Erick Vargas

Redes III

Contents

1 Introducción

1.1 Temario

1. Administración de redes de computadoras
   (a) Administración de redes de computadoras
   (b) Administración de redes en el modelo OSI
   (c) Servicios de administración común de información (CM15)
   (d) Protocolo de administración comín de información (CM1P)
   (e) El nivel de administración en OSI
   (f) Administración del sistema (SMAP, SMAE, SMASE)
   (g) Administración de fallas
   (h) Administracion de configuraciones
   (i) Administracion de rendimiento
   (j) Administracion de seguridad
   (k) Administracion de objetos
   (l) Monitoreo de la carga de trabajo
2. Administración de switch y ruteadores
   (a) Configuración básica de switch y ruteadores
      i. Asignación de nombres y contraseñas
      ii. Configuración de interfaces
      iii. Copias de respaldo
      iv. Ruteo estático
      v. Ruteo dinámico (RIP, OSPF, IGRP)
      vi. Administración del tráfico IP

vii. Traducción de direcciones de red
viii. Redes de área local virtual (VLANs)

3. Protocolo simple de administración de red (SNMP)
   (a) Introducción a SNMP
   (b) Administraciones de alarmas SNMP
   (c) Bases de datos de administración MIB
   (d) Tipos y estructuras de paquetes SNMP
   (e) SNMPv3
   (f) Capas de comunicación
   (g) Ventajs y desventajas de la implantación de un administrador SNMP
4. Monitorización de la administración de red
   (a) El proceso y principios de monitorización
   (b) Monitorizción para la administración de redes
   (c) Recolección, análisis y notificación
   (d) Análisis de tráfico y su limitación
   (e) Los sitemas NSM
   (f) Arquitectura de RMON
   (g) RMON
   (h) Comparación de RMON y RMON 2
5. Calidad de servicio en red
   (a) Introducción
   (b) Calidad de servicio en internet
   (c) Servicios integrados
   (d) Protocolo RSVP
   (e) Arquitectura de servicios diferenciados
   (f) MPLS (MultoProtocol label switching)
6. Administración del sistema
   (a) Configuración y servicios de red
   (b) Convivencia de los sitemas operativos
   (c) Servicores DNS y DHCP
   (d) Servidores de correo electrónico y POP
   (e) Servidores de red
   (f) Entornos PXE

1.2 Evaluación

	Primer parcial	Segundo parcial	Tercer parcial
Prácticas	40%	40%	40%
Examen teórico	30%		
Examen práctico	30%	60%	
Proyecto final			60%
Tareas	+10%	+10%	+10%

Miércoles 8:30 - 12:00, edificio central, al lado del laboratorio de física

1.3 Fechas importantes

- 6 de septiembre, examen primer parcial práctico y teórico entrega 13 de septiembre
- 18 de octubre, examen segundo parcial, entrega 25 de octubre.
- 28 de octubre, proyecto final, entrega 29 de noviembre.

1.4 Reglas

- Tareas y prácticas 1 semana para ser subida al moodle
- Semana extra para entregar (calificación sobre 5)

1.5 Bibliografía

- Henshall, Shaw S. (1990). OSI Explained, End-to-end Computer Communication Standards. 2nd ed. England, Ellis Horwood Ed.
- Lewis, C. (1999) Cisco switched Internetworks. VLANs, ATM, Voice/Data Integration 1st Ed. Editorial, McGraw Hill
- Stalling, W. (2004) Redes e internet de alta velocidad, rendimiento y calidad de servicio
- Stalling, W. (1999) SNMP, SNMPv2, SMNPv3 and RMON y RMON2, Ed. Addison-Wesley
- Alegria I. Cortiñas R. (2005) Administración del sistema y la red, LINUX Editorial Person

2 Direcciones IP

- Clase A hasta 127
- Clase B hasta 191
- Clase C en adelante

3

Unidad II

3.1 Modelo OSI

Pensemos en administración en la integración de varios elementos para manejar de forma eficiente y eficaz el manejar las edes de computadoras.

- Administrar: planificación de la mejor manera para una mejor gestión de la red-
- Gestionar: implementación de modificaciones y crreccionaes para alcanzar los objetivos de la red

Administración de sistemas

Suma total de las políticas y procedimientos que intervienen en la configuración, control y monitoreo que conforman una red, con el fin de aseurar el eficiente y efectivo empleo de sus recursos.

Se le solicita a la ISO que diseñe un modelo de administración OSI

Modelo de administración OSI

La Organización de Estándares INternacionales creó una comisión para crear un modelo de administración de redes, bajo la dirección del grupo OSI.

Surge como un modelo que involucra tanto la PC como la red, buscando una coordinación e integración entre si aún que se traten de modleos distintos.

Modelo de administración de redes OSI (OSI-NMM)

Es un modelo estándar que proporciona el marco conceptual para la organización de una amplia gama de recursos de la red.

Planificación de la capacidad de red

Gestión del rendimiento de la red

Comprende la administración de sistemas que delimita la operación de cualquiera de las 7 capas del modelo OSI, y la administración de los objetos gestionados, Plantea los modelos de:

- Organización
- Información
- Comunicación
- Función

Modelo organizacional

Describe lso componentes de la administración de redes tales como administrador, agente y otros, y sus interrelaciones. Sus relaciones vienen dadas por la arquitectura de red.

El modelo organizacional del modelo OSI define los bloques y la relación entre estos.

