Universidad Tecnológica Fidel Velázquez
Ingeniería en Redes Inteligentes y Ciberseguridad - Administración de Redes Empresariales

Resolver el siguiente ejercicio contestando únicamente en las hojas. Enviar un sólo archivo en formato PDF a través de la plataforma Google Classroom. Valor de la actividad: 10 puntos.

Nombre del estudiante	
Fecha de la actividad	
Calificación	

Práctica 5: Escalabilidad de Red y Servicios de Resolución (DHCP y DNS BIND)

1. Introducción y Visión General del Laboratorio

Objetivo de la práctica: Al finalizar esta sesión, el estudiante habrá escalado la red estática de la práctica anterior hacia un modelo dinámico y centralizado. El servidor `master` será configurado para asignar direcciones IP automáticamente (DHCP) y resolver nombres de dominio localmente (DNS) para los clientes `c10` y `c20`. Además, se analizarán los principios matemáticos que rigen el rendimiento de estos servicios.

Prerrequisitos:

- Las tres máquinas virtuales (`master`, `c10`, `c20`) de la Práctica 3 y 4.
- Acceso con el usuario `root`.
- Adaptadores de red en modo *Bridged* (Puente) o en su defecto Red Interna si se configuran correctamente los enrutadores.

---

2. Módulo 1: Fundamentos Matemáticos Teóricos

Antes de configurar los servicios, es imperativo comprender la teoría matemática que sustenta la administración de la red.

2.1. 1. Matemáticas del Subnetting (Direccionamiento IPv4)

El protocolo DHCP requiere la definición de un ámbito de red. La cantidad de hosts (dispositivos) que se pueden asignar en una subred depende directamente de los bits de la máscara de red. La fórmula matemática para calcular el máximo número de hosts válidos en una subred es:

$$\text{Hosts} = 2^n - 2$$

Donde n es el número de bits destinados a la porción de host. Se restan 2 porque la primera dirección identifica la red y la última es la dirección de difusión (broadcast). En nuestro laboratorio, utilizamos una red `/16`, lo que deja 16 bits para hosts, permitiendo un máximo de $2^{16} - 2 = 65534$ direcciones útiles.

2.2. 2. Teoría de Colas (Rendimiento del Servidor DNS)

Un servidor DNS procesando peticiones de clientes puede ser modelado matemáticamente mediante la Teoría de Colas, específicamente usando el modelo estocástico M/M/1. En este modelo:

- Las peticiones DNS llegan de forma aleatoria siguiendo un proceso de Poisson con una tasa de llegada promedio λ (consultas por segundo).
- El tiempo que tarda el servidor DNS en buscar en su base de datos y responder sigue una distribución exponencial con una tasa de servicio promedio μ.

El nivel de saturación o utilización del servidor (ρ) se calcula como:

$$\rho = \frac{\lambda}{\mu}$$

Para que el servidor DNS sea estable y no colapse, se debe cumplir obligatoriamente que $\rho < 1$. Si la red crece, el tiempo promedio que una consulta DNS pasa en el sistema (W, tiempo de espera más tiempo de procesamiento) se define matemáticamente como:

$$W = \frac{1}{\mu - \lambda}$$

Este modelo demuestra que a medida que λ se acerca a la capacidad máxima μ, el tiempo de latencia W tiende al infinito, lo que requiere escalar el servidor añadiendo caché o hardware adicional.

---

3. Módulo 2: Configuración del Servidor DHCP en `master`

El protocolo DHCP automatizará la entrega de parámetros de red.

1. **En `master`:** Instala el paquete del servidor DHCP.

```
yum install -y dhcp
```

2. **En `master`:** Copia el archivo de configuración de ejemplo para tener una plantilla base.

```
cp /usr/share/doc/dhcp*/dhcpd.conf.example /etc/dhcp/dhcpd.conf
```

3. **En `master`:** Edita el archivo de configuración principal.

```
nano /etc/dhcp/dhcpd.conf
```

   Borra el contenido y agrega la siguiente configuración para nuestra red de laboratorio (172.24.0.0/16):

```
subnet 172.24.0.0 netmask 255.255.0.0 {
  range 172.24.0.50 172.24.0.100;
  option routers 172.24.0.1;
  option domain-name-servers 172.24.0.1;
  option domain-name "example.com";
  default-lease-time 600;
  max-lease-time 7200;
}
```

