What All Network Administrators Know

A Guide to Becoming a Network Administrator

By Douglas Chick
Network Administrator/IT Director
MCSE, CCNA

Published by The Network Administrator.com

ISBN 0-9744630-0-0

Publisher –TheNetworkAdministrator.com
www.thenetworkadministrator.com

Schlaine Chudeusz, Editor

Table of Contents

Preface

This book is in response to the daily e-mails I receive from my website www.thenetworkadministrator.com that ask the question; “What do I need to know to become a network administrator?” Some of you reading this book might find that you have all the qualifications needed, while others may become easily discouraged. Don’t be discouraged. Nothing long lasting or worth having such as a professional career can happen overnight. As an experienced network administrator and a computer professional I can help you avoid the pitfalls that I see many new computer people encounter and help you realize your objective by making you more employable, by knowing what you can expect as a network administrator and the types of programs you will be expected to know. The problem with most books on computers and networking is they are thick with trivial data that either doesn’t help you get a job or doesn’t tell you what to do once you have one. *What All Network Administrators Know* is a short book that is to the point from a network manager’s perspective. All the books that you’ve read about computers and networking before this one addressed configurations, program usage and enough acronyms to fill a popular vegetable soup can. This book addresses what you should know before you interview and what you should expect once you have the job.

As you may have already discovered, there are not a lot of resources on the Internet or from your school or university that address how to become a network administrator. Though there is a network administrator

in every company with computers in the world, and there are million of us, no one addresses any of the basic questions associated with the job. This is why I have a site for network administrators and is precisely the reason for this book. As an experienced network administrator, I can give you valuable insight and help guide you in the direction that you need to collect the knowledge and tools to advance your career. I will address not only the basic fundamentals, but which operating systems will help you find a job faster, the real tools that you will need to help you do your job, and the corporate politics within every company that is rarely discussed outside of a group therapy session. When you finish reading this you will either be charged up and ready to get started, or realize you'd rather pursue that Liberal Arts Degree that your high school guidance counselor once spoke of.

There is a lot to know to be a network administrator, and reading this book might make is seem a bit overwhelming. It is not my intention to discourage anyone from being a network administrator. For many people, including myself, this is one of the greatest jobs you can have, but I'm not going to sugar coat it either. Being a network administrator can be hard and very demanding. Most books about networking only tell you how to configure software, this book will tell you what to expect when you get the job.

...

What To Do When a Server Crashes

There is no drug or single event in the world that can make a computer person focus more clearly than when a server crashes. The mere act of a crashing hard drive, database or server component can temporarily raise one's IQ as much as 50 points. You suddenly become more aware of the universe around you and less aware of trivial aspects in life, such as reality TV, what type of car you should drive and if wearing socks with sandals is cool. You can for a brief moment see dimly into the immediate future as your pleasure centers temporarily shutdown and you put your resume on standby for a mass mailing campaign. You move much quicker as time seems to slow down, you can calculate rational and irrational numbers using math that hasn't been invented yet and you become a little more spiritual—no, a lot more spiritual. A crashed server sometimes brings a network administrator closer to God, his or her fellow workers and the unemployment line. And in a single point of light (pixilated light) when you discover that your backups haven't run for over two months, a cold perspiration blankets your feverous body while your knees weaken and the contents of your stomach climb to the top of your reflux valve. This is it; your mission critical server crashed and you don't have a backup. So what do you do next? You do what every network administrator does when this happens; you calmly walk into your office, throw up in your trashcan and slowly begin gathering up your personal items while waiting for someone from Human Resources to bring you a box. And as you sit at your desk trying to

figure out how you're going to get 2 gigs of MP3s to your home computer it hits you like a brick—you read this book and configured a redundant backup to another server on another hard drive. Suddenly the feeling in your hands and feet return and you go back to the server room and restore the data.

