Mahmmoud A. Mahdi

Configuring Name Resolution

Name Resolution

- When we connect to a computer, we normally specify it by a name such as www.microsoft.com.
  - Computer names such as these are used only for human benefit.
- For a connection to be established to a remote computer, the name we specify must be translated into an IP address to which packets can be routed.
- In computer terminology, to resolve a computer name means to translate the name into an address.

Name Resolution Methods in Windows

- Windows server 2008 networks include no fewer than three name resolution systems:
  1. DNS
  2. Link Local Multicast Name Resolution(LLMNR)
  3. NetBIOS.

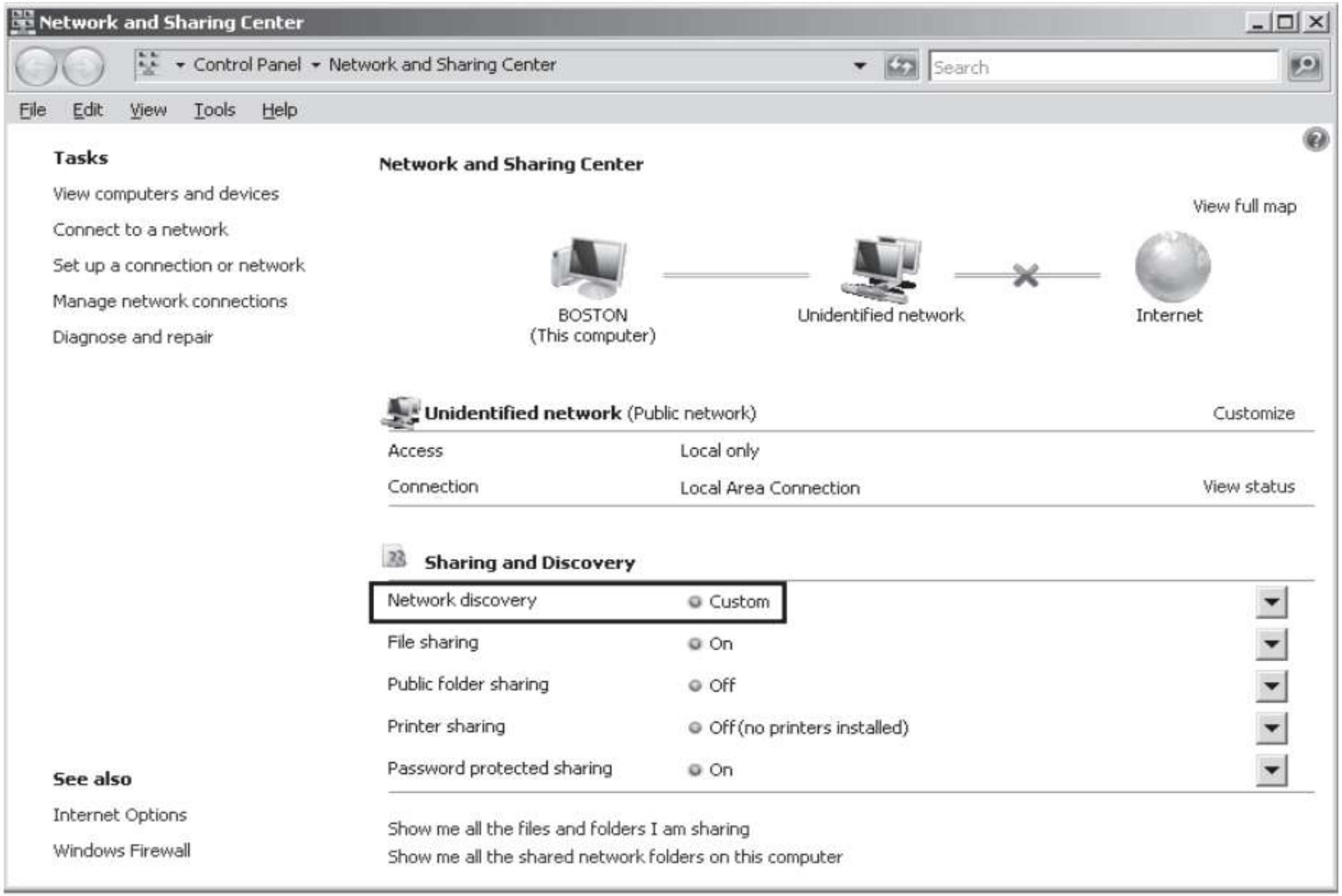
Name Resolution Basics

- DNS
  - Primary name resolution mechanism
  - Provides network-wide name resolution
- link- Local Multicast Name Resolution(LLMNR)
  - Used in Workgroups (not Domains)
  - Name Resolution on the local subnet only
  - Part of Network Discovery (must be turned on)
  - Windows Server 2008 and Vista only
  - Uses multicasting to resolve IPv6 addresses

Name Resolution Basics

- NetBIOS
  - Legacy protocol and naming system
  - Works by default on IPv4 Windows networks without DNS
- Windows Name Resolution Order
  - DNS
  - LLMNR
  - NetBIOS

What Is Link Local Multicast Name Resolution(LLMNR)?



Network and Sharing Center
Control Panel ▸ Network and Sharing Center
Search
File Edit View Tools Help

Tasks

View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair

Network and Sharing Center

View full map
BOSTON
(This computer)
Unidentified network
Internet

Unidentified network (Public network) Customize

Access	Local only	
Connection	Local Area Connection	View status

Sharing and Discovery

Network discovery	● Custom
File sharing	● On
Public folder sharing	● Off
Printer sharing	● Off (no printers installed)
Password protected sharing	● On

Show me all the files and folders I am sharing
Show me all the shared network folders on this computer

See also

Internet Options
Windows Firewall

What Is Link Local Multicast Name Resolution(LLMNR)?

- LLMNR uses multicasting to resolve IPv6 addresses to the names of computers found on the local subnet only.
- LLMNR is the name resolution method used for a single subnet that:
  - Has no DNS infrastructure
  - Contains computer running only Windows Vista or Windows Server 2008.
  - Has both IPv6 and Network Discovery enabled on its computers.

