Teaching Tip

Using Selected Options of the Ipconfig Command to Teach Network Troubleshooting Techniques

Thomas P. Cavaiani
Department of Networking, Operations, and Information Systems
Boise State University
Boise, Idaho 83725, USA
tcavaiani@boisestate.edu

ABSTRACT

Students often have difficulty troubleshooting common problems that involve network operating system services. Improperly configured network settings can cause unexpected results that add confusion to the troubleshooting process. Commonly used command-line tools may provide students with the information they need to eliminate confusion and provide them with insights for fixing some problems. This teaching tip investigates selected options of the Microsoft Windows ipconfig command and how these options can be used to troubleshoot Active Directory access problems resulting from outdated entries in a local DNS cache.

Keywords: Effective Instruction, Networking, Troubleshooting, Microsoft Windows

1. INTRODUCTION

Becoming proficient at troubleshooting network communications issues is, to say the least, an extremely involved and difficult task. Intensive study of complex technical materials is required just to become superficially familiar with operating systems and networks. Effective instructional techniques typically include hands-on laboratory exercises that provide students with an opportunity to develop a deeper understanding of the processes involved in network communications. To provide such an experience for my students, I have developed a series of lab activities that provide the opportunity to investigate network connectivity as it relates to the TCP/IP protocol stack. Command-line utilities and protocol analyzers are used to provide information regarding the messages sent between client and server during network communications. To illustrate the approach used in these labs, this teaching tip covers an Active Directory lab that my students perform. It demonstrates how selected options of the command-line utility, *ipconfig*, can provide information to help students analyze network connectivity issues.

2. BACKGROUND

The *ipconfig* command displays the Internet Protocol (IP) configuration for computers using Microsoft Windows operating systems. IP address, subnet mask, Domain Name System (DNS) addresses, physical addresses, and default gateway addresses are some of the items that are displayed when this command is issued. Ipconfig also supports a number of options for modifying existing configurations. For example, the */release* and */renew* options are commonly used by administrators to reset IP address information for a given network adapter. The ipconfig command also supports additional options that can be used to reset other existing configurations. One such option is *flushdns* which can be used to purge entries from the local DNS cache. Operating systems store results of queries to DNS servers in a local cache so that clients do not need to repeatedly query the DNS server for the same address. These DNS cache entries are known as DNS resource records, and the DNS resolver always checks the local cache before it queries the DNS server (DNS Caching, Network Prioritization, and Security, 2005).

The default time-to-live (TTL) for most entries in the local DNS resolver cache is 86,400 seconds or 24 hours. Thus a location or service may become inaccessible if an IP address for the service or location changes before the 24 hour period has expired (DNS Caching, Network Prioritization, and Security, 2005). Knowing how to rectify this problem is an essential skill for a network administrator. A description of a lab activity designed to guide students through the process of restoring accessibility of certain network services using the *displaydns* and *flushdns* options of ipconfig follows.

3. THE LAB ACTIVITY

3.1 Configuring Active Directory Services

The lab activity is designed to provide domain client computers access to *Active Directory* (AD) services located on a server designated as a domain controller. The lab involves the following three activities: (1) implementation of a domain model, (2) providing access to DNS services, and (3) installation of software on the clients that provides access to AD services.

To implement a domain model, a standalone server is first promoted (converted) to a domain controller using the *dcpromo* command. This is accomplished by clicking the *Start* button on the Windows Taskbar, choosing the *Run...* option, typing *dcpromo* in the *Open* text box, and clicking the *OK* button. A wizard then guides the user through the promotion process, during which the address of an existing DNS server is either specified or DNS software is installed on the server. In this lab, DNS is installed on the domain controller, since no other DNS server is available on the lab network. Upon completion of the promotion process, students modify IP addresses, subnet masks, default gateway, and DNS settings on client computers by manually configured the *Internet Protocol (TCP/IP)* settings in the *Local Area Connection Properties* dialog box. Students then join client computers to the domain, by changing the *Member of* option in the *Identification Changes* dialog box under *Network Identification* option in the *System Properties* dialog box. After restarting their computers students log into the new domain using the domain administrator account, download *adminpak.msi* from a shared directory on the domain controller, and install it on their client computers so that they can access Active Directory services on the server from their client machines. Finally, students click on the *Start* button then point to *Programs-Administrative Tools-Active Directory Users and Computers* to view the Active Directory Users and Computers dialog box that allows them to browse and modify account information (see Figure 1).
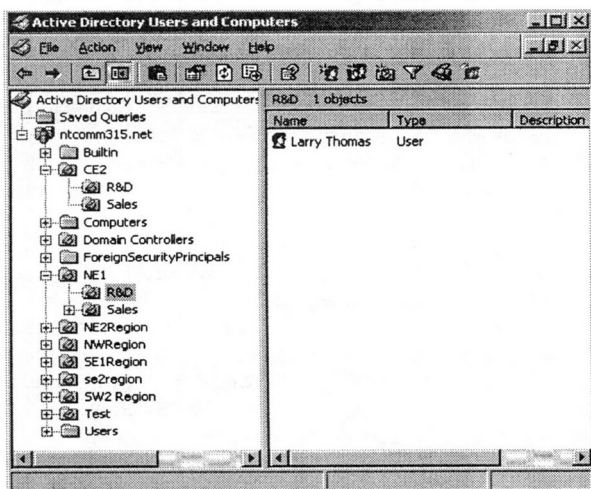

