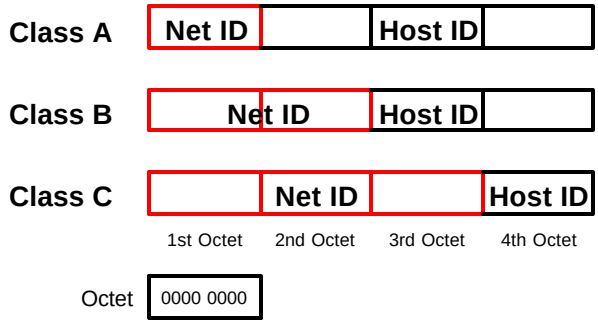
TCI/IP

Chapter 1. IP Addresses, Subnet Masks, & Subnetting

An IP address is used for Network Layer identification of hosts and routers on a TCP/IP network. The address consists of a 32-bit binary number of 4 octets and is usually displayed in the decimal format 100.100.100.100, which is called dotted decimal notation.

The class of the Network is determined by the high order bits

Class	1st Octet Range	High Order Bits
A	1~127	000.000.000
B	128~191	100.000.000
C	192~223	110.000.000.000



1. The network ID 127.x.y.z is a reserved address used for the local loopback and self-diagnostic.
2. A Network and host ID cannot be all binary 1's (decimal 255). If all bits are set to 1's, this is interpreted as a broadcast.
3. A Network and host ID cannot be all binary 0's. If all bits are set to 0's, this is interpreted as a network ID.
4. The high order bits of 1110 (224.0.0.0 to 239.255.255.255) Class D is used for multicasting technologies and the high order bits of 11110 (240.0.0.0 to 247.255.255.255) Class E are reserved for future use.

AND Boolean table

Bit 1	Bit 2	Result
1	1	1
1	0	0
0	1	0
0	0	0

And IP address and Subnet Masks

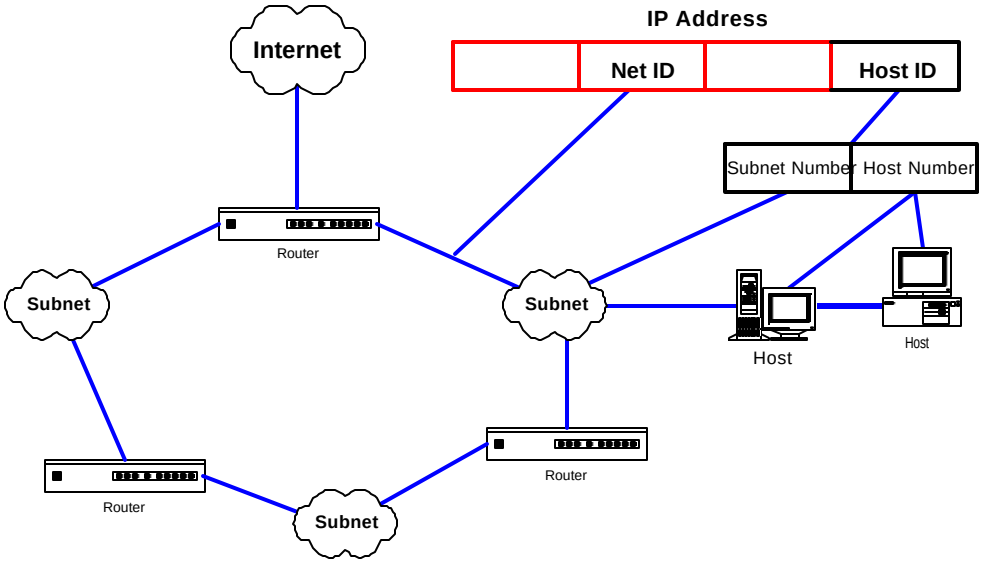
198.53.147.45	11000110	00110101	10010011	00101101
255.255.255.0	11111111	11111111	11111111	00000000
Result	11000110	00110101	10010011	00000000

The higher order bits of 198.53.147.45 are 110 thus this is a class C address. The Host ID of this Class C address 198.53.147.0 is 45. From the example above it is visible that with this subnet mask the net ID and host ID remained unchanged after the AND calculation.

1-1 Define a Subnet Mask

Subnetting is a technique that allows the network administrator to divide a network into smaller networks by using the same network number assignment. The advantages of subnetting are below:

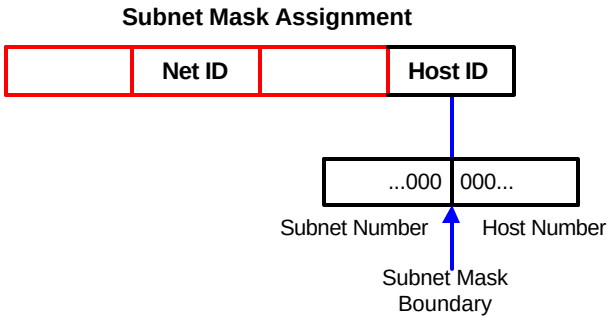
1. Simplified administration: With the help of routers networks can be broken up into smaller subnets that can managed more independently and efficiently.
2. Restructuring of the internal network without affecting external networks: A organization can continue to use it's allocated IP addresses without having to obtain additional IP blocks.
3. Improved security: Subnetting will allow an organization to separate internal networks on the internetwork but will not be visible to external networks.
4. Isolation of network traffic - With the help of routers and subnetting, network traffic can be kept to a minimum.



In the diagram above illustrates how a subnetted IP appears on an internal Intra-Net and the Internet. The Internet only reads the Net ID and the routers on the Internet are only concerned with routing the IP packet to the Intra-Net external router. When the IP packet reaches the external router, which has been configured for subnet routing reads the HostId. The router then forwards the packet to appropriate subnet where it is delivered to the host.

1-2 Determining the Subnet Mask to Use

The diagram below shows that when subnetting an IP address the Net ID remains unchanged but the Host ID is further sectioned or divided up.



1-3 Current Classfull Standard

There a number of different ways to define the available range of IP addresses. The MCSE exams use the existing Classful standard. Some network equipment may follow a more current addressing scheme called CIDR. To date, CIDR has not been adopted as the standard."

Just for reference, MS stacks do not adhere to the Classful standard. They will allow you to use all subnets, including the first and last. For example, look at the KB article, Q139983 "Class C Subnetting Options for RAS Routing"

The Current Classfull Standard rules are as follows.

1. The original Network ID (defined by the default class mask)
2. The Subnet ID (defined by any bits beyond the default class mask)
3. The Host ID

Example

Class B address with a subnet of 255.255.240.0

11111111.11111111. 1111 0000.00000000

Network ID Subnet ID Host ID

Bit Pattern	Masked Bits	Provided Subnets	Subnet Mask
11000000	2	2	192
11100000	3	6	224
11110000	4	14	240
11111000	5	30	248
11111100	6	62	252
11111110	7	126	254
11111111	8	254	255

The above chart represents how a subnet mask is represented in binary format, to determine the values is quite simple.

1. Determine the number of Physical segments required in your network and covert to binary format. In the example below 6 segments are required.
2. Count the number of bits required to represent the number of physical segments in binary. With 6 required subnets (Binary value is 110). Representing 6 in binary requires 3 bits .
3. Convert the required number of bits to decimal format in high order (left to right).
4. Configure the 3 required bits as the first bits of the host id. The decimal value for binary 11100000 is 224. Representing a subnet mask of 255.255.255.224.

Example of a Class C Subnet

Number of Subnet 6

Binary Value 000000110

Convert to Decimal	**11111111**	**11111111**	**11111111**	**11100000**
Subnet Mask	**255**	**255**	**255**	**224**
198.53.147.45	**11000110**	**00110101**	**10010011**	**00101101**
255.255.255.224	**11111111**	**11111111**	**11111111**	**11100000**
	11000110	**00110101**	**10010011**	**00100000**
	198	**53**	**147**	**32**

Host address range
198.53.147.33 to 198.53.147.62

00100000
6 Subnets **30 Hosts**

Question: What happened to 198.53.147.32 and 198.53.147.63 why can't these be IP addresses ?

198.53.147.32 - Is the subnet's Network ID which is reserved for the physical segment (00100000).
198.53.147.63 - Is the subnet's Broadcast Address (00111111)

As stated above every network or subnet has a IP address for the Physical segment and a Broadcast Address.

1-4 Calculating Hosts

Bit Pattern	Masked Bits	Provided Subnets	Subnet Mask	Class A Host/Subnet	Class B Host/Subnet	Class C Host/Subnet
11000000	2	2	192	4,194,301	16,382	62
11100000	3	6	224	2,097,150	8,190	30
11110000	4	14	240	1,048,574	4,096	14
11111000	5	30	248	524,286	2,046	6
11111100	6	62	252	262,142	1,022	2
11111110	7	126	254	131,070	510	0
11111111	8	254	255	65,534	254	0

Question: I want to set up a TCP/IP LAN in my organization what IP addresses should I use?

For hosts that need to be connected to the Internet you can get a block of valid IP addresses from an ISP. Larger Organizations or ISP's can get IP blocks from the American Registry for Internet Numbers (http://www.arin.net/).

The following IP address ranges have been set aside for Internal use. These IP's are will not be routable on the Internet.

Class A: 10.xx.xx.xx
Addresses: 10.0.0.1 to 10.255.255.254

Class B: 172.16.xx.xx - 172.32.xx.xx
Addresses: 172.16.0.1 to 172.31.255.254

Class C: 192.168.xx.xx
Addresses: 192.168.0.1 to 192.168.255.254

1-5 Command Line Utilities

Arp- Arp.exe is used to resolve an IP address to its hardware (MAC address). Local Arp cache is checked first before initiating an ARP request broadcast.

Switches
-a - View the contents of the local ARP cache table.
-s - Add a static Arp entry for frequent accessed hosts.
-d - Delete a entry.

ipconfig- The ipconfig is a command line tool for NT that shows how the computer's IP stack is configured.

C:\ipconfig

Windows NT IP Configuration:

Ethernet adapter E100B1:

IP Address ….....:198.133.234.23
Subnet Mask ….....:255.255.255.0
Default Gateway.....:198.133.234.2

Switches
/all - Extra information is revealed; IP host name, DNS, WINS server.
/release - If DHCP is enabled, you release the lease with this switch.
/renew - The renew switch will update and renew DHCP lease information from the DHCP server.

netstat- The netstat tool displays protocol statistics and the state of current TCP/IP connections.

C:\WINDOWS>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

-a Displays all connections and listening ports.
-e Displays Ethernet statistics. This may be combined with the -s option.
-n Displays addresses and port numbers in numerical form.

-p proto Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, or IP.
-r Displays the routing table.
-s Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.
interval Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

nbtstat- The nbtstat checks the state of NetBIOS over TCP/IP connections and returns NetBIOS session and name resolution statistics. This tool can also be used to update the local NetBIOS name cache.

Displays protocol statistics and current TCP/IP connections using NBT(NetBIOS over TCP/IP).
NBTSTAT [-a RemoteName] [-A IP address] [-c] [-n]
[-r] [-R] [-s] [S] [interval]]

-a (adapter status)	Lists the remote machine's name table given its name.
-A (Adapter status)	Lists the remote machine's name table given its IP address.
-c (cache)	Lists the remote name cache including the IP addresses.
-n (names)	Lists local NetBIOS names.
-r (resolved)	Lists names resolved by broadcast and via WINS.
-R (Reload)	Purges and reloads the remote cache name table.
-S (Sessions)	Lists sessions table with the destination IP addresses.
-s (sessions)	Lists sessions table converting destination IP addresses to host names via the hosts file.

RemoteName Remote host machine name.
IP address Dotted decimal representation of the IP address.
interval Redisplays selected statistics, pausing interval seconds between each display. Press Ctrl+C to stop redisplaying statistics.

Note: Netstat works for TCP/IP connections, and Nbtstat works for NetBIOS connections.

nslookup- The nslookup tool is used to trace DNS queries from start to finish.

Ping- Ping.exe verifies configurations and tests connectivity.

Troubleshooting:
If you can ping a hostname but cannot connect to a share point in Explorer, then the LMHOST file does not have an entry for that hostname or WINS is not working.
Conversely, if you CAN connect to a share in Explorer yet cannot ping the hostname, then either the HOST file entry is wrong or DNS is not working.

NetBIOS-problems are due to problems with WINS or LMHOST file.
DNS- problems are due to HOST file errors or DNS server problems.

tracert-The Tracert tool shows the route a packet will take over a network from one computer to another.

winipcfg- The winipcfg is a GUI version for Windows 95/98 of ipconfig.

Chapter 2. NT & Network Routing

2-1 Multi-homing

A multi-homed computer consists of two or more network interface cards connected to two or more subnets. Multi-home computers have a "home" on more than one subnet.

WINS handles multi-homed computers and entries can also be added to the computers local lmhost file.

When to Multi-home

When connecting and joining two or more different subnets to act as router between the two networks can be the easiest and most cost effective way for connectivity between the two.

File and printer servers used in conjunction by different subnets can improve network performance and take the load of routers.

Servers not to Multi-home

Domain Controllers don't work well multi-homed because they use NetBIOS broadcast to participate in browsing. When a DC causes a master browser election a DC with the two IP's can conflict with each other.

WINS does not work well multi-homed.

Exchange and other Servers don't perform well when multi-homed, check you server documentation before multi-homing an important server in your organization. What you think will elevate network traffic can crash or render the server inoperable.

2-2 Network Routing

A router (also called gateway) is function of the network layer. Routers are passive in that they do not actively forward packets to a corresponding network. A host must be configured to send and move remote network packets to a router for remote transport.

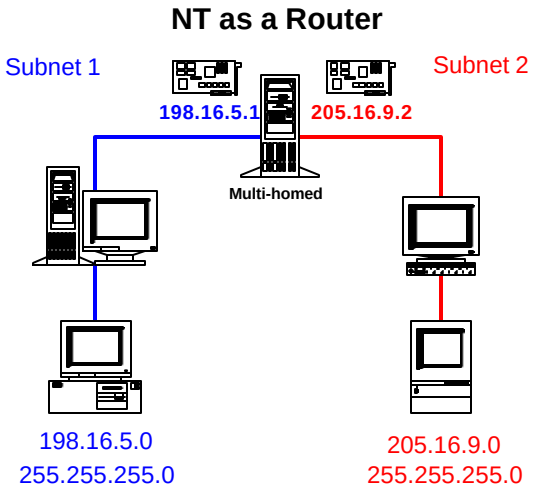
Bridges, which are active, operate on the data link layer and listen to all traffic on the network and forward traffic to the network it is connected too.

The IP layer uses a routing table to figure out where the packet should sent on the network. There are two types of routing, static and dynamic.

Static-Does not exchange information with other routers, it uses only a programmed internal routing table.

Dynamic- Learns about other networks automatically, using one of several routing protocols such as Routing Internet Protocol (RIP) or Open Shortest Path First (OSPF).

Static Routing



In the above diagram, the NT router knows about subnet 1(198.16.5.0) and subnet 2 (205.16.9.0) all hosts on subnet 1 will use 198.16.5.1 as the default gateway and hosts on subnet 2 will use 205.16.9.2 default gateway.

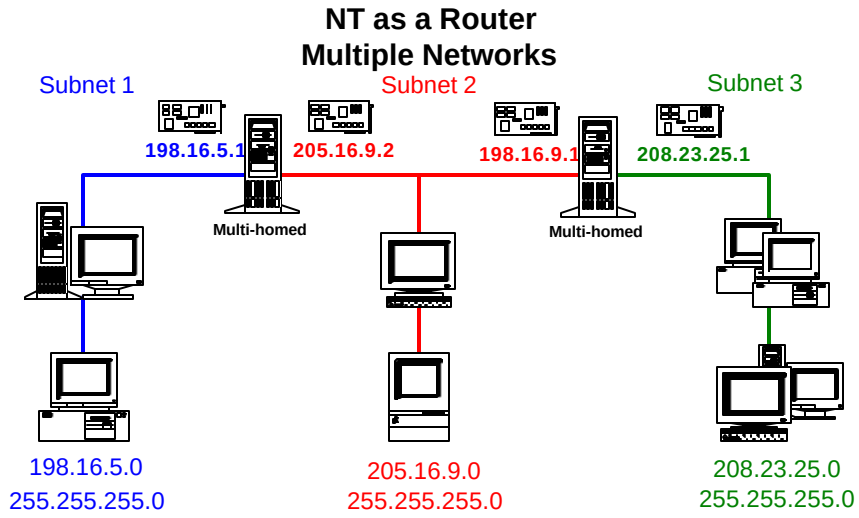
Installation

1. Install two or more NIC cards and physically connect to the remote network.
2. Assign a valid IP address to the card that the network is connected too.
3. After the cards are functioning, Enable IP Forwarding check box on the routing tab.

Route- utility is used for configuring static gateways

Route add *[network]* mask *[netmask] [gateway]* - Adds a route.
Route -p add *[network]* mask *[netmask] [gateway]* - Adds a persistent route.
Route delete *[network] [gateway]* - Deletes a route.
Route change *[network] [gateway]* - Modifies a route.
Route print Displays routing table.
Route -f - Clears all routes.

In the diagram below any computer on subnet 1 will be able to send and receive packets from subnet 2 because the NT router between the two networks is physically connected to both networks. But the NT Router of Subnet 1-2 does not know about address on subnet 3. This information must be programmed in the routing table.



Router 1-2: Route -p -add 208.23.25.0 mask 255.255.255.0 205.16.9.1
Router 2-3: Route -p -add 198.16.5.0 mask 255.255.255.0 205.16.9.2

Dynamic Routing

Windows NT 4.0 only supports RIP routing, more efficient faster routing protocols are supported in various systems by Cisco systems.

RIP

All RIP messages send over UDP port 520. Rip enabled routers exchange Network ID's of the networks that the router can reach. It uses a hop count field, or metric, in its routing table to determine the distance to a network ID. The maximum hop count for RIP is 15. Networks with 16 or more hops are considered unreachable. If multiple routes to a host are entered in the routing table, a RIP router will always use the route with the least of hops as default.

Disadvantages

RIP is a distance vector routing protocol so each router holds a complete table of the entire network and routes to all known hosts. Routing tables can be become large, many RIP routers contain RAM and hard drives to store the RIP table. The maximum size of a RIP packet is 512 bytes, so large routing tables have to be sent as multiple packets, this can lead to an overwhelming amount of data traffic.

RIP routers advertise the contents of their tables through a MAC level broadcast on all attached networks every 30 seconds.

The problem with Distance Vector routing is slow convergence. In Distance Vector routing, when a change is made, the changes must be propagated to each router. This propagation causes all routing tables affected by this change to be recalculated. Distance Vector routing can be very slow converging after a topical change. When a router goes down, it can take several minutes for the changes to be propagated throughout the network.

Silent RIP router - The purpose of a silent RIP router is to receive all broadcasts by other RIP enabled routers .It does not broadcast because it does not have any network to advertise, It's only purpose is to enable you to view the networks that your routers have found.

Chapter 3. DHCP SERVER

The Dynamic Host Configuration Protocol (DHCP) is used to automatically assign TCP/IP settings to clients IP Addresses come from a pool that is defined in the DHCP servers database called a Scope. The server grants the IP address for a specified amount of time called a Lease.

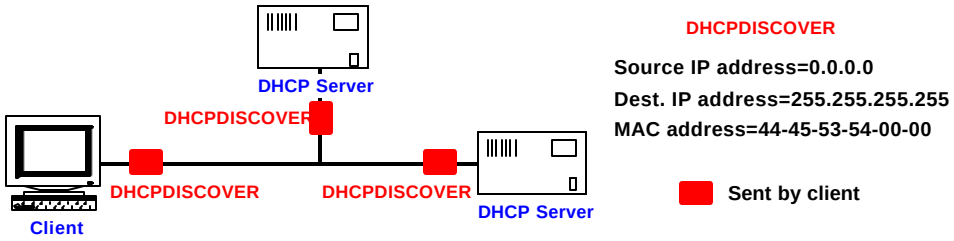
3-1 DHCP Configuration Process

The DHCP process is a four-step process

1. IP Lease request

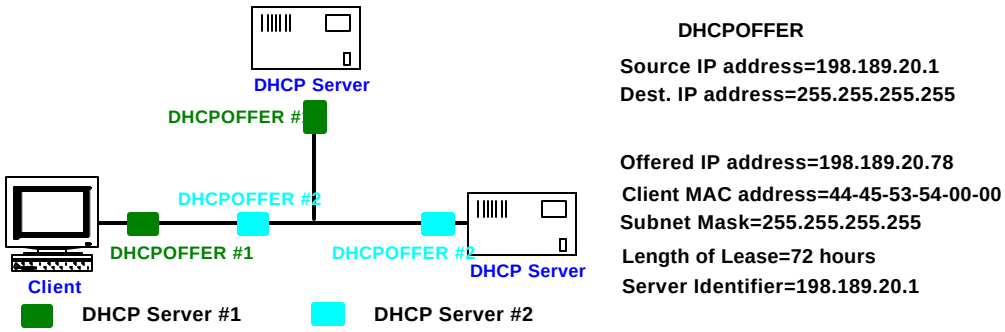
The client first initializes a limited TCP/IP stack and has been configured to automatically receive a lease for an IP address from a DHCP server on the network. The client requests this lease by a network broadcast. The IP address of the DHCP server is unknown and the client has not yet received an IP so it uses 0.0.0.0 as the source address and 255.255.255.255 as the destination address.

This request is sent in a **DHCPDISCOVER** message, which contains the client's hardware MAC address and computer name.



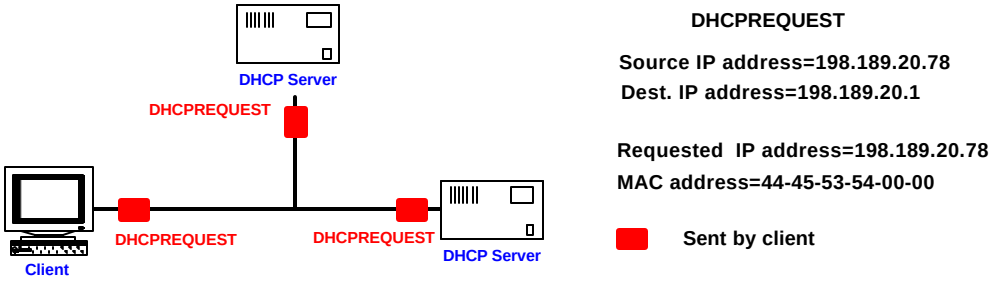
2. IP Lease Offer

The DHCP server sends a broadcast message to the client in the form of a DHCPOFFER message. The client will take the first IP lease it receives, if there are multiple DHCP servers on the network other requests will be ignored.



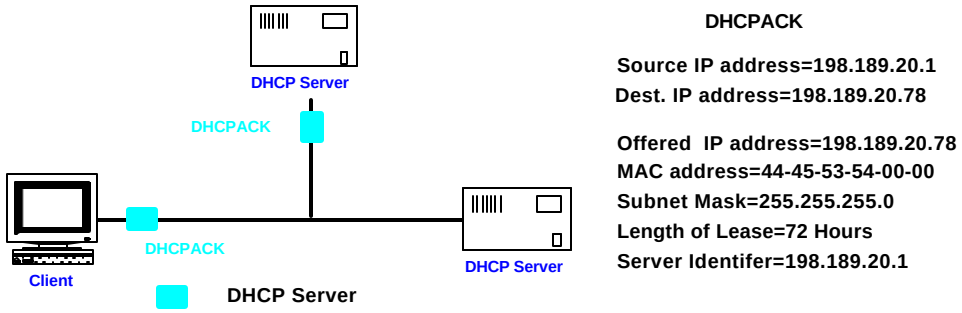
3. IP Lease selections

After the client receives an offer it broadcasts to all DHCP servers that it has accepted an offer. The Broadcast is in the form of a DHCPREQUEST message and includes the server identifier (IP address of the server) whose offer was accepted. All other DHCP Servers retract their offers.



4. IP Lease selections

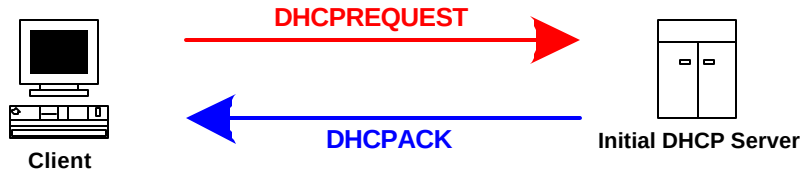
DHCP server broadcasts a successful ACK to the client in a DHCPACK message, containing a valid IP lease address. After the client receives ACK it is fully initialized and stores the lease in the registry.



3-2 DHCP Lease Renewal

1. First Renewal Attempt

All DHCP clients will attempt to renew their lease when 50% of the lease time has expired. From the Initial DHCP server the client obtained the lease from. The client sends a DHCPREQUEST message. If the DHCP Server is available, the lease is renewed and a successful DHCPACK acknowledgement is sent with any updated parameters. If the Client does not receive a DHCPACK, the client will continue to still use the lease because 50% is still available.