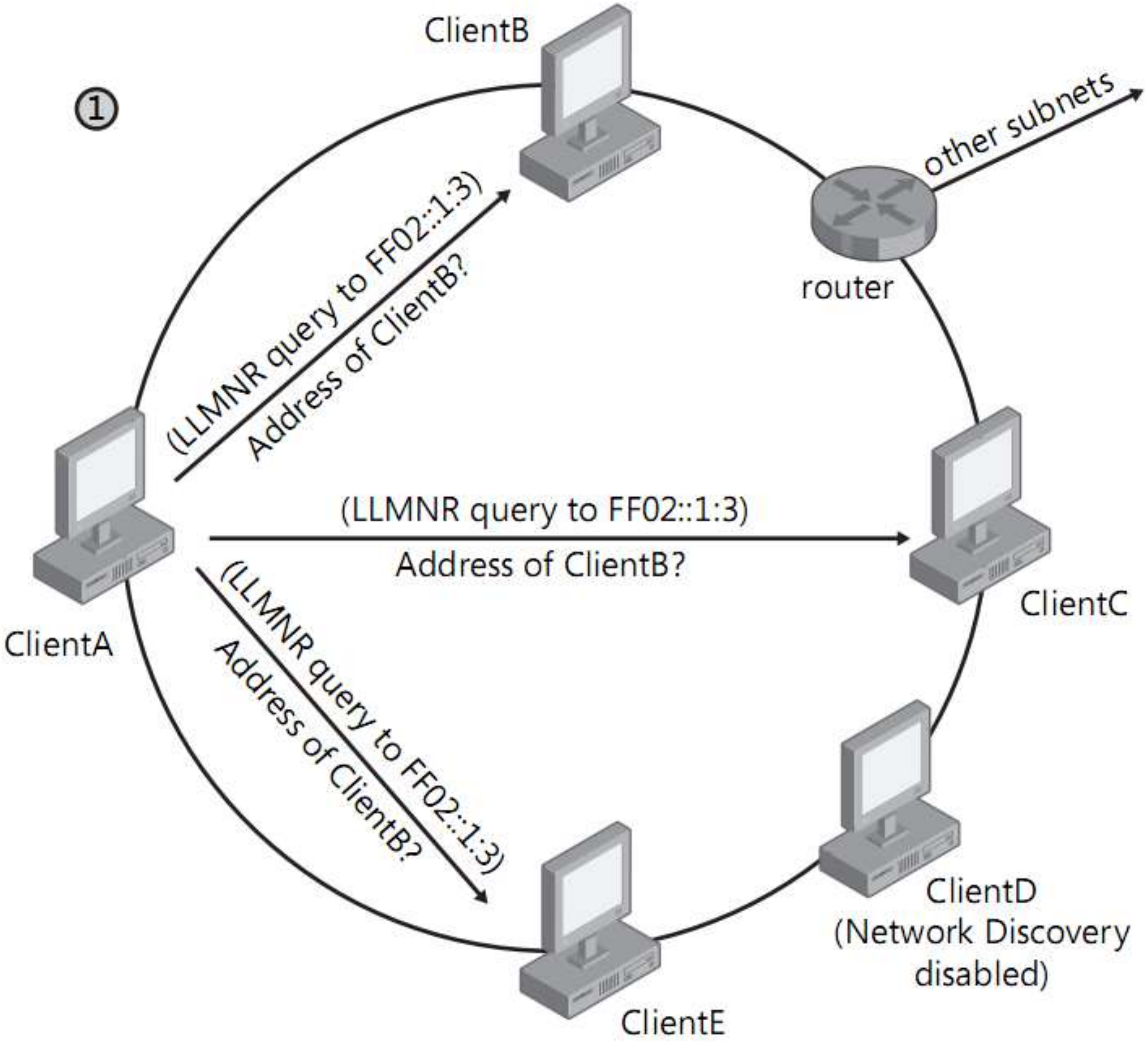
LLMNR Advantages

1. Requires no configuration to resolve computer names on the local subnet.
2. Unlike NetBIOS, it is compatible with IPv6.
3. Compared to NetBIOS, it is a much smaller service and therefore has a reduced attack surface.

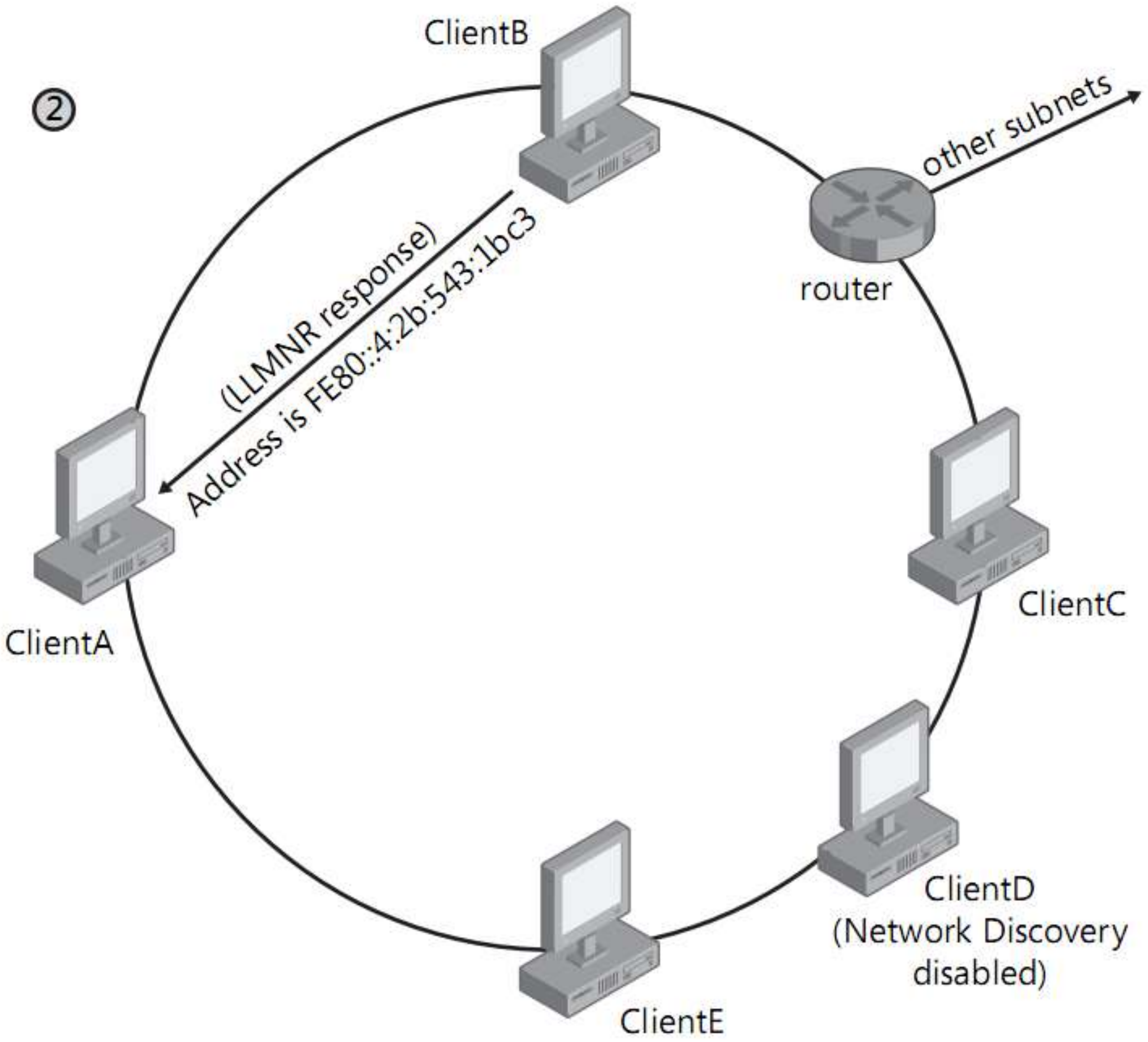
LLMNR Disadvantages

1. It Does not resolve the names of computers running Windows Server 2003, Windows XP.
2. LLMNR in practice does not enable connectivity to clients in a Windows IPv4-only network.
3. You have to enable Network Discovery on all computers in the subnet for the LLMNR to work
4. It can not be used to resolve the names of computers beyond the local subnet.

