African Virtual University

Applied Computer Science: CSI 5100

NETWORK ADMINSTRATION

Thadee Gatera

Foreword

The African Virtual University (AVU) is proud to participate in increasing access to education in African countries through the production of quality learning materials. We are also proud to contribute to global knowledge as our Open Educational Resources are mostly accessed from outside the African continent.

This module was developed as part of a diploma and degree program in Applied Computer Science, in collaboration with 18 African partner institutions from 16 countries. A total of 156 modules were developed or translated to ensure availability in English, French and Portuguese. These modules have also been made available as open education resources (OER) on oer.avu.org.

On behalf of the African Virtual University and our patron, our partner institutions, the African Development Bank, I invite you to use this module in your institution, for your own education, to share it as widely as possible and to participate actively in the AVU communities of practice of your interest. We are committed to be on the frontline of developing and sharing Open Educational Resources.

The African Virtual University (AVU) is a Pan African Intergovernmental Organization established by charter with the mandate of significantly increasing access to quality higher education and training through the innovative use of information communication technologies. A Charter, establishing the AVU as an Intergovernmental Organization, has been signed so far by nineteen (19) African Governments - Kenya, Senegal, Mauritania, Mali, Cote d'Ivoire, Tanzania, Mozambique, Democratic Republic of Congo, Benin, Ghana, Republic of Guinea, Burkina Faso, Niger, South Sudan, Sudan, The Gambia, Guinea-Bissau, Ethiopia and Cape Verde.

The following institutions participated in the Applied Computer Science Program: (1) Université d'Abomey Calavi in Benin; (2) Université de Ougagadougou in Burkina Faso; (3) Université Lumière de Bujumbura in Burundi; (4) Université de Douala in Cameroon; (5) Université de Nouakchott in Mauritania; (6) Université Gaston Berger in Senegal; (7) Université des Sciences, des Techniques et Technologies de Bamako in Mali (8) Ghana Institute of Management and Public Administration; (9) Kwame Nkrumah University of Science and Technology in Ghana; (10) Kenyatta University in Kenya; (11) Egerton University in Kenya; (12) Addis Ababa University in Ethiopia (13) University of Rwanda; (14) University of Dar es Salaam in Tanzania; (15) Universite Abdou Moumouni de Niamey in Niger; (16) Université Cheikh Anta Diop in Senegal; (17) Universidade Pedagógica in Mozambique; and (18) The University of the Gambia in The Gambia.

Bakary Diallo

The Rector

African Virtual University

Production Credits

Author

Thadee Gatera

Peer Reviewer

Ashenafi Kassahun

AVU - Academic Coordination

Dr. Marilena Cabral

Overall Coordinator Applied Computer Science Program

Prof Tim Mwololo Waema

Module Coordinator

Robert Oboko

Instructional Designers

Elizabeth Mbasu

Benta Ochola

Diana Tuel

Media Team

Sidney McGregor

Barry Savala

Edwin Kiprono

Kelvin Muriithi

Victor Oluoch Otieno

Michal Abigael Koyier

Mercy Tabi Ojwang

Josiah Mutsogu

Kefa Murimi

Gerisson Mulongo

Copyright Notice

Supported By

AVU Multinational Project II funded by the African Development Bank.

Table of Contents

Course Overview

Welcome to Network Administration

This course is senior module within the Applied computer science program of the African Virtual University. It aims to provide in-depth knowledge in computer network technology and Communication by exploring the network administration. Network administration in any organization is in a charge of operation that involves IT infrastructure. With the convergence of computer networks and telecommunications networks, network administration work has also evolved tremendously and has become more demanding. This module encloses all the aspects needed for a network administrator to be well equipped. Having a network put in place, the administrator has is required to understand; legal aspects for network administration, ethical conduct for the network administrator, network services run on your network to enable provision of IT service(s), administration services, securing both hardware and application as well as maintenance and troubleshooting the network.

Prerequisites

As prerequisite to this module one must have knowledge of the following modules:

- Fundamentals of computer.
- Data communication and Computer networks.
- Operating system administration.
- Computer security.

Materials

The materials required to complete this course are:

- A personal computer installed with Windows/Linux.
- MySQL database.
- Apache web server and PHP.
- Browser software.
- Access to network.

Course Goals

At the end of this course, the student should be able to demonstrate the technical and administrative skills that enable him/her to manage networks in all levels of IT companies.

Units

Unit 0: Pre- Assessment

This module is a senior module. To successfully follow a student must have sufficient knowledge in fundamentals of computers, data communication and networks, operating system administration as well as network security.

Unit 1: Introduction

This is an introductory unit which talks about network administration in general, responsibilities of network administrator, ethical and legal issues concerning network administrator.

Unit 2: Network Services

This discusses some network services that put value to the network and saves energy as well as resources of the user and organization.

Unit 3: Network Management tools

This part includes the network administration architecture and tools that manage and monitor the life of network connected compone

Unit 4: Securing hardware and application

This unit entails all details for ensuring a possible secure network starting from the plan and identifying physical vulnerabilities.

Unit 5: Maintenance and troubleshooting

This unit tackles maintenance, backups and recovery. It emphasizes that maintenance should be performed according to a plan and that the organization should have a policy governing maintenance.

Assessment

Formative assessments, used to check learner progress, are included in each unit.

Summative assessments, such as final tests and assignments, are provided at the end of each module and cover knowledge and skills from the entire module.

Summative assessments are administered at the discretion of the institution offering the course. The suggested assessment plan is as follows:

1	Test 1	10
2	Test 2	10
3	Assignment	10
4	Lab practice	20
5	Final exam	50
6	Total marks	100%

Schedule

Unit	Activities	Estimated time
Pre - Assessment	Overview.	15 hours
	Computer network types.	
	Computer network topologies.	
	Computer network types.	
Introduction	Motivation	10 hours
	Administrator's scope	
	Ethical aspect	
	Legal aspect	
Network services	2.1. Network Address Translation.	15 hours
	2.2. Dynamic Host Configuration Protocol	
	2.3. Domain Name Service	
	2.4. Web Server	
	2.5. Mail Server	
	2.6. File and Print server	
Network administration tools	3.1. Administration architecture	10hours
	3.2. Administration via WWW.	
	3.3. Network management protocol	

Securing hardware and applications	4.1. Security plan.	15 hours
	4.2. Risk analysis.	
	4.3. Security policies.	
	4.4. Physical policies.	
Maintenance and troubleshooting	5.1. Types of maintenance	15hours
	5.2. Maintenance tasks.	
	5.3. Policy and schedules of maintenance	
	5.4. Backup and disaster recovery.	
	5.5. Maintenance contracts	
Lab		10hours

Readings and Other Resources

The readings and other resources in this course are:

Unit 0

Required readings and other resources:

- Forouzan, B. A. (2007). Data Communications and Networking. New York: McGraw - HillCompanies.
- Stallings, W. (2007). Data and Computer Communications. New Jersey: Pearson Prentice Hall.
- http://www.tutorialspoint.com/data_communication_computer_network/ visited February, 2016.

Optional readings and other resources:

- Forouzan, B. A. (2007). Data Communications and Networking. New York: McGraw - HillCompanies.

Unit 1

Required readings and other resources:

- Charles P. Pfleege, S. L. (2007). Security in Computing, Fourth Edition. Prentice Hall.
- Craig, H. (2002). TCPIP Network Administration, 3rd Edition. Sebastopol: O'Reilly Media.
- Forouzan, B. A. (2007). Data Communications and Networking. New York: McGraw - HillCompanies.

Optional readings and other resources:

- Charles P. Pfleege, S. L. (2007). Security in Computing, Fourth Edition. Prentice Hall.

Unit 2

Required readings and other resources:

- Forouzan, B. A. (2007). *Data Communications and Networking*. New York: McGraw - HillCompanies.
- Hunt, C. (2002). TCPIP *Network Administration, 3rd Edition*. Sebastopol: O'Reilly Media.

Optional readings and other resources:

- Hunt, C. (2002). TCPIP *Network Administration, 3rd Edition*. Sebastopol: O'Reilly Media.

Unit 3

Required readings and other resources:

- Cisco. (2016, February 27). networkers/nw03/presos/docs/NMS-1001.pdf. Retrieved February 27, 2016, from http://www.cisco.com/: http://www.cisco.com/networkers/nw03/presos/docs/NMS-1001.pdf
- Pras, A. (2016, February 27). ~jakab/edu/litr/TMN/Network_Management_Architectures_extr.pdf. Retrieved February 27, 2016, from http://www.hit.bme.hu/: http://www.hit.bme.hu/~jakab/edu/litr/TMN/Network_Management_Architectures_extr.pdf
- Thomas A. Limoncelli, C. J. (2007). The Practice of System and Network Administration Second Edition. Boston: Addison Wesley.

Optional readings and other resources:

- Thomas A. Limoncelli, C. J. (2007). The Practice of System and Network Administration Second Edition. Boston: Addison Wesley.

Unit 4

Required readings and other resources:

- Charles P. Pfleege, S. L. (2007). *Security in Computing, Fourth Edition*. Prentice Hall.
- Craig, H. (2002). TCPIP *Network Administration, 3rd Edition*. Sebastopol: O'Reilly Media.
- Thomas A. Limoncelli, C. J. (2007). *The Practice of System and Network Administration Second Edition*. Boston: Addison Wesley.

Optional readings and other resources:

- Charles P. Pfleege, S. L. (2007). *Security in Computing, Fourth Edition.* Prentice Hall.

Unit 5

Required readings and other resources:

- Habraken Joe, H. M. (2004). SAMS *Teach yourself Networking in 24 hours Third Edition*. Indiana: SAMS Publishing.
- Kizza, J. M. (2009). *A Guide to Computer Network Security. London:* Springer-Verlag London Ltd.
- Thomas A. Limoncelli, C. J. (2007). *The Practice of System and Network Administration Second Edition.* Boston: Addison Wesley.

Optional readings and other resources:

- Kizza, J. M. (2009). *A Guide to Computer Network Security. London*: Springer-Verlag London Ltd.

Unit 0 Pre-Assessment

Unit Introduction

The motivation behind investing too much in computer networks is the sharing of data and resources plus exchanging information despite the distance separating exchanging/ communicating parties. As shown in the pre-requisites network administration is accomplished where the working network is in place. One or more communicating devices are connected to allow themselves (or their users) to exchange data. These connected devices form a network where the achieved the media of communication could either be wires or wireless media.

This unit will allow you to check the knowledge you need before starting the course. You can take the assessments of this unit before you go to further activities; all exercises here help refresh your knowledge.

Unit Objectives

Upon completion of this unit you should be able to:

- Define what a network is.
- Describe network types based on geographic location.
- Differentiate among network topologies.
- Illustrate network models.

Key Terms

Computer network: Computers and their peripherals which are connected to service resource sharing and data exchange.

Node: Every network device that participate in the communication intended by the user.

Network topology: This is the arrangement of nodes in the network.

LAN: This is Local Area Network.

WAN: Widen Area Network

Learning Activities

1. Overview

Computer networks are formed by connecting computers and their peripherals. The built network spans a certain size of area range to a very small area, medium size and wider area. This network can be private or public which is discussed in later parts. The nodes connected to each other follow some topologies like star topologies, mesh topologies, bus topologies, ring topologies, tree topologies, and hybrid topologies. Where the devices share roles; two communicating nodes have equal capabilities hence peer-to-peer. Another arrangement could be done where one node could possess super role (server) and serve others (client), hence client-server communication. There is a hybrid architecture which is achieved as a combination of the two architectures above. An accomplished network is dedicated to serve different applications: resources sharing email reading/sending, file sharing, instant messages, distributed computing, video conferencing, browsing, etc.

Conclusion

There is ever increasing need that compels human being to put in place computer networks, such as need to share resources and data. Computer networks serve several applications in human lives for example, share printers, sending/receiving email, instant messages, to mention but a few.

Assessment

What are the applications of computer networks you know?

Feedback

There are four basic uses or areas of application as far as computer networks are concerned.

i. Communication: people communication through the network. Be it phone calls, chatting, and many more ways available.

ii. Sharing resources: different resources like scanners, printers are shared by different computer instead of using one per computer.

iii. Sharing software: In case a node is servicing as a server, clients can access software which are stored there.

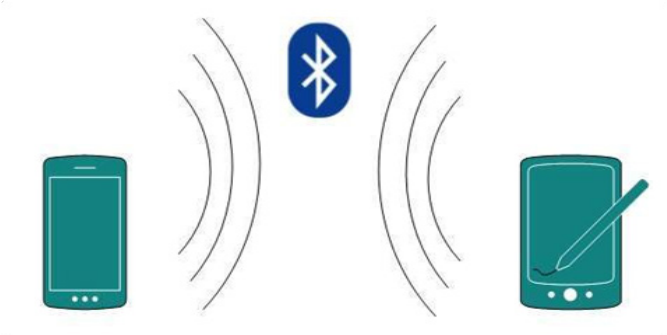
iv. Sharing data: in a networked environment, an authorized user files and data stored on other nodes. An authorized employee can access a report on the computer of the boss.

Computer network types

We differentiate the types of computer networks based on the area they span. Some network nodes are separated by small distance, which might increase until the whole globe is spanned.

Personal Area Network (PAN)

This is a smallest network which ranges up to 10 meters for Bluetooth enabled devices and infra-red communicating devices. Let us talk of mobile phones sharing files through Bluetooth placed on a table, wireless mice and keyboard.

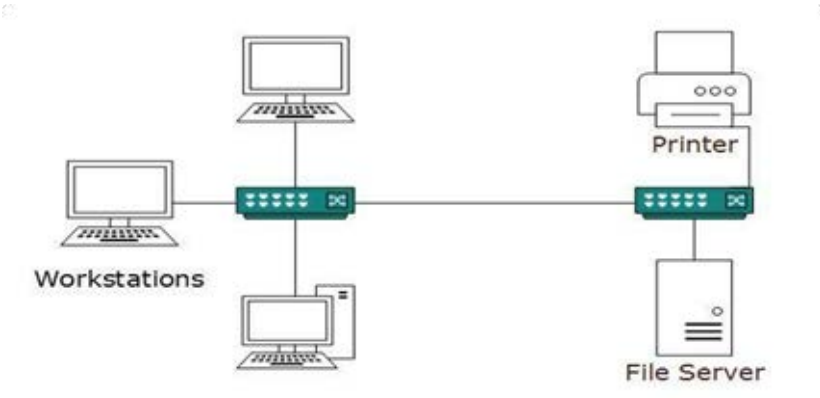


Source:

http://www.tutorialspoint.com/data_communication_computer_network/computer_network_types.htm

Local Area Network (LAN)

This is a network spanning a building or an organization working in one place. Talk of a university network, or a hospital network; this spans an organization in one location. Both wireless and wired media can be media of communication.

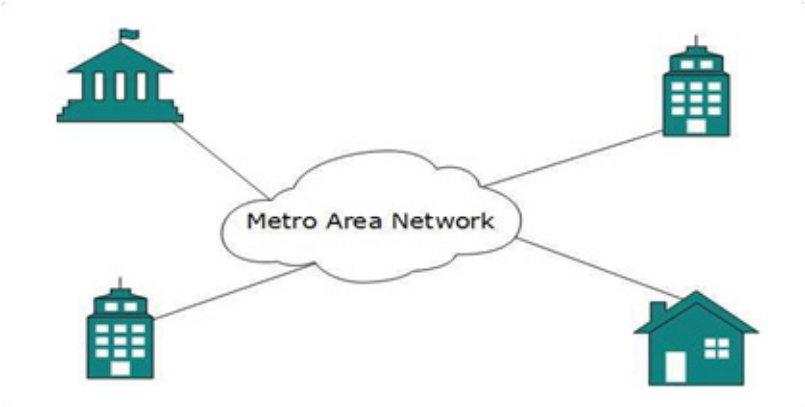


Source:

http://www.tutorialspoint.com/data_communication_computer_network/computer_network_types.htm

Metropolitan Area Network (MAN)

This is an extended local area network where local area networks located in different locations under one organization can be connected. We take the context of a bank that has branches in a city. MAN spans some few city blocks or entire city.

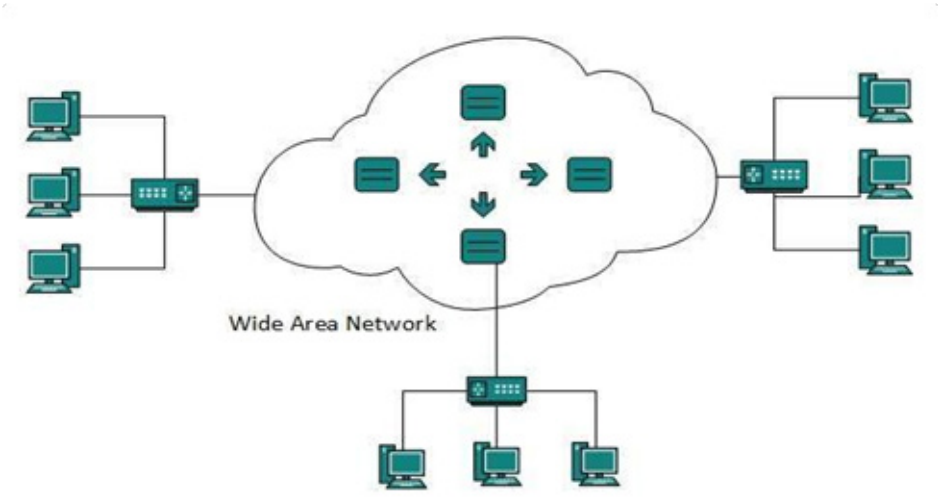


Source:

http://www.tutorialspoint.com/data_communication_computer_network/computer_network_types.htm

Wide Area Networks (WAN)

This is a network that extends over a large geographical location it is always bigger than MAN, to the level of connecting a country.



Source:

http://www.tutorialspoint.com/data_communication_computer_network/computer_network_types.htm

WANs connected together form an internetwork which is network of networks. The widest WAN on the planet is the internet.

