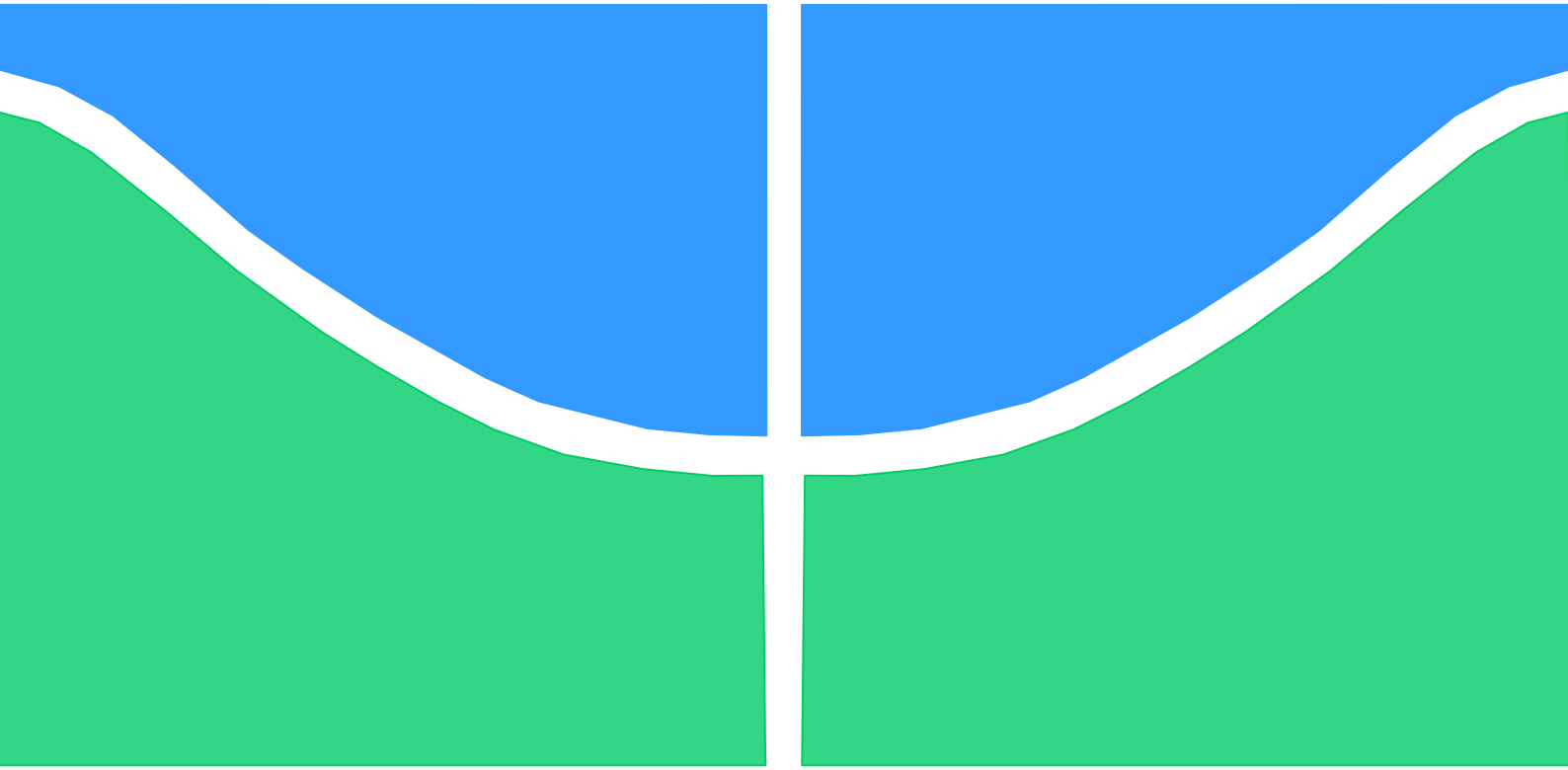


TRABALHO DE GRADUAÇÃO

ANÁLISE DOS ASPECTOS DE SEGURANÇA E DISTRIBUIÇÃO DE ROTAS EM FUSÃO DE REDES COORPORATIVAS

Felipe Xavier Souza Cruz
Rodrygo Torres Córdova

Brasília, 24 julho de 2013

UNIVERSIDADE DE BRASILIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASILIA
Faculdade de Tecnologia

TRABALHO DE GRADUAÇÃO

ANÁLISE DOS ASPECTOS DE SEGURANÇA E DISTRIBUIÇÃO DE ROTAS EM FUSÃO DE REDES COORPORATIVAS

Felipe Xavier Souza Cruz
Rodrygo Torres Córdova

Relatório submetido como requisito parcial para obtenção do grau de Engenheiro de Redes de Comunicações

Banca Examinadora

Prof. Dr. Edgard Costa Oliveira (Orientador)
Universidade de Brasília

Prof. Dr. Rafael Timóteo de Sousa Jr
Universidade de Brasília

Prof. Me. José Edil Guimarães de Medeiros
Universidade de Brasília

Dedicatória(s)

Este trabalho é primeiramente o fruto da dedicação e do amor dado por meus pais a mim, sem os quais nada seria possível. Dedico a eles, Rosineide e Córdova, este trabalho. A minha irmã, conselheira e amiga, Nathalya, por me inspirar a ser uma pessoa cada vez melhor. A minha namorada, Marcella, por estar sempre ao meu lado com seu lindo sorriso me apoiando e incentivando durante os momentos mais adversos nesta jornada.

Rodrygo Torres Córdova

Dedico este trabalho primeiramente aos meus pais, Lenilda e Euripedes, sem os quais eu não chegaria aonde cheguei e não seria nem metade da pessoa que sou. Dedico ao meu irmão que com um ar competitivo sempre me ajudou a ir além e me esforçar cada vez mais. Dedico a minha linda noiva que sempre me apoiou nos mais exaustivos momentos de estudo.

Felipe Xavier Souza Cruz

Agradecimentos

Agradeço a Deus primeiramente por me ajudar até aqui sempre me dando forças e não deixando esmorecer. Gostaria de agradecer também aos professores que me guiaram nessa graduação com valiosos ensinamentos, em especial meu ao meu orientador pela paciência e atenção nas mais diversas situações. Agradeço a todos meus companheiros do Ministério da Saúde, principalmente a minha chefe que sempre me deu total apoio nessa jornada. E por fim gostaria de agradecer aos meus amigos e familiares que sempre me apoiaram.

Felipe Xavier Souza Cruz

Agradeço a todos os meus amigos, familiares e professores que durante o percurso da graduação contribuíram para o meu amadurecimento pessoal, acadêmico e profissional, preenchendo este caminho com boas recordações. Agradeço ao meu orientador pelo empenho e responsabilidade neste importante processo final de formação. Agradeço a Deus por tornar tudo possível, sempre iluminando o meu caminho e as pessoas que passam por ele.

Rodrygo Torres Córdova

RESUMO

O presente texto apresenta conceitos básicos referentes a protocolos presentes no mercado de telecomunicações e um cenário controlado de redistribuição de rotas em redes coorporativas com protocolos heterogêneos, levantado primeiramente de maneira isolada os principais problemas que podem ser encontrados nesse tipo de contexto. Tem também como objetivo analisar as principais vulnerabilidades presentes nos diferentes domínios de roteamento de maneira conjunta nesse cenário. Por fim, esse estudo permitiu a elaboração de uma série de recomendações com a finalidade de minimizar ou eliminar essas vulnerabilidades e riscos.