Guarda con ***Ctrl+O****, presiona* ***Enter*** *y sal con* ***Ctrl+X****.*

4. **En `master`:** Inicia el servicio y habilítalo para el arranque del sistema.

```
systemctl start dhcpd
systemctl enable dhcpd
systemctl status dhcpd
```

(Verifica que diga ***active (running)*** *en color verde).*

---

4. Módulo 3: Configuración del Servidor DNS (BIND) en `master`

Sustituiremos el archivo manual `/etc/hosts` por un servidor DNS real utilizando BIND.

1. **En `master`:** Instala los paquetes necesarios.

```
yum install -y bind bind-utils
```

2. **En `master`:** Edita el archivo principal de BIND.

```
nano /etc/named.conf
```

Modifica las siguientes dos líneas para que el servidor escuche y responda a cualquier IP de nuestra red de laboratorio:

```
listen-on port 53 { any; };
allow-query       { any; };
```

3. **En `master`:** Define las zonas directa e inversa.

```
nano /etc/named.rfc1912.zones
```

Agrega al final del archivo:

```
zone "example.com" IN {
        type master;
        file "example.com.zone";
};

zone "0.24.172.in-addr.arpa" IN {
        type master;
        file "172.24.0.db";
};
```

4. **En `master`:** Crea el archivo de la **Zona Directa** (traduce nombres a IPs).

```
nano /var/named/example.com.zone
```

Agrega este contenido exacto:

```
$TTL 86400
@   IN  SOA     master.example.com. root.example.com. (
        2024021301  ; Serial
        3600        ; Refresh
        1800        ; Retry
        604800      ; Expire
        86400 )     ; Minimum TTL

@       IN  NS      master.example.com.
master  IN  A       172.24.0.1
c10     IN  A       172.24.0.10
c20     IN  A       172.24.0.20
www     IN  CNAME   master
```

5. **En `master`:** Ajusta los permisos de los archivos creados para que el servicio pueda leerlos.

```
chown root:named /var/named/example.com.zone
```

6. **En `master`:** Inicia y habilita el servicio DNS.

```
systemctl start named
systemctl enable named
systemctl status named
```

(Opcional) Si tu firewall está activo, debes permitir el tráfico en el puerto 53 UDP:

```
firewall-cmd --permanent --add-port=53/udp
firewall-cmd --reload
```

---

5. Módulo 4: Pruebas de Integración en los Clientes

Ahora verificaremos que los clientes `c10` y `c20` puedan obtener su configuración de forma dinámica y resolver nombres a través de nuestro nuevo servidor DNS.

1. **En `c10` y `c20`:** Cambiaremos el adaptador de IP estática a dinámica por DHCP.

```
nano /etc/sysconfig/network-scripts/ifcfg-ens33
```

   - Cambia `BOOTPROTO="static"` a `BOOTPROTO="dhcp"`.
   - Borra las líneas `IPADDR` y `NETMASK` (si existen).
   - Guarda el archivo y reinicia la red:

```
systemctl restart network
```

2. **En `c10`:** Verifica la IP asignada.

```
ip a s
```

Deberías recibir una IP dentro del rango `172.24.0.50` a `172.24.0.100` que definiste en el DHCP.

3. **En `c20`:** Prueba el servidor DNS consultando una dirección web y la IP del master.

```
nslookup master.example.com
```

La salida debería mostrar que el "Serverrespondiendo es tu **`master`** *y devuelve la .Addressçorrecta.*

4. **Opcional (Herramienta avanzada de DNS):** Para ver métricas y rendimiento del DNS, utiliza el comando `dig`.

```
dig c10.example.com
```

6. Conclusión

Al culminar esta práctica, el laboratorio simula de forma fidedigna una arquitectura corporativa real. El servidor central es ahora el responsable de gestionar los alquileres de direcciones dinámicas (DHCP) y de centralizar la libreta de direcciones lógica de toda la red (DNS), eliminando la dependencia de configuraciones estáticas manuales y mitigando los problemas de escalabilidad calculados mediante la teoría de colas.