Assessment

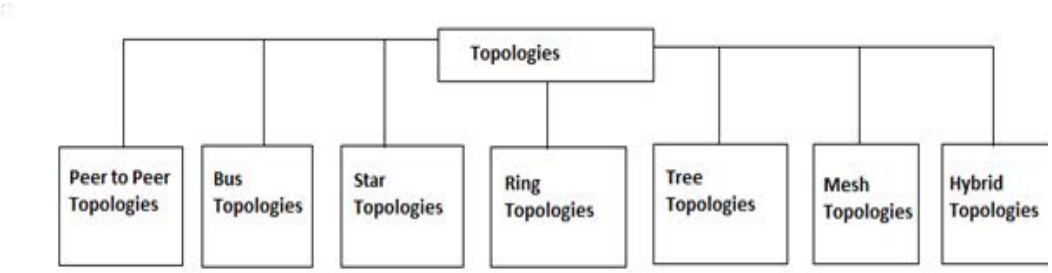
What is the difference between LAN and WAN?

Feedback

LAN is a private network of an organization in one place. This might span an office, a building or multiple buildings in same location. WAN on the other hand connects many LAN in different geographical locations. In short it spans bigger area.

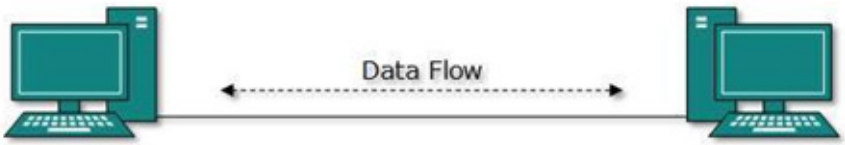
Computer network topologies

Computer network topology is the arrangement of nodes over the network. The diagram below shows the different topologies.



Different computer network topologies

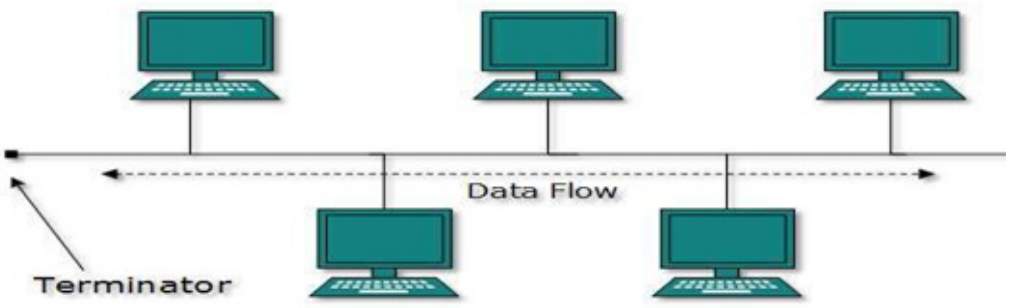
Peer to Peer topology is when a node is seen by another node as if it is connected directly. There might be some intermediate devices but each node on either side is unaware of intermediate layers.



Source:

http://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.htm

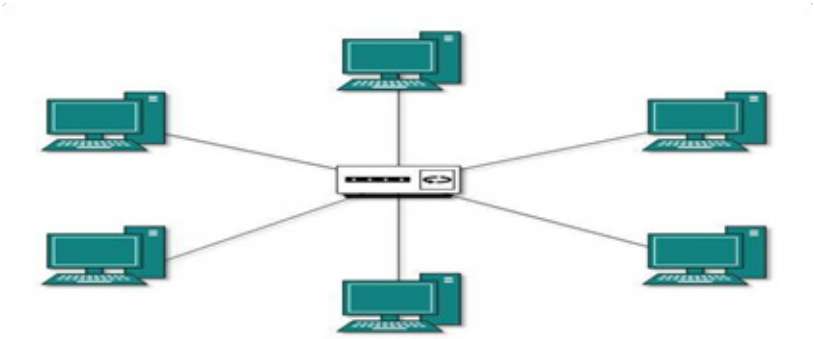
Bus topology is when there is a single and a common communication channel on which all nodes are connected with terminators on both ends to absorb signals as they reach their.



Source:

http://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.htm

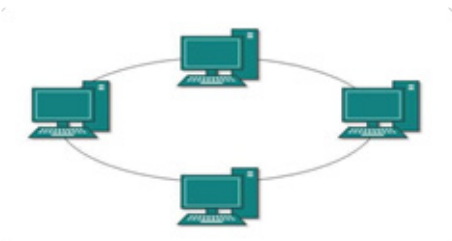
Star topology is the arrangement of nodes where there is central node from which all other nodes are connected from.



Source:

http://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.htm

Ring topology is the sequence of all nodes connected, one gets connection from the preceding node and the first node is the last node which makes a cycle (ring).

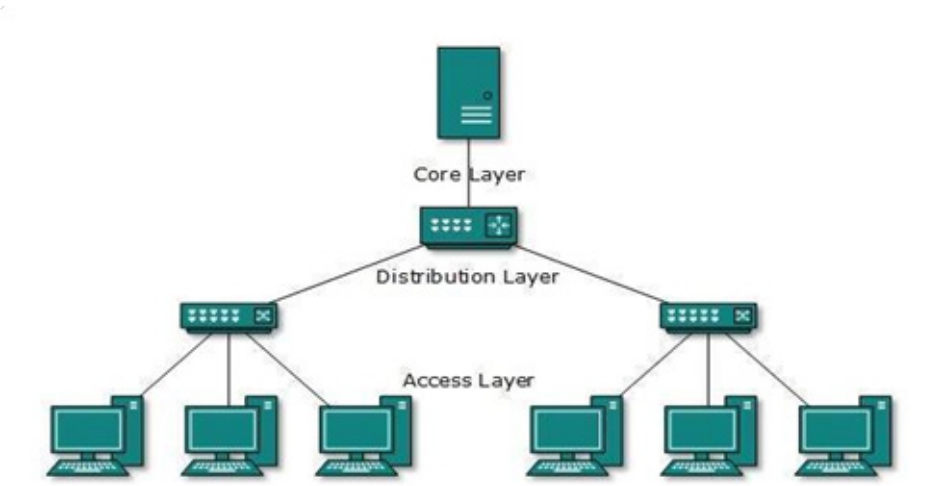


Source:

http://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.ht

Tree topology is the arrangement of nodes based on levels or layers. There is always one node at button of the network (root node), below this level is another level of nodes (which all

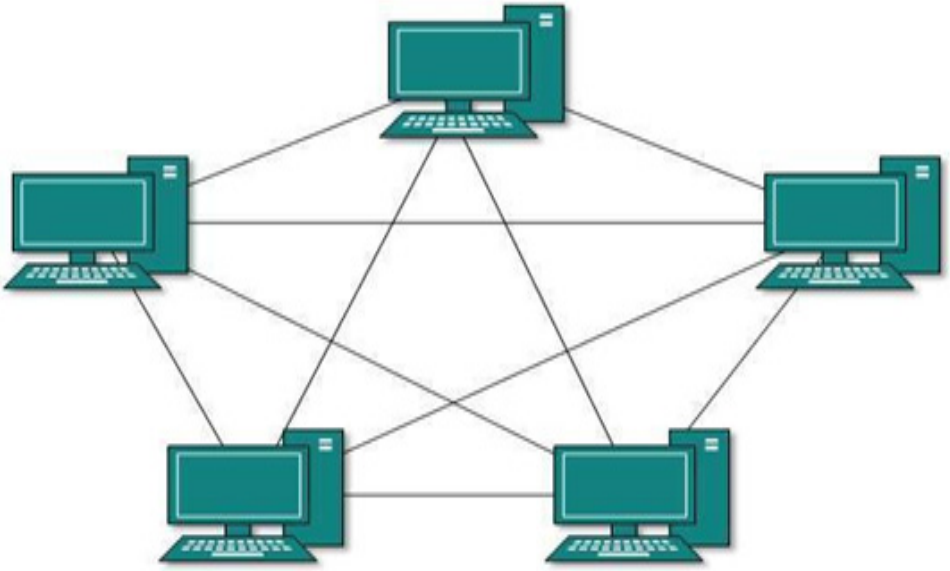
share the same parent), and below each of those nodes are other nodes. At each level there is one root node where with its children they form a star topology.



Source:

http://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.htm

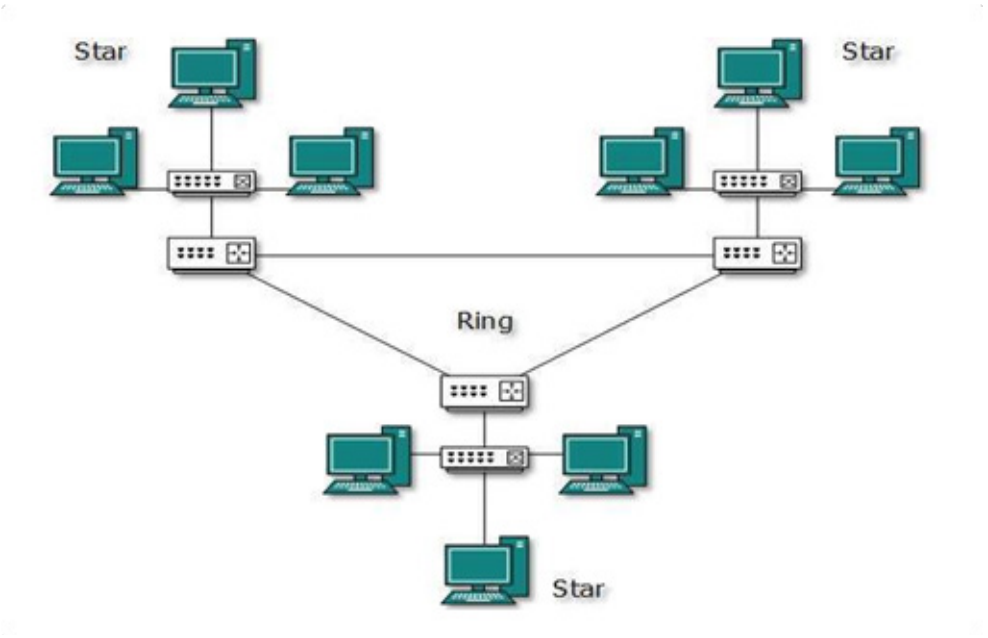
Mesh topology is the arrangement of nodes in such a way that each node in the network is connected to the rest of other nodes.



Source:

http://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.htm

Hybrid topology this is implementation of two or more topologies together to form a result network.



Source:

http://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.htm

Assessment

What is the best computer network topology?

Feedback

We can say that there is no specific answer to this, it depends on the environment. Some of the cheap topologies in implementation might not ensure availability. For example home network might be of star topology but if the central devices fail all the rest devices fail to be accessible on the network but this topology is easily implemented.

Computer network models

This is a definition of a set of layers which interact with each other in the whole process to achieve communication between different nodes. Each layer is involved in a particular task independent of other layers. These standards are needed due to the presence of heterogeneous networks. The most known models are OSI model and internet model. The OSI model has seven layers; application layer, presentation layer, session layer, transport layer, network layer, data link layer, and the physical layer which is the bottom layer. Whereas the internet model has four layers which are; application layer, transport layer, network layer and link layer which is the bottom most layer.

Assessment

What is the difference between OSI model and internet model?

Feedback

Both models are based on the concept of layers and each layer is independent as per model. Internet model does not consider all the 7 layers of OSI but rather it considers 4 layers and these layers achieve full functionality.

Link layer of the internet model corresponds to data link and physical layer of OSI, network layer of internet layer corresponds to network layer of OSI, transport layer of the internet model corresponds to the transport layer of the OSI, whereas application layer of internet layer correspond to three layers (session, presentation, application) of the OSI model.

Conclusion

Network administration comes later after the network has been put in place. While building a network a network topology should be thought about, a geographical location that spans the organization detects the network type. While communicating between different nodes, either wireless or wired media is used and different layers that play part in information flow during communication.

Unit Assessment

1. What is a computer network? What is the difference between network and internet?
2. How does information get transferred through network?
3. Who sends and receive information?

Grading scheme

The unit's assessments are graded out of 10% which are categorized as follows:

- Activity assessments are out of 3%.
- Unit assessment is out of 2%.
- Unit test is out of 5%.

Feedback

1. A computer network is a set of connected computer for the purpose of sharing resources, files, data and services. The minimum network is composed of two communicating nodes and can reach maximum as the number of IP addresses available. Internet is the interconnected networks, which is implemented by connected massive networks globally. By connecting different networks the internet is in place, given permissions on one node access from other nodes accomplished.

2. The information is transferred in form of packets through the network. A packet is the basic unit of information transferred; the packet has the header and message body. The header

has the source and destination of the message and other information that will handle the packet as it travels through different layers of protocol suite. A packet sent has a finite number of bytes.

3. While sending and receiving a message on network, the message will be sent from node on network and will be going to another node on the same network or different network but initiated by person/application who/which is considered as the user. The network node sends and receives information which is owned by a user.

Unit Readings and Other Resources

- Forouzan, B. A. (2007). *Data Communications and Networking. New York:* McGraw - HillCompanies.
- Stallings, W. (2007). *Data and Computer Communications. New Jersey*: Pearson Prentice Hall.
- http://www.tutorialspoint.com/data_communication_computer_network/ visited February, 2016

Unit 1. Introduction

Unit Introduction

This first unit aims to provide an introduction to this module of network administration. The goal is to generate interest and curiosity to the learner such that he/she can actively follow the module and complete it successfully. In addition, it demonstrates to the learner how network administration currently occupies a prominent place among the IT professional enterprises and how network administrators are highly rated specialists in nowadays, the unit would also bring the student to recognize the need for good human and technical skills to work as a network administrator. In this realm the multitude and diversity of network administration tasks, as well as the ethical and legal dimension that go with network administration are presented.

Unit Objectives

Upon completion of this unit you should be able to:

- Provide an overview of the role and requirements of network administration in the current technological and economic environment.
- Identify the place of a network administration.
- Explain the diversity of administrative activities.
- Show how administrative activities fit into ISO reference model.
- Identify the legal and ethical dimension of network administration.

Key Terms

Network administration: This is a set of activities performed to keep the network running smoothly and efficiently.

Network administrator: A person responsible for all activities to keep the network smooth and efficient.

IT Ethical issues: These are moral values that a network administrator keeps while accessing and using information in the organization's network.

IT Legal issues: These are legal concerns that might raise against the network administrator due to malpracticing his/her duties.

Learning Activities

MOTIVATION

INTRODUCTION

We want to open this introductory unit in this module on network administration by the presentations of the motivations that drove the network administration to emerge as a profession to occupy the special place it occupies today among computer professionals and information and communications technology.

DETAILED ACTIVITY

Network administration is an IT function that is a priority in the context of the operation of information systems in organizations and modern enterprises. It has a central objective of achieving continuous operation and optimal network infrastructure as well as hardware and software systems it supports. Indeed, almost all computer systems that we encounter today, ranging from simple to complex, are deployed in the networks. In particular, when the infrastructure and systems become complex, the chance of discovering the malfunction is equally big; hence the detection and correction of failures require systematic professional approach and expertise. This demonstrates how network administration is a noble work that requires one to be equipped with great skills to accomplish it.

The duties of a network administrator include:

- Establish and maintain infrastructure.
- Installation and maintenance of network services that enhance network function. DHCP (Dynamic Host Configuration Protocol) is one of them which allows machine to receive IP dynamically. DHCP is unavoidable when the network size is changing and / or there is device mobility.
- Securing data against attempts of theft, destruction and other attacks.
- Data management in compliance with legal provisions.
- Assign appropriate rights to users and to enforce these rights.
- Managing Network File Systems.
- Maintenance and upgrade of hardware and software in a network.
- Creating and maintenance of infrastructure documentation since his duties are not only tied to technical activities. Indeed, the administration of a network infrastructure requires the existence of log information which describes the hardware and software components that need to be monitored as part of the administration: that is to say, all administered objects. The systematic documentation is part of the organizational aspects of network administration.

Conclusion

The network infrastructure has become a very high investment and a tool for productivity and competitiveness for the organization. Network administration is in need to get this infrastructure available and reliable.

Assessment

Which advantages does network administration have over computer administration?

Feedback

Computer administration is very important but in the period of internet where we need to access our information and/or resources with both remote and local access modes hence connecting computers which results into computer networks. For a standalone machine every malpractice is accomplished with only kinetic contact whereas with computer networks any malpracticing agent can remotely accomplish it, as a result there is a need to set procedures and activitiesto keep the beauty of computer network reliable.

DOMAIN ACTIVITIES

We will discover the range of tasks involved in network administration and the consolidation

carried out by the ISO for reference and ease of understanding.

NETWORK ADMINISTRATION ACTIVITIES.

Network administration and management are generally used as synonyms. Naturally, within the community there are different. In the late 1980s network management was the term used. Evolution has spent more frequent use of network administration. In all cases the activities or tasks required for the IT setting to function within the organization are numerous. The International Organization for Standardization (ISO) wanted to create visibility from the start by grouping these tasks in five areas also called eras:

Configuration Management: Includes all tasks related to the installation, identification and configuration of hardware and software components and services visible to network users.

Performance Management: Is responsible for supervision and the overall performance of the corporate network setting. To achieve the network administration there must be monitoring infrastructure and its components, take measurements and collect statistical data on the level of resource use, the charge level of traffic, communication flows and the occurrence of malfunctions in the network.

Fault Management: Includes activities relating to the detection, isolation and correction of abnormal functioning conditions that occurred in the network.

Accounting Management: Group tasks to answer the question of who uses this resource and to such an extent in the network. In other words, we must assign the users resource consumption for billing purposes or, if appropriate, to reallocate resources optimally among users.

Security Management: Is responsible for protecting the network, its resources and its users against attacks and other malicious activities that can come either from outside or from within. This includes ensuring the confidentiality, integrity and availability of data used in the network.

Conclusion

The tasks performed as part of network administration are many and it is almost not possible to memorize. ISO has grouped them for easy remembering, overview and understanding.

Assessment

What are network administration categories as per ISO?

Feedback

There are five categories as per ISO

1. Configuration management.
2. Performance management.
3. Fault management.
4. Accounting management.
5. Security management.

NETWORK ADMINISTRATOR PROFILE

This activity will allow us to discover the profile necessary to work successfully as a network administrator.

NETWORK ADMINISTRATOR'S KNOWLEDGE SCOPE

The working environment of the network administrator requires him to be sufficiently equipped technically, to be flexible and possess human competence. Indeed, network administrators working in varied environments include large companies, SMEs, academic institution, training institutions; government organizations, health, etc.The sensitivity and the challenges of the central aspects of the administration vary from one environment to another. In addition to technical skills network administrator possesses, he/she must also present some competences such as:

- Capacity to analytically resolve problems and communications.
- Ability to focus on details and to pay particular attention to some events.

