Network Infrastructure

Network administration is the process of managing the computer network from acquiring the requirements of the network, deploying the various computer network entities configuring these for fine-tuned operations, and maintaining these entities for continuous and effective operations.

- ***Infrastructure*** refers to the various resources necessary in interconnecting the different network devices. The infrastructure includes network connectivity and the various network devices that allow network extensions, segmentation, and redundancy.
- ***Systems***, on the other hand, refer to computer hardware and software for servers and workstations that provide services and the means for end-users to access these network services.

Tasks in Network Administration

- ***Monitoring and Analyzing:*** This concerns the detection, isolation, and correction of abnormal operation of the data network to keep the network up and running smoothly.
- ***Evaluating and Controlling:*** This concerns with keeping track of the individuals' utilization and grouping of network resources to ensure that users have sufficient resources.
- ***Configuring:*** This concerns with performing repairs and upgrades to resources in the network to support a given service.

Things to consider in organizing the resources of a computer network:

- ***Geographical coverage*** – Determines whether your network is a single site network or a multisite network.
    - ***Single site network*** – This exists when multiple pieces of computer equipment in one geographic location (e. g. campus, office or home) is connected together for the purpose of sharing information.
    - ***Multisite (Multicountry) network*** – This exists when multiple pieces of computer equipment in multiple geographic locations (where all local requirements of each country must be taken into consideration) are connected together.
- ***Nature of access to the network*** – It determines the subsidiaries of the larger mother company. Often, the mother company can afford to set up a network that can offer the same services to sister companies or subsidiaries.
- ***Types of platforms*** – It determines whether the server will be a single platform of either Windows Servers or Linux Servers or will be a mixed environment to be more appropriate.
- ***Kinds of network services*** – It determines the services and applications that may be available in versions compatible with common platforms.
- ***Size of the network*** – It determines the number of users expected to utilize the network. This includes the kind of users expected to avail of the offered network services.

Structured Cabling System

It is a complete arrangement of cabling and associated hardware (as indicated by standards), which gives an extensive telecommunications infrastructure. This infrastructure serves a wide range of uses, such as to provide telephone service or transmit data through a computer network.

- ***Horizontal cabling*** – It is a wiring/cabling that extends from the telecommunications information outlet in the work area to the horizontal cross-connect, intermediate cross-connect, or main cross-connect in the telecommunications room or telecommunications enclosure.
- ***Entrance facility*** – It specifies the point in the building where inside building cabling interfaces with the outside plant cables.

- ***Telecommunications rooms and enclosures*** – It houses cabling components such as cross-connects and patch panels. Also, this is where the horizontal structured cabling originates and the backbone-cabling equipment rooms terminate.
- ***Equipment room*** – It is an environmentally controlled centralized space that houses a more sophisticated equipment than the entrance facility or the telecommunications rooms. Backbone cabling is specified to terminate here.
- ***Backbone cabling (vertical cabling)*** – It provides interconnection between entrance facilities, equipment rooms, and telecommunications rooms and enclosures within a single building or between other buildings.
- ***Work area*** – It is where the horizontal cable terminates at the telecommunications outlet.

Network Policy

It refers to rules and procedures that serve as guidelines to both network administrators and end-users in availing network services and resources. In practice, these policies apply to network users and are implemented by network administrators – ***Authentication-Authorization-Accounting***. This is widely used because it features good scalability and facilitates centralized user information management. Currently, the device uses the ***Remote Authentication Dial-In User Service (RADIUS)*** or ***Huawei Terminal Access Controller Access Control System (HWTACACS)*** protocol to implement AAA.

- ***Authentication*** – It is a process that validates the integrity and verifies the identity of the user that tries to log-on to the network using his or her credentials (username/password pair).
- ***Authorization*** – It specifies the individual access rights to the network resources given to users.
- ***Accounting*** – It is a facility within the network that monitors the resources that are frequently used within the network and the behavior and network activities of the users.

Network Security

It involves various measures of safeguarding all of the components associated with a network, including data, media, and infrastructure.

- ***Confidentiality/Secrecy*** – It is a property of a secured communication which guarantees that only authorized users can view sensitive information. This implies that only the sender and the intended receiver should be able to understand the contents of the transmitted message.
    - *Identity Interception* usually occurs when an attacker gains all the necessary information (usually a username and password) about a user to masquerade themselves as the same user.
- ***Authentication*** – It is a property of secured communication, in which one is able to prove his/her identity to someone else. This implies that both the sender and the receiver should be able to confirm the identity of the other party involved in the communication.
- ***Message integrity and Non-repudiation*** – It is a property of a secured communication which guarantees that only authorized users can change sensitive information and provides a way to detect whether data has tampered during transmission; this might also guarantee the authenticity of data. This implies that both the sender and the receiver ensure that the information is not altered, either maliciously or by accident in transmission.
- ***Availability and access control*** – It is a property of a secured communication that provides uninterrupted access by authorized users to important computing resources and data. This implies that entities that seek to gain access to resources are allowed to do so if they have the appropriate access rights and perform their accesses in a well-defined manner.

Kinds of Network Attacks:

- ***Internal attacks*** come from compromised nodes that are actually part of the network. This compromised nodes and maybe in the form of:
  - A person that has no valid user account in the computer network and is trying to access certain network resources
  - A valid computer network user that tries to access network resources beyond his or her authorization
  - Small programs that somehow got into the network (through external storage, email attachments, etc.) and are instructed to do damage on network objects (i.e., servers, connectivity devices, and even physical links)
- ***External attacks*** come from nodes that do not belong to the domain of the network. This is especially true to those computer networks that hold very important or sensitive information (e.g. in banks and other financial institutions).

Common flaws and attacks in TCP/IP protocols:

- ***Denial of Service (DOS) attack*** – It is an IP security threat that is designed to interrupt or completely disrupt operations of a network device or network communications by sending a large number of data packets. As a result, the system cannot receive requests from the valid users or the host is suspended and cannot work normally.
- ***Packet Sniffing*** – It is an IP security threat that refers to an act of intercepting and reading any or all network traffic that is being transmitted across a shared network communication channel.
- ***IP Spoofing attack (aka IP address forgery or a host file hijack)*** – It is an IP security threat, in which an intruder generates a packet that carries a bogus source address, which can make unauthorized client access the system applying the IP authentication even in the root authority. In this way, the system can also be destroyed even though the response packet does not reach the system.
- ***Process table attack*** – It is a kind of denial-of-service IP security threat that exploits the feature of some network services to generate a new process each time a new TCP/IP connection is set up. The attacker tries to make as many uncompleted connections to the victim as possible in order to force the victim's system to generate an abundance of processes. Hence, because the number of processes that are running on the system cannot be boundlessly large, the attack renders the victim unable to serve any other request.
- ***TCP sequence number prediction attack*** – It is an IP security threat, in which an attacker hopes to correctly guess the sequence number used by the sending host and later send counterfeit packets to the receiving host which will seem to originate from the sending host.
- ***IP Half Scan (SYN Scanning)*** – It is an IP security threat, in which an attacker determines the state of a communications port without establishing a full connection.

Devices and Services used to protect the perimeter of a network:

- ***Firewall*** – Similar to the partition wall used to prevent fire from spreading in the building, it is an integrated collection of security measures designed to filter or reject incoming or outgoing packets based on a predefined set of rules defined in any layer of the OSI model. It can monitor the access channels between the ***Trust zone (the internal network)*** and the ***Untrusty zone (the external network)*** to prevent the hazard from external networks.
- ***Proxy server*** – It is a computer system or an application that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service such as file, connection, web page, or other resources available from a different server.

- ***Demilitarized Zone (DMZ)*** – It is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.
- ***Bastion Host*** – It is a special purpose computer on a network specifically designed and configured to resist and oppose illicit or unwanted attempts at entry. It is used to guard the boundary between internal and external networks.
- ***Boundary Router (Border Router)*** – It is a router that serves as an external firewall that connects to the company's internal firewall and proxy server in the DMZ.
- ***Network Address Translator (NAT)*** – It is an admittedly useful kludge that sits between the network and the Internet, and permits internal network addresses to be translated into public network addresses when packets leave inside networks. This is to make sure that only public IP addresses are exposed to the public Internet.

References:

Mueller, S. (2013). *Upgrading and Repairing PC's 21st Edition*. Indianapolis, Ind.: Que

Oliviero, A. (2014)., *Cabling: the complete guide to copper and fiber-optic networking, 5th ed.* Indianapolis, IN: John Wiley and Sons

Sosinsky, B. (2009). *Networking bible*. Indianapolis, IN: Wiley Pub., Inc.

Tanenbaum, A. (2011). *Computer Networks (5th Edition*). Boston: Pearson Prentice Hall