1.- Bosque DNS

Podemos entender como bosque DNS (Sistema de Nombres de Dominios), como un sistema de nomenclaturas (nombres) que permite identificar el nombre físico de una computadora, servicio o cualquier otro recurso o dispositivo que se encuentre conectado en una red de internet, en la cual se adjudica una etiqueta de identificación a cada uno de los objetos que se encuentren en la red con el fin de localizar y direccionar servicios o recursos que cada uno de estos dispositivos solicite a nuestro servidor.

Entre otras palabras un Bosque DNS es el compendio de nombre de todos lo dispuesto en nuestra red, en esta lista podemos identificar a los recursos por IP, un segmento de red o la MAC Address.

De esta manera será mas fácil recordar la ruta que deben tomar los paquetes en entramado y encapsulado de los mismos al momento de usar los servicios que nos brinda el protocolo TCP/IP, evitando la perdida de paquetes y agilizando los pool de conexión entres estos.

Al igual que los Routers y AP de Capa 3 el direccionamiento de equipos permite mantener una comunicación constante con los dispositivos permitiendo ahorrar recursos y mantener la red funcional para realizar otras actividades, aunado a ellos permitirá consumir recursos como FTP, SMTP con el uso de los sufijos (etiquetas , alias) que se encuentren en nuestra lista de DNS.

2.- Mascara de Subred

La máscara de subred permite agrupar un total de dispositivos que se encuentren en nuestra red (segmentos de red) con el fin de direccionar o agilizar la comunicación entre dispositivos del mismo segmento, al mismo tiempo permite indicar a dicho segmento si puedes o no ver a otros segmentos de red, bloquear accesos a diferentes direcciones de red o inclusive decirle al segmento que tanto potencial de red tendrá al momento de usar y compartir recursos, estos segmentos de red pueden estar en la misma red troncal pero cada segmento tendrá a disposición diferentes recursos y servicios.

Para determinar los segmentos de red y la cantidad de dispositivos que contendrá, es necesario hacer uso de el sistema de particionamiento de red conocido como VLSM (Variable Length Subnet Mask) o Mascara de Longitud Variable, mejor conocido como subneteo de red, el cual es un calculo que permite el fraccionamiento de la red de manera estable y eficiente.

Ejemplo:

Dada la red 192.168.0.0/24, se requiere desarrollar el direccionamiento que cumpla con los siguientes requerimientos.

Una subred de 20 hosts para ser asignada a la VLAN de Profesores

Una subred de 80 hosts para ser asignada a la VLAN de Estudiantes

Una subred de 20 hosts para ser asignada a la VLAN de Invitados

Tres  subredes de 2 hosts para ser asignada a los enlaces entre enrutadores.

**Solución**

Ordeno las subredes en orden decreciente: 80, 20, 20, 2, 2, 2.

Para 80 hosts necesito 7 bits (2^7=128, menos red y broadcas 126 hosts máx.), por lo tanto el prefijo de subred del primer bloque sería /25 (8-7=1; 24+1=25) Tomando la subred cero, la primera dirección de subred sería 192.168.0.0/25, broadcast 192.168.0.127, por lo tanto el rango asignable sería .1 hasta .126.

Para 20 hosts necesito 5 bits (2^5=32, es decir 30 hosts máx.). Prefijo: /27 (8-5=3, 24+3=27); Dir. de red: 192.168.0.128/27, broadcast 192.168.0.159. Rango asignable .129-.158.

La siguiente subred es del mismo tamaño y el prefijo es el mismo. Dir. de red: 192.168.0.160/27 , broadcast 192.168.0.191, rango .161-.190.

Los enlaces entre enrutadores sólo necesitan 2 bits (2^2=4, es decir 2 hosts máx) por lo tanto el prefijo debe ser /30 (8-2=6, 24+6=30). Dir. de enlace 1: 192.168.0.192, dir. de broadcast en enlace 1: 192.168.0.195, rango .193-.194.  Dir. enlace 2: 192.168.0.196/30, broadcast en enlace 2: 192.168.0.199, rango .197-.198. Dir. enlace 3: 192.168.0.200/30, broadcast enlace 3: 192.168.0.203, rango: .201-.202.

El esquema resultado es:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Red | Dir | Broadcast | Rango | Máscara |
| Estudiantes(80) | 192.168.0.0/25 | 192.168.0.127 | .1-.126 | 255.255.255.128 |
| Profesores(20) | 192.168.0.128/27 | 192.168.0.159 | .129-158 | 255.255.255.224 |
| Invitados(20) | 192.168.0.160/27 | 192.168.0.191 | .161-190 | 255.255.255.224 |
| Enlace 1(2) | 192.168.0.192/30 | 192.168.0.195 | .193-194 | 255.255.255.252 |
| Enlace 2(2) | 192.168.0.196/30 | 192.168.0.199 | .197-198 | 255.255.255.252 |
| Enlace 3(2) | 192.168.0.200/30 | 192.168.0.203 | .201-202 | 255.255.255.252 |
|  |  |  |  |  |

Se puede observar que los rangos de direcciones asignados son contínuos y que queda disponible para crecimiento futuro un rango de direcciones desde 204 en adelante.

