Network Analysis Tool

Aisyatul Karima - 2012

Jarkom Lanjut - Week 3
Standar Kompetensi

- Pada akhir semester, mahasiswa mampu merancang, mengimplementasikan dan menganalisa sistem jaringan komputer

Kompetensi Dasar

- Mahasiswa mampu mempraktekkan perintah ping
- Mahasiswa mampu mempraktekkan perintah tracert
- Mahasiswa mampu mempraktekkan perintah route
- Mahasiswa mampu mempraktekkan perintah ipconfig
- Mahasiswa mampu mempraktekkan perintah arp
- Mahasiswa mampu mempraktekkan perintah netstat
Contents

1. Ping
2. Traceroute
3. Route
4. Ipconfig
5. Arp
6. Netstate
Background

- Two tools that are indispensable when testing TCP/IP network connectivity are ping and tracert.
- The ping utility is available on Windows, Linux, and Cisco IOS, and tests network connectivity.
- The tracert utility is available on Windows, and a similar utility, traceroute, is available on Linux and Cisco IOS.
- In addition to testing for connectivity, tracert can be used to check for network latency.
Background

- For example, when a web browser fails to connect to a web server, the problem can be anywhere between client and the server.
- A network engineer may use the ping command to test for local network connectivity or connections where there are few devices.
- In a complex network, the tracert command would be used. Where to begin connectivity tests has been the subject of much debate;
- it usually depends on the experience of the network engineer and familiarity with the network.
Background

- The ping and tracert commands will be examined, and command options will be used to modify the command behavior.
Ping

- The ping command is used to verify TCP/IP Network layer connectivity on the local host computer or another device in the network.
- The command also used to know the response time
- The command can be used with a destination IP address or qualified name, such as eagle-server.example.com, to test domain name services (DNS) functionality.
Ping

- The ping operation is straightforward.
- The source computer sends an ICMP echo request to the destination.
- The destination responds with an echo reply.
- If there is a break between the source and destination, a router may respond with an ICMP message that the host is unknown or the destination network is unknown.
Ping

View of command Ping:

C:\Users\karima>ping google.com

Pinging google.com [74.125.235.14] with 32 bytes of data:
Reply from 74.125.235.14: bytes=32 time=3814ms TTL=53
Reply from 74.125.235.14: bytes=32 time=769ms TTL=53
Reply from 74.125.235.14: bytes=32 time=647ms TTL=53
Reply from 74.125.235.14: bytes=32 time=1526ms TTL=53

Ping statistics for 74.125.235.14:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 647ms, Maximum = 3814ms, Average = 1689ms

C:\Users\karima>
Ping

- Use the ping command to verify TCP/IP Network layer connectivity on the local host computer/LAN.
- By default, four ping requests are sent to the destination and reply information is received.
- Destination address, set to the IP address for the local computer.

Reply information:

- bytes—size of the ICMP packet.
- time—elapsed time between transmission and reply.
- TTL—default TTL value of the DESTINATION device, minus the number of routers in the path.

- The maximum TTL value is 255, and for newer Windows machines the default value is 128.
Ping

- **Summary information about the replies:**
  - **Packets Sent**—number of packets transmitted. By default, four packets are sent.
  - **Packets Received**—number of packets received.
  - **Packets Lost**—difference between number of packets sent and received.
  - **Information about the delay in replies,** measured in milliseconds.
    - Lower round trip times indicate faster links.
    - A computer timer is set to 10 milliseconds.
    - Values faster than 10 milliseconds will display 0.
Ping

[-r count] [-s count] [-j host-list] [-k host-list]

Options:
- t Ping the specified host until stopped.
  To see statistics and continue - type Control-Break;
  To stop - type Control-C.
- a Resolve addresses to hostnames.
- n count Number of echo requests to send.
- l size Send buffer size.
- f Set Don’t Fragment flag in packet (IPv4-only).
- i TTL Time To Live.
- v TOS Type Of Service (IPv4-only). This setting has been depre
cated and has no effect on the type of service field in the IP
header.
- r count Record route for count hops (IPv4-only).
- s count Timestamp for count hops (IPv4-only).
- j host-list Loose source route along host-list (IPv4-only).
- k host-list Strict source route along host-list (IPv4-only).
- w timeout Timeout in milliseconds to wait for each reply.
- R Use routing header to test reverse route also (IPv6-only).
- S srcaddr Source address to use.
Traceroute