When a server crashes and you don't have a current backup you are fired. When a hard drive crashes and you don't have a backup you are fired. And when there is a fire in your server room and all of the company's data is lost to fire, you are fired. Twice in my career a hard drive has crashed with critical company data on it and I didn't have a current backup to restore from. Backup software is not as reliable as many companies will lead you to believe. You should pick a day every week to check if your backups are successfully. I've made it a habit to check my backups every Monday without fail. Because if you don't… you know the rest. Another issue with backups is that you don't always know what should be backed up. It's a nice thought to have every drive on every server backed up every night, but in reality it's just not feasible. At my company, we have every server operating system imaged to a CD-ROM. If the server crashes, we can have another one re-imaged and up before you can restore from tape. Now all that's left to do is restore data files. When you are new to a company, it is almost impossible to guess what should and shouldn't be backed up. The best you can do is back up everything that looks like a data file and bring the head of every department in to show you what needs backing up. The first drive that crashed on me without a backup was the marketing department is

Macintosh drive. I didn't see it, I didn't know it was there and when it was lost there was someone there trying to monopolize on the situation for my job. So don't leave it up to guess-work, bring in someone from every department to help you. Later you will be thankful that you shared the responsibility. If your company manager tells you to back up everything, then they are going to have to invest in the proper equipment.

Types of Backups

- **Full** includes files whether they have been changed or not;

- **Differential** includes all files changed since the last full backup, whether they have been changed since the last backup operation or not;

- **Incremental** includes only those files that have changed since the last backup operation of any kind.

To choose which method of the above types of backups depends on three factors: the size of your tape, the period of time available for backups, and how long you want your restore to take.

A **Full Backup** on a daily basis requires a lot of tape and needs a longer duration to run. I've seen backups that start late at night and finish in the next afternoon, only to pause for a short breather and start

What to know about Security

Security is as important to your network as backups and corporate managers see little value in the necessary tools to keep your network safe until something happens. But what tools are there to help protect against intruders? These range from Firewalls, VPNs, Intrusion Detection software, Honeypots, Auditing, Forensics tools, Anti-virus and Anti-Spam for network protection. There are Vulnerability testing software and port scanners, Access Control Lists (ACL), Demilitarized Zones (DMZ), Proxy and Packet Filtering Crypto-Capable Routers.

Firewalls – Typically a Firewall will sit as a sentry that connects your network to the rest of the world. Firewalls will analyze data packets and compare requests against a pre-configured security list. Many network administrators configure their routers with security access-lists to avoid the necessity of a Firewall. Firewalls can also slow down access speeds because it inspects every packet.

- Checkpoint -One of the most popular software based firewalls.
- NetScreen - An excellent hardware based firewall that keeps your traffic moving at line speed.

Symantec Firewall/VPN Appliance An integrated security and networking device that provides easy secure, and cost-effective Internet connectivity between locations.

- Fortinet Dedicated hardware/software platforms that break the Content Processing Barrier, supporting network-based deployment of application-level services - including virus protection and full-scan content filtering - and enabling organizations to improve security, reduce network misuse and abuse, and better utilize their communications resources, without compromising network performance.
- Zone Alarm Provides solid, basic PC protection for the home user. An intuitive user interface that makes firewall management easier than ever, as well as a host of security enhancements. And Zone Alarm is free for personal use. Excellent for VPN users, too.

Virtual Private Networks (VPN) – Virtual private networks provide an encrypted connection between a user's distributed sites over a public network (e.g., the Internet). By contrast, a private network uses dedicated circuits and encryption. The basic idea is to provide an encrypted IP tunnel through the Internet that permits distributed sites to communicate securely. The encrypted tunnel provides a secure path for network applications and requires no changes to the application.

Proxy Servers – A server that sits between a client application such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

Linux -- servers have a great built-in proxy program. Here's a good link on the net that does a good job

explaining how to configure a proxy server using Linux.
http://www.tldp.org/HOWTO/Firewall-HOWTO.html

Wingate -- is popular proxy software for Windows:
http://www.wingate.com/

Access Lists – An access list is generally associated with a router or a computer that is acting as a Firewall. Simply put, an access list either accepts or rejects access to network resources as per configured in its tables. A Cisco router utilizes access list as a security measure to either route traffic to its intended destination or reject it by sending it to a bit bucket. (A null port configured to route a packet to nowhere instead of wasting resources by rejecting it to it's originator.)