LLMNR resolves names query to an IPv6 multicast address



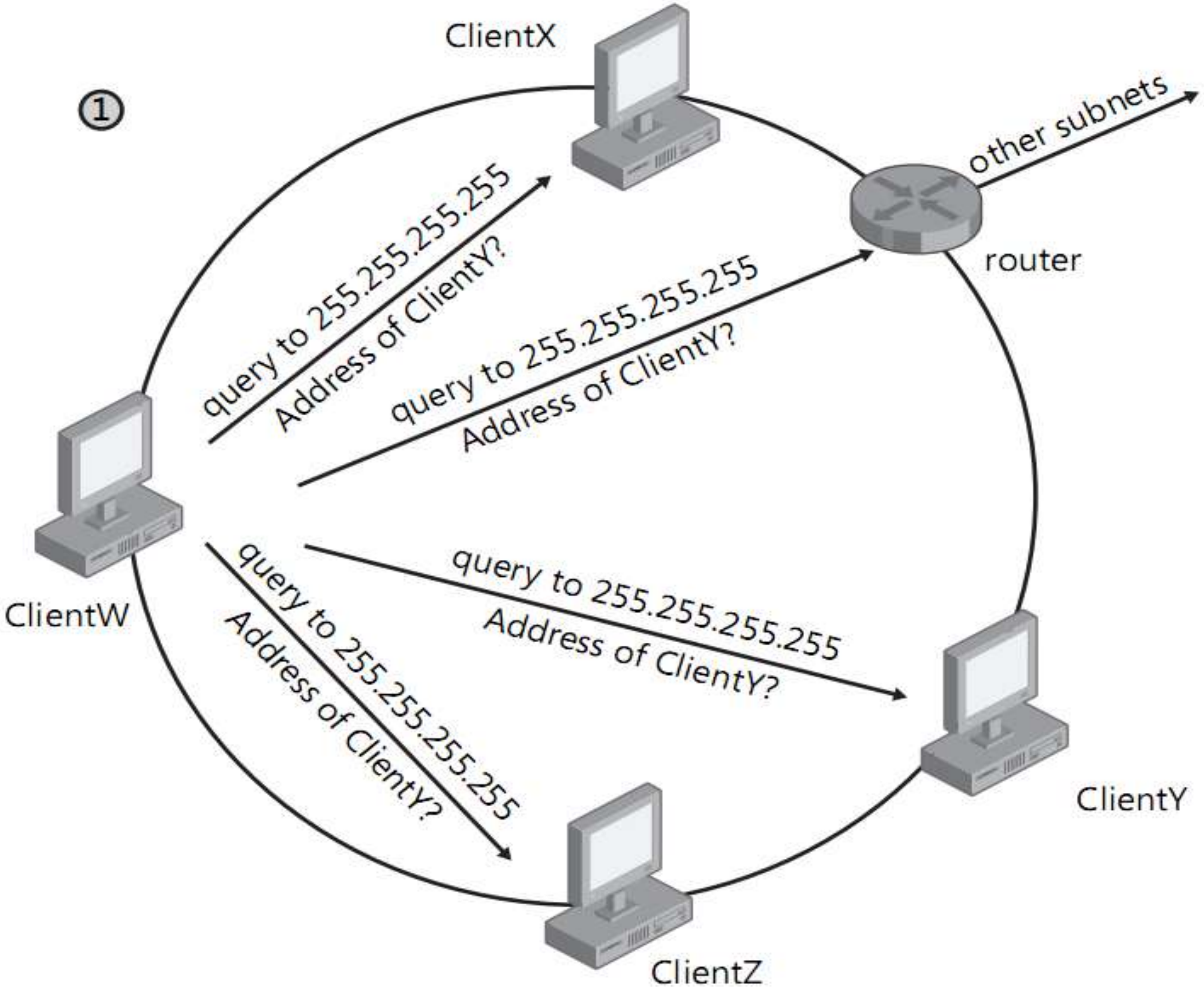
LLMNR resolves names query to an IPv6 multicast address



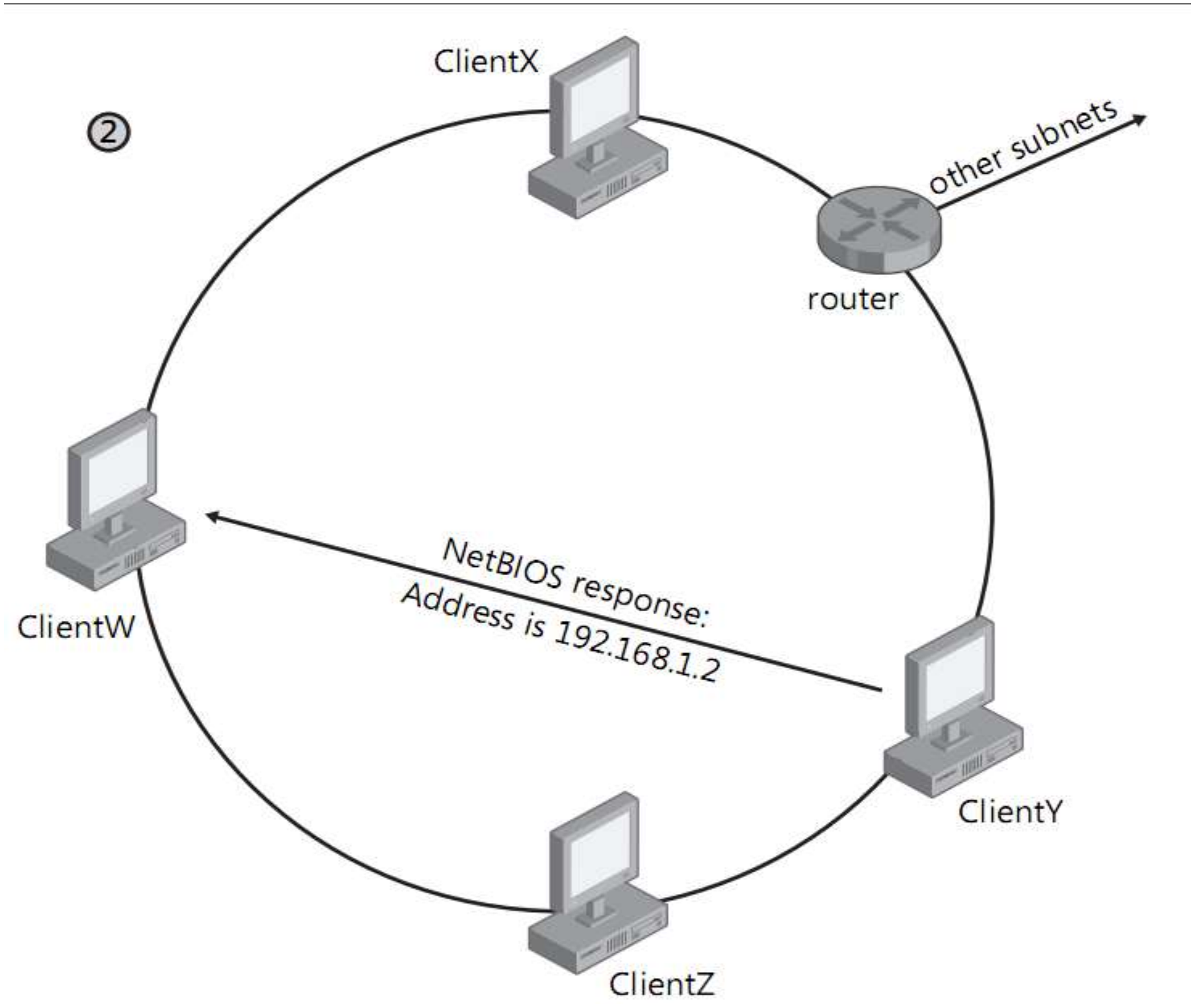
NetBIOS Name Resolution Methods

- NetBIOS includes three name resolution methods:
  - Broadcasts
  - WINS
  - The Lmhosts file.
- NetBIOS broadcasts:
  - the first name resolution mechanism enabled by NetBIOS is the use of NetBIOS broadcasts over IPv4.
  - Local area connections in Windows have NetBIOS enabled by default.

