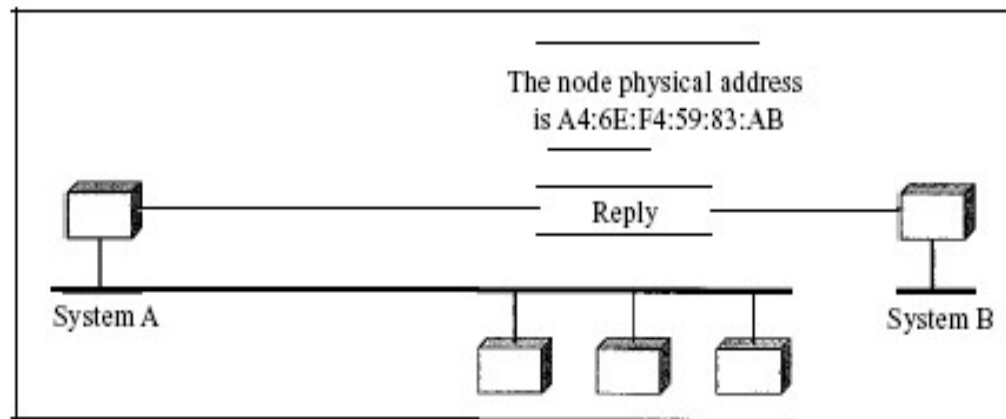
- 
- Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet.
 - The response packet contains the recipient's IP and physical addresses. The packet is unicast directly to the inquirer by using the physical address received in the query packet.

Figure 21.1 ARP operation



a. ARP request is broadcast




b. ARP reply is unicast



RARP


- Reverse Address Resolution Protocol
- (RARP) finds the logical address for a machine that knows only its physical address.
- A diskless machine is usually booted from ROM, which has minimum booting information. The ROM is installed by the manufacturer.
- It cannot include the IP address because the IP addresses on a network are assigned by the network administrator.

- 
- The machine can get its physical address (by reading its NIC, for example), which is unique locally. It can then use the physical address to get the logical address by using the RARP protocol.
 - A RARP request is created and broadcast on the local network.
 - Broadcasting is done at Data Link Layer.
 - Another machine on the local network that knows all the IP addresses will respond with a RARP reply.
 - The requesting machine must be running a RARP client program the responding machine must be running a RARP server program.
 - This is the reason that RARP is almost obsolete. Two protocols, BOOTP and DHCP, are replacing RARP.



BOOTP: Bootstrap Protocol

- The Bootstrap Protocol (BOOTP) is a client/server protocol designed to provide physical address to logical address mapping.
- BOOTP is an application layer protocol.
- BOOTP messages are encapsulated in a UDP packet, and the UDP packet itself is encapsulated in an IP packet.
- One of the advantages of BOOTP over RARP is that the client and server are application-layer processes.

- 
- The BOOTP request is broadcast because the client does not know the IP address of the server.
 - A broadcast IP datagram cannot pass through any router.
 - To solve the problem, there is a need for an intermediary. One of the hosts (or a router that can be configured to operate at the application layer) can be used as a relay.
 - The host in this case is called a relay agent.


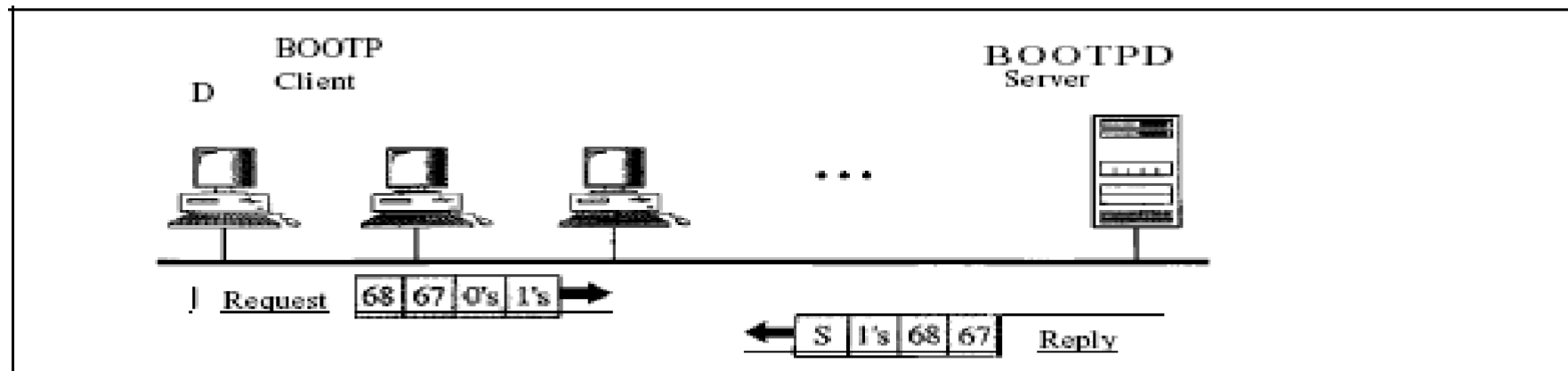
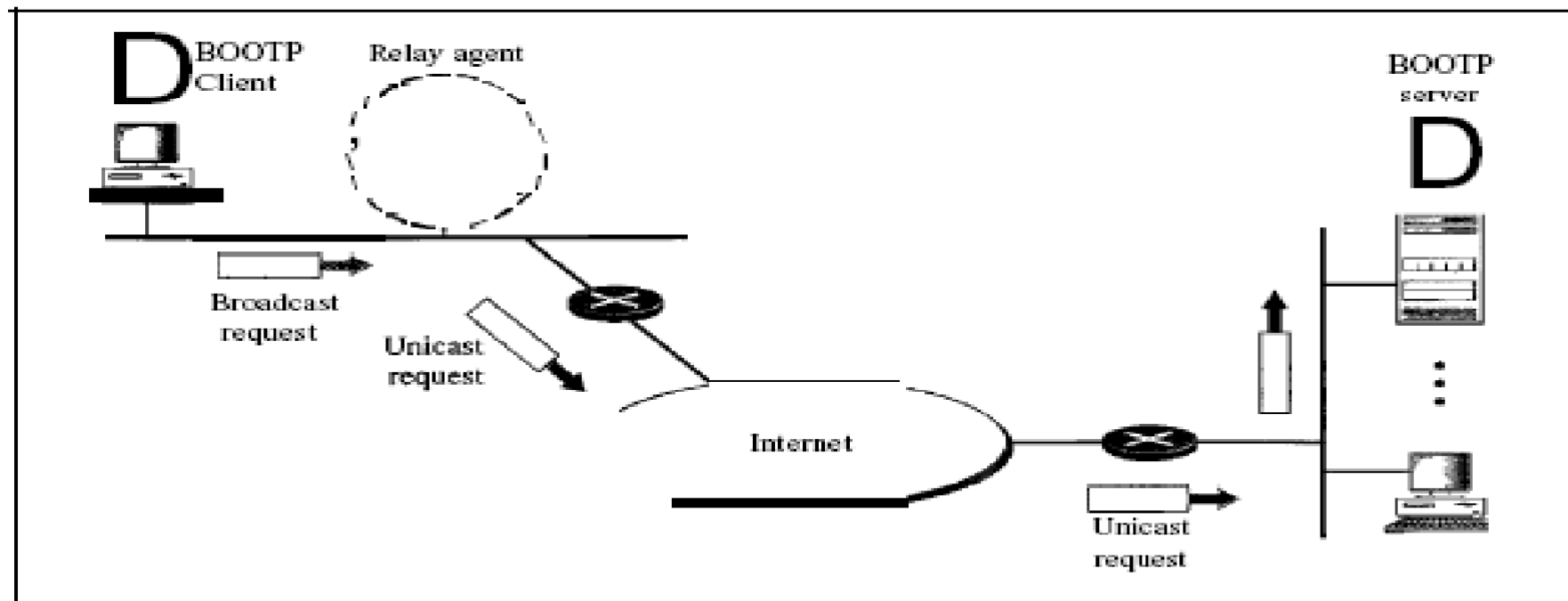
- 
- The relay agent knows the unicast address of a BOOTP server. When it receives this type of packet, it encapsulates the message in a unicast datagram and sends the request to the BOOTP server.
 - The packet, carrying a unicast destination address, is routed by any router and reaches the BOOTP server.

Figure 21.7 *BOOTP client and server on the same and different network*



a. Client and server on the same network



b. Client and server on different networks



- The BOOTP server knows the message comes from a relay agent because one of the fields in the request message defines the IP address of the relay agent.
- The relay agent, after receiving the reply, sends it to the BOOTP client.




DHCP: Dynamic Host Control Protocol


- 1) Introduction
- 2) DHCP origins
- 3) RARP
- 4) ARP
- 5) BOOTP
- 6) DHCP Objectives
- 7) IP address assignments
- 8) DHCP Architecture





Introduction to DHCP

- BOOTP is not a dynamic configuration protocol.
- DHCP was created by the Dynamic Host Configuration Working Group of the **Internet Engineering Task Force(IETF)**
- Runs over **UDP**
- Utilizing ports:
 - **67 – connections to server**
 - **68 – connections to client**
- DHCP is basically used for **dynamic configuration**
- Uses **client-server model**

- 
- When a client requests its IP address, the BOOTP server consults a table that matches the physical address of the client with its IP address.
 - The binding is predetermined.
 - The Dynamic Host Configuration Protocol (DHCP) has been devised to provide static and dynamic address allocation that can be manual or automatic

- 
- Static Address Allocation In this capacity DHCP acts as BOOTP does.
 - It is backward compatible with BOOTP, which means a host running the BOOTP client can request a static address from a DHCP server.
 - A DHCP server has a database that statically binds physical addresses to IP addresses.
 - Dynamic Address Allocation DHCP has a second database with a pool of available IP addresses. This second database makes DHCP dynamic.
 - When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available (unused) IP addresses and assigns an IP address for a negotiable period of time.

- 
- When a DHCP client sends a request to a DHCP server, the server first checks its static database. If an entry with the requested physical address exists in the static database, the permanent IP address of the client is returned.
 - On the other hand, if the entry does not exist in the static database, the server selects an IP address from the available pool, assigns the address to the client, and adds the entry to the dynamic database.
 - The dynamic aspect of DHCP is needed when a host moves from network to network or is connected and disconnected from a network (as is a subscriber to a service provider).

- 
- The addresses assigned from the pool are temporary addresses. The DHCP server issues a lease for a specific time. When the lease expires, the client must either stop using the IP address or renew the lease.
 - The server has the option to agree or disagree with the renewal. If server disagrees, the client stops using the address.



Objectives of DHCP

- The DHCP server should be able to provide a workstation for configuration.
- The DHCP server should prevent the duplication of addresses on the network.
- The DHCP server should be able to configure clients by use of relayagent.
- DHCP clients should be able to retain their TCP/IP parameters despite a reboot of either client or server system.



IP address Assignment

- **Manual allocation:** The administrator configures the DHCP server to assign a specific IP address to a given system, which will never change unless it is manually modified. This is equivalent in functionality to RARP and BOOTP.
- **Automatic allocation:** The DHCP server assigns permanent IP addresses from a pool, which does not change unless they are manually modified by the administrator.
- **Dynamic allocation:** The DHCP server assigns IP addresses from a pool using a limited-time lease, so the addresses can be reassigned if the client system does periodically renew it.



DHCP architecture


- Dynamic configuration protocol consists of two basic elements:
 - A service that assigns TCP/IP configuration settings to client system
 - A protocol used for communications between DHCP clients and server.
- The DHCP architecture defines the message format for the protocol and the sequence of message exchanges that take place between the DHCP client and server.




- The DHCP architecture defines the message format for the protocol and the sequence of message exchanges that take place between the DHCP client and server.

op(1)	htype(1)	hlen(1)	hops(1)
xid(4)			
secs(2)		flags(2)	
claddr(4)			
yladdr(4)			
siaddr(4)			
gladdr(4)			
chaddr(16)			
sname(64)			
file(128)			
option(variable)			


- **OP (Op code), 1 byte: specifies whether the message is request or reply, using the following code.**
 - 1. BOOTREQUEST
 - 2. BOOTREPLY
- **htype (Hardware type), 1 byte: Specifies the type of hardware used in the chaddr field. For ex 1 for Ethernet (10 MB)**
- **hlen (Hardware address length), 1 byte: Specifies the length of the hardware address found in the chaddr field, according to the value of the htype field (for ex if htype=1, indicating an Ethernet hardware address, the value of hlen will be 6 byte)**
- **hops (1 byte): Specifies the number of network segments between the client and server. The client sets the value to 0 and each DHCP relay system increments it by 1 during the journey to the server.**
- **Xid (Transaction Id), 4 bytes: Contains a transaction identifier that systems use to associate the request and response messages of a single DHCP transaction.**

- 
- **Secs (Seconds), 2 bytes:** Specifies the number of seconds elapsed since the IP address was assigned or the lease last renewed. This enables the systems to distinguish between messages of the same type generated during a single DHCP transaction.
 - **Flags (2 byte):** Contains the broadcast flag as the first bit, which, when set to a value of 1, specifies that DHCP servers and relay agents should use broadcasts to transmit to the client and not unicast. The remaining bits in the field are unused and must have a value zero.
 - **Ciaddr (client IP address), 4 bytes:** Specifies the client's IP address in DHCP REQUEST messages transmitted while in the bound, renewal or rebinding state. At all other times the value must be zero.
 - **Siaddr (Server IP address), 4 bytes:** Specifies the IP address of the next server in a bootstrap sequence. Servers include this information in DHCP OFFER message DHCPACK messages only when DHCP is configured to supply an executable boot file to clients.