ABSTRACT

This text presents basic concepts related to protocols present in the telecommunications market and a scenario controlled of route redistribution on corporate networks with heterogeneous protocols, raised primarily in isolation the main problems that may be encountered in this type of context. It also analyzes the major vulnerabilities present in different routing domains jointly in this scenario. Finally, this study allowed the elaboration of a series of recommendations in order to minimize or eliminate these vulnerabilities and risks.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS

Siglas

ABNT	Associação Brasileira de Normas Técnicas
ABR	*Area Border Router*
ACK	*ACKnowledgement*
ARP	*Address Resolution Protocol*
AS	*Autonomous System*
ASBR	*Autonomous System Border Router*
ASN	*Autonomous System Number*
BDR	*Backup Designated Router*
BGP	*Border Gateway Protocol*
BSD	*Barkeley Software Distribution*
CE	*Costumer Equipment*
CIDR	*Classless Inter-Domain Routing*
CPU	*Central Processing Unit*
DARPA	*Defense Advanced Research Projects Agency*
DD	*Database Description*
DR	*Designated Router*
DUAL	*Diffuding Update Algorithm*
EGP	*Exterior gateway Protocol*
EIGRP	*Enhanced Interior Gateway Routing Protocol*
EVC	*Ethernet Virtual Connection*
IETF	*Internet Engineering Task Force*
IGP	*Interior Gateway Protocol*
IGRP	*Interior Gateway Routing Protocol*
IP	*Internet Protocol*
IPX	*Internetwork Packet Exchange*
IR	*Internal Router*
ISO	*International Organization for Standardization*
ISP	*Internet service provider*
LAN	*Local Area Network*
LSA	*Link-State Advertisements*
LSAck	*Link-State ACKnowledgement*
LSDB	*Link State Database*
LSR	*Link State Request*

LSU	*Link State Update*
MAC	*Media Access Control*
MD5	*Message-Digest algorithm 5*
MEN	*Metro Ethernet Network*
MPLS	*Multiprotocol Label Switching*
MTU	*Maximum Transmission Unit*
NBMA	*Non-Broadcast Multiple Access*
NBR	Norma Brasileira
NSSA	*Not-So-Stubby-Area*
OSI	*Open Systems Interconnection*
OSPF	*Open Shortest Path First*
PDM	*Protocol-Dependent Modules*
PVC	*Permanent Virtual Circuit*
QOS	*Quality of Service*
RFC	*Request For Comments*
RID	*Router-id*
RIP	*Routing Information Protocol*
RTP	*Reliable Transport Protocol*
SPF	*Shortest Path First*
SVC	*Switched Virtual Circuit*
TCP	*Transport Control Protoco*
UDP	*User Datagram Protocol*
UNI	*User-Network Interface*
VL	*Virtual Link*
VPN	*Virtual Private Network*
WAN	*Wide Area Networks*

1 INTRODUÇÃO

Este capítulo apresenta considerações gerais preliminares relacionadas à maneira como esse texto foi produzido levando em consideração os objetivos adotados, metodologia utilizada e todo o contexto motivador para sua criação.

1.1 ASPECTOS GERAIS

Nos últimos tempos o mundo tem ficado cada vez mais conectado devido aos avanços no ramo das tecnologias de comunicações, principalmente a internet. A rede mundial de computadores tem se tornado mais densa a cada dia e acessada por milhares de novos usuários, seja para ler notícias, receber e enviar e-mails ou até mesmo se comunicar com outros usuários. A demanda por maneiras mais eficientes de transmissão de dados pela rede tem sido um dos focos dos pesquisadores no mundo moderno, essa demanda vem pela quantidade crescente de usuários e serviços utilizando a rede, seja por empresas ou simples usuários.

Nesse contexto se fez necessária a criação dos Protocolos, regras de sintaxe, semântica e comunicação, para padronização dessa rede que cresce a cada dia. Com diferentes necessidades na rede foram criados diferentes protocolos.

Atualmente protocolos para comunicação entre computadores em uma empresa podem ser diferentes dos usados por outra empresa, o que pode gerar certos problemas ou conflitos quando envolvidos no mesmo contexto de comunicações. As mais variadas adversidades podem ser relacionadas quando protocolos de topologias diferentes são associados. Um procedimento necessário para contornar esse tipo de situação é a redistribuição de rotas, que consiste em, basicamente, uma rede implementada em um protocolo se comunicar com uma rede implementada em outro.

Esse documento propõe com um estudo de caso modificado, maneiras de prevenir e evitar as principais vulnerabilidades presentes em um ambiente de redistribuição de rotas, em que pode se observar o uso dos principais protocolos utilizados no mercado atual.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Apresentar os principais aspectos de segurança e roteamento envolvidos em um ambiente real de rede coorporativa com protocolos heterogêneos.

1.2.2 Objetivos Específicos

- Apresentar as principais características e funções dos protocolos mais presentes no atual mercado tecnológico de redes de telecomunicações;
- Analisar de maneira isolada os principais problemas característicos encontrados em conexões entre protocolos heterogêneos;
- Realizar um estudo de caso onde são apresentados diversos problemas de conexão entre empresas que adotam protocolos diferentes, identificando os principais desafios desse cenário;
- Propor recomendações para uma melhor comunicação entre empresas com protocolos de redes heterogêneos.

1.3 METODOLOGIA.

O projeto foi elaborado em quatro partes. Primeiramente foi feito um levantamento e pesquisa bibliográfica, a seguir uma análise documental de problemas reais de estudos referentes a roteamentos e protocolos utilizados no mercado atual de redes de telecomunicações.

Para atingir o primeiro objetivo foi feita uma análise documental por meio de comparações, fichamentos e tabulações que ajudaram a identificar os principais protocolos e procedimentos adotados nas empresas de telecomunicações.

No segundo objetivo foi feito um estudo com casos reais de pequeno porte de implantação de redistribuições entre empresas com protocolos diferentes, abordando cada problema isoladamente.

Em seguida, com base nos resultados obtidos, partimos para um cenário adaptado de um caso real onde pudessem ser abordados vários dos problemas de conexão entre protocolos diferentes de maneira geral. Produzindo imagens referentes ao tema com objetivos de melhor explorar esses tipos de procedimentos.

Para finalizar, são apresentados os resultados de todo o caso real abordado e as recomendações para melhor implantação de uma distribuição eficaz entre empresas com protocolos diferentes.

1.4 JUSTIFICATIVA

Com a diversificação cada vez maior do mercado empreendedor se faz necessário um estudo aprofundado das principais características e vulnerabilidades dos protocolos usados por elas, justifica-se também a busca de um maior entendimento de como esses protocolos se comportam em presença de outros, verificando medidas de segurança, adequação e principais recomendações para a eficiente redistribuição das rotas desses.

Nessa abordagem ainda, é necessária não só a enumeração e a elucidação desses protocolos e suas situações atípicas, mas sim um levantamento de casos reais e sólidos para um melhor entendimento prático do contexto desses protocolos e seus devidos comportamentos em face de tais situações, preparando uma apanhado documental que reúna uma significativa quantidade de informação para melhor auxiliar futuros profissionais que venham se deparar com situações semelhantes no mercado tecnológico.

2 REVISÃO LITERÁRIA

Nesse capítulo serão abordados de maneira elucidativa os principais protocolos e seus antecessores mais significativos para um melhor entendimento contextual do cenário atual encontrado no universo de redes de comunicação que serão abordados nos próximos capítulos desse texto.

2.1 PROTOCOLO TCP/IP

O TCP/IP é a sigla de *Transfer Control Protocol / Internet Protocol* que representa um conjunto de protocolos de comunicação entre computadores, também chamados de pilha de protocolos TCP/IP, que pode ser visto como um modelo de camadas, onde se vê uma divisão clara de funções onde se define os serviços dedicados a cada camada e os quais serão fornecidos a camada superior (Kurose, 2009).