NetBIOS broadcasts, represent the only name resolution method enabled by default in Windows networks



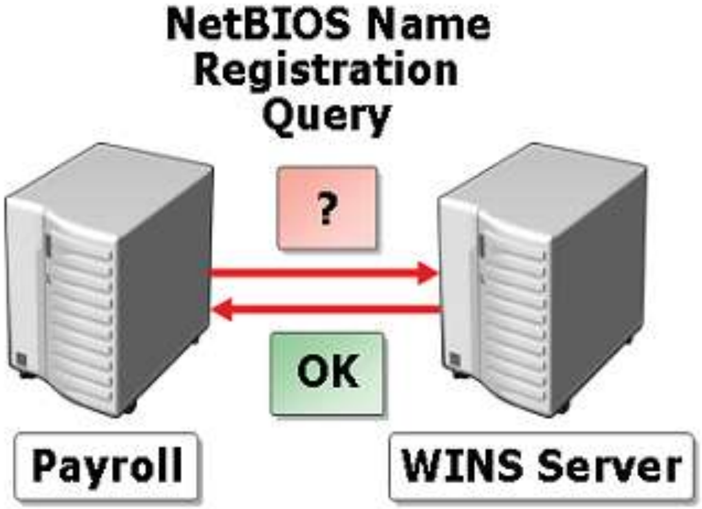
NetBIOS broadcasts, represent the only name resolution method enabled by default in Windows networks



NetBIOS Name Resolution Methods

- WINS:
  - A WINS server is essentially a directory of computer names
  - When you configure a network connection with the address of a WINS server, you perform two steps in one:
    - You enable the computer to look up computer names that can not be resolved by DNS or LLMNR.
    - You register the local computer's name in the directory of the WINS server
  - It enables NetBIOS name resolution beyond the local subnet.

What Is WINS?



1- queries a WINS server

2- determines whether name is in use

3- If not in use, then registers the NetBIOS name and associated IP address

NetBIOS Name Resolution Methods

- Lmhosts File:
  - The Lmhosts file is a static, local database file that is stored in the directory *%SystemRoot%\System32\Drivers\Etc* and that maps specific NetBIOS names to IP addresses.
  - Recording a NetBIOS name and its IP address in Lmhosts file enables a computer to resolve an IP address for the given NetBIOS name when every other name resolution method has failed.

NetBIOS Node Types

- The exact mechanism by which NetBIOS names are resolved to IP address depends on the NetBIOS node type that is configured for the computer.
- Four node types exist:
  - Broadcast or b-node:
    - Uses broadcast NetBIOS name queries for name registration and resolution.
    - B-node has two drawbacks:
      - Broadcasts disturb every node on the network.
      - Routers typically do not forward broadcast.

Exam Tip:

- Expect to see a question about node types on the 70-642 exam.

NetBIOS Node Types

- Point-to-point or p-node: this type
  - Uses point-to-point communications with a WINS server to resolve names.
  - P-node does not use broadcasts , instead, it queries the name server directly.
- Mixed or m-node:
  - Uses broadcasts first (b-node) and then uses WINS queries (p-node) if broadcast are not successful.
- Hybrid or h-node:
  - Uses WINS queries first (p-node) and then uses broadcasts (b-node) if the name server is unavailable or if the name is not registered in the WINS database.
  - To reduce IP broadcasts, these computers also use an Lmhosts file to search for name-to-IP address mapping before using B-node IP broadcasts.

NetBIOS Node Types

- By default, Windows clients are configured in hybrid or h-node.
- You can determine the current node status assigned to a windows computer by viewing the output of **Ipconfig/all**.

Advantages and Disadvantages of NetBIOS

- Advantages of NetBIOS:
  1. It resolves the names of neighboring computers by default and without requiring any user configuration
  2. It is enabled on all versions of Windows.
  3. It is easier to manage and configure than DNS.
  4. It works on familiar IPv4 hosts.
  5. It provides a useful backup method for resolving computers within broadcast range and in small networks.
- Disadvantages of NetBIOS:
  1. It is impractical for very large networks.
  2. Each computer name on the entire network has to be unique.
  3. It is not recommended for high-security areas.
  4. NetBIOS is not compatible with IPv6 networks.

Exam Tip:

- when you have multiple WINS server in a large organization, you must configure replication among them so that each WINS database remains up-to-date.
- In most cases, you want to configure *push-pull* replication among all WINS servers (often in a star configuration) so that they can efficiently and effectively update one another.

What Is DNS Name Resolution?

- DNS enables you to locate computers and other resources by name on an IP internetwork. By providing a hierarchical structure and an automated method of caching and resolving host names.

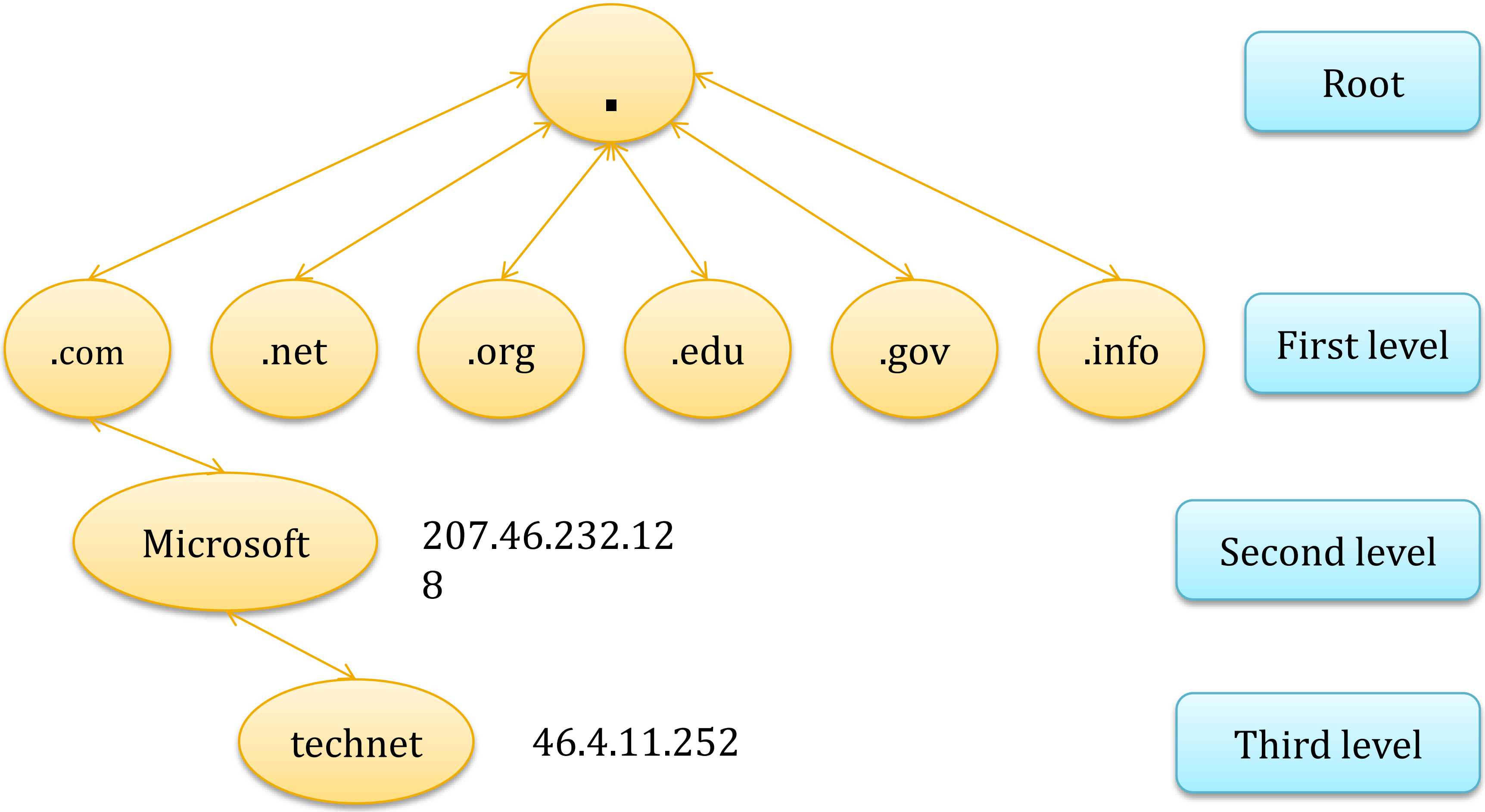
DNS Namespace:

- The naming system on which DNS is based is a hierarchical and logical tree structure called the DNS namespace.
- It has a unique root that can have any number of sub-domains.

