Journal of Information and Operations Management
ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-284-288
Available online at http://www.bioinfo.in/contents.php?id=55

THE DESIGN OF NETWORK IN IMPLEMENTATION PHASE

JUGELE R.N.[1*] AND CHAVAN V.N.[2]

[1]Department of Computer Science, Shri Shivaji Education Society Society Amravati's, Science College, Congress Nagar, Nagpur.
[2]Department of Computer Science, S. K. Porwal College, Kamptee, Dist. Nagpur.
*Corresponding Author: Email- rn_jugele@yahoo.com

Received: December 12, 2011; Accepted: January 15, 2012

Abstract- We have designed network method and implementation phase according to requirements and location of site place. During this we have collected more & more information regarding office functionality, present system and expectation form computer network which is to be analyzed. We have tried to consider each & every points, which is important during analysis and implementation phase of network. We have also considered cost factor, which plays important role during implantation of network in any company. We got more practical knowledge about network concept during implementation and trouble shooting of networking .
Keywords- IP address, Broadcast, network operator; networking; network user; Routers, topology requirements; active node; telecommunication networks

Citation: Jugele R.N. and Chavan V.N. (2012) The Design of Network in Implementation Phase. Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp-284-288.

Implementation

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

This protocol is used to assign IP addresses to hosts or workstations on the network. Usually a DHCP server on the network performs this function. Basically it "leases" out address for specific times to the various hosts. If a host does not use a given address for some period of time, that IP address can then be assigned to another machine by the DHCP server.When assignments are made or changed, the DHCP server must update the information in the DNS server.As with BOOTP, DHCP uses the machine's or NIC ethernet (MAC) or hardware address to determine IP addressassignments. The DHCP protocol is built on BOOTP and replaces BOOTP. DHCP extends the vendor specific area in BOOTP to 312 bytes from 64. RFC 1541 defines DHCP.

DHCP RFCs

DHCP RFCs are 1533, 1534, 1541, and 1542. Sent from DHCP server:

- IP address
- Netmask
- Default Gateway address
- DNS server addresse(s)
- NetBIOS Name server (NBNS) address(es).
- Lease period in hours
- IP address of DHCP server.

DHCP Lease Stages

Lease Request The client sends a broadcast requesting an IP address
Lease Offer The server sends the above information and marks the offered address as unavailable. The message sent is a DHCPOFFER broadcast message.
Lease Acceptance The first offer received by the client is accep ed. The acceptance is sent from the client as a broadcast (DHCPREQUEST message) including the IP address of the DNS server that sent the accepted offer.Other DHCP servers retract their offers and mark the offered address as available and the a cepted address as unavailable.
Server lease acknowledgement The server sends a DHCPACK or a DHCPNACK if an unavailable address was requested.
DHCP discover message The initial broadcast sent by the client

to obtain a DHCP lease. It contains the client MAC address and computer name. This is a broadcast using 255.255.255.255 as the destination address and 0.0.0.0 as the source address. The r quest is sent, then the client waits one second for an offer. The request is repeated at 9, 13, and 16 second intervals with addition al 0 to 1000 milliseconds of randomness. The attempt is repeated every 5 minutes thereafter. The client uses port 67 and the server uses port 68.

DHCP Lease Renewal

After 50% of the lease time has passed, the client will attempt to renew the lease with the original DHCP server that it obtained the lease from using a DHCPREQUEST message. Any time the client boots and the lease is 50% or more passed, DHCP the client will attempt to renew the lease. At 87.5% of the lease completion, the client will attempt to contact any DHCP server for a new lease. If the lease expires, the client will send a request as in the initial boot when the client had no IP address. If this fails, the client TCP/IP stack will cease functioning.

DHCP Scope and Subnets

One DHCP scope is required for each subnet.

DHCP Relay Agents

May be placed in two places:

- Routers
- Subnets that don't have a DHCP server to forward DHCP requests.

