Network Browsing with SoftRemote

The browsing service on a Microsoft network enables a workstation to see what other resources are available on the network through Windows Network Neighborhood. This document describes how network browsing works and also how it affects remote users using SafeNet SoftRemote and Soft-PK.

Network Browsing

The Network Browser service provides a list of currently available network resources. This service is important because it eliminates the need for each computer on the network to maintain its own list of available resources. Instead, only designated computers perform this function, which increases network efficiency.

A networked computer can play a particular role vis-à-vis network browsing:

- The master browser builds, maintains, and distributes the master list, called the browse list, of all currently available network resources.
- The domain master browser is a Windows NT server that functions as a primary domain controller (PDC) computer that the network administrator designates to serve as the master browser.
- The backup browser receives copies of the browse list from the master browser, and then distributes them to client machines upon request.
- The potential browser becomes a master browser only when the current master browser tells it to do so.

Typically, client machines do not maintain a browser list and, thus, serve no network browser role.

Domain Master Browser

TCP/IP networks with multiple segments require a domain master browser. Each segment elects a master browser for the segment; the master browser on one segment becomes a domain master browser.

Every 12 minutes, the domain master browser asks the master browser on each segment for its browse list. The domain master browser then compiles all the browse lists into a single, complete browse list, and distributes it to each segment's master browser.

When each computer that runs a browser service starts up, it checks in with its domain or workgroup's master browser through a B-node broadcast. The first time SoftRemote attempts to contact the master browser, it sends a request to the master browser for a list of the backup browsers. SoftRemote also requests a list of network resources from the backup browsers, not the master browser. Every 15 minutes, the backup browsers contact the master browser for the latest browse list. Thereafter, the backup browsers forward the list to any client that requests it.

When the master browser goes offline, a process called a browser election occurs. When a computer is unable to reach the master browser, it issues a broadcast called an election datagram. This election datagram contains the election version—the operating system of the source computer. Windows NT servers have priority over Windows NT workstations, which have priority over computers running Windows 9x.

WINS

Master browsers receive notices through B-node broadcasts; routers do not pass these broadcasts. Windows Internet Naming Service (WINS) is required to browse across networks that require a "hop-across" router. On Microsoft networks, the browser service primarily relies on NetBIOS name broadcasts to receive the information from the connecting systems. This is where WINS enters the picture.

A WINS server maintains a dynamic database of NetBIOS names that correspond to IP addresses. When the WINS client starts up, it registers its NetBIOS name and IP address with the WINS server. When the WINS client attempts to communicate with another host, the name resolution request is sent directly to the WINS server instead of being broadcast all over the local network. This reduces network traffic significantly, thus optimizing the performance of the network.

There are four WINS message modes:

- Client name registration-—When the client boots up, it registers its name and IP address with the specified WINS server. When the WINS server receives the information from the client, it transmits a successful registration message. The server also gives the client a TTL period, specifying how long that name can be used.
- Client lease renewal—-When 50% of this TTL period is expired, the client sends a name renewal message to the primary WINS server. This message includes the client's current computer name and IP address. The WINS server responds by sending the client a new TTL period.
- Client name release—-When a WINS client is shutting down, it sends a name release message, with the client's IP address and name, to the WINS server. The client waits for a confirmation, called a positive release message, which contains the released name, IP address, and a TTL of zero.
- Server name query and name resolution response-—This final mode specifies the order in which the client attempts to resolve the computer name to an IP address.

    a. The system checks its local address cache. If this is successful, it uses the Address Resolution Protocol (ARP) to resolve the hardware address. If the address is not in the local cache, WINS is utilized.
    b. If both primary and secondary WINS fail to resolve the names, the system sends a B-node broadcast. If this is unsuccessful, the client checks these files in this sequence:

i. LMHOSTS
ii. HOSTS
iii. DNS

Implement WINS with SoftRemote

Although SoftRemote and WINS work independent of each other, for the remote user to be able to browse the corporate network, WINS must be configured in the TCP/IP properties for the interface used to connect remotely with the remote connection.

The specific steps to do this vary with each Windows version. This is the general procedure:

1. Right-click the dial-up networking (DUN) or connections icon.
2. On the Server Types tab, select TCP/IP Settings.
3. Enter the IP address of the DNS and WINS Servers.
4. Select OK.

Common Issues with Network Browsing Over Remote Connections

- After a VPN connection is made, you are unable to browse the remote network from Network Neighborhood on your computer. You can, however, PING by name, and you can execute the NET USE command in a command prompt.

    - For Windows 95/98/Me, add the File and Print Sharing service. On the FPS Properties dialog box (look this up in the Windows help to find it), set the Master Browser setting to Disabled. This forces the system to go to the WINS server.
    - For Windows NT and 2000, edit the registry: In HKLM\System\CCS\Services\Browser\Parameters, make sure that IsDomainMaster and MaintainServerList are both set to FALSE.
    - If using a personal firewall, verify that ports 137 and 138 are open.

- A WINS or LMHOSTS file is required. Consider these limitations when using an LMHOSTS File:

- All computers on the network must have a LMHOSTS file that includes an entry for all domain controllers for network browsing to work. This is the syntax for the domain controllers:

  199.199.199.1 #PRE #DOM:

- To connect to computers in your browse list (Network Neighborhood), you must have an entry in your LMHOSTS file for that computer. Just because you can see it on your desktop doesn't mean that you can establish a connection with it.