

700 – PAT, DHCP, NetBIOS, DNS

Document ID: 10247

Questions

Introduction

What is DNS?

What is WINS?

Can I use Port Address Translation (PAT) and Windows Internet Naming Service (WINS) together?

My XWindows application does not work. What is wrong?

What is PPTP?

Can I use Point-to-Point Tunneling Protocol (PPTP) with Port Address Translation (PAT)?

Why can I not see my network through Network Neighborhood?

What is NetBIOS name spoofing?

What is DHCP?

How do I configure NetBIOS/WINS name server spoofing?

I have problems understanding Port Address Translation (PAT). Can you help?

Why does my Netware IP not work when I have Port Address Translation (PAT) enabled?

Is there any support for devices that require BOOTP?

Why does my link stay up when I am configured for NetBIOS over TCP/IP with Windows NT servers?

How do I configure NetBIOS over TCP/IP with Windows NT servers?

How many sessions are permitted with Port Address Translation (PAT) on?

Can I use Port Address Translation (PAT), dynamic IP address, and DHCP server all at once in my 766?

How can I use SNMP traps to monitor link activity?

How can I configure Port Address Translation (PAT) on remote 760 routers and get my WAN IP addresses dynamically assigned from an NT server at the home office?

Can I use Xterms and Port Address Translation (PAT)?

Is there a way to prevent NetBIOS (UDP 137, 138) from triggering a call, yet allow it to flow on the ISDN link once that link is up?

How do I filter some MAC addresses from the LAN but still use the 700 series as a router and not a bridge?

What is the default Maximum Receive Unit (MRU) for the 760 router?

How do I set up DHCP with the 700 Series Routers?

Related Information

Introduction

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Q. What is DNS?

A. DNS stands for Domain Name Services. DNS translates host names to IP addresses so that email, Telnet, FTP, and web browsers can connect to the various servers.

An example is www.cisco.com translated to 192.31.7.130. For the web browser of your PC to connect to www.cisco.com, it must translate the verbal address to an IP address. This is done through a DNS server.

Q. What is WINS?

A. WINS stands for Windows Internet Naming Service. WINS is similar to Domain Name Services (DNS), but provides a slightly different function. WINS provides a dynamic NetBIOS name to IP address registration and resolution. WINS allows your Windows machine to connect with other Windows machines via their names so you do not have to remember IP addresses.

For example, if you want to share files on ALEX_MACHINE, this machine registers its name and IP address with the WINS server. Whenever another machine needs to connect with ALEX_MACHINE, it queries the WINS server and gives the IP address of ALEX_MACHINE.

Q. Can I use Port Address Translation (PAT) and Windows Internet Naming Service (WINS) together?

A. No. PAT uses the port numbers in order to keep track of connections between the public and private networks. WINS needs to use port 137 for both directions.

Q. My XWindows application does not work. What is wrong?

A. Some PC-based XWindows applications have problems with Port Address Translation (PAT) because they send the station address when establishing a session via XDM (which does not get translated), and the server cannot find this address.

Q. What is PPTP?

A. PPTP stands for Point-to-Point Tunneling Protocol. It is used to allow Network Access Server functions to be separated. This basically means that a server in one location can use a tunneling mechanism in order to be a part of the network services in another.

Q. Can I use Point-to-Point Tunneling Protocol (PPTP) with Port Address Translation (PAT)?

A. No. PAT translates a local, or private, IP address to the public IP address and allocates a high port number to the private IP address. This way, PAT can understand return packets. With PPTP, the originating IP address (from the private network) is embedded within the PPTP packet, thus PAT cannot translate it.

Q. Why can I not see my network through Network Neighborhood?

A. Your machine might not be able to get to your Windows Internet Naming Service (WINS) Server. Check the IP address of your WINS server, and try to ping it. If your WINS server is on the other side of the router, ensure that you have NetBIOS name spoofing enabled on your Cisco 700. Also, WINS does not work across Port Address Translation (PAT). If you use PAT, you need to have a WINS proxy server on your local private network.

Q. What is NetBIOS name spoofing?

A. NetBIOS names work in a similar fashion to IP host names. A name is associated with an IP address. However, with NetBIOS the name allows for services such as file and print sharing.

NetBIOS name spoofing is a function that allows the router to respond to a common NetBIOS name request instead of pulling up the ISDN line and forwarding the request to the Windows Internet Naming Service (WINS) server. This feature is designed to reduce the traffic that is sent across the ISDN line.

Q. What is DHCP?

A. Manually addressing TCP/IP clients consumes time and is prone to errors. The Internet Engineering Task Force (IETF) developed DHCP in order to solve this problem. DHCP is designed to automatically provide clients with a valid IP address and related configuration information. Each range of addresses that a DHCP server manages is called a scope.

In addition to its IP address, a DHCP client can get other TCP/IP configuration information from a DHCP server. This includes the subnet mask, default gateway, and Domain Name Services (DNS) information. These pieces of information, called DHCP options, can be configured in the DHCP Manager on your Windows NT DHCP server.

Q. How do I configure NetBIOS/WINS name server spoofing?

A. First, configure the Windows Internet Naming Service (WINS) server address on the client workstation (WS), or set up DHCP in order to provide the WINS server address to the client WS. Next, open the WAN profile and configure **<set netbios name spoofing <minutes>|off>**.

The NetBIOS Name Server feature is configured on the WAN interface only. Each outgoing and incoming UDP port 137 packet is interrogated on that interface in order to intercept the Name Service Query or Response. An outgoing Name Service Query from the client is intercepted, the 766 checks its cache, and either of these occur:

- ◆ Responds with the WINS entry if it exists in the cache.
- ◆ Forwards the request to the original IP destination if no entry exists in the cache.

The incoming Name Service Responses from the WINS servers are intercepted and interrogated, compares the packet data against the current cache of the 766, then either of these occur:

- ◆ Updates the cache, if necessary
- ◆ Forwards the response to the client.

If the incoming or outgoing packets are not destined for UDP port 137, the 766 does not interrogate the packet and forwards it normally.

The current cache Entry Age Out is four hours. This is not configurable. The Spoofing Timer (in minutes) indicates how long the spoofing is active. Normal users want the spoofing feature to be a toggle – either ON or OFF – such as DHCP Server or Port Address Translation (PAT). However, the minutes value is required and the maximum (32,000 minutes = 22+ days) should be sufficient (unless the customer keeps the ISDN line up constantly). If you set the spoofing minutes to 60 minutes and the call goes down after 30 minutes, it is okay. The spoofing timer resets when the next call begins. If the spoofing timer

is set to 60 minutes and call lasts 90 minutes, the NetBIOS Name Service feature is disabled for the last 30 minutes of the call.

Q. I have problems understanding Port Address Translation (PAT). Can you help?

A. PAT takes away the end-to-end significance of an IP address. Therefore, limitations exist when PAT is enabled.

PING from an outside host to a host in the private network ends at the Cisco 700 router, and is not forwarded to the inside host. Telnet from an outside host to a host in the private network also ends at the Cisco 700 router if there is no telnet port handler defined.

Only one inside or private WWW server is supported. WWW linkages with other inside hosts or servers are not translated. Only one FTP Server, Telnet Server and so forth is supported in the inside network.

Packets, such as DHCP, SNMP, PING and TFTP, destined for the Cisco 700 router are not subject to PAT.

A maximum of 12 personal computers can simultaneously boot in the inside network. If more than 12 personal computers try to boot up simultaneously, one or more can receive an error message about not being able to access the server.

400 PAT entries are allocated to share among the inside machines. If TCP connections are setup and TCP timeouts are set to keepalive, no more than 400 machines can get to the outside world.

The Cisco 700 PAT feature does not handle fragmented FTP packets.

Multidestination with unnumbered links does not work for PAT and is not recommended.

When a packet is received from the outside, PAT compares the port number with an internally configured port handler list (15 entries maximum). If there is a port handler defined for this port, it routes the packet to the appropriate port handler. Otherwise, if there is a default port handler defined it routes the packet there. If it fails to find entries for either of these cases, the Cisco 700 handles the packet itself.