Client Reservation

Client Reservation is used to be sure a computer gets the same IP address all the time. Therefore since DHCP IP address assignments use MAC addresses to control assignments, the following are required for client reservation:

- MAC (hardware) address
- IP address

Exclusion Range

Exclusion range is used to reserve a bank of IP addresses so computers with static IP addresses, such as servers may use the assigned addresses in this range. These addresses are not assigned by the DHCP server.

DHCP Is a Message -

Based System

We might not think about DHCP in this way, but it's truly a client! Server system. When we install the TCP/IP protocol on a Windows client com-puter, the client component is smart enough to know how to go looking for a DHCP server and obtain its IP address, unless we configure it statically. The client broadcasts, looking for a DHCP server that can fulfill its needs; this step is called *DHCPDISCOVER.* DHCP is a message-based system that involves the sending of messages back and forth between the client and the server, and DHCPDISCOVER is only one of several transactional messages that might take place When a DHCP server answers the client's request, it offers the client an IP address (and associated configuration information); this step is called *DHCPOFFER.* If the DHCP server's scope is all used up and it can't supply the client with an IP address, it will send a *DHCPNAK* (NAK is "negative acknowledgement") instead of an offer. Multiple DHCP servers may acknowledge the client and offer an address. The DHCP client accepts the first offer that it receives.

Change to Windows 2000 DHCP :

Manual Allocation of IP Addresses

In the Windows NT 4 world, if we had a diskless workstation (sometimes called a *NetPC),* we had to install the BootP protocol on one or more of the NT boxes in order to answer BootP requests. Recall that BootP, a predeces-sor to DHCP, is a method whereby client computers request an IP address. DHCP does. Instead, the NT 4 administrator has to enter the IP data for his BootP machines on the server. This way, each requesting computer can obtain a unique IP address and associated configuration information.

DHCP Integrated into DNS

Since Windows 2000 is very DNS-oriented, DHCP was modified so that it now notifies DNS of its registered clients. This feature is enormously handy for non-Windows 2000 computers participating in DHCP. Prior to Win-dows 2000, if we had a Windows 95 comput-er that was participating in DHCP and had DNS running, we have to manually enter the DNS information for that client. Today, if we DHCP server is so configured, when a non-Windows 2000 client receives an IP lease from the DHCP server, a DNS record is created as well.

DHCP Integrated into RRAS

Suppose that we set up a Routing and Remote Access Services (RRAS) server with several modems and phone lines. We want to give our telecommuters automatic IP address information. DHCP and RRAS are now integrated in such a way that the RRAS server merely requests a block of IP addresses and is given 11 addresses, one for itself and 10 for clients. Then, if all 10 IP addresses are given out by the RRAS server, it merely requests another block of 10 addresses so it can handle additional RAS clients. In the NT 4 world, we would've had to configure a range of addresses for the RAS server to use.

DNS (DOMAIN NAME SERVICE) :

Host Names

Domain Name Service (DNS) is the service used to convert human readable names of hosts to IP addresses. Host names are not case sensitive and can contain alphabetic or numeric letters or the hyphen. A fully qualified domain name (FQDN) consists of the host name plus domain name as in the following example:

computername.domain.com

The part of the system sending the queries is called the resolver and is the client side of the configuration. The nameserver answers the queries. Read RFCs 1034 and 1035. These contain the bulk of the DNS information and are superceded by RFCs 1535-1537. Naming is in RFC 1591. The main function of DNS is the mapping of IP addresses to human readable names.

