

TCP/IP Diagnostic Utilities on Windows 2008 Server

June 20, 2012

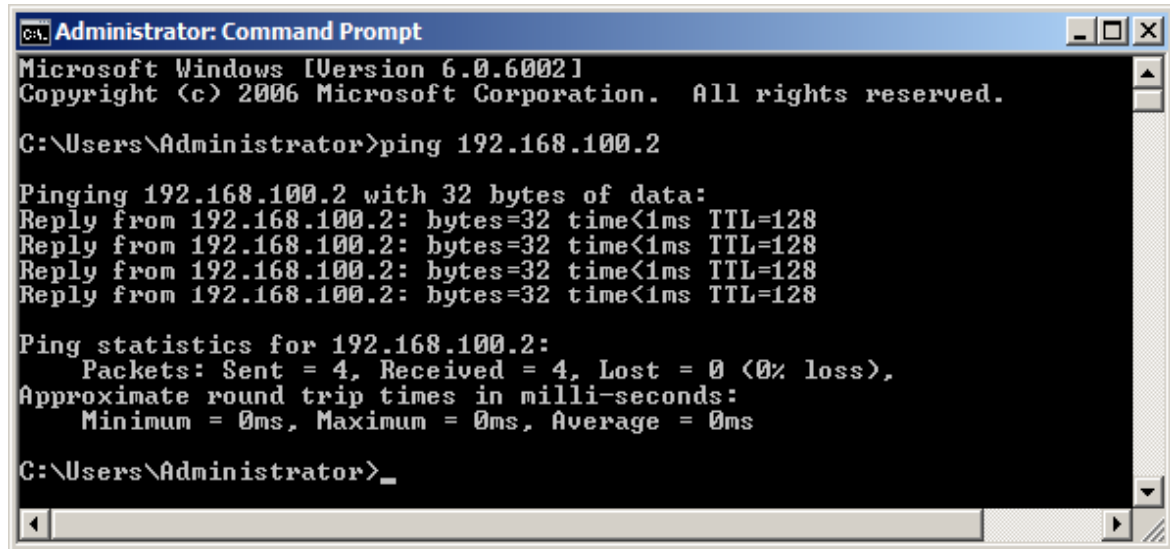
TCP/IP Utilities

In this lesson, we will learn about how to use the TCP/IP utilities to test our network. These functions come in handy when troubleshooting problems on a network.

Name	Description
Ping	A utility to test connectivity with a network device
Ipconfig	Gives the technician the complete listing of addresses for our device's Network Interface Card
Nslookup	Returns the DNS server IP address
Tracert	Shows the number of hops from our device to the IP address requested
ARP	Address Resolution Protocol utility that returns the MAC address of the gateway router or server
Hostname	Returns our computer name
Nbtstat	Shows NETBIOS connections
Pathping	Acts as a Ping and Tracert utility

Ping

Ping is a TCP/IP Utility is designed to test for connectivity to another device on the network. We can use the function to test to see if we are connected to a router or to see if the cable is functioning.

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the output of a ping command. The text is as follows:

```
Microsoft Windows [Version 6.0.6002.1]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:
Reply from 192.168.100.2: bytes=32 time<1ms TTL=128
Reply from 192.168.100.2: bytes=32 time<1ms TTL=128
Reply from 192.168.100.2: bytes=32 time<1ms TTL=128
Reply from 192.168.100.2: bytes=32 time<1ms TTL=128

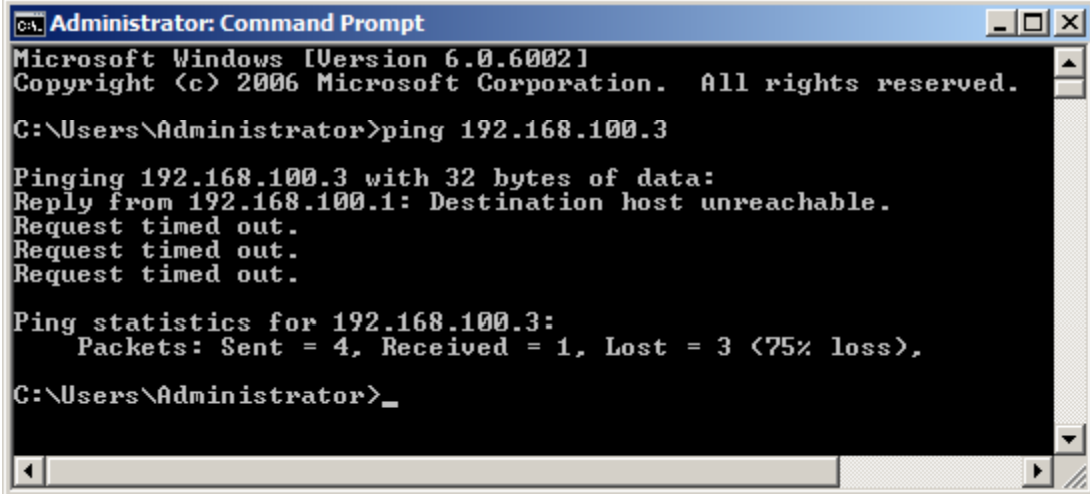
Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>_
```

We can type “ping”, then a space and then a IP address that exists on our network. In this example, we ping 192.168.10.1. We receive from 192.168.10.1 four times in 1 millisecond. There is a summary report showing the number of packets sent, received, and the approximate round trip time. The minimum, maximum and average round trip is shown.

Request Timed Out

If the device being pinged is not on or maybe the cable is defective or unplugged, we will get a “request timed out” return four times as we see in our example.

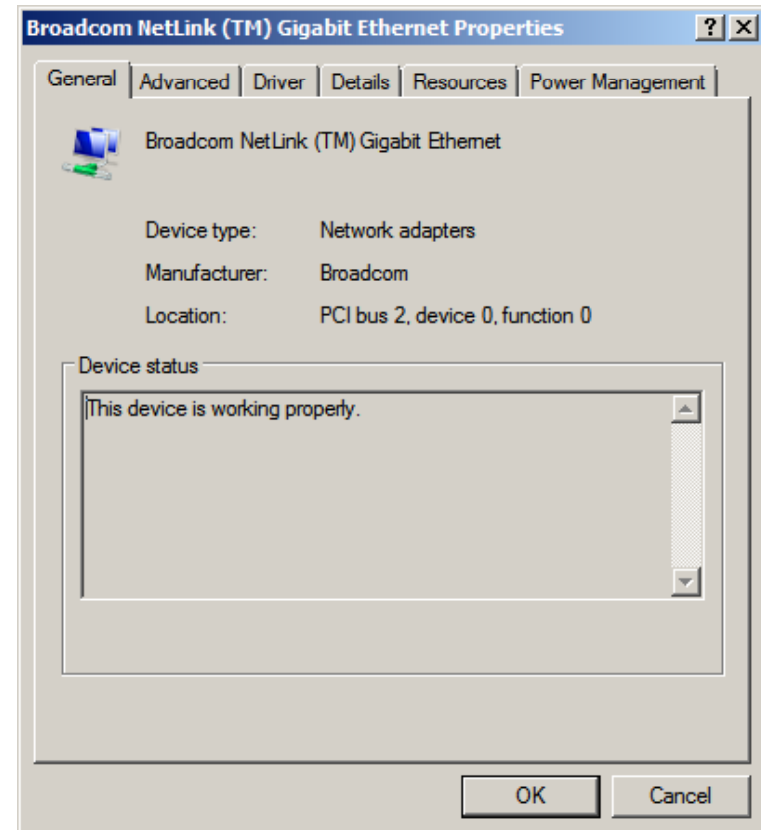
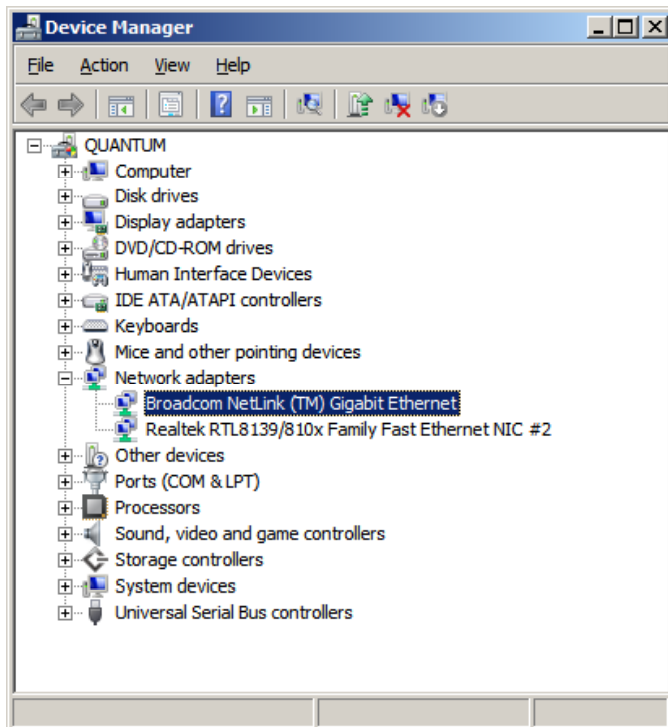
A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the output of a ping command. The text inside the window is as follows:

```
Microsoft Windows [Version 6.0.6002]  
Copyright (c) 2006 Microsoft Corporation. All rights reserved.  
  
C:\Users\Administrator>ping 192.168.100.3  
  
Pinging 192.168.100.3 with 32 bytes of data:  
Reply from 192.168.100.1: Destination host unreachable.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 192.168.100.3:  
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),  
  
C:\Users\Administrator>_
```

If we get a request timed out, we should always check that the cable is connected to the personal computer. Next, we should check the computer's Device manager to see if the network interface card is operating. Between these two checks, we typically can determine why the ping to the server is not working.

Checking the Device Manager

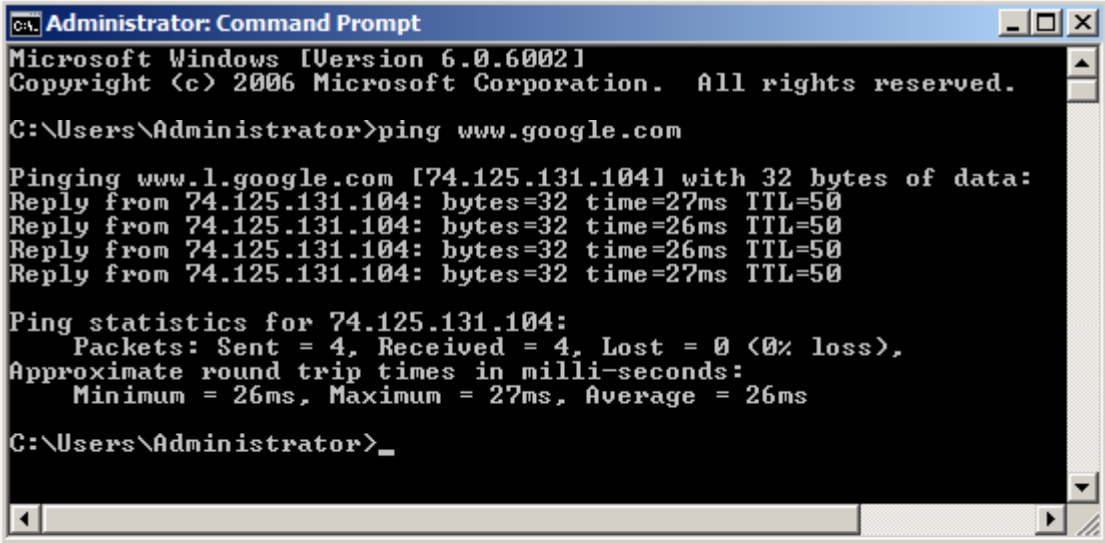
In the Device Manager, we can see the Network Adapter is loaded and when we double click on the device, we can see that the device is working properly in the status report.



Ping by Name

We can ping a device by its name on the network or we can ping a web server by typing the Internet address such `www.google.com`.

In our example, we pinged a device called `computer1`. We can check the computer name of another device on the network and ping that machine.



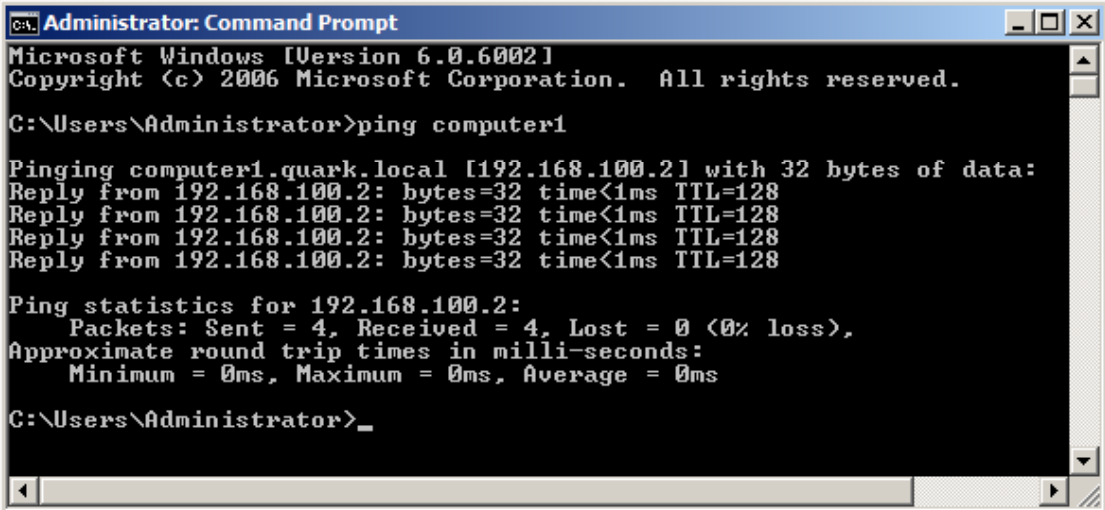
```
C:\>Administrator: Command Prompt
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping www.google.com

Pinging www.l.google.com [74.125.131.104] with 32 bytes of data:
Reply from 74.125.131.104: bytes=32 time=27ms TTL=50
Reply from 74.125.131.104: bytes=32 time=26ms TTL=50
Reply from 74.125.131.104: bytes=32 time=26ms TTL=50
Reply from 74.125.131.104: bytes=32 time=27ms TTL=50

Ping statistics for 74.125.131.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 27ms, Average = 26ms

C:\Users\Administrator>
```



```
C:\>Administrator: Command Prompt
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping computer1

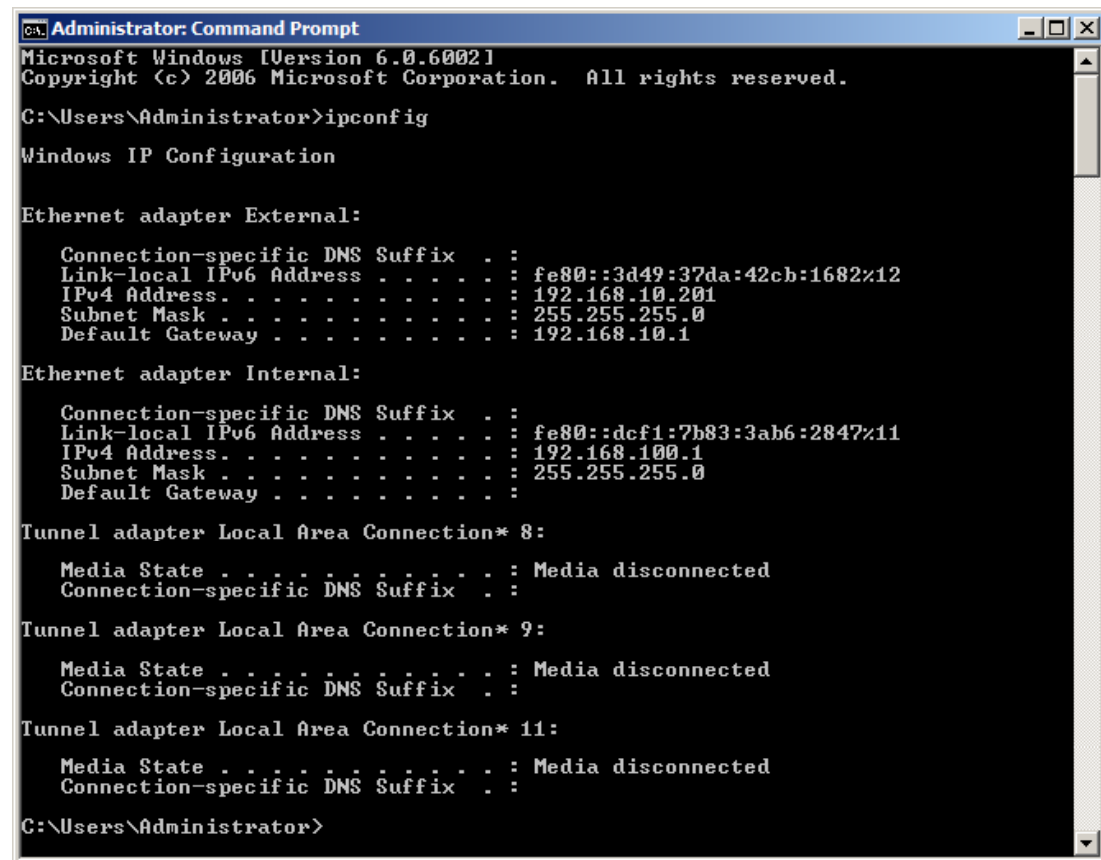
Pinging computer1.quark.local [192.168.100.2] with 32 bytes of data:
Reply from 192.168.100.2: bytes=32 time<1ms TTL=128
Reply from 192.168.100.2: bytes=32 time<1ms TTL=128
Reply from 192.168.100.2: bytes=32 time<1ms TTL=128
Reply from 192.168.100.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

IPConfig

The IPConfig function will give us the IP address of our network interface cards and of the gateway. A gateway could be a router or another server. After opening the command line, we type “ipconfig” and Enter. We see the external network connection of 192.168.10.201 and subnet mask of 255.255.255.0. The default gateway of the router is 192.168.10.1

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the output of the "ipconfig" command. It displays configuration for three network adapters: Ethernet adapter External, Ethernet adapter Internal, and three Tunnel adapters (Local Area Connection* 8, 9, and 11). The External adapter has an IPv4 address of 192.168.10.201 and a default gateway of 192.168.10.1. The Internal adapter has an IPv4 address of 192.168.100.1. All tunnel adapters show a media state of "Media disconnected".

```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter External:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::3d49:37da:42cb:1682%12
    IPv4 Address. . . . . : 192.168.10.201
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

Ethernet adapter Internal:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::dcf1:7b83:3ab6:2847%11
    IPv4 Address. . . . . : 192.168.100.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Tunnel adapter Local Area Connection* 8:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 9:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

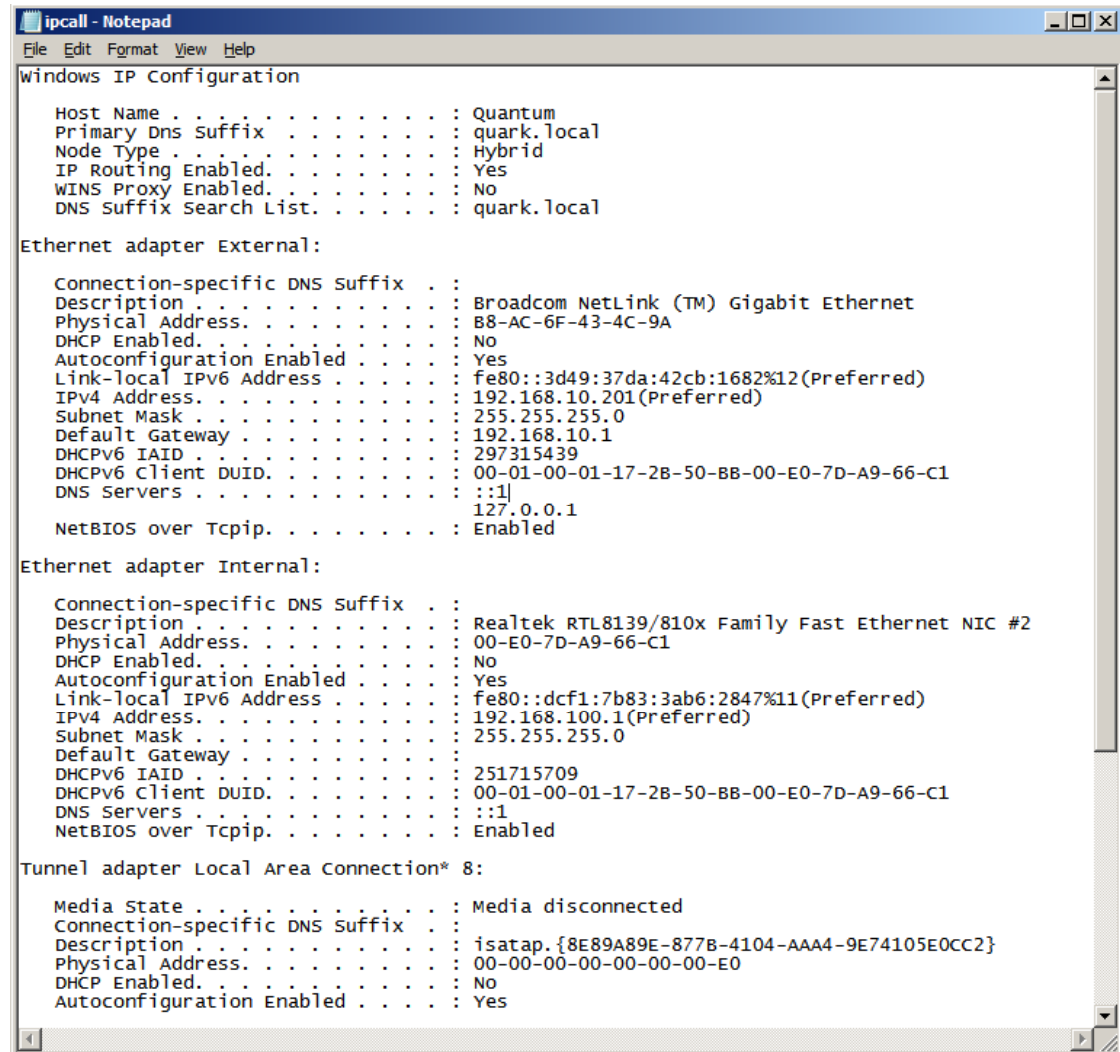
C:\Users\Administrator>
```

We also can observe the internal network adapter has an IP address of 192.168.100.1, a subnet mask of 255.255.255.0 and no default gateway.

IPConfig/all

A more complete report about our computer and the devices we are connected to is the Ipconfig/all report. This report also contains the network card's Media Access Control (MAC) address that is unique. This complete report is more helpful when troubleshooting client server connections.

Type ipconfig/all>ipcall.txt to write the long report to a text file.



```
ipcall - Notepad
File Edit Format View Help
Windows IP Configuration

Host Name . . . . . : Quantum
Primary Dns Suffix . . . . . : quark.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : Yes
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : quark.local

Ethernet adapter External:

Connection-specific DNS Suffix . : 
Description . . . . . : Broadcom NetLink (TM) Gigabit Ethernet
Physical Address. . . . . : B8-AC-6F-43-4C-9A
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::3d49:37da:42cb:1682%12(Preferred)
IPv4 Address. . . . . : 192.168.10.201(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1
DHCPv6 IAID . . . . . : 297315439
DHCPv6 Client DUID. . . . . : 00-01-00-01-17-2B-50-BB-00-E0-7D-A9-66-C1
DNS Servers . . . . . : ::1
                        127.0.0.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Internal:

Connection-specific DNS Suffix . : 
Description . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC #2
Physical Address. . . . . : 00-E0-7D-A9-66-C1
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::dcf1:7b83:3ab6:2847%11(Preferred)
IPv4 Address. . . . . : 192.168.100.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 
DHCPv6 IAID . . . . . : 251715709
DHCPv6 Client DUID. . . . . : 00-01-00-01-17-2B-50-BB-00-E0-7D-A9-66-C1
DNS Servers . . . . . : ::1
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Local Area Connection* 8:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : isatap.{8E89A89E-877B-4104-AAA4-9E74105E0CC2}
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```


IPConfig Release

When we are connecting to our server from a client using Dynamic Host Control Protocol (DHCP) , we can change our IP address by using ipconfig/release at the command line. The report will show the IP address and subnet mask as 0.0.0.0.

```
C:\Documents and Settings>ipconfig/release

Windows IP Configuration

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 0.0.0.0
    Subnet Mask . . . . .             : 0.0.0.0
    Default Gateway . . . . .         :
```

IPConfig Renew

To get a new IP address from the server, we type ipconfig/renew at the command line. The request is sent to the router and in a few seconds, the NIC is assigned an IP address.

```
C:\Documents and Settings>ipconfig/renew
Windows IP Configuration

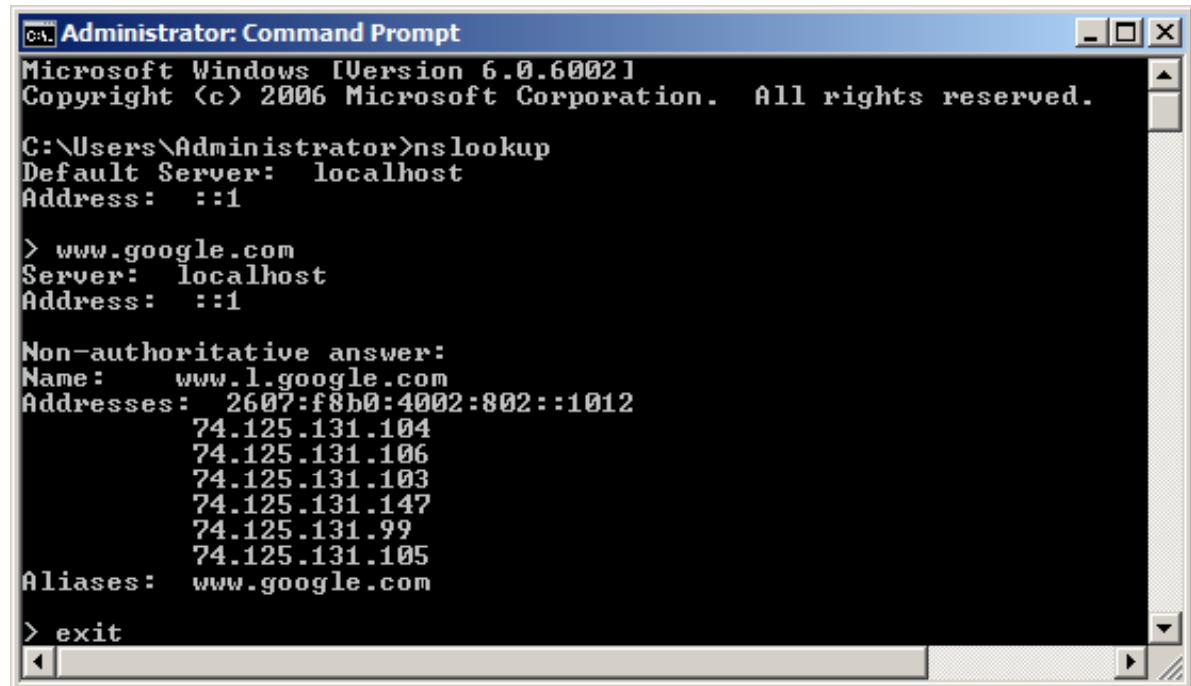
Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix  . : Instructor
    IP Address. . . . .               : 192.168.10.100
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.10.1
```

NSLookup

We can check the DNS server by using the NSLookup utility.

We type “nslookup” at the command line and www.google.com. Our DNS server resolves the URL to their IP address as they are shown. We type exit to leave the command.



```
C:\> Administrator: Command Prompt
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

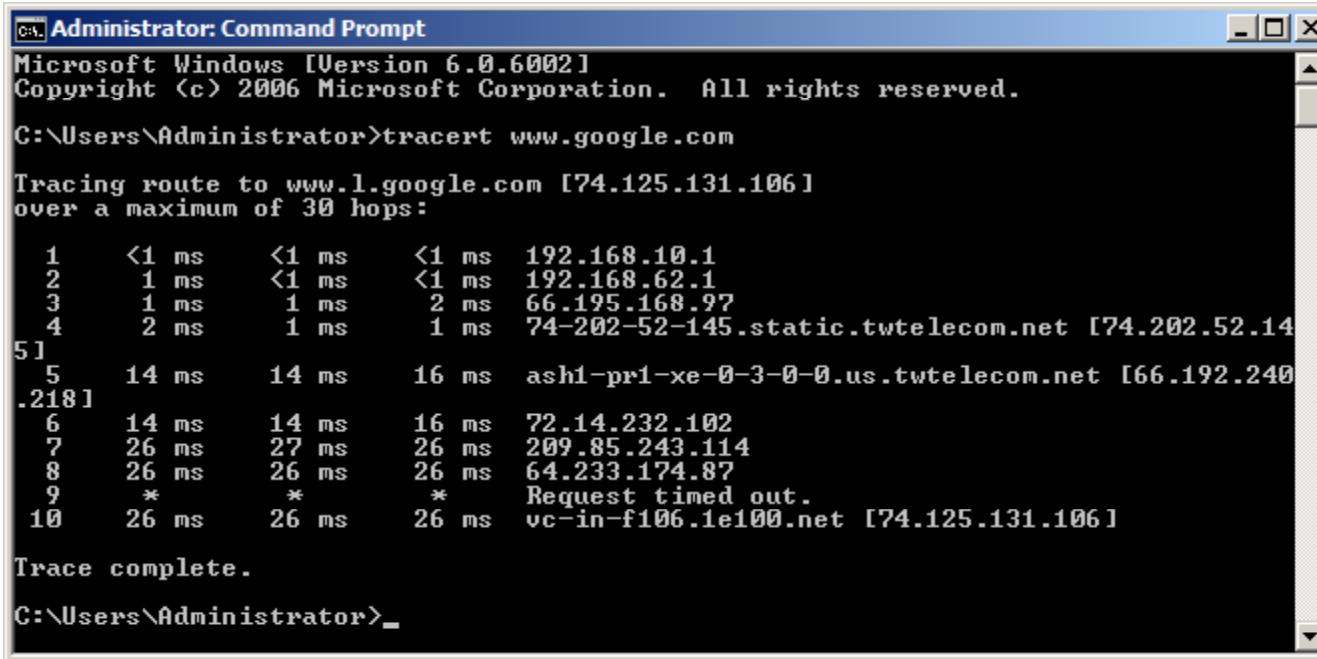
C:\Users\Administrator>nslookup
Default Server:  localhost
Address:  ::1

> www.google.com
Server:  localhost
Address:  ::1

Non-authoritative answer:
Name:    www.l.google.com
Addresses:  2607:f8b0:4002:802::1012
           74.125.131.104
           74.125.131.106
           74.125.131.103
           74.125.131.147
           74.125.131.99
           74.125.131.105
Aliases:  www.google.com

> exit
```

Tracert



```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>tracert www.google.com

Tracing route to www.l.google.com [74.125.131.106]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    192.168.10.1
  1  1 ms     <1 ms    <1 ms    192.168.62.1
  2  1 ms     1 ms     2 ms     66.195.168.97
  3  2 ms     1 ms     1 ms     74-202-52-145.static.twtelecom.net [74.202.52.145]
  4  14 ms    14 ms    16 ms    ash1-pr1-xe-0-3-0-0.us.twtelecom.net [66.192.240.218]
  5  14 ms    14 ms    16 ms    72.14.232.102
  6  26 ms    27 ms    26 ms    209.85.243.114
  7  26 ms    26 ms    26 ms    64.233.174.87
  8  *        *        *        Request timed out.
  9  26 ms    26 ms    26 ms    vc-in-f106.1e100.net [74.125.131.106]

Trace complete.

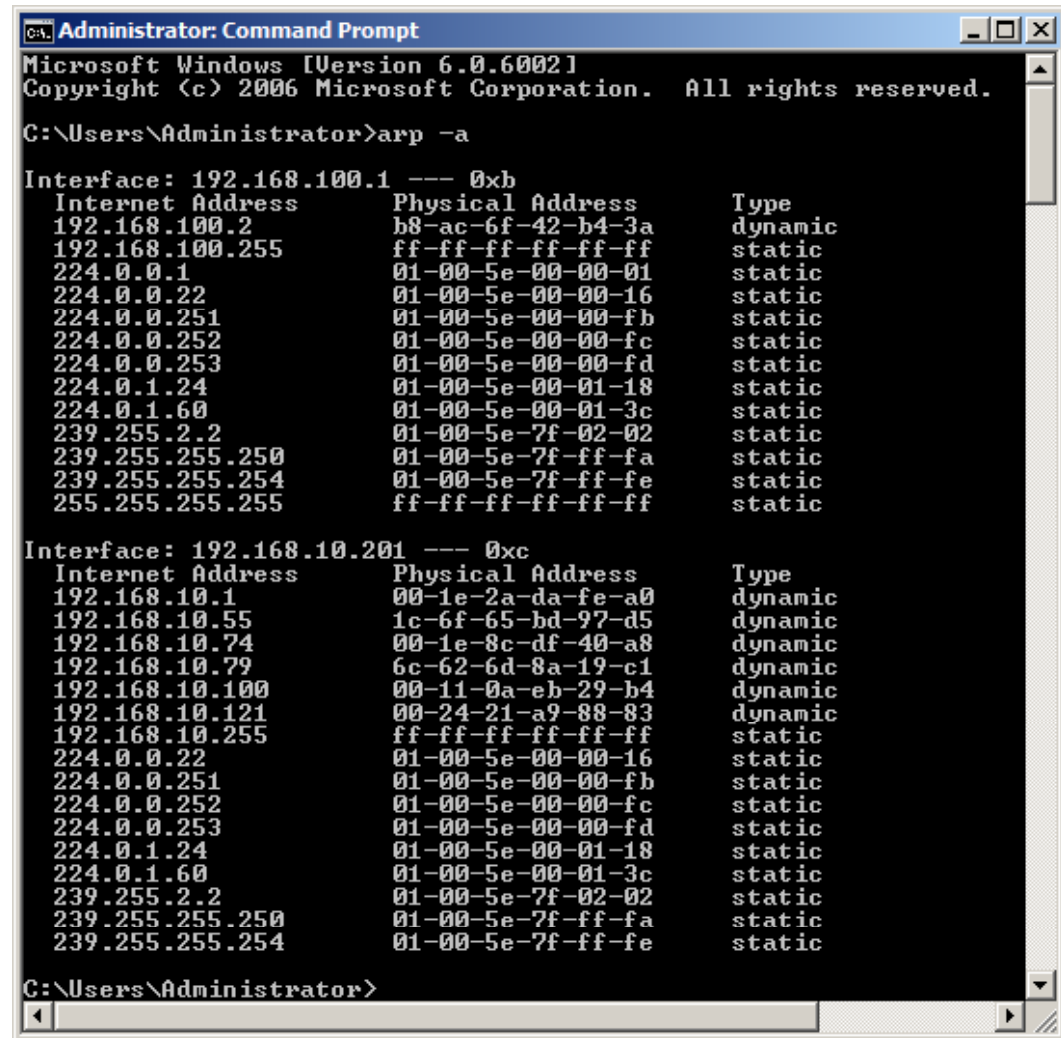
C:\Users\Administrator>
```

When we want to obtain the route that our computer is taking to communicate with another network device, we use the Tracert TCP/IP utility.

In our example, we trace route the Google server by typing “tracert www.google.com” at the command line. Starting at our location we can see each hop to the Google web server.

ARP-A

The ARP (Address Resolution Protocol) TCP/IP Utility will find the server or router gateway's IP address, MAC address and type of IP address, whether static or dynamic.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>arp -a

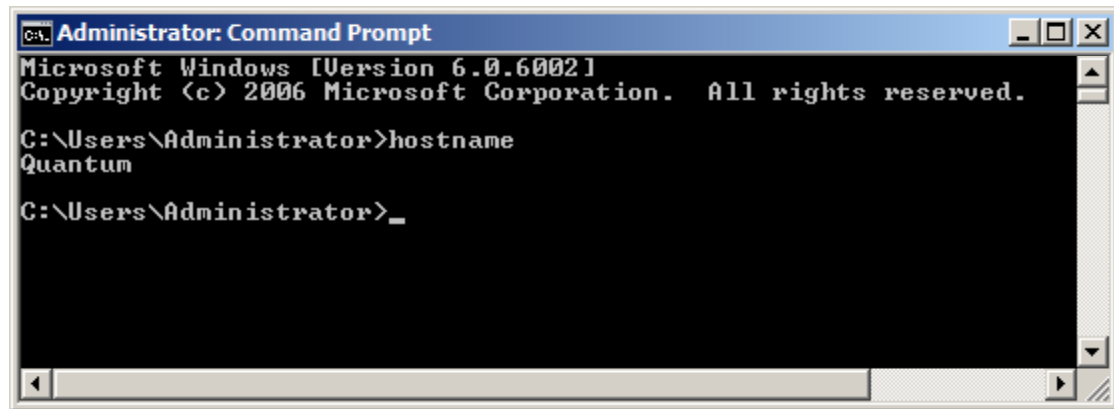
Interface: 192.168.100.1 --- 0xb
Internet Address      Physical Address      Type
192.168.100.2         b8-ac-6f-42-b4-3a     dynamic
192.168.100.255       ff-ff-ff-ff-ff-ff     static
224.0.0.1             01-00-5e-00-00-01     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
224.0.0.253           01-00-5e-00-00-fd     static
224.0.1.24            01-00-5e-00-01-18     static
224.0.1.60            01-00-5e-00-01-3c     static
239.255.2.2           01-00-5e-7f-02-02     static
239.255.255.250       01-00-5e-7f-ff-fa     static
239.255.255.254       01-00-5e-7f-ff-fe     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.10.201 --- 0xc
Internet Address      Physical Address      Type
192.168.10.1          00-1e-2a-da-fe-a0     dynamic
192.168.10.55         1c-6f-65-bd-97-d5     dynamic
192.168.10.74         00-1e-8c-df-40-a8     dynamic
192.168.10.79         6c-62-6d-8a-19-c1     dynamic
192.168.10.100        00-11-0a-eb-29-b4     dynamic
192.168.10.121        00-24-21-a9-88-83     dynamic
192.168.10.255        ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
224.0.0.253           01-00-5e-00-00-fd     static
224.0.1.24            01-00-5e-00-01-18     static
224.0.1.60            01-00-5e-00-01-3c     static
239.255.2.2           01-00-5e-7f-02-02     static
239.255.255.250       01-00-5e-7f-ff-fa     static
239.255.255.254       01-00-5e-7f-ff-fe     static

C:\Users\Administrator>
```

Hostname

The Hostname TCP/IP Utility will bring up our computer's name.



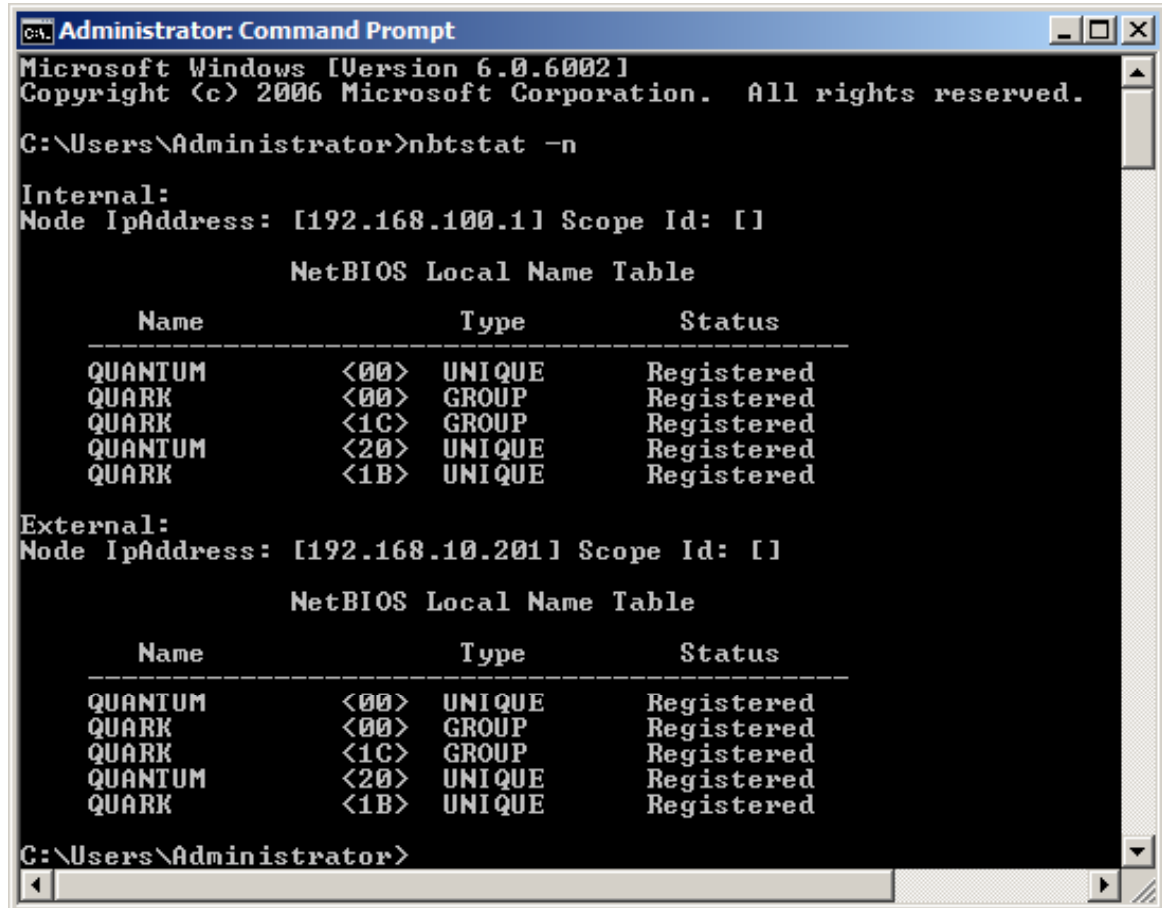
```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>hostname
Quantum

C:\Users\Administrator>_
```

NBTSTAT

The NBTSTAT TCP/IP Utility will show NETBIOS connections for each network card in our computer.



```
C:\>Administrator: Command Prompt
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -n

Internal:
Node IpAddress: [192.168.100.1] Scope Id: []

        NetBIOS Local Name Table

        Name                Type                Status
        -----
        QUANTUM              <00> UNIQUE           Registered
        QUARK                 <00> GROUP           Registered
        QUARK                 <1C> GROUP           Registered
        QUANTUM              <20> UNIQUE           Registered
        QUARK                 <1B> UNIQUE           Registered

External:
Node IpAddress: [192.168.10.201] Scope Id: []

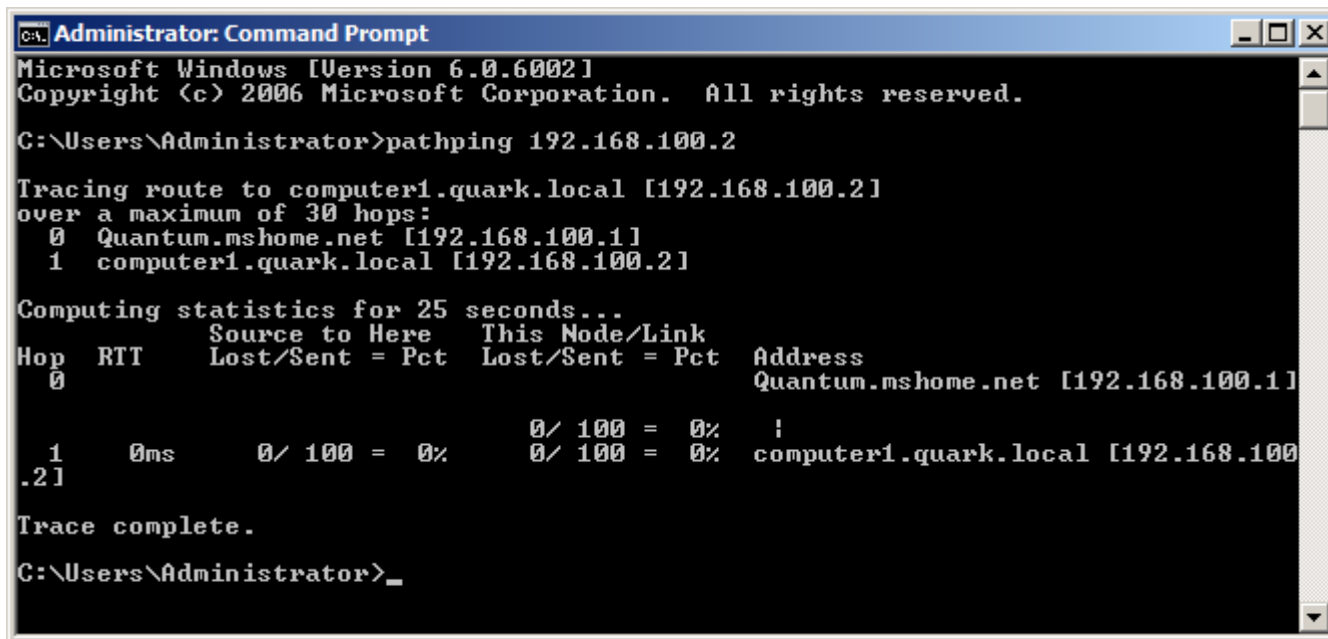
        NetBIOS Local Name Table

        Name                Type                Status
        -----
        QUANTUM              <00> UNIQUE           Registered
        QUARK                 <00> GROUP           Registered
        QUARK                 <1C> GROUP           Registered
        QUANTUM              <20> UNIQUE           Registered
        QUARK                 <1B> UNIQUE           Registered

C:\Users\Administrator>
```

Pathping

The Pathping TCP/IP Utility will conduct a ping test and tracer test at the same time.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>pathping 192.168.100.2

Tracing route to computer1.quark.local [192.168.100.2]
over a maximum of 30 hops:
  0  Quantum.mshome.net [192.168.100.1]
  1  computer1.quark.local [192.168.100.2]

Computing statistics for 25 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
  0                               Lost/Sent = Pct  Lost/Sent = Pct
  0                               0/ 100 = 0%      0/ 100 = 0%      Quantum.mshome.net [192.168.100.1]
  1    0ms      0/ 100 = 0%      0/ 100 = 0%      !
  1    0ms      0/ 100 = 0%      0/ 100 = 0%      computer1.quark.local [192.168.100.2]

Trace complete.

C:\Users\Administrator>_
```


Review

1. How do we open the command window to run a TCP/IP Utility?
2. What TCP/IP Utilities will give us the number of hops to an IP address destination?
3. What TCP/IP Utility will give us the DNS server address for our network?
4. What TCP/IP Utility will tell us our computer's name?
5. What TCP/IP Utility will give us the gateway's MAC address?
6. What TCP/IP Utility will give us the NETBIOS names of our connections?
7. What is the difference between the IPConfig and IPConfig/all report?
8. What happens to the Ping report if the cable is unplugged?
9. How do we change our IP address on a DHCP router?
10. When we are in the NSlookup function, what do we type to close out the report?