Es una estructura dividida en dominios de red, los cuales comprenden su operabilidad y ofrece soporte de los aspectos de gestión del mismo.

Define conceptos para una gestión cooperativa, como para una gestión basada en jerarquías:

- COncepto simétrico - entre dominios
- Concepto asimétrico - entre dominios y subdominios

Dominio ejemplo www.ipn.mx
www.escom.ipn.mx
www.saes.escom.ipn.mx Dónde el tercer y segundo ejemplo son subdiminios del primero

Gestión de dominios

Define la división de entorno, teniendo en cuenta dos moibos principales:

- Políticas funcionales, donde se incluyen políticas de seguridad contabilidad etc
- Políticas no funcionales, como la gestión geográfica, tecnologías, etc

Sub modelo informativo

Trata de la estructura y almacenamiento de la información relativa a la administración de la red

Esta información se guarda en una base de datos la cual recube nombre de base de datos de información de administración **(MIB)** Es un archivo que guarda información sobre nuestras redes, el cual se encuentra en todas las capas de administración.

Sub modelo conunicacional

Habla de la forma como se comunican los datos de administración en el proceso gestir-agente

Atiende lo relacionado con el protocolo de transporte, el protocolo de aplicaciones y los comandos y respuestas entre pares. (Como me comunico, como lo hago, formato de mis tramas, que protocolos usaré, etc.)

Modelo funcional

Divide la complejidad de la administración en áreas funcionales de administración e intenta especificar funciones de administración genéricas.

EL modelo funcional proporciona las bases para construir librerías y soluciones.

áreas de administración del modelo OSI

- Administración de fallas (fault management)
- Administracion de configuración (configuration management)
- Administración de estadísticas y contabilidad (accounting amanager) [Comportamiento de la red y si todo está dentro de los rangos permitidos, además de saber cuanto se va a cobrar]
- Administración de desempeño (performance management) [Que todo este funcionando bien, saber si es posible hacer mejoras, etc.]
- Administración de seguridad (security management) [Quién tiene acceso a que si quien trata de accesar tiene permisos, etc]

3.1.1 CMIS (Servicios de interopabilidad de gestión de contenidos)

Es un estándar, solo sabemos que cosas debe hacer. CMIS permite la interoperabilidad entre los distintos servicios que tenemos, el gestor hace pull-in y recaba información de todos los agentes.

T-1.1 Levantar la siguiente topología GNS3 192.168.0.0/24: Bajar las ISOS router3600, Switch3600 crear dos máquinas virtuales basadas en linux.

```
enable
conf
configure ter
configure terminal
inte
interface e
ip add
ip address
ip address 192.268.0.1 255.255.255.128
no shutdown
e
exit
inte e 0/1
ip address
```

3.2 CMIS (Servicio de interoperabilidad de gestión de contenidos)

Surge como un impulso de varias instituciones privadas.

Estandar abierto de OASIS diseñado para la interoprabilidad de lso sistemas de gestión de contenidos a través d einternet

A través d euna capa de abstración permite la gestión de contenidos.

3.2.1 Sistema de gestión de contenidos o CMS

Podemos hacer una analogía con el periódico, antes si se compraba un periódico a cualquier hora del día tenías la misma información, hoy en día tienes información en tiempo real, además de tener aglomeradas varias fuentes. CMS funciona de esta manera, un manejo dinámico de la información.

Aplicación que explota un entorno de trabajo para la creación y administración de contenidos.
Se usa intensamente en páginas web.
Usa una o varias bases de datos para alojar el contenido del sitio web.
Permite manejar de forma independiente el contenido y el diseño.

3.2.2 Objetivos

CMIS fué diseñado para majorar los sitemas de administración de contenido empresarial que existen junto con sus interfaces de aplicación actual junto con una capa de abstracción que nos permite homogeneizar la información.

3.2.3 Historia

EMC, IBM y Microsoft propusieron este formato.

Las tres empresas enviaron de forma conjunta CMIS a OASIS. Esta propuesta fue aprobada en 2010 y tuvo una actualizació en 2012.

3.2.4 Definiciones

- Modelo de dominio
- Enlaces de servicios web
- Rest ful y AtomPub: Difusión web usando XML y un protocolo simple basado en HTTP

3.2.5 Enfoque de CMIS

CMIS se enfoca en las capacidades de contenido básico d eun sistema de administración de contenido empresarial, las cuales son la **creación, lectura, escritura, borrar y funciones de petición** todo se maneja jerarquicamente como un árbol.

3.2.6 Alcances CMIS

CMIS incorpora conceptos contemporáneos de una orientación de servicios web y especificaciones ambas basadas en SOAP y REST (Estos últimos nos permiten tener una interoperabilidad entre objetos).

3.2.7 CMIS

Los trabajadores pueden usar una única aplicación para acceder e intercambiar contenido que esta almacenado en varios sistemas de gestión empresarial sin importar que sean diferentes las computadoras.

Otros estándares

- JCR Java Content Repository (Bastante complicado de utilizar)
- WebDAV (Muy jóven)

3.2.8 Funciones genéricas de CMIS

Crear, acceder a versiones de documentos y crear, leer actualizar, relacionar y borrar obketos

3.2.9 Object identity ODI

En el momento que se crea un objeto se crea un OID el cual es intransfereible (como una primary key de un objeto).

Jerarquía de documentos

Se usan folders y usa unaestructura de árbol normal, se manejan archivos completos y sin flujo de contenidos '

3.2.10 CRUD

- Creación
- Recuperación
- Actualización
- Eliminación

3.3 CMIP

CMIS es un protocolo!, no nos dice como hacer las cosas solo como deben hacerse las cosas. Desarrollado por la ISO, ofrece un mecanismo de transporte en la forma de servicio pregunta-respuesta para las 7 capas del modelo OSI. Imaginemos que tenemos una PC que ejecuta un software de administración de servicios y diversos dispositivos de red (Switch, routers, PC, etc) en cada uno de esos dispositios está en ejecución un pequeño programa llamado agente, mientras que en en la PC que tiene el software de administración de servicios tenemos el gestor. El gestor usando pull-in hace preguntas a los agentes (Dame información en el MIB (Base de Información de Administración), el agente responde). El recaba información, realiza estadisticas etc. Posteriormente el gestor envia una respuesta con el fin de ajustar algo en los agentes. Finalmente los dispositivos de red responden si se ha hecho lo que el gestor ha pedido.

Es considerada como parte d euna arquitectura de administración de red, que provee mecanismos de intercambio de información, entre un administrador y elementos remotos de red, cuyo funcionamiento está basado en los servicios CMIP.

Los sistemas de administración de red, basados en CMIP son utilizados en la administración de:

- Redes de área local, LAN.
- Redes corporativas y provadas de área amplia.
- Redes nacionales e internacionales.

Define la información en términos de objetos administrados.
Permite su modificación y acciones sobre archivos

3.3.1 Sistemas de administración de red o NMS

Es un conjunto de aplicaciones que supervisan y controlan los dispositivos administrados.

Proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red.

Uno o más NMS deben existir en cualquier red.

3.3.2 Unidad de datos de protocolo de aplicación

Las tramas que utiliza CMIP para su funcionamiento

3.3.3 Caracteristicas del protocolo

- Ocupa muchos recursos
- Tramas muy grandes
- Peticiones muy complicadas de realizar

3.3.4 Protocolos del CMIP

ACSE, ROSE, CMISE

4 Configuración básica de R1 y Routers

4.1 Conexiones a la interfaz de comandos

- Terminal de consola: podemos hacerlo de forma local
- Telnet/SSH: nuestro propia red de internet (La primera es sin protección la otra de forma segura)

4.2 Acceso a la interfaz de comando CLI.

Interfaz de Línea de Comandos. Requerimos cuenta de usuario. La consola muestra algo más o menos así.

```
dispositivo:ruta>comando                \\Switch
dispositivo:ruta#comando                \\Router
dispositivo:ruta(enable)#comando
dispositivo:ruta(config)a#comando
dispositivo:ruta(config-vlan)#comando
dispositivo:ruta(config-it)#comando
```

Si en el prompt tenemos el símbolo > estamos en modo switch y en modo router tenemos otro símbolo el cual provee más permisos, tenemos modo de privilegio y finalmente configuración específica.

Podemos tener del 0 - 15 modelos de dispositivo, en los dispositivos CISCO hay 0, 1 y 15. Podemos definir el medio y asignar diverss permisos o comandos de ejecucion generando nuevos grupos.

4.2.1 Modos de acceso

- Solo lectura: show

- Lectura-escritura: set show

4.2.2 USAMOS GNS3

- 1. crear proyecto nuevo
- 2. Cuantas direcciones IP requiero para una comunicación troncal? Requiero dos, pero también la IP y dirección de broadcast, además la máscara es decir 10.10.0.0/30,

Configuramos Router 1 abriendo consola:

```
R1#disable
R1>enable
R1# ?                //Comandos a ejecutar
R1# c?               //Comandos que inician con c
R1# configure?       //'comandos' del comando
R1# conf terminal           //configurar terminal
R1(config)#interface et
R1(config)#interface ethernet 0/1
R1(config-if)#ip a
R1(config-if)#ip add
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)# inter e0/0       //Segundo router
R1(config-if)#ip add
R1(config-if)#ip address 10.10.0.0 255.255.255.252
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#
```

Virtual PC

```
PC-1> ip ? // que podemos hacer
PC-1> ip address ip 192.168.0.2 24 192.168.0.1
PC-1> ping 192.168.0.1
```

```
R1#show ip address brief
```

```
R1#show ip route     //Tabla de enrutamiento (Hasta a donde
    llega mi router)
```

Algunos comandos simples

```
R1#conf t
R1(config)#prompt "Curso4CM1"
```

```
R1#conf t
R1(config)#host name "Curso4CM1"
Curso4CM1#
```

Usando password

```
R1#conf t
R1(config)#enable password 1234
R1(config)#end
R1#disable
R1>enable //Ahora pedirá password
```

```
R1#show running-config //Configuración y comandos que debo
    ejecutar

R1#show running-config | include pass //Mostrar el password
```

Contraseña segura

```
R1#conf t
R1(config)#enable secret 12345678
R1#end
R1#show running-config | include enable
```

Activar el servicio de encriptación

```
R1#conf t
R1(config)#service password-encryption
R1(config)#exit
R1#show running-config | include pass
```

Ya hemos crado un password, el cual tiene como fin el cambio de privilegios, pordemos también poner un password para abrir la consola.

```
R1#conf t
R1(config)#line console 0
R1(config-line)#password 1234
R1(config-line)#login
R1(config-line)#exit
R1(config)#exit
R1#disable
R1enable //Pedirá password
```

Quiero conexión remota de R2 a R1
Puerto telnet = 22, requerimos un password.

```
R2#telnet 10.10.0.1 //Requiere password y no la tenemos,
    entonces debemos configurar primero a donde nos vamos a
    conectar (añadir password a R1)
```

Configuramos password para telnet

```
R1#conf t
R1(config)#line vty 0 15 //Accesos completos, cisco usa
    permisos de seguridad de 0 a 15 pero solo tenemos acceso
     a 3
R1(config)#password 1234
```

Intentamos de nuevo con R2 conectarnos

```
R2#telnet 10.10.0.1 //Ahora nos pedirá password, para
    nuestro caso es 1234, ahora estamos en R1
R1
```

Configuración de SSL: tiene mayor nivel de seguridad. Podemos encriptar las tramas

```
R1disable
R1show ssh //Esta desactivado
```

Asignando llave y dominio

```
R1enable
R1#conf t
R1(config)#ip domain-name curso4CM1.com//Configuramos el
    dominio, este tiene relación lógica o práctica algo que
    nos vuelve comunes.
R1(config)#crypto key generate rsa general-keys //Definimos
    una llave de encriptación
How many bits in the modulus [512]: 1024 //Asignamos el tama
    ño de llave en este caso 1024 bytes
```

Tiempo de inactividad, se cae la conexión en n segundos

```
R1(config)#ip ssh time-out 30 //En 30 segundos se cancela la
     conexión
```

Número de intentos si falla el password

```
R1(config)#ip ssh authentication-retries 3 //A los 3
    intentos se cancela la conexión
```

Configuración versión de ssh

```
R1(config)#ip ssh version 2
```

Privilegios

```
R1(config)#username admin privilege 15 pass 1234 //Asignamos
     un nivel de privilegios 15 con el password 1234
```

```
R1(config)#line vty 0 4 //Modo de configuración de una
    terminal virtual (remota)
R1(config-line)#transport input ssh //Me comunicaré usando
    SSH
R1(config-line)#login local //Desde dónde haré la verificaci
    ón de password, imaginemos que tenemos un server que
    tiene los controles de acceso. En este caso todo se hará
     localmente
```

Verificamos usando R2 que todo esté bien

```
R2#ssh -v 2 -l admin 10.10.0.1 //En mi caso no pude
    especificar la versión por tanto removemos ese comando
R2#ssh -l admin 10.10.0.1 //Me pedirá el password el cual es
     1234 y ahora puedo acceder remotamente a R1
```

Verificamos si esta activo el SSH

```
R1(config)#end
R1show ssh
```

Niveles de privilegio

```
R1conf t
R1(config)#privilege line//Definimos el conjunto de comando
    a asignar
```

4.3 Enrutamiento estático y dinámico

Estas tienen una diferencia: Recordemos en el ejemplo anterior hacíamos ping a R2 pero no teníamos respuesta. En enrutamiento dinámico cada router sabe que va ha hacer, si envian una petición sabe por que interfaz enviar una respuesta. Nosotros como adminsitradores definimos un registro en la tabla de enrutamiento.

```
R1show ip route //Vemos tablas de enrutamiento del router
```

Si el paquete no está en alguno de los renglones de la tabla de enrutamiento no envia nada el router.

4.4 Protocolos CMIP

- ACSE: Se encarga de establecer las conexiones entre gestor y agente.
- ROSE: Se encarga de generar la transferencia de datos entre gestor y agente.
- CMISE: Utiliza los protocolos anteriores para administrar la red, etc. Entre los agentes.

5 Enrutamiento estático y dinámico

5.1 Enrutamiento estático

Es la forma más simple de enrutamiento, en la que las tareas de descubrimiento de rutas y su propagación en la red son realizadas manualmente por el administrador de la internetwork. (El administrador añade una dirección)

En un esquema de enrutamiento estático una vez que la ruta es configurada, no hay necesidad de que los routers intenten descubrimientos de rutas para comunicar entre si información acerca de las mismas.

- La distancia administativa predeterminada de una ruta estática es 1
- Las rutas estáticas serán incluidas en la tabla de ruteo a menos que la red esté dieractamente conectada, o que la interfaz de salida especificada no pueda ser alcanzada por el router

Supongamos que tenemos configurados varios protocolos, el router le da prioridad a un protocolo sobre otro, esto es la distancia administrativa.

5.2 Enrutamiento dinámico

EN el enrutamiento dinámico, la determinación de una ruta se hace usando información que es obtenida de los protocolos de enrutamiento.

Esta información se genera en respuesta a cambios en la red.

5.2.1 Ventajas del enrutamiento estático

- Eficiencia de recursos: no consume ancho de banda para intercambio y descubrimiento de rutas, no ocupa procesamiento del CPU en cálculo de rutas y requiere menos memoria

- Mayor segurodad
- Control sobre el tráfico
- Respaldo sobre rutas dinámicas: puede configurarse una ruta estática con una distancia administrativa mayor a la ruta obtenida por un protocolo a un mismo destino, en caso de que el protocolo falle se añade una ruta estática.

5.2.2 Desventajas del enrutamiento estático

- No se adapta a cambios a al topología
- Costo de administración
- No ofrece gran escalabilidad

5.2.3 Ventajas enrutamiento dinámico

- Redundancia
- Multiple acceso
- Carga compartida
- Escalable y flexible

5.2.4 Desventaja del enrutamiento dinámico

- Procesamiento

5.2.5 ENrutamiento estático

Se realiza utilizando ip route

```
ip route prefijo máscara {dir-reencio | vlan vlan-id}[
    distancia][permanente][tag valor]
```

- prefijo: identificador de red
- máscara: máscara de la subred
- dir-reenvio | vlan vlan-id: a dónde se dará un ”brinco”
- distancia (opcional): especifica la métrica de la distancia para esta ruta, los valores son válidos entre 1 y 255. Las rutas con valores pequeños son las preferidas
- Permanente (opcional). Especifica una ruta permanente
- tag (opcional): especifica una etiqueta para la ruta con valores válidos entre 1 a 4294967295

5.3 Protocolos

Hay dos tipos de protocolos, los protocolos enrutables y los de enrutamiento

5.3.1 Protocolos enrutables

Tienen una dirección que deja moverse.

1. IP
2. IPX
3. AppleTalk

5.3.2 Protocolos no enrutables

Funcianan sobre una sola LAN.

1. NetBEUI
2. DLC
3. LAT
4. DRP
5. MOP

5.3.3 Protocolo de enrutamiento

Mecanismos necesarios para compartir la información de enrutamiento. Hace que los routers compartan información, para que construyan sus tablas de enrutamientO .

1. RIP
2. OSPF
3. IGRP

Objetivos

1. Identificar rutas potenciales
2. Deteterminar rutas óptimas
3. Detectar cualquier cambio en las topologías
4. Optimización
5. Simplicidad y bajo gasto

6. Solidez y estabilidad
7. Flexibilidad
8. Convergencia rápida: Si existe un cambio en la topología hay un tiempo que se da para notificar a los routers estos cambios y recalcular los algoritmos con los que se construye la tabla de enrutambiento

- Proveen reglas sintácticas y semánticas
- Contienen los detalles del formato de los mensajes
- Describen intercambio de mensajes
- Describen los proceso de comunicación

5.4 Distancia administrativa

Valores predeterminados

Origen de la ruta	Valores predeterminados de la distancia
Interfaz conectada	0
RUta estática	1
Ruta resumen EIGRP	5
Protocolo BGP	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	150
BGP interno	200
Desconocido	255

5.5 COncepto de métrica y sus componentes

- Un algoritmo de enrutamiento debe determinar las ventajas de una ruta sobre otra
- Para cada ruta a través de la res, un protocolo utiliza valores llamados métricas para determinar cuál es laruta óptima
- Las métricas pueden tomar como base una sola característica de la ruta, o pueden calcularse tomando en cuenta distancias características
- Con las métricas, el algoritmo genera un valor llamado valor métrico

5.5.1 Metrícas de enrutamiento

1. Ancho de banda
2. Retardo
3. Carga: permite reajustar las rutas
4. Confiabilidad: índice de error
5. Número de saltos
6. Tictacs
7. Costo

5.5.2 Clases de protocolos de enrutamiento

- Protocolos de enrutamiento Interior (IGPs)
- Protocolos de enrutamiento exterior (EGPS)

Cuando nos referimos a interno y externo hablamos de dominios
EL método en que descubren y calculan rutas

- Protocolos vector-distancia
- Protocolo de estado de enlace
- Protocolos híbridos balanceados

DIreccionamiento IP

- Protocolos classful
- Protocolos classless

Convergencia

Si es menor el tiempo de convergencia es mejor.

5.6 Protocolos classful

- Los protocolos de enrutamiento classfull no incluyen máscara de red en los anuncios de red
- Dentro de la misma red, se asume una consistencia de máscaras de subred

5.7 Protocolos classless

Requerimos enviar las máscaras y construye una estructura jerárquica dependiendo de las direcciones IP y las máscaras que se estan utilizando

- RIPV2
- OSPF

5.8 Protocolos de enrutamiento interior

Se utilizan para intercambias información dentro de un siste aautónomo.

5.9 Principales tipos de enrutamiento

- Vector-distancia: Determina la dirección a partir de pares, básicamente se tiene un router y ese router tiene el identificador de red y su costo (tabla de enrutamiento)
- Estado del enlace:

5.10 Ejemplo de configuración RIPv2

5.10.1 Configuración básica

Configurar RIPv1

- Activar protocolo RIPv1
  router rip
- Anunciar redes:
  network <dirección de red>

Configurar RIPv2 en R4

- Activar el protocolo RIPv2:
  router rip
- Especificar la versión 2:
  version 2
- Anunciar redes:
  network <dirección de red>

```
Rx#write //Para mantener la configuración de los routers
```

Damos por hecho que las IP

```
R1# conf t
R1(config)#router rip
R1(config-router)#version 2
```

Recordemos que RIP envia sus tablas de enrutamiento a los routers vecinos. Cada 30s se refresca esta información.

```
R1# conf t
R1(configure)# router rip
R1(configure-router)# version 2
R1(configure-router)# network 200.1.1.0 //Subred de la
    computadora
R1(configure-router)# network 40.0.0.0  //Subred con los dem
    ás routers
```

¿Porqué necesito saber de donde voy y a donde voy? Imaginemos que tenemos una topología con switches o algo intermedio entre routers, debemos saber hacia donde hay que moverse, por esa razón es que rip nos dice a donde vamos a ir.

Rip soporta balanceo de cargas hasta en cinco rutas.

Hay que indicarle a RIP que haga un superneteo de las redes ya que recordemos que RIP es orientado a clases:

```
R3# conf t
R3(configure)#router rip
R3(configure--router)#no auto-summary
```

Más comandos para monitorizar

```
R1#show ip protocols
```

Como evitamos sobrecarga en ciertas interfaces? Debemos indicarselo a rip

```
R3#conf t
R3(configure)#router rip
R3(configure-router)#passive-interface ethernet 0/0 //donde
    tenemos las LAN (las computadoras conectadas)
```

Supongamos que queremos configurar un router como router de frontera en nuestro caso el router R5, como lo configuramos?

```
R5#conf t
R5(configure)#router rip
R5(configure-router)#default-information origin
```

Si hacemos show ip route en el router R3 tenemos una red por defecto la que es la 0.0.0.0 (último renglón)

¿Que pasa si quiero combinar un protocolo dinámico con uno dinámico? Para esto rip va a difundir información que no pertenece al protocolo RIP.

Requerimos informar al router Rf que toda subred que no esté en 200.20.20 y 60.6.6.4 salga por el router R5 ¿Cómo hacemos eso? Hay que definir primero un enrutamiento estático. Que ID de red necesitamos? 0.0.0.0 con la máscara 0.0.0.0 esto para capturar todas las IP que no caigan en las dos subredes que hemos mencionado antes. Nuestro siguiente punto de salto es 60.6.6.5

```
Rf(config)#ip route 0.0.0.0 0.0.0.0 60.6.6.5
```

Nótese que tenemos una prioridad de 1 en este caso.
Debemos hacer lo mismo con el router R5 en este caso.

```
R5(config)#ip route 200.20.20.0 255.255.255.0 60.6.6.6
```

Los demás routers no conocen esta configuración así que este router debe de informar al resto de routers

```
R5(config)# router rip
R5(config)# redistribute static
```

5.11 Cuenta a infinito

Cuando hablamos de RIP el número máximo de saltos o métrica es 15 si es 16 o mayor el destino es inalcanzable. Por ejemplo si removemos una conexión a una LAN y estamos usando RIP vamos a generar una especie de ciclo hasta que elk valor de los saltos llegue a 16 esto hace que el destino se convierta en inalcanzable.

6 Protocolo OSPF

6.1 Aspecto básico del protocolo OSPF

Definido por la IETF en la RFC 2328, de Abril-98.

- Se encapsula en IP con rpotocolo 59h
- Se define 05 tipos de mensajes
- Lectura obligada

6.2 Características

- Se hace uso del protocolo HELLO
- Se envía periodicamente a la dirección multicast IP 224.0.0.5

Requiere mucha memoria ya que genera una base de datos, requiere mucho ancho de banda, ya que envía la tabla de enrutamiento e información de la BD a los routers vecinos. EN este protocolo como ya se mencionó antes se utilizan 5 tipos de mensajes, dónde el más sencillo es el mensaje ”HELLO”. OSPF hace que los routers conozcan la información de toda la tabla de enrutamiento.

OSPF divide todo el sistema autónomo en áreas, dónde todas las áreas deben estar conectadas al área 0, dónde el área cero es el área de backbone es la columna vertebral de OSPF.

6.2.1 Observaciones al estado de enlace

- Los routers de enlace requieren más memoria y potencia de procsamiento, que un router vector-distancia

- Al inicio del proceso se debe inundar la red con mensaje LSA, puede degradar la red
- Hay que dividir la red en áreas

6.2.2 Configuración

```
Rx#conf t
Rx(config)#router ospf process-ID //Debe ser el mismo para
    todos los routers
Rx(config-router)# network dirección_de_red wildcard /*comod
    ín*/ area area_ID
Rx(config-router)#exit
```

El wildcard es el inverso de la máscara por ejemplo si la máscara es 255.255.255.252 el inverso es 0.0.0.3

6.3 Wildcard

6.3.1 Bits de máscara wildcard

Una máscara wildcard es un número de 32 bits dividido en cuatro octetos (como IP)
El enmascaramiento wildcard es utilizado por las ACL para identificar una sola dirección o múltiples direcciones para pruebas d epermiso y denegación
No guardan relación funcional con las máscaras de subred
ALgunas veces, se refiere a una máscara de wildcard como una máscara inversa.

Un bit a 0 en la mmáscara significa comprobar el valor correspondiente y un 1 es ignorar el valor correspondiente.

Ejemplo: tenemos la dirección
30.15.25.0/26 supongamos que me interesan todas las direcciones IP pares de esta LAN. La máscara es 255.255.255.192

255	255	255	192
30	15	25	00xxxxxx
Los primeros 26 bits nos interesan es decir:			
0	0	0	00
El último bit nos define la paridad por tanto, solo el último bit nos importa saber que valor tiene (debe ser cero			
0	0	0	0011111110
Con lo cual obtenemos nuestro wild card			
0	0	0	62

Tomemos de nuevo el wildcard 0.0.0.3:

wildcard:	0	0	0	00000011
IDred:	10	2	3	00000100
	10	2	3	000001({00}, {01}, {10}, {11})
	Por tanto tenemos redes definidas desde			
	10	2	3	4
	.			
	.			
	.			
	10	2	3	7

6.4 Aspectos de configuración

- AL iniciarse el proceso OSPF en un router, el IOS utiliza la dirección IP activa local más alta como ID del router
- Si no existe una interfaz activa, el proceso OSPF no se iniciará
- Para asegurar la estabilidad del proceso OSPF, es necesario que el router tenga una interfaz activa en todo momento
- La interfaz loopback es importante para este objetivo

Supongamos que tenemos las siguientes direcciones IP

- 20.20.20.1
- 20.20.30.1
- **20.20.40.1**

OSPF va a tomar la dirección IP **20.20.40.1** ya que es la más alta. Esto vuelve inestable todo OSPF ya que al conectar más redes no obtendremos a veces la dirección IP más alta, si la interfaz con la IP más alta falla nuevamente volvemos OSPF inestable. Es decir OSPF es dependiente de las interfaces con las que se está trabajando. Para solucionar esto utilizamos interfaces loopback. Si se tienen varias ip de loopback nuevamente elige la que tenga la IP más alta.

Ahora debemos de responder lo siguiente ¿Cómo definimos el router designado y el designado de respaldo? Esto se realiza con la prioridad

```
R(config)#interface serial 0/0/0
R(config-if)#ip priority n_prioridad
```

Un valor de prioridad puede variar de 0 a 255

Valor 0 de prioridad imposibilita al router que sea elegido DR

7 Nivel de administración en OSI

Una red tiene tres componentes básicos

- Dispositivos administrados
- Agentes
- Sistemas administradores de la red

7.1 Estándares

- CMIS: era la parte del protocolo encarga de dedefinir como se realiza la comunicación
- CMIP: como se comunicaban los elementos de la red

7.1.1 Elementos de CMIS

- APlicación de sistemas SMAP (gestiona la red)
- Entidad de aplicación de gestión de sistemas (SMAE) esta del lado de los dispositivos se conecta con el SMAP para gestionar los dispositivos, esta gestión va desde la capa 1 hasta la capa 7.
- Entidad de gestión de nivel LME
- Base de información de gestión MIB

7.2 Manager information base MIB

7.2.1 Almacenamiento de la información

- En un agente el almacenamiento de la información se realiza en objetos, los cuales están definidos por:

  1. Atributos
  2. Operaciones que realizan
  3. Notifiaciones que pueden emitir
  4. Interacción con otros objetos

La forma de representación y almacenamiento de los datos es un agente no se estandariza. Funciones locales utilizadas para convertir la información relacionada con los objetos gestionados a un formato que se pueda almacenar localmente . Una función específica se encarga de realizar las conversiones necesarias . La información se almacena en objetos.

7.2.2 MIB, estándar ISO 10165-1 (x 720)

Define como se debe realizar la gestión de la información

7.2.3 Estructura de la MIB

La unidad básica de información es el objeto

- Atributos
- Comportamientos
- Notificaciones

Existen dos formas de crear jerarquias para estructurar la MIB

- Definición de subclases, o clases derivadas de otras clases que heredan sus características
- Una instancia de objeto puede estar contenida en otra instancia de objeto

SMAP Gestor	↔	SMAE Adente

MIB no está diseñado para la administración de redes si no la administración de empresas.

8 Funciones de gestión de sistemas

Son las distintas áreas que tenemos que considerar para el funcionamiento de nuestra red, tenemos

- Gestión de fallas
- Gestión de costos
- Gestión de configuración: actualizaciones, documentación, etc.
- Gestión de prestaciones: que se le ofrece a los usuarios
- Gestión de seguridad

Todos los gestores mencionados tienen relación con más elementos.

8.1 Áreas funcionales

Se les conoce como FCAPS

8.1.1 Fallas

Busca encontrar dónde ocurren los errores pero además de solucionarlos busca mecanismos para que las soluciones ocurran lo más rápido posible

8.1.2 COnfiguración

BUsca una automatización de confiuraciones de red.

8.1.3 Contabilidad

Uso de recursos de nuestros clientes

8.1.4 Desempeño

Que tan eficiente es nuestra red, usa estadísticas, alarmas, etc.

8.1.5 Seguridad

Todo está conectado donde debe estar, se conecta quien debe ser, etc.

8.2 Acciones básicas

Lectura(sondeo), Justificacion(trampa), escritura

9 Gestión de fallas

Tiene como objetivo registrar, detectar y contrarestar las condiciones de fallo de una red.

9.1 ¿Qué implica administrar fallas?

- Identificación del prolblema
- Crear, aprobar la solución y se propaga
- Resolución del problema y documentación

10 EIGRP

Es una versión de IGRP mejorada por CISCO.

10.1 Objetivos

- ¿Como está configurado?
- Historia
- Comandos báiscos
- Calcular la métrica compuesta por EIGRP
- Describir los conceptos y el funcionamiento de DUAL
- Describir los usos de los comoandos adicionales de EIGRP

Tiene una característica importante, nos permite trabajar de distintas formas, permite trabajar con el protocolo DUAL o vector distancia o bien estado de enlace. También permite configurar las prioridades dependiendo de la fuente de información.

En la capa de transporte usa el protocolo RTP. Tiene ciertas catracterísticas especiales

- Soporta envios confiables y no confiables dependiendo de las necesidades
- Soporte para unicast o multicast

También tiene 5 tipos de paquetes

- Saludo: permite detectar routers vecinos para establecer adyacencias e informar que estamos activos
- Actualización

- Reconocimiento (En respuesta a una actualizacion)
- Consulta
- Respuesta a la consulta

10.2 Tiempo en hold

Tiempo en espera que un router maneja antes de recibir un mensaje de saludo. Si en cierto tiempo no se recibe un mensaje de saludo se entiende como que el router tiene problemas y lo marca. Si se rebasa un segundo tiempo de espera se da por hecho que el router está inactivo y se elige otro router por el cual pasar.

11

Implementación de VLAN's y troncales

Al tener un primer diseño de una red es común no pensar que nuestra red puede crecer, debemos considerar varias cosas al realizar el diseño de una red. Aquí tenemos una pequeña lista de errores comunes en las redes.

- Dominios de falla; Es más probable que ocurra alguna situación si perdemos una sección perdemos varias LANS
- Dominios de broadcast
- Gran cantidad de trfico unicast con MACs desconocidas
- Trafico multicast en puertos donde no se requiere
- Dificultad en el manejo y soporte
- Posibles vulnerabilidades de seguridad

11.1 Agrupando funciones del negocio dentro de VLANs

Las VLANs nos permiten una separación lógica de las LAN aún que estas no se encuentren físicamente contiguas.

- Direccionamiento jerárquico de red significa que un número de red es asignado a una VLAN
- Beneficios:
    1. Fácil mantenimiento y resolución de
    2. Errores minimizados
    3. Tablas de enrutamiento reducumas

11.1.1 Describiendo tecnologías de interconexión

Cuando estemos en secciones donde hay una concentración de envíos de paquetes debemos utilizar tecnologías de mayor ancho de banda, a continuación se muestra un listado de tecnologías que son posibles utilizar, desde la que debe ser utilizada desde abajo hacía arriba.

- Fast ethernet
- Gigabit ethernet
- 10-gigabit ethernet
- EtherChannel

11.1.2 Determinando el equipo y el cableado a necesitar

Los cuatro objetivos en el diseño de una red de alto desempeño son

- Seguridad: la información de un departamento no sale d euna sección
- Disponibilidad
- Escalabilidad
- Manejabilidad

11.2 Enlace troncal

Es un enlace de nuestra red donde circulan tramas de distintas VLANs.

- Un enlace troncal se puede comprarar con las carreteras d euna autopista
- Las carreteras que tienen distintos puntos d einicio y fin que comparten una autopista principal durante algunos kilimetros, luego se vuelven a dividir par allegar a destinos diferentes
- Este método es considerablemente económico

EN resumen es un enlace punto a punto que soporta varias VLANs y nos permite el ahorro entre distintos puertos.

11.2.1 Explicando enlaces troncales

Hay dos tecnologías principales

- ISL (CISCO)
  - Soporta multiples protocoloas de capa 2 (Ethernet, Token Ring, FDDI y ATM)

  - Soporta PVST
  - No usa VLAN nativa, solo encapsula cda trama
  - El proceso de encapsulación deja las tramas originales sin modificación

- 802.1Q (IEEEE standard trunking protocol)
  - Permite la transmisión en un enlace físico troncal
  - Permite ethernet y token ring
  - Sporta hasta 5096 VLANs
  - Soporta STP, RSTP
  - Soporta topologías punto a multipunto
  - Facilita el tráfico
  - Soporta QoS (Quality of service)

Estos dos protocolos son necesarios para cuando se necesite interconectar

- Dos switch
- Switch y router
- Switch y tarjeta nick

Asignamos el modo trunk a un puerto

```
Switch(config)#interface [Interfaz]
Switch(config-if)#switchport mode trunk
```

Configuración del router para VLAN

```
Router>en
Router#configure t
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#interface fastEthernet 0/0.1
Router(config-subif)#encapsulation dot1Q [Número de la VLAN]
Router(config-subif)#ip address [IP] [Mascara]
```

11.3 Rangos de VLANs

Cada VLAN en la red debe tener un VID único

El rango válido configurable por el usuario es

- VLAN ISL de 1 a 1024
- —

Hay algunas VLANs reservadas

VLAN ranges	Range	Use	VTP propagated
0, 4096	reservado	Uso del sistema. VLANs no vistas o usadas	-
1	Normal	VLAN por defecto. Esta VLAN puede ser usada pero no borrada o modificada	Si
2-1001	Normal	Pueden ser creadas, usadas y borradas	Si
1002-1005	Normal	VLANs por defecto para FDDI y Token Ring estas no pueden ser borradas	Si
1006-4094	Extendido	Solo para VLANs Ethernet	No

11.4 VTP

Es un protocolo de capa 2. Mantiene las configuraciones de la VLAN consistentes, permite borrar, cambiar, agregar los nombres de la VLAN en todos los switches del dominio VTP

Características

- Protocolo de cisco
- Anuncia VLANs de la 1 a la 1005 solamente
- Actualziaciones e intercambio através de solo enlaces troncales

Permite compatibilidad y hay versiones de 1 a 5

11.5 Modos de VTP

11.5.1 Servidor

- Crea, modifica y borra VLANs
- Manda y envía avisos
- Sincroniza configuraciones de VLANs
- Graba la configuración en NVRAM

11.5.2 Client

- No puede crear, cambiar o borrar VLANs
- Re-envia los avisos
- Sincroniza configuraciones de VLANs
- No graba a NVRAM

11.5.3 Transparent

- Crea, modifica y borra VLANS
- Re-envía avisos
- No sincroniza configuraciones de VLANs
- Graba la configuración a NVRAM

11.6 Describiendo la operación de VTP

- Administrador crea una VLAN
- Revisión 3 se actualiza a versión 4
- VTP propaga revisión 4
- Revisión 3 actualiza a 4
- VRP sincroniza y re-envía la información

11.7 VTP pruning

- VTP pruning usa los avisos de VLAN para determinar cuando una conexión troncal está mandando tráfico innecesario
- VTP pruning incrementa el ancho de banda restringindo el flujo de tráfico en enlaces troncales dónde no se necesita
- Restricciones:
  1. En la VLAN 1 no se puede activar esta opción
  2. Sólo se puede implementar VTP pruning solo en los servidores de VTP