Hay que recordar que en todos los aspectos del subneteo siempre debe respetarse la IP para la Puerta de enlace y la IP que se requiere para el broadcast, este ejemplo es para el segmentado de red clase B, ya que la clase A,C,D,E son IP's que se utilizan para investigación y sector privado.

**3.- Puertos de Enlace**

Podemos definir puerto de enlace o gateway, como un dispositivo que puede ser una computadora, que permite interconectar dispositivos con protocolos y arquitecturas de red distintos a todos los niveles de comunicación.

El Geteway tiene la capacidad de acceso a redes externas por lo que este resuelve dicha petición mediante la traducción de las IP realizando un NAT (Network Address Translation), esta capacidad de traducción, además permite aplicar una técnica de IP Masqueranding (enmascaramiento de IP) que se realizar para asignar una sola IP como puerta de enlace y dar acceso a la red externa desde dicho puerto.

Esta es la ruta por defecto que se le asigna a un equipo y tiene como función principal direccionar o enviar cualquier paquete de información a su destino en la línea de comunicación que le corresponde esto se realizar por la ruta predeterminada de los equipos cuando estas rutas son desconocidas para la interfaz de la red.

La dirección por defecto del Gateway se parece a 192.168.1.1 o 192.168.0.1

**4.- Grupos de Trabajo**

Un grupo de trabajo se define como el conjunto de computadoras que comparten diferentes recursos en la red (Imágenes, Videos, Audio, Documentos), es una forma rápida y fácil de compartir estos recursos ya que no se requiere de un Cliente / Servidor que resuelva las peticiones que se generen a partir de estas solicitudes.

Para estos grupos de trabajo no solo se puede compartir información sino también recursos como impresoras, cama del equipo, servicios de internet entre otros, y permite dar privilegios a los grupos para realizar dichas actividades de manera frecuente.

Estos grupos usualmente son empleados en redes locales para facilitar la trasferencia de archivos y el uso de herramientas en un equipo determinado, para esta funcionalidad es indispensable nombrar al equipo de una manera única y especifica que permita su identificación inmediata y de esa maneta poder agregarla a la libreta de direcciones o equipos del grupo de trabajo

**5.- Servidor de Dominio**

Un servidor de dominios o servidor de nombres, es un servidor en la red que mapea todos los dispositivos conectados en la red con el fin de identificar cada uno de ellos mediante la IP o la Dirección Física del equipo (MAC Address) o de igual manera puede darse el uso de la traducción de las rutas de un sitio web ya que para ello los navegadores no pueden identificar de manera natural los esquemas de red que emplean los protocolos web como lo son los HTTP y HTTPS.

Claramente podemos denotar que este servisio

**6.- Servidor de Correo Electrónico**

Al igual que los servidores de dominós y los servidores web, estos son servidores dedicados a la programación y almacenamiento de correos electrónicos que permiten entre otras cosas gestionar y direccionar los correos entre diferentes servicios o aplicaciones de correo electrónico desde una computadora a otra.

En un servidor de correos podremos encontrar los siguientes protocolos:

SMTP: Simple Mail Transfer Protocol (Protocolo de Transferencia), es el protocolo que se encarga de enviar un correo desde un servidor de correo a otro o bien desde una aplicación Cliente / Servidor a un Servidor de Correo, un punto importante de este protocolo es que no requiere autentificación para enviar y entregar los correos enviados lo que permite que cualquier persona en la red pueda enviar mensajes a cualquier otra persona en la red o a grandes grupos de personas haciendo posible los correos basura o spam.

POP: Post Office Protocol, es empleado en el servidor web para recibir e interpretar los correos enviados a través del SMTP, para este protocolo se pueden emplear capas de seguridad como las SSL (Secure Socket Layer), para la autentificación de los clientes y las secciones de transferencia de datos. Actualmente existe la versión POP3 que permite automatizar la entrega de los mensajes y eliminarlos después de un tiempo determinado para ahorrar espacio en el servidor y cuenta con seguridad adicional para la autentificación de los clientes.

IMAP: Internet Message Access Protocol, su finalidad es la misma que el POP pero a diferencia de este, mantiene y administra los correos recibidos para poder borrarlos en tiempo indefinido además de permitir a los clientes, archivar, borrar y renombrar los correos para su clasificación posterior.

Un servidor de correo consta de 2 servidores: un servidor SMTP que se encarga de enviar los mensajes y un servidor POP que se encarga de recibir los mensajes, mientras que el IMAP se encarga de enlazarlos y enviarlos en la red.

Estos servidores virtuales o protocolos son los encargados de administrar y gestionar los servicios de emisión y recepción de los correos así como el de traducir los paquetes binarios y ser mostrados como mensajes entendibles por el cliente.

**Programas de Correos Electrónicos:**

Mercury Mail Server: Disponibles para Windows, Linux

Microsoft Exchange Server: Disponible para Windows

Zimba: Linux, Windows

Lotus Dominio: Linux, OS400, Windows