Figure 1. The Active Directory Users and Computers Dialog Box

3.2 Initiating the Troubleshooting Activity

Next a troubleshooting exercise is initiated. Students delete the *Preferred DNS Server* address in the *Internet Protocols (TCP/IP)* dialog box on their client machines (See figure 2) to determine what types of error messages they might encounter when attempting to access AD from client computers.
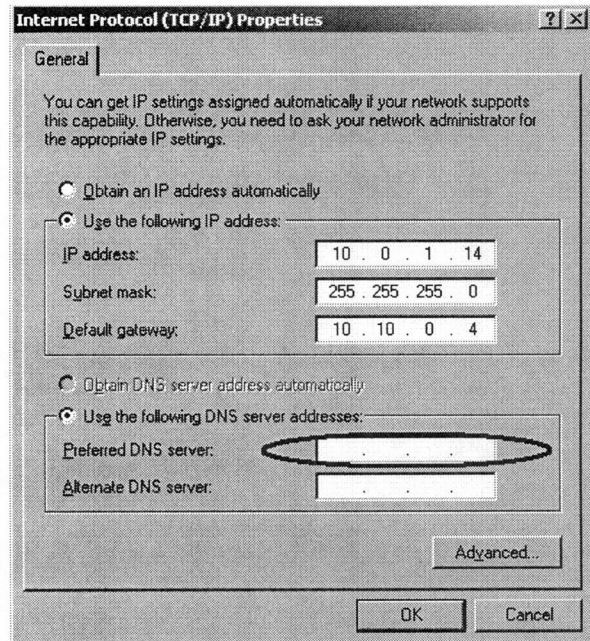

Figure 2. The Preferred DNS Server Address is Deleted by Clearing the Circled Text Box

After saving changes, but not restarting their computers (Note: restarting the computers would clear the DNS cache; the exercise is designed to allow students to learn how to clear the cache manually), students again attempt to access AD from the client computers, under the assumption that the clients will not be able to connect to the service. Surprisingly, they are successful and somewhat puzzled. Questions in the lab handout ask students to speculate why clients can still access AD. They are asked to consider whether an alternate naming system is being used or if DNS addresses have been stored in a cache. If they select caching, they are then asked if they know which cache is being used or where the cache resides.

3.3 Using a Command-line Utility to Troubleshoot the Problem

At this point it is suggested that common command-line utilities used in previous lab activities be investigated. One of the first utilities that students encountered in this course was the *ipconfig* command. Figure 3 shows the help screen that is displayed when students type *ipconfig/?* at a command prompt.

As students review the options shown in the usage screen they discover the */displaydns* and */flushdns* options and the effect these commands have on the DNS Resolver cache
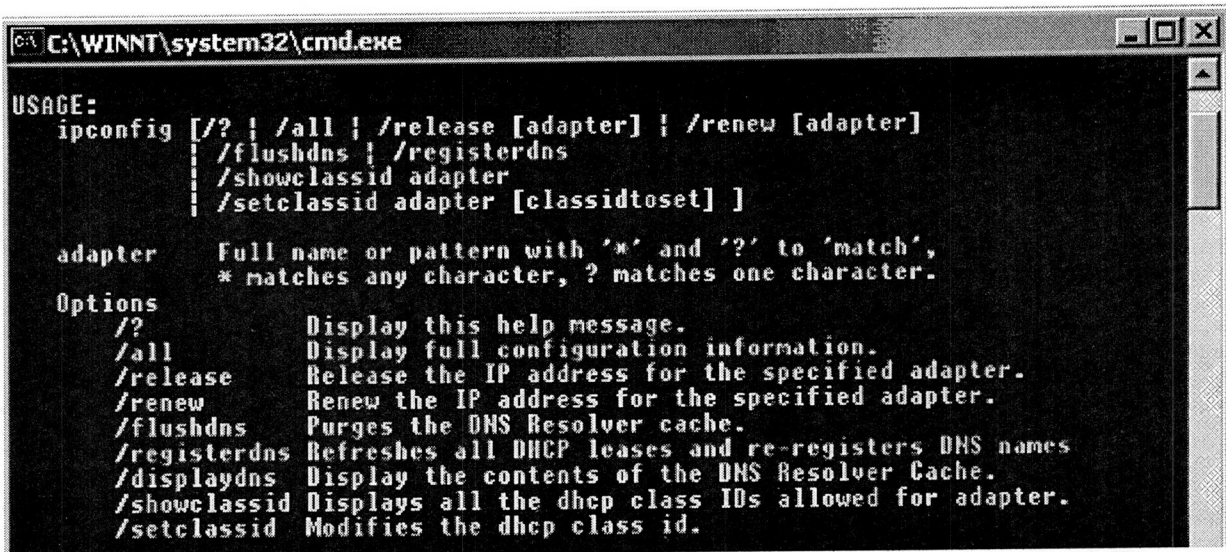
Figure 3. Command-Line Display of ipconfig Options

(Note: the /displaydns option is only available on computers running Windows 2000, Windows XP, or Windows Server 2003 operating systems).

