International Journal of Research (IJR) Vol-1, Issue-9 October 2014 **ISSN 2348-6848**

Elements of Network and System Administration

Smita Srivastava, Shweta Kurda & Priya Dubey

Information Technology, Dronacharya College of Engineering, Gurgaon, India

Email: srivastavasmita1993@gmail.com

Abstract:

Network and system administration is a branch of engineering that concerns the operational management of human–computer systems. It is unusual as an engineering discipline in that it addresses both the technology of computer systems and the users of the technology on an equal basis. It is about putting together a network of computers (workstations, PCs and supercomputers), getting them running and then keeping them running in spite of the activities of users who tend to cause the systems to fail.

Keywords: Network, TCP/IP, OSI, FTP

Introduction:

A system administrator works for users, so that they can use the system to produce work. However, a system administrator should not just cater for one or two selfish needs, but also work for the benefit of a whole community. Today, that community is a global community of machines and organizations, which spans every niche of human society and culture, thanks to the Internet. It is often a difficult balancing act to determine the best policy, which accounts for the different needs of everyone with a stake in a system. Once a computer is attached to the Internet, we have to consider the consequences of being directly connected to all the other computers in the world. In the future, improvements in technology might render system administration a somewhat easier task – one of pure resource administration – but, today, system administration is not just an administrative job, it is an extremely demanding engineer's job. It's about hardware, software, user support, diagnosis, repair and prevention. System administrators need to know a bit of everything: the skills are technical, administrative and socio-psychological. The terms *network administration* and *system administration* exist separately and are used both variously and inconsistently by industry and by academics. System administration is the term used traditionally by mainframe and Unix to describe the management of computers whether they are coupled by a network or not. To this community, network administration means the management of network infrastructure devices (routers and switches). The world of personal computers (PCs) has no tradition of managing individual computers. Network and system administration are increasingly challenging. The complexity of computer systems is increasing all the time. Even a single PC today, running Windows NT, and attached to a network, approaches the level of complexity that mainframe computers had ten years ago. We are now forced to think *systems* not just computers.

Applying technology in an environment

A key task of network and system administration is to build hardware configurations, another is to configure

software systems. Both of these tasks are performed for users. Each of these tasks presents its own challenges, but neither can be viewed in isolation. Hardware has to conform to the constraints of the physical world; it requires power, a temperate (usually indoor) climate, and a conformance to basic standards in order to work systematically. The type of hardware limits the kind of software that can run on it. Software requires hardware, a basic operating system infrastructure and a conformance to certain standards, but is not necessarily limited by physical concerns as long as it has hardware to run on. Modern software, in the context of a global network, needs to inter-operate and survive the possible hostilities of incompatible or inhospitable competitors.

Today the complexity of multiple software systems sharing a common Internet space reaches almost the level of the biological. In older days, it was normal to find proprietary solutions, whose strategy was to lock users into one company's products. Today that strategy is less dominant, and even untenable, thanks to networking. Today, there is not only a physical environment but a technological one, with a diversity that is constantly changing. Part of the challenge is to knit apparently disparate pieces of this community into a harmonious whole. We apply technology in such an environment for a purpose (running a business or other practice), and that purpose guides our actions and decisions, but it is usually insufficient to provide all the answers. Software creates abstractions that change the basic world view of administrators. The software domain .com does not have any fixed geographical location, but neither do the domains .uk or .no. Machines belonging to these software domains can be located anywhere in the world. It is not uncommon to find foreign embassies with domain names inside their country of origin, despite being located around the world. We are thus forced to think globally. The global view, presented to us by information technology means that we have to think penetratingly about the systems that are deployed. The extensive filaments of our inter-networked systems are exposed to attack, both accidental and malicious in a competitive jungle. Ignore the environment and one exposes oneself to unnecessary risk.

The human role in systems

For humans, the task of system administration is a balancing act. It requires patience, understanding, knowledge and experience. casualty ward of a hospital. Administrators need to be the doctor, the psychologist, and – when instruments fail – the mechanic. We need to work with the limited resources we have, be inventive in a crisis, and know a lot of general facts and figures about the way computers work. We need to recognize that the answers
are not always written down for us to copy, that machines do not always behave the way we think they should. We need to remain calm and attentive, and learn a dozen new things a year.
Computing systems require the very best of organizational skills and the most professional of attitudes. To start down the road of system administration, we need to know many *facts* and build confidence though experience – but we also need to know our limitations in order to avoid the careless mistakes which are all too easily provoked.

Ethical issues

Because computer systems are human–computer communities, there are ethical considerations involved in their administration. Even if certain decisions can be made objectively, e.g. for maximizing productivity or minimizing cost, one must have a policy for the use and management of computers and their users. Some decisions have to be made to protect the rights of individuals. A system administrator has many responsibilities and constraints to consider. Ethically, the first responsibility must be to the greater network community, and then to the users of our system. An administrator's job is to make users' lives bearable and to empower them in the production of real work.

Is system administration a discipline?

Is system administration a science? Is computer science a science? The same question has been asked of many disciplines. We can answer the question in like mind here. Unlike physics, chemistry or biology, system administration is lacking in a systematic body of experimental data which would give its rules and principles an empirical rigor. However, that is not to say that system administration cannot be made to follow this scientific form. Indeed, there is good reason to suppose that the task is easier in the administration of systems than in fields like software engineering, where one cannot easily separate human subjective concerns from an objective empiricism.

System administration practices, world-wide, vary from the haphazard to the state of the art. There is a variety of reasons for this. The global computer community has grown considerably, operating systems have become increasingly complex, but the number of system administrators has not grown in proportion. In the past, system administration has been a job which has not been carried out by dedicated Professionals, but rather by interested computer users, as a necessary chore in getting their work done. The focus on making computers easy to use has distracted many vendors from the belief that their computers should also be easy to manage. It is only over the gradual course of time that this has changed, though even today, system administrators are a barely visible race, until, something goes wrong.

The challenges of system administration

System administration is not just about installing operating systems. It is about planning and designing an efficient *community* of computers so that real *users* will be able to get their jobs done. That means:

• Designing a network which is logical and efficient.

• Deploying large numbers of machines which can be easily upgraded later.

• Deciding what services are needed.

• Planning and implementing adequate security.

• Providing a comfortable environment for users.

• Developing ways of fixing errors and problems which occur.

• Keeping track of and understanding how to use the enormous amount of knowledge which increases every year.

Some system administrators are responsible for both the hardware of the network and the computers which it connects, i.e. the cables as well as the computers. Some are only responsible for the computers. Either way, an understanding of how data flow from machine to machine is essential as well as an

understanding of how each machine affects every other. In all countries outside the United States, there are issues of internationalization, or tailoring the input/output hardware and software to local language.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.

TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network. TCP/IP communication is primarily point-to-point, meaning each communication is from one point (or host computer) in the network to another point or host computer. TCP/IP and the higher-level applications that use it are collectively said to be "stateless" because each client request is considered a new request unrelated to any previous one (unlike ordinary phone conversations that require a dedicated connection for the call duration). Being stateless frees network paths so that everyone can use them continuously. (Note that the TCP layer itself is not stateless as far as any one message is concerned. Its connection remains in place until all packets in a message have been received.)

FTP

File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers e-mail, FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It's also commonly used to download programs and other files to your computer from other servers.

As a user, you can use FTP with a simple command line interface (for example, from the Windows MS-DOS Prompt window) or with a commercial program that offers a graphical user interface. Your Web browser can also make FTP requests to download programs you select from a Web page. Using FTP, you can also update (delete, rename, move, and copy) files at a server. You need to logon to an FTP server.

However, publicly available files are easily accessed using anonymous FTP.

Basic FTP support is usually provided as part of a suite of programs that come with TCP/IP. However, any FTP client program with a graphical user interface usually must be downloaded from the company that makes it.

Internet Protocol (IP)

In the most widely installed level of the Internet Protocol (IP) today, an IP address is a 32-bit number that identifies each sender or receiver of information that is sent in packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

An IP address has two parts: the identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. On the Internet itself - that is, between the router that move packets from one point to another along the route - only the network part of the address is looked at.

