THE EXPERT'S VOICE® IN SYSTEM ADMINISTRATION

The Accidental SysAdmin Handbook

A Primer for Entry Level IT Professionals

—

Second Edition

—

Eric Kralicek

Apress®

The Accidental SysAdmin Handbook

A Primer for Entry Level IT Professionals

Second Edition

Eric Kralicek

Apress®

The Accidental SysAdmin Handbook, Second Edition: A Primer for Entry Level IT Professionals

ISBN-13 (pbk): 978-1-4842-1816-7

ISBN-13 (electronic): 978-1-4842-1817-4

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director: Welmoed Spahr
Lead Editor: Steve Anglin
Editorial Board: Steve Anglin, Pramila Balan, Louise Corrigan, Jonathan Gennick, Robert Hutchinson, Celestin Suresh John, Michelle Lowman, James Markham, Susan McDermott, Matthew Moodie, Jeffrey Pepper, Douglas Pundick, Ben Renow-Clarke, Gwenan Spearing
Coordinating Editor: Mark Powers
Copy Editor: Kezia Endsley
Compositor: SPi Global
Indexer: SPi Global
Artist: SPi Global

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a Delaware corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

Apress and friends of ED books may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Special Bulk Sales–eBook Licensing web page at www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this text is available to readers at www.apress.com/9781484218167. For additional information about how to locate and download your book's source code, go to www.apress.com/source-code/. Readers can also access source code at **SpringerLink** in the Supplementary Material section for each chapter.

Contents at a Glance

Contents

About the Author

Eric A. Kralicek has worked in the field of computer technology for over two decades, specifically with computer networking since 1984. He has been employed in companies large and small, public and private, using a variety of network operating systems in mixed environments. As a networking professional he has written numerous internal documents that have guided other professionals in their use of technical applications both on and off networked systems. Eric has been employed by Digital Computer Corporation as a Senior Information Management Specialist, Compaq Computer Corporation as a Senior System Software Engineer, dot com companies as an Information Technology Manager, and educational institutions providing network management and system integration. In every instance he has provided both technical skills and training documentation. Eric has a Bachelor's of Science degree in Computer Networking from Regis University, Denver, CO. He is Microsoft, ITIL and PRINCE II certified. Eric worked for the California State University system as a Network Analyst supporting administrative computer operations in a mixed network environment prior to working for NATO as an IT Engineer**.**

About the Technical Reviewer

Mark Beckner is a technical consultant specializing in business development and enterprise application integration. He runs his own consulting firm, Inotek Consulting Group, LLC, delivering innovative solutions to large corporations and small businesses. His projects have included engagements with numerous clients throughout the U.S., and range in nature from mobile application development to extensive backend integration solutions. He is the author of The Coder's Path to Wealth and Independence and a number of technical books on BizTalk and Dynamics CRM. Beckner, his wife Sara, and his boys Ciro and Iyer Blue live on a farm in a high desert town in Colorado. His website is http://www.inotekgroup.com and he can be contacted directly at mbeckner@inotekgroup.com.

CHAPTER 1

Introduction

The *Accidental SysAdmin Handbook* is designed to give new system administrators an understanding of concepts, processes, and technologies that will aid in their professional development. It is assumed that you have little to no experience in a professional information technology environment. While every information technology culture is specific to its parent organization, there are commonalities that apply to all organizations. This book looks at those commonalities and provides a general introduction to critical aspects associated with system administration. It further acts to provide definitions for common computer terms and acronyms.

System Administrator Duties

Each organization has uniquely defined system administrator roles and responsibilities. The scope of those duties can change from organization to organization and often change as an organization matures. But there are some basic tasks that all system administrators share.

Task List

- Installation of servers and clients
- Application installation and maintenance
- Creation of user accounts and security groups
- User support
- Shared drive mapping
- Backups and disaster recovery
- Security
- Housekeeping
- Automating tasks
- Printer installation and queue management
- Network operation support/management
- Change management

This list can contract or expand depending on the size of the information technology support team. However, someone will end up responsible for most if not all of these tasks. Many organizations add the role of technology mentor to the list. A growing use of the ITIL v3[1] framework has helped to standardize information system roles and responsibilities as well as processes.

Many information technology support teams divide tasks into roles. This allows each role to build a deep knowledgebase for processing tasks and resolving issues. There should be a deliberate effort by management to balance the workload so that all tasks can be completed effectively without overloading team members.

Task Management Roles (Example)

User Services

- User support (level two support)
- Printer installation and queue management
- Application installation and maintenance
- Installation of workstations or clients

Server Administration

- Installation of servers
- Creation of user accounts and security groups
- Shared drive mapping
- Backups and disaster recovery
- Housekeeping
- Automating tasks

Information Assurance

- Network operation support/management
- Security
- Change management

In this example, roles are separated into three sections (user services, server administration, and information assurance). These sections provide a separation of responsibilities to better facilitate operations and troubleshoot. This allows better management of skillsets and technical training programs so that each role is properly managed. Members of each section are better able to manage their responsibilities and respond to changes in the organization as technologies evolve.

Smaller organizations may merge many of these roles. The balance is found in the number of servers and services as well as the size and complexity of network operations. In this case, many of the tasks that system administrators must perform are automated and generic (meaning that canned scripts downloaded from vendor web sites do most of the common task required to maintain system services). This usually requires the understanding that issues may arise when generic scripts cause unforeseen damage. Further, standardization in creating servers and clients is imperative. The more each server and client looks and feels

[1] ITIL v3 home web site: http://www.itil-officialsite.com/home/home.asp

the same, the easier it is to resolve problems that can crop up from daily use. This also requires longer hours for a smaller number of staff. The possibility for employee turnover is greater and the quality of support is less than that of a more complete IT department.

Larger IT departments can provide greater scrutiny for testing and approving scripts, service packs, and hot fixes. They can deploy updates through a process of downloading, testing, and pushing updates with less risk. Services are managed by sections trained to support role-based tasks. This results in a more cohesive deliberate formal process that benefits the end users and operations. Security can be monitored more consistently and issue resolution can be methodically processed. The larger the team, the more focused each team member can be.

Operational Awareness

Whether the IT department is large or small, creating daily/weekly/monthly checklists to ensure that services and tasks are completed and managed methodically will benefit operational awareness.

In larger, more mature IT departments there are well established procedures and mechanisms in place. These processes are integrated in service support applications (such as BMC's Remedy) and integrate both operational aspects of service delivery and document key service management processes (such as change management, configuration management, asset management, service catalogue management, service level management, incident management, and feed a service knowledge management system). Solutions such as Remedy are expensive and require advanced understanding of business process management and technical integration. Because the service support application is interactive and part of business as usual, IT personnel feed the data as part of their daily activities.

In small or new IT departments, the maturity level for documenting processes and recording service knowledge management can be ad hoc with no standardization in place. Appendix A provides sample templates for daily/weekly/monthly checklists.

The Monday checklist found in Appendix A is meant to be simple one page list that would be performed at the beginning of each day by a selected system administrator, who would coordinate with other system administrators to ensure that all listed services were operational.

The weekly checklist is done during the weekly maintenance cycle.

The monthly checklist is compiled over the month and acts to produce a series of reports to ensure that management has an audit trail of changes, issues, and usage of all services and assets. The monthly report is used to evaluate the current operation performance of services rendered so that remediation can take place when discrepancies are noted.

Monthly reports are tied to the internal trouble ticket system, SOPs[2] in place to perform each of the checklist items, and internal report templates.

Communication

All too often people forget that communication is a two-way street. Many IT departments absorb information, act on that information, record their actions, and then move on to the next issue. The user community is left outside the process. Keeping the person who first notified the system administrator of the progress of each ticket (including a follow up after the ticket is finally resolved) benefits the initiator and the team resolving the issue.

[2] SOP – Standard Operational Procedures: *"A Standard Operating Procedure is a document which describes the regularly recurring operations relevant to the quality of the investigation. The purpose of a SOP is to carry out the operations correctly and always in the same manner. A SOP should be available at the place where the work is done"*. FAO Corporate Document Repository, "2 Standard Operational Procedures"; 1998, Natural Resource Management and Environment Department. http://www.fao.org/docrep/W7295E/w7295e04.htm

Internal communication is also extremely important. Many IT departments fail to share information internally, even though much of what they are doing crosses over between projects or solutions to issues for the customers. Keeping everyone informed about what's going on can prevent multiple system administrators from stepping over each other in working issues or projects.

As IT professionals depend on e-mail, phones, remote video sessions, and portals for communicating, the value of face-to-face collaboration can be lost. The need to have frequent and well planned meetings with team members is critical to maintaining momentum.

E-mail and video conference sessions tend to limit discussion and cooperation. E-mails are either too short or too long. E-mail content can be misinterpreted. Video conferencing is often time-limited and focused, not allowing detailed conversations to evolve.

