Chapter II
TCP/IP Infrastructure: WINS

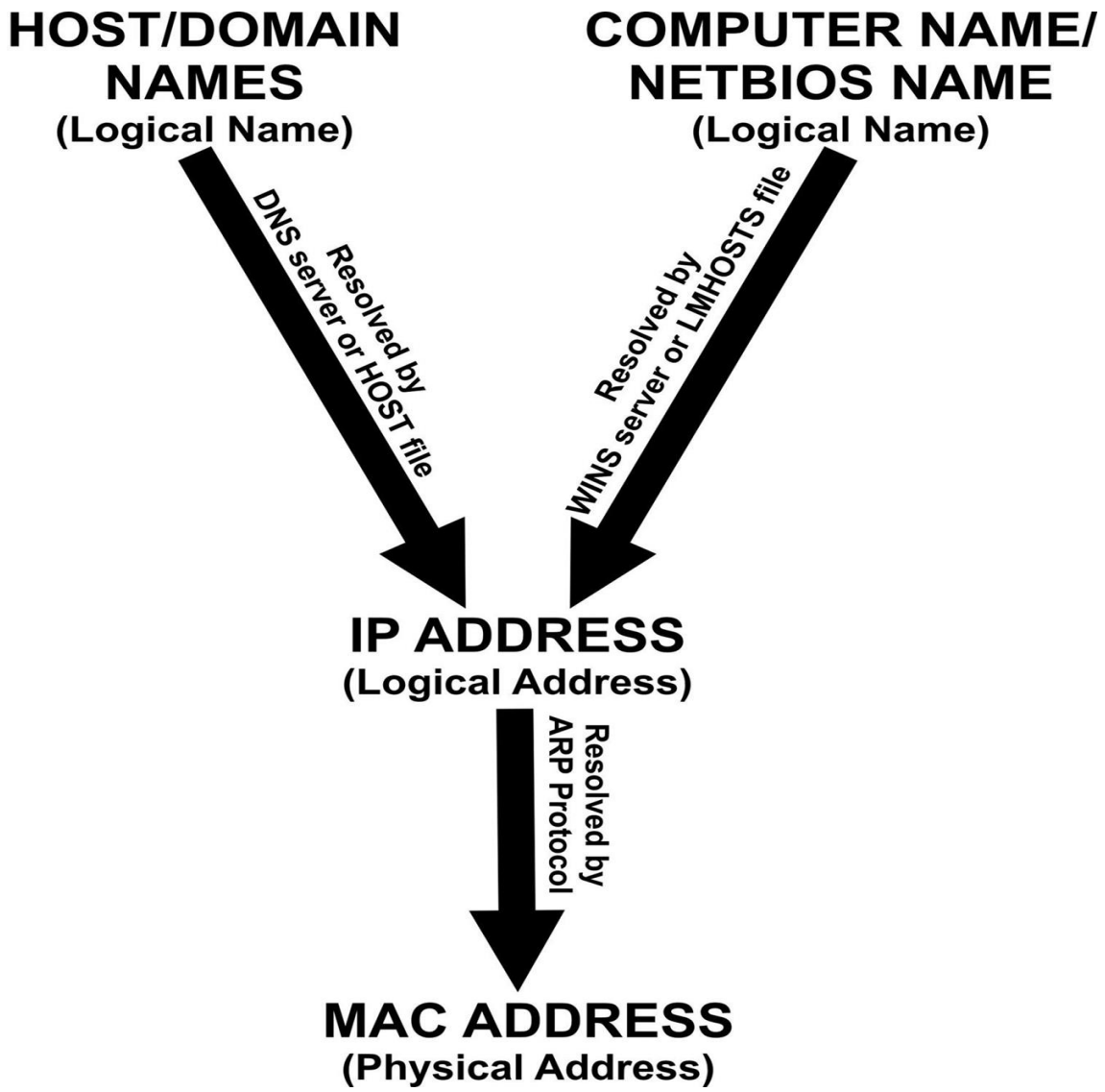
General background information

- **NetBIOS Names**
  - NetBIOS names are used to identify and locate computers and other shared or grouped resources needed to register or resolve names for use on the network
  - NetBIOS names are 16 characters in length
  - Microsoft networking components allow the first 15 characters of a NetBIOS name to be specified by the user or administrator, but reserve the 16th character (the suffix) of the NetBIOS name (00-FF hex) to indicate a resource type
  - NetBIOS names can be registered as unique or as group names. Unique names have one address associated with a name. Group names have more than one address mapped to a name.