- **Giaddr (gateway IP address), 4 bytes:** Specifies the IP address of the DHCP relay agent to which a server should send its replies when the client and server are located on different subnets. When the server and client are on the same segment, the value must be zero.

- **Chaddr (Client hardware address) 16 bytes:** specifies the hardware address of the client system in DHCPDISCOVER and DHCPREQUEST messages, which the server uses to address its unicast responses to the client.

- 
- **Sname (server host name) 64 bytes:** Specifies the hostname of the DHCP server. The field is more commonly used to hold overflow data from the options field.
 - **File (boot file name) 128 bytes:** Specifies the name of an executable boot file for diskless client workstation in DHCPDISCOVER messages or DHCPOFFER messages. The field is more commonly used to hold overflow data from the options field.
 - **Options (variable size minimum 312 bytes):** Contains the magic cookie that specifies how the rest of the field should be interpreted and the DHCP message type option that defines the function of the message.

DHCP Options

- The option field always begins with the so-called magic cookie, which informs the server about what is contained in the rest of the field.
- **The option Format**
- The individual options in the options field contain various types and amount of data, but most of them use the same basic structure, which consists of three subfields.

Code(1 byte)


Length (1 byte)

Data(variable)



DHCP Message type option

- **1. DHCPDISCOVER:** Used by client systems to locate DHCP servers and request an IP address.
- **2. DHCPOFFER:** Used by server to offer IP addresses to clients.
- **3. DHCPREQUEST:** Used by clients to request specific IP address assignment or to renew leases.
- **4. DHCPDECLINE:** Used by clients to reject an IP address offered by a server.

- 
- **5. DHCPACK: Used by servers to acknowledge a client's acceptance of an offered IP address.**
 - **6. DHCPNACK: Used by servers to reject a client's acceptance of an offered IP address**
 - **7. DHCPRELEASE: Used by clients to terminate a lease.**
 - **8. DHCPINFORM: Used by clients that have already been assigned an IP address to request additional configuration parameters.**



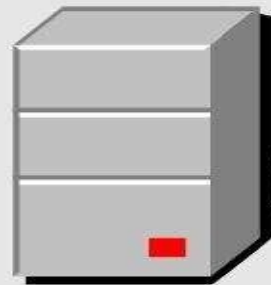
DHCP Communications

- When you configure a workstation to be a DHCP client, the system initiates an exchange of messages with a DHCP server.
- **DHCP Address Pool**
- DHCP address pool is a virtual container that contains all the IP addresses that have been configured in the DHCP range to make available to the client computers.
- As soon as any IP address from the address pool is assigned to a client computer, the address is temporarily removed from the pool.

DHCP Lease

- When the DHCP server assigns an IP address to a DHCP client computer, the address is assigned for a specific time duration. The time duration for which an IP address is assigned to a DHCP client computer by the DHCP server is technically called the DHCP lease.
- When the DHCP lease expires, the IP address is revoked from the DHCP client computer and is sent back to the DHCP address pool.

DHCP Address Pool and Lease



DHCP Server

DHCP IP Address Pool

192.168.0.6, 192.168.0.8,
192.168.0.9, 192.168.0.10,
192.168.0.12, 192.168.0.13,
192.168.0.14

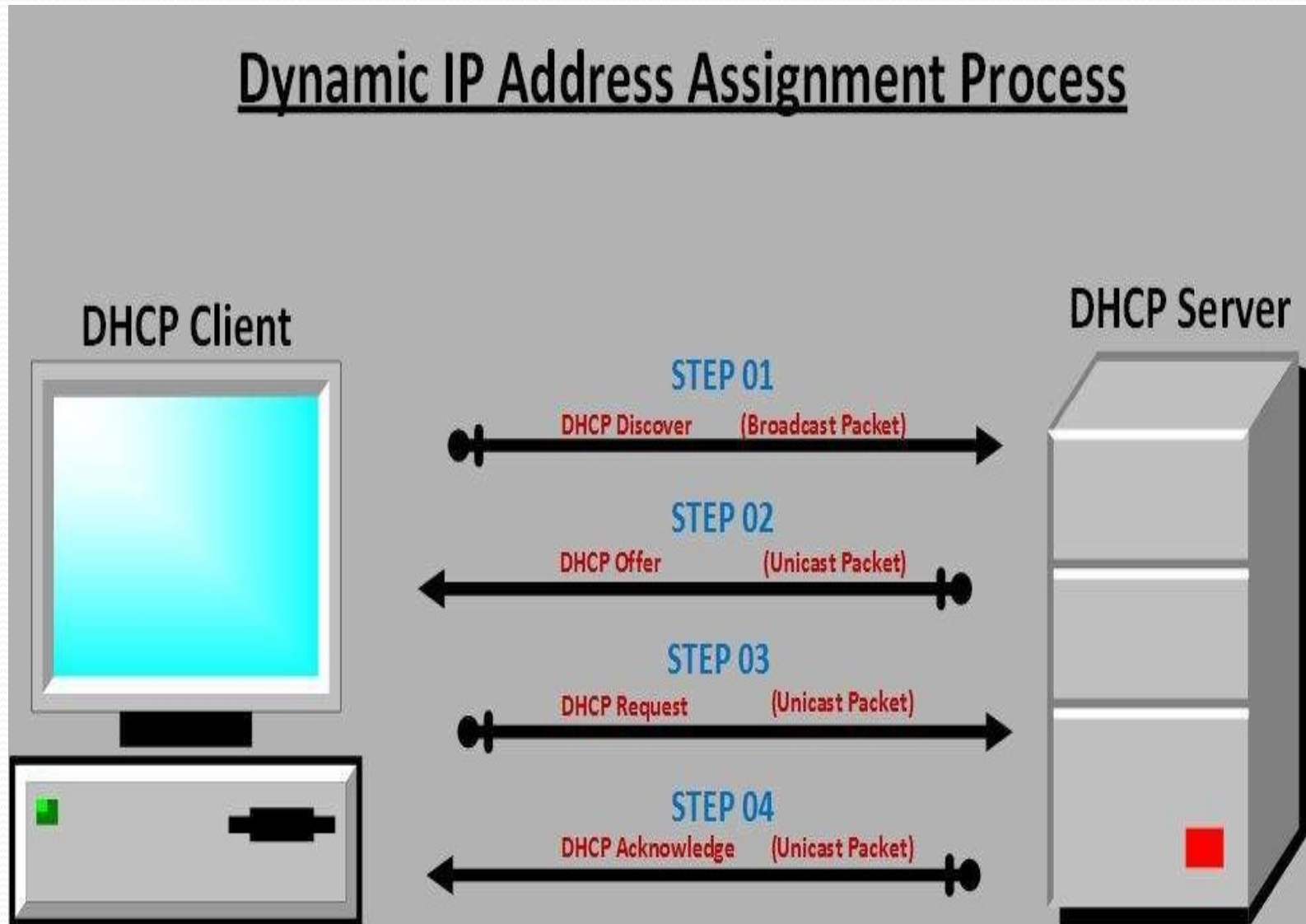


DHCP Client 01
IP Address: 192.168.0.7
Lease Duration: 24 Hrs.



DHCP Client 02
IP Address: 192.168.0.11
Lease Duration: 24 Hrs.

Dynamic IP Address Assignment Process

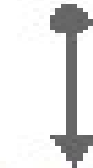




Lease renewal

- The renewal process occurs when a client already has a lease, and needs to renew that lease with the server. To ensure that addresses are not left in an assigned state when they are no longer needed, the DHCP server places an administrator-defined time limit, known as lease duration, on the address assignment.
- Halfway through the lease period, the DHCP client requests a lease renewal, and the DHCP server extends the lease.
- If a computer stops using its assigned IP address (for example, if a computer is moved to another network segment or is removed), the lease expires and the address becomes available for reassignment.

Start



Requesting State:
Client with a
current lease
nearing expiration.

DHCP Request



No — **DHCP Ask** —>
*DHCP server
renews current
lease?*



**Client must
initialize**

DHCP Ack




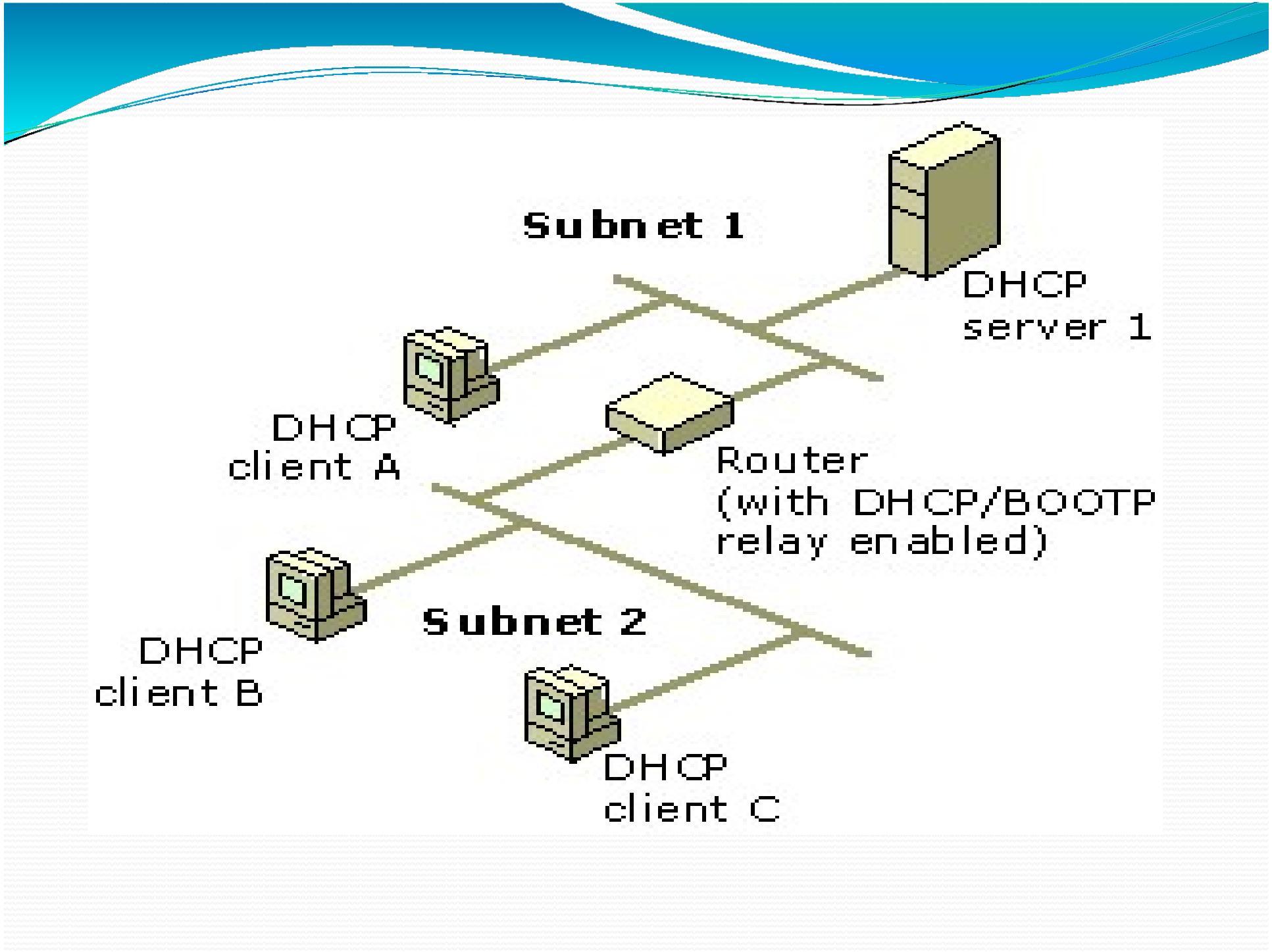
**Client updates
TCP/IP settings.**



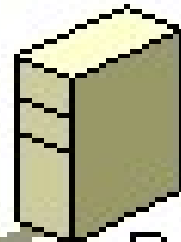
DHCP Relay Agent

- A relay agent is a small program that relays DHCP/BOOTP messages between clients and servers on different subnets.
- In TCP/IP networking, routers are used to interconnect hardware and software used on different physical network segments called *subnets* and forward IP packets between each of the subnets.
- To support and use DHCP service across multiple subnets, routers connecting each subnet should comply with DHCP/BOOTP relay agent capability.

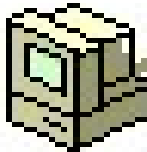
- 
- If a router cannot function as a DHCP/BOOTP relay agent, each subnet must have either its own DHCP server or another computer that can function as a relay agent on that subnet. In most cases, routers support DHCP/BOOTP relay.



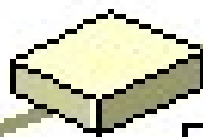
Subnet 1



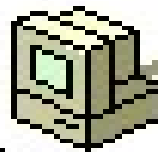
DHCP server 1



DHCP client A

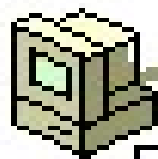


**Router
(with DHCP/BOOTP relay enabled)**



DHCP client B

Subnet 2



DHCP client C



DNS

Domain Name System or Domain Name Service



The Domain Name System (DNS) is used to resolve human-readable hostnames like `www.Dyn.com` into machine-readable IP addresses like `204.13.248.115`. DNS also provides other information about domain names, such as mail services.



