

Laboratorio 3

Packet Tracer

Laboratorio de Redes 2015, UTFSM

Valparaíso, 24 de enero de 2016

Índice

1. Introducción	3
2. Objetivo general del laboratorio	3
3. Objetivos específicos del laboratorio	3
4. Descripción del laboratorio	4
5. Actividades y Preguntas	4
5.1. Trabajo previo	4
5.2. Trabajo en el laboratorio	5
5.2.1. Conectividad mediante Switch	5
5.2.2. Conectividad mediante Router	6
5.2.3. Enrutamiento Estático	7
5.3. Trabajo fuera del laboratorio	10
5.3.1. Enrutamiento Dinámico usando RIP	10
6. Informe	10
7. Consideraciones	11
8. Anexos	11
8.1. Packet Tracer	11
8.2. Conectividad mediante Switch	12
8.3. Conectividad mediante Router	12
8.4. Enrutamiento estático	12
8.4.1. Rutas Por Defecto	13
8.5. Enrutamiento Dinámico	13
8.5.1. Protocolo de enrutamiento RIP (Routing Information Protocol)	13

1. Introducción

Para poder crear redes de computadores, es necesario comprender los distintos componentes que se conectan para poder lograr la comunicación, seguridad, conectividad y otras características importantes que se requieren. En este laboratorio, se pretende que se interiorice con la capa de red y de enlace de datos del modelo OSI que abarcan componentes que cumplen con la implementación de las características mencionadas anteriormente. Después de esta experiencia, el alumno debería poder diseñar sus propias redes de computadores y tener herramientas para comprobar su funcionamiento. La herramienta principal para desarrollar esta experiencia es el programa Packet Tracer¹

Algunos conceptos básicos que debe ud. conocer antes de realizar este laboratorio son:

- Funcionamiento de Packet Tracer.
- Direccionamiento IP y máscara de Red.
- Utilidad de un switch.
- Utilidad de router.
- Enrutamiento estático.
- Enrutamiento dinámico.
- Nociones básicas del funcionamiento de Packet Tracer.

2. Objetivo general del laboratorio

Estudiar y comprender la capa de red y de enlace de datos del modelo OSI (*Open System Interconnection*).

3. Objetivos específicos del laboratorio

- Comprender la finalidad de utilizar switches.
- Comprender la importancia de la máscara de red.
- Comprender la finalidad de utilizar routers.
- Aprender a crear una red local.
- Interiorizarse con los comandos IOS: ip, route, y rip.
- Conocer las ventajas del enrutamiento dinámico.
- Aprender el funcionamiento del Packet Tracer.

¹http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html

4. Descripción del laboratorio

Esta experiencia entrega herramientas para configurar routers y switches Cisco mediante Packet Tracer. Se crearán distintas topologías de red y se logrará conectividad entre computadores en una red local para después realizar un enrutamiento estático y dinámico (RIP).

Contará de 3 partes:

- 1) Trabajo previo.
- 2) Trabajo en el laboratorio.
- 3) Trabajo fuera del laboratorio.

Se deberá acordar un horario para la segunda parte entre el grupo de trabajo y el ayudante a cargo.

Finalmente, los temas a trabajar son los siguientes:

- Nociones básicas de Packet Tracer.
- Conectividad mediante Switch (Capa de enlace de datos).
- Conectividad mediante Router (Capa de red).
- Enrutamiento estático (Capa de red).
- Enrutamiento dinámico (Capa de red).

5. Actividades y Preguntas

5.1. Trabajo previo

Actividad 1. Estudie los temas de la sección Anexos y busque los comandos Cisco para realizar las siguientes configuraciones:

- Mostrar listado de direcciones MAC conectadas al switch.
- Acceder a la interfaz X del router.
- Asignar dirección IP y máscara a la interfaz X.
- Configurar enrutamiento estático del router.
- Configurar enrutamiento dinámico con RIP del router.
- Eliminar dirección IP asignada a interfaz X del router.

Deberá llevar este listado de comandos el día de la parte en el laboratorio.

Actividad 2. En esta experiencia se emulan routers y switches Cisco, pero en la vida real es posible que nos toque interactuar con otras marcas y es necesario tener conocimientos generales de su manipulación. Investigue 2 marcas aparte de Cisco que ofrezcan switches y/o routers con características similares. Para poder comparar, busque aquellos que tengan 24 puertos o más (bocas). Realice una tabla comparativa entre las marcas con las características que usted considere relevantes. Por último, ejemplifique la configuración de una interfaz con los comandos correspondientes de cada marca, ¿Cuál es más intuitiva? ¿Cual ofrece más posibilidades de configuración? ¿Son similares?.

5.2. Trabajo en el laboratorio

Es importante que cada actividad de esta sección documente cada paso para que le sea más fácil confeccionar el informe. Además, esta parte contará con el asesoramiento del ayudante encargado de la experiencia.

5.2.1. Conectividad mediante Switch

Primero, se deben agregar 4 *laptop's* al *logical workspace* de Packet Tracer y deben conectarse con cables FastEthernet directos a un *switch* 2950-24 (ejemplo: Laptop0 a puerto FastEthernet0/1 switch, Laptop1 a puerto FastEthernet0/2 switch) como indica la figura:

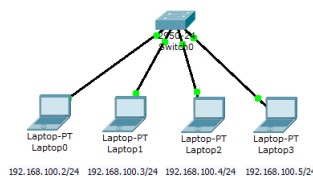


Figura 1: Conectividad básica mediante switch

Es importante que se configure cada *host* con su respectiva dirección IP porque será utilizada para comprobar la conectividad. Se debe hacer *click* en cada *laptop* y seleccionar la pestaña *Desktop*. A continuación se muestra la configuración de Laptop0 y se deberá realizar este paso para cada uno.

```
Laptop0: 192.168.1XX.2 255.255.255.0
Laptop1: 192.168.1XX.3 255.255.255.0
Laptop2: 192.168.1XX.4 255.255.255.0
Laptop3: 192.168.1XX.5 255.255.255.0
```

Nota: XX representa el número de su grupo (01, 02, 03, etc.)

Haga click en el ícono del switch y vaya a la pestaña CLI (Command Line Interface) y ejecute los siguientes comandos para ver la tabla de direccionamiento.

Para poder apreciar como se forma la tabla de direcciones, hay que ingresar al modo de simulación de Packet Tracer y hacer *click* en *Edit Filters*, asegurarse de que sólo quede seleccionado ICMP. Luego, se debe hacer *click* en Laptop0 e ingresar a la pestaña *Desktop*, después hacer *click* en *Command Prompt* e ingresar el siguiente comando (En la pestaña de simulación de Packet Tracer se deberá seleccionar Auto Capture/Play):

```
PC>ping 192.168.1XX.4
```

Una vez que se haya visto como se transmite un paquete ICMP y se reciba en Laptop0, hay que detener la simulación y en modo CLI del *switch* volver a ejecutar el comando para ver las tablas de direcciones. Notar que ahora se ha agregado la dirección de Laptop0 y Laptop2. Las simulaciones se deben realizar hasta completar la tabla del *switch*.

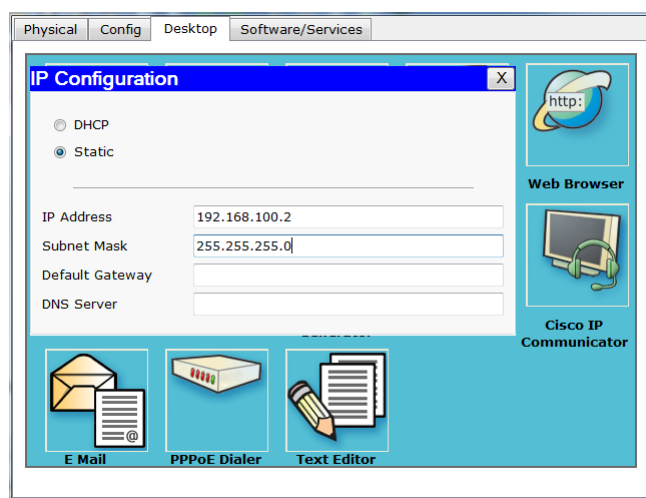


Figura 2: Configuración Host

Pregunta 1. Si cada computador conectado al *switch* es capaz de ver el tráfico de la red ¿Qué ventajas tiene usar un *switch*?

Pregunta 2. Si hay 2 redes conectadas a un *switch* ¿Es posible que un computador de una red sea capaz de ver el tráfico de la otra red?

Pregunta 3. ¿Cómo se puede separar la información de cada red conectada a un switch?.

En esta etapa se ha logrado crear una red local, la cual es escalable según el número de puertos que disponga el *switch*. Durante los años, el uso de los *switches* ha facilitado la conexión para empresas con numerosos *host* que deben estar conectados a una misma red local. Queda a disposición del lector los siguientes temas si desea investigarlo: VLAN, STP y RSTP.

Nota: Sin el modo simulación de Packet Tracer, el uso de *ping* para probar conectividad entre dos computadores le permitirá al *switch* resolver las direcciones y puertos de todos los *host* conectados, se realizó la simulación anterior para que pudiera aprender la configuración interna del *switch*.

5.2.2. Conectividad mediante Router

Se debe crear otra red de 4 *laptop's* y 1 *switch*. Conectar ambos *switches* por medio de un *router* como indica la figura:

Laptop4: 192.168.2XX.2 255.255.255.0
 Laptop5: 192.168.2XX.3 255.255.255.0
 Laptop6: 192.168.2XX.4 255.255.255.0
 Laptop7: 192.168.2XX.5 255.255.255.0

Nota: La dirección 192.168.x.x corresponde a una red privada. Estas redes son comunes porque muchas compañías no tienen necesidad de una dirección IP global (pública) para cada estación de trabajo pero permiten conectividad entre redes internas. Antes de configurar el *router*, recordar que la máscara es de 24 bits (255.255.255.0) esto quiere decir que la dirección 192.168.1XX.0 es el identificador de red, la dirección 192.168.1XX.1 se suele reservar para la interfaz conectada al *router* y la dirección

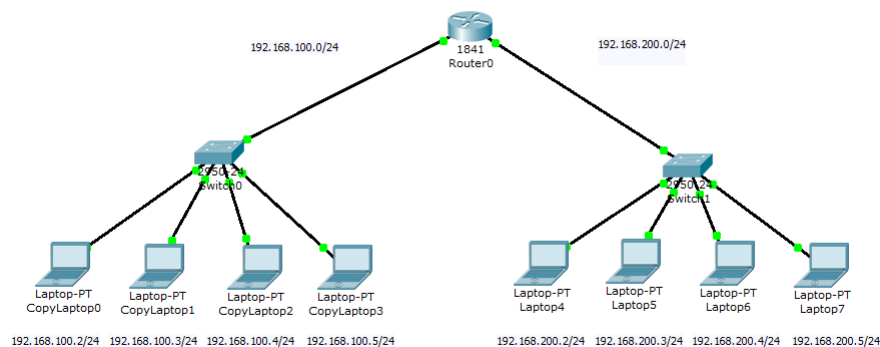


Figura 3: Conectividad mediante router

192.168.x.255 es la utilizada para *broadcast*. Es decir, la primera dirección del segmento indica la red, la segunda se utiliza para indicar la dirección de la interfaz del *router* (Gateway) y la última se reserva para *broadcast*.

Ingrese al modo CLI del router y ejecute los comandos correspondientes para configurar la interfaz 0/0 para el switch0.

Como se indicó anteriormente, la interfaz 0/0 se ha configurado para la subred 192.168.1XX.0/24 . Ahora, se deberá ingresar a cada *laptop*, ingresar a la pestaña Desktop → IP Configuration → Default Gateway y agregar 192.168.1XX.1 lo que permitirá al *laptop* enviar paquetes a otras redes a través del *router*, si usted desea utilizar otra dirección para la salida no habrá problema pero es considerado como una mala práctica.

Hay que realizar el paso anterior para la interfaz FastEthernet1/0 del *router* configurando la red 192.168.2XX.0/24 y modificar el *Default Gateway* de cada *laptop* de la topología.

Comprobar conectividad entre las redes utilizando *ping*. Ejemplo: desde Laptop0 de Red 192.168.1XX.0/24

```
PC>ping 192.168.2XX.4
```

Pregunta 4. ¿Qué pasaría si la interfaz del *router* se configura con una máscara distinta a la del *host*?

Pregunta 5. Si se configura de forma incorrecta la interfaz del *router* ¿Cuál sería el comando para eliminar la configuración?

5.2.3. Enrutamiento Estático

Ya se ha logrado tener conectividad entre 2 redes conectadas directamente a un *router*. En la práctica, existen muchos *router's* interconectados para generar conectividad a través de todo internet, por lo que ahora se dará el siguiente paso para acercarse al mundo real.

A la topología creada anteriormente, agregue otro *router* y conéctelo con el Router0 mediante un cable serial. Al nuevo *router*, que será llamado Router1, agregue 1 *switch* y 2 *laptop's* con la red: 192.168.XX.0/24 (Ej: grupo 01, red 192.168.1.0/24) como indica la figura:

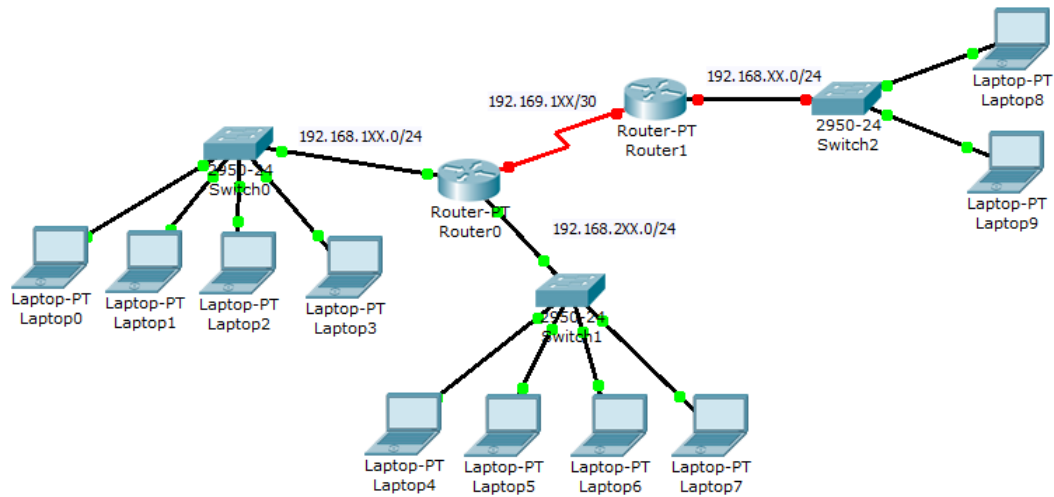


Figura 4: Enrutamiento Estático

Como no es necesario tener más de 2 direcciones IP en la red que conecta a los routers, utilice la red 192.169.100/30. Con una máscara de 30 bits (255.255.255.252) tendrá 4 direcciones: 2 reservadas y una para cada router. Configure las interfaces de la misma forma que antes.

Pregunta 6: ¿Hay conectividad?, si la respuesta es negativa ¿Por qué no hay conectividad?.

Existe conectividad entre terminales directamente conectados a un *router*, pero cuando se intenta acceder a una red de otro *router* se debe indicar el camino para llegar a dicha red. Cuando se le indica al *router* los puertos que debe usar para salir a una red específica se llama enrutamiento estático. Para Router0 y Router1 ingrese los comandos necesarios para que haya conectividad.

Una vez hecho este paso se comprueba que la configuración fue exitosa mediante el comando *show ip route*, este comando muestra la tabla de enrutamiento del dispositivo. Las rutas marcadas con “C” pertenecen a las redes directamente conectadas, las marcadas con “S” son las rutas que enrutó de manera estática.

Como se puede apreciar, se indica la red destino, la máscara de la red y la interfaz a la que está conectada el *router* para alcanzar la red (no es la interfaz propia, si no que la interfaz del “siguiente salto”). Vuelva a probar conectividad entre Laptop(192.168.1XX.2/24) y Laptop(192.XX.2/24).

Pregunta 7: Si se hiciera sólo el enrutamiento en el Router0, ¿Por qué el ping no es efectivo si el Router conoce como llegar a la red destino?.

Recordar que el *gateway* o puerta de enlace, debe ser la misma que la IP del *router* para entregar la salida correspondiente fuera de la subred. Tampoco hay que olvidar como colocar el *switch* para unir la o las máquinas conectadas al *router*. En esta parte se puede utilizar el comando *show cdp neighbors* en cada *router* (si no está habilitado el protocolo CDP, se habilita desde RouterX(config)# *cdp run*), que mostrará todos los *router's* y *switches* conectados directamente, si alguno no aparece revisar su configuración. Ahora que la conectividad está realizada se procede a configurar las rutas estáticas para cada *router*.

Se deberá guardar el archivo Packet Tracer con el nombre XX_ruteoEstatico.pkt, donde la XX será el número del grupo. Ahora, guardar el mismo archivo con el nombre XX_ruteoDinamico.pkt ya que se realizará el ruteo dinámico a partir de la topología ya creada.

5.3. Trabajo fuera del laboratorio

En esta parte, deberá trabajar con su grupo de forma independiente.

5.3.1. Enrutamiento Dinámico usando RIP

En el archivo XX_ruteoDinamico.pkt se deberá borrar las tablas estáticas para realizar el enrutamiento dinámico.

Para Router0 y Router1 elimine las direcciones IP de las interfaces utilizadas.

Ahora, agregue una nueva red utilizando 1 router, 1 switch y 2 laptop como indica la figura:

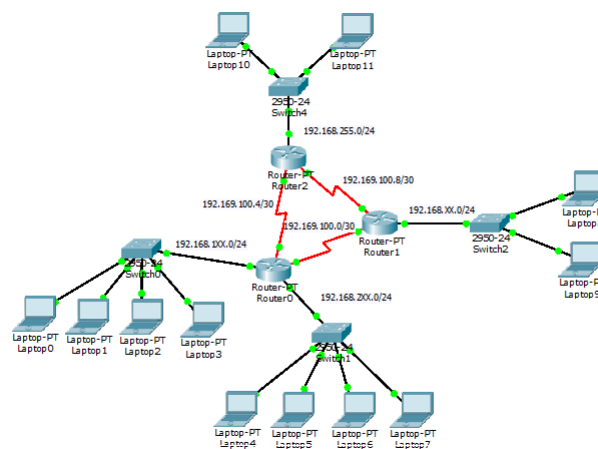


Figura 5: Enrutamiento Dinámico mediante RIP

La subred conectada directamente al nuevo router debe ser 192.168.255.0/24

Si utilizara enrutamiento estático, se debería agregar cada red no alcanzable directamente por los *router's*, lo cual podría convertirse en algo engorroso si se sigue aumentando la complejidad de la red. Con enrutamiento dinámico, cada *router* deberá agregar las redes que tiene directamente conectadas. Ingrese los comandos necesarios para lograr conectividad entre todos los *laptop's* de la topología y compruebe con comando ping.

Pregunta 8. ¿Qué ventajas presenta el uso de RIP respecto a OSPF?. Indicar 2 situaciones donde RIP sea mejor que el enrutamiento estático.

6. Informe

El informe debe hacerse en \LaTeX . Se deberá describir cada procedimiento realizado, responder las preguntas de cada sección y realizar las siguientes actividades: Del primer archivo, enrutamiento estático:

1. Mostrar la configuración de cada uno de los *router's*.
2. Mostrar la configuración de cada uno de los *switches*.

3. Mostrar la configuración de una de las máquinas de cada red.
4. Mostrar la tabla de direcciones del primer *switch* configurado.
5. El *show cdp neighbors* de los 2 *router's*.
6. El *show ip route* de los 2 *router's*.
7. Realizar *ping's* entre las máquinas y mostrar, de la forma que se estime conveniente, que la conexión fue exitosa.
8. Utilizar el comando *tracert* entre 2 máquinas e indicar el *output* generado por dicho comando.

Del segundo archivo, enrutamiento dinámico:

1. Mostrar la configuración de cada uno de los routers.
2. El *show cdp neighbors* de los 2 routers.
3. El *show ip route* de los 2 routers .
4. Realice pings entre las máquinas y muestre, de la forma que estime conveniente, que la conexión fué exitosa.
5. Utilice el comando *tracert* entre dos máquinas e indique el output generado por dicho comando.

7. Consideraciones

- No olvidar de adjuntar los archivos .pkt (para el caso estático y el dinámico) necesarios para la evaluación y adjuntados junto al informe en Trac en un archivo llamado XX_PacketTracer.tar.gz donde XX es el número de su grupo.
- El informe debe estar de acuerdo a las reglas estipuladas adjuntas en moodle y Trac.
- Si tiene dudas con el desarrollo del laboratorio, no dude en consultar al correo labit@inf.utfsm.cl.
- Los horarios del ayudante encargado son: YYYYYY, WWWWW, ZZZZZ.
- La fecha de entrega es XXXXX hasta las 23:59 hrs.

8. Anexos

8.1. Packet Tracer

Packet Tracer es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA². Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Este software tiene el propósito de ser usado como un producto educativo que brinda exposición a la interfaz comando—línea de los dispositivos de Cisco para practicar y aprender por descubrimiento.

En este programa se crea la topología física de la red simplemente arrastrando los dispositivos a la pantalla. Luego haciendo *click* en ellos se puede ingresar a sus consolas de configuración. Allí

²http://en.wikipedia.org/wiki/Cisco_Career_Certifications

están soportados todos los comandos del Cisco OS e incluso la función *Tab Completion*. Una vez completada la configuración física y lógica de la red, se puede hacer simulaciones de conectividad (pings, traceroutes, etc.) todo ello desde las mismas consolas incluidas. Además, soporta los siguientes protocolos:

1. HTTP, TCP/IP, Telnet, SSH, TFTP, DHCP y DNS.
2. TCP/UDP, IPv4, IPv6, ICMPv4 e ICMPv6.
3. RIP, EIGRP, OSPF Multiárea, enrutamiento estático y redistribución de rutas.
4. Ethernet 802.3 y 802.11, HDLC, Frame Relay y PPP.
5. ARP, CDP, STP, RSTP, 802.1q, VTP, DTP y PAgP, Polly Mkt.

8.2. Conectividad mediante Switch

Un *Switch* es un dispositivo digital lógico que opera en la capa de enlace de datos del modelo OSI. Se encarga de interconectar equipos dentro de una misma red (LAN) mediante sus direcciones MAC, las cuales son aprendidas y almacenadas. Las especificaciones técnicas siguen el estándar Ethernet (IEEE 802.3) y se suelen emplear en las redes de acceso.

Es importante tener claro que un switch NO proporciona por si solo conectividad con otras redes, y obviamente, tampoco proporciona conectividad con internet (Para ello es necesario un router).

Para entender como se crea la tabla de direccionamiento, se supone una red de 4 computadores conectados a un *switch*. Cuando un computador envía un paquete a otro, el *switch* registra su dirección MAC y el puerto al cual está conectado. Como el *switch* no conoce la dirección MAC ni el puerto destino, se envía a los otros 3 computadores conectados. Los computadores reciben el paquete pero solo el computador destino responderá al *switch*, el cual almacenará su dirección MAC y su puerto. Este procedimiento se realiza hasta alcanzar un estado estable donde el *switch* conoce todas las direcciones y puertos conectados.

8.3. Conectividad mediante Router

Un *router*³ es un dispositivo de red que redirecciona paquetes de datos. Usando tablas de enrutamiento, este dispositivo puede leer e identificar el destino de estos paquetes. Estas tablas de enrutamiento permiten decidir por cual interfaz o puerto saldrá el paquete redireccionado. La principal diferencia entre un *router* y un *switch* radica en que los *router's* son utilizados con el fin de unir redes de área local (LAN) y redes de área amplia (WAN).

El funcionamiento básico de un *router* consiste en enviar los paquetes de red por el camino o ruta más adecuada en cada momento. Para ello almacena los paquetes recibidos y procesa la información de origen y destino que poseen. Con arreglo a esta información reenvía los paquetes a otro encaminador o bien al *host* final. Cada *router* se encarga de decidir el siguiente salto en función de su tabla de encaminamiento, la cual se genera mediante protocolos estáticos o dinámicos.

8.4. Enrutamiento estático

El principal problema que plantea mantener tablas de enrutamiento estáticas, además de tener que introducir manualmente en los routers toda la información que contienen, es que el *router* no puede

³<http://wiki.inf.utfsm.cl>

adaptarse por sí sólo a los cambios que puedan producirse en la topología de la red. Sin embargo, este método de enrutamiento resulta ventajoso en las siguientes situaciones:

- En un circuito poco fiable que deja de funcionar correctamente, el protocolo de enrutamiento dinámico podría producir demasiada inestabilidad, en cambio el enrutamiento estático las direcciones no cambian, por lo que conservan su estabilidad.
- Se puede acceder a una red a través de una conexión de acceso telefónico. Dicha red no puede proporcionar las actualizaciones constantes que requiere un protocolo de enrutamiento dinámico.
- Existe una sola conexión con sólo un ISP. En lugar de conocer todas las rutas globales, se utiliza una única ruta estática.

8.4.1. Rutas Por Defecto

Este enrutamiento es definido manualmente por el administrador del sistema como la ruta a tomar cuando no existe ninguna ruta conocida para llegar al destino. Es la forma más fácil de enrutamiento para un dominio conectado a un único punto de salida. Esta ruta se indica como la red de destino 0.0.0.0/0.0.0.0.

8.5. Enrutamiento Dinámico

En el enrutamiento dinámico es el *router* quien determina las rutas más adecuadas para que un paquete llegue a su destino y no el Administrador de la Red. Para alcanzar tal objetivo, el *router* ejecuta un proceso de actualizaciones periódicas a través del cual envía y recibe de los demás *router's* de la red, información acerca de las tablas de enrutamiento IP. Todo el proceso asociado al enrutamiento dinámico recae sobre un conjunto de protocolos denominados “protocolos de enrutamiento”.

8.5.1. Protocolo de enrutamiento RIP (Routing Information Protocol)

RIP es un protocolo de enrutamiento de puerta de enlace interna (IGP - Internal Gateway Protocol) basado en un protocolo original de Xerox, el GWINFO. Este protocolo pasó por varias modificaciones y versiones anteriores, pero RIP perduró a su implementación junto a TCP/IP, su sencillez de configuración y compatibilidad. Hoy en día hay 3 versiones: RIPv1, RIPv2 y RIPng.

RIPv1: La versión 1 del protocolo de enrutamiento RIP es “con clase”, es decir, no soporta subredes VLSM (Variable Length Subnet Masks) ni CIDR (Enrutamiento entre dominios sin clase), no posee mecanismos de autenticación y no realiza actualizaciones desencadenadas por eventos. Todas estas limitaciones hicieron que con el paso del tiempo y las nuevas necesidades cayera en desuso.

RIPv2: La versión 2 del protocolo de enrutamiento RIP es “sin clase”, soporta subredes VLSM, CIDR, resumen de rutas, posee mecanismos de autenticación mediante texto plano o codificación MD5, realiza actualizaciones desencadenadas por eventos.

RIPng: La versión ng del protocolo de enrutamiento RIP es para implementaciones IPv6.