Three main components of DNS

1) resolver
2) name server
3) database of resource records(RRs)

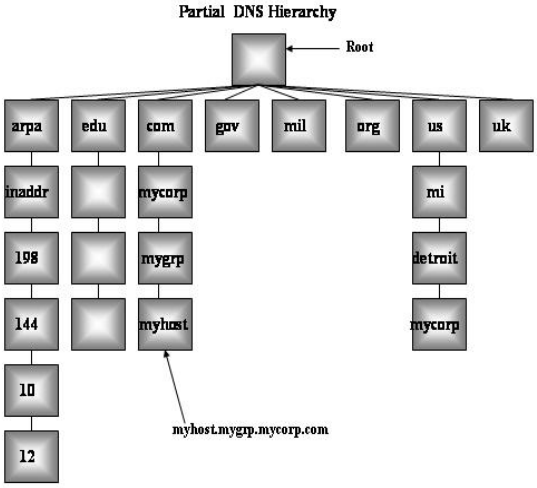
Domain Name System

The Domain Name System (DNS) is basically a large database which resides on various computers and it contains the names and IP addresses of various hosts on the internet and various domains. The Domain Name System is used to provide information to the Domain Name Service to use when queries are made. The service is the act of querying the database, and the system is the data

structure and data itself. The Domain Name System is similar to a file system in Unix or DOS starting with a root. Branches attach to the root to create a huge set of paths. Each branch in the DNS is called a label. Each label can be 63 characters long, but most are less. Each text word between the dots can be 63 characters in length, with the total domain name (all the labels) limited to 255 bytes in overall length. The domain name system database is divided into sections called zones. The name servers in their respective zones are responsible for answering queries for their zones. A zone is a subtree of DNS and is administered separately. There are multiple name servers for a zone. There is usually one primary nameserver and one or more secondary name servers. A name server may be authoritative for more than one zone. DNS names are assigned through the Internet Registries by the Internet Assigned Number Authority (IANA). The domain name is a name assigned to an internet domain. Access to the Domain name database is through a resolver which may be a program or part of an operating system that resides on users workstations.

Structure and message format

The figure below shows a partial DNS hierarchy. At the top is what is called the root and it is the start of all other branches in the DNS tree. It is designated with a period. Each branch moves down from level to level. When referring to DNS addresses, they are referred to from the bottom up with the root designator (period) at the far right. Example: "myhost.mycompany.com."



DNS is hierarchical in structure. A domain is a subtree of the domain name space. From the root, the assigned top-level domains are:

- GOV - Government body.
- EDU - Educational body.
- INT - International organization
- NET - Networks
- COM - Commercial entity.
- MIL - U. S. Military.
- ORG - Any other organization not previously listed.

Name Server Types

There are three types of name servers:

1. The primary master builds its database from files that werepreconfigured on its hosts, called zone or database files. The name server reads these files and builds a database for the zone it is authoritative for.
2. Secondary masters can provide information to resolvers just like the primary masters, but they get their information from the primary. Any updates to the database are provided by the primary.
3. Caching name server - It gets all its answers to queries from other name servers and saves (caches) the answers. It is a non -authoritative server.

The caching only name server generates no zone transfer traffic. A DNS Server that can communicate outside of the private network to resolve a DNS name query is referred to as forwarder.

DNS Query Types

There are two types of queries issued

1. **Recursive** queries received by a server forces that server to find the information requested or post a message back to the querier that the information cannot be found.
2. **Iterative** queries allow the server to search for the information and pass back the best information it knows about. This is the type that is used between servers. Clients used the recursive query.
3. **Reverse** - The client provides the IP address and asks for the name. In other queries the name is provided, and the IP address is returned to the client. A reverse lookup entry for a network 192.168.100.0 is "100.168.192.in-addr arpa".

DNS Files

CACHE.DNS - The DNS Cache file. This file is used to resolve internet DNS queries. On Windows systems, it is located in the WINNTROOT\system32\DNS directory and is used to configure a DNS server to use a DNS server on the internet to resolve names not in the local domain.

WINS (Windows Internet Name Server)

Creating a WINS Design

If we started a network from scratch with new applications and Win -dows 2000 Professional workstations for the users and Windows 2000 servers for server farm, we never have to use WINS on the network. It's when we have legacy applications requiring NetBIOS name resolution, or legacy Windows computers on the network (and Windows NT servers), that WINS must be involved. If we are working in that kind of environment and we are planning a Windows 2000 upgrade, we have almost undoubtedly got a WINS server or two.