DNS :Domain Name System

- DNS stands for service that translates domain names into IP addresses.
- Domain names are alphabetic, they're easier to remember. The Internet however is really based on IP addresses.
- For example, the domain name www.example.com might translate to 198.105.232.4.
- The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.



Objective of DNS

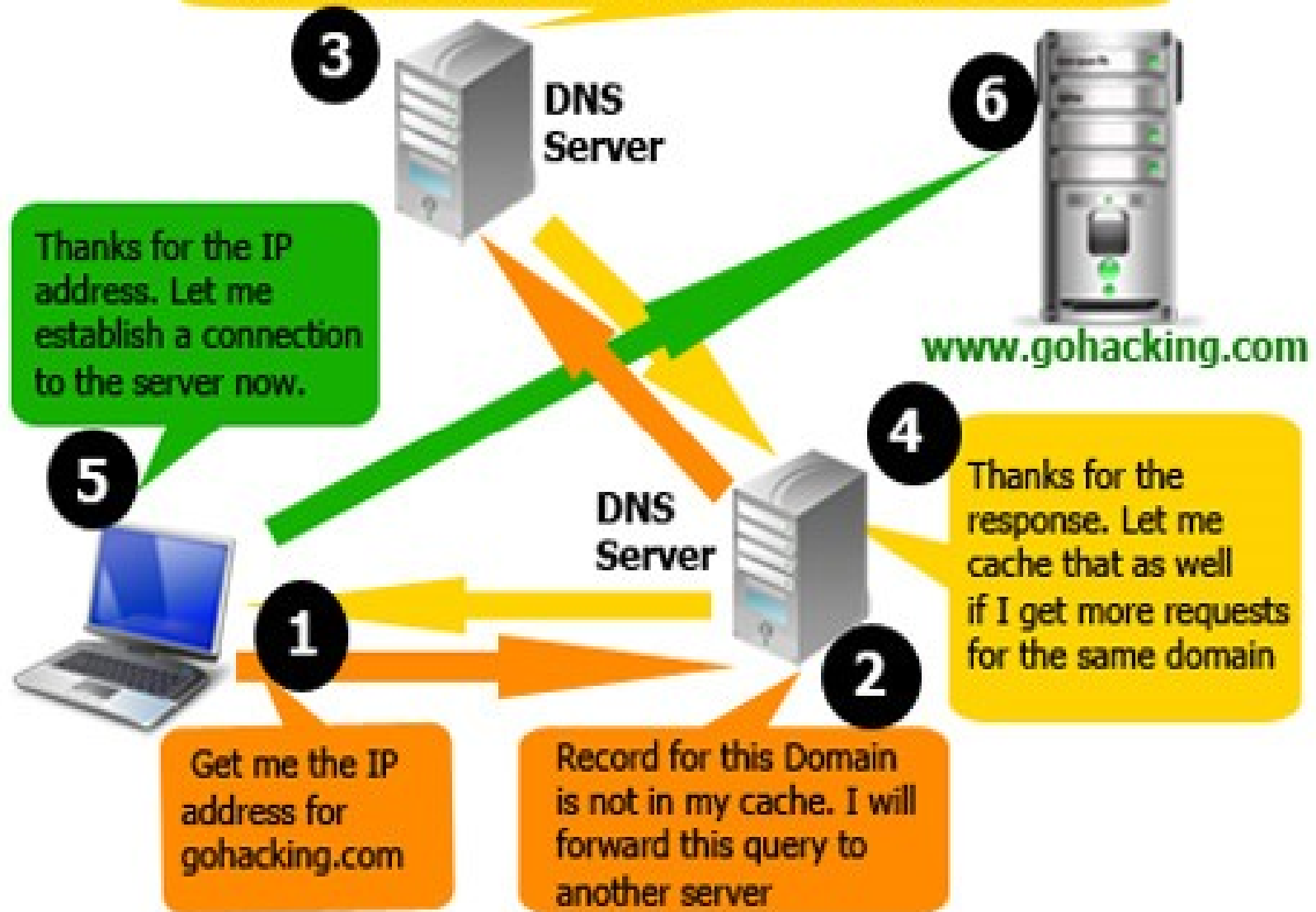
- To create a means for administrators to assign host names to their computers without duplicating the names of other systems.
- To store the host names in a database that would be accessible by any system, anywhere on the network.
- To distribute the host name database among servers all over the network.
- To avoid creating traffic bottlenecks and a single point of failure.



Root Name server

- The root name servers know how to find the authoritative name servers for all top-level zones.
- There are only 13 root name servers.
- Root servers are critical for the proper functioning of name resolution

That's in my cache. Domain points to the IP: 173.245.61.120





DNS naming

DNS designed by Peter Mocka petris in 1983.

Consists three basic elements:

- Hierarchical name space that divides the host system database in to discrete elements called *Domain*.
- Domain name servers
- Resolvers



Hierarchical Name Space

That divides the host system database into discrete elements called *domains*.



Domain Name Servers

- Computers and other network devices on the Internet use an IP address to route your request to the site you're trying to reach.
- This is similar to dialing a phone number to connect to the person you're trying to call.
- Thanks to DNS, though, you don't have to keep your own address book of IP addresses.
- Instead, you just connect through a **domain name server**, also called a **DNS server** or **name server**, which manages a massive database that maps domain names to IP addresses.



Cont..

- When you use an alphanumeric address such as WWW.EXAMPLE.COM, your computer needs to understand what numerical IP addresses it needs to contact, and this is accomplished through DNS servers. The answer is delivered back to the requesting computer via the DNS listed for the domain name.
- All domains have at least two DNS servers as seen through [WHOIS lookups](#) such as NS1.EXAMPLE.COM and NS2.EXAMPLE.COM, and your request for anything related to the domain name gets sent to one of these servers. In response, the DNS server sends back the IP address that you should contact. This works for the Web Site, Mail Servers, and anything else based on the domain name.



Resolvers

- Also called *domain name resolvers* are the names given to computers, commonly located with Internet Service Providers (ISPs) or institutional networks that are used to respond to a user request to resolve a domain name. These computers translate a domain name into an IP address. Also called *DNS resolvers*.



Cont...

- for example, if you need to resolve host names for a zone that's not local, you might create a stub zone that contains a list of authoritative DNS servers for that zone. Local queries then are referred to one of the DNS servers on that list. There has to be a reliable network connection between the two servers.



Cont.....

- The component in the client system that generates the DNS query is called *resolver*.
- The resolver is a simple set of library routines in the operating system that generates the queries to be sent to the DNS server, reads the response information from the server's replies, and feeds the response to the application that originally requested it.
- Resolver can resend a query if no reply is coming after a given timeout period, and can process error message returned by the server, such as when it fails to resolve a given name.



Top level Domains

- First word in right represent TLD.
 - Functions as registrars for SLD.
 - TLD dedicated to specific purpose as follows:
 - Com, edu, gov, int, mil, net, org, generic top level domains like aero, biz, coop, info, museum, name, pro , country code domain like in.uk, usetc.
 - For example, in the domain name www.example.com, the top-level domain is com.
- Responsibility of management of most top-level domains is delegated to specific organizations by the [Internet Corporation for Assigned Names and Numbers](http://www.icann.org) (ICANN), which operates the [Internet Assigned Numbers Authority](http://www.iana.org) (IANA), and is in charge of maintaining the [DNS root zone](http://www.root-servers.org).



Second level Domain

Registrars of TLD

- Can register second level domain
- Maintains records of SLD
- Identify owner of second level domain
- Specify 3 contact within registrar
 - Administrative contact
 - Billing contact
 - Technical contact
- Have 2 IP address of two DNS server that act as a source for further information.



Cont....

- To host SLD, organization have 2 DNS servers.
- DNS server product are available for all NOS.
 - Also DNS servers are the alternate source of information about that domain.
 - DNS server not located on registrants network.
 - DNS server identified in TLD's record & are the authority for the second level domain
 - N/W admin wants to create sub domain, they do so in their own DNS servers.
 - In DNS –request pass to TLD-> turned to SLD-> get requested information.



Cont.....

- That is why DNS is called distributed database.
- That eliminates traffic congestion problem
- Distributes duties of administrators among thousands of N/W around the world.
- Domain name registrants are responsible for their own area of name space.



Sub domains

- Administrators of SLD- can create sub domains to form additional levels.

- Organizations use sub domain to divide their N/W according to organization or geographical boundaries.

Like sales.abc.com, hr.abc.com

Paris.abc.com

Newyork.abc.com

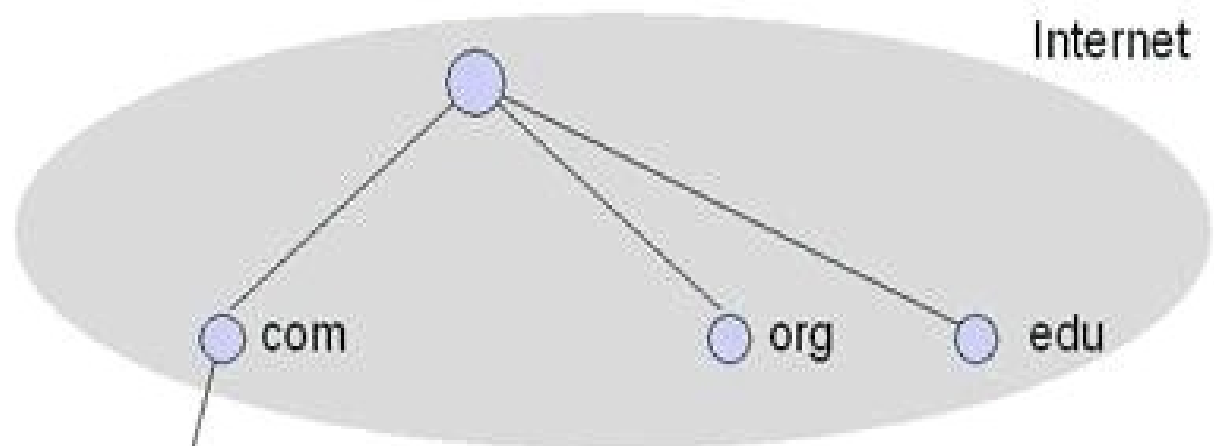
Use of sub domains-can make it easier to identify hosts on a large N/W.



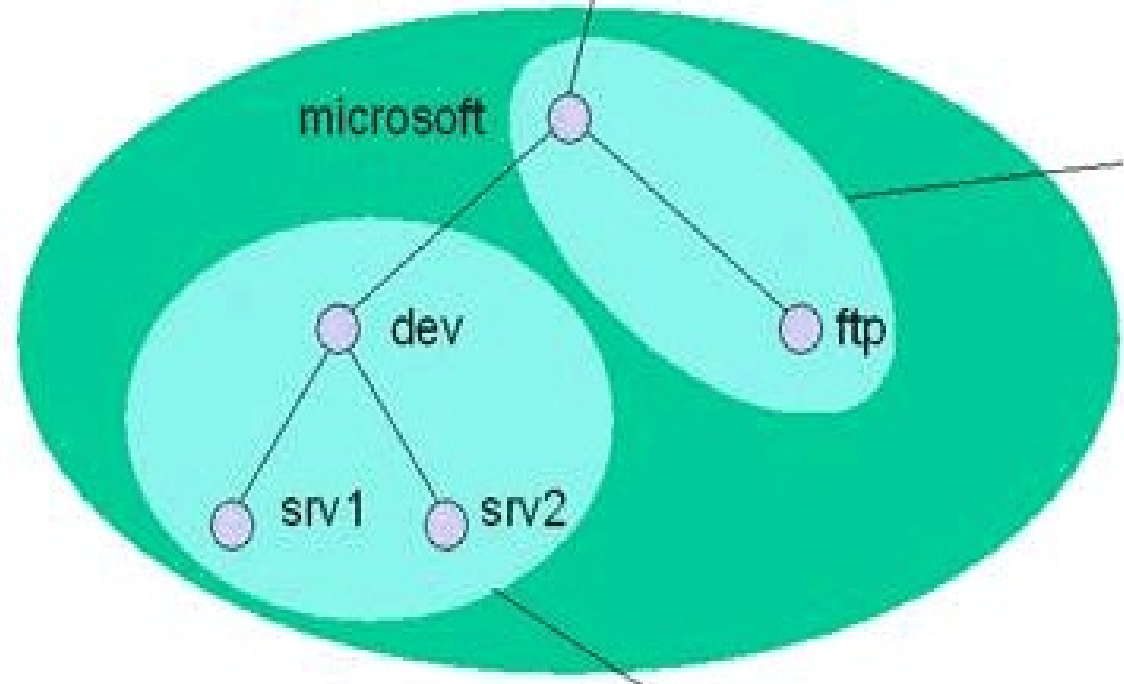
Cont.....

- DNS server for TLD contains address of SLD
- SLD domain's server contains address of sub domains (third level domain).
- DNS servers can breakup domain's space in to administrative units called ZONE.
- Domain with 2 levels- called single zone.
- Domain with 3 levels- can divided in to multiple zone.

Internet



microsoft.com domain



microsoft.com zone

dev.microsoft.com zone

Resolving Domain Name

- The DNS Resolution process starts when the user types a URL address on the browser and hits Enter. At this point, the browser asks the operating system for a specific page, in this case google.com.
- Application generate API call to resolver on client system.
- Resolver generate recursive query message .
- Client sys. Transmit recursive query message to DNS server identified in TCP/IP configuration.
- Then client's DNS server checks its resource records to see if it is authoritative source for the zone containing the requested server name.

Cont....

- If it is authority, it generates a reply message and transmits it back to the client.
- If the DNS server is not the authority for the domain in which the requested server is located, it generates an iterative query and submits it to one of the root name servers.
- The root name server checks the name requested by the DNS server and consults its resource records for the name's top level domain.
- Because the root server received an iterative query, so it does not send its own request to the TLD server.
- So it transmits request to the DNS server & then the DNS server generates a new iterative query and transmits it to the TLD server.

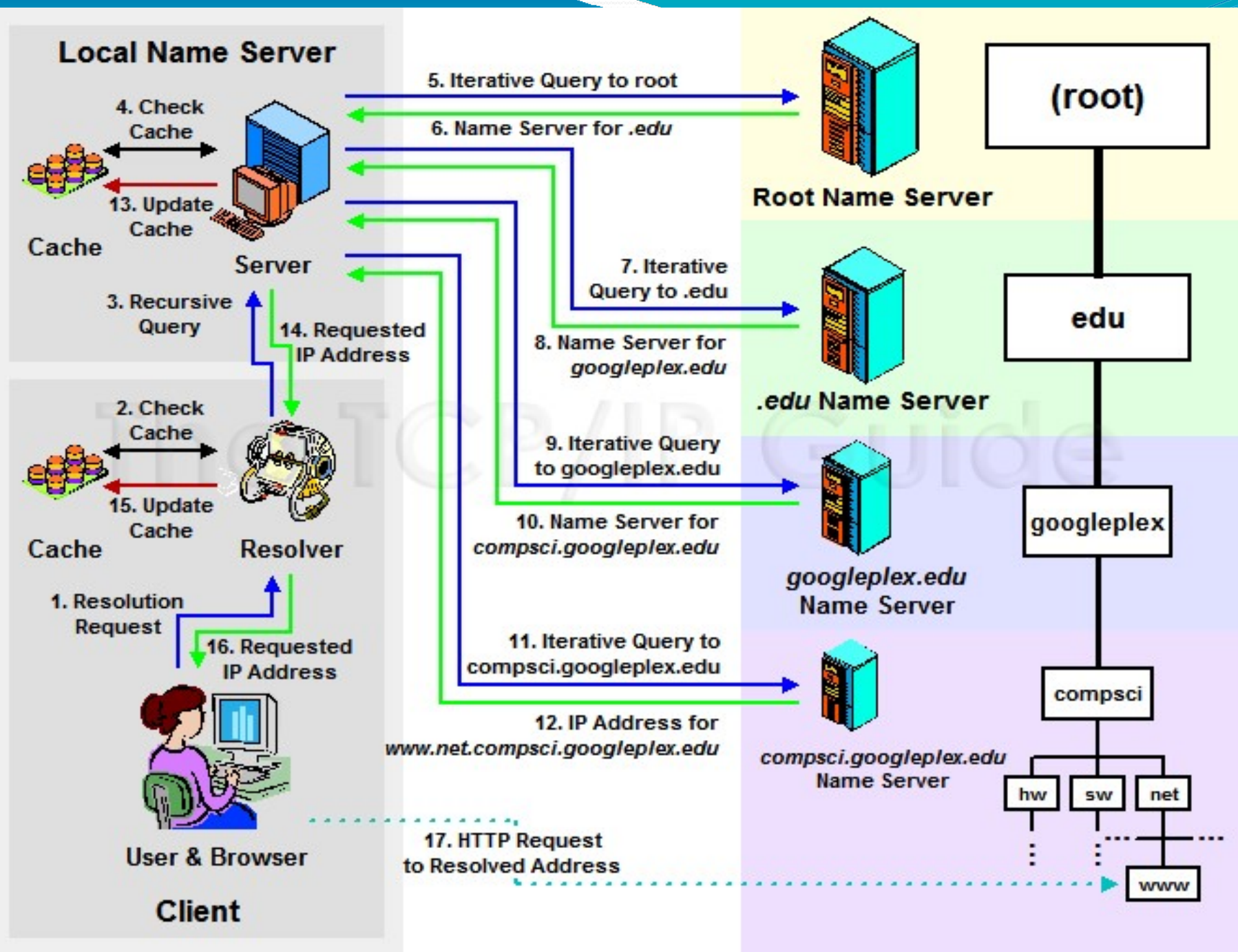
Cont....

- The TLD server checks the SLD in the requested name and transmit to the DNS server a referral containing the address of authoritative servers for SLD.
- Then DNS server generates new iterative query and transmit to SLD server.
- If the requested name contain additional domain name then SLD server replies with another referral to the TLD servers.
- This process continues until the original server receives a referral to the domain server that is the authority for the domain containing the requested host.
- Once the authoritative server for the domain containing the host receives a query from the original server, it consult its resource records to determine the IP address of the requested system and transmit it in a reply message back to that original server.



Cont.....


- The original server receives the reply from the authoritative server and transmit the IP address back to the resolver on the client system.
- The resolver replays the address to the application, which can then initiate communication with the system specified by the user.






DNS Functions

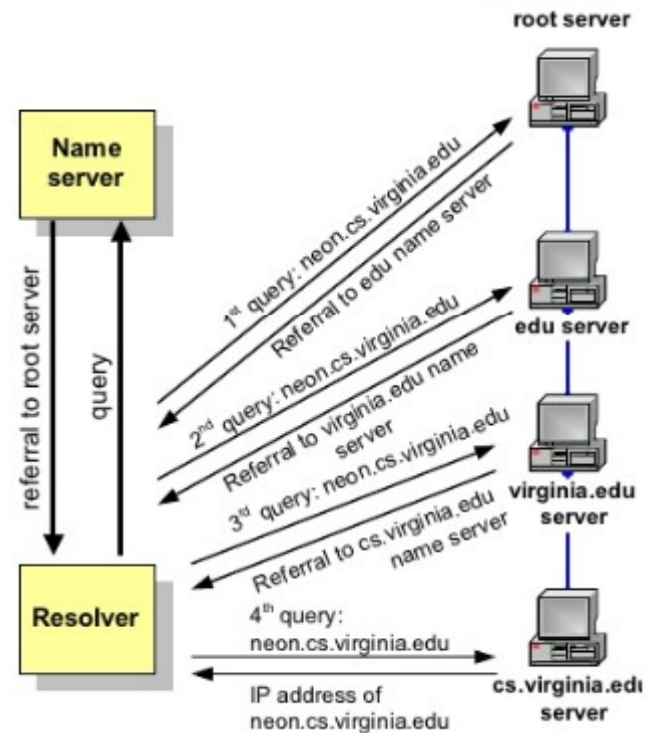
- **Resource Records:** DNS servers are basically database servers that store information about the hosts and subdomain for which they are responsible in resource records (RRs).
- **SOA (Start of Authority):** Indicates that the server is the best authoritative source for data concerning the zone. Each zone must have an SOA record and only one SOA record can be in a zone.

- 
- **NS (Name Server) :** The name server resource record indicates the servers authoritative for the zone. They indicate primary and secondary servers for the zone specified in the SOA resource record, and they indicate the servers for any delegated zones. Every zone must contain at least one NS record at the zone root.
 - **A (Address):** Provides a name to IP address mapping that supplies an IP address for a specific DNS name. This record type performs the primary function of the DNS, converting names to addresses.

- 
- **PTR: Provides an address to name mapping. This is the functional opposite of an A record, used for reverse lookup only.**
 - **CNAME (Canonical Name): Creates an alias that points to the canonical name of a host identified by an A record. CNAME records are used to provide alternative names by which the systems can be identified.**
 - **MX (Mail Exchanger): Identifies a system that will direct e-mail traffic sent to an address in the domain to the individual recipient, a mail gateway or another mail server.**

ITERATIVE QUERY:

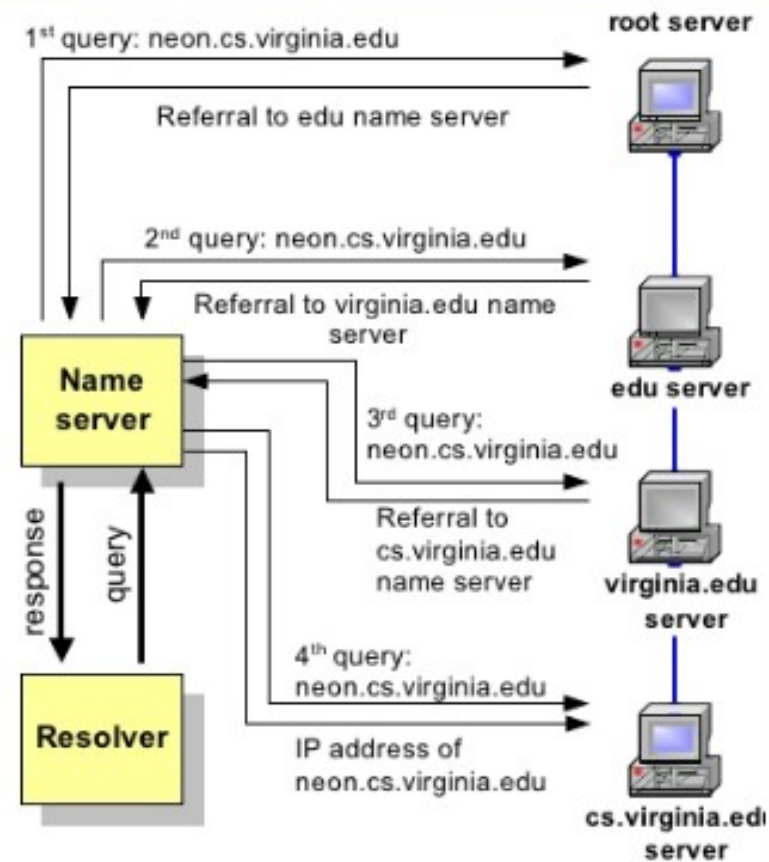
- In an iterative query, the name server sends a closest known authoritative name server a referral to the root server.
- This involves more work for the resolver



Recursive queries

Clip slide

- In a recursive query, the resolver expects the response from the name server
- If the server cannot supply the answer, it will send the query to the “closest known” authoritative name server (here: In the worst case, the closest known server is the root server)
- The root server sends a referral to the “edu” server. Querying this server yields a referral to the server of “virginia.edu”
- ... and so on





DNS Name Registration

- If you have a web site and to register own domain name then this is done through a registrar.
- A registrar first verifies that the requested domain name is unique and enters into the DNS Database.
- To register, the organization needs to give the name of its server and the IP address of the server to the registrar.



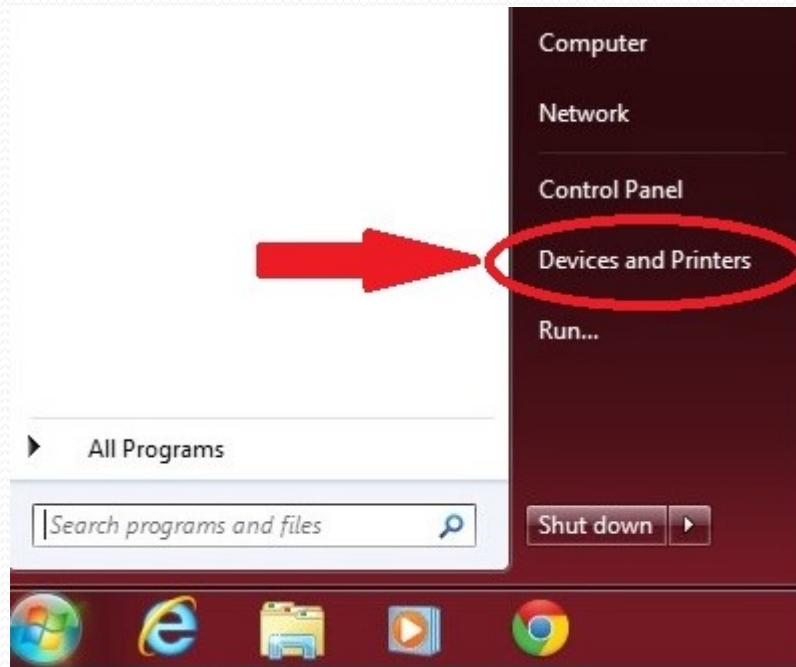
2.3 NETWORK PRINTING CONCEPT

- Local Printer, Shared printer and Network printer are the three basic printing configurations.
- A software is required to control the printing process.
- The printer determines where and when the output should be sent.

