Effect of Windows XP Firewall on Network Simulation and Testing

Akram Al-Rawi
College of CS & IT,
King Faisal University,
Al-Hassa, Saudi Arabia

aalrawi@kfu.edu.sa

Azzedine Lansari
College of IT,
Zayed University,
Abu Dhabi, UAE

azzedine.lansari@zu.ac.ae

Abstract

The objective of this paper is to report findings from simulating and testing local area network (LAN) connectivity using Windows XP operating system and Cisco Networking Academy network devices. In this study, a simple routing protocol, RIP, is used as routing protocol. Two different techniques, Cisco Networking Academy hardware lab and Cisco Packet Tracer 4, were used to compare their performance to simulate network connectivity. Primary findings showed that the settings of the Windows XP firewall on the host computer have a direct impact on the test results. These findings are critical as there are no similar reports in the literature and only a careful investigation allowed the researchers to come to this conclusion. Furthermore, study results also offer suggestions for fixing problems that hinder simulation results of LANs that use Windows XP workstations. These findings can help CCNA students and faculty understand the reasons for unexplained connectivity problems when performing CCNA labs. The study also provides a simple method to avoid connectivity problems when using Windows ping.exe and tracert.exe which implement the TCP/IP protocol ICMP

Keywords: Cisco Networking Academy, Windows XP Firewall, Network Simulation, ICMP.

Introduction

Cisco Networking Academy (CNA) is widely used in high schools, colleges, and universities all over the world. The Cisco Networking Academy Programs provide critical skills needed by students to work in the IT field. The program offers Web-based content, online assessment, hands-on labs, instructor training, and preparation for industry certifications such as CCNA and CCNP (http://www.cisco.com/web/learning/netacad/). The networking academy is used primarily to prepare students for Cisco certifications; it is also used for non Cisco certificates, such as CompTIA A+ and Sun Certified Java Programmer (SCJP). The Cisco Networking Academy courses include lab components which are an integral part of all CNA courses. For instance, the CCNA1-CCNA4 courses lab components include routers, switches, as well as some basic equipment and cables, to simulate and test network protocols in a lab environment using Cisco Internetwork Operating System (IOS). Cisco Networking Academy also promotes a product called Packet Tracer 4.0 (PT4) to simulate and

test LAN connectivity. It is used as an alternative to the hardware lab to assist students who have no access to CNA hardware lab.

Typical Cisco Networking Academy Program which offers CCNA1-CCNA4 consists of a rack-mounted routers and switches along with few other devices to simulate and test network connectivity. The lab deals with different routing protocols: some of them are Cisco proprietary routing protocols such as EIGRP, and some non Cisco proprietary protocols such as RIP and OSPF. The simulation problem under investigation in this paper involves two Cisco routers, one Cisco switch, and two PC's (hosts) running Windows XP along with a serial cable (DCE/DTE) to connect the two routers.

Following the completion of a particular Cisco Networking Academy lab simulation, it is typical to test the connectivity between the host computers using Windows ping.exe and tracert.exe which implement the TCP/IP protocol ICMP. A successful ping from all the hosts means that the network is functioning properly at the network layer level. If the ping is not successful it is necessary to start troubleshooting the network until the ping is successful. However, there are cases when the ping is not successful and yet it was not possible to find any problem with the network. On the other hand repeating the same simulation using Cisco Packet Tracer 4.0 simulation software the phenomena is not observed. The objective of this paper is to investigate the reasons behind the ping failure when a network is configured a certain way under the Windows XP, and provides a solution to resolve this connectivity issue in a lab environment. A brief introduction to Windows XP Firewall settings is given in the last section of this paper.

Connectivity Tests using Ping and Tracert

The ping command is a good tool for troubleshooting Layer 1 through 3 of the OSI (Open Systems Interconnection) model and diagnosing basic network connectivity (Odom, 2005). Using ping sends an ICMP (Internet Control Message Protocol) packet to the specified device (host, server, router or switch) and then waits for reply. The IP address or host name can be pinged. In order to ping the host name of a router, there must be a static host lockup table in the router or a DNS server for name resolution to IP addresses.

