



## Lab 1.1.7 Using ping and tracert from a Workstation

### Objective

- Learn to use the TCP/IP Packet Internet Groper (**ping**) command from a workstation.
- Learn to use the Traceroute (**tracert**) command from a workstation.
- Observe name resolution occurrences using WINS and/or DNS servers.

### Background

This lab assumes the use of any version of Windows. This is a non-destructive lab and can be done on any machine without concern of changing the system configuration.

Ideally, this lab is performed in a LAN environment that connects to the Internet. It can be done from a single remote connection via a modem or DSL-type connection. The student will need the IP addresses that were recorded in the previous lab. The instructor might also furnish additional IP addresses.

**Note:** Ping has been used in many DOS attacks and many school network administrators have turned off ping, echo reply, from the border routers. If the network administrator has turned off echo reply then it is possible for a remote host to appear to be offline when the network is operational.

### Step 1 Establish and verify connectivity to the Internet

This ensures the computer has an IP address.

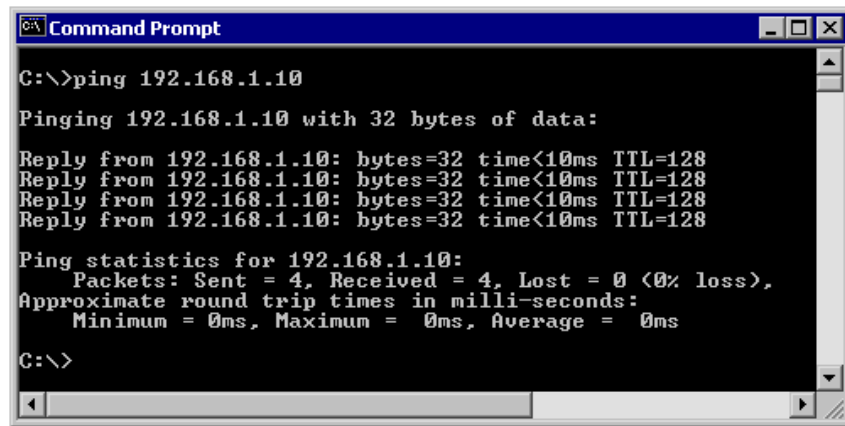
### Step 2 Access the command prompt

**Windows 95 / 98 / Me users** – Use the Start menu to open the MS-DOS Prompt window. Press **Start > Programs > Accessories > MS-DOS Prompt** or **Start > Programs > MS-DOS**.

**Windows NT / 2000 / XP users** – Use the Start menu to open the Command Prompt window. Press **Start > Programs > Accessories > Command Prompt** or **Start > Programs > Command Prompt** or **Start > All Programs > Command Prompt**.

### Step 3 ping the IP address of another computer

In the window, type **ping**, a space, and the IP address of a computer recorded in the previous lab. The following figure shows the successful results of **ping** to this IP address.



```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

**ping** uses the ICMP echo request and echo reply feature to test physical connectivity. Since **ping** reports on four attempts, it gives an indication of the reliability of the connection. Look over the results and verify that the **ping** was successful. Is the **ping** successful? If not, perform appropriate troubleshooting. \_\_\_\_\_

If a second networked computer is available, try to **ping** the IP address of the second machine. Note the results. \_\_\_\_\_

#### Step 4 ping the IP address of the default gateway

Try to **ping** the IP address of the default gateway if one was listed in the last exercise. If the **ping** is successful, it means there is physical connectivity to the router on the local network and probably the rest of the world.

#### Step 5 ping the IP address of a DHCP or DNS servers

Try to **ping** the IP address of any DHCP and/or DNS servers listed in the last exercise. If this works for either server, and they are not in the network, what does this indicate?

Was the **ping** successful? \_\_\_\_\_

If not, perform appropriate troubleshooting.

#### Step 6 ping the Loopback IP address of this computer

Type the following command: **ping 127.0.0.1**

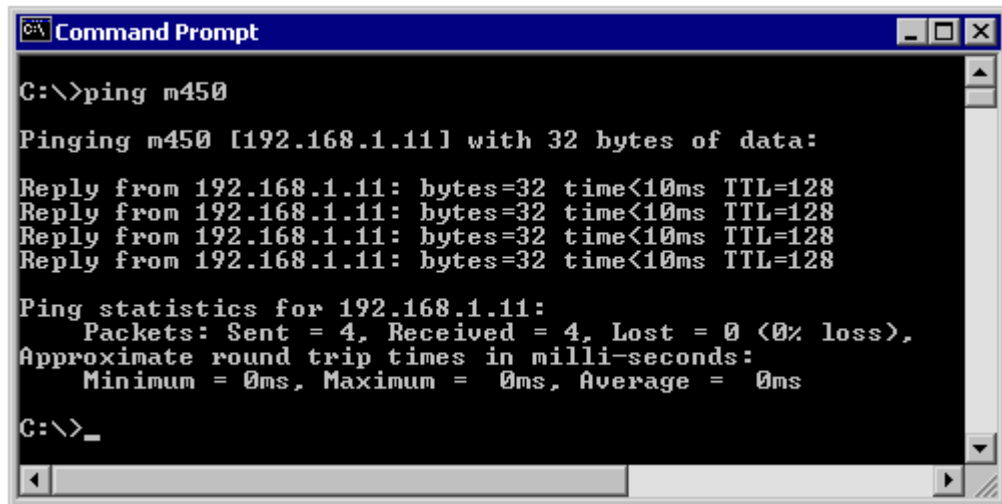
The 127.0.0.0 network is reserved for loopback testing. If the **ping** is successful, then TCP/IP is properly installed and functioning on this computer.

Was the **ping** successful? \_\_\_\_\_

If not, perform appropriate troubleshooting.

#### Step 7 ping the hostname of another computer

Try to **ping** the hostname of the computer that was recorded in the previous lab. The figure shows the successful result of the **ping** the hostname.



```
C:\>ping m450

Pinging m450 [192.168.1.11] with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time<10ms TTL=128
Reply from 192.168.1.11: bytes=32 time<10ms TTL=128
Reply from 192.168.1.11: bytes=32 time<10ms TTL=128
Reply from 192.168.1.11: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>_
```

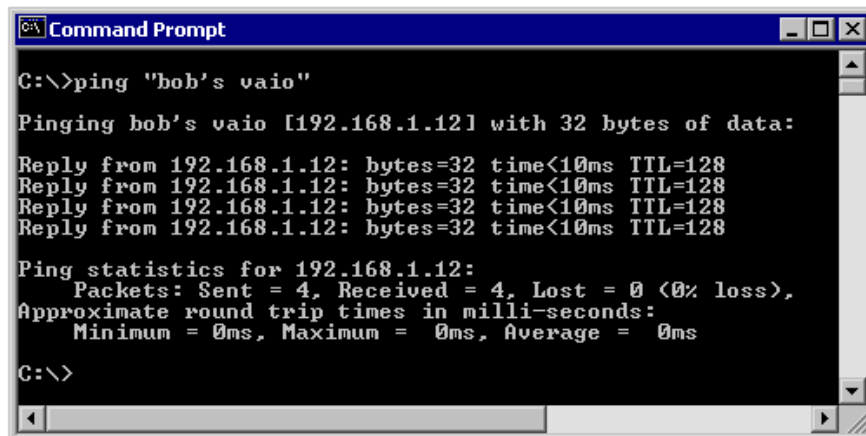
Look over the results. Notice that the first line of output shows the host name, m450 in the example, followed by the IP address. This means the computer was able to resolve the host name to an IP address. Without name resolution, the `ping` would have failed because TCP/IP only understands valid IP addresses, not names.

If the `ping` was successful, it means that connectivity and discovery of IP addresses can be done with only a hostname. In fact, this is how many early networks communicated. If successful, then `ping` a hostname also shows that there is probably a WINS server working on the network. WINS servers or a local "lmhosts" file resolve computer host names to IP addresses. If the `ping` fails, then chances are there is no NetBIOS name to IP addresses resolution running.

**Note:** It would not be uncommon for a Windows 2000 or XP networks to not support this feature. It is an old technology and often unnecessary.

If the last `ping` worked, try to `ping` the hostname of any another computer on the local network. The following figure shows the possible results.

**Note:** The name had to be typed in quotes because the command language did not like the space in the name.



```
C:\>ping "bob's vaio"

Pinging bob's vaio [192.168.1.12] with 32 bytes of data:

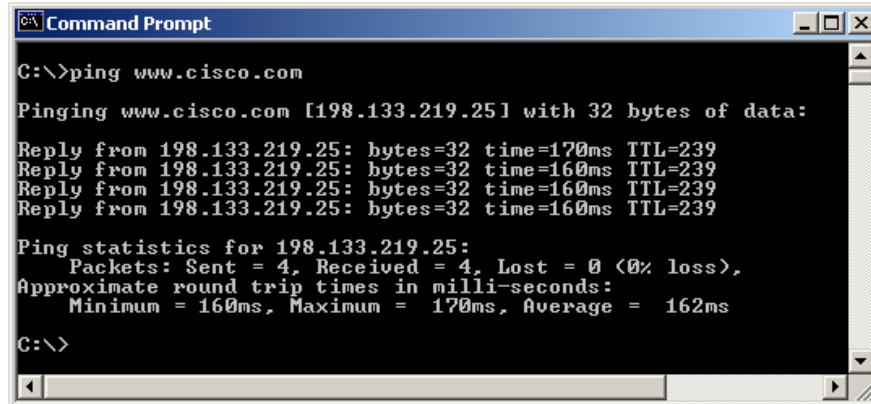
Reply from 192.168.1.12: bytes=32 time<10ms TTL=128
Reply from 192.168.1.12: bytes=32 time<10ms TTL=128
Reply from 192.168.1.12: bytes=32 time<10ms TTL=128
Reply from 192.168.1.12: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

## Step 8 ping the Cisco web site

Type the following command: `ping www.cisco.com`



```
C:\>ping www.cisco.com

Pinging www.cisco.com [198.133.219.25] with 32 bytes of data:

Reply from 198.133.219.25: bytes=32 time=170ms TTL=239
Reply from 198.133.219.25: bytes=32 time=160ms TTL=239
Reply from 198.133.219.25: bytes=32 time=160ms TTL=239
Reply from 198.133.219.25: bytes=32 time=160ms TTL=239

Ping statistics for 198.133.219.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 160ms, Maximum = 170ms, Average = 162ms

C:\>
```

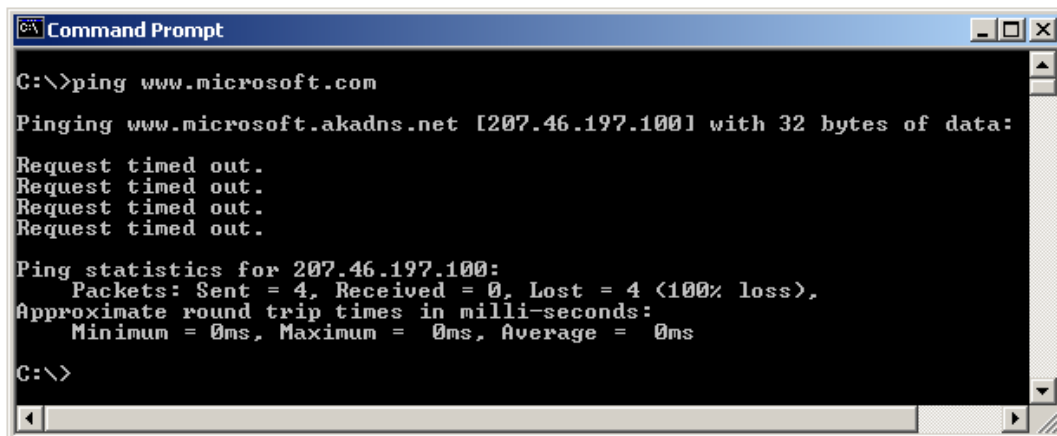
The first output line shows the Fully Qualified Domain Name (FQDN) followed by the IP address. A Domain Name Service (DNS) server somewhere in the network was able to resolve the name to an IP address. DNS servers resolve domain names, not hostnames, to IP addresses.

Without this name resolution, the `ping` would have failed because TCP/IP only understands valid IP addresses. It would not be possible to use the web browser without this name resolution.

With DNS, connectivity to computers on the Internet can be verified using a familiar web address, or domain name, without having to know the actual IP address. If the nearest DNS server does not know the IP address, the server asks a DNS server higher in the Internet structure.

## Step 9 ping the Microsoft web site

a. Type the following command: `ping www.microsoft.com`



```
C:\>ping www.microsoft.com

Pinging www.microsoft.akadns.net [207.46.197.100] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 207.46.197.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Notice that the DNS server was able to resolve the name to an IP address, but there is no response. Some Microsoft routers are configured to ignore `ping` requests. This is a frequently implemented security measure.

`ping` some other domain names and record the results. For example, `ping www.msn.de`

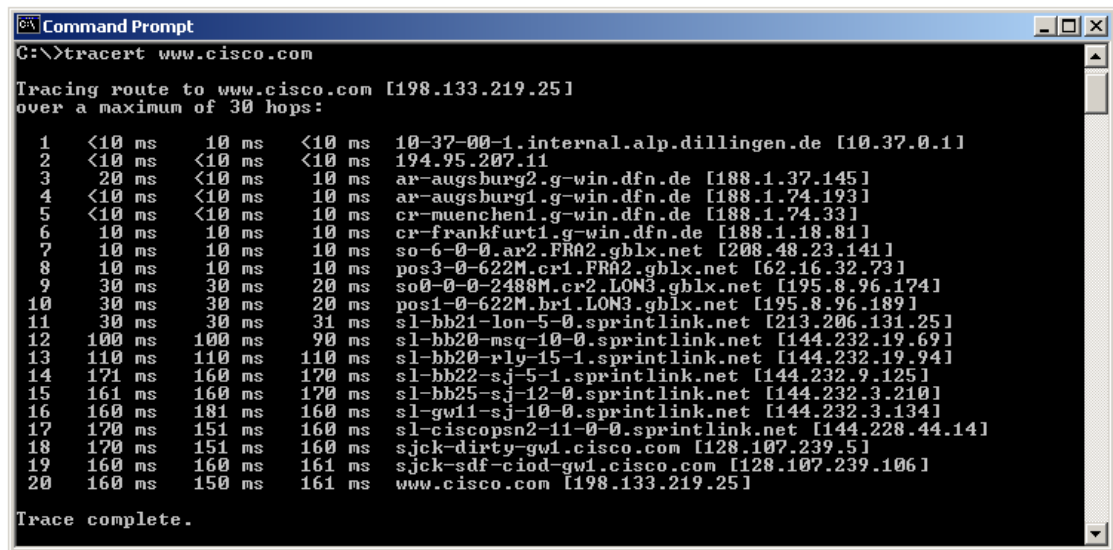
---

---

---

## Step 10 Trace the route to the Cisco web site

Type `tracert www.cisco.com` and press **Enter**.



```
Command Prompt
C:\>tracert www.cisco.com

Tracing route to www.cisco.com [198.133.219.25]
over a maximum of 30 hops:
  0  <10 ms    <10 ms    <10 ms    10-37-00-1.internal.alp.dillingen.de [10.37.0.1]
  1  <10 ms    <10 ms    <10 ms    194.95.207.11
  2  20 ms     <10 ms    <10 ms    ar-augsburg2.g-win.dfn.de [188.1.37.145]
  3  <10 ms    <10 ms    <10 ms    ar-augsburg1.g-win.dfn.de [188.1.74.193]
  4  <10 ms    <10 ms    <10 ms    cr-muenchen1.g-win.dfn.de [188.1.74.33]
  5  <10 ms    <10 ms    <10 ms    cr-frankfurt1.g-win.dfn.de [188.1.18.81]
  6  10 ms     10 ms     10 ms     so-6-0-0.ar2.FRA2.gblx.net [208.48.23.141]
  7  10 ms     10 ms     10 ms     pos3-0-622M.cr1.FRA2.gblx.net [62.16.32.73]
  8  30 ms     30 ms     20 ms     so0-0-0-2488M.cr2.LON3.gblx.net [195.8.96.174]
  9  30 ms     30 ms     20 ms     pos1-0-622M.br1.LON3.gblx.net [195.8.96.189]
 10  30 ms     30 ms     31 ms     sl-bb21-lon-5-0.sprintlink.net [213.206.131.25]
 11 100 ms    100 ms    90 ms     sl-bb20-msq-10-0.sprintlink.net [144.232.19.69]
 12 110 ms    110 ms    110 ms    sl-bb20-rly-15-1.sprintlink.net [144.232.19.94]
 13 171 ms    160 ms    170 ms    sl-bb22-sj-5-1.sprintlink.net [144.232.9.125]
 14 161 ms    160 ms    170 ms    sl-bb25-sj-12-0.sprintlink.net [144.232.3.210]
 15 160 ms    181 ms    160 ms    sl-gw11-sj-10-0.sprintlink.net [144.232.3.134]
 16 170 ms    151 ms    160 ms    sl-ciscopsn2-11-0-0.sprintlink.net [144.228.44.14]
 17 170 ms    160 ms    161 ms    sjck-dirty-gw1.cisco.com [128.107.239.5]
 18 160 ms    160 ms    161 ms    sjck-sdf-ciod-gw1.cisco.com [128.107.239.106]
 19 160 ms    150 ms    161 ms    www.cisco.com [198.133.219.25]
 20 160 ms    150 ms    161 ms

Trace complete.
```

`tracert` is TCP/IP abbreviation for trace route. The preceding figure shows the successful result when running `tracert` from Bavaria in Germany. The first output line shows the FQDN followed by the IP address. Therefore, a DNS server was able to resolve the name to an IP address. Then there are listings of all routers the `tracert` requests had to pass through to get to the destination.

`tracert` uses the same echo requests and replies as the `ping` command but in a slightly different way. Observe that `tracert` actually contacted each router three times. Compare the results to determine the consistency of the route. Notice in the above example that there were relatively long delays after router 11 and 13, possibly due to congestion. The main thing is that there seems to be relatively consistent connectivity.

Each router represents a point where one network connects to another network and the packet was forwarded through.

## Step 11 Trace other IP addresses or domain names

Try `tracert` on other domain names or IP addresses and record the results. An example is `tracert www.msn.de`.

---

---

---

---

## Step 12 Trace a local host name or IP address

Try using the `tracert` command with a local host name or IP address. It should not take long because the trace does not pass through any routers.

```
C:\>tracert lh-1700us

Tracing route to lh-1700us [10.37.0.186]
over a maximum of 30 hops:

  1  <10 ms  <10 ms  <10 ms  lh-1700us [10.37.0.186]

Trace complete.

C:\>
```

This concludes the lab.

### Reflection

If the above steps are successful and `ping` or `tracert` can verify connectivity with an Internet Web site, what does this indicate about the computer configuration and about routers between the computer and the web site? What, if anything, is the default gateway doing?

---

---

---

---