A good IT department tends to have weekly meetings to coordinate activities, share information, understand what each teammate is working on, and assist as needed when another team member needs help. They document meeting minutes, keep their internal portal up to date, and coordinate all change management activities transparently. When applicable, they include stakeholders from outside the IT department to fine-tune service delivery and propose improvements.

Providing user education is almost as important as keeping users in the loop regarding issues. A well trained user group makes the job of system administrators easier and helps facilitate the troubleshooting process. It also helps by making everyone aware of housekeeping and preventative maintenance. There is a goal in IT to have a 90-8-2 policy[3] in effect. If users can resolve 90 percent of their problems, and the service desk can solve 8 percent of the more difficult problems, then the system administrators can focus on the most complex 2 percent of the issues. This leaves much of their time allocated to maintaining servers, services, and network security and operations.

Research

Keeping in tune with what's current in IT helps make you proactive with potential external issues. There are lots of free technical magazines (i.e., *TechNet,*[4] *Information Week,*[5] *Redmond Magazine,*[6] *Information Security Magazine,*[7] *The Journal,*[8] etc.). Additionally, you can find excellent research sites on the web (i.e., Whatis.com,[9] a service by Tech Target, EventID.net[10] and Tech Republic,[11] etc.). Expanding your pool of research materials will greatly add to your understanding of how to manage your network, servers, and users base. Along with all of the free research resources out there are paid vendor services (such as Microsoft's MSDN and TechNet subscriptions, which give you test software and in-depth technical support). Each vendor provides added technical services and can be a great advantage in keeping the IT environment up to date and secure.

[3] This is the 90/8/2 rule, that is 90 percent will be self-directed, 8 percent will be provided by a "generalist resource," and 2 percent will be provided by a "specialist resource," "Computer Technology Planning," paragraph 5.12; Langa College, December 6, 2005; http://www.langara.bc.ca/about-langara/policies/media/pdfs/B1004.pdf

[4] http://technet.microsoft.com/en-us/magazine/default.aspx

[5] http://www.informationweek.com/

[6] https://subscribe.1105pubs.com/sub/MI?WP=NEWFREE&TC=1

[7] http://searchsecurity.techtarget.com/

[8] http://thejournal.com/articles/2000/09/01/sun-microcomputer-systems.aspx

[9] http://whatis.techtarget.com/

[10] http://eventid.net/

[11] http://techrepublic.com.com/

Training

Attending vendor-specific courses for certification not only helps your professional development but also benefits the organization by increasing your depth of knowledge in handling IT issues. In fact, certification makes you and your IT operation more respectable to your customers and user base. It provides in-house expertise that is recognized by the IT industry and assures those who use your services that you conform to IT standards. It also allows those who attend courses to network with other IT professionals and build relationships that would be hard to build otherwise.

Maintaining certification[12] ensures your organization that its IT department is prepared for the present and the future. Having in-house experts (developed through certification coursework) also provides a wealth of knowledge that can be shared in the IT organization community and its user base. This knowledge can also help build operational policies and directives that further improve performance and reduce the amount of personnel needed to maintain services. It also reduces the dependency on outside experts to support major projects.

Leadership

System administrators provide the organization with a stable information platform in which to conduct business. System administration provides a technical layer in which the user base can conduct daily operations without the need to understand information architecture, infrastructure, or administration. Guidelines set by the IT community help the user base to use complex communication resources without having in-depth knowledge about what goes on behind the scenes.

Developing simple-to-understand processes and IT policies that simplify daily routines for the user base acts as both a standardization mechanism and organizational cultural foundation where everyone knows what is expected from IT and from the user base. This in turn promotes trust and cooperation between IT and the rest of the organization.

When they combine training, research, and communication with simple-to-follow rules, system administrators have a professional presence in the organization. Establishing daily routines to ensure service availability enforces this perception of professionalism. Acting quickly and completely to resolve user issues builds respect and cooperation between the IT community and its user base. Knowing that no one knows everything and being willing to let users know when you don't have the answer but will take the time to learn builds a sound IT/user relationship.

History in Brief

General

History is cyclic. This holds true for information technology and system administration. Policies, processes, and technology cycle between centralized and distributed management. Early on in the development of automated information processing, everything was centralized and system administration was performed in a bubble. As networks evolved, distributed information systems broke the bubble and complicated system administration and security.

[12] Example certifications: Microsoft MTA, MCSA, MCSE, MCSD. Cisco CCENT, CCDA, CCNA, CCT, CCNP. VMware Certified Associate, Professional, Implementation Expert, and Design Expert. SANS Institute GICSP, GIAC, GCCC. ITIL Foundation, Service Operations, Service Transition, and Service Design.