Demilitarized Zone (DMZ) – is a computer or small subnetwork that sits between a trusted internal network, such as a corporate private Local Area Network, and an untrusted external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. The term comes from military use, meaning a buffer area between two enemies.

Honeypots & Tar Pits– An Internet attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system. Honeypots are designed to mimic systems that an intruder would like to break into but limit the intruder from having access to an entire network. If a honeypot is successful, the intruder will have no idea that s/he is being tricked and monitored. Most honeypots are installed inside a firewall so that they can better be controlled, though it is possible to install them outside of firewalls. A honeypot in a firewall works in the opposite way that a normal firewall works: instead of restricting what comes into a system from the Internet, the honeypot firewall allows all traffic to come in from the Internet and restricts what the system sends back out. If you want to learn more about "Honeypots" and "How to Create a Honeypot" follow the links below.

http://www.spitzner.net/honeypots.html
http://www.auditmypc.com/freescan/readingroom/honeypot.asp

Auditing – Event auditing is used to log either equipment or security actions such as deleted files, failed logons and sometimes unauthorized tampering. Event auditing can be used to prevent security break-ins or forensics work after the fact when it is too late.

Sniffers – A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal and a network administrator.

Commview – Commview is one of my favorite sniffer programs. Unlike the others I've used it displays live results and is inexpensive.

http://www.regnow.com/softsell/nph-softsell.cgi?item=1526-5&affiliate=18752

Ethereal – Ethereal is a free network protocol analyzer for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk.

http://www.ethereal.com/

WinPcap – WinPcap is another free network analyzer. If you are going to be a network administrator or engineer, another of these programs is a good start to learning sniffers.

http://winpcap.polito.it/301a/download.htm

Port Scanners – Every computer program and utility that is designed to interact with a network is also assigned a specific port number. A port number can range from 1 to whatever the designer assigns. Your browser uses port 80 because this is the number assigned to HTTP. FTP is 21, mail or SMTP is 110 or 25 for POP3. Because ports are the entrance in any network-ready device, they have to sometimes be blocked off to prevent intrusion. This is where a port scanner comes into place. It can be aimed at a single IP address or an entire network to scan to see which ports are open and available. Because of this, many network administrators limit the number of ports to be used. There are several methods to closing off port access, either by blocking them on your workstation or server, through a security access-list from a router or firewall, or using port translation. (Port translation is where all in- coming requests for port 80 are translated to port 2080.) A network administrator uses a port scanner to test his or her network as well as a hacker. Follow this LINK to a series of FREE Scanning tools.

http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm

What types of Attacks can be expected on my network?

Attacks against IP are the most common method of penetrating a node because it is the network protocol of the Internet. For any type of computer equipment to participate on the Internet it requires a valid IP Address and a Hardware Address. The network card maker burns a hardware address onto every network card. This number is unique to every other network and is expressed in a hexadecimal value. An IP Address is also unique and is either assigned statically or dynamically by your Internet provider. An IP Address can be tracked to its origination point to where it enters the Internet. This is where many hackers use some form of IP Spoofing. IP Spoofing is when someone purposely uses a forged IP Address so their exploits cannot be tracked back to their computer or location. IP and ARP (Hardware Addresses) are commonly spoofed although these days I don't know how effective it is.

Denial-of-Service – On the Internet, a denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. In the worst cases, for example, a Web site accessed by millions of people can occasionally be forced to temporarily cease operation. A denial of service attack can also destroy programming and files in a computer

system. Although usually intentional and malicious, denial of service attack can sometimes happen accidentally. A denial of service attack is a type of security breach to a computer system that does not usually result in the theft of information or other security loss. However, these attacks can cost the target person or company a great deal of time and money.