2. Second Renewal Attempt

If the DHCP lease was not successful on the first attempt, the client will attempt to renew the lease from the initial DHCP after rebooting, directly after 50% of lease completion. If unsuccessful the client will continue to still use the same lease because 50% is still available.

3.Third Renewal Attempt

If the client was unable to renew the lease at the initial 50% attempt from the initial DHCP server. The client will attempt to renew the lease at 87.5% of lease completion by contacting any available DHCP server on the network.

4.IP Lease Expiration

After the lease expires the client will un-initialize the lease and attempt to renew the lease, in the same fashion the client initially obtained the lease and the entire process will start all over again. If the client is unable to obtain a lease, the client's TCP/IP stack will not function and network errors will occur.

3-3 DHCP Installation, Manager, & Maintenance

Installation

Example:

IP Address: 198.183.20.51
Unique Identifier: 00aa00627d59
Client Name: Sps98
Client Comment: Windows 98 Workstation

Manager

In DHCP Manager, select the IP number of local machine.

DHCP Scope Options

Global- Global options are available to all DHCP clients and are used on all subnets that require the same configuration. Global options are always used, unless scope or a client options are configured.

Scope - Scope options are available to clients who lease an address from a specific scope. Scope options override global options. Activate 003 Router.

Client- Client options are used for a specific client. Client options override global or scope options.

DHCP Options for Microsoft TCP/IP

DHCP server complies with RFC 1533, the table below summarizes the options available to Microsoft clients. In DHCP options you notice other scope options available to other non-Microsoft clients.

Code	Name	Description
1	Subnet Mask	Client Subnet Mask, This option is configured in the Create Scope or Scope Properties, can't be configured as scope option.
3	Router	IP address for routers.

6	DNS Servers	IP address for DNS servers.
15	Domain Name	Specifies domain name to be used when resolving DNS host names.
44	WINS/NBNS	Specifies a list of IP addresses for NetBIOS name servers.
46	WINS/NBT	Specifies the NetBIOS over TCP/IP node type 1=b-node 2=p-node 4=m-node 8=h-node
47	NetBIOS ID	Specifies a string to be used as the NetBIOS over TCP/IP scope ID.

DHCP Maintenance

Ipconfig- Command line utility that enables you to verify the clients IP configuration. Windows 95/98 has a GUI based utility WINIPCFG.EXE.

Switches

/**all**- Lists all TCP/IP Configuration parameters, DHCP,WINS,NetBios Information
/**renew**- The client sends a DHCPREQUEST to the DHCP server to get updated options.
/**release**- The client releases it lease and sends a DHCPRELEASE message to the DHCP server for a new lease

Backing up the DHCP Database

The DHCP database is backed up every 60 minutes and this property can be change in the registry.

File Location: \systemroot\system32\DHCP
Backup File Location: \systemroot\system32\DHCP\backup\jet
Registry Key: KEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DHCPServer\Prameter
Flag: Backup Interval (Minutes)

Files:

DHCP.MDB - DHCP database file
DHCP.TMP - Temporary file where non-committed transactions are stored .
JET.LOG - Logs all transactions
SYSTEM.MDB - DHCP directory structure database

Restoring a DHCP database

Stop and restart the DHCP service, the DHCP service will detect a corrupt database automatically restore the database if the restore flag has been set in the registry.

Registry Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DHCPServer\Prameter\Restore
Flag: Restore Flag 0/Off, 1/On

Chapter 4. NetBIOS over TCP/IP

NetBIOS over TCP/IP (NBT) is the session-layer network service that performs name-to-IP address mapping for name resolution.

NetBIOS Name Types

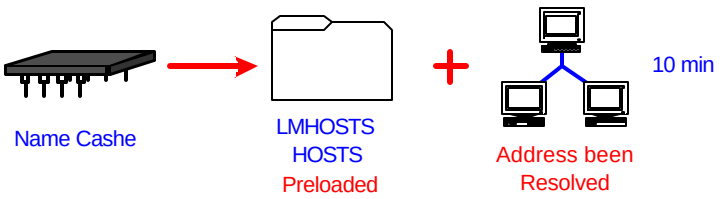
NetBIOS computer names are always 16 byte strings. Computer names can be up to 15 characters long, the last byte is reserved for a suffix that is the resource or service code. Below is a table of resource and service codes. When naming a computer it is best to use characters that are compatible with the DNS naming convention for WINS-DNS integration.

Common NetBIOS Names	Service That Registers the Name
<computer name>[00h]	Workstation (your NetBIOS Redirector)
<computer name>[03h]	Messenger (listens for messages sent to your computer)
<computer name>[20h]	Server (shares your resources to the network)
<user name>[03h]	Messenger (listens for messages sent to your logon ID)
<domain name>[1Dh]	Master Browser
<domain name>[1Bh]	Domain Master Browser

Methods of Resolution

Name Cache

The NetBIOS name cache is checked first no matter what node type is configured on the machine. The cache is always local. Names resolved in the last 600 seconds (10 minutes) remain in the cache. Names can permanently be loaded in the cache. Machines defined with the #PRE tag in the LMHOSTS file. To check the name cache nbtstat -c will show all resolved names.



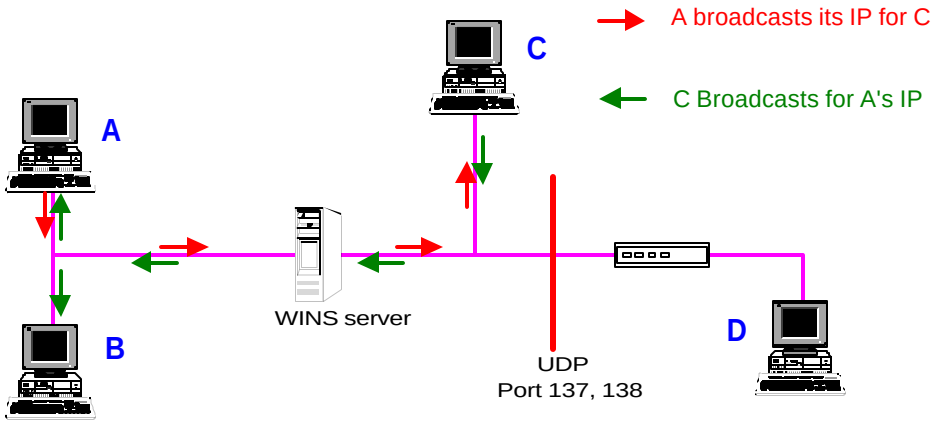
Netbios Name Server

B-Node (Broadcast Node)
Broadcast mode uses broadcasts only.

1. NetBIOS Name Cache.
2. Broadcast a NetBIOS Name Query.
3. Checking the LMHOSTS file.
4. Checking a HOSTS file.
5. Checking with a DNS server .

Configuration- Leave the WINS address empty

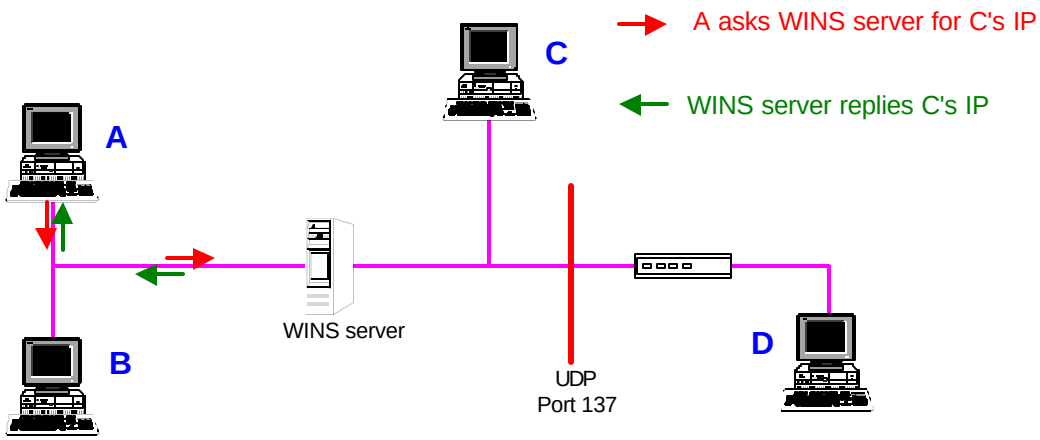
Use- Broadcasts are typically blocked by routers so a b-node configuration will only be effective on a single subnet.



P-Node(Peer-to-Peer Node)

1. NetBIOS Name Cache.
2. Asking a NetBIOS Name Server.
3. HOSTS file.
4. DNS.

Configuration - Configure though DHCP lease offering



M-Node(Mixed Node)

1. NetBIOS Name Cache.
2. Broadcast a NetBIOS Name Query.
3. Checking the LMHOSTS file.
4. Asking a NetBIOS Name Server.
5. Checking a HOSTS file.
6. Checking with a DNS server.

Configuration - Configure though DHCP lease offering

H-Node(Hybrid Node)

1. NetBIOS Name Cache.
2. Asking a NetBIOS Name Server.
3. Broadcast a NetBIOS Name Query.
4. Checking the LMHOSTS file.
5. Checking a HOSTS file.
6. Checking with a DNS server .

Configuration - Enter the WINS server address

Chapter 5. Static Resolution Files

5-1 LMHOSTS File

Location: %winroot%\system32\drivers\etc
File Name: LMHOSTS
Sample File: LMHOSTS.SAM

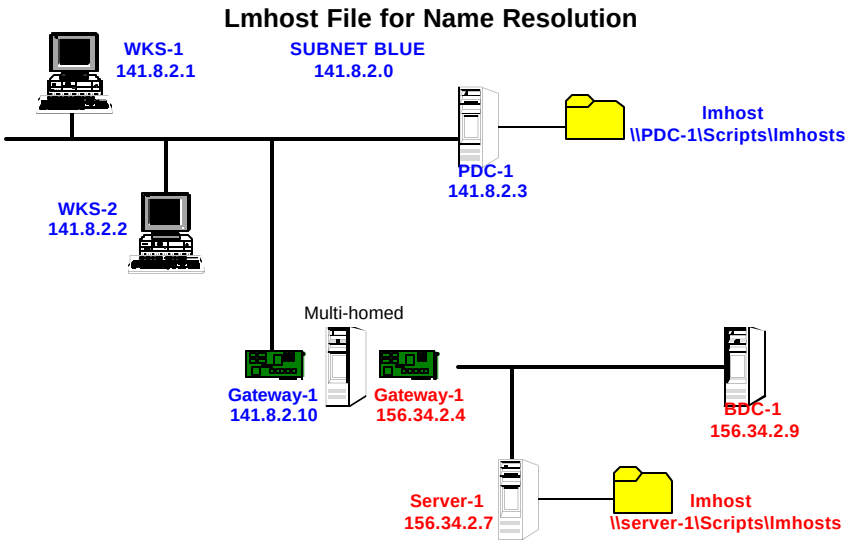
Tags Available for use in LMHOSTS file

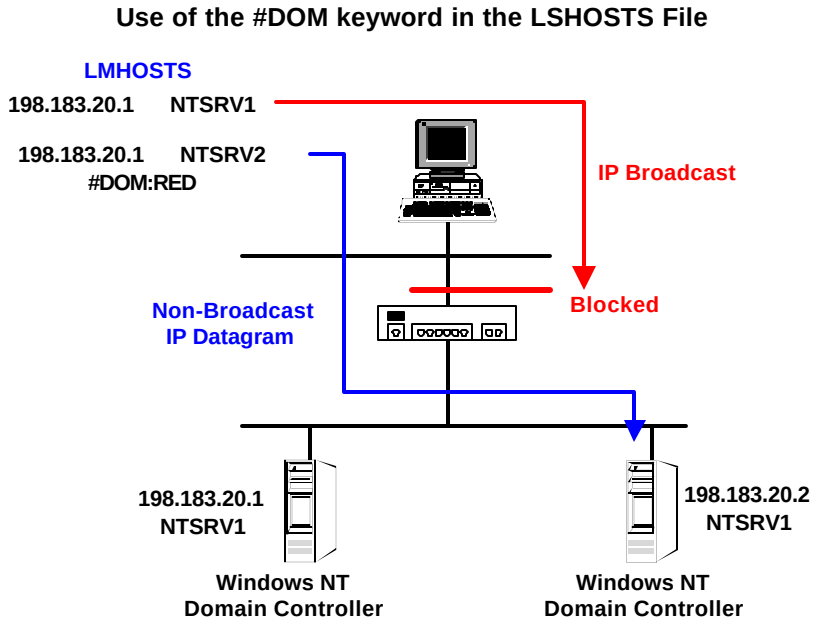
Tag	Use
#PRE	A #PRE tag tells the computer to pre-load the entry to the name cache during initialization or after the NBTSTAT -R command has been issued at the command prompt. Entries of #PRE are static in the cache.
#DOM:[domain_name]	Indicates the computer is a domain controller.
#NOFNR	Avoids using NetBIOS name queries on older LAN manager for UNIX environments.
#INCLUDE	Directs the system to the location of the central LMHOSTS file
#BEGIN_ALTERNATE	Used in conjunction with the #INCLUDE file. This entry marks the beginning of entries that are alternative locations for the central LMHOST file. If the first entry is unavailable.
#END_ALTERNATE	End of alternative locations statement.
#MH	Multi-homed computers that have more than one entry

```
141.8.2.1       WKS-1
141.8.2.2       WKS-2       #PRE
141.8.2.3       PDC-1       #PRE #DOM:BLUE
156.34.2.9      BDC-1       #PRE #DOM:RED

141.8.2.10      Gateway-1   #MH
156.34.2.4      Gateway-1   #MH
156.34.2.7      Server-1    #PRE #INCLUDE

\\PDC-1\Scripts\lmhosts    #BEGIN_ALTERNATE#INCLUDE
\\SERVER-1\Scripts\lmhosts #END_ALTERNATE
```





5-2 HOSTS File

On heterogeneous networks containing NT and Unix systems a way to resolve host names to IP addresses is to use a locally stored database file called a HOST file. The disadvantage of a HOST file and a LMHOST file is that each users machine must have it's own copy and lacks any central administration of updating the file.

NT Location: %winroot%\system32\drivers\etc
Unix Location: /etc/hosts
File Name: HOSTS

The format is a follows

Each entry should be placed on an individual line. The IP address is placed in the first column followed by the corresponding host name.

Comments are noted by the "#"

```
#
# Hosts file for  SPS Domain
#


127.0.0.1           local host
13.41.85.1          router
13.91.45.121        server1

13.91.45.122        mcsunix       #     x86 Solaris 7 machine
14.33.121.121       mars          #     HP Unix 10.1 System

189.11.121.11       sunshinemtn.com       web     # Web server
```

Multiple host names can be assigned to the same IP address. The 189.11.121.11 system can be referred by its FQDN **sunshinemtn.com** or it's nickname **web**. Be aware that Unix systems are case sensitive and NT systems are not

5-3 NBTSTAT

The NBTSTAT utility checks the state of the current NetBIOS over TCP/IP connections, updates LMHOSTS, and determines your registered name and scope ID.

Switches
-*n* Lists the NetBIOS name registered by the client
-*c* Displays NetBIOS name cache.
-*R* Manually reloads the NetBIOS name cache using entries in the LMHOSTS file with a #PRE parameter.

Chapter 6. WINS SERVER

1. WINS is a Microsoft NetBIOS name server (NBNS),WINS Eliminates the need for broadcasts to resolve computer names to IP addresses.
2. A WINS Server can be configured with both WINS and DNS to work in conjunction for NetBios and hostname resolution for Microsoft Clients only.
3. WINS is a Dynamic database, so name resolution is always current and does not have to be changed manually like a lmhost file.

6-1 WINS Resolution Process

Name Registration

When a WINS client initializes, it registers its NetBIOS name by sending a name request to the configured WINS server. All services get registered as they are initialized in the WINS server database

such as Workstation, Server and Messenger. If the WINS server is available and the name is not registered by another machine, the WINS server returns a successful registration message.

Duplicate Name

If the NetBIOS name is already registered in the WINS database, the WINS server will send a challenge to the current registered owner. This request will be sent 3 times at 500ms intervals. If the current owner responds the WINS server will send a negative name resolution response to the WINS client attempting to register the name. If there is no response the registering client will receive a Name Registration response.

WINS Server Unavailable

A WINS client will make three attempts to register its name with the configured Primary WINS server. If the client fails after the third attempt, the client will attempt to register with the configured secondary WINS server, if that fails the client will use broadcasts to register it's name.

