Routers e encamiñamento.

(versión 1.0)

Índice

Resumo

Un encamiñador é un dispositivo que une dúas redes distintas para se podan comunicar entre si. Se as redes están conectadas directamente, o router enviará os paquetes ao receptor. Se para chegar ao destino cómpre ir a outra rede e xa que logo cruzar máis routers daquela cada un ten que saber por cal das súas interfaces debe mandar a información. Para facelo os routers utilizan as súas táboas de enrutamento para consultar cal é a seguinte etapa no seu camiño cara o destino.

Introdución

Cando envío un correo electrónico a un amigo, a mensaxe debe pasar por varios dispositivos de rede antes de chegar ao seu destino. Para que os ordenadores que están nunha rede sexan quen de comunicarse cos ordenadores conectados a outra precisan de dispositivos intermediarios chamandos routers. Como sabe o meu router a onde mandar os paquetes que forman a miña mensaxe? Como sabe o router do meu amigo a onde enviar a súa resposta?

Para navegar por internet preciso ter na miña casa un router que conecte os meus equipos a outro router dunha operadora que será a que me leve a internet. Se quero que me traia a páxina web que me interesa visitar o meu router debe ter información que lle permita saber chegar ao servidor web ou, cando menos ao seguinte paso a dar para coñecer o camiño para chegar ata el.

Nunha empresa grande, nun instituto ou nunha universidade os routers son esenciais para manter a comunicación entre as distintas redes dos distintos edificios ou departamentos e para que os empregados, estudantes ou profesores poidan comunicarse entre eles, compartir recursos e acceder a internet.

1. Encamiñadores ou routers

Un encamiñador ou router é un dispositivo que permite que redes distintas se poidan comunicar entre si, por exemplo a rede interna da miña casa coa rede do meu operador de telefonía e este co resto de internet.

Dende o punto de vista do hardware un router é un ordenador especializado coa súa propia CPU, memoria, sistema operativo e unha ou máis interfaces de rede. O que ten de especial é a súa misión de dirixir paquetes ao seu destino atravesando distintas redes con cadanseu router. Un ordenador cun sistema operativo de rede pode facer as funcións dun router, pero un router propiamente é máis eficiente para encamiñar paquetes de datos. Necesitamos determinar que facer para que os paquetes de datos cheguen ao seu destino e xorde asi a necesidade do **encamiñamento ou enrutamento**.

```
Os switches permiten conectar varios dispositivos nunha mesma rede, mentres que os
routers permiten conectar distintas redes.
```

Un router ten varias interfaces ou portos que veñen sendo equivalentes ás tarxetas de rede dun ordenador. Cada interfaz está conectada a unha rede, pode que coa axuda dun switch, ou a outro router. Se por unha desas interfaces chega unha información que se ten que enviar a outra rede será o router o responsable de saber cal é a interfaz pola que ten que reenviarla entre todas as que teña.

Como sabe o router onde mandar cada paquete? Utiliza a información gardada na chamada **táboa de enrutamento** que ten en cada fila datos das redes ás que ten conexión ou das que ten coñecemento. Os routers cercanos intercambian este coñecemento para determinar o mellor camiño para enviar paquetes de datos. Este mellor camiño determinarase tendo en conta o custo asociado a cada unha das rutas posibles, por exemplo o número de routers intermedios que ten que cruzar ou a calidade da conexión. Sempre pode ter unha ruta "para todo o resto dos casos"que se chama *default gateway*.

Cando chega un paquete o router mira a súa cabeceira onde está almacenada información do destino

e mira na súa táboa de enrutamento para determinar cal é a interfaz pola que ten que enviar o paquete

Hai varios casos que debemos contemplar. Se hai sorte e o destinatario está na mesma rede que está conectada directamente a unha das bocas do router, daquela consúltase a táboa ARP e xa se envía. De ser o caso que o destinatario estea nesa rede pero non na táboa ARP xenérase unha petición ARP para averiguar cal é a MAC que coresponde con esa IP. Cando se ten a resposta envíase o paquete ao equipo que ten esa MAC (e aproveitase para deixala anotada na táboa ARP) e xa remata alí o seu camiño. As redes que estean conectadas ao router anótanse tal cal na táboa de enrutamento.

Pode ser o caso de que non estea o destinatario nas redes conectadas directamente a unha das bocas do router. Non hai outra que consultar a táboa de enrutamento. Como se crea a táboa de encamiñamento? Pode ser de xeito manual, o chamado enrutamento estático, ou por enrutamento dinámico.

Para que o router escolla entre estes tipos de enrutamento empregar existe a chamada **distancia administrativa** que é un indicador da fiabilidade dunha ruta. Vén sendo un número entre 0 e 255 que equivale ao *prezo* que temos que pagar por usar un tipo de protocolo ou outro para o enrutamento. Como podemos consultar no cadro. Un router usa rutas obtidas con menor distancia administrativa.

Protocolo	Distancia administrativa
Directamente conectado	0
Estático	1
OSPF	110
RIP	120

Cadro 1: Distancia administrativa de distintos protocolos de enrutamento.

En caso de empate, por exemplo se hai dúas rutas anotadas na táboa con igual distancia administrativa, o router escolle a ruta coa métrica máis baixa. A **métrica** é un parámetro asociado a cada ruta que indica a súa calidade, por exemplo o número de saltos ou a velocidade da conexión. Se aínda así hai empate o router pode usar o **balanceo de carga** para enviar paquetes por unha ruta ou outra o que vén sendo repartir os paquetes entre as distintas rutas posibles.

2. Encamiñamento estático

O enrutamento estático implica a configuración manual das rutas. Estas son fixas e requiren intervención dunha persoa experta que configure o router. Terá que facer as modificacións pertinentes cando calquera cambio se produza na rede.

A principal desvantaxe é a dificultade de xestionar e manter as rutas manualmente ante calquera

cambio, algo tan simple como pode ser que deixe de funcionar un router require da intervención do técnico. Esta pega faise especialmente relevante en redes grandes ou en constante cambio xa que e enrutamento estático é útil só para redes pequenas ou para rutas específicas que non cambian con frecuencia.

As vantaxes de usar este tipo de enrutamento son a seguridade, a simplicidade e a eficiencia. Como podemos ver no cadro este tipo de enrutamento terá prioridade sobre calquera outro agás que a rede esta directamente conectada a unha boca do router.

Un operador de rede pode configurar unha ruta estática nun router cun comando semellante a:

```
ip route add 192.168.2.0/24  via 10.0.0.2
```

Neste comando indícase cal é a rede á que vai destinado que sería a rede 192.168.2.0 e a máscara desa rede, 24 bits. O seguinte enderezo IP refírese á entrada no router seguinte. Esta IP chámase **gateway** traducido por porta de entrada do seguinte router que atravesará o paquete. Cada router ten configurada esta IP en cada boca e será unha IP do rango da rede que se conecta por esa interfaz.

3. Encamiñamento dinámico

Os routers veñen programados para utilizar diversos protocolos de enrutamento dinámico para construír a súa táboa de enrutamento. Cada protocolo ten as súas propias regras e métodos para determinar as rutas máis eficientes.

Estes protocolos establecen a comunicación entre os encamiñadores para que intercambien información sobre rutas. Ninguén ten que teclear nada manualmente, os routers constrúen as súas táboas de enrutamento pasándose información sobre as redes ás que ten acceso cada quen.

Un concepto importante a ter en conta no enrutamento dinámico é a **converxencia.** Cando se produce un cambio na rede, por exemplo unha conexión que cae, un novo dispositivo que se une ou unha ruta que mellora, os routers deben actualizar as súas táboas de enrutamento para reflectir esas novidades. A converxencia é o proceso polo cal os routers intercambian información e actualizan as súas táboas de enrutamento para adaptarse aos cambios. A converxencia rápida é esencial para manter a conectividade e a eficiencia da rede.

Chamaremos **tempo de converxencia** ao tempo que lle leva a un router atopar o mellor camiño despois de que se produza un cambio na rede. Terá que recalcular as rutas para adaptarse á nova situación. O desexable é que escollamos un protocolo de enrutamento co menor tempo de converxencia posible para que sexa capaz de minimizar o impacto dos cambios.

Protocolos de enrutamento dinámico

Os obxectivos deste tipo de protocolos son a eficiencia, a escalabilidade e a converxencia rápida facendo todo automaticamente e empregando os algoritmos axeitados para determinar as rutas máis eficientes en cada situación.

Cada protocolo escolle un criterio para calcular a mellor ruta para a viaxe do paquete, sexa a cantidade de etapas intermedias, o tráfico que hai nun intre determinado, a calidade da conexión ou a velocidade da mesma.

Cómpre ter en conta tamén que o algoritmo utilizado non consuma moitos recursos de memoria ou de CPU, xa que os routers teñen que facer cálculos constantemente para determinar as rutas máis eficientes. Estas contas deben ser rápidas e eficientes para non afectar ao rendemento da rede e evitar bloqueos ou caídas do sistema. O router ten que continuar traballando a pesar dos cambios na rede e debe ser capaz de adaptarse a eles sen problemas.

Clasifícanse en dous tipos principais: os protocolos de vector de distancia e os protocolos de estado de enlace. Nun caso só importa o intercambio de información entre veciños e no outro queremos ter unha visión global sobre o funcionamento de toda a rede.

3.1. Protocolos de vector distancia

Os protocolos de vector distancia, como RIP *Routing Information Protocol,* utilizan o número de saltos como métrica para determinar a ruta máis eficiente. Entendemos por saltos o número de routers intermedios que ten que cruzar un paquete no seu camiño.

Cada router anota na súa táboa as redes que ten conectadas directamente e envía a súa táboa de enrutamento a só os seus routers veciños regularmente (cada 30 segundos). Cando un router recibe unha táboa actualiza a súa propia e engade un salto á información que lle chega. En caso de duplicados quédase coa ruta coa menor métrica, neste caso o número de routers intermedios ou saltos. Esta táboa ampliada é o que enviará pola súa banda aos seus propios veciños.

Entre todos comparten información para construír cadansúa táboa e chegaremos á converxencia nalgún intre no que cada router terá información de toda a rede e poderá determinar o mellor camiño, entendido neste caso o mellor itinerario coa menor cantidade de saltos polos que ten que pasar. A súa converxencia pode ser lenta en redes complexas.

Existen dúas versións deste protocolo, RIP e RIP2. Unha das diferencias é que a primeira é un protocolo de claseful, mentres que a segunda é un protocolo de claseless, ou sexa, a versión 2 permite o uso de máscaras de subrede de longuras variables.

RIP é un protocolo simple e fácil de configurar, pero pode ser menos eficiente en redes grandes debido á súa limitación de saltos xa que non permite máis de 16 saltos para evitar bucles infinitos. A versión RIP2 permite 255 saltos. RIP2 tamén permite a inclusión de información adicional na súa táboa de enrutamento, como a calidade da conexión ou a velocidade da rede.

3.2. Protocolos de estado de enlace

Esta variante dos protocolos dinámicos *link-state* considera o estado da rede e non só os saltos intermedios polos que ten que pasar a información. Cada encamiñador crea unha especie de mapa das redes ás que ten acceso e comparte esta información con todos os outros routers da rede. Esta información inclúe non só as rutas dispoñibles, senón tamén a calidade da conexión, a velocidade e a carga da rede. Se por unha ruta hai moito tráfico ou a conexión é lenta, o router pode decidir que

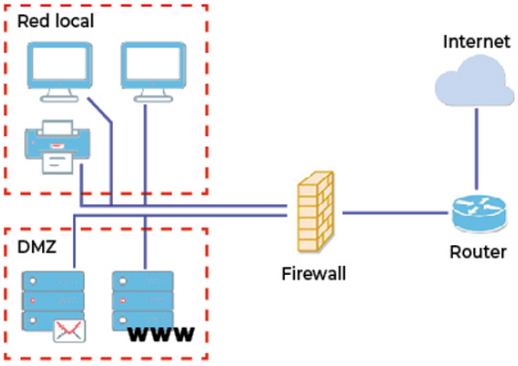

Figura 1: Exemplo de seguridade perimetral con DMZ.

outra ruta é máis eficiente nun determinado momento cando unha rede estea saturada.

OSPF é un exemplo de protocolo de estado de enlace que calcula sempre camiños mínimos utilizando o algoritmo de Dijkstra.

A súa principal vantaxe é a súa eficiencia e a súa capacidade para manexar redes grandes e complexas xa que unha das cousas que fai é enviar notificacións dos cambios só cando acontece algo, non cada 30 segundos, reducindo así o tráfico de rede.

A súa converxencia é máis rápida ca de RIP e permite unha mellor adaptación aos cambios na rede. O seu tempo de converxencia é xa que logo menor tamén grazas a que non usa protocolos da capa de transporte como RIP, senón que emprega protocolos da capa de rede, encapsulando a información nun datagrama IP. Por multicast envía a súa información a todos os routers, non só aos cercanos, usando o enderezo 224.0.0.5 ou 224.0.0.6

A súa principal desvantaxe é a súa complexidade e a súa difícil configuración en comparación con RIP.

3.3. Protocolos híbridos

Hoxe en día existen protocolos híbridos que combinan as vantaxes dos protocolos de vector de distancia e de estado de enlace. Un exemplo é EIGRP *Enhanced Interior Gateway Routing Protocol* que utiliza unha combinación de métricas e información de estado de enlace para determinar as rutas máis eficientes. EIGRP é un protocolo propietario de Cisco que ofrece unha converxencia rápida e unha alta escalabilidade. Aínda por riba xenera pouco tráfico de xestión do enrutamento cun mellor rendemento para a transmisión de datos.

4. Control de acceso e seguridade en redes

Cada empresa ou sistema autónomo debe ter un xeito de controlar quen se pode conectar aos seus servidores dende o exterior. Normalmente empregan unha táboa de enrutamento especial que se chama táboa de acceso ou **ACL** que se configura para permitir ou denegar o acceso a determinadas redes internas vou servizos.

Outra forma de facelo é con **cortalumes** tamén chamados devasas ou firewalls que son software

ou dispositivos de hardware que controlan o tráfico de rede e protexen a rede interna de accesos non desexados.

Hoxe en día os traballadores dunha empresa igual teletraballan polo que hai que ter en conta a seguridade dos accesos. O uso de **VPN** ou redes privadas virtuais é unha forma de protexer e asegurar a información sensible que se transmite a través de redes públicas como internet, que é intrinsecamente inseguro.Cando unha parte importante da rede empresarial debe estar especialmente protexida existen outras técnicas da chamada **seguridade perimetral** adicionais aos firewalls como son as **DMZ** ou zonas desmilitarizadas que é unha subrede que se sitúa entre a rede interna e a rede externa e que contén servidores que deben ser accesibles dende fóra, como servidores web ou de correo electrónico.

Imaxinemos unha empresa de venta por internet, as bases de datos de productos e os servidores web deben ser accesibles dende fóra, pero non queremos que os atacantes poidan acceder á rede interna da empresa onde se garda información confidencial pero os teletraballadores teñen que dar accedido. A DMZ permite separar os servidores públicos dos servidores privados e protexer a rede interna de accesos non desexados. Na figura podemos ver un exemplo de seguridade perimetral con DMZ. Os servidores de correo e as páxinas web da empresa están na DMZ, mentres que a rede interna está protexida detrás dun firewall. Os clientes poden acceder á DMZ, pero non á rede local. Un suposto atacante que acceda á DMZ non poderá acceder á rede interna da empresa ou viceversa.

5. Outros detalles

Queremos lembrar que os routers teñen a cotío máis dunha táboa de enrutamento, unha para IPv4 e outra para IPv6. Tamén poden ter unha táboa de enrutamento para cada protocolo de enrutamento que empreguen.

Debemos distinguir un par de conceptos que son confusos. Unha cousa é un protocolo de enrutamento como son RIP ou OSPF que é unha serie de regras e procedementos que os routers empregan para intercambiar información e construír as súas táboas de enrutamento. Outra cousa son os protocolos enrutables que son os que se usan para enviar os paquetes de datos pola rede, os que proporcionan os paquetes, un exemplo de protocolo enrutable é o IP.

Máis información

- Presentación sobre encamiñamento moi avanzado, pero moi chulo
- ccnadesdecero.es
- apuntesinformaticafp.com sobre enrutamento, con vídeos explicativos e incluso OSPF

Material elaborado para traballar na asignatura *Redes de área local* conxuntamente con: