

Win2k Ras/VPN and a SCO Unix Machine and some difficulty getting to the SCO Machine [LONG]

Source: <http://unix.derkeiler.com/Newsgroups/comp.unix.sco.misc/2006-02/msg00103.html>

- *From:* Brian Keener <bkeener@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 13 Feb 2006 13:25:46 -0500
-

First let me say I am sorry for the length of this but I wanted to provide as much info as possible. I have a client that has a Compaq system running SCO Unix 5.0.7 system in conjunction with a Win2k System providing VPN access.

#uname -X

```
System = SCO_SV
Node = theirnode
Release = 3.2v5.0.7
KernelID = 2003-02-18
Machine = Xeon
BusType = ISA
Serial = XXXXXXXXXXXXX
Users = 30
OEM# = 0
Origin# = 1
NumCPU = 1
```

The bulk of their processing is done via dumb terminal connections but they also have a few in-house workstations connected via ethernet and then DSL access via Windows VPN. There is a Netopia DSL modem, a Linksys DSL/Broadband hub (acting as a Hub, router and gateway), a Linksys wireless Access Point and a Windows 2000 system which is the VPN Server and also handles some DNS functions. The Windows 2k machine has 2 NICS – one classed as WAN and one as LAN but they are on the same subnet (as you will see). Our problem is that while the internal network connections all work flawlessly the connections via the VPN are really a hit and miss sort of thing. It always seems and my testing seems to confirm that we can get to the VPN server on the Win2k box and get an IP address (using DHCP via the VPN) but then we will only be able to ping the NIC cards the Win2k machine possesses or the Linksys routers (which we had to go through to get to the VPN Box anyways) but our access to the SCO Unix box will fail while trying to connect – pings will fail as well. As I say it is hit and miss – sometimes connecting to SCO works without a hitch but then others it seems there are either extensive pauses or no connect at all. It seems we can always see the Win2k machine and when attempting to reach the SCO machine if it fails – several attempts (full disconnect and reconnect) will ultimately get you in. It also seems as if we can ping one of the Win2k NIC but not the other – this I wonder as well if it is because they are on the same

Win2k Ras/VPN and a SCO Unix Machine and some difficulty getting to the SCO Machine [LONG]

subnet.

The entire network is currently setup to run on the 192.168.1. subnet but I have gotten several opinions and found some research indicating that for the entire network to be on the one subnet with the type configuration they have is a poor setup and that it should be broken into 2 or more subnets because of the VPN, the Wireless DHCP connections and the internal fixed IP addresses. The following network configuration and IP addresses will I think make this clear to many of you who are more network savvy than we are why we are into that thought process. We also found several Microsoft Knowledge Base articles which seem to confirm issues with VPN when used with DNS and DHCP on the same server in a Microsoft environment when all the devices are on the same subnet.

The clients network configuration is as follows and except where noted (the VPN on the Win2k machine) all Network setup uses a netmask of 255.255.255.0:
DSL line into Netopia/Cayman 3347W modem

Ethernet from modem to Linksys BEFSR11 wired router (192.168.1.254) this is a two port device – one port for the WAN in and one for Ethernet out. Gateway mode, handles DHCP requests for the network (Range 192.168.1.100 for 50 ports) and also acts as DNS with its DNS set to itself.

Ethernet from router to Linksys BEFW11S4 wireless router (192.168.1.250) This is a 4 port device – one port for the wan and 4 for ethernet. Gateway mode. DNS set to point to .254.

Ethernet from wireless router to HPJ3289A hub

SCO Unix machine (192.168.1.245) is connected to hub, Gateway set to .254 and uses resolv.conf for DNS and also pointing at .254.

Both NICs on the Windows 2k machine connected to hub:

192.168.1.252 LAN Uses a gateway of .254 but set to use itself for DNS.

192.168.1.253 WAN Uses .254 for the Gateway and for DNS

192.168.1.192 is the target IP for the VPN with a mask of 255.255.255.224 and the range of VPN IP addresses is from 192.168.1.200 to 192.168.1.219 with the 200 being reserved for the VPN Server IP. I noticed the target IP in Microsoft VPN during a check of their configuration and after some research using various subnet calc programs it appears that that IP is chosen because it is the low address in the subnet range we requested for the VPN. It appears Windows bases the target IP and netmask on our selected range of a start and end of 192.168.1.200 to 192.168.1.219 – not sure why this is or how it impacts the setup but that is what it does and as I say the numbers do appear to coincide with making a small network (subnet) within the larger 192.168.1 network.

I am told that both the WAN and the LAN NIC on the same subnet is a problem and it makes sense to me why it would be – not sure why it was set up this way in the first place. I also imagine the LAN NIC set to use itself for DNS is probably also a problem and the VPN on the same subnet could also be confusing.

Win2k Ras/VPN and a SCO Unix Machine and some difficulty getting to the SCO Machine [LONG] 2

Win2k Ras/VPN and a SCO Unix Machine and some difficulty getting to the SCO Machine [LONG]

My apologies but I honestly cannot remember which but one of the Linksys devices handles the port forwarding to get the VPN traffic to the Win2k machine as it needs to be but I know one is set for port forwarding and they are both capable.

As I said at times you can access (IE Ping for testing) the Linksys (.254) and one of the Windows WAN (.253) and LAN (.252) but you cannot get to the SCO Machine (.245) and then at times all is well. Now I have also been connected via the VPN when I cannot connect to the SCO machine and called someone on-site and had them ping the SCO machine from the Windows Server and the ping is successful so the Windows 2k machine and SCO Unix Machine are still talking but it appears the VPN is failing. Obviously I think the problem is with the VPN software and research of Microsoft Knowledge Base articles would seem to confirm that. There are several articles that reference Windows machines being the PDC and doing DNS and VPN and using a subnet within the existing subnet ("On Subnet"). According to Knowledge base article 171185 from Microsoft having an "On Subnet" Vpn is acceptable. It also mentions that this is commonly accomplished by letting VPN IP addresses be handed out using DHCP. However there also appears to be connection issues when the Windows server handling VPN is also a DNS server or the PDC (Primary Domain Controller). According to Microsoft Knowledge base articles 292822, 830063 and 289735 there have been various types of connection issues when the above is true. Among other suggestions (some involving the registry) there is also one advising to change the IP Static Address range for the VPN to an "Off Subnet" network. This is in some cases part of a larger fix and in one of the Articles it was actually an alternate fix.

Two thoughts I had on eliminating some of the potential problem was 1) reassign the DHCP range to the 150 range or so and put the VPN below it at 100 or 50 or something and then we can reassign netmasks on the rest of the network so we end up with two subnets not one inside the other – all the dhcp and vpn on a low subnet and the servers on a high subnet. Since our servers and routers are at the high end this would allow two subnets but it would also require a netmask change on the SCO machine – that I am not thrilled with. 2) I had also thought about simply moving the VPN to say the 192.168.2.200 to 192.168.2.219 subnet and see if that helps but then I am sure I will run into routing issues getting connections to and from the SCO Unix box to the VPN Connections since Windows will probably not handle the routing between its own VPN and its LAN NIC which would be on 192.168.1. I have also thought that in addition to that I would move the WAN NIC of the Windows machine and the Linksys Routers (actually only one and loose the other – we do not need them both) to the 192.168.3 subnet but then that really compounds my routing issues as I will now have 3 subnets but my thoughts on this from what I have read is that this is the best way to go.

I had thought I would attempt the VPN change first (#2 above) and then depending on the results I would consider (if still necessary) changing the WAN NIC and the Linksys Router and changing my routes and Gateways accordingly. I really am trying to stay away from mucking with the SCO IP addresses and netmask.

Win2k Ras/VPN and a SCO Unix Machine and some difficulty getting to the SCO Machine [LONG]

I am hoping someone can offer some further insight as to the most appropriate changes to make and what routes I need or someplace I can go to research how you determine routes and then I would also like some discussion on their network setup as a whole and how to improve or eliminate these glitches.

Thanks to all for any suggestions , insight, and info.

bk

.