- Ability to work independently as well as part of a team.
- Motivation to continue to develop the knowledge and to keep track to the latest technologies.

Note that in the chain of exploitation of the IT infrastructure, the network administrator is considered a last resort in solving problems or when one is looking for help. It is to him that are directed all the problems that have not been resolved at the level of assistance (Help Desk) or at the administrators of equipment and special systems.

Conclusion

Network administrator needs more than just technical skills but on top of technical skills he/she should be eager to learn, be flexible and possess human competences.

Assessment

What is the scope of network administrator's task?

Feedback

The network administration's scope involves:

- Technical skills
- Human competences
- Flexibility to adapt to changes in technologies and learning new technologies

ETHICAL ASPECT

Previous activities have allowed us to understand that the network administration requires impeccable technical skills. We will now find out that the requirements of this profession go beyond technical knowledge.

NETWORK ADMINISTRATOR'S ETHICS

The exercise of the network administrator has an ethical dimension that must be notified and the respect which must be taken. Ethics refers to all the principles of conduct that should govern life in a group of people. The moral that results can distinguish what is good and just what is wrong and unnatural. Ethically it is respect for the privacy of users and corporate interests that are the main concern in the context of administrative activities. In some two situations can be quickly in conflict. For example, network administration proceeds with the traffic analysis in relation to performance management or network security. This analysis can reveal some information on private and potentially incriminating communications of some people in the organization. Another example is in the ubiquitous mobile communication networks where some administrators can easily generate communication history of a given subscriber number. Such history can quickly reveal undesirable details on certain relationships

of the subscriber in question. In short, the network administrator has the privilege of having access to sensitive information about users and the company. Ethical requirements imposed on it to avoid any use of such information outside the strict framework of the exercise of its function and cannot fall without justifiable reasons in the hands of third parties, even if it comes from his superiors in the company.

Some codes of conduct for network administrator as per ethics:

- The integrity of a network administrator must be above all reproach.
- A network administrator should not violate user rights.
- The interactions a network administrator makes with all the people he/she can find in contact with must be maintained at the highest standards of professional behavior.
- Anytime the network administrator must demonstrate professionalism in executing his duties.
- Continued professional training is critical but a network administrator must remain on course.

Code shows that the network administrator can quickly end up in conflict with ethical standards if he/she does not have a strong personality.

Conclusion

Moral values are always encouraged for network administrators to accomplish their duties blamelessly. Having access on confidential information, it is possible to release them to the non authentic community but good ethic value will compel the administrator to open every piece of information and grant access to the authentic user.

Assessment

What are your ethic codes of conduct as network administrator in your organization?

Feedback

Good ethic values should be maintained on every operation performed by the network administration not forgetting access to every piece of information.

LEGAL ASPECT

The network administrator is responsible for what happens in the network of which he/she is responsible for. This responsibility is not limited to the ethical: it is also legal.

LEGAL BINDINGS TO NETWORK ADMINISTRATION

Indeed, some activities undertaken by the network administrator in connection with the exercise of his duties falls in legal follow-up. When the administrator reviews the traffic and the flow of communications he/she makes monitoring communications. When conducting security safeguards he/she makes archiving. And archiving as control communications are subject to the limits imposed by law. The modernization of the legislation to adapt to the digital era remains a challenge for many entities. However some countries already have legislation that sets a status for the network administrator, his rights and duties, as well as the implementation framework of certain administrative activities. The emerging trend known cases is that the law generally allows technical measures usually performed as part of network administration: filtering traffic by firewalls and other systems, electronic archiving, using sensors in places of network, and the use of log files (logs), etc. However, the network administrator is subject to the obligation of means to protect the privacy and confidentiality with respect to personal data he/she has access to: he/she can not disclose this data, even to his superiors.

Conclusion

The network administrator must demonstrate good moral character and a strong personality not to get tempted and violate the law. She/he should possess a character and a strong personality not to yield to temptation and violate the law. The law recognizes his/her rights but also imposes obligations.

Assessment

What actions/practices of a network administration that could lead to legal follow-u?

Feedback

The actions and practices numerous but the main can be disclosing companies data to non-authentic personnel and/or using information that she/he has access to in way different from the way the information has been planned to be used.

Unit Summary

Network infrastructure lies almost at the heart of every organization and institution well trained personnel should be available to administer it. This person should not ignore life's good ethics in practicing his duties and should also be aware of legal aspects that might involve his duties.

Unit Assessment

1. What is the motivation behind striving to become a network administrator?
2. What are the duties of the network administrator?
3. What is the place ethical and legal aspect in the network administration?

Grading scheme

The unit's assessments are graded out of 20% which are categorized as follows:

1. Activity assessments are out of 6%.
2. Unit assessment is out of 4%.
3. Unit test is out of 10%.

Feedback

1. Different companies, organization and governmental institutions around the world especially developed countries (but in developing countries this technology is developing very fast) depend computer networks to connect their employees and to keep the businesses flowing. All these networks need hard working men and women who are skilled to accomplish hands on approach to troubleshooting and maintaining these networks. This job is highly paying as well, hence the need for these individuals and remuneration for the job is a good motivation.

2. The duties of a network administrator include:

- Establish and maintain infrastructure.
- Installation and maintenance of network services that enhance network function. DHCP (Dynamic Host Configuration Protocol) is one of them which allows machine to receive IP dynamically. DHCP is unavoidable when the network size is changing and / or there is device mobility.
- Securing data against attempts of theft, destruction and other attacks.
- Data management in compliance with legal provisions.
- Assign appropriate rights to users and to enforce these rights.
- Managing Network File Systems.
- Maintenance and upgrade of hardware and software in a network.
- Creating and maintenance of infrastructure documentation since

his duties are not only tied to technical activities. Indeed, the administration of a network infrastructure requires the existence of log information which describes the hardware and software components that need to be monitored as part of the administration: that is to say, all administered objects. The systematic documentation is part of the organizational aspects of network administration.

3. Ethical and legal aspects remind the administrator on how to perform any technical operation. Good ethics will prohibit an administrator to perform any bad operation even if it is requested. While legal aspect will reveals the measures to be taken if the line is crossed while manipulating some operations or communication done in human networks.

Unit Readings and Other Resources

Required readings and other resources:

Charles P. Pfleege, S. L. (2007). *Security in Computing, Fourth Edition*. Prentice Hall.

Craig, H. (2002). TCPIP *Network Administration, 3rd Edition.* Sebastopol: O'Reilly Media.

Forouzan, B. A. (2007). *Data Communications and Networking. New York*: McGraw - HillCompanies.

Optional readings and other resources:

Charles P. Pfleege, S. L. (2007). Security in Computing, Fourth Edition. Prentice Hall.

Unit 2 : Network Services

Unit Introduction

Some network servers provide essential computer-to-computer services. These differ from application services in that they are not directly accessed by end users. Instead, these services are used by networked computers to simplify the installation, configuration, and operation of the network.

The functions performed by the servers covered in this chapter are varied:

- Dynamic leasing of IP address to workstation in saving effort and avoiding IP conflict
- Name service for converting IP addresses to hostnames
- Electronic mail services for moving mail through the network from the sender to the recipient.
- Web Servers that allows access to pages over HTTP protocol.
- File servers that allow client computers to transparently share files.
- Print servers that allow printers to be centrally maintained and shared by all users
- All of the services discussed in this chapter can be installed on one or several systems on your network. This leads to fact that the hosts on a TCP/IP networks are peers (all systems are equal).

Unit Objectives

Upon completion of this unit you should be able to:

- Define what a network service is.
- Identify different network services.
- Select the appropriate network service depending on the needed service.

Key Terms

Client: This is a hardware device or software that accesses services made available by a centralized machine to which it connects.

Server: This is centralized, powerful computer which serves other computers (clients) connected to it.

Service: This is an activated action on a machine to be consumed by a connecting machine so as to fulfill user's request.

Learning Activities

NETWORK ADDRESS TRANSLATION (NAT)

NATis an acronym for Network address translation. NAT exist as a result of existence of private networks and public networks. NAT is a router function where IP addresses of IP'sdata gramson a packet are replaced at the boundary of a private network. This is afeature that enables hosts on private networks to communicate with hosts on the Internet. NAT runs on routers that connect private networks to public internet (or simply internet).

PRIVATE AND PUBLIC NETWORK

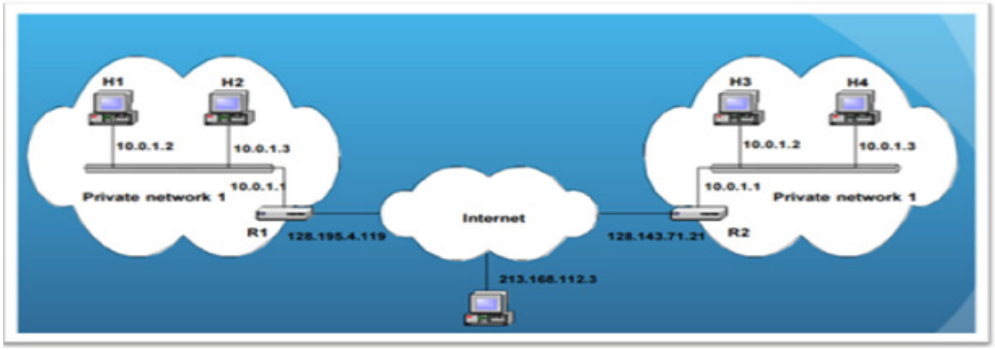
Private network came into existence to make IPv4 addresses to fit with the number communicating devices which use IP address in communication. IPv4 seems not enough to serve all communicating devices since every machine is having a unique IP address to communicate over the internet.

PRIVATE NETWORK

Private IP network is an IP network that is not directly connected to internet. IP addresses in private network can be assigned arbitrary without a guarantee to be globally unique. Generally, private networks use addresses from the following address range.

- **10.0.0.0** up to **10.255.255.255**
- **172.16.0.0** up to **172.31.255.255**
- 192.168.0.0 up to **192.168.255.255**

Below is a diagram showing private network:

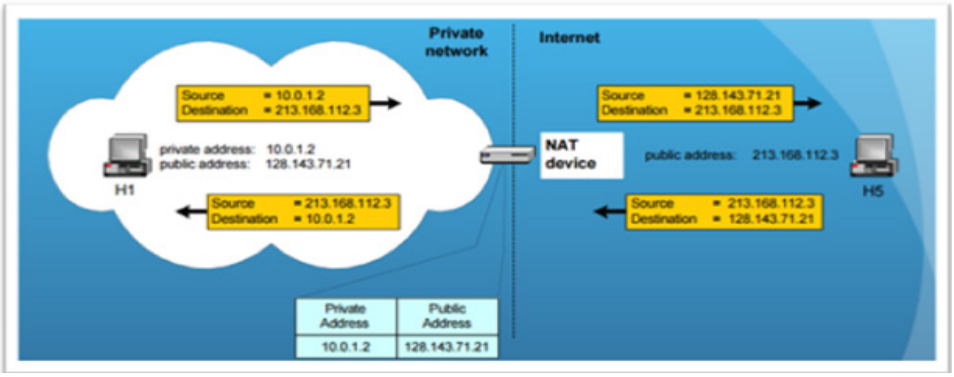


PUBLIC NETWORK

A public network is a type of network wherein a connected node in the general public has access and through it can connect to other networks or the Internet. For the public network to exist, connected nodes should be provided with public IP address where each IP address used is globally unique.

BASIC OPERATION OF NAT

NAT device has address translation table with which one to one translation is accomplished. The diagram below holds the details about basic NAT operation.



Conclusion

The NAT address resolution service has helped alleviate the shortage of IP addresses. In fact it masks the real address (Private IP) of the internal machines in communication with the outside in a more secure way. So, it is made to be used between two networks (be it private network to private network or private network to public network).

Assessment

What is NAT?

Feedback

NAT is a function of the router to translate the private IP address of the connected node to appear public so as to be able to communicate over internet as if that machine has public IP address. This service alleviated the shortage of IPv4 addresses.

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

DHCP is an acronym for Dynamic Host Control Protocol; it serves the dynamic assignment of IP addresses to the node(s). There are reasons to why dynamic assignment is desirable:

- IP addresses are assigned on-demand.
- Avoid manual IP configuration.
- Support mobility of nodes

DHCP CLIENT/SERVER COMMUNICATION

DHCP MESSAGE TYPE

While the client (which receives IP) and the server (which leases IP) are communicating, there are messages used which are included in the table below:

VALUE	MESSAGE TYPE
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNAK
7	DHCPRELEASE
8	DHCPINFORM

DHCPDISCOVER: This is a broadcast by a client to find available DHCP servers.

DHCPOFFER: Response from a server to a DHCPDISCOVER and offering IP address and other parameters.

DHCPREQUEST: Message from a client to servers that does one of the following:

- Requests the parameters offered by one of the servers and decline all other offers.
- Verifies a previously allocated address after a system or network change (a reboot for example).
- Requests the extension of a lease on a particular address.

DHCPACK: Positive acknowledgement from server to client with parameters, including IP address.

DHCPNACK: Negative acknowledgement from server to client, indicating that the client's lease has expired or that a requested IP address is incorrect.

DHCPDECLINE: Message from client to server indicating that the offered address is already in use.

DHCPRELEASE: Message from client to server canceling remainder of a lease and relinquishing network address.

DHCPINFORM: Message from a client that already has an IP address (manually configured for example), requesting further configuration parameters from the DHCP server.

CLIENT SERVER INTERACTIONS

The client broadcasts a DHCPDISCOVER message to all DHCP servers on the network. The DHCPDISCOVER message may include some options such as IP address suggestion or lease duration.

Each DCHP server may respond the client with a DHCPOFFER message that includes an available IP address and other configuration options. The servers record the address as offered to the client to prevent the same address being offered to other clients in the event of further DHCPDISCOVER messages being received before the first client has completed its configuration.

The client will receive one or more DHCPOFFER messages from one or more servers. In this case, the client chooses one based on the configuration parameters offered and broadcasts a DHCPREQUEST message that includes the server identifier option to indicate which message it has selected and the requested IP address option, taken from your IP address in the selected offer. In the event that no offers are received, if the client has knowledge of a previous network address, the client may reuse that address if its lease is still valid, until the lease expires.

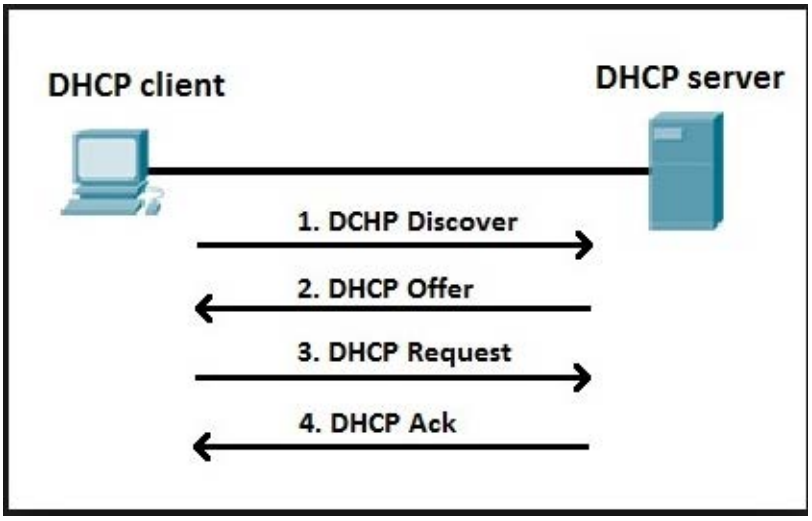
The servers receive the DHCPREQUEST broadcast from the client. Those servers not selected by the DHCPREQUEST message use the message as notification that the client has declined that server's offer. The server selected in the DHCPREQUEST message commits the binding for the client to persistent storage and responds with a DHCPACK message containing the configuration parameters for the requesting client.

The combination of client hardware and assigned network address constitute a unique identifier for the client's lease and are used by both the client and server to identify a lease referred to in any DHCP messages. Then your IP address field in the DHCPACK messages is filled in with the selected network address.

The client receives the DHCPACK message with configuration parameters. The client performs a final check on the parameters and notes the duration of the lease and the lease identification cookie specified in the DHCPACK message. At this point, the client is configured. If the client detects a problem with the parameters in the DHCPACK message (the address is already in use on the network, for example), the client sends a DHCPDECLINE message to the server and restarts the configuration process. The client should wait a minimum of ten seconds before restarting the configuration process to avoid excessive network traffic in case of looping.

On receipt of a DHCPDECLINE, the server must mark the offered address as unavailable. If the client receives a DHCPNAK message, the client restarts the configuration process.

The client may choose to relinquish its lease on a network address by sending a DHCPRELEASE message to the server. The client identifies the lease to be released by including its network address and its hardware address.



DHCP server and DHCP client communication

Source: http://study-ccna.com/dhcp-dns/

LEASE RENEWAL

When a server sends the DHCPACK to a client with IP address and configuration parameters, it also registers the start of the lease time for that address. This lease time is passed to the client as one of the options in the DHCPACK message. The client is rightfully entitled to use the given address for the duration of the lease time. When timer for the lease time expires, the client will send a DHCPREQUEST (unicast) to the server that offered the address, asking to extend the lease for the given configuration. The client is now in the RENEWING state. The server would usually respond with a DHCPACK message indicating the new lease time, and the timer is reset at the client accordingly. The server also resets its record of the lease time. Under normal circumstances, an active client would continually renew its lease in this way indefinitely, without the lease ever expiring. There are two timers T1 and T2 where the renew takes place at the expiration of T1 followed by DHCPREQUEST initialized and responded with the DHCPACK. If no DHCPACK is received until timer T2 expires, the client enters the REBINDING state. Client now broadcasts a DHCPREQUEST message to extend its lease. This request can be confirmed by a DHCPACK message from any DHCP server on the network. If the client does not receive a DHCPACK message after its lease has expired, it has to stop using its current TCP/ IP configuration. The client may then return to the INIT state, issuing a DHCPDISCOVER broadcast to try and obtain any valid address.

Conclusion

For a small network is possible give IP address to every machine and remember it in order to avoid IP conflict that arises as a result of assigning one IP address to more than one machine. But when the network size keeps changing and growing, it becomes hard. DHCP serves to dynamically assign IP address to every connected machine and insures no IP conflict.

Assessment

What is DHCP?

Feedback

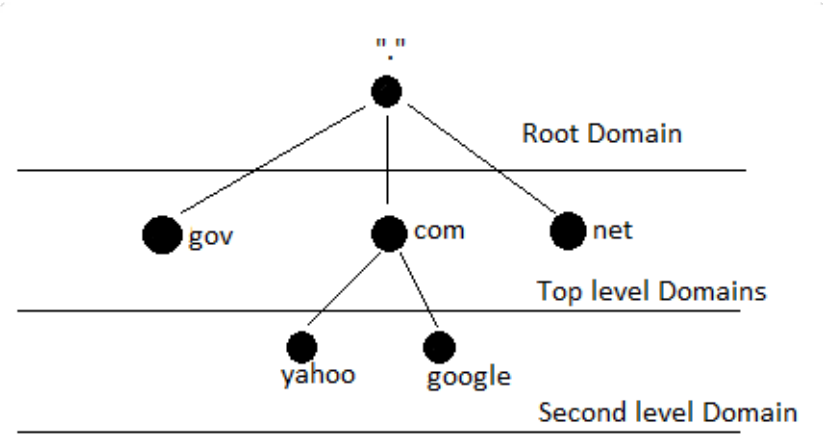
This is Dynamic Host Configuration Protocol used to dynamically assign IP address to the nodes which are connected on the network in a manner assuring that each node has a unique address. Each node uses an IP for a lease time and after it expires the renew process takes on and if renew fails completely, INIT state is entered.

DOMAIN NAME SERVICE (DNS)

DNS is an acronym for Domain Name Service which serves host name to IP address translation service. An issue would rise as to why translate if access with IP address is possible? It is easier to remember a host name than it is to remember an IP address (a 4 Byte number). Practically, applications such as HTTP and Email use DNS. They all require the user to input a destination, user types host name then it is the role of DNS to translate this name to an IP address.

DNS HIERARCHY

DNS is a distributed database implemented in a hierarchy of name servers. The diagram below shows the DNS tree.



DNS Tree

Following this hierarchy, the communication which intends address translation by DNS servers is followed. Here we shall take a scenario for "www.google.com" translation;

- The client queries a root server to find "com" DNS server.
- The client queries "com" DNS server to get "google.com".
- The client queries "google.com" DNS server to get IP address for "www.google.com".

A. DNS: Root name servers

Like the name implies, it is at the root of the tree contacted by local name server that cannot resolve name. Root name server contacts top level domain servers and returns mapping to local name server.

B. Top-Level Domain Servers (TLD).

Top level domain servers for com, org, net, mil, edu, etc, and all top level country domains. For all domain names in lower levels, it is the last part of the domain name. That is, the last label of a fully qualified domain name. For example "www.avu.org ", org is the top level domain.

C. LOCAL NAME SERVER

The name local reflects where this server resides; here we are talking about the client's side where the request is initiated from. The local name server does not strictly belong to the hierarchy but each residential ISP, company, university, etc has one which is also called "default name server". Local name server (or default name server) receives DNS query made by hosts in that network after which it forwards to the hierarchy.

DNS QUERY

DNS queries can be recursive or it can be iterative.

A. ITERATIVE QUERY

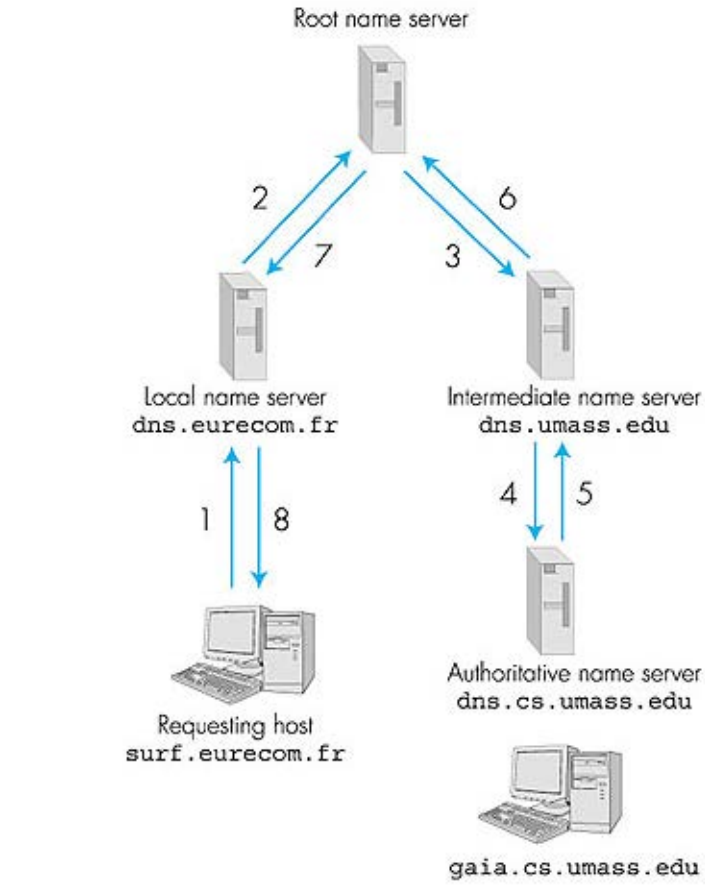
An iterative name query is one in which a DNS client allows the DNS server to return the best answer it can give based on its cache or zone data. If the queried DNS server does not have an exact match for the queried name, the best possible information it can return is a referral (that is, a pointer to a DNS server authoritative for a lower level of the domain namespace). The DNS client can then query the DNS server for which it obtained a referral. It continues this process until it locates a DNS server that is authoritative for the queried name, or until an error or time-out condition is met. The figure below describes the DNS iterative query.

B. RECURSIVE QUERIES.

With a recursive name query, the DNS client requires that the DNS server respond to the client with either the requested resource record or an error message stating that the record or domain name does not exist. The DNS server cannot just refer the DNS client to a different DNS server. Thus, if a DNS server does not have the requested information when it receives a recursive query; it queries other servers until it gets the information, or until the name query fails. We can view it from the figure below.

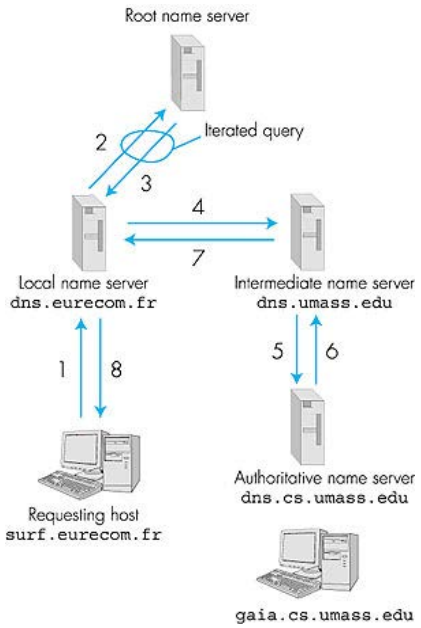
The recursive query puts burden of name resolution on contacted root name server which leads to heavy load.

Contacted server replies with name of server to contact.



DNS Recursive query

Source: http://netlab.ulusofona.pt/rc/book/2-application/2_05/index.htm



DNS Recursive query

Source: http://netlab.ulusofona.pt/rc/book/2-application/2_05/index.htm

Conclusion

If DNS was not in place we could not have been able to use names such as www.avu.org or www.google.com but instead we could be using numbers like 8.8.8.8 which is hard to remember but DNS serves the translation. We give it a name it maps the right number.

Assessment

Why do we need host name translation to the IP address?

Feedback

It is possible to access Google by typing http://8.8.8.8/ even other resources can be accessed using http://IP_address/application. For the IP address is always a number (4bytes which are separated by a dot and each bytes is composed of a value that ranges from 0 to 255) which is hard to remember. The DNS serves to translate these numbers to human natural language to ease the work remembering. Nodes understand IP addresses but human beings easily remember their natural language strings, it is the role of DNS to translate human understandable in the machine understandable and the vice versa.

WEB SERVER

A web server is a computer with special software to host web pages and web applications. This is computer that provides Web services and pages to intranet and Internet users. A web server serves web pages to clients across the Internet or an Intranet. The web server hosts the pages, scripts, programs, and multimedia files and serves them using HTTP, a protocol designed to send files to web browsers and other protocols. A number of server-side technologies can be used to increase the power of the server beyond its ability to deliver pages (for example; HTML pages, JSP pages)

WEB SERVER INTERACTION

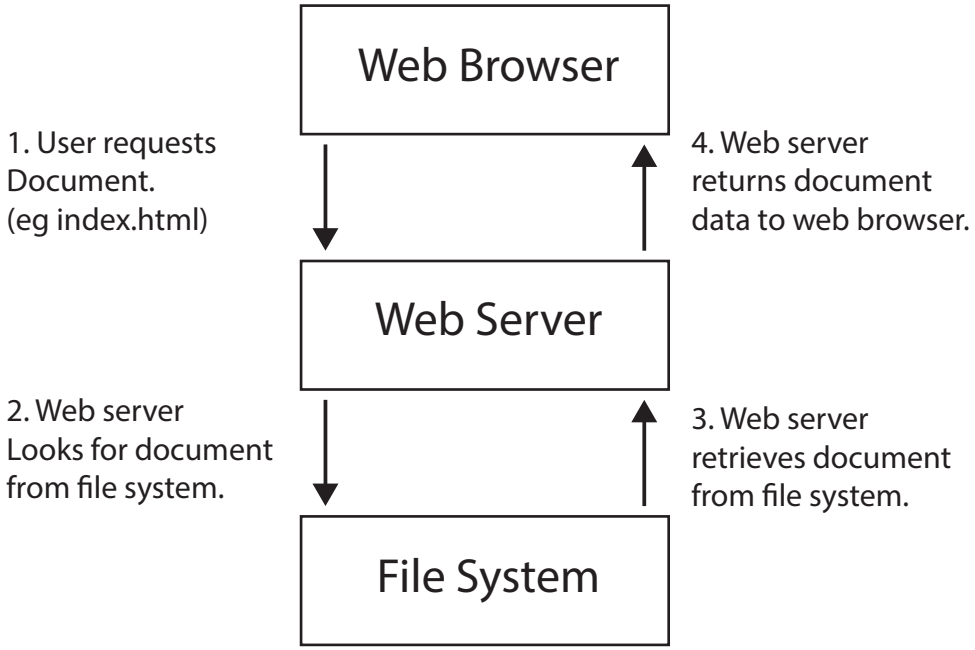
The web server seats between web browser and the file system that needs to be accessed. A Web Browser acts as an interface between the user and the Web server. The browser carries out the following on behalf of the user

- Contacts a web server
- Sends a request for information
- Receives the information and
- Displays it on the user's computer

The web server seats between the browser and the file system where it carries out the following:

- Receives the request from the browser.
- Looks for the requested file from file system.
- Receives the response from the file system.
- Returns the response to the browser.

The figure below holds all the details for web server interaction.



Web Server interaction

For example, if you open your browser and enter the following url "www.avu.org/index.html" this sends a request to the Web server whose domain name is "avu.org". The server then fetches the page named "index.html" and sends it to your browser. Any computer can be turned into a Web server by installing server software and connecting the machine to the internet. There are many Web server Programs which include: Apache web server, Microsoft Internet Information Server, Google Web Server, etc.

Conclusion

This is a service that is put on one machine and gives it the capability to serve web pages to other remote machine. Without this service we cannot be able to browse all the websites that we browse. The only trick in doing this is to install that service on the machine that will be serving such services.

Assessment

Which web servers are you familiar with? And how does work?

Feedback

There a lot of web servers available out there such as; apache tomcat, xampp, easyPhP, etc. Once this software is installed on the machine it gives this machine to be accessible by other machine connected on the network in which that machine is accessible. The web server has a folder in which web pages and web application are put for the remote access to be possible. For tomcat the folder is WebApp, for easyPhP the folder is www, for xampp the folder is htdocs, etc.

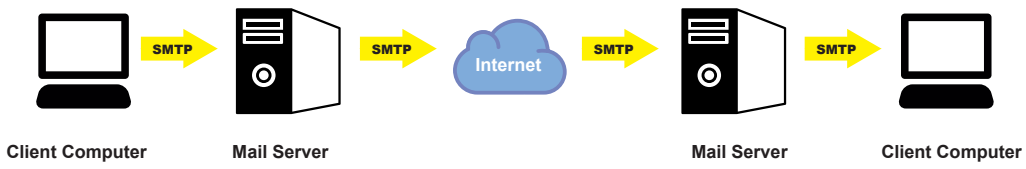
MAIL SERVER

A mail server (sometimes also referred to an e-mail server) is a server that handles and delivers e-mail over a network, usually over the Internet. A mail server can receive emails from client computers and deliver them to other mail servers. A mail server can also deliver emails to client computers. A client computer is normally the device where you read/write your e-mails, for example your computer at home or in your office, your Smartphone, your tablet and iPad, all can be regarded as a client computer in these circumstances.

SENDING AND DOWNLOADING EMAILS

Mail server starts its journey after the message is composed, when the sender presses the "Send" button in your e-mail program (e-mail client) the program will connect to a server on the network / internet that is called an SMTP server. SMTP is an acronym for Simple Mail Transfer Protocol and it is a protocol that is used when emails are delivered from clients to servers and from servers to other servers.

When the receiver downloads emails to their e-mail program the program will connect to a server on the network / internet that is known as a POP3 server. A POP3 server uses a protocol named POP3 for its communication. POP3 is an acronym for Post Office Protocol version 3. The figure below illustrates the details.



Mail sender and recipient communication

When the sender sends an e-mail from his local computer to a mail server, the e-mail has just started its journey to the recipient despite the distance that is separating them. Before the mail server (SMTP server) that your e-mail program communicates with knows where to deliver the e-mail message sent, it will examine the e-mail address that you have specified as a receiver of the message. The mail server will extract the domain name of the e-mail address and use it to locate the mail server (POP3 server) that your receiver's client computer communicates with. The domain name is found after the "@" character in an e-mail address. If for example

the e-mail address is student@avu.org, the domain name is avu.org. By using this domain name as an address the mail server will find which mail server on the Internet to deliver the e-mail message to. When the server has been identified and it has responded that it will accept an e-mail delivery, the email is sent to this server. Now that the message has reached the destination mail server (POP3 server) it is downloaded to the receiver.

Conclusion

Friends, family members all around the world open their computer, compose emails and send them; in a time of blinking we receive the message despite the distance. But there is a service which makes this possible and that is email service. This service uses SMTP protocol to send the message to the destination server, and the recipient use uses POP3 to download it to his inbox.

> ### Assessment
>
> How does SMTP differ from POP3?

Feedback

SMTP protocol sends an email from its source and gets it through all the nodes which are intermediate until it reaches the final destination server and there SMTP completes its job where by the remaining job is download the email from that node to the inbox and this remaining job is accomplished by POP3.

FILE AND PRINT SERVER.

The two network services discussed here; file and print services, make the network more convenient for users. Not long ago, disk drives and high-quality printers were relatively expensive. Today every system has a large hard drive and many have their own high-quality printers, but this will never eliminated the need for sharing resources. File servers allow users to store important files at a central location in the network from which it's easy to add security and to allow users to share files. A file server also typically offers a print service, which provides an easy and convenient way to share printers on the network.

FILE SHARING

File sharing is not the same as file transfer (the ability to move a file from one system to another). A true file-sharing system does not require you to move entire files across the network. It allows files to be accessed at the record level so that it is possible for a client to read a record from a file located on a remote server, update that record, and write it back to the server - without moving the full file from the server to the client. Through file sharing, users and programs access files located on remote systems as if they were local files. In a perfect file-sharing environment, the user neither knows nor cares where files are actually stored. The network administrator will have to choose the type of file server to accomplish file sharing, very many options are available but NFS (for Linux clients) and Samba (for Windows clients) are the two most popular.

PRINTING SERVICES

This is a useful network service which allows printers to be shared by everyone on the network. The advantages of sharing printers are as follows:

- Fewer printers are needed, and less money is spent on printers and supplies.
- Reduced maintenance. There are fewer machines to maintain, and fewer people spending time fiddling with printers.
- Access to special printers. Very high-quality color printers and very high-speed printers are expensive and needed only occasionally. Sharing these printers makes the best use of expensive resources.

Conclusion

Having a computer which cannot share some files to your colleagues and for every computer is having its own connected printer would be expensive and boring. File sharing and printer sharing cuts on expenses and saves some energy.

Assessment

Why is it important to share files and printers?

Feedback

Administrator's effort is saved since one machine is maintained instead of maintaining many printers one is in place. Not only that, but the cost as well minimized where instead of buying many printers the company buys one printer. Since files can be centralized them the cost of sharing are minimized to the extent that they can be completely removed in some contexts.

Unit Summary

Network services have been growing increasingly aiming to simplify network installation, configuration and use. The network administrator will have to acquire enough knowledge about network services such that he/she can provide the needed service in the organization which leads to proper utilization of resources.

Unit Assessment

1. What is a service? Support the answer with an example.
2. What is the best service of all services?
3. What is the beauty of sharing resources?

Grading scheme

The unit's assessments are graded out of 20% which are categorized as follows:

- Activity assessments are out of 6%.
- Unit assessment is out of 4%.
- Unit test is out of 10%.

Feedback

1. A service is an activated action on one machine to be consumed by another machine. A connecting machine (a client) makes a request and waits for the response to achieve its tasks. For example; web server, sharing resources, IP dynamic assignment, etc.

2. There is no best and there is no bad service because the beauty of every service lies behind the need for it. Every service is specific on some action and if it can accomplish it as needed then that service is considered good or best and it be considered on bad side if it cannot achieve what it is not expected to achieve.

3. Sharing a resource means the use of few resources to achieve the same output as more resources can achieve. The total cost spent on resource is hence minimized having in mind that the output will not be crippled.

Unit Readings and Other Resources

- Jang, M. (2009). Ubuntu Server Administration. New York: McGraw-Hill Companies.
- Forouzan, B. A. (2007). Data Communications and Networking. New York: McGraw - HillCompanies.
- Hunt, C. (2002). TCPIP Network Administration, 3rd Edition. Sebastopol: O'Reilly Media.

- Optional readings and other resources:

- Hunt, C. (2002). TCPIP Network Administration, 3rd Edition. Sebastopol: O'Reilly Media.

Unit 3 : Network management Tools

Unit Introduction

The services provided by the networks must reach an optimal level or nearly optimal quality because otherwise we risk great frustration with users and administrators. Apart from frustration, installation effort as well as the expenses incurred might be used improperly while the network might still not reach satisfaction. It is essential to adopt tools and mechanisms for monitoring and correcting abnormal situations that may arise during the operation, in order to increase the degree of assurance that the service adequately received by its users. This unit is dedicated to the presentation of the main concepts related to measurement and monitoring computer networks. In the end, we provide a few tools for monitoring and control networks, such as Cacti, Nagios, Dude and NTOP.

Unit Objectives

Upon completion of this unit you should be able to:

- Propose a set of solutions that improves network performance.
- Select and propose a set of network management tools.
- Analyze the traffic and packets in computer networks.
- Monitor and manage the computer network via SNMP.

Key Terms

Monitoring: It is the continuous control activity of the computer network by measuring the state of various parameters of devices.

Management: This is the set of actions to control, plan, allocate, implement, coordinate and monitor network resources.

Control: This is the action taken by the administrator intending to adjust the network devices or services to enhance performance.

Metrics: The metrics are related to speed parameters, accuracy, system availability, error rate and volume of work produced.

Learning Activities

ADMINISTRATION ARCHITECTURE

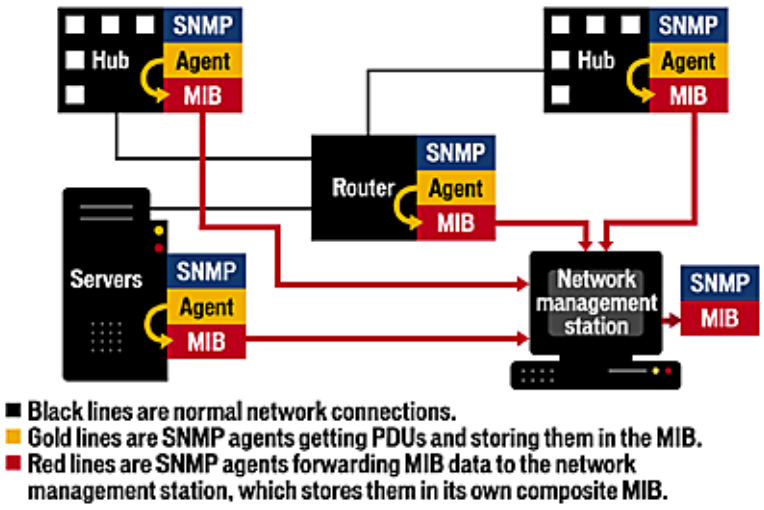
The administration architecture identifies the functions, components, and the organization of administrative tools. In order to proceed with the standardization of a generic architecture for network management, some international organizations presented models and management architectures. Currently, networking architectures are highly polarized around three solutions that are discussed in this unit.

NETWORK MANAGEMENT ARCHITECTURE

This concerns administration or management of a local network in a manner that will anticipate, identify and correct malfunctions. The basic operations performed by such a system can be grouped into:

- Data collection.
- Data processing.
- Taking corrective measures.

The exchanged notification and commands between management entities take place according to a specific management protocol; On the other hand, the exchanged information implies various operational parameters, relating to a specific entity, a set of entities, or communications infrastructure.



Network management architecture

Source:

http://userscontent2.emaze.com/images/9c66ff34-e8cc-402e-b6fa-d7a59f804827/baf0086a-9246-45bc-8b6f-17cdefa6cb3fimage6.png

OSI MANAGEMENT MODEL

Early in the development of network management the International Organization for Standardization (ISO) has developed an organizational framework within which administrative activities have been grouped into five areas or areas.

- Fault Management: In Fault Management, the aim is to recognize, isolate and correct log faults on the network. As System and Network Administrator, it is your duty to put in place monitoring tools so you are alerted to when faults exist. For example, you want to be alerted when a critical service goes down on the network. If there is a fault, you have to test, fix, update, and repair any faults that occur on the network.
- Configuration Management: One of the main issues which cause a system to fail is when someone changes a configuration setting. Configuration management facilitates the control of any system configuration both on the hardware and software side. It is important that you record all configuration changes such as what has been changed, why and who did the change; and document system configuration standards. If a fault does arise (it may not be instantly, but a couple of months later), you can track who completed the configuration change.
- Accounting Management: Accounting Management is concerned with aspects of the system users. It mainly focuses on charging and billing users for services they consume, and regulating service use.
    - For example, some organizations charge its users or departments on:
        - Printing Internet/Bandwidth
        - Disk space
        - CPU
        - Application and software use.

Therefore, it is important to implement ways to properly charge use of IT facilities.

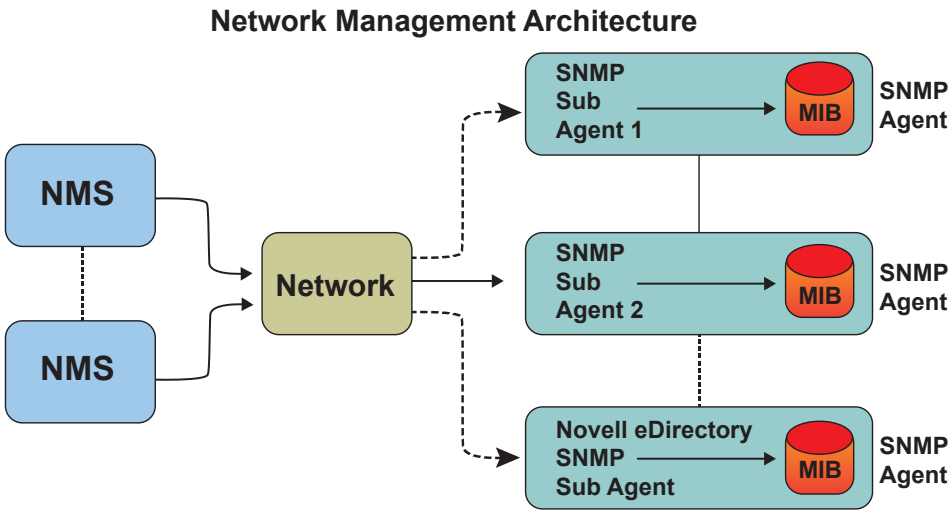
- **Performance Management:** Performance Management involves analyzing your network and gather information so that you can prepare it for the future. The performance of a network varies all the time. Most organizations find that the internet is very slow during lunch as many of the staff is browsing the internet, yet in the morning, it will be super quick. Not only this; but the performance of the network must meet the users and organizations desires. The network and systems services must be available, the speed must be efficient, there must not be bottlenecks and the network should never be used to its maximum capacity for prolonged period of times. System and Network Administrators must actively monitor the network performance to ensure problems do not occur.
- **Security Management**: Security management is important as you control user's access to network resources. Without it, your network will be exposed, as well as all the information and document it contains. As a Network and System Administrator, you are to address network authentication and security auditing to detect and prevent network sabotage, abuse and to prevent unauthorized access.

The administrators are required to:

- Records logs.
- Have a firewall setup.
- Control spam.
- Prevent viruses, Trojans, spyware.
- Upgrade software, install OS patches.
- Implement authorization techniques and password control.

SNMP MANAGEMENT ARCHITECTURE

The SNMP architecture is essentially based on the network management protocol of the same name. SNMP stands for Simple Network Management Protocol and designate a specialized network administration protocol that is currently in version 3 (SNMPv3)



SNMP Management architecture

Source: https://www.netiq.com/documentation/edir88/edir88/data/ag7hbgr.html

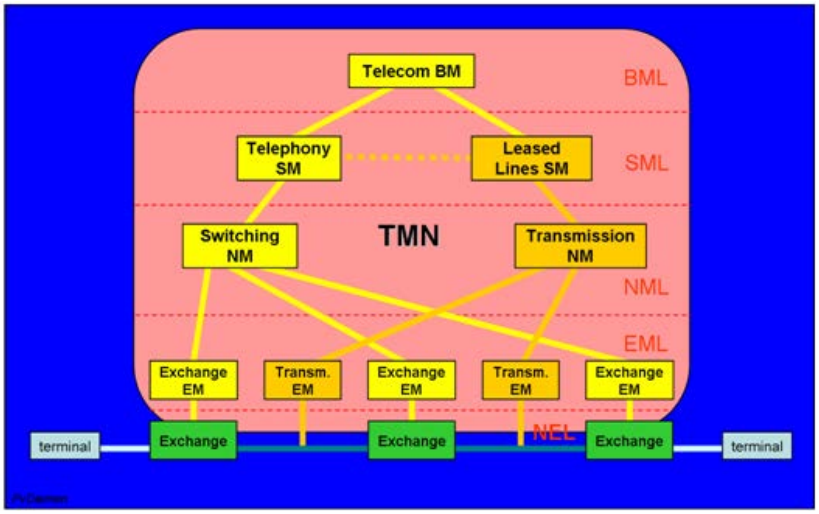
- **SNMPv1** This is the standard version of SNMP, defined in RFC 1157. Which is based on communities, which are nothing more than password: plain text string that allows any SNMP-based application (which recognizes the string) to have access to device management information. Usually, there are three communities SNMPv1: Read-only, read-write and trap.
- **SNMPv2** It is the second version of the SNMP protocol. This version has improvements over the first version SNMPv1 including additional operations, performance improvement, security and communication settings between NMS.

- **SNMPv3** This differs from other versions of SNMP with regard to three major services: authentication, privacy and access control. These services can be used by SNMPv3 in an organized and efficient manner; the agent software allows the creation of security policies that are used at authentication, privacy and access control. The SNMPv3 is composed of modules, and each entity has an SNMP mechanism. This mechanism implement various functions, for example: sending messages, control access to objects, authentication and encryption of messages.

Communities in SNMP allowdefining reliability between NMS and agents. An agent is configured with three community names: read-only, read-write and trap. The community names are basically keys to restrict certain types of operations. Most equipments that SNMP are configured with default community strings, usually public for read-only community and private for read-write community.

TMN MANAGEMENT ARCHITECTURE

The Telecommunication Network management (TMN) provides operations and management mechanisms for telecommunications networks. In particular, the system was developed so as to perform control and monitoring of telecommunication networks, it includes fault monitoring functions, performance Analysis, routing control and configuration, taxation and control access. TMN provides a framework for achieving interconnectivity and communication across heterogeneous operations system and telecommunication networks. To achieve this, TMN defines a set of interface points for elements which perform the actual communications processing (such as a call processing switch) to be accessed by elements, such as management workstations, to monitor and control them. The standard interface allows elements from different manufacturers to be incorporated into a network under a single management control.



TMN Architecture

Source:

(http://www.van-diemen-de-jel.nl/TMN/LLA/LLA_example.png)

This architecture has three distinct architectures:

- Functional Architecture: These are functional modules or simply blocks which act as reference points between modules.
- Physical architecture: These are physical interfaces between blocks.
- Informational architecture: This concerns information exchange between entities.

Conclusion

The administration architectures representing the basis for the creation of administrative tools, whether software, hardware or hybrids. The architecture discussed in this activity are SNMP and TMN.

Assessment

What is the difference between SNMP and TMN architecture?

Feedback

TMN is based on heterogeneous networks interconnectivity whereas SNMP is based on NMS and agents

ADMINISTRATION VIA WWW.

Local networks are inherently heterogeneous. It is common the coexistence of components from different manufacturers, resulting from the implementation of different technologies or implementing different standards. The administration of such a network is generally carried out using a combination of multiple tools from different vendors. The administrator of a network of this type needs to use a variety of tools, depending on the variety, or acquire a general approach to solution.

Administration based on the WWW (World Wide Web) took advantage of the popularity of the web interface. The commonness of browsers and the current trend for the integration of multiple services enables the coexistence of various types of information in a local or distributed manner. These features make the web the appropriate technology for the integration of different management solutions, whether standard or proprietary.

Conclusion

There are a lot of different tools available for network management but you will find that each is proprietary to one or few technologies applied but WWW based management takes the advantage of HTTP protocol to work on heterogeneous environment.

Assessment

Identify tools which are used to manage networks based on web technology?

Feedback

One most used network management tool to that uses browser software is nagios, once this tool is installed and its database in installed it is accessed from the browser.

NETWORK MANAGEMENT PROTOCOL

Network management protocols are responsible for ensuring communication between network resources that are increasingly heterogeneous. Some network management protocols are includes: CMIP (Common Management Information Protocol), the SGMP (Simple Gateway Management Protocol), the SNMP (Simple Network Management Protocol), and the o RMON (Remote Network Monitoring). However, the SNMP network management protocol will be covered in more detail.

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

The development of this protocol started 1988. It is a standard from the IETF (Internet Engineering Task Force). The aim of development was to manage a growing number of network elements in a computer network. Gradually this protocol started to become popular and now forms the basis of network management. With SNMP, you can retrieve information about the components operating in the network such as routers, printers, hubs, or even normal computers.

Below are some examples of the type of information that can be retrieved:

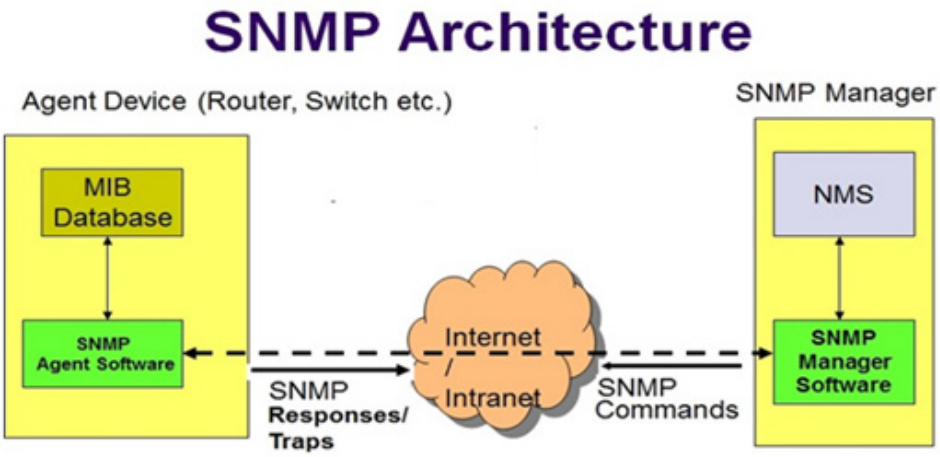
- System clock.
- Processor usage.
- Hard disk usage.
- Network usage.

In addition to recalling components configuration, SNMP also allows sending configuration data to them. Despite being simple in design and approach, the power of this protocol as a network management tool was confirmed in practice.

The SNMP-based network management architecture consists of the following elements:

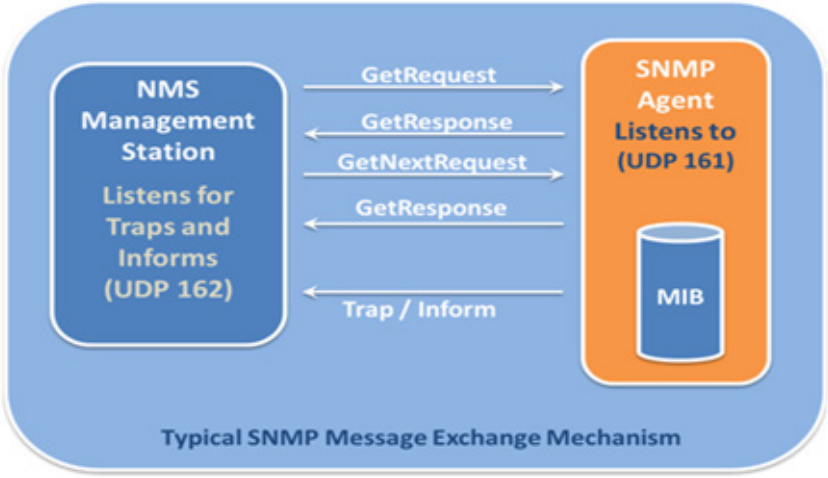
- NETWORK MANAGEMENT STATION (NMS): This is a machine (server) that runs a network management application. All network elements communicate with the NMS to relay management and control information. The NMS also enables network data analysis and reporting.

- AGENT: This is a program running on a network that performs a task on behalf of some other entity (like a person or larger program). It can be monitored by the NMS.
- POLLING: This is the continuous checking of agents to see what state they are in, usually to see whether they are still connected or want to communicate.
- TRAPS: This is an asynchronous notification from agent to manager. The agent notifies the NMS of the significant event happened.



SNMP Architecture client/server model

(Source: http://computernetworkingsimplified.com/wp-content/uploads/2014/02/snmparchitecture1.jpg



NMS and Agent message exchange

Source: http://blog.ipexpert.com/wp-content/uploads/2012/06/SNMP_TRAFFIC1.png

PERFORMANCE ANALYSIS

Each performance evaluation study, a set of performance criteria and measures should be chosen. One way to prepare this set is to list the services offered by the system. Different results are returned. In general, these results can be classified into three categories: the system is performing correctly, incorrectly or does not operate. If the system works correctly, your performance is measured by the time required to perform the service, the speed at which the service is performed and the resources consumed during the execution of the service. These parameters are named; response time (reactivity), productivity, and use. If the system runs the service incorrectly, there is said to be an error. It is useful to classify errors and to determine the probabilities of each class of errors. If the system fails to operate a service, it is considered unavailable. Again, it is useful to classify failure modes or unavailability and determine the probability of each class of errors. The measures associated with the three outcomes, namely the successful service, error and downtime, are also called speed indicators; speed, reliability and availability.

PERFORMANCE METRICS:

It is very important to keep in mind what should be measured to obtain the desired result analysis. There are three methods that are used to obtain data on the network: query network devices for stored information, observe network traffic signs which affect network performance, plus generation of test traffic and send it in the network to test its performance. We describe below the measures studied in this work:

- Throughput: This is the rate of production or the rate at which something can be processed. This is the rate of successful message delivery over a communication channel in some time intervals. For interactive systems, the flow is measured in requests per second, CPU, the flow is measured in millions of instructions per second (MIPS), in computer networks, throughput is measured in packets per second (pps) or bits per second (bit/s), etc.
- Round Trip Time (RTT): It is the length of time taken for a signal to be sent plus the length of time taken for an acknowledgment of that signal to be received. The asymmetry of roads and loading systems involved in each direction, is only approximation.
- Packet Loss: This is defined as when one or more packets of data travelling across a computer network fail to reach their destination. It is the index that measures the success rate of the transmission of packets between two network points. It is usually expressed as a percentage, indicating the percentage of lost packets. And the lower the packets loss the greater network efficiency is.