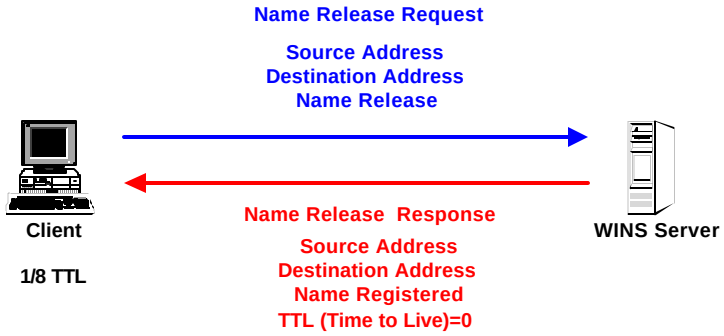
Name Renewal

To continue using the same NetBIOS name, a client must renew its lease before it expires. If the client does not renew the lease, the WINS server makes it available to another WINS client. A WINS client will first attempt to refresh its name registration request after 1/8 of the TTL is completed. If the client is successful subsequent name registration requests will occur when ¼the TTL is expired

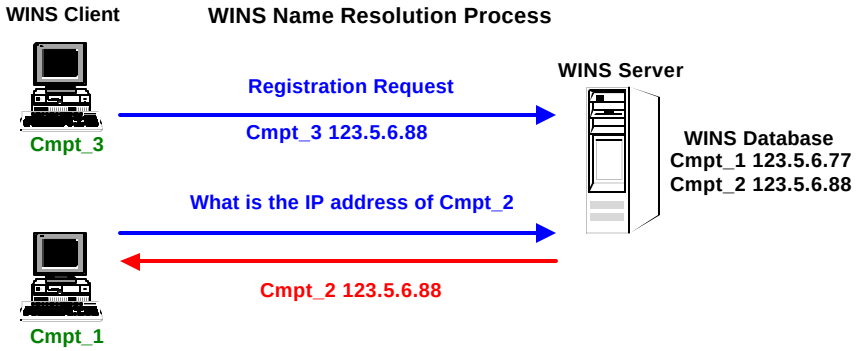
Failure of Initial Name Renewal

If the client is unsuccessful with lease renewal on the initial attempt the client will try every 2 minutes until ½TTL is remaining. At ½of TTL the client will revert to the secondary WINS server if configured in 1/8 TTL intervals. At completion of TTL lease, the WINS client will revert back to the primary WINS server and start the process all over again.

Name Release



Name Query and Response



Name Resolution

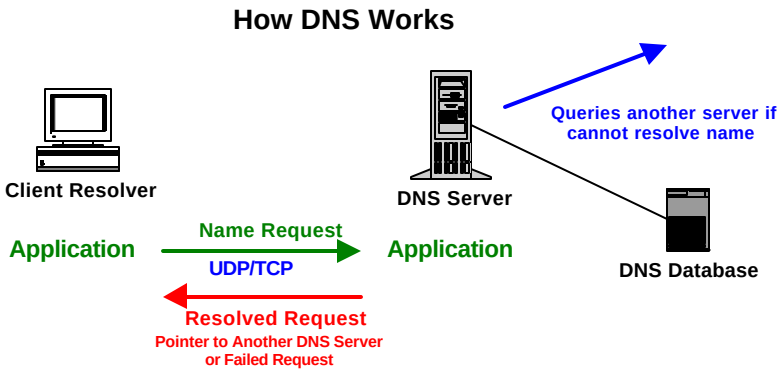
On a Windows NT Network, A host will check different options to perform name resolution.

1. Local Cache.
2. WINS Server.
3. Netbios Name Broadcast.
4. LMHOSTS File.

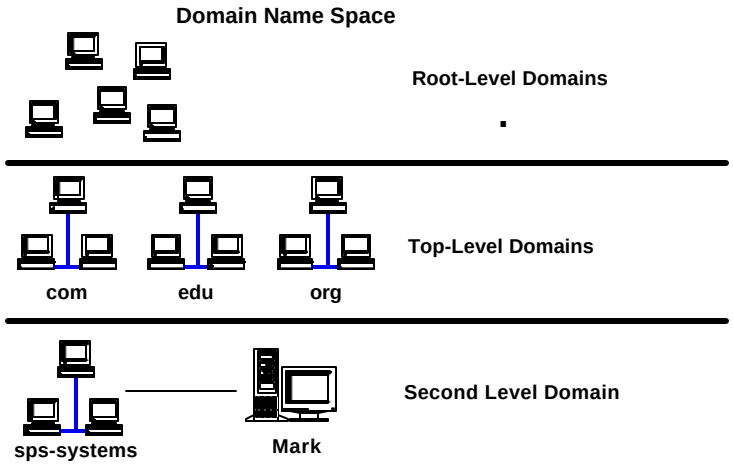
Chapter 6. DNS Server

6-1 Domain Name Resolution

1. DNS is a hierarchical based distributed database of indexed hostnames.
2. Rsolvers 1st send queries in UDP packets for increase performance and resort to TCP if data truncation occurs.



1. Root-level domains define different levels of authority in a hierarchical structure. Top of the hierarchy is called root domain (.).
2. Top-level domains com, edu, org, net, gov, mil and two letter country codes.
3. Second-level domains can contain both hosts and other domains called sub-domains. For example *sps-systems.com* can contain a hosts ftp.sps-systems.com or sub-domains such as *dev.sps-systems.com*.
4. Host names are added to the beginning of the *domain.mark.sps-systems.com*.



6-2 Domain Names

FQDN = Host name + Domain Name

FQDN = NTSRV + MYCOMPANY.COM = NTSRV.MYCOMPANY.COM

The domain name can any combination of letters A to Z, digits 0 to 9 and the hyphen (-), the period (.) is used as a separator. Domain names are not case sensitive. When naming hosts on your Windows Network that will act as Internet hosts it best to use characters that comply with Netbios and FQDN names avoid the Underscore (_).

Recursive, Iterative and Reverse Queries

Recursion- When a DNS server perform a recursive query on the client's behalf the DNS server stays with the query until the request has been resolved.

Query 1

In the Diagram below the client at pc.mycompany.com makes a request to the corporate DNS server. The DNS checks it's cache to see if the query has already been resolved and in the cache. In this query the corporate DNS server has no record of this query. The corporate DNS switches roles and now acts as client to issue an iterative query to the local ISP.

Iterative- queries enable DNS servers to pass back pointers or referrals. When a client issues a iterative query to a DNS server, the DNS server may not have the answer but may refer the client where the answer can be obtained.

Query 2

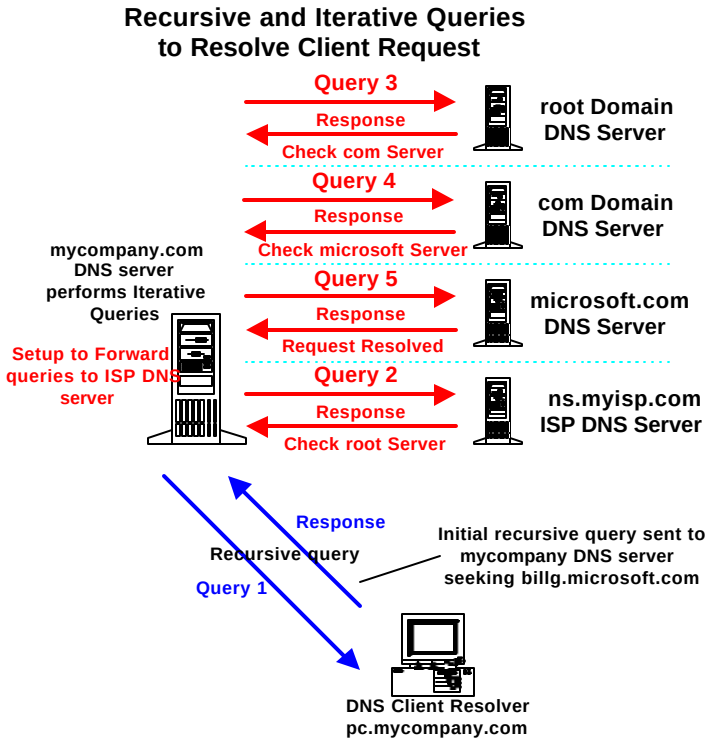
The corporate DNS sever is set up to forward requests to the ISP DNS name server. The ISP name server has no record of this resolved request. The ISP server replies back with a hint to query the root domain server.

Query 3-5

The DNS server issues an iterative query at the top of the DNS hierarchy to the root level server. After each query and response the server goes down the DNS tree to it finally finds the correct resolved name.

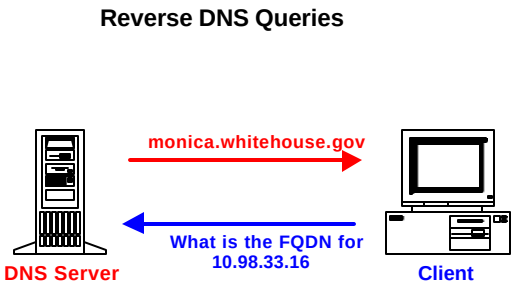
Response

The corporate DNS server returns the response to the client, completing the recursive query.