NetBIOS Name Resolution

- **NetBIOS-Based Networks**
  - NetBIOS is responsible for establishing logical names on the network, establishing sessions between two logical names on the network, and supporting reliable data transfer between computers that have established a session
  - NetBIOS over TCP/IP is called NetBT
  - Name resolution in a NetBIOS network has traditionally been broadcast-based (there are several disadvantages to a broadcast-based name resolution system)

Name and Address Resolution Done on an IP Network



NetBIOS Name Resolution (continued)

- Microsoft clients use the following four methods to resolve NetBIOS names
  - NetBIOS name cache
  - LMHOSTS
  - Windows Internet Naming Service (WINS)
  - Broadcast

NetBIOS Name Cache

- Client computers use the NetBIOS name cache to speed up the name resolution process
- A reduction in network traffic occurs because if the current NetBIOS name being resolved has a record in the cache, its IP address in the cache is used and no further resolution is performed

LMHOSTS

- The LMHOSTS file was introduced to assist with remote NetBIOS name resolution
- Despite the many uses of the LMHOSTS file, there are some limitations to its design. Its greatest limitation is that it is a static file
- This limitation of the LMHOSTS file has been exacerbated by the introduction of the Dynamic Host Configuration Protocol (DHCP)

LMHOSTS

- The LMHOSTS file is a static text file located on the workstation
- The file contains a list of NetBIOS names and their associated IP addresses
- If no other method is successful, Windows clients parse an LMHOSTS file to find the NetBIOS name
- The most common use of LMHOSTS files is to test NetBIOS name resolution

Sample LMHOSTS File Works with WINS server.

```
102.54.94.97    rhino       #PRE  #DOM:networking #File Server
182.102.93.122 MISSERVER    #PRE                  #MIS Server
122.107.9.10    SalesServer                       #Sales Server
131.107.7.29    DBServer                          #Database Server
191.131.54.73   TrainServ                         #Training Server
```

LMHOSTS File

- The lmhosts file is in %Systemroot%\ System32 \Drivers\etc\lmhosts.sam.
- If entries in this file contain the entry "#PRE", the value of that line is loaded into the NetBIOS name cache memory and broadcasts will not be used to resolve these host name to IP addresses.
- When TCP/IP is initialized, the lines with #PRE are loaded into memory. The #PRE entry lines should be near the bottom of the file.

- #INCLUDE statements may be used to embedded one lmhosts file locally or on a remote computer into the main lmhosts file. Shared lmhosts must be accessable to all users. Regedit32 can be used to make a share accessible to a null user. The names of the shares can be added to the following registry entry:
  - \HKey_Local_Machine\System\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionShares

- The NBSTAT - R command could be used from a login script to load the additional remote lmhosts file(s). LMHOSTS file keywords:
  - #BEGIN_ALTERNATE and #END_ALTERNATE - Alternate locations for lmhosts files. Subsequent entries are only checked if the initial computers are not available.
  - #DOM domain name - Indicates that this machine is a domain controller. This prevents a broadcast from being sent to find the domain controller when changing a password or a user is logging onto a domain.
  - #NOFNR - No NetBIOS name queries for older LAN MANAGER based computers.
  - #INCLUDE - Used to embed one lmhosts file locally or on a remote computer into the main lmhosts file.
  - #MH - Multiple entries for a computer with multiple network cards or addresses.
  - #PRE - Preload the line information into memory(NetBIOS name cache).

