TÉCNICO LISBOA

Arquitecturas de Redes

Licenciatura em Engenharia Telecomunicações e Informática

Mini-Projeto de Arquitecturas de Redes

Parte II

Grupo 63

João Silva – 51355
Afonso Caetano – 82539
Bruno Santos – 82053

Introdução

A rede da parte 2 do projecto é substancialmente diferente da rede que foi apresentada na parte 1. Tal opção, deveu-se ao facto de querermos demonstrar o funcionamento da tecnologia MPLS VPN, criando para isso duas VPNs (2 ou três áreas geográficas diferentes em cada uma) e um ISP central.
Desta forma, o número de routers e de ligações aumentou consideravelmente, e como tal, decidimos eliminar alguns elementos do desenho anterior, cuja tecnologia e modo de funcionamento já tinham sido demonstrados, como por exemplo, o OSPF multiárea.
Preservou-se a área 3 e o NAT, bem como a área 4, que ganhou uma nova funcionalidade.
A área 2 reduziu-se a um host e um router. A área 1 desapareceu.
Pretende-se demonstrar as seguintes tecnologias:

EtherChannel
EIGRP
BGP (eBGP/iBGP)
Tunneling
Virtual Private Networks em MPLS

Elementos de Rede

Área ISP
Conjunto de routers pertencentes a um ISP, que têm como função ligar vários *sites* do mesmo cliente, localizados em locais geograficamente distantes.
Tecnologias usadas: OSPF, MPLS VPN, MP-BGP

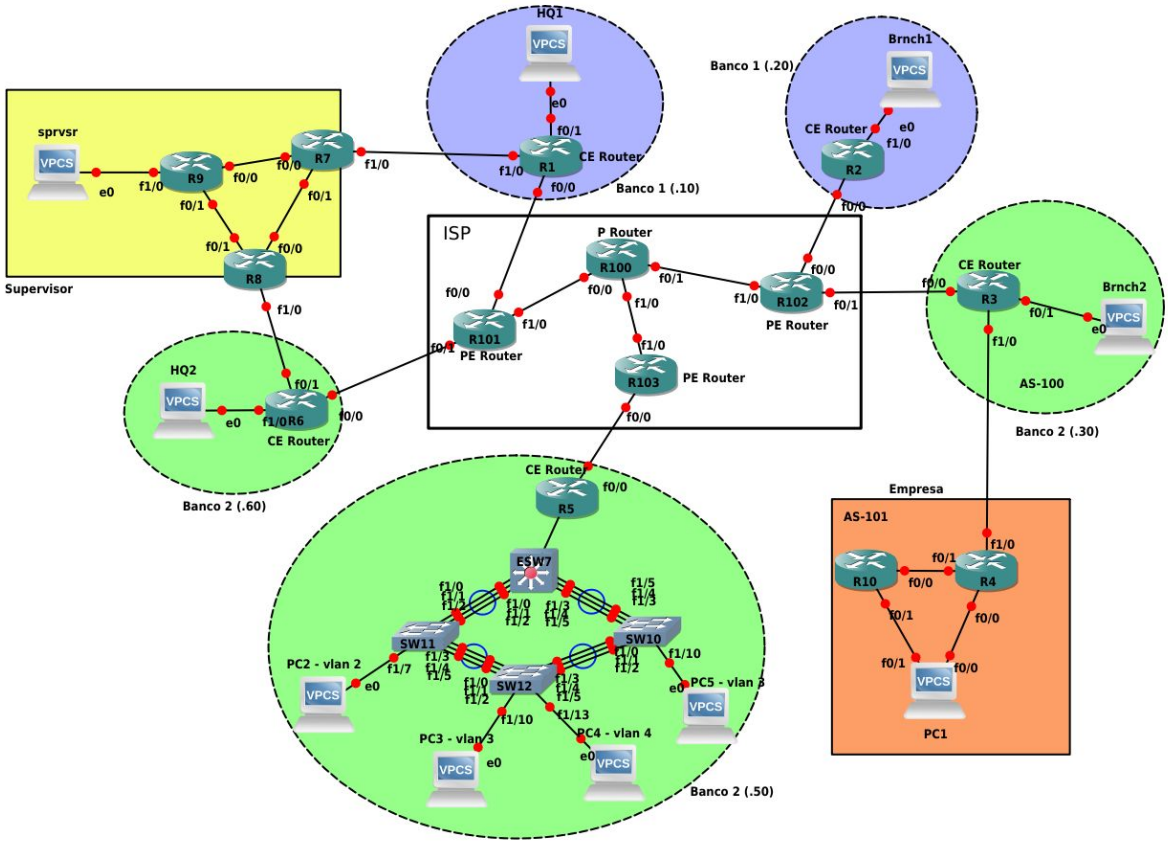
Áreas Banco 1/Banco2
Áreas contendo pelo menos um router e um host, que se destinam a demonstrar o funcionamento da VPN MPLS para dois clientes.

Área Banco 2 (.50)
Área pertencente ao Banco 2, herdada da parte 1 do mini-projecto. Destina-se a demonstrar o funcionamento do NAT dentro de uma VPN, bem como a utilização de EtherChannels.
Tecnologias usadas: NAT, DHCP, VLAN, EtherChannel

Supervisor
Área herdada da parte 1 do mini-projecto, com algumas modificações, nomeadamente a implementação do protocolo EIGRP. Destina-se também a demonstrar o funcionamento de túneis de ligação ponto a ponto, abstraindo a rota seguida, ligando HQ1 e HQ2 a sprvsr através de dois túneis GRE.

Área Empresa
Área criada para demonstrar o funcionamento do protocolo BGP nas suas variantes eBGP, através da ligação a routers pertencentes a Sistemas Autónomos diferentes, e iBGP através da ligação de routers pertencentes ao mesmo sistema autónomo.

Desenho da Rede



EtherChannel

No desenho apresentado, a rede definida por SW10, SW11, SW12 e ESW7 serve não só para comunicação entre os hosts, mas também de acesso dos hosts a uma rede exterior.
Um ponto de estrangulamento da performance da rede é a largura de banda das ligações partilhadas, isto é, das ligações entre os SW.
Uma das soluções possíveis para o problema poderia ser aumentar a largura de banda do link individual, de 100Mb/s para 1Gb, por exemplo, no entanto esta solução é dispendiosa e apresenta limitações de escalabilidade.
A solução alternativa, e aquela que foi implementada, passa por aumentar o número de ligações físicas entre switches. As ligações são agregadas numa ligação lógica, chamada EtherChannel, para impedir que o STP reconheça as ligações múltiplas como redundantes e as bloqueie como forma de prevenir o aparecimento de ciclos de encaminhamento.
Assim, como todas as ligações físicas do EtherChannel estão activas, a largura de banda é aumentada, uma vez que o tráfego passa a ser distribuído pelas várias ligações físicas.
Este método tem ainda a vantagem de proporcionar redundância, pelo que se uma das ligações se perder, as restantes continuam a assegurar a passagem de tráfego.
Note-se que todas as interfaces num EtherChannel têm que ter a mesma configuração e características.

Após a criação do EtherChannel, todas as configurações aplicadas a uma interface do mesmo, afectam igualmente as interfaces que lhe pertencem. Os EtherChannels foram criados em modo estático (on) e todas as suas interfaces foram definidas como trunk.
As portas de acesso a cada uma das 3 VLANs foram alteradas:
f1/7 a f1/9 - VLAN A
f1/10 a f1/12 - VLAN B
f1/13 a f1/15 - VLAN C
As interfaces trunk:
f1/0 a f1/5

EIGRP

O Protocolo EIGRP é um protocolo de encaminhamento dinamico *classless*, proprietário da Cisco, que combina as vantagens dos protocolos *link-state* e *distance vector*. Enquanto exibe um comportamento link-state, usando um protocolo de *Hello* para manter as relações de vizinhança, e enviando updates parciais quando uma mudança é detectada, a informação acerca do resto da rede é obtida unicamente através dos vizinhos directos, à semelhança de protocolos *distance vector*.
Designa-se muitas vezes por Advanced Distance Vector ou Híbrido.
Como vantagens contam-se:
Tempo de convergência (100% livre de ciclos de encaminhamento, sem *hold-down timer*, rota sucessora);
Classless routing (cada destino de rede é anunciado com uma máscara, suporta VLSM);

Load Balancing (entre ligações com custos iguais ou desiguais, permitindo maior controlo ao gestor de rede);
Reduzida utilização de largura de banda (não há updates periódicos, apenas quando alguma mudança ocorre. Só é enviada a informação relevante e apenas para os routers que dela necessitam, usando para isso multicast).

Na configuração apresentada, o protocolo EIGRP encontra-se instalado na área denominada “Supervisor”, nomeadamente entre os routers 7, 8 e 9.

O EIGRP foi definido apenas para encaminhamento IPv4.

BGP

O BGP (Border Gateway Protocol) é um protocolo de encaminhamento entre domínios, ou seja, trata-se de um protocolo dinâmico, utilizado na comunicação entre sistemas autónomos (AS’s). O BGP recorre ao uso de vetores de distância para a troca de informações de encaminhamento, enviados (entre routers BGP) através de uma rede TCP, que é criada para o efeito sobre a rede existente. Os BGP *speakers* (router’s que usam BGP) formam uma ligação TCP entre um e o outro com o objetivo de trocarem informações de encaminhamento, sendo assim referenciados como *neighbors*.
O BGP divide-se em dois tipos:

- iBGP (*internal*) - sessão entre routers que pertencem ao mesmo sistema autónomo.
- eBGP (*external*) - sessão entre routers pertencentes a diferentes sistemas autónomos.

Este protocolo utiliza 4 tipos de mensagens, sendo estas, a mensagem OPEN utilizada para iniciar uma sessão entre dois routers, a mensagem UPDATE para a troca de informações de encaminhamento, a mensagem KEEPALIVE para que a comunicação seja mantida e por fim a mensagem NOTIFICATION utilizada para reportar erros ou terminar ligações.

Na configuração apresentada, o protocolo eBGP encontra-se instalado nos routers R3 e R4 das áreas “Banco 2 (.30)” e “Empresa” respetivamente, enquanto que o iBGP encontra-se instalado nos routers R10 e R4.

Tunneling

Um túnel GRE (*Generic Routing Encapsulation*) é um protocolo de *tunelling* que garante um caminho seguro para transporte de pacotes IP sobre uma rede pública, encapsulando-os. Desta forma, o caminho seguido é abstraído dos hosts em comunicação.
O GRE adiciona um cabeçalho IP de 20 bytes e um cabeçalho GRE de 4 bytes, escondendo os cabeçados pré-existentes.
Note-se que a informação não é encriptada. Para isso poderia ser implementado o protocolo IPsec que funcionaria em conjunto com o GRE.
Na configuração apresentada, ligou-se o R9 a R6 através de um túnel GRE, de modo a que o host sprvsr conseguisse chegar a HQ2 pelo mesmo túnel. Para o efeito também foi instalado o protocolo OSPFv2, distribuindo assim a informação relativa à rede privada do lado oposto.

O mesmo processo foi usado para criar uma ligação entre R9 e R6, ligando assim não só HQ1 e sprvsr, mas também HQ1 e HQ2.
Criou-se assim uma solução para os três intervenientes conseguirem comunicar entre eles usando túneis.

MPLS VPN

A parte central da rede apresentada, representa um ISP, com 4 routers. Esse ISP serve de interligação entre dispositivos que, apesar de estarem em localizações geográficas diferentes, deviam estar ligados entre si como se se encontrassem fisicamente juntos, inclusivé dentro da mesma rede física. Uma VPN é uma solução que pode ser implementada, permitindo a utilização partilhada da rede ISP (geograficamente abrangente) para esse fim.

A VPN escolhida para implementação é de nível 3 e o seu modelo *peer-to-peer*. Neste modelo, a informação de encaminhamento é primeiramente trocada entre cliente e ISP (CE Router - PE Router), sendo depois encaminhada dentro do ISP até aos outros *sites* do mesmo cliente, através da melhor rota.
A tecnologia de encaminhamento da informação dentro do router é MPLS, que atribui etiquetas aos pacotes. Estes são encaminhados dentro da rede através dessas mesmas etiquetas e não dos endereços IP, permitindo assim maior rapidez. O facto de não usar endereços de IP é uma característica usada no caso das VPN.
Um ISP, pode ter vários routers a desempenhar este papel, e vários clientes a partilhar a mesma rede de routers. Para cada cliente pode existir uma rede virtual (VPN) criada com base nos mesmos routers, mas que pode ter um desenho diferente, consoante a utilização dos mesmos. A tecnologia que permite isto chama-se VRF - *Virtual Routing and Forwarding*.

Desta forma, para além da tabela de encaminhamento global do Router, vão existir tabelas de encaminhamento virtuais, baseadas em VRFs, para cada uma das VPNs suportadas.

Note-se que para o protocolo MPLS funcionar, necessita de um protocolo de encaminhamento de nível 3 em funcionamento (ou rotas estáticas). Sendo assim, no ISP corre também o protocolo OSPFv2.

Há alguns elementos de rede com designações e funções especiais que importa explicitar:
PE Router - *Provider Edge Router* - existe do lado do ISP, e mantém as regras de redistribuição de rotas e os mapeamentos de prefixos IPv4 da VPN e os prefixos VPNv4 na rede ISP.
P Router - *Provider Router* - existe no lado do ISP enquanto router de trânsito MPLS, no entanto não tem conhecimento de informação relativa à VPN.
CE Router - *Customer Edge Router* - Routers do lado do cliente, que estão directamente ligados aos PE Routers. Não necessitam de suportar VPN ou MPLS.

A informação de encaminhamento dentro de cada *site* da VPN é obtida pelos PE Routers através de protocolos de encaminhamento IP ou de rotas estáticas. Essa informação é depois distribuída entre PE Routers da rede ISP usando o protocolo MP-BGP (Multi-Protocol BGP). No caso apresentado, as rotas não são injectadas nos CE Routers, apesar de tal poder ser feito. Ao invés, optou-se pela definição de um default gateway nos CE Routers, o que leva a que os pacotes sejam enviados directamente para o PE correspondente, que tem conhecimento da rota a seguir.

Cada VPN é identificada univocamente por um campo de 64 bits chamado *Route Distinguisher* (RD). O RD juntamente com o prefixo IPv4 designa-se por VPNv4 e identifica a rede dentro de cada VPN. O protocolo BGP apenas suporta endereços IPv4, e como tal não é capaz de lidar com os 64 bits extra do RD. Usa-se então o MP-BGP para esse fim. É com base no VPNv4 que os routers do ISP conhecem a rota a usar e o destino a atingir para cada VPN.

Conclusão

A segunda parte do mini-projecto serviu para demonstrar tecnologias de redes que não eram requeridas na primeira parte.
Procuramos criar condições relevantes para a instalação de determinadas soluções que se pretendiam demonstrar, tendo para isso que alterar significativamente o desenho da rede e os seus componentes, como indicava o enunciado.
Foram implementados e apresentados: uma solução relativa ao encaminhamento de nível 2 (EtherChannel), dois protocolos de encaminhamento de nível 3 (EIGRP - mesmo sistema autónomo e BGP - entre sistemas autónomos) e uma tecnologia de tunneling, que permite encaminhar tráfego entre dois destinos em IPv4 abstraindo o caminho seguido. Finalmente, foi implementado em maior detalhe a solução que permite que a conectividade entre clientes em locais geográficos distintos seja assegurada através de uma infraestrutura partilhada, com o mesmo acesso e politicas de segurança que uma rede privada (MPLS VPN).