

Re: Can I remote desktop to this?

Re: Can I remote desktop to this?

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2007-07/msg07361.html>

- *From:* "Vanguard" <vanguard.x@xxxxxxxxxxxxx>
 - *Date:* Tue, 31 Jul 2007 00:21:04 -0500
-

"DeanB" wrote in message news:1185856685.030425.170820@xx

When I type IPCONFIG on my home computer, I get the following:

```
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : XXXXXXXXXX.net
IP Address. . . . . : 192.168.1.XXX
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

Can anyone tell me the address I should put into Remote Desktop, to be able to see this from a typical office LAN? I have XXXXed out some of the values for security.

On the other computer (where you run the Remote Desktop Client), you will need to enter the WAN-side IP address of your router or cable modem. If you are using a router, you will need to configure port forwarding so connects on the WAN-side of the router to port 3389 (unless you change the RDP listening port per <http://support.microsoft.com/kb/306759>). Port forwarding on the router says to which host connects on its port go to which host in your intranet.

Since your IP address is dynamic, it can change after it expires. That means you may be unable to RDP to the remote host until you update your RDP client to use the new IP number. Looking into using DynDNS which gives you an IP name to which you can connect. You use their IP name for your host and their nameserver returns what is the current IP address for your host (or your router, if you use one). Some routers support DynDNS but I find the IP update isn't reliable. Instead I run their client program on my host to which I want to connect, and then use port forwarding on the router so connects to port 3389 get forwarded to my host (also with RDP listening on port 3389).

Company networks may block outbound connects using RDP to prevent their employees from adding their home PCs onto the corporate network. They will definitely block inbound RDP connects from your home to a host on their corporate network. They don't want you screwing up their security by adding your host to their network, and they don't want hackers coming in to attempt to hack into one of their hosts. Even if you do get it working, you had better tell your IT department what you are doing. It is likely they will bar you from adding your host to their network or allowing anyone, including yourself, from hacking into their network using RDP – and not telling them can get your fired (because they do run packet sniffers and traffic loggers to

Re: Can I remote desktop to this?

determine what their employees are doing).

If you do get RDP to work and you are allowed to do so, make damn sure you change the login password for your account. Make sure it is a very strong password. After all, anyone can probably guess the username that you select but how hard it is for them to hack into your host will depend on the strength of your login password. This is the login password for your Windows session.

.