

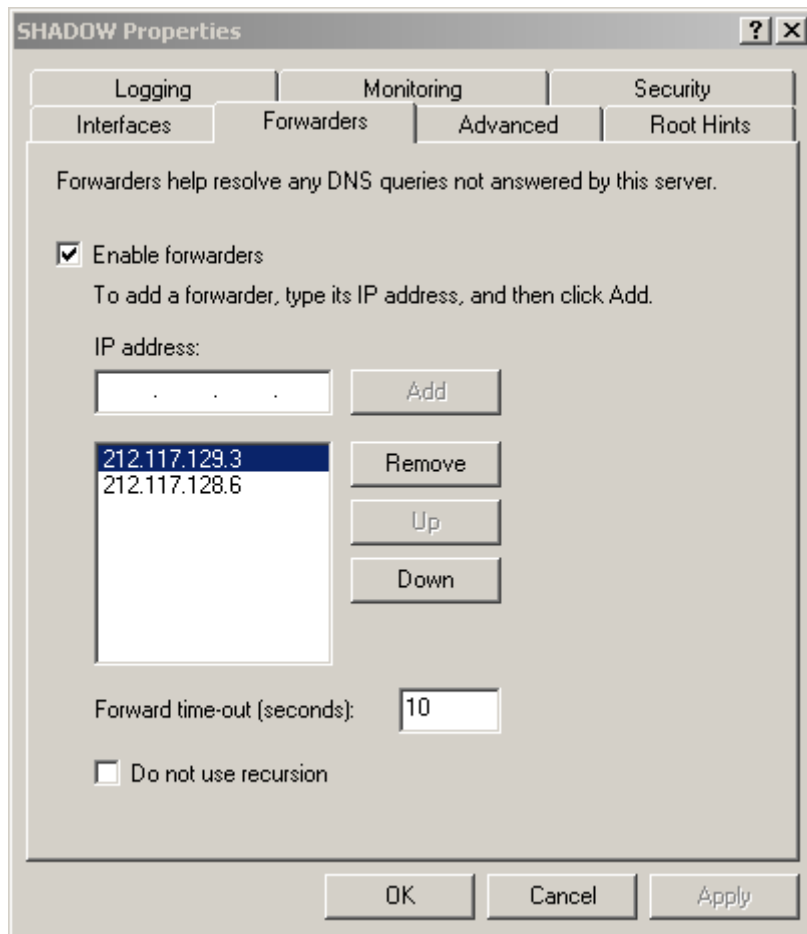
NAT on Windows 2000 Server Via RRAS service

Beta Version 4

Author: Yuval Sinay (MCSE)

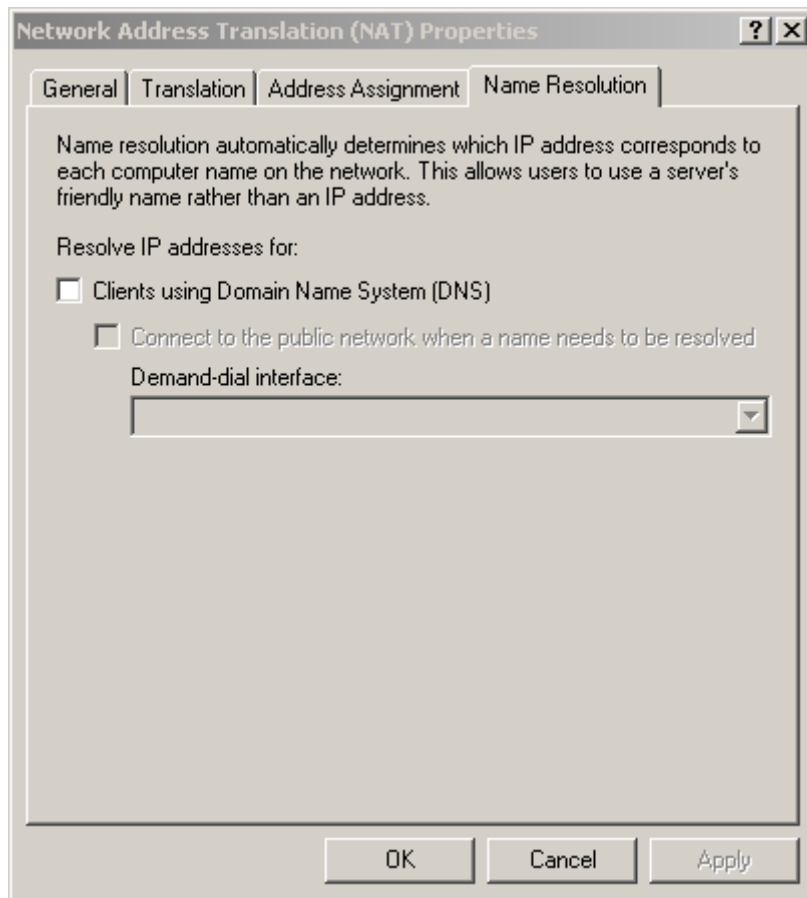
Here a short manual for NAT configuration on Windows 2000 Server. I assume that you have a moderate experience on Windows 2000.

Local DNS server that will contain also the RRAS service on it:



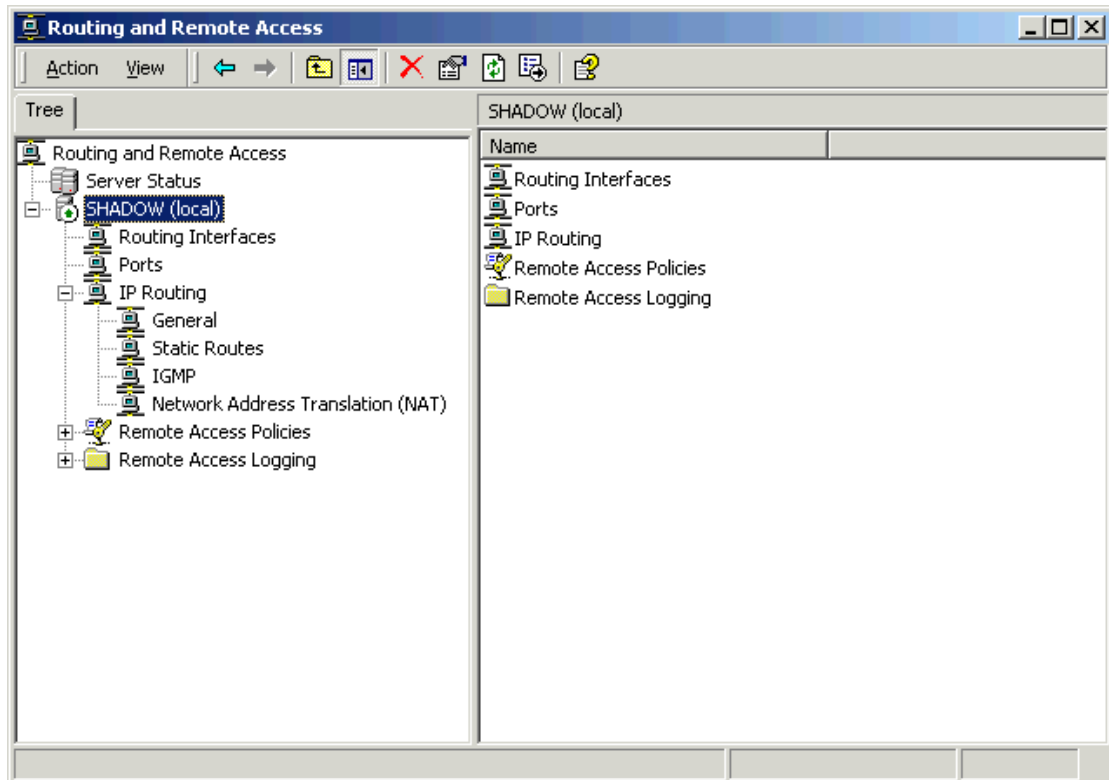
The IP that I use are my ISP DNS servers, you should configure yours ISP DNS IP.

If you don't have local DNS server in yours network you should configure this on NAT protocol on the RRAS:

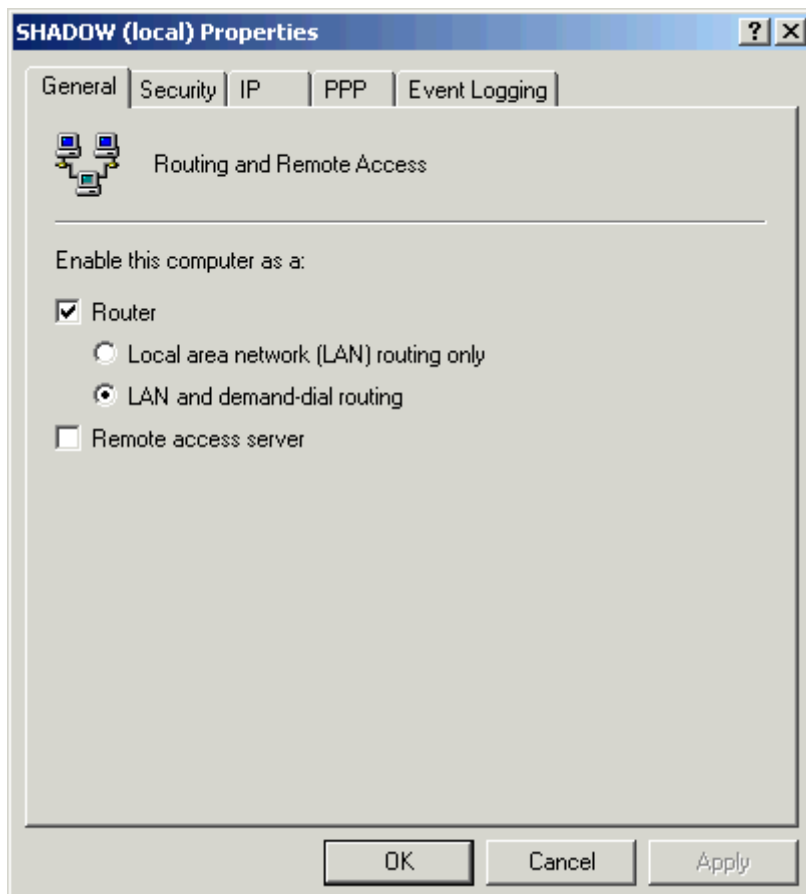


We have to use RRAS wizard to configure the server and after this change some Of the base configuration:

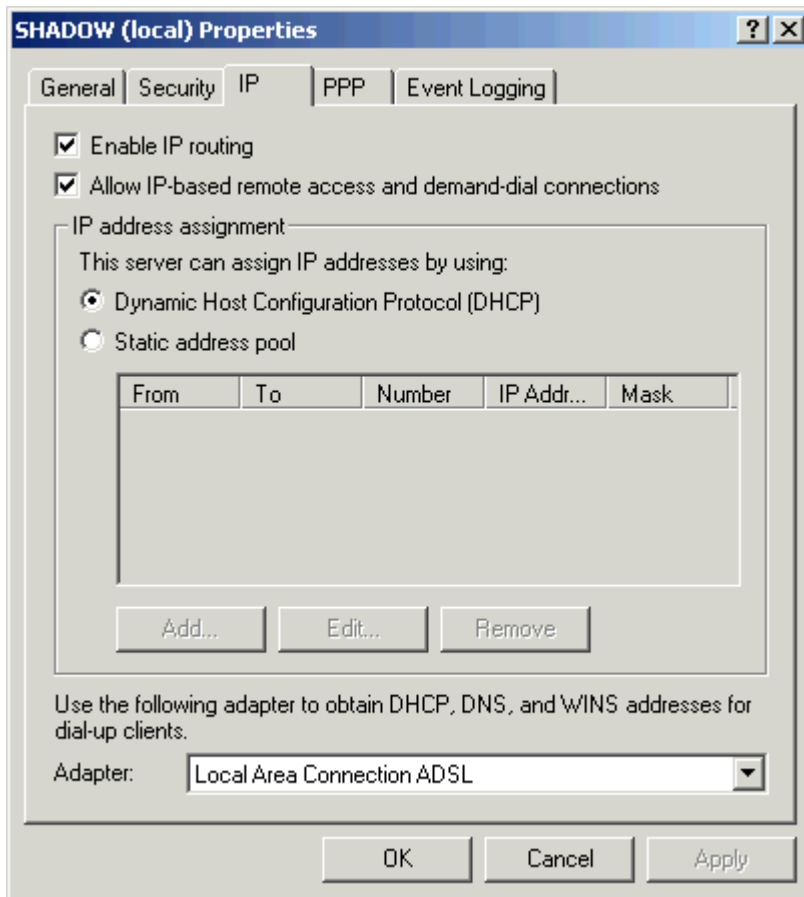
Main RRAS server screen:



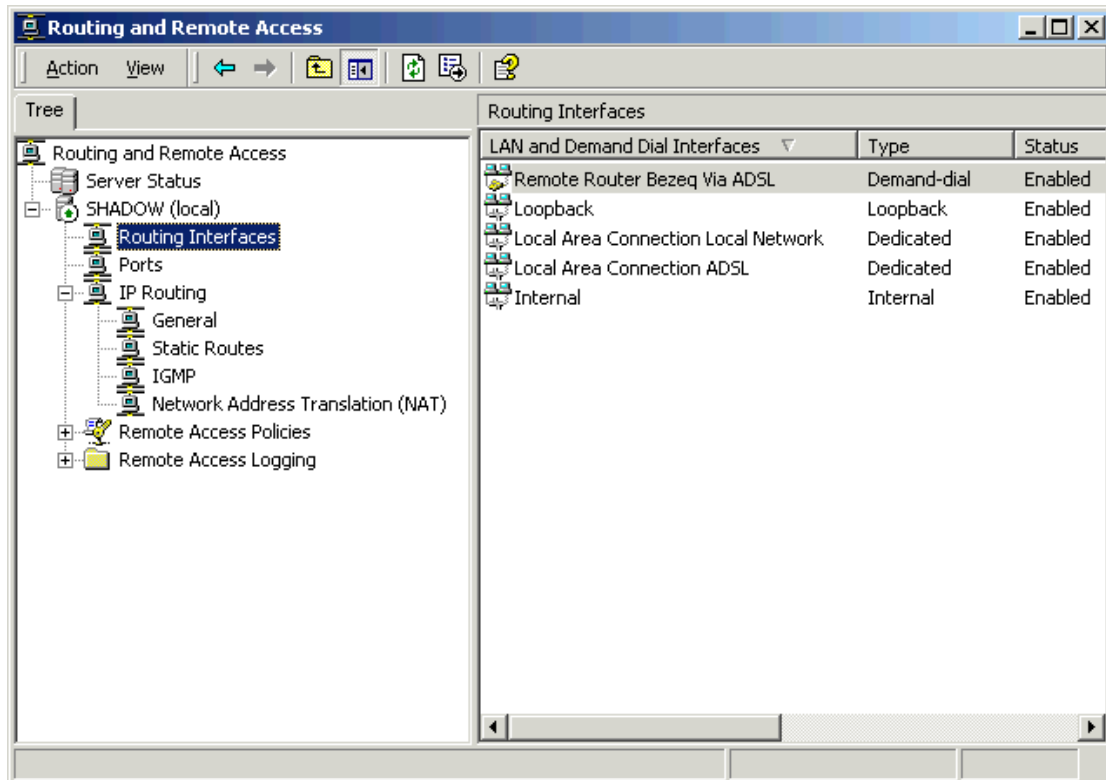
RRAS server Properties:



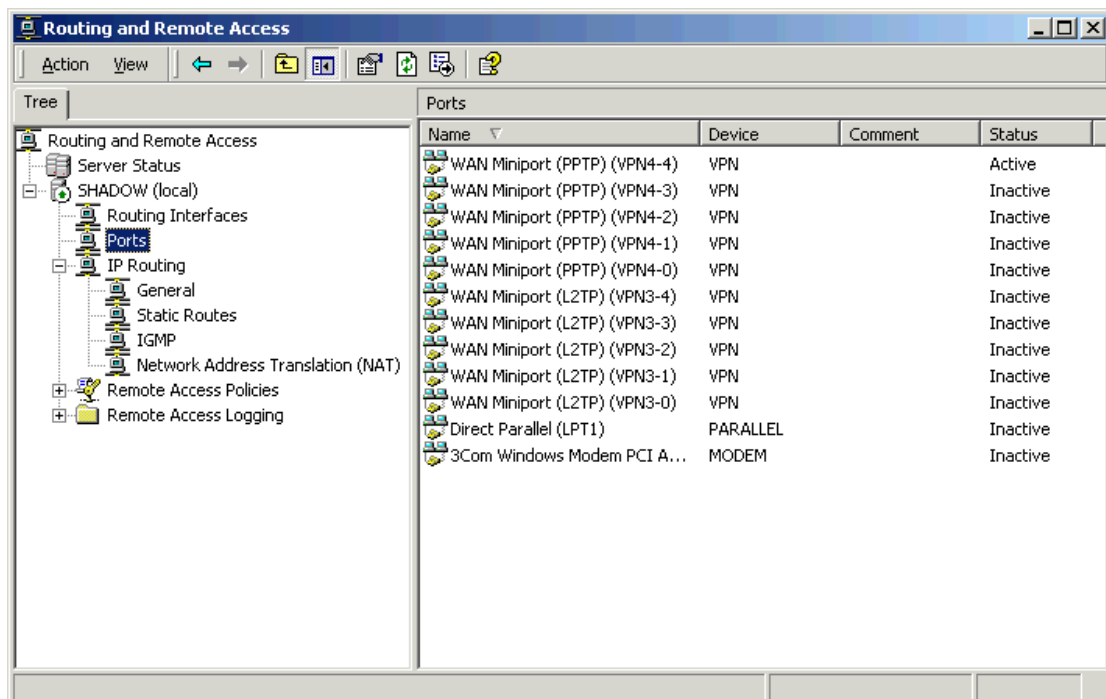
Don't use this server also for RAS ! It's a big security risk.



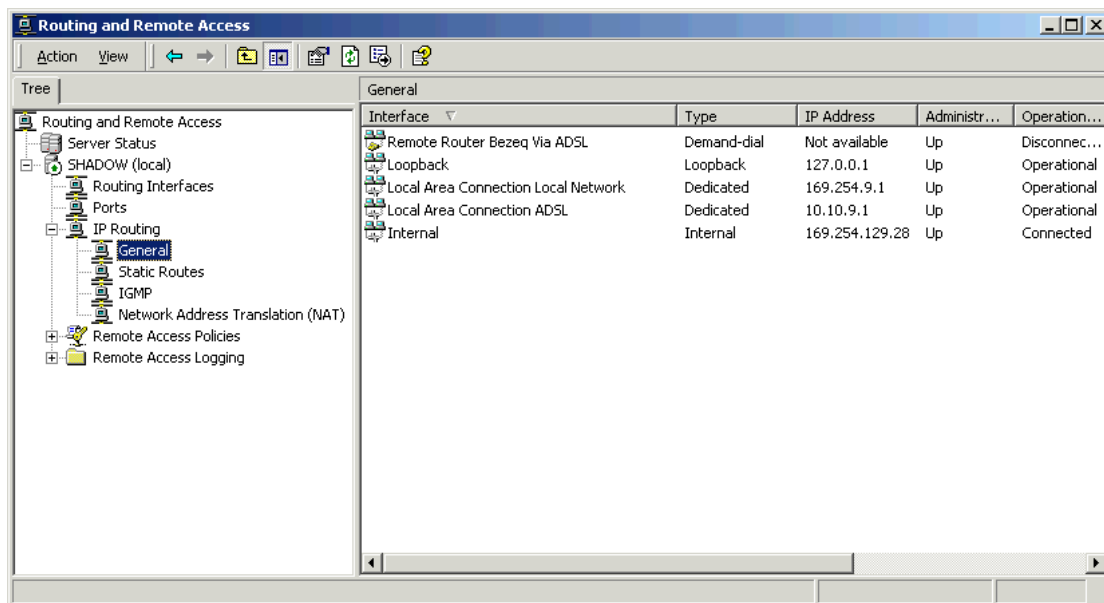
After you use the RRAS wizard, you should have at least 5 Interfaces:
 (Of course you need to configure a demand dial and add to it yours information:
 user name + password + Authentication method and so on)



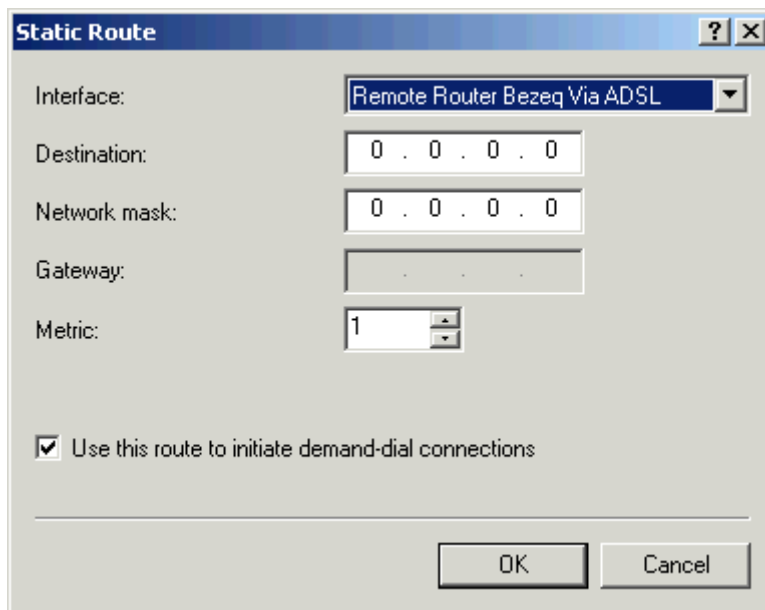
By default you will have these ports on the RRAS:



In IP Routing you need to see the 5 interfaces again:

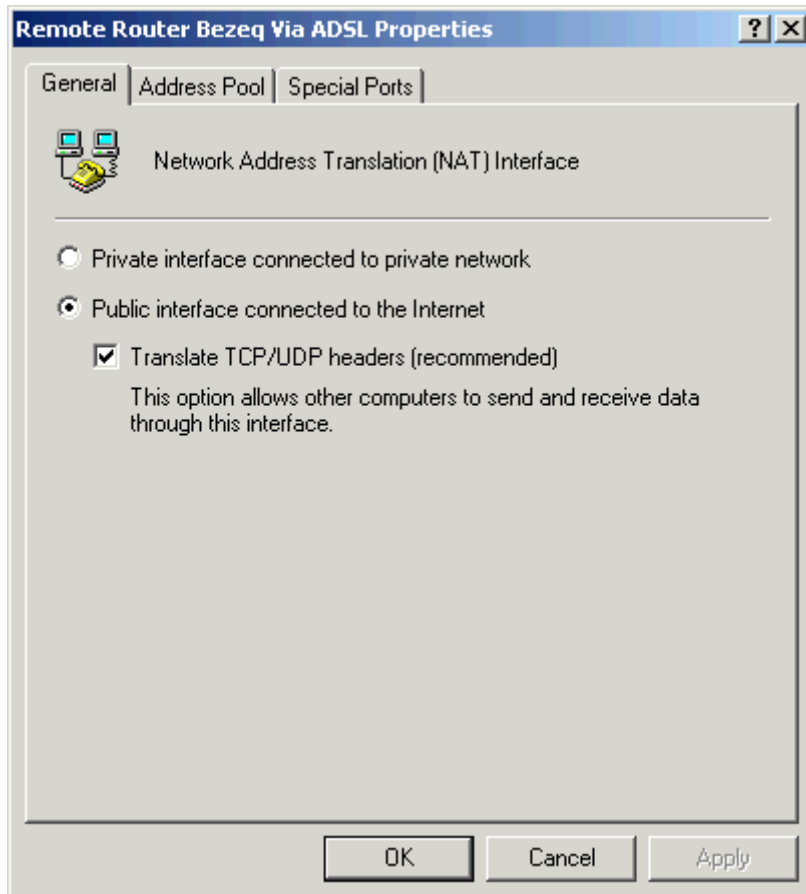


The demand dial have to have a static route like this:

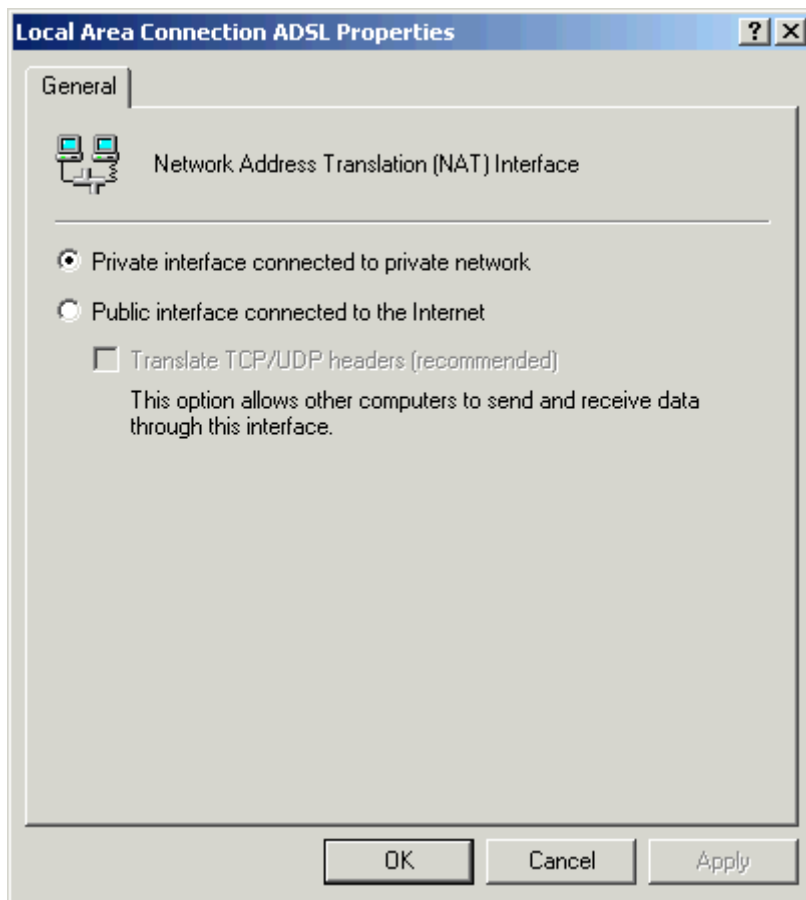


In NAT Protocols section you will have two interfaces:

- a. Outbound connection Via the Demand dial up:
(You can see the properties of the connection on NAT protocols, and press twice on the interface that you want to see)



b. Inbound connection Via Local NIC interface:



I use the NIC interface that connect to the ADSL modem for Inbound (you can choose to use the other NIC – but it's depend on yours security configuration)

My RRAS Server Configuration:

Main Nic That Connect To ADSL Modem:

IP: 10.10.9.1/8

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.138 (ADSL Modem)

DNS Primary: 127.0.0.1

WINS IP: 169.254.9.1/16 (or other local WINS IP - if you have)

Main Nic That Connect To Local Private Network:

IP: 169.254.9.1/16 (Its depend if you use DHCP of RRAS or DHCP from NAT
Or a Static IP for the clients)
Subnet Mask: 255.255.0.0
Default Gateway: Null
DNS Primary: 127.0.0.1
WINS IP: 169.254.9.1/16 (or other local WINS IP - if you have)

Client configuration:

IP: 169.254.9.2/16 (Its depend if you use DHCP of RRAS or DHCP from
NAT or a Static IP for the clients)
Subnet Mask: 255.255.0.0
Default Gateway: 169.254.9.1/16
DNS Primary: 169.254.9.1/16 (or other local DNS IP)
DNS Secondary: DNS IP of yours ISP (this usually need by old OS)
WINS IP: 169.254.9.1/16 (or other local WINS IP - if you have)

- You have to use WINS server, if you have old OS or UNIX/Linux in the LAN (Remember that UNIX/Linux need to have a static mapping on the WINS)
- You could use instead a static IP, IP from DHCP server or NAT allocation table DHCP (I recommend to use DHCP server instead NAT allocation table).
By using a Dynamic IP, the client should be configuring to be DHCP client.

Security:

1. Don't use any dynamic route protocol.
2. Don't use on the server any other Server service although you will
Need good antivirus software for servers.
3. Use IP filter on each NIC + demand dial interface.
4. You can't use L2TP from local intranet to internet if you use NAT.
5. Choose ISP that support using encrypt password/information transfer.
6. Use IPSec on yours local network or any other information encryption
Process (It has to support authentication).
7. If you have only Windows 2000 OS, disable the support for LAN manager
and NTLM authentication on the DC and the RRAS.
8. Use NTFS on each machine and remove the Everyone group full control
Permission.

For more information read:

http://www.microsoft.com/ISN/Columnists/windows_2000_home_office_gateway.asp?A=0

<http://www.labmice.net/networking/NAT.htm>

<http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/columns/cableguy/cg0301.asp>

<http://www.windows-help.net/windows2000/nat-routing.html>

<http://www.win2000mag.com/Articles/Index.cfm?ArticleID=7882>

<http://www.mcseguide.com/2000/2000netinf.htm>

<http://www.intac.com/~cdp/cptd-faq/>

<http://www.labmice.net/articles/securingwin2000.htm>