Reverse Queries

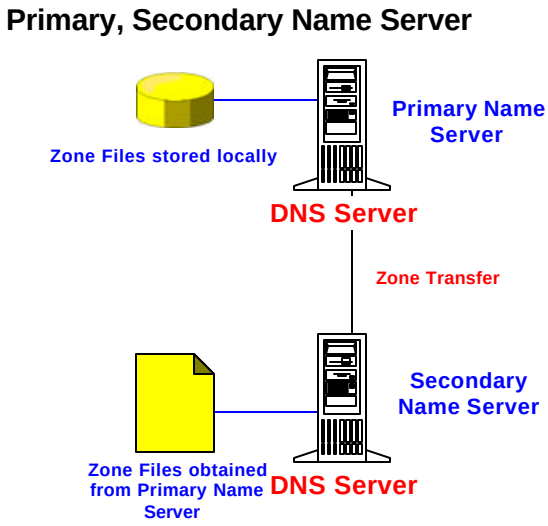
In a reverse query the client issues a IP address and queries the DNS server for a fully qualified domain name (FQDN).



6-3 Types of DNS Servers

Primary, Secondary and Master Name Servers

A primary name server is a name server that gets the data for its zones from local files. Changes to a zone, such as adding domains or hosts, are done at the Primary Name Server. A secondary name server gets the data for its zones from another name server across the network which is authoritative for that zone. The processes of obtaining this zone information (that is the database file) across the network is referred to as a zone transfer.



Forwarders and Slaves

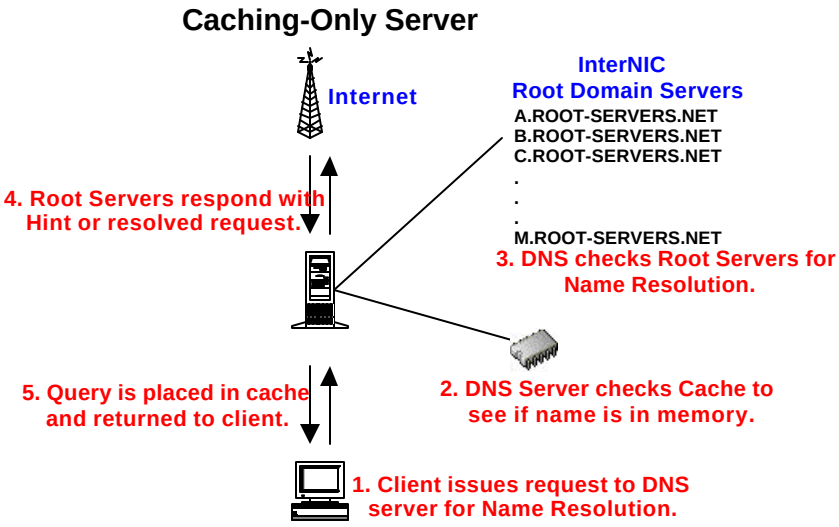
When a DNS server receives a request it first attempts to locate the request in it's own zone files or cache. If the information is not located on the server or that server is not authoritative for the domain request. The DNS must communicate with other DNS servers.

To address the above issue, A DNS server on the network can be designated as a **Forwarder**. Only a forwarder is allowed to query other DNS servers outside the network.

Slaves are DNS servers that use Forwarders. They will return a failure message if the forwarder is unable to resole the request. Salves will not attempt to contact other forwarders if the request fails.

Caching- Only Servers

Caching-only servers are DNS names servers whose only job is to perform queries, cache the answers and return the results. A Caching Only Server role in a network is to perform load balancing; the server does not participate in zone transfer.



6-4 DNS BIND Database Files

1. BIND text database files can be used for configuring the MS DNS server. BIND is the most widely used format for DNS servers on the Internet.
2. MS DNS has a GUI to manage any feature of the DNS server.
3. The MS DNS server and BIND compatable DNS servers contain four files:
    a. database file.
    b. reverse lookup file.
    c. cache file.
    d. boot file .

BIND Database Files

Editing BIND database files requires the DNS server to be stopped and restarted where the GUI DNS changes are dynamically changed.

File Location - %WINROOT%\SYSTEM32\DNS

domain.dns

The Database file (domain.dns) stores resource records for the domain. For the "*mycomany.com*" zone, the zone file will be called *mycomany.com.dns*. The database file should be named as for the zone it represents. This is the file that is replicated between master name servers and secondary name servers.

Within the domain.dns file there are several types of resource records defined in DNS. RFC 1034 defines these records in more detail.

Boot

The boot file is the master configuration file. Contained with in the boot file is the location of all the BIND database files. MS DNS server uses the boot file only once. When initially importing an existing BIND database into MS DNS, values are taken from the database file and imported into the NT registry.

Cache.dns

Defines the addresses of the root name servers for the DNS.

127.0.0.dns

This file contains the reverse lookup data for IP numbers on the 127 loop back address. This file ensures that local loopback tests do not pass out of the local network.

reverse-netid.in-addr.arpa.dns

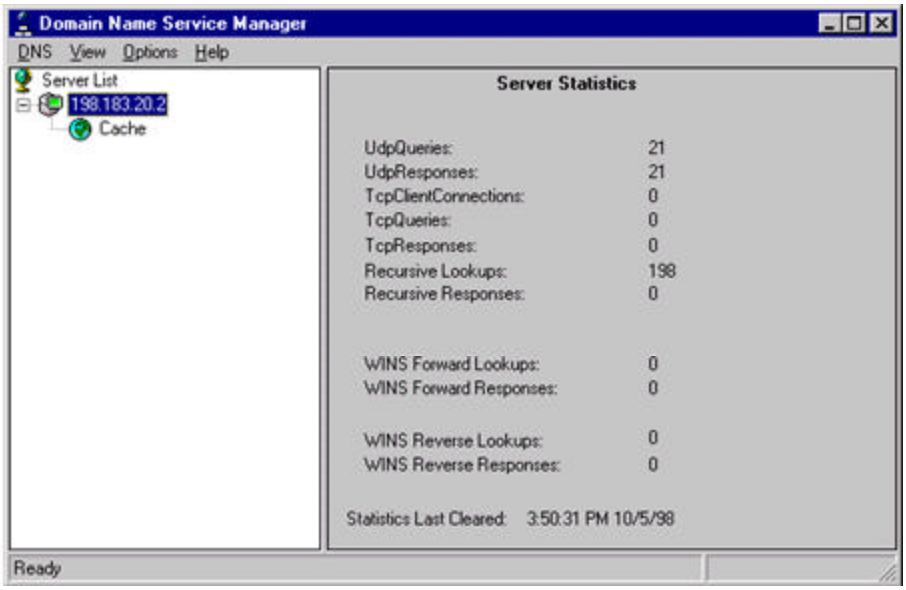
The reverse lookup file allows a resolver to provide an IP address to a matching host name. When a client issues a Reverse Query with an IP address the DNS server will return a FQDN. A reverse lookup file is structured liked like a zone file and contains SOA and name server records. To provide a reverse lookup for the network 100.55.200.143 a file is created with the name 55.100.in-addr.arpa.

6-5 DNS Implementation

Install the DNS Services by adding it under sevices in Network Services applet and reboot the machine.

Registry Key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\

The DNS server will now function as cache server. The cache file contains the root name servers for the Internet. The server can resolve queries sent to it by consulting with an authoritative server for the domain that the client is looking for.



Setting up name resolution on your domain

Adding the Reverse-Lookup Zones

Before you create a zone for a domain that is to manage, you need to create a zone that will support a reverse lookup (*in-addr.arpa.zones*). As you add **A** records to your primary zones **PTR** records will automatically be inserted for reverse lookups.

Creating Primary Zones

After the reverse-lookup zones have been created you can begin to add your primary zone. Now you can populate your records with the different host configurations as needed.

6-6 DNS Configuration Options

BIND Database Files

Editing BIND database files requires the DNS server to be stopped and restarted where the GUI DNS changes are dynamically changed.

File Location - %WINROOT%\SYSTEM32\DNS

domain.dns

The Database file (*domain.dns*) stores resource records for the domain. For the "*mycomany.com*" zone, the zone file will be called *mycomany.com.dns*. The database file should be named as for the zone it represents. This is the file that is replicated between master name servers and secondary name servers.

Within the *domain.dns* file there are several types of resource records defined in DNS.
RFC 1034 defines these records in more detail.

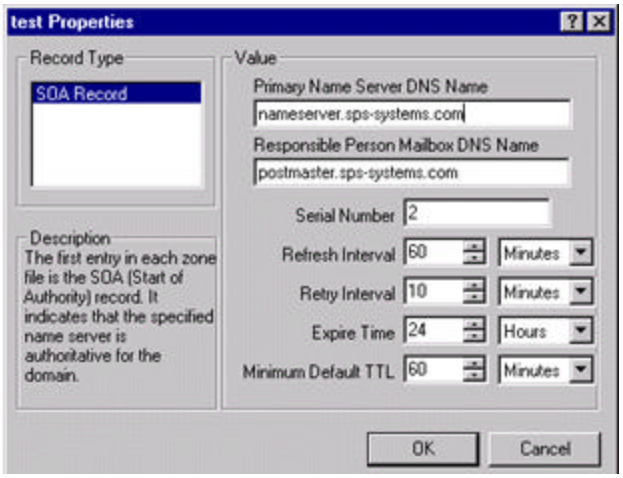
Start of Authority record (SOA)

1. First record in forward and reverse (in-addr) database file.
2. Defines what Name Server is authoritative for domain.
3. RFC 1035 defines SOA records in more detail.

```
@       IN      SOA     nameserver.sps-systems.com      postmaster.sps-systems.com  (
                2       ; serial number
                36000   ; refresh   [1h]
                600     ; retry     [10m]
                86400   ; expire    [1d]
                3600 )  ; min TTL   [1h]
```

Key to SOA records

1. The at symbol (@) in a database file indicates "this server".
2. IN indicates an Internet record.



SOA record in MS DNS Manger

Key to SOA records and GUI MS DNS Manager

Serial number- The Serial number indicates the version of the file.

Refresh- The interval in seconds at which a secondary name server checks to download a copy of the zone data from the primary name server.

Retry- The time in seconds a secondary name server waits to reinitiate a zone transfer if the initial transfer fails.

Expire- The period of time a secondary name server continues to try to initiate a zone transfer after a failed transfer. If the DNS server reaches the expired time, the server discards all the data for that zone.

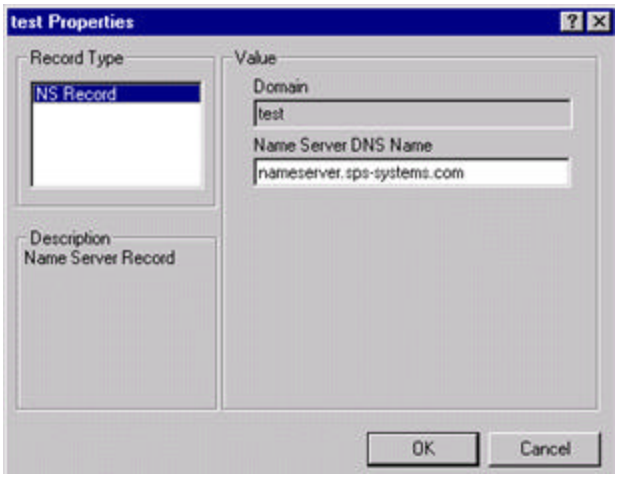
Min TTL-Time to Live is the minimum time that the resource record retains an address mapping in the cache.

Name Server record (NS)

1. List additional name servers.

2. Database file may contain more than one.

```
@       IN      NS      nameserver.sps-systems.com
@       IN      NS      nameserver2.sps-systems.com
```

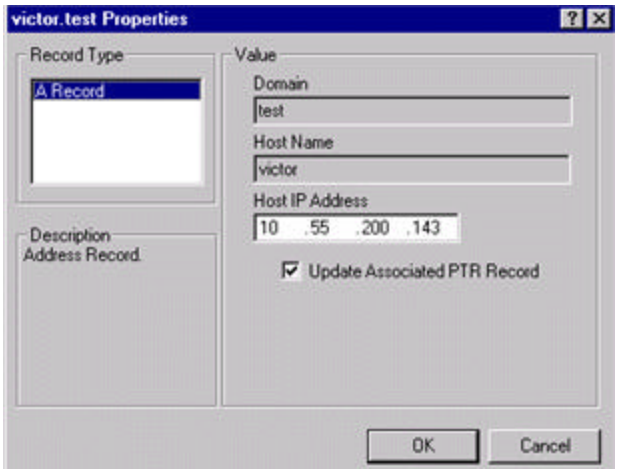


Name Server (NS) record in MS DNS Manger

Host record (A)

1. Statically associates (A) a host name with IP address.
2. Lists all hosts within the zone.

```
victor          IN A    10.55.200.143
localhost       IN A    127.0.0.1
```

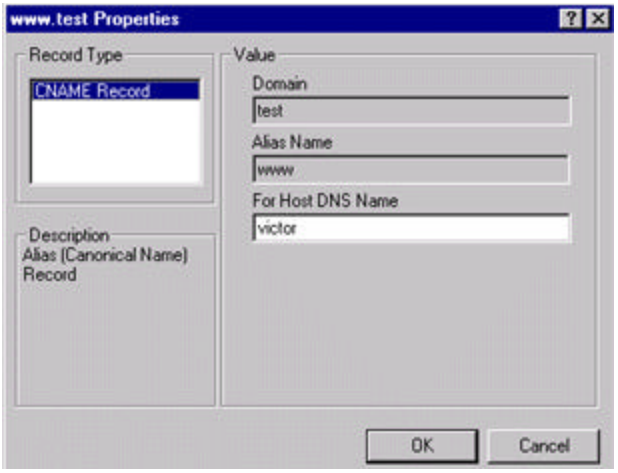


Address (A) record in MS DNS Manger

Canonical Name record (CNAME)

Enables you to associate more than one host name with one IP address (aliasing)

```
www     CNAME   victor
ftp     CNAME   victor
```



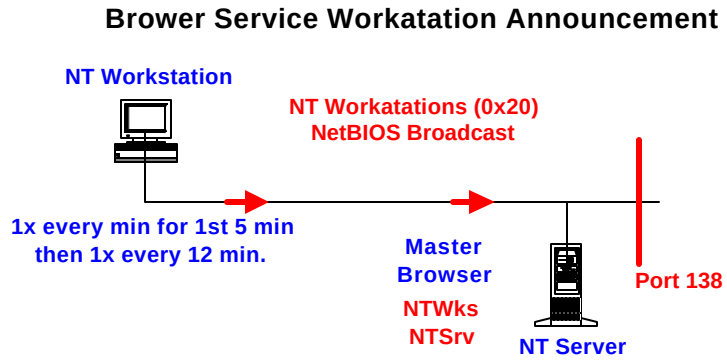
Canonical Name (CNAME) record in MS DNS Manger

Chapter 7. The Browser Service & TCP/IP

Building the Browse List

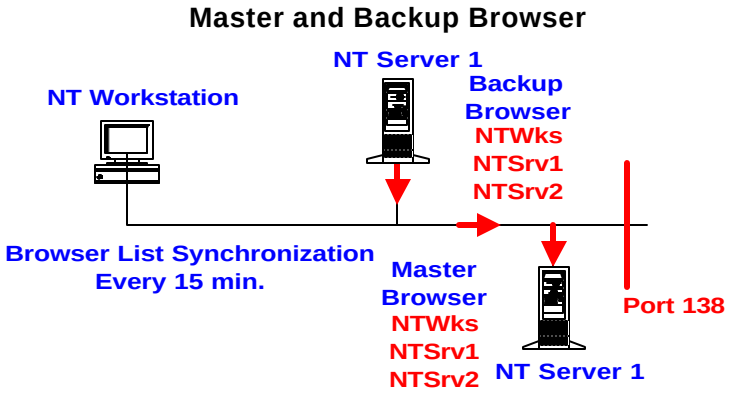
Master Browser-When a client starts up it broadcasts its name on the network. The Master browser collects and maintains the master list of available computers. Windows NT Server, Workstation, Windows 95/98 and WFW machines can act as a master browser

Domain Master Browser- A Windows NT server acting as a PDC can synchronize with other Master browsers on remote networks to obtain a complete synchronized browse list.



Distributing the Browse List

Every 15 minutes the backup browser contacts the master browser and downloads the browse list from the master browser.



Client Browsing Request

When a client attempts to access a resource in a domain or workgroup the master browser will forward a list of up to 3 backup browsers where the client can obtain the browse list.

The Client after receiving the backup browser list will ask the backup browser for the list of network resources.

After the client has selected the server it wishes to obtain resources from the client will ask the server and obtain a list of available resources from the server.