Gateway Window

The Gateway Window allows you to configure the operation of the IPNetRouter gateway.

IP Forwarding: It is possible to receive datagrams on an IP interface whose IP address is not an address for this computer. In this case, you can decide whether to discard such datagrams (normal behavior), or try to forward them on to their destination. Select "IP Forwarding: Never" to discard datagrams that are not addressed to this machine (RFC 1122 compliant). Use "IP Forwarding: Always" to always forward datagrams. Use "IP Forwarding: Automatic" to only forward datagrams when more than one IP interface is active (SunOS compatible).

In general, only designated routers should forward datagrams, but there are situations where you might want one machine to forward datagrams to another that would not otherwise have access to that network.

Dial On Demand: When selected, IPNetRouter will request PPP to connect when it detects IP traffic sent to a PPP interface that is not connected. The Log Window shows the source IP address of the datagram that triggered the dial request. When unselected, IPNetRouter will open PPP before requesting a connection so PPP can decide when to dial for the first time. Press and hold the Option key while adding a PPP interface to temporarily override this behavior.

Show PPP Dialogs: Enables the PPP modal dialogs to appear when connecting or disconnecting using OT/PPP.

Remain Connected: Causes IPNetRouter to ping a PPP interface every three minutes and try to reconnect immediately if the PPP connection is lost for any reason.

Disconnect PPP At Quit: IPNetRouter will request PPP to disconnect when the application quits.

Enable Local NAT: When enabled, datagrams from the non-IP Masqueraded interface(s) addressed to the public IP (Masqueraded) address of the gateway are port mapped to machines behind the gateway prior to routing. If experiencing problems accessing or using the gateway machine for an IP service, try disabling this option until the problem is resolved.

TR Cable Modem: For Telco Return style cable modems ONLY. These are special modems that use an Ethernet downlink and PPP uplink over a telelphone line. Selecting this feature tells the NAT module to unmasquerade packets received on the first Ethernet interface that were masqueraded by the PPP interface.

DNS Forwarding: allows clients behind an IPNR gateway to use the router address as their DNS Server address. This simplifies setting up the clients, and also allows IPNR

to redirect DNS requests at appropriate times. With DNS Forwarding, IPNR can: (1) Change the actual DNS server on the fly if PPP gets a new DNS server address when it connects; (2) Defer DNS requests if the modem is not currently connected to prevent clients from timing out while PPP is connecting; (3) Not try to connect if it gets an address to name request (PTR query) while PPP is not connected.

Better PPPoE Routing: This feature modifies TCP connection request packets to limit the MSS to MTU-40 to insure TCP segments will pass through a PPPoE connection that does not correctly handle oversize datagrams.

Exposed Host: this setting allows you to specify which host if any on your LAN will receive requests sent to the public IP address used for IP masquerading (NAT). Certain protocols such as CU-SeeMe and NetMeeting do not easily work through NAT. Previoulsy these protocols could only be used from the gateway machine. This setting allows you to select which host on your LAN will be visible to the public Internet and thus able to use these protocols transparently. If the Exposed Host is set to None, even the gateway machine will be protected behind the NAT firewall and will not be accessable from outside your LAN unless you specify a corresponding inbound port mapping.

Dialup DNS Client: if your gateway is normally assigned a dynamic IP address from your ISP (via PPP or DHCP), this setting allows you to access your gateway using a fixed domain name such as "myComputer.dialupdns.com". To use this feature, you must first sign up for FREE dialup DNS service at <http://www.dialupdns.com> specifying the name you wish to use (which will replace "myComputer" in the example above) and a Username and Password. You then enter the corresponding Username and Password in the Gateway Window and enable Dialup DNS Client. Each time IPNetRouter connects to your ISP possibly getting a different IP address, it will open a TCP connection to "client.dialupdns.com" and login updating your dialup domain name so it points to the IP address assigned to your gateway computer. When entering your Username and Password in the Gateway Window, remember to press Tab or Enter so that IPNetRouter records the text you typed. The IPNR Log Window will indicate when your Dialup DNS Client has logged in successfully.

Exclude From NAT: Allows you to specify a network that should not be translated via NAT. The "Net" field is used to specify the network in the form IP_address/prefix_length. Datagrams whos source or destination IP address match this network will skip the NAT function allowing you to create a publicly addressable network behind your NAT gateway.

You can save an IP configuration (interfaces and routes) to a settings document and then restore this configuration later by opening the corresponding document. Since the "Interfaces" and "Routes" window show the actual interfaces and routes the IP module knows about, you can only open one document at a time to restore a previous configuration (since there is only one IP module). Use the "Upon Open" popup menu in the Gateway window to control what happens when a configuration document is opened

(configure only, configure and display). This is especially useful for placing a settings document in your Startup Items folder to configure multiple IP interfaces each time your Macintosh starts up.

Detailed instructions for using IPNetRouter are available from the Sustainable Softworks web site at <http://www.sustworks.com>.