AltiGen KB

Using Netcat to Troubleshoot IP Connections

Using Netcat to Troubleshoot IP Connections
Date: June 12, 2009
Subject: Troubleshooting network connections with Netcat and Wireshark
Distribution: All Dealers
Doc Type: Tech Note
Release: N/A
Scope: 5.2 - 6.0
Application: Admin
Hardware: N/A
Keywords: Troubleshoot, Network, Utility, Netcat, TCP, IP, Port, Wireshark, Connectivity, Test
Obsolete: No

Introduction:
Netcat is a networking utility which reads and writes data across network connections using the TCP/IP protocol. Put simply, it is a utility that will generate IP traffic to a target IP address and port. Used in conjunction with a traffic analyzing tool like Wireshark you can view the traffic you generate to help isolate network issues. .

Download and Install Netcat:
Download Netcat here. Copy the .zip to your PC, and then extract the nc.exe file into C:\Windows\System32.

Command Syntax:
The syntax for using it is similar to using telnet for testing port connectivitiy. Open a command shell in windows:

nc [options] hostname port[s] [ports] …. nc = program name
options = use –u for UDP
hostname = IP address to connect to
ports = destination port to connect to

Example: nc –u 99.155.163.158 10060 would open a connection to the target IP on port 10060. After pressing enter the cursor will move to the next line and anything you type here will be sent as a UDP packet to that address and port.

Sample Troubleshooting:
The following is an example of how we might use Netcat with Wireshark to verify proper port forwarding configuration for the RTP ports that carry the talk path on a SIP call. .

On the server running Netcat:
To test port forwarding on UDP port 49152 (First VoIP RTP Port) use the command: nc –u 99.155.163.158 49152

After pressing enter the cursor will move to the next line. Type anything in that line and press the enter key to send the data to the AltiGen server. In the case of AW server 99.155.163.158, this port is opened and forwarded, so the received packet is seen with wireshark as we will confirm in the next steps.

On the server running Wireshark:

Our guide to configuring and running Wireshark can be found here: Using Wireshark to Capture Packets in AltiWare

1. Load Wireshark on the server.
2. Run Wireshark on the server
3. Select Capture.
4. Select Options.
5. In the Interface drop down, select the correct Network Adaptor.
6. In the Capture Filter field, enter the following to capture packets from 71.63.158.198 and udp port 49152.

Filter: Host 70.160.243.195 and udp port 49152

7. Press Start.

From the remote location (71.63.158.198) using NetCat:

1. Open a command prompt window
2. Type the following: nc –u 70.243.195.160 49152

3. Press Enter

4. On the blank line, ‘type this is a test.‘

5. Press Enter.

On the server running Wireshark:

The text from step 5 above should be visible in the bottom window of the Wireshark Capture in plain text.

https://know.altigen.com/questions/924/