The Network Part of the IP Address

The Internet is really the interconnection of many individual networks (it's sometimes referred to as an *internetwork*). So the Internet Protocol (IP) is basically the set of rules for one network communicating with any other (or occasionally, for broadcast messages, all other networks). Each network must know its own address on the Internet and that of any other networks with which it communicates. To be part of the Internet, an organization needs an Internet network number, which it can request from the Network Information Center (NIC). This unique network number is included in any packet sent out of the network onto the Internet.

The Local or Host Part of the IP Address

In addition to the network address or number, information is needed about which specific machine or host in a network is sending or receiving a message. So the IP address needs both the unique network number and a host number (which is unique within the network). (The host number is sometimes called a *local* or *machine address*.)

Part of the local address can identify a subnetwork or subnet address, which makes it easier for a network that is divided into several physical subnetworks (for examples, several different local area networks or) to handle many devices.

IP Address Classes and Their Formats

Since networks vary in size, there are four different address formats or classes to consider when applying to NIC for a network number:

- **Class A** addresses are for large networks with many devices.
- **Class B** addresses are for medium-sized networks.
- **Class C** addresses are for small networks (fewer than 256 devices).

- **Class D** addresses are multicast addresses.

The first few bits of each IP address indicate which of the address class formats it is using. The address structures look like this:

Class A

0 Network (7 bits) Local address (24 bits)

Class B

10 Network (14 bits) Local address (16 bits)

Class C

110 Network (21 bits) Local address (8 bits)

Class D

1110 Multicast address (28 bits)

The IP address is usually expressed as four decimal numbers, each representing eight bits, separated by periods. This is sometimes known as the dot address and, more technically, as *dotted quad notation*. For Class A IP addresses, the numbers would represent "network.local.local.local"; for a Class C IP address, they would represent "network.network.network.local". The number version of the IP address can (and usually is) represented by a name or series of names called the domain name.

The Internet's explosive growth makes it likely that, without some new architecture, the number of possible network addresses using the scheme above would soon be used up (at least, for Class C network addresses). However, a new IP version, IPv6, expands the size of the IP address to 128 bits, which will accommodate a large growth in the number of network addresses. For hosts still using IPv4, the use of subnets in the host or local part of the IP address will help reduce new applications for network numbers. In addition, most sites on today's mostly IPv4 Internet have gotten around the Class C network address limitation by using the Classless Inter-Domain Routing (CIDR) scheme for address notation.

Relationship of the IP Address to the Physical Address

The machine or physical address used within an organization's local area networks may be different than the Internet's IP address. The most typical example is the 48-bit Ethernet address. TCP/IP includes a facility called the Address Resolution Protocol (ARP) that lets the administrator create a table that maps IP addresses to physical addresses. The table is known as the *ARP cache*.

Static versus Dynamic IP Addresses

The discussion above assumes that IP addresses are assigned on a static basis. In fact, many IP addresses are assigned dynamically from a pool. Many corporate networks and online services economize on the number of IP addresses they use by sharing a pool of IP addresses among a large number of users. If you're an America Online user, for example, your IP address will vary from one logon session to the next because AOL is assigning it to you from a pool that is much smaller than AOL's base of subscribers.

Conclusion

While the age-old concept of the network is foundational in virtually all areas of society, Computer Networks and Protocols have forever changed the way humans will work, play, and communicate. Forging powerfully into areas of our lives that no one had expected, digital networking is further empowering us for the future. New protocols and standards will emerge, new applications will be conceived, and our lives will be further changed and enhanced. While the new will only be better, the majority of digital networking's current technologies are not cutting-edge, but rather are protocols and standards conceived at the dawn of the digital networking age that have stood solid for over thirty years.

References

[1] Huang Zhilong. Research on computer network security analysis model [J]. *Research on computer network security analysis model* , 2014(05).

[2] Zhang Tao; Hu Mingzeng; Yun Xiaochun, Zhang Yongzheng. Research on computer network security analysis model [J]. *Journal of communications*, 2005(12).

[3] Zhang Baoshi. Research on computer network security analysis model [J]. *Electronic technology and software engineering*, 2014(04).

[4] Hong Yaling. On modeling of computer network security [J]. *Computer CD Software and Applications*, 2013(02).

[5] Xv Liuwei. Modeling of computer network security [J]. *Computer CD Software and Applications*, 2013(06).