As networks matured, an appreciation for centralized management reemerged. This recreated a centralized environment that reined in the less controllable distributed management technologies and grew a host of system administration tools that have defined today's IT world. Understanding how this cycle affects the modern IT organization builds appreciation for all of the thought that has gone into the industry.

IT Timeline

- 1947 – The first electronic computing system was the ENIAC[13].
- 1951 – UNIVAC[14] computer became the first commercial computing system
- 1953 – IBM 701 EDPM[15] led to the FORTRAN programming language
- 1960 – The IBM 7090 was the first electronic computer to use transistors
- 1963 – Douglas Engelbart[16] invents the mouse
- 1969 – Arpanet was born,[17] which was the early Internet, and UNIX[18] was developed
- 1971 – Intel 4004, the first microprocessor,[19] and e-mail[20] was invented
- 1973 – Ethernet computer networking, TCP/IP[21]
- 1975 – Microsoft[22] was founded
- 1976 – Apple I[23] II and TRS-80
- 1978 – VisiCalc spreadsheet
- 1979 – WordStar word processing
- 1981 – IBM PC, MS DOS
- 1982 – Sun Microsystems[24] was incorporated

[13] "The ENIAC Story", Martin H Weik, 1961, Ordinance Ballistic Research Laboratories, Aberdeen Proving Ground, MD. http://ftp.arl.army.mil/~mike/comphist/eniac-story.html

[14] "The History of the UNIVAC - J Presper Eckert and John Mauchly", Mary Bellis, 1997, http://inventors.about.com/library/weekly/aa062398.htm

[15] "The History of International Business Machines and IBM Computers", Mary Bellis, 1997, http://inventors.about.com/od/computersandinternet/a/IBM701.htm

[16] 1963: "Douglas Engelbart invents the Mouse", Berkley Engineering, 2007, http://www.coe.berkeley.edu/about/history-and-traditions/1963-douglas-engelbart.html

[17] "History of the Internet", Hilary Poole, Tami Schuyler, Theresa M. Senft, Christos J.P. Moschovitis, May, 1999, http://www.historyoftheinternet.com/chap2.html

[18] "UNIX, LINUX ,and variant history", Computer Hope, 1998-2009, http://www.computerhope.com/history/unix.htm

[19] "Intel's First Microprocessor – the Intel® 4004" , Intel Corporation, 2009, http://www.intel.com/museum/archives/4004.htm

[20] "The History of E-Mail & Ray Tomlinson", Mary Bellis, About.com, 2009, http://inventors.about.com/od/estartinventions/a/email.htm

[21] TCP/IP History; http://www.tcpipguide.com/free/t_TCPIPOverviewandHistory.htm

[22] "Microsoft Corporation", International Directory of Company Histories, Vol.63. St. James Press, 2004; http://www.fundinguniverse.com/company-histories/Microsoft-Corporation-Company-History.html

[23] "The Beginning", The Apple Museum, 2009, http://www.theapplemuseum.com/index.php?id=55

[24] "Company Profile", Sun Microsystems, 2009. http://www.sun.com/aboutsun/company/history.jsp#1982

- 1983 – Apple Lisa, Novell[25] Networking
- 1984 – Apple Macintosh
- 1985 – Microsoft Windows
- 1989 – HTTP[26] was created to share files
- 1991 – Linux[27] was introduced
- 1992 – DEC introduces the Alpha[28] 64 bit processor
- 1993 – Microsoft Windows NT[29]
- 1995 – OpenBSD and Windows 95 released
- 1996 – Microsoft Windows NT 4.0
- 1998 – Microsoft Windows 98, and Solaris 7, and VMware Inc. founded
- 1999 – Apple OS X (Darwin) was released
- 2000 – Microsoft Windows 2000 and Active Directory, Red Hat Linux 6.2
- 2001 – Microsoft Windows XP
- 2003 – Microsoft Windows 2003, Red Hat Enterprise Linux 3, ESX Server 2.0 released
- 2004 – Microsoft Windows XP Sp2
- 2006 – Microsoft Windows Vista, VMware infrastructure 3 released
- 2008 – Microsoft Windows Server 2008, Vista SP1
- 2009 – Microsoft Windows 7, VMware Vsphere released
- 2011 – Microsoft Windows 8
- 2015 – Microsoft Windows 10

Personal Computing and Networking

Many people tend to look at the IBM PC as the beginning of personal computers and networking, but in 1973, Xerox introduced not only the concept of personal computers but also networking. Xerox created a computer that introduced Ethernet, mice, and an icon-based graphic user interface. While the concept was expensive and power hungry, it was to be the base for all modern business computers. But, not until the Apple Lisa did the concept of a point-and-click desktop really take off.