The whole purpose of WINS is to resolve NetBIOS names to IP addresses by sending unicast messages across routers. In other words, WINS is designed to work with the shortcomings of broadcasting across a router, just as DNS does. So on a small network where we don't have any routers to cross, we may not need WINS at all. However, on larger networks, WINS can be a bandwidth saver. WINS clients will send a message directly to the WINS server asking it to resolve the NetBIOS name instead of broadcasting for a resolution. Any time we can cut down on broadcasts on network, it's a good thing.

WINS servers provide two major benefits on a network:

- They resolve NetBIOS names to IP addresses. While resolving names, WINS servers help reduce network broadcast traffic.
- WINS servers on a network can easily handle name registrations and "name resolution requests for 10,000 client computers.

Pushing and Pulling

If we have multiple WINS servers on a network, we should synchronize their databases with each other. To do this, set up what is called a *push/ pull partner* relationship. If the first server *sends* its contents to the second, that's called a *push.* If the first server *obtains* the contents of the second server on its own, it's called a *pull.* We can {and should} set up WINS servers so they update one another's database regularly. WINS servers can be push partners, pull partners, or push/pull partners. Pushes are based on a certain number of database updates, and pulls are based on time interval. If WINS servers have a slow WAN link between them, Microsoft recommends making them pull partners only, Proxy Server.

Types of Services Proxys Provide

- Caching
- Authentication/Authorizatiom
- Access Through a Firewall
- Anonymization

Proxy Servers can be used to perform the following functions.

- Control outbound connections and data.
- Monitor outbound connections and data.
- Cache requested data which can increase system bandwidth performance and decrease the time it takes for other users to read the same data.
- Application proxy servers can perform the following additional functions:
- Provide for user authentication.
- Allow and deny application specific functions.
- Apply stronger authentication mechanisms to some applications.

Configuring a Proxy Server

- The following packages are available in Linux:
- Ipchains soon to be replaced by netfilter (Packet filtering supported by the Linux kernel). It comes with Linux and is used to modify the kernel packet routing tables.
- SOCKS - Circuit Switching firewall. Normally doesn't come with Linux, but is free.
- Squid - A circuit switching proxy. Normally comes with Linux.
- Juniper Firewall Toolkit - A firewall toolkit product used to build a firewall. It uses transparent filtering, and is circuit switching. It is available as open source.
- The TIS Firewall Toolkit (FWTK). A toolkit that comes with application level proxies. The applications include Telnet, Rlogin, SMTP mail, FTP, http, and X windows. it can also perform as a transparent proxy for other services.

Firewalls

Firewalls are mainly used as a means to protect an organization's internal network from those on the outside (internet). It is used to keep outsiders from gaining information to secrets or from doing damage to internal computer systems. Firewalls are also used to limit the access of individuals on the internal network to services on the internet along with keeping track of what is done through the firewall.

Types of Firewalls

1. **Packet Filtering** - Blocks selected network packets.
2. **Circuit Level Relay** - SOCKS is an example of this type of firewall. This type of proxy is not aware of applications but just cross links and connects to another outside connection. It can log activity, but not as detailed as an application proxy. It only works with TCP connections, and doesn't provide for user authentication.
3. **Application Proxy Gateway** - The users connect to the outside using the proxy. The proxy gets the information and returns it to the user. The proxy can record everything that is done. This type of proxy may require a user login to use it. Rules may be set to allow some functions of an application to be done and other functions denied. The "get" function may be allowed in the FTP application, but the "put" function may not.

Packet Filtering Firewalls

In a packet filtering firewall, data is forwarded based on a set of firewall rules. This firewall works at the network level. Packets are filtered by type, source address, destination address, and port information. This type of firewall is fast, but cannot allow access to a particular user since there is no way to identify the user except by using the IP address of the user's computer, which may be an unreliable method. Also the user does not need to configure any software to use a packet filtering firewall such as setting a web browser to use a proxy for access to the web. The user may be unaware of the firewall. This means the firewall is transparent to the client.

Circuit Level Relay Firewall

A circuit level relay firewall is also transparent to the client. It listens on a port such as port 80 for http requests and redirect the request to a proxy server running on the machine. Basically, the redirect function is set up using ipchains then the proxy will filter the package at the port that received the redirect.

Ipchains and Linux Packet filtering

The administration of data packet management is controlled by the kernel. Therefore to provide support for things like IP masquerading, packet forwarding, and port redirects, the support must be compiled into the kernel. The kernel contains a series of tables that each contain 0 or more rules. Each table is called a chain. A chain is a sequence of rules. Each rule Firewalls contains two items.

1. **Characteristics** - Characteristics such as source address, destination address, protocol type (UDP, TCP, ICMP), and port numbers.
2. **Instructions** - Instructions are carried out if the rule characteristics match the data packet.

The kernel filters each data packet for a specific chain. For instance when a data packet is received, the "input" chain rules are checked to determine the acceptance policy for the data packet. The rules are checked starting with the first rule (rule 1). If the rule characteristics match the data packet, the associated rule instruction is carried out. If they don't match, the next rule is checked. The rules are sequentially checked, and if the end of the chain is reached, the default policy for the chain is returned. Chains are specified by name. There are three chains that are available and can't be deleted. They are:

1. Input - Regulates acceptance of incoming data packets.

2. Forward - Defines permissions to forward packets that have another host as a destination.
3. Output - Permissions for sending packets.

Each rule has a branch name or policy. Policies are listed below:

- ACCEPT - Accept the data packet.
- REJECT - Drop and the packet but send a ICMP message indicating the packet was refused.
- DENY - Drop and ignore the packet.
- REDIRECT - Redirect to a local socket with input rules only even if the packet is for a remote host. This applies to TCP or UDP packets.
- MASQ - Sets up IP masquerading. Works on TCP or UDP packets.
- RETURN - The next rule in the previous calling chain is examined.

Conclusion

We concluded that during study of implementation phase we have get opportunity to learn regarding How to trouble shoot the problem of networking, What are the necessary steps when we have to design network for any company? How can we consider every person requirements? During implementation of network, we have to analyze the need for networking at the company. As good network administrator we have to apply necessary measure for securing the entire network, so that it is difficult to penetrate the network for intruders, hackers and many more and resources should be access quickly.

References

[1] Braden B., Clark D and Shenker S. (1993) *Integrated Services in the Internet Architecture : an Overview, Internet Draft*.
[2] Comer D. and Stevens D.L. (1991) *Internetworking with TCP/ IP, Volume II, Prentic-Hall, Englewood Cliffs, NJ*.
[3] Feng T. (1981) *A Survey of Interconnection Networks, Computer,* Volume 14, Number 12, Pages 12-27.
[4] Goddard I.J. and Baker N. (1988) *Conference Record of the International Conference on Communications (ICC)*, Philadelphia, PA, USA.
[5] Hattig M. (1999) *Internet Engineering Task Force, Internet Draft, Work in progress*.
[6] Ivens K. and Hallberg B. (1996) Inside Windows NT Workstation 4, New Rider Publishing, Indianapolis, IN.
[7] Jugele R.N., Hedau M.J. and Chavan V.N., *Planning Phase Networking Service Industries*, 99th Indian Science Congress.
[8] Tony King (1998) *BT Technology Journal*, vol. 16, no. 1, pp. 9 -15.
[9] Radhakrishnan S. (1999) *The University of Kansas, Information and Telecommunication*, Technical Report.
[10] Moser M., Sugiura S., Sugawara K. and Shiratori N. (1995) *Intenational Conference on Network Protocols (ICNP), Tokyo, Japan*.