- The tracert command is useful for learning about network latency and path information.
- Instead of using the ping command to test connectivity of each device to the destination, one by one,
- On Linux and Cisco IOS devices, the equivalent command is traceroute.
Traceroute

- Verify TCP/IP Network layer connectivity with the tracert command.

```
C:\>tracert www.yahoo.com
Tracing route to www.yahoo.akadns.net [66.94.230.33]
over a maximum of 30 hops:
1  3 ms  <1 ms  <1 ms  192.168.1.254
2  6 ms   5 ms   6 ms  125.162.0.1
3  6 ms   5 ms   6 ms  125.160.0.1
4 353 ms 353 ms 356 ms 203.208.145.97
5 347 ms 350 ms 366 ms 203.208.182.237
6 491 ms 490 ms 500 ms 500.POS2-1.IG2.SAC1.ALTER.NET [157.130.210.217]
7  -  492 ms  487 ms  0.so-0-0-0.XR2.SAC1.ALTER.NET [152.63.54.118]
8 499 ms  494 ms  491 ms  0.so-3-0-0.XL2.SCL2.ALTER.NET [152.63.48.94]
9 488 ms  478 ms  474 ms  ge-3-0-0-p240.msr1.scd.yahoo.com [216.115.106.17]
10 475 ms  476 ms  475 ms  UNKNOHN-66-218-82-219.yahoo.com [66.218.82.219]
11 475 ms  480 ms  482 ms  p2.www.scd.yahoo.com [66.94.230.33]
Trace complete.
```
Traceroute

- Observe tracert output to a host that lost network connectivity.
- If there is a loss of connectivity to an end device, the tracert command can give valuable clues as to the source of the problem.
- The ping command would show the failure but not any other kind of information about the devices in the path.
Route

- Command route used to verify the routing of the network.
  - It is consist of the type of routing
  - To verify routing table of network

- Example:
  - Show ip route
Ipconfig

- Ipconfig used to verify IP address of computer
- This command support by Windows XP/2000 and running from DOS command prompt
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Bridge:

Connection-specific DNS Suffix . : 
IP Address. . . . . . . . . . . . : 192.168.1.101
Subnet Mask . . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . : 192.168.1.254
C:\>ipconfig /all

Windows IP Configuration

Host Name ...............: ss-cpe-maintenance
Primary Dns Suffix ......:
Node Type ...............: Unknown
IP Routing Enabled ......: Yes
WINS Proxy Enabled ......: Yes

Ethernet adapter Bridge:

Connection-specific DNS Suffix . :
Description .............: Realtek RTL8139 Family PCI Fast Ethernet NIC
Physical Address ........: 00-A0-B0-0D-13-27
DHCP Enabled ..........: Yes
Autoconfiguration Enabled.: Yes
IP Address .............: 192.168.1.101
Subnet Mask ............: 255.255.255.0
Default Gateway .........: 192.168.1.254
DHCP Server ..........: 192.168.1.254
DNS Servers ..........: 203.130.206.250
202.134.0.155
Lease Obtained ..........: Wednesday, December 14, 2005 3:13:32 AM
Lease Expires ..........: Thursday, December 15, 2005 3:13:32 AM
**ARP**
*(Address Resolution Protocol)*

- Displays and modifies address resolution, including ATM (Asynchronous Transfer Mode) interfaces.
- The `arp` command displays and modifies the Internet-to-adapter address translation tables used by the `Address` in *Networks and communication management.*
ARP
(Address Resolution Protocol)

- The **arp** command displays the current ARP entry for the host specified by the *HostName* variable. The host can be specified by name or number, using Internet dotted decimal notation.

- Example:
  - Show ip arp
ARP
(Address Resolution Protocol)
Netstat

- Netstat is a useful tool for checking network and Internet connections.
- Some useful applications for the average PC user are considered, including checking for malware connections.
- It provides a way to check if various aspects of TCP/IP are working and what connections are present.
  - In Windows XP SP2, a new switch "-B" was added that allows the actual executable file that has opened a connection to be displayed.
Netstat
Netstat

- The information that is displayed includes the protocol, the local address, the remote (foreign) address, and the connection state.
- Note that the various IP addresses include port information as well.
Thank You!