Lab 11.2.6 Troubleshooting TCP/IP Issues

Estimated Time: 20 minutes

Number of Team Members: Students will work in teams of two.

Objective

In this lab, standard TCP/IP commands are utilized to troubleshoot connectivity problems between the wireless client and the AP.

Scenario

Basic troubleshooting for TCP/IP on Windows machines combines facts gathered from the perspective of all of the following:

- The router
- The switch
- The bridge
- The AP
- The Windows client or server

Check to see if it is possible to connect using IP addresses. Use an IP address as a target for the standard TCP/IP commands such as **`ping`**, **`tracert`**, and **`telnet`**. Basic IP setup can be verified with the **`winipcfg`** utility for Windows 95 and 98 and the **`ipconfig`** utility for Windows NT, 2000, and XP.

Preparation

The student should read and understand the material presented in FWL Chapter 11 prior to the lab.

Tools and resources

The following tools and resources will help with this lab:

- AP configured on a wired network
- PC with wireless client adapter and utility properly installed
- A NeoTrace Express freeware program can be downloaded at the following URL:

  http://www.networkingfiles.com/PingFinger/Neotraceexpress.htm

Additional materials

Microsoft

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/proddocs/tcpip_utils.asp

Step 1 Ping

The ping command can be used to confirm basic network connectivity on IP networks. For IP, the ping command sends Internet Control Message Protocol (ICMP) Echo messages. ICMP is the Internet protocol that reports errors and provides information relevant to IP packet addressing. If a station receives an ICMP Echo message, it sends an ICMP Echo Reply message back to the source.

It is a good idea to use the ping command when the network is functioning properly to see how the command works under normal conditions and to have something to compare against when troubleshooting.

a. From the PC, ping the AP and examine the results.

```
C:\>ping 172.25.0.149

Pinging 172.25.0.149 with 32 bytes of data:

Reply from 172.25.0.149: bytes=32 time<10ms TTL=249
Reply from 172.25.0.149: bytes=32 time<10ms TTL=249
Reply from 172.25.0.149: bytes=32 time<10ms TTL=249
Reply from 172.25.0.149: bytes=32 time<10ms TTL=249

Ping statistics for 172.25.0.149:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
C:\>
```

Step 2 Tracert

The **tracert** tool on a Windows host reports each router a TCP/IP packet crosses on its way to a destination. It does essentially the same thing as the **trace** command in the Cisco IOS Software. The syntax for the **tracert** command is as follows:

- **tracert [-d [-h maximum_hops] [-j host-list] [-w timeout] target_name.**
- The following is an explanation of the parameters of the command:
- **d** – specifies to not resolve addresses to host names (use recommended in test networks to avoid DNS delays)
- **h maximum_hops** - specifies the maximum number of hops to search for target
- **j host-list** – specifies loose source route along the host list
- **w timeout** – waits the number of milliseconds specified by timeout for each reply
- **target_name** – name or IP address of the target host
- Errors that may occur include the asterisk (*) and the 'request timed out' message. These messages indicate a problem with the router or a problem elsewhere on the network. The error may relate to a forwarded packet or one that timed out.
- Another common error is a report of 'destination network unreachable'. This error usually indicates that network filtering is happening, likely from a firewall. It may also indicate a routing problem, such as a failed network link.

  a. From the PC, perform a `tracert` to http://www.cisco.com

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



```
Tracing route to www.cisco.com [198.133.219.25] over a maximum of 30 hops:
  1   <10 ms   <10 ms   <10 ms  sjc8-00-gw1.cisco.com [171.71.88.2]
  2   <10 ms   <10 ms   <10 ms  sjc2-dtb-gw1.cisco.com [171.71.240.105]
  3   <10 ms   <10 ms   <10 ms  sjc5-sbb4-gw1.cisco.com [171.71.241.153]
  4   <10 ms   <10 ms   <10 ms  sjc12-rbb-gw4.cisco.com [171.71.241.254]
  5   <10 ms   <10 ms   <10 ms  sjck-rbb-gw2.cisco.com [171.69.7.229]
  6   <10 ms   <10 ms   <10 ms  sj-wall-1.cisco.com [171.69.7.182]
  7   <10 ms   <10 ms   <10 ms  sjce-dirty-gw1.cisco.com [128.107.240.197]
  8   <10 ms   <10 ms   <10 ms  sjck-sdf-ciod-gw2.cisco.com [128.107.239.102]
  9   <10 ms   <10 ms   <10 ms  www.cisco.com [198.133.219.25]
Trace complete.
```

Step 3 Ipconfig

The command syntax for **ipconfig** and **winipcfg** is as follows:

- **ipconfig** [**/all** | **/renew** [*adapter*] | **/release** [*adapter*]]
- The following are the parameters of the command:
- **All-** Produces a full display. Without this switch, **ipconfig** displays only the IP address, subnet mask, and default gateway values for each network card.
- **/renew** [*adapter*]– Renews DHCP configuration parameters. This option is available only on systems running the DHCP Client service. To specify an adapter name, type the adapter name that appears when you use **ipconfig** without parameters.
- **/release** [*adapter*]- Releases the current dynamic host configuration protocol (DHCP) configuration. This option disables TCP/IP on the local system and is available only on DHCP clients.
- With no parameters, the **ipconfig** utility presents all of the current TCP/IP configuration values to the user, including IP address and subnet mask.
- To check the local host configuration, enter a DOS window on the host and enter the **ipconfig /all** command. This command shows your TCP/IP address configuration, including the address of the Domain Name System (DNS) server. If any of the IP addresses are incorrect or if no IP address is displayed, determine the correct IP address and edit it or enter it for the local host.

  a. Complete the information table below:

IPCONFIG COMMAND	INFORMATION
Host Name	
Primary DNS Suffix	
Node Type	
IP Routing Enabled	
WINS Proxy Enabled	
DNS Suffix Search List	
Connection-specific DNS Suffix	
Description	
Physical Address	
DHCP Enabled	
Autoconfiguration Enabled	
IP Address	
Subnet Mask	

Default Gateway	
DHCP Server	
DNS Servers	
Primary WINS Server	
Secondary WINS Server	
Lease Obtained	
Lease Expires	

Step 4 Telnet

a. Telnet from the host PC to the AP to test layer 7 connectivity:

```
C:\>telnet 10.0.P.1
User Access Verification
Username:
Password:
AP1200#
```

b. Was the Telnet successful?

_____

c. Which command will be used for testing in the following situations?

Situation	Command
Host cannot access other hosts through AP or bridge.	
Host cannot access certain networks by the way of AP or bridge.	
Users can access some hosts, but not others.	
Some services are available and others are not.	
Users cannot make any connections when one parallel path is down.	
Certain protocols are blocked and others are not.	

Step 5 Freeware Software utilities for telnet, trace and ping

There are freeware utilities available for download over the Internet that allow telnet, trace and ping in a Graphical User Interface (GUI) environment. One such program is NeoTrace Express. It can be downloaded at the following URL site:

http://www.networkingfiles.com/PingFinger/Neotraceexpress.htm

Other programs are:

A great free utility for the PocketPC is vxUtil. The utilities include:

- DNS Audit
- DNS Lookup
- Finger
- Get HTML
- Info
- IP Subnet Calculator
- Password Generator
- Ping
- Ping Sweep
- Port Scanner
- Quote
- Time Service
- Trace Route
- Whois

http://www.cam.com/vxutil.html

a. Perform an Internet search to find two other TCP/IP utlities? Record them below. Share with the class.

_____