- Example:
  - 192.168.20.33 Machine1
  - 192.168.20.45 Machine2
  - 192.168.20.3 Server1 #PRE 192.168.20.4 Server2 #PRE #DOM: MYDOMAIN

  - #INCLUDE \\ourserver\public\lmhosts
  - #INCLUDE \\nextserver\public\lmhosts

  - #BEGIN_ALTERNATE #INCLUDE \\mainserver\public\lmhosts
  - #INCLUDE \\backupserver\public\lmhosts
  - #END_ALTERNATE
- The benefits of using #PRE and #DOM in the LMHOSTS file allow non-WINS clients to do:
  - Registration
  - User account verification
  - Password changing
- The #PRE entry prevents broadcasts from being made to access the host. The #DOM entry supports:
  - Domain validation
  - Account synchronization
  - Browsing

WINS

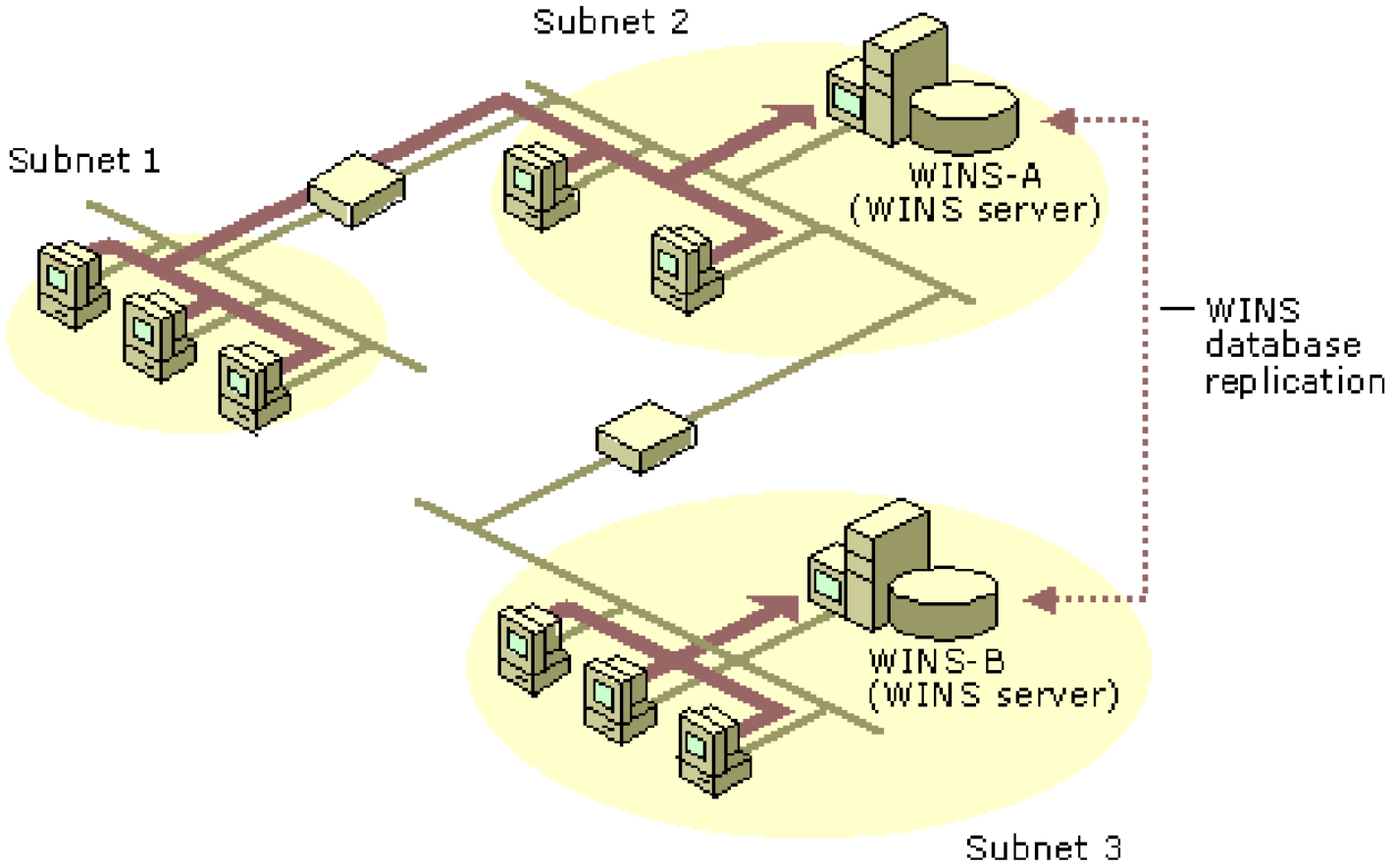
- A WINS server is used to resolve NetBIOS names
- A WINS server is a central repository of NetBIOS name information on the network
- The advantages of WINS over other NetBIOS name resolution methods are:
  - It functions across routers
  - It can be dynamically updated
  - It can be automated
  - It offers client configuration through DHCP
  - It offers integration with DNS