Some well known ports cannot have port handlers defined. This includes the DHCP client port, used by the Cisco 700 to receive DHCP server responses, and the Windows Internet Naming Service (WINS) NetBIOS ports, used by Inside Win95 PCs to receive WINS information.

Q. Why does my Netware IP not work when I have Port Address Translation (PAT) enabled?

A. It appears as though the Netware server ignores the source port when it replies to a packet. In this case, PAT does not work because it relies on the port numbers to keep track of the connections between the public and private networks.

Q. Is there any support for devices that require BOOTP?

A. As of 4.0(2), DHCP replay agent in Cisco IOS®-700 supports this feature. Simply configure the **set dhcp relay <IP address of server>** command on the LAN.

Q. Why does my link stay up when I am configured for NetBIOS over TCP/IP with Windows NT servers?

A. NetBIOS name resolution traffic (and to a much lesser degree, NT security traffic) keeps your line up.

This is a common problem. Cisco and Microsoft are both working on various solutions. If you have an NT server on each side of the communication, you should configure each as the local Windows Internet Naming Service (WINS) server for the respective LAN. This should reduce WAN communications significantly.

The problem is most likely the 4.1 servers. These servers send out sync packets to every server in the NDS tree. If you have 4.1 servers on both sides and they are in the same tree, you can request a module from Novell called timesync. This lets you set the duration between syncs. Also, watch for mail servers that send data to each other. You might have to figure out which side is calling and get the **log traffic ver** from inside the profile. Also, make sure to block NetBIOS traffic, use IPX spoofing, and **rip update snapshot** routing.

Q. How do I configure NetBIOS over TCP/IP with Windows NT servers?

A. For NetBIOS over TCP/IP, set up these:

- ◆ In the TCP/IP config on NT 4.0, set it as the Windows Internet Naming Service (WINS) server.
- ◆ In the TCP/IP config on NT 3.51, set the NT 4.0 as the WINS server.

You should be able to use all NT 4.0 services from the NT 3.51.

Q. How many sessions are permitted with Port Address Translation (PAT) on?

A. You can have up to 400 entries in the translation table. This means that, at any instance, the router can handle up to 400 TCP/UDP sessions. Therefore, you can have 400 users with one session each, or 100 users with four sessions each, or four users with 100 sessions each. As you can see, it does not provide you much information when you ask for the number of users (on the LAN segment). It all depends on the usage.

Q. Can I use Port Address Translation (PAT), dynamic IP address, and DHCP server all at once in my 766?

A. Yes. The Cisco 766 supports these features independently and separately. However, PAT is not turned on automatically when the 766 receives an assigned IP address from the remote router, because it is not a good idea to assume that dynamic IP is always used with PAT.

As independence or separation means, these features must be turned on and set up independently. The most common and recommended combination is to use DHCP on the LAN side, and PAT on the WAN side. Dynamic IP address negotiation is always there, which means there is no ON | OFF switch. Also, with the **set ppp address negotiation local on | off**

enhancement in 4.0(2), the user has more flexibility as to where or which interface the negotiated IP address can be assigned.

Q. How can I use SNMP traps to monitor link activity?

A. You can issue the **set snmp trap** command in order to configure when traps are sent to the network management system. Traps can be sent for these:

- ◆ **coldstart** The coldstart trap is sent when the router is powered on.
- ◆ **linkup** A new connection is established. This does not apply to individual B channel establishment.
- ◆ **linkdown** A connection is closed. This does not apply to individual B channels that close.
- ◆ **authenticationfail** When authentication fails.

Where the trap is sent depends on where the trap host you specify resides. If the trap host resides on the LAN side, the trap is sent to the LAN. If the trap host resides on the WAN side, the trap is sent to the WAN profile through which the trap host can be reached.

For coldstart, the trap is generated when the 760 is powered up. During the power up, the 760 is set up for the LAN profile. If the linkup trap is enabled and a trap host exists, a linkup trap for the LAN profile is sent to this trap host. During power up, the 760 also reads all the user (WAN) profiles that existed before it was powered down. It retrieves this data from its NVRAM. As it reads the user profile, it creates the user profile that corresponds. If the profile has the attribute of power up active, the 760 sets the profile to active and the linkup trap for this profile is sent to the trap host. Therefore, during the power up, linkup traps are sent to the trap host.