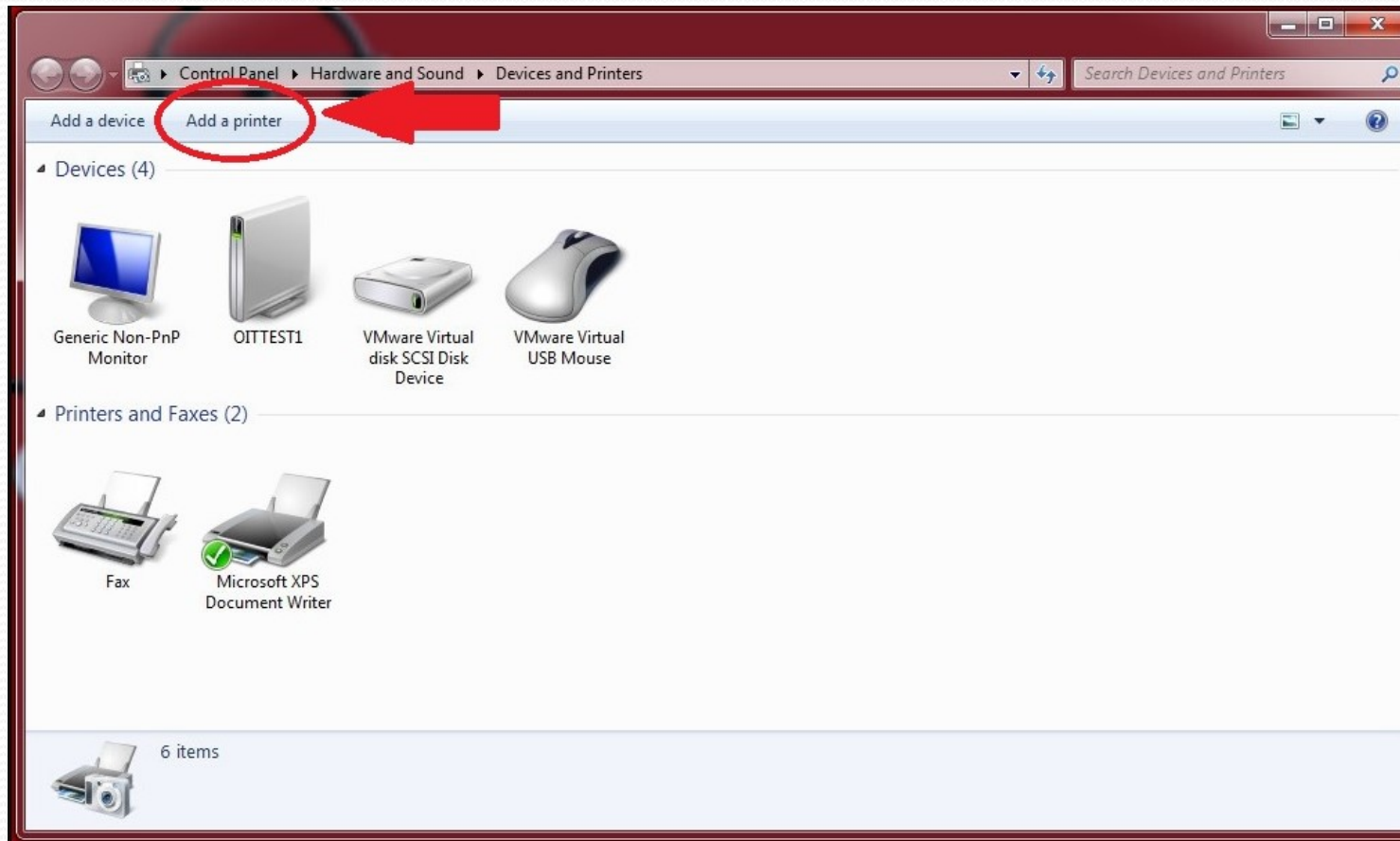
CONT...

❖ Setting up Local Print Device

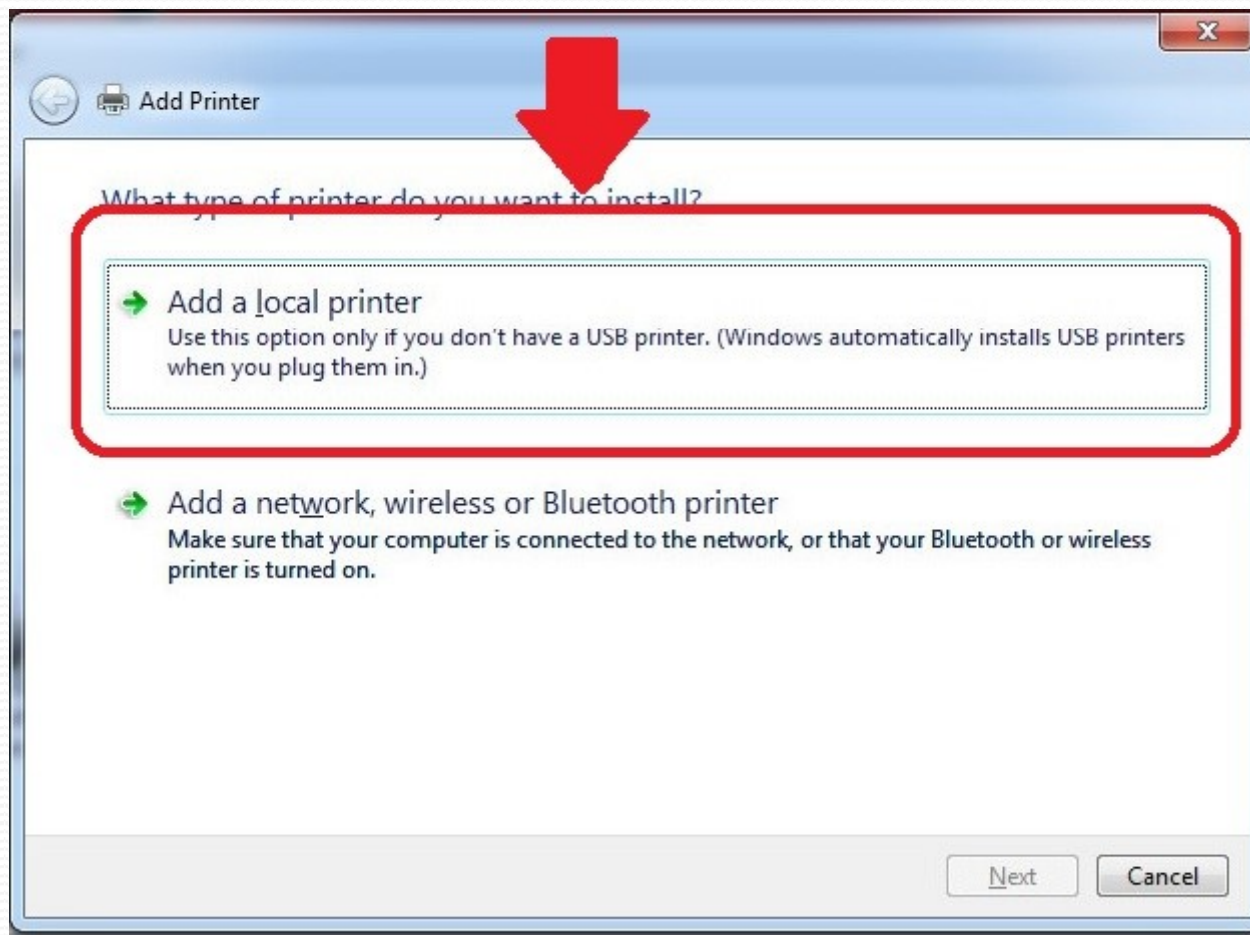
❖ Click the START button and select DEVICES AND PRINTERS.



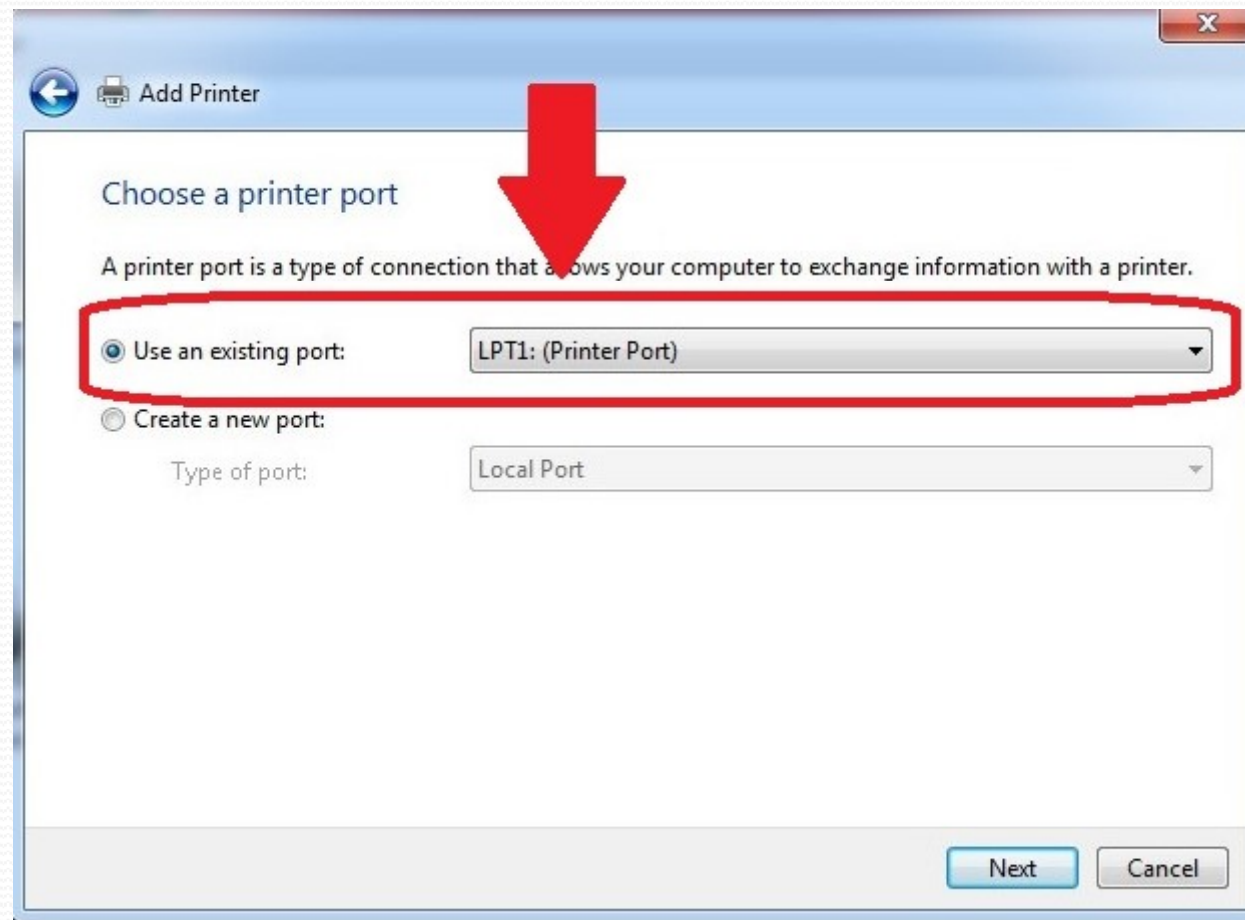
Select "Add a Printer"



Select "Add a Local Printer"

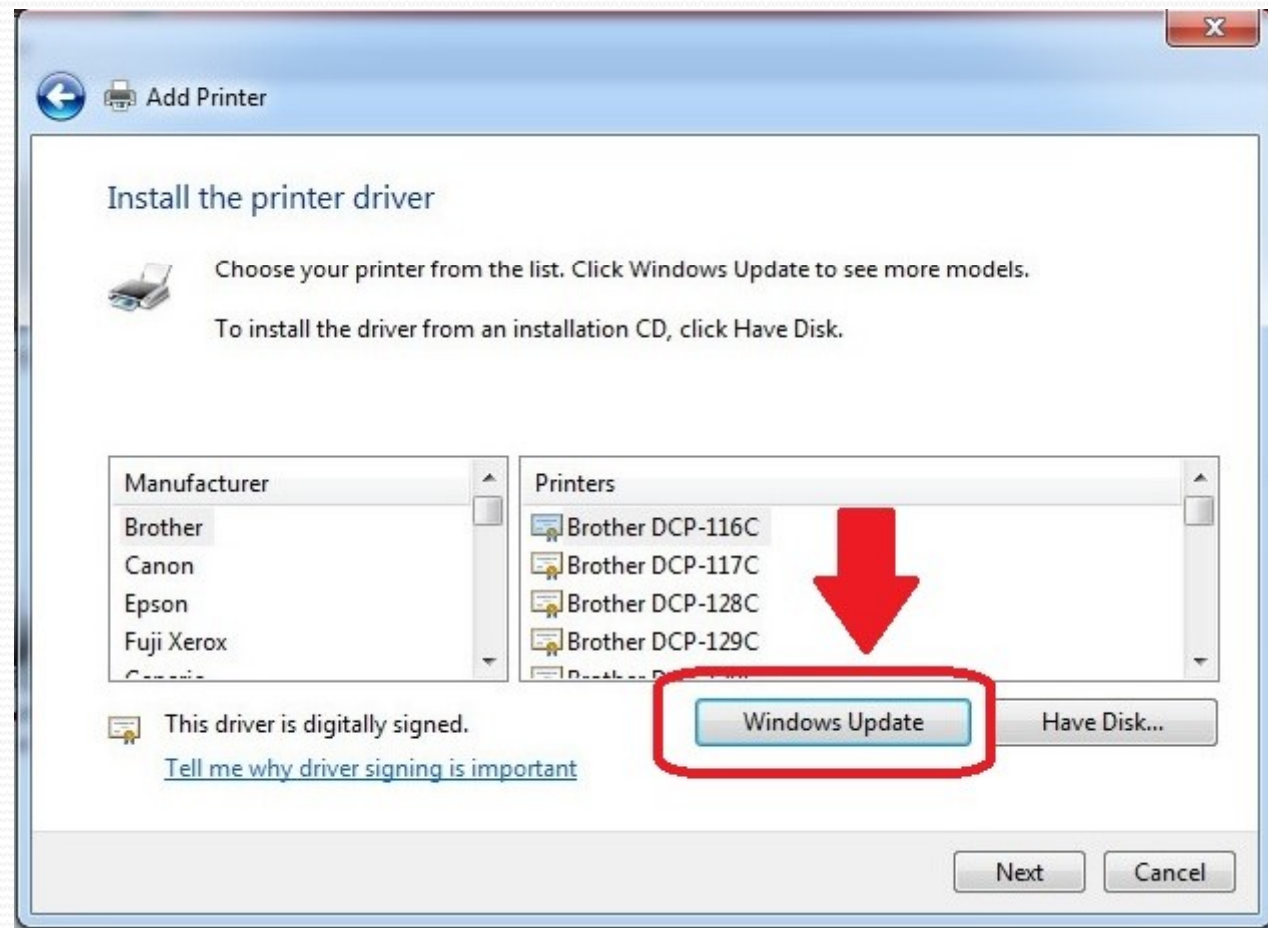


Choose to "Use an Existing Port", and leave as default "LPT1: (Printer Port)" If you already have another printer connected to this PC, you may need to change to LPT2