DNS Basics

- www.207.46.232.128.com
- www.microsoft.com
- DNS
  - Domain Name System
  - Translates IP addresses into names

DNS Basics


.
.com
.net
.org
.edu
.gov
.info
Microsoft
technet
207.46.232.12
8
46.4.11.252
Root
First level
Second level
Third level

Domain Name:

- You can identify every node in the DNS domain tree by a *fully qualified domain name*, or FQDN.
    - FQDN is a DNS domain name that has been stated unambiguously to indicate its location relative to the root of the DNS domain tree.
- The DNS root (the top most level) of the Internet domain namespace is managed by the Internet Corporation for Assigned Names and Numbers (ICANN)
    - IP address numbers, and protocol parameter and port numbers.

What Is DNS Name Resolution?

- Beneath the root DNS domain lie the top-level domains. Three Types of top-level domains exist:
  - Organizational domains:
    - Named using a code that indicates the primary function or activity of the organizations contained within the DNS domain.
    - The best-known organizational domains are
      - .com, .net, .edu and .org.
  - Geographical domains:
    - Named using the two-character country and region codes established by the international Organization for Standardization(ISO).
  - Reverse domains:
    - These are special domains, named in-addr.arpa, that are used for IP address-to-name resolution.

Important:

- Top-level domains: for the most up-to-date information about these new top-level domains, consult
  - *http:// www.icann.org/tlds.*

What Is DNS Name Resolution?

- Private Domain Namespace:
  - A private namespace: a DNS namespace based on a private set of root servers independent of the Internet's DNS namespace.
  - Within a private namespace, you can name and create your own root .
  - Private names can not be seen or resolved on the Internet.

DNS Components

1. DNS servers.
2. DNS Zones.
3. DNS resolvers.
4. Resource Records.

DNS servers:

- A DNS server is a computer that runs a DNS server program
  - DNS service in Windows Server
  - Berkeley Internet Name Domain (BIND) in UNIX.
- Contain DNS database information about some portion of the DNS domain tree structure and resolve name resolution queries issued by DNS clients.
- When queried, DNS server can:
  1. Provide the requested information.
  2. Provide a pointer to another server that can help resolve the query.
  3. Respond that the information is unavailable or does not exist.
- A server is authoritative for a domain when that server relies on locally hosted database data in order to answer queries about host within a given domain.
- Server can be authoritative for one or more levels of the domain hierarchy.

DNS Zones:

- A DNS zone is a contiguous portion of namespace for which a server is authoritative.
- A server can be authoritative for one or more zones, and a zone can contain one or more contiguous domains.
- Zone files contain the data for the zones for which a server is authoritative.
- In many DNS server, zone data is stored in text files.
- DNS servers running on Active Directory domain controllers can also store zone information in Active Directory.

Note:

- what are forward and reverse lookup zones?
  - Zones can occur in one of two varieties:

1. Forward lookup zones.
2. Reverse lookup zones.

- A forward lookup zone is the main type of zone.

DNS resolvers:

- A DNS resolver is a server that uses the DNS protocol to query for information from DNS servers.
- DNS resolvers communicate with either remote DNS servers or the DNS servers or the DNS server program running on the local computer.
- In Windows server 2008, the function of the DNS resolver is performed by the DNS Client service.
- The DNS Client service provides the added function of caching DNS mappings.

Resource Records:

- Resource Records are DNS database entries that are used to answer DNS client queries.
- Each DNS server contains the resource records it needs to answer queries for its portion of the DNS namespace.
  - Such as IPv4 host address (A), IPv6 host address (AAAA, pronounced “quad-A”), alias (CNAME), pointer(PTR), and mail exchanger (MX).

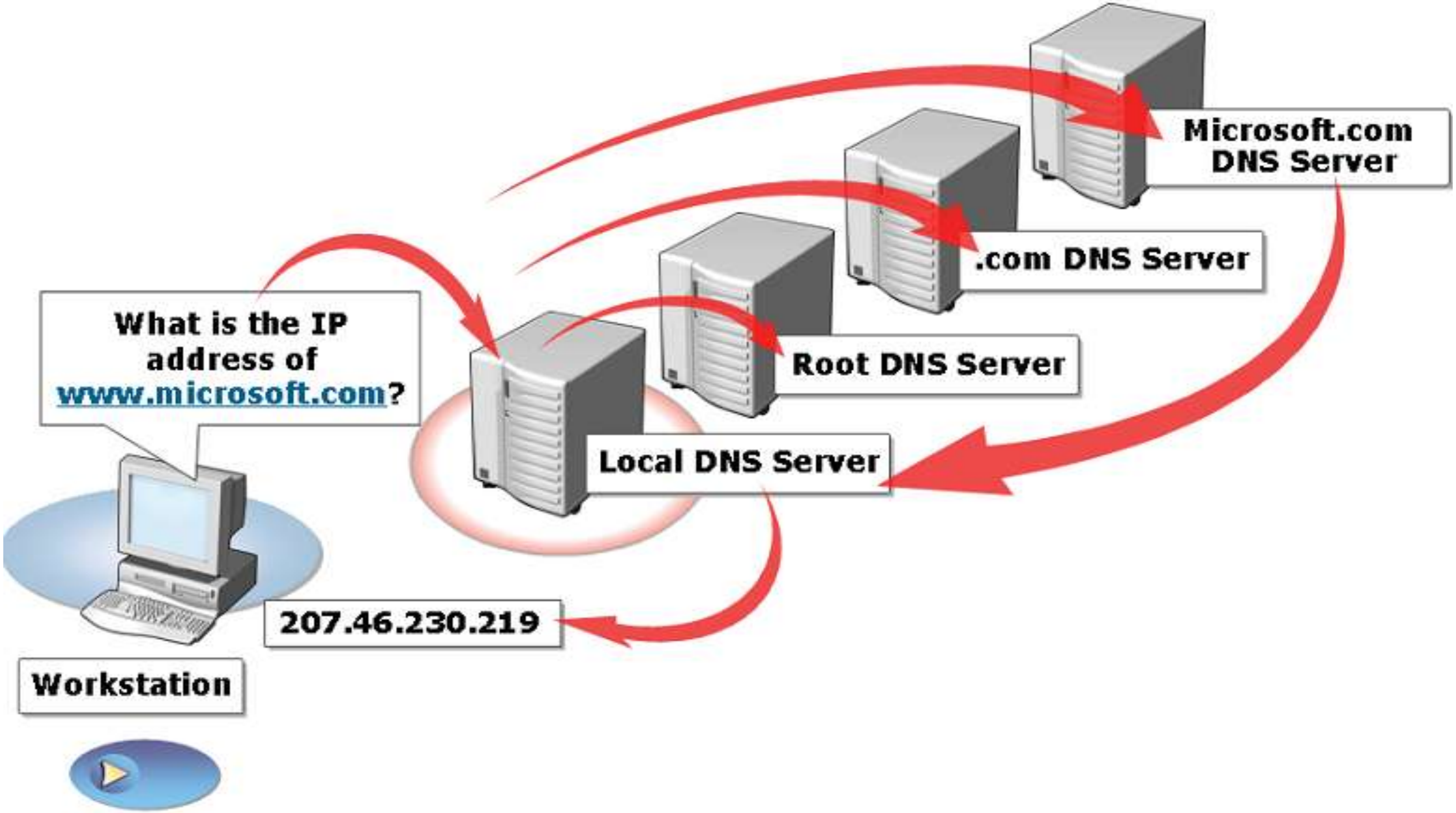
Understanding How a DNS Query Works:

- Each query message the client the client sends contains the following three pieces of information:
  - A DNS domain name, stated as an FQDN.
  - A specified query type, which can specify either a resource record by type or a specialized type of query operation.
  - A specified class for the DNS domain name.

Understanding How a DNS Query Works:

- DNS Resolution Methods:
  - DNS queries resolve in a number of different ways:
    - In a basic scenario
      - the DNS client contacts a DNS server , which then uses its own database of resource records to answer a query.
    - Recursion
      - a DNS server can query the other DNS server on behalf of the requesting client in order to resolve the FQDN. When the DNS server receives the answer to the query, it then sends an answer back to the client.
    - Iteration
      - the client itself attempts to contact additional DNS servers to resolve a name. A client typically performs iteration only when a DNS server has been specifically configured not to perform recursion.

How Internet DNS Names are Resolved

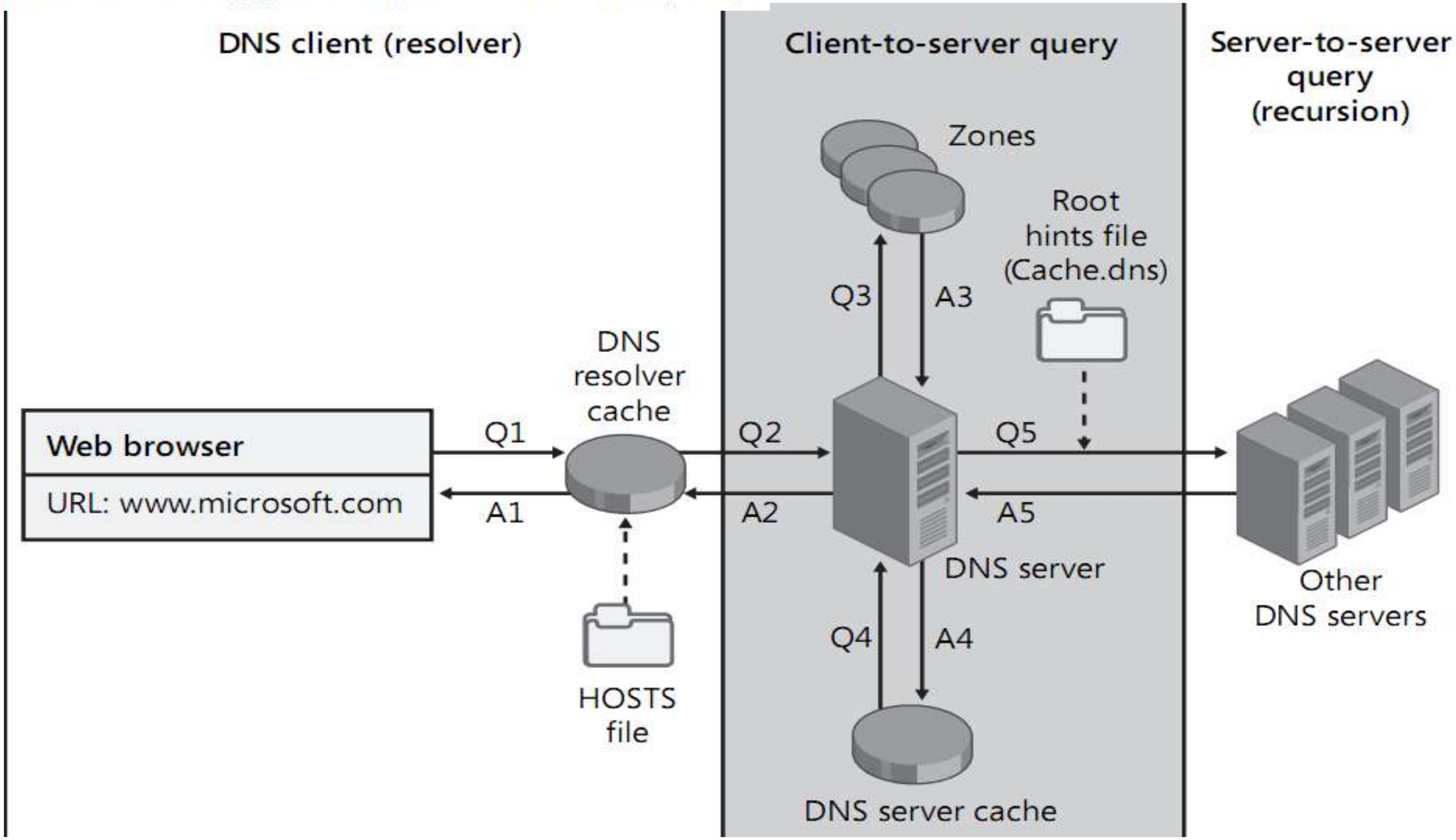


Understanding How a DNS Query Works:

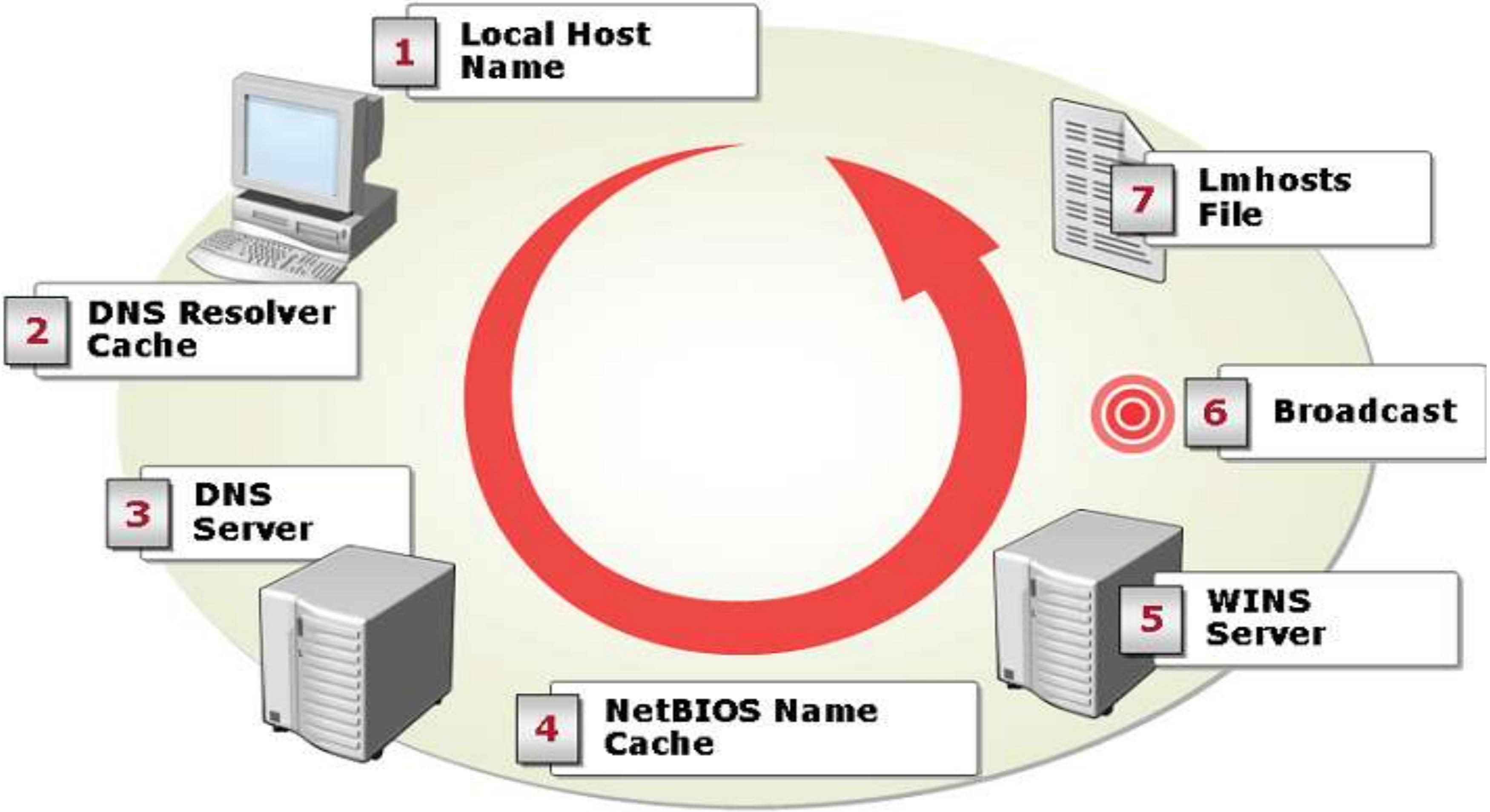
- DNS query steps:
  - The DNS query process occurs in two stages:
  - A name query begins at a client computer and is passed to the DNS Client service for resolution.
  - When the query cannot be resolved locally, the DNS Client service passes the query to a DNS server.

DNS query steps:

A possible chain of events triggered by a DNS name query



The Host Name Resolution Process



DNS query steps:

- Step 1: The Local Resolver:
  - if the DNS Client service cannot resolve the query from locally cached information.

DNS query steps:

- Step 1: The Local Resolver:
  - The local resolver cache can include name information obtained from two possible sources:
    - If a Hosts file is configured locally, any host-name-to-address mappings from that file are loaded into the cache when the DNS Client service it started and whenever the Hosts file is updated.
    - Resource records obtained in answered responses from previous DNS queries are added to the cache and kept for a period of a time.

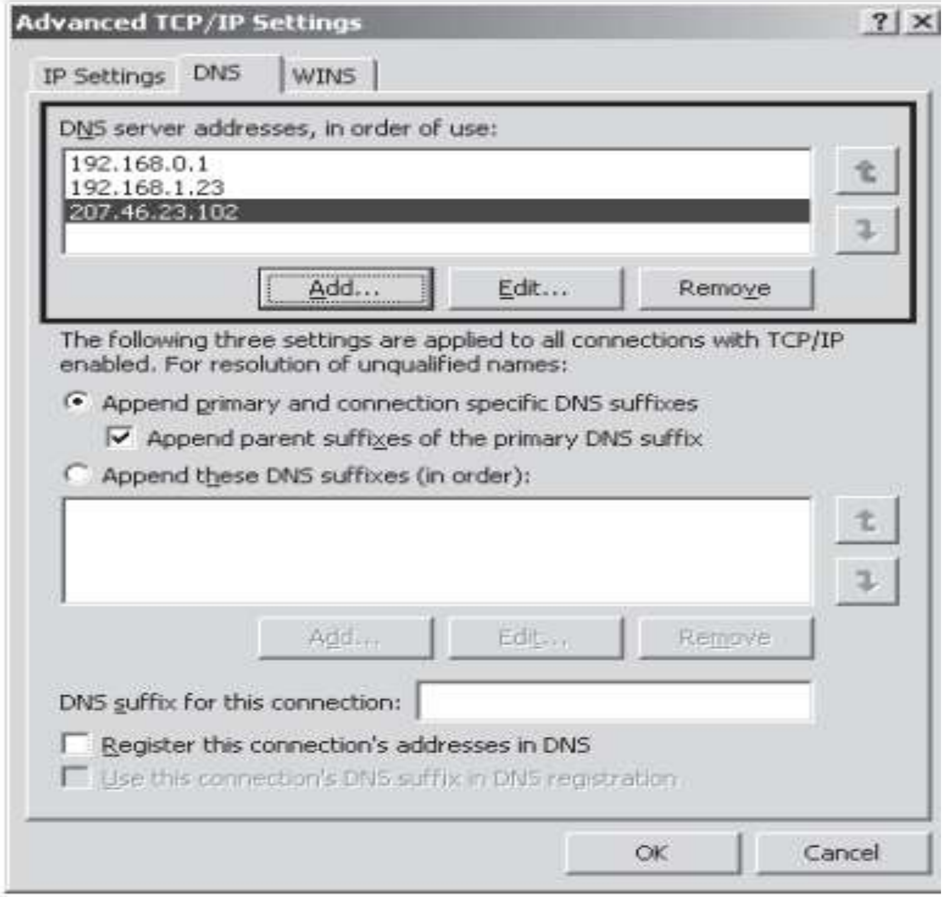
Quick check:

- If a computer needs to resolve a DNS name, what is the first method it attempts to use?
  - Quick check answer:
    - A computer first checks resolver cache to answer a query.

Step 2: Querying a DNS Server:

- The DNS Client service uses a server search list ordered by preference.
  - if the required name matches a corresponding resource record in local zone information, the server answers authoritatively, using this information to resolve the queried name.
  - If no zone information exists for the queried name, the server then checks to see whether it can resolve the name by using locally cached information from previous queries.

Step 2: Querying a DNS Server:



Advanced TCP/IP Settings

DNS server addresses, in order of use:

192.168.0.1
192.168.1.23
207.46.23.102

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

● Append primary and connection specific DNS suffixes

☑ Append parent suffixes of the primary DNS suffix

○ Append these DNS suffixes (in order):

DNS suffix for this connection:

□ Register this connection's addresses in DNS

□ Use this connection's DNS suffix in DNS registration

Preferred and alternate servers

Quick Check:

- If a DNS cannot resolve a query by using the first method, which method will it use next?
  - Quick check answer:
    - If a DNS server cannot resolve a query by using zone data, it attempts to answer the query by using cached information.

Understanding How a DNS Query Works:

- Understanding Recursion:
  - If the queried name does not find a matched answer at its preferred server-either from its cache or zone information-the query process continues in a manner dependent on the DNS server configuration.
    - Recursion in DNS refers to the process of a DNS server querying other DNS servers on behalf of an original querying client. This process, in effect, turns the original DNS server into a DNS client.
  - If recursion is disabled on the DNS server, the client itself performs iterative queries by using root hint referrals from the DNS server.
    - Iteration refers to the process of a DNS client making repeated queries to different DNS servers.

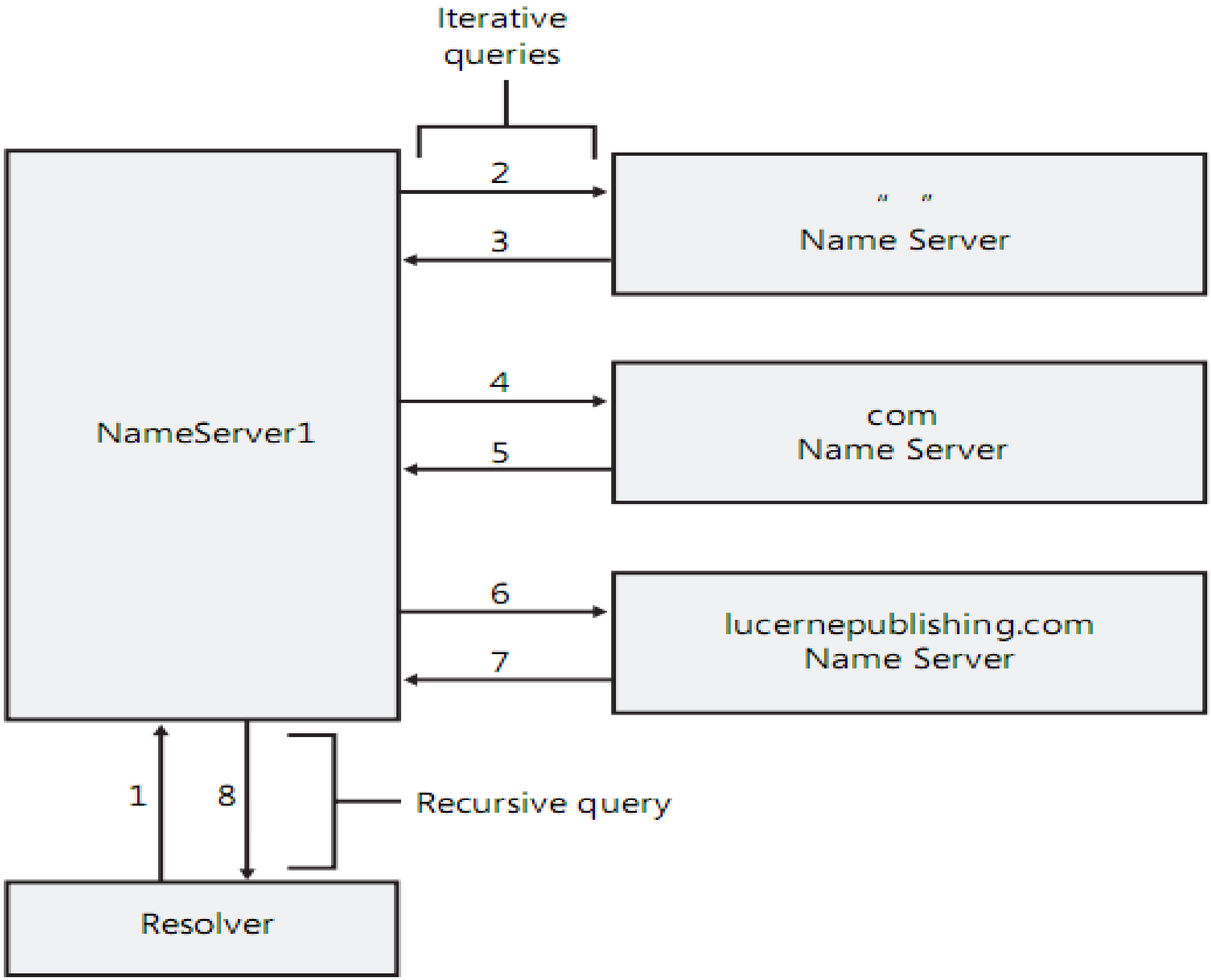
Understanding How a DNS Query Works:

- Root Hints:
  - A list of preliminary resource records used by the DNS service to locate servers authoritative for the root of the root of the DNS domain namespace tree.
  - By default, DNS servers running Windows Server 2008 use a preconfigured root hints file, Cache dns., that is stored in the WINDOWS\S system 32\Dns folder on the server computer.
  - The contents of this file are preloaded into server memory when the service is started and contain pointer information to root service for the DNS namespace .

Query example:

- A client somewhere on the Internet needs to resolve the name example. lucernepublishing.com to an IP address.

Query example:



Query example:

- When the DNS Client service on the client computer begins the query process, the following events tack place:
  1. The client contacts NameServer 1 with a query for example.lucernepublishing.com.
  2. NameServer checks and zones for the answers but does not find it, so it contacts a server authoritative for the Internet (that is a root server) with a query for example. lucernepublishing.com.
  3. The server at the root of the Internet does not know the answer, so it responds with a referral to a server authoritative for the .com domain.

Query example:

4. NameServer 1 contacts a server authoritative for the .com domain with a query for example. lucernepublishing.com.
5. The server authoritative for the .com domain does not know the exact answer, so it responds with a referral to a server authoritative for the.lucernepublishing.com domain.
6. NameServer 1 contacts a server authoritative for the lucernepublishing.com domain with a query for example.lucernepublishing.com.

Query example:

7. The server authoritative for the lucernepublishing.com domain does not know the answer. It responds with the requested IP address.
8. NameServer 1 responds to the client query with the IP address for example. lucernepublishing.com.

Quick Check:

- When would a DNS server contact a root server?
  - Quick Check answer:
    - A DNS server contacts a root server when it cannot answer a query with its own cached or authoritative data.

Quick Check:

- If a DNS server contacts a root server to resolve the name www.contoso.com and the root server cannot answer the query, how does the original server know which server to query next?
  - Quick Check answer:
    - The root server responds to the DNS server with a referral for the address of the DNS server authoritative for the ".com" domain. The DNS server then contacts this server for which it has received a referral.

Understanding How Caching Works:

  - Caching provides a way to improve DNS performance and to substantially reduce DNS-related query traffic on the network.
- DNS Client cache:
  - The DNS Client service starts, all-host-name-to-IP-address mappings contained in a static file named Hosts are preloaded into the DNS resolver cache.

Note: How is the Hosts file used?

- Whenever you add an entry to the Hosts file, that entry is immediately loaded into the DNS resolver cache.

Exam Tip:

- For the 70-642 exam, you need to know the difference between the Hosts file and the Lmhosts file.
  - The **Hosts** file helps resolve host names (essentially DNS names) to IP addresses
  - The **Lmhosts** file helps resolve NetBIOS names to IP addresses.

Types of Names That Computers Use

Name	Description
Host Names	•Up to 255 characters in length •Can contain alphabetic and numeric characters, periods, and hyphens •Part of FQDN
NetBIOS Names	•Represent a single computer or group of computers •15 characters used for the name •16th character identifies service •Flat namespace

Understanding How Caching Works:

- DNS server cache:
  - As DNS server make recursive queries on behalf of clients, they temporarily cache resourced records.
  - When other clients place new queries that request information matching cached resource records, the DNS server can use the cached information to answer these queries.
    - The DNS server cache is cleared whenever the DNS Server service is stopped.
    - You can clear the DNS server cache manually in the DNS consul.
    - You can clear the server cache at the command line by typing the command Dnscmd /clearcache at a command prompt.
  - Time to Live Values:
    - A Time to Live (TTL) value applies to all cached resource records, whether in the DNS resolver cache or the DNS server cache.
    - By default, the TTL is 3600 seconds (1 hour).

Contact Me: qursaan@gmail.com

Any Question?