In Microsoft Windows, starting from Windows XP, there is a built-in ability to set up **network ports forwarding** (port forwarding). Due to it, any connection coming to any port can be forwarded to another local port or even to port on remote computer. Not necessarily that the system has a service listens on this port.

Port forwarding in Windows can be configured using **Portproxy** mode of the command **Netsh**. The syntax of this command is as follows:

```
netsh interface portproxy add v4tov4 listenaddress=localaddress listenport=localport connectaddress=destaddress connectport=destport
```

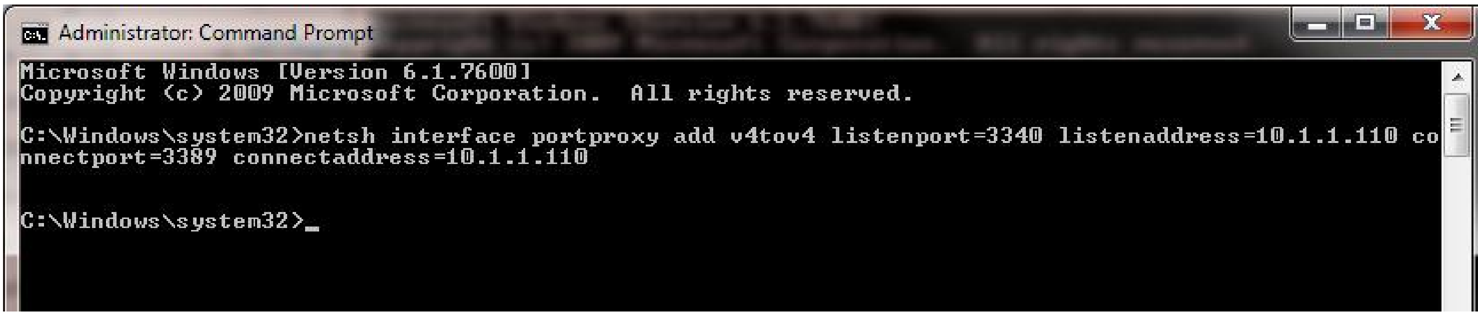
where

1. **listenaddress** is a local ip address waiting for a connection
2. **listenport** listening port (the connection is waited on it)
3. **connectaddress** is an IP address or DNS name to which the connection will be forwarded
4. **connectport** is a TCP port to which the connection from listenport is forwarded to

Suppose, that our task is to make the RDP service to respond on a non-standard port, for example 3340 (the port can be changed in the settings of the service, but we will use RDP to make it easier to demonstrate forwarding).

Start the command prompt as an administrator and perform the following command:

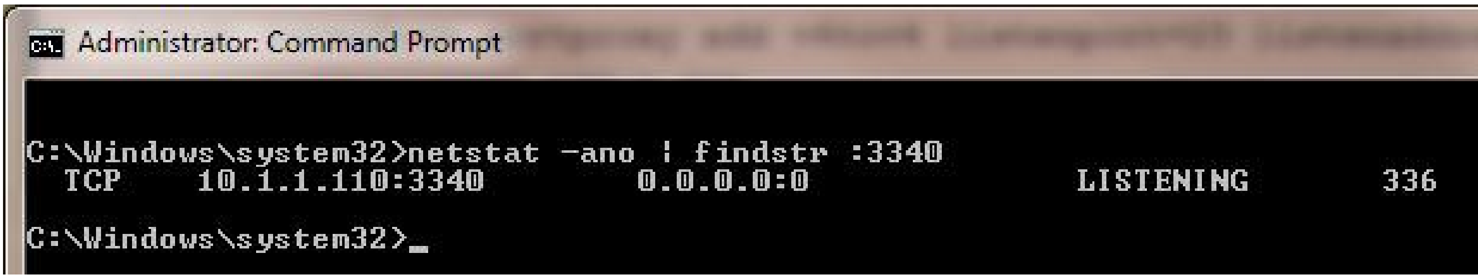
netsh interface portproxy add v4tov4 listenport=3340 listenaddress=10.1.1.110 connectport=3389 connectaddress=10.1.1.110



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>netsh interface portproxy add v4tov4 listenport=3340 listenaddress=10.1.1.110 co
nnectport=3389 connectaddress=10.1.1.110

C:\Windows\system32>_
```

Using netstat make sure that port 3340 is listened now

netstat -ano | findstr :3340

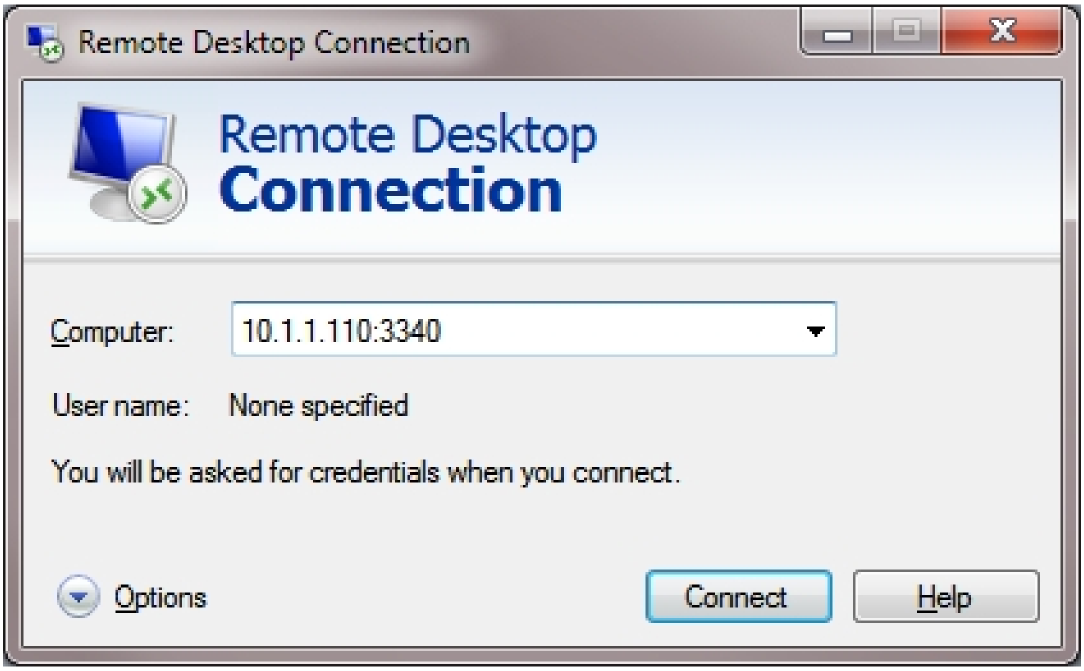


```
C:\Windows\system32>netstat -ano | findstr :3340
  TCP    10.1.1.110:3340        0.0.0.0:0              LISTENING       336

C:\Windows\system32>_
```

You can find out what process is listening to this port use its PID (in our example, the PID is 336):

tasklist | findstr 336

Let’s try to connect to this computer from a remote system using any RDP client. Port 3340 should be specified as the RDP port. (It is specified after the column following the RDP server address):



Computer: 10.1.1.110:3340

User name: None specified

You will be asked for credentials when you connect.

The connection should be established successful.

Important. Make sure that your firewall (Windows Firewall or a third-party one that are often included into an antivirus software) allows incoming connections to the new port. If necessary, you can add a new Windows Firewall rule using this command:

```
netsh advfirewall firewall add rule name=”RDP_3340” protocol=TCP dir=in localip=10.1.1.110 localport=3340 action=allow
```

Display the list of forwarding rules in the system:

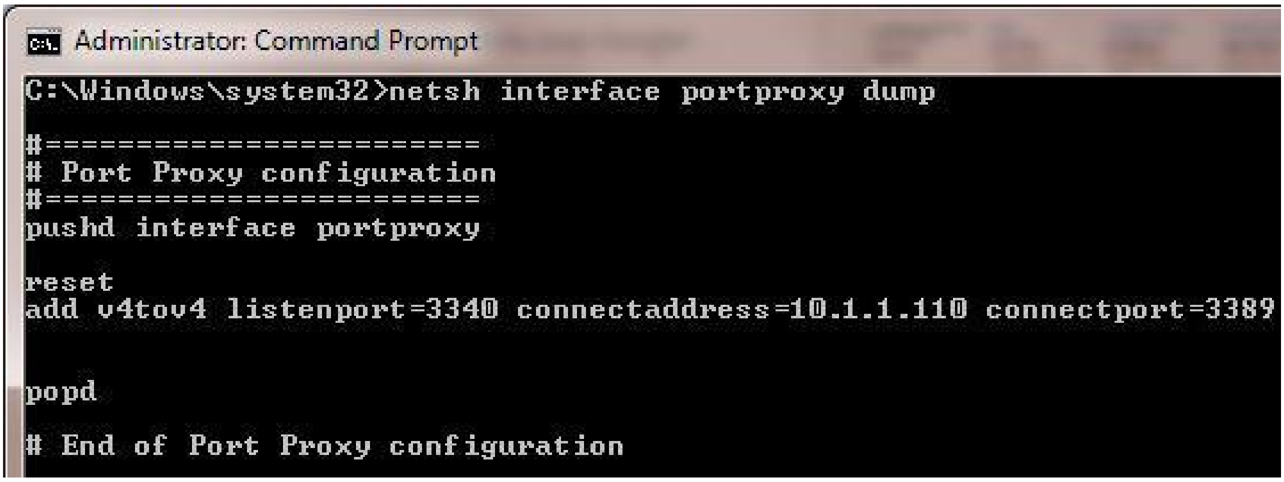
```
netsh interface portproxy show all
```

In our case there is only one forwarding rule from port 3340 to 3389:

```
Listen on ipv4:             Connect to ipv4:
 Address        Port       Address        Port
 --------------- ----------  --------------- ----------
 10.1.1.110     3340       10.1.1.110     3389
```

Tip. Also, portproxy settings can be obtained as follows:

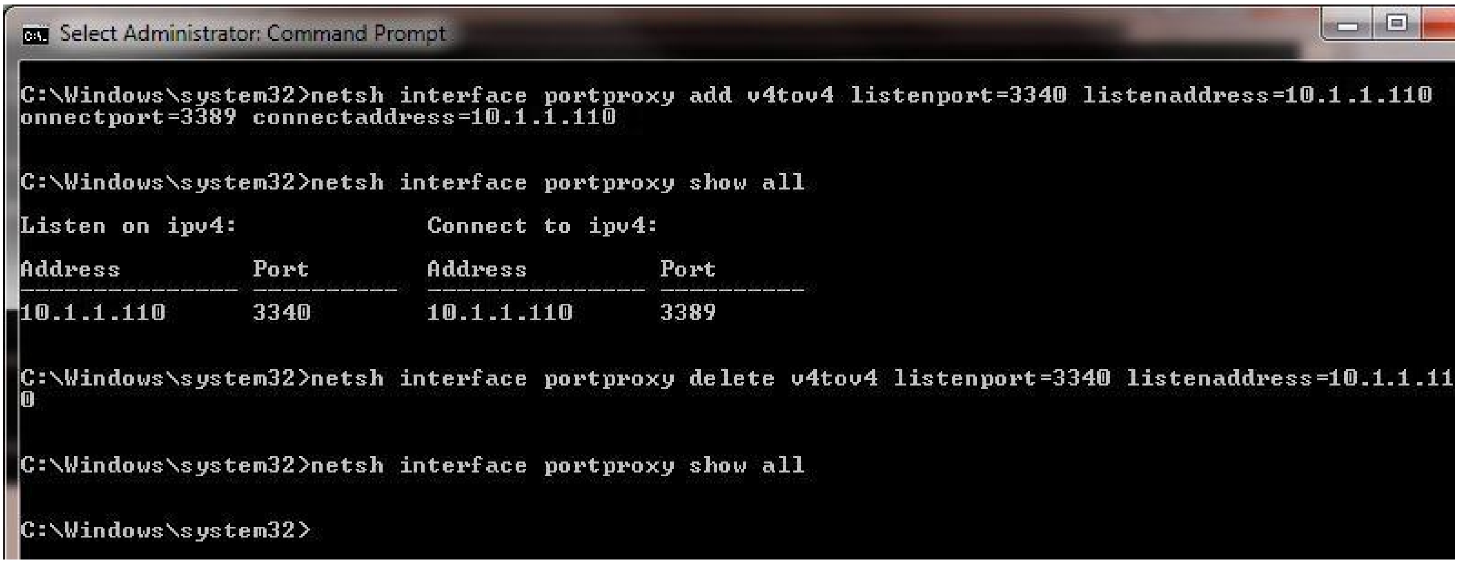
```
 netsh interface portproxy dump
 #========================
 # Port Proxy configuration
 #========================
 pushd interface portproxy
 reset
 add v4tov4 listenport=3340 connectaddress=10.1.1.110 connectport=3389
 popd
 # End of Port Proxy configuration
```



```
C:\Windows\system32>netsh interface portproxy dump

#========================
# Port Proxy configuration
#========================
pushd interface portproxy

reset
add v4tov4 listenport=3340 connectaddress=10.1.1.110 connectport=3389


popd

# End of Port Proxy configuration
```

To remove a forwarding rule:

netsh interface portproxy delete v4tov4 listenport=3340 listenaddress=10.1.1.110



```
C:\Windows\system32>netsh interface portproxy add v4tov4 listenport=3340 listenaddress=10.1.1.110
onnectport=3389 connectaddress=10.1.1.110

C:\Windows\system32>netsh interface portproxy show all

Listen on ipv4:             Connect to ipv4:

Address         Port        Address         Port
--------------- ----------  --------------- ----------
10.1.1.110      3340        10.1.1.110      3389

C:\Windows\system32>netsh interface portproxy delete v4tov4 listenport=3340 listenaddress=10.1.1.11
0

C:\Windows\system32>netsh interface portproxy show all

C:\Windows\system32>
```

To clear all current forwarding rules:

netsh interface portproxy reset

Important. This forwarding scheme works only for TCP ports. You won’t be able to forward UDP ports this way. Also you can’t use 127.0.0.1 as connectaddress.

If you wont to forward an incoming TCP connection to another computer, the command can look like this:

netsh interface portproxy add v4tov4 listenport=3389 listenaddress=0.0.0.0 connectport=3389 connectaddress=192.168.100.101

This rule forwards all incoming RDP requests to the IP address 192.168.100.101

Another portproxy feature is an opportunity to make it look like any remote network service is operating locally.

For example, forward the connection from the local port 5555 to the remote address 157.166.226.25 (CNN website):

```
netsh interface portproxy add v4tov4 listenport=5555 connectport=80 connectaddress=
157.166.226.25 protocol=tcp
```

Now if you go to http://localhost:5555/ in your browser, CNN Start page will open. So despite the browser addresses the local computer, it opens a remote page.