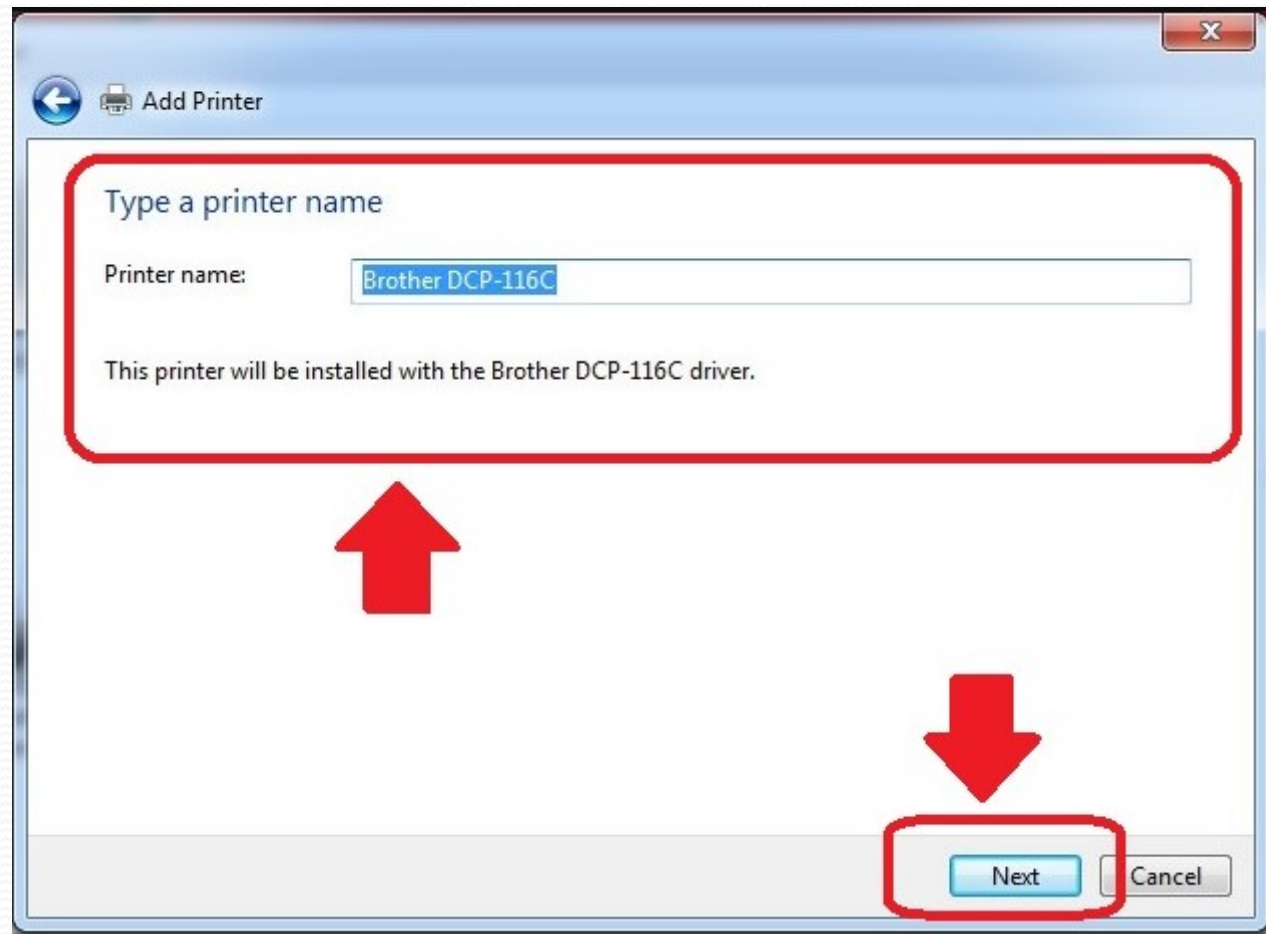


Select "Windows Update" to populate the list of known printers. This may take several minutes.

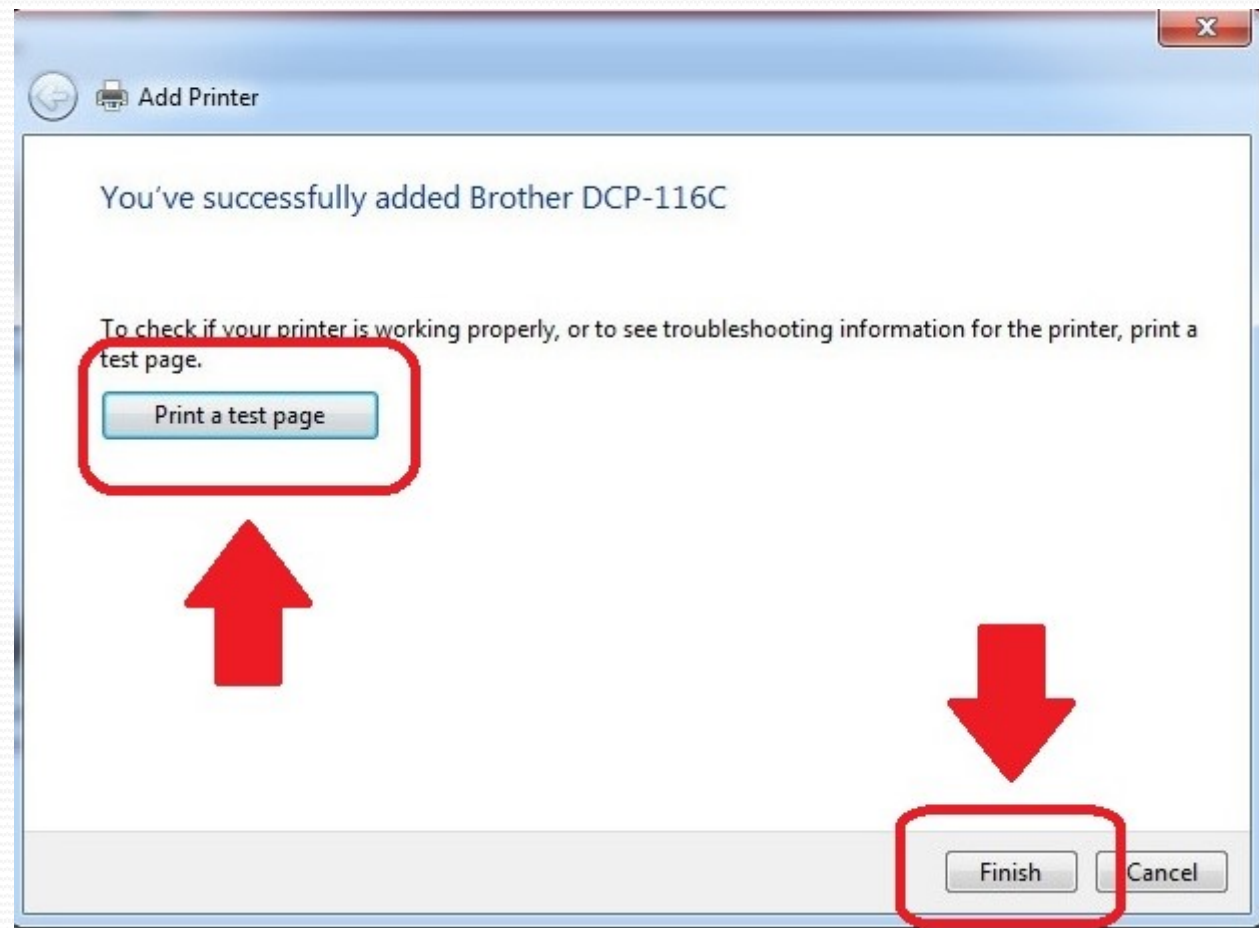
Then choose your printer from the list. If multiple drivers are listed for your printer, select the one that say PCL
For instance: Dell 5130PCL

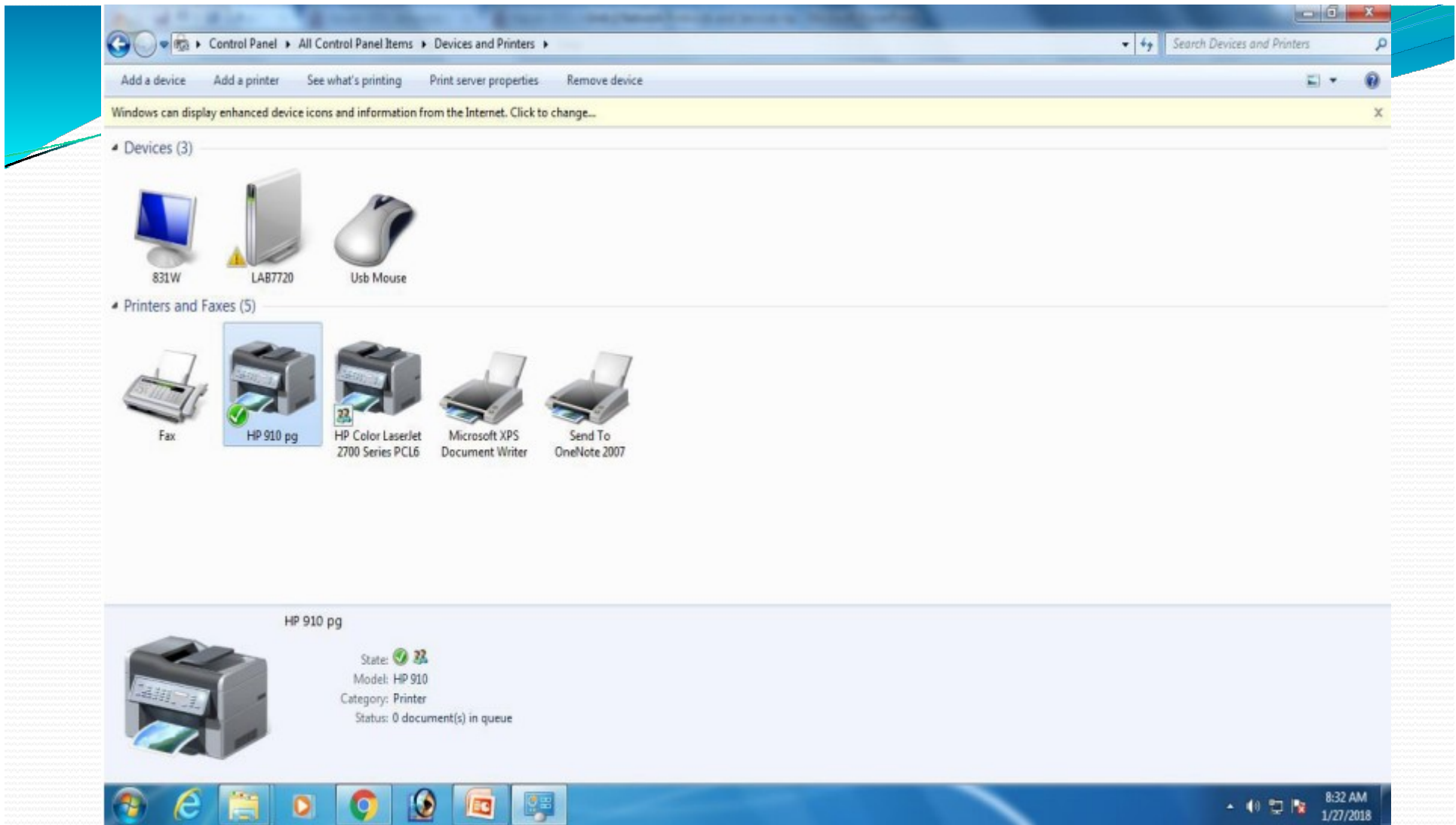


Choose a name for your printer. The default name is fine, unless you have multiples of the same printer.