Windows Internet Name Service (WINS)

- WINS provides a distributed database for registering and querying dynamic NetBIOS names to IP address mapping in a routed network environment
- WINS is the best choice for NetBIOS name resolution in routed networks that use NetBIOS over TCP/IP (NetBT)
- However, data will not be replicated between the WINS server and the non-WINS NBNS (NetBIOS Name Servers). Therefore the WINS system as a whole will not converge and name resolution will not be guaranteed.

WINS components

- WINS consists of two main components, the WINS server and WINS clients.



WINS servers

- Handles name registration/release requests from WINS clients and registers/releases their names and IP addresses.
- Responds to name queries from WINS clients by returning the IP address of the name being queried (assuming the name is registered with the WINS server).
- Replicates the WINS database with other WINS servers.

WINS clients

- Registers/releases its name with the WINS server when it joins/leaves the network.
- Queries the WINS server for remote name resolution
- Each WINS Client can be one of four node type: B-node, P-node, M-node and H-node

WINS Client Node Type

Table 6-1 NetBIOS node types

Registry Value	Node Type	Description
1	B-node	When configured as a broadcast node, a computer uses only the NetBIOS name cache, broadcasts, and LMHOSTS to resolve NetBIOS names. WINS is not used. This is also referred to as Microsoft enhanced b-node because of the inclusion of LMHOSTS. RFC 1001, which defines concepts and methods for NetBIOS over TCP/IP, does not include LMHOSTS files. This is the default configuration when a WINS server is not configured.
2	P-node	When configured as a peer-to-peer node, a computer uses NetBIOS name cache, WINS, and LMHOSTS to resolve NetBIOS names. Broadcasts are not used.
4	M-node	When configured as a mixed node, a computer attempts to use broadcasts before using a WINS server.
8	H-node	When configured as a hybrid node, a computer attempts to use a WINS server before broadcasts. This is the default configuration when a WINS server is configured.

Benefits of Using WINS

- Dynamic database maintenance to support computer name registration and resolution.
- Centralized management of NetBIOS name database.
- Reduction of IP broadcast traffic in the Internetwork, while allowing the clients to locate remote systems easily across local or wide-area networks.

Broadcast

- If WINS has not been installed on the network or the client has been incorrectly configured, WINS cannot resolve the NetBIOS name → In such a case, a broadcast is sent on the network
- The computer using the NetBIOS name being resolved receives the request and then responds with its IP address

Designing a WINS Infrastructure

You need to consider following:

- Fault tolerance
- Duplicate replication traffic
- Server size
  - *Database size*
  - *Server Performance*

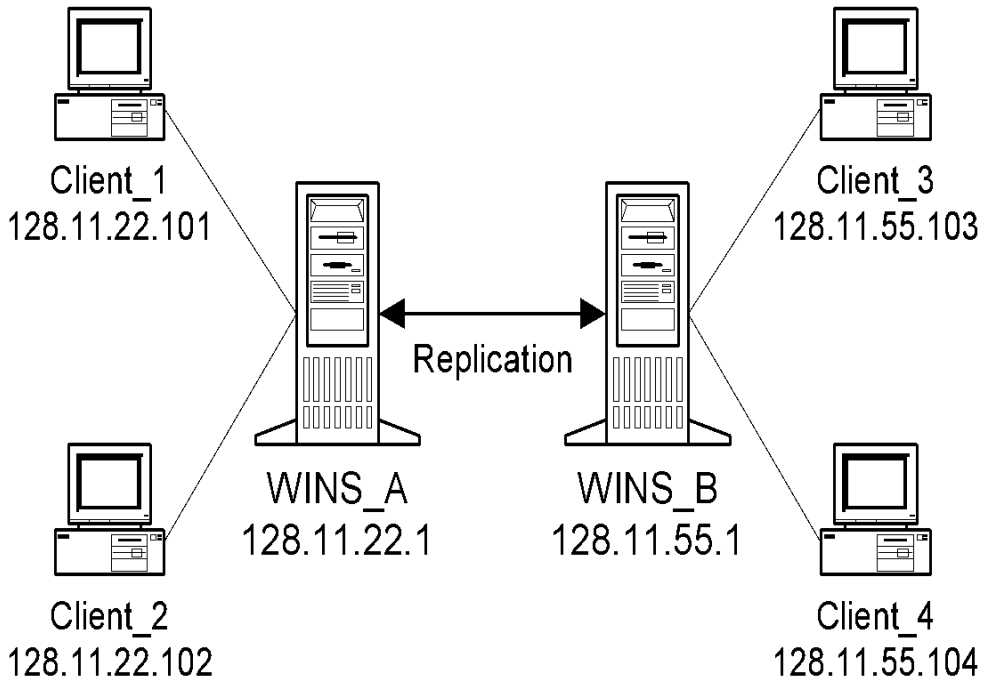
Multiple WINS Server and Replication

- Multiple WINS servers increase availability and balance the load among servers
- If a node has registered a name-to-address mapping with one WINS server, that mapping must be available reliably from any WINS server. This is accomplished through replication of the WINS databases among WINS servers
- Replication of registered names to all WINS servers is necessary to allow resolution of names registered to different servers
- Replication is carried out among partners, rather than each server replicating to all other servers

Replication

- Each WINS server must be configured with at least one other WINS server as a replication partner. This ensures that a name registered with one WINS server is eventually replicated to all other WINS servers
- A replication partner can be a ***pull*** or a ***push partner****.*
- A pull partner is a WINS server that requests new WINS database entries (replicas) from its partner
- A push partner is a WINS server that sends update notification messages. When replication is configured between two WINS servers, it is recommended that both servers be push and pull partners of the other

Replication Example



The database tables for WINS_A and WINS_B on August 20, 2010. All four clients were powered on this morning between 8:00 AM and 8:15 AM. Client_2 has just been shut down.

The following parameters are set in WINS_A and WINS_B:

- **WINS_A and WINS_B are push/pull partners to each other**
- **The Replication Interval is 30 minutes**
- **The Renewal Interval is 4 days**
- **The Extinction Interval is 4 days**
- **The Extinction Time-out is 1 day**
- **The Verify Interval is 24 days**

Replication Example

Before replication, WINS_A has the following two entries:

Name	Address	Flags	Owner	Version ID	Time Stamp
Client_1	128.11.22.101	unique,active,h-node,dynamic	WINS_A	4B3	1/5/01 8:05:32 AM
Client_2	128.11.22.102	unique,released,h-node,dynamic	WINS_A	4C2	1/5/01 8:23:43

WINS_B has the following two entries:

Name	Address	Flags	Owner	Version ID	Time Stamp
Client_3	128.11.55.103	unique,active,h-node,dynamic	WINS_B	78F	1/5/01 8:11:12 AM
Client_4	128.11.55.104	unique, active,h-node,dynamic	WINS_B	79C	1/5/01 8:12:21 AM

Replication takes place at 8:30:45 by WINS_A's clock. After replication, the WINS_A database will look like the following:

Name	Address	Flags	Owner	Version ID	Time Stamp
Client_1	128.11.22.101	unique,active,h-node,dynamic	WINS_A	4B3	1/5/01 8:05:32 AM
Client_2	128.11.22.102	unique,released,h-node,dynamic	WINS_A	4C2	1/5/01 8:23:43 AM
Client_3	128.11.55.103	unique,active,h-node,dynamic	WINS_B	78F	1/25/01 8:30:45 AM
Client_4	128.11.55.104	unique, active,h-node,dynamic	WINS_B	79C	1/25/01 8:30:45 AM