Buffer Overflows – A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to hold a specific amount of data, the extra information—which has to go somewhere—can overflow into the adjacent buffers, corrupting or overwriting the valid data stored. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information.

Data Diddling -- This kind of an attack involves altering the raw data just before a computer processes it and then changing it back after the processing is completed.

E-mail Spoofing – A spoofed e-mail is one that appears to originate from one source but actually has been sent from another source.

Spammers utilize this type of spoofing from mail servers that allow open forwarding. Because most

companies do not employ an E-mail Administrator, most network administrators don't know to close this vulnerability.

Worm / Virus Attack – This form of Virus is a program that attaches to a computer or a file and then propagates to other files and computers on a network.

Logic Bombs -- This is an event-dependent program that relies on a specific event such as a date to trigger the execution of the virus. (Like the Chernobyl virus).

Password Cracking – Password cracking isn't a complex procedure, as many people would think. I can tell you from experience that more than half of all passwords within a company are identical to any other company. People tend to use the same passwords as well as do network administrators. Most of the time, password cracking is more like password guessing. A network is only as secure as its passwords. Passwords are an ineffective security measure. They don't keep out the internal or external hackers, pranksters and criminals (there's software that can guess ½ the passwords in an average organization in only a couple of hours); Passwords are an administrator's nightmare. Users are constantly forgetting their password, even though it is typically their child or pet's name. There are many network administrators that force password expirations. This means that they've configured the server to expire passwords and force the users to change to a new password as a means of security. It is in my opinion that this practice causes more work for

the network administrator than it does protecting the network.

Confidentiality Breaches – It is reported that 90 percent of all security breaches are from the inside by employees. It is not uncommon to be asked to monitor company e-mail to help protect a company from lawsuits and valuable information being sent outside the company. I've seen everything you could possibly imagine from monitoring e-mail, pictures of hairy babies, adultery to embezzlement. For this reason most corporations monitor e-mail and if this surprises you, it is only because you haven't been careful yourself. Every packet of data that leaves and enters your router is most likely being monitored from either within your company itself or from outside entities.

What to Know About E-mail Servers

There are three types of mail servers that you should be aware of, MS Exchange, Send Mail and Lotus Notes. These are the three systems most commonly in use. If I had to suggest a mail server to try to learn I would select a Linux based mail server because they are the most common to the net and growing daily.

http://support.novell.com/
http://www.redhat.com/apps/support/

Tools of the Network Administrator

Ping – The ping utility is typically embedded into the computers operating system and is used to test a TCP/IP connection. If you are having connectivity issues here is a quick tip to follow:

- First ping your local loopback address, [ping 127.0.0.1] if you don't get a successful reply there is a problem with your TCP/IP configuration on the local computer. Un-install and then Re-install the TCP/IP Service. If your ping was successful next ping another address on your same network. If you can ping your loopback but not another computer on your network, check your cable connection or see if your subnet mask is correct. If you can successfully ping your loopback, and a computer on the same network but cannot ping outside of your network, then your default gateway is wrong. Here are a gaggle of ping utilities if you don't like it the old fashion way.

http://compnetworking.about.com/cs/pingtools/

Trace Route – Use trace route, or tracert in DOS on a Microsoft computer, to help in troubleshooting connectivity issues. Trace route is used to track the path of out going packets to see which routers they do and do not pass though. Many times a network problem

may lie on a remote network and trace route shows you the last successful hop.

Programs like Visual Route http://visualroute.com/ will give you a graphical view of where your target is and shows you a visual path.

Telnet – Telnet is a utility used to connect to a router or remote computer. Finding a Telnet program that you are comfortable with is important. I liked the one that came with Windows 98 or NT Server. I don't like the telnet program packaged in XP or Windows 2000. I've copied the old telnet program from NT and placed it on my laptop. Hackers typically use telnet to gain access to routers and test open and closed ports.

Protocol Analyzers – A protocol analyzer, or sniffer as most people will call it, is used to examine data packets entering and exiting your network. A sniffer can show you what traffic is dominating your network, from which computer sources and if someone is running a port scanner on any of your systems. Sniffer Pro is a good sniffer program but it has always been too expensive for me. Recently I found a program called Commview that I love. Very few computer people will spend their own money for software, but I did with Commview. Most operating systems come with their own packet analyzers, but they are basic and often clumsy to use. I prefer a real time program so I can watch the action as it happens. http://www.tamos.com/products/commview/

NSLOOKUP – is a program that quires a company's DNS server and resolves hostnames, aliases and mail exchanges. Hackers will sometimes use NSLOOKUP to profile the naming convention of a company. Here is an online tool to help you get the feel for what this utility does. http://www.trulan.com/nslookup.htm

Whois – Finds information about an IP address or hostname, including country, state or province, city, name of the network provider, administrator, etc. http://www.whois.net/

Netstat – is a built in tool with many Windows products, or you may purchase a more elaborate program off the Internet. Netstat displays current connection information and port numbers.

Nbtstat – A NBTSTAT command can be used to see who is currently logged onto any Windows system that is still using NetBIOS (all are by default, even Windows 2000). A NBTSTAT -A [IP address] will list the contents of the NetBIOS name table on the target system.

Vulnerability Assessments / Penetration Testing – Vulnerability assessments are generally performed by a network security company to test the integrity of your firewall, routers, and servers. What they are looking for is unpatched vulnerabilities left open by the network administrator because he or she didn't install security patches, or close port numbers or secure the system correctly. The last penetration test I ran, I examined

over 600 known vulnerabilities. It breached the computer before reaching the third vulnerability. Penetration testing can come in the form of software. Not every network administrator has access to penetration testing software, as it is often expensive and typically used by security testing groups. There are some companies that offer this type of software on a 30-day evaluation. It is worth the effort to search the net for and at least become familiar with the workings of such programs. Below you will find some of the more popular vulnerability programs.

Nessus:
http://www.nessus.org/download.html

Microsoft Assessment Tools:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools.asp

N-Stalker:
http://www.nstalker.com/downloads.php

GFI LANguard:
http://www.webattack.com/Freeware/server/fwserversecurity.shtml

Intrusion Detection Systems – As the name suggests, intrusion detection software analyzes users and system activities, configurations vulnerabilities, file integrity, recognizes patterns of typical attacks and analyzes abnormal activity patterns. http://www.lucidsecurity.com/

Command Line Utilities

Command Line Utilities are also important to know. On a Microsoft server simply type in NET and you will see the following:

NET [ACCOUNTS | COMPUTER | CONFIG | CONTINUE |
FILE | GROUP | HELP | HELPMSG | LOCALGROUP |
NAME | | PAUSE | PRINT | SEND | SESSION | SHARE |
START | STATISTICS | STOP | TIME | USE | USER | VIEW]

NET VIEW, USE, and SHARE are the 3 more useful commands that I use. You may type in "?" behind the command for a more detailed description on how to use this command.

NET USE ?

NET USE [devicename | *] [\\computer\sharename [\volume] [password | *]] [/USER: domainname\]username]

A more useful example might be:

NET USE F: \\servername\C$

You may use a * in the place of F: and it will give you the first available letter and the $ is a hidden administrative share. Often I will access a server from the command prompt by using the hidden administrator share. (Note: so do hackers)

The above is just an example of network command lines used in Microsoft products; Linux, Netware and Unix have their own.

...

About The Author

Doug Chick is currently an IT Director for a large health care group that spans across several Eastern states. As an IT Director, Doug prefers the technology side of his position and keeps an active hand on the companies servers and routers. His turn ons are learning new technology and testing network security protocols, his turn offs are helping people with too many cat pictures on their desk and people that bring him their home computer for repair. You may contact Doug at, DougChick@TheNetworkAdministrator.com

Cover Photos by Ellen & Kaitlyn Chick

And Special Thanks to:
Network Administrators
Joe Ritchey, David Whittaker, Erik Hansen