If you wish to test your printer to make sure it was installed correctly, select "Print a test page"
When you're all done, press "Finish"





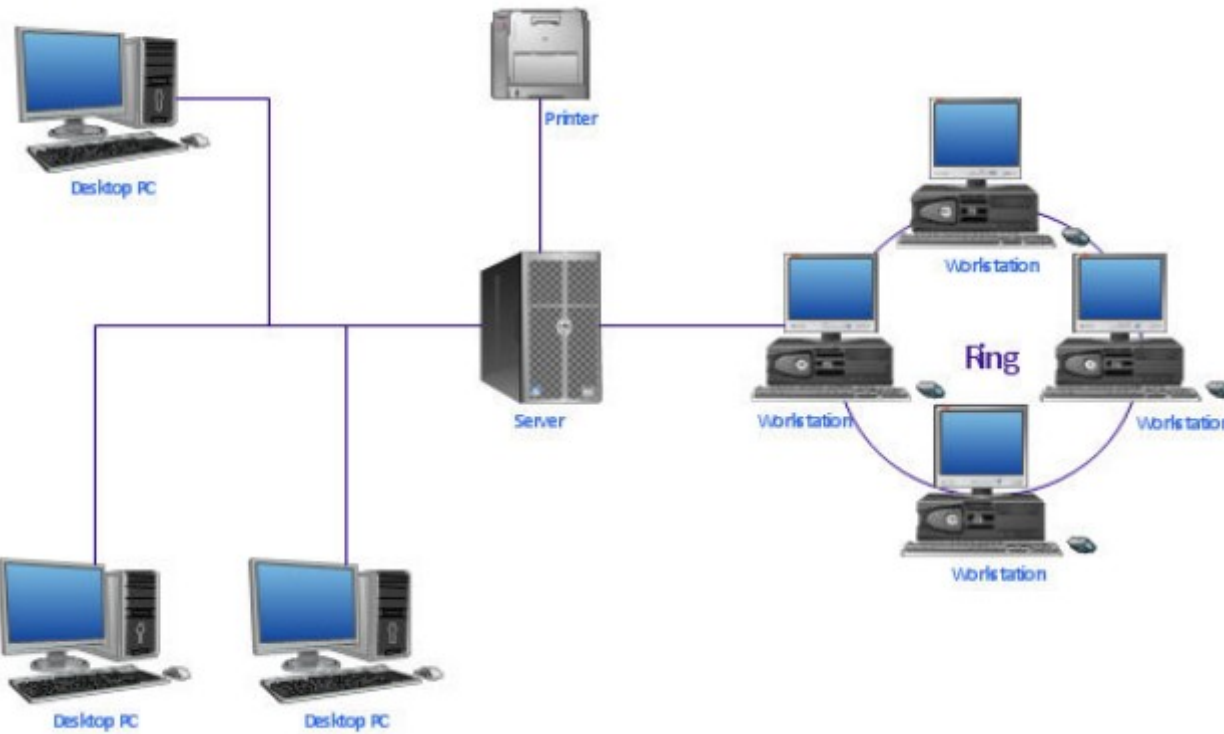
Now you can see “Devices and Printers” window.



To Share a Print Device

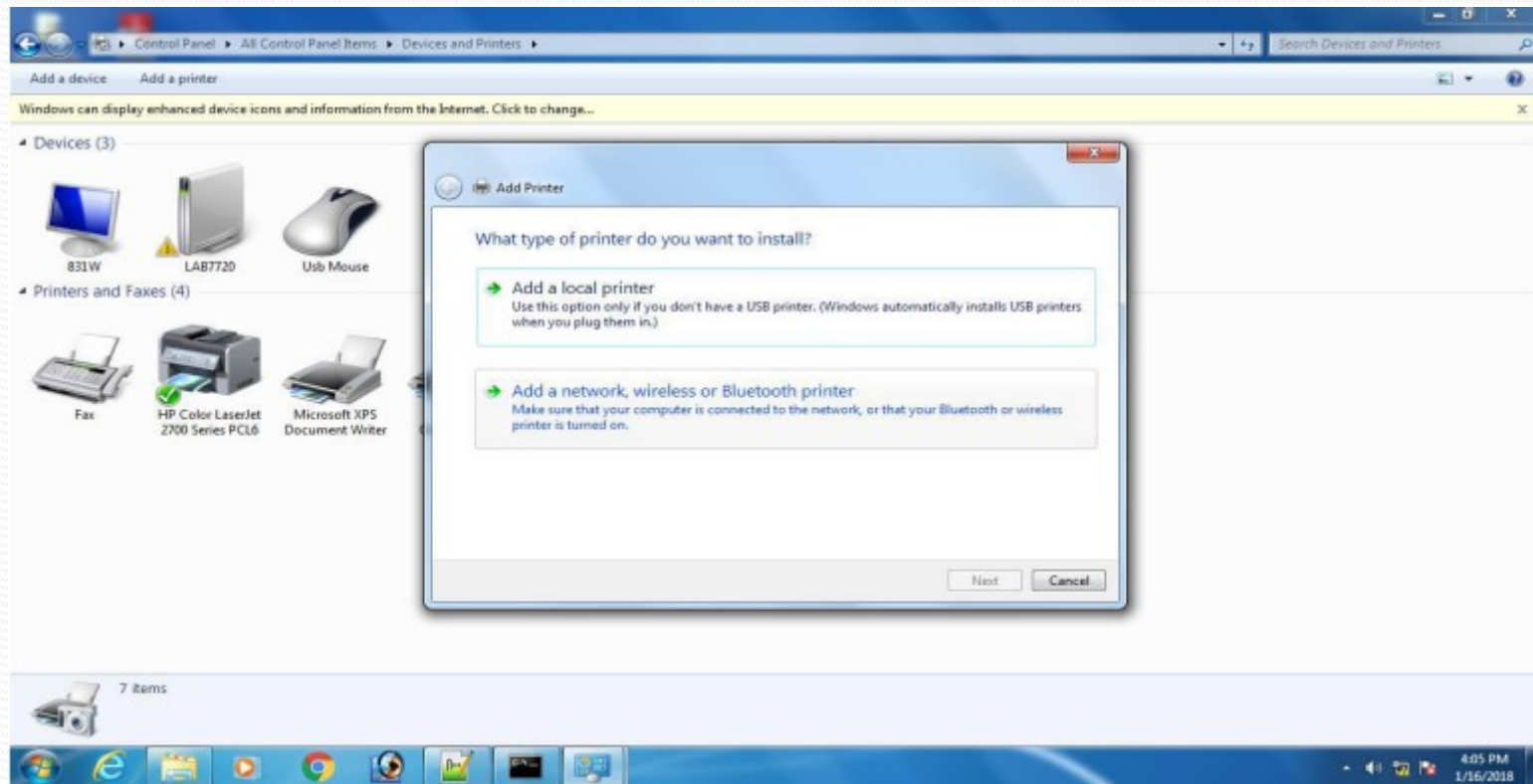
1. Click the Start menu, then select "Devices and Printers."
2. Right-click the printer you want to share, then click Printer properties.
3. Click the Sharing tab, and check the box next to "Share this printer."

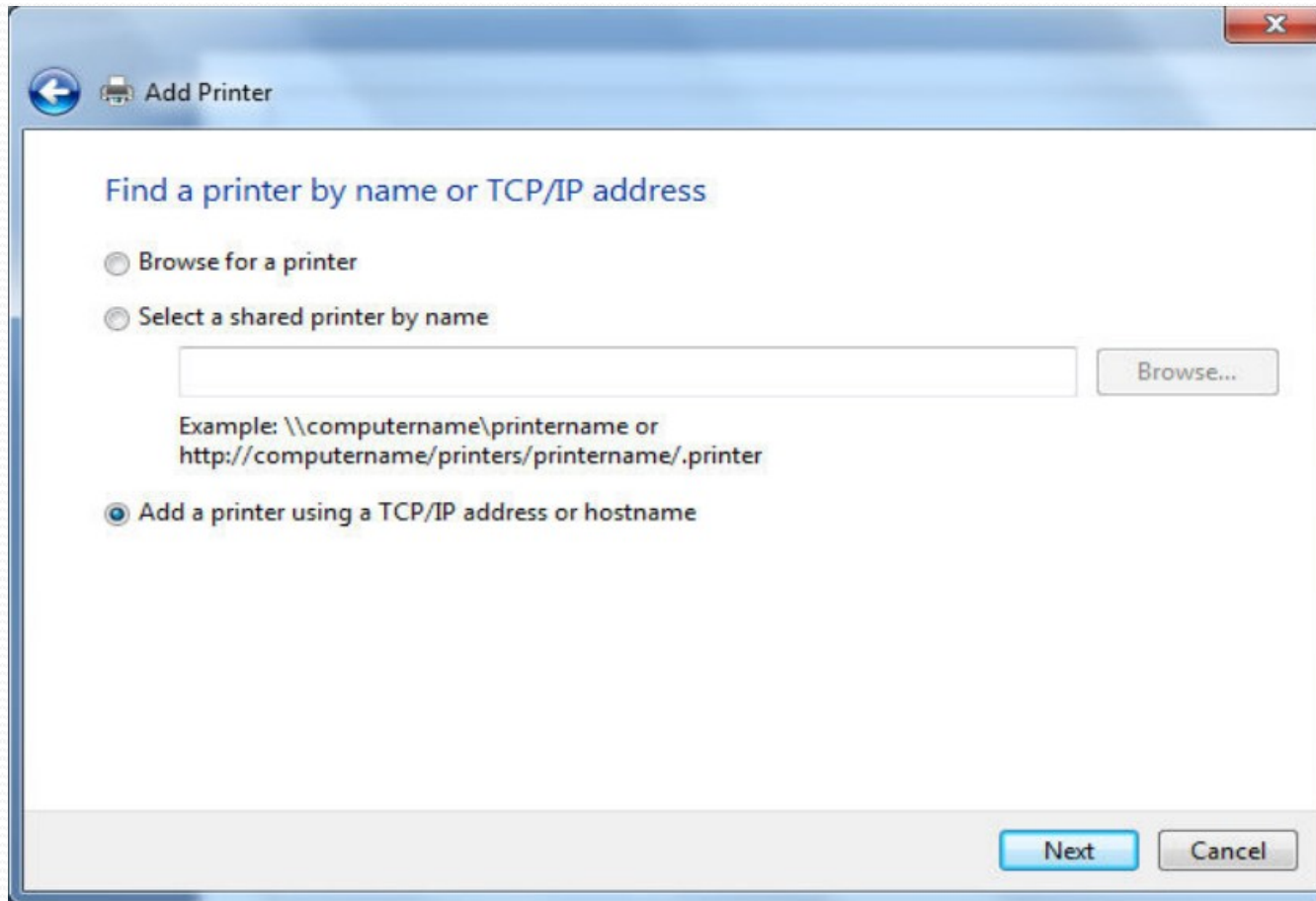
Network Print Device



TO USE SHARED PRINTER FOLLOW THE STEPS.

1. Click the Start menu, then select "Devices and Printers."
2. Select "Add a printer."





Select “add a printer using TCP/IP address”

Add Printer

Type a printer hostname or IP address

Device type: Autodetect


Hostname or IP address: 160.160.18.94

Port name: 160.160.18.94

Query the printer and automatically select the driver to use

Next Cancel

Specify IP address for printer host.

 Add Printer

Type a printer hostname or IP address

Device type:

Autodetect

Hostname or IP address:

160.160.18.94

Port name:

160.160.18.94

Query the printer and automatically select the driver to use

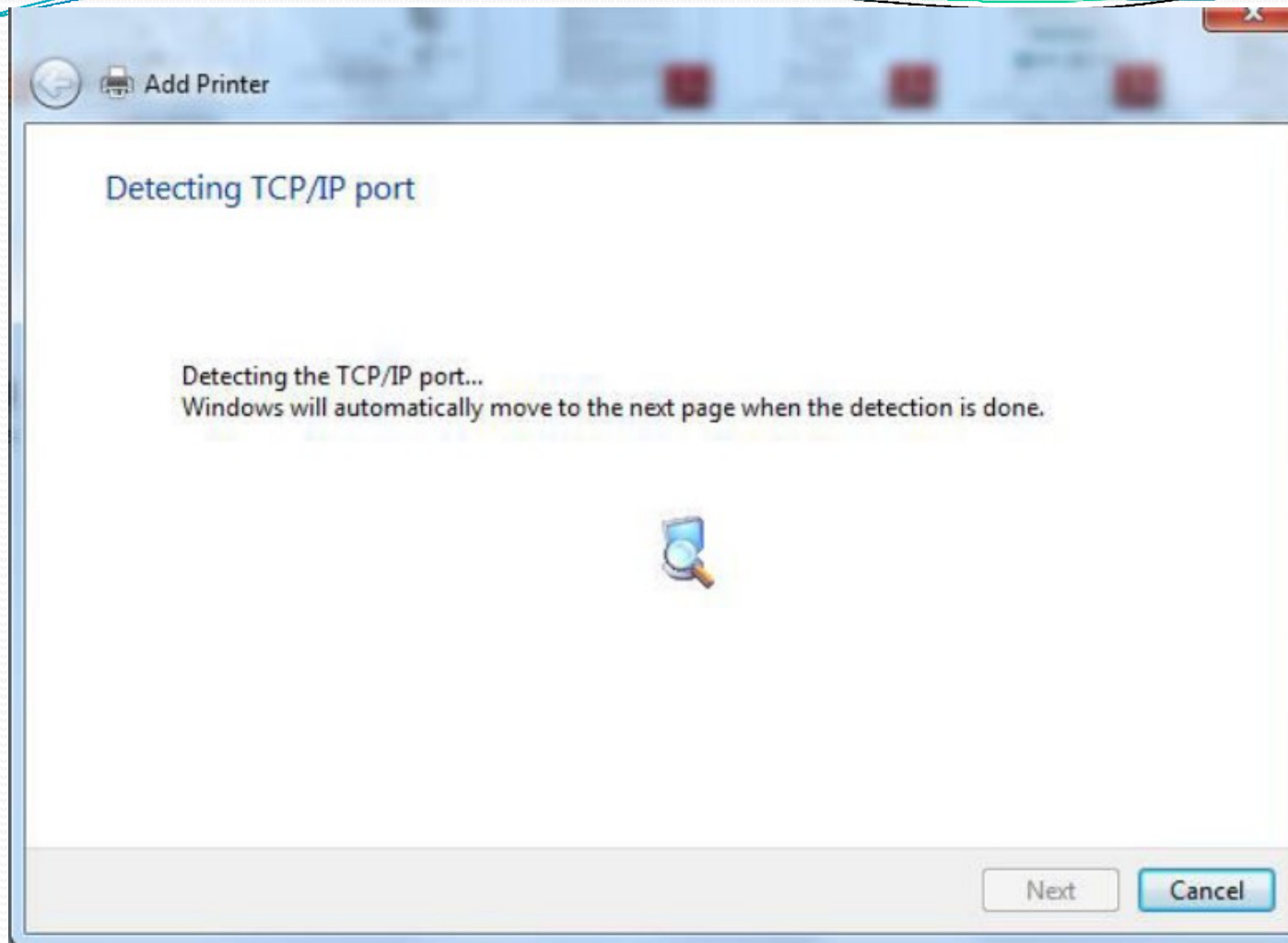
Contacting printer...