3.4 Identifying the Problem using ipconfig Options

The output of the *ipconfig/displaydns* command now provides students with some valuable information, i.e., the contents of the DNS client resolver cache. Local Hosts file entries, as well as recently obtained resource records for queries resolved by the system are loaded into this cache (Display and View a Client Resolver Cache Using the ipconfig Command, 2005). The output of this command is a long list of resource record information. An abbreviated version of this list is shown below:

Record Name	1.0.0.127.in-addr.arpa.
PTR Record	localhost
Record Name	ntcomm315.net
A (Host) Record	10.0.1.75
Record Name	_ldap._tcp.Default-First-Site-Name._sites.ntcomm315.net
SRV Record	server1.ntcomm315.net
Record Name	server1.ntcomm315.net
A (Host) Record	10.0.1.75
Record Name	_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.ntcomm315.net
SRV Record	server1.ntcomm315.net
Record Name	server1.ntcomm315.net
A (Host) Record	10.0.1.75
Record Name	localhost
A (Host) Record	127.0.0.1

The presence of SRV records indicates that the local machine continues to point at the DNS server even though client computers no longer contain the correct IP address for that server in their TCP/IP configuration.

3.5 Resetting the Cache

Students are now instructed to issue an ipconfig/flushdns command (Troubleshooting Common Active Directory Setup Issues in Windows 2000, 2005), followed by another ipconfig /displaydns command. The following results are displayed in the command window:

1.0.0.127.in-addr.arpa

Record Name	1.0.0.127.in-addr.arpa.
Record Type	12
Time to Live	604208
Data Length	4
Section	Answer
PTR Record	localhost

localhost

Record Name	localhost
Record Type	1
Time to Live	604208
Data Length	4
Section	Answer
A (Host) Record	127.0.0.1

The absence of SRV records indicate that the cache has been cleared of all references to the DNS server. To verify that they have rectified the accessibility issue, students again attempt to access Active Directory from client computers. The following error message is displayed:
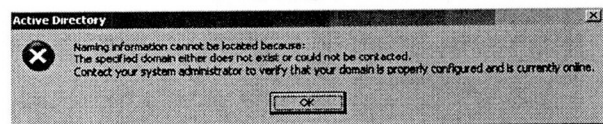

Figure 4. Active Directory Error Message Displayed After DNS Cache Has Been Reset

253

4. CONCLUSION

The lab activity described in this teaching tip illustrates the interaction of different operating system processes and how an improperly configured system can affect accessibility to certain services. It also illustrates how common command-line tools can be used to provide an administrator with useful information for troubleshooting these connectivity problems. These utilities are easy to use, are an inherent part of the operating system, and are well documented, thus making them readily accessible and understandable. In most cases they do not overwhelm the user with an excessive amount of information, and can be easily filtered and reissued to provide a more focused view of the state of the system. Knowledge of these utilities and how they are used for troubleshooting network problems is essential to those planning a career in information technology.

5. REFERENCES

Display and View a Client Resolver Cache Using the ipconfig Command (2005), Retrieved May 7, 2005 from http://www.microsoft.com/technet/prodtechnol/window sserver2003/library/ServerHelp/7356d145-e8ee-4dae-9edb-8b08a37e5384.mspx

DNS Caching, Network Prioritization, and Security (2005), Retrieved May 16, 2005 from http://www.microsoft.com/resources/documentation/Wi ndows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/Windows/ XP/all/reskit/en-us/prjj_ipa_vitx.asp

How Domain Controllers Are Located in Windows (2003), Retrieved May 3, 2005 from http://support.microsoft.com/default.aspx?scid=kb;en-us;247811

Troubleshooting Common Active Directory Setup Issues in Windows 2000 (2005), Retrieved April 23, 2005 from http://support.microsoft.com/?kbid=260371

AUTHOR BIOGRAPHY

Dr. Thomas P. Cavaiani is a Special Lecturer in the Department of Networking, Operations, and Information Systems at Boise State University. He received his Ph.D. in Mathematics Education from Oregon State University in 1988. He has published in the *American Technical Education Association Journal*, the *Journal of Information Systems Education,* and the *Journal of Research on Computing in Education.* He has also published two books on computer support, and has written and edited numerous computer application training manuals. His teaching interests include Java programming, operating systems and networking and telecommunications.