Jacek WOŁOSZYN
Technical University of Radom, Poland

TCP/IP Administration tools

1. TCP/IP Address Resolution Protocol Utility

All devices on an internetnetwork are considered to be virtually connected at layer 3, since the process of routing lets any device communicate with any other device. However, there is no way for device son distant networks to communicate directly. The internetwork communication at layer 3 actually consists of a number of steps, called hops, that carry the data from its source to destination. Each hop in a route requires that data be sent between a pair of hardware devices, and each transmission must use layer 2 hardware addresses. Since TCP/IP [Komar 2000] uses layer 3 addresses, this means each hop requires that we translate the IP address of the target of the hop to a hardware address. This is called address resolution; the reasons why it is needed and the methods used for it are explained in detail.

In TCP/IP, address resolution functions are performed by the aptly named Address Resolution Protocol. When a device needs to transmit to a device with a particular IP address, it can use ARP's request reply messaging protocol to find out which hardware device corresponds to that IP address. However, each such message exchange takes time and network bandwith, so for efficiency, every device maintains an ARP [Komar 2000] cache, which is a table containing mappings between IP and hardware addresses. The ARP cache table can contain a combination of static cache entries that are manually inserted for frequently accessed devices, and dynamic entries, which are entered automatically when a request/reply resolution is done. The next time it is necessary to send a device mapped in the ARP cache table, the lookup process can be avoided.

To allow administrators to manage this ARP cache table, TCP/IP devices include an arp utility. It has following three basic functions, which are invoked using three different versions of the command /wchich, for once, are the same in UNIX/LINUX and Windows/.

ARP Cache Table Display – when the –a options is used with the utility, it displays the current contents of the ARP cache table. The syntax is arp –d <hostname>. Each entry in the tables shows the IP address and hardware address pair for one device /interface, actually/. Usually, it also indicates whether each entry is static or dynamic. The exact format of the display varies from one implementation to the next, some programs show IP addresses, others show host names, and still others may show both. Some systems default to displaying host

names but allow the –n option to also be used to force only IP addresses /not names/ to be displayed.

ARP Cache Table Entry Addition – This version allows an administrator to make a new manual ARP cache table entry that maps the given host name to the specified hardware address. The syntax is arp –s <hostname> <hw-addr>.

ARP Cache Table Entry Delection – using arp with the –e options removes the specified cache entry from the table. Some implementations allow the addition of another parameter to specify that all entries should be removed from the cache. The basic syntax is arp –d <hostname>.

Certain versions of the software may also supplement these basic commands with additional features. One common additional option on UNIX systems is the ability to specify a file from which cache table entries may be read, using the syntax arp –f <filename>. This saves a considerable amount of time and effort compared to typing each entry manually using arp –s. Note also that the operating system may allow only authorized users to access options that cause the ARP cache table to be changed. This is especially true of delete function.

2. TCP/IP DNS Name Resolution and Lookup

DNS [Karanjit, Parker 2002] is a critically important part of TCP/IP internetworks, especially the modern Internet, because it allows hosts to be accessed using easily remembered names rather than confusing numerical addresses. Two different primary types of devices are involved in the operation of DNS. DNS name servers that store information about domains and DNS resolvers that query DNS servers to transform names into addresses, as well as perform other necessary functions.

DNS resolvers are employed by Internet users on a continual basis to translate DNS names into address, but under normal circumstances, they are always invoked indirectly. Each time a user types a DNS name into a program such as web browser of FILE Transfer Protocol /FTP/. There is no need for users to manually resolve DNS names into addresses. However, administrators often do need to perform a DNS resolution manually. For example, when troubleshooting a problem, the administrator may know a host's name but not its address. In the case of a security problem, the address may show up in a log file but the host name not be known. In addition, even though users do not need to know the specifics of the resource records that define a DNS domain, administrators often need to be able to check these details, to make sure a domain properly. Administrators also need some way to be able to diagnose problems with DNS servers themselves. To support all of these needs, modern TCP/IP implementations come equipped with one or more DNS name resolution and information lookup utilities. Here, we will look at three such utilities nslookup,host, dig.

The nslookup utility.

One of the most common DNS diagnostic is nslookup, which has been around for many years. The details of how the program is implemented depend on the operating system, though most of them offer versions that are quite similar in operation and settings. The utility can normally be used in two models interactive or noninteractive.

The noninteractive version of nslookup is the simplest, and it is most often used when an administrator wants to just quickly translate a name into an address or vice versa. To run this version, issue the nslookup command using the following simple syntax:

nslookup „host" [„servers"]

Here, „host" can be a DNS domain name, for performing a normal resolution, or it may be an IP address, for a reverse resolution to return the associated DNS domain name. The „server" parameter is optional if it's omitted, the program users the default name server of the host where the command was issued.

Listing 1 shows a simple example of noninteractive use of nslookup

```
Microsoft Windows [Wersja 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Wszelkie prawa zastrzeżone.
C:\Users\jacek>nslookup onet.pl
Serwer:  e.home
Address:  192.168.1.1
Nieautorytatywna odpowiedź:
Nazwa:  onet.pl
Address:  213.180.146.27
C:\Users\jacek>
```

The interactive mode of nslookup is selected by issuing the name of the command with no parameters. This will cause the program to display the current default name server's DNS name and addresses, and then provide a prompt at which the administrator may enter commands. Interactive mode allows someone to perform multiple lookups easily without having to type nslookup each time. More important, its provides more convenient control over the type of information that can be request and requested and how the lookups are performed. You can usually determine the exact command set available in an nslookup implementation by issuing the command help or ? at the nslookup prompt. Table 1 shows some of the commands that are usually found in most nslookup implementations.

Table 1

Typical nslookup Utility Commands

Commmand and Parameters	Description
<host> [<server>]	Look up specified host, optionally using the specified DNS name server. Note that there is no actual command here, you just enter name directly at the command prompt.
Server <server>	Change the default server to <server>, using information obtained from the current default server.
Lserver <server>	Change the default server to <server>, using information obtained from the initial name server, that is, the system's default server that was in place when the nslookup command was started /prior to any preceding changes of the current name server in this session/
root	Changes the default name server to one of the DNS root name servers
Ls [-t <type>] <name>	Request a list of information available for the specified domain name, be conducting a zone transwer. By default, the host names and addresses associated with the domain are listed, the –t option may be used to restrict the output to a particular record type. Other options may also be definied. /Most servers restrict the use of zone transfers to designated slave servers, so this command may not work for ordinary clients/
help	Display help information
?	Some a help /work on only some systems/
Set all	Display the current value of all nslookup options
Set <option> [=<value>]	
exit	Quits the program

The nslookup utility is widely deployed on both UNIX and Windows systems, but the program is not without its critics. The complaints about it mainly center around its use of nonstandard methods of obtaining information, rather than standard resolution routines. I have also read reports that it can produce spurious results in some cases. One example of a significant problem with the command is that it will abort if it is unable to perform a reverse lookup of of its own IP address. This can cause confusion, because users mistake that error for an error trying to find the name they were looking up. For this and other reasons, a number of people in UNIX circles consider nslookup to be a hack of sorts. In

some newer UNIX systems, nslookup has been deprecated /still included in the operating system for compatibility, but not recommended and may be removed in the future/

3. The host utility

The host utility is most often used for simple queries such as those normally performed using nslookup noninteractive mode. It is invoked in the same way as noninteractive nslookup

Listing 2 Command host
host <host> [<server>]
%host www.onet.pl
www.onet.pl is an alias for onet.pl
onet.pl has address 213.180.146.27

Even though host does not operate interactively, in includes a number of options that can allow an administrator to get the same information that would have been obtained using nslookup's interactive mode. Some of the more common options are shown in table 2.

Table 2

Typical host Utility Options and Parameters

Option/Parameters	Description
-d	Turn on debug mode
-l	Provides a complete list of information for a domain, this is similar to the 1s command in interactive nslookup. This may be used with the –t option to select only a particular type of resource record for the domain
-r	Disables recursion in the request. When this is specified, only the server directly queried will return any information, it will not query other servers
-t <query-type>	Specifies a query for a particular resource record type, allowing any type of DNS information to be retrieved.
-v	Uses verbose mode for output /additional details are provided/
-w	Waits as long as necessary for response /no timeout/

4. The dig utility

The second alternative to nslookup is dig, which stands for Domain Information Groper /likely a play on the supposed origin of the name ping/. It differs from the host command in that it provides considerably more information about

a domain, even invoked in the simplest of ways. It is also quite a bit more complicated, with a large number of options and features, such as a batch mode for obtaining information about many domains.

The basic syntax for the dig command is different from that of nslookup and host. If you specify a nondefault name server, it is prepended with an at sign /@/ and comes before the host to be looked up. You can also specify a specific type of resource record, like this

Dig [@<server>] <host> [<type>]

Listing 3 shows the output from running dig.

```
%dig www.onet.pl
; <<>> DiG 9.2.1 <<>> www.onet.pl
; ;global options :   printcmd
;; Got answer:
;;  ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15912
;; flags: qr rd ra; QUERY: 1,  ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 0
;; QUESTION SECTION:
; www.onet.pl.              IN      A
;; ANSWER SECTION:
www.onet.pl.        3600 IN      CNAME onet.pl.
onet.pl             3600  IN      A   213.180.146.27
;; AUTHORITY SECTION:
Onet.pl.            3600  IN      NS  ttr.tp.pl.
Onet.pl             3600  IN      NS ttr44.tp1.pl.
;;Query time: 1285 msec
;;SERVER: 213.45.77.88#53(213.45.77.88)
;;WHEN: Wed May 16 16:06:08 2011
;;MSG SIZE rcvd: 109Server: ns1-tp.pl
```

The dig command includes dozens of options and settings

5. TCP/IP DNS Registry database Lookup Utility

Utilities such as nslookup [Haugdahl 2001] and host allow administrators to resolve a DNS domain name to address and also view detailed information about a domain's resource records. There are cases, however, where administrators need to know its DNS registration information, rather technical information about a domain. This includes detail such as which organization owns the the domain, when registration expires, and who are designated contacts who manage it.

In the early days of DNS, all domain names were centrally registered by a single authority, called the Internet Network Information Center. /InterNIC or NIC/. To allow Internet users to look up information about domains and con-

tacts, InterNIC set up a special server. To allow users to retrieve information from this server, developers created a protocol called both nickname and whois. It was initially described in RFC 812 and then later in RFC 943. Over time, the name whois has become the preferred of the two, and it is the one used today for the utility program that allows an administrator to look up DNS registration data. /it can also be used to look up information about IP addresses, but is used for that purpose much less commonly/.

As the Internet grew and expanded, it moved away from having a single centralized authority. The modern Internet has a hierarchical structure of authorities that are responsible for registering domain names in different portions of the DNS name space. In recent years, this has been further complicated by the deregulation process that allows multiple registries for the generic top-level domains such as .com, .net… All of this means that more work is needed to look up domain registration information, since is distributed across many databases [Sportack 2004] on different servers.

To make it easier for administrators to find about domains in this large distributed database, modern TCP/IP implementations generally come with an intelligent version of the whois utility. It is able to accept as input the name of a domain and automatically locate the apprioritate registry in which that domain's information is located. The utility is usually used as follows:

whois [-h <whois-host>]

Listing 4 Short listing whois:

NAZWA DOMENY:	onet.pl
typ abonenta:	organizacja
serwery nazw:	dns2.onet.pl. [213.180.137.160]
	ns1.ikp.pl. [2001:4190:8002:1::302][157.25.5.2]
	dns1.onet.pl. [213.180.128.242]
	ns1.aster.pl. [212.76.32.1][2001:4050:0:101::1]
	dns3.onet.pl. [213.180.147.200]
utworzona:	1996.06.22 01:00:00
ostatnia modyfikacja:	2011.01.05 14:34:22
opcja utworzona:	2010.08.16 16:52:03
wygasa:	2013.08.16 16:52:03
ABONENT:	
firma:	Grupa Onet.pl SA
ulica:	ul. G. Zapolskiej 44
miasto:	30–126 Krakow

lokalizacja: PL
ostatnia modyfikacja: 2008.02.26

REJESTRATOR:

Grupa Onet.pl SA
ul. G. Zapolskiej 44
30–126 Kraków
Polska/Poland
+48. 12 2600200
bok@onet.pl

Conclusions

Most TCP/IP implementations provide one or more utilities that can be employed by an administrator to manually resolve DNS domain names to IP addresses or perform related searches for DNS information. One of the most common is nslookup, which allows a host name to be translated to an address or vice versa, it has both interactive and noninteractive modes. On some operating systems, nslookup has been replaced by the host utility for simple DNS lookups and by the dig program for more detailed inspections of DNS resource information. The TCP/IP whois utility allows registration information to be displayed for a DNS domain, such as its owner, contact information, and the date that is registration expiries. The program is most commonly found on UNIX operating systems, where it is given intelligence that allows it to automatically query the correct servers to find the information for most domains. Never Web-bassed whois also exist, but they are usually limited to displaying information about domains in only a specific subset of top-level domains.

Literature

Komar B. (2000), *Administracja sieci TCP/IP dla każdego*, Gliwice.
Karanjit S. Siyan, Parker T. (2002), *TCP/IP Księga eksperta*, Wydanie II, Gliwice.
Sportack M. (2004), *Sieci komputerowe. Księga eksperta*, Wydanie II, Gliwice.
Haugdahl S.J. (2001), *Diagnozowanie i utrzymanie sieci. Księga eksperta*, Gliwice.

Abstract

Even though millions of people use TCP/IP every day without even knowing that these applications exist much less how they are critically important to those who maintain TCP/IP interworks. Since many of you are studying TPC/IP so that you can implement and administer this technology, understanding how these

applications work is well worth your time. In this paper, I provide an overview of a number of software utilities that are commonly employed to help set up, configure, and maintain TCP/IP internetworks. These programs allow network administrator to perform functions such as checking the identity of a host, verifying connectivity between two hosts, checking the path of routers between devices, examining the configuration of a computer, and looking up a Domain Name System domain name.

Key words: system administration, administrative Tools, TCP / IP network.

TCP/IP Narzędzia administracyjne

Streszczenie

W artykule tym przedstawiono niezbędne narzędzia, którymi powinien się posługiwać każdy użytkownik pracujący w sieciach komputerowych opartych na protokołach TCP/IP. Ten obecnie najpopularniejszy standard komunikacyjny oparty na tego typu rozwiązaniach wymusza na użytkownikach znajomość podstawowych zasad komunikacji, aby samemu bez pomocy administratora wstępnie zdiagnozować problem, bądź też samemu go rozwiązać. Przedstawione tu narzędzia pozwalają w głównej mierze sprawdzić poprawność działania DNS, zawartych w ich strefach wpisów, sprawdzić zgodność odpowiedzi na przychodzące zapytania. Znajomość zasad działania serwera DNS jest kluczowa, jeżeli chodzi o bezpieczeństwo systemu.

Słowa kluczowe: administrowanie systemem, narzędzia administracyjne, sieć TCP/IP.