The other situation to send the linkup trap is as the 760 runs. After you create a new user profile or for a user profile that exists, issue the **set active** command. This command sets up the user profile so that it is available for the 760 to make the call and establish connection if the traffic demands it. Therefore, this trap is sent only when a profile is issued a **set active** command, either by the 760 or by the user. This trap has nothing to do with the B channel being activated or a call being made to initiate a connection.

If the trap host resides on the WAN side that can be reached by a user profile, the trap is sent to this profile. If demand is turned on (auto on), the packet can trigger a call to be made based on the call number in this profile. When a connection is established, the queued trap packet is forwarded. For example, you have two 760s connected via ISDN as shown here:

| 760a |-----ISDN-----| 760b |-----LAN-----|-----| trap host |

In this diagram, if you turn on **log connection traf ver** in the 760b, where connection is that of the WAN user profile, you should see a SNMP linkup trap packet received and displayed by the 760b. This is sent by the 760a when you issue the **set active** command for this profile.

If the trap host resides on the same connection as the profile that has been set inactive, it does not see this trap. If the trap host resides on the LAN connection or in another WAN profile, the linkdown trap is sent to these profiles and the trap host sees it.

For the LAN profile, because it is permanent and always active, it does not accept the **set active** or **set inactive** commands. Therefore, you do not see the linkdown trap at all. If you unplug the LAN cable, any linkdown trap is not sent.

However, if you have the Novell LAN Analyzer software which runs on Windows 3.x, or connect a sniffer to the 760, you can capture all packets from the 760 and it tells you if the SNMP linkup/linkdown or other traps have been sent by the 760.

Q. How can I configure Port Address Translation (PAT) on remote 760 routers and get my WAN IP addresses dynamically assigned from an NT server at the home office?

A. On the 760, PAT is set up and a bogus LAN network is used:

```
SET DHCP SERVER
SET DHCP ADDRESS 10.0.0.2 128
SET DHCP NETMASK 255.0.0.0
SET DHCP DNS PRIMARY 171.68.122.99
SET DHCP DNS SECONDARY 171.68.10.70
SET DHCP DOMAIN cisco.com
SET DHCP GATEWAY PRIMARY 10.0.0.1
SET DHCP WINS PRIMARY 171.68.235.228
SET DHCP WINS SECONDARY 171.68.235.229

SET USER LAN
SET BRIDGING ON
SET ENCAPSULATION CPP
SET IP ROUTING ON
SET IP ADDRESS 0.0.0.0
SET IP NETMASK 0.0.0.0
SET IP FRAMING ETHERNET_II

SET USER Internal
SET BRIDGING ON
SET ENCAPSULATION PPP
SET SUBNET 255.0.0.0
SET IP ROUTING ON
SET IP ADDRESS 10.0.0.1
SET IP NETMASK 255.0.0.0
SET IP FRAMING ETHERNET_II
SET IP PROPAGATE ON
SET IP COST 1
SET IP RIP RECEIVE V1
SET IP RIP UPDATE OFF
SET IP RIP VERSION 1

SET USER home
SET PROFILE POWERUP ACTIVATE
SET PROFILE DISCONNECT KEEP
SET BRIDGING OFF
SET ENCAPSULATION PPP
SET 1 NUMBER 2205006
SET 2 NUMBER 2205007
SET CLICALLBACK OFF
SET IP ADDRESS 0.0.0.0
SET IP NETMASK 0.0.0.0
SET IP FRAMING NONE
SET IP PAT ON

===== Home 4500 config =====

hostname home
!
username 766 passowrd removed
ip address-pool dhcp-proxy-client
ip dhcp-server 171.68.36.4
isdn switch-type basic-nil
```

```

!
interface Ethernet0
  description Denver LAN
  ip address 171.68.36.1 255.255.255.128
  media-type 10BaseT
!
interface BRI4
  no ip address
  no ip mroute-cache
  encapsulation ppp
  no ip route-cache
  isdn spid1 30322050111111
  isdn spid2 30322050121111
  peer default ip address dhcp
  dialer idle-timeout 300
  dialer rotary-group 1
  no fair-queue
  compress stac
!
interface Dialer1
  ip unnumbered Ethernet0
  no ip mroute-cache
  encapsulation ppp
  peer default ip address dhcp
  dialer-group 1
  no fair-queue
  compress stac
  ppp multilink
  ppp authentication chap
!
ip domain-name cisco.com
access-list 102 deny eigrp any any
access-list 102 permit ip any any
dialer-list 1 protocol ip list 102
dialer-list 1 protocol appletalk permit
end

```

Q. Can I use Xterms and Port Address Translation (PAT)?

A. Yes. You need to specify PAT at the system level, as shown here:

```

(192.168.144.1 is the private network)

SET IP PAT UDPTIMEOUT 5
SET IP PAT TCPTIMEOUT 30
SET IP PAT PORTHANDLER 6000 192.168.144.1 *** Required for X-Server
SET IP PAT PORTHANDLER HTTP 192.168.144.1 *** for web browsing
SET IP PAT PORTHANDLER FTP 192.168.144.1 *** for ftp
SET IP PAT PORTHANDLER 69 192.168.144.1

```

Also, PAT needs to be specified on the WAN profile:

```
SET IP PAT ON
```

On the 766, you need to enter a PAT porthandler for port 6000 in order to map to the inside address of the PC where the X server will run.

Note that with PAT porthandler, you can only map from a server port (in this case 6000) to a single inside IP address. Therefore, on a private LAN served by a 766, you can only have one X server that runs on port 6000. If multiple PCs that run on an X server are on the same inside LAN, then all but one of the PCs need to configure their X servers to use an alternate port (normally 6001, 6002, and so on). Also, you need to enter an additional porthandler for each

PC. This involves the X server software on the additional PCs being configured to use a server number other than 0.

For example, the second PC on an inside LAN sets its X server number to 1. Then, set up a PAT porthandler for TCP port 6001 that maps to the IP address of that PC. On the UNIX X client side, you have something similar to this:

```
% setenv DISPLAY pat.ip.global.addr:1.0
```

This makes the X client make a TCP connection to port 6001 on pat.ip.global.addr, which makes the PAT porthandler map that to 6001 on the inside IP address.

You cannot use DHCP relay with PAT. If you run PAT, you need to configure the PCs manually with static IP addresses, or else use the built-in DHCP server of the 766.

Q. Is there a way to prevent NetBIOS (UDP 137, 138) from triggering a call, yet allow it to flow on the ISDN link once that link is up?

A. No. However, you can do this manually by using **SET 1 AUTO OFF** and **SET 2 AUTO OFF** in the user profile. This forces you to manually make a call whenever you want to use the ISDN link.

Q. How do I filter some MAC addresses from the LAN but still use the 700 series as a router and not a bridge?

A. If you want to limit the number of devices that the router can see from the LAN, you can perform these:

- ◆ **SET LEARN OFF** This disables the router from automatically learning MAC addresses.
- ◆ **CD LAN** Change to LAN profile.
- ◆ **SET ADDRESS xxxxxxxxxxxx** This allows you to specify the MAC addresses statically.

Q. What is the default Maximum Receive Unit (MRU) for the 760 router?

A. The default MRU is 1524 bytes for the 700 Series Router.

Note: This is the payload, which excludes the PPP/Multilink PPP (MLP) encapsulation.

Q. How do I set up DHCP with the 700 Series Routers?

A. Refer to the samples in Section 1 – Basic Configuration, ISDN, and PPP Troubleshooting. Basically, this involves the set up of **SET DHcp RELay <IP_Address>** on the LAN interface where the DHCP requests originate (PCs with no addresses). The DHCP Request packet (from the PC) is converted to unicast (when it leaves the local 760) and address/send directly to the DHCP server. As long as the far-end 760 knows how to route the DHCP Ack/Nak packet back (via static route or RIP), it should be fine.

Related Information

- **700 Series – Interoperability**
 - **700 Series – ISDN Issues**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

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

Updated: Oct 09, 2006

Document ID: 10247
