LAB 12 – Understanding Basic Networking Commands

OBJECTIVE(S)

- Learn about Basic Networking Commands

Basic Networking Commands

PING Command

The Ping (Packet Internet Grouper) command is one of the simplest and most effective tools you can use to resolve issues. It works in the same way as active sonar on a submarine, where a submarine will send out a loud sonar "ping" and then listening to the resulting sound bounce back off the target. This provides information on the direction of the target, while measuring the time taken for the sound to bounce back will provide some indication of the distance of the target.

The Ping command works in the same manner, providing direction information, and the time taken to respond to the Ping request.

How it works

First, Ping uses DNS to match a domain name to an IP address. Once it has the IP of the domain name it sends a request (called echo request) to that IP address using ICMP protocol and then starts an internal timer.

When the receiving IP address receives these echo requests it will send an echo reply to the originating computer. When the originating computer receives this reply it will see how long it took to receive the reply and display this in a report.

By default Windows operating systems will send 4 separate requests to the destination.

Uses

The ping command is most commonly used by network administrators to check that remote computers are able to respond to communications. It can also be used to check that the DNS for a domain name is set up correctly and the domain name resolves to the correct server.

Syntax

- ***Ping*** domainname_or_IP_address

Example

- ***Ping*** www.google.com

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

Pinging www.google.com [172.217.169.228] with 32 bytes of data:
Reply from 172.217.169.228: bytes=32 time=36ms TTL=52
Reply from 172.217.169.228: bytes=32 time=36ms TTL=52
Reply from 172.217.169.228: bytes=32 time=36ms TTL=52
Reply from 172.217.169.228: bytes=32 time=37ms TTL=52

Ping statistics for 172.217.169.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 37ms, Average = 36ms
```

NSLOOKUP Command

NSlookup (Name Server lookup) is a useful suite of tools for looking at specific DNS records. It allows you to question your domains nameservers, and find out much more information regarding your domains DNS.

How it works

The nslookup utility can be used to lookup the specific IP addresses associated with a domain name. If this utility is unable to resolve this information, there is a DNS issue. Along with simple lookup, the nslookup utility is able to query specific DNS servers to determine an issue with the default DNS servers configured on a host.

Uses

NSlookup is useful for checking that certain subdomains that you want to use exist. For example, mail.google.com. It is also really useful for analyzing multiple email records. Often people create multiple email records on their domain name, and then don't know where the email is sent to.

Syntax

- ***Nslookup*** domain_name

Example

- ***Nslookup*** www.google.com

```
C:\Users\Administrator>nslookup www.google.com
Server:  ldap1.dsu.edu.pk
Address:  10.50.0.5

Non-authoritative answer:
Name:    www.google.com
Addresses:  2a00:1450:4018:801::2004
          172.217.169.228
```

```
C:\Users\Administrator>nslookup
Default Server:  ldap1.dsu.edu.pk
Address:  10.50.0.5
```

TRACERT Command

The command stands for “Trace Route”. If you’re ever curious to see the path your internet traffic takes to get from your browser to a remote system like Google servers, you can use Tracert to see it. Once the ping utility has been used to determine basic connectivity, the tracert utility can be used to determine more specific information about the path to the destination host including the route the packet takes and the response time of these intermediate hosts.

How it works

It works the same as a ping request, but sends out packets with differing TTL (Time To Live) levels. Each time the TTL level is reached the router responsible for that “hop” will reply. Tracert then displays these bouncebacks as a way of showing a route through the internet.

It provides you with all of the following information:

- Number of hops (intermediate servers) before getting to the destination
- Time it takes to get to each hop
- The IP and sometimes the name of each hop

Uses

Tracert is a useful tool for checking for speed of connectivity, you can find out if your connection to a website is short, or is across many hops. As you can see the time at each hop, it will also give you an indication if there is a particular area of your route that is slower than the others.

It can reveal how the routes of your internet requests change depending where you’re accessing the web. It also helps with troubleshooting a router or switch on a local network that may be problematic.

Syntax

- ***Tracert*** domain_name

Example

- ***Tracert*** www.google.com

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

Tracing route to www.google.com [172.217.169.228]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.80.0.1
  2    <1 ms    <1 ms    <1 ms  10.50.0.20
  3     1 ms    <1 ms     1 ms  super11-line-001.super.net.pk [203.130.11.1]
  4     1 ms     2 ms     1 ms  10.50.53.49
  5     2 ms     1 ms     1 ms  10.241.241.30
  6     2 ms     2 ms     2 ms  khi77.pie.net.pk [202.125.134.41]
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9    36 ms    36 ms    36 ms  74.125.50.30
 10    37 ms    36 ms    36 ms  108.170.240.49
 11    38 ms    37 ms    37 ms  172.253.51.133
 12    36 ms    36 ms    36 ms  mct01s10-in-f4.1e100.net [172.217.169.228]

Trace complete.
```

NETSTAT Command

The command stands for “Network Statistics”. Often, one of the things that are required to be figured out is the current state of the active network connections on a host. This is very important information to find for a variety of reasons. For example, when verifying the status of a listening port on a host or to check and see what remote hosts are connected to a local host on a specific port. It is also possible to use the Netstat utility to determine which services on a host that is associated with specific active ports.

How it works

Netstat displays instant statistics regarding your network connections. It will tell you what connections you have open, what applications are using these connections, and the status of each connection.

Uses

This is useful for finding out which applications are active on the internet and to ensure that unauthorized software is not connecting to the internet without your knowledge.

Syntax

- ***Netstat***

Example

```
C:\Users\Administrator>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.80.215.220:49384    38.117.98.230:http     CLOSE_WAIT
  TCP    10.80.215.220:50274    wk-in-f188:https       ESTABLISHED
  TCP    10.80.215.220:50304    ec2-52-43-166-90:https  ESTABLISHED
  TCP    10.80.215.220:51095    ec2-108-128-130-224:https  ESTABLISHED
  TCP    10.80.215.220:51768    mct01s05-in-f78:https  ESTABLISHED
  TCP    10.80.215.220:51838    151.101.129.44:https   ESTABLISHED
  TCP    10.80.215.220:51890    mct01s06-in-f14:https  ESTABLISHED
  TCP    10.80.215.220:51891    KAVSRV08:13111         TIME_WAIT
  TCP    10.80.215.220:51892    KAVSRV08:13111         ESTABLISHED
```

IPCONFIG Command

The command stands for “IP Configuration”. One of the most important things that must be completed when troubleshooting a networking issue is to find out the specific IP configuration of the variously affected hosts. The utility that can be used to find out this IP configuration information is the ipconfig utility on Windows machines.

How it works

The ipconfig command gathers data relating to your network card and connections from your operating system and displays the results. This command returns detailed information about your current network adapter connection including:

- Current IP Address
- Subnet Mask
- Default Gateway IP
- Current domain

Uses

This information can help you troubleshoot router issues and other connection issues you could be having with your network adapter.

Syntax

➢ ***Ipconfig***

Example

```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : dsu.edu.pk
   Link-local IPv6 Address . . . . . : fe80::9d7d:92df:46d0:152b%10
   IPv4 Address. . . . . . . . . . . : 10.80.215.220
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.80.0.1

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::94cd:d52a:d1c8:bfe4%15
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.dsu.edu.pk:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : dsu.edu.pk

Tunnel adapter Teredo Tunneling Pseudo-Interface:

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

Tunnel adapter isatap.{D358C5FF-AF2B-4A29-8C0C-C0D6FCA0B430}:

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

SYSTEMINFO Command

If you need to know what brand of network card you have, details of the processor, or the exact version of your Windows OS, the SYSTEMINFO command can help.

This command pulls the most important information about your system. It lists the information in a clean format that's easy to read.

Syntax

- ***Systeminfo***

Example

```
C:\Users\Administrator>systeminfo

Host Name:                 FYP-01
OS Name:                   Microsoft Windows 7 Professional
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          CS001
Registered Organization:
Product ID:                00371-OEM-8992671-00008
Original Install Date:     11/27/2013, 8:08:11 PM
System Boot Time:          12/17/2019, 11:29:49 AM
System Manufacturer:       Hewlett-Packard
System Model:              HP EliteDesk 800 G1 USDT
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 60 Stepping 3 GenuineInt
el ~992 Mhz
BIOS Version:              Hewlett-Packard L01 v02.53, 10/20/2014
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:00) Islamabad, Karachi
Total Physical Memory:     8,098 MB
Available Physical Memory: 5,711 MB
Virtual Memory: Max Size:  16,195 MB
Virtual Memory: Available: 12,059 MB
Virtual Memory: In Use:    4,136 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\FYP-01
Hotfix(s):                 146 Hotfix(s) Installed.
                           [01]: KB974405
                           [02]: KB2764913
                           [03]: KB2764916
```

```
Network Card(s):           2 NIC(s) Installed.
                           [01]: Intel(R) Ethernet Connection I217-LM
                                 Connection Name: Local Area Connection
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.50.0.5
                                 IP address(es)
                                 [01]: 10.80.215.220
                                 [02]: fe80::9d7d:92df:46d0:152b
                           [02]: VirtualBox Host-Only Ethernet Adapter
                                 Connection Name: VirtualBox Host-Only Network
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.56.1
                                 [02]: fe80::94cd:d52a:d1c8:bfe4
```