The traceroute command, abbreviated as trace, is an excellent utility for troubleshooting the path that a packet takes through an internetwork of routers. It can help to isolate problem links and routers along the way. The tracert command uses ICMP packets and the error message generated by routers when the packet exceeds its Time-To-Live (TTL). The Windows version of this command is tracert.

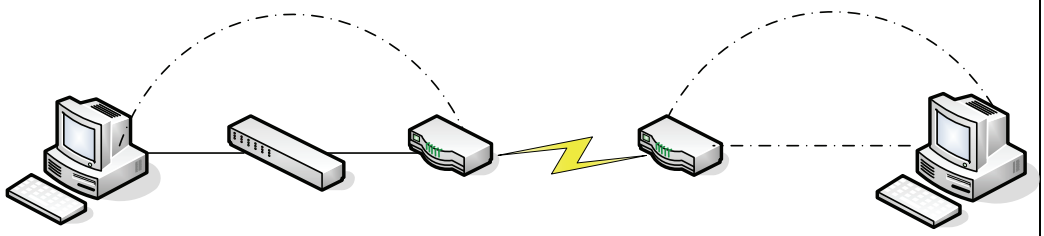
Cisco Networking Academy uses the ping command in the lab of the CCNA1-CCNA4 curriculum as a means to verify that the network layer between the source and destination is working properly. The ping can also be used to determine delays over the path and whether the host can be reached or is functioning. Cisco Networking Academy uses the tracert command to verify that the network layer between source, destination, and each router along the way is working properly.

The Simulated Network under Investigation

The network under simulation is shown in Figure 1. It consists of two host computers, one switch (Catalyst 2950) and two routers (Cisco 621XM). Table 1 shows the information needed for the configuration of the routers and the hosts. The two hosts which are connected to the routers simulate local area networks. The two hosts are also connected to the routers using a console cable to configure and test the network. After configuring the fast Ethernet 0/0 IP address for both routers, the serial 0/0 interface for both routers are configured and the hosts IP address, subnet mask and default gateway are configured. The configuration of the two routers requires the knowledge of the Cisco Internetwork Operating Systems (IOS). To test the connectivity of the network we used

the TCP/IP protocol command ping to test the connectivity between routers 1 and 2 (Macfarlane, 2006). Router 1 can ping router 2 successfully and router 2 can ping router 1 successfully. However, host 1 can not ping router 2 or host 2 without using static routes or enabling a routing protocol such as RIP. Routing protocols propagate network routing information among routers in order to build routing tables. Figure 2 shows the contents of the routing tables for router 1 and router 2 before the routing protocol is configured on the routers. The routing table, shown in Figure 2, shows directly connected links to routers 1 and 2.

Next, the configuration of the routing protocol, RIP, is entered into routers 1 and router 2. Figure 3 shows the routing tables in routers 1 and router 2 after enabling RIP. It is clear that the new routing tables contain routes to all the networks. The next section lists the tests which are done to test the network connectivity.



Host 1 Switch 1 Router 1 DCE/DTE Router 2 Host 2

Figure 1: Network under Simulation

Table 1: Routers and Hosts Basic Data

Router Designation	Router Name	Ethernet 0/0 IP address	Interface Type	Serial 0/0 IP address	Subnet mask	Host IP address
Router 1	GAD	172.16.0.1	DCE	172.17.0.1	255.255.0.0	172.16.0.2
Router 2	BHM	172.18.0.1	DTE	172.17.0.2	255.255.0.0	172.18.0.2

Network Connectivity Testing

Several tests are conducted to make sure connectivity is available between all network devices. While at the command prompt of host 1 a ping to the IP address of host 2 is issued. The ping was successful. A ping to the Ethernet address of router 2 was also successful. While at the command prompt of host 2, a ping was sent to the IP address of host 1 but it was not successful. However, a ping to the Ethernet address of router 1 was successful. A tracert command to the router 1 Ethernet address was successful; the tracert to host 1 IP address was not successful (Figure 2). All cables were tested. The routers and the switch were tested for possible access list configuration. No access list was found in the switch or the router. Host 1 was replaced with a different host and the host ip address, subnet mask, and default gateway was configured identical to the previous one (172.16.0.2, 255.255.0.0, 172.16.0.1). Then the previous test was repeated and it was found that the ping from host 2 to host 1 was successful (Figure 3). The old host was put back into the network to identify the difference between the settings of the two computers. From the simulation

```
GAD#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
Gateway of last resort is not set
C    172.17.0.0/16 is directly connected, Serial0/0
C    172.16.0.0/16 is directly connected, FastEthernet0/0
GAD#
BHM#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 Gateway of last resort is not set
C    172.17.0.0/16 is directly connected, Serial0/0
C    172.18.0.0/16 is directly connected, FastEthernet0/0
BHM#
GAD#ping 172.17.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/36 ms
GAD#ping 172.18.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.0.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
BHM#ping 172.17.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
BHM#ping 172.16.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
BHM#
```

Figure 2: Router Testing before RIP is Configured

perspective the only setting at all that was done to the computer was to configure the IP address, subnet mask, and default gateway for each host. So the issue must be with Windows firewall settings. We searched Cisco home page and the literature (Ciampa, 2006; Caudle & Cannon, 2004; Cisco Networking Academy Program, 2005, 2005; Easttom, 2006; Macfarlane, 2006) to find if such issues were reported but did not find any thing in the literature. After, examination of Windows firewall setting we found an option to enable echo reply, and for some reason in a number of personal computers the echo reply was not checked (by default).

While at Zayed University (a laptop university in the UAE), students and faculty were unable to use their laptops for the Cisco Networking Academy lab because of this problem. This problem was reported to the IT department which provides supports for the students and faculty laptops. However, the IT department was unable to identify the problem. The results of the network testing before changing the Windows Firewall setting are shown in figure 4. After changing the Windows Firewall setting of host 1, the ping and tracert from host 2 to host 1 were successful as shown in figure 5.

```
GAD#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
Gateway of last resort is not set
C    172.17.0.0/16 is directly connected, Serial0/0
C    172.16.0.0/16 is directly connected, FastEthernet0/0
R    172.18.0.0/16 [120/1] via 172.17.0.2, 00:00:12, Serial0/0
BHM#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
Gateway of last resort is not set
C    172.17.0.0/16 is directly connected, Serial0/0
R    172.16.0.0/16 [120/1] via 172.17.0.1, 00:00:27, Serial0/0
C    172.18.0.0/16 is directly connected, FastEthernet0/0
```

Figure 3: Route Tables after RIP is Configured

```
GAD#ping 172.18.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
GAD#ping 172.18.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/36 ms
GAD#
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\kfu>ping 172.18.0.2
Pinging 172.18.0.2 with 32 bytes of data:
Reply from 172.18.0.2: bytes=32 time=23ms TTL=126
Reply from 172.18.0.2: bytes=32 time=20ms TTL=126
Reply from 172.18.0.2: bytes=32 time=20ms TTL=126
Reply from 172.18.0.2: bytes=32 time=20ms TTL=126
Ping statistics for 172.18.0.2:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 23ms, Average = 20ms
BHM#trace 172.16.0.2
Type escape sequence to abort.
Tracing the route to 172.16.0.2
  1 GAD (172.17.0.1) 16 msec 16 msec 16 msec
  2  *  *  *
  3  *  *  *
  4  *  *  *
  5  *  *  *
BHM#ping 172.16.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
```

Figure 4: The effect of Windows Firewall Setting on Host 1

```
BHM#ping 172.16.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/36 ms
BHM#Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\kfu>ping 172.16.0.2
Pinging 172.16.0.2 with 32 bytes of data:

Reply from 172.16.0.2: bytes=32 time=20ms TTL=126
Reply from 172.16.0.2: bytes=32 time=20ms TTL=126
Reply from 172.16.0.2: bytes=32 time=20ms TTL=126
Reply from 172.16.0.2: bytes=32 time=20ms TTL=126
Ping statistics for 172.16.0.2:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 20ms, Average = 20ms
C:\Documents and Settings\kfu>
C:\Documents and Settings\kfu>tracert 172.16.0.2

Tracing route to 172.16.0.2 over a maximum of

  1    <1 ms    <1 ms    <1 ms  172.18.0.1
  2    24 ms    24 ms    24 ms  172.17.0.1
  3    29 ms    29 ms    29 ms  172.16.0.2
Trace complete.
```

Figure 5: Effects of Windows Firewall Setting on Network Connectivity

Network Simulation Using Packet Tracer 4.0

Cisco introduced Packet Tracer 4.0 (PT4) so that students and instructors can design, build, configure, and troubleshoot networks using virtual equipment. However, PT4 represents the host by an IP (Internet Protocol) address, subnet mask and default gateway. Therefore, the effect of Windows XP Firewall could not be simulated. Figure 6 shows the output of the same simulation performed using PT4. The ping from host 1 to host 2 and from host 2 to host 1 was successful following the RIP configuration on both routers. Although, the effect of the Windows XP Internet Firewall (ICF) can not be simulated, the simulation software was found to be very useful for CCNA students who have no access to Cisco Networking Academy hardware.

Windows XP Firewall

Windows firewall was first released as part of Microsoft Windows XP Service pack 2. It protects the computer by blocking communications that might be dangerous or software trying to find a way to connect to the computer and allowing communications from people or programs that are wanted. The windows XP firewall is designed to block all inbound packets, unless those packets are in a direct response from a query that was sent out from the machine. The firewall is designed to help keep hackers out of the system. However, the windows XP firewall is not a full featured

```
Packet Tracer PC Command Line 1.0
PC>ipconfig /all
Physical Address.....: 0060.70E5.1676
IP Address.....: 172.16.0.2
Subnet Mask.....: 255.255.0.0
Default Gateway.....: 172.16.0.1
PC>ping 172.18.0.2

Pinging 172.18.0.2 with 32 bytes of data:
Request timed out.
Reply from 172.18.0.2: bytes=32 time=135ms TTL=120
Reply from 172.18.0.2: bytes=32 time=139ms TTL=120
Reply from 172.18.0.2: bytes=32 time=143ms TTL=120

Ping statistics for 172.18.0.2:
   Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
   Minimum = 135ms, Maximum = 143ms, Average = 139ms

PC> Packet Tracer PC Command Line 1.0
PC>ipconfig /all
Physical Address.....: 0090.0C05.ECC1
IP Address.....: 172.18.0.2
Subnet Mask.....: 255.255.0.0
Default Gateway.....: 172.18.0.1

PC>ping 172.16.0.2
Pinging 172.16.0.2 with 32 bytes of data:
Reply from 172.16.0.2: bytes=32 time=141ms TTL=120
Reply from 172.16.0.2: bytes=32 time=136ms TTL=120
Reply from 172.16.0.2: bytes=32 time=138ms TTL=120
Reply from 172.16.0.2: bytes=32 time=142ms TTL=120

Ping statistics for 172.16.0.2:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 136ms, Maximum = 142ms, Average = 139ms
```

Figure 6: Packet Tracer 4 Connectivity Testing Result

firewall. Normally firewalls allow users to specifically control each TCP and UDP port. Windows XP's firewall does not provide a user with this capability. Instead, it takes a point and click approach to enabling or disabling a few common ports. Windows XP firewall advanced settings has a tab called ICMP which can be used to enable the echo reply. By default the echo reply is not selected. If the firewall is enabled in a host then the ping and tracert to the IP address of that host will fail. If the Windows XP firewall advanced settings is selected and the echo reply is enabled then ping to the IP address of that host will be successful. Figure 7 shows the Windows XP advanced setting options.

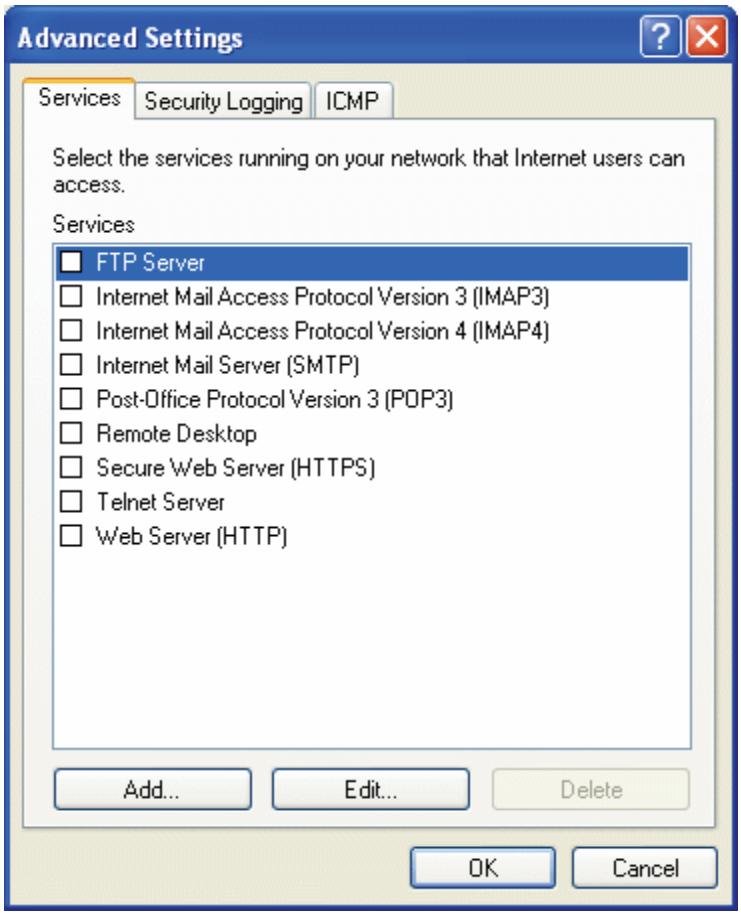


Figure 7: Windows XP Firewall Advanced Settings

Conclusions

Cisco Networking Academy is used in colleges and universities all over the world to provide students with skills needed to work in the IT fields. The Cisco Networking Academy Program lab is an integral part of all Cisco Networking Academy courses. The CCNA1-CCNA4 lab is mainly used to simulate and test network connectivity in a lab environment using Cisco routers and switches. At the completion of each lab, students are asked to test the connectivity between hosts using the ping.exe command which implements the TCP/IP protocol ICMP. In a number of cases there were unexplained connectivity problem between two hosts. After extensive testing the authors came to the conclusion that Windows XP Internet Connection Firewall (ICF) setting has an impact on the test results. By default, ICF does not responds to the ping command (allow incoming echo request box is unchecked). This will leads to the failure of the ping and tracert commands. Using Cisco Packet Tracer 4.0 did not show this phenomenon because the host is represented by an IP address, subnet mask, and default gateway only. To avoid such problem in network connectivity testing it is recommended to set the ICF so that it responds to the echo request. These findings can help CCNA students and faculty understand the reasons for sometimes unexplained connectivity problems when performing CCNA labs and provides quick ways to avoid these connectivity problems when using Windows ping.exe and tracert.exe which implements the TCP/IP protocol ICMP.

References

Caudle, K. & Cannon, K. (2004). *CCNA guide to Cisco networking* (3rd ed.). Course Technology.

Ciampa, M. (2006). *Security+ guide to network security fundamentals* (2nd ed.). Course Technology.

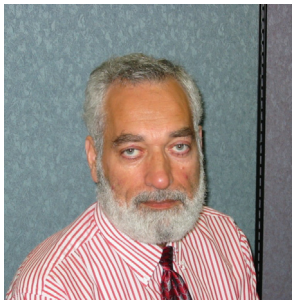
Cisco Networking Academy Program. (2005). *CCNA 1 and 2 companion guide, Revised* (3rd ed.). Cisco Press.

Easttom, C. (2006). *Computer security fundamentals.* Prentice Hall

MacFarlane, J. (2006). *Network routing basics: Understanding IP routing in Cisco systems.* Wiley Publishing, Inc

Odom, W. (2005). *CCNA ICND exam certification guide.* Cisco Press

Biographies



Akram Al-Rawi is a Professor of CS at King Faisal University, Saudi Arabia. He has worked at several academic institutions of which the last three were Zayed University, Columbia College, and University of Missouri-Columbia, MO. His teaching interests include programming languages, Networks, logic design, and computer architecture. His research interests include computer simulation, wireless, security, embedded systems, and curriculum design. He holds certifications in A+, Network+, Sun Certified Java Programmer, ICDL, i-Net+, Server+ and CCAI.

Azzedine Lansari received a PhD in Bioengineering from North Carolina State University in 1992. From 1992-1998, he was a senior researcher at Computer Sciences Corp. and MANTECH, Inc. He joined Zayed University in August 1998. Currently he is an assistant professor of Information Technology. His teaching interests include instructional technology and statistical modeling. His research interests include systems modeling, educational technology and curriculum design in Information Systems.