[25] Novell, Inc. History of the Company, http://www.fundinguniverse.com/company-histories/Novell-Inc-Company-History.html

[26] “Hypertext and CERN”, Tim Berners-Lee, CERN, March 1989, May 1990, http://www.w3.org/Administration/HTandCERN.txt

[27] “UNIX, LINUX ,and variant history”, Computer Hope, 1998-2009, http://www.computerhope.com/history/unix.htm

[28] http://www.cpu-collection.de/?l0=co&l1=DEC&l2=Alpha%20AXP

[29] “Windows History”, Microsoft Incorporated, 2009, http://www.microsoft.com/windows/WinHistoryDesktop.mspx

IBM looked at the personal computer in a very different way—text based and individual (not networked). IBM also put a heavy price on its interpretation of what business needed. IBM executives did not take the concept of home computers seriously until IBM clones flooded the market. IBM used public available technology to engineer most of its product (a mistake that would cost them dearly). Further, they contracted with a little known company (Microsoft) to manufacture their operating system. Both of these choices are now realized to be dramatic failures in forecasting the market.

The birth of the IBM PC clone started the personal computer boom and the public's interest. This interest grew exponentially. For a while there was the family computer store that made cheap IBM clones and flooded the market. From these came more elaborate "national" brands (such as Compaq and Wise) with newer technologies that included portable computers. Companies like the Sinclair and HeathKit promoted cheaper reliable systems that introduced the concept of non-technical people building their own systems from scratch.

Apple, with founders Steve Jobs and Steve Wozniak created educational systems such as the Apple II series, which led to the Macintosh. Apple tried to corner the market on graphic-based operating systems (GUI[30]), suing Microsoft when they manufactured the first versions of Windows. Apple lost the suit given that they themselves had copied Xerox in order to create their popular GUI. The failed suit opened the door for Microsoft to battle head on with Apple for that market share.

Novell Inc. (to be referred from this point on as Novell) and Sun Microsystems (to be referred from this point on as Sun) built a strong market for network operating systems (aka NOS[31]). For many years it seemed that no one could compete with Novell for PC networking systems. There were specialized networking systems such as PICK and LANTastic, but these did not compete on the same level as Novell. UNIX, ULTRIX, and VMS were expensive to own and manage. They required specialized knowledge that was not common to the layperson. Microsoft challenged all of these with its release of Windows for Workgroups, which made peer-to-peer[32]networking possible at a fraction of the cost.

Novell, in an attempt to corner the market on personal computer software (to accent its networking strategy), started buying up companies such as WordPerfect to build an office suite. This strategy over-tasked Novell and took its eye away from its core business (networking). At the same time, Microsoft enlisted the aid of a software engineer from the company that made VMS[33] and incorporated its technology into its Windows GUI, creating what is now known as NT technology. Since VMS was a mature operating system used for large-scale networking operations, the marriage of technologies became the downfall of Novell as the leader in the networking marketplace.

Novell tried to regain ownership of the networking marketplace by creating an innovative directory concept, NDS.[34] Novell had touched on an area of networking management that would set the level of administration for many years to come. Unfortunately for Novell, Microsoft quickly engineered its own

[30] GUI stands for graphical user interface.

[31] NOS is a computer operating system that is designed primarily to support workstations, personal computers, and, in some instances, older terminals that are connected on a local area network (LAN). Artisoft's LANtastic, Banyan VINES, Novell's NetWare, and Microsoft's LAN Manager are examples of network operating systems. In addition, some multi-purpose operating systems, such as Windows NT and Digital's OpenVMS, come with capabilities that enable them to be described as a network operating system.

[32] Peer-to-peer is a communications model in which each party has the same capabilities and either party can initiate a communication session. Other models with which it might be compared include the client/server model and the master/slave model. In some cases, peer-to-peer communications are implemented by giving each communication node server and client capabilities. In recent usage, peer-to-peer has come to describe applications in which users can use the Internet to exchange files with each other directly or through a mediating server.

[33] VMS (Virtual Memory System) is an operating system from Digital Equipment Corporation (DEC) that runs in its older mid-range computers. VMS originated in 1979 as a new operating system for DEC's new VAX computer, the successor to DEC's PDP-11. VMS is a 32-bit system that exploits the concept of virtual memory.

