

# How to Enable Browsing Using NetBIOS Over IP

Document ID: 17057

---

## Introduction

### Prerequisites

- Requirements
- Components Used
- Conventions

### Background Information

- Set the Workgroup Name to be the Domain Name
- Disable the Master Browser
- Network Diagram

### Individual Users: How to Browse With NETBIOS Over IP Across Routers

- Network Diagram
- Configure the Local Router to Bridge
- More NetBIOS Hints

### Related Information

---

## Introduction

This document describes how to use IP across the access router to reach the Primary Domain Controller (PDC) and Windows Name Service (WINS) server, and how to set up a PC to reach the WINS server.

## Prerequisites

### Requirements

Readers of this document should have knowledge of these topics:

- How to set the workgroup name to be the domain name. For more information, see Set the Workgroup Name to be the Domain Name.
- How to disable the master browser on all Windows 95 machines on the broadcast domain. For more information, see Disable the Master Browser.

### Components Used

The information in this document is based on these software and hardware versions:

- A WINS server.
- A PDC where the login name of the user exists.
- A PC running Windows 95.

**Note:** In most cases, you will use domains, and not workgroups (WINS and NetBIOS over TCP (NBT), for example, work without domains).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

## Background Information

This section provides the required background information for you to proceed with this document.

### Set the Workgroup Name to be the Domain Name

To set the workgroup name to be the domain name, complete these steps:

1. On the PC running Windows 95, click the **Start** button, select **Control Panel**, then click **Network**.
2. From the network components list, select **Client for Microsoft Networks**.
3. Click the **Properties** button.
4. When the client window is displayed, type your domain name in the **Windows 95 Domain** box. Click **OK**.

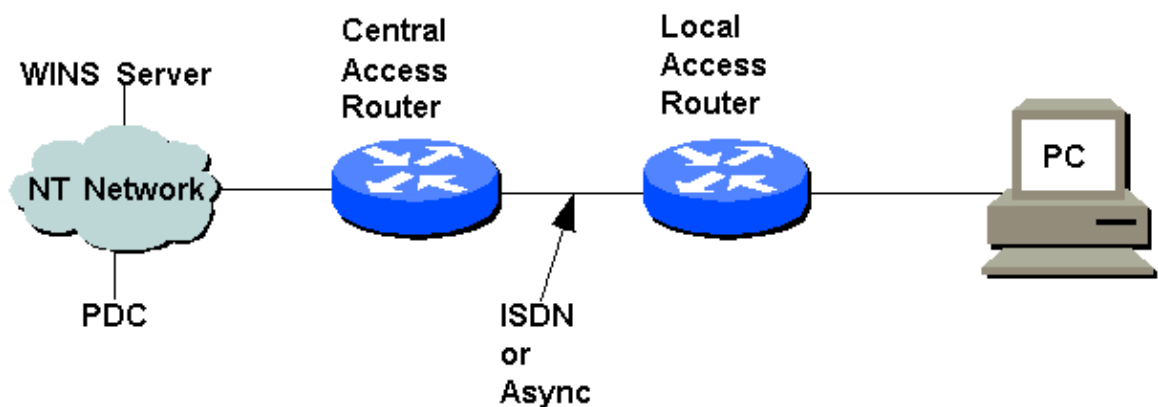
### Disable the Master Browser

You need to ensure that the master browser is disabled on all computers that have Windows 95 installed on the broadcast domain. This is because, if you do not do so, they will break browsing for all computers on that wire, and render them invisible to the domain browsing. Complete these steps:

1. Click the **Start** button, select **Settings**, and click **Control Panel**.
2. Select **Network**.
3. In the Network window, select **TCP/IP <card manufacturer and model> Adapter**.
4. Click the **Properties** button.
5. In the TCP/IP Properties window, click the **Advanced** tab.
6. If there are any entries for Master Browser, select the entries, and change the value to **Off**.

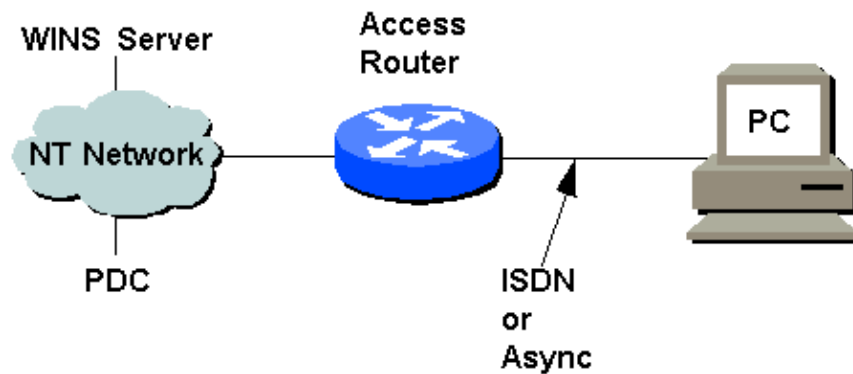
## Network Diagram

Here is the network diagram that represents the general setup described in this document:



## Individual Users: How to Browse With NETBIOS Over IP Across Routers

## Network Diagram



If the user uses Async or Integrated Service Digital Network (ISDN) to dial in from an individual end host, and the user wants to browse, you need to complete the steps in the Set the Workgroup Name to be the Domain Name and Disable the Master Browser sections. You will also need to provide RFC1877 information through global commands on the router that accepts the dialing connection:

1. Set **async-bootp dns-server x.x.x.x** (x.x.x.x is the DNS server).
2. Set **async-bootp nbns-server y.y.y.y** (y.y.y.y is the WINS server).

## Configure the Local Router to Bridge

**Note:** It is recommended that you use domains.

**Note:** If you cannot use domains, you need to flood broadcasts. This is not yet possible on Async lines.

On LAN interfaces, complete these steps:

1. Run these commands:

- ◆ **ip forward-protocol udp 137**
- ◆ **ip forward-protocol udp 138**
- ◆ **ip forward-protocol spanning-tree**

2. Next, configure bridging on all interfaces that require flooding. This will create a Spanning-Tree to flood IP broadcasts. The command reference manual for the **ip forward-protocol spanning-tree** command says:

Packets must meet the following criteria to be considered for flooding:

- ◆ The packet must be a MAC-level broadcast.
- ◆ The packet must be an IP-level broadcast; that is, an all-network broadcast (255.255.255.255) or major network broadcast (131.108.255.255, for example).
- ◆ The packet must be a Trivial File Transfer Protocol (TFTP), Domain Name Service (DNS), Time, NetBIOS, ND, BOOTP packet, or a User Data Protocol (UDP) specified by the **ip forward-protocol udp** global configuration command.
- ◆ The Time-To-Live (TTL) value for the packet must be at least two.

A flooded UDP datagram is given the destination address specified by the **ip broadcast-address** interface configuration command on the output interface. The destination address can be set to any desired address.

Thus, the destination address can change as the datagram propagates through the network. The source address is never changed. The TTL value decreases. After a decision has been made to send the datagram out on an interface (and the destination address possibly changed), the datagram is handed to the normal IP output routines, and is therefore subject to access lists, if they are present on the output interface.

The **ip forward-protocol spanning-tree** command uses the database created by the bridging Spanning-Tree Protocol (STP). Therefore, the transparent bridging option must be in the routing software. In addition, bridging must be configured on each interface that must participate in the flooding in order to support this capability. If an interface does not have bridging configured, it still will be able to receive broadcasts, but it will never forward broadcasts received on that interface. Also, it will never use that interface to send broadcasts received on a different interface.

If no actual bridging is required, you can configure a type-code bridging filter that will deny all packet types from being bridged. Refer to the Configuring Transparent Bridging chapter in the Bridging and IBM Networking Configuration Guide for more information about using access lists to filter bridged traffic.

**Note:** You can use the Find feature in your browser to locate the section mentioned above.

The Spanning-Tree database is still available to the IP forwarding code to use for the flooding. The Spanning-Tree based flooding mechanism forwards packets whose contents are all ones (255.255.255.255), all zeros (0.0.0.0), and, if subnetting is enabled, all networks (131.108.255.255 as an example in the network number 131.108.0.0). This mechanism also forwards packets whose contents are the zeros version of the all-networks broadcast when subnetting is enabled (for example, 131.108.0.0).

## More NetBIOS Hints

For IPX-based NetBIOS, issue the **ipx type-20-propagation** command to allow input and output of type 20 propagation packets on all interfaces for browsing to work. Type 20 packets are subject to loop detection and control as specified in the IPX router specification.

For NetBIOS Extended User Interface (NetBEUI) based NetBIOS, all participating interfaces need to bridge.

For more details on NetBIOS over IP related issues, see Domain Browsing with TCP/IP and LMHOSTS Files .

Alternatively, you can browse to the Microsoft support site, and search for article **Q150800**, which is titled *Domain Browsing with TCP/IP and LMHOSTS Files*.

---

## Related Information

- **Technical Support – Cisco Systems**

---

Contacts & Feedback | Help | Site Map

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

---

Updated: Sep 01, 2005

Document ID: 17057

---