

# CONTRIBUTED DOCUMENTATION

This document is NOT supported by Computing Services.  
DO NOT contact the Help Center with questions on this document.

## Peer to Peer Networking

---

### What is Microsoft Peer to Peer Networking?

Microsoft Peer to Peer Networking (sometimes referred to as just Windows Networking) is what lets you see other Microsoft Peer to Peer or server computers in the Network Neighborhood on your Windows machine. It also lets your computer connect to these computers over the network. It is unsupportable because even though your computer may be configured correctly, another computer configured incorrectly on your network segment can cause your Network Neighborhood to not function correctly. Because we do not have administrative access to dormitory and office Windows computers, there is no way that Computing Services can control the integrity of the Windows network.

### How does Microsoft Peer to Peer Networking work?

Windows networking was originally designed to work on small (LAN) networks in which a central administrator had control over the configuration of all machines. Windows networking works very well in such environments.

#### Enumeration

When you open your network neighborhood, your machine sends out a request to get a list of who's in your workgroup. A "master browser" computer responds to your computer and gives your computer a list of the computers that are "backup browsers" for your workgroup on your subnet. Your computer then picks a "backup browser" at random from that list and contacts that computer, which finally gives you the list of computers to display in your network neighborhood. This process of listing members of a workgroup is called "Enumeration". Having multiple "backup browsers" distributes the load of enumeration across multiple computers. Each subnet has one "master browser" and two or more "backup browsers" per workgroup.

#### Election

Any Windows computer (including yours) on the network can become a "backup browser". Whenever a computer enters (starts up) or leaves (shuts down) from the workgroup, an "election" takes place among all the Windows computers on that network segment, and the most eligible machines become the "master browser" and "backup browsers". The number of "backup browsers" grows and shrinks to maintain a certain ratio of browsers to non-browsers. This all happens dynamically without the user knowing it. (There are ways to control the likelihood of your machine becoming a browser though using registry settings).

#### Subnets

Browsing works using 'broadcasts' which are confined to a subnet and do not go across routers. Dormitories are in their own 'subnets', and broadcasts in one subnet will not reach other subnets such as other dormitories or academic buildings. (Some dorms are in the same subnet). Routers are the hardware that separates subnets.

If the "master browsers" are properly configured, they will communicate with our "domain master browser" (which is also our primary domain controller (PDC) and Windows Internet Naming Server (WINS)), to register themselves as the designated "master browser" for their subnet. The "domain master browser" collects the lists of computers from each subnet's "master browsers" and shares that

list with all the other "master browsers". Eventually each master browser will have the list of all computers in all subnets.

This process breaks down when a "master browser" computer is not configured properly and doesn't communicate with the "domain master browser", and therefore will not contain the list of computers from other subnets.

## Resolution:

Correctly configured Windows 95/NT computers use only the NBT (NetBIOS over TCP/IP) protocol to communicate with other Microsoft computers. In order to communicate with a computer over NBT, you need to know the target machine's IP address. When you double-click on a machine name in the Network Neighborhood, your computer asks the WINS server to translate the NetBIOS name into an IP address. If for some reason if this fails, your machine then broadcasts on the local subnet asking for the computer to identify itself.

This system can fail if:

- the target machine is on another subnet and is configured in a way that causes it to not register itself with the WINS server.
- the WINS server entry is for the wrong machine.
- the WINS server is inaccessible (in certain circumstances, a particular type of configured machine can conflict and interfere with the WINS server)

## Tracking Problems

The program 'nbtstat -c' shows you the list of machines that your computer has recently communicated with. When you first boot up your machine and open the network neighborhood, the only machines in that list should be either a master or backup browser.

If that computer belongs to someone you know you could then let that person know that their machine may be configured incorrectly. It is also possible that that machine is just a "backup browser", and that the "master browser" that it communicated with is not configured correctly.

## Augmenting Enumeration with NetHood Entries

There is a folder called NetHood, which can contain shortcuts to machine names. Even if Enumeration fails, entries that have been manually placed in the NetHood folder will still appear in the Network Neighborhood. To make an entry in NetHood, drag the desired computer from the Network Neighborhood into the NetHood folder, which will create a shortcut to that computer.

The NetHood folder is located at C:\Windows\NetHood for Windows 95 users, and C:\WinNT\Profiles\[username]\NetHood for Windows NT users, where [username] is the username you logged into NT with. Your installation drive and directory may of course be different.

## Augmenting Resolution with LMHOSTS

The LMHOSTS file is similar to the /etc/hosts file on a Unix machine: it's a plain text file that maps computer names to IP addresses. For example:

```
128.2.35.168 helpcenter
```

When you double-click on a computer name, your computer checks the following places, in order, to resolve the name:

- The internal name cache of recently accessed machines
- WINS
- Send a broadcast to the local subnet
- LMHOSTS

You can force an entry to be loaded into your name cache at boot time with the #PRE keyword:

128.2.35.168 helpcenter #PRE

When your machine boots, it reads the LMHOSTS file and enters any entries with the #PRE keyword into the name cache. Such entries do not time out. By default, the name cache can only hold 16 entries.

Your computer does not have an LMHOSTS file by default, but it will have a sample file named LMHOSTS.SAM. You can search on your hard drive to locate this file.

## Potential Problems

Enumeration and Resolution are dynamic protocols, meaning that you can still get to a machine even if it's IP address changes (which can happen if they move to a different building, install a different Ethernet card, or addresses are reassigned during network upgrades).

NetHood and LMHOSTS use "static" entries, meaning that if for some reason the IP address of the machine changes, you won't be able to get to it at all.

NetHood and LMHOSTS is not a general solution, and not a long term solution, but it may help you access your friends machines during times that peer-to-peer networking is otherwise inaccessible.

For help on configuring an lmhost file, please refer to [Configuring LMHOST](#).

## Disclaimer

These suggestions are offered "as-is" to assist students in using peer-to-peer networking, but do not imply any level of support. Peer-to-peer networking is unsupported by Computing Services, which includes the functionality of WINS, the NetHood folder, and the LMHOSTS file.