Next

Cancel

Searching printer in network.



Next based on IP address you provided, it will search printer.



Add Printer



Additional port information required

The device is not found on the network. Be sure that:

1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.

If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.

Device Type

Standard

Custom

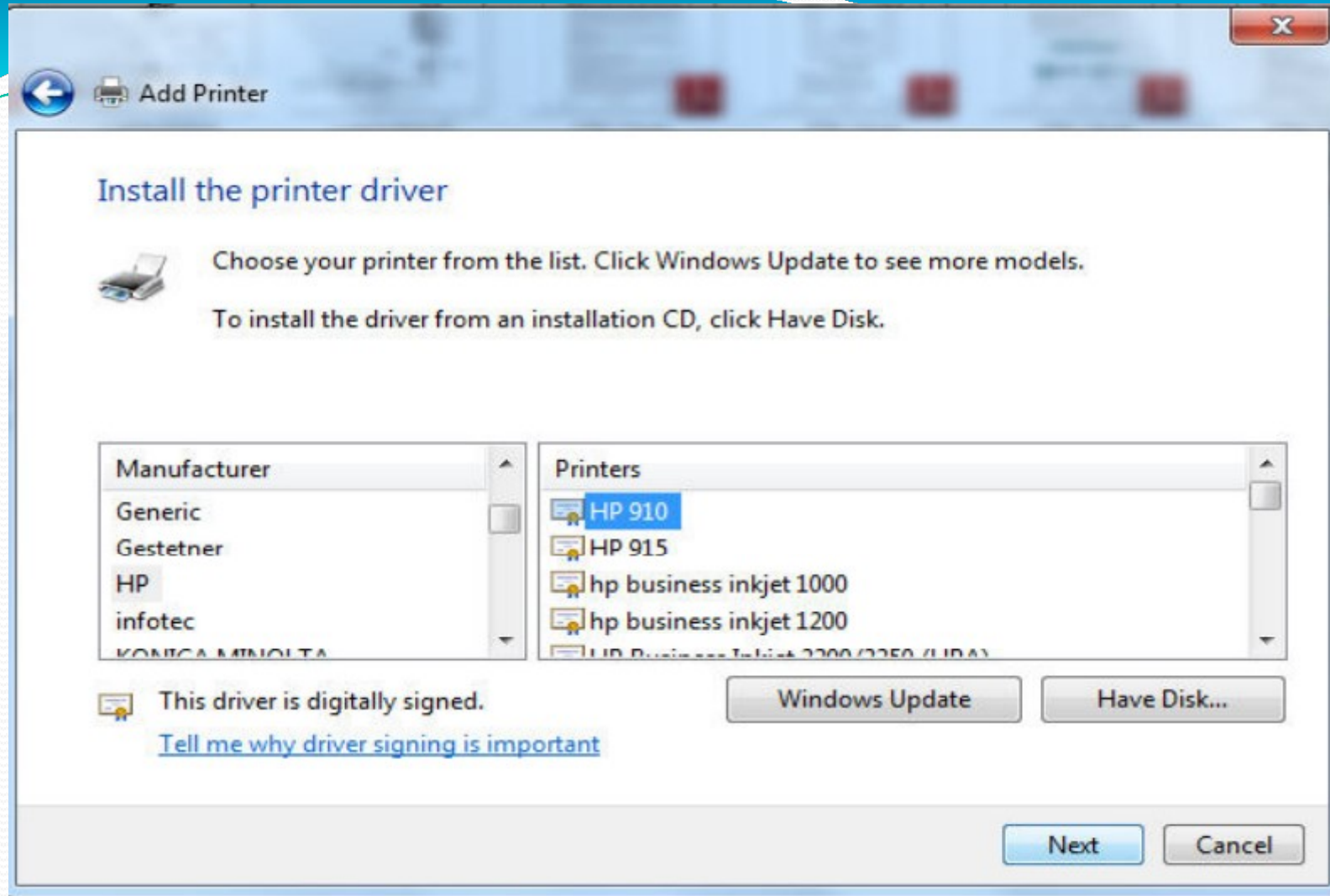
Generic Network Card

Settings...

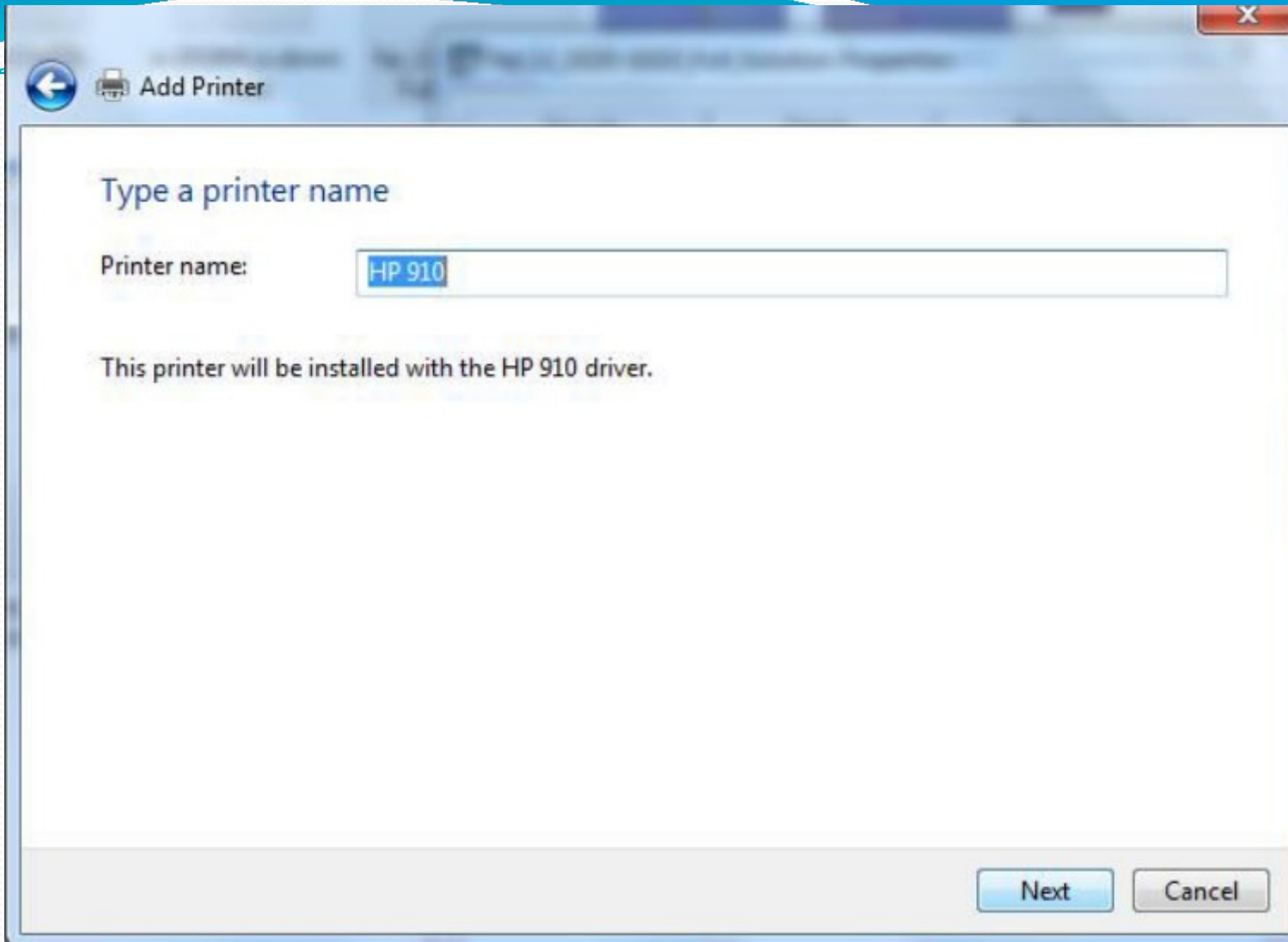
Next

Cancel

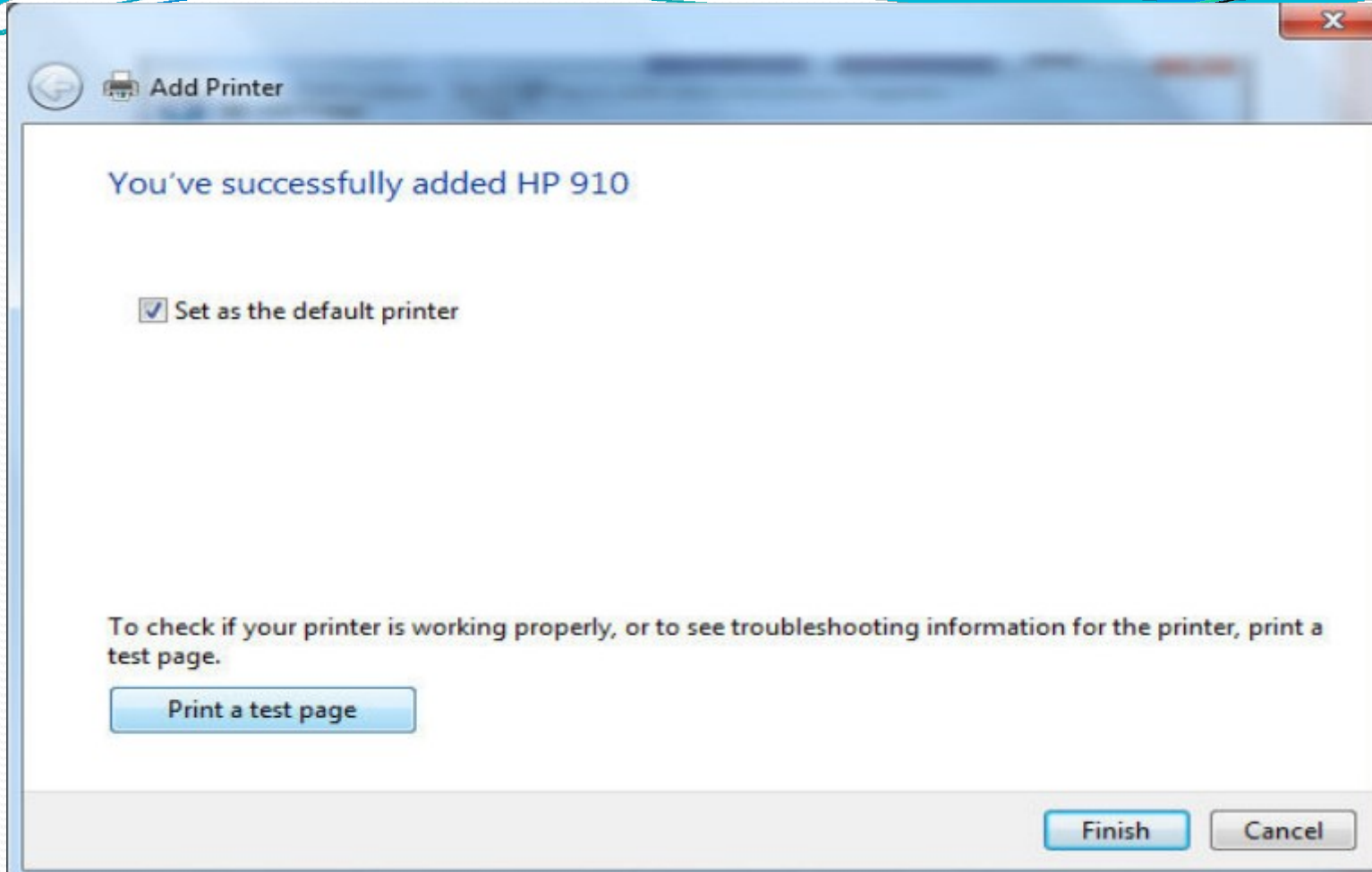
Choose device type.



Select driver for printer appropriate to the printer shared in network.



Choose printer name.



Select “print a test page” and FINISH.