- Camada de Aplicação: Contém aplicações de redes e seus protocolos em um nível processo-a-processo.
- Camada de Transporte: Controla a comunicação *host-a-host*, transportando mensagens entre cliente e servidor da camada de aplicação, podendo ser orientado ou não a conexão.
- Camada de Rede: Responsável pela movimentação de datagramas, pacotes de camada de redes, recebe o endereço de envio da camada de transporte provendo o serviço de entrega do segmento à camada de transporte.
- Camada de Enlace: Recebe da camada de rede o datagrama para que seja feita a entrega ao nó seguinte, onde a camada de enlace o passa novamente para a camada de rede subsequente.
- Camada Física: Faz a movimentação dos bits individualmente que estão dentro do pacote de um nó ao outro.

O TCP/IP é um projeto da DARPA (*Defense Advanced Research Projects Agency* - Agência de Projetos de Pesquisa Avançada de Defesa) sobre a conectividade entre redes, no final dos anos 70. O TCP está definido nas RFC's 793, 1122, 1323, 2018 e 2581.

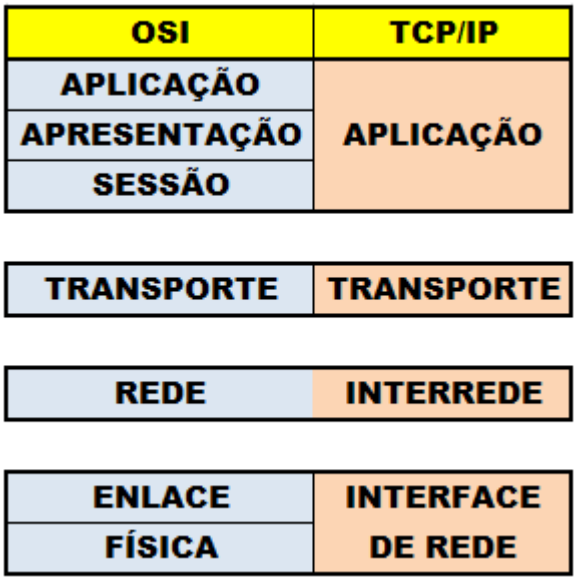


Figura 1 – Comparativo entre os modelos OSI e TCP/IP (Adaptado Kurose,2009).

O modelo TCP/IP não é o único modelo de camadas encontrado no mercado existe também um modelo proposto pela Organização Internacional para Padronização (ISO) que propõe a divisão em sete, e não cinco camadas, denominadas de modelo de Interconexão de Sistemas Abertos (OSI). As sete camadas do modelo OSI são: Camada de Apresentação, Camada de Sessão, Camada de Transporte, Camada de Rede, Camada de Enlace e Camada Física. Como pode ser visto, a diferença principal está nas duas camadas adicionais, essas duas camadas estão presentes no TCP/IP dentro da Camada de Aplicação. A Camada de Apresentação provem serviços que ajudam na interpretação dos dados trocados entre as aplicações de comunicação e a Camada de Sessão delimita e sincroniza a troca de dados com pontos de verificação e recuperação.

2.2 ROTEAMENTO

O roteamento é o processo que determina como um pacote deve ser encaminhado e qual caminho deve seguir quando se trafega entre redes diferentes. Ele permite a comunicação entre hosts localizados em redes distintas. O processo de roteamento pode ser definido estaticamente ou dinamicamente.

O roteamento estático requer a intervenção manual para implementação de rotas para a comunicação de acordo com a topologia de rede, a construção e modificação da tabela de roteamento são realizadas administrativamente com a inserção de todas as informações das rotas necessárias em cada roteador. Geralmente são utilizadas de e para *stub networks* (redes que possuem apenas uma saída e entrada), em redes menores que não possuem mudança ou crescimento significativo esperado e para o uso de rota padrão.

O roteamento dinâmico promove a troca automática de informações de rotas entre os roteadores da rede permitindo que a tabela de roteamento seja criada e modificada dinamicamente com os melhores caminhos de acordo com a métrica utilizada pelo protocolo de roteamento. Geralmente utilizado em grandes redes que são intermediarias para o tráfego de dados, redes com potencial de crescimento e que precisam responder rapidamente a mudanças de topologia.

Tabela 1 – Roteamento Estático X Roteamento Dinâmico

Roteamento:	**Roteamento Estático**	**Roteamento Dinâmico**
Vantagens:	Processamento mínimo de CPU	Escalável
	Fácil entendimento	Automático
	Estável	Menos propenso a erro
	Previsível	Menor sobrecarga de configuração
Desvantagens:	Sobrecarga de Configuração e Manutenção	Uso de recursos de largura de banda e processamento do roteador
	Configuração propensa a erros	Pode se tornar instável
	Intervenção administrativa	Exige maior conhecimento para configuração e manutenção
	Não escalável	

Os protocolos de roteamento dinâmico são separados em duas categorias:

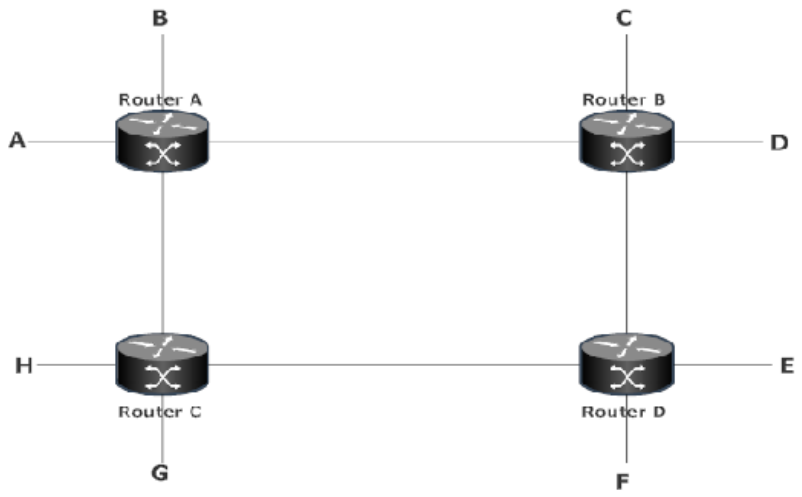
- *Interior Gateway Protocol* (IGP): quando as informações de roteamento são distribuídas internamente somente entre roteadores pertencentes ao mesmo *Autonomous System* (AS).
- *Exterior gateway Protocol* (EGP): quando as informações de roteamento são distribuídas entre limites de *Autonomous System* (AS), entre roteadores pertencentes a AS's distintos.

Entre os protocolos dinâmicos IGP, existem dois tipos:

- *Distance Vector*: determinam as rotas para os caminhos baseado em algumas informações obtidas diretamente dos roteadores vizinhos relacionadas a vetores de distância, como módulo e direção. Não possuem o conhecimento completo da topologia de rede, as informações completas de roteamento precisam ser periodicamente atualizadas. A determinação das melhores rotas leva em consideração as informações dos roteadores vizinhos.
- *Link*-State: determinam as rotas para os caminhos baseado em algumas informações obtidas pelos roteadores presentes na rede, como estado e largura de banda de *links*. Possuem o conhecimento completo da topologia de rede, apenas quando necessário são enviadas informações de roteamento. A determinação das melhores rotas é realizada de maneira independente por cada roteador pertencente ao domínio.

2.3 PROTOCOLO RIP

O protocolo *Routing Information Protocol* (RIP) é um protocolo de roteamento da internet baseado em vetor distâncias para envio de *datagramas*, a sua grande difusão no mercado se deu quando distribuído gratuitamente e com suporte a TCP/IP na versão do UNIX do *Barkeley Software Distribution* (BSD), Universidade da Califórnia, um melhoramento do protocolo criado pela Xerox Corporation, em 1982. O RIP possui duas versões a primeira especificada na RFC 1058 e a segunda versão, compatível com a primeira, na RFC 2453.



DESTINO	SALTOS
A	1
B	1
C	2
D	2
E	3
F	3
G	2
H	2

Figura 2 – Exemplo de roteamento RIP e tabela do *Router* A.

A primeira versão do RIP tem sua métrica de custo baseada na contagem de saltos, ou seja, cada enlace que passa conta com um salto, essa métrica é trocada entre os roteadores próximos em forma de tabela de roteamento. Esse tipo de roteamento não é preciso já que só leva em consideração o número de saltos e não o possível tráfego e questões de banda que podem interferir na transmissão. Essas rotas são atualizadas a cada 30 segundos, caso a rota não seja atualizada em 180 segundos é dado uma métrica de valor infinito a ela, posteriormente sendo removida da tabela.

Na segunda versão foram melhorados aspectos de suporte a máscaras de comprimento varáveis e acréscimo de rota, tornando assim as mensagens de roteamento menores e uma melhor alocação de endereços. Mesmo com mudanças significativas ainda sofre problemas de roteamento como na primeira versão.

2.4 PROTOCOLO EIGRP

O protocolo *Enhanced Interior Gateway Routing Protocol* (EIGRP), proprietário da CISCO, é um protocolo *classless* baseado em *distance-vector* lançado em 1992. É um aprimoramento do protocolo *Interior Gateway Routing Protocol* (IGRP) da CISCO. O propósito principal no desenvolvimento do EIGRP foi criar uma versão *classless* do IGRP e que atendesse ao cenário das novas redes de comunicação, que devido ao seu crescimento, limitou significativamente a eficiência dos antigos protocolos de *distance-vector* RIP e IGRP, principalmente no quesito convergência e escalabilidade. O EIGRP possui vários recursos para tornar o seu desempenho superior e que não são encontrados nos tradicionais protocolos de *distance*-vector como:

- *Reliable Transport Protocol* (RTP) e *Protocol-Dependent Modules* (PDM);
- *Bounded Updates*;
- Algoritmo *Diffuding Update Algorithm* (DUAL);
- Estabelecimento de Adjacências;
- Tabela de Topologia e Vizinhança.

O EIGRP foi projetado para realizar o roteamento de vários protocolos da camada de rede, como por exemplo, IP, IPX e *AppleTalk*, tornando-se independente da camada de rede. Módulos específicos, com a utilização do *Protocol-Dependent Modules* (PDM), gerenciam a troca de informações de roteamento exigidas para cada protocolo de camada de rede, cada módulo é responsável por tarefas específicas para cada protocolo.

Isso impossibilita o EIGRP de utilizar os serviços dos protocolos de transporte tradicionais como o TCP e UDP, pelo fato de que eles não são utilizados pelos protocolos IPX e *AppleTalk*. Como solução o EIGRP utiliza outro protocolo proprietário da CISCO, o *Reliable Transport Protocol* (RTP). O RTP trabalha com transporte confiável de entrega ordenada e garantida que exige uma confirmação do recebimento da mensagem, similar ao TCP, e transporte não confiável, que não exige uma confirmação, similar ao UDP. O transporte confiável ou não é utilizado dependendo do tipo de mensagem EIGRP que será envida. Os pacotes enviados com RTP podem ser *unicast* ou *multicast* para o endereço IPv4 224.0.0.10.

Cinco pacotes são utilizados para a comunicação: *Hello Packet*, utilizado para troca de parâmetros e descoberta de vizinhos, podendo ser enviados em modo *multicast* ou *unicast*; *Update Packet*, utilizado para propagar informações de roteamento e informar mudanças de topologia, sendo enviados somente quando necessários, com as informações necessária e somente para os roteadores necessários, podendo ser enviado em modo *multicast* ou *unicast*; *Querry Packet e Reply Packet*, utilizados pelo algoritmo do EIGRP para solicitar e responder informações de rotas, *Querry* para solicitar, enviado em *multicast* e *Reply* para responder, enviado em *unicast* e *ACK Packet*, empregado para confirmar o recebimento de um pacote quando é utilizada a entrega confiável do RTP. Os pacotes *Update*, *Querry* e *Reply* utilizam o protocolo RTP confiável requerendo que um pacote ACK seja enviado para assinalar o recebimento, já o pacote *Hello* utiliza o protocolo RTP não confiável e não requer uma resposta de recebimento (CISCO, 2009).

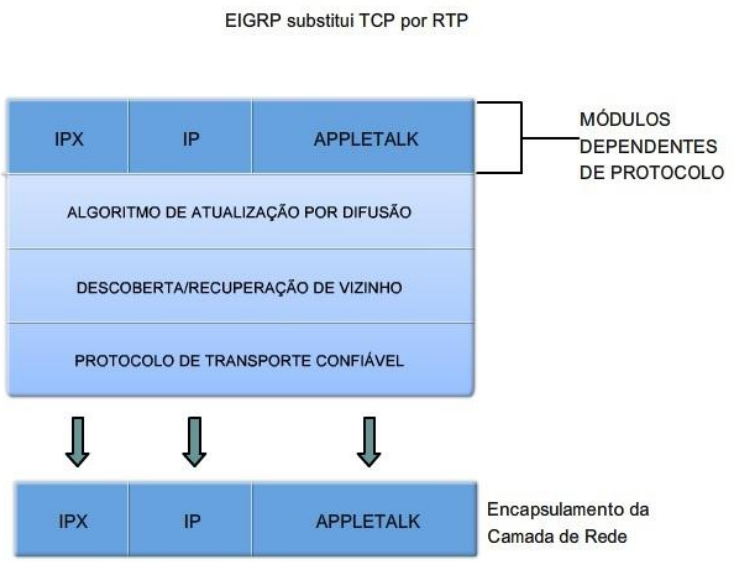


Figura 3 – *Protocol-Dependent Modules* e *Reliable Transport Protocol* (CISCO, 2009).

Os protocolos tradicionais de *distance-vector* utilizam algumas variantes do algoritmo *Bellman-Ford*, onde as informações de roteamento devem ser periodicamente enviadas para que as informações individuais não expirem acusando uma falsa mudança de topologia e sendo desconsideradas no processo de construção da tabela de roteamento. Dependendo da largura de banda do canal utilizado e do tamanho da tabela de roteamento, esse processo pode provocar o aumento do consumo de banda e do processamento do roteador, afetando o desempenho da rede.

Estas atualizações periódicas e o processo pelo qual elas são realizadas estão propensos a causar alguns problemas como *loops* de roteamento e contagens até o infinito, quando uma rota não é mais considerada válida. Para evitar estes problemas, alguns artifícios são utilizados como, por exemplo, o *Split-Horizon* e temporizadores como *Hold-down*, estes artifícios afetam a velocidade e a limitação de convergência da rede.

O EIGRP é um protocolo de *distance-vector* que utiliza o *Split-Horizon*, mas não utiliza o temporizador *Hold-down*. Para evitar *loops* de roteamento é utilizado um algoritmo para cálculos de rota que são executados de uma forma coordenada entre os roteadores, chamado de *Diffuding Update Algorithm* (DUAL). Este algoritmo resulta em uma rápida convergência em comparação com os protocolos tradicionais de *distance-vector*.

O algoritmo DUAL é o ponto principal do EIGRP. Ele não envia atualizações periódicas e as entradas individuais com as informações de roteamento não expiram, ao invés disso, ele utiliza pacotes *Hello* para monitorar os estado de seus vizinhos. Estes pacotes *Hello* são utilizados para descobrir automaticamente outros roteadores diretamente conectