OrbitNet™

A User's Manual

Publish Date: November 1999.

Orbit Co0mmunication Cop.
P.O Box 74
Sudbury, MA 01776-0074
USA

Table of Contents

INTRODUCTION TO ORBITNET

Proxy *(pròk'sê) noun: A person authorized to act for another; an agent or substitute.*

Welcome to OrbitNet 3.0, the finest firewall proxy server available for Windows 95/98 and NT 4. As you'll soon discover, OrbitNet will transform every aspect of your Internet experience. In today's world, when Internet access is a key factor in your business and personal life, OrbitNet gives you all the access you need:

- **Easy Access**. OrbitNet is easy to install. You simply load OrbitNet on one computer—the one with an existing Internet connection—point the other PCs in your network to the OrbitNet PC, and you're done! No special software is required on the network's client computers.
- **Simultaneous Access**. All your PCs, linked to the Internet through a single modem or other connection, can now be online at the same time.
- **Transparent Access**. Thanks to the simplicity of Network Address Translation (NAT) technology, combined with the flexibility of our classic proxy server, OrbitNet is a transparent proxy. When accessing the Internet, users will see no difference after OrbitNet has been installed.
- **Affordable Access.** With all your computers sharing a single phone line and one Internet Service Provider, you'll see big savings. And the more computers you have, the more money you'll save.
- **Secure Access.** Your computers and the valuable data they contain are now protected from Internet pranksters, hackers and other intruders. And you're also protected from Net-borne viruses.
- **Fast Access.** Advanced network-wide caching makes for speedy page loading and quick access to frequently-visited sites. No longer will you have to wait…and wait…and wait…for your favorite pages to download.
- **Controlled Access.** You'll find it easy to restrict user access to sites you consider objectionable, and you can easily limit access to certain hours of the day.
- **Applications Access.** You'll gain quick access with your favorite Internet browsers and to Internet applications like Email, News, and Chat groups. OrbitNet operates transparently—just click on your browser or other Internet application, and you're online.

In addition to OrbitNet's versatile accessibility, you'll gain powerful new capabilities for working with:

- **Any Internet connection**, including modems, cable modems, DSL, ISDN, Frame Relay, T1-T3, Wireless Links.
- **All popular protocols**, including HTTP, Real Audio/Video, Mail, FTP, News, Telnet, Socks, Secure Sockets, DNS, IMAP 4, and more.
- **Any Internet Service Provider**, including AOL and MSN.

Finally, OrbitNet provides you with many extras, including:

- **Banner Ad Blocking**. At last, freedom from the irritating banner ads that seem to accompany every move on the Web. OrbitNet allows you to block them before they're downloaded; you'll never notice them again.

- **Telephone technical support**. Orbit Communication Corp., makers of OrbitNet, offers technical support via telephone, email or at our online SupportBase.

Once you become accustomed to OrbitNet, you'll never have a reason to leave. Whether your computer access capabilities expand or grow smaller, five separate user editions of OrbitNet 3.0—suitable for 3, 5, 10, 25 or an unlimited number of users—can match your needs. Each edition has the same functionality, differing only in the number of users it will support.

HOW TO USE THIS BOOK

The OrbitNet User's Manual tells you everything you need to know to install and use OrbitNet. You'll also learn the ins and outs of networking, how to set up your own LAN, and how to take advantage of OrbitNet's advanced features.

- If you're a beginning networker—or if you're experienced but lack a functioning LAN—start at the beginning and work your way through.
- If you're familiar with networking, browse the early chapters before skipping ahead to "Section III: Beyond the Basics."
- If you're an experienced networker with a working LAN, you may want to proceed immediately to the Quick Start in Appendix A.

Chapter 1

The Basics

Chapter 1: THE BASICS

What Is A Network?

In its simplest form, a network consists of a group of connected computers sharing resources such as documents and printers. A term you'll often hear to describe computers connected in this way is "local-area network," or LAN.

Networks are popular because they can save a great deal of time and money. Imagine a five-person office in which all five computers are connected to each other and to a single printer. Only one computer is connected to a phone line.

Just a few ways in which this setup would be time- and cost-effective include the ability to:

- **Buy fewer floppy/zip disks**: Business plans, letters and other documents can be sent back and forth electronically, removing most of the need for disks.
- **Buy/service/depreciate fewer printers and other expensive peripherals**: If everybody in the office uses one printer instead of five separate printers, the costs of buying and operating four printers completely disappears.
- **Pay a smaller monthly telephone or ISDN bill**: Since a single phone/ISDN line gives Internet access to everyone, monthly charges are saved on four other lines. You can save on both phone lines and the number of user accounts.

Servers and Clients

You may have heard networks described as "peer-to-peer" or as "client-server."

A peer-to-peer network is one in which all of the machines connected together have the same capabilities. A network put together with tools built into Microsoft 95/98 , NT 4 or Win 2000 is a peer-to-peer network.

In client-server networks, one computer—called the server—is designated to serve the needs and carry out requests from the other computers, called clients. It's similar to being waited on in a restaurant: you're a client, and the person who brings the meal you requested is the server.

The distinction between peer-to-peer and client-server networks has blurred as desktop computers have gained power. It's become common for a network to have characteristics of both, and the distinction is more often made at the applications level than at the machine level. You can have one computer acting as a file server and another as a mail server on a network that is otherwise peer-to-peer.

OrbitNet is server software. This means that, when it's installed on a computer, that computer becomes the network's proxy server. The other computers on the network are client computers.

The computer running the proxy server software—called the OrbitNet computer or the server throughout this book—can also be a client computer. This may sound confusing but it really isn't. It simply means that the OrbitNet computer fulfills its job as a proxy server, but other applications on that computer can be clients to the proxy server. The OrbitNet computer doesn't need to dedicate itself solely to proxy tasks—you can keep using it for your regular computing.

NATS, Proxies and Firewalls

A proxy is simply someone/something who acts on behalf of someone/something else. Think of OrbitNet as a trusted, computerized associate who acts for you on the Internet.

NAT stands for Network Address Translation. It's a simple, efficient technology used for connecting one Internet address to another.

Both NATs and Proxies provide methods to connect computers on private networks to the Internet at large, while making it appear to the Internet that all of the connections from that private network come from one computer.

A NAT provides an easy interface and is transparent to the application, but provides little opportunity for the user to modify or control the connection.

A Proxy provides much more control and makes possible a greater range of features to the user, but can only be used by proxy-supported applications. Most major Internet applications have such support, but many packages do not.

In real-world terms, a firewall is a fireproof wall used as a barrier to prevent the spread of fire. In computer parlance, a firewall acts as a barrier to Internet intruders. In other words, it protects networked computers (behind the firewall) from unwanted access by Internet computers (outside the firewall). At the same time, it allows networked computers to gain access to the Internet.

Acting as a proxy, the OrbitNet computer gains access to the Internet on behalf of the other computers on your network. Then it acts as a firewall, preventing Internet intruders from gaining access to your computers and wreaking havoc with your data.

The OrbitNet 4.0 Network

OrbitNet 4.0 is a combination NAT/Proxy/firewall server designed to run on computers using Windows 95/98/2000or NT4. The other computers on your network can run on any operating system capable of communicating with the TCP/IP protocol, including Mac and Unix/Linux systems. Every computer on the OrbitNet network can access the Internet through the OrbitNet computer and its single Internet connection. All network computers can attain simultaneous access while the users appear, to computers on the Internet, to be at the same computer address.

All computers on the network operate behind a protective and secure firewall. Although people inside the firewall can connect out, people on the outside cannot connect to computers behind the firewall. This provides security to the data on your network's computers.

Security is very important to those of us at Orbit Communications. You'll notice throughout this guide that we offer many tips to enhance your network's security.

Chapter 2

Before Setting up OrbitNet 3.0

CHAPTER 2:
BEFORE SETTING UP ORBITNET 4.0

Overview of OrbitNet Setup

Many software applications don't require much in the way of preparation: you just pop in a CD-ROM and, after a couple of mouse clicks, you're on your way. If you already have a functioning TCP/IP network, OrbitNet's installation can be just that easy. If you don't, we urge you to lay a proper installation groundwork by gathering the information and hardware you'll need before you start. Doing so ensures that you'll have no problems during setup.

This section tells you what needs to be done—and, when appropriate, shows you how to do it—before installing OrbitNet. There are seven categories of preparation, but you've probably already met the requirements in at least a few of them. The categories are:

- System Requirements
- Internet Connection
- Internet Service
- Network Hardware
- Addressing Information
- TCP/IP Protocol
- Your OrbitNet Serial Number

Most people will have other computers—clients—on their networks (some single-computer users, with no need of simultaneous access, will nonetheless install OrbitNet for its superior security capabilities). You should know that, as long as they have TCP/IP installed, clients can be almost any type of computer, including PCs, Macs, or UNIX/Linux-based systems.

The following chart provides a checklist of requirements to be met, and the remainder of this section gives a brief overview of each. Additionally, more comprehensive information about network hardware, addressing, and TCP/IP is contained in later chapters.

OrbitNet Computer Pre-Installation Checklist

√	*CATEGORY*	*REQUIREMENT*
	OrbitNet PC	IBM PC/compatible computer
	Processor	90MHz Pentium or better
	Operating System	Windows 95/98 OR Windows NT4
	Disk Space Needed	26MB RAM: • 3 MB for OrbitNet software • 3 MB for anti-virus program • 10 MB for optimal caching • 10 MB for site filtering
	Internet Connection (OrbitNet Computer Only)	One modem or other connecting device (cable modem, DSL, ISDN, T1-T3, frame relay, wireless)
	Internet Service	One user account through an Internet Service Provider

	Network Hardware	• Clients: 1 Network Interface Card (NIC) each. • Servers: 1 LAN connection NIC or equiv); 1 Internet connection (dial-up adapter or another NIC). • Optional hub and cables depending on network configuration.
	Addressing Information	Nothing needed unless you disable NAT and use Classic Proxy. If so, you'll need IP addresses for news, mail, and pop servers (available from your service provider).
	TCP/IP Protocol	The TCP/IP protocol that is standard in Windows and NT will do just fine
	OrbitNet Serial #	Obtained at time of purchase (located on the back of the Quick Start Guide contained in the jewel case). Not needed for 30-day trial period.

SYSTEM REQUIREMENTS

To run OrbitNet, your system must be an IBM/PC or compatible computer running Windows 95/98/2000 or NT, with at least a 90 MHz processor chip. While the application itself uses only a small amount of disk space, 26 megabytes of disk space is recommended to take advantage of OrbitNet optional capabilities (caching—the storage the program uses when retrieving web pages—is available only if you enable browsing through the Proxy). However, you can get away with less, depending on the size of your network.

INTERNET CONNECTION

You'll need one modem (or other type of connecting device, such as a cable modem) on the OrbitNet computer. Any Internet connection that uses TCP/IP works, including ISDN, T1–T3, Frame Relay, DirectPC, and wireless.

INTERNET SERVICE

Internet Service Providers, or ISPs, provide access to the Internet and to mail and news servers. ISPs can be large and nationwide like Netcom or WorldNet, or they can be small and local. A user account from any Internet Service Provider is needed to access the Internet once OrbitNet is running. You'll need only one account, since, by using OrbitNet, all computers on your network can gain Internet access through the same account.

NETWORKS HARDWARE

The exact kind of network hardware you use depends on the kind of access you have to the Internet.

Dial-Up Access. If you're using a modem, you must use dial-up access. For each computer on the network you'll need an installed and operational network card. You'll also need one network hub and a cable for each computer connecting to that hub.

Cable Modem/ADSL Modem/Direct Access. Each computer needs an installed and operational network card, as well as one additional card for the OrbitNet computer (for connection to the Internet).

You'll also need a hub if you have more than two computers, and a cable for each computer connecting to the hub.

More details about network cards, cables, and hubs are contained in "Section II: Preparing for OrbitNet."

ADDRESSING INFORMATION

Computers need addresses to which various kinds of data can be sent. If you'll be doing the easy OrbitNet setup using transparent proxy/NAT connectivity (which we recommend for beginners), you can skip this section. The reason: that particular configuration allows OrbitNet to determine all addresses for you.

However, if you'll be using the more advanced Cproxy or Tproxy setups, you may need to provide certain addressing information to OrbitNet, including any or all of the following: ISP news servers, mail servers, pop servers, and DNS servers. You may have received this information when you first joined your current ISP. If not, you'll learn how to obtain it in Section II.

TCP/IP PROTOCOL

TCP/IP is the Internet's official "language," or protocol, which allows computers to communicate. All communication between and among the OrbitNet computer, clients, and the Internet use the TCP/IP protocol. The TCP/IP protocol capability is supplied as part of the standard installation of Microsoft Windows 98 (it must be manually added for Windows 95).

YOUR ORBITNET SERIAL

When you download OrbitNet, you have full use of the program and all of its features for a 30-day. At the end of thirty days OrbitNet becomes unresponsive except for the menu, which allows you to enter a serial number. You'll receive a single reminder notice via email about five days before the 30day period ends.

You can enter a serial number at any time. When you do, the copy of OrbitNet you have downloaded returns to full functionality.

ANTI-VIRUS AND SITE-FILTERING SERIAL #'s

The Anti-Virus and Site-Filtering options are also operational during the 30-day trial period. When you purchase and install a OrbitNet serial number, the Anti-Virus and Site-Filtering options are automatically enabled for a 6-month period. You can purchase additional extensions for these options at any time from our website or by calling our toll-free number, 1-888-OrbitNet. The new extensions are enabled when you enter the newly-purchased anti-virus or site-filtering serial number in the box provided. If you purchase and install an extension before your previous period has expired, the new extension is added onto the existing period.

After the initial 6-month period, these features will be disabled unless you purchase the extensions. Anti-Virus and Site-Filtering extensions can be purchased separately.

Chapter 3

Setting Up Your Own Local Area Network

CHAPTER 3: SETTING UP YOUR OWN LAN

Overview: LAN

This chapter shows how to set up a local network in your home or office (if you already have a functioning network, feel free to skip to the next chapter). In the next few pages, we'll take a look at:

- The basics of network hardware
- Basic hardware requirements for your local network
- Installing the hardware and setting up a local peer-to-peer network
- Inspecting and changing network settings

A. NETWORK HARDWARE BASICS

Cables. We recommend Category 5 cables for new users. Officially called Ethernet 10/100BaseT, they're the most common type of network cable and provide a good upgrade path should you need it. Cat 5 allows either 10- or 100-megabyte communication. These terms have simple meanings, so don't let them put you off:

- The "10" or "100" in 10/100BaseT refers to network connection speed—i.e., 10 Megabits or 100 Megabits per second. Most networks actually top out at less, though most users would never know.
- The "T" in BaseT refers to the wire type, twisted-pair, which consists of pairs of thin wires twisted around each other. It also refers to the connector, commonly called an RJ-45, which resembles a bigger and wider telephone connector.
- "Base" means that the cable is used for baseband (i.e., simple, single frequency) rather than broadband (multiplex or analog) networks.

Cables can be purchased in different lengths and often different colors. They come with a male RJ-45 plug at each end. Cards and hubs have female RJ-45 jacks.

Network Cards. A wide variety of network cards—officially called Network Interface Cards and nicknamed NICs—is available. Most do at least an adequate job. If you're a novice networker, the primary things to look for are:

- Connection Jack. Be sure the NIC's jack matches the type of cable you're using. If you're using 10BaseT cable, for instance, the NIC you buy should have an RJ-45 compatible connector.
- Plug and Play compatibility. This feature allows Windows 95/98 to automatically configure the card, saving you a lot of time in the process.
- Interrupt Addresses. Interrupts on any machine are at a premium, so you'll want to determine which ones the NIC has available. Generally, the more you pay, the more latitude you'll have. ISA-bus cards are usually fast enough for a 10BaseT network; if you're running 100BaseT you'll probably want to go with PCI-bus card for speed. If you've only got one interrupt left and must add two cards, use two PCI-bus network cards; part of the PCI spec is that cards can share interrupts.

NOTE

Running Windows95/98? Look in **ControlPanel/System/DeviceManager/ Properties/IRQ** for a list of available interrupts, as well as to determine if the card can utilize remaining interrupts.

Hubs. Ethernet is a standardized way of connecting computers together to create a network. A hub is an ethernet device used in conjunction with 10BaseT and 100BaseT cables. The cables run from the network's computers to ports on the hub. Using a hub makes it easier to move or add computers, find and fix cable problems, and remove computers temporarily from the network (if they need to be upgraded, for instance).

Hubs are available in most computer stores. It's probably a good idea to buy one with more ports than you need, just in case your network expands. Look for:

- A connection jack compatible with your cabling.
- A cascading jack which allows you to add an additional hub later, if necessary, without replacing the entire unit.
- Lights on the front. These can be useful when you're trying to diagnose network connection problems.

B. HARDWARE FOR YOUR SPECIFIC LAN REQUIREMENTS

The kind of hardware you use depends on the kind of access and/or modem you're using.

If you're using dial-up access you'll need:

- One network card for each computer.
- One hub.
- A cable for each connection to the hub.

If you're using cable modem, DSL modem or direct access you'll need:

- One network card for each computer.
- One additional network card to connect to the modem (your OrbitNet machine receives two cards, one for the modem and one for the local network).
- One hub.
- A cable for each hub connection.
- An additional cable for the connection from the computer to the modem. If the modem is the type that connects directly to the hub, make this last cable a cross-over cable instead and you'll still be able to connect directly to the network card as shown.

Before you rush out and buy a ransom's worth of network hardware, however, take a few moments to draw a topography—a diagram which shows the relation between the network's various components. Doing so lessens the chance that you'll buy unnecessary cables or forget to buy a hub.

Let's look at a very simple topography. Assuming that you already have Internet access through an ISP, you're probably connected to the Internet in this manner:

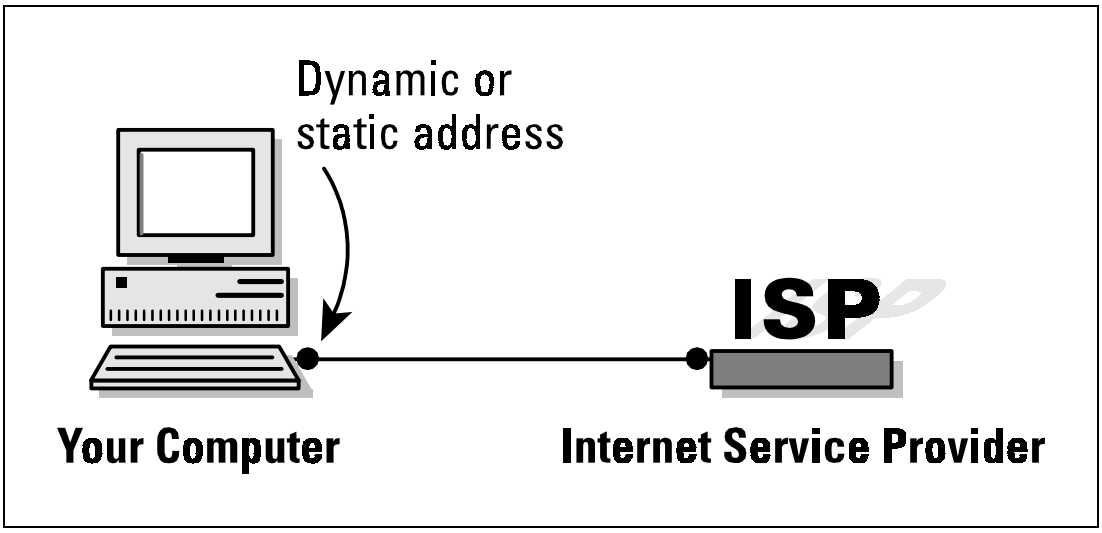


Figure 3-1: Topography for a simple Internet connection.

Now let's look at the topography for a simple LAN. The network shown here—the number of client machines can be far greater, of course—is the standard configuration for most setups, including dial-up access and cable-modem access:

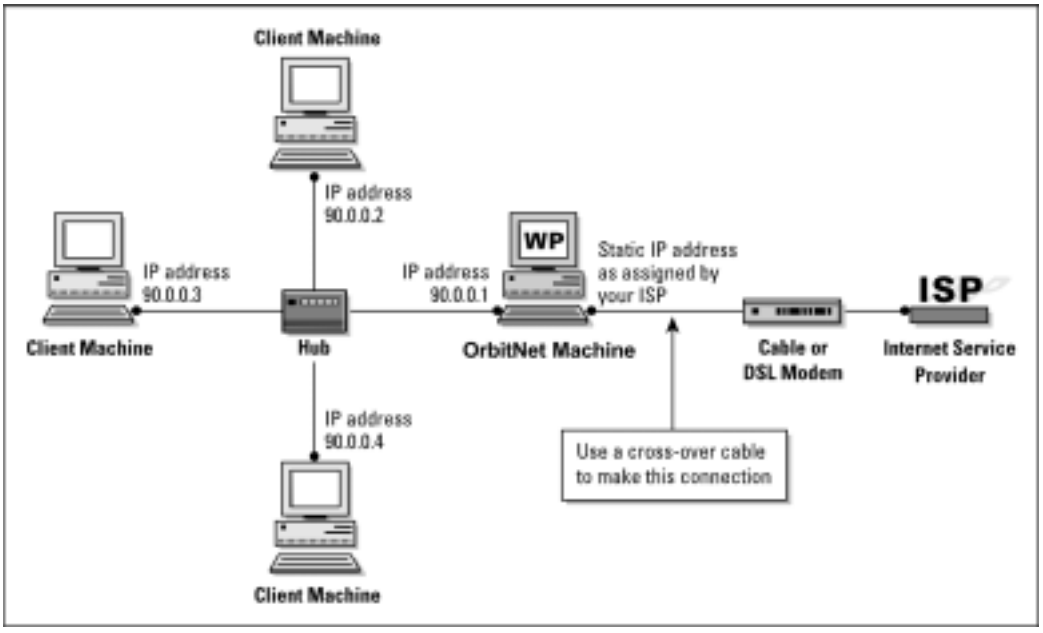


Figure 3-2: This topography shows a standard setup for a simple local area network with cable or DSL modems.

As you can see, only one computer—the OrbitNet computer—has a modem. The other computers are connected to each other and to the OrbitNet computer by a device called a hub (more on this later).

The computer using the modem and receiving the OrbitNet installation must be a Windows95/98 or Windows NT machine. Other computers on the local network can be any kind—including Macs, Unix boxes, and WfWG3.11—as long as they're capable of "speaking" TCP/IP.

Once you've drawn your network topography, including all components, make a list of everything you need.

Notes

1. Many cable modem providers insist on installing the cable modem card themselves, and may insist upon using their own card. Before purchasing your own cables and cards, check to see what the provider's policy is.
2. If you have only two computers, it's possible to save the expense of a hub by connecting them back-to-back. To do so, run a cross-over cable directly from one network card to the network card on the other machine. IP addressing will still be done as described here

C. HARDWARE INSTALLATION/SETTING UP THE PEER-TO-PEER NETWORK

The best way to install an NIC is to simply follow the manufacturer's directions. Win95/98 usually finds a new card when it starts up and then configures it for you. If it doesn't, consult the directions that came with the card.

Run a cable between each card and the hub (except for the external network card if you have a cable modem setup). Although you can probably get away with plugging/unplugging a cable from a card while the computer is running, it's safer to do it when the computer is turned off. You can usually plug or unplug from the hub at any time.

You'll need at least one protocol assigned to each card once it's installed. Choose NetBEUI (NetBios Extended User Interface) at a minimum; you can have others as well. There isn't any problem with having multiple protocols on your local network. You'll need the TCP/IP protocol later in order to run OrbitNet, but it's not needed now when setting up a basic peer-to-peer network. Set up your basic network first, get it working, and we'll add TCP/IP later on.

During the card setup, you'll be prompted for certain settings. If not already installed, be sure to add for each machine:

- Client for Microsoft Networks
- File and Printer Sharing

You can make changes to your settings at any time in the future. You must reboot the computer for the changes to take effect.

D. INSPECTING AND CHANGING NETWORK SETTINGS

At this point, let's double-check the computer network setup at **Control Panel/Networks**. In the window under the Configuration Tab, you'll see a list of adapters and protocols.

A typical setup is represented by a couple of small computer-shaped icons, one captioned *Client for Microsoft Networks*, and the other *File and Printer Sharing*. You'll also see small green icons, similar in shape to a network card—one for each network card, and one for the Dial-Up Adapter (the Dial-Up Adapter counts as a network connection, with its own set of addresses and protocols). Finally, you'll see a series of

wire-and-node icons, each listing a different protocol-and-adapter combination, written in a form something like *NetBEUI → NE2000 Compatible Card*.

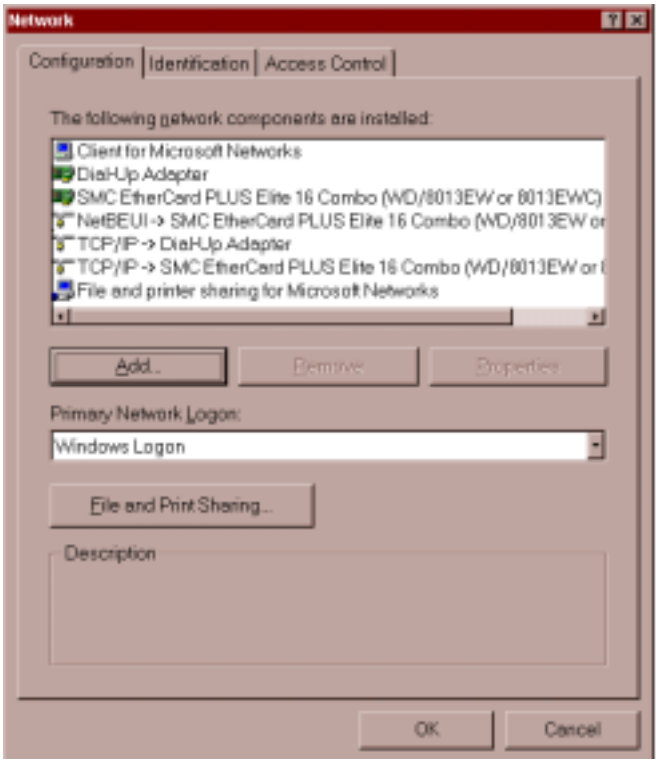


Figure 3-3: The Configuration Tab under Networks allows you to fine-tune your network settings.

If you haven't already added *Client for Microsoft Networks*, do so now:

- Highlight an adapter.
- Click through the path **Add/Client/Microsoft/Client for Microsoft Networks**.

To add a protocol capability to a network card:

- Highlight the network card.
- Click through the path **Add/Protocol/Microsoft/Your Protocol.** Click on the Identification Tab, where you'll see three entry boxes titled:

Computer name: A name assigned by you to a computer (each computer on the network should have a unique name). Avoid punctuation marks. These names are frequently used in network configurations, and you'll save confusion later by assigning distinctive names now. *Old486* is a good name if you only have one 486 computer, but if you have several, assign them names like *PapaBear*, *MamaBear*, etc. NetBEUI uses this name to find things so it can perform its networking magic. You'll sometimes see this computer name referred to as "the NetBios name."

Workgroup Name: A group name you can assign to all the computers on your network (or you can use the default).

Computer Description: A caption that gives users on your local network information about an individual computer. An example: *Maria's Computer*.

> **Security Alert**
>
> The designated protocol will usually be assigned exactly as you've requested. (In Windows 95 and 98, however, Microsoft assigns the NetBEUI protocol to all network adapters when you assign it to any single network adapter). If you don't want that protocol in the other locations, highlight each one you don't want and click **Remove**.

A Final Word on Your LAN

Congratulations! You now possess a working local network. You can see the other computers, move files between them, and print documents.

To prepare for OrbitNet and the Internet, you'll need to add the TCP/IP protocol to each of the computers on your local network. You'll learn how to do so in the next chapter. Once that's done, it's on to OrbitNet!

Chapter 4

Adding TCP/IP To Your Network

CHAPTER 4:
ADDING TCP/IP TO YOUR NETWORK

Overview: TCP/IP

The easiest way to install and configure OrbitNet is to first add TCP/IP—the language spoken by OrbitNet and the Internet—to your local network. This chapter covers the following topics:

1. Protocols and Addressing
2. Double-Checking Your Installed Network
3. Installing TCP protocol on your computers
4. Assigning IP addresses
5. Testing TCP/IP connectivity

A. FIRST THINGS FIRST: PROTOCOLS AND ADDRESSING

Protocols. In networking terms the word "protocol" refers to the accepted standards or rules for the way data is transferred between computers and over the Internet. When everybody uses the same rules, it all works. There are many protocols in use. The three commonly used by local networks are NetBEUI, IPX/SPX, and TCP/IP.

NetBEUI is an acronym which stands for NetBios Extended User Interface. NetBEUI is a networking standard well suited for small networks and is easy to set up. It is also non-routable; since it uses computer names to find its way around, it can't find distant computers.

IPX/SPX is Novell network's version of IP addressing, used on Novell NetWare networks for both small and large systems. It works on Novell networks, but not between different types of networks (as TCP/IP will).

TCP/IP, the language of the Internet, can be used on any size network. Data is sent over the network in chunks called packets. TCP (Transmission Control Protocol) is the protocol for packets of data sent over the wires. IP (Internet Protocol) is the addressing method used to get these packets to and from the right place. It is a routable protocol, designed to find distant computers. Some carefully-defined address groups are designated as intentionally non-routable; we'll be using one of these to set up TCP/IP on your local network in the next chapter.

Network Addresses. These addresses may be assigned manually by the user, or automatically by another computer. They're called static (i.e., fixed) assignments when assigned by the user, because they stay the same over time. When assigned automatically by computer, they're known as dynamic (i.e., changing) assignments. If you connect via a dial-up connection, you'll probably have a dynamic IP assignment to your Dial-Up Adapter. Your ISP assigns a different IP address to your Dial-Up Adapter each time you connect. If connecting with a cable modem, you'll most likely have to make a static IP assignment for your Internet connection. Once this assignment is made, the IP address will not change.

In addition, you'll also have the choice of static or dynamic addresses on most of your networked computers. You can either set static IP addressing information yourself or have OrbitNet make dynamic IP assignments for you.

Addresses are not assigned to the computer itself, though people often speak that way as a convenient shorthand. The addresses are actually assigned to each network connection. The computer on which OrbitNet will be installed, for instance, will have two network connections: an internal connection to the rest of your computers, and an external connection to your Internet Service Provider, or ISP.

In "Internet speak," any machine with a network address is called a Host. For most simple TCP/IP systems, each host is a computer, and each computer is a host.

The IP address is a 32-bit address, subdivided into four fields. Although it's a binary number, it's usually written in decimal form—222.5.83.47, for example. Each field can have a value from 0 through 255. However, since the end values are used for special purposes, the actual range available is from 1 to 254. What this boils down to for you, the user, is this: when entering an IP address, use only numbers between 1 and 254 in that last field.

Associated with the IP address is the subnet mask. This mask tells the computer which part of the address is unique to that machine, and which part is the general network address. Subnet masks allow you to accomplish many esoteric addressing capabilities; however, for most simple networks the subnet mask of 255.255.255.0 is the best and easiest choice. When you use this mask, the numbers in the final field of the IP address are unique to each computer, and the preceding three fields define the network address. To learn more about the intricacies of subnet masks, read "Appendix H: Network Knowhow."

Some specific IP address ranges are reserved for special uses. We'll discuss these later when setting up IP addressing on your local network. Network addresses reserved for testing or for local networks are 10.x.x.x, 90.x.x.x, 172.16-31.x.x and 192.168.x.x. These addresses all share a crucial distinction: routing computers on the Internet will not route these numbers. Since they are perfectly good numbers on a local network, but cannot be routed across the Internet, using them adds security to your local network.

Parts of a TCP packet are fields that specify the source and destination ports. These are 16-bit fields, and can thus specify more than 65 thousand ports. You'll see many references to ports when interfacing your local net to the Internet. Ports 1 through 1024 are set aside for specific uses. Each Internet protocol has a standard port assigned to its use (e.g., Port 25 to send mail, Port 119 for news groups). In many cases, things can be easier to follow if you consider a port designation to be part of the address; some software even allows you to specify an IP address and port combination in the same statement.

B. DOUBLE-CHECKING YOUR INSTALLED NETWORK

Before going further, let's double-check to be sure you have a basic network installed. At this point, after following the plan in Chapter 3, your network should look like this:

- Your computers are connected via a working Ethernet network.
- One of the computers has an Internet connection, and is using Windows 95/98 or NT. That computer gets the OrbitNet installation and will be known as the OrbitNet computer.
- You already have some network protocols installed, including NetBEUI, and your computers already have NetBios names. The NetBios name of each computer can be found at **Control Panel/Network/Identification/Computer Name**.

If your network doesn't match these specifications, please bring it into line, using Chapter 3 to guide you, before attempting to install TCP Protocol and OrbitNet.

On the other hand, if you do have a basic network, read on!

C. INSTALLING TCP/IP PROTOCOL ON YOUR COMPUTERS

All communication between the client applications and OrbitNet, and between OrbitNet and the Internet, use TCP/IP protocols. Thus, the first thing you must do is add the TCP protocol and IP addresses to the network's computers.

As you proceed, pay attention to the dictates of the following three connection types:

1. The external OrbitNet connection to the Internet. The type of IP address used—dynamic (commonly used for standard modems) or static (commonly used for cable modems)—is dictated by the ISP to which you connect and the type of service it provides.

2. The internal OrbitNet connection. This connection *must* be a static IP assignment, and it must be assigned by you. Two reasons exist for a static assignment. First, some client applications must have a single, known address for the proxy server; second, the static assignment is used by OrbitNet as a starting place for its DHCP assignments when providing tcp/ip assignments to your other computers.

3. The client computer network connections. These connections can be either dynamic or static. If they're dynamic, OrbitNet automatically makes all IP assignments and settings—the preferred method when using the OrbitNet 3.0 Install Wizard. If they're static, you must enter IP settings for each client computer. *We recommend dynamic assignments for new users.*

Several protocols can co-exist on a local network, and you'll usually need to have more than one. One protocol is sufficient on the connection to the Internet, and for security reasons you should have only TCP/IP. Let's proceed. To install TCP:

1. On the machine receiving the OrbitNet installation, click **Control Panel/Network/Configuration**. You'll see a list of installed new components, and there should be listings for a Dial-Up adapter and a LAN adapter (exact wording varies). Look under LAN adapter to see if you have TCP installed—if it is, the listing will read something like TCP/IP → LAN Adapter. Again, the exact wording varies.
2. If TCP/IP isn't listed, click through this path**: LAN Adapter/Add/Protocol/ Microsoft/TCP-IP/OK**. That's it! You'll be prompted to restart, finishing the installation. Do so if you like, or you can wait until completing the next step before restarting.
3. Return to the initial screen. Look under Dial-Up Adapter to see if you have TCP/IP installed. If not, click through this path: **DialUp Adapter/Add/ Protocol/Microsoft/TCP-IP/OK**. When prompted to restart the computer, do so.
4. Add the TCP/IP protocol to each client machine (unless it's already installed). The process is the same: in **Control Panel/Networks** look for a TCP/IP → LAN Adapter line, adding the TCP/IP protocol to the LAN adapter if it isn't already installed.

For Client Machines Only

After completing Step 4, take a quick look at any dial-up adapters. If any are installed and have the TCP protocol assigned, look under **Properties** to ensure that the dial-up adapter does *not* have the option **Assign a specific IP address** selected. It should be set to **Obtain an IP address automatically**. This will save you trouble down the road.

D. ASSIGNING IP ADDRESSES TO ALL NETWORK COMPUTERS

Each computer must be assigned a unique IP address. Strictly speaking, an IP address is assigned to each network connection, but it's convenient to speak of a "machine address."

If you set your client computers to **Obtain an IP address automatically** (see the boxed note immediately above), OrbitNet takes care of all of these settings for you.

We recommend using the 90.0.0.x series of addresses on your local network. You'll reap three major benefits by doing so:

- Your setup will match the numbers used for diagrams and instructions on the OrbitNet website.
- You'll find it much easier to follow explanations and trouble-shoot your network problems should the need arise.

- You'll add to the security of your local computers by using this non-routing series on your local network.

Now let's proceed to assigning IP addresses.

1. First, let's assign an IP address to the OrbitNet machine. To do so, follow this path**: Control Panel/Network Configuration/TCP/IP/LANAdapter/Properties**. Bring the IP Address Tab to the front. Click **Specify an IP Address** and enter an IP address and subnet mask. We recommend 90.0.0.1 and 255.255.255.0, as shown in the screen. You shouldn't need to make any changes on other tabs for this basic installation.
2. Use the method shown above to install an IP address on each client machine. It's easiest to use a sequential series such as 90.0.0.2, 90.0.0.3 and so on. Each computer gets a subnet mask of 255.255.255.0. Each IP address on your local network must be unique, and you can only vary the number in the final group—in other words, don't change the 90.0.0 portion of the address.

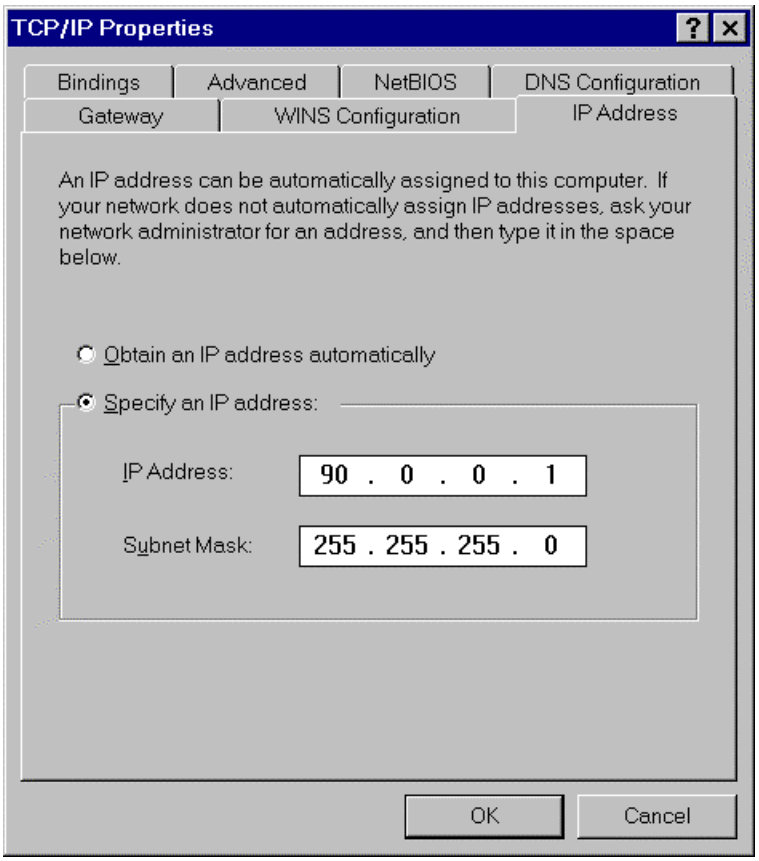


Figure 4-1: The TCP/IP Properties screen allows you to assign IP and subnet mask addresses to the computers on your network.

3. If you'll be using a dial-up connection to an Internet provider, the dial-up adapter does not get a specific IP assignment. Set it to **Obtain an IP Address Automatically**. The IP address for this

connection will be dynamically assigned by the ISP each time you connect. These addresses come from a pool, and will probably (but not necessarily) be different each time you connect.

4. If, instead, you'll be using a direct connection to your Internet provider (as many cable modems do), the network card connected to the modem should be assigned the IP address and subnet mask specified by your ISP for your individual Internet connection. Remember: you must have two network cards on this machine—one for the direct external connection to your provider and one for the internal connection to the rest of the computers on your local network.

   The network card connecting to the rest of your local network retains the IP assignment it received in Step 1, above. At the conclusion of your installation, click through to **OrbitNet/Settings/General/Multiple IP**. While there, check to see that the IP number assigned to your Internet connection is defined as an external connection, and the IP number assigned to your local network is defined as an internal connection.

E. TESTING TCP/IP CONNECTIVITY

Now that you've added TCP/IP to all your computers, let's run a test to determine if Network Neighborhood is up and running properly. If it is, you'll know that the hub and cables are working correctly. We'll use Ping for our test. It's a simple tool included in Windows 95/98 and NT that allows easy checking of TCP/IP connectivity.

First, open a DOS box (**Start/Program/MS-DOS Prompt in Windows 95/98,** and **Start/Program/Command Prompt in Windows NT**) and type the word **ping**. You'll see a list of commands and command syntax. If you're on, say, client machine 90.0.0.2, you can check your connectivity to the OrbitNet machine by typing in its IP address (90.0.0.1) after you type the word ping. If TCP/IP is properly set up on both machines you'll get several lines that say **Reply from 90.0.0.1…**, as shown in the screen below. If you get no reply, something is wrong with the protocol installation of the IP address on one (or both) machines.

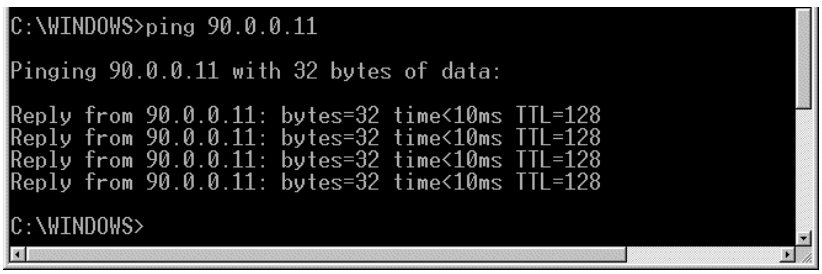


Figure 4-2: The ping program can be helpful when you're tracking down problems with your network.

This series of three tests, run on each machine with a communications problem, will probably help isolate the problem:

1. Ping 127.0.0.1 to ensure that your tcp/ip software is working.
2. Ping yourself to ensure that the card is working.
3. Test to see that you can communicate with another machine.

- To run the first test (pinging the loopback address), type **ping 127.0.0.1** at the DOS prompt. This verifies that the software TCP/IP stack on that machine is working and that the TCP protocol has been assigned (bound) to the card. The loopback address is specifically designated for such tests and doesn't

generate any actual network traffic. A failure at this point would implicate the software. If that's the case, consider re-installing Winsock from your Windows CD-ROM, or download and install the latest Winsock from Microsoft.

- Now ping the IP address of the OrbitNet computer, verifying that the card is working and IP addressing is correctly configured on that machine. If you discover a problem at this point, check to see that your network card is working properly. In Windows 95/98, go to **Control Panel\System\Device Manager** to see if there is a yellow exclamation point or question mark on your network card. If there is, click **Drivers**, and then choose **View Resources** to determine if Windows reports a conflict—e.g., an interrupt conflict. If so, you may be able to resolve the conflict by assigning an unused interrupt. If not, try reinstalling the card.
- Ping the IP address of another machine on your network. To work properly, the configuration must be correct on *both* machines. A problem at this stage usually indicates an IP addressing error. You've probably violated one of the basic IP rules, perhaps assigning the same number to two different machines, assigning a number outside the allowed range, or simply mis-typing an address. Check and double-check the assigned addresses.

If you get a response such as **request timed out**, it means that ping did not reach (or return from) the other machine. Look for misconfigured IP addresses or unplugged hubs. If your response is something like **destination unreachable**, then ping didn't know how to follow through on your request. You might get this response if, for example, you pinged an address with a different set of network fields. Look for misnamed nets or misconfigured subnet masks.

> ✔***USER'S CHECKPOINT***: If everything works except the last test (pinging another computer) an old proxy installation may be interfering. Proxy software that requires installation of software components on client machines as well as on the proxy server can cause tcp/ip communication problems. This software must be removed from each machine for proper tcp/ip communication.

If there seems to be a problem with a network card, go to **Control Panel/ System/Device Manager/View Devices by Type**. Look under Network Adapters. If you see a yellow exclamation point or question mark over the adapter, the system is having a problem with that adapter. Use the Win95/98 wizards to help track down problems. If you upgraded from Windows 95 to Windows 98, your network card drivers are probably out of date. Download new drivers made specifically for Windows 98 from the manufacturer's web site.

A Final Word on TCP/IP

Once TCP/IP is successfully working, you'll be ready to install and configure OrbitNet. The next chapter will walk you through this process step-by-step.

Chapter 5

Installing and Configuring OrbitNet

Chapter 5:
Installing and Configuring OrbitNet

Overview: Installing/Configuring

Now that you've added TCP/IP to your network, you're ready to install and configure OrbitNet. Two configuration Wizards built into OrbitNet will assist and guide you through this process, making the install quick and easy:

- **The Install Wizard** gets OrbitNet up and running using the program's default communications configuration. You'll be asked a few simple questions along the way and then verifies your Internet connection. Once this process is complete—about 10 minutes—you'll be completely set up with a secure firewall in place.
- **The Properties Wizard** allows you to fine-tune settings within OrbitNet, changing default configurations to those that more aptly suit your needs. The Properties Wizard helps make this task easy and straightforward—as long as you've obtained the information listed in the box below. You'll be prompted during installation to enter that information, so having the answers handy smoothes the entire process.

Important Note

If you access the Internet through a standard Internet Service Provider (ISP) ***or*** if you're an AOL user who has non-AOL applications requiring mail and news access, please obtain the following information from your ISP before running the Properties Wizard: (1) The name of the Dial-Up Networking connection used to connect to your ISP; (2) Your user name; (3) Your password.

Let's begin. The rest of this chapter guides you through the following steps.
Step 1: Installing OrbitNet.
Step 2: Running the Install Wizard.
Step 3: Running the Properties Wizard.
Step 4: Configuring Internet Applications on All Your computers.
When you've completed all four steps, OrbitNet will be up and running on your network.

A. INSTALLING ORBITNET

Installing the software is as simple as A, B, C:

1. Obtain the Software. You can purchase OrbitNet software in two ways: in retail stores or online.

If you'd like to go the retail route, you can buy OrbitNet on a CD-ROM at major office supply and computer stores.

To download the software, log onto our web site, www.Orbitsat.com/orbitnet.exe. Downloading gives you the added opportunity to evaluate OrbitNet for 30 days before purchase. Purchase can be made with a valid credit card either via a secure connection from our web site or by calling Orbit Communication Corp. directly at 978-440-8899.

2. Prepare the Software to Run. Depending on the delivery mechanism you've tosen for obtaining OrbitNet—CD-ROM or download—this step will vary.

If you're downloading OrbitNet:

- Go to our website, www.OrbitSat.com/OrbitNet.exe

- Choose **Save to Disk**. The saving process takes a few minutes. Once the file is downloaded, log off.
- When you're ready to install the software, click on the OrbitNet icon. The Win-Zip Self-Extractor will unzip the files you've downloaded. Follow the steps outlined in C, immediately below.
- *If you're using a OrbitNet CD-ROM:*
- Insert the OrbitNet CD-ROM in the computer's CD-ROM drive.
- The program will start. Follow the steps outlined in C, immediately below.

3. Run the Software. At this point, OrbitNet's Install Program begins. The chart below shows the screens you'll be seeing and gives a brief overview of what they're meant to accomplish.

1. Welcome	Advises you to close all currently-running Windows programs.
2. License Agreement	Choose Yes to accept license stipulations and continue installation.
3. Destination Directory	Where the software will be installed on your computer. The default is c:\OrbitNetSoftware\OrbitNet 4.0.
4. Type of Setup	Typical: All files are installed Compact: All files except Help are installed. Custom: You choose files for installation (experts only).
5. Select Program Folder	Choose the program folder to hold OrbitNet icons. The default folder is "OrbitNet 3.0."
6. Review Settings/Restart	Allows you to review chosen settings before installation proceeds. When you're ready, choose Yes to restart computer and complete installation of OrbitNet drivers.
7. Initialization	Information on contacting OrbitNet. If you've downloaded an evaluation copy you'll be reminded of the 30-day limitation.

You are now through running the software. You can proceed to Step 2, "Running the Install Wizard."

B. RUNNING THE INSTALL WIZARD

The Install Wizard runs automatically when you first install OrbitNet, and can be re-run again at any time by choosing **File\Install Wizard**.

Registration. Before proceeding to the setup, all users must register OrbitNet. If you've purchased your copy of OrbitNet, enter the serial number you were given. If you're using a 30-day evaluation copy, simply leave the serial number blank. Enter the other requested information—for the program to proceed, you *must* enter your name and email address. The information you enter will be saved, so you'll never need to repeat this process. *Remember: Orbit Communication Corp. Software respects your privacy. We do not and will not share this information with any third parties.*

Once you've registered the software, OrbitNet's Install Wizard will start.

Step 1: AOL Users. If AOL is installed on your OrbitNet machine, the first Install Wizard screen you'll see is shown in Figure 5-1 (if you don't have AOL installed, skip to Step 2).

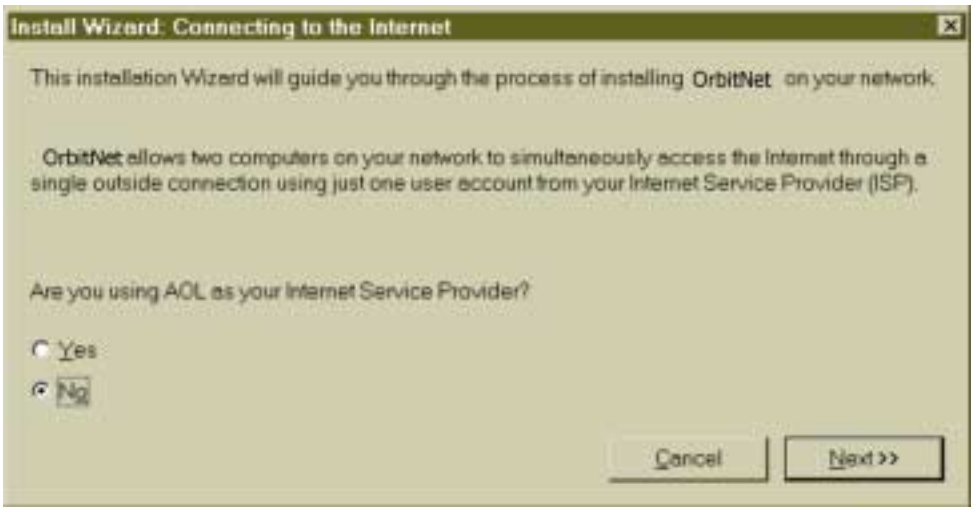


Figure 5-1: If you're an AOL user, this is the first screen you'll see with the Install Wizard.

If you dial in to an AOL server for your Internet access, check **Yes**. If you want to use an AOL account, but you dial into another service provider for access (like Best or Verio), choose **No**. And if you don't plan on using AOL at all, choose **No**.

Step 2: Dial-Up Connections. If you use a standard, analog dial-up modem for your Internet connection, choose **Yes** (OrbitNet implements Dial-Up using the Dial-Up Networking capabilities built into Windows). Proceed to Step 3.

If you plan to use a direct connection (like most cable or DSL modems), choose **No**.

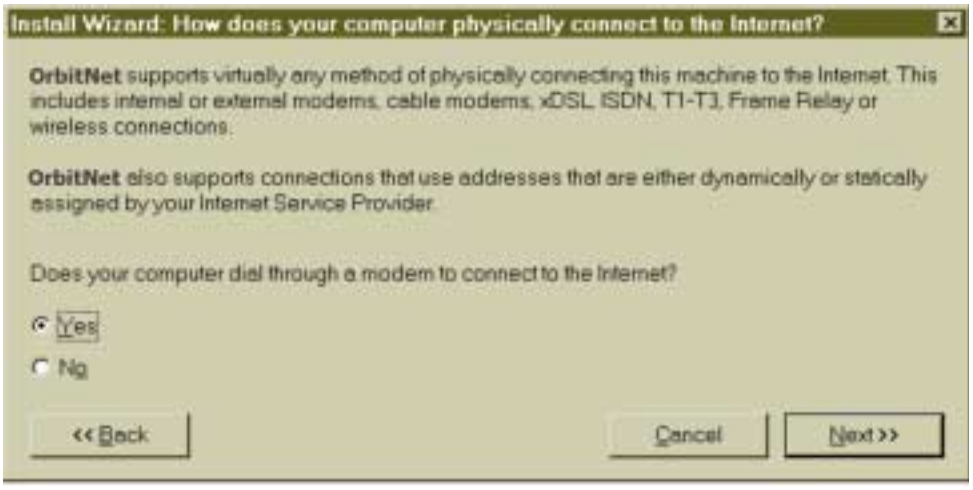


Figure 5-2: If you're using a Dial-Up Connection, this is the first screen you'll see when using the Install Wizard.

Step 3: Establishing Dial-Up Connections. Figure 5-3 appears only if you answered Yes in Step 2:

Figure 5-3: This list will only appear if you're using a dial-up connection.

What you see here is a list of all dialing connectoids that OrbitNet found on your computer. Highlight the one that you use to access the Internet. Click **Next** to get to the next screen.

Step 4: User Name and Password. Enter the same username and password used when you dial in to your Service Provider. Do so even though you already have this information recorded in the dial-up connectoid (because of the way that DUN is implemented, OrbitNet needs to have this information directly entered).

Figure 5-4: A sample screenshot in which both a user name and password have been assigned.

Case is important. Be careful to use the correct upper/lower-case characters, and be sure the CAPSLOCK and NUMLOCK keys are in the proper position when entering your password. Lastly, take care to not inadvertantly add extra spaces to either the username or the password.

If you've indicated that you use AOL as your Service Provider, the "Username" field will be greyed out. The AOL connector automatically uses the default username in the AOL browser, but you still need to enter the password here.

When you're through, click **Next**.

Step 5: Network Configuration. OrbitNet now looks at the IP addresses on your computer and takes its best guess as to which goes where. You should make sure that the right address goes in the correct box.

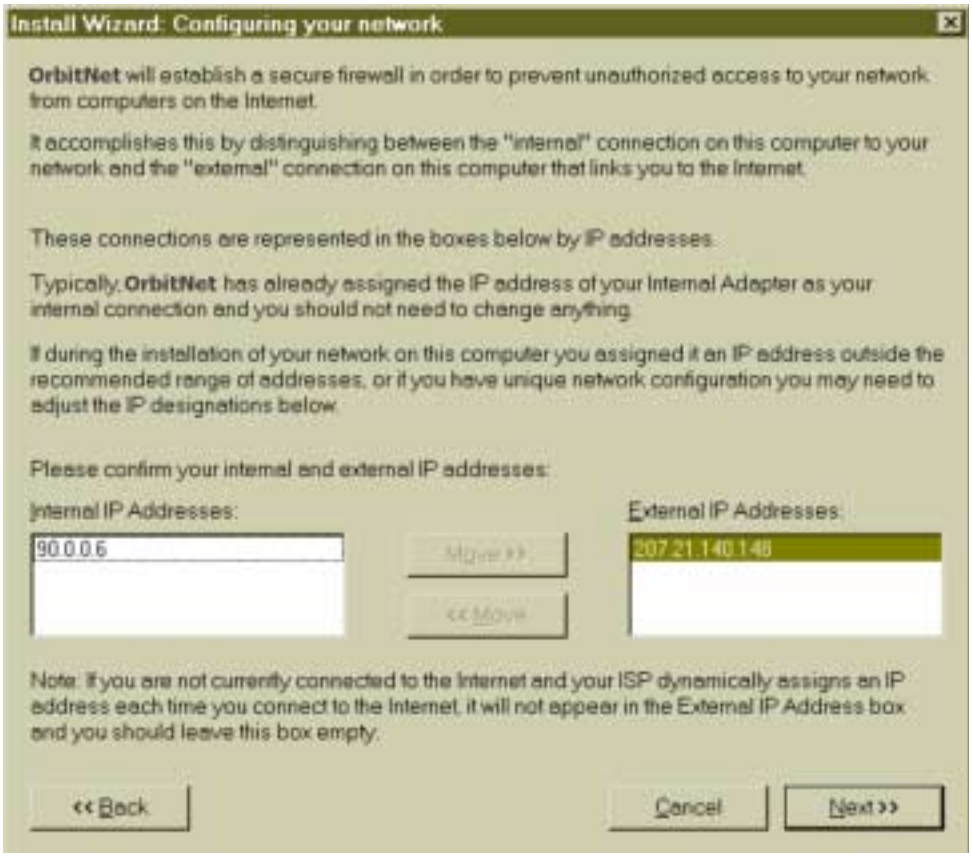


Figure 5-5: Internal and External IP addresses assigned to the computer you're configuring.

If you're using a standard modem, and the modem is connected to the Internet when this screen opens, you'll see the IP address assigned by your ISP to your modem when the connection was made (as in the example above). If your modem isn't connected to your ISP at the moment, OrbitNet shows the Dial-Up connectoid name.

The Internal IP box should have the IP address of the network connection to the rest of your computers (usually, this is the connection that goes to your hub). If this address is displayed in the External box instead, highlight it and use **Move** to correct it.

If no addresses are shown, then Windows cannot find any IP addresses on your system. You can continue with the setup, but afterward you'll need to assign an IP address to your network card before OrbitNet can work. You can do this by entering **Windows/Control Panel/Network**.

✔***USER'S CHECKPOINT***: Network IP addresses are actually assigned to every network connection instead of to the computer itself. Thus it's possible for one computer to be associated with many IP addresses. Your OrbitNet computer will have two network IP addresses, and the two are treated quite differently. The one we call the Internal address connects to the rest of your computers, whereas the External address connects to the Internet. The external address can be assigned to a Dial-Up Adapter (standard modem), or to a network card (cable or ADSL modem, or direct connection).

Other computers can connect to OrbitNet at will on the Internal connection, but cannot connect to OrbitNet on the External connection. It's thus important to your connectivity and to the firewall's operation that these designations are correct

That's all the setup you need to get OrbitNet up and running. You're now ready to enter the check-out phase.

Step 6: Choosing to Disconnect. This next screen appears only if the modem is already connected to your ISP:

Figure 5-6: After configuration and first-time Internet connection, OrbitNet gives you the choice of disconnecting now or later in order to fully test and ensure that the configuration is working properly.

Getting the modem to work is part of the check-out. For it to be tested requires you to disconnect now before proceeding to Step 7, the final step in the Installation Wizard. However, if this is not your first time through and you already know that dialing works, you may want to avoid the disconnect and save a little time.

Step 7: Verifying Setup. OrbitNet works its way through each step shown in Figure 5-7. Each time a checkout is completed, a check appears in the appropriate box.

Figure 5-7: When testing your configuration, OrbitNet works through each step shown here.

If you have a direct connection, or you start this page with the modem already connected, the modem boxes will be grayed out. If trouble develops during the checkout process, OrbitNet opens a box and gives you the opportunity to change any settings affecting the operation. You can go back and forth, or repeat the Install Wizard as often you want, to trouble-shoot and fix any problems.

That's it, folks! With the check-out completed, you're ready to begin using OrbitNet.

NOTE

When you click **Begin Using OrbitNet**, a Client Configuration Document opens, allowing you to double-check your configuration information. See Section 4, below, for more details.

C. RUNNING THE PROPERTIES WIZARD

The Properties Wizard is a bit like the Install Wizard, but more comprehensive. It covers more configurations and settings than the Install Wizard, and it's a good intermediate step if you don't yet feel up to making all of the settings yourself. You can run the Properties Wizard at any time by clicking through the path **OrbitNet/File/Properties Wizard**. On your first installation you'll be presented with a registration screen before you can enter the Properties Wizard:

- *If you've already purchased OrbitNet*, simply enter the serial number and other information. Once that's done, proceed to the Properties Wizard.
- *If you're evaluating OrbitNet*, leave the serial number entry blank but fill in the other fields. You can fill in the serial number later, after purchase.

Once registration is complete you'll begin working with the Properties Wizard. The following pages will guide you through the 10-step installation process:

Step 1: Dial-Up Networking. The Wizard asks if you plan to use a dial-up connection to your ISP. If not—perhaps you're using a cable modem or other direct connection—accept the default option ("I am NOT using…")

If you *will* be using Dial-Up Networking, choose the other option ("I AM using…"). OrbitNet implements Dial-Up using the Dial-Up Networking capabilities built into Windows.

Figure 5-8: Using this screen, you'll inform the Properties Wizard whether or not you'll be using dial-up networking.

Step 2: Dial-Up Configuration. This screen asks for details about your planned dial-up connections. The inactivity timer is used to automatically hang up the phone line after a specified amount of time in which no activity has occurred between the proxy and your service provider. Enter the number of inactive minutes you consider reasonable. If you don't want a hang-up to occur, simply enter 0.

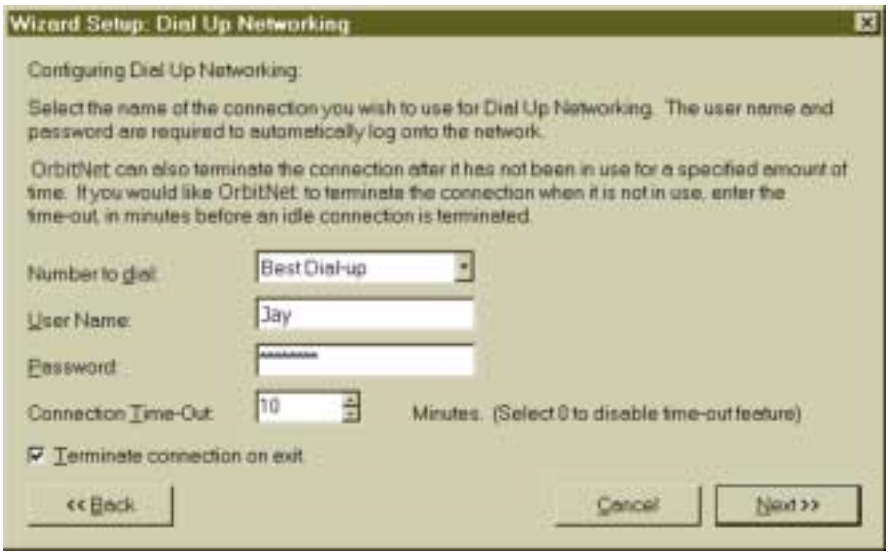


Figure 5-9: Configuring your dial-up options.

Step 3: Identifying Internal/External Connections. Correctly identifying internal/external connections is crucial to your network's firewall and security capabilities. When you first enter the Properties Wizard, it immediately searches for IP addresses. If a problem exists with these addresses, you'll receive one of the following messages:

No Addresses Found. The Properties Wizard was unable to find an IP address. OrbitNet won't work correctly until the proper IP addresses are entered. To correct the problem, please refer to Chapter 4.

One Address Found. The Properties Wizard found only one IP address; however, the installation proceeds. Some guidelines for interpreting this message:

- *If your dial-up connection has not been made*, chances are that the single IP found is the one you assigned to your internal network card. This is the expected result in this condition and you can ignore the message.
- *If you're connected to your ISP,* then OrbitNet has found the IP address dynamically assigned to your Dial-Up Adapter and nothing else. Your internal network card has not been properly configured, the client configuration document will be incorrect, and your local network will not function through the proxy. You need to reconfigure your network card.
- *If you have a static IP assignment from your ISP (*most cable modems do), OrbitNet should find two IP addresses whether or not you're connected. One or the other, or both, are incorrectly configured.

Two or More Addresses Found. If more than one IP address is found, the Properties Wizard asks you to designate which are external and which internal. Keep in mind that the Dial-Up adapter IP address (or the network for the cable modem) is your external address; and that all network cards connecting to your other computers (including through the hub) are internal addresses. Each address—internal and external—must be designated as such.

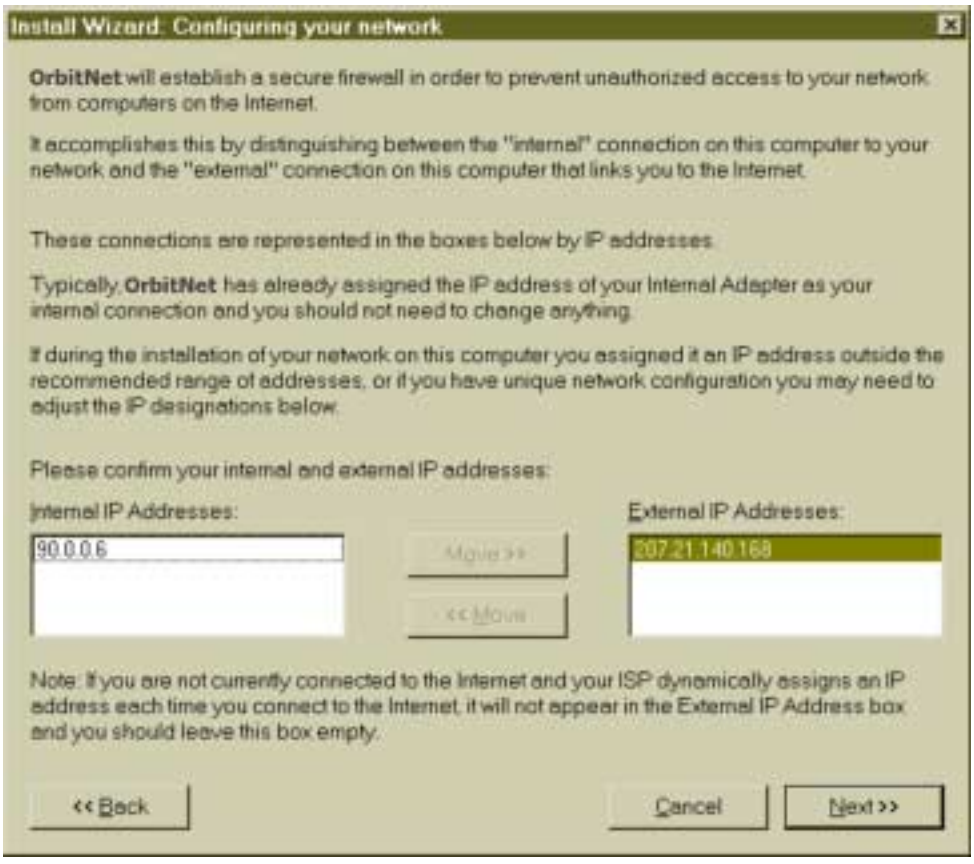


Figure 5-10: Identifying (and, if necessary, correcting) Internal/External IP addresses.

Use the Move button to move IP addresses to the proper category if they aren't already there. If you fail to do so, the proxy won't function correctly—or, if it does, you'll be leaving yourself open to a major security breach.

Step 4: Internet Protocols. You'll be asked which protocols you want added to OrbitNet. A few tips to help you decide:

- The HTTP and FTP protocols are necessary for your browsers.
- You probably won't need Telnet unless you already know what it is.
- RealAudio is usually enabled (or can be purchased as a browser add-on).
- The AOL protocol enables AOL account-holders to run their AOL software and access their AOL accounts through a standard ISP. If you enable this protocol, you'll also need to set up DNS on your local network (you'll learn how to do so later in this guide).

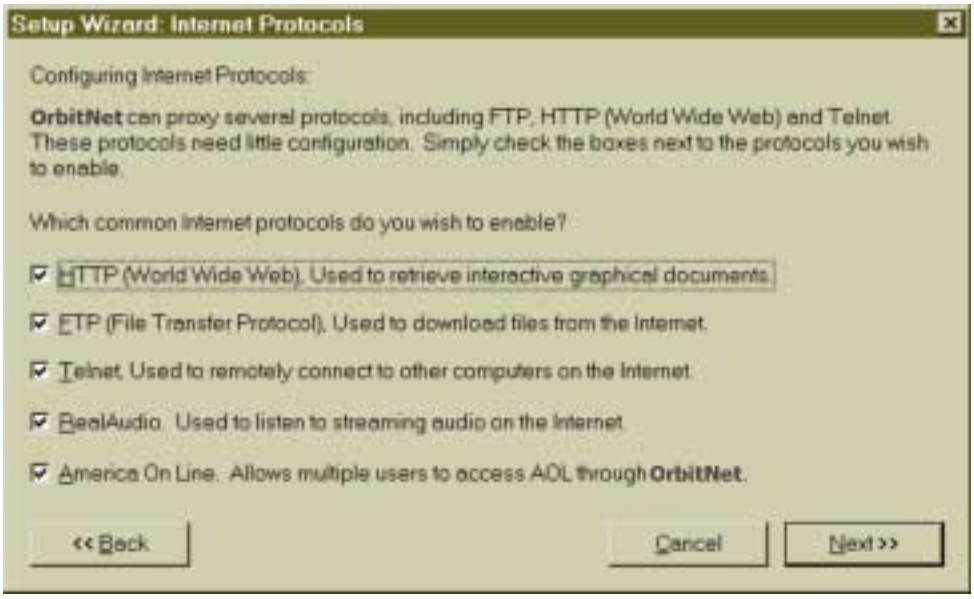


Figure 5-11: Configuring Internet Protocols with the Properties Wizard.

Step 5: Proxy Port. This page allows you to set the port on your CERN HTTP proxy—the primary port used for your browsers. It's best to leave it at the default (port 80) unless you have a web server running on the OrbitNet machine.

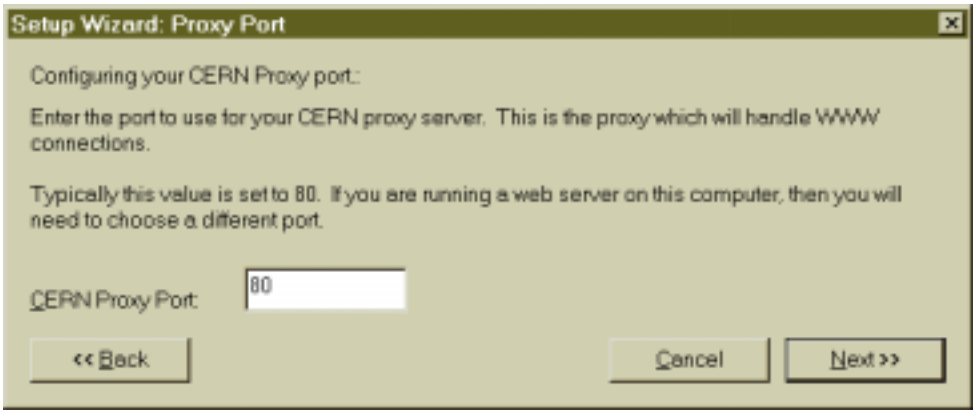


Figure 5-12: Establishing the port on the CERN HTTP Proxy.

Step 6: Internet News. The program asks for the address of your news server. Enter the numeric IP address if you have it. If you don't—*and* if you're currently connected to the Internet—enter the news server's name (for example, **news.myprovider.com**). OrbitNet automatically looks up the address and stores it. You can also leave this box blank, filling it in later under Settings.

Figure 5-13: Configuring Internet News.

Step 7: Mail Setup . The Wizard now asks for the address of your SMTP server (to which you send the e-mail you've written) and your POP (from which you get mail) server. The SMTP address is the one to which you send your mail. The POP address is for the computer from which you have been getting email addressed to you.

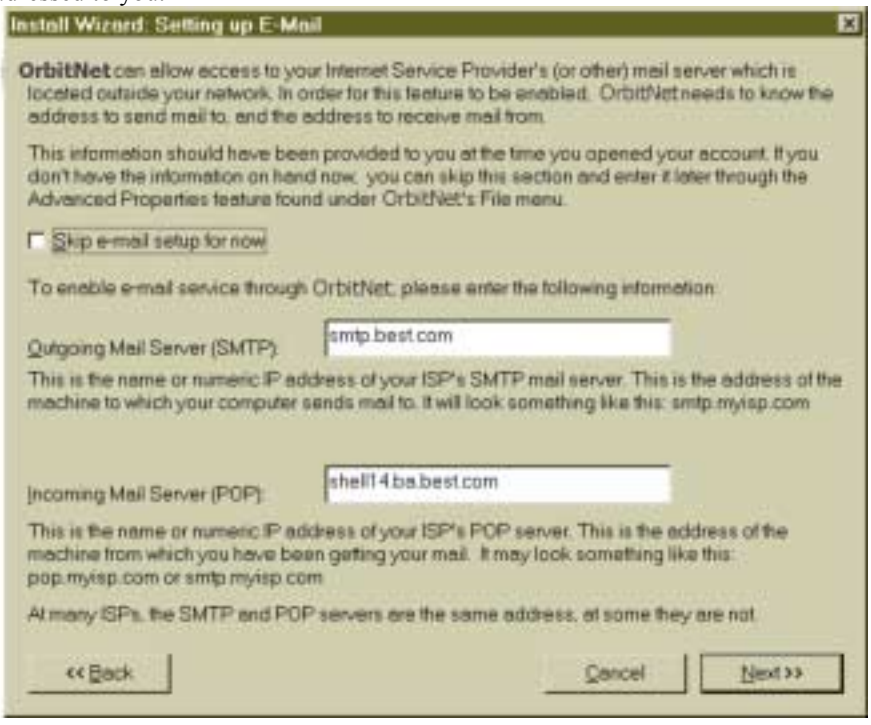


Figure 5-14: Configuring e-mail.

Step 8: Socks. The next screen allows you to configure Socks 4 and Socks 5, a flexible proxy protocol used for several types of connections, including chat programs. Socks is a forgiving and fairly easily-implemented protocol. If you'll be using OrbitNet for casual Internet browsing, you won't need Socks (and you can always add it later). Simply accept the default choice ("I do NOT want…"), enter the number of your ISP's DNS server in the box, and move on to Step 9.

If you *do* want Socks enabled, remember that, in order for Socks to work, DNS must be set up throughout your local system (DNS setup is explained later in this book). To enable Socks, choose the first option ("I DO want…") and enter the IP address of your service provider's DNS server usually given in the form of a numeric IP address. If your ISP provided the numbers of a primary and secondary DNS server, enter the primary number here. The second number can be entered later, after Setup, in the DNS Setup menu under File/Settings/Protocols/DNS Setup.

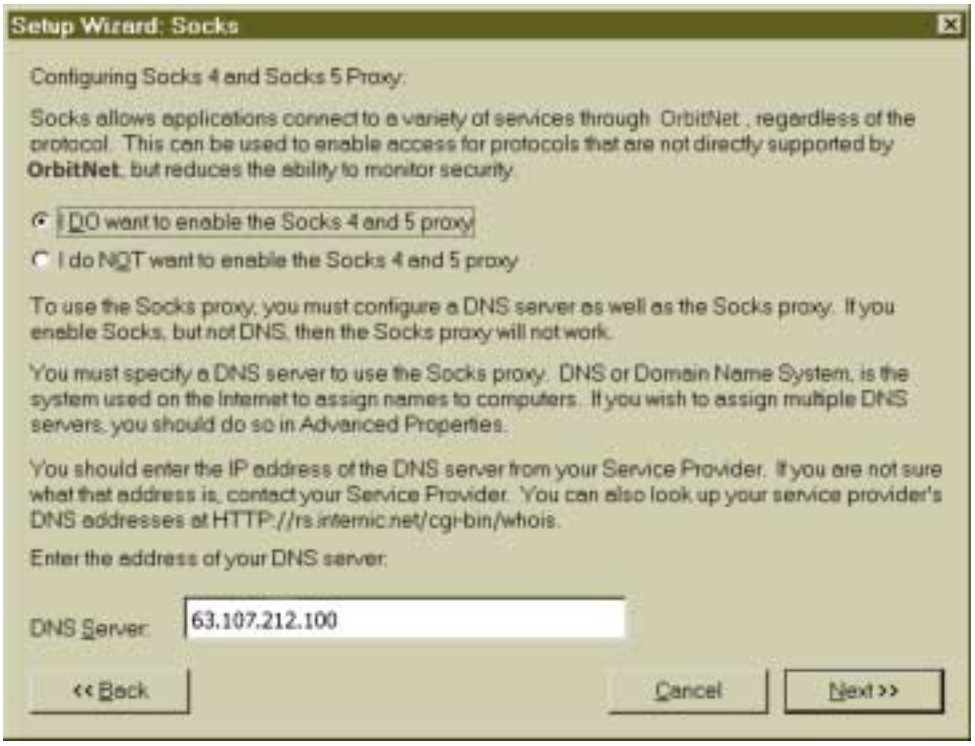


Figure 5-15: Configuring Socks 4 and Socks 5.

Step 9. Cascading. You may not need to use this capability, particularly if you live in the United States. Proxy cascading is required when your service provider gives you service through its own proxy. This is a fairly common occurrence outside the U.S., especially in Europe, Asia and South America. In North America such service is rarely used except with some cable modem providers and within large educational and corporate institutions. If you're not running behind another proxy server, leave this setting disabled and move on to Step 10.

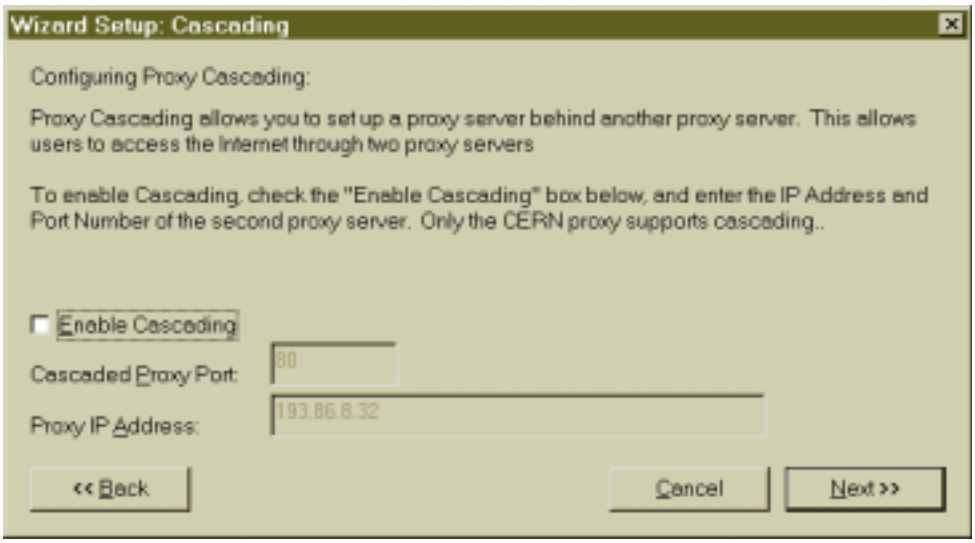


Figure 5-16: Configuring Proxy Cascading.

There's a simple way to tell if you're operating behind an ISP's proxy. First, start OrbitNet. If you find that you can then browse web sites with the same domain name as your ISP but can't go anywhere else, then you're probably behind another proxy (e.g., you can see **membershipinfo.myisp.com** but can't get to **microsoft.com**). To fully browse the Internet you must enable proxy cascading and provide the IP address and port number of the previously-existing proxy server (obtained from your ISP). Besides a specific listing for a proxy server, look for other information from your service provider:

- If you were instructed to use an "automatic setup" in your browser, you were probably given a URL to enter during setup.
- You may have been given settings to enter under the browser's manual proxy configuration settings. If so, use the same IP address and port number for proxy cascading. If you've been given an automatic setup, you'll need to obtain your ISP's IP address and their proxy server's port number.

Step 10: Administration and Security. This screen allows you to enable/disable **Reverse Name Lookup** and set an administration password. (Special Note: If you enabled proxy cascading in Step 8, you won't see this screen, because reverse name lookup won't work when cascading).

Reverse Name Lookup is a nice security feature. When you give your browser a named location with a URL, it first institutes a lookup to find the numeric IP address corresponding to the name. RNL, if enabled, takes that numeric address and determines which named domain it corresponds to. If the answer isn't the same as the site you asked for in the first place, you'll receive an explanatory error message instead of a connection.

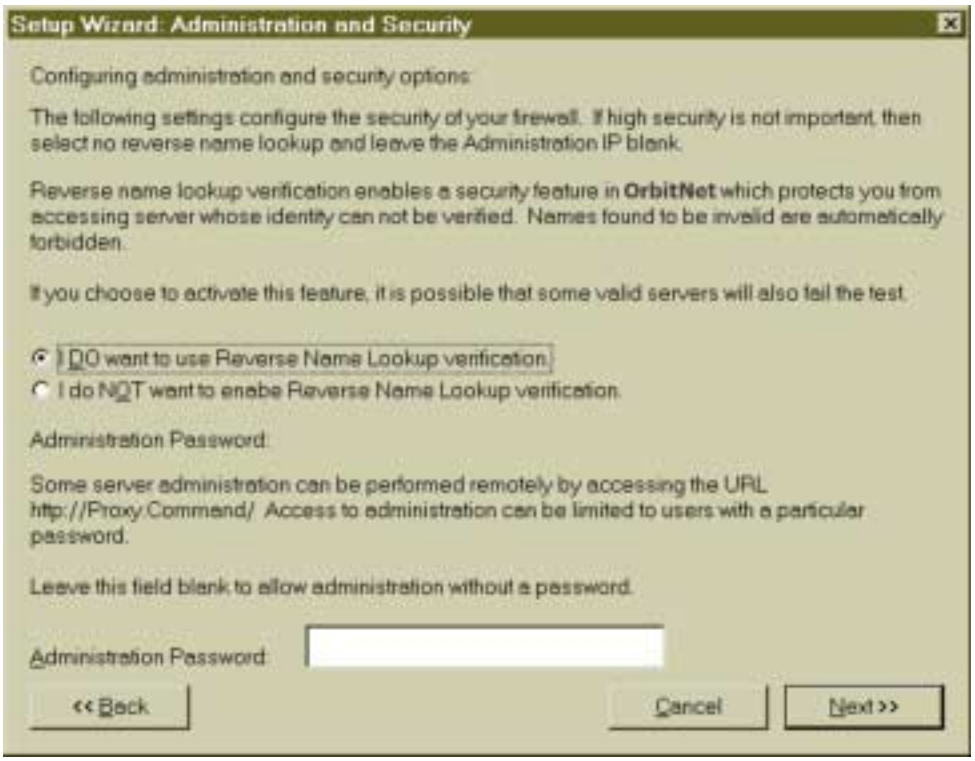


Figure 5-17: Configuring administrative and security options.

The **Administration Password** can be set to restrict user access to OrbitNet's Settings, to the remote configuration settings available (with a browser) through **http://proxy.command**, and to the time window override. If this is your initial experience with networking, you'd be better off leaving this blank until you're happy with your configuration. A password can be added at any time.

Step 11: Logging. The Logging screen enables/disables activity logging—a "list" of activities performed by an individual user on the Internet. Enabled logging provides a log in readable text which can be useful for troubleshooting. Another logging capability, Detailed Logging, is machine-readable (providing files suitable for activity summaries when analyzed by other programs) and must be set up within Settings.

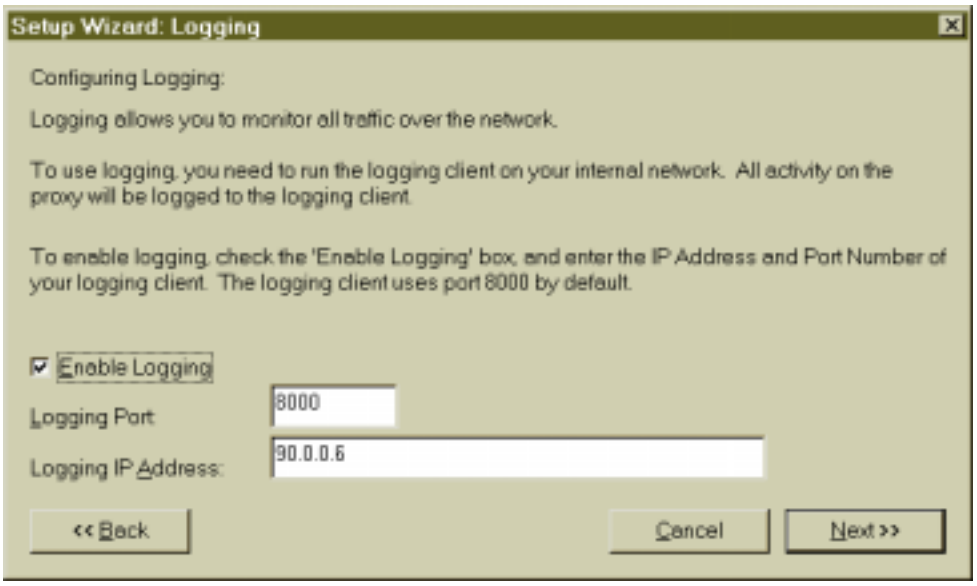


Figure 5-18: Configuring/enabling logging.

If you want to enable activity logging, set the port to 8000 and enter the IP address of the network machine which will be running the logging application (it can be the OrbitNet machine or any other machine). If you want to use another machine, copy the **proxylog.exe** file to the machine you want to use. Run proxylog from a DOS prompt; OrbitNet connects to the proxylog app within a few seconds. You can also type in **proxylog/?** for instructions on how to log to a file as well as the screen.

Step 12: ConnectionView. When enabled, ConnectionView displays all listening protocols and active connections in the OrbitNet main screen. It's probably a good idea to leave this enabled while setting up and fine-tuning OrbitNet. Afterward, however, you might want to disable ConnectionView; turning it off can provide more speed if your Internet connection is faster than your computer. It takes a lot of CPU cycles to carry out ConnectionView's rapid screen updates.

Figure 5-19: Configuring OrbitNet's display.

Step 13: Client Configuration. OrbitNet presents you with the option of opening your client configuration document. This document differs according to what specific OrbitNet settings are enabled. Since it's updated whenever you change OrbitNet's settings, the instructions are always up to date.

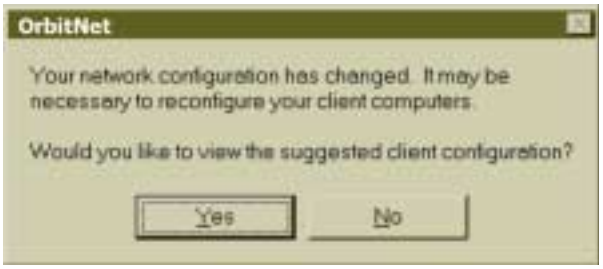


Figure 5-20: We strongly recommend that you choose to review the client configuration document. Keep in mind that it will change each time you reconfigure OrbitNet, reflecting important alterations you've made to your network.

Step 14: OrbitNet updates its settings. The Updating box is a timed announcement and will disappear after a few seconds. If you click on the 'OK' button, it goes away a little sooner.

Figure 5-21: When you see this box, all the settings you've entered are being updated.

At this point, the Properties Wizard is finished. A short dialog screen announces that OrbitNet's settings will be updated when you exit the Wizard.

D. CONFIGURING INTERNET APPS ON ALL YOUR COMPUTERS

One last step remains before you're set to run OrbitNet: your Internet applications must be configured and enabled for proxy use. If they're not "told" where the proxy server is, they won't be able to connect to the Internet.

If this is your first time setting up OrbitNet, we strongly recommend going to the Client Configuration Document (CCD) for help in preparing to configure Internet applications. Prepared by the OrbitNet program, the CCD provides information customized to your installation and based upon your specific OrbitNet configuration. There are actually two basic CCDs. You'll see one if you've enabled NAT/Tproxy, and the other if you haven't. You'll find instructions for many protocols, including some we haven't yet discussed.

To see the CCD, follow the path **OrbitNet/File/Show Client Configuration**. You'll find a Notepad document describing how to configure the Internet applications on each computer in your local network. It's a good idea to print this document for referral while configuring those applications.

You'll notice that the configuration shown in the document is quite specific. That's because it's based upon OrbitNet's TCP/IP data and other information you provided during setup. The CCD is called a "dynamic document" because it changes frequently. Whenever you alter certain OrbitNet settings, the

document changes too, reflecting the new information. Whenever you make changes to your network, consult the CCD to ensure that you're configuring other applications correctly.

A sample Client Configuration Document, with accompanying explanatory text, is contained in the Appendices.

When Do Changes Take Effect?

Any time you make a change in OrbitNet and **OK** your way back to the main screen, OrbitNet updates and saves the new information (you'll see a dialog box when this occurs). If you have a connection at the time (that is, an active connection between an application and a computer on the Internet, not a dial-up connection) OrbitNet waits to update until that connection ceases. As soon as these settings have taken effect, the Client Configuration Document reflects the new settings.

Chapter 6

Some Security Considerations

Chapter 6: Some Security Considerations

Overview: Security

The security of your local system can be considerably enhanced simply by changing a few settings. The changes listed here affect only your external connections to the Internet, and won't affect the operation of your local network. More advanced security capabilities are discussed in Chapter 10.

A. THE PHYSICAL SETUP

OrbitNet—and the computer on which it's installed—should be the *only* physical connection to the Internet. The point is to force *all* traffic between your network and the Internet to pass through OrbitNet, including traffic you don't even know about.

Beware of cable and DSL modems that connect to a hub rather than to a network card. *We don't recommend this topology*. With such a setup, no product—not even OrbitNet—can fully protect your system. While the modem itself may provide some protection, you can't be sure: the protective capabilities of these modems varies widely. Besides, no modem provides the same protection as a firewall, and many provide none at all. This setup leaves your network wide open to attack from unauthorized persons outside your network.

We can't say it strongly enough: *do not use cable and DSL modems that connect to a hub*. Move the connection from the hub to the OrbitNet computer. It's pretty easy to do. If you need assistance, we provide instructions on the tech support section of our website.

NOTE

The only difference between a network component that connects to a hub and one that connects to a network card is the connector's pin order. There are only two pin orders. To move your modem over, use a cross-over cable instead of a regular cable—that's all there is to it. If your OrbitNet computer has only a single network card, then you'll need to add a second network card.

If you have more than one subnet behind your firewall, we recommend that you do not use the OrbitNet machine to route between the subnets. Use a router or multi-homed NT machine behind the firewall to route between your subnets.

B. NETWORK DESIGNATIONS AND DRIVERS

The most important designation you'll make when installing OrbitNet is the distinction between the internal and external network connections. The two are treated quite differently. If you inadvertently designate your Internet connection as *internal* rather than *external*, everybody on the Internet can enjoy the same access to your network as you do! Needless to say, this is not a desirable situation. *Your Internet connection must be designated as an external connection*. You can double-check to be sure you've done this at **OrbitNet\Settings\General\Internal IP**.

You'll also want to check on the installation of the OrbitNet Transparent Proxy drivers, which allow regulation of your external network connection at a system level instead of an application level. If for some reason these drivers don't load, you'll still have OrbitNet's application-level firewall—one of the best around—but it's not as strong and inclusive as a system-level firewall.

Look under **OrbitNet\Help\About OrbitNet**. If the Transparent Proxy drivers are loaded, the version number will be reported. If they are *not* loaded, OrbitNet reports that "Transparent Proxy and NAT are not

loaded." The best thing to do at this point is to reinstall OrbitNet (there's no need to uninstall first). When you reinstall, built-in OrbitNet routines will help to fix any problems with the NAT drivers.

A setting within OrbitNet accomplishes the same task. If you set your Client Access to "Classic Proxy" under **OrbitNet\Advanced Settings\Client Access Method**, you'll disable the system-level firewall. With this setting, OrbitNet 3.0 will be just the same as OrbitNet 2.1 (including the excellent 2.1 application-level firewall), but without the new system-level firewall. If you set OrbitNet to "Client Proxy only," you'll then see that "Transparent Proxy and NAT are disabled" under **OrbitNet\Help\About OrbitNet**.

NOTE

An application level firewall takes cares of its own doings on network connections, but cannot prevent other applications from opening their own ports and waiting for connections on your proxy machine. These other connections are not visible to the application-level firewall, and can be invisible to the user as well.

A system-level firewall can prevent other applications on your computer from opening and using ports, including the file- and printer-sharing ports that Windows otherwise opens.

C. ORBITNET PROGRAM SETTINGS

Establish the OrbitNet firewall setting at Medium or higher (**OrbitNet\Advanced Settings\Firewall**). Medium is the default setting. If you need custom settings, allowing for special apps or games, **start** with a medium or higher setting before you go to custom settings.

✔***USER'S CHECKPOINT***: As soon as you define a custom filter (or enable a pre-defined filter) under the firewall settings, the slider bar for the firewall disappears. It's replaced with a Custom Security description. It **does** make a difference where you start, though. If you've already defined some filters, examine the filter list. You'll see a system entry indicating the base Security setting, such as "High Security Level," or "Medium Security Level."

If you do set up your own filters on the OrbitNet firewall, pay careful attention to the port ranges. OrbitNet puts the lowest and highest possible numbers in those boxes before your start. If you're not careful, it's easy to forget to change that second number. Instead of opening a few ports, as you intend, you'll open tens of thousands! If more than one person has access to the filter settings, it's a good idea to look through them once in a while.

Do not set up or enable anything labeled "incoming" unless you're *certain* you need to do so. When enabling an incoming port, you're setting up a listening port on your external network connection. Anybody on the Internet can connect to that port whenever they want. The only reason to set up an incoming port is to purposely allow people on the Internet to reach a server behind your firewall.

Security Alert

Three protocols—HTTP, FTP and Mail—contain individual "incoming proxy" settings. Any mapped port configured as an incoming mapped port is likewise a potential security problem.

D. OTHER SETTINGS ON THE ORBITNET MACHINE

You can have file and printer sharing enabled on the *internal* network connection, but do not do so on the external connection. OrbitNet can prevent access on these ports when all other settings are correct, but

just in case you should disable file and printer sharing and the NetBeui protocol on your external connection. To do so:

1. Look at the settings in **Control Panel/Network**. If you see a protocol line which shows **NetBEUI→Dial-Up Adapter** (or **NetBEUI** with the network card connected to your cable modem), remove it. If you're using AOL as a provider, remove any protocol line showing **NetBEUI→AOL Adapter**.
2. Highlight the entry **TCP/IP→Dial-Up Adapter** (or **TCP/IP→AOL Adapter** if using AOL as your provider). If you have a cable modem, highlight the entry for TCP/IP with the network card connected to your cable modem). Click **Properties**, and then choose the Bindings Tab. Uncheck the box titled **Client for Microsoft Networks.** Uncheck the box **File and Printer Sharing**. When you click OK, Windows complains about the lack of bindings; when it politely asks if you want to choose one, choose **No**. Restart the computer for the changes to take effect.

If you're running NT on your OrbitNet computer, make sure that "IP forwarding" is disabled. Just as with file and printer sharing, other OrbitNet firewall settings will prevent access because of IP forwarding—but its better to be safe in case it slips your mind while making configuration changes at a later date.

If you run browsers on the OrbitNet machine, we recommend (a) setting them to run through the proxy, and (b) using the Classic Proxy method (configure the browser to use a proxy, and use the OrbitNet internal IP address as the proxy address). Running a browser in other configurations could expose you to a known or future browser security problem. It's a good idea to set *any* Internet application on the OrbitNet machine to use the Classic Proxy whenever possible.

E. ANTI-VIRUS

If anti-virus scanning is important to you, make sure you don't have the "NAT Only" option selected under **OrbitNet\Advanced Settings\Client Access**. The anti-virus scanner will work on HTTP, FTP and Mail files—but only when they are visible in the main ConnectionView screen.

Interested in the reason why? It's because Anti-Virus works only on connections that pass through the application level (i.e., Cproxy (i.e., Classic Proxy) and Tproxy (Transparent Proxy) connections, which are visible in the ConnectionView screen when its up). NAT connections, by their very nature, don't pass through the application level. They're thus never visible in ConnectionView and won't be scanned.

Bottom line: if *you* can't see it, the Anti-Virus can't either—and it won't be scanned.

F. GENERAL SECURITY

Use a non-routable network address for your local network. OrbitNet will work with any network address as long as the internal/external addresses are on different networks. However, using a non-routable address for your local network adds extra security for free.

> **NOTE:** IP addresses are routable across large and diverse networks—that's what makes the Internet work. There are some pre-defined IP address groups that Internet routers intentionally toss away instead of passing on. These groups work fine within a local network, but cannot be directly accessed across the Internet. Using addresses from one of these groups—such as 10.x.x.x or 192.168.x.x—is an easy way to give your local computers more security.

A Final Word on Security

Security is built into OrbitNet and remains one of the most important objectives at Orbit Communication Corp.. You'll notice throughout this guide that we offer many tips to enhance your network's security.

Chapter 7

DNS/Socks

CHAPTER 7: DNS/SOCKS

OVERVIEW: DNS/Socks

If you're satisfied with your basic browsing and mail features, you can skip this chapter. However, more and more services on the Internet seem to need DNS to operate. If you'd like full Internet functionality, adding DNS to your network setup, read on.

The Domain Name System (DNS) is used in conjunction with IP addressing to map computer names to IP addresses. Basically, DNS is just another way to navigate a network. The Internet addresses you're used to seeing—**OrbitNet.com**, for instance—are part of the Domain Name System. Just as the Internet uses DNS to help people and applications find their way around the global network, you can use DNS to help your applications find their way around your local network.

Many applications, both large and small, require DNS in order to work. Among them are Java applets, the Socks Protocol and the AOL protocol within OrbitNet. You may not be familiar with the Socks protocol yet, but you'll see it more often as you become conversant with networking. The flexible and powerful Socks protocol is becoming a popular choice among programmers when adding proxy support to applications.

A NOTE OF CAUTION

The very flexibility and power that Socks provides also makes it a bit more of a security risk than other protocols. If your local network hosts extremely sensitive material, think twice before allowing the Socks protocol.

A. SETTING UP DNS ON YOUR LOCAL NETWORK

In the example given below, (1) OrbitNet is used as the DNS server on your local network; and, (2) each computer on the network is set up to be a DNS client. Although the instructions indicate click-paths used in Windows 95/98, the NT setup is similar. Screenshots of all settings for Windows 95/98 and NT are on our website.

Setting Up the Server Machine

To begin, you'll need the IP address(es) of your ISP's Domain Name Servers. These addresses are usually listed on the ISP paperwork (often as "primary" and "secondary" servers). If necessary, OrbitNet can obtain them for you. Here's how:

- From the Settings Tab, click **Protocols/DNS Set-Up/Find My Name Server**.
- Follow the formatting instructions, clicking on **Find my DNS Server**.
- OrbitNet brings up your default browser, using the information you provided to find your ISP's listing with InterNIC. Part of that listing includes the IP addresses of your ISP's DNS servers.

Once you have the appropriate IP addressing information, you can proceed. The first step is to set up the OrbitNet machine as your DNS server:

- In OrbitNet, click **File/Settings/Protocols.**
- Check the box beside DNS Set-up, enabling DNS.
- If you intend to use Socks, put a check in the appropriate box.
- Click **DNS Set-Up**.

- Look in the **Current DNS Server List** to see if your ISP's primary DNS server is already listed (it might have been added during the original setup). If not, enter the address in the **DNS Server IP to add** box and click **Add** to include it in the Server List.
- Using the same procedure, add the secondary DNS server IP. If you weren't given one by your ISP, just leave this line blank; the secondary is used only when the first fails to respond.
- Enter a name in the Domain box where the instructions ask for your local domain name. You can use your ISP's domain here, but it's better to use your own. Feel free to make one up: fred.com or suzie.org will work just fine. The name doesn't need to be officially listed with any Internet bodies—since it's on your local, private network, it's invisible to the rest of the world. All of your computers should have the same domain name, and because of the way DNS lookups are made it's best if you have a **.com** or other standard domain name on the end.
- Click **Namelist** and follow the directions to make a local name list for your DNS server—that is, a list of all local computer names and the IP address for each. Using this list speeds up local lookups. If you don't know a computer's name you can find it at **Settings/Control Panel/ Network/Identification/Computer Name**. You can change that name whenever you want, but remember to also change it in the namelist.

Finally, click **OK** buttons until you've returned to OrbitNet's Main Screen. You should see a small dialog box telling you that settings are being updated. You won't need to restart OrbitNet for the settings to take effect. OrbitNet is now configured as your DNS server.

Setting Up the DNS Client on the OrbitNet Machine

One of OrbitNet's benefits is that it doesn't need to run on a "dedicated" computer (a computer with only one function). In other words, when a computer becomes a OrbitNet server, it continues running all the applications it ran before with no changes whatsoever. Further, the OrbitNet server can also be a client—just like all the other PCs on the network, it can access the Internet through OrbitNet.

For this reason, the OrbitNet computer is configured with both server and client settings. Now that the computer is established as a DNS Server, you'll set it up to also be a DNS client. Doing so allows applications on this machine to work with your ISP's DNS server if you happen to use them while OrbitNet isn't running. And don't worry: you'll experience no conflict with client/server settings, since they're entered in different locations

- On the OrbitNet machine, go to **Control Panel** and then choose **Networks/Identification/Computer Name**. Write down the name you see listed for the computer (you'll use it in a moment).
- Click the **Configuration Tab**.
- Double-click on the **TCP/IP protocol** line for the local (LAN) adapter.
- Click the **DNS Configuration Tab** and then **Enable DNS**.
- Under Host, type in the computer's name. Under Domain, enter the same name you used when setting up OrbitNet. In the **DNS Server Search Order** box enter the IP address of the OrbitNet machine itself (i.e., 90.0.0.1) and then the same ISP DNS addresses you entered in OrbitNet.

The OrbitNet machine is now set up as a DNS client machine. Let's proceed to setting up DNS on the other computers in your network.

Setting Up Your Other Machines as DNS Clients

If your client computer/s have the default settings—i.e., TCP/IP has been set to "Obtain Automatically" and DNS to "Disable"—you needn't enter DNS information. OrbitNet's DHCP server automatically supplies all necessary DNS information for you.
(By way of explanation, the "Disable" setting is something of a misnomer, since in practice it really means the same "Obtain automatically").

However, if you're not using the default settings, let's proceed with setting up your DNS clients. For each machine on your local network:

- In the Control Panel, double-click **Networks** and then **Identification**. Double-check the individual computer name—you'll be using it in the next step.
- Double-click the TCP/IP protocol line for the local (LAN adapter.
- Click the DNS Configuration Tab and then **Enable DNS**. Under **Host**, enter the computer name obtained in the previous step.
- Under **Domain**, enter the same domain name used on the OrbitNet machine.
- In the **DNS Server Search Order** box, enter the IP address of the OrbitNet machine (e.g., **90.0.0.1**).
- Click **OK** until you return to the Main Screen. Windows should inform you that you must restart the computer for the settings to take effect.

Your entire local system is now configured to use DNS in its network activities. If you plan on using the Socks protocol (most people will) or the AOL protocol, make sure that those protocols are enabled within OrbitNet (you can do so at **Settings/Protocols**).

Testing Your DNS Setup

You might want to check and see that your local DNS search is working properly. You can use Ping for this, though in a slightly different format than we used before. Make sure OrbitNet is running and connected to your Service Provider, and use Ping with domain names instead of IP addresses:

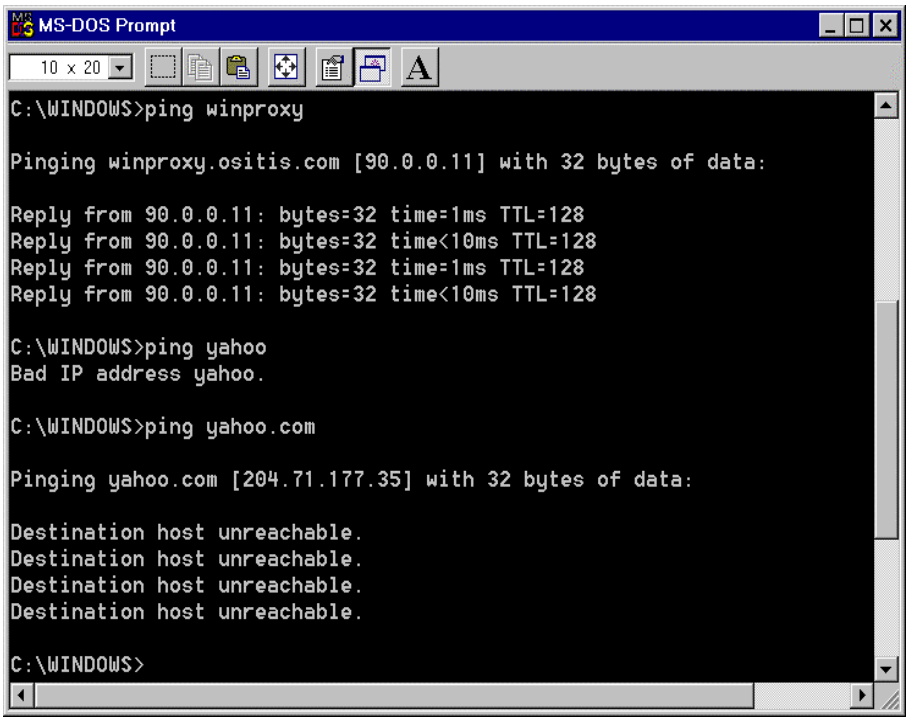


Figure 7-1: Testing your DNS setup with ping.

All three of the Ping attempts shown here were done on a client computer behind OrbitNet.

The first example is **ping OrbitNet**. It gives the results shown if you have configured the client computer and the OrbitNet computer for DNS. This test works whether or not you're connected to the ISP. Test each client computer this way. You'll notice that the ping command is concatenated with the local domain name, in this case **Orbitsat.com**. The IP address shown, 90.0.0.11, was the IP address of our office OrbitNet machine at the time we tested. This test confirms that your local DNS setup is working, at least on the OrbitNet and client machines used.

The second test shown, **ping yahoo**, illustrates the result to be expected when you've specified a bad domain name, or when DNS can't resolve the name.

The expected results of the third test will vary depending on the OrbitNet version you're running. We'll cover OrbitNet 2.1 first, as shown in Figure 6-1. You may think things aren't working when you first glance at the third test, **ping yahoo.com**. But the results actually confirm that the DNS lookups are functioning just fine. Though it says **Destination Host Unreachable**, a close look reveals that it also returned the IP address of yahoo.com. Ping itself won't work through OrbitNet 2.1, but the DNS lookup was correctly handled: the local client asked the OrbitNet machine, OrbitNet asked your ISP's DNS server (which may have known the address or may have asked another DNS server on the Internet for it), and the result was passed all the way back to the client machine. This last test, then, confirms that the chain of DNS lookups is complete from the client machine to the Internet.

With OrbitNet 3.0, the DNS portion of the third test works just the same—you ping a name and DNS returns (as part of the message) the IP address to which the name resolved. The one big difference is that

OrbitNet 3.0 *will* allow client machines to ping computers outside the firewall. Instead of "Destination Host Unreachable," you'll see "Reply from…." when pinging through OrbitNet 3.0.

B. ADDING THE SOCKS PROTOCOL TO YOUR BROWSERS

Adding Socks is only necessary for browsers operating through Cproxy. Otherwise, don't bother with it. Just as other browser protocols such as HTTP and FTP work without configuration within the OrbitNet default, so too does Socks.

But if you need to add Socks it's easy to do so. Here's how:

- In OrbitNet, click through the path **File/Settings/Protocols**.
- Enable Socks, and enter in the Socks box the IP address of the OrbitNet computer.
- Set the port to 1080.
- Blank the entry for FTP so the browser uses Socks for FTP connections. This prevents the occasional problems that may result when both are checked. Also, transfers are usually more robust when using the Socks protocol.

The two major browsers treat the other protocols a bit differently when Socks is enabled. Netscape preferentially uses Socks for everything, including mail, and also for unconfigured protocols such as Gopher or WAIS. Internet Explorer uses Socks for protocols that aren't otherwise enabled, like Gopher.

Enabling Other Socks-Based Applications

Many newer Internet-capable applications—especially chat programs and some games—use Socks to support operation behind a proxy. The number or type of applications using the Socks protocol will likely increase rapidly. Technical Support at the Orbit's website (www.Orbitsat.com) contains screens for a few such common applications configured to run through OrbitNet.

The general rule for enabling these applications is to look for a configuration tab or setting about connections, firewalls, or proxies. Once there, check the box that says Socks or Socks 5. OrbitNet supports both Socks 4 and Socks 5, but if the application gives you a choice, choose Socks 5. Under Server IP enter the IP address of your OrbitNet machine. Under "port" choose the standard Socks port 1080.

Chapter 8

ConnectionView

CHAPTER 8: CONNECTION VIEW

Overview: Connection View

ConnectionView, OrbitNet's Main Screen, is a helpful tool which displays important information:

- The status of all current connections to OrbitNet.
- The enabled protocols and mapped ports which you have set up.
- Information about modem status (if you're using a dial-up connection).
- Status of enabled "services" such as site filtering, anti-virus, banner blocking, caching, and so on. You'll find this information at the bottom of the screen.

In addition, ConnectionView provides the entry point for all menu options.

Connectionview In An Idle State

The screenshot below shows a sample ConnectionView when OrbitNet is idle. The modem, as indicated, is not currently in use or connected to the Internet Service Provider. The number shown, 90.0.0.1, is the internal network IP address of the OrbitNet machine. All enabled protocols are visible below. The last entry, "gilliganvcn," is an incoming mapped port for a VNC computer-sharing application.

Figure 8-1: The ConnectionView screen in an idle state.

At this moment OrbitNet is listening for activity on the internal network connection. Each protocol shown—including the mapped port—has an associated port. For instance, the CERN HTTP, which is used primarily for web browsing, is on port 80. OrbitNet responds to activity only on the ports shown; it will not respond to activity on any other ports.

This is true for external connections, also. If any incoming proxies are set up, they have their own set of listings under "Incoming Proxies" at the same hierarchic level as the 90.0.0.1 shown here. OrbitNet

would listen for connections only on the ports deliberately enabled, and would not be interested in connection attempts on any other ports. Since only one incoming port is shown here, OrbitNet will respond to connection attempts only on that port (which is on its external network connection). It will not respond to any connection attempts on any other external ports. Most installations won't have incoming proxies set up.

Security Alert

If you have other network-responding applications on the OrbitNet computer, they won't be shown here. For instance, if you have a web server running on port 8080, you won't see it or any other connections to that port. The behavior of other applications is the network administrator's responsibility. See "Security Considerations," later in this guide.

Connectionview When A Browser Is Running

The next screenshot shows ConnectionView when a browser is running and actively downloading a page:

Figure 8-2: The Connection View screen when the browser is actively downloading a page.

Connections are displayed in this window as soon as established and disappear shortly after completion. ConnectionView uses a fair amount of processor power, and may slow things down a bit if you have a fast Internet connection. Disabling ConnectionView increases the speed (and you'll still have access to the menu options). However, it's a good idea to maintain ConnectionView until you've satisfactorily configured OrbitNet. For most common setups, like a Pentium machine connected through a regular modem, ConnectionView won't slow things down.

In this view, a browser on a client machine named "Gilligan" is connected through the Classic proxy to http://www.Orbitsat.com. The URL shown after the arrow (www.OrbitSat.com) is the name of one of our Web Servers. It's a valid alias for the URL requested by the browser, and thus passes OrbitNet's Reverse

Name Lookup test. The third group—"HTTP:GET http://www2.OrbitNet.com"—reveals the name of the protocol and http command being used, as well as the name of the file being downloaded. Several different connection lines may be shown for a single browser connection, since browsers commonly download multiple files to form a requested page.

When the modem idle time reaches the limit established in the inactivity timer (see Dial-Up Setup in Chapter 9), OrbitNet hangs up the modem. If you see **modem in use by another program** on the modem status line, OrbitNet will not connect or hang-up the modem. If you manually use Dial-Up Networking to connect, this also counts as "another program;" OrbitNet won't hang up unless you've enabled the option **always own the connection**. OrbitNet will be able to communicate over the modem even if another program connects it to the ISP.

Right-Clicks In ConnectionView

A new feature offered in version 3.0 is the use of Right-Clicks to change OrbitNet settings or connection status. For example, if you hold the mouse over the modem information line in ConnectionView and then click the right mouse button, OrbitNet presents you with a couple of dialing options:

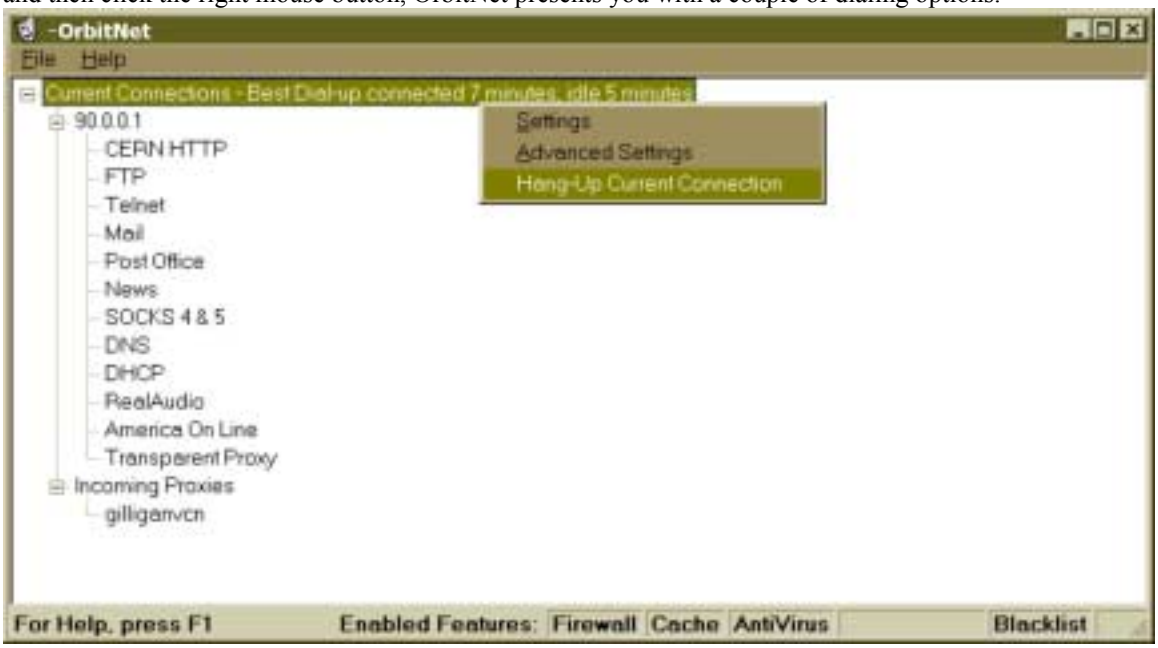


Figure 8-3: Right-clicking in ConnectionView allows easy access to options.

Clicking **Settings** takes you to the General and Dial-Up Setup section in Settings. If you click **Hang-Up,** OrbitNet hangs up the modem connection *immediately*. It doesn't wait until active Internet connections are complete, nor will it double-check to determine if you really want to hang up. It's an immediate "guillotine" hangup.

The screenshot below shows the results of a Right-Click on the **Telnet** protocol, which presents you with three options:

Figure 8-4: ConnectionView options available by right-clicking on the Telnet protocol.

You can enable or disable this protocol as you like. Keep in mind that it's a universal setting: enabling/disabling applies to all users on your network. Clicking on **Properties** takes you directly to the Telnet settings (the same Telnet page found under **Settings/Protocols**). The third option allows you to add/delete user access to telnet. The user list is taken from entries found under the Users Tab. If no entries have been made there, you won't have any choices here. In the example shown above, Chadwick is allowed to use Telnet, but Sales is not. To change either one, put the mouse pointer over the user name and left-click to toggle user permission.

This final example, below, illustrates another ability of Right-Clicking. If you hold the pointer over any connection line, you will see the option to **Terminate**:

Figure 8-5: Effecting immediate termination in ConnectionView.

If you then left-click on Terminate, the connection is terminated immediately—no ifs, ands, or buts. This feature is helpful when you're configuring new settings (OrbitNet won't update settings while there are active connections).

Trouble-Shooting With Connectionview

The information provided in ConnectionView can help you track down connection problems. The figure below shows a single, complete connection as a browser downloads a file:

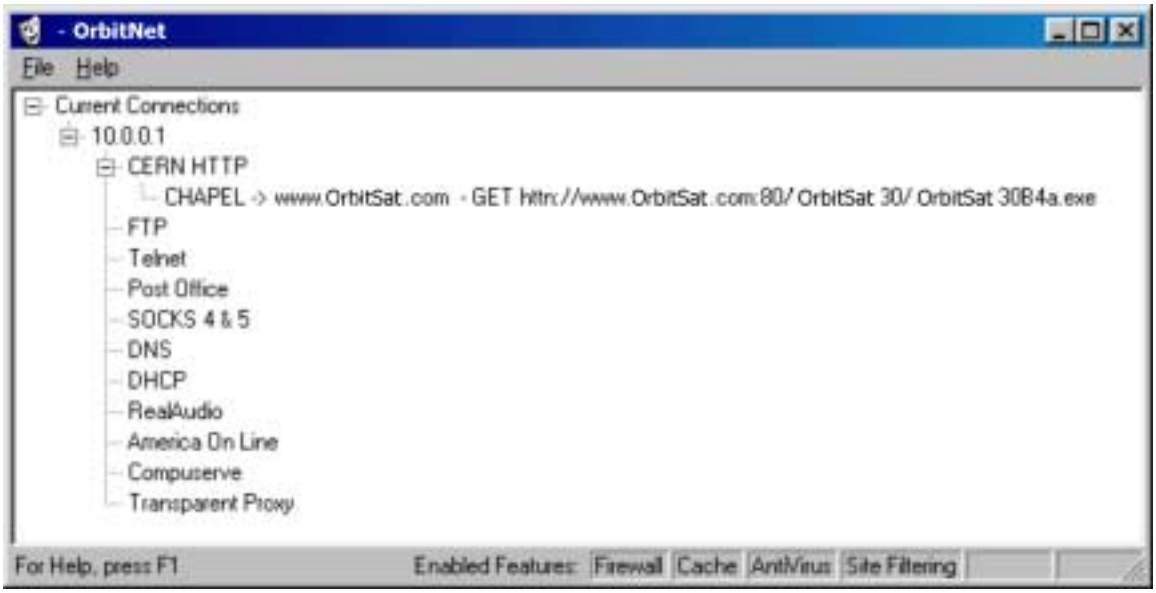


Figure 8-6: Tracking down problems (Transparent Proxy vs. Classic Proxy connection).

The connection shown here is almost the same as the browser connection we showed you earlier, with one difference: it says "GET httn" instead of "GET http." This indicates that the browser is connecting through the Transparent Proxy rather than Classic Proxy.

Figure 7 shows one complete connection—a client computer downloading the files that make up a Web page—and a partial one:

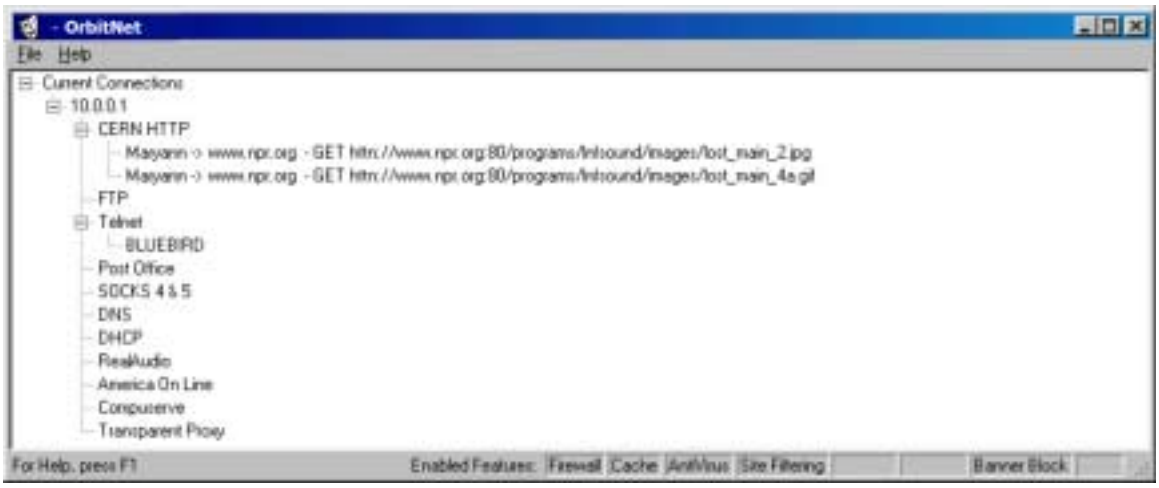


Figure 8-7: Tracking down problems (complete/partial connections).

In this view, the OrbitNet machine has an internal IP address of 10.0.0.1. The client machine, "Maryann," is actively downloading a web page from npr.org. Another client machine, BLUEBIRD, has made a telnet connection to the OrbitNet machine, but has not yet made a telnet connection through OrbitNet to another machine.

The figures below illustrate two conditions that will appear the same in ConnectionView.

The first example shows a failed external connection. We set up a direct connection on the external side—the sort obtained with a cable or DSL modem—and then physically disconnected the cable and made a browser request through OrbitNet. Since OrbitNet is unable to make a connection to the Internet, ConnectionView looks like this:

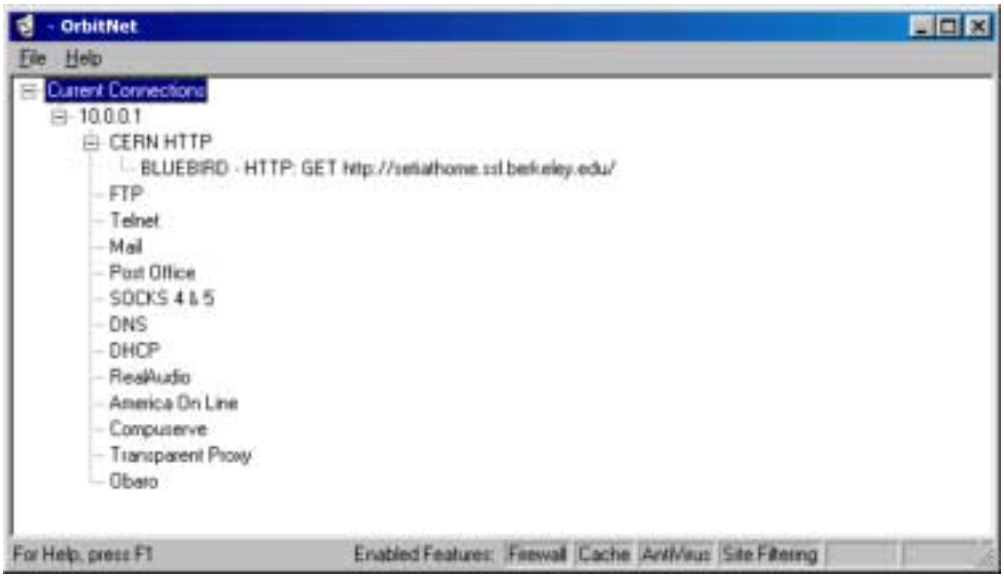


Figure 8-8: Tracking down problems (failed external connection leading to "404 Not Found" error).

In the above example, the internal IP address of the OrbitNet machine is 10.0.0.1. The browser is on the computer named "BLUEBIRD." After a minute or so the connection line will disappear in the OrbitNet window, and the browser will report a "**404 Not Found**" error.

The next example looks the same, but there is actually something a little different going on:

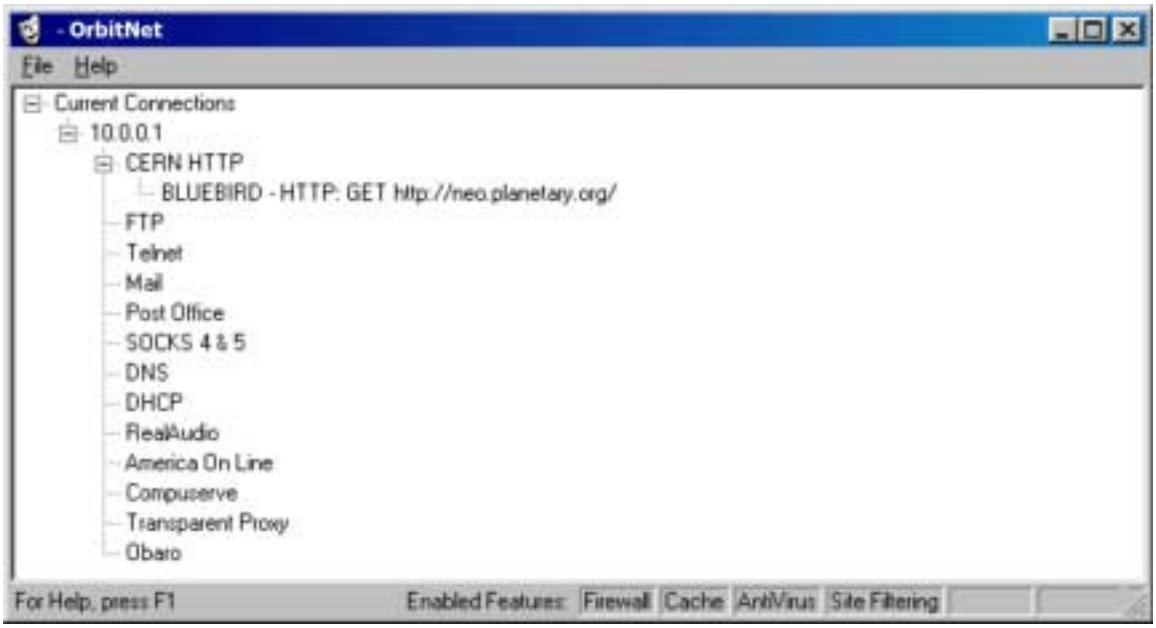


Figure 8-9: Tracking down problems (failed DNS request leading to "430 Unable to Resolve" error).

Here, the OrbitNet machine has an internal IP address of 10.0.0.1. At the point shown, the browser on BLUEBIRD has made a connection request and OrbitNet has initiated a DNS request to the ISP's DNS server to resolve the name into an IP address. The ISP's server has not come back with an answer—the DNS request has failed—and the connection does not proceed further. At the end of the time-out period (one to two minutes), this connection line will disappear and the browser will usually report a "**430 unable to resolve"** message.

The next example shows a failure at the final connection stage. The connection to the ISP is working, and the DNS lookup has succeeded:

Figure 8-10: Tracking down problems (failure at final connection).

The bottom connection is the one that has failed. For a minute or so, this line appeared only as "BLUEBIRD," with no further information shown. The line will normally be visible on the screen in the form shown for only a second or so at the end of the time-out period (about 45-60 seconds). The DNS lookup has succeeded. Now that OrbitNet knows the numeric IP address of the target machine, it has tried several times to connect to that machine. When the connection attempt fails, OrbitNet reports a "0.0.0.0" address and closes the connection attempt. The browser will probably report a "**425 Unable to Connect**" message.

It takes several packets back and forth to establish a connection, and somewhere in the process a packet wasn't received in time. Reasons include:

- a computer is there, but it's down at the moment
- a computer is there, but it's not accepting connections on that port
- a computer is there, but it's busy and fails to return connection packets in the allowed interval
- the TTL (Time To Live entry in the registry's packet settings) is too low
- a high packet-loss rate on the connection means that some packets just never show up (there is some redundancy built into the connection process, but a 5% packet loss rate is enough for you to see some failed connections).

The final example shows two things: 1) an incoming connection—a connection initiated from outside the firewall, connecting through an incoming mapped port to an IP address behind the firewall; and, 2) the form used for incoming connection information.

Figure 8-11: Incoming connections can sometimes take a surprising form.

In this view, a distant machine at IP address "dynamic51.pm02.pleasanton.best.com" has connected through an incoming mapped port on the OrbitNet machine to the client machine at IP address 90.0.0.1. This connection line shows the IP address of the internal machine receiving the connection. That internal connection will almost always be to a machine *other* than the OrbitNet machine itself, but we were playing around a bit while putting OrbitNet through its paces. Take a look under the telnet protocol (the name shown, "ginger.minnow.com," is the OrbitNet machine). The connection you see is OrbitNet responding to the telnet connection request on its **internal** network connection—the one that just came in through the incoming port!

Chapter 9

Settings

CHAPTER 9: SETTINGS

Overview: Settings

This section covers, on a tab-by-tab basis, all configuration screens available under **OrbitNet/File/Settings**. Each topic discussed contains a general description, an explanation of the tab's options, and tips for effective use. The tabs covered are:

1. General
2. Dial-up Setup
3. Protocols
4. User's
5. Site Restrictions
6. Cache
7. Logging
8. Anti-virus

Once you make a change to a configuration setting, it takes effect immediately—or, more precisely, as soon as you've returned to the Main Screen. You'll receive confirmation of changes through a small dialog box informing you that the new settings are now in affect. OrbitNet waits for an end to all communications through the proxy before updating, so any connections in progress won't be disrupted.

If you have a dial-up connection to your Internet Service Provider, you'll be prompted to dial the ISP each time you enter Settings. Once connected, you can use names such as **mail.myisp.com** instead of numeric IP addresses. OrbitNet does an immediate lookup if you use names; if you're not connected, the lookup fails and is followed by a routine time-out period.

A. THE GENERAL TAB

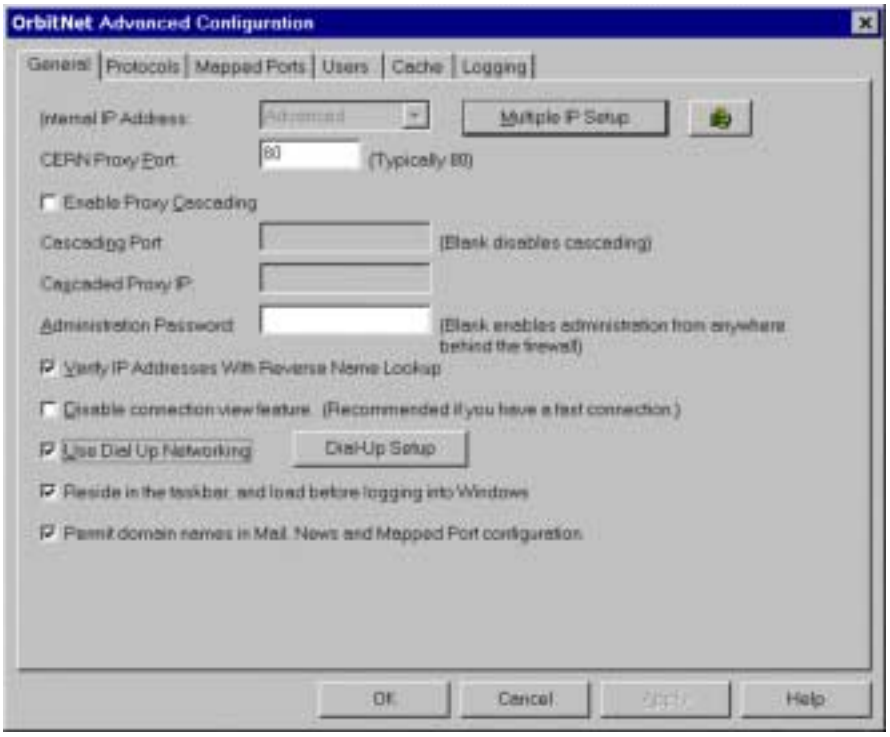


Figure 9-1: The General Tab under Settings determines OrbitNet's fundamental behavior.

The General Tab determines OrbitNet's basic behavior. The screen shown above is from OrbitNet on a Windows 95 operating system. If you're running OrbitNet under NT, the only change will be the next-to-last option. Instead of *Reside in the taskbar, and load before logging into Windows*, this option will read *Run as Service.*

TAB OPTIONS

A. Internal IP Address: The Internal IP address is the one used by OrbitNet to listen for connections on your network from other computers. After OrbitNet examines your system, the IP address (or addresses) it has found appears in the window or drop-down tab. The address displayed is not directly configurable from this tab: if you intend to use an IP address different from the one shown, changes must be made within Control Panel/Networks.

A NOTE OF CAUTION

The IP address shown in the Internal IP box must not be the address of your external connection to the Internet.

For additional information, including a short discussion on the distinction between internal and external connections, click on the question mark.

B. Multiple IP Setup If only one IP address is found, the Multiple IP selection is grayed out. If more than one IP address is found the selection is enabled, as shown in Figure 9-1. Clicking the enabled button produces this screen:

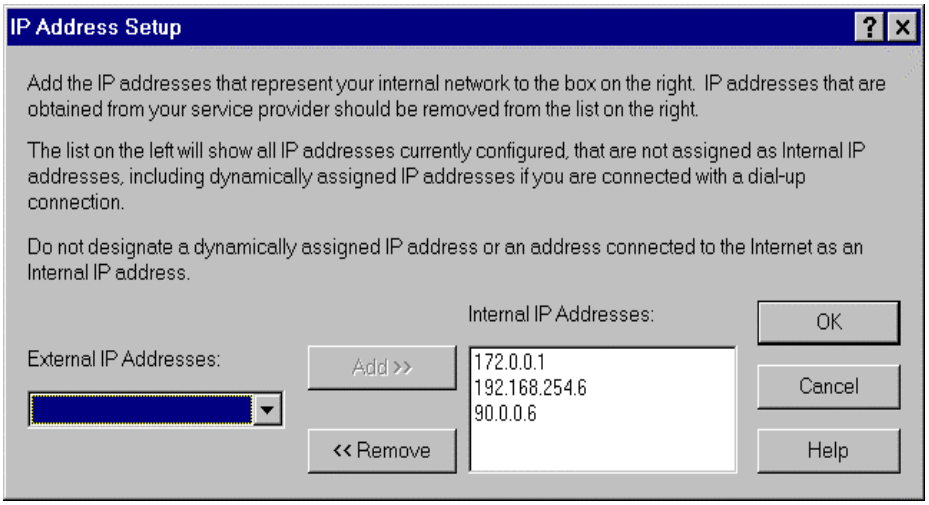


Figure 9-2: Selecting internal IP addresses.

OrbitNet can find IP addresses but doesn't necessarily know which are internal and which external. It makes an "educated" guess and tentatively puts non-routable numbers in the Internal box, but this placement isn't always accurate. Therefore, you need to double-check and be sure that: (1) ONLY the IP address(es) connecting to your local network are listed in the Internal IP box, and (2) the connection to your Service Provider is listed in the External box.

C. CERN Proxy Port: This is the internal port on which OrbitNet listens for Web connections. When doing so, OrbitNet uses the CERN Proxy specification, which supports the CERN Proxy protocol for HTTP and FTP. This port is the primary port used by your browsers for HTTP, FTP, and secure connections. The default setting for this proxy port, 80, is commonly used as the port for World Wide Web activity. If you're already running a web server on your internal network, you may need to change this setting. Port numbers 81, 8080, and 8081 are common alternatives.

D. Proxy Cascading: If OrbitNet is the only firewall/proxy between you and the Internet, you can ignore Proxy Cascading—it won't be needed for most installations in the U.S. and Canada operating behind standard service providers.

However, if you have one or more additional firewalls, you'll want to enable this feature. Some U.S./Canadian institutions do have multiple firewalls in place (certain cable modem providers, large corporations, government agencies, educational institutions, etc.). In addition, service providers outside North America commonly use a proxy when providing service to customers. For more pointers on determining whether you're operating behind another proxy server, look at Step #9 the Properties Wizard in Chapter 5.

Another use of proxy cascading is to secure a network within another network while maintaining access to the Internet through an "upstream" firewall.

Proxy Cascading configures OrbitNet to forward requests from itself to another proxy server. To set it up, you'll need to know the IP address and the Proxy port of the other proxy machine. Cascaded proxies can be nested as deeply as you like, but keep in mind that performance is degraded with each additional proxy cascade. Proxy cascading is currently only supported for HTTP and Secure Sockets requests. Other protocols, such as Mail and News, can be supported indirectly by pointing to the external proxy as the server. Telnet can be done by telnetting to the first proxy, then to the second, and then outside.

Cascading provides access to the intermediate network only when allowed by the next firewall. In practice you will often have access, including when another copy of OrbitNet serves as the external firewall. An example: a company runs one copy of OrbitNet used by all its employees, while a second copy is used by the R&D staff to further secure its valuable data. If you find that you have access to the intermediate net, but not to the outside world, then you probably need cascading to get out.

Cascading Port: This value must be set to the port number of the next proxy server between you and the Internet. If left blank (or if it's invalid), proxy cascading is disabled.

Cascaded Proxy IP: This value must be set to the IP Address of the next proxy server.

E. Administration Password: OrbitNet allows simple administration from any machine on the internal network. Access to such remote administration—as well as to OrbitNet's Time Window override—can be restricted with Administration Password. If this field is left blank:

- Remote administration via http://proxy.command can be done from any machine on the Internal network.
- Any user can override the time window.
- Any user at a OrbitNet computer can enter the Settings and Advanced Settings pages.

Be A Savvy User

Don't forget the password. Write it down and put it in a safe place. *There is no easy way to recover a lost or forgotten password.*

F. Verify IP Addresses with Reverse Name Lookup: OrbitNet contains a security feature that causes all name lookups to be verified with a reverse lookup before a connection is made. In normal operation an address in the domain name form—e.g., OrbitNet.com—is converted to a numeric IP address with a DNS lookup before the page is retrieved from the Internet. When Reverse Name Lookup is enabled, OrbitNet takes the results of the DNS lookup and does a reverse lookup—from number back to name—to ensure retrieving the name you started with.

This procedure adds security to the system by making it very difficult for hackers to use IP spoofing. OrbitNet makes provision for common address changes like legitimate aliases and alternate servers, but it doesn't permit access to valid web pages if they are improperly configured. With a browser you'll see an explicit failure message, while other protocols show a non-specific message such as "403 forbidden." If you encounter trouble accessing certain sites, try disabling this feature.

Note: This option will be grayed out if you have enabled Proxy Cascading.

G. Disable Connection View Feature: ConnectionView allows OrbitNet to show all connections on the main display. Keep in mind that such a display can slow down the system. If you are running on a slower machine with a fast Internet connection, you may want to disable Connection View by checking this box, thus speeding up Internet access. You'll still have access to menu items, but the main portion of the window is left blank.

H. Use Dial-Up Networking: If you want OrbitNet to oversee the modem connection, click Dial-Up Setup to enable and configure this feature. OrbitNet supports only the Microsoft Windows Dial-up Networking program and the AOL automatic dialer, which provide the connection to your Service Provider. More information on this feature is contained under General Properties.

> **Note:** If you have a permanent connection or connect to the Internet manually, leave this option disabled.

I. Reside In The Taskbar And Load Before Logging Into Windows (Windows 95 and higher) or Run as a Service (Windows NT): OrbitNet can reside in the taskbar or system tray under Windows 95/98 and Windows NT 4.0. When OrbitNet is running in the system tray, it shows up as a small "mask" icon on the right side of the taskbar. Double-click on this icon to display/hide the main window. You can also right-click on the icon to connect or hang-up the modem.

Under Windows 95/98, checking this option causes OrbitNet to load before logging into Windows. This allows OrbitNet to restart automatically even after a power failure, when nobody has yet logged into Windows.

Under NT, when running as a service, the options are more extensive. For more information on installing OrbitNet as a service, refer to Chapter 13, "Running OrbitNet As a Service Under Windows NT."

J. Permit Domain Names In Mail, News And Mapped Port Configuration: Checking this box allows you to enter domain names in Mail, News and mapped port settings, rather than using IP addresses. More and more ISP's are using named servers, so they change the actual IP address at will. Most users these days must use names for their mail and servers. If it's possible to use the actual IP address instead of the name, you add some security to your system. By using IP addresses you are much less susceptible to IP spoofing.

> **Note**
> You should be connected to the ISP when entering names into the configuration boxes.

B. The Dial-Up Setup Tab

The Dial-Up Setup Tab is used to configure the way your modem accesses the Internet. The screenshot below will look familiar to people who have already used OrbitNet—a few options have been added in the latest release, but otherwise it looks much the same as in earlier versions of OrbitNet.

However, although it's user-transparent, OrbitNet 3.0 handles dial-up connections in a completely new way, with Background Dialing. Unlike previous versions, you can still use, change and configure OrbitNet while dialing proceeds as a background operation. OrbitNet 3.0 provides a great deal of information about the Dialing State. Along with data available in version 2.1 (connected/not connected and connected/idle time), 3.0 reports via ConnectionView's modem line about dialing, connecting, negotiating, authenticating, and more. There are altogether nine distinct dialing states, though some occur so rapidly they won't be visible.

Besides providing more information, 3.0 offers a more "forgiving" dialing method: it won't leave OrbitNet in an unusable state when Dial-Up Networking fails to return from its task.

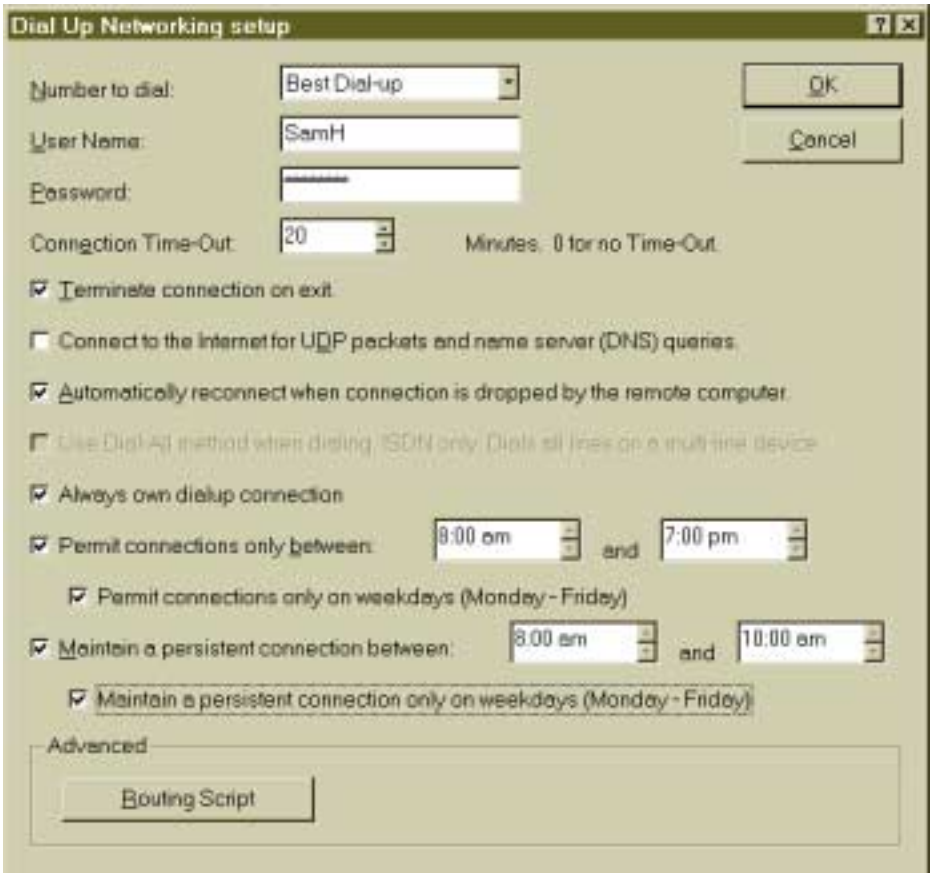


Figure 9-3: Use the Dial-Up Setup Tab to configure the way your modem accesses the Internet.

TAB OPTIONS

A. Number to dial: The drop down list shows all the entries in your dial-up networking phone book. Select the number you wish to dial to connect to the Internet. OrbitNet then tells Dial-Up Networking to dial this number. If you need to alter any Dial-Up settings other than name or password in OrbitNet, do so within Windows Dial-Up Networking.

B. User Name: Enter the logon name you use when connecting to the Internet. This name was assigned by your service provider, and will be used when OrbitNet logs onto the Internet. Most providers use case-sensitive usernames and passwords.

AOL users take note: when you choose the AOL connectoid, the username option will be greyed out (unavailable), but you'll still be able to enter a password. The username for connections to AOL is the same as the default name in the AOL browser on the OrbitNet machine—and can't be altered.

C. Password: Type in the password you use when logging onto the Internet. This password was chosen by you or assigned by your service provider. Both user name and password are required for automatic connection to the Internet. If you change your ISP password, be sure to change it in this field as well.

D. Connection Time-Out: If you choose, OrbitNet can disconnect from the Internet after it falls idle. It accomplishes this via an inactivity timer; if there has been no communication activity through OrbitNet for an amount of time specified in Connection Time-Out, OrbitNet informs Dial-Up Networking to end the connection. If you want OrbitNet to stay permanently connected, set Connection Time-Out to 0. Some Service Providers have their own inactivity timers and will disconnect you after a specified amount of inactivity; the Connection Time-Out setting has no effect on their actions. The inactivity timer works only on Classic Proxy and Transparent Proxy connections. Connections through the NAT are not visible on the main screen and thus won't affect the inactivity timer in any way. OrbitNet may hang up on these connections in mid-stream if no visible activity resets the timer.

E. Terminate Connection on exit: Check this box if you want OrbitNet to hang up its modem connection when you the program. If this box is unchecked, the connection remains active when you exit OrbitNet.

F. Connect To The Internet For UDP Packets And Name Server (DNS) Queries: OrbitNet automatically dials when contacted via HTTP, FTP or other protocols using the Classic Proxy or the Transparent Proxy (it won't dial for NAT connections). However, unless enabled here, it does *not* automatically connect for UDP packets or DNS queries. Thus, if you want Socks applications (which start with a DNS query) to force an automatic dial, check this box.

A NOTE OF CAUTION

Many unseen network activities also utilize UDP and DNS. When this box is checked, you'll see a lot of "ghost" dialing whereby OrbitNet dials for no reason apparent to the user. We ship the product with this option disabled.

G. Automatically Reconnect When Connection Is Dropped By The Remote Computer: If it's important to keep an Internet connection maintained at all times, check this box. OrbitNet will then automatically reconnect to the Internet if the connection is broken. If the box is *not* checked, OrbitNet reconnects only when specifically requested to do so.

H. Use Dial-All Method When Dialing: This option is available for Windows 98 and Windows NT. It will be grayed out when running on Windows 95. When you check the box, the operating system supports both channels on an ISDN device; if you have Multi-Link on NT 4.0, it provides dialing for

multiple lines with increased bandwidth. For multiple lines to work, however, your ISP must also support Multi-Link.

I. Always own dialup connections: OrbitNet can communicate over the modem to an ISP no matter who initiates the connection. Normally, however, OrbitNet cannot enforce its inactivity timer or allowed dialing period unless it initiated the modem connection. Enabling this option allows OrbitNet to take control of the modem even when another program initiated the connection.

J. Permit Connections Only Between: By enabling this option, OrbitNet allows connections only during specific time periods: it dials during the specified interval, disconnecting at the interval's end. Users trying to utilize a browser outside the interval see a page allowing an optional extension of time. If the Administration Password on the General Tab has been set, the user must enter the password before extending the time. If a user tries a different protocol "after hours," the connection attempt times out with no explanation given. All dialing time settings rely on the time information that Windows maintains on the OrbitNet computer. This information must be correct for these time restrictions to operate as expected.

K. Permit Connections only on Weekdays: This is a modifier to *Permit connections only between*, above. When the weekday-only option is enabled, dial-up connections won't be permitted on weekends unless the user initiates the password override or persistent connection period options.

L. Maintain A Persistent Connection Between: Check this box if you want OrbitNet to maintain a persistent connection during a specific time period. During this period OrbitNet will not hang up, will dial immediately at the beginning of the period even if there is no request from a client, and will redial immediately and repeatedly if the connection is lost. OrbitNet doesn't try spoofing the ISP into thinking there is traffic on the line when none exists. *Persistent connection* overrides *Permit Connections*, and establishes a connection outside the allowed time window if so configured.

M. Maintain a Persistent connection only on weekdays: This is a modifier for *Maintain a Persistent Connection*. When enabled, OrbitNet ignores the persistent command settings on Saturdays and Sundays.

N. Routing Script: Skip this option if you have a single local network. However, if you have more than one local network, and some of your subnets disappear when you call your ISP, read on.

The routes in your TCP/IP stack are rewritten each time you connect via the Dial-up Adapter, and in certain cases (especially in Windows 95/98) can leave a subnet unreachable. The Routing Script option gives you a way around this problem, allowing OrbitNet to later accomplish its own route additions and restore the paths. Click **Routing Script** to read extensive details on this option.

C. The Protocols Tab

The Protocols Tab allows you to enable and configure, for use on your local system, a wide variety of protocols, including HTTP, FTP, Telnet and Socks.

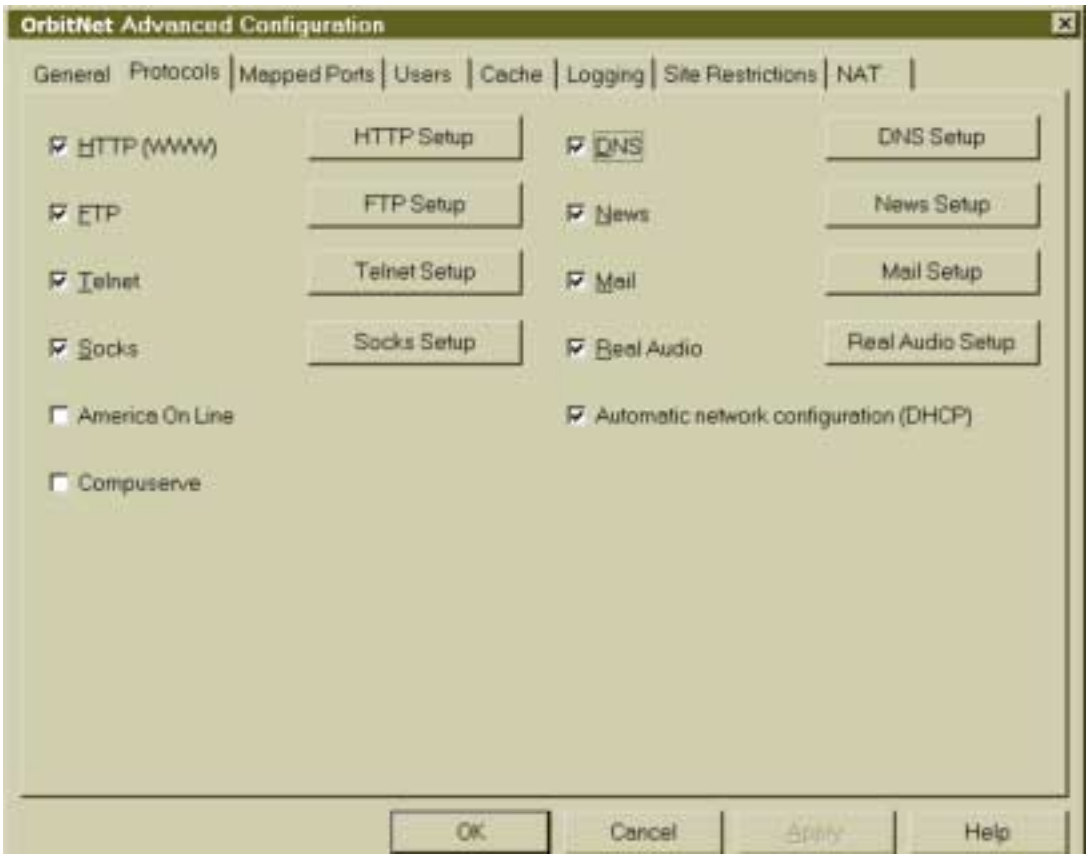


Figure 9-4: Use the Protocols Tab to establish protocols settings, including those for HTTP, FTP, Telnet and Socks.

TAB OPTIONS

1. HTTP SETUP: HTTP (HyperText Transfer Protocol)—the protocol used on the World Wide Web—allows one computer to retrieve documents from another. The HTTP checkbox option shown above enables the HTTP Proxy, often called the "proxy server." HTTP servers usually listen for connections on port 80.

When you enable the HTTP proxy in OrbitNet, you also automatically enable secure sockets connections (known as HTTPS or SSL, and used for secure transactions on the Internet), unless it's specifically prohibited by command filtering (see below). Enabling the HTTP proxy also enables the classic CERN HTTP proxy, which allows the Transparent HTTP Proxy. If the Transparent HTTP Proxy is to work, however, both the HTTP setting and the transparent proxy setting on the NAT Tab must be on.

If you leave the HTTP checkbox blank, both the classic HTTP proxy and the Transparent HTTP proxy will be disabled.

✔***USER'S CHECKPOINT***: Browsers configured to use a proxy server go through the classic proxy. Client browsers configured to use a network connection **but not a proxy server** connect through the Transparent proxy or the NAT, Classic Proxy and Transparent Proxy connections) take advantage of caching and submit to user and site restrictions set in OrbitNet. The classic proxy provides better performance when your browsers connect to Internet http 1.1 servers.

The HTTP Setup Dialog allows you to configure command filtering and a reverse proxy path for an HTTP (Web) server, as well as enable SSL (secure sockets connections) on non-standard ports.

A. Enable Command Filtering allows you to specify which specific HTTP commands OrbitNet users can utilize. Command Filtering works on both Proxy (http) and Transparent Proxy (httn) connections. The various sub-options are grayed out until you check Enable Command Filtering; you may then select the sub-options you want available to users. We discuss here the four most commonly-used commands (you'll probably never need to use the others, which are proposed HTTP extensions):

- **Get**: Retrieve a document from the server. Get is the most common command.
- **Put:** Put a document onto the server. Put is used when authoring a web page and should be enabled only if it's needed.
- **Connect**: Connect establishes a secure sockets connection. OrbitNet supports secure sockets proxying. If you don't want secure sockets, disable this command.
- **Post**: Post is used to fill out a form on the web and submit the results. If this option is disabled, many standard web features will also be disabled.

NOTE TO LAN ADMINISTRATORS

If command filtering is disabled, all commands are permitted—even those not recognized—as long as they are formatted correctly.

B. Permit SSL Connections on non-standard ports allows secure connections on non-standard ports. This option applies to connections through the standard proxy, and is not needed for connections through Transparent Proxy. Enable this option if software you're using—or a website you're accessing—establishes SSL connections on ports other than the standard 443 and 563, and the software is configure to go through a proxy. Secure servers using non-standard ports are becoming more common on the Internet.

C. Incoming HTTP Proxy allows you to open a web server on your local net to other people on the Internet (if you don't have a web server, leave this option disabled). To reach your internal web server, outsiders must have the external address of your OrbitNet machine (either a static external address or a maintainable dynamic address with IP address publishing software). OrbitNet can use command filtering on the incoming connection. The internal location of the web server can be changed at any time without having to change the name registered with official Internet organizations.

Once this option is enabled, OrbitNet makes an exception to its rule of never listening for external connections. It passes any external connection on the HTTP port (80) directly into the machine specified in Internal Server IP (see below), with no validation except the command filtering you've established.

A NOTE OF CAUTION

Enabling this option, which allows outsider access to the web server constitutes a hole in your firewall. The web server is responsible for its own security. See *Using Wildcards With Settings* for pointers on enhancing the security of internal servers which are outsider-accessible. The example shown is for a mail server, but the same method works with an internal web server.

- **Internal Server IP:** Enter the local IP address of your machine with the web server.
- **Internal Server Port:** You would normally use the common port 80 here, but you don't have to.

D. Permitted Incoming Commands allows you to specify commands that others can send to your local web server. It pays to be selective. **Get** and **Post** cover most common web interactions; don't enable the others unless you're sure you need them.

2. FTP SETUP: The File Transfer Protocol (FTP) Proxy, the second checkbox option on the Protocols Tab, is used to transfer files between computers on the Internet. Click **FTP Setup** to change the port number used for FTP connections—the port used by other FTP programs such as CuteFTP or WS_FTP when operating through the proxy. This box enables/disables only the classic FTP proxy. The Transparent FTP proxy is enabled when you enable **Transparent Proxy for FTP connections** on the NAT Tab.

Take Note: FTP access through proxy-enabled browsers can use either the CERN HTTP Proxy protocol or the Socks protocol.

✔***USER'S CHECKPOINT***: FTP applications (including the command line) which connect to the OrbitNet machine first on the FTP port, wait for the prompt, and **then** connect to the distant server are using the classic FTP proxy. Applications which connect **directly** to the remote address are connecting through the Transparent Proxy or the NAT.

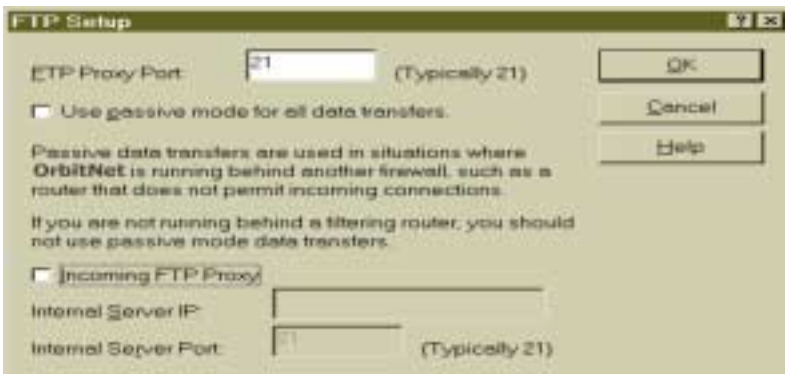


Figure 9-5: FTP Setup allows computers on your network to transfer files back and forth with computers on the Internet.

Port 21 is a standard port for FTP connections. If your firewall machine is already running an FTP server on port 21, you may want to choose another port. A commonly-used alternate is 8021.

For more information about using command-line FTP and various FTP software applications with the classic proxy, refer to **Configuring Common Applications** in the Technical Support section of our website (http://www2.OrbitNet.com).

OrbitNet will first attempt a PASV mode connection when establishing an FTP session between a client *browser* and an FTP server on the Internet. The setting in the **use passive mode for all data transfers** box determines what happens if OrbitNet fails to connect in the PASV mode.

- If this box is *not* checked, OrbitNet falls back to the **User@Site** method and attempts another connection. If the second attempt fails, OrbitNet passes along the server's error message (if one was received) or a "failed to connect" message.
- If the box *is* checked, OrbitNet immediately reports as an error that the distant server does not support the PASV mode. These error reports are only visible in the browser.

Check this box when using OrbitNet behind a filtering router. Many such routers don't permit the return connection required for a **User@Site** connection.

When you use an FTP application such as CuteFTP or WS_FTP on a client machine, OrbitNet passes along whichever of the two supported modes (PASV or User@Site) the application uses.

NOTE TO FTP GURUS

When you attempt an FTP connection with a browser, OrbitNet preferentially uses the PASV mode between itself and network servers, but the connection on your internal network between the browser and OrbitNet will not be a PASV connection. A browser will use either HTTP via the CERN HTTP proxy, or Socks via the Socks proxy.

When setting up another FTP program, enable its **User@Site** option. See our website for screenshots of specific applications.

Version 3 of OrbitNet offers a new feature: support for a publicly-accessible FTP server behind the firewall. To reach your internal web server, outsiders must use the external address of your OrbitNet machine.

NOTE

We recommend putting your FTP server on a client machine, not on the OrbitNet machine. The only way to make an FTP server work well on the OrbitNet machine is to set the Firewall setting to Low or Medium Low, disabling much of your firewall. PASV connections will fail on any other firewall setting, and PASV connections are at the discretion of the FTP client, not the FTP server. Putting your FTP server on a client machine allows you to use higher firewall settings, and permits PASV connections to your server.

Just as with any other incoming connection, when you enable the incoming FTP server, you create a potential firewall hole. Whatever program receives the incoming connection is responsible for the security of that connection. See *Using Wildcards with Site Restrictions* for pointers on enhancing security when you must have a public server behind your firewall. The example given also applies to an FTP server.

Internal Server IP: Enter the IP address or computer name of the local network machine with the FTP server. The name won't be saved; OrbitNet executes an immediate lookup to resolve the name to an IP address. Your FTP server should have a static local IP address. Any connection request seen on OrbitNet's external IP address on port 21 will be forwarded directly to the Internal Server IP and Port.

Internal Server Port: Enter the port on which your FTP server will listen for connections. In most cases the standard FTP port 21 won't interfere with other FTP applications on that machine.

3. TELNET SETUP: This option enables the classic Telnet Proxy, which connects Internet computers through a remote connection. Click **Telnet Setup** to change the port number used for the Telnet proxy. The

standard telnet port number is 23 (don't change it unless you have a specific reason). Telnet will be enabled through the Transparent Proxy whenever **Transparent Proxy for all connections** is enabled on the NAT Tab.

✔ **USER'S CHECKPOINT** : If you telnet from a client machine to the OrbitNet telnet port and wait for a prompt before connecting to the Internet, the connection is being made through the classic proxy. If you telnet using the final destination as the address, you're going through the Transparent Proxy or the NAT.

The following options apply *only to the classic Telnet proxy*:

A. **Time out after xx minutes of idle time**: OrbitNet will discontinue inactive connections after a specified time, preventing an inadvertent failure to close from keeping OrbitNet connected to the internet. The user can specify the time out length for telnet connections.
B. **Echo Characters In Domain Name** allows OrbitNet to echo typed characters back to the telnet application. If you plan on using telnet, you'll probably want to enable this.
C. **Permit Telnet to Ports Other Than 23** is a useful diagnostic tool, allowing you to telnet to other ports besides the standard 23.
D. The following instructions (for Windows telnet) illustrate how to use the Classic Proxy telnet from a client.
E. Start telnet: open a DOS box (**Start/Program/MS-DOS Prompt**) and type **telnet** on the command line.
F. When telnet comes up, click **connect** and then **remote system**.
G. Enter the IP address of the OrbitNet machine in the Host box. Enter OrbitNet's telnet port in the Port box (the default is 23).
H. Click **connect**. You should see a few lines and a prompt back from the OrbitNet machine. You're now ready to telnet out to the Internet.

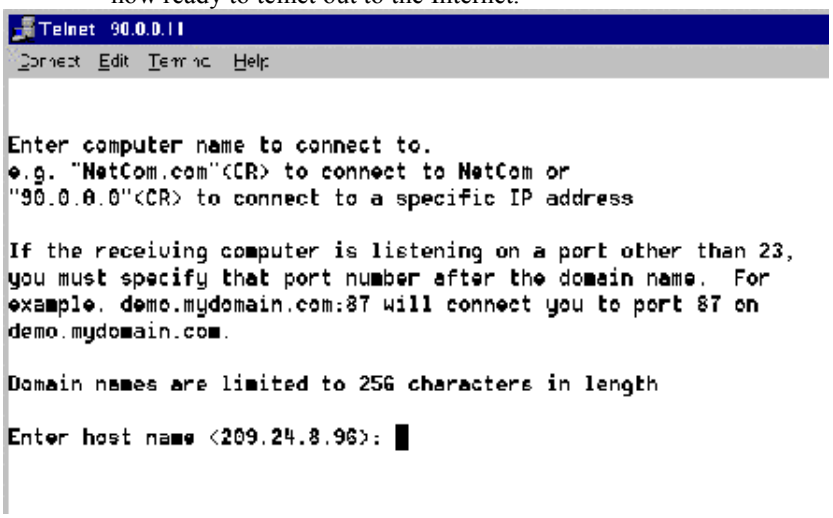


Figure 9-6: Classic Proxy saves Telnet addresses, making it easy to return to the same site.

With these options enabled, Telnet can be a useful tool. On the example screen you'll notice that OrbitNet Classic Proxy saves your previous telnet entry. Thus, if you visit the same place repeatedly you need only hit **Enter** instead of re-typing the destination.

To use telnet via the Transparent proxy, open telnet and enter the name or IP address of the final destination (rather than the IP address of the OrbitNet machine). You will not get a prompt from the OrbitNet machine. Classic proxy telnet connections will appear under the Telnet protocol heading in ConnectionView, and Transparent proxy telnet connections will appear under the Transparent Proxy heading. No options shown here will apply to Transparent proxy telnet connections. Inactive Transparent proxy telnet connections are automatically closed after twenty minutes.

4. SOCKS: SETUP: This option enables the Socks Proxy, a powerful and flexible protocol used for several types of connections. The Socks Setup Dialog allows you to configure the port number OrbitNet uses when listening for Socks connections (usually 1080). If you enable the Socks proxy, be sure to also enable the DNS proxy and set up DNS on your local system (DNS is required when using Socks). Socks is a powerful and flexible protocol. Your browsers can use Socks for news, mail, and FTP functions.

✔***USER'S CHECKPOINT***: Socks is implemented **only** via the classic proxy.

5. AOL SETUP On Client Computers, using alternate ISP: This section describes how to set up AOL access on client computers when OrbitNet is connected to a standard ISP (that is, not AOL—see the note below). Although the paths and screenshots shown here are for the AOL 4.0 browser, the principles remain the same for AOL 3.0.

IMPORTANT NOTE

If America Online is your Internet Service Provider, you *must* install AOL on the server computer and verify that you have a working connection to AOL before you can utilize OrbitNet. For detailed information, refer to Chapter 14, "Running OrbitNet with AOL as an ISP."

To begin, open the AOL program on the client computer. When you get to the Logon Screen click **Setup** on the bottom right. When a new window opens, click **Expert Setup** button on the bottom right (see image below).

Figure 9-7: The first step in changing how your computer connects to AOL.

In the next window, illustrated in the figure below, click **Expert Add**:

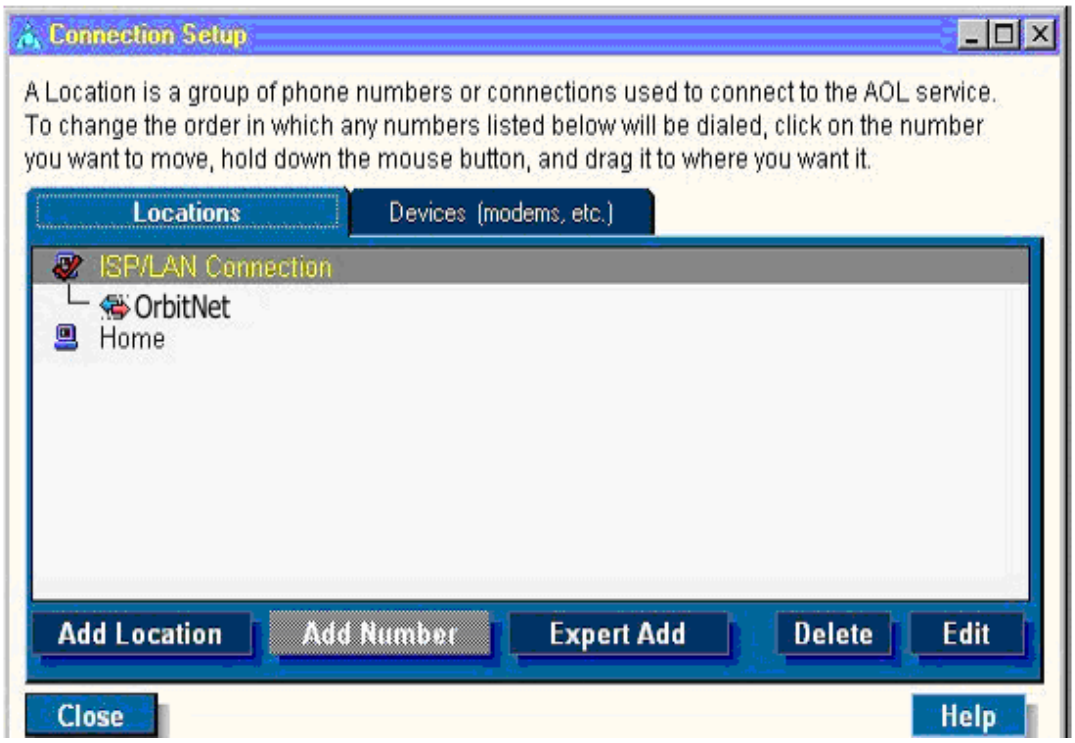


Figure 9-8: The second step in adding AOL to your OrbitNet setup.

You will now see the "Add Number (Connection)" window, which is where we'll set the client computer up to connect through OrbitNet.

Figure 9-9: Permitting the client computer to connect through OrbitNet.

To do so:

1. In the "Name" field, enter OrbitNet.
2. The field "Will Be Added To This Location:" should be changed to "ISP/LAN Connection," and "Connect Using:" should be changed to "TCP/IP, LAN or ISP."
3. Place a check in the "Automatic Connection Script: Direct TCP/IP Connection" box. Finally, click **OK** followed by **Close**.
4. Exit from AOL to ensure that settings are updated.

When you've completed all the steps outlined above, open the AOL program and logon using your AOL account name and password.

NOTE: A few caveats to keep in mind when running AOL clients behind OrbitNet connected to a standard ISP:

1. Only one instance of any single AOL account may be open at a time (and you can't get around this by using different aliases from the same account).
2. Any number of *different* AOL accounts can be open at the same when connecting through a standard ISP.
3. AOL browsers must be run from client machines when accessing AOL in this manner; you cannot use an AOL browser on the OrbitNet machine.

6. COMPUSERVE SETUP:

NOTE TO COMPUSERVE VERSION 4/2000 USERS

If you're using CompuServe version 4, we recommend using OrbitNet's Classic Proxy.

If you're a CompuServe2000 user, however, we recommend the Transparent Proxy. If that's the case, you won't need to enable OrbitNet's CompuServe protocol before proceeding with the steps outlined below.

CompuServe 4 Users:

- Enable the CompuServe protocol in OrbitNet.
- Configure CompuServe browsers on client machines to use the TCP/IP protocol (rather than a dial-up connection).
- On each client computer with a CompuServe browser you'll need to modify one of the CompuServe files so that the browser can find the OrbitNet server. To do so, find the CIS.INI file. Under the heading **[Connector (CIS Connection)]** look for these two entries:

  HostIPName=
  HostIPAddress=

  Enter the name and internal IP address of the OrbitNet machine after the = sign.

CompuServe2000 Users:

Make sure that OrbitNet has Transparent Proxy or NAT settings enabled (Transparent Proxy is enabled by default). On the machine with CompuServe2000, check to see that the machine's network settings includes a Gateway setting with the OrbitNet internal IP address—this will be needed by *any* application using Transparent Proxy, not just CompuServe.

When you start up CompuServe2000 and see the screen "Connect to CompuServe," hit the "Setup" button. Choose "Add Location," and then "Add Custom Location (for example TCP/IP)." Make sure the

connection setting has "TCP/LAN." Finally, enable the box for "AutoConnection Script." Okay your way back out.

Open the "Connect to CompuServe" screen and connect.

7. DNS SETUP: This option enables DNS, permitting OrbitNet to act as a DNS server on your local network. Anything OrbitNet can't resolve on the local network it tries to resolve through the servers you list in the DNS Setup Dialog. These will be the DNS servers provided by your ISP; they will be queried in their listed order.

If you have multiple DNS servers available from your ISP, add the Primary DNS server first. Enter the secondary DNS servers in the order you want them searched.

The DNS server IP addresses should be available—and are best obtained—from your service provider. However, if necessary, OrbitNet can link you to a web site displaying the IP addresses used by your service provider: just click **Find my Name Server**. You may see some unfamiliar IP addresses when you first look in the OrbitNet DNS settings; if no DNS address was specified during initial installation, then OrbitNet enters default addresses. For best results, use your service provider's DNS addresses instead.

To add a server to the list: type the server name into the box on the left and click **Add**.

To remove a server from the list: select it in the list on the right and click **Remove**.

OrbitNet will function as a full Domain Name Server, resolving names for computers inside your firewall. To do so efficiently, it needs to know the domain name which refers to your network (this needn't be a domain recognized on the Internet). In the setup dialog, enter the name you want used in the Domain field; you should enter the same name in the TCP/IP configuration on each internal computer. Searches are quicker if the domain name is appended by a common appellation such as **.com** or **.org**.

> **Note**
> For OrbitNet to function as the DNS server for your entire local network, you'll have to configure the other computers as DNS clients. See Chapter 7 for details.

Next, enter the names and IP addresses of your local computers in **NameList.pxy**, the file used by OrbitNet's Domain Name Services and DHCP server to associate names with local addresses. This file can be edited by clicking **Edit NameList**. If your domain is **MyDomain.com** and your computer is named **MyComputer**, enter **MyDomain.com** as the domain in the DNS configuration and specify an IP address for **MyComputer**. OrbitNet then resolves the name for MyComputer, as well as MyComputer.MyCompany.com. Computer names are not case sensitive: it makes no difference whether you type *mycomputer* or *MyComputer*.

Edit Name List configures name services. When you click **Edit Name List**, a notepad with the NameList.pxy file is brought up. A sample file is included which contains detailed instructions on formatting names and IP addresses. If OrbitNet is your DNS server, the namelist will hasten local lookups.

Proxy DNS Through TCP enables the TCP proxy for DNS, which is typically transmitted through UDP (The TCP method is rarely used with DNS). Unless you're certain it's needed, we recommend leaving TCP disabled to save system resources and obtain improved performance.

Many new features in OrbitNet, such as BannerBlocker, rely for functionality on a close coupling with OrbitNet's DNS server. In other words, for these features to work correctly OrbitNet must be your DNS server. If you already have a DNS server on your local network, we recommend that the client machines recognize OrbitNet as the DNS server; OrbitNet can then use your other DNS server as the first machine in its search order. This other DNS server must in turn have an Internet DNS server as part of its own search order. Be sure to avoid DNS loops where each of your local servers references the other.

8. NEWS SETUP: News has its own protocol, called NNTP. The Internet News Setup dialog allows you to configure (a) the port number on which the classic News proxy will listen for connections, and (b) the IP address of an external News server to which it will connect them. NEWS Setup enables only the classic News protocol; the Transparent news protocol is enabled when you choose **Transparent Proxy for all connections** on the NAT Tab.

✔***USER'S CHECKPOINT***: When a news application uses the OrbitNet IP address as the location of its news server, it's utilizing the classic proxy. When using the "real" IP address of the news server, it utilizes the Transparent Proxy or the NAT.

News Server IP: Enter the IP address of the external News server (usually your ISP's News Server). OrbitNet always uses port 119 on its *external* network connection to communicate with the News Server at the IP address specified here.

News Proxy Port: Enter the port number on which OrbitNet listens for News requests on its *internal* network connection. All client connections arriving on this port are forwarded to port 119 at the IP address specified in News server IP, described above. The default value for this field is 119.

The Classic proxy news settings allow access to only a single news server. With Transparent Proxy enabled, you can connect to as many different servers as you want. In some cases, service providers won't allow connection to news server unless you use their dial-up facilities.

9. MAIL SETUP: This protocol enables only the classic Mail proxy, permitting you to enable incoming SMTP. If you prefer, client mail applications can continue to access external mail servers via the Transparent Proxy or the NAT.

Several different protocols are used for mail:

- SMTP is used for sending mail.
- POP3 is used when receiving mail.
- IMAP4 is an alternative protocol for receiving mail.

SMTP and POP are commonly used; IMAP4 less so. As a general rule, if you don't know what protocol you're using, you probably have POP service. Most service providers locate their SMTP and POP servers at the same IP address, but a substantial minority use different addresses.

To use the classic Mail proxy, you must first configure an external Mail server and an external POP server. The Mail Setup Dialog allows configuration of the IP addresses used for connecting to external SMTP, POP3, or IMAP4 servers. OrbitNet won't permit you to change the *external* ports used for mail communication (they're standard and don't vary). You can, however, change ports on the *internal* network connection where it listens for mail communication from client mail applications.

USER'S CHECKPOINT: If your mail application is configured to use the OrbitNet address as the mail server address, it's connecting through the classic proxy. If the mail application is configured to use the real mail server address, it's using the Transparent Proxy or the NAT. The Classic Proxy provides a greater degree of control; the transparent proxy makes it easy to reach many different mail servers.

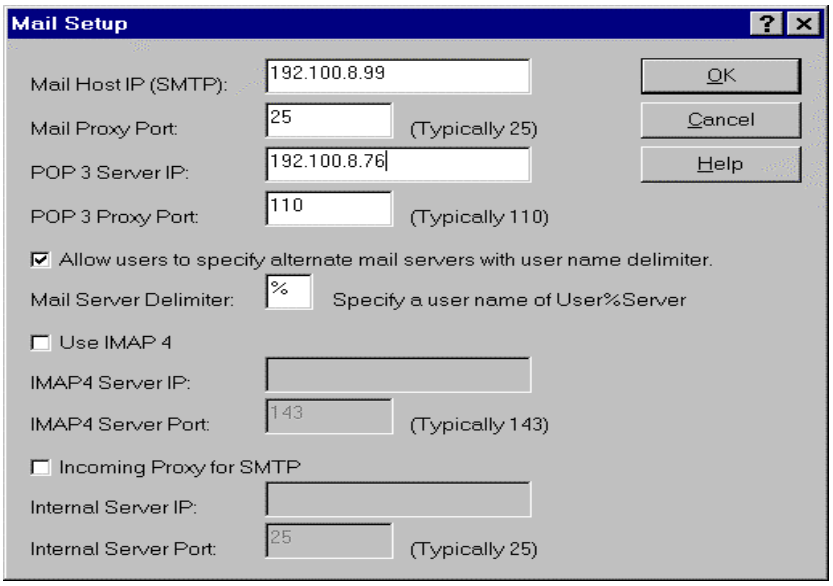


Figure 9-10: The Mail Setup Screen.

The following options (except the final options pertaining to Incoming SMTP proxies) apply ***only to the Classic proxy implementation*.**

A. ***Mail Host IP*** specifies the IP address for connecting to an *external* SMTP server to which outgoing mail is sent. OrbitNet always uses the standard SMTP port 25 to connect to this server. You can specify on which *internal* port OrbitNet listens for mail in the Mail Proxy Port, described below. If connected to the Internet, you can enter a name instead of an IP address; however, an IP address is preferable.

B. ***Mail Proxy Port*** is the port number on which OrbitNet listens for SMTP communications from client computers. All connections are forwarded to the standard SMTP port at the IP address specified in Mail Host IP. The default value for this field is 25. Unless you have special configuration needs (such as installing your own local mail server) you won't need to change the default setting.

C. ***POP 3 Server IP*** specifies the IP address of the external POP3 server, where you go to check your incoming mail. OrbitNet always uses the standard POP3 port 110 to connect to this server.

D. ***PPOP 3 Proxy Port*** is the port number on which OrbitNet listens for POP3 communication from your local client computers. All connections are forwarded to the standard POP3 port at the IP address specified by POP3 Server IP, described above. The default value for this field is 110, and shouldn't need to be changed unless you have specific configuration needs.

E. ***Use IMAP 4*** is only for IMAP 4 users. Unless you specifically know otherwise, you probably won't need to use this option.

F. ***IMAP 4 Server IP*** specifies the IP address used to connect to an external IMAP 4 server. OrbitNet always uses the standard IMAP4 port 143 to connect to this server.

G. ***IMAP 4 Server Port*** specifies the port on which OrbitNet listens for IMAP4 connections from your local network. The default value for this field is 143.

ALTERNATE MAIL SERVERS

NOTE

As a security precaution, some service providers won't permit mail access from another Internet site but only via a direct dial-up connection. As an anti-spamming measure, many providers won't permit you to send mail (SMTP) except through their own dial-up connection. A smaller but growing group won't allow you to receive mail (POP or IMAP) except through their own dial-up connection.

This section applies only to network administrators who wish to control which mail servers their users can reach and have both NAT and the Transparent Proxy turned off. When either one is enabled, users can enter the real IP address of any external mail server and reach it. With both disabled, the only way to reach additional mail servers is through the classic proxy.

Three different methods are used to specify additional mail servers (mostly used for additional POP servers). One method is useful when a single user needs a different server than the one ordinarily configured; this can be set with the User/New Tab, described elsewhere. The second is similar to the method used for adding news services; it's shown in the section on Mapped Ports. The third method is enabled with the two settings described here:

A. Allow users to specify alternate mail servers is modeled after the POP3 server usage of delimiters. This feature will not work through a cascaded proxy.

B. Mail Server Delimiter allows you to choose a delimiter, within reason. Most non-alphanumeric keyboard characters are eligible; OrbitNet will not permit those in common usage for other purposes (the @ sign, for example).

Using these methods you can specify the mail server *wiithin the client application*. Usage will vary, depending on the specific mail application. One example: use the delimiter # in the **username** field, as in **username#mail.distantserver.com**. You can have as many additional mail servers as the application allows. More information about delimiters is posted on our website.

INTERNAL MAIL SERVERS

The following settings configure access to an internal mail server behind OrbitNet. This option generally applies to medium and larger businesses; if you're getting mail from a service provider's server, you won't need to use these settings.

Mail Servers use the SMTP protocol to send mail to each other. The following settings allow outside mail servers to send mail directly to your mail server behind the firewall. There is little provision for "maybe later" between mail servers; any single mail server expects to be able to send mail directly to another at any time. In practice, this means having OrbitNet and your internal Mail Server running all the time, and a static IP address for your Internet connection.

External mail servers use the static IP address of the OrbitNet machine as the address to send mail. Any mail connection to the external OrbitNet SMTP port will be sent directly to the internal IP address and port you specify in the settings below.

A NOTE OF CAUTION

Do not underestimate the fact that these settings constitute a hole in your firewall, allowing potential entry to your network by an outsider. ***Your internal mail server is responsible for its own security***. Some mail servers have well-known security holes, and it's possible for hackers to enter through the incoming SMTP, and exploit the mail server holes to gain access to the rest of the internal network. ***It's up to the mail server to prevent this***. See *Using Wildcards with Site Restrictions* for a method of limiting your exposure through the mail server.

A. Incoming Proxy for SMTP. OrbitNet can work as a reverse proxy for SMTP, allowing you to place an internal SMTP server behind the firewall. This protects the server from unauthorized access, while permitting people to send mail to it from the Internet. Once this option is enabled, OrbitNet makes an exception to its rule of never listening for external connections, and will listen for incoming connections on port 25. It will not qualify or validate the incoming connections.

B. Internal Server IP specifies the (local) IP address of your internal SMTP server. When a connection is received on external port 25, OrbitNet forwards the connection to this machine.

C. Internal Server Port specifies the port number of the Internal SMTP server. When a connection is received on external port 25, OrbitNet forwards the connection to this port number on the machine specified (typically port number 25). Users should configure their e-mail mail servers to use the proxy server as Mail and Post Office hosts. Even though all e-mail transactions take place with another computer outside the firewall, to the e-mail application OrbitNet appears to be the server.

10. REAL AUDIO: SETUP: The RealAudio Setup dialogue lets you configure the port number used by OrbitNet to listen for RealAudio connections—usually port 1090. In some versions, Progressive Networks changed the default port number to 1080, which conflicts with the port number typically used for Socks. We still default to 1090, removing the possibility for conflict. The RealAudio Classic proxy in OrbitNet supports both TCP and UDP (connected and streaming) data stream types.

To configure your RealAudio client machines to use the Classic Proxy:

- Select the Proxy Tab in **Preferences**
- Enter the IP address of the OrbitNet server.
- Enter the port number as 1090.

To configure your Real Audio G2 client to use the Transparent Proxy:

- Go to Options/Preferences/Transport.
- Deselect both “Automatically select best transport” and “Use specific UDP port.”

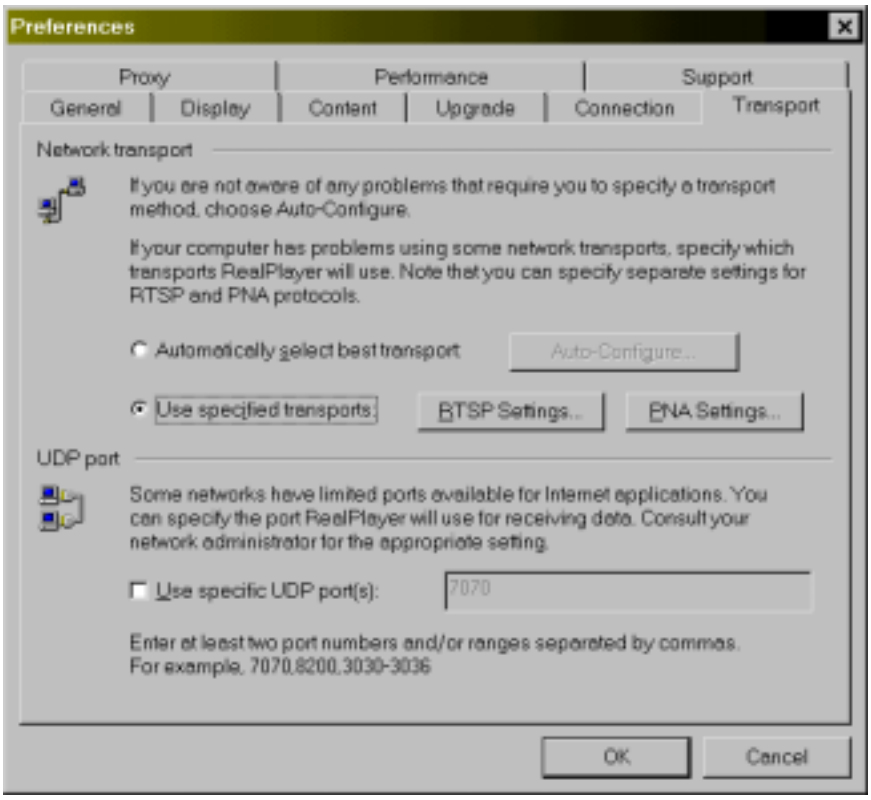


Figure 9-11: The Transport Tab under Preferences.

While you're here, click **RTSP Settings** and select "Attempt to use TCP for all content":

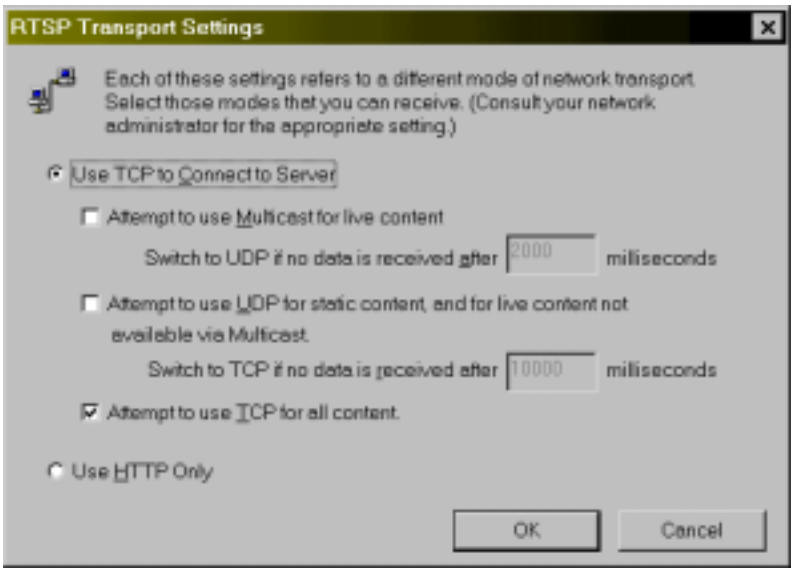


Figure 9-12: RSTP Transport Settings let you establish the modes of RSTP network transport you want to receive.

When you're finished establishing RSTP Transport Settings, go back to the Transport Tab. Choose PNA settings:

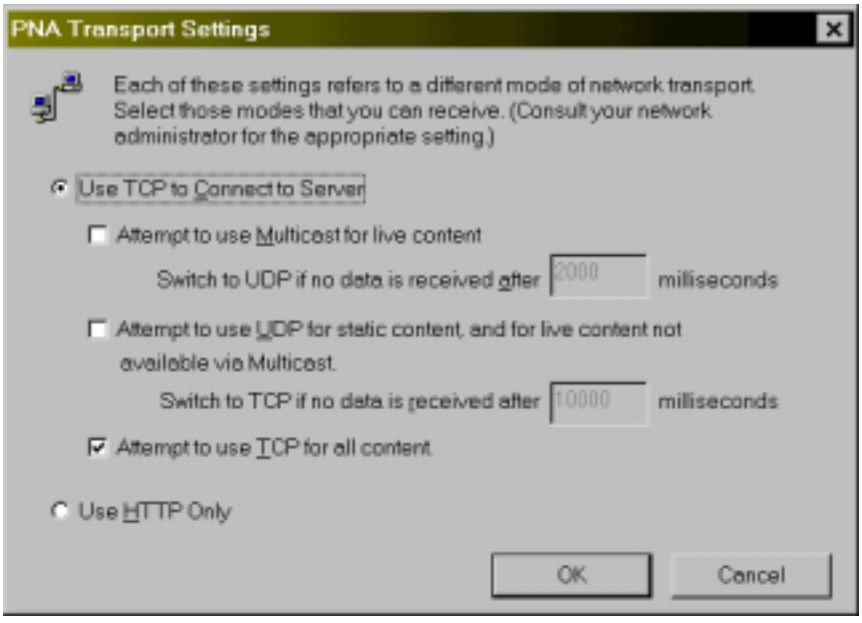


Figure 9-13: PNA Transport Settings let you establish the modes of PNA network transport you want to receive

Finally, select the Proxy Tab. Choose **No HTTP Proxy**. De-select everything else.

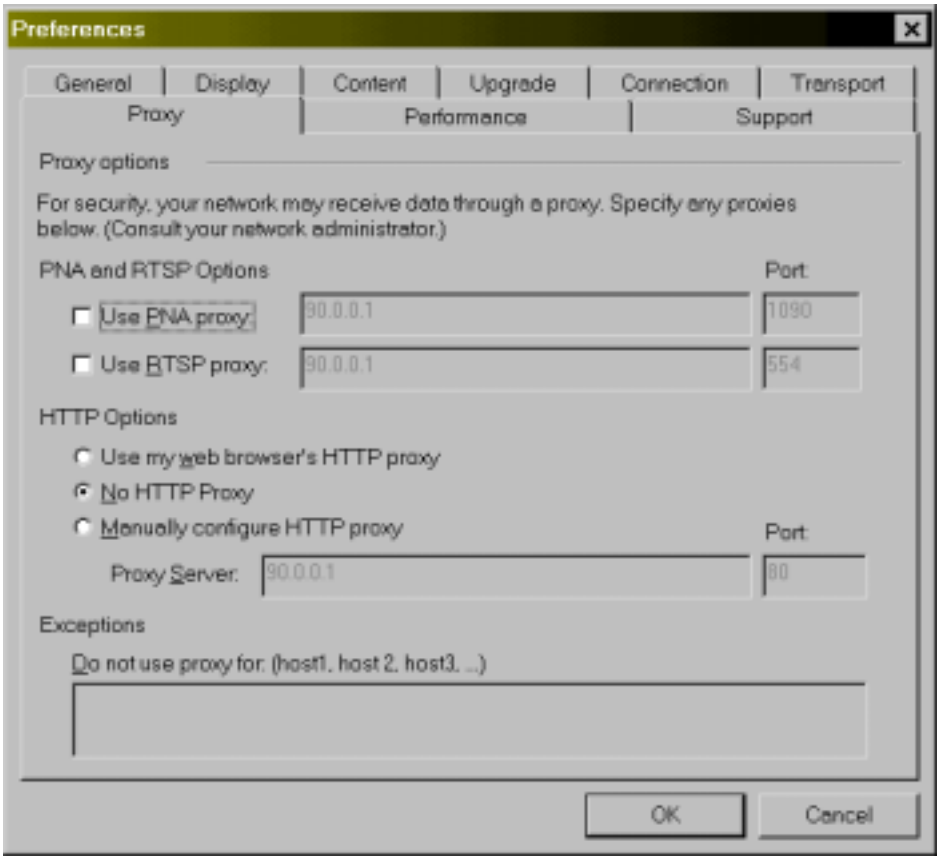


Figure 9-14: "No HTTP Proxy" is the only option selected.

From now on, your Real Audio player will make its connections through OrbitNet's Transparent Proxy. As with any application running through the Transparent Proxy, the network Gateway setting must be set to OrbitNet's internal IP address—and, of course, OrbitNet must have Transparent Proxy or NAT enabled under the Client Access Method Tab.

11. AUTOMATIC NETWORK CONFIGURATION (DHCP)

Dynamic Host Configuration Protocol provides a means for a central computer to assign network addresses and information to individual computers as needed. Enabling this protocol allows OrbitNet to perform as a DHCP server. Most people have used the services of a DHCP server without realizing it. For instance, when you dial into an ISP with a standard modem, the ISP uses a DHCP server to assign your modem a network address from a pre-defined pool of available addresses.

OrbitNet can perform this same function for the computers on your local network. You may have noticed in your network TCP/IP settings that you have the choice of assigning a static IP address yourself, or choosing **Obtain an IP address automatically**. With the latter, that computer broadcasts a DHCP request when its network programs start up; if there is a DHCP server on the network, that server will

respond with settings for the requesting machine. A DHCP server can provide IP address, subnet mask, and gateway address information.

In addition, if you have DNS disabled on that card, then the DHCP server provides DNS settings, including Server Search order, domain name, and host name (that's because, in this case, the disabled setting is more akin to "obtain automatically"). OrbitNet will use a pool of numbers based upon the IP address and subnet mask of the internal network card on the OrbitNet machine. It uses some simple rules to make these assignments:

1. **Lowest first**. The lowest number in the range is assigned first.
2. **Namelist assignments**. You can pre-assign specific numbers to specific machines by using the NameList function (part of the DNS protocol settings). OrbitNet will assign numbers to computers as shown there, and will not give a pre-assigned number away until it must. As an example, if your namelist has the following entries:

    ArthurP 90.0.0.7
    LianaA 90.0.0.8

   Then the "LianaA" computer will be assigned 90.0.0.8 even if OrbitNet hasn't yet reached that number. On the other hand, if those computers are not yet online when OrbitNet reaches those numbers, it will skip them and continue with the next non-pre-assigned number.
3. **Give it if you've got it**. If OrbitNet runs out of numbers to assign, it starts assigning unclaimed NameList numbers, lowest first.

DHCP will also work when OrbitNet is installed on a multi-homed machine (one with more than one internal network connection); each subnet will get the appropriate information assigned.

The only static IP address(es) that you *must have* are the internal network connections on the OrbitNet machine. The remainder of your local machines can get their TCP/IP settings automatically if you wish. It doesn't hurt anything at all to run the OrbitNet DHCP server even when your client machines don't need the service. For most folks, the more relevant question is whether they want their client machines to use the services (you can of course mix-and-match, having some machines with static tcp/ip settings and others receiving settings dynamically from OrbitNet).

Upside to Using the Service	**Downside to Using the Service**
1. It's real, real easy. You don't have to configure any of those myriad tcp/ip thingies.	1. The OrbitNet machine must be on whenever two client machines need to communicate via tcp/ip: (a) File and Printer sharing and network neighbor-hood don't rely on tcp/ip. (b) Windows 98 machines assign themselves default numbers when a DHCP server is not present, so W98 machines could converse anyway.
2. No mistakes. You needn't understand what all those thingies mean. You don't have to trouble-shoot pesky tcp/ip misconfigurations.	2. User restrictions are harder to configure. Actual tcp/ip addresses, which use wildcards, are more flexible if you have to configure many user restrictions. Each computer with a dynamically assigned address must be listed separately by name (although Namelist can be a way around this).
3. What settings? Months from now, when you add another machine, you don't have to remember settings for the other machines.	3. Internal servers (mail, web, or FTP) should have a static IP address assigned.

D. The User's Tab

The User's Tab lets you determine which users have access to the Internet through OrbitNet. Each user is designated by an IP address; a user's access can be restricted by choosing which protocols he or she is allowed to use.

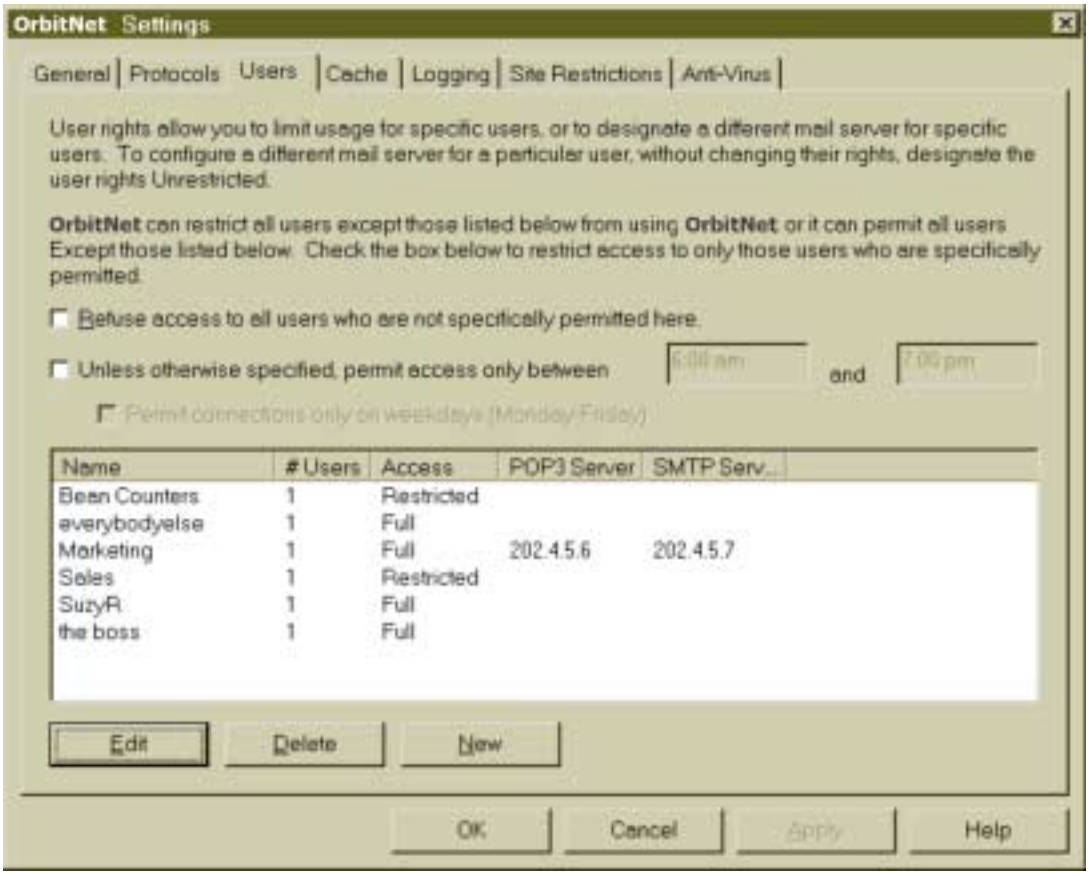


Figure 9-15: The User's Tab under Settings allows you to determine who has access to the Internet through OrbitNet.

When the **Unless otherwise specified, permit access only between** box is checked, all users will be limited to the specified time window. This feature permits those with direct access (such as cable modems or ISDN routers) to restrict Internet access. The other allowed time-window option in OrbitNet applies only to dial-up connections.

For those users with a dial-up connection who enable both time-window restrictions, the rule is: the most restrictive one wins. Or, to put it another way, *both* functions must permit a connection or you can't get out to the Internet.

The weekday only box works the same as it does on the other time options.

There are two ways to administer users in OrbitNet:

1. Allow access to all users unless listed here with restrictions. This method is enabled only when you have *not* checked **restrict access to all users**. This option starts with the premise that everyone on your network is allowed to use the Internet, and then trims back. If you choose to restrict an individual user, add his or her name to the User List with the requisite restrictions. This will not change the ability of other users to access the Internet

2. Restrict access to all users except those listed here. This method permits access only to those users specifically listed in the User List. You must list each individual user in a group. Users not listed will not be allowed Internet access. We recommend that you avoid putting a single IP address in different groups. OrbitNet won't sort out overlapping privileges, and the results are unpredictable.

This restriction applies to both internal and external IP addresses. If you have an incoming connection setup (such as an internal mail or web server), checking this option disables access for all outside users. We show a way around this restriction below.

NOTE

User administration can be done on either a user basis or a group basis. Each entry in this list is essentially a group, which can have up to 500 users. If you don't have many users, you can assign a different group for each user.

The entries in Figure 9-7 shows the users as currently configured, and allows you to make new additions:

- To Add a new user group click **New**
- To Modify an existing group, select the group you wish to modify and click **Edit**
- To Remove an existing group, select the group you wish to modify, and click **Delete**

EDIT USERS DIALOG

When you click **Edit** or **New**, you'll see the **Edit Users Dialog**, which allows you to either (1) enter information required to establish a user group, or (2) modify information about an existing group. A group has a group name, as well as a list of IP addresses in that group. Each group has from 0 to 500 users who can access the Internet under the same rights.

In the example below, every machine in the "Marketing Guys and Gals" group (except ".54," which hasn't yet been added) is allowed to use the web, get mail and news, and utilize Socks and RealAudio. No user is permitted to do FTP or telnet. Since **Use a different Mail Server** is enabled and configured, every machine in this group with mail applications configured to use a proxy uses a different mail and POP server than specified within the OrbitNet Mail Setup. Mail apps which use Transparent proxy are unaffected.

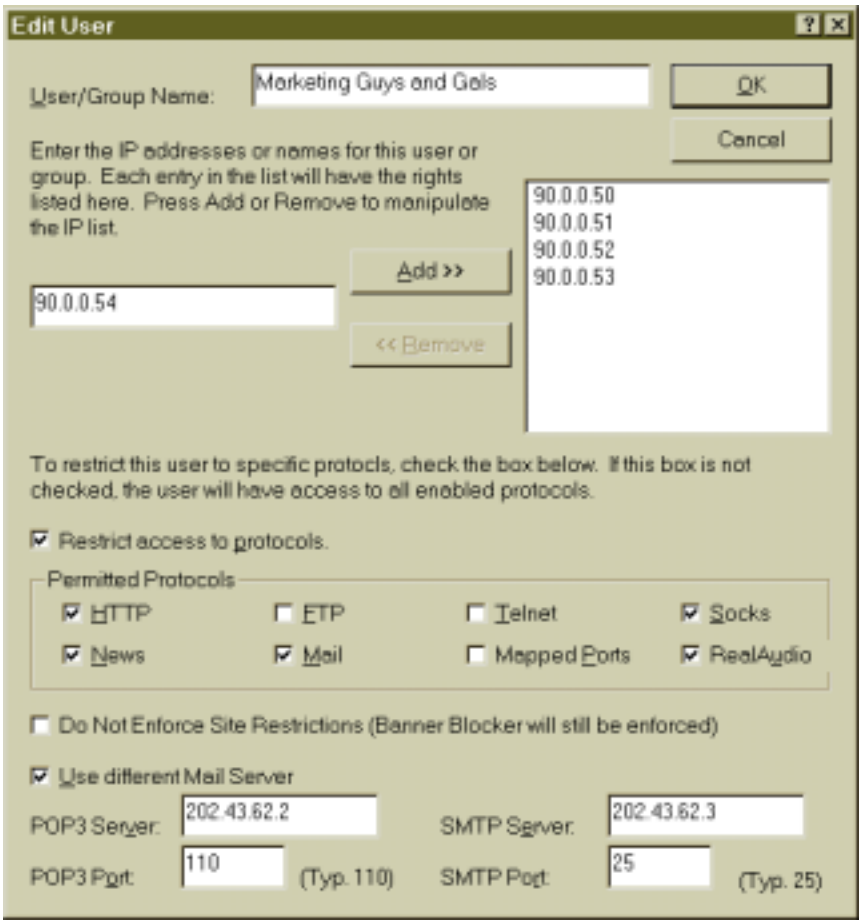


Figure 9-16: As configured here, no user in this group can utilize FTP or Telnet.

The option **Do Not Enforce Site Restrictions** is new to version 3.0. When enabled, no machine in the defined group will have Blacklist, Whitelist, or SmartFilter restrictions enforced.

Network administrators have doubtless noticed the little "gotcha!" in the example above. Since users are allowed to utilize the Socks protocol, they can still do FTP through their browsers (if their browsers are configured for Socks protocol). If Socks is available, browsers use it for many functions. Other options:

User/Group Name: The group name, displayed in the Users Tab under Properties. You can assign any name you like.

IP Address List: Add and remove IP addresses from this list to add/remove users to and from this group. If you add a user who is already in another group, you'll receive a warning message but won't be prevented from making the addition. The results, however, will be unpredictable. You can add up to 500 users to this list. You're not restricted to internal addresses here; if you have some incoming ports already set up—an internal web server or an internal mail server, for example—you can restrict the rights of incoming connections by their IP address.

Restrict Access: Check this box if you want to restrict access for a particular user. When this box is checked, all protocols are enabled; you can then select which protocols to allow. Any protocol not checked will not be permitted from any IP address in the user list.

Use Different Mail Server: Select this item if a particular group requires a different mail server. Although most users can be accommodated with a single mail server, occasions arise where a particular user or group needs access to a different mail server. This is where the address of the POP3 and SMTP server should be entered. All users in this group will be connected to the specified POP3 and SMTP servers. This feature is not supported for IMAP4.

USING WILDCARDS WITH SITE RESTRICTIONS

OrbitNet 3.0 supports use of the ***** wildcard in configuring User-restricted IP addresses. For instance, if everybody on the **90.0.0.x** subnet is part of a group, type in **90.0.0.*** as the IP address for the entire group rather than typing in each individual address.

Larger groupings are legal, as well. For instance, the IP address **192.168.*** applies to any machine whose IP address begins with those numbers. You can carry this to the logical extreme: the IP address ***** is considered a legal address meaning "any possible IP address." Overlaps are possible when using wildcards; the rule is that the most specific designation wins. It doesn't matter in which order you enter the groups and restrictions in the user settings.

With careful forethought you can use the wildcard and internal and external IP addresses to enhance the security of almost any complex setup. An example would be the user or business with an internal mail server. The nature of SMTP decrees that you can't know ahead of time which server on the net will forward mail to your server—but you *do* know that your mail server must allow incoming connections at any time, day or night.

This situation becomes difficult when you want to use the option **refuse access to all users except**. At first glance it seems that you can't restrict access and still allow mail through an incoming port to an internal email server. Here's how to get around that:

1. Enable the option **refuse access to all users except those listed here**.
2. Define a group as "Incoming Mail." Use the IP address (see note, immediately below) to specify the group IP address, and allow that group to use *only* the mail protocol.
3. Define another group by a name such as "Internal Users." Give this group the IP address **90.0.0** (see note, immediately below) and allow it to use any protocol.

Note: Since the more specific **90.0.0** wins, all internal users can do anything, but everybody else—including the incoming connections on port 25—are allowed use of the mail protocol and nothing else. You can, of course, increase the restrictions on your local users or define multiple groups.

E. The Site Restrictions Tab

As its name implies, the Site Restrictions Tab allows you to restrict user access, via a variety of methods, to Internet sites.

A few things to keep in mind when working with this tab:

- You can determine whether or not an individual computer will be subject to Site Restrictions, but you cannot have different sets of restrictions for different computers—each is subject to all restrictions or none at all.
- A good rule of thumb to remember is: "More restrictive wins." In other words, if you enter "playboy.com" in both the Blacklist and the Whitelist (described below), the more restrictive blacklist rule will win—nobody will be able to get to playboy.com.
- New user restriction settings are enforced as soon as you return to OrbitNet's Main Screen.
- When checking out new OrbitNet restrictions with a browser, use the Reload or Refresh button instead of the Back button to ascertain if the new settings are working the way you want. The Back button returns the document from the local browser cache, while Reload returns it from the original site.

SMARTFILTER

SmartFilter uses a list of known URLs to decline access (when access is declined, a message appears in the browser stating the reason why).

OrbitNet has five basic categories of SmartFilter. Each contains a list of sites that have content about that subject. *When you select SmartFilter and choose the option* **Enforce this list**, *access is refused to any site you check in that list (Hatespeech and/or Drugs, for example).*

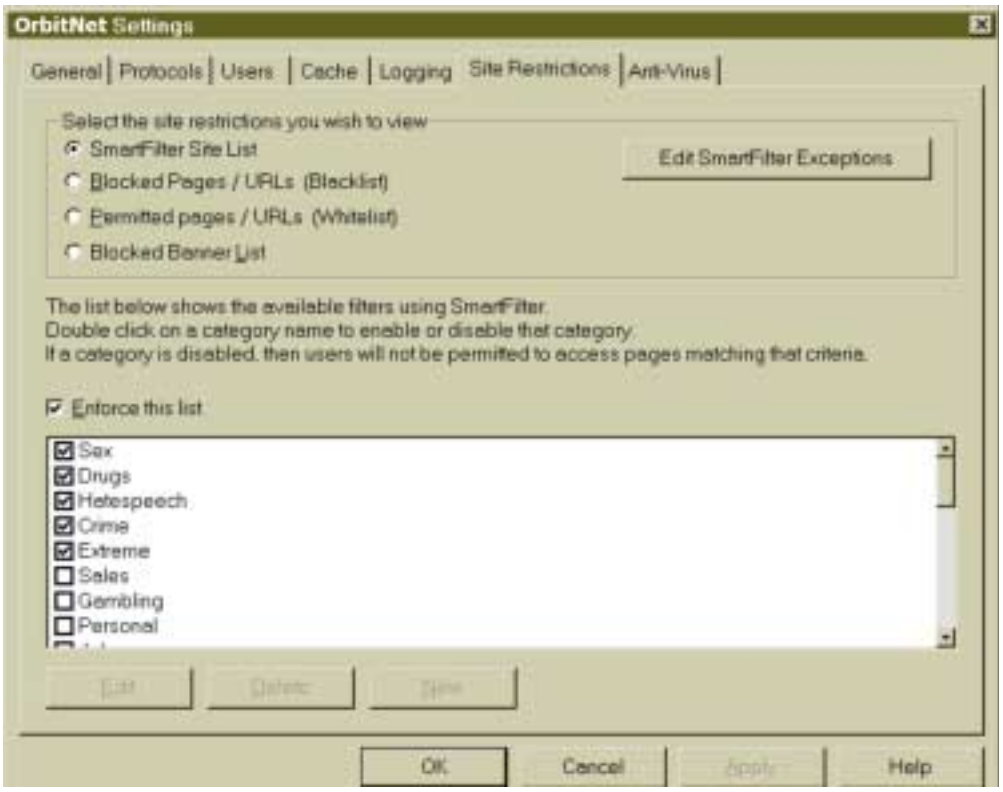


Figure 9-17: The Site Restrictions Tab allows you to place certain limitations on user access. The Site Tab opens to SmartFilter, which allows you to restrict access by site type.

The box to the right, **Edit SmartFilter Exceptions**, provides an access method to individual sites appearing in the list. This allows you to access certain individual sites and block the others. It also allows access to a location which hosts several kinds of sites, one of which appears on a restricted list. If you find that you cannot access a site that seems otherwise innocuous, try listing it here. You also have the option to list individual sites that users will not be permitted to access.

A fully-functioning version of SmartFilter is included in OrbitNet's 30-day trial version. When you purchase the software, Smartfilter will be enabled for six months, including any free updates. SmartFilter works only during the licensed period. Thereafter, licenses must be purchased for additional time periods and upgrades. If the license lapses, you'll no longer be able to use the old filter list for access control. Licenses can be purchased from the OrbitNet website or directly from our offices.

BLACKLISTING

The Blacklisting feature forbids access to selected sites by comparing all requests to previously blacklisted names and IP Addresses. If the host name, IP Address, or an alias is contained in the blacklist the connection is forbidden.

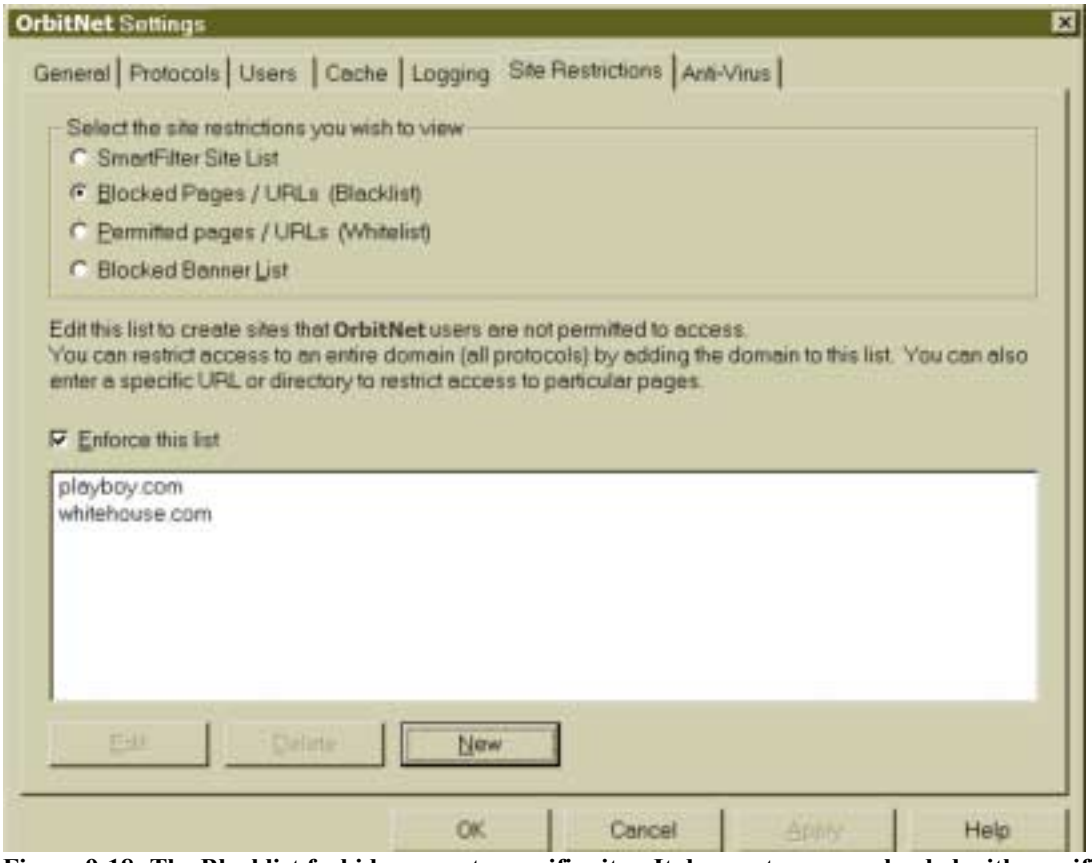


Figure 9-18: The Blacklist forbids access to specific sites. It does not come preloaded with specific settings.

Access to specific Internet servers can be denied. To do so, we recommend using an actual IP Address (see the example below), since aliases are not always reported correctly in Windows TCP/IP stacks. A hacker (or the office hacker wannabe) could use an alias to circumvent the blacklist.

A wild-card character, *, can be used in Blacklist—but carefully! You can use the wild-card character anywhere to the left of the root-level domain (i.e., the com, gov, org, or country designation, the last thing to appear before any following slashes). You cannot use it to *replace* the root-level domain. You can also use the wild-card character to the right of the root-level domain.

In the string **www.Orbitsat.com/resellers**, for instance, you could use the wild-card in place of the **www** or in place of **www.OrbitSat**, but nowhere else. If you used ***.com** as a blacklist entry, access would

be denied to *any* site with a **.com** root-level domain. As a special case, if you simply use * as a blacklist entry, nobody could get anywhere.

Also, you should be aware that words to the left of the root-level domain are not case-sensitive, but words to the right *are* case sensitive. If in doubt about capitalization, make two entries—one spelled each way—just in case.

WHITELISTING

The Whitelist comes at things from another direction. When it's enforced, your users get only the sites listed and no others. Sites or rules are listed in the same manner as in Blacklist. If you listed ***.gov** and ***.net** and ***.org**, for instance, then the users can get to those places but not to any place with a **.com** or an **.edu**. The Whitelist can be powerfully limiting.

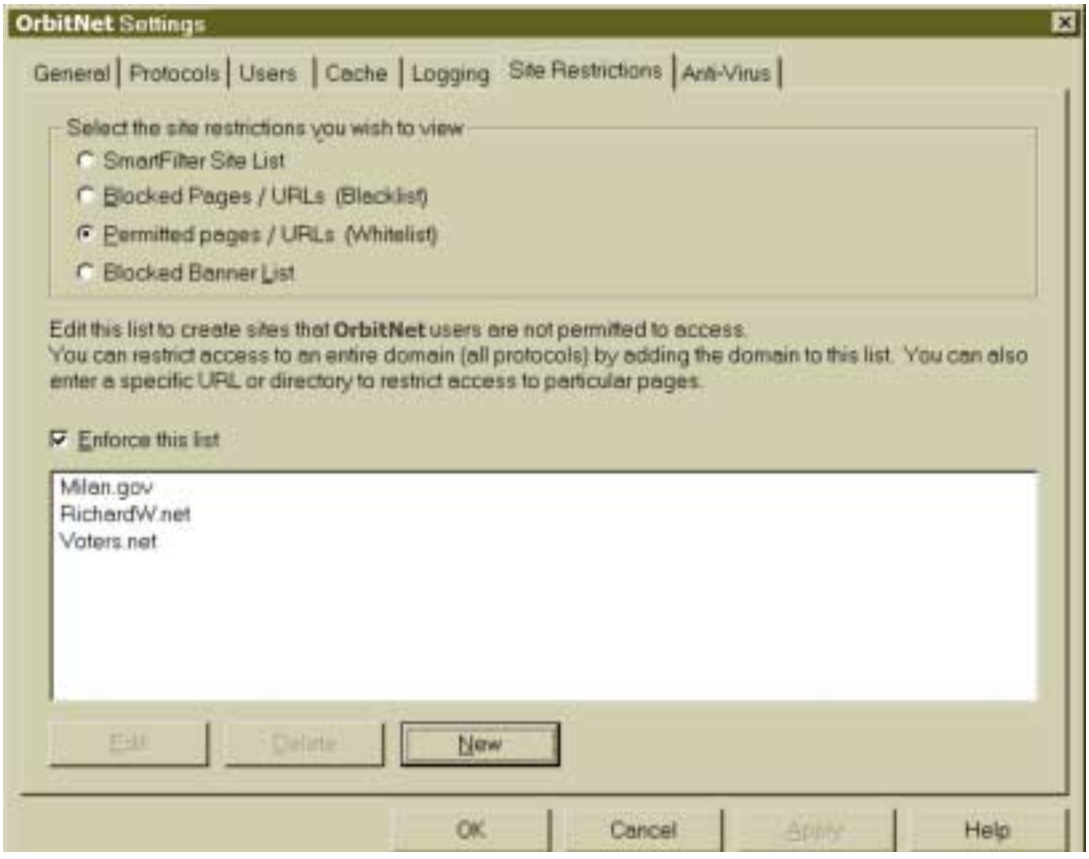


Figure 9-19: Whitelist allows access to specifically-listed sites. It does not come pre-loaded with specific settings.

BANNERBLOCKER

BannerBlocker is another restriction—but with a twist. It doesn't prevent access to any specific site, but is intended to remove the majority of banner ads. It relies on the fact that most of these ads actually

come from a different server than the rest of the page (Each www page is composed of many files, including text files, html files, picture files, and sometimes ads).

When a requested file is listed in BannerBlocker, OrbitNet will not download that file. It replaces the file with a transparent image. In most cases users are unaware that a banner was ever there. In a very few cases a blank box is left.

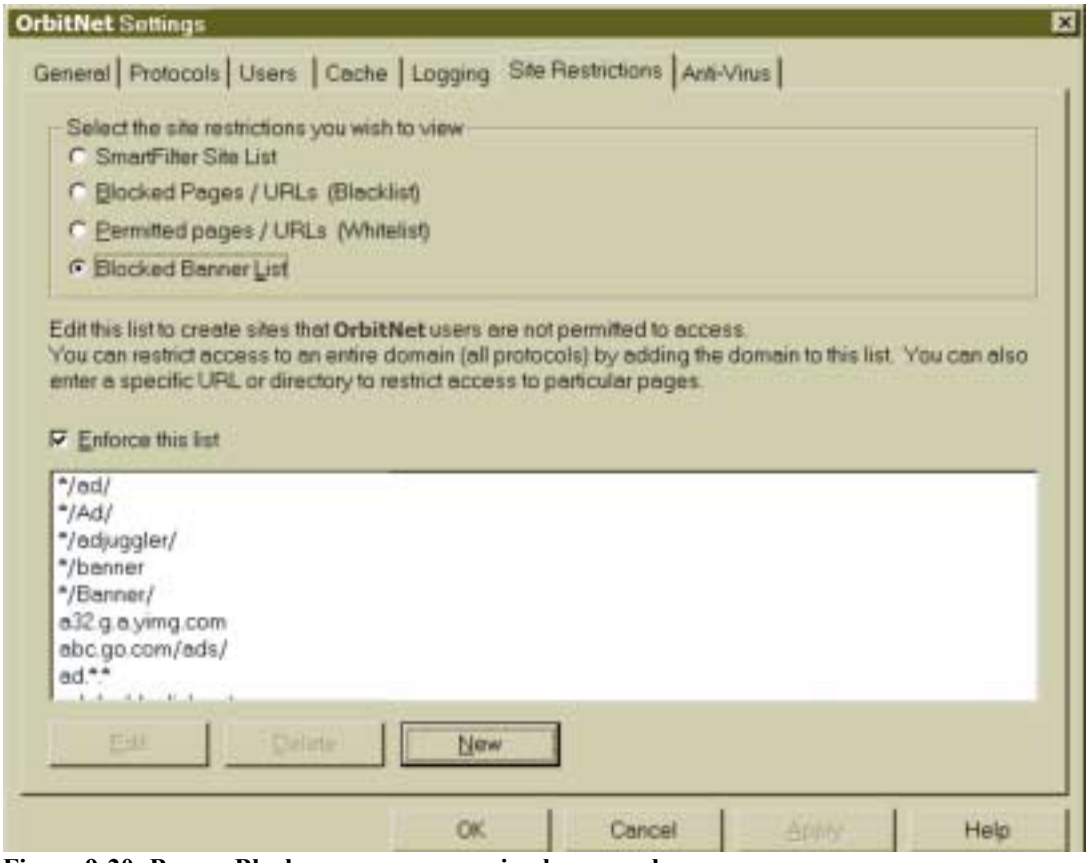


Figure 9-20: BannerBlocker removes annoying banner ads.

BannerBlocker itself doesn't know if the declined file is an ad or something else. Indeed, if you listed **intel.com** in the BannerBlocker list, anybody who tried to access the Intel site would get a blank page and a **document done** message from the browser. (It's only funny the first time.)

If you'd like to add ad servers (or other servers) to your BannerBlocker list, it's easiest to do so with an IE browser. Right-click on the offending ad, then click on **properties**. IE will show you the URL for that file. If it can be distinguished in some way from the rest of the site, you can add your entry to your BannerBlocker list.

F. The Cache Tab

The cache is a directory on your hard disk used by OrbitNet to store web documents. You are not required to have a cache, but caching can speed up access times by returning documents locally rather than from a distant server. Caching also reduces the data load on your Internet connection, which is typically the bottleneck for Internet access.

When a browser requests a document, OrbitNet can check to see, without requesting the entire file, if the server has a newer version of the requested files than those already stored in the cache. If the document has not been modified, the server returns a message stating that the document is unchanged. OrbitNet then sends the cached copy of the document to the browser. You can alter the configuration so that OrbitNet returns the cached copy to the browser without checking its validity.

Disk Space and Ram. If you enable the caching feature, be sure you have plenty of disk space to hold the amount of cache specified. Though the primary cache storage is on the hard disk, some system RAM is also required for cache administration. As a rule of thumb, plan on 1 Meg of RAM beyond normal system requirements for every forty Megs of disk cache specified.

HTTP Documents. The cache is used to store only HTTP documents like web pages and pictures. It won't store FTP files, mail, news groups, or anything retrieved with a secure connection. Documents responding to a query—like those generated using a search engine—are not cached. When using AOL as a provider, anything accessed by AOL software will not be cached (however, web pages accessed with other browsers will be cached).

Most browsers have their own cache; they may save documents that OrbitNet won't or may have their own copy of a cached document. When a user clicks her browser's Reload or Refresh button, OrbitNet always returns the document from the distant server rather than its local cache.

Documents have defined standard HTTP caching extensions; these are sent to the proxy server and browser as part of the document header and are meant to modify caching behavior. Among these extensions are information on the document type and length, whether the document should be cached, and when it should be considered obsolete.

OrbitNet won't place documents into the cache if the web server has instructed it not to do so, and it won't cache documents not reporting content length. It won't automatically download newer versions of these files without user intervention; it uses these rules to determine how to retrieve documents *as they are requested* by the user's application.

System Clock. OrbitNet's ability to accurately verify documents depends on the accuracy of the system clock. If the time on the OrbitNet computer is incorrect, or if the time-zone is incorrectly configured, OrbitNet won't be able to properly request modified documents. The Internet uses Universal Time (Greenwich Time) as the standard time for all Internet documents and communication. If the time, time-zone, or date is not correctly set on the OrbitNet computer, OrbitNet calculates the time incorrectly and your document caching malfunctions.

Viewing Cache Contents. If you want to view the contents of the OrbitNet cache, or statistics on its usage, request the document **http://Proxy.Command/** using a browser on any client machine (If configured to require a password, OrbitNet asks for one). You will have three options: **View Cache Statistics**, **Browse Cached Files** or **Delete The Files From The Cache**. This is the only way to view cache statistics.

NOTE

DNS cache functions are also available under proxy.command. Be aware that they'll specifically say "DNS cache"—if the option says just "cache," it refers to the web documents cache.

Other options also available on the Cache Tab under Settings:

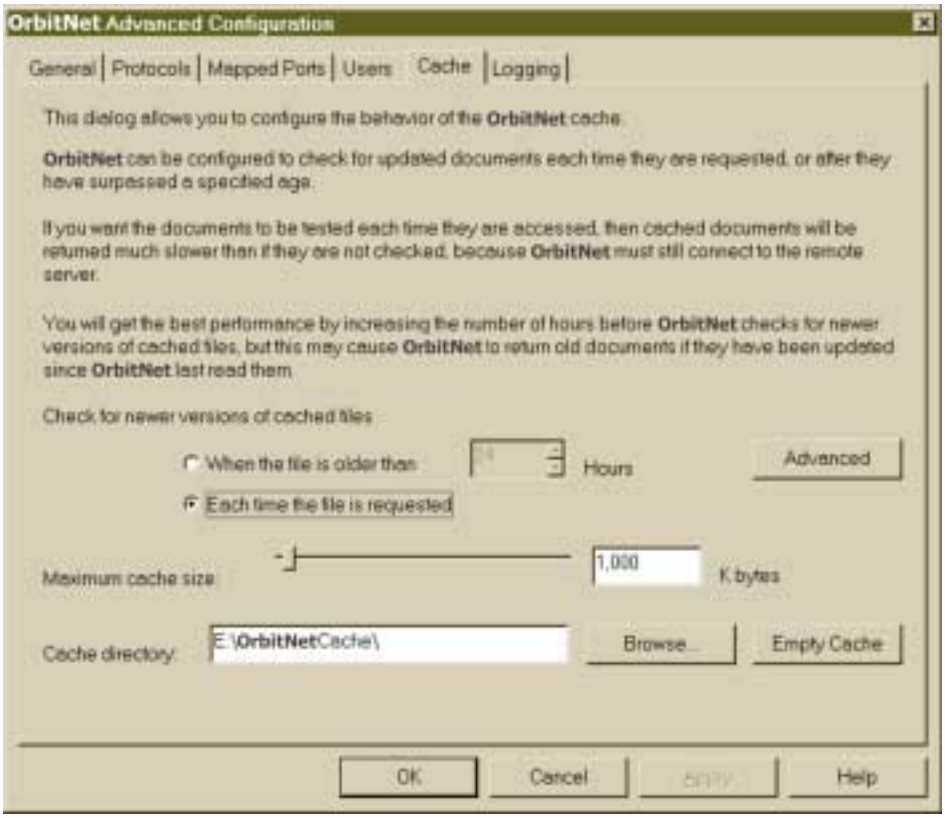


Figure 9-21: A generous number of options are available for configuring cache.

Check for newer versions of cached files. This determines how often OrbitNet checks for modified files before supplying the requested file to a browser. If **Each time the file is requested** is selected, OrbitNet verifies all documents each time they are requested by a browser. This can significantly slow down access to Internet files, but it guarantees that you always get the most current file. If **When the file is older than XX hours** is selected, OrbitNet only checks for newer files when files are older than the specified time. This value is typically set to 12 or 24 hours, so that documents are verified once a day. This is a good setting, as the majority of web sites are unlikely to change often. However, the value can be set for a time range of one hour to one week.

If a user hits the **Reload** or **Refresh** button, OrbitNet always retrieves the page from the Internet server, overriding any settings here.

Maximum Cache Size: The slider and edit box allow you to configure cache size. The number displayed in the edit box represents a byte size in kilobytes (1024 bytes) . For instance, if you set the size to 100,000 KB, then your cache will be 100 Megabytes large. It's usually impractical to make your cache larger than 100 megabytes, because a large cache reduces system performance. If your cache is too small, however, you may not have enough space to fully optimize usage. Optimal cache size varies widely depending upon a user's needs, but a good starting place would be to allocate five to ten megs for each of your first five users, and a couple of megs for each additional user. If you find that these amounts are too little or too great, you can easily change them later.

Cache Directory: This allows you to change the location of the OrbitNet cache. You can type in the new location or press the browse button to find a directory to use for the cache. Remember: if you change the cache location before emptying the cache, you'll need to delete the old cache file directory yourself. You can empty the cache named here by pressing **Empty Cache**. When you hit "empty cache," give it several minutes to complete. It's deliberately set as a low-level priority, and its got a lot of housekeeping to do as it clears out the cache.

ADVANCED CACHE

The advanced cache options allow you to have a finer degree of control over caching. You can specify the rule to be used for individual sites; for instance you can designate that a specific site be checked for newer files each time, while other sites are only checked once a day

Figure 9-22: With advanced cache, you can configure the way in which specific sites are handled by OrbitNet's Web cache.

As in general caching, this doesn't mean that OrbitNet downloads a newer file without being requested. Rather, OrbitNet uses a rule table to determine when to verify the "freshness" of documents on specific sites. If ever rules for all sites overlap rules for a specific site, the rule for the specific site will win.

G. The Logging Tab

OrbitNet provides the ability to log all network activity passing through it. There are two types of logs, the Activity Log and the Detailed Log.

The Activity Log is a sequential text log. Designed for a human-readable report of OrbitNet activity as it happens, it's better suited for trouble-shooting than is the machine-readable detailed log (which is better suited for third-party applications which produce activity summaries).

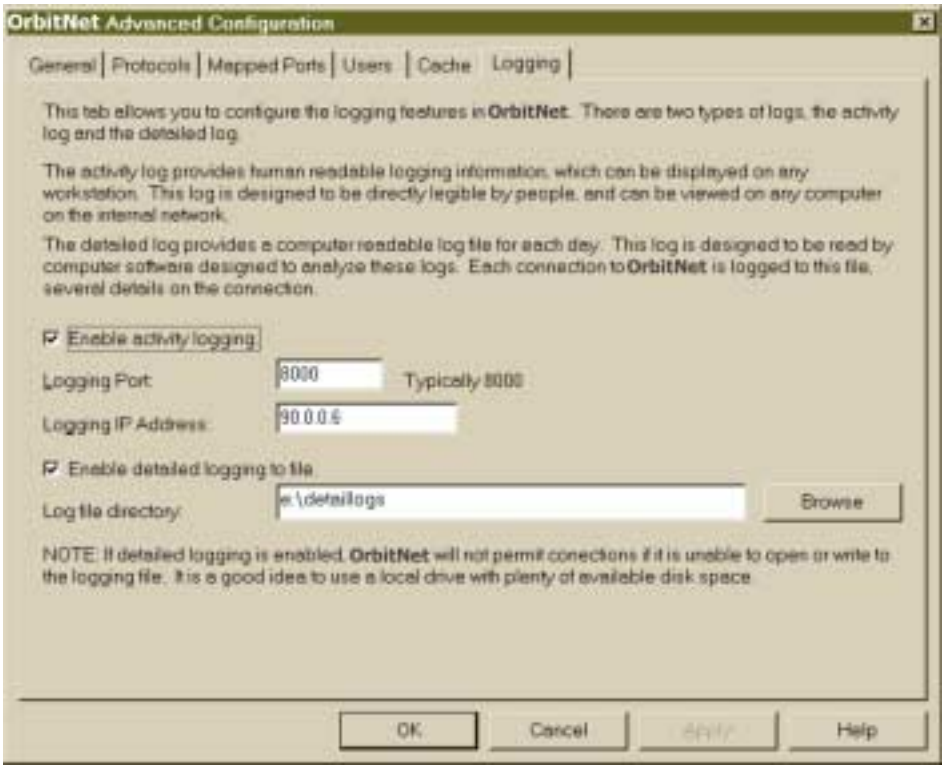


Figure 9-23: The Logging Tab allows you to maintain logs of connection activity.

A sample activity logging application, ProxyLog.exe, is included with OrbitNet, along with its source code. You're welcome to modify this source code for your own use, though not to distribute or sell such modifications. ProxyLog is written as a Windows 95/98/NT console application (i.e., it runs in a DOS box) and it outputs all logging information directly to the screen. If the **log to a file** switch is selected, it writes to both screen and file. To see the command line switches, type in **proxylog/?**. This application listens on port 8000 for a connection unless you specify otherwise on the command line.

Proxylog can be started at any time. Soon after proxylog starts, OrbitNet connects to it and begins sending log information. Proxylog is strictly a passive "listening" application. It won't send information back to OrbitNet, and OrbitNet won't listen for any such information.

The Detailed Log is designed to be readable by applications such as WebTrends Professional Suite (the version with a "proxy analysis" function). It contains information such as which computer was connected to the Internet and which sites were visited for how long.

TAB OPTIONS

A. Enable Activity Logging: When this option is enabled, OrbitNet sends activity log information to the designated port and IP address. The listening application can be run anywhere on the network. All HTTP requests and commands, FTP requests, Telnet and other protocol connections, Dialing requests, and error messages are logged, together with the date and time of occurrence. If OrbitNet is unable to connect to a logging application, it continues to function with logging disabled.

Logging IP: This parameter tells OrbitNet the location of a logging application. This application can be located anywhere on the network, including the OrbitNet machine itself. Although it's possible to send logging information outside your local network, it's a significant security risk. As such, we strongly discourage doing so. The default IP setting for this box is the loopback address, 127.0.0.1. We recommend changing it to do logging from one of your client computers—or, at the least, changing the IP address to the OrbitNet internal IP address (rather than the loopback address).

Logging Port: Along with the logging IP, this parameter tells OrbitNet where to send activity logging information. The default value of port 8000 is also the default port used by the sample logging application. If this value is left blank or is invalid logging is disabled.

B. Enable Detailed Logging: The detailed log provides a log file in comma delimited format for each day. This log is designed to be read by software which does statistical reporting on proxy servers. Each connection through OrbitNet is logged, as well as all connection information. These files can become quite lengthy. You must ensure that you have enough room for these logs; if this option is enabled and OrbitNet is unable to write to the detailed log file for any reason, access to the Internet is shut down.

Log File Directory: Specify the directory where daily log files are stored. Note: If detailed logging is enabled, OrbitNet won't permit connections to the Internet if it's unable to open or write to the logging file.

Delete old logs after: OrbitNet can be set to automatically delete older detail logs. These files can get quite large, taking up lots of disk space. The default setting is 31 days.

H. Anti-Virus

Anti-Virus can scan incoming http (web) documents, ftp downloads, email and email attachments for viruses.

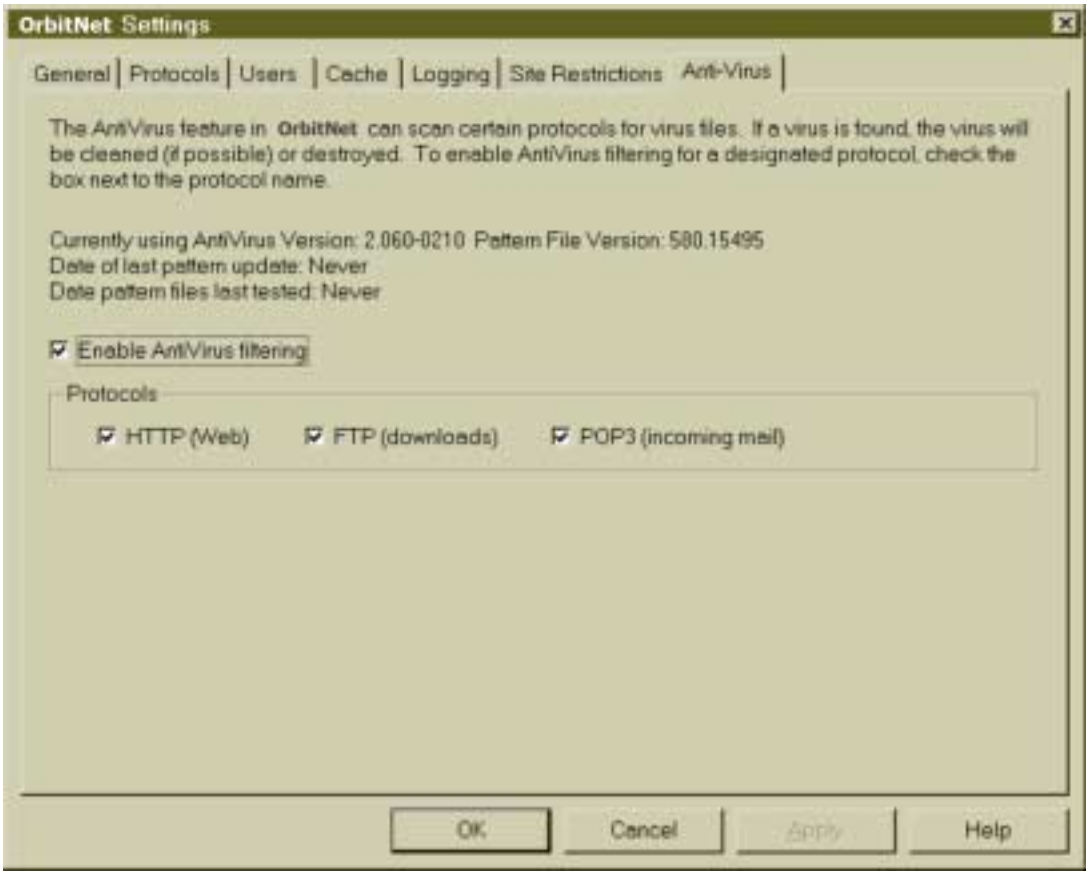


Figure 9-24: Anti-virus protects your network from invasion by infections outside the firewall.

Anti-Virus will work only on those connections visible in ConnectionView. In other words, connections made through the NAT will *not* be scanned by Anti-Virus. Classic or Transparent Proxy connections, each visible in the main OrbitNet window, will be scanned.

You can enable scanning for the supported protocols on the Anti-Virus page. Once enabled, scanning works for all client computers connecting through OrbitNet; you cannot exempt any machines. To ensure that scanning works for applications on the OrbitNet machine itself, we recommend that you set up those applications to use Classic Proxy whenever possible.

When a virus is found within an http document, the download will fail. Users trying to reach the site again will instead receive a OrbitNet browser document explaining that a virus was found in one of the files.

Email and email attachments are scanned completely before being passed on to the email program. If you have large attachments on a slow connection, users will notice that the "working" icon on the mail program spins endlessly; nothing seems to be happening—until the email is passed on all at once. If a virus is found, the infected email or attachment is discarded. Text explaining that a virus was found is added to the email message.

When doing ftp downloads using an ftp program (instead of a browser), the download appears to work fine for most of the file—but will then fail with several KB of the file undelivered. No other indication will be visible within the ftp program.

A fully-functioning version of Anti-Virus is included in OrbitNet's 30-day trial version. When you purchase the software, Anti-Virus will be enabled for six months. During this period, OrbitNet will download anti-virus pattern files once a week as a background operation. Anti-Virus works only during the licensed period. Thereafter, licenses must be purchased for additional time periods and upgrades. If the license lapses, you'll no longer be able to use the old filter list for access control. Licenses can be purchased from the OrbitNet website or directly from our offices.

If you've download a trial version of OrbitNet, anti-virus works for the entire 30-day trial period. When the software is purchased, anti-virus is immediately enabled for six months. During this period, OrbitNet will download the anti-virus pattern files once a week as a background operation. To extend anti-virus operation beyond this period, you'll need to purchase extensions from our website or from our office. Extensions are available in one- and two-year increments, priced according to the user-version you have purchased (i.e., 3, 5, 10, 25 or an unlimited number of users).

Chapter 10

Advanced Settings

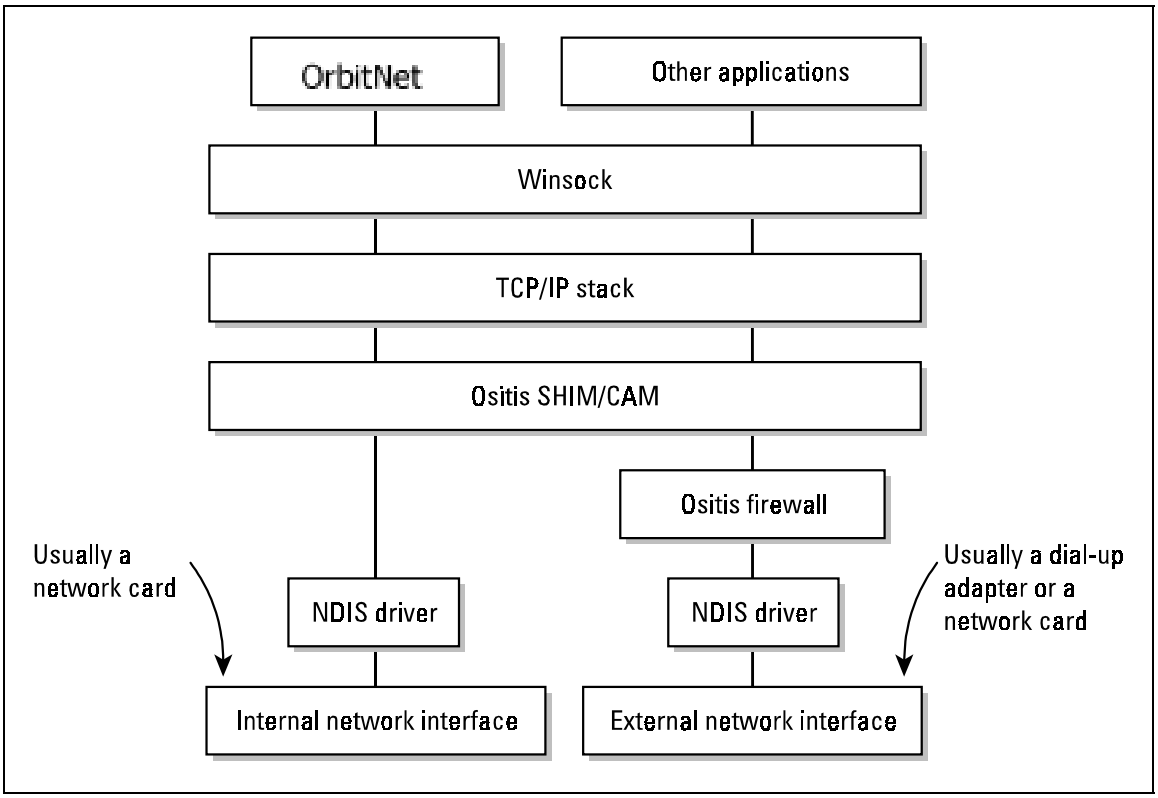
CHAPTER 10: ADVANCED SETTINGS

Overview

Advanced Settings is a new menu item in OrbitNet 3.0. Intended for the experienced and knowledgeable networker, it allows unsurpassed control of OrbitNet's features and settings. Among the features:

- Client Access Method
- Firewall
- Mapped Ports
- Advanced Firewall Settings

We'll begin our discussion by taking a look at the way OrbitNet 3.0 works in your computer:


OrbitNet
Other applications
Winsock
TCP/IP stack
Ositis SHIM/CAM
Ositis firewall
Usually a network card
NDIS driver
NDIS driver
Usually a dial-up adapter or a network card
Internal network interface
External network interface

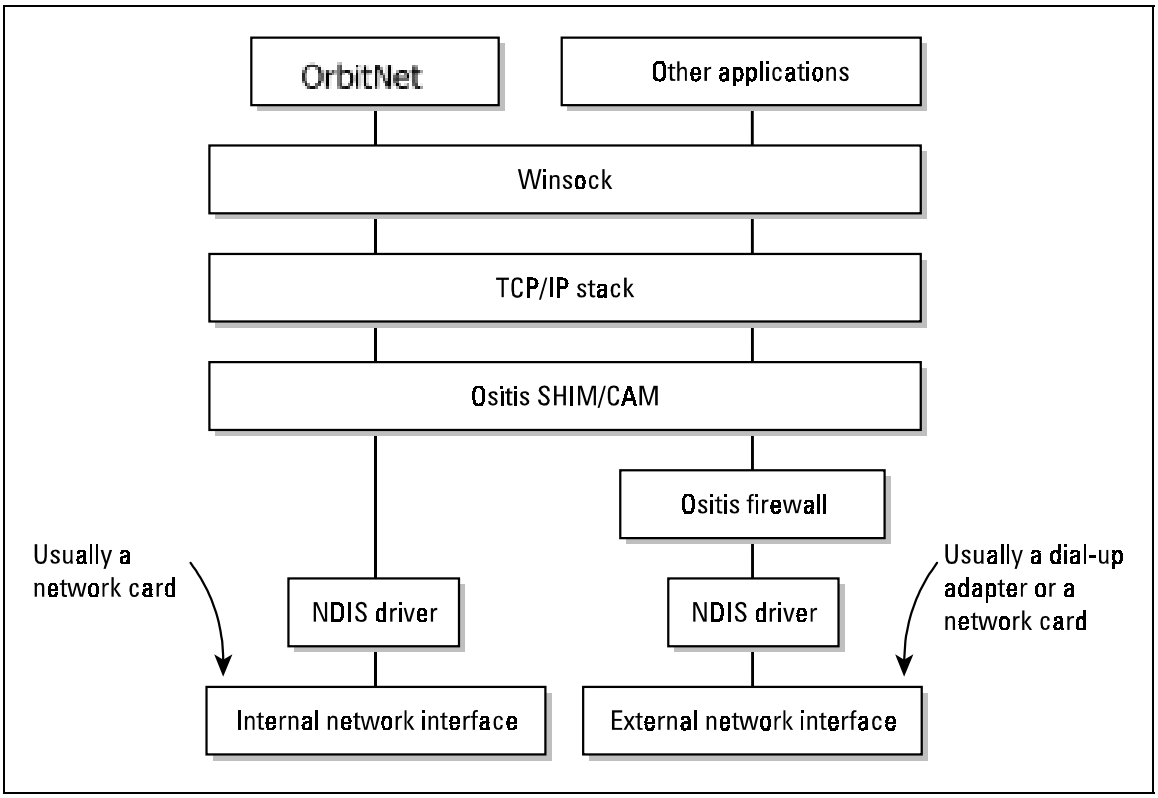


Figure 10-1: How OrbitNet Works

To give you some perspective, all of OrbitNet 2.1—a Classic Proxy—could fit within the functional box labeled "OrbitNet." The new features in version 3.0 are mostly within the functional boxes labeled "Oribit SHIM/CAM" and "Orbit Communication Corp. Firewall."

OrbitNet 2.1 worked entirely at the application (user) level, with the same access to Winsock and the TCP/IP stack as any other application. Version 3.0 works at both the application level and at a level below the tcp/ip stack. Both levels can communicate with each other to provide you maximum flexibility and a peerless firewall.

User settings for these "lower levels" affect OrbitNet in two ways: (1) how it interacts with the applications on your client machines, and (2) how it interacts on the Internet connection.

A. CLIENT ACCESS METHOD

The settings on this Tab affect how OrbitNet interacts with your client applications and the amount of control you have over those connections. A trade-off exists between ease of client application configuration and the amount of control a OrbitNet administrator has over Internet access.

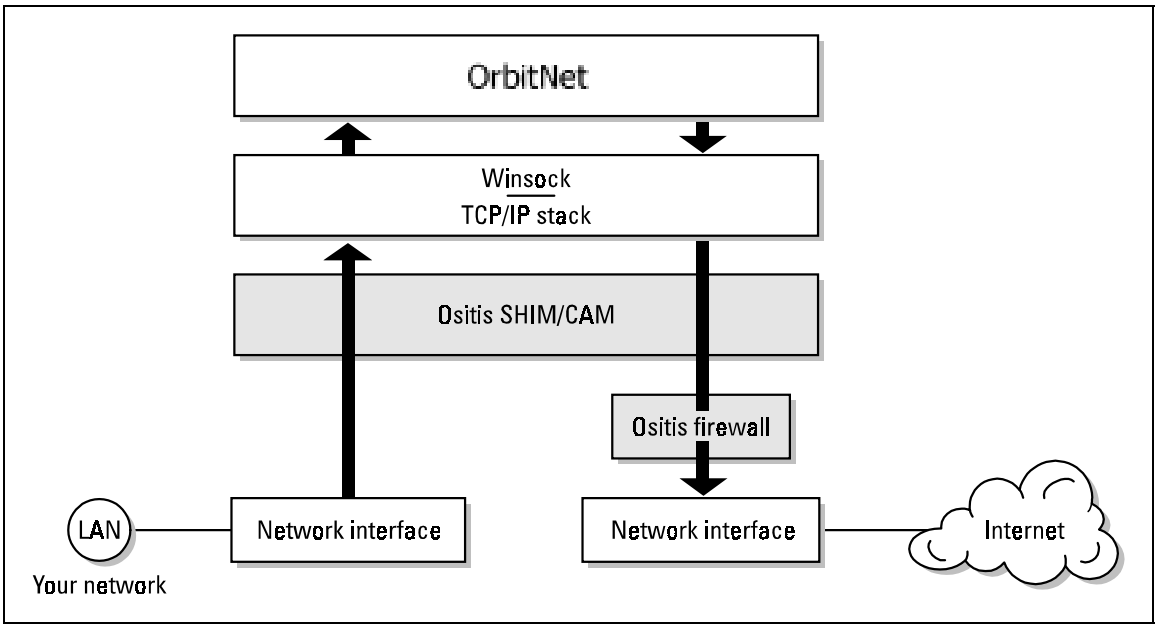


Figure 10-2: Classic proxy path. Choosing Classic Proxy Only disables the lower-level functions of OrbitNet 3.0

The Classic Proxy Only Setting. The least transparent setting is the Classic Proxy Only setting (NAT and Transparent Proxy are disabled), in which each and every application must be specifically configured to run through a proxy. When this setting is chosen, OrbitNet 3.0 works exactly as OrbitNet 2.1 did—no more, no less.

Classic Proxy provides the *maximum control* over user access to the Internet (e.g., you can set things so that clients access only mail servers designated by you). This setting is appropriate for schools, churches, businesses or anybody who wants to control site access. All that's required is the willingness to spend time on occasional administrative duties.

When choosing the Classic Proxy position on the slider, you disable the lower-level functions in OrbitNet. You'll retain the application-level firewall (the same firewall as OrbitNet 2.1), but not the system-level firewall provided by the 3.0 drivers.

The Classic Proxy is included as a subset of other access methods, thus offering its connectivity as well as the system-level firewall available with the other settings.

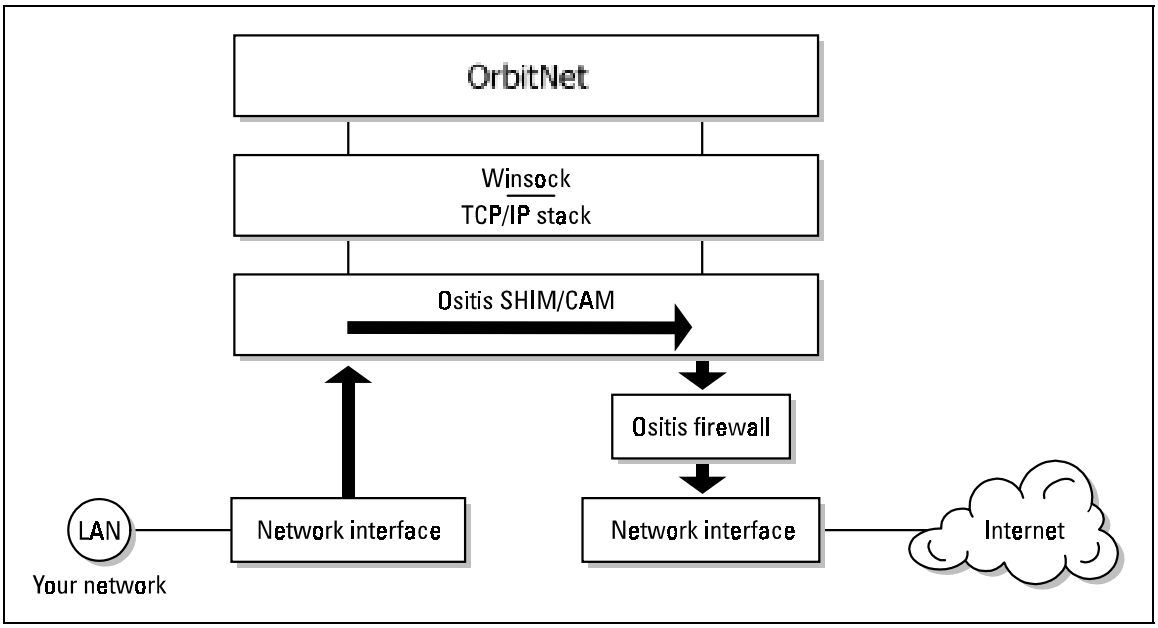


Figure 10-3: NAT path connections pass through the nether regions. You'll never see evidence of them at the user level.

The Network Address Translation Setting. The setting providing the least control over user access, NAT enables lower-level drivers but does not pass the connections through the OrbitNet application level. Client Applications are then allowed to access the Internet through the NAT.

With NAT, Internet applications configured to use a proxy are shown in ConnectionView when active, and are subject to all of the restrictions and control available in the OrbitNet interface. Unlike the Classic Proxy Only setting, however, the external driver-level firewall is active; proxy access through the firewall is regulated by the firewall settings.

Internet applications not configured to use a proxy go through the NAT. The connections are not visible in ConnectionView, and are not subject to any of the restrictions and control otherwise available in the OrbitNet program. The application-level of OrbitNet won't be aware of these connections, which means that you can't see them, log them, or regulate them.

For client machines to access the Internet through NAT, they must have the OrbitNet IP address listed in their Network Gateway setting.

A Note for Dial-Up Users:
Connections made through the NAT will *not* be seen by OrbitNet's inactivity timer, making it possible for the inactivity timer to cut you off in mid-download. We recommend that Dial-Up users leave their Client Access Method at the default Transparent Proxy setting instead of switching to the NAT setting.

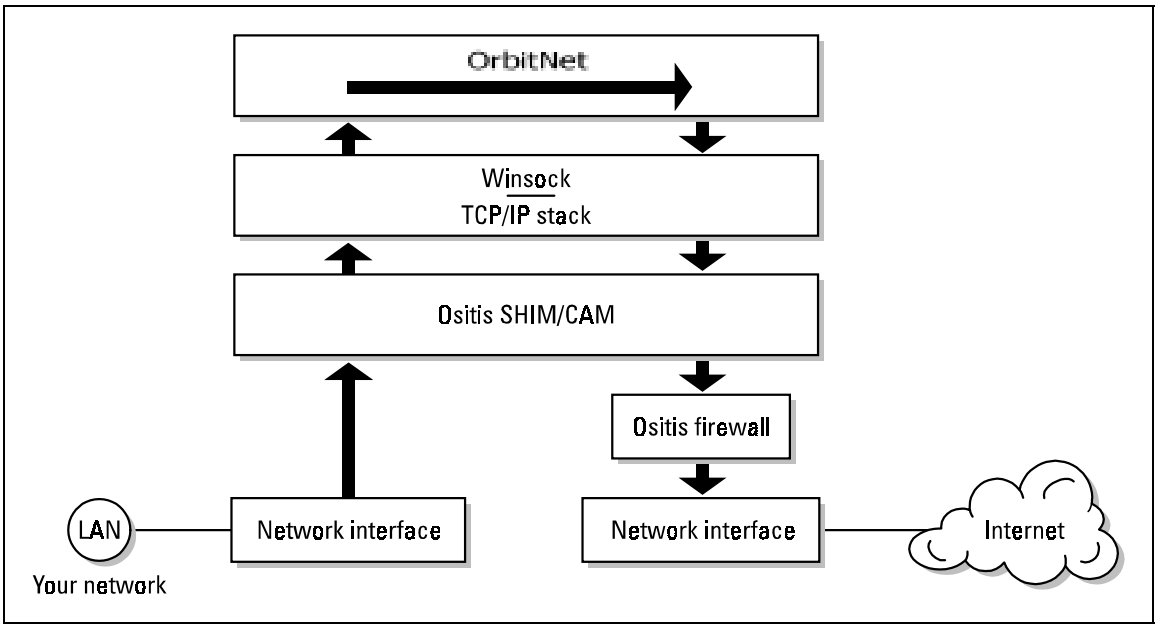


Figure 10-4: Transparent Proxy path. Transparent Proxy connections utilize lower-level drivers, passing through the application level interface where you can see them.

The Transparent Proxy Setting. Having control over the different levels allows OrbitNet a choice of connection paths. If the connection is handled entirely at lower levels, then the operation is entirely by NAT and will be invisible at the user level.

The other choice: doing Network Address Translation down in the gutty-wuts, but passing the connection through the application level where you can see it, log it, and control it. This method, known as a Transparent Proxy, allows an ideal combination of ease of use and potential control.

There are two variations of Transparent Proxy provided: The first is Transparent Proxy for Web (HTTP), FTP and Mail only. NAT connections using any of these three protocols are routed through the application level where they can take advantage of caching (for HTTP), Anti-Virus scanning (all three), and all other OrbitNet functions. Anti-Virus scanning is specifically for these three protocols—a major reason for providing this as a choice under Transparent Proxy. All other NAT connections go straight through the NAT, and are not visible to OrbitNet at the user level. A slight speed advantage may be gained by having these other connections run only through the NAT.

The second variation of the Transparent Proxy is the one most users will find amenable. This choice is to send all NAT connections through OrbitNet's application (user) level, where they can be seen and controlled (if necessary). This is the default setting: "Transparent Proxy – all connections." As you view the connections in OrbitNet, you'll see little visible difference between Classic Proxy and Transparent Proxy connections; that's why we provide you with some clues such as using httn for Transparent proxy connection reports, and adding "Transparent Proxy" at the end of connection lines for other protocols.

When this setting is chosen, any applications configured to use a Proxy connect through the OrbitNet Classic Proxy. Applications configured to use a network (but not a proxy) connect through the OrbitNet Transparent Proxy.

B. FIREWALL AND FILTERING

The Firewall Tab, which gives you control over the ports allowed on your external connection, greatly enhances OrbitNet's security capabilities.

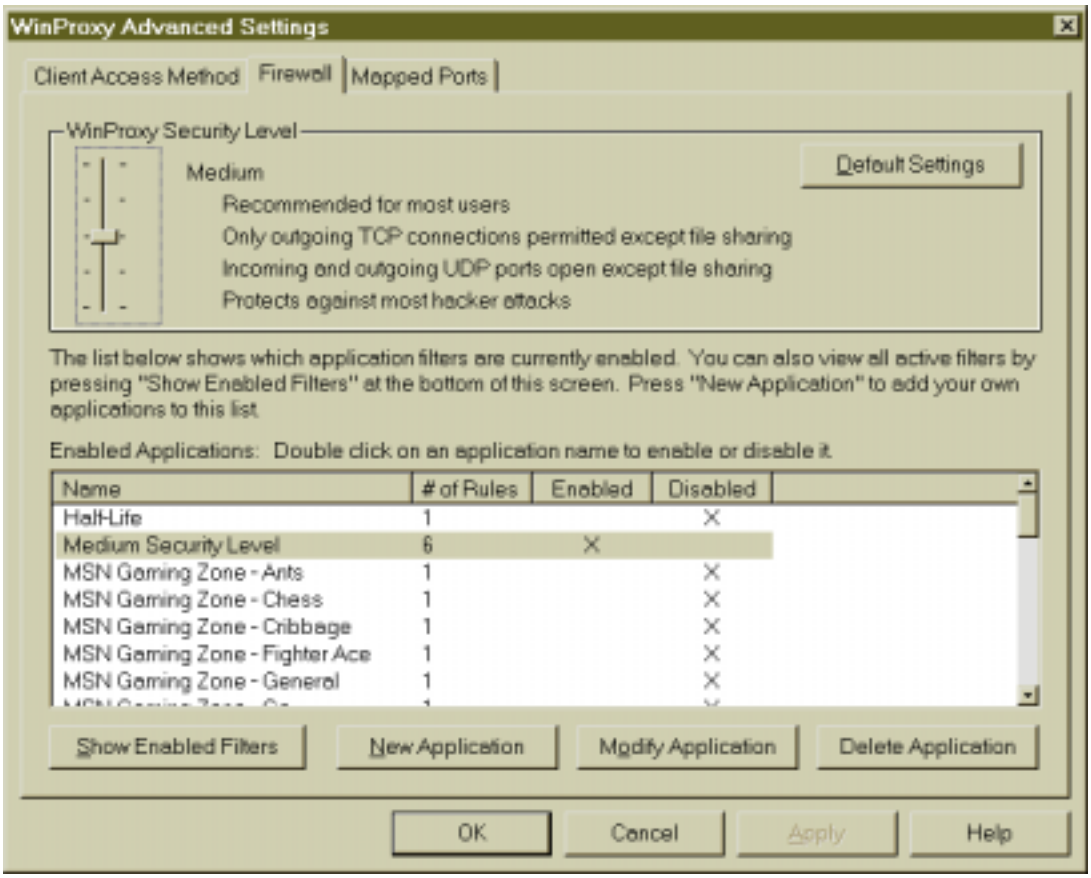


Figure 10-5: The Firewall Tab greatly enhances your network's security by giving you control over external ports.

The following diagram illustrates how the firewall fits into OrbitNet:

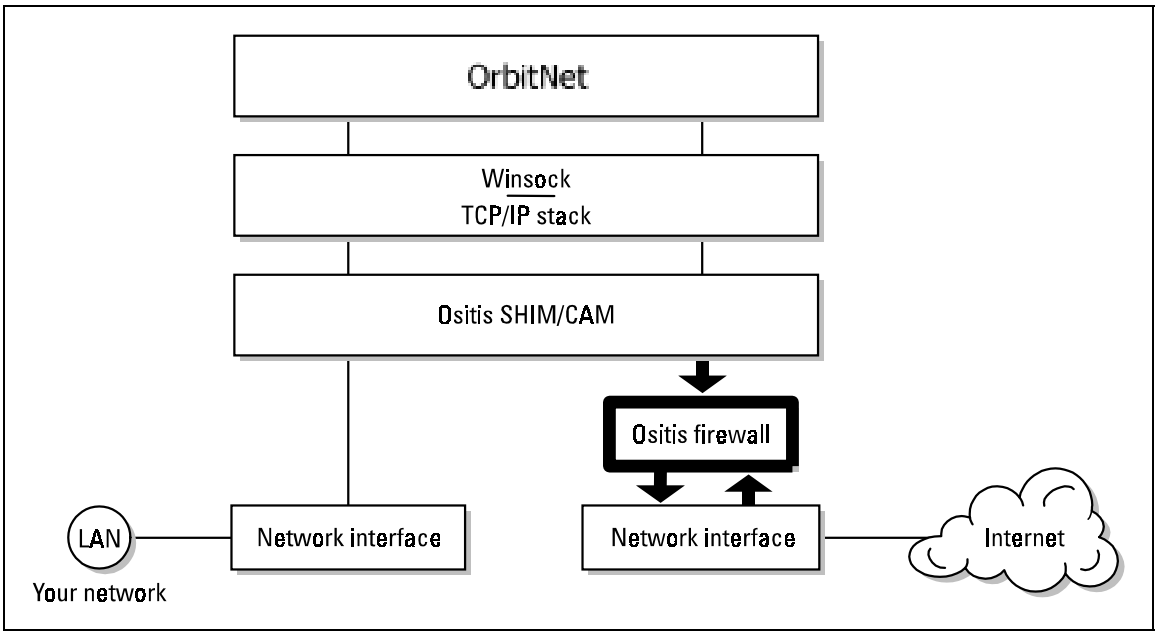


Figure 10-6: OrbitNet's Firewall.

As shown here, the Firewall Tab is where you control the system-level firewall. You can regulate exactly which ports allow TCP and UDP for both incoming and outgoing traffic.

An important point: the settings you make here determine what traffic will be permitted, but they don't automatically enable any protocols. As an example, although you can enable file and printer sharing on your external connection, it won't work unless you also "open up" ports 135-139 for outgoing connections with your firewall settings. There's a very good reason for this: since allowing file and printer sharing on your external connection is a security problem, all but the lowest security setting in OrbitNet prohibit these outgoing ports.

The slider shown in the screen shot above allows you to choose from a number of pre-defined security settings. The default setting is Medium, which allows the greatest flexibility with the best security for most users. The lowest settings permit most games, but don't close much at the system-level firewall. With the highest settings, nearly everything is shut off. In addition, ports are allowed only if specified by you with their own filters, as in the pre-defined list (or if you've enabled them elsewhere in OrbitNet).

Once you specify filters of your own, the slider vanishes and OrbitNet confirms that you're now using custom settings. To return to any default firewall settings, simply click the default button. If any custom filters you've defined won't work under a chosen default setting, OrbitNet disables that filter (the filter stays in the list, however, saving you the trouble of figuring out the settings again). The long and short of it is: when using custom settings, the security level you start with *does* make a difference.

You'll notice that OrbitNet places two entries in the filter list. You'll be able to change one, but not the other.

The unchanging filter is the "System Defined Filter." It's a compilation of all of the settings you've made elsewhere in OrbitNet—under the Protocols Tab, for example. These settings, which form the core of the Classic Proxy, can't be disabled as group. Changes can only be made to the basic OrbitNet settings.

The changeable filter is the preset security level, whose name changes depending on the security level you've selected. Under the Medium setting, for example, it's called "Medium Security Level." It's possible to change these, but we recommend simply changing security levels with the slider and using your own filters to make firewall adjustments. It's instructive, though, to open each of these filters for inspection: click Modify Application, and then analyze what the preset security filters and how they're constructed at each level.

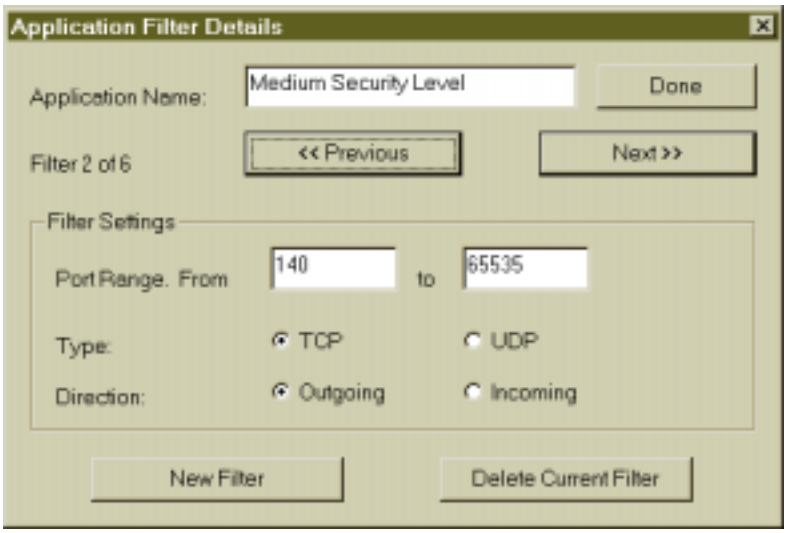


Figure 10-7: An example of a user-defined rule in the security filter.

While you're free to define a range of ports, be careful: it's easy to overstep, opening up more than you intend. Since any one application might take a number of protocols and ranges, you can define as many rules for an application as you need. In the figure above, we're looking at Rule No. 2 of 6 rules. You can step through the rules by using the Previous and Next buttons. To add a new rule to an existing filter, click New Filter. When finished with the rules, click Done.

If you step through the medium security rules you'll see that almost all outgoing TCP and UDP connections are allowed, except for ports 135 through 139—those used by Microsoft for file and printer sharing.

C. MAPPED PORTS

The Mapped Ports Tab is used to configure access for Internet services and applications not directly supported by OrbitNet. Mapped ports come in two primary forms: outgoing and incoming.

Outgoing mapped ports are most common under applications using Classic proxy settings. These ports are used for Internet sessions originating on a machine behind the firewall and connected to a machine on the Internet. The HTTP proxy, FTP and Mail proxies used by browsers and other applications are examples of outgoing ports directly supported by OrbitNet. If you have Transparent proxy enabled in OrbitNet (the default setting), Transparent proxy will handle most outgoing connections without the need for setting up an outgoing mapped port.

Incoming mapped ports allow outside access to a machine on your local network. The session originates on the web somewhere (you have no control over where). *Incoming ports are a hole in your*

firewall, and should be treated carefully. Most small networks will never need an incoming mapped port. The incoming HTTP proxy and incoming SMTP proxy are examples of incoming ports directly supported by OrbitNet.

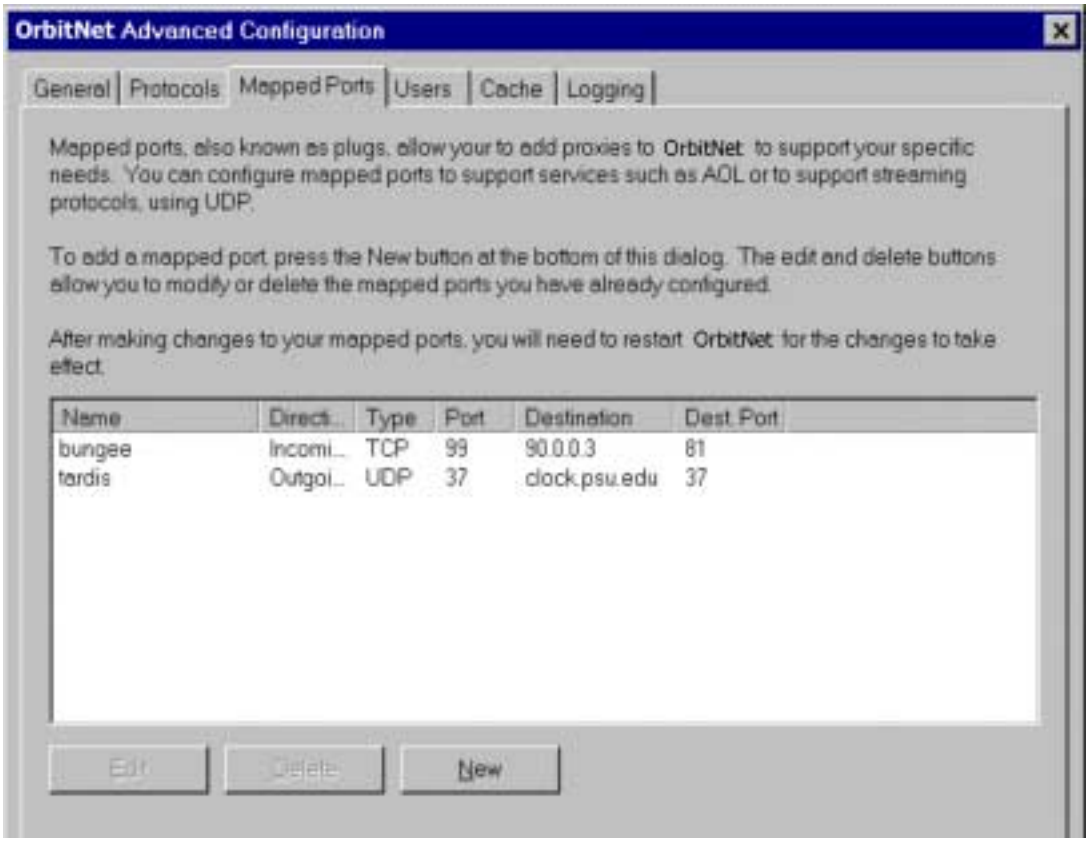


Figure 10-8: The main Mapped Port page allows you to add other proxies to OrbitNet, finely-tuning the program to suit your specific needs.

The main Mapped Port page shows which mapped ports have been configured, along with their settings. The mapped port name also appears on the main OrbitNet ConnectionView screen as another protocol. To add a mapped port, click **New**.

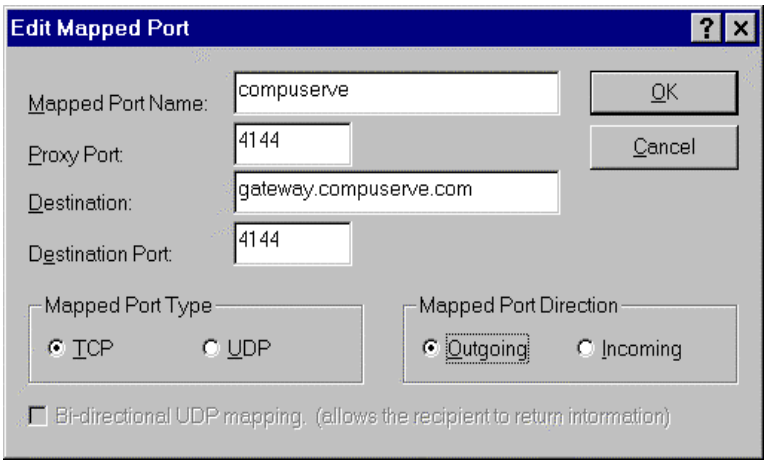


Figure 10-9: This screen allows you to edit mapped ports.

The dialogue in Figure 10-8 allows you to: (1) modify an existing mapped port, or (2) create a new mapped port. The options are:

1. Mapped Port Name: Enter any name you like for the mapped port. After mapping is installed, this name will be displayed in the main window. It's helpful to use a name describing the connection type. As in our example, CompuServe users would enter **CompuServe**.

2. Proxy Port: Enter the port number OrbitNet uses when listening for mapped connections. This is the port number you need to tell your application to connect to. In the example shown the proxy port is 4144. The proxy port can be different than the destination port.

Outgoing Direction: OrbitNet uses this port on its internal network connection to listen for activity from any of your client computers. Communication from any client computer will be sent to the address and Destination Port you configure (see below).

Incoming Direction: OrbitNet uses this port on its external network connection to listen for activity from any computer on the Internet. Any communication will be passed directly to the internal Destination IP address and Port you specify (see Destination IP, below).

3. Destination: IP: Enter the IP address of the machine you want to receive the connection request. In the example, this address is **gateway.compuserve.com**. When OrbitNet receives a connection on the Proxy Port, it connects to this IP address.

Outgoing: Enter the IP address of the distant server to which your application connects. You can only connect to a single IP address.

Incoming: Enter the IP address of the machine on your local network to which an Internet user will connect. You can only specify a single machine.

4. Destination: Port: Enter the port number of the machine to which you are mapping. When OrbitNet receives a connection on the Proxy Port, it connects to this port on the machine specified in Destination IP. It may be helpful to think of the Destination IP and Port as two parts of one address. In the example shown above, the destination is **gateway.compuserve.com:4144**.

Outgoing: This will be the port on the Internet machine (specified by Destination IP) to which OrbitNet sends whatever it has received on the proxy port.

Incoming: This will be the port on the machine on your local network (specified by Destination IP) to which OrbitNet passes on whatever it has received on the proxy port.

5. Mapped Port Type: Select from TCP or UDP to choose the type of mapping to use. TCP, the most common type of connection, is used in most Internet protocols. UDP is streaming data, typically used for protocols such as RealAudio, which transmit continuous data. The primary difference between the two is that UDP packets do not guarantee delivery. TCP is usually the wisest choice, unless your application specifically states that it uses UDP.

6. Mapped Port Direction: An outgoing mapped port is appropriate when the session originates from a machine *behind* the firewall and connects to a server *outside* the firewall. A typical example: a weather application which connects to an Internet server for updates. Using TCP, once the session is established communication can flow both ways. The majority of mapped ports utilized by most users will be TCP/outgoing.

An incoming mapped port is appropriate when the session originates *outside* the firewall and connects to a machine (i.e., computer) *behind* your firewall. An example: a business which allows some of its clients to connect directly to one their servers.

7. Bi-directional UDP Mapping: If you've chosen TCP protocol, this selection is grayed out; it's allowed if you've selected UDP. Unlike TCP, a UDP session does not automatically provide for communication in both directions once the connection is established. Enable this selection if you're using UDP and want data to travel in two directions.

8. Disabled: Checking this box disables the mapped port without losing the settings.

Additional Examples of Mapped Ports

One of the common uses of mapped ports is allowing access (via Classic Proxy) to additional News servers.

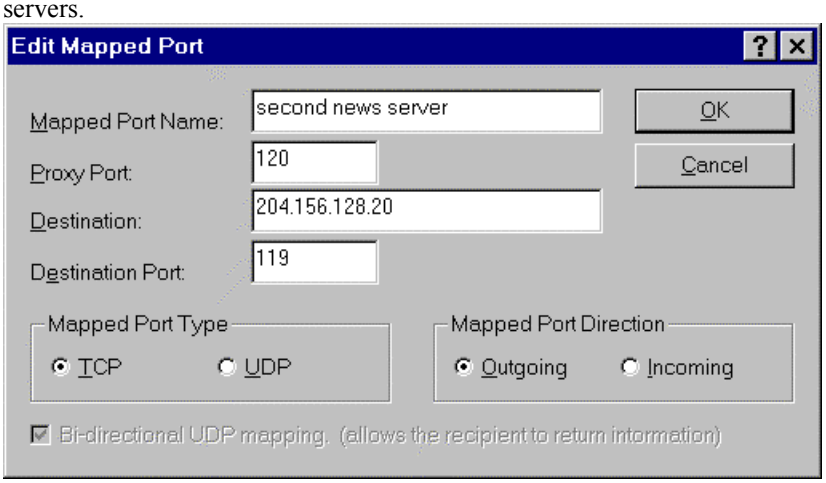


Figure 10-10: A mapped port that sets up access to additional News servers.

It's best to use the numeric IP address of the other News server (the one shown here is for Best's News Server). However, you can also use a domain name form such as **mail.best.com** if (1) OrbitNet is connected to your Service Provider at the time and, (2) you enabled, on the General page, **permit domain names in mail, news and mapped ports**.

You can use port 120 as a proxy port (8119 is another common choice). You'll need to use a different proxy port for each additional News server. As you can see from the example shown here, you can have different proxy and destination ports. In this case, OrbitNet listens on the proxy port on its internal

connection; anything arriving on that port from one of your client computers will be sent to the destination IP and destination port.

The News application needs to be configured with the IP address of the OrbitNet machine; it must also be given the new port number. Many applications will let you do this as part of the IP address, using the form **90.0.0.1:120** or **OrbitNet:120** to designate server name and port.

The destination port for News Servers should always be port 119, unless you are certain that the destination is a different port.

Another example of a mapped port:

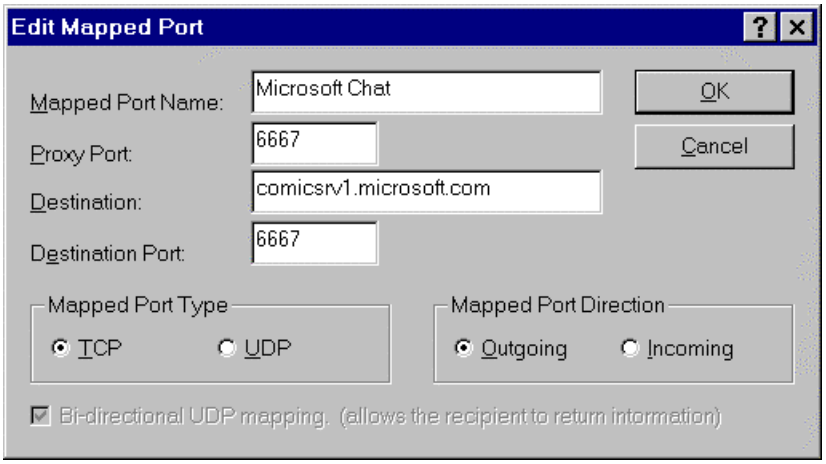


Figure 10-11: A mapped port used to set up Microsoft Chat.

Figure 10-9 is an example of a mapped port used to set up Microsoft Chat. The application does its business on port 6667, where the server expects to hear from it. In the application itself you'd specify that the server can be found at the OrbitNet internal IP address. The mapped port name appears in the mapped port screen and on the main view screen. This name can be anything you choose.

A last look at a mapped port—an incoming port, this time.

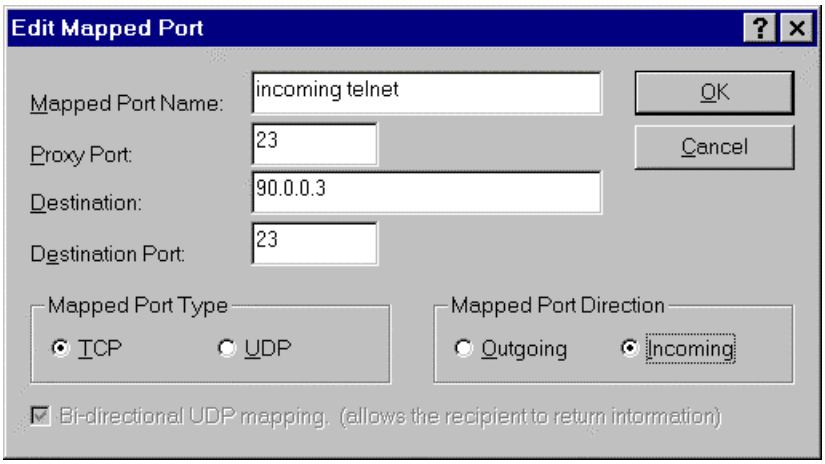


Figure 10-12: An incoming mapped port.

A NOTE OF CAUTION

The settings described above constitute a hole in your firewall, since you have no way of knowing who is coming in on the proxy port. For an incoming port, the proxy port is on the *external* connection. Anybody telnetting to your OrbitNet machine will immediately connect to the machine at 90.0.0.3.

Revealing the Mysteries of Mapped Ports

New users often find the concept of a Mapped Port (sometimes called a "plug") to be mysterious. Like much else, though, once you know what the words mean a lot of the mystery disappears. We'll try to dissolve anything mysterious about mapped ports in this section.

Here at Orbit Communication Corp., most questions we've received about mapped ports can be categorized in two ways. First, users simply don't have a good feel for what a mapped port is, or for what the various settings mean when they try to set up a mapped port. Second, they're unclear about the difference between Incoming and Outgoing connections.

What's a Mapped Port? The fact is, many of you have already seen a mapped port in action, even if you thought you hadn't messed with one yet. Most of what a Classic Proxy does is, in fact, a mapped port in one form or another. All of the functions you configured in OrbitNet to allow browsing, email, news, ftp and telnet are a form of mapped ports. They don't look like it at first, because we've wrapped them up in a nicer-looking interface and hidden some details. But the bottom line is that they are much the same as mapped ports.

Here's an example. Let's say that you configured the News protocol in OrbitNet, telling it that (1) your news server is at news.myisp.com, and (2) to use the standard port 119 for news. You could configure a mapped port that would do **exactly** the same thing, like this:

Mapped Port Name:	Any name you choose
Proxy Port:	*119*
Destination IP:	*news.myisp.com*
Destination Port:	119
Protocol:	TCP
Direction:	Outgoing

In the chart above, the two entries in italics are the settings made by you when configuring the news protocol. The others are known in advance: since these particular news protocol settings never change, their unnecessary details aren't presented to the user.

One last thing that mapped ports and other protocol configurations have in common: application settings. With the Classic Proxy, you must configure your news application to find its news server at the OrbitNet IP address instead of the "real" address. You must do the exact same thing if you configure the news application using Mapped Ports instead of the news protocol settings.

We chose not to use browsing, telnet or ftp as examples here because they have one crucial distinction from a regular mapped port. Using methods carefully specified and standardized by the Internet community, OrbitNet can "peek" at the connection request from those protocols to ascertain the destination. Thus, it's not limited to a single destination as regular mapped ports are.

Incoming/Outgoing Connections. Now we'll turn to the distinction between incoming and outgoing connections. In a standard installation, all or almost all connections are *outgoing*. A browser, an email application, or any other local application begins a connection session by sending a connection request *out* through the firewall.

This is simply the nature of Internet communication (you can read more about this in "Ports is Ports," contained in Appendix H: Network Knowhow). A *server* listens and listens on a particular port, waiting for connection requests. That's what a server is. A *client* doesn't listen; it sends a connection request to a waiting server. That's what a client is. For most simple local networks, *all* of your local applications are client applications, and if you need to set up a mapped port it will be an outgoing mapped port.

Here's a diagram showing what the settings for an Outgoing Mapped Port refer to:

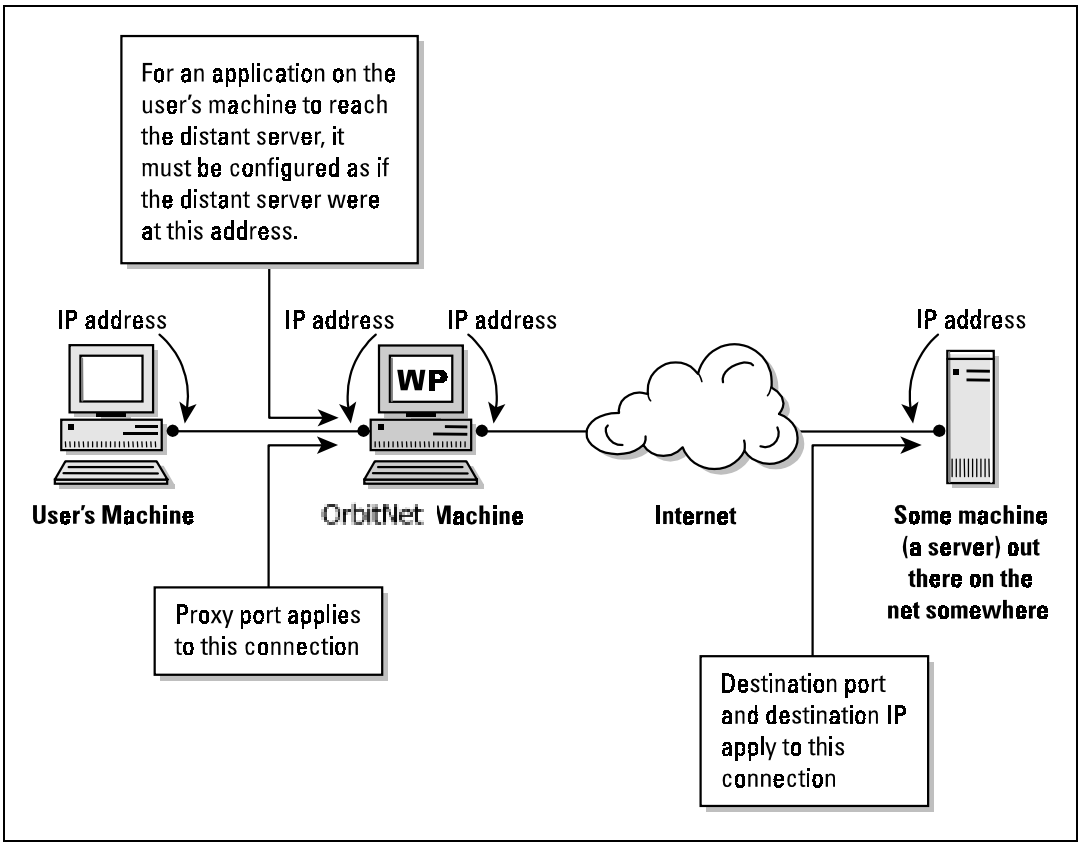


Figure 10-13: This schematic, representing an Outgoing connection, illustrates how a client application behind OrbitNet reaches a distant server computer on the Internet.

An *incoming* connection is only needed when your local network contains a server and you intend to allow people on the Internet to connect to that server. You need to open a port on the external side of your firewall, allowing connection requests to come *in* through your firewall.

OrbitNet already has an interface for some of the more common internal servers, including a web server, a mail server, and an ftp server. The settings for each of these is found in Settings: Protocols. Look under the appropriate protocol name, where you'll see it listed as an *incoming* connection. As soon as you enter settings in these boxes and say "OK," you have a hole in firewall that allows incoming connections.

You need to provide one piece of information to those outside users: the address of your server. The internal address of your server will do them no good, as they can't see into your network. Give them the IP address of the *external* OrbitNet network connection; also—if you use a non-standard port—tell them the port number. When you set up an incoming mapped port, OrbitNet opens that port on the external side to listen for connection requests; it thus acts as a proxy server for those folks on the outside just as it does for your client applications on the inside.

Here's a diagram showing what the settings for an Incoming Mapped Port refer to:

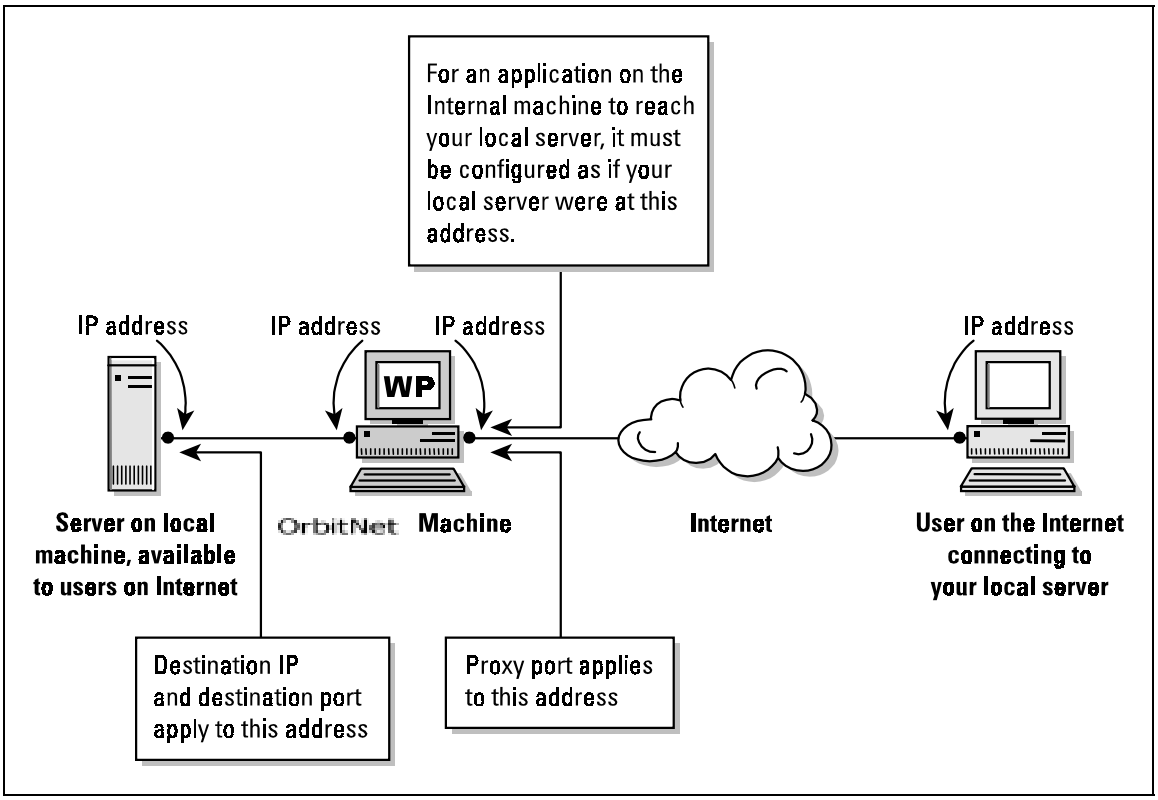


Figure 10-14: This schematic, representing an incoming connection, illustrates how a distant client application on the Internet reaches a Server behind OrbitNet.

When a user needed a mapped port in OrbitNet 2.1—a Classic Proxy—95% of the time they would need an outgoing mapped port. The user would almost always have a client application that needed to connect to a server elsewhere.

This last part holds true in OrbitNet 3.0, as well. However, with the new connection engines you need only set up outgoing mapped ports when OrbitNet 3.0 is configured to act *only* as a Classic Proxy and the NAT/Transparent Proxy functions are disabled. When the NAT engine is enabled, outgoing connections that formerly needed mapped ports now work seamlessly and invisibly. No further configuration is required.

Incoming ports, though, need to be configured in either version. OrbitNet will *not* open up incoming connections unless you specifically configure it to do so.

Bi-Directionality. There's a little more to connections than just sending the connection request. After the request is made, the client and server send many packets back and forth. For TCP connections, return packets are allowed through the firewall; you needn't make any special allowances.

UDP, on the other hand, is a connection-less protocol with no particular provision in the tcp/ip stack for handling return packets. In most cases, when you are configuring a UDP mapped port, you'll want to enable the Bi-Directional option so that returning packets will be allowed through the firewall.

Some rules of thumb for configuring Mapped Ports:

1. If behind a Classic Proxy, 95% of the mapped ports are outgoing mapped ports.

2. When configuring an outgoing mapped port, you *must* know the destination IP address. Many site FAQs specify only the ports you need to open and fail to mention the IP address. You need to know that IP address for proper configuration.
3. When they don't specify which protocol, start with TCP, which is most commonly used (not only was it the "original," but it also provides error-checking and an assurance that packets arrived). Most places specify UDP when it's required, but if they don't use words like "streaming," it's possible that they're using UDP.
4. When you do use UDP, enable the Bi-Directional option.
5. Most of the time, the proxy port and destination port will use the same port number.

Our last offering here is a complete group of sample diagrams for setting up mapped ports. The application featured in this group is "WinVNC," a freeware program somewhat like PCAnywhere or CarbonCopy. This program allows you to control a distant computer, viewing their screen on yours, and controlling it with your keyboard and mouse.

This program comes in two major pieces. One is the VNC Server. It runs on the machine that will be controlled, and like any good server sits and patiently waits for a connection request. The other portion is called the VNC Viewer—the client application. You use VNC Viewer to connect to VNC Server; once connected the server asks for a password and then allows you control of the machine on which VNC Server is running.

With default settings, VNC Viewer and Server communicate on port 5900, the port setting shown throughout all but one—the last—of these diagrams. The IP addresses shown are sample addresses; those, too, remain the same throughout the diagrams to aid in readability. The first diagram shows the connection without a proxy/firewall, simple as can be. Increasingly complex topologies follow, starting with a single firewall on the client side (the most common configuration) and working up through more interesting scenarios.

The first illustration below shows the simplest possible setup – no proxies, no firewalls. It'll give you an idea of our starting place.

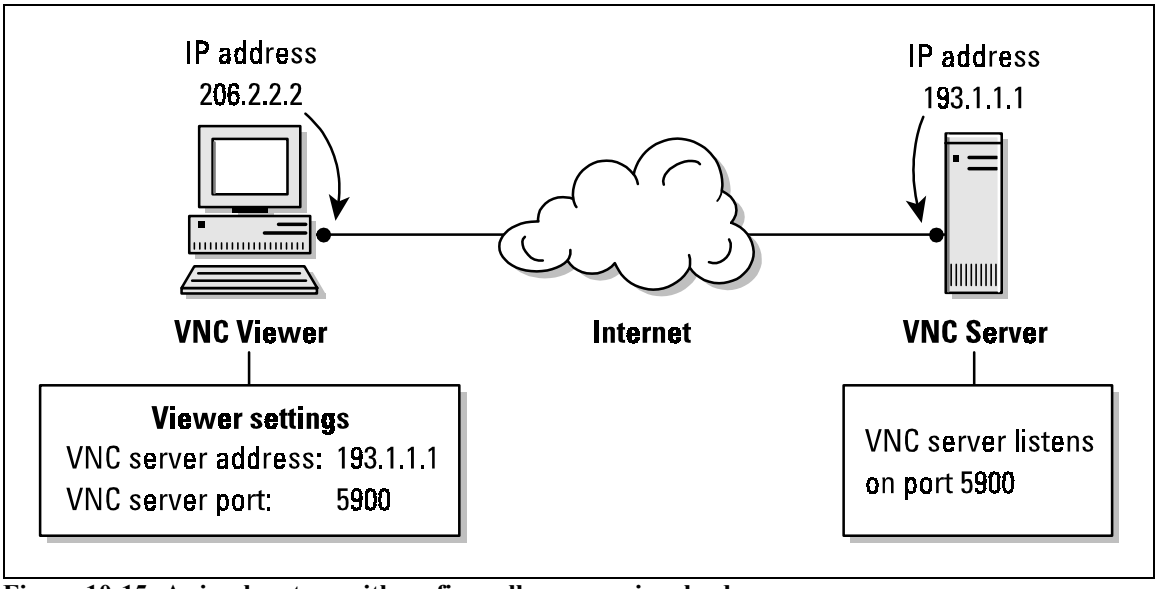


Figure 10-15: A simple setup, with no firewall or proxy involved.

The VNC viewer (in Internet parlance, it's the client application; it starts the communication by sending connection requests) must be told where the VNC server is and on what port the server is listening.

The next picture is the first showing a proxy/firewall in place. The firewall is on the client's side of the Internet cloud. This shows the settings you'll need if OrbitNet 3.0 is your firewall:

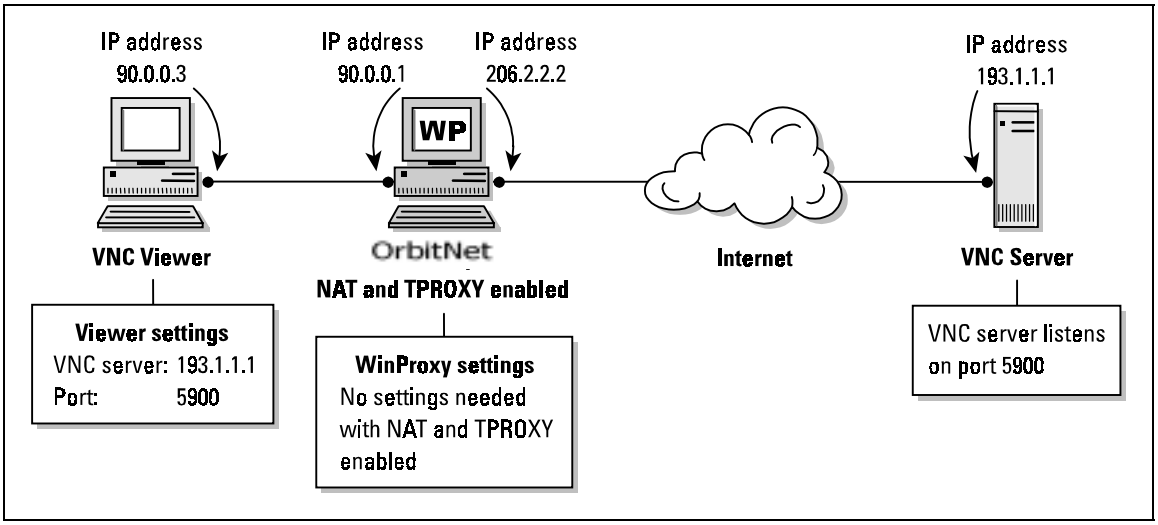


Figure 10-16: A simple OrbitNet setup in place. This situation, with a client-side firewall, is the most common situation seen by users.

As you can see, no additional settings or changes are needed. The NAT or Transparent Proxy functions in OrbitNet accomplish any translations needed to connect to the server.

Without the NAT drivers, however, things are a little more complicated:

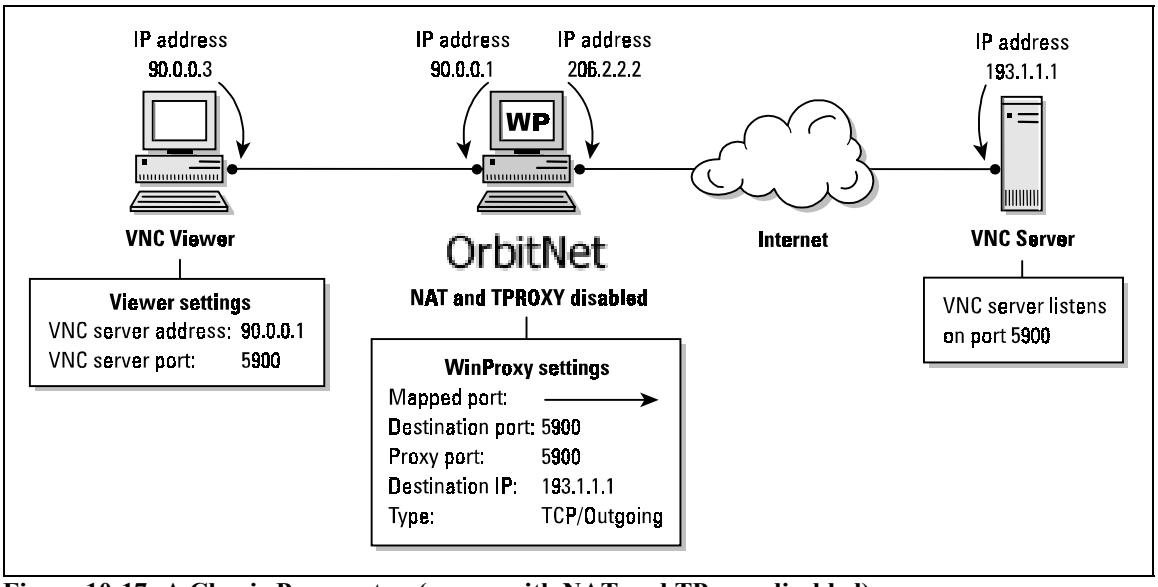


Figure 10-17: A Classic Proxy setup (or one with NAT and TProxy disabled).

Figure 10 shows the settings if you're using a Classic Proxy (like OrbitNet 2.1) or if you have the NAT and Tproxy (Transparent Proxy) settings disabled in OrbitNet 3.0. In this situation, you'll need a mapped port. Since the viewer (client app) is behind the firewall, you'll need to set up an *outgoing* mapped port. The mapped port setting contains information about where the Server *really* is. As far as the client knows, the server is at the OrbitNet internal IP address. For that matter, as far as the client knows the *entire Internet* lives at that address. Any other address makes no sense to the TCP/IP routing software.

Figure 11 illustrates the firewall on the Server side. You'll see only one illustration in this case—not two as for the firewall on the client side. Since the client is attempting access from *outside* the firewall, no automatic translation takes place. The settings are the same for OrbitNet 3.0 with Transparent Proxy as they are for OrbitNet 2.1 with Classic Proxy:

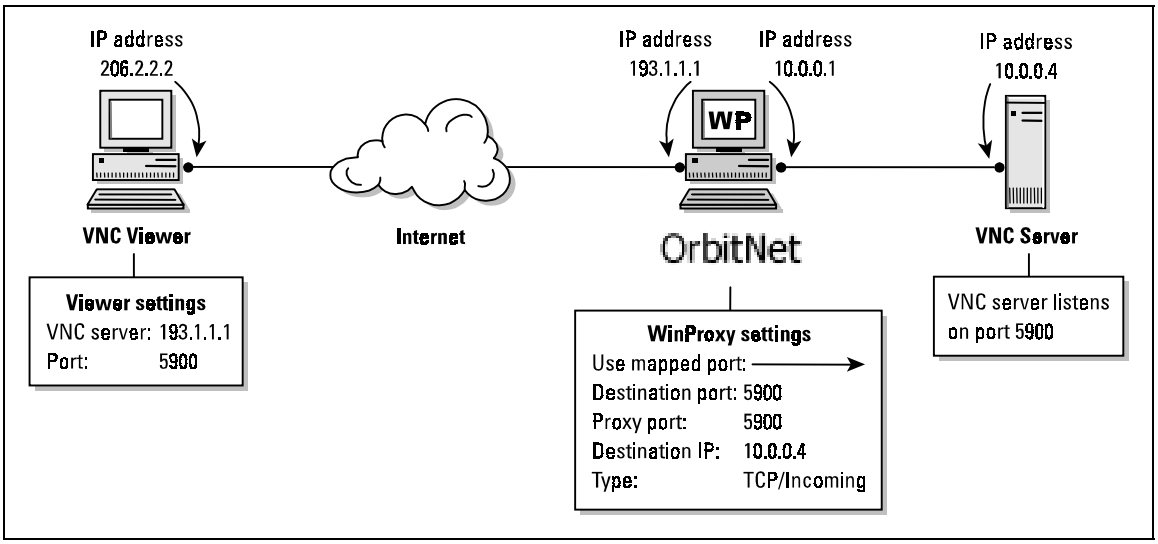


Figure 10-18: The server side firewall.

Only when somebody outside your firewall attempts to contact a server inside your firewall do you need to set up an *incoming* mapped port. The mapped port settings contain information about where your server *really* is. The distant client must be configured as if your server were at the OrbitNet external IP address, the only point on your local network visible to the Internet.

Now let's look at a more complicated situation, one that people are increasingly running into as private networks become more pervasive. In Figure 12 you'll see a firewall on *both* sides, which means that both client and server apps are hidden behind their own firewall:

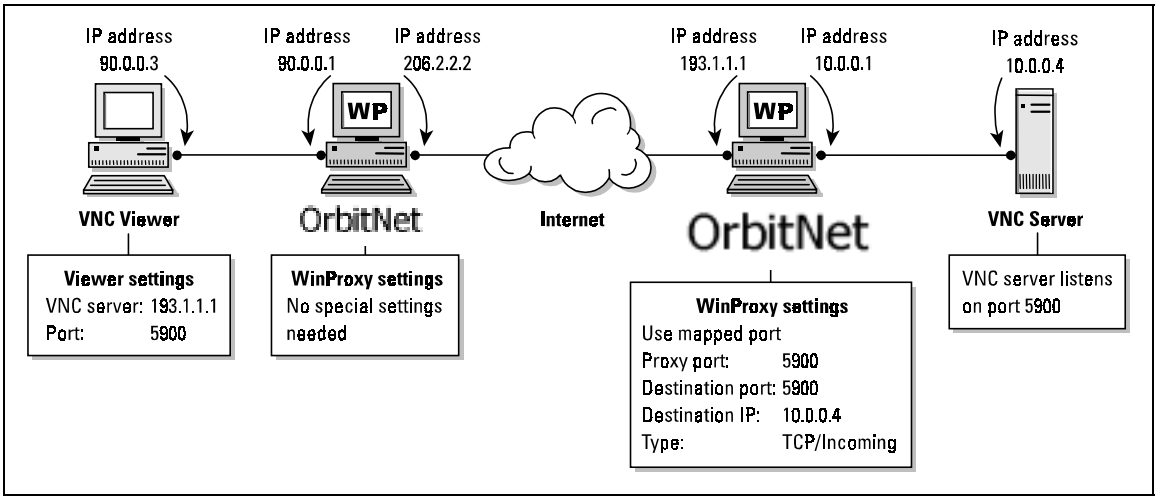


Figure 10-19: A setup with a firewall on both client and server sides.

The same rules apply as before. If you're using OrbitNet 3.0 (with default settings) on the client side, there's no need to do anything special with OrbitNet. However, you *do* need to configure the client

application as if the distant server resided at the only visible IP address for that network—the firewall's external address. On the VNC server side, you need to set up an incoming mapped port no matter which type of firewall you have. This incoming mapped port on the server-side firewall has the information about where the server really is.

Figure 13 illustrates a slight variation of the setup just presented. The only difference is that the client-side firewall is now a Classic Proxy, so you *will* have set up a mapped port on the client-side firewall:

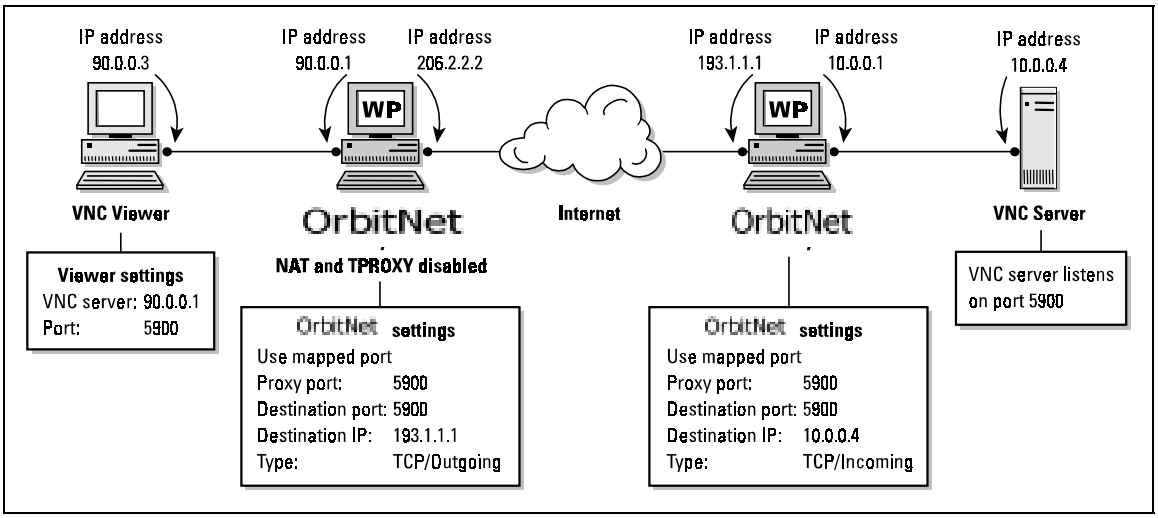


Figure 10-20: A setup with a firewall on both client and server sides; the client-side firewall is a Classic Proxy.

Once again, the familiar rules apply. On the client-side firewall you must configure an *outgoing* mapped port, telling it that the distant server lives at the other network's external IP address. On the server-side firewall, you have to configure an *incoming* mapped port with the actual server address. As you go through this, you'll notice that the client side has to know the server side's external address; if you look closer, you'll also notice that *nobody* has to know the client side's external address.

Now here's one last illustration for those who've hung on this long: a variation on the setup just above. The situation is exactly the same—*except* that we're not using the same port numbers throughout:

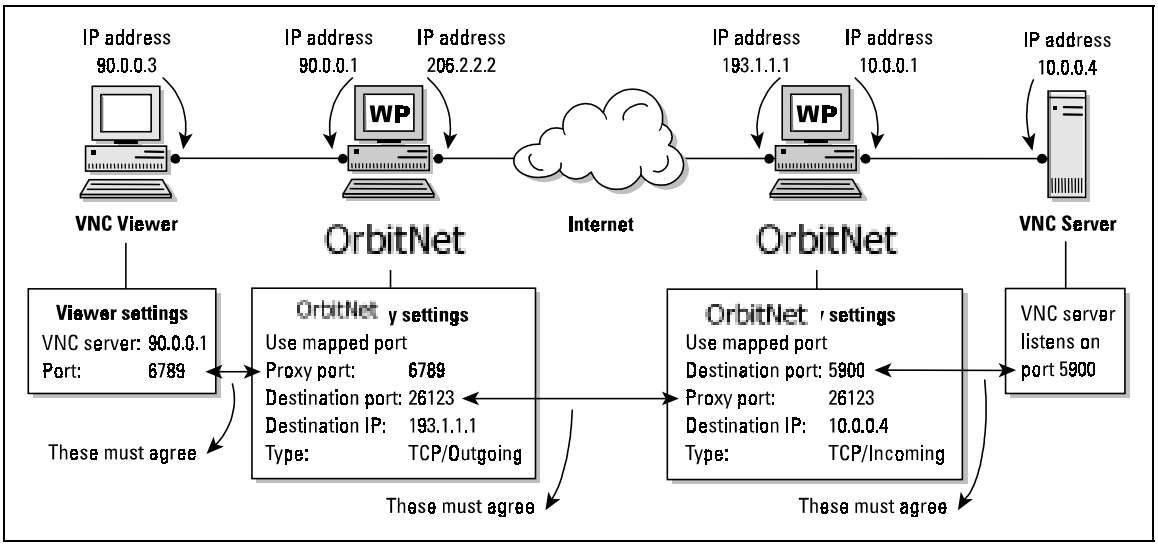


Figure 10-21: A setup with a firewall on both client and server sides. The client-side firewall is a Classic Proxy. Identical port numbers are not used throughout.

This diagram shows that the destination port and proxy port settings for any one mapped port configuration don't have to agree. The only rule is that the "destination port" on the source machine *must* match the "proxy port" on the destination machine. In other words, the port you're sending too must be the port they're listening on.

Chapter 11

Remote Administration

CHAPTER 11: REMOTE ADMINISTRATION

OVERVIEW

OrbitNet allows routine proxy server maintenance to be accomplished remotely; however, for the sake of security, the administrator must be behind the firewall. Accessible features for remote administration are:

- Override Dialing Lockout
- Flushing the Cached DNS List
- Displaying Cached Names
- Displaying Connection Statistics
- Displaying the URL & IP Blacklist
- Hanging Up the Current Dial-Up Networking Connection (if any)
- Displaying Cache Statistics
- Browsing Cached Files
- Deleting All Cached Files

Remote configuration can only be accomplished from behind the firewall. If an Administration Password has been specified in OrbitNet's configuration, that password is required to access remote administration.

To utilize remote administration, use a World Wide Web browser configured to access the net through the proxy (any properly-configured browser on a client machine will do). Then request the URL **http://Proxy.Command/Help.** OrbitNet returns a page with the header "OrbitNet Command Help" and the OrbitNet version number. Beneath this you'll see a menu of options, each followed by a descriptive sentence. Select any option by clicking on its name. Any document requested from the Proxy.Command host name responds with the help menu (unless the requested document is one of the commands listed below).

OPTIONS

A. Override Dialing Lockout: When the time window option is enabled, OrbitNet permits dialing only within the time period specified. This command permits overriding the specified time period, thereby allowing a call during normally disallowed hours. A user attempting to connect during off-hours is also presented with this screen, preceded by a password-entry screen if the program is set to use an administration password.

This command is not visible if **Use Dial-Up Networking** has not been checked.

B. Flush the cached DNS list: Clicking on this command purges the name cache maintained within OrbitNet. All cached DNS entries and URL lookups are deleted. This command cannot be undone. Internet access may appear slower until the cache of frequently-accessed sites is rebuilt (as each is called during normal activities). The cache can be maintained for up to two days; it's useful to clear this cache if you know that a location has changed but the proxy hasn't updated its cache to the new numeric address.

C. Display cached names: Displays the names contained in the name cache.

D. Display connection statistics: Displays the number of requests made through OrbitNet, and the percentage of successful connections. This page refreshes itself every fifteen seconds.

F. Hanging up current Dial Up connection): Terminates the current Dial-Up Networking connection as soon as there are no active connections to the Internet. The connection isn't terminated immediately, but at the soonest possible convenience. If you want to use this command often, it's useful to store the URL **http://proxy.command/HangUp.htm** among your bookmarks.

G. Display Cache Statistics: Displays current statistics for the document cache. The information updates automatically every 15 seconds.

H. Browse Cached Files: Allows you to browse files in your OrbitNet document cache. You can click on the hyperlinks to view individual cached files. You should refresh this page periodically, as the files in the cache are changed by OrbitNet.

I. Delete All Cached Files: Deletes all files from the OrbitNet document cache. There is no way to undo this command, so use it only when you want all cached files to be permanently deleted.

Chapter 12

The Name Cache

CHAPTER 12: THE NAME CACHE

OVERVIEW

The name cache is altogether different from the user-configured Cache Tab discussed in Settings (Chapter 9). It is independent of any settings made in the DNS setup dialog.

The name cache holds DNS lookups, thus speeding up subsequent net access—the user, not having to wait for return results from the lookup, sees the requested web page one or two seconds faster. The name cache can't be altered or changed in any way by the user, although it can be deleted. The information provided below is intended to fill in the edges of your OrbitNet knowledge.

HOW THE NAME CACHE WORKS

The first step in most Internet sessions is a name lookup. When a user types in a URL or domain name—**www.OrbitSat.com**, for example—the name must be converted into a numeric, machine-usable address. This process is referred to as a name lookup. Most commonly performed by your ISP's DNS (Domain Name System) Server, a name lookup must be done before a connection can be completed.

OrbitNet's name caching feature speeds up the initial connection significantly by storing names and URLs *along with their corresponding IP Addresses*. When the request goes to your ISP with a numeric address instead of a name, the look-up process (and the time it takes) is bypassed.

- If the Reverse Name Lookup feature is *not* enabled, OrbitNet stores every name and URL it looks up.
- If the option *is* enabled, only verified addresses are stored.

The lookups stored include mail and news connections as well as web browsing. Each name is placed into the cache, where it is stored for up to 2 days. Older names are purged. OrbitNet maintains an internal DNS list, and also a DNS Cache file within the OrbitNet directory.

By storing only verifiable names when RNL is enabled, OrbitNet offers a security feature which significantly reduces the risk of being provided with a "bad" name. It also improves performance by reducing the requirement for repeated name requests. The JAVA virtual machine, for instance, requires RNL to enforce its security, which requires that a JAVA applet only connect to the originating server. Without name caching, this feature cannot be guaranteed, thus creating a security risk.

Since all names are cached, it is sometimes necessary to purge the name cache. For instance, if your mail server's IP Address has been changed and you must ensure that the mail goes through immediately, you'll need to purge the entries in the name cache to force a new lookup. You can do this in Remote Administration (Chapter 11). Purging the name cache flushes both internal and filed DNS caches.

Chapter 13

Running OrbitNet as a Service Under Windows NT

CHAPTER 13: RUNNING ORBITNET AS A SERVICE UNDER WINDOWS NT

OVERVIEW

Windows NT allows you to customize the way you run OrbitNet. You can run it:

- As a standalone application.
- As a service, configuring it to either start manually or automatically when Windows NT boots.
- In hidden mode it isn't visible on the screen and the user interface is not available. Even with a visible interface, most service options won't permit OrbitNet configuration changes and generate an error if you try.

The following sections describe several different service options, starting with the simplest. All NT system services are configured by following the click-path **Control Panel/ Services**. Services are listed alphabetically in the window. Highlight the service to be configured and click **Startup**.

If you plan to run OrbitNet on a computer with more than one user account, we recommend running it under its own account and not as a system account. To assign the rights for running services to that account, go into **Policies** (NT4 Service Pack 3 and higher will prompt you for it; earlier versions will not). When running on a machine where the user account may change, run OrbitNet as a hidden service.

A Few Helpful Tips

If you'll be installing OrbitNet as a service, we recommend first configuring it to suit your needs: once it's running as a service, the service must be stopped (and the computer restarted) when configuration changes are made. This is not only tedious but makes it difficult to determine causes if things don't work the way you expected. We also suggest enabling activity logging in OrbitNet before running it as a service. Then, if you need to use logging to help with trouble-shooting, you can start the logging application.

A. Visible Service, Desktop or Start Menu Start and Stop

User Interface: YES	Loads Automatically: Only From Startup Group
Permits Configuration: YES	Loads Before Logging On: NO

You're not required to start the program automatically even if you've checked the box in OrbitNet instructing it to run as a service. When you begin OrbitNet from the Start Menu, it runs in the System Tray so that it doesn't occupy desktop space. You can bring up the user interface by double clicking on the mask icon. OrbitNet won't start up with its main screen visible; if it did, you'd have to minimize it before logging into Windows. To put OrbitNet in the Startup Group:

1. Click the path **Start/Settings/Taskbar/Start Menu Programs/Add/ Browse**. Double-click **OrbitNet**.
2. Click **Next.**
3. Double-click the StartUp folder.
4. Enter the name you want.
5. Click **Finish**.

B. Visible or Hidden Service, Manual Start and Stop

User Interface: OPTIONAL	Loads Automatically: NO
Permits Configuration: NO	Loads Before Logging On: NO

1. If OrbitNet is already installed as a service, skip to Step 6.
2. Click the OrbitNet mask icon in the Start Menu.
3. Select **Settings** from the OrbitNet File Menu.
4. Check **Run As A Service** in the General Tab.
5. Click **OK** to exit the configuration. Close OrbitNet.
6. Click the path **Settings/Control Panel** from the Start Menu.
7. Double-click the **Services** icon in the Control Panel.
8. Scroll to the bottom of the list of services until you find the OrbitNet Service. If it's not present, check to make sure that you've exited OrbitNet. If it's still running in the task bar, close it and reopen the Services control.
9. Select **OrbitNet Service** and click **Startup**.
10. Set the Startup Type to Manual.
11. In the Log-On section, select **System Account**.

If you want the service to be visible, check **Allow Service to Interact with Desktop**. If you want the service to stay hidden, leave the box blank.

You're done! Any time you want to start or stop the OrbitNet service, go to the Services applet in the control panel, select the OrbitNet service, and click **Start** or **Stop**.

C. Visible or Hidden Service, Automatically Loaded After Logging In

User Interface: OPTIONAL	Loads Automatically: YES
Permits Configuration: NO	Loads Before Logging On: NO

1. If OrbitNet is already installed as a service, skip to Step 6.
2. Click the OrbitNet mask icon in the Start Menu.
3. Select **Settings** from the OrbitNet File Menu.
4. Check **Run As A Service** in the General Tab.
5. Click **OK** to exit the configuration. Close OrbitNet.
6. Click the path **Settings/Control Panel** from the Start Menu.
7. Double-click the **Services** icon in the Control Panel.
8. Scroll to the bottom of the list of services until you find the OrbitNet Service. If it's not present, check to ensure you've exited OrbitNet. If it's still running in the task bar, close it and reopen the Services control.
9. Select **OrbitNet Service** and click **Startup**.
10. Set the Startup Type to Automatic (it should already be selected).
11. In the Log-On section, click **System Account**
12. If you want the service to be visible, check **Allow Service to Interact with Desktop**. If you want the service to stay hidden, leave the box blank

You're done! Press **OK** to return to the Services list. OrbitNet should now load the

next time you log into Windows NT.

D. Hidden Service, Automatically Loaded

User Interface: NO	Loads Automatically: YES
Permits Configuration: NO	Loads Before Logging On: YES

This is the most complex configuration for running OrbitNet as a service. The following set of instructions is for NT 4.0. Windows NT 3.51 users can also run OrbitNet as a service, and the configuration is similar.

1. If OrbitNet is already installed as a service, skip to Step 6.
2. Click the OrbitNet mask icon in the Start Menu.
3. Select **Settings** from the OrbitNet File Menu.
4. Check **Run As A Service** in the General Tab.
5. Click **OK** to exit the configuration. Close OrbitNet.
6. Click the path **Settings/Control Panel** from the Start Menu.
7. Double-click the Services icon in the Control Panel.
8. Scroll to the bottom of the list of services until you find the OrbitNet Service. If it is not present, check to make sure you have exited OrbitNet. If it's still running in the task bar, close it and reopen the Services control.
9. Select **OrbitNet Service** and click **Startup**.
10. Set the Startup Type to Automatic (it should already be selected).
11. In the Log-On section, select **This Account** and click the small button on the right containing three dots.
12. You should now have a dialog box labeled **Add User**, allowing you to select an existing user—any user you like—to run with this service. It's a good idea to go to the User Manager and add a new user called OrbitNet.
13. Select the user name OrbitNet should use when logging in and press **Add**. The user's name should appear in the **Add Name** field.
14. Click **OK** to return to the Service configuration. The selected user should now appear in the **This Account** field.
15. Enter this user's password in both password fields (**Password** and **Confirm Password**). If your password is blank, simply select the entire field, and press **Delete**.

All done! Click **OK** to return to the Services list. OrbitNet will now load the next time you boot Windows NT. It may take one or two minutes before the service is enabled; give OrbitNet another minute before it starts working.

Chapter 14

Running OrbitNet With AOL As An ISP

CHAPTER 14:
RUNNING ORBITNET WITH AOL AS AN ISP

OrbitNet works seamlessly when America Online is your standard Internet Service Provider, with this caveat: when AOL is your ISP, you cannot use other AOL browsers on your client machines for access. However, you *can* access the Internet with any other Internet applications on any client computers.

Manually Assigning IP Addresses to Client Computers

To begin, you *must* (1) install AOL on the server computer, and (2) verify that you have a working connection to AOL before you can utilize OrbitNet.

Once you've accomplished these tasks, the next step is to assign IP addresses to the computers on your network, verifying that they can "see" the proxy computer. To do so:
Open a DOS Prompt.
Using the "ping" command, ping the IP address of the proxy computer. (See Chapter 4, "Adding TCP/IP to Your Network," for more information about pinging.)

OrbitNet 3.0 includes a Dynamic Host Control Protocol server. More commonly known as a DHCP server, it can assign IP addresses to the computers on your internal network. If you want to use the DHCP server built into OrbitNet, set your client computers to Obtain an IP address automatically and disable DNS. After OrbitNet has been configured, it will then assign IP addresses, Gateway information and DNS information to each system.

You are now ready to install OrbitNet. Run the installation file. Once all files have been installed onto your computer OrbitNet will ask you to restart the system. Once you have rebooted and the operating system is back up, OrbitNet will automatically start the Installation Wizard. The First screen you will see is the one below:

Figure 14-1: The Install Wizard's First Screen.

When it asks you if you are using AOL as your Service Provider, click Yes and then Next. The next screen you will get is this:

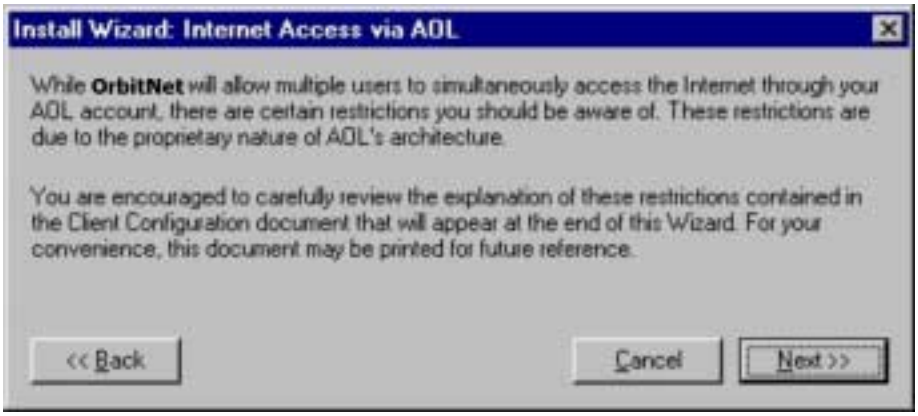


Figure 14-2: Take the time to read the Client Configuration Document.

We strongly suggest that you read the Client Configuration document that will appear at the Wizard's conclusion. It will allow you to fully understand the restrictions in play when using AOL as your ISP. Click the Next to get to this screen:

Figure 14-3: Entering a password with the Install Wizard.

Enter the password for your Default screen name. Each AOL account allows up to five different usernames; you must enter in the password for the original account. Once entered, press Next. At this point

OrbitNet will test your connection out to AOL and verify all information. If, for some reason, something fails, OrbitNet gives you the option of going back and changing the information you entered.

Once OrbitNet checks and okays the settings, you can begin using the program.

Having OrbitNet Assign Client Computer IP Addresses

As mentioned earlier, OrbitNet can assign IP addresses and other pertinent information to the client computers so they can connect through OrbitNet. All you need to do to set this in motion for each individual computer is:

Reboot.

When you return to the operating system, request an IP address. OrbitNet will assign a unique IP address to that computer.

Once you've done this, each client computer's browser can be used as soon as it's opened. OrbitNet will automatically detect connection requests and connect to AOL. Upon connection, the main OrbitNet window will look like this:

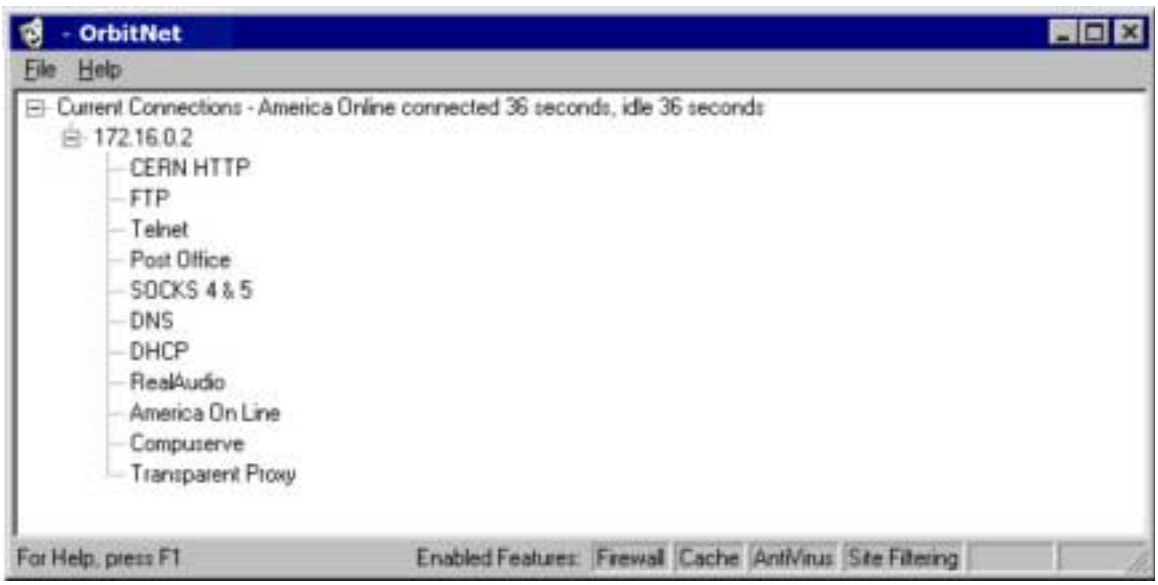


Figure 14-4: What you'll see when you're successfully connected.

You can change any of the connection settings, at any time, by clicking **File/Settings/Dial-Up Settings** on the General Tab.

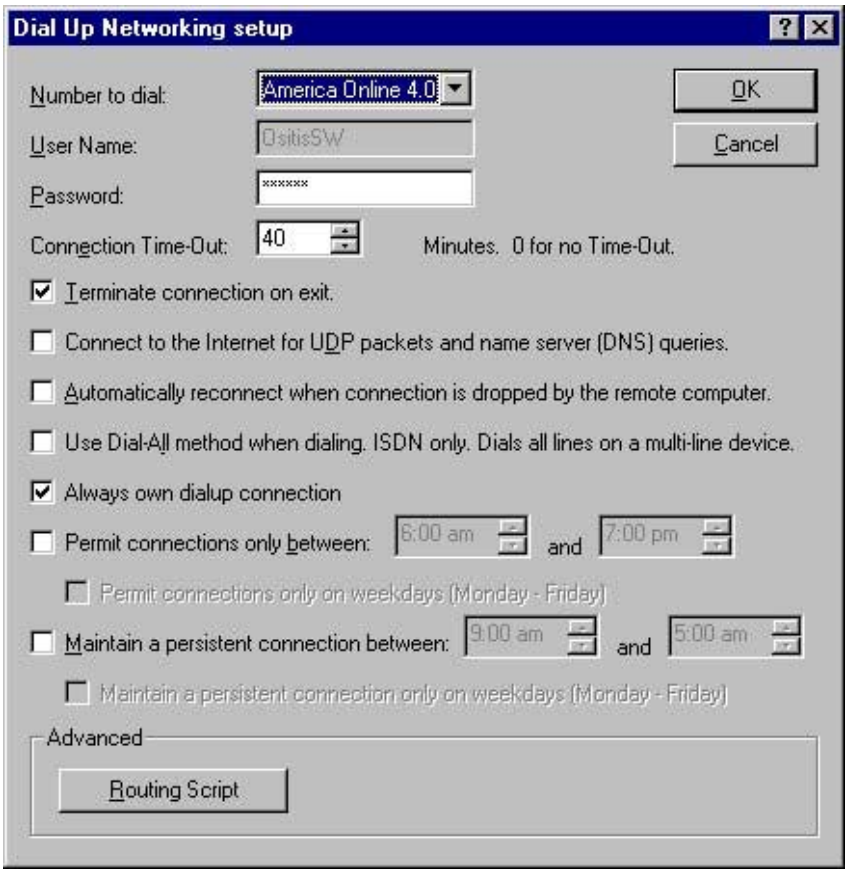


Figure 14-5: A sample installation.

Browser Tricks

With the installation as shown, OrbitNet will automatically dial the chosen AOL connection whenever a client machine tries to access the net, just as it does normally. *However*, the AOL browser on the OrbitNet machine appears as an icon in the taskbar. You cannot click on this icon to see the aol browser and access your account.

If you want to use that browser to access your AOL account while other computers are accessing the net, you must (a) disable the OrbitNet dial-up; (2) start OrbitNet; (3) start the AOL browser; and, finally (4) dial-in yourself via the AOL browser.

The browser will remain up and accessible to your account and OrbitNet—and, therefore, to the client computers. You sacrifice having OrbitNet in charge of the connection, so you'll have to hang it up yourself.

Note toLAN Administrators

When using AOL as an ISP, OrbitNet must be your DNS server. You cannot successfully use a DNS server from another local machine.

APPENDICES

APPENDIX A:
Quick-Start For Users With a Working LAN

IS THIS SECTION FOR YOU?

Yes—*if* you're a network user with a working network (LAN). It will also help immeasurably if you have a good basic knowledge of TCP/IP. If you meet these requirements, you can get OrbitNet up and running immediately by following the instructions below. To fine-tune the program later, refer to "Section IV: Advanced Users," which contains detailed information on advanced configurations, blacklisting, remote administration, caching, protocol setup and a great deal more.

QUICK-STARTING ORBITNET

A Few Tips: (1) We recommend establishing client network settings by choosing "obtain automatically" (see Chapter 9/Section 11 for detailed information). (2) We also recommend that you allow Transparent proxy as the primary connection method (that's the default). (3) The OrbitNet machine itself must be configured on the internal network connection to a static IP address (that's how it knows what addresses to assign to the other computers). (4) Set your client applications to "use the network."

The following quick-start guide assumes that you have the necessary network connections and a working network in place.

For the working network, Microsoft's peer-to-peer network is fine. As for network connections, the OrbitNet computer needs two: (1) an internal connection to the rest of your network; and, (2) an external connection to your Internet Service.

If your Internet connection is via a dial-up device (e.g., an analog modem) then the dial-up adapter will be the second network connection. If you have a direct connection to the Internet (i.e., no dialing involved) you'll have to add a second network card for the connecting device.

Once the network and connections are in place, proceed with the following steps:

1. Add the TCP protocol and IP addresses to each computer. OrbitNet can be installed on its computer as soon as it has an internal IP address assigned. You can add IP addresses to the other computers later if you wish.
    a. If you decide to use OrbitNet as a DHCP server, no problem. It will figure out all the correct settings to assign based upon its internal IP address.
    b. If you already have another computer on your local network acting as a DHCP server, the OrbitNet computer must be exempted from the assignments and given a static IP address (so that you can configure your other applications with a known IP address). Also, be aware that the client machines **must** have the OrbitNet machine as their gateway address; you may have to change the gateway assignment that your DHCP server makes.
2. Install OrbitNet on one computer (the one with an internet connection).
3. Configure OrbitNet with the IP addresses of your service provider's DNS, mail and news servers. These settings will only be used by programs which connect via Classic Proxy, but you might as well put them in now.

4. Note: If you are behind another proxy—including one that your ISP might be using—configure OrbitNet to use proxy cascading.
5. Set your client computers to "Obtain an IP Address Automatically."
6. If you want to use Socks applications (e.g., ICQ, chat or AOL), enable Socks and set up DNS on your local system (if you use "Obtain automatically," you get the DNS settings for free—no other action needed.)
7. For the best security, disable all protocols except TCP/IP on your external connection, and disable file and printer sharing on your external connection. Use non-routable numbers for your interior network. Disable IP forwarding (NT). Ensure that you have correctly designated internal/external IP numbers within OrbitNet.
8. If you have other servers (mail or web) on your local network, it's best to place them behind the firewall. If you place them on the OrbitNet machine, you'll have to do some port changing to avoid port conflicts. These other servers are responsible for their own security.
9. You needn't configure applications unless you want specific applications to route through the Classic proxy (remember: default is to Transparent proxy). To do so, configure your applications by directing them to use a proxy at the IP address of the OrbitNet internal connection.
10. To open a port for others to come in through your firewall, use an Incoming Mapped Port. The destination IP and port must be a machine inside your firewall. Only one destination per port is allowed.

APPENDIX B:
Client Configuration Documents

Two sample Client Configuration documents are shown below. You'll get the first one—the easiest one—with the default settings in OrbitNet.

A Sample Client Configuration Document (NAT/Tproxy ARE Enabled)

This document should help you configure your client computers to use OrbitNet.

The Client Configuration Document is what's called a "dynamic document"—that is, it changes each time you reconfigure OrbitNet. Whenever you reconfigure, check this document to be sure you've accounted for any changes.

This document is intended only as a helpful guide. It may not represent your precise situation.

The IP addresses on your server should be configured such that each network adapter is on its own subnet. If your Internet IP address is 198.13.30.128, then your internal network IP addresses should not start with 198.13.30. We recommend using subnet 90.0.0 (IP addresses 90.0.0.1 through 90.0.0.255) on your internal network, because those addresses are not routable.

In order to configure each of the computers on your network, please follow these instructions on each of your client PCs:

** From the desktop, right click on "Network Neighborhood."*
** Click on "Properties."*
** In the "Configuration" tab, click once on "TCP/IP → {your Ethernet card}" and then click on "Properties."*
** In the "Configuration" tab, select "Obtain an IP address automatically."*
** Click the "OK" button to close this dialog box, click "OK" to close the "Network" dialog box.*
** At the prompt, click "OK" to restart your computer for the settings to take effect. Click "OK" to reboot.*

Since OrbitNet will be managing your network configuration and assigning addresses to the other computers on the network, we recommend that you leave this machine running at all times.

If your computer has a power-save mode, it should be configured to shut off your monitor and hard drives after a desired idle time. You can also have the CPU go into a "low power" mode.

It is not recommended that you allow the machine to "suspend" or "enter sleep mode."

If you prefer to configure your computers manually please follow these instructions on each of your client PCs:

** From the desktop, right click on "Network Neighborhood."*
** Click on "Properties"*
** In the "Configuration" tab, click once on "TCP/IP → {your Ethernet card}," and then click on "Properties."*
** Specify an IP address from 90.0.0.1 through 90.0.0.255, excluding 90.0.0.6.*
** Specify a subnet mask of 255.255.255.0.*
** Set the DNS server to 90.0.0.6.*
** Give each computer a unique name on your network.*
** Select an appropriate domain name that will not conflict with names used on the Internet.*
** If you are using other internal DNS servers, not recognized by OrbitNet, then those should also be added to the DNS list on your client computers.*
** Leave all other TCP/IP settings blank, unless your particular situation requires specific values.*

This next sample shows the Client Configuration document you'll see if you have disabled the NAT and Transparent Proxy functions in OrbitNet.

To the beginning networker it may appear as a daunting and confusing number-jumble; however, the underlying principle is pretty simple. It boils down to this: Any mail or news application or browser you use must first be instructed to use a proxy and then be given directions for finding that proxy. The "instruction" is given merely by clicking a setting; directions are established by giving the IP address of the OrbitNet machine.

For instance, in your browser's News settings, where you formerly listed the IP address of your news server, you'll now enter the IP address of the OrbitNet machine. OrbitNet itself will have the news server's IP address. OrbitNet thus looks like a news server to your application, and like a news browser to your service provider.

The sample document below assumes that all protocols are enabled.

Note: The Client Configuration document is a text file and, like all text files, contains no formatting. For this reason the document below, intended as a sample, also contains no formatting.

A Sample Client Configuration Document (NAT/Tproxy Are NOT Enabled)

This document will assist you in configuring your client computers to use OrbitNet. We will assume throughout that your internal subnets use a subnet mask of 255.255.255.0. If this is not the case, then some of the settings may be incorrect.

The Client Configuration Document is what's called a "dynamic document"—that is, it changes each time you reconfigure OrbitNet. Whenever you reconfigure, check this document to be sure you've accounted for any changes.

This document is intended only as a helpful guide. It may not represent your precise situation.

The IP addresses on your server should be configured such that each network adapter is on its own subnet. If your Internet IP address is 198.13.30.128, then your internal network IP addresses should not start with 198.13.30. We recommend using subnet 90.0.0 (IP addresses 90.0.0.1 through 90.0.0.255) on your internal network, because those addresses are not routable.

The following section of the document describes how to configure network settings on your client computers. In this example, there is only one network adapter on the server. If there were several network adapters, the remainder of the document would repeat for each section.

For computers connected to subnet 90.0.0—i.e., those directly connected to server IP address 90.0.0.2:

*** IP address configuration:*
** Use IP addresses from 90.0.0.1 through 90.0.0.255, excluding 90.0.0.2*
** Use a subnet mask of 255.255.255.0.*

In the following example, the user has enabled the DNS proxy, allowing name services to be available to the network's computers. If you do not enable DNS services, this section of the document won't be present.

*** DNS configuration:*
** Use a DNS server of 90.0.0.2.*
** Give each computer a unique name on your network.*
** Select an appropriate domain name that will not conflict with names used on the Internet.*
** If you are using other internal DNS servers not recognized by OrbitNet, they should also be added to the DNS list on your client computers.*

** Leave all other TCP/IP settings blank, unless your particular situation requires specific values.

The next section of the document describes how to configure applications on the client computers. If you don't have the necessary protocols enabled, some applications may not appear in the Client Configuration document. For instance, if you don't have the Socks proxy enabled, then the mIRC description will not be present.

*** Applications:*

** Netscape 3.0: Under Network Preferences in the Options menu, select the Proxies tab. Select Manual Proxy Configuration. Press View and enter the following information:*

FTP Proxy: (leave blank)
FTP Proxy Port: (leave blank)
Gopher Proxy: (leave blank)
Gopher Proxy Port: (leave blank)
HTTP Proxy: 90.0.0.2
HTTP Proxy Port: 80
Security Proxy: 90.0.0.2
Security Proxy Port: 80
WAIS Proxy: (leave blank)

WAIS Proxy Port: (leave blank)
SOCKS Host: 90.0.0.2
SOCKS Host Port: 1080

No Proxy For: Enter the domain name you selected in your IP configuration.

Since you are using SOCKS, you should enter the real name of your mail server if you are using Netscape for mail. Netscape will use the SOCKS proxy to access mail. This way each client can also access a different mail server.

** Internet Explorer 3.0: Under Options in the View menu, select the Connection tab. In the Proxy Server section, check the Connect Through Proxy Server box, and press the Settings button.*

Enter the same proxy information described under Netscape configuration. Do not check the box to use the same proxy for all protocols.

** In your Mail client:*

Set the SMTP server to 90.0.0.2. Set the POP3 server to 90.0.0.2.

** In your IMAP4 client:*

Set the IMAP4 server to 90.0.0.2.

** In your News client:*

Set the News server to 90.0.0.2.

** CuteFTP: Under Options from the FTP menu, select the Firewall tab.*

Enter 90.0.0.2 as the host, and 21 as the Port. Select the User@Site proxy type. Check the box to enable firewall access

** WS_FTP: Under Session Properties, select the Firewall tab.*

Enter 90.0.0.2 as the Host Name. Enter 21 as the Port. Check the box to Use Firewall Select the "USER with No Logon" Firewall Type.

** mIRC: Select Setup from the File menu, and select the Firewall tab.*

Check the box labeled "Use SOCKS firewall" Enter 90.0.0.2 as the Hostname Enter 1080 as the Port

** RealAudio: Select Preferences from the View menu, and select the Proxy tab*

Check the box labeled "Use Proxy" Enter 90.0.0.2 as the RealAudio Proxy Enter 1090 as the RealAudio Proxy Port Enter 90.0.0.2 as the HTTP Proxy Enter 80 as the HTTP Proxy Port.

APPENDIX C:

Configuring Browsers to Work with OrbitNet (Classic Proxy or Transparent Proxy)

Configuring a browser to use the Classic Proxy connection method

Configuring Netscape 4.0

1. Select **Preferences** from the Edit Menu. Under Category, select **Advanced** and then **Proxies**.
2. Select **Manual Proxy Configuration** and click **View**.
3. Under **HTTP** enter the internal IP address of the computer running OrbitNet. Enter 80 under **Port**. Be sure not to include extra characters (such as a leading space) along with the IP address.
4. Under **Security** enter the internal IP address of the computer running OrbitNet. Enter 80 under **Port**.
5. Under **FTP** enter the internal IP address of the computer running OrbitNet. Enter 80 under **Port**.
6. Do not enter anything under **Gopher** or **WAIS**. Leave Socks blank until you have enabled DNS (described elsewhere).
7. Okay your way back out. You do not have to restart Navigator for the changes to take effect.

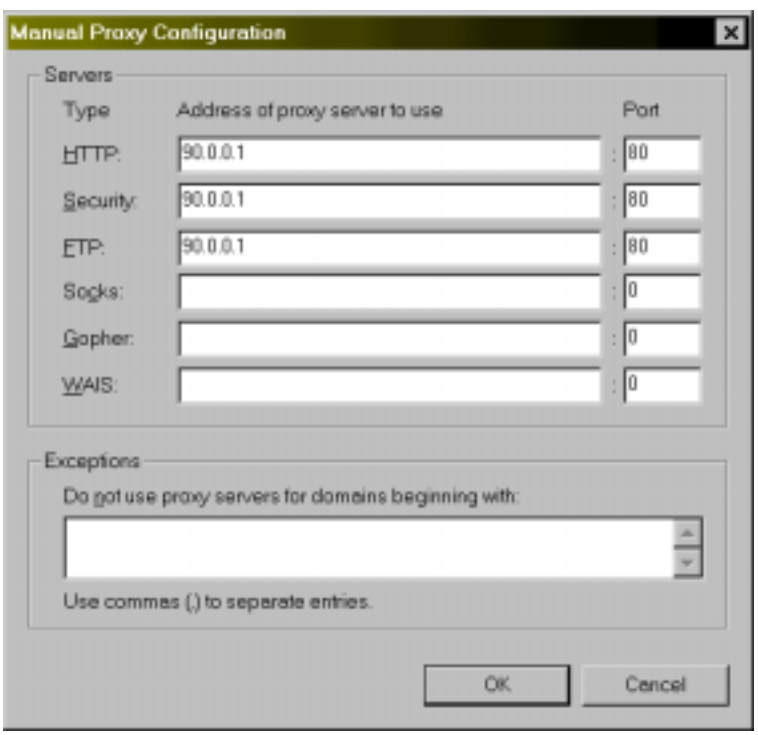


Figure C-1: Configuring the Netscape 4.0 browser to work with the Classic Proxy.

Configuring Netscape 3.0

1. Select **Network Preferences** from the Options Menu.
2. Select the Proxies Tab.
3. Select **Manual Proxy Configuration**, then **View**.
4. In the **HTTP Proxy field**, enter the IP Address of the OrbitNet server. Be sure not to have any extra characters (such as a leading space) along with the IP address. Enter the port number specified for the CERN proxy in the OrbitNet Properties dialog (probably the default port 80).
5. Enter the same information in the Security Proxy section. See SSL.
6. Enter the same information in the FTP Proxy section.
7. Do not make an entry for **Gopher** or **WAIS**. Leave the Socks entry blank until you have enabled DNS (described elsewhere).
8. Click **OK** in the Manual Proxy Configuration dialog.
9. Click **OK** in the Preferences dialog.
10. You do not have to restart Navigator for the changes to take effect.

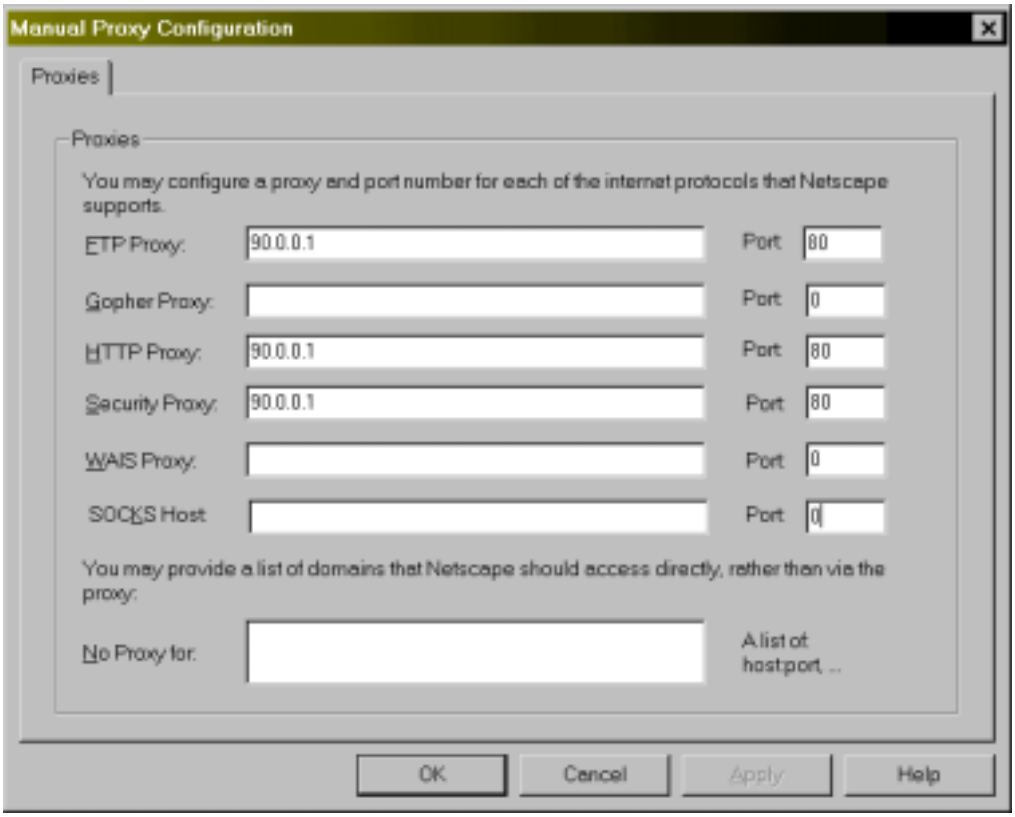


Figure C-2: Configuring the Netscape 3.0 browser to work with the Classic Proxy.

Configuring Internet Explorer 5.0

1. Select **Internet Options** from the Tools Menu and then select the Connections Tab.
2. Select **Connect to the Internet** using a local area network.
3. Select **LAN Settings** and check the box entitled **Use a proxy server**.
4. Check the box labeled **Bypass proxy server for local (Intranet) addresses** if you wish to do so.
5. Click **Advanced**.
6. Under HTTP enter the internal IP address of the computer running OrbitNet and the OrbitNet CERN proxy port (probably the default port 80).
7. Under **Secure** enter the internal IP address of the computer running OrbitNet and the OrbitNet CERN proxy port.
8. Under FTP enter the internal IP address of the computer running OrbitNet and the OrbitNet CERN proxy port.
9. Do not enter anything under **Gopher, a**nd leave Socks blank until you have enabled DNS (described elsewhere in the manual).
10. Make sure **Use the same proxy server for all protocols** is *not* checked.

Okay your way back out. You do not have to restart IE in order for the changes to take effect.

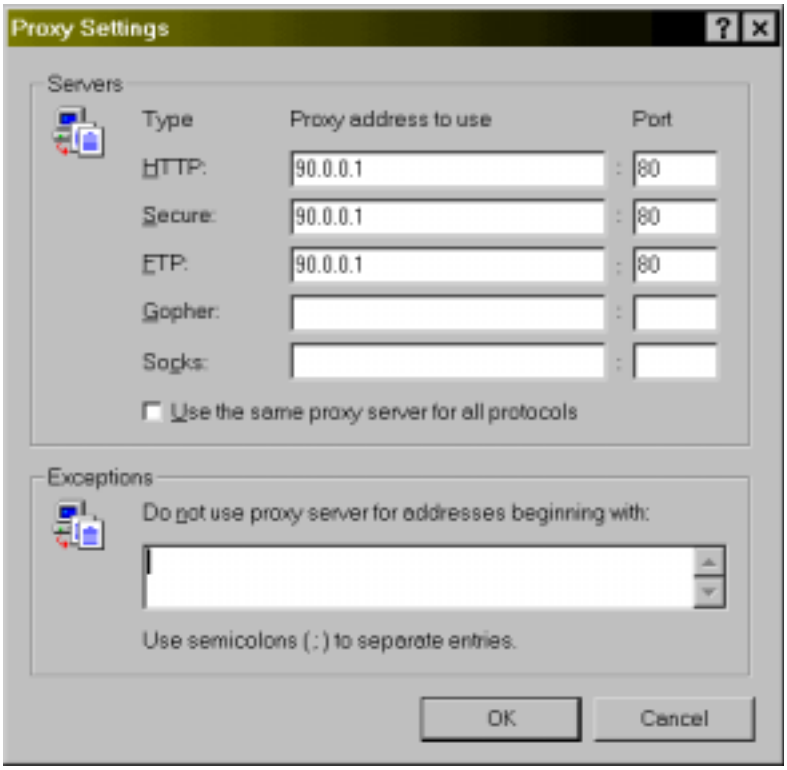


Figure C-3: Configuring the Internet Explorer 5.0 browser to work with the Classic Proxy.

Configuring Internet Explorer 4.0

11. Select **Internet Options** from the View Menu and then select the Connection Tab.
12. Select **Connect to the Internet** using a local area network.
13. Under **Proxy Server** check the box labeled **Access the Internet using a proxy server**.
14. Check the box labeled **Bypass proxy server for local Intranet addresses** if you wish to do so.
15. Click **Advanced**.
16. Under HTTP enter the internal IP address of the computer running OrbitNet and the OrbitNet CERN proxy port (probably the default port 80).
17. Under **Secure** enter the internal IP address of the computer running OrbitNet and the OrbitNet CERN proxy port.
18. Under FTP enter the internal IP address of the computer running OrbitNet and the OrbitNet CERN proxy port.
19. Do not enter anything under **Gopher**, and leave Socks blank until you have enabled DNS (described elsewhere in the manual).
20. Make sure **Use the same proxy server for all protocols** is *not* checked.
21. Okay your way back out. You do not have to restart IE in order for the changes to take effect.

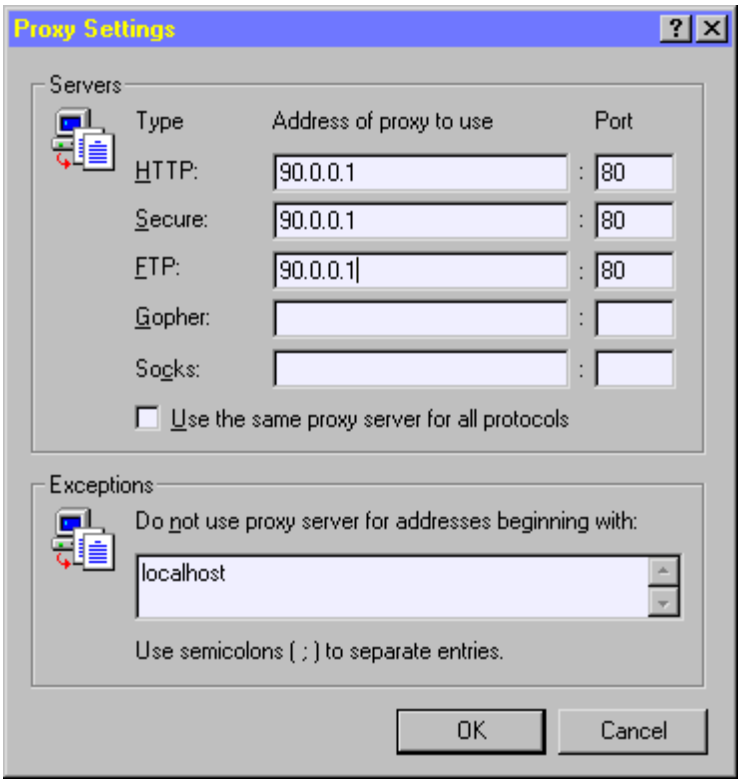


Figure C-4: Configuring the Internet Explorer 4.0 browser to work with the Classic Proxy.

Configuring Internet Explorer 3.0

1. Connect to a web page (Internet Explorer cannot be configured until it is has successfully read a web page). If you're having trouble at this stage, specify the address **c:\windows\system\blank.htm**. That file is standard in Windows installations, and provides a fast page without an actual connection to the Internet.
2. Select **Options** in the View Menu.
3. Select the **Connection** Tab.
4. Check **Connect to the Internet through a proxy server**.
5. Click **Change Proxy Settings**.
6. Under HTTP, type in the IP address of the OrbitNet machine, and the OrbitNet CERN proxy port (probably the default port 80).
7. In the FTP line of the list of servers, enter the IP Address of the OrbitNet server in the first space and the port number of the CERN proxy, probably 80.
8. In the Security (SSL) line of the server listings, enter the IP Address of the OrbitNet server in the first space, and the port number of the CERN proxy, probably 80, under the port listings.
9. Do not put anything in the Gopher listing. Leave the Socks listing blank until you enable DNS on the local system.
10. Press **OK** for the Proxy Settings dialog.
11. Press **OK** for the Options dialog.
12. You don't have to restart IE for the changes to take effect.

Configuring your browsers to work through Transparent Proxy

For your browsers to use Transparent Proxy from a specific client computer, that machine *must* have a Gateway assigned to the network card. The Gateway address *must* be the OrbitNet internal IP address if the client machine is set to "obtain automatically," then it will get the correct information from the OrbitNet DHCP server automatically.

Directions follow for specific browser versions.

Configuring Netscape 4.x (4.0, 4.5, 4.6)

1. Go to **Edit/Preferences/Advanced/ Proxies**.
2. Enable the option "Direct connection to the Internet," as shown below:

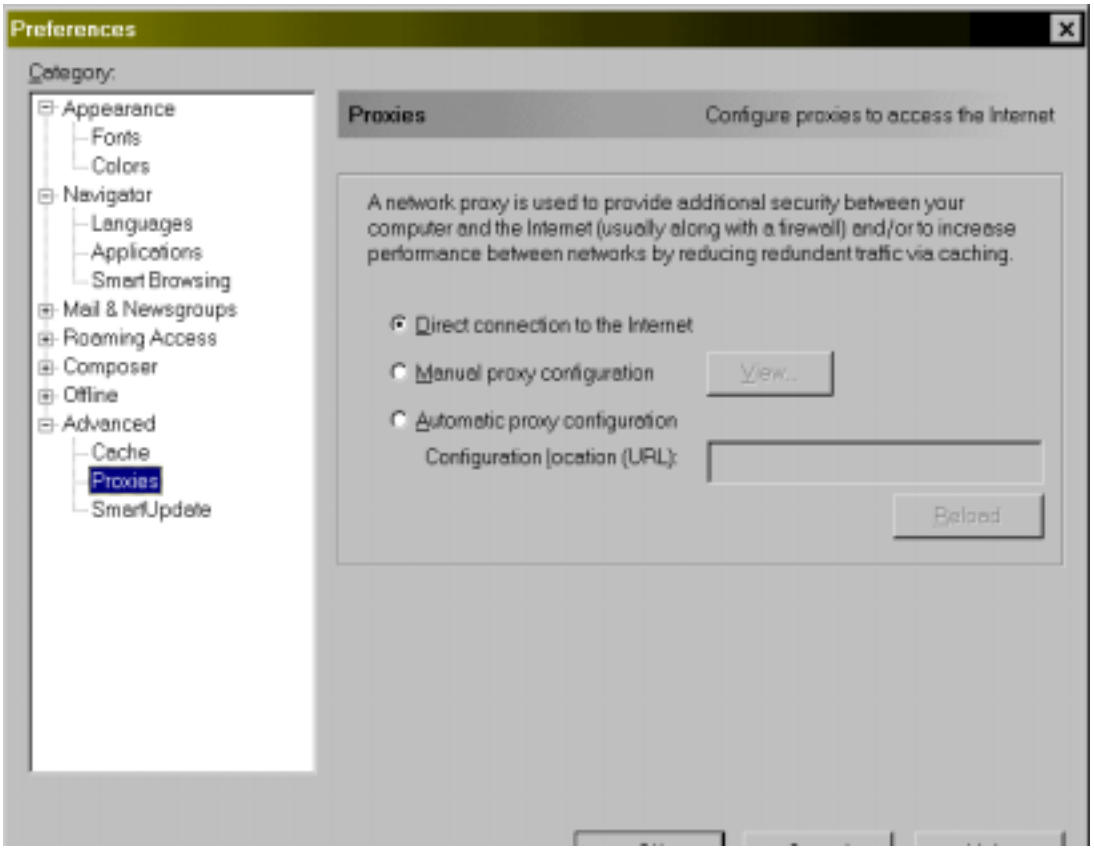


Figure C-5: Configuring Netscape 4X browsers to work with OrbitNet.

Configuring Netscape 3.0

1. Go to **Options/Network Preferences/Proxies**.
2. Choose the option "No Proxies," as shown below:

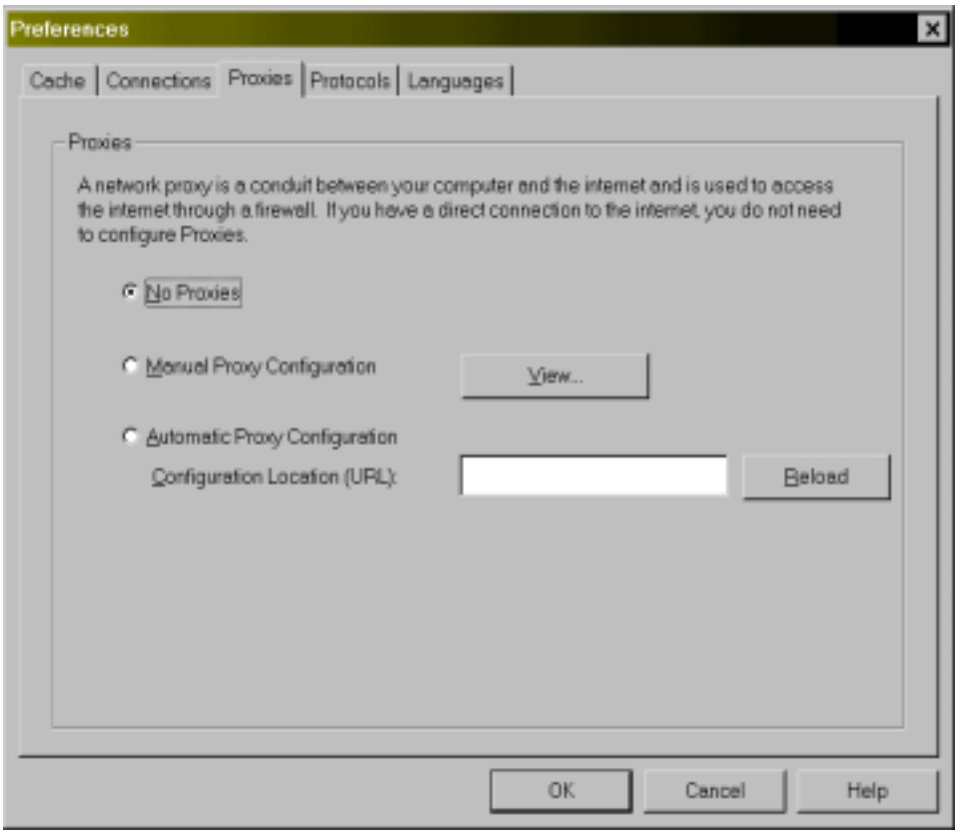


Figure C-6: Configuring Netscape 3.0 browsers to work with OrbitNet

Configuring Internet Explorer 5.0

1. Go to **Tools/Internet Options/Connections**. \
2. Choose the option "Never dial."
3. Click **LAN Settings** and uncheck any checked boxes, as shown below.

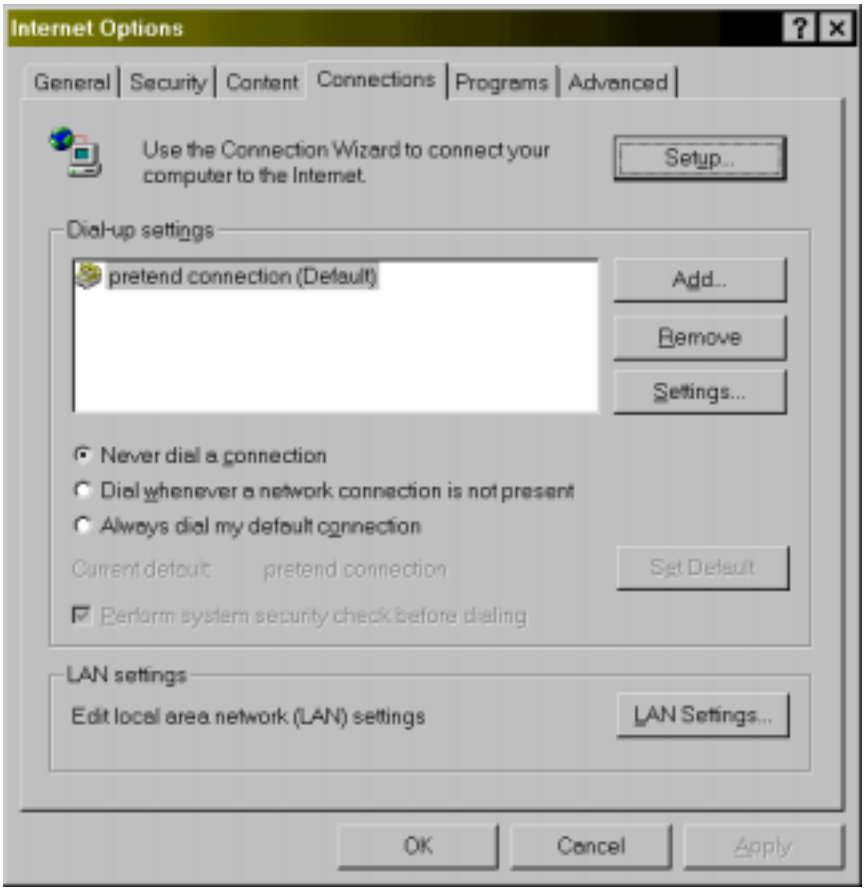


Figure C-7: Configuring Internet Explorer 5.0 browsers to work with OrbitNet.

Configuring Internet Explorer 4.0

1. Go to **View/Internet Options/Connections**.
2. Enable the option "Connect to the Internet using a local area network," as shown below:

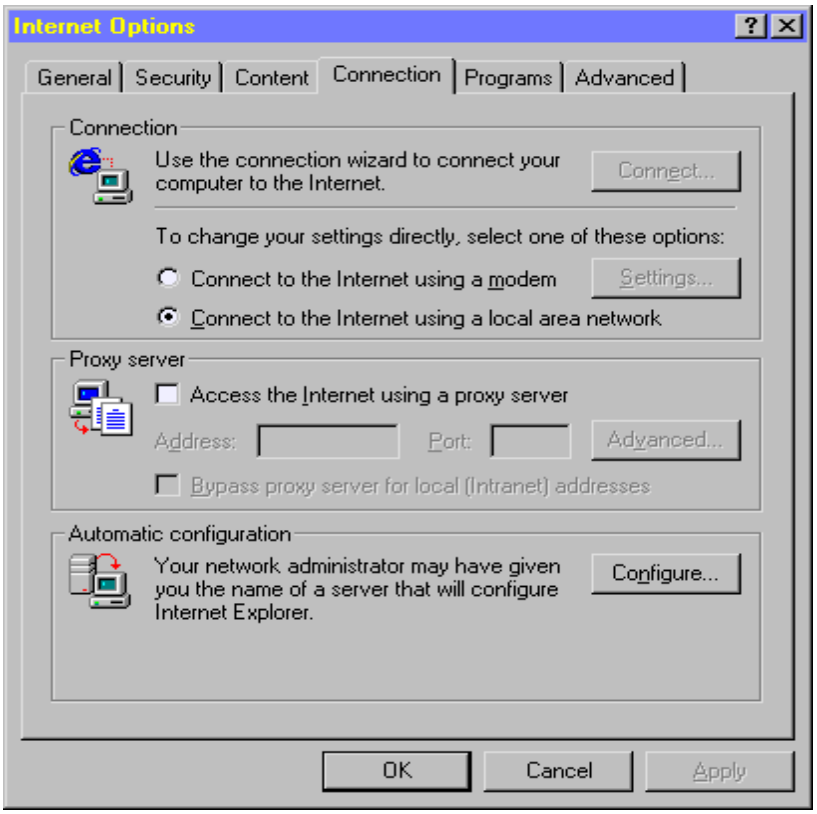


Figure C-8: Configuring Internet Explorer 4.0 browsers to work with OrbitNet.

APPENDIX D:
Glossary

Address: A unique name which identifies the sender or receiver of transmitted data. This name can be an email address, an address in your computer's memory, or a network address. As a networker, you'll often run across IP addresses. Also see IP Address.

Administration IP: Some OrbitNet features can be configured remotely. Although remote administration is a convenience for the network administrator, it adds some security risk. Up through version 2.0, OrbitNet permits you to limit such administration to a specific IP address. If the Administration IP value is set to 0.0.0.0 or left blank, administration can be done from any computer behind the firewall. To disable remote administration altogether, set the value to an invalid IP address such as 127.0.0.0. In version 2.1, Administration IP was superceded by Administration Password.

Administration Password: Beginning with version 2.1, access to remote administration is set by password rather than by IP address. Once the password is set in Advanced Configurations, the password is required to change any configurations. This applies to all computers on your local network, including the OrbitNet computer itself. The password will also be required to override dialing time restrictions.

Aliases: Computers on the Internet can be referred to by names, which can be translated to an IP address on the serving computer. Several names, however, can point to a single computer. In such a case one name is specific to the computer, and the others are aliases.

Applet: A small application. When you double click on an icon, it's usually an applet.

Browser: Software used to navigate the World Wide Web. Netscape and Internet Explorer are examples of browsers.

Cache: A holding area for often-accessed information and files, it is commonly used in computers to speed up operations. The average desktop computer has several caches for the CPU, hard disk, and other devices. OrbitNet has two caches, the Name Cache and Cache. The name cache holds the results of DNS lookups and is not configurable by the user (though the user can delete the cache if desired). The cache available through the user interface is a cache of WWW documents and files.

Cascading: It is sometimes necessary to secure a network within another network, but still maintain the ability to access the Internet behind the second firewall. OrbitNet allows this with Proxy Cascading, which forwards requests from OrbitNet to another proxy server. Assume, for example, that OrbitNet is located between Network A and Network B. Network B is connected to the Internet through a second OrbitNet or other proxy firewall.

Net A ¾ ® Cascading OrbitNet ¾ ® Net A ¾ ® Second Firewall ¾ ® Internet

Using proxy cascading the appearance to the users in Network A will be as though Network B were not even there.

Net A ¾ ® Cascading OrbitNet ¾ ® Internet

In reality all requests are still proxied through the external firewall, but users of Network A only have to configure their systems to proxy to the cascading OrbitNet.

Cascading can be configured in the Properties dialog with the Cascading Port and Cascaded Proxy IP address. Cascaded proxies can be nested as deeply as desired, but each nesting degrades performance.

Proxy cascading is currently only supported for HTTP and Secure Sockets requests. Other protocols, such as Mail and News, can be supported indirectly by pointing to the external proxy as the server. Telnet can be done by logging into the first proxy, connecting to the second proxy, and then outside. Cascading

does not provide access to the intermediate network, unless the next firewall specifically provides such access. In practice this access is usually provided. You will always have this access when OrbitNet serves as the external firewall.

Cascading Port: OrbitNet can be run on a subnet behind another proxy server, providing an additional layer of security for that subnet. In this case computers outside the subnet will not have access to the computer inside; computers inside can communicate with computers beyond a second firewall. Also see Proxy Cascading for more information on cascading.

This value must be set to the port number of the next proxy server. If left blank (or invalid), proxy cascading is disabled. The Cascaded Proxy IP address must also be configured for Proxy Cascading to function. Allowed values are from 1 through 32000.

Cascading Proxy IP Address: OrbitNet can be run on a subnet behind another proxy server, providing an additional layer of security for that subnet. In this case computers outside the subnet will not have access to the computer inside, but computers inside the subnet can communicate with computers beyond a second firewall. Also see Proxy Cascading for more information. This value must be set to the numeric IP address of the next proxy server. If the Cascading Port is left blank, proxy cascading is disabled.

CERN: Also known as the European Laboratory for Particle Physics, CERN is the birthplace of the World Wide Web . The CERN group, including Tim Berners-Lee, known as the father or the World Wide Web, devised the HTTP protocol and the protocols used to proxy with it. The CERN proxy protocol includes a method to proxy HTTP, FTP and other protocols through a HTTP proxy server. This is the proxy protocol used by Netscape's Navigator® and Microsoft's Internet Explorer®.

CERN Proxy Port: The port on which OrbitNet listens for connection requests from the other computers on your local network. OrbitNet will support the CERN Proxy specification on this port, including CERN Proxy protocol for HTTP *and* FTP. A CERN proxy server usually listens for connections on the HTTP port and will proxy other protocols using the HTTP protocol. Hence, it only listens for connections on a single port. This is the proxy protocol used by Netscape's Navigator® and Microsoft's Internet Explorer®. The range of valid values is from 1 through 65K.

Client: A network computer that is not a server. The computers on your network that don't run OrbitNet are all clients. Also see Server.

Connectoid: The name that Microsoft uses for a related group of network settings. Each group, represented by an icon in your Dial-Up Box, defines a different dial-up connection and its settings.

Connection: A TCP/IP connection is a link between two IP addresses. An application can listen for a connection on a specific IP address and port number. Other computers can then establish a connection to that application by connecting to the specific IP address and port number. If the receiving computer is willing to establish a connection, it will accept the request, completing the link.

Cross-Over Cable: An Ethernet cable in which the wires cross over to different pins in the connector on each end of the cable (instead of going straight through, like a standard cable). As an example, in a two-computer network it's possible to avoid using a hub by connecting directly from one network card to the other with a cross-over cable. Note, however, that this won't work if one of the computers has a dial-up adapter, because the dial-up adapter and direct cable connection software use some of the same underlying drivers.

DHCP (Dynamic Host Configuration Protocol): Used by one computer—a DHCP server —to assign an IP address to a DHCP client. Most dial-up connections to ISPs use this; each time you call your provider it assigns a new IP address to your Dial-Up Adapter from a general pool of numbers. If you use DHCP on your local network, the OrbitNet computer's internal address must be exempted from the assignments, as all of the client applications must be configured with a static IP address for the proxy server.

Dial-Up Adapter: A network device for connection through the public phone system. It is distinct from Dial-Up Networking, which handles modems and passwords; the Dial-up Adapter is a device driver at the same network level as a network card, and is listed and configured on most computers in the same place as network cards. A Dial-Up Adapter can have a permanent (static) network IP address configured, or it can have a different (dynamic) network IP address assigned by the ISP each time you connect.

Dial-Up Networking: OrbitNet can automatically connect to the Internet when required by using Dial-Up-Networking in Windows 95 or Windows NT. Microsoft's DUN is the only dial-up program supported.

DNS (Domain Name System): DNS is the Internet protocol used to translate names, such as **www.OrbitSat.com** into numeric IP addresses. This protocol is required to use the Socks proxy in OrbitNet. Many Java applets will also require DNS on your local network.

DNS Spoofing: DNS Spoofing is similar to IP Spoofing with this exception: instead of pretending to be a different IP address, a name lookup is faked to return an incorrect IP address. This is a fairly common way for hackers to gain access to proprietary information, including credit card numbers and bank accounts. Each time the computer looks up a name, such as **www.orbisat.com**, it makes a request to a domain name server to translate the name to a numeric IP address. If the DNS server doesn't know the answer, it asks another DNS server; that's part of the protocol. At any point a hacker can intercept the request to provide a fake response which points to their own IP address. When a request is made to the returned IP address, it goes to the address specified by Joe Hacker instead of the one you originally asked for.

OrbitNet provides two types of protection against this type of attack:

Reverse Name Lookups are used to verify that the IP address really represents the requested name. This feature is enabled by the *Verify IP Address* option in the Properties dialog. If a name and IP address fail the RNL test, OrbitNet returns an error message to the browser originating the URL request (beginning with version 2.1).

Name Caching remembers names that have been verified, reducing the number of name requests and, hence, reducing the risk of retrieving a false response. The name cache is lost each time you quit the program.

Blacklisting can be used to prevent subsequent requests to an IP address or domain names that have been spoofed.

Domain: A logical grouping of computers. Most simple local networks have only one domain.

Dynamic IP Address: An IP address assigned automatically by another computer. Though assigned from a pool, the exact IP address that will be assigned is not known in advance. As used by ISPs, the IP address is assigned while connecting to your ISP; it is returned to the pool as soon as you disconnect.

Ethernet: A network protocol standard that permits computer data, audio, and video information to be carried across a network. Ethernet was originally developed by Xerox.

Ethernet Hub: When you need to connect more than two computers together in an Ethernet network, use a hub. Each computers network card connects to the hub.

FTP (File Transfer Protocol): The name of the Internet protocol used to transfer files between computers. Although HTTP can also be used to receive files, FTP allows users to browse directories and upload/download files to a remote computer. FTP servers usually listen for connections on port 21.

Gopher: An earlier version of the World Wide Web with no graphics and a less flexible menu system.

Hop: A journey from one computer host to the next is called a hop. An average Internet communication averages a dozen hops, although increasingly

Host: Any machine supporting a network connection. A PC with one or more network cards is a Host.

Host Name: Since IP addresses are not easy for humans to remember, users can identify computers by names instead. The TCP/IP protocol can convert a name into an IP address using a process called name resolution. Names are organized in a hierarchical structure with a network name, a domain name, and a computer name. For example in the name WWW.ORBISAT.COM, COM is the network name, ORIBIT is the domain name and WWW is the computer name. Multiple names can point to the same computer, using aliases.

HTML (HyperText Markup Language): A document-encoding format that allows documents to be written with links to other documents, images and bookmarks. This format is used in the World Wide Web to format documents in a device- and application- independent manner.

HTTP (HyperText Transfer Protocol): The name of the client-server based protocol used by the World Wide Web, it allows computers to retrieve documents from other computers. The World Wide Web uses, but is not limited to, HTML documents. HTTP servers usually listen for connections on port 80.

Hub: A centrally-located device for connecting wires of a star-shaped topology network. Hubs are a bit like "traffic cops" who manage network data.

ICMP: an acronym for Internet Control Message Protocol. This protocol is used pass information and error messages between routers on the Internet. It is also used in the Ping and Tracert utilities. ICMP is not supported by OrbitNet.

IP Spoofing: Manipulating packet addresses so that the packets appear to be from somewhere else. Used by hackers (usually by replacing the source IP address with one of their choosing) to make the packets they send appear to come from a trusted source, thereby gaining privileged access to other networks and computers. There are blind attacks, usually meant to disrupt the target computer, or non-blind attacks to gain information or use the target as a stepping-stone to the next target.

IMAP 4: A new post office protocol similar to POP 3. It offers better mail retrieval capabilities than POP 3 services, resulting in generally faster access. If you don't know what it is, you probably don't need it.

Internal IP Address: The IP address OrbitNet uses to listen for connection requests from other computers on your local network. This value should be set to the IP address directly connected to the internal network. OrbitNet only accepts connections on the internal IP address unless an incoming port has been specifically configured by the user. All other connections are refused.

InterNIC (Internet Network Information Center): A quasi-official body that provides Internet services such as domain name registrations.

Intranet: An Intranet is a network of computers connecting all computers in an organization. It is generally not accessible to computers outside the organization.

IP Address A 32 bit number, usually expressed as four numbers separated by periods, such as 192.0.0.12. It is a unique number in which the most significant bits define a subnet.

IPX-SPX: A routable network protocol used by Novell Networks. It is suitable for small to large local networks.

IRC (Internet Relay Chat): A popular chat protocol used for text conversations on the Internet. Users can connect to a chat server with several "rooms." They can enter a room and talk to others in the same room in real time. Many users can participate at once. To use IRC through OrbitNet, you must enable the Socks and DNS proxies, and configure your IRC client to use the Socks protocol to connect to the server.

ISP: A commonly used acronym for Internet Service Provider. ISPs can be large like American Online, or they can be small and local. See "Service Provider."

Java: A programming language and environment invented by Sun Microsystems. It provides for programs that are (1) independent of the operating system on which they run; and (2) easily retrieved across a network. Java applications and "applets" are becoming more common on the web.

Java uses the HTTP protocol to exchange information between computers. Many Java applets will also require that DNS be set up on your local network.

LAN: Short for Local Area Network, a LAN is a group of computers connected to share resources and information.

Logging IP Address: OrbitNet can log all activity that takes place through the proxy server. Logging is done by establishing a connection between OrbitNet and the OrbitNet sample logging application, ProxyLog. The connection is established when OrbitNet is started or when it is specifically requested through remote configuration. If OrbitNet is unable to connect to a logging application, it continues to function with logging disabled. For security reasons, OrbitNet does *not* listen for a connection from the logging application. The ProxyLog application listens for a connection on the port number specified here and writes all logging information to the screen as well as to a log file, if requested. Although it is possible to send logging information outside of the intranet, this is not recommended since it would be a significant security risk.

This parameter, along with the Logging Port, tells OrbitNet the location of a logging application, which can be located anywhere on the network (including the OrbitNet machine itself). This value must be a valid IP address and should be somewhere within the intranet for security. The Logging Port must also be specified for logging to be enabled. Also see **Logging Port** for more information on logging.

Logging Port: This parameter, along with the Logging IP address, tells OrbitNet the location of a logging application, which can be located on the same machine as OrbitNet. Placing the logging application on the same machine as OrbitNet can reduce the bandwidth used for logging, but may open a security hole if the connection has not been established. If this value is left blank (or invalid) then logging will be disabled. The range of valid values for this setting is from 1 through 65K.

Mail: Electronic mail is transmitted over the internet using two protocols: SMTP and POP3. IMAP4 is also occasionally used instead of POP3. When you send electronic mail, your e-mail client application first connects to its designated SMTP server, gives it your e-mail name, the destination name, and the text of the document you're sending. The SMTP server then reads the text behind the @ in the destination address, connects to the POP3 server at that location, and gives it the transmitted message.

The user on the other end later opens another e-mail application, which connects to the same POP3 server to determine if any mail has arrived. The server responds with a message stating that mail has arrived and the e-mail client retrieves the mail.

Essentially, the SMTP server acts as a delivery agent to assist in sending mail. An SMTP server may transfer the mail to another SMTP server before it stops at a POP3 server.

The POP3 Server is merely a post office box, holding mail until a user wants to read it. This allows mail to be delivered to a computer not currently on-line, because when the user *does* come on-line, the mail is waiting. The POP3 server is always on-line.

Mapped Ports: (maybe just a one-liner with a pointer to the chapter).

Modem: Short for modulator/demodulator, a modem is hardware that lets your computer make connections to other computers over telephone lines.

Multi-homed host: A multi-homed host is a computer residing on two different subnets with at least two IP addresses.

NAT (Network Address Translation): NAT is a simple, efficient technology used for connecting one Internet address to another. NAT translates all IP addresses used on an internal network into a different return IP address for the Internet. It rewrites the addresses in the header of each outgoing (network-to-

Internet) packet to reflect a new address and keeps track of this change so it may route incoming packets to the correct machine.

NetBios (Network Basic Input/Output System): Developed by IBM as part of a client/server communication process, it has become a widely accepted standard for simple networks.

NetBEUI (NetBios Extended User Interface): A network protocol designed for systems with Netbios support. It is the protocol used in Windows for peer-to-peer networking. It is not a routable protocol, and is suitable only for small networks.

NIC: a commonly used acronym for Network Interface Card. This is not the same as the nic in InterNIC, which stands for Network Information Center.

NNTP (Network News Transfer Protocol): The protocol used for Internet News. The news services, also known as UseNet groups, are essentially bulletin boards on the Internet, allowing Internet users to exchange ideas and have discussions. Some news groups are read only, and provide actual news as well. Reuters and Associated Press, for instance, publish much of their news in news groups.

Non-Routable IP addresses: Certain special IP addresses have been set aside for specific uses, including testing and local networks. These have been designated as non-routable numbers, which means that Internet routers will not pass packets with these addresses. Among these addresses are 10.x.x.x, 90.0.x.x, 172.16-31.x.x, and 192.168.x.x.

Ping: A simple tool that allows you to check your TCP/IP connection to see if it's working properly. To ping, open a DOS window while online. Type ping.www.Orbitsat.com. If everything's working, you'll receive feedback from ping.

POP3 (Post Office Protocol): The protocol used to receive mail stored in a "post office." Another way of explaining it: POP3 is the "language" used by your email program when it "talks" to your ISP to retrieve your mail. Usually mail sent using SMTP ends up in a POP3HID_POP3 server where it can be eventually retrieved by a user. Mail may travel through multiple SMTP server before reaching a post office.

Port Number: Each time a computer accepts or listens for a connection on a specific IP address, it uses a Port Number. The port number distinguishes various connections or network processes on a computer. Although all connections have a unique port number, the number is usually used to allow one process to connect with another specific process on a computer. HTTP, for instance, uses port 80 to listen for connections. By having a port number as well as an IP address, many processes can be listening for connections on a single computer. Port numbers in the range 1 through 1024 are designated by Internet governing bodies as standardized port numbers for common applications such as mail, news, and WWW.

Protocol: A formal set of conventions used to carry out and complete a task. Protocol standards are established by agreement between governing organizations in the computer industry.

Real Audio: A protocol developed by Progressive Networks which allows you to listen to streaming audio on the Internet. The latest versions of real audio enable you to receive CD quality sound over connections as slow as 28.8k BPS. You can learn more about RealAudio on Progressive Networks' web site, http://www.RealAudio.com.

Reverse Name Lookup: Computers on the Internet can be referred to by names, which can be translated to an IP address. After the name is translated, a Reverse Name Lookup can be used to translate the IP address back into a name, as well as its aliases. This allows OrbitNet to verify that the computer to which it is connecting is the expected computer.

Secure Sockets: To facilitate secure connections on the Internet, the Secure Sockets (SSL) protocol was invented. It is used on a separate connection from regular HTTP and is encrypted to prevent hackers who have access to the network from tapping the connection. SSL is often used to purchase products on the Internet when private information such as credit card numbers must be exchanged. OrbitNet supports

proxying of secure sockets. This feature is automatically enabled with the CERN HTTP proxy. It can be disabled by enabling HTTP command filtering and disabling the connect command.

Serial Number: OrbitNet requires a unique serial number in order to function beyond the thirty-day evaluation period. When you purchase a serial number, enter it on the form available under "Set New Serial Number." OrbitNet automatically registers itself the first time it connects after its next restart. The message displayed when starting OrbitNet disappears once the permanent serial number is registered online.

Server: A network computer that handles one or more specific functions for the rest of the network. The OrbitNet computer is your network's server.

SMTP (Simple Mail Transport Protocol): The protocol used to transmit mail to the receiving mail server. Usually mail sent using SMTP ends up in a POP3 server where it can be retrieved by a user. Mail may travel through multiple SMTP servers before reaching a post office.

Socks: A very flexible proxy protocol used for several types of connections. Netscape and Internet Explorer can use the Socks protocol to connect to every protocol they support. The Socks proxy protocol requires support for DNS on your local network. The Socks proxy is required to support IRC, Gopher and WAIS in your browsers. The Socks proxy also allows you to have a more flexible interface to FTP in web browsers such as Netscape and Internet Explorer.

Static IP Address: An IP address that is stable and does not change. A static IP address is assigned to a network connection, usually by a human filling in configuration information. Many Internet connections that do not require dialing will have static IP addresses.

Subnet: A network of computers that communicate with each other directly. In a TCP/IP network, a number of significant bits in the IP address define the subnet. IP addresses not on the same subnet must be reached through a router, which forwards network packets between subnets.

Subnet Mask: A number used to define which portion of an IP address designates the network, and which portion is an identifier for the local machine.

System Tray: The system tray is on the right side of the taskbar in Windows 95/98 and NT. Often the clock or system agent will be visible in the tray. When OrbitNet is configured to "run in the taskbar" in Windows 95/98, it loads before you log on to Windows, and appears as a white mask icon in the system tray.

Taskbar: Part of the main screen in Windows 95/98 and NT. Its default position is a strip at the bottom of the screen.

TCP/IP (Transmission Control Protocol /Internet Protocol): A combination of two protocols, TCP/IP is the Internet's official "language," allowing computers to communicate. TCP breaks information apart so it can be transmitted, and then puts the information back together on the receiving end. IP is the method by which the pieces of information are transferred across the Internet. TCP/IP is a flexible, routable network protocol, suitable for any size network, that includes dynamic routing along with acknowledgements and flow control to ensure data receipt.

Telnet: A protocol used for communicating with other computers on the Internet as if you were typing at the console of that computer. Telnet does not, however, provide a graphical interface such as the World Wide Web or X-Windows.

URL (Universal Resource Locator): A string identifying a specific document on the network. A full URL consists of a protocol, such as HTTP or FTP, a host name and a document path. As an example: **http://www.orbitsat.com/index.asp** is a full URL. The characters before // designate the protocol (HTTP in this case), the subsequent string, **www.orbitsat.com** is the host name, and the remainder, Index.asp, designate the document. Any computer on the Internet can use this URL to retrieve the same document.

WAIS (Wide-Area Information Services): WAIS allows searches for words and documents within databases. Browsers such as Netscape use Socks to implement WAIS.

OrbitNet Computer: The computer on which OrbitNet is or will be installed. Only one computer in a network runs OrbitNet. That computer must have a connection to the Internet and a connection to the rest of your local network..

UDP (User Datagram Protocol): An alternative to TCP, UDP is a streaming protocol that neither requires nor expects flow control or acknowledgements. Faster than TCP but less robust, it is commonly used for things like audio streams where a few missing packets don't matter all that much.

WWW (World Wide Web): A network of Internet computers using HTTP and HTML to provide graphical documents to users.

APPENDIX E:
Trouble-Shooting

This guide is designed to assist if you encounter any problems while using OrbitNet. Find a statement that describes the trouble you're having and follow the tips provided.

OrbitNet doesn't seem to install properly.

Reinstall OrbitNet from the original disk or download the file again. *Don't uninstall the program before you do this.* The Install program (from OrbitNet 3.0 and up) has some intelligent trouble-shooting built into it. Thus, it will attempt to repair any problems originating from the initial installation.

1. Don't be alarmed when OrbitNet reboots the system. The re-install requires OrbitNet to execute at least two reboots while uninstalling/reinstalling selected components and correcting any problems it might find.
2. In Windows95/98, the reboots will probably progress automatically. If not, you'll be presented with a dialogue box asking you to reboot. Do so.
3. In Windows NT, there are many instances where the reboot will not progress automatically. Watch for the dialogue boxes. When you're asked to reboot, please do.
4. If you're still having trouble, take a look at your other network drivers. If you see some weird drivers that you don't use, remove them (*don't* remove any Deterministic drivers—that's us!). We've had some problem with some of the more rare network drivers (like the IRDA driver, although we've already fixed that one) running at the same time. Once you've removed the old drivers, re-install the program.

OrbitNet works fine the old way, but the new stuff doesn't work.

Folks who are already using OrbitNet 2.1 and older will already have settings (both in OrbitNet and in their client applications) for operation through a Classic Proxy. If things work fine this way, but you can't make your browsers or mail programs work without putting in proxy settings, then the NAT drivers may not be loading properly. Take a look under **OrbitNet/Help/About**. A couple of lines down you'll find information about the Transparent Proxy (which uses the NAT drivers).

1. If you see version information, then the drivers have loaded. The problem is most likely with IP addressing instead, especially the Gateway setting on your client computers. A gateway setting is not needed for Classic Proxy operation (like you had with version 2.1) but it is *required* for operation through the NAT and Transparent Proxy—the cool new stuff in 3.0.
2. If the "About" box reports that Transparent Proxy hasn't loaded, do a reinstall of OrbitNet as shown in the first Trouble-Shooting entry, above.

OrbitNet complains about my IP address when it starts.

When OrbitNet starts, it looks for any IP addresses on your system. You must have two network connections on the OrbitNet machine if it's to do its job. Usually, those two connections are a network card and dial-up adapter (for dial-up users) or two network cards (for cable and DSL modem users). If it doesn't find any addresses, or if the internal address has changed since the last time OrbitNet ran, it will let you know that there's a problem. A few things to keep in mind:

1. IP addresses cannot be set from within OrbitNet. Addresses are assigned to cards via the operating system. OrbitNet asks the operating system for the IP addresses, and lets you know what it finds.
2. Take a look under **OrbitNet/Settings/General/Internal IP** to see which addresses OrbitNet finds. If more than one is found, the "multiple IP" button will be enabled.
3. If no IP address is showing in the Internal IP box, hit the drop-down button and take a look at the listing there. If you see your internal network connection listed, highlight it and check to see if it shows in the Internal IP box when you close the drop-down menu.
4. If the address 127.0.0.1 shows up there, then either
    - You have the internal network card on the OrbitNet machine set to "obtain automatically" instead of being statically assigned; this address is the one address on your whole system that *must* be statically assigned.
    - You have an address assigned, but it still shows as 127.0.0.1 (or it doesn't show at all) in the Internal IP box. This means that there's a problem with the network card, or with tcp/ip on that system, or that you haven't rebooted the system since assigning the number (under Windows 95/98 and NT you must reboot for new network settings to take effect).

I can't seem to connect through OrbitNet to the Internet

Start off by breaking this problem in half. Determine if the cause derives from 1) connecting from OrbitNet to the Internet; or, 2) connecting from an application (like a browser) to OrbitNet.

In OrbitNet, run the Install Wizard at **OrbitNet/File/Install Wizard**. At the end of the three or four screens it steps through, there's a page entitled "Verifying OrbitNet Setup" where it attempts to connect to the Internet. If OrbitNet puts a check mark in the box "Verifying communication with the Internet"—it may take a few minutes to accomplish this—then OrbitNet was successful in sending and receiving packets via the Internet.

- If unsuccessful, verify that you have Internet connectivity *without* OrbitNet.
- If you can connect without OrbitNet, but OrbitNet cannot connect, double-check the IP addresses listed in OrbitNet. Be sure you have properly designated them as Internal (meaning for your own local network) or External (meaning your Internet connection) addresses.

2. Open a browser, and type in the URL http://proxy.command. You should get a response back immediately from OrbitNet which shows a page with your Remote Admin choices. If you've entered an administrative password in OrbitNet, though, the proof of connection will be that it asks for a password.
    - If you cannot connect this way, then make sure that the client machine has an IP address and can ping the OrbitNet machine, and that (a) for Transparent Proxy connections, the client machine has the OrbitNet internal IP address listed as its Gateway address, the browser is set to use the LAN and not a modem, and OrbitNet has Transparent Proxy enabled; or that (b) for Classic Proxy connections, the browser is set to use a proxy, has the OrbitNet IP address in the proxy settings boxes, and the port in the browser http, security, and ftp proxy settings matches the CERN proxy port in OrbitNet (default is port 80).

- If you have previously installed a proxy, NAT, or firewall on your system—particularly those requiring software installation on the client machines as well as on the server—then you must remove that software from *all* machines, because many will interfere with normal TCP/IP operation. The most common symptom when this happens is that ping and (often) NetBeui/Network Neighborhood will work, but not TCP/IP.

My browser won't connect to the Internet.

425 Errors. Instead of downloading a web page, all you get from your browser is a 425 "can't connect" error message. A 425 generally indicates that the name lookup (DNS) has succeeded, but the actual connection has not. When a browser on one of your client machines won't connect during your initial setup, the three most common causes are:

1. **IP addressing errors**: An error exists in the IP addressing of either the OrbitNet machine or the client machine, or both. Use the ping utility to check your TCP/IP connections. See Chapter 4 ("Testing TCP/IP Connectivity") for more information about ping and how to use it.
2. **Ping works, but the browser still reports a 425 error**: Transparent Proxy has been disabled in OrbitNet, or the local machine has an incorrect Gateway address (those two are required for Transparent Proxy connections), or the browser has not yet been configured to use a proxy (required for a Classic Proxy connection). Refer to the section on configuring your browsers.
3. **Ping works, and the browser is configured**.
   a. *You can reach sites within your Service Provider's domain, but you get a 425 when you try to go to any other site*: Your Service Provider has a proxy, too, and is using it to provide your Internet Service (this is common outside North America, and also for some cable modem providers). You'll have to enable Proxy Cascading (at **OrbitNet/File/Settings/General**); you'll need to know the IP address and port of their proxy server in order to configure it.
   b. *Sometimes you can reach a site, and sometimes not*:
      1. If it's the default home site, try setting your browser to a different home site. The default home sites—the ones preset in the browsers—get overloaded every few months and stay that way until the servers are upgraded. There are millions of browsers accessing those default sites.
      2. For other sites, look for high packet loss rates (a loss rate of 5% is enough to give you a lot of 425 errors). You can use Ping to investigate your packet loss rate. Another possibility is that the TTL setting (Time To Live; it's a registry setting for how many hops your system allows for TCP/IP packets) is too low. As the Internet gets more crowded, the default settings for this are not always adequate. You can use a "packet-tuner" program like or MTUSpeed to inspect and change these settings.
4. Access is disabled within "Users" in OrbitNet. This will give 425 and the additional message "You are not authorized to use the xxx protocol through OrbitNet". The machine trying to get access has been specifically denied access as one of the user groups defined under the 'Users' tab, **OR** you have inadvertantly enabled the option 'Refuse access unless specifically permitted' (also on the Users tab) and then forgotten to allow access from this machine.

430 Errors. A 430 error generally indicates that the name lookup (DNS) has failed. You browser has not yet tried to connect to the site. When it asked the system what the numeric address for a site was (that's what DNS does for you), it—or OrbitNet—didn't get an answer. Without that information, it can't even attempt a connection.

1. If socks is enabled on your browser proxy settings, try turning it off. Browsers will use socks preferentially if it's listed. If your local DNS is not working correctly, the socks connection will fail.
2. You need to have DNS configured on every machine (not just the OrbitNet machine) for many functions to work correctly. Take a look at the chapter on DNS for instructions on how to configure it, or you can set the IP settings on your clients to "obtain automatically," and OrbitNet will supply those clients with IP settings (including DNS information). See the chapter on DNS for instructions on using a Ping variant to check your local DNS.
3. Some cable companies require that the domain name on your proxy computer match their own domain name. Try putting their domain name in OrbitNet under the DNS settings, and also in the network settings under **Control Panel/Network/TCP/DNS.**

I keep getting password errors when I try to get e-mail.

OrbitNet itself does *not* ask you for passwords for your email. That request is coming from one of two places, either the mail server you're trying to reach or from the application itself.

Most email applications remember the email password for you. However, if the password ever fails the application asks for it again—and it will ask every time you try to get mail until the password succeeds.

The mail server (which, for most people, is the ISP's mail server) will ask your application for a password. This request passes unchanged through OrbitNet, and your email application passes it along to you. The password is often not the same as the password you use to connect to your ISP, and it's usually case-sensitive. If the email server is asking for a password, then you're connecting to the email server.

I can *receive* e-mail, but I get errors when *sending* e-mail.

More and more users are seeing errors like "Relaying not permitted" or "Transport not available" when attempting to send email. These reported errors are the result of more and more ISP's installing anti-spamming measures on mail servers.

1. Many ISPs won't permit you to send email unless you are physically connected to their modem bank. Sending email to their servers via another ISP or Internet Connection is not permitted.
2. Many ISPs will reject your email if your return address domain does not match their own domain name. In the Reply To and Return Address fields, make sure to use their domain name, or one that you've registered with them (for an email address like joeuser@isp.com, "isp.com" is the domain name).

OrbitNet won't dial out.

Take a look at the modem information line next to "Current Connections" on the OrbitNet main screen. If the info line says "modem in use by another program," then OrbitNet cannot invoke Dial-up Networking to dial out. You'll need to figure out what that other program is and resolve the conflict.

If you're attempting your inital connection with a program using the Socks protocol, OrbitNet won't dial unless this option is enabled: "Connect to the Internet for UDP and DNS queries." Be prepared for ghost dialing if you enable this option; it can be triggered by network activity invisible to the user.

Check the "time window" under Dial-Up Setup. If you're outside the window, OrbitNet won't dial. A browser receives a message to that effect, but other programs won't; all the user sees is that the program doesn't dial out.

OrbitNet dials too often.

Check to see if you have the "persistent connection" option set, and are within the time band configured. If so, OrbitNet dials immediately when it enters the specified time period, and whenever the connection is lost.

Check to see if you have the option "Connect to the Internet for UDP and DNS queries" enabled. If so, you'll see OrbitNet dial often for no apparent reason. A lot of random network activity uses these two protocols, and they'll force the dialing.

Look at your mail programs, including those in the browsers: many contain default settings to check the mail every five or ten minutes.

And, check to see if you have IE5 on your OrbitNet machine. Whenever IE on the OrbitNet machine is set to use a modem instead of the LAN, it will intercept TCP traffic and dial for you. OrbitNet's installation changes that setting to "use the LAN," but if you upgrade your IE it will change it back. IE5 in particular seems to have a bug where it spontaneously reverts to "use a modem" no matter what setting you have put in there.

OrbitNet doesn't hang up.

Since OrbitNet can't tell if a browser or other application is open—but can ascertain that it's actively communicating—it must rely on an inactivity timer to decide when to hang up. Check the setting of your inactivity timer under Dial-Up Setup.

Check the modem information line in the main window. If it says "modem in use by another program," then OrbitNet will not hang up. It's possible that the user is "the other program;" if you invoked DUN yourself to establish the connection, OrbitNet assumes that you know what you're doing and won't interfere with the connection. If you want OrbitNet to take control of a modem connection no matter who starts it, enable the option "Always own the connection" under **OrbitNet/File/Settings/General/DialUp**.

Watch the "idle time" indicator on the modem information line. Many mail programs—including those in the browsers—have a default setting to check the mail every five minutes. If that idle timer is getting reset every few minutes, look around. News alert programs and time refresh programs can also do this, even if they fail to connect: a mere attempt to connect resets the inactivity timer. Take a look at the little icons in your System Tray, too. Many such programs always run in the background.

OrbitNet hangs up too much.

The inactivity timer works only on those connections it knows about. Take a look at the main OrbitNet screen. If a connection shows up in that window, then OrbitNet knows about it. If it doesn't show up—NAT connections, for instance, won't show—change it to Transparent Proxy under Client Access Method.

I can't get AOL, AOL Instant Messenger, ICQ, or mIRC to work.

All of these programs rely on the Socks protocol to support operation behind a proxy. You'll need to enable Socks in OrbitNet, and set up DNS on your local network to make them work. AOLIM, mIRC and other chat programs work through Transparent Proxy with no additional setup; for ICQ you'll need to enable the proxy and socks settings within ICQ.

I keep getting errors about Java applets.

Many Java applets require that DNS be set up on your local system.

I have trouble with secure connections on some sites.

Not all websites use the standard ports (443 and 563) for secure connections. If they use a different port, enable the option "Permit Secure connections on non-standard ports" under **Settings/Protocols/HTTP**.

Another source of trouble—especially if you've gotta log in to the site—can occur if you don't have DNS working properly all the way to the client machine you're connecting from. If the site fails the Reverse Name Lookup test, you won't be able to make a secure connection. If you really wanna connect, try disabling RNL at OrbitNet/File/General.

We've also found that some ad-blocking software will interfere with secure connections.

OrbitNet is warning me about a security problem.

OrbitNet will pop up a warning about a possible security problem if too many of your connections are made to its internal address. There are two common causes:

1. Your Internet connection is incorrectly configured as an internal connection instead of as an external connection. This is a bad thing. It means that anybody on the Internet is treated as being behind your firewall—which ain't no firewall at all! Fix it. Your Internet connection *must* be configured as an external connection (**OrbitNet/File/Settings/General/Internal IP**).
2. Your Internet connection comes into your hub instead of to the OrbitNet machine. This happens most often with cable and DSL modems and must be changed. Your Internet connection must come in *only* to the OrbitNet computer. Add a second network card to the OrbitNet machine if you don't already have one. Some cable and DSL modems will connect to either a hub or a card (they reconfigure the network plug connections automatically). Most require that you change the cable type when changing what you're plugging into. If, like most people, you've got a standard CAT-5 cable connecting the modem to the hub, then go get a Cross-over CAT-5 cable to connect it to a network card. Cross-over cables are commonly available in the network section of computer stores.

How do I uninstall OrbitNet 3.0?

First off, don't remove any files or folders before you do the uninstall. Missing files may make it impossible for the uninstall program to run correctly. OrbitNet 3.0 has an Uninstall program; you'll find it in the OrbitNet 3.0 directory. In the Start menu system, the icon looks like the OrbitNet icon with a red circle and slash over it.

1. If you're dropping back to 2.1 from 3.0, be sure to write down all your IP settings, names, and registration information (including the serial number) before running the uninstaller.
2. Make sure that OrbitNet is not running, not even in the taskbar or as a hidden service in NT.
3. Run the uninstall program.

Didn't find it here?

Take a look on our website in the Tech Support section. The SupportBase is a searchable database of asked-and-answered questions loaded with information. It gets new additions on a near-daily basis.

APPENDIX F:
Error Messages

This section is designed to help you ascertain and fix problems signaled by a OrbitNet error message.

BINDING MESSAGES

- **Unable to Bind DNS Proxy**: The DNS Port (53) is being used by another application. If you're operating under Windows NT, be sure the Microsoft DNS Server isn't running. If you want to use a different DNS server, disable DNS in OrbitNet. If you don't know of a DNS server on this machine, look for other proxy or firewall applications that you may have tried recently. Many will use the DNS port. You'll need to disable that software.
- **Unable to Bind DHCP**: The DHCP Port (67) is being used by another application. This is often another proxy or firewall that is still operating on the machine. You'll need to disable this other application for OrbitNet's DHCP server to operate.
- **Unable to Bind HTTP Proxy**: The HTTP Port (typically 80) is being used by another application. If you're running a web server on this machine, set it (or OrbitNet) to listen on a different port (e.g., 8080). In Windows NT, disable the Web Services or change the port under Internet Service Manager. On the Windows NT Server, go to Microsoft Internet Information Server/Internet Services Manager. On Windows NT WorkStation, go to Microsoft Peer Web Services.
- **Unable to Bind Mail Proxy**: The Mail Port (typically 25) is being used by another application. This port is used for sending mail. You'll typically get this message when you're running a mail server on the same machine. Disable Mail Host IP (SMTP services in OrbitNet or assign different ports to the mail server and OrbitNet for SMTP.
- **Unable to Bind Post Office Proxy**: The POP3 (typically 110) is being used by another application. This port is used for checking mail. You'll typically get this message when you're running a mail server on the same machine. Disable POP3 Host IP (POP) services in OrbitNet or assign different ports to the mail server and OrbitNet for POP.
- **Unable to Bind FTP Proxy**: The FTP Port (typically 21) is being used by another application. You'll typically get this message when you're running an FTP server on the same machine as OrbitNet. If this is the case, disable FTP in OrbitNet or assign a different FTP port to OrbitNet (i.e.. 8021). In Windows NT, disable the Web Services under Internet Service Manager or change the port in OrbitNet. On Windows NT Server go to Microsoft Internet Information Server/ Internet Services Manager. On Windows NT WorkStation go to Microsoft Peer Web Services.

COMMON ORBITNET & WEB BROWSER ERROR MESSAGES

- **304 Invalid port number or address specified:** The port number or the address specified in the Post command was invalid. Please retry your command.
- **400 OrbitNet Modem Connection Failed:** OrbitNet was unable to establish a dial-up connection to the Internet. Dial Up networking returned e*rror_code*.
- **403 Forbidden Commands: There are several things in OrbitNet** – particularly the site restriction functions – that can give you a forbidden error. Whenever OrbitNet issues a 403 error code, it will also supply additional information about the reason for the 403, including what function (such as the blacklist)

is responsible for the message. If you are getting a 403 message with no additional information, then most likely the error message is coming from a server or an application other than OrbitNet**.**

- **The request was not properly formatted.** OrbitNet will permit requests only with properly formatted strings. This error is usually generated by programs that do not strictly follow the http 1.0 or 1.1 specification.
- **Secure Sockets attempted to use a restricted port - CONNECT command refused.** This problem is typically caused by a secure server improperly configured, or by an application attempting to access a protocol other than SSL through the SSL proxy. The CONNECT command restriction can be disabled in the HTTP Setup in *OrbitNet/ File/Settings***.** The specified request was not permitted due to a possible security breach or memory allocation error.
- **420 Socket Errors:**
  • Unable to create socket—the OrbitNet server may be too busy. This means that all available sockets on the system are in use. Wait until some of the socket connections are freed. If OrbitNet is running on a Windows 95 system, consider moving it to a Windows NT system with its higher number of sockets.
  • Unable to bind data connection to specified port. OrbitNet was unable to listen for a connection on a specific port. This could happen if there is another service already using that port. It can also happen in FTP if there is an error binding the data connection.
  • Unable to set up asynchronous communication. This is an internal TCP/IP error.
  • Incorrectly Formatted URL. The URL was formatted incorrectly. For example, a URL with a space in it (spaces are not permitted in URLs).
  • Protocol Not Supported. The requested protocol is not supported; i.e., Gopher enabled in the browser.

- **425 Connection Errors:**
  • Unable To Connect To Remote Host. Either the host is not accepting connections or there was a network error (an error in local IP addressing during setup might cause this). OrbitNet tried to establish a connection to a server but the server either refused the connection or was not available. This could indicate that the remote server is down, or that the name or IP address specified is incorrect, or that the appropriate server is not running on the specified machine.
  • Connection Refused by Remote Host. Same as above.
  • Connection Refused. Too many people are already using OrbitNet. Try again later. In OrbitNet Home Edition this message is returned when the simultaneous three-user limitation has been reached.
  • Connection refused. You are not authorized to use the specified protocol through OrbitNet. This message indicates that the particular user requesting the connection does not have permission to use the requested protocol (if user restrictions were enabled under the User's Tab). It's also possible that a connection was requested and the required protocol was not configured. User configuration is available in *OrbitNet/File/Settings/Users*. Protocol configuration is available in *OrbitNet/File/Settings/Protocols*.
  • Unable to establish PASV FTP connection. The FTP server returned an error to the PASV command. This error is only returned if the checkbox in FTP setup states that all the FTP transactions should use PASV mode. That checkbox should only be set if you're running behind a filtering router, which does not permit incoming connections.

- **430 Protocol Errors:**
  • **Unable to Resolve Name.** You'll generally get this message when DNS is not configured correctly on the OrbitNet Server or client machine. It may also be caused by an incorrect URL. For DNS configuration please refer to Chapter 7.
  • **Unauthorized. You are not authorized to use this protocol.** A connection was received on a protocol not permitted in the OrbitNet configuration. This message may be returned if FTP is disabled but a user requests a FTP connection through OrbitNet. Protocol configuration is available in *OrbitNet/File/Settings/Protocols*.

501 FTP Error. FTP server returned an invalid response to PASV command: The response from the PASV command could not be understood. Try disabling the Passive option in the FTP Protocol in OrbitNet. In FTP clients, select the USER@SITE FTP method instead of PASV method.

APPENDIX G:
Interpreting Fields in Log Connection Entries

Fields reported in the activity log and detailed log are similar, but sorted differently.

The activity log writes to the screen. It's a sequential ascii file used primarily for troubleshooting. As an option it will write to file: use **proxylog /?** to utilize the **save to a file** option.

The detailed log saves only to a file in a format easily utilized by summary programs such as WebTrends Professional with Proxy Analyzer.

Activity Logs

In this section we'll display a sample activity log connection entry and show how to interpret it.

The sample:

90.0.0.5, cnnfn.com, 207.25.71.61, 80, 266, 146, 311, http, -, GET, http://cnnfn.com.images.ticker.gif, -, Unknown, 304

The field interpretation:

1. 90.0.0.5. Source IP, if available. The IP address of the requesting machine; this is the address of the client machine initiating the connection. This entry is shown for TCP connections; other connections (UDP and socks, for example) display a hyphen (-) instead.

2. cnnfn.com. Destination Name, if available. It won't be available for socks connections if the user supplied the IP address in numeric form, or if the file was returned from the cache.

3. 207.25.71.61. Destination IP address. Only returned if an actual connection is made. If a document is returned from the cache, a hyphen (-) will be displayed instead.

4. 80. Destination Port. Shown only if a connection is made. A return from the cache will produce a zero (0) or a hyphen (-).

5. 266. Length of connection in milliseconds. The total connection length. Specifically, it's the length of time that OrbitNet is connected to the client machine, not the length of time it's connected to the distant server.

6. 146. Bytes sent. The number of bytes OrbitNet sends to the server on the Internet. This could be 0 if the request is returned from the cache.

7. 311. Bytes received. The number of bytes OrbitNet sends to the client machine. As some packets are parsed as part of the proxy function, it may not be exactly the same as the number of bytes OrbitNet received from the server.

8. http. Protocol used, by name or by number. If a number is shown (e.g., 1080 for a socks connection), it's the standard port used for that protocol—not necessarily the port actually used.

9. -. Always a dash.

10. GET. The http command used, such as GET, POST, PUT, etc. This information is provided only for CERN connections—i.e., the connections going through the CERN proxy port designated by you. For example, an ftp connection through the CERN proxy port shows the command, while an ftp connection through the FTP proxy port will not.

11. http://cnnfn.com.images.ticker.gif. The URL requested. This information is provided only for requests proxied through the CERN port.

12. -. Mime type; not currently implemented (will return a dash).

13. Unknown. Document Source. This field shows where OrbitNet obtained the document that it delivered to the client.

The available options:

- **Cache:** Delivered from the OrbitNet cache to the client.
- **Rcache**: Retrieved from the Internet, stored in the cache, and delivered to the client
- **Unknown**: - doc was requested, found to have no changes, and not returned to the client. Documents which browsers fill from their own cache (usually after verifying no changes from the Internet server) will show as Unknown.
- **Vcache**: Verified on the Internet, returned to client from cache.
- **NVCache**: Not verified, returned to client from cache.
- **VFINET**: Verification failed, returned from Internet.
- **INET**: Returned from Internet, not cached.
- **304 (not modified) Return code**. The code returned to OrbitNet from the Internet server. Common return codes are 200 (success), 403 (forbidden), 404 (not found), 500 (server error).

Detailed Log Fields

In this section we'll display a sample detailed log field connection entry and show you how to interpret it.

The sample:

90.0.0.6, -, -, N, 03/05/99, 18:47:26, 1, -, -, www.winfoseek.com, 90.0.0.1, 80, 1846, 10128, 344, http, -, GET, http://www.infoseek.com/ads/ATT_1079.gif, -, Rcache, 200

The field interpretations:

1. 90.0.0.6. Source IP Address. Source IP, if available. The IP address of the requesting machine; the address of the client machine initiating the connection. This entry shown is for TCP connections; other connections (e.g., UDP and socks connections) display a hyphen (-) instead.

2. -. User Name, not implemented. For user authentication. Always a dash.

3. -. Always a dash.

4. N. User-authenticated; Y/N. Not implemented.

5. 03/05/99. Start date. This date is derived from the machine, not the Internet.

6. 18:47:26. Start time. Derived from the machine, not the Internet.

7. 1. Service Name. 1 = web, 2 = winsock.

8. - . Proxy name. Always a dash.

9. -. Referring server name. Always a dash.

10. www.infoseek.com. Destination Name. Blank if from cache.

11. 90.0.0.1. Destination address; blank if from cache. In this case, OrbitNet is running on 90.6, and cascaded through another OrbitNet on 90.1, which explains why the address and name don't match).

12. 80. Destination port.

13. 1846. Process Time. The connection time in milliseconds. The example time is for the connection from OrbitNet to the client, not from OrbitNet to the server.

14. 10128. The number of bytes OrbitNet sent to the remote server.

15. 344. The number of bytes OrbitNet sent to the client.

16. http. Name of the protocol used. This might appear in name or numeric form. If numeric, it will be the number of the standard port used for that protocol, not necessarily the port number configured within OrbitNet.

17. -. Always a dash.

18. GET. HTTP command used, shown only for connections which go through the CERN proxy.

19. http://www.infoseek.com/ads/ATT_1079.gif. URL/document name. Shown for connections which go through the CERN proxy.

20. -. Mime type, not implemented. Always a dash.

21. RCache. Document source. One from the following list:

- Unknown. Doc was requested, found to have no changes, not returned from the Internet or the cache. Docs filled from the browser cache or connections with errors are examples.
- RCache. Retrieved from the Internet, delivered to the client, and stored in the cache.
- Cache. Delivered from OrbitNet cache to client.
- VCache. Verified on Internet, returned to client from OrbitNet cache.
- NVCache. Not verified on Internet, returned to client from OrbitNet cache.
- VFInet. Verification failed, returned to client from Internet.
- Inet. Returned from Internet, verified but not stored in cache. Docs with no content length, with a no-cache pragma, part of a query, or that exceed 1/8 of the OrbitNet cache size are not cached.

22. 200. Result Code from distant server. 200 indicates success.

APPENDIX H:
Network KnowHow

Overview: Network Knowhow

Those of you seeking a more-than-casual knowledge of the way in which networks function will find this section particularly helpful. The information that follows discusses:

- Ports
- Gateways and Routers
- Subnet Masks

Ports is Ports

So what the heck *are* ports, anyway? Simply put, they're part of the addressing that controls how data travels from one computer to another. You've already seen how IP addresses work to identify a single, unique location somewhere on the Internet, thus enabling you to send packets to a distant computer. But before this can be done, one more tiny hurdle must be overcome.

A single wire connects the network to the distant computer, but there may be many applications on that machine—a web server, an ftp server, a telnet server, etc.—waiting for somebody to connect. So the question arises: How do you use one wire and one IP address to connect to the right application? The answer: Ports.

Here's an analogy. Let's say you send a package to a friend. The Zip Code you include on the mailing label is similar to an IP address in that it gets your package to the one and only town in which your friend lives. Once there, however, the package still needs to get to your friend's doorstep. That's where the street address—akin to a port number—comes in. In other words, an IP address connects you to the right computer; a port number lands you in the right application. Computers have many ports (about 65,000), and each has a unique number.

So, let's say a network card, listening on its network, has accepted packets intended for its IP address. The port, a kind of junior-level address, tells the computer who (i.e., which local application) gets which packets.

Kinds of Ports: Source Ports, Destination Ports, Listening Ports, Standard Ports, Ephemeral Ports and Proxy Ports.

An important principle behind the Internet's smooth functioning is that some common applications always have the same ports. In other words, you needn't know in advance which port on a distant machine accepts mail, because *every* machine every*where* uses port 25 to accept email transport. If a mail server application is running on a machine and is ready to accept mail, the server application opens port 25 and listens for incoming mail packets.

Some common **standard** ports:

Telnet	Port 23
Mail (smtp, or send mail)	Port 25
World Wide Web	Port 80
Post Office (pop, or get mail)	Port 110
news (nntp)	Port 119

In general, ports 1 through 1023 are reserved for common usage, while those in higher ranges are used in other ways. There is, however, much leeway.

> ✔***USER TIP***: Ports 1 through 1023 have standard, well-known, uses. Almost all common Internet applications use listening ports in that range. Since they're used as ephemeral ports, they're always available for use as listening ports by local applications.

You might think that the application sending mail uses port 25, but that's not the case. The usual procedure involves an application requesting and being given a socket by the operating system; that is, it asks for and receives a port. Any port will do (the application doesn't even need to know what the exact port number is), but the operating system will typically hand over a port from somewhere above 1023. These ports are known as ephemeral ports. They are used briefly, and then returned to the pool for another application's later use.

The application sending the mail, using an ephemeral port, sends a connection request to a standard port. When the actual packets join to accomplish this, part of the information in each packet is the source IP address and port as well as the destination IP address and port. The ephemeral port is the source port; the standard port is the destination port. When the distant machine returns packets—and for any single connection, many packets are exchanged back and forth—it returns them using the original ephemeral port as its destination port. Although this sounds complicated, the underlying principle is easy to grasp: when a program uses an ephemeral port, any replies arrive back at that same port.

Here's one last bit of complexity. Since standard listening ports are for everybody, the answering machine doesn't actually use it for data transfer. It only listens on that port. As soon as a connection is established it hands that connection to a local ephemeral port and immediately resumes listening for new incoming connection requests on the standard port. That's how a web server can listen for (and handle!) thousands of connections from client browsers.

Now that you've waded through all this you must be wondering what the payoff is. How, exactly, does this information help you use OrbitNet? Well, think back to clients and servers. Those terms have definite meanings for Internet communication. A client application—a browser or an email application, say—sends a connection request to a server (a web or mail server, for example) listening on a standard port. Servers always listen on standard ports for incoming connection requests from client applications. *A server waits and listens for connection requests from a client*—that's pretty much what server and client means these days.

OrbitNet is a Proxy Server. It actually serves a dual-purpose role, acting as a server to any client machine making a connection request, and acting as a client application when connecting to a server on behalf of the client. There are many places where you are permitted to make port settings in OrbitNet. A few of these are labeled a "Destination Ports," and that is what they are—the ports to which OrbitNet sends its connection requests while acting as a proxy client. A destination port setting is *always* labeled as such in OrbitNet. When you configure a Destination Port, it's a sub-address on a different machine. It's up to you to know (1) whether a machine is actually listening on that port; and (2) that machine's IP address.

Most port designations you can make in OrbitNet are listening ports. They are also labeled as proxy ports. When you designate a proxy port, OrbitNet opens it up as a listening port and answers connection requests coming in to that port. For instance, when you do the mail protocol settings, it asks what ports you want to use. These are listening, proxy ports. When you give it port 25 for smtp, it opens a listening port on the internal network connection and waits for connection requests from mail applications on your local LAN.

> **NOTE**: Unlike many proxy servers, OrbitNet will not open a listening port on all network connections; it makes a careful distinction between the internal (outgoing connections) and external

(incoming connections) listening ports. These distinctions are important for the security of your firewall. For more information about incoming/outgoing connections, check out the section entitled "Mapped Ports" in Advanced Settings.

Gateways and Route Lists

Although the concept of IP routing is simple, the details are sometimes difficult to grasp. But take heart! You needn't be a computer guru to gain a working knowledge of the subject.

There is no way any computer can know the location of every other computer in the world. However, the Internet works on the principle that a given computer can reach any computer it needs to. This sounds like an unsolvable dilemma, but the *real* computer gurus worked out a simple way to make it work. Because they did, you can quickly reach a far-away computer even when you don't know where it is. Their solution: *Any network connection has a very limited number of choices to make when it sees a packet. It can ignore it, accept it, or pass it along.* That's it!

The "pass it along" part is where the Gateway Address comes in. When the machine decides it should pass the packet along, it sends it to the Gateway Address. Very few networks exist entirely on their own, with no access to or ingress from outside computers. Thus, most networks contain a computer with more than one network connection; it's connected to another network as well as to the local network. This computer is, of course, the logical place for the Gateway.

In a sense, that's all the Internet is: a series of individual networks, each with one or more Gateway Addresses. When you connect to a web server, your packets might pass through many other networks. All those networks need to know is where to send the packets that aren't accepted or ignored.

When setting up OrbitNet on your local network, the OrbitNet machine's IP address becomes the Gateway Address on each of the network's client machines. Thereafter, when an application on a client machine sends out a packet, it sends it using the tcp/ip stack on that machine. Unless other rules govern where the packets should be sent (see immediately below), the stack sends the packet to the OrbitNet machine.

Every machine with tcp/ip has a route table, a series of rules that tell the tcp/ip stack what to do with each packet it sees. These packets might come across the network, or they might come from local applications to be sent over the network. The route table is human-readable, so you can take a look to see what rules your machines are using to handle packets. To see a machine's route table, open up a DOS prompt and type: **route print**.

Below you'll see a route table from a Windows 95 machine. It has a network card with IP address 90.0.0.1 and subnet mask 255.255.255.0. OrbitNet is installed (you can't tell this from the route table) and the machine is not currently connected to the Internet (you *can* tell this from the route table):

Network Address	NetMask	Gateway Address	Interface	Metric
90.0.0.0	255.255.255.0	90.0.0.1	90.0.0.1	1
90.0.0.1	255.255.255.255	127.0.0.1	127.0.0.1	1
90.255.255.255	255.255.255.255	90.0.0.1	90.0.0.1	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
224.0.0.0	224.0.0.0	90.0.0.1	90.0.0.1	1
255.255.255.255	255.255.255.255	90.0.0.1	0.0.0.0	1

Each line constitutes a routing rule. When the tcp/ip stack decides where to send packets, it looks through the routing table and uses the following priorities:

1. If there is an exact match for the **IP** addresses, use that rule. If not, then:

2. If there is a match for the **network** address, use that rule. If not, then:
3. If there is no match, use the default Gateway.

A word about what each column means:

1. **Network Address** is checked for a match to the destination address in the packet IP header. Entries in this column can be individual addresses, network addresses, or gateways. Let's say a packet arrives addressed to 90.0.0.3. The first check is to see if 90.0.0.3 is in the network address portion of the table. *If so*, it's an exact match for a unique network connection, and the tcp/ip stack uses the rest of the line to specify what is done with that packet. *If not*, it looks to see if there is a match for the network address (don't be confused by this unfortunate double use of the term "network address"). There is a 90.0.0.0 entry, so it follows the rule for packets which are addressed to the 90.0.0.x network and which do not have an exact match in the table.
2. **NetMask** is used in much the same way as the Subnet Mask, though it isn't precisely the same thing. It tells you which part of the network address is important for the match.
3. **Gateway Address** is where packets are sent that match the rule.
4. **Interface** is which network connection to use when sending to that address.
5. **Metric** is the number of hops (a journey from one computer host to the next) to fulfill the rule. If it happens that two rules match, then the one with fewer hops is chosen. The metric becomes quite important on large Internet routers, but is less so on small local networks.

Now lets look at some individual entries. There are three individual addresses listed in the route table (take a look at the NetMask column—a netmask of 255.255.255.255 means that "every single bit of the network address must be considered for a match"—i.e., an individual address). 90.0.0.1 is the address of the network card on this machine. 90.255.255.255 is a special purpose address used for broadcasts to the 90.x.x.x network. 255.255.255.255 is a special-purpose limited broadcast. Neither of the last two are much used.

There are three network addresses in the list: 90.0.0.0, 127.0.0.0, and 224.0.0.0. The first is the network to which 90.0.0.1 belongs; the second is a special-use address for local loopback (in particular, the address 127.0.0.1 is defined as the local loopback address, and means "this machine right here." When used on any machine anywhere, it *always* means "this machine right here that I'm running on right now." The last, 224.0.0.0, is a reserved number for multi-casting. It's not much used presently, but will become more important with future technologies.

How does the machine use these? There are three entries of interest to us. The first is the individual address, 90.0.0.1. The Gateway Address of 127.0.0.1 tells you that any packet with that destination is intended for this machine, right here, right now. Any packet arriving with that address is available to the application level on that machine.

The local network address is 90.0.0.0. A packet from an application on the local machine addressed *to* any address in the 90.0.0.x group (except for 90.0.0.1) is passed on to the network card. A packet *from* the network with one of those addresses (since it came through the 90.0.0.1 address) is ignored.

The way the 127.0.0.0 address is written, with the netmask 255.0.0.0, implies that this machine will respond to *any* address in the 127.x.x.x range, not just the loopback address. If you give it a try, you'll see that it does just that.

And one last bit of info about what *isn't* in the route table. There is no gateway address, which can be confusing since there *is* a Gateway Address column; however, no entry in the table tells the computer what to do when the other rules fail. Since this machine only has one network address, and there is no other access to another network, there is no need for a gateway rule. The next table shows you what a gateway rule looks like.

The following example shows a route table after the OrbitNet machine is connected to the Internet:

Network Address	Netmask	Gateway Address	Interface	Metric

0.0.0.0	**0.0.0.0**	**207.21.140.5**	**207.21.140.5**	**1**
90.0.0.0	*255.255.255.0*	*90.0.0.1*	*90.0.0.1*	*2*
90.0.0.1	*255.255.255.255*	*127.0.0.1*	*127.0.0.1*	*1*
90.255.255.255	*255.255.255.255*	*90.0.0.1*	*90.0.0.1*	*1*
127.0.0.0	*255.0.0.0*	*127.0.0.1*	*127.0.0.1*	*1*
207.21.140.0	**255.255.255.0**	**207.21.140.5**	**207.21.140.5**	**1**
207.21.140.5	**255.255.255.255**	**127.0.0.1**	**127.0.0.1**	**1**
207.21.140.255	255.255.255.255	207.21.140.5	207.21.140.5	1
224.0.0.0	224.0.0.0	207.21.140.5	207.21.140.5	1
224.0.0.0	*224.0.0.0*	*90.0.0.1*	*90.0.0.1*	*1*
255.255.255.255	255.255.255.255	207.21.140.5	207.21.140.5	1

Windows rewrites this route table after every dial-up connection. We've added a few touches to help you decipher what's going on. The entries that are carried over essentially unchanged from the unconnected version are in italics. Those in regular type are the new special-purpose entries that we'll just ignore for now since they don't affect normal operation. The entries we're really interested in, the new ones, are in boldface.

As you can see, this machine now has *two* network addresses, 90.0.0.1 and 207.21.140.5. See the 127.0.0.1 entries in the Gateway Address column? That's how you know. That number indicates a local loopback, meaning "this computer right here." The entry in the "gateway address" column is where the computer is to send a packet that matches the rule. A packet addressed to 90.0.0.1 is an exact match; look in the gateway column to see what to do with it; find 127.0.0.1, and "Aha! its for me!"

Or do it in reverse order. Glance down the gateway column, looking for the "You are Here" signs—the loopback address. Every time you see the magic loopback address, look over to the network address column, and you'll see 90.0.0.1 and 207.21.140.5.

Since that second address wasn't there before, you know a dynamic address was assigned when you connected to the ISP. There are a couple of simple new rules, and one important one. The simple rules are: anything addressed to the 90.0.0.0 network goes to the 90.0.0.1 network connection, and anything addressed to the 207.21.140.0 network goes to the 207.21.140.0 network connection. That seems simple enough. The very first line, though, changes the behavior quite a bit. The Network Address of 0.0.0.0 translates roughly as "any address." This is the gateway rule. If a packet destination doesn't match an individual address in the table, and if it doesn't match a network address, it *must* still match this rule. Any address not otherwise specified will be sent to the 207.21.140.5 network connection.

So, when OrbitNet sends a packet to a machine at, say, 188.3.2.1, the stack sends the packet to the 207.21.140.5 network connection. That address is part of your ISP's network, and somewhere on that network is another machine with a gateway address, so that packet will just keep on going, from gateway to gateway, until it arrives at its intended destination.

This information is useful because, at the least, it illustrates the importance of DNS. As you can see, there are no names in the route table; there isn't even a place for names. When one of your applications uses a name (such as http://www.excite.com) it must first be converted to an IP address before packets can be sent.

Another thing you'll notice is that when a computer is part of two different networks—as your OrbitNet computer is—there must be a clear distinction between the two networks. If not, the tcp/ip stack will be sending packets to heaven-knows-where. You *cannot* have the two address on your OrbitNet machine be part of the same network.

What else do you look for? It's possible that your local network is a subset of your ISP's network, differentiated only by a different subnet mask. If that is the case, you'll need to change one or the other….guess which one.

Most of the time, people with a simple, single local network won't need to look at the route list to help trouble-shoot a connection problem. It's most often used by those who oversee multiple networks. If that's your situation, study the route table to be sure that packets have a route to the Internet and that return packets can proceed along an unambiguous path back to the originating computer.

The most common problem with multiple networks occurs when using dial-up connections. After carefully setting up your networks and making sure that every machine can ping every other machine, you may find that, when the OrbitNet machine dials in, other networks are suddenly unable to connect. The subnet farthest away from the proxy machine will seem to be unable to ping anybody; what is actually happening is that the ping is going to the correct place, but the *answer* to the ping is being sent out the new gateway instead of back to the originating machine. This holds true for all types of tcp/ip communication, of course. The fault lies with Windows' rewriting your table and "helpfully" supplying a new gateway for you.

We call this "the vanishing subnet" problem, and provide a feature in OrbitNet to correct it (RouteList, found under the Dial-Up Setup Tab). On NT machines only it can be fixed via a new persistent route addition to the route table, providing a return path from the OrbitNet machine to the vanishing subnet.

Subnet Masks

You may be asking: "So what the heck is a subnet mask, and why is it important?" If so, read on!

Have you ever noticed that IP addresses are often specified in pairs (IP address and subnet mask)? The subnet mask tells you—more importantly, it tells the tcp/ip stack in your computer—two things about the IP address: (1) which part of the address is designated as the network identifier; and, (2) which part designates individual connections on that network.

For the casual user, the most important thing to take from this is that the subnet mask *must* be the same on every network connection within that subnet. Thus, when setting set up your local network, use the same subnet mask throughout. You needn't use the one we recommend for new users—255.255.255.0—but that's a simple and common way to set up a small to moderate local network, and its hard to go wrong with it.

To see how a subnet mask works, we change the usual form of IP addresses to the "real" form, the 32-bit binary number for which it stands:

IP address	90.0.0.0	= 01011010000000000000000000000000
Subnet mask	255.255.255.0	= 11111111111111111111111100000000

The portion of the IP address that corresponds to a portion of the subnet mask is the network identifier. The portion with the zeroes is for individual addresses. The subnet mask *must* have all ones to the left, and all zeroes to the right. In the example above, the left-most 24 positions of the IP address specify the network address, accounting for the other notation you sometimes see: 90.0.0.0/24. This latter notation gives the same exact information as the IP address/ subnet mask pair.

The eight positions on the right are for individual addresses on the 90.0.0 network. The lowest number (00000000) and the highest number (11111111) are reserved for special uses. The lowest number—90.0.0.0—is called the "network address." It's used in routing tables and other places; it's also commonly used as the name to designate the entire subnet. The highest number, 90.0.0.255, is called the "broadcast address."

This leaves you 00000001 through 11111110 for your addresses, i.e., 1 through 254. (Or, impress your friends by calculating it this way: eight binary digits with two exceptions is 2^8-2, or 256-2 = 254 total addresses available). The first address available for your use in the 90.0.0.0 subnet is 90.0.0.1. This is the number that we usually recommend for the OrbitNet computer. There's nothing particularly special about the "1"—the unique identifier—it's just easy to remember and fast to write down.

On a simple local network, the network address portion of the IP address and the subnet mask must be the same *for each computer*. In our example here, all local computer addresses would start with "90.0.0" and each and every computer would have a subnet mask of 255.255.255.0. Only the individual address portion of the IP address will be different, and that portion *must* be unique for each connection.

Subnet masks don't have to be on the byte boundaries. As an example, let's do this with 90.0.0.0/29:

IP address	90.0.0.0	= 01011010000000000000000000000000
Subnet mask	255.255.255.248	= 11111111111111111111111111111000

As you can see, you have the right-hand three bits for individual addresses. 2^3-2 gives you six usable addresses on each network. Thus, 90.0.0.0 is the network address, 90.0.0.7 is the broadcast address, and you can use 90.0.0.1 through 90.0.0.6 for individual addresses. You don't lose all that other space, though.

90.0.0.8 is also a network address, and 90.0.0.15 a broadcast address. The 90.0.0.8/29 network is a completely different network than 90.0.0.0/29; this is true all the way up through the available space….90.0.0.16/29, 90.0.0.24/29, etc. As a real-world example you'll see this kind of addressing when an ISP supplies its customers with several IP addresses instead of just one.

APPENDIX I:
Dynamic/Static IP Addresses

Windows 98 IP Address Settings

Whether you're doing static or dynamic addressing, the procedure in the first few steps below are identical.

To begin, follow the path **Start\Settings\Control Panel\Network** to the Network screen, which will look something like this:

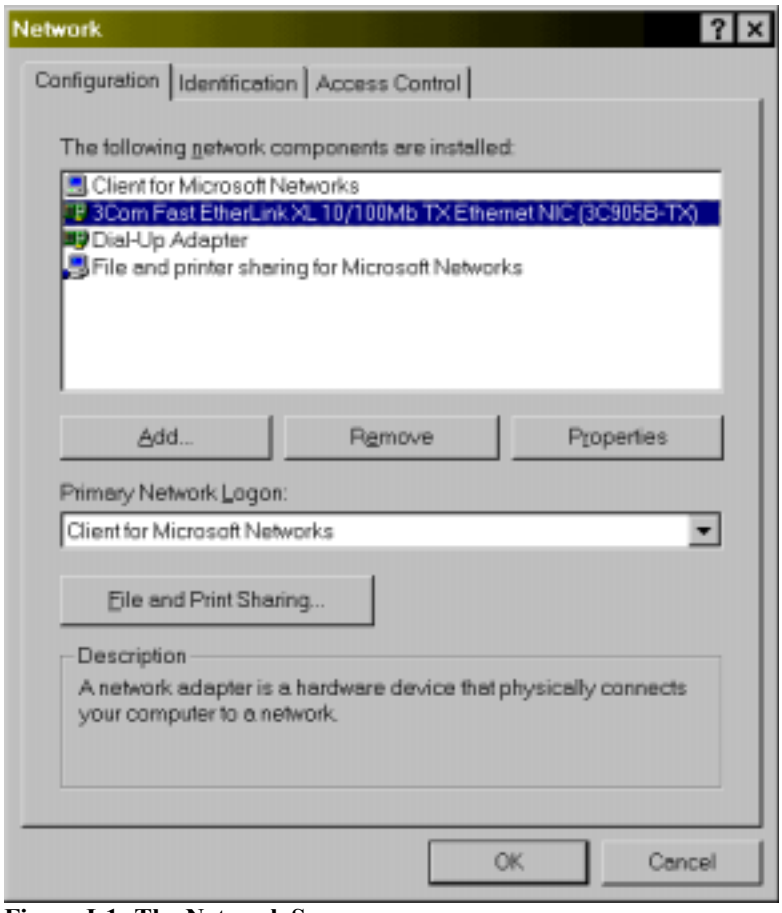


Figure I-1: The Network Screen.

If you'll be needing protocols not listed here, this is a good time to add them. For a first-time setup we recommend:

- TCP/IP protocol for all network connections; and,
- NetBEUI for all local, internal connections (but *not* for your external Internet connection).

To add a protocol:

- Highlight the network adapter
- Click Add
- Click Protocol
- Choose Microsoft
- Choose the desired protocol.

Be sure to back your way out; if you hit Cancel, the new settings will be dropped. Settings won't take effect until you reboot (Windows will ask if you want to restart when you click OK in the network box and drop back to Control Panel).

Here's an example of what your Windows 98 network setup might look like:

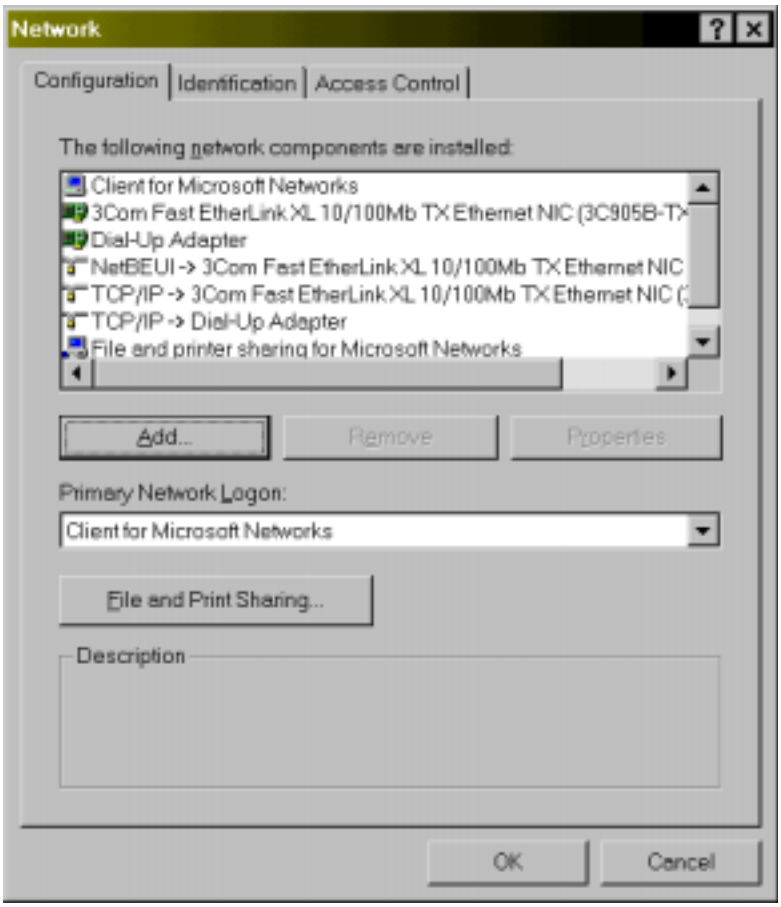


Figure I-2: A typical Windows 98 setup.

A couple of things you'll want to look out for when adding/removing protocols in Windows 98:

1. Windows 98 installs the TCP/IP protocol by default when you add a new network adapter.
2. If you only have one network adapter installed, the lines showing the protocols reveal only the protocol name, not the adapter name (unless you have more than one adapter).
3. Windows 98 won't install the NetBeui protocol unless you tell it to do so.
4. When you install a protocol, Windows sometimes adds it to *all* adapters instead of just the one specified by you. After adding a protocol, take a look to see if the protocol has been erroneously added to an adapter; if so, remove unwanted protocols by highlighting them and clicking Remove.

Now, to set the IP address, highlight the TCP/IP protocol line for the network adapter you want to set and hit the "Properties' button:

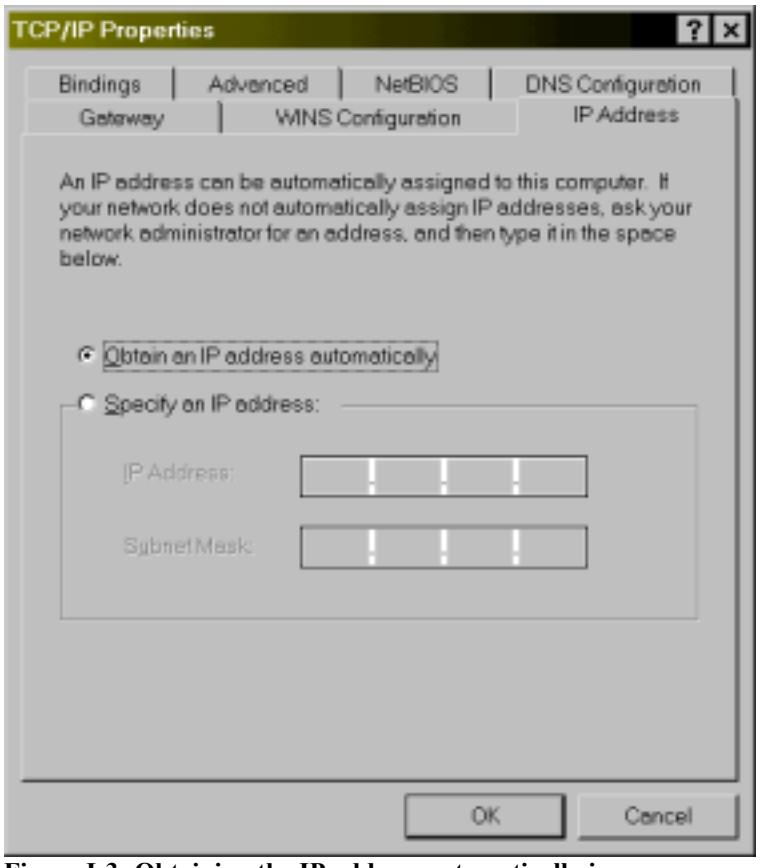


Figure I-3: Obtaining the IP address automatically is easy.

This setting has a number of advantages, and we recommend it for all of your client machines—especially if you're new to networking. This setting:

- Automatically configures IP settings via a DHCP server such as OrbitNet.
- Takes care of *all* your network settings for this network connection—gateway, DNS, etc., with no further action on your part.

The only place you *can't* use this configuration is in the internal network setting on the OrbitNet machine. In that case, a static assignment must be utilized.

Static IP Addressing. Let's move on now to setting a static IP address. Starting from the same screen above, click **Specify an IP address**. Specify it like this:

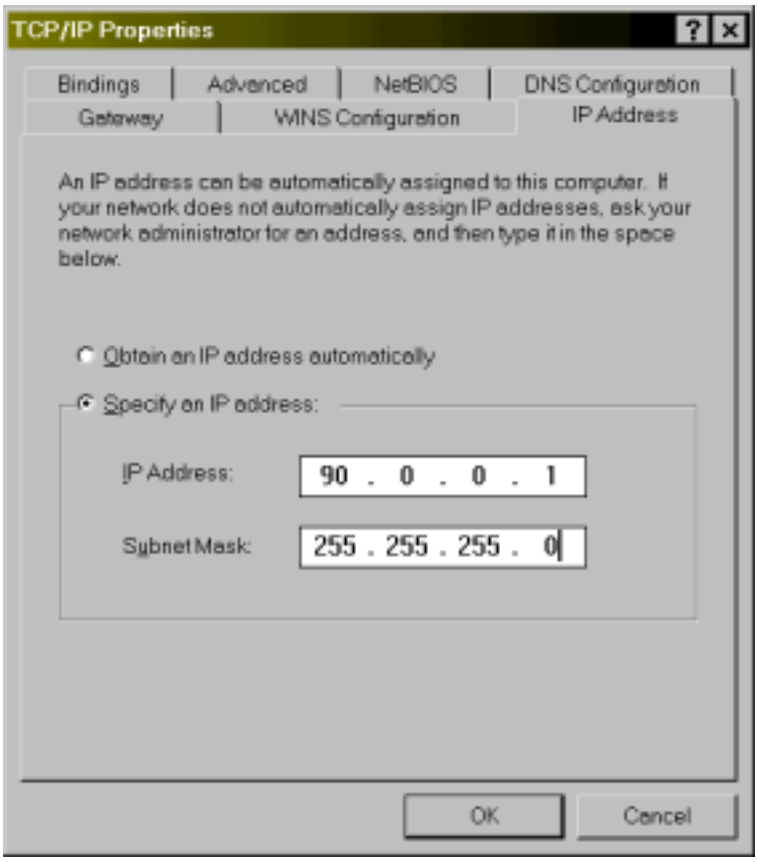


Figure I-4: Setting a static IP address.

We recommend these settings for the OrbitNet machine's internal IP address. If specifying the IP addresses on any of your client machines (you can mix and match, having some specified and others obtained automatically), follow these rules for each additional IP address you specify:

1. Each machine gets the same subnet mask as the OrbitNet machine.
2. Each machine gets a unique IP address. Having two machines with the 90.0.0.1 address, for instance, would really confuse matters. It's easier to remember addresses if you number them sequentially: the next machine gets 90.0.0.2, then 90.0.0.3, and so on.
3. You can use any number between 1 and 254. You cannot use 0, and you cannot use 255 or any higher number.
4. When setting unique addresses, make changes *only* in the IP address field corresponding to "0" in the subnet mask. IP fields that correspond to the "255" blocks in the subnet mask *must* be the same on all internal network connections.

You'll need to specify a few other settings here. To do so, click on the Gateway Tab:

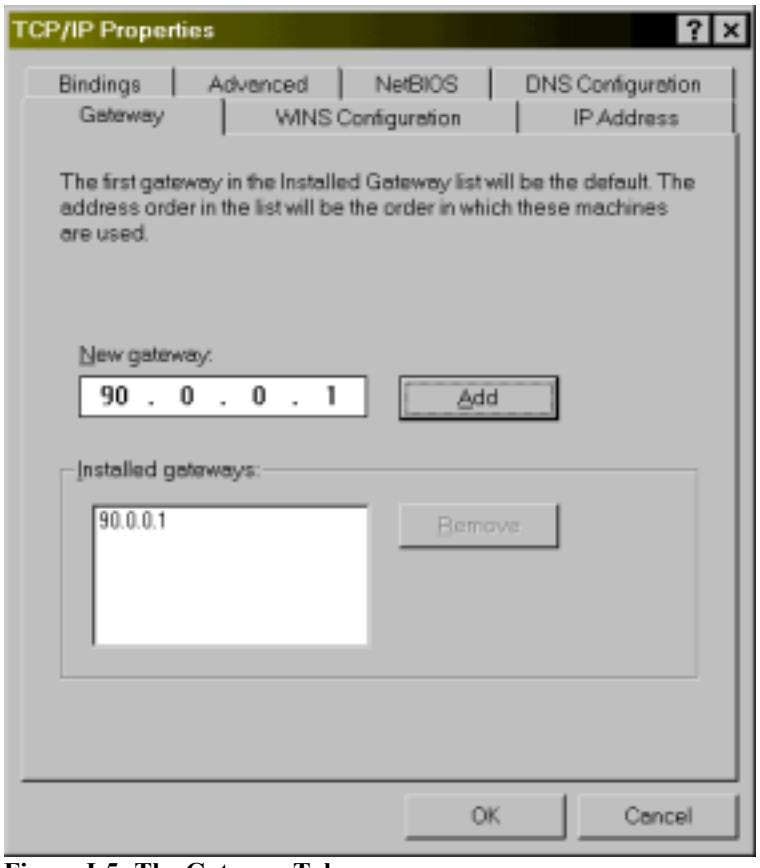


Figure I-5: The Gateway Tab.

For each network connection in which you specify an IP address—including OrbitNet's internal network connection—you must specify the gateway. The gateway address is the address of OrbitNet's internal network connection; each and every network connection on the local network needs that very same gateway address.

That's all that's required for basic network communication—and if basic communication is all you need, you can stop here.

However, if you're feeling daring, it's easy to add a couple of settings that may come in handy later. You'll only need these settings if you're specifying the IP address (or if you already have a DNS server on your local network and you prefer to use it). To proceed click on the DNS Tab:

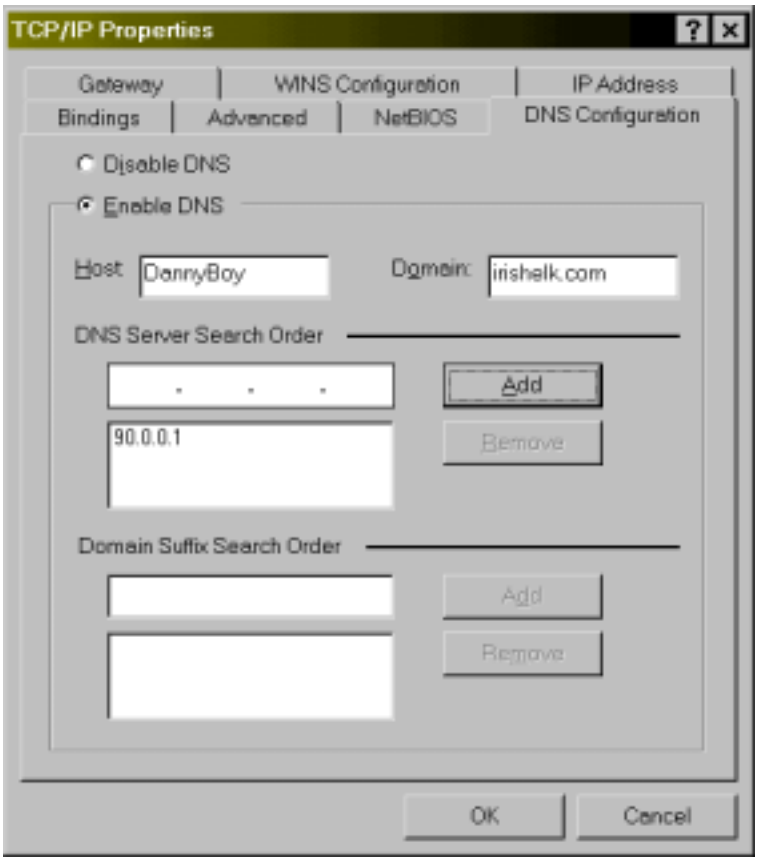


Figure I-6: The DNS Tab.

If you set the network IP address connection to "Obtain Automatically," it gets the DNS information as well (even if you've checked the "Disable DNS" box—it's not *really* disabled; it's merely obtaining settings from a DHCP server if one exists).

The setting for "DNS Server Search Order" is the OrbitNet internal IP address. Every machine on your local network uses the OrbitNet machine as its DNS server. The setting for the domain can be anything you like—as long as it's the same on *all* of your computers. The "Host" setting is the name of the computer you're currently configuring.

You don't need anything under the suffix search, and you don't need to add anything to any of the other tabs.

However, if you're playing around with the DNS settings, keep one thing in mind. The way you get to the DNS settings (by going through the TCP/IP settings) can be misleading. While TCP/IP settings are "per network connection," DNS settings are "per host." So, while a computer (a "host") can have as many TCP/IP settings as it does network connections, it can have only one DNS configuration. If you change a DNS setting while working on one network connection, you'll see that change reflected in every place that you find DNS settings. Why? Because, in the end, there can be but one DNS configuration.

Windows NT IP Address Settings

To begin, follow the path **Start\Settings\Control Panel\Network** to the Network screen:

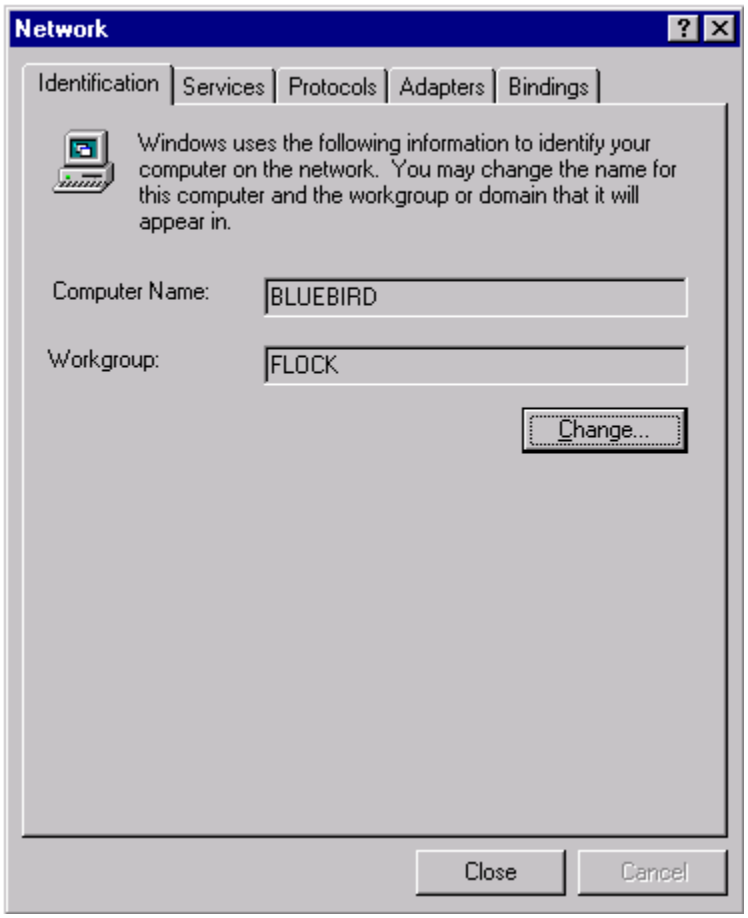


Figure I-7: The main Network screen.

The computer name should be a unique name given by you to the computer (it's best to change it from the default settings). The workgroup is also a name given by you: it should be the *same* for all of your computers. Now, click on Protocols Tab:

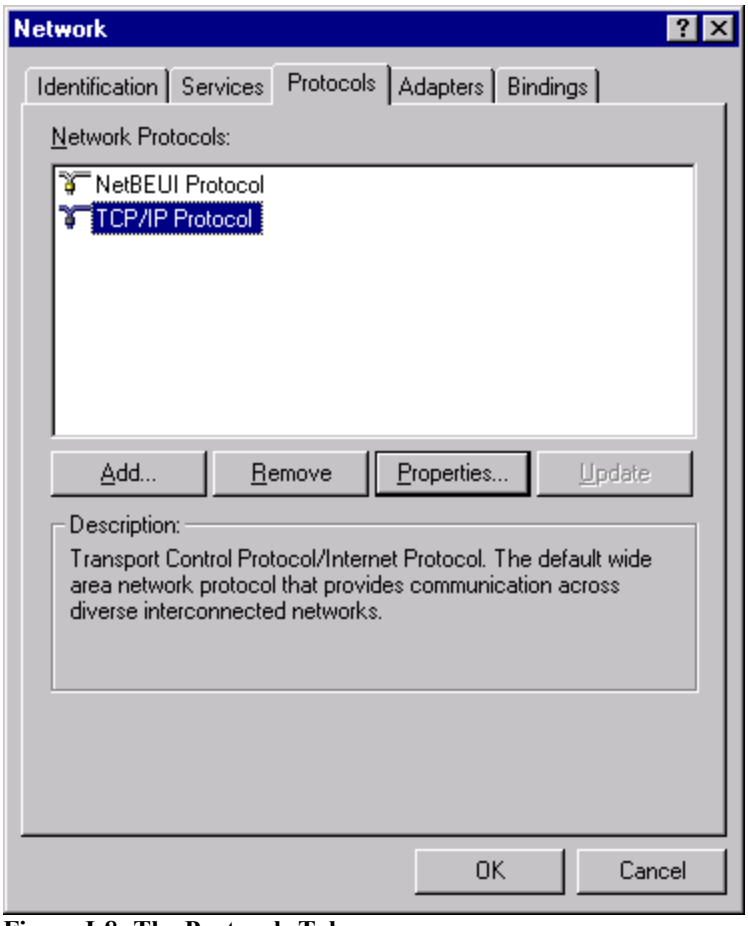


Figure I-8: The Protocols Tab.

Here you'll see the protocols that have been assigned ("bound") to the network adapters on this machine. TCP/IP and NetBeui is a good starter set. Highlight the TCP/IP protocol line, and click Properties. All network adapters recognized by the system are listed in the drop-down box. Choose the one you want, and you're ready for the settings:

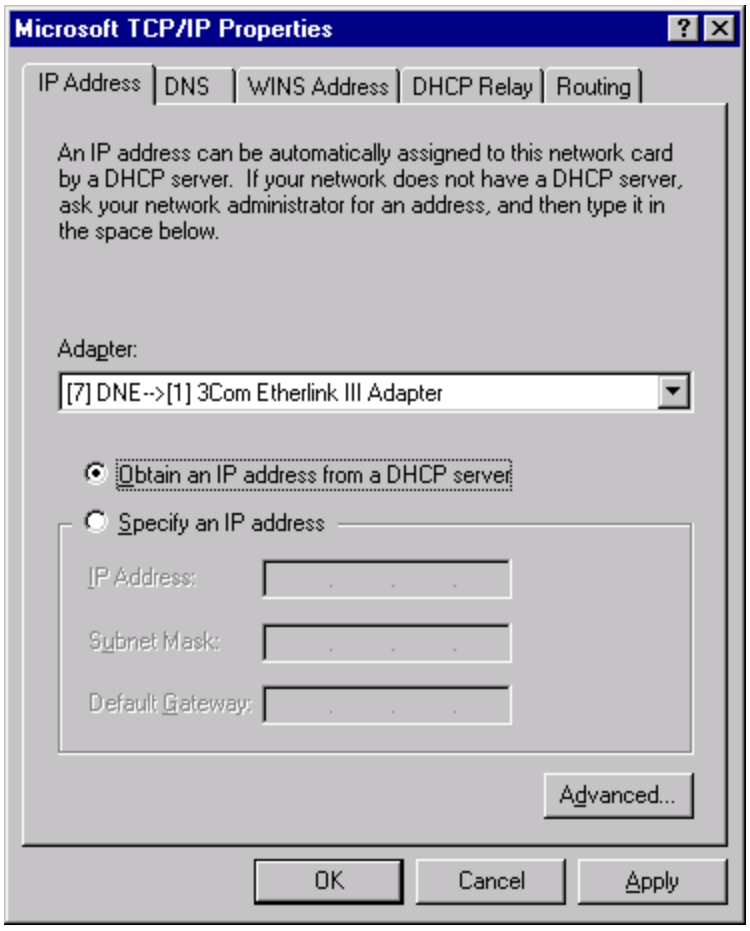


Figure I-9: Obtaining IP addresses automatically is the best way to go!

This setting shown here will allow the chosen network connection to obtain its IP settings from a DHCP server such as OrbitNet. We recommended this setting for all your client machines, especially if you're new to networking. The only place where you cannot use this setting is on the internal network connection of the OrbitNet machine. That connection must be a statically-assigned address.

You can assign a static IP address on that same screen. To do so, click "Specify an IP Address."

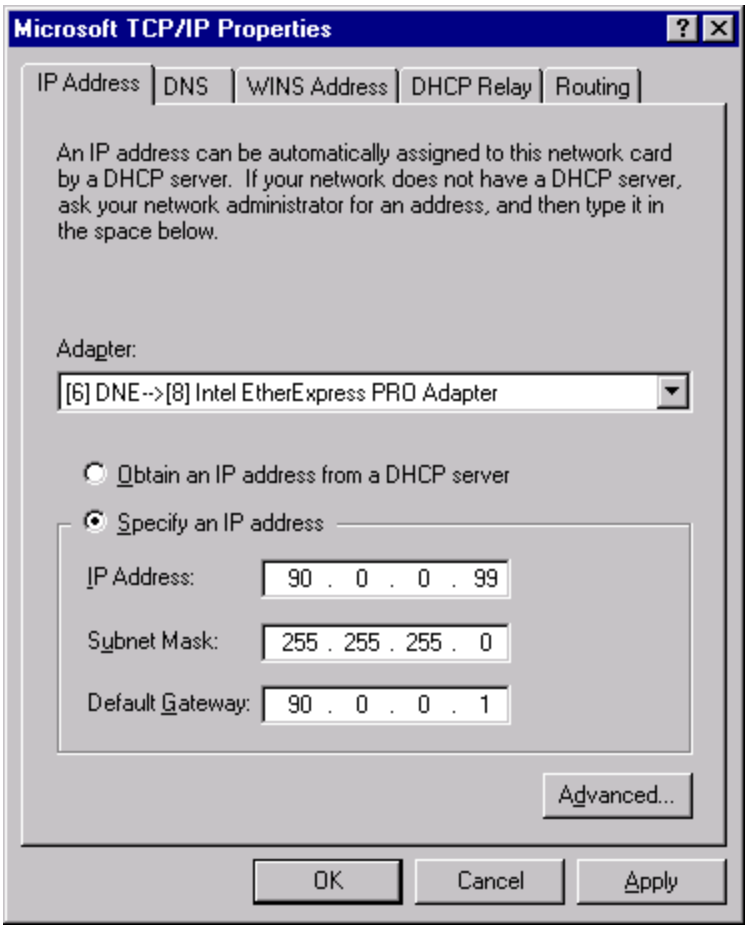


Figure I-10: Assigning a static IP address.

The settings shown here are for an NT client behind OrbitNet. This network connection has been assigned an IP address of 90.0.0.99; OrbitNet is at the IP address 90.0.0.1. To specify the IP address on any client machine (you can mix and match, having some specified and others obtained automatically), follow these rules for each additional IP address specified:

1. Each machine gets the same subnet mask as the OrbitNet machine.
2. Each machine gets a unique IP address. Having two machines with the 90.0.0.1 address, for instance, would confuse things. It's easier to remember addresses if you number them sequentially: the next machine is 90.0.0.2, then 90.0.0.3, etc.
3. You can use any number between 1 and 254. You cannot use 0, and you cannot use 255 or any higher number.

When setting unique addresses, you can make changes only in the IP address field corresponding to the '0' in the subnet mask. The IP fields corresponding to the '255' blocks in the subnet mask must be the same on all internal network connections.

On each network connection where you specify an IP address, you'll also need to specify the gateway. The gateway address is the address of the OrbitNet internal network connection. Each and every network connection on your local network must have that very same gateway address. If running OrbitNet on an NT machine, here's how to configure that internal network connection:

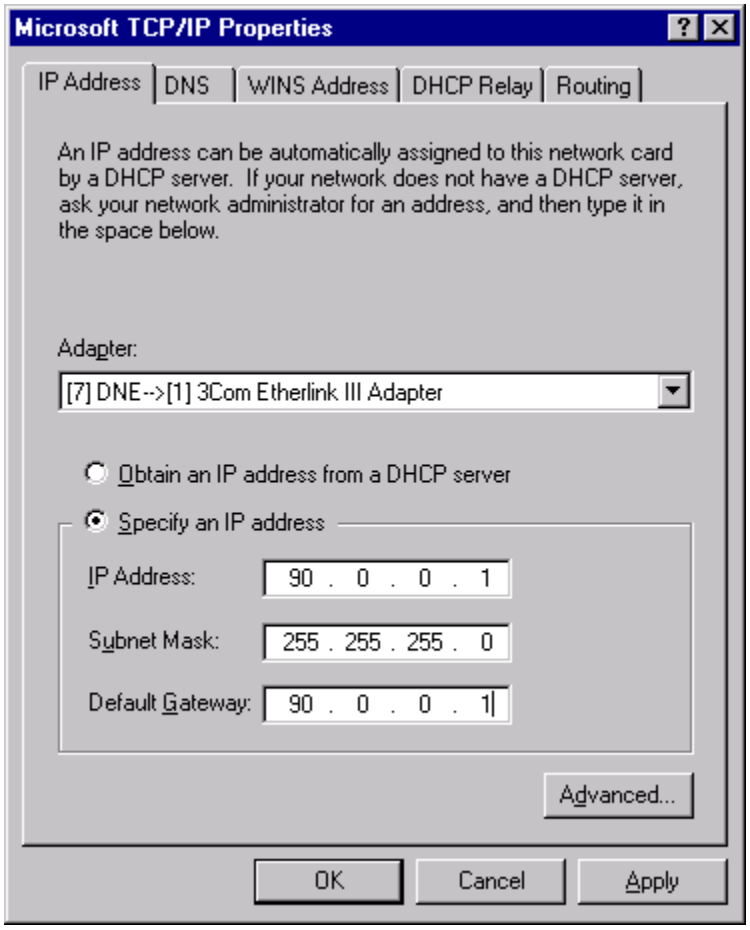


Figure I-11: Configuring the internal network connection.

That's all that's required for this machine to connect and communicate on a TCP/IP network. However, you can do one more thing to make your life easier down the road. Click on the DNS Tab:

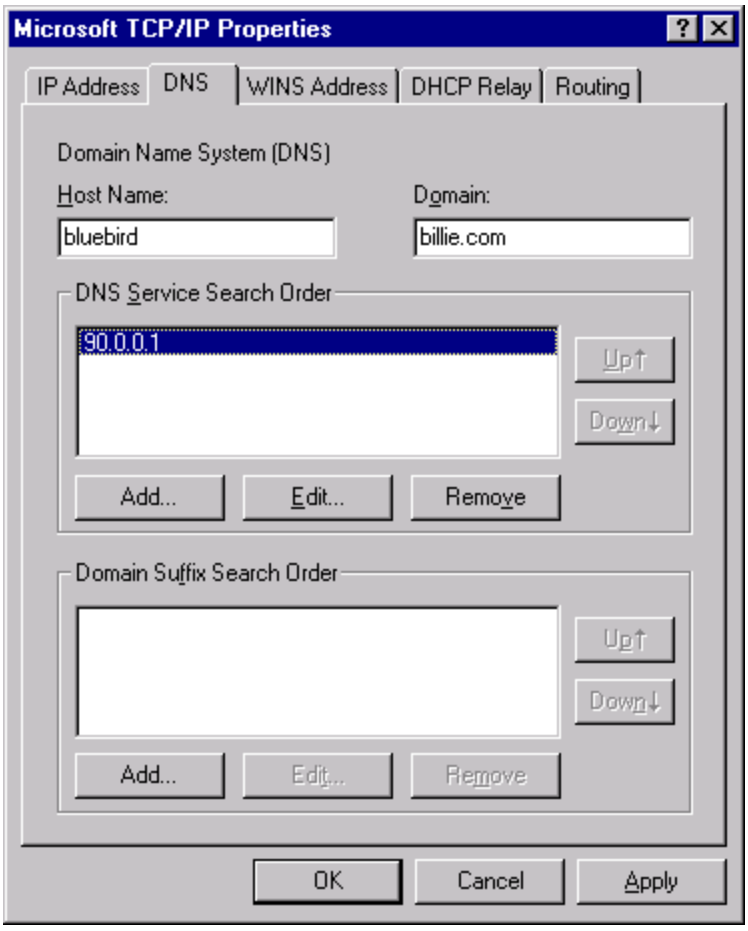


Figure I-12: Setting DNS information manually.

These settings are needed only if you're specifying the IP address. If you set the network IP address connection to "Obtain Automatically," it obtains the DNS information as well.

The setting for "DNS Server Search Order" is the OrbitNet internal IP address. Each machine on your local network uses the OrbitNet machine as its DNS server. The setting for the domain can be anything you like as long as it's the same on all computers. The "Host" setting is the name of the computer you're currently configuring.

You don't need anything under the suffix search, and you don't need to add anything to any of the other tabs.

Here's one last thing to keep in mind about DNS settings. While TCP/IP settings are "per network connection," the DNS settings are "per host." Thus, while a computer (or "host") can have as many TCP/IP settings as it does network connections, it can have only one DNS configuration.

Windows 2000 IP Address Settings

Note: At the time of this writing, Windows 2000 works as a platform for OrbitNet 2.1 only—not for 3.0. You can, of course, have W2000 as a client. We anticipate adding support for Windows 2000 shortly, so check back with us.

The path for the settings in Windows 2000 is a little different than the other Windows operating systems. To start with, you'll get access to the network settings by using the path **Start\Network and Dial-Up**:

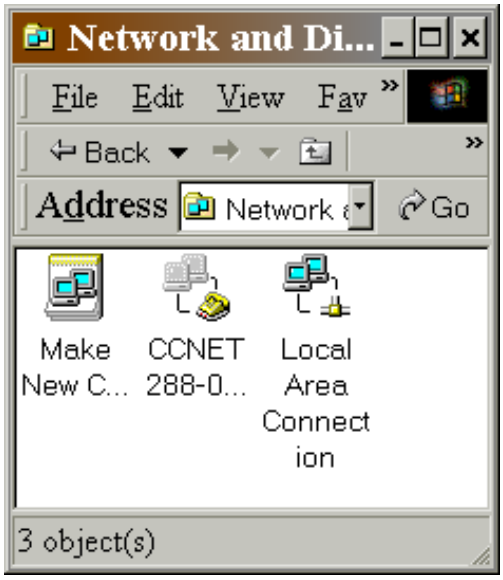


Figure I-13: The Dial-up Screen in Windows 2000.

To change the network settings on your Dial-Up Adapter, highlight the connectoid (here it's labeled 'CCNET 288-…) and then click on **File\Properties**.

We're going to *set* the network card, though. In this case, you'll highlight "Local Area Connection," click File, and then click Properties. You'll see this screen:

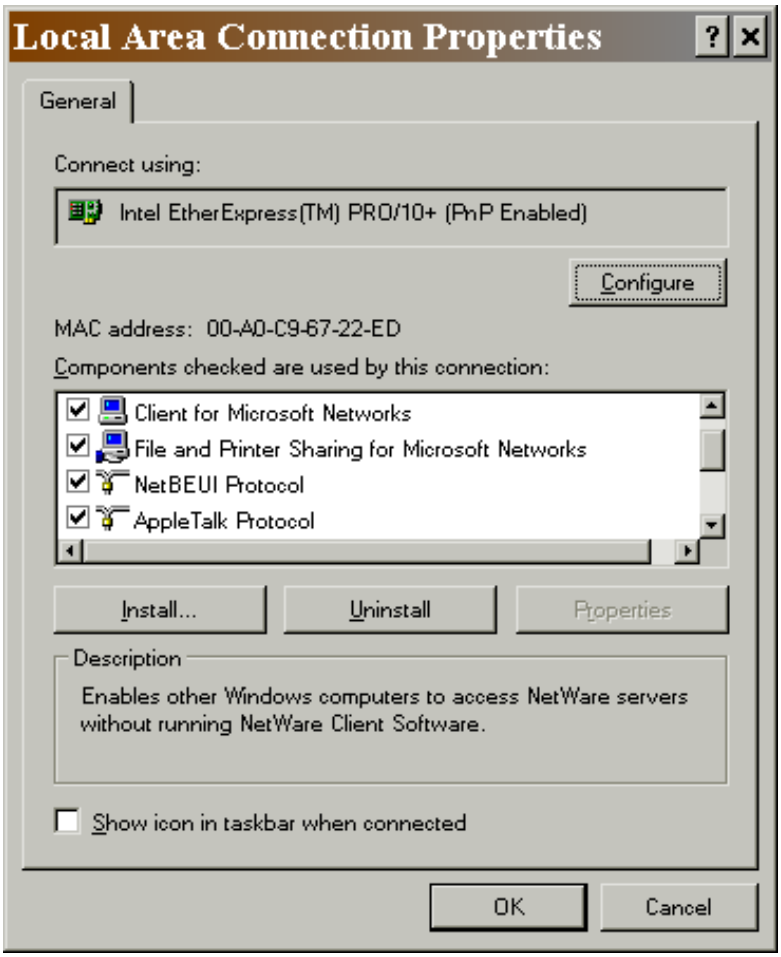


Figure I-14 Enabling network components.

In the example shown here, many components are enabled. They're not all needed with a simple network (and there's no problem enabling multiple protocols on your internal connections). For setting up your first network, a good starter set would be TCP/IP and NetBeui on the internal (or only) connection. Then you'll want to configure your TCP/IP settings:

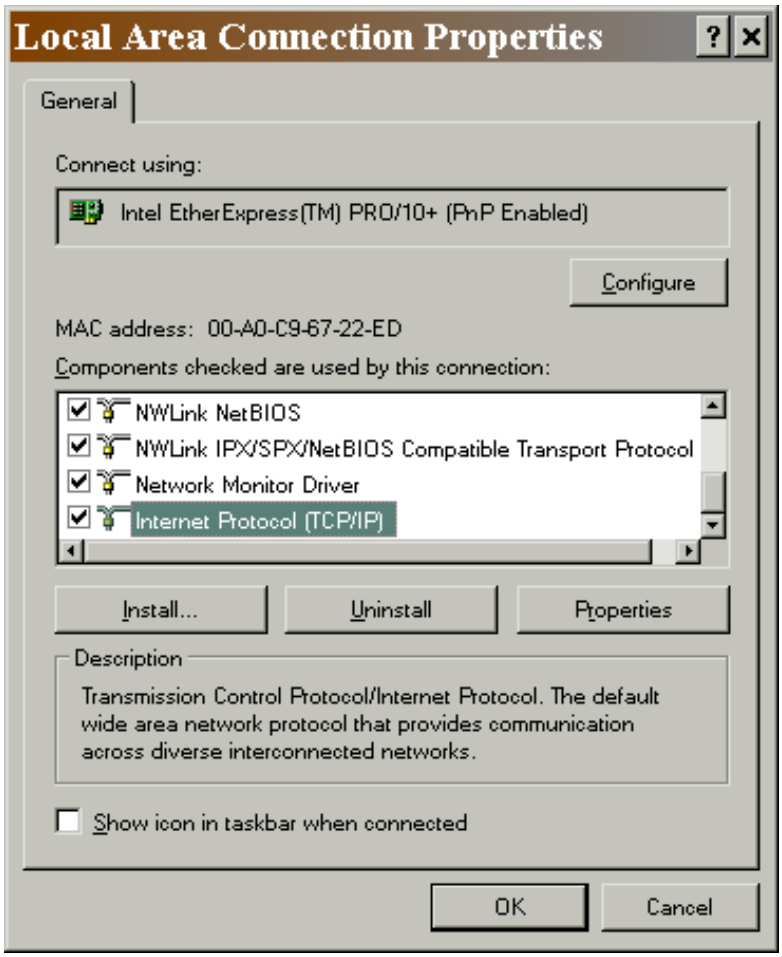


Figure I-15: TCP/IP is highlighted on the Local Area Connections Tab.

Find "Internet Protocol (TCP/IP)" in the list. Highlight it, click "Properties." You'll see the following screen:

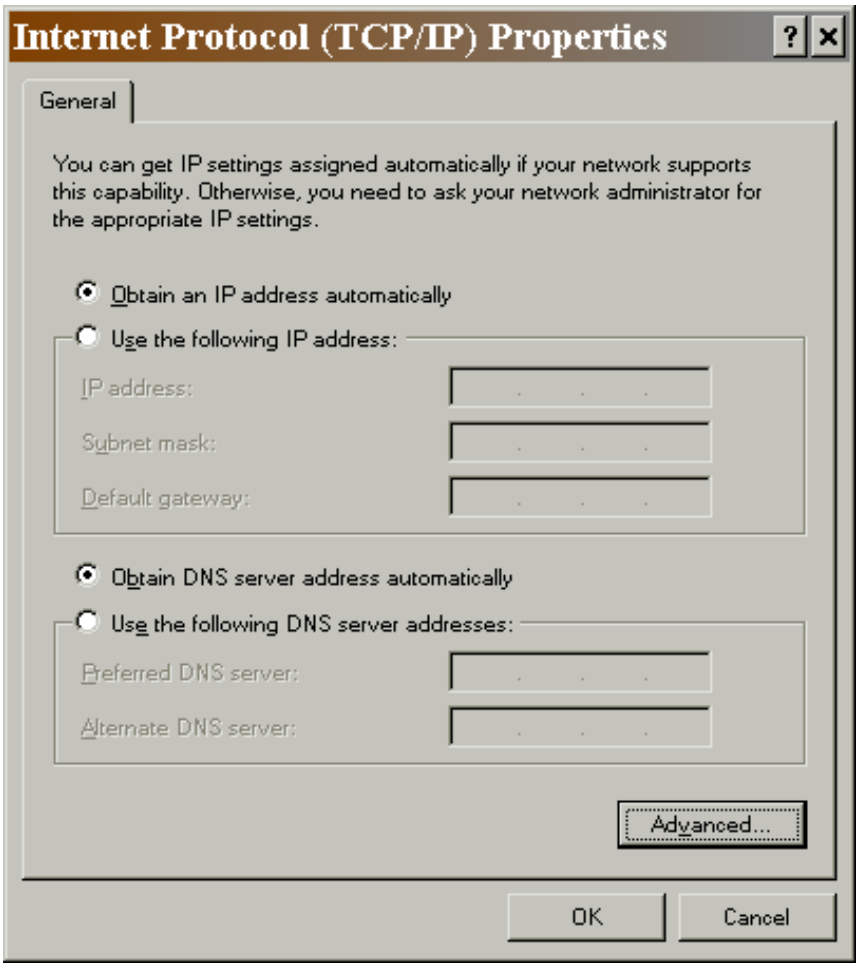


Figure I-16: How to obtain IP settings automatically.

If you want the machine to obtain IP settings automatically from OrbitNet, you're done. That's all there is to it!

If you want to make your own IP assignments, click on both "Use the following" buttons. Enter addresses as in this example:

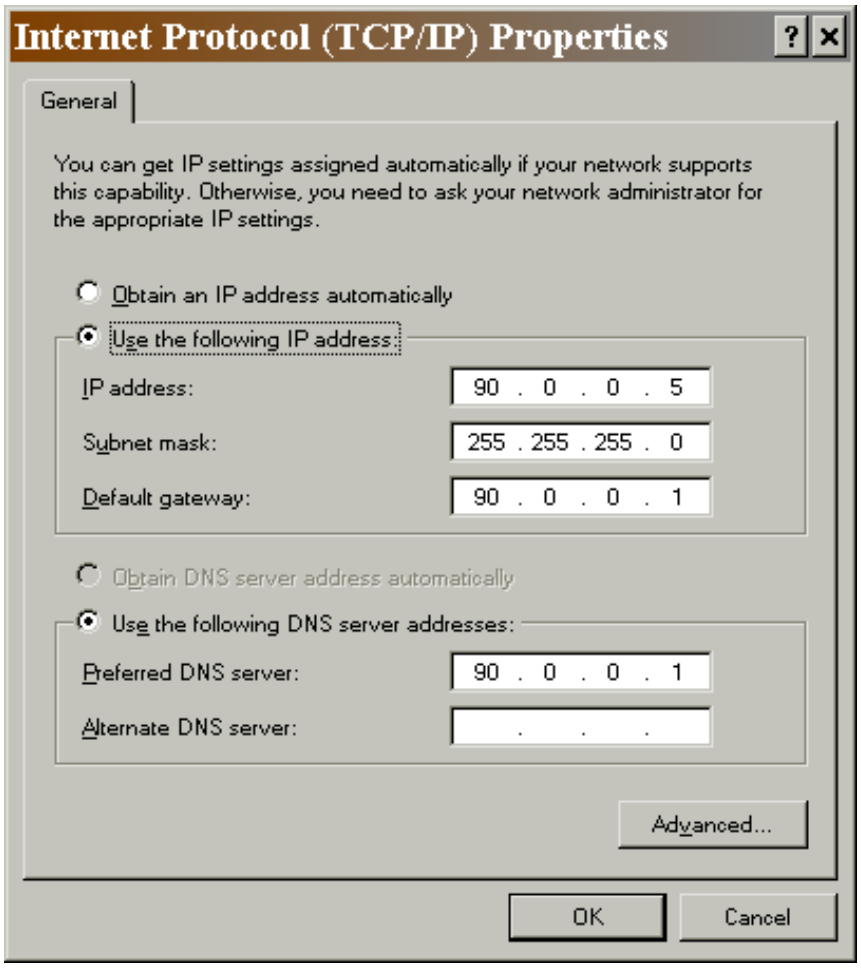


Figure I-17: Making IP assignments manually.

As shown here, the computer was given the IP Address 90.0.0.5. OrbitNet is at 90.0.0.1. (On a simple system, the gateway and DNS servers are always the OrbitNet internal address.)

There's a nice little touch in Windows 2000 that's different from earlier Windows operating systems: you *do not* have to reboot for your new tcp/ip settings to take effect.

In Windows 2000, the ComputerName and Workgroup configurations are found in a different place than the other network settings. Follow the click-path **Control Panel/System/Network Identification/Properties /Member of/Workgroup** to reach this page:

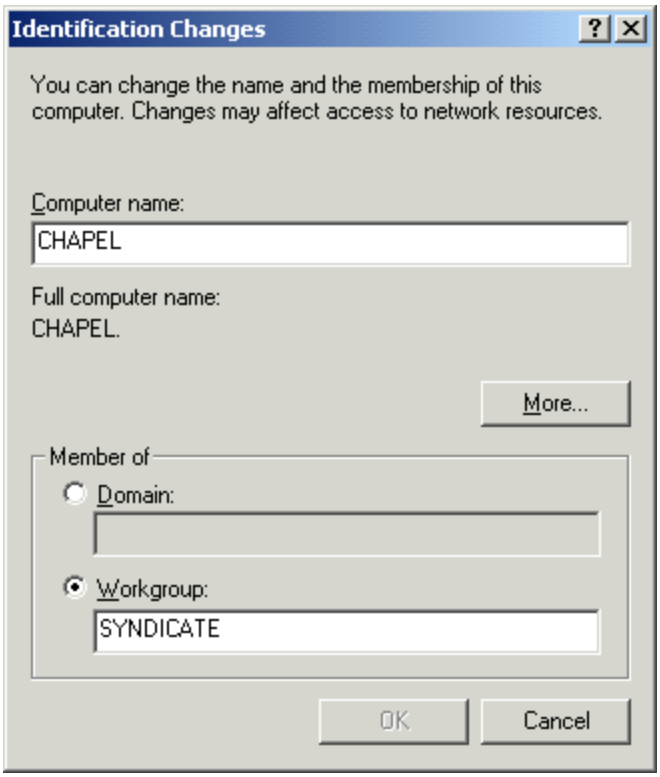


Figure I-18: Changing the computername in Windows 2000.

The computername must be unique to this computer. The workgroup name should be the same on all of your computers, at least on a simple network. It's certainly possible to use a Domain instead of a Workgroup, but it's a lot harder to set up. A workgroup is more than adequate for most local networks.

Windows 95 IP Address Settings

To begin, follow the path **Start\Settings\Control Panel\Network**. Double-click on the Network icon. You'll see a screen similar to this:

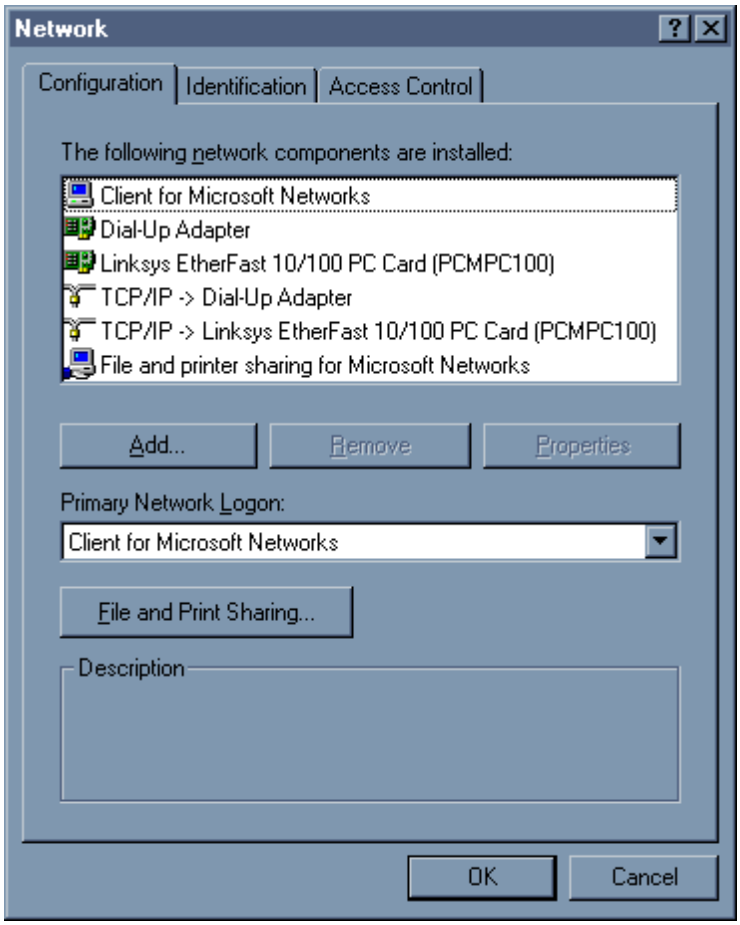


Figure I-19: The main Windows 95 Network screen.

We've cropped the screenshot, allowing you to see all the network services (like "File and printer sharing") in the window. If this is your first trip into this window, most likely you will see the line **NetBEUI → Linksys Etherfast** (or whatever brand your network adapter happens to be), and you won't see any TCP/IP lines. Windows 95 installs the NetBeui protocol by default; you must add any others that you want.

While here, examine the "Identification" tab. You may need to refer to a couple of its entries a bit later on:

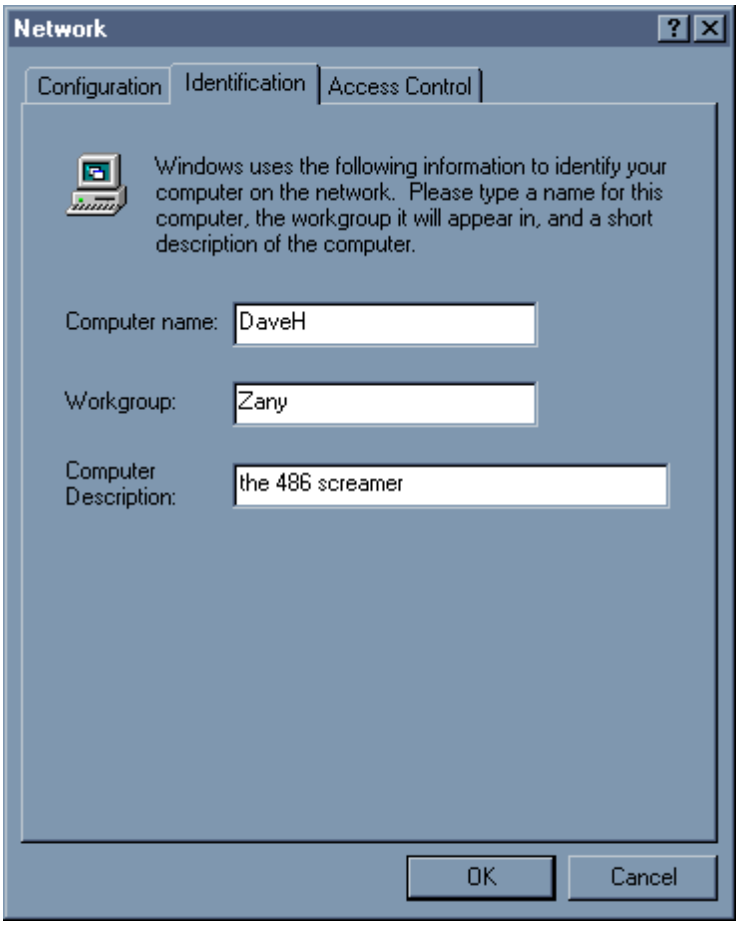


Figure I-20: The identification lists unique information about each computer in your network.

The ComputerName is the name of this particular computer. Make it something easy to remember. It should be a unique name on your network (you may need this name in few minutes). The workgroup is *not* a unique name—it should be the same on every computer. It's best to change this name from the default setting, using one of your own. Don't use punctuation in either name.

The computer description can be anything you like; it's merely a few helpful characters that show up in various windows when you're looking around your network.

If you need to add a protocol, first highlight the network adapter (we've taken the screen back to no protocols to make it simpler):

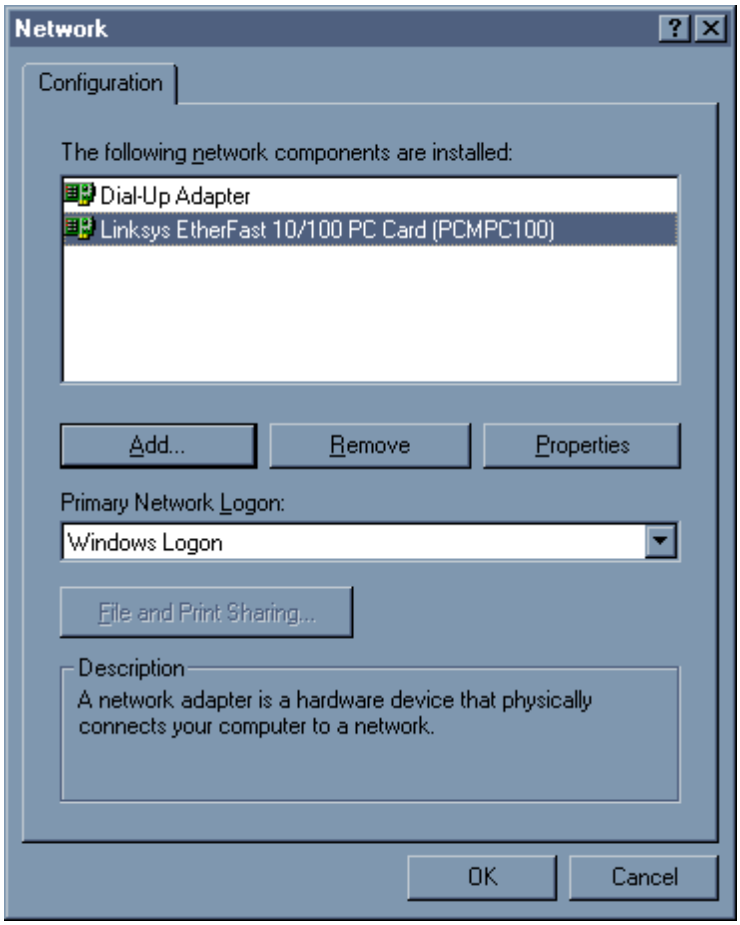


Figure I-21: Highlighting the network adapter.

Then click "Add." You'll see a list of things to add; we've chosen Protocols."

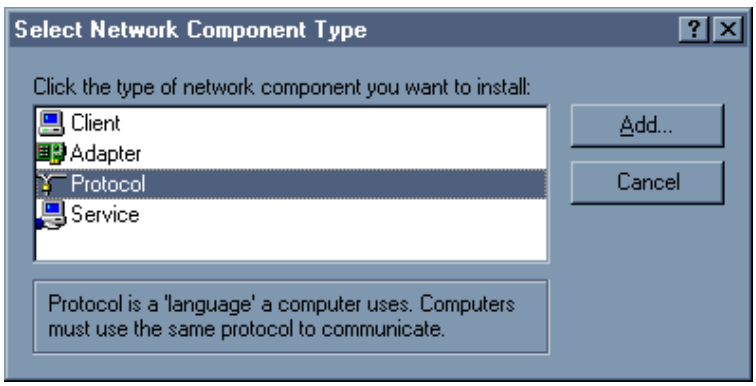


Figure I-22: Adding components.

Click “Add.” You’re presented with a list of manufacturers:

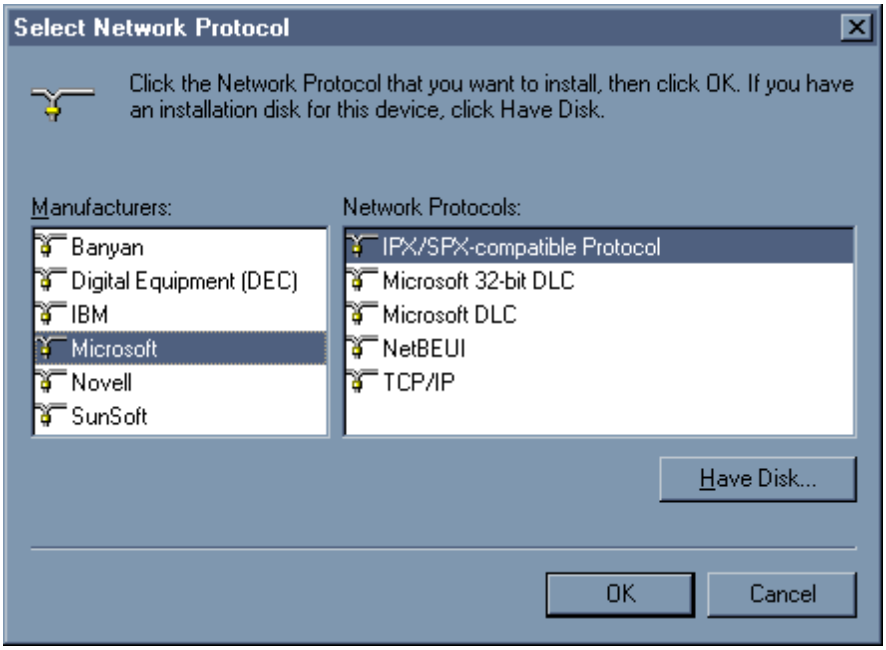


Figure I-23: A list of manufacturers makes the installation easy.

We’ve chosen Microsoft here—the Microsoft TCP/IP stack is the one supported by OrbitNet. Highlight “TCP/IP.” Click “OK.” When making network changes, take care to “OK” back out of the boxes; if you click “Cancel,” Windows drops your changes. You’ll need to add the TCP/IP protocol to your adapters one a time.

When adding protocols, examine the list of installed protocols in the network window. Windows 95 will add the NetBeui protocol at the drop of a hat; thus, if you add NetBeui to one adapter, it cheerfully adds it to all adapters. It’s okay if you have it on the internal network adapter (here, that’s the network card), and most people want it for file and printer sharing. But be sure it’s not installed on the external connection, assuming this will be the OrbitNet machine. To remove NetBeui where you don’t want it, simply highlight the line and click “Remove.”

Now, to configure your TCP protocol, highlight the TCP/IP line for the network adapter you’re working on:

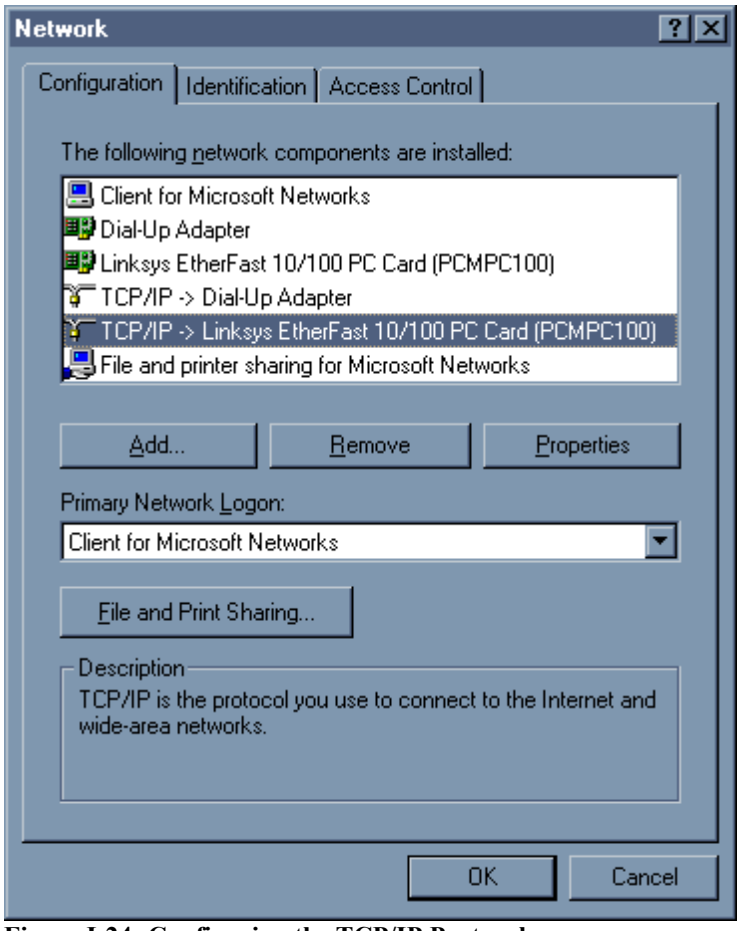


Figure I-24: Configuring the TCP/IP Protocol.

In this case, we've highlighted the network card, which means we'll be working on the internal network connection. If we had highlighted the line **TCP/IP → Dial-Up Adapter**, we'd be getting ready to work on the external network connection—the one to the Internet (assuming that this is the OrbitNet machine and not one of the clients). Once you've highlighted, click "Properties." You'll see a screen like this:

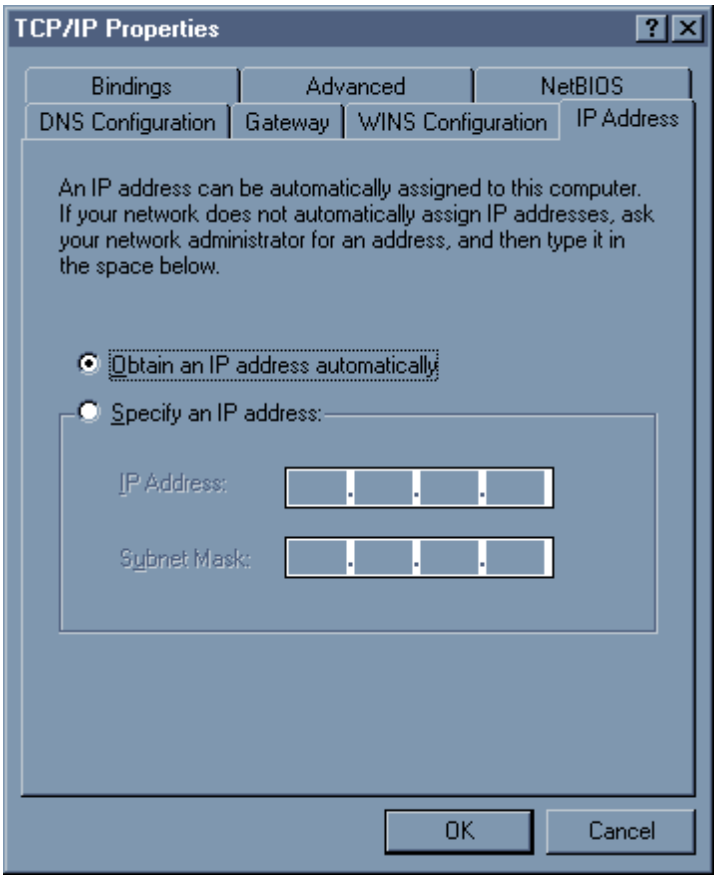


Figure I-25: Obtaining an IP address automatically is the way to go!

If this were a client machine, you could stop right here because OrbitNet supplies all IP settings automatically in a process known as "dynamic assignment" (which we recommend for new users). If you're working on the OrbitNet machine, then you'll have to do a static assignment. The OrbitNet internal connection is the one place on the network where you *must* have a static assignment.

To set a static address, start right here on this screen. Click "Specify an address," and enter an IP address:

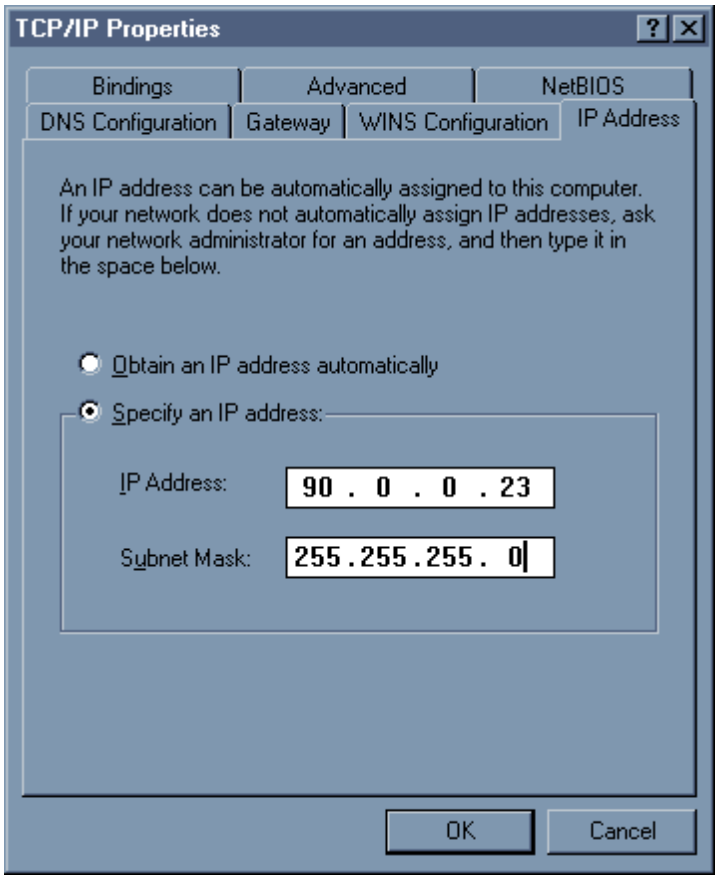


Figure I-26: Specifying a static address.

This is called a static address. It remains unchanged, even through shutdowns. We recommend the network address 90.0.0.1 for the OrbitNet internal IP address and others in the same network group for your client machines. However, you have a fair amount of latitude in assigning addresses as long as you follow some simple rules:

1. Each machine gets the same subnet mask as the OrbitNet machine.
2. Each machine gets a unique IP address, since having two machines with the 90.0.0.1 address, for instance, would confuse things. It's easier to remember addresses if you number them sequentially: the next machine is 90.0.0.2, then 90.0.0.3, and so on.
3. You can use any number between 1 and 254. You cannot use 0, and you cannot use 255 or any higher number.

When setting unique addresses, you can make changes *only* in the IP address field corresponding to the '0' in the subnet mask. The IP fields corresponding to the '255' blocks in the subnet mask *must* be the same on all internal network connections.

One last rule while setting things up. The address group you use *cannot* be the same as the address group used by your ISP, otherwise the TCP protocol becomes hopelessly confused. If your ISP gave you a static address, make sure to utilize numbers from a different group. If your ISP assigns a number to your modem

dynamically, utilize numbers from an IP address group that the ISP could never use (such as the 90.0.0.x group or the 10.x.x.x group).

Each network connection has its own TCP configuration. TCP/IP settings are "per connection," not per computer. If a computer has more than one network connection (your OrbitNet machine, for example) then each TCP/IP connection is configured individually.

When making a static IP assignment, you'll need to set a few things first. Click on the Gateway Tab:

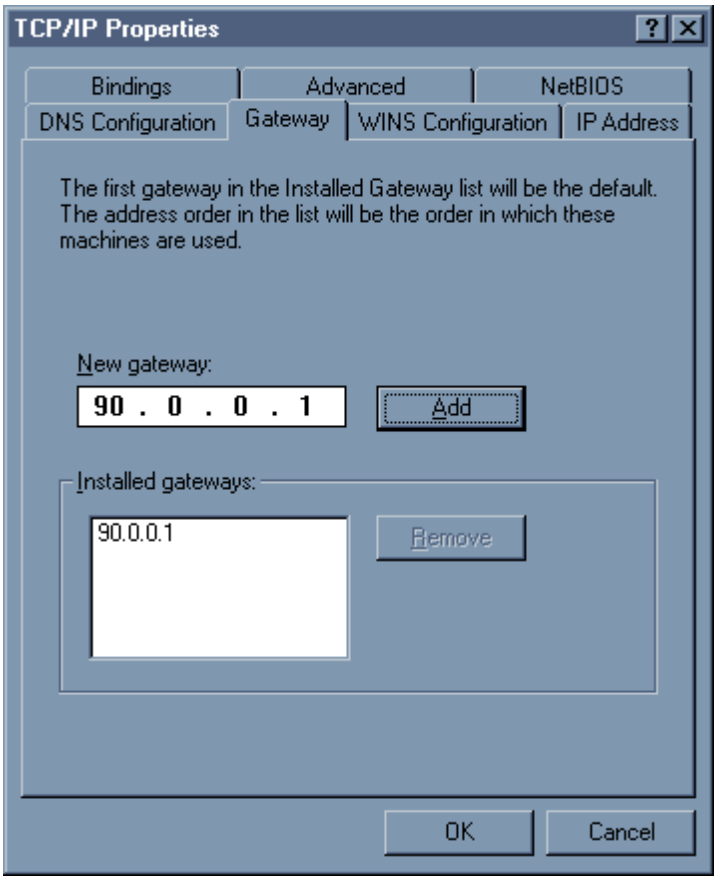


Figure I-27: Setting a gateway.

Use the OrbitNet internal IP address as the Gateway address on all internal network connections, even on the OrbitNet machine itself. On a simple network, use it on every network connection *except* the OrbitNet external connection. The gateway setting here will be dictated by the ISP if they've provided you with a static address, or will be assigned via your ISP's DHCP server if you have a dynamically assigned Internet address.

That's all you'll need for basic browsing. However, you'll likely soon find that you'd like to accomplish more tasks for which you need to use DNS. While you're here, it's an easy matter to think ahead and set up DNS. To do so, click on the DNS tab:

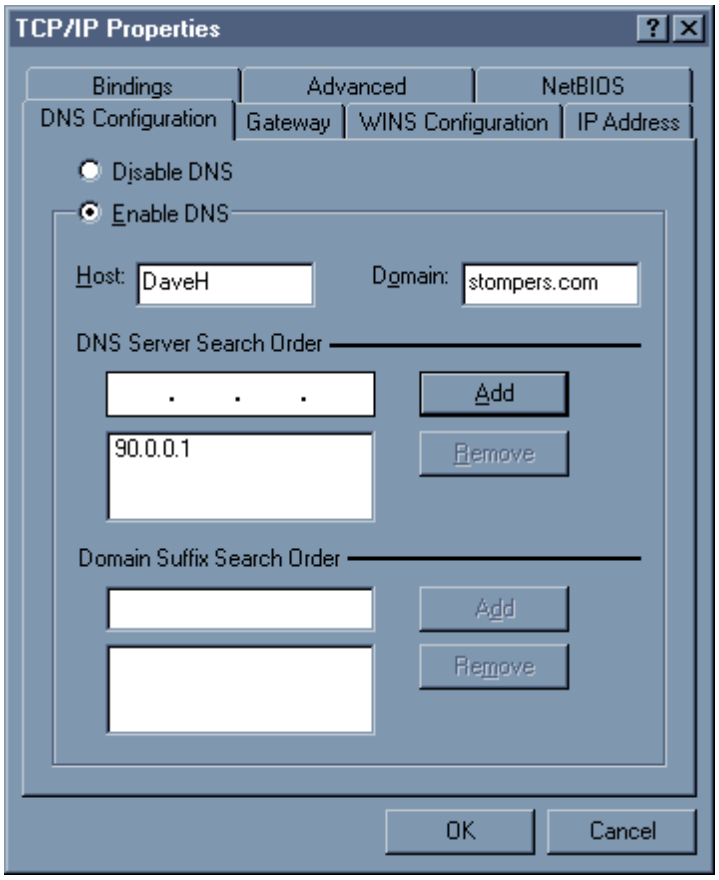


Figure I-28: The DNS Tab.

Now, a quick word about DNS. DNS—Domain Name Service—is a sort of adjunct protocol to TCP/IP. It's a method for Internet applications to use names to get IP addresses. The way the Internet works, you can't send packets unless you (meaning "the application") know the numeric IP address. You should enable DNS on all of your machines…

And this brings up a crucial difference between DNS and TCP. Where TCP is "per connection," DNS is "per computer." Each computer can have only one DNS configuration. If you change it in one place on the computer, you'll see changes everywhere. It's a bit misleading to access DNS via the TCP/IP properties if you don't already know it implies something that may not be so.

On each machine you'll want to put in the OrbitNet internal IP address—90.0.0.1 if you use the numbers we suggest—as the number in the "DNS Server Search Order." You don't need anything in the "suffix" box. Take a look at the setting in the "Host" box: put the Computer Name we told you about at the beginning of this section. For each computer, enter that computer's name in the Host box.

Finally, everything works better if you enter a domain name. If you don't have one, make one up. Yours is a private network, so you don't have to register it or anything. Use the same domain name on all machines.

APPENDIX J:

Alert Rules

Overview: Alerts

This section covers the use of alerts and their configuration, available under the **Alerts** menu in OrbitNet. Alerts can be used to notify the system administrator when certain events take place. For example, it is especially important to know when OrbitNet catches a virus being sent through SMTP because this means that the virus resides somewhere on your network. The alert can take several forms, including sending an email message and writing to a log file.

A. THE ALERTS MAIN SCREEN

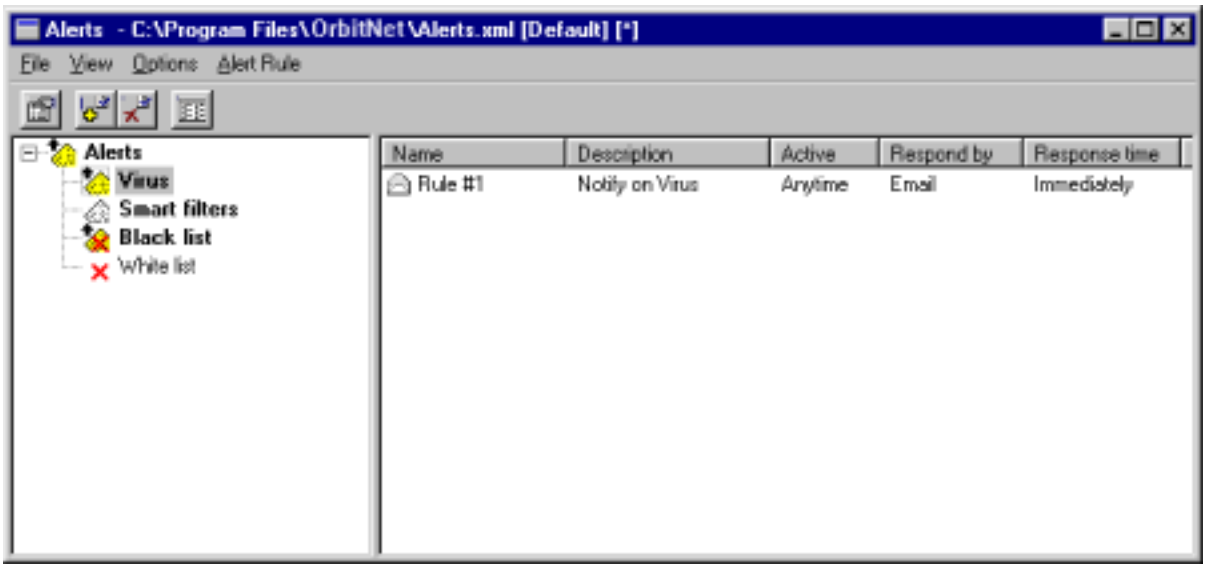


Figure J-1: The Alerts main screen. Rule #1 is a Virus rule.

There are two items in the **Alerts** menu: **Set Rules** and **View Logs**. Choosing **Set Rules** will open the Alerts main screen. This screen is made up of the Menu Bar, Tool Bar and two window panes. The left pane lists the different types of alerts in a tree view. It is organized by the type of event that triggers an alert. The right pane displays individual alert rules. Selecting a type of event on the left reveals the individual rules associated with that event.

MENU BAR

File Menu: The Alert Settings dialog box lets you configure general alert settings. These settings apply to all alerts; properties for individual alerts are configured by editing each rule.

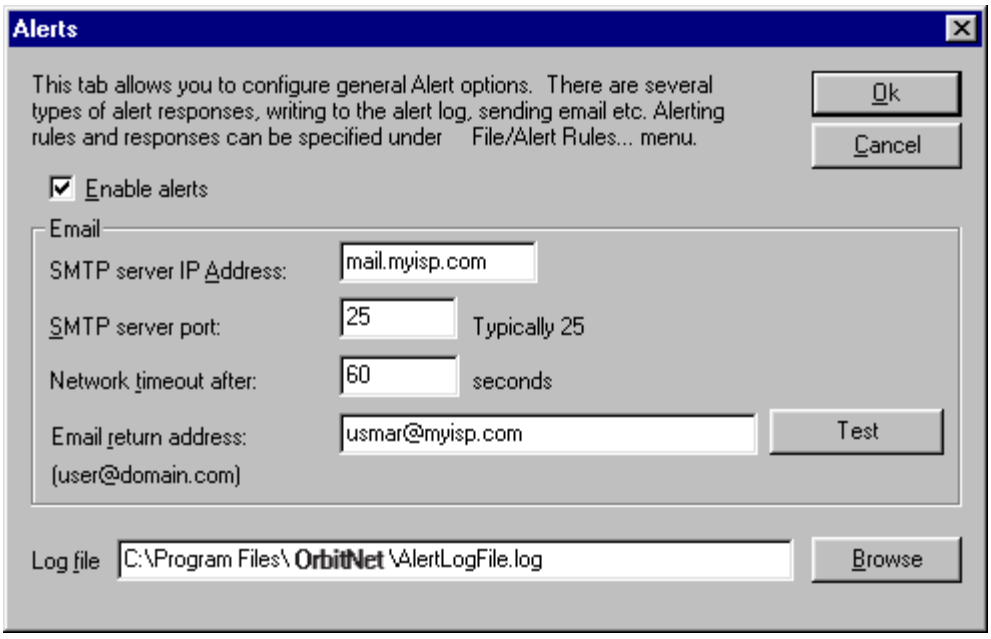


Figure J-2: The Alert Settings dialog box controls the basic behavior of Alerts.

When the **Enable Alerts** box is checked, OrbitNet will apply all alert rules defined in the Alerts main screen. If this box is unchecked rules will not be applied, even if they are defined.

Among the alert features is the ability to send alerts via Email. In order for OrbitNet to send an alert, it must know which mail server to use. The SMTP server IP address is the address of the mail server. This server is probably the same server that you use to send your own email. If you do not know the name or IP address of you SMTP server, you should be able to find it in the settings section of you email program (Outlook, Eudora, etc.). The return address for the Alert Email can be any email address you specify. Some SMTP servers require that the return address be a valid email address on that server, so be careful that your server will accept the outgoing mail from OrbitNet. OrbitNet will try to connect to the Mail Server on the port you specify.

Some alerts are written to a log file in addition to or instead of being sent via email. The **Log file:** filename box is where you can tell OrbitNet where to keep your default log file. You can call it anything you want, although is should be of the type ".log". The log can be kept in any directory you choose. Just make sure there is enough space on the drive.

You may keep more than one set of alert rules on the OrbitNet computer. It may be convenient to have several alert definition files with slightly different rules to be enforced at different times. The file menu is where you choose which set of rules you are using. Each set of rules is saved as an ".xml" file. OrbitNet uses a file called Alerts.xml in the OrbitNet directory by default. Commands in the File menu allow you to create new alert definition files or open, save, or set a new file as the default.

View Menu: The View Menu affects the layout of the two panes in the window. The top two commands, **Expand All** and **Collapse All**, affect the tree view in the Left Pane. The lower commands affect the view of the Right Pane. They work just like the same commands found in the View Menu in Windows Explorer.

Options Menu: This menu allows you to determine characteristics of rules already established. The **Disable** option can work two ways. If a rule or rules are selected in the Right Pane and this option is selected, those rules will be disabled. The disabled rules will be marked with a red "X" in the Right Pane. If a heading in the Left Pane is selected, **Disable** will affect all rules under the heading. This will be marked by the yellow rule icon turning gray. The **Don't trigger parent Alerts** option can be used to avoid

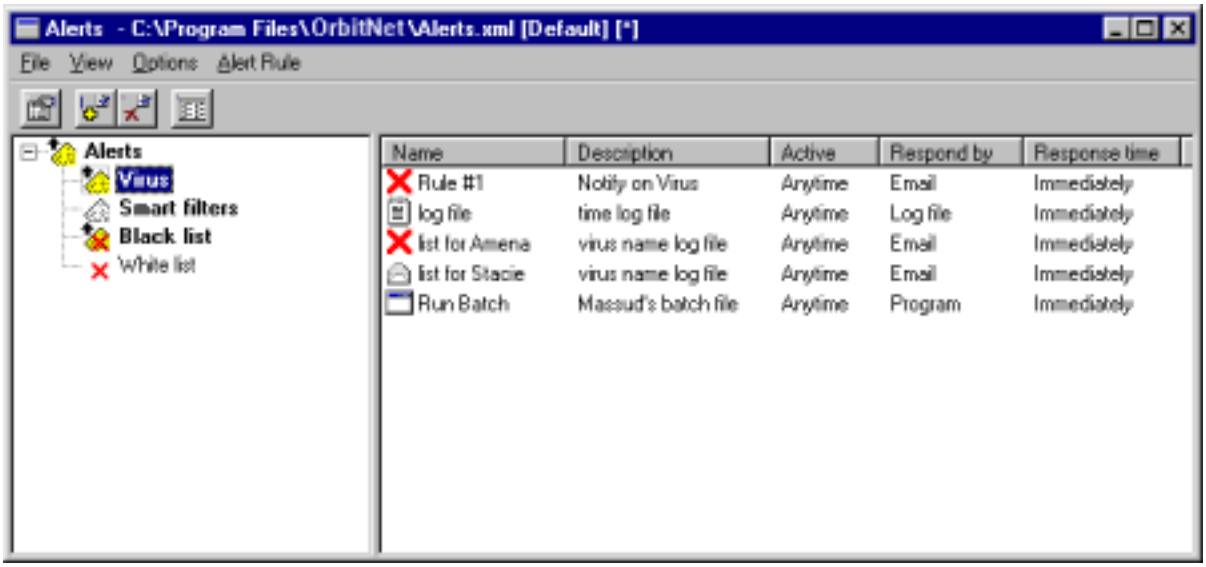


Figure J-3: All Smart Filter rules are disabled, and two individual rules under Virus are disabled.

sending multiple alerts for the same event. Consider, for example, the case of two alert rules. One is defined under the Black List heading and the other is defined under the Alerts parent heading. Ordinarily, an event that would trigger the Black List rule would also trigger the Alerts rule. By activating the **Don't trigger parent Alerts** option for the Black List heading, the Alerts rule will not be triggered.

> **Note:** This option applies to headings and sub-headings in the Left Pane only. If a particular heading has more than one rule, selecting only one of those rules and then choosing the **Don't trigger parent alerts** option means that none of the alert rules in the heading will "cascade up" to other headings.

Alert Rule Menu: The Alert Rule Menu contains commands that affect the rules listed in the Right Pane of the window. Cut, Copy and Paste can be used to place copies of rules under different headings. Add is used to create new rules, and Properties is used to edit individual rules that have already been created.

TOOLBAR

The Toolbar contains easy shortcuts to commands otherwise found in the Menu Bar. Hovering your mouse pointer over each icon will give you a tool tip that names the command. The commands are **Enable**

Alerts from Settings; **Properties**, **Add**, and **Delete** from the Alert Rule Menu; and **Next View Mode** from the View menu.

LEFT and RIGHT PANE

The majority of the Alerts main screen is taken up by the left and right panes of the window. This display works much the same way as the familiar Windows Explorer program. The tree of headings and sub-headings on the left lists the types of alerts possible, and the pane on the right lists specific alert rules. Each heading on the left can have its own set of alert rules. The headings are marked by various icons representing different conditions.

Icon States	
No Icon	No rules are defined for this heading
Yellow Rule	Rules are defined, and at least one is active
Grey Rule	Rules are defined, but none are enabled
Up Arrow	Trigger Parent Alerts is turned on
Red "X"	The feature is turned off in OrbitNet

When a heading is selected, a small box appears around the icon, and the individual alert rules for that heading are displayed in the Right Pane. When the Right Pane is in "Detail" view, the rules can be sorted by clicking on the column heading. Clicking on the Name column will alphabetize the rules.

OrbitNet still stops the virus!

Keep in mind that all alerts are triggered when OrbitNet detects an *attempt* to make one of these transgressions. When a virus is detected or a Black list rule is triggered, OrbitNet still keeps the virus from reaching its destination or keeps the user from reaching the disallowed web site.

Alerts: This is the master heading. Any rule placed in this heading will be triggered whenever an event occurs, regardless of the type of event. The only time that this is not true is when a heading below it has been disabled. If the Smart filters heading has been disabled (the icon will turn gray), a rule placed in the Alerts heading will be triggered by a virus, black list, or white list violation, but it will not be triggered by the Smart filter.

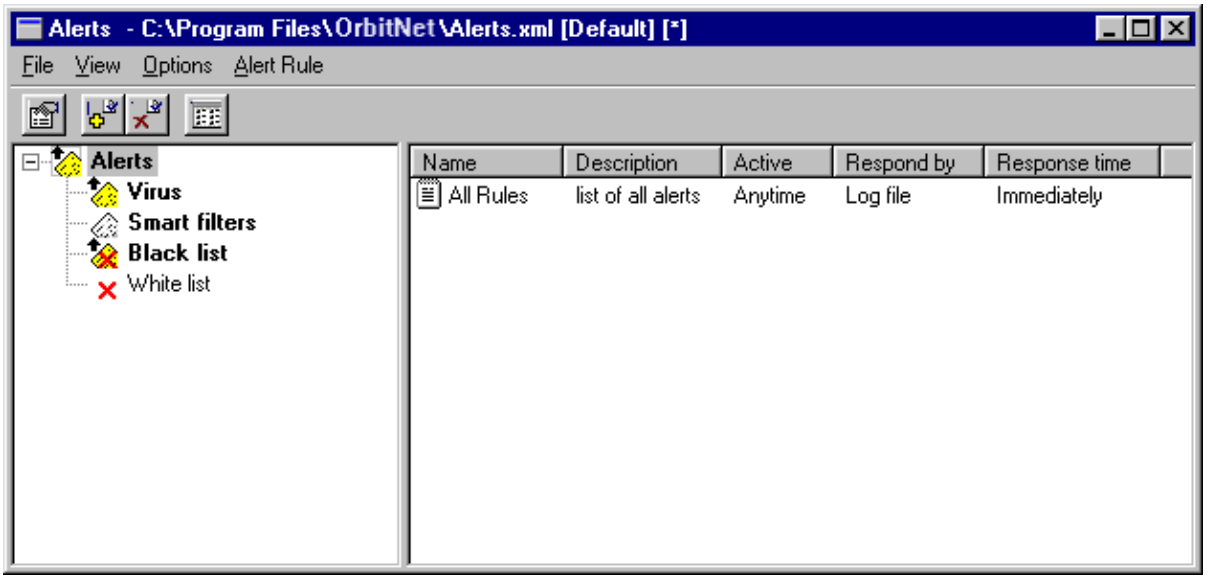


Figure J-4: The "All Rules" alert will not be triggered by a Smart Filter event because Smart Filter rules are disabled.

Virus: A Virus rule would be triggered each time OrbitNet detects a virus. If rules are defined under the Virus heading, OrbitNet eliminates the virus first, then performs the instructions contained in the rule. A Virus rule can be limited to being triggered only by certain methods of transport. These settings are found in the individual Properties for each rule. A virus can arrive on your network in a file obtained through File Transport Protocol (**FTP**), or from a web page (**HTTP**) or via email. **POP3** is incoming email (mail you receive from others) and **SMTP** is email you send out. In the case of SMTP, OrbitNet is protecting the recipient of the message; it keeps you from sending a virus to your friends.

Warning!!! If OrbitNet detects a virus that is being transported via SMTP, it means that you have the virus on your network already! OrbitNet will keep you from spreading the virus, but you must find it and eliminate it from your network. A good Alert Rule will tell you the sender of the virus and the name of the virus: this should be enough to track it down.

Smart filters: If you have purchased a SmartFilter license, you can send an alert each time a computer on your network tries to access a forbidden site.

Black list and White list: These alerts are triggered in the same way as the SmartFilter alerts. If you enforce a Black list or a White list, you can make an alert rule to notify you when an attempt is made to access a site that is disallowed. Like Virus rules, Black list and White list rules can be limited by transport protocol.

CREATING ALERT RULES

An alert rule can be added by choosing **Add** from the Alert Rule menu, or Right-Clicking on a heading and choosing **Add Rule**, or by Right-Clicking in the Right Pane of the window and choosing **Add**. When you add a rule, you are presented with a Properties box for the new rule. The Properties box is at the heart of alert rule-making. It has three tabs where you will define how each rule operates.

General tab: The General tab allows you to give the rule a name and a description and if appropriate, transport protocols. There is also a checkbox for disabling the rule. A disabled rule appears in the Right Pane with a red "X" icon. It can be re-enabled by opening the properties and deselecting the Disabled checkbox. Virus, Black List, and White List rules can be limited by which method of transport will trigger the alert. By default, all transport protocols are enabled, but you can turn them on or off individually.

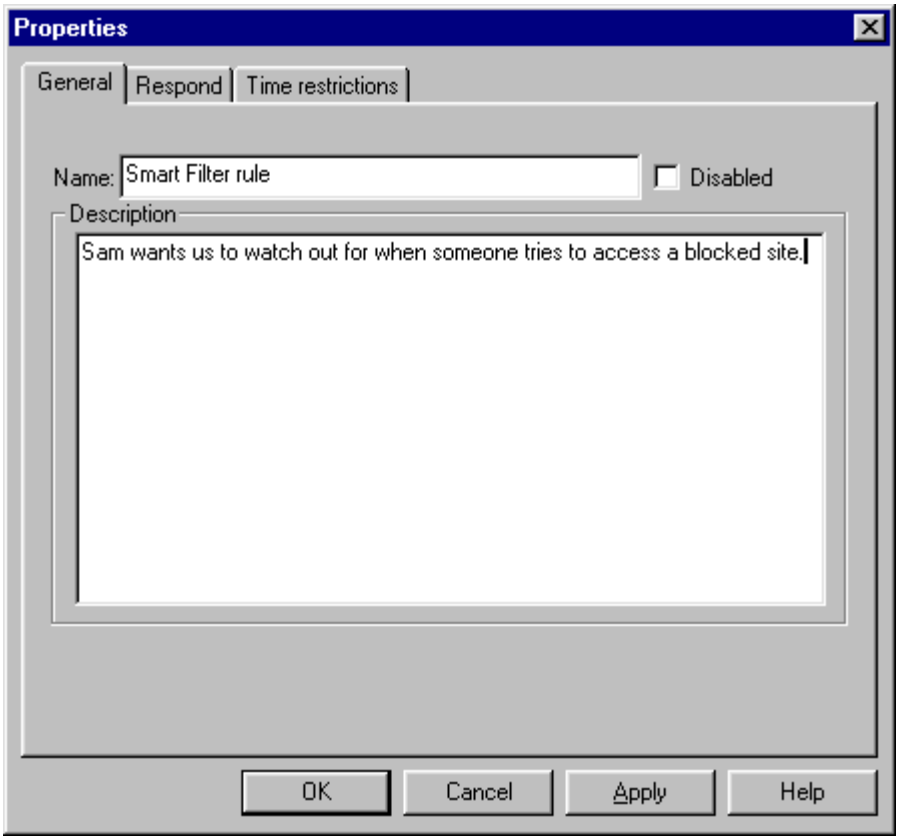


Figure J-5: The General tab allows you name and describe the rule.

Respond tab: There are four ways that an alert rule can respond to an event. It can send an **Email** or a **Message**, write an entry into a **Log File**, or run a **Program**. When sending an Email, the respond tab asks for an email address (usually the address of the system administrator) in the form: *name@isp.com*. It also provides boxes where you can enter the subject and text of the message. The *Insert Auto Text* drop-down box contains a list of variables that can be generated in each alert. For example, your email message to the system administrator can contain the name of the virus that was caught or the user that was sending it.

The **Message** type of rule is only available in Windows NT and 2000. It will send a message to the destination using the Net Send method.

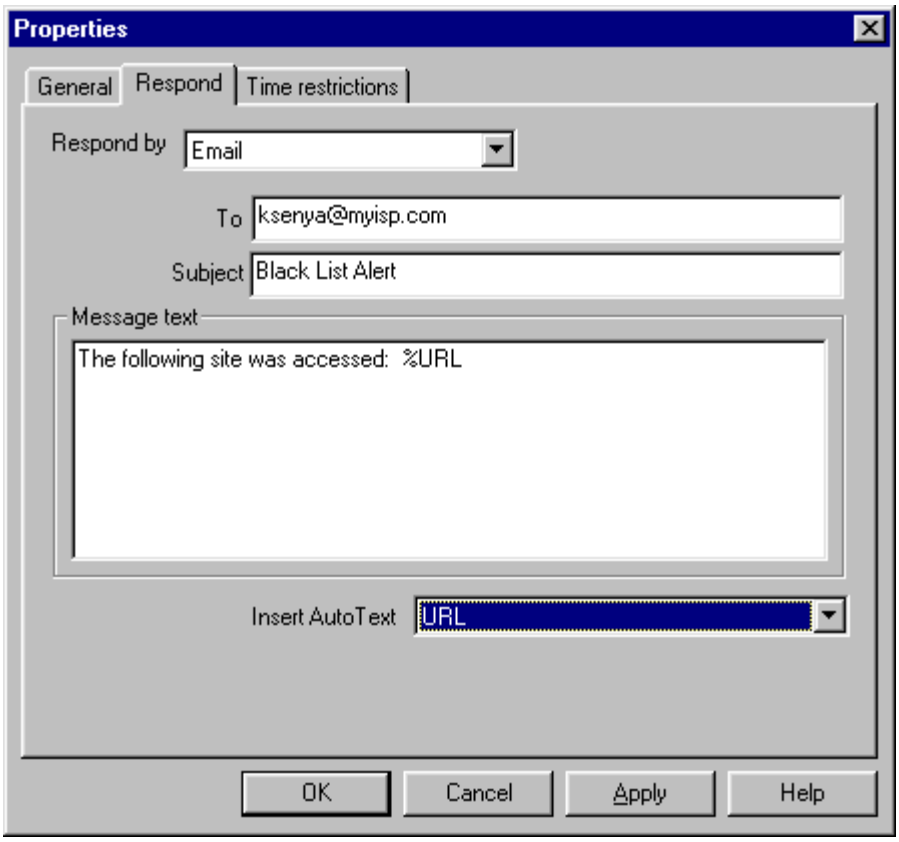


Figure J-6: This alert rule will send an email message to the recipient specified.

A rule that writes to a Log File will add an entry to the file whenever the rule is triggered. The entry will contain the text typed into the Message Text field and can contain Auto Text. If **Use default log file** is checked, the log file entry field will be disabled and OrbitNet will write to the default log file defined in the Alert Settings dialog box (File/Alert Settings). If this box is unchecked, you may enter the name and location of any log file you wish. You may have as many log files on the OrbitNet machine as you wish. In fact, you might find it convenient to keep a different log for each type of alert.

When you choose **Program** in the **Respond by** drop-down box, OrbitNet will run a program that you specify each time the rule is triggered. This can be *any* program, including batch files. Running programs and batch files, combined with the option of including command line parameters, makes the Program option extremely powerful and flexible.

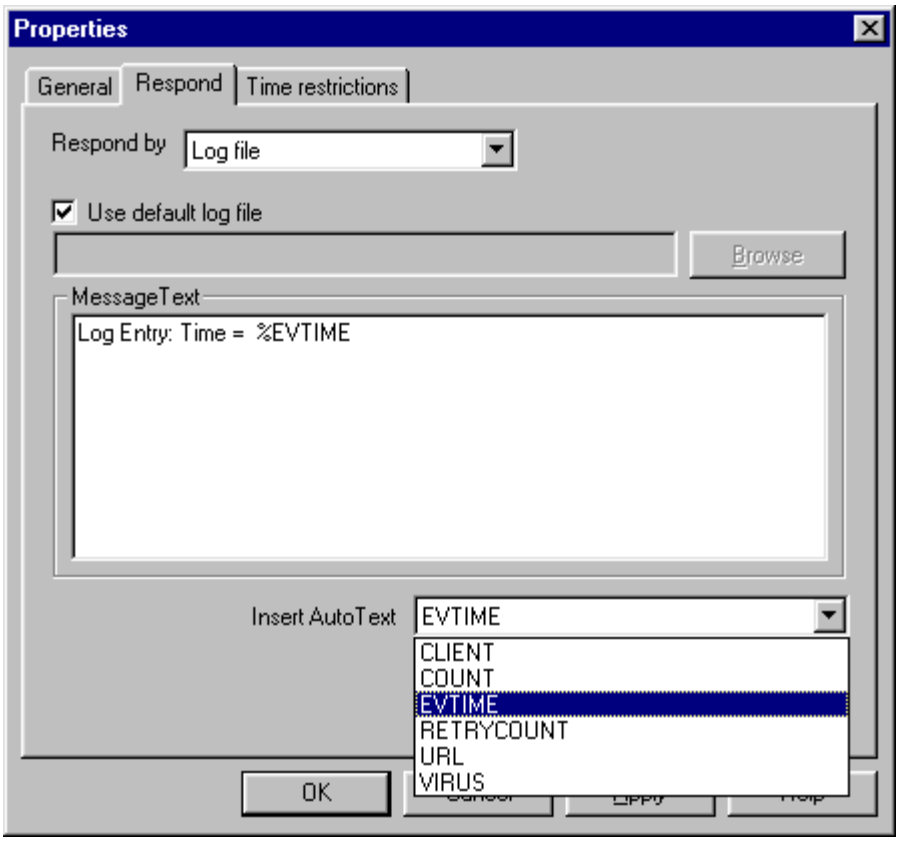


Figure J-7: Insert Auto Text allows you to include details about the event. This log file rule will record the time when an event happened.

Time Restrictions tab: Settings on this tab allow control over both when an alert is triggered and when the response to the alert is sent. **Source** time restrictions set parameters for when an alert rule is active. If an event happens outside of the Source hours, it will not trigger the alert. The **Response** time restrictions let you control when

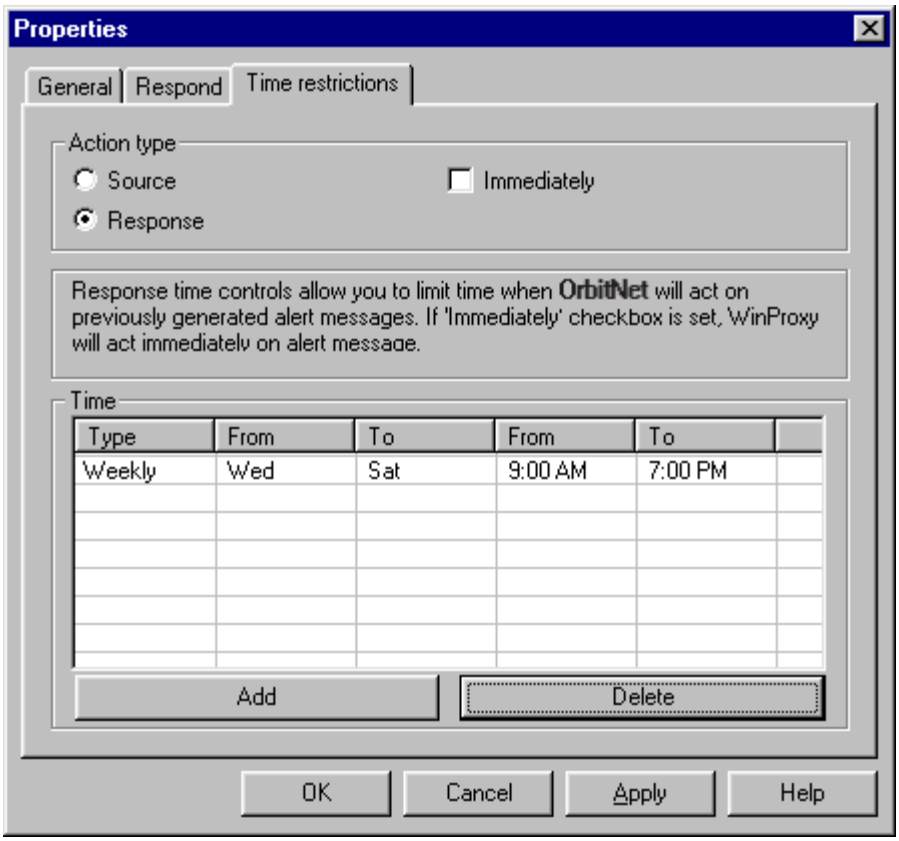


Figure J-8: Time Restrictions can affect either whether the rule is triggered at all (source) or when the alert is recorded (Response).

the response to an alert happens. Perhaps you want to know about all alerts, but you don't want to be notified after midnight. With the proper settings, the Response restrictions can make it so that you only receive alerts between 8:00 am and 5:00 pm. For both Source and Response, the **Anytime** checkbox means that they are active 24 hours a day. When this box is unchecked, the detailed time restrictions list becomes available. Click the **Add** button to add a time restriction. Clicking on the times and days will allow you to enter the parameters for your time restriction.

A NOTE OF CAUTION

The alert rules are very flexible. Carefully consider the effects of each rule before they are put into place. For example, it is possible to make a rule that is only triggered when a virus arrives via FTP between noon and 1:00 pm on a Tuesday. It may never be triggered, but OrbitNet might still be catching virii at other times. Conversely, sending an email message to the network administrator every time the Whitelist is violated could end up overflowing the mailbox.

B. VIEW LOGS

The **View Logs** dialog box found in OrbitNet's **Alerts** menu allows you to quickly locate and view log files kept on your computer. You may open any log by selecting it in the list.

APPENDIX K:

The Users Tab

The Users Tab lets you determine which users have access to the Internet through OrbitNet. Each user is designated by computername or IP address; a user's access can be restricted by choosing which protocols he or she is allowed to use, and when.

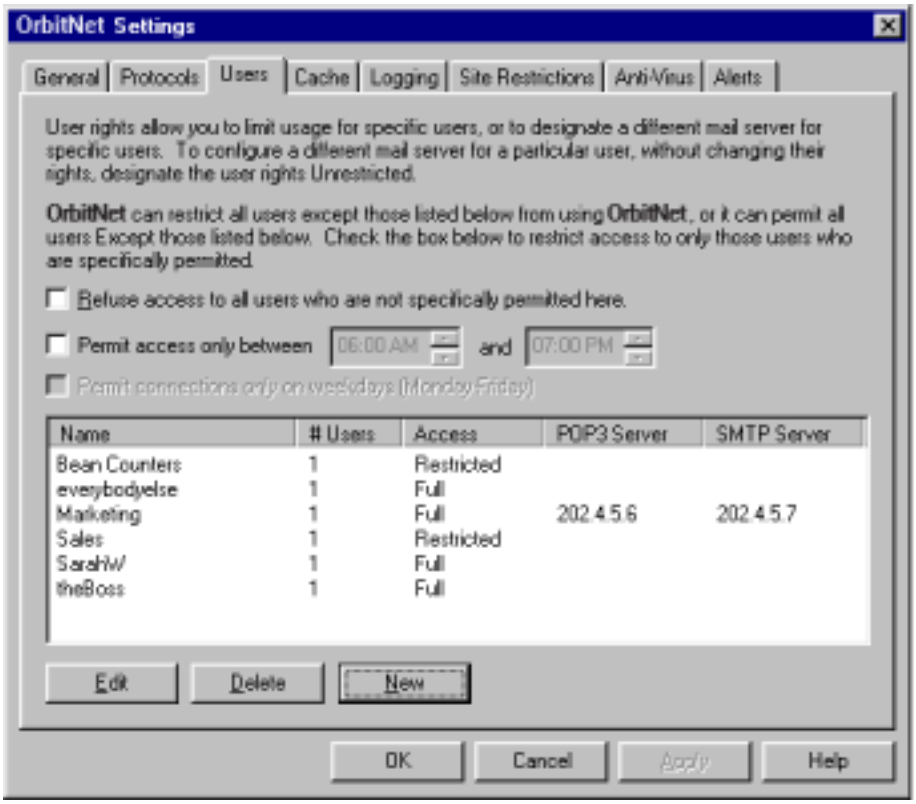


Figure K-1: The Users Tab under Settings allows you to determine who has access to the Internet through OrbitNet.

(***user_tab.bmp)

When the **Unless otherwise specified, permit access only between** box is checked, all users will be limited to the specified time window. This feature permits those with direct access (such as cable modems or ISDN routers) to restrict Internet access. The other allowed time-window option in OrbitNet applies only to dial-up connections. These time restrictions will affect all groups. Different time restrictions for individual groups can be set in the **Edit Users Dialog**.

For those users with a dial-up connection who enable both time-window restrictions, the rule is: the most restrictive one wins. Or, to put it another way, *both* functions must permit a connection or you can't get out to the Internet.

The weekday only box works the same as it does on the other time options.

There are two ways to administer users in OrbitNet:

1. Allow access to all users unless listed here with restrictions. This method is enabled only when you have *not* checked **restrict access to all users**. This option starts with the premise that everyone on your network is allowed to use the Internet, and then trims back. If you choose to restrict an individual user, add his or her name to the User List with the requisite restrictions. This will not change the ability of other users to access the Internet.

2. Restrict access to all users except those listed here. This method permits access only to those users specifically listed in the User List. You must list each individual user in a group. Users not listed will not be allowed Internet access. We recommend that you avoid putting a single IP address in different groups. OrbitNet won't sort out overlapping privileges, and the results are unpredictable.

This restriction applies to both internal and external IP addresses. If you have an incoming connection setup (such as an internal mail or web server), checking this option disables access for all outside users. We show a way around this restriction below.

NOTE

User administration can be done on either a user basis or a group basis. Each entry in this list is essentially a group, which can have up to 500 users. If you don't have many users, you can assign a different group for each user.

The entries in Figure 9-7 shows the users as currently configured, and allows you to make new additions:

- To Add a new user group click **New**
- To Modify an existing group, select the group you wish to modify and click **Edit**
- To Remove an existing group, select the group you wish to modify, and click **Delete**

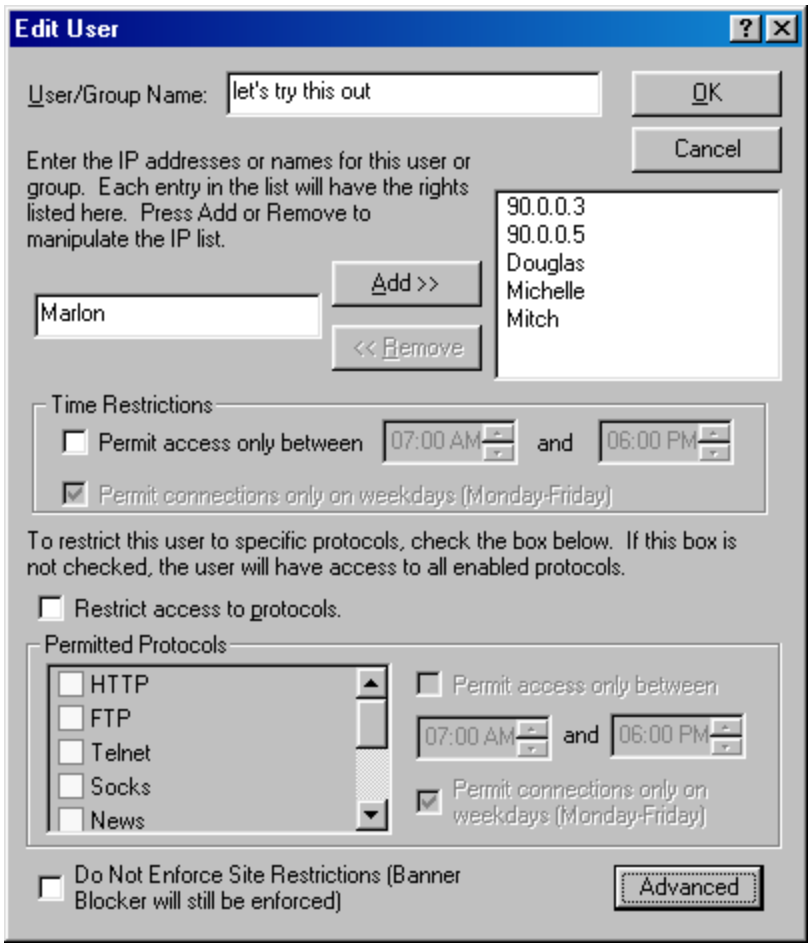
EDIT USERS DIALOG

When you click **Edit** or **New**, you'll see the **Edit Users Dialog**, which allows you to either (1) enter information required to establish a user group, or (2) modify information about an existing group. A group has a group name, as well as a list of IP addresses in that group. Each group has from 0 to 500 users who can access the Internet under the same rights.

You can use either a computername or an IP address to add computers to the group. If you use the name, it must be the name of the computer, not the name of the person. When using a name, OrbitNet will immediately try to resolve the name. If it cannot, you won't be allowed to add it to the group.

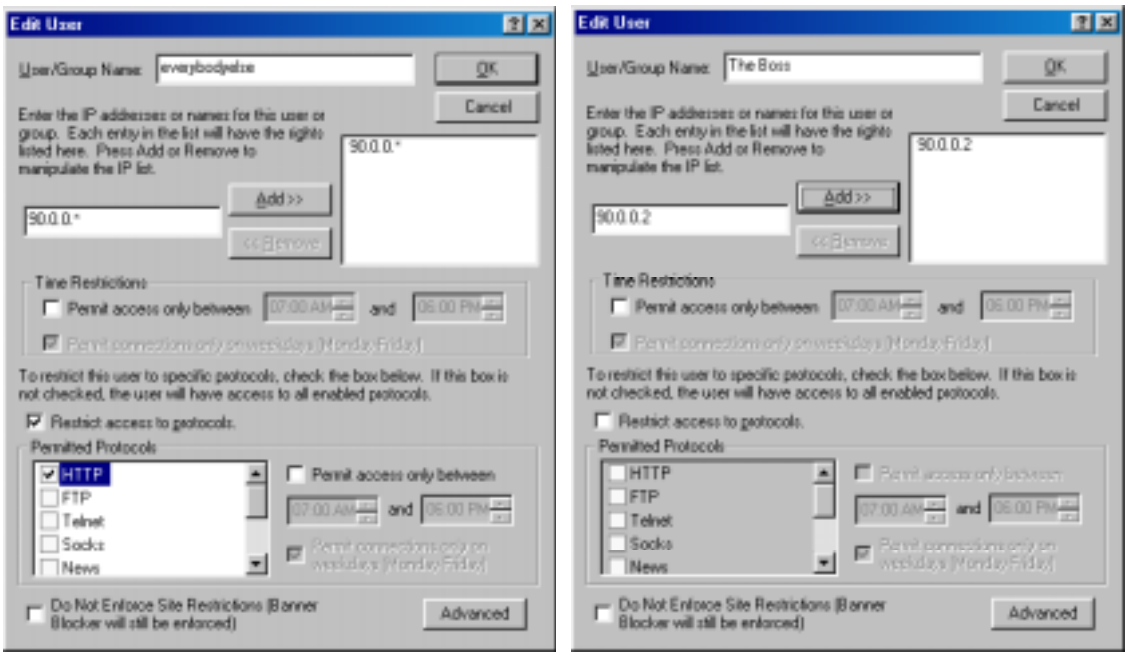
The best and easiest way to ensure resolution is to have the computername listed in OrbitNet's Namelist file (you can get access to that under Protocols – DNS). Otherwise, make sure the computername is spelled correctly and the computer is online and connected to your network when you add the name.

Names will generally work well here and they're certainly easier to read and recognize, but for the most consistent results you should use IP addresses to designate members of a group.



(*editusernames.bmp)**

There is one wild-card that is allowed when defining user groups by IP address – the symbol '*'. As an example, the IP address "90.0.0.*" would be interpreted as "any member of the 90.0.0 network". This wild-card can only be used in the right-most field – that is, "90.0.*" is a legal construction, but "90.0.*.0" is not. This wild-card can come in very handy when you are defining entire subnets with the same access.



(***everybodyelse.bmp, theboss.bmp)

These examples show a way to use the wild-card to your advantage. In this case, the boss is allowed access to everything, and everybody else on that network is allowed only to use the HTTP protocol. When you have users in overlapping groups, then the most specific IP designation wins. In this case, 90.0.0.2 is more specific that 90.0.0.*. As we mentioned before, if you have the actual IP address 90.0.0.2 mentioned in more than one group – and therefore with identical levels of specificity – the results are unpredictable. If you use it like we have shown here, it will work reliably. We'll cover a further use of this feature a little later in the chapter.

Now that you have a group defined, you can configure the kinds of access that the group is allowed. Let's start with protocols. In the example below, every machine in the "Consumer Affairs" group (except ".54," which hasn't yet been added) is allowed to use the web, get mail and news, and utilize Socks. No user is permitted to do FTP or telnet. This group does not have time restrictions separate from any that affect all groups, those set on the main Users tab.

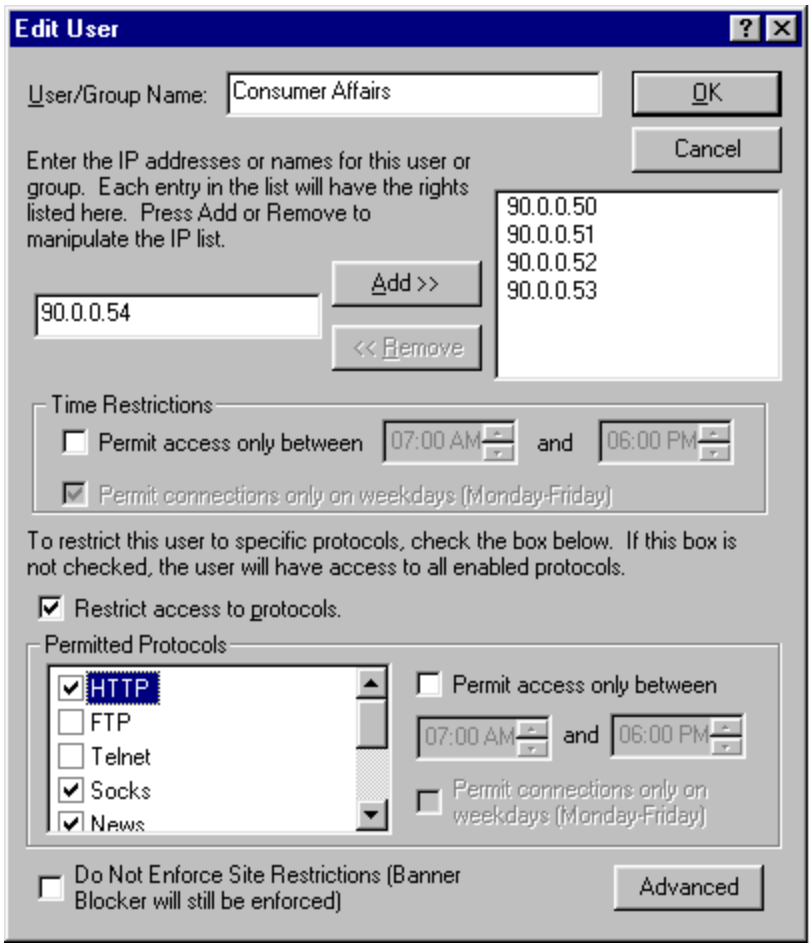


Figure K-2: As configured here, no user in this group can utilize FTP or Telnet.

Now let's take a look at using time to enforce user access. There are two places to enter time restrictions within the Edit User dialog. The **Time Restrictions** box in the center of the Edit User dialog governs the connections made by each member of the group.

Restrictions can be further defined by using the **Restrict access to protocols** section. Here, you can set separate time restrictions, protocol by protocol. Once a protocol is enabled (by checking the box next to it) , select it by clicking on its name. The time boxes are now available for your use. Since time restrictions can be set up in several places (including Dial-Up Setup) it is possible to have conflicting time rules for an individual or a set of users. In these cases, the most restrictive rule will prevail.

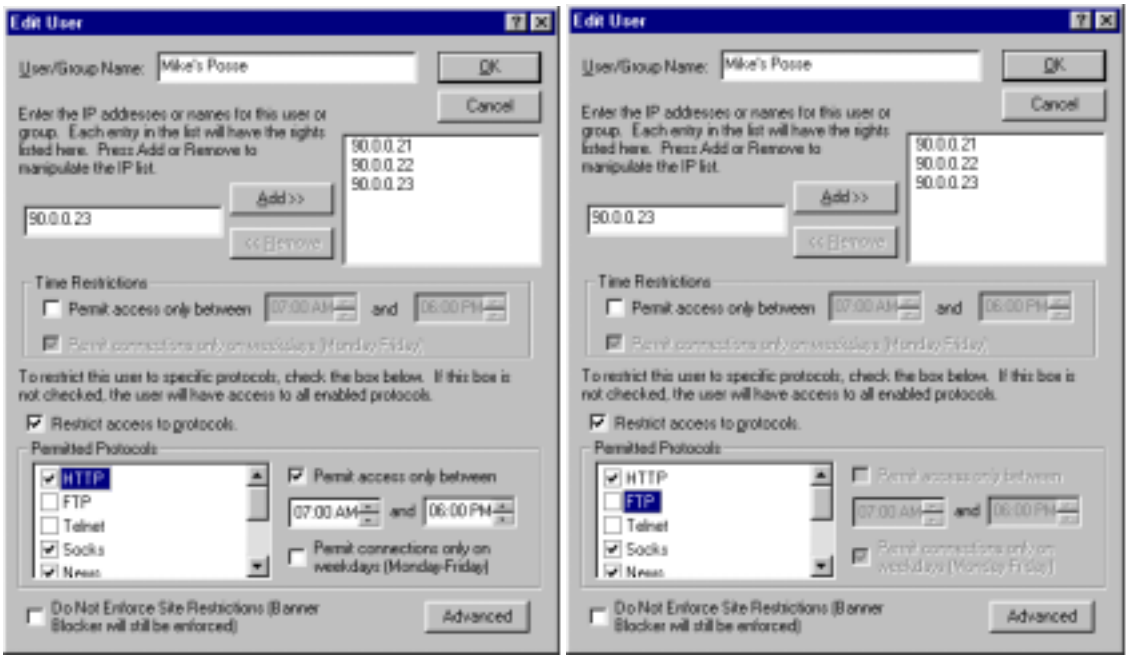


Figure K-3: Since HTTP is enabled (left), you may edit the time restrictions. FTP is disabled (right), so the time restriction controls are grayed out.

Note: Experienced network administrators may have noticed the little "gotcha!" in the example above. Since users are allowed to utilize the Socks protocol, they can still do FTP through their browsers if their browsers are configured for Socks protocol. If Socks is available, browsers may use it for many functions that otherwise might be restricted.

Other options:

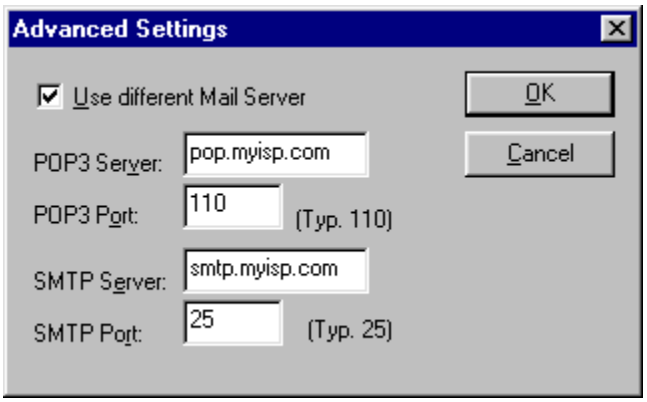
The option **Do Not Enforce Site Restrictions** can be used to allow privileged access to a group of users. When enabled, no machine in the defined group will have Blacklist, Whitelist, or SmartFilter restrictions enforced. Bosses like it.

Advanced: The advanced properties can be employed to send users to a different mail server in Classic Proxy.

Note: This feature is only useful to users whose mail applications are set up to use a Classic Proxy. Transparent Proxy is not affected by this setting.

Select this item if a particular group requires a different mail server. When **Use a different Mail Server** is enabled and configured, every machine in the group with mail applications configured to use a proxy uses a

different mail and POP server than specified within the OrbitNet Mail Setup. Mail apps which use Transparent proxy are unaffected.
Although most networks can be accommodated with a single mail server, occasions arise where a particular user or group needs access to a different mail server. This is where the address of the POP3 and SMTP server should be entered. All users in this group will be connected to the specified POP3 and SMTP servers. This feature is not supported for IMAP4.



USING WILDCARDS WITH SITE RESTRICTIONS

OrbitNet supports use of the * wildcard in configuring User-restricted IP addresses. For instance, if everybody on the **90.0.0.x** subnet is part of a group, type in **90.0.0.*** as the IP address for the entire group rather than typing in each individual address.

Larger groupings are legal, as well. For instance, the IP address **192.168.*** applies to any machine whose IP address begins with those numbers. You can carry this to the logical extreme: the IP address * is considered a legal address meaning "any possible IP address." Overlaps are possible when using wildcards; the rule is that the most specific designation wins. It doesn't matter in which order you enter the groups and restrictions in the user settings.

With careful forethought you can use the wildcard and internal and external IP addresses to enhance the security of almost any complex setup. An example would be the user or business with an internal mail server. The nature of SMTP decrees that you can't know ahead of time which server on the net will forward mail to your server—but you *do* know that your mail server must allow incoming connections at any time, day or night.

This situation becomes difficult when you want to use the option **refuse access to all users except**. At first glance it seems that you can't restrict access and still allow mail through an incoming port to an internal email server. Here's how to get around that:

4. Enable the option **refuse access to all users except those listed here**.
5. Define a group as "Incoming Mail." Use the IP address "*"(see note, immediately below) to specify the group IP address, and allow that group to use *only* the mail protocol.
6. Define another group by a name such as "Internal Users." Give this group the IP address **90.0.0.*** (see note, immediately below) and allow it to use any protocol.

Note: Since the more specific **90.0.0** wins, all internal users can do anything, but everybody else—including the incoming connections on port 25—are allowed use of the mail protocol and nothing else. You can, of course, increase the restrictions on your local users or define multiple groups.

INDEX

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W