[34] NDS (Novell Directory Services) is a popular software product for managing access to computer resources and keeping track of the users of a network, such as a company's intranet, from a single point of administration. Using NDS, a network administrator can set up and control a database of users and manage it using a directory with an easy-to-use graphical user interface (GUI).

version of directory services (Active Directory) and packaged it with their common server package Windows 2000. While Active Directory was a less mature technology than NDS, it was cheaper and backed by a company on the rise in the market place. It can be said that NDS was a better directory service but Microsoft turned out to be a more viable company. Today Microsoft commands a 75 percent market share on all software sold throughout the world. If you were to bet your company's IT budget on any one company, it would be very difficult to choose someone other than Microsoft at this point.

Apple has built a significant place in the market. Apple has a strong user base that will not give up on the company and a growing multimedia market. They have re-tooled their operating system to incorporate UNIX and have made a strong showing by doing so. They have also deversified creating the iPad, iPhone, and a host of other well received products.

Summary

The timeline presented depicts sample milestones that have led to current modern system administration. Footnotes are added to help the reader go more in-depth on select topics. While this list is in no way complete, it is intended to act as a beginning to understand what has transpired over the years.

Much of what is taken as "best practices" is the result of trial and error with great economical cost. As time goes on and technology moves forward, more errors will take place and money will be spent.

It is true that people who do not learn from history are destined to repeat it. Taking time to explore the development of technology, including who designed it and why, helps in understanding procedures and processes that have developed over time.

It often seems that policies and procedures are over complicated, tedious, and time consuming. Experience tells us that this is necessary. Trial and error fine tunes each process to the point that anyone can follow. What is required from the system administrator is the ability to work with issues caused when the procedures fail to give the expected results.

Here is a short list of some books that may prove helpful:

- *PowerShell in Depth: An Administrator's Guide,* by Don Jones, Richard Siddaway, and Jeffrey Hicks
- *Microsoft Windows Networking Essentials*, by Darril Gibson
- *Windows Server 2008 Inside Out*, by William Stanek
- *VMware Horizon Suite: Building End User Experience,* by Paul O'Doherty and Stephane Asselin
- *Essential Virtual SAN (VSAN): Administrator's Guide to VMware Virtual SAN,* by Cormac Hogan
- *Cybersecurity for Dummies*
- *Cyber Security Essentials 1st Edition,* by James Graham (Editor), Ryan Olson (Editor)

CHAPTER 2

Home Networking

Like it or not, the majority of users often compare performance of an organization's network to the network in their home. Knowing how to explain the fundamental difference between the two benefits users and system administrators. Being able to present the many layers of administration overhead may lead home users to adapt some of the practices that organizations use to protect and maintain their IT investment. This chapter covers the fundamentals of the home network and builds the foundation for understanding an organization's network.

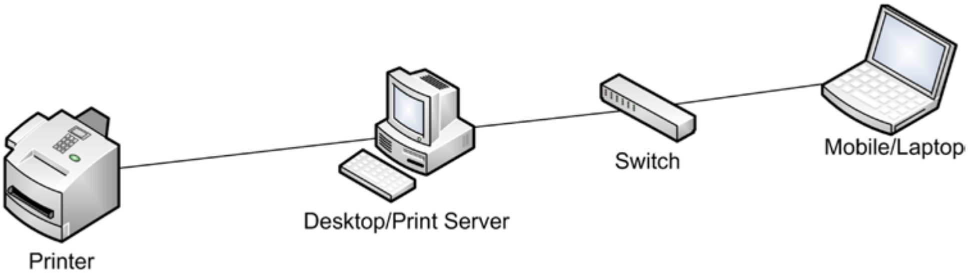

Figure 2-1. *Basic home network*

In Figure 2-1, there are four primary devices:

- Printer
- Desktop computer
- Networking switch
- Laptop computer

Each device presents a type of physical asset. The printer can include a scanner, fax, and more. The desktop provides access to the printer device and may also act as central storage for the laptop. The networking switch can connect desktops, laptops, and even printers if they are networkable and share the same communication interface. The laptop acts as a mobile office device to either work outside the home or transport data. The network connection can be wired or wireless.

Computers purchased for the home are consumer products, preconfigured and simplified for the mass market. They are quickly configured and brought online with little technical expertise. Consumer computer products differ from commercial computer products purchased for office use. They are essentially *turn key* products that have a shorter life span and come with a lot of sample software that eats up disk space and advertises vendor preferences.

Wired Networking

The four basic network home devices can be configured several ways. The various options have their pros and cons. In Figure 2-2, the desktop acts as print server and is connected to the printer via a USB cable. The desktop and laptop computers are connected by Ethernet cables via a networking switch.

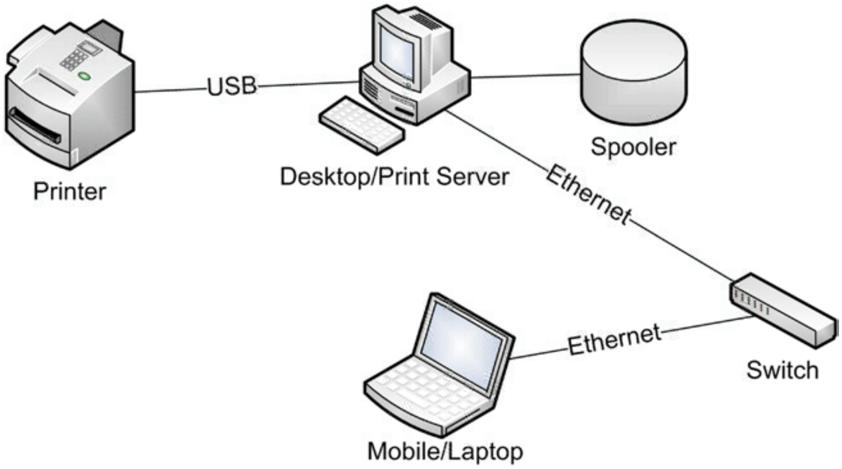

Figure 2-2. *Wired network with print server*

Since there is no Internet access, the only external access to this network is through physically connected devices (such as USB devices and CD/DVD disks). One must gain physical access to this network or provide physical media to perform malicious acts.

A network is *two or more* computers connected by a communication device in order to share information and peripherals (printers, modems, etc.). Even in the most basic network there is the foundation for all networks:

- Network interface (the technology that connects computers)
- Protocols (the way in which computers understand each other)
- Shared devices (printers, modems, hard drives, etc.)

These three things (network interface, protocols, and shared devices) work together to form an alliance of resources that combine their software and hardware to extend the capabilities beyond that of a single computer. Instead of a single desktop anchored to one physical location, the combination of laptop and desktop expand resources to include both a home office and mobile office extension.

In Figure 2-2, there is a shared disk drive on the desktop labeled “spooler”. For the desktop to share the printer, it must also share a common folder for print jobs to be staged so that the printer can process them. The print server (desktop) must allow the laptop to process print jobs through this shared folder. In order for that to take place, the laptop must have permission granted by the desktop.

Permission is granted through shared user accounts. The desktop must allow select laptop user accounts to place print jobs into its spooler folder (see Figure 2-3).

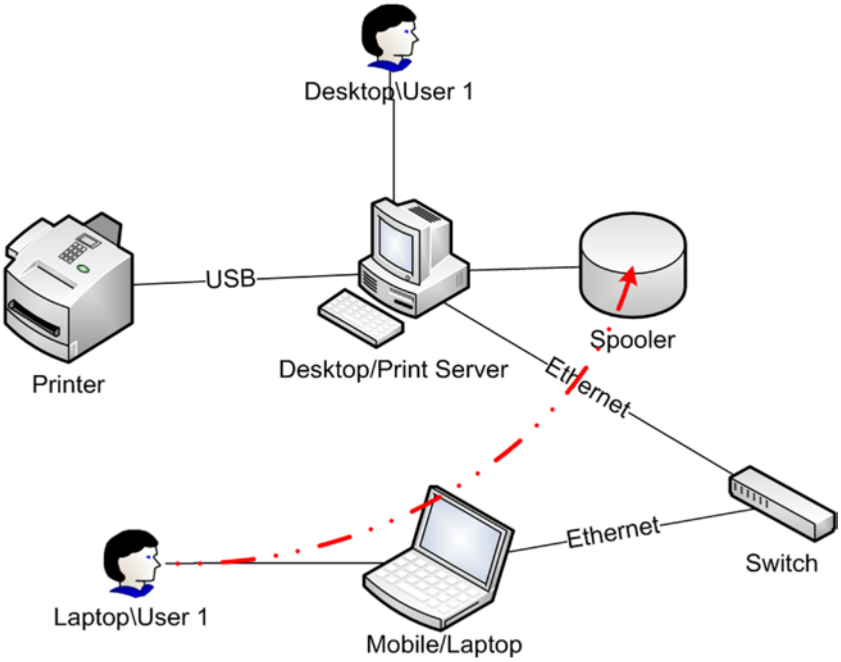

Figure 2-3. *Shared user accounts*

The shared user accounts only provide part of the solution. The desktop and laptop must also share a common print driver that can communicate with the printer in order to process the final print job. The complication arises from the fact that the system administrator must maintain common user accounts on both computers as well as print drivers and any special software that operates any secondary functions the printer provides (such as a scanner or fax).

There must also be an open port[1] granted by the desktop computer so that the print application can communicate between the desktop and laptop. Ports are numbered and have standards by which system administrators can evaluate their purpose. Port 35 is used for "any private print server".[2] All external communication goes through ports, and every open port is a potential security threat. Knowing the basic port numbers and their associated application helps you better understand the threat level associated with the number of open ports on a desktop or laptop.

The de facto protocol for modern networks is TCP/IP.[3] A product of the U.S. DOD in 1973, it is both *the* Internet protocol and the default protocol for all modern networking systems, personal computers, and servers sold today. All consumer computers auto-configure TCP/IP to connect to any visible workstation and/or network device, whether the device is wired or wireless.

[1] "In programming, a port (noun) is a "logical connection place" and specifically, using the Internet's protocol, TCP/IP, the way a client program specifies a particular server program on a computer in a network." See `http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212807,00.html`.

[2] IANA Port Assignments, 1998-2009 Network Sorcery, Inc. See `http://www.networksorcery.com/enp/protocol/ip/ports00000.htm`.

[3] Introduction to TCP/IP; H. Gilbert, Yale University, 1995. See `http://www.yale.edu/pclt/COMM/TCPIP.HTM`.

Figure 2-4 provides an alternative to having a dedicated print server. In this example, the printer is connected to the network via an Ethernet interface. The benefit is that each computer can access the printer without going through another computer, thereby removing the need to have shared user accounts to print. It also removes the need to have open ports, which can expose your computer to potential attack. Further, it also removes the need to have a dedicated print server turned on so other computers can use the printer. You still have to install printer drivers and software onto each machine.

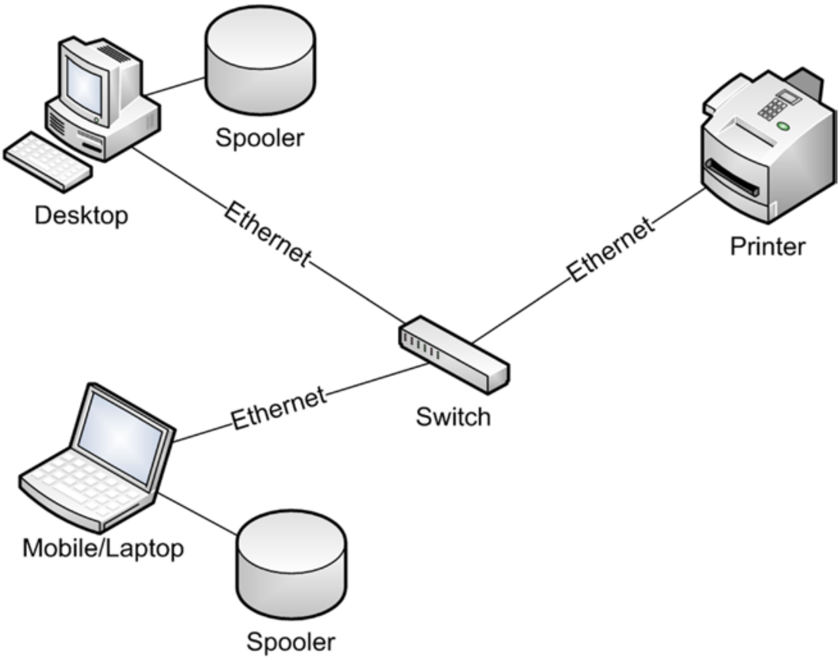

***Figure 2-4.** Network-enabled printer*

There are some multifunction printers that won't allow computers to remotely use their extended functions (scanners, faxes, etc.). By setting up network TCP/IP printers, every computer is considered to be directly connected. This eliminates that limitation.

Since each computer has its own spooler, there is no single point of failure other than the printer device itself. The drawback is that whoever prints first, prints first. With a print server you can queue print jobs, set priorities, and override priorities. In Figure 2-4, each spooler ignores the other.

Wired Network Pros

1. Physical security
2. Reliable bandwidth
3. Easy to troubleshoot