MONITORING METHODS:

Measurements carried out on the operational of the network provide useful information on the performance and characteristics of the traffic: Common measurement methods can be classified into two categories:

- Passive measures. Active measures.

The passive measurement is to observe the traffic that passes through the selected points within the network. Analysis of data collected allows us to know the use and traffic characteristics. We speak of passive in this approach because data collection did not significantly alter circulating traffic on the network. Most network measurement tools fall into this category. Unlike the passive measurement, the active measure as test packets in the network. Also referred to as intrusive. The number of additional packets injected into the network must be limited to not overly consume network resources and skew performance that one would like to measure.

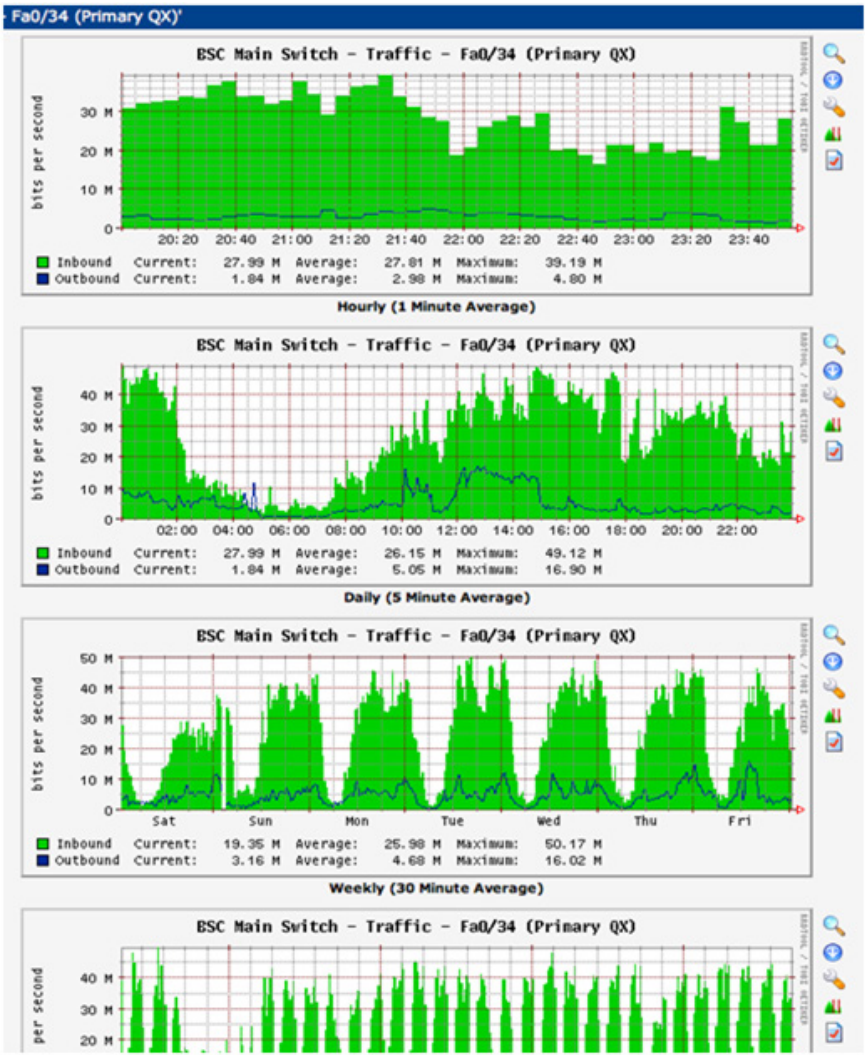
MONITORING TOOLS

A monitoring tool or surveillance function is to collect performance data on systems using a protocol. In addition, it also conducts analysis of received data and interprets the results to the network administrator. Some common monitoring tools there are: specialized software, specialized hardware, firmware, and hybrid systems. In general, monitoring tools based on software are much cheaper than those comprising hardware components.

EXAMPLES OF MONITORING TOOLS

To measure the performance of a network, we have to make a choice of metrics, methods and tools. After selecting the parameters that will be analyzed and methods to use, the next step is to choose the tools for collecting analyzed data. The data is then displayed according to the metric in graphs or tables. We present below some of the commonly used monitoring tools:

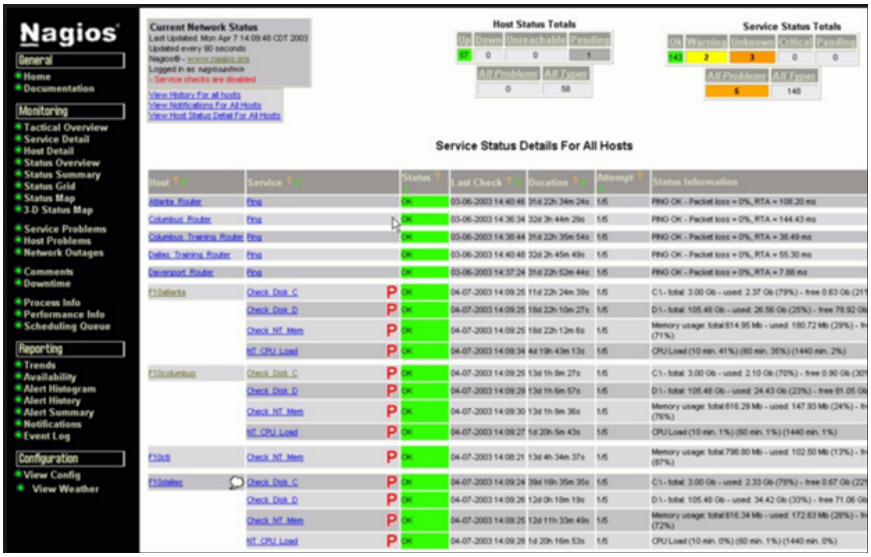
Cacti: Cacti is a web-based network monitoring and graphing tool designed as a front-end application to poll parameters of running services on the network. It collects data on computer network, retrieves information about the network status, and displays to the graphical user interface (GUI-browser). It was designed with a goal of flexibility, so it easily adapt to different needs, while being easy to use. With this tool, you can monitor the status of network elements, applications, bandwidth and CPU usage. Behind Cacti there is RRDTool which is powerful tool to analyze the data. After analyzing it stores all the necessary information and generate the graph from its database. The interface of Cacti is purely in PHP, and keeps several graphs. Cacti uses SNMP to query the information from components and / or software that support this protocol. Its architecture is open and allows plug-ins that add new features as per installed plugin.



Traffic flow generated by Cacti

Source: http://www.whitakerfamily.ws/blogs/jason/wp-content/uploads/2010/11/qxgraph.jpg

- Nagios: An open source software that monitors services. Nagios offers monitoring and alerting services for servers, switches, applications and services. It alerts users when things go wrong and alerts them a second time when the problem has been resolved. It monitors service such as HTTP, FTP, SSH, PING, SMTP or POP3. The figure below shows how nagios works.



Nagios working interface

Source: http://books.tag1consulting.com/sites/default/files/nagios-pic.png

ntop: It is a tool that has a graphical interface for managing and visualizing information to better understand network status.

Conclusion

Different monitoring tools are in place; it calls upon some one's choice and experience to choose the one that he/she is comfortable with. But all the tools have in common the following: collecting data, processing data and populating the component or network status in order for the administrator to take decision.

Assessment

How does SNMP protocol achieve network management function?

Unit Summary

In this unit, we discussed aspects related to the computer networks administration, surveillance and monitoring. We presented a number of available network administration tools, including SNMP protocol. The main concepts related to SNMP were presented. The methods of performance measurement and the possible metrics were also discussed.

Unit Assessment

1. Describe network management by grouping basic operation?
2. What is the beauty lying behind use of administrative tools based on www?
3. Identify some information that can be retrieved while acquiring information for network monitoring?

Grading scheme

The unit's assessments are graded out of 10% which are categorized as follows:

1. Activity assessments are out of 3%.
2. Unit assessment is out of 2%.
3. Unit test is out of 5%.

Feedback

1. Basic operations are grouped into 3:

    - Data collection.
    - Data processing.
    - Taking corrective measures.

2. Most of networks are heterogeneous in nature. This means that while monitoring a component would require its native platform. By avoiding use of many platforms, it is worth taking one tool that do what many can accomplish hence www tools are better suiting in heterogeneous networks.

3. When acquiring information for monitoring purposes the following parameters are retrieved:

    - System clock.
    - Processor usage.
    - Hard disk usage.
    - Network usage.

Unit Readings and Other Resources

Required readings and other resources:

- Cisco. (2016, February 27). networkers/nw03/presos/docs/NMS-1001.pdf. Retrieved February 27, 2016, from http://www.cisco.com/: http://www.cisco.com/networkers/nw03/presos/docs/NMS-1001.pdf
- Pras, A. (2016, February 27). ~jakab/edu/litr/TMN/Network_Management_Architectures_extr.pdf. Retrieved February 27, 2016, from http://www.hit.bme.hu/: http://www.hit.bme.hu/~jakab/edu/litr/TMN/Network_Management_Architectures_extr.pdf
- Thomas A. Limoncelli, C. J. (2007). *The Practice of System and Network Administration Second Edition*. Boston: Addison Wesley.

Optional readings and other resources:

- Thomas A. Limoncelli, C. J. (2007). *The Practice of System and Network Administration Second Edition*. Boston: Addison Wesley.

Unit 4 Secure Hardware And Application

Unit Introduction

Network here is referred to as the connected nodes for the purpose of accessing and sharing data. On the other hand security is there to ensure that only authentic users have access to the sensitive information and resources. Nodes connected to a network - particularly the internet (biggest network), are exposed to a wider range of security threats than unconnected nodes. Network security (securing hardware and applications) is put in place to reduce the risks that would result in connecting to a network. A network is a data highway designed to increase access to remote nodes, while security is designed to control access.

Network security is a combination of technical, administrative, and physical controls

Unit Objectives

Upon completion of this unit you should be able to:

- Explain the need to plan security.
- Demonstrate how the security plan is supported by risk analysis.
- Describe how the security policy is based on implementing security.
- Explain how physical control is part of security.

Key Terms

Security plan: A security plan is a document that describes how an organization will address its security needs.

Risk analysis: Risk analysis is the review of the risks associated with a particular event or action. Risk analysis leads to understand the loss associated with the event or action, likelihood of the occurrence of such risk and the degree to which we can change the outcome.

Security policy: A security policy is a document that states in writing how an organization plans to protect the its physical and information logical assets. A security policy is often considered to be a "living document", meaning that the document is never finished , but is continuously updated as technology and employee requirements change.

Physical security: This is part of security concerned with measures designed to safeguard against against external physical threats, internal physical threats and human physical threats.

Security vulnerability: Weakness that makes targets susceptible to an attack.

Security threat: The expressed potential for the occurrence of a harmful event such as an attack.

Learning Activities

SECURITY PLANNING

One of the most important network security tasks is developing a network security policy. Network administrators are expected to follow the day to day life of network and securing it. There will always be a need to find a solution that solves/fixes the network security problem. A well-thought-out and planned security plan will help the administrator to decide what he/she needs to be protected, how much is worth to invest in protecting it, who will be responsible for carrying out the steps to protect it and who or what to be protected. A security plan is a document that describes how an organization will address its security needs. Since the organization's security is not one time plan but rather ever changing as per organization's needs, the security plan is subjected to future revision.

Following sections entail the issues addressed by the plan.

POLICY

A security plan must state the organization's policy on security. A security policy is a high-level statement of purpose and intent. Intentions made on how to open or secure network to whom or to what would lead to a policy.

The policy statement should specify the following:

- The organization's goals on security. For example, protect against loss of data due to physical disaster such as flood or fire, protect the data's integrity, or avoid users to deny operations they have performed.
- Another statement should be where the responsibility for security lies. For example, should the responsibility rest with a small computer security group, with each employee, or with relevant managers?
- And lastly, the organization's commitment to security. For example, who provides security support for staff, and where does security fit into the organization's structure?

CURRENT SECURITY STATUS

To be able to plan for security, an organization must understand the current vulnerabilities to which it may be exposed. A careful investigation of the system, its environment, and the things that might go wrong is performed with intention of finding out vulnerabilities. The status can be expressed as a listing of organizational assets, the security threats to the assets, and the controls in place to protect the assets. The status also indicates who is responsible to protect an identified asset.

REQUIREMENTS

Security plan is built on top of security requirements which are usually derived from organizational needs. For example, access to the data records should be restricted (and note to whom the access should be restricted). The requirements should not include implementation aspect; they only elicit what to be done but not how. Each requirement should be:

- Correct: A requirement is clearly understandable and error free.
- Consistent: A requirement is not conflicting with another and holds a single meaning.
- Complete: A requirement addresses all situations for its need.
- Real: A requirement that is possible to implement.
- Needed: A requirement should be needed by the organization.
- Verifiable: When a requirement is implemented, it should be measured and prove that its exact need has been met.
- Traceable: A requirement is traced to the functions and data related to it so that changes in a requirement can lead to the necessary reevaluation.

RECOMMENDED CONTROLS

The security requirements lay out the system's needs in terms of what should be protected. The security plan must also recommend what controls should be incorporated into the system to meet those requirements. Risk analysis is needed to create a map from vulnerabilities to controls. The mapping tells us how the system will meet the security requirements. That is, the recommended controls address implementation issues: how the system will be designed and developed to meet stated security requirements.

RESPONSIBILITY FOR CONTROLS

A security plan should identify which people are responsible for the implementation of the security requirements. There will always be an individual or individuals responsible for the implementation of each requirement recommended. Hence accountability will be attributed to such individual(s).

TIME TABLE

A comprehensive security plan cannot be executed instantly. The security plan includes a timetable that shows how and when the elements of the plan will be performed. These dates also give milestones so that management can track the progress of implementation (on both sides; controls and responsible individuals). The plan should specify the order in which the controls are to be implemented so that the most serious exposures are covered as soon as possible.

CONTINUING ATTENTION

Good intentions are not enough when it comes to security. We must not only take care in defining requirements and controls, but we must also find ways for evaluating a system's security to be sure that the system is as secure as we intend it to be. Thus, the security plan must call for reviewing the security situation periodically. As users, data, and equipment change, new exposures may develop. In addition, the current means of control may become obsolete or ineffective. The inventory of objects (passive entities) and the list of controls should periodically be examined and updated, and risk analysis is performed. The security plan should set times for these periodic reviews, based either on calendar time (such as, review the plan every nine months) or on the nature of system changes (such as, review the plan after every major system release).

Conclusion

This document holds security that describes how an organization will address its security needs. It considers the top level security policy, the current security of the infrastructure, security requirement that addresses a problem, recommended control measure, then what/who is responsible to implement the control, and schedules that are followed while implementing different control. This is a naturally document because the security of an organization's infrastructure evolves as the organization evolve.

Assessment

What do you consider in your security plan?

Feedback

The list bellow includes what is found in the security plan:

- Security policy.
- Current security status in an organization.
- Security requirements.
- Recommended controls in the network.
- Responsibility for implementation which associate an operation with the responsible personnel.

- Time table for implementing controls.
- Continuous attention as the plan is revised.

RISK ANALYSIS

A risk is a potential problem that the system or its users may experience. A good and effective security planning is made after a careful risk analysis. A risk is associated with the following:

- Loss associated with the event. This is a negative effect occurred as a result of a risk: compromised security, lost time, diminished quality, lost money, lost control, lost understanding, and so on. This loss is called the risk impact.
- The likelihood that the event will occur. This is probability of occurrence associated with each risk which is measured from 0 (impossible) to 1 (certain). When the risk probability is 1, we say we have a problem.
- The degree to which we can change the outcome. We must determine what to do in case of occurrence of a risk; if anything, we can do to avoid the impact or at least reduce its effects. Here we are talking about a set of actions to reduce or eliminate the risk.

Risk is inevitable in life, our reactions towards it are; identify it, limit it, avoid it, transfer it, and controlling its existence. Steps of risk analysis are discussed below:

IDENTIFY ASSETS

Before we can identify vulnerabilities, we must first decide what we need to protect. Thus, the first step of a risk analysis is to identify the assets of the computing system which are available in our network settings. The assets can be considered in categories, as listed below.

- Hardware: processors, boards, keyboards, monitors, terminals, microcomputers, workstations, tape drives, printers, disks, disk drives, cables, connections, communications controllers, and communications media.
- Software: source programs, object programs, purchased programs, in-house programs, utility programs, operating systems, systems programs (such as compilers), and maintenance diagnostic programs.
- Data: data used during execution, stored data on various media, printed data, archived data, update logs, and audit records.
- People: skills needed to run the computing system or specific programs.
- Documentation: on programs, hardware, systems, administrative procedures, and the entire system.
- Supplies: paper, forms, laser cartridges, magnetic media, and printer fluid.

This list and its order is not a must but rather it should be tailored according to the organization situation. Some assets are not worth protecting in some organizations but highly prioritized in other organizations.

DETERMINE VULNERABILITIES

The next step in risk analysis is to determine the vulnerabilities of these assets. This step requires imagination; we want to predict what damage might occur to the assets and from what sources. We can enhance our imaginative skills by developing a clear idea of the nature of vulnerabilities. This nature derives from the need to ensure the three basic goals of computer security: confidentiality, integrity, and availability. Thus, vulnerability is any situation that could cause loss of confidentiality, integrity, and availability. We want to use an organized approach to considering situations that could cause these losses for a particular object.

ESTIMATE LIKELIHOOD OF A RISK

The third step in conducting a risk analysis is determining how often each risk is likely to happen. Likelihood of occurrence relates to how the existing controls solve such uprising issue and the likelihood that someone or something will dodge the existing controls. There are different methods used to evaluate an event's probability, one of methods is to ask an analyst familiar with the system to approximate the number of times a described event occurred in some period of time (like in a year). The count might not be exact (because the analyst is unlikely to have complete information), the analyst's knowledge of the system and its usage may yield reasonable estimation.

COMPUTE EXPECTED LOSS

By this time, we have gained an understanding of the assets we value, their possible vulnerabilities, and the likelihood that the vulnerabilities will be exploited. Next, we must determine the likely loss if the exploitation does indeed occur. As with likelihood of occurrence, this value is difficult to determine. Some costs, such as the cost to replace a hardware item, are easy to obtain. The cost to replace a piece of software can be approximated reasonably well from the initial cost to buy it (or specify, design, and write it). However, we must take care to include hidden costs in our calculations. For instance, there is a cost to others of not having a piece of hardware or software. Similarly, there are costs in restoring a system to its previous state, reinstalling software, or deriving a piece of information. These costs are substantially harder to measure.

In addition, there may be hidden costs that involve legal fees if certain events take place. For example, some data require protection for legal reasons. Personal data, such as police records, tax information, census data, and medical information, are so sensitive that there are criminal penalties for releasing the data to unauthorized people. Other data are company confidential; their release may give competitors an edge on new products or on likely changes to the stock price. Some financial data, especially when they reflect an adverse event, could seriously affect public confidence in a bank, an insurance company, or a stock brokerage. It is difficult to determine the cost of releasing these data.

SURVEY AND CONTROL NEW CONTROLS

By this point in our risk analysis, we understand the system's vulnerabilities and the likelihood of exploitation. We turn next to an analysis of the controls to see which ones address the risks we have identified. We want to match each vulnerability with at least one appropriate security technique.

PROJECT SAVING

By this point in our risk analysis, we have identified controls that address each vulnerability in our list. The next step is to determine whether the costs outweigh the benefits of preventing or mitigating the risks. Recall that we multiply the risk probability by the risk impact to determine the risk exposure. The risk impact is the loss that we might experience if the risk were to turn into a real problem. There are techniques to help us determine the risk exposure.

The effective cost of a given control is the actual cost of the control (such as purchase price, installation costs, and training costs) minus any expected loss from using the control (such as administrative or maintenance costs). Thus, the true cost of a control may be positive if the control is expensive to administer or introduces new risk in another area of the system. Or the cost can even be negative if the reduction in risk is greater than the cost of the control.

Conclusion

A risk or risks always occur in works but not everything is serious, analysis is required to see what loss a risk might cause, the likelihood of such risk to happen and finally to identify the most likely solution to minimize or prevent such risk. It is after analysis that we know what to control.

Assessment

What do you maintain while analyzing risk?

Feedback

While analyzing a network risk the following should be followed and maintained;

- Identification of assets to be protected.
- Determination of vulnerabilities that might exist or existing in the identified assets.
- Estimate the likelihood of a risk.
- Compute the loss associated with a risk.
- Survey and select new controls.
- Savings achieved as a result of selecting a control.

SECURITY POLICIES

Security planning based on risk analysis of any organization should lead to an effective security policy. A security policy must answer three questions: who can access which resources in what manner?

A security policy is a high-level management document to inform all users on using a system. A policy document is written in broad enough terms that it does not change frequently. The security policy is the foundation upon which all protection efforts are built. It should be a visible representation of priorities of the entire organization, definitively stating underlying assumptions that drive security activities. The policy should articulate senior management's decisions regarding security as well as asserting management's commitment to security. To be effective, the policy must be understood by everyone as the product of a directive from an authoritative and influential person at the top of the organization.

MISCONCEPTION

There are some misconceptions which are around network security policy:

- The goal of network security is considered as securing the network. Rather the goal is to secure the organization or business. Security policies describe what you must secure, and the ways you secure them, to support your business or mission. It is the blueprint for using different mechanisms: the what, how, why, when, and by whom.
- Security policies are considered they must be long and complex. In fact, just the opposite is true. We believe the well-known security axiom, "Complexity and security are inversely proportional." Complex systems are usually less secure than simple systems. Complex policies are usually ignored; simple policies might live. A good security policy is really a set of documents, each addressing a specific need. By breaking your overall policy into smaller pieces, each managed separately; you greatly simplify the process of creating effective, consistent, relevant, and useable documents.
- Security policies are considered they have to be nearly perfect, or 100% complete. No. Good enough security now is better than perfect security never. A good plan executed right now, is far better than a perfect plan executed next week. It is perfectly fine to build security policies in parts, refining each part separately in the ongoing process of security policy development.
- Security policies are considered have to be written once for all. No. Until there are no more bad guys in the world and/or everyone agrees to mind his or her own business, the process of managing a security policy never ends. The threats the organization faces will change over time. As the threats to the business change, so too will the company's business requirements. The vulnerabilities will change as well, and so will the risks you are willing to take to do business, and so will the tools you use to reduce or counter those risks. Because of all this, the security policy process is never really done. It only lies dormant for a time.

Conclusion

There are a lot of misconceptions that lead most network administration to ignore setting network policy. But all cases network policy should be established as statements which imply what to secure, how to secure it and what/how to secure it against.

Assessment

Why is it a must to have a network security policy?

Feedback

The security policy is the foundation upon which all protection efforts are built. In case the policy is not in place then there is no where to find what to protect against what.

PHYSICAL SECURITY

Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an organization. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism. Typical physical security controls include guards, locks, and fences to deter direct attacks. In addition, there are other kinds of protection against less direct disasters, such as floods and power outages; these, too, are part of physical security. As we will see, many physical security measures can be provided simply by good common sense. To understand physical security, we firsts need to understand physical threats which are categorized in three:

- External physical threats: Here we are talking about; floods, earthquakes, winds, hurricanes, fire, ice, chemicals, etc
- Internal physical threats: Here we are talking about; electrical interruption, liquid leakage, environmental failure, etc.
- Human physical threats: Here we are talking about; theft, unauthorized access, vandalism, sabotage, espionage, etc

Physical security controls should be put in place to prevent these threats from being reality. Hence, fences, barriers, gates, doors with locks, badges, escorts, detection systems, power protection, water protection, fire protection, etc are put in place to control the attacks. The diagrams below show some of physical security control.

Physical security access control with a hand geometry scanner

Source: https://en.wikipedia.org/wiki/Access_control

Locks

Source: http://www.losspreventionplan.com/choose-suitable-doors-windows/

Conclusion

Physical security threats like other security threats will always be there, putting them into consideration in security planning and implementation opens more reliable and assured security.

Assessment

Why do we even care concentrating on physical security after the confidentiality, integrity and availability are in place for our information?

Feedback

Network assets and resources can damaged and destroyed by natural catastrophes like floods, fire, effects of volcanic eruption, earthquakes. Not only that but bad people might gain kinetic contact to the resources where they can steal them or do any other thing which is bad. It is to be on safe side when physical security is as well implemented together with other security.

Unit Summary

Securing hardware and applications achieved by network administrator is an exercise which surpasses understanding security assets, threats, vulnerabilities, and controls; it also includes management and implementation. To accomplish security, security planning should be accomplished supported by risk analysis to come up with a security policy. An organizational security policy is a document that specifies the organization's goals regarding security. It lists policy elements that are statements of actions that must or must not be taken to preserve those goals. Policy documents often lead to implementation procedures. Securing hardware and applications has a strong human component, from the writing of plans and policies, to the mental work in performing a risk analysis, to the human guards that implement or reinforce many physical controls and technical team that implements technical controls.

Unit Assessment

1. Describe security policy of in an organization's network.
2. Why would you consider project saving while implementing security?
3. Describe physical security in different categories.

Grading scheme

The unit's assessments are graded out of 20% which are categorized as follows:

- Activity assessments are out of 6%.
- Unit assessment is out of 4%.
- Unit test is out of 10%.

Feedback

1. A security plan must state the organization's policy on security. A security policy is a high-level statement of purpose and intent. Intentions made on how to open or secure network to whom or to what would lead to a policy.

The policy statement should specify the following:

- The organization's goals on security. For example, protect against loss of data due to physical disaster such as flood or fire, protect the data's integrity, or avoid users to deny operations they have performed.
- Another statement should be where the responsibility for security lies. For example, should the responsibility rest with a small computer security group, with each employee, or with relevant managers?
- And lastly, the organization's commitment to security. For example, who provides security support for staff, and where does security fit into the organization's structure?

2. We implement security to secure either some resources or some information. We secure anything we secure because it valuable to us but what would happen if security we implement outweighs what we are securing. That means we are doing wrong calculations. The total cost of security we are implementing should be less than the cost of what we are protecting.

3. Physical security is categorized in 3:

- External physical threats: Here we are talking about; floods, earthquakes, winds, hurricanes, fire, ice, chemicals, etc
- Internal physical threats: Here we are talking about; electrical interruption, liquid leakage, environmental failure, etc.
- Human physical threats: Here we are talking about; theft, unauthorized access, vandalism, sabotage, espionage, etc

Physical security controls should be put in place to prevent these threats from being reality. Hence, fences, barriers, gates, doors with locks, badges, escorts, detection systems, power protection, water protection, fire protection, etc are put in place to control the attacks.

Unit Readings and Other Resources

Required readings and other resources:

- Charles P. Pfleege, S. L. (2007). *Security in Computing, Fourth Edition.* Prentice Hall.
- Craig, H. (2002). TCPIP *Network Administration, 3rd Edition*. Sebastopol: O'Reilly Media.
- Thomas A. Limoncelli, C. J. (2007). *The Practice of System and Network Administration Second Edition.* Boston: Addison Wesley.

Optional readings and other resources:

- Charles P. Pfleege, S. L. (2007). *Security in Computing, Fourth Edition*. Prentice Hall.

Unit 5: Maintenance And Troubleshooting

Unit Introduction

From the perspective of network administration the lifecycle of components and the infrastructure can be summarized in three phases: installation, maintenance and upgrade. Maintenance is defined as the set of measures, technical and administrative activities to maintain unity in a state (or bring it back in such a state) where it can normally perform its intended services. Thus, maintenance is the large exploitation of a network infrastructure. All components ranging from simple cables to other equipments and complex software systems are the units to be maintained.Maintenance has a cost, which is why all the units may not receive the same level of maintenance. The maintenance policy proceeds in most cases based on the economic value and significance of the components in the infrastructure. Therefore maintenance activities are numerous and require effective organization.

Unit Objectives

Upon completion of this unit you should be able to:

- Explain the importance of maintenance as part of network administration.
- Differentiate the various types of maintenance.
- Highlight the need to plan maintenance and content of a maintenance plan.
- Explain the importance of network documentation in performing maintenance.
- Describe the role of backup and restoring in securing network components.
- Discuss why in many cases companies are advised to operate with maintenance contracts.

Key Terms

Maintenance: These are corrective and preventive measure taken to have a working and reliable network infrastructure.

Troubleshooting: Network troubleshooting is the collective measures and processes used to identify, diagnose and resolve problems and issues within a computer network.

Failure: This is the complete or partial failure of a component or components of a network because of malfunction or natural or human-caused disasters.

Disaster: This is a sudden event, such as an accident, a natural catastrophe, that causes damage to a component or components and makes them fail functioning normally.

Backup: This is the process of making extra copies of data in other places to be assured that will always have them despite the damages happened

Recovery: This is the area of security planning that deals with protecting an organization's network configuration and data from the effects of significant negative events/disasters.

Learning Activities

TYPES OF MAINTENANCE

We open the unit discovering the two main types of maintenance and with the various activities carried out under maintenance.

TYPES MAINTENANCE.

Maintenance includes an important organizational component that technical tasks perform during maintenance execution. In a context network administration there must be a well-known maintenance policy which defines among other the plan and applicable maintenance methodologies. We can distinguish two main types of maintenance encountered in IT environments:

- Corrective Maintenance.
- Preventive Maintenance.

The corrective maintenance is a simple approach to network maintenance. It is to respond to failures and other problems as they arise. The disadvantages of this approach are considerable. We should first mention that the beneficial tasks to a proper functioning network in the long term are ignored, postponed or forgotten. After we have managed to bring back a failed unit into operation mode we easily forget causes, consequences, and lessons drawn from the repair. Another essential drawback is that maintenance work will not be performed in the order of priority (emergency), but rather in the order subjective to the administrator or in the order of occurrence of a failure. In conclusion, reactive maintenance is becoming increasingly unsustainable in a competitive business environment because it leads ultimately to larger periods of unavailability of components, or an entire infrastructure. Structured maintenance and

preventive maintenance can reduce the number of failures in infrastructure and more effectively respond to failures that do occur. It defines in advance the procedures and maintenance tasks and establishes plans. The preventive maintenance presents clear advantages over corrective maintenance: reducing downtime, increase operating safety, alignment with organization goals, but also cheap. The approaches and methodologies of maintenance are taken into account in network management model such as TMN (Telecommunications Management Network) or management of computer systems such as comme ITIL (IT Infrastructure Library). The choice of maintenance type determines the types and quantities of resources as well as tools required for maintenance.

Conclusion

Both corrective and preventive maintenance are used but preventive the most preferable though the choice of the type depends on the present scenario and maintenance plan.

Assessment

Differentiate corrective and preventive types of maintenance?

Feedback

Corrective maintenance responds to failures and other problems as they arise. There is a tendency of forgetting measures taken while correcting the issue. Preventive maintenance on the other hand defines in advance the procedures and maintenance tasks and establishes plans.

MAINTENANCE TASKS

This activity shows the different categories of maintenance tasks and allows to look into their diversity. Illustrative examples are given in each category.

SCOPE OF NETWORK MAINTENANCE

Maintenance tasks within the network administration can be grouped into five major categories:

- Installation and configuration of components.
- Reaction to failures.
- Performance Management.
- Organizational procedures
- Security.

The installation and configuration of hardware and software components are not just one time tasks in the operation of a network infrastructure. A component is configured for the first time when it is put in place and then it can be reconfigured again over and over as a result of

failures, due to some changes in the environment or some updates are necessary. Update is particularly high for software component. This is particularly the case for operating systems and other systems where update is needed to download some module almost daily. For application software migration to a new version should be evaluated, prepared and justified in relation to the organization: it is not just to pass a new version just because it is available. Maintenance tasks as part of the installation and configuration also includes the backup and restoring configuration data.

The second category of maintenance tasks groups the tasks which react to the occurrence of failures either in individual components or in the network infrastructure as whole. Among these include assistance to users who encounter problems with network communication, fault diagnosis of the equipment and communication lines, replacing equipment and restoring backups. One of the expected consequences of failures that can occur in a network is obviously the loss of data. Network administration should aim in this context to reduce losses to a minimum. Network is an important asset and an essential productivity tool for the company, there is always a need to gain optimum use of it. The performance perceived by users every day is an immediate measure of this optimum.

Maintenance tasks related to managing network performance include: monitoring of the use, tuning the performance, and the capacity planning. Capacity planning is the basis for predicting the evolution of the infrastructure (in the month time and some years). It concerns observing the level for the rate of change of different components use (servers, routers, communication lines, hard drives) and assess the need for additional capacity that is needed. Monitoring and performance tuning are tasks to exercise daily. Monitoring allows for example to detect unbalanced use and take appropriate measures. For example a line of communication or some application systems that is saturated by some users over others.

Organizational procedures include tasks such as documentation, compliance audit and management of SLA (Service Level Agreement). The SLA describes the level of service/ performance that the organization have taken is as per agreement with the service provider in a contract. For example, the organization might have paid for a certain level of service in the contract that binds it to the ISP. Network administration should regularly assess the level of service received whether the SLA is met or not.

The last category of maintenance tasks includes tasks related to the implementation and monitoring of the enterprise security policy. Much of the work in the context of network administration is dedicated to the administration and maintenance of security systems such as firewalls and intrusion detection systems (IDS).

Conclusion

Network maintenance has a wide range of activities performed whose ranges from fresh installation, updating the existing environment and removing the unwanted components. Maintenance involves: installation and configuration, actions taken in case of failures, managing the performance, organization of procedures and ensuring security.

Assessment

What are the activities included in the scope of network maintenance by the network administrator.

Feedback

The list of activities cycled in the scope of network maintenance is:

- Installation and configuration of components.
- Reaction to failures.
- Performance Management.
- Organizational procedures
- Security.

POLICY AND SCHEDULES OF MAINTENANCE

We have learned from previous activities that maintenance require administrative procedures than it needs technical activities. In fact in a comprehensive administrative framework defined in an organization, we cannot make effective decisions for the maintenance and especially allocate the necessary financial means. It is the maintenance policy which provides the framework for the organization of maitenance execution.

MAINTENANCE POLICY

The policy of network maintenance represents the repository for all decisions and activities related to the network maintenance in an organization. It sets the first philosophy of maintenance. That is to say; a set of principles to be followed within the organization and maintenance execution within the company, the maintenance policy should also set:

- The type of maintenance to apply.
- The level of maintenance applied to different types of components.
- The maintenance plan.

The plan or maintenance schedule comes within the preventive maintenance. The aim of the preventive maintenance is to prevent failures. Thus, it can be systematic, that is to say, the maintenance operations are planned and will be implemented on schedule, regardless of the status of the unit concerned. But on the other hand it can be conditional, that is to say, maintenance operations are executed according to the state of degradation observed during the prior inspection.

To sum up a, a maintenance plan must include procedures for performing the following tasks:

- Installation, configuration and setting up of new components.
- Update software.
- Adaptation to the changes made.
- Backup of equipment configuration and softwares.
- Troubleshooting equipment and communication lines.
- Repair or replace failed equipments.
- Performance measurement and capacity planning.
- Writing and updating documentation.

Conditional preventive maintenance is therefore based on inspections that are scheduled in advance or can be ordered on the basis of some clues from operating data of the unit concerned. We can define an inspection as all activities performed on a component in order to detect conditions that may cause malfunctions and / or lead to deterioration of the component.

Conclusion

Network maintenance policy should be developed and followed while operating maintenance activity. It acts a roadmap of what to do on any instance of time and while implementing any maintenance activity a schedule should be followed.

Assessment

Why does a network administrator need a maintenance policy?

Feedback

The maintenance policy is needed since whatever the administrator has to do in executing maintenance operation should be as per policy of the organization. It is the roadmap that guides the administrator while maintaining the network or network components.

NETWORK DOCUMENTATION

The information needed to locate the components and their configuration data are crucial for network maintenance. There should be a network documentation that holds all this information.

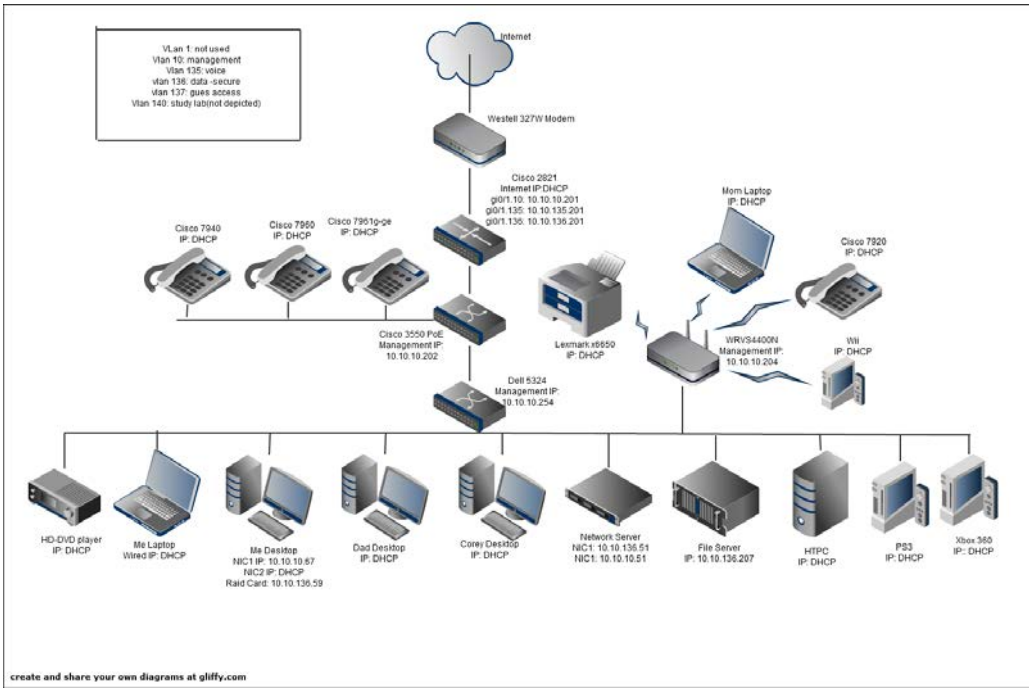
DOCUMENT DETAILS

The documentation of the network infrastructure is an essential tool for implementing the various maintenance tasks.

Here is what each network documentation file should contain:

- Network Map: These diagrams giving all the physical and logical topology of the network. That is to say, the map must show the components and connections between them.
- Connection List: This list must present all important physical connections to the network. In addition to network cables and other transmission lines there including electrical circuits.
- Equipment List: Contains the list of all devices, numbers, serial numbers; installed software and versions, information on licenses and warranties.
- Addressing Plan: Describes the IP addressing scheme of the network.
- Configurations: Shows all current configurations of equipment and even the archives of previous configurations.

In nowadays network administration softwares in particular monitoring tools provide a valuable support to produce network documentation.



Network map

Source: http://forums.evga.com/Edited-Whats-wrong-with-my-Network-Diagram-m241618.aspx

Conclusion

The Network map provides the basic document for network administration and especially for maintenance. Specialized software now facilitates the creation and updating of network map.

Assessment

Why would you need network documentation yet the network is so small that is understandable by the administrator?

Feedback

Every administrator has start time and end time but the network exists as long as the organization exists. If a new administrator or an employee related comes in the organization will easily understand the network, and in case a failure happens or maintenance is needed in this document we might find it easy to locate the component and its location. Lastly, even the network is small but there is no grant that will always be of the same size, the documentation serves a lot on scaling up the network.

BACKUP AND DISASTER RECOVERY

The occurrences of incidents that can lead to loss of resources (including loss of data) in a network infrastructure are inevitable, despite the preventive measures that can be implemented. It is for this reason that regular data backup is the only feasible solution to respond to incidents and potential losses.

BACKUP

To backup is to regularly create copies of data and softwares installed in the machines (especially servers) and active equipment of the network infrastructure. Backups are used to restore the state of equipment configuration, to re-install servers and other systems and/or to restore the application data after incidents that led to losses of data or system failure. The situations that can lead to data loss are many and some of them are as follows:

- Equipment failure (hardware failure).
- Accidental deletion or unintended modification.
- Security incidents happened.
- Upgrading and migration.

The backup must be based on a plan that should obviously be in line with the general maintenance police of the organization. The characteristics of a good backup plan are: Backup execution should be easy (Automatic backups), ability to schedule backups, ability to check backups (for example, backups accomplished), and ability to make copies and relocate them. The backup plan also determines the security strategy. Among the existing strategies are:

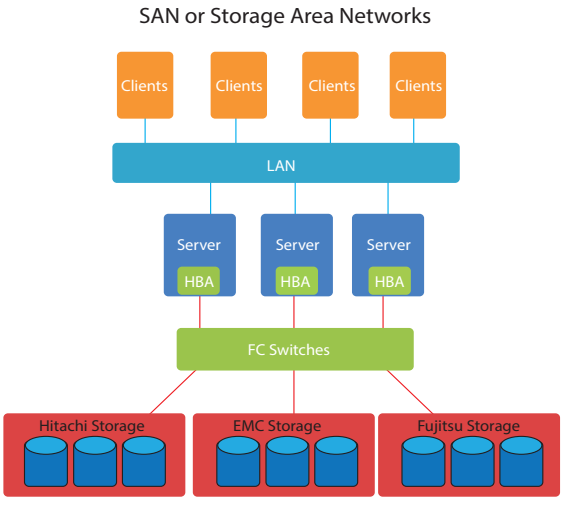
- Full Backup: We secure the entire file system. As the name implies, this type of backup makes a copy of all data to another set of media.

- Incremental Backup: An incremental backup operation will result in copying only the data that has changed since the last backup operation of any type. The modified timestamp on files is typically used and compared to the timestamp of the last backup. Backup applications track and record the date and time that backup operations occur in order to track files modified since these operations.

The backup plan can for example set that an incremental backup is performed daily (at the end of the work day) and a full backup is performed every last working day (to get all weekly work saved).Modern operating systems offer effective tools for backup and restore. Thus, under the UNIX / Linux system, for example, we include:

- dump and restore: For backups of the entire file system. Both also support incremental backups.
- tar: Allows archiving file and backup (archiving).
- compress and gzip: These two tools allows to perform compression to be the backup the compressed file.

For a long time the tapes were kind of secondary memory backup, Then came the removable hard drives and then backup systems constructed on the basis of a combination hard drives, such systems are designed to connected directly to the network. In this regard Storage Area Network (SAN) was also very beneficial to the backup technology. The SAN allows servers to save data directly to external backup systems of large capacity and high performance, with the possibility of duplication. This presents a security aspect. The purpose of the backup is also to achieve disaster recovery. A disaster could be any catastrophic event that causes massive destruction, or entire site destruction. The figure below depicts the Storage Area Network technology.



SAN

Source: http://www.what-is-my-computer.com/fibre-channel.html

Conclusion

Faults in the systems, disasters and attacks are inevitable the only we can stay assured that despite what has happened we can keep on normal track in our network is the back our data, software and configuration.

Assessment

Having a good security in place, why would someone use extra effort and resource to ensure backup?

Feedback

At any point of time the security can be bypassed or hacked which leads to loss of information and/or configuration. Not only but natural catastrophes can cause any kind of destruction in our network to ensure after all destruction and hackers activities we can use backups to restore to our information and configurations which have been destroyed or changed.

MAINTENANCE CONTRACTS

The network infrastructure maintenance activities can be partially entrusted to outside companies, such as suppliers of systems and outsourcing companies. In this regard the components in the network, data and/or network map are accessible to the outsider. While insuring maintenance, security should also be maintained.

MAINTENANCE STAKEHOLDER

Network administration also concerns the management of the interfaces with several technical partners, equipment suppliers, developers, and other more. All these entities should be bound by maintenance contract. Indeed, the diversity and complexity of IT components makes it almost impossible taking total work of all network infrastructure of the organization. Moreover the maintenance contract is automatically part of the package offered by software vendors. For hardware component, it is a good idea to plan maintenance contract with high valued (expensive) and complex systems. For example, an organization can take a maintenance contract for its backbone routers and take into its responsibility to maintain internal routers. Since the contracts are governed by the law, the challenge is to have a maintenance contract formulated in a way that does not have different interpretations and contradiction between contradicting parties.

Conclusion

Network administrator is also responsible for monitoring maintenance contracts that the company may have had with outside companies. A good environment between contractors should be maintained.

Assignment

Why would outsiders appear in the organization for maintenance yet you are hired for such work?

Feedback

The complexity of IT components makes it almost impossible taking total work of all network infrastructure of the organization. Moreover the maintenance contract is automatically part of the package offered by software vendors. For hardware component, it is a good idea to plan maintenance contract with high valued (expensive) and complex systems.

Unit Summary

Maintenance is one of the most important heavy duties in network administration. The components, the compartments and even the entire network infrastructure will always experience either minor malfunctions, or breakdowns leading to a total unavailability. As part of the maintenance activity, the network administrator must detect failures, diagnose and perform the restore operation of the affected units. Maintenance should also be preventive to anticipate failures. The maintenance of every network infrastructure should be drafted as a policy and the schedule of when to do what.

Unit Assessment

1. Describe maintenance policy.
2. What are the benefits of network documentation?
3. What is backup and what are situations that lead its need?

Grading scheme

The unit's assessments are graded out of 20% which are categorized as follows:

- Activity assessments are out of 6%.
- Unit assessment is out of 4%.
- Unit test is out of 10%.

Feedback

1. The policy of network maintenance is a document which represents the repository for all decisions and activities related to the network maintenance in an organization. It sets the first philosophy of maintenance. That is to say; a set of principles to be followed within the organization and maintenance execution within the company, the maintenance policy should also set:

- The type of maintenance to apply.
- The level of maintenance applied to different types of components.
- The maintenance plan.

2. Below are benefits of having a network documentations:

- Fast network troubleshooting: A network document will timely identify and pinpoint the problem and the area of occurrence.
- Smooth transition between different staffs: Once a staff is leaving and a new is coming, it will help the loss of information in such transition and hence transition period will always be less painfully in the life of an organization.
- Easier assignment of duties: Network administrator can quickly and effectively assign responsibilities to staffs because everything is clearly documented.
- Improved network design: The structure of the current network will always be a starting point to improve the network to more desirable point. Hence there is a room for improvement that is better first visualized from the document.

3. To backup is to regularly create copies of data and softwares installed in the machines (especially servers) and active equipment of the network infrastructure. Backups are used to restore the state of equipment configuration, to re-install servers and other systems and/or to restore the application data after incidents that led to losses of data or system failure. The situations that can lead to data loss are many and some of them are as follows:

- Equipment failure (hardware failure).
- Accidental deletion or unintended modification.
- Security incidents happened.
- Upgrading and migration.

Unit Readings and Other Resources

Required readings and other resources:

- Habraken Joe, H. M. (2004). SAMS Teach yourself Networking in 24 hours Third Edition. Indiana: SAMS Publishing.
- Kizza, J. M. (2009). A Guide to Computer Network Security. London: Springer-Verlag London Ltd.
- Thomas A. Limoncelli, C. J. (2007). The Practice of System and Network Administration Second Edition. Boston: Addison Wesley.

Optional readings and other resources:

- Kizza, J. M. (2009). A Guide to Computer Network Security. London: Springer-Verlag London Ltd.

Unit 6 LAB WORK

Introduction

This guide includes several exercises of practical work that will lead the learner to achieve the objectives listed below.

Unit objectives

At the end of this unit the student will be able to:

- Identify the main utilities for network configuration under UNIX.
- Demonstrate IP addressing and address translation.
- Demonstrate some protocols at work: ARP, ICMP.
- Configure DHCP server.

Learning activities

Network Interface Card

A network interface identify a device to connect to a network, it can be a network card, modem, serial port, USB port. On Linux, an interface corresponds to an entry point in the kernel. Send messages through the network interfaces back to pass data to the kernel special procedures responsible for carrying out physical input-output operations. An interface is usually identified by a logical name of eth0 type eth1, wlan0, wlan1.

Commands

Execute the following commands;

- Determine the network interface cards you have on your machine with the following command. dmesg | grep eth.
- Display the configuration of your computer (IP address, MAC) on network by usingifconfig.

ICMP Protocol

Internet Control Message Protocol is an administration protocolbased on IP used by network nodes to report errors for example if the node is accessible on the network.

Commands

– Determine the reach ability of node from your working node by using ping command. Use ping followed by IP address or domain name. For example, ping 8.8.8.8 or ping www.google.com. It shows reached packets or lost packets.

– Identify the path to the remote machine using traceroute and how long to reach that machine. This command is followed by the IP address or the domain name (traceroute 8.8.8.8 or traceroute google.com) which returns the maximum hop count.

Address Resolution Protocol

The arp command that relies on the protocol of the same name resolves IP addresses, to find the physical address corresponding to a given logical address.

Commands

- Retrieving the physical address of a machine with its corresponding IP address. Type the arp –a command where the results indicate a 3 column table in which you have IP address, physical address, and type. Where the type contains values like static or dymanic.

DHCP Server configuration

The DHCP server allows dynamic IP assignment to machine on the network despite the number machines connected.

Commands

DHCP server configuration involves two task in ubuntu:

- Downloading and installing the package using apt –get install dhcp-server command.
- Starting the service using /etc/init.d/networking restart.
- The configuration file can be found by typing /etc/default/dhcp3-server. Having this file some changes can be done.

Nagios tool

Nagios is a network monitoring tool that enables an organization resolve IT infrastructure issues before the failure or any network problem would result into some loss. In so doing the monitoring tool can monitor applications, service and entire infrastructure tools.

Nagios setup on a computer

This process involves different steps where the first step is installing the required packages for the tool to work as needed; the packages are apache and PHP. This is achieved by the following command:

– Apt –get install wget apache2 apache2 –utils php5 libapache2 –mod –php5 build –essential libgd2 –xpm –dev. (You can use sudo at the beginning of the command if your account is limited in privileges and you want to take that privilege from another account)

– Now it is the time to start the service (web server service) which is achieved by the following command(service apache2 start).

The next step is about creating an account for nagios which requires the user name and password for nagios.

– To create a username you type (useradd username) username here means any user name of your choice.

– To create a password you type (passwd password) password here stands for any password of your choice.

– Now it is time to create a group for the account created where the account will be added to the group. (groupaddnagrp) them add user to the group (usermod –a –G nagrpusername) and finally add nagios user in apache group (usermod –a –G nagrp www-data).

After the required packages are installed and the nagios account has been created it is time install the core services by running the following commands.

– cd /opt/

– wgethttps://assets.nagios.com/downloads/nagioscore/releases/nagios-4.1.1.tar.gz

– tar xzf nagios-4.1.1.tar.gz

– cd nagios-4.1.1

– ./configure –with-command-group=nagrp

– make all – make install

– make install-init

– make install-config

– make install-commandmode

It is time to create nagios apache2 configuration file.

– vim /etc/apache2/conf-available/nagios.conf

We need to setup apache authentication for user but not the one create above nagiosadmin is used in this case.

– Htpasswd –c /usr/local/nagios/etc/htpasswd.usernagiosadmin

After this command the time to enable apache configuration comes and restart apache service comes.

– a2enconf username

– a2enmod cgi

– service apache2 restart

The next step will involve installingup plug-ins for nagios tool.

- cd /opt
- wgethttp://www.nagios-plugins.org/download/nagios-plugins -2.1.1.tar.gz
- tar xzfnagios-plugins – 2.1.1.tar.gz
- cd nagios-plugins -2.1.1
- ./configure –with-nagios-user=username –with-nagios-group=username
- make
- make install

After the plug-ins are installed it is time to verify the nagios and start it

- /usr/local/nagios/bin/nagios –v /usr/local/nagios/etc/nagios.cfg
- service nagios start

Last we access nagios tool from the web browser using the IP address or computer name.

- http://ip_address/nagios then login with your admin username and password.

Module Summary

A complete network is put in place by connecting different devices and enabling services that enable those devices to accomplish designated roles with the purpose of sharing information and resources. Once a network is in place another step ahead is needed to secure that network to ensure that only authentic users never access beyond their authorization permission.

Network administration lies on top of all above as it is a process that gives life to the network on every instance of time by discovering network problems and resolving presenting issues. A network administrator has to be equipped with technical skills to manipulate devices and services such that network delivers as supposed. But also profession ethics are needed in legal stand should be equally strong to accomplish the task.

Module Readings and Other Resources

Charles P. Pfleege, S. L. (2007). Security in Computing, Fourth Edition. Prentice Hall.

Cisco. (2016, February 27). networkers/nw03/presos/docs/NMS-1001.pdf. Retrieved February 27, 2016, from http://www.cisco.com/:

http://www.cisco.com/networkers/nw03/presos/docs/NMS-1001.pdf

Craig, H. (2002). TCPIP Network Administration, 3rd Edition. Sebastopol: O'Reilly Media.

Forouzan, B. A. (2007). Data Communications and Networking. New York: McGraw - HillCompanies.

Habraken Joe, H. M. (2004). SAMS Teach yourself Networking in 24 hours Third Edition. Indiana: SAMS Publishing.

Jang, M. (2009). Ubuntu Server Administration. New York: McGraw-Hill Companies.

Kizza, J. M. (2009). A Guide to Computer Network Security. London: Springer-Verlag London Ltd.

Pras, A. (2016, February 27). ~jakab/edu/litr/TMN/Network_Management_Architectures_extr.pdf. Retrieved February 27, 2016, from http://www.hit.bme.hu/:

http://www.hit.bme.hu/~jakab/edu/litr/TMN/Network_Management_Architectures_extr.pdf

Stallings, W. (2007). Data and Computer Communications. New Jersey: Pearson Prentice Hall.

Thomas A. Limoncelli, C. J. (2007). The Practice of System and Network Administration Second Edition. Boston: Addison Wesley.

The African Virtual University Headquarters

Cape Office Park

Ring Road Kilimani

PO Box 25405-00603

Nairobi, Kenya

Tel: +254 20 25283333

contact@avu.org

oer@avu.org

The African Virtual University Regional Office in Dakar

Université Virtuelle Africaine

Bureau Régional de l'Afrique de l'Ouest

Sicap Liberté VI Extension

Villa No.8 VDN

B.P. 50609 Dakar, Sénégal

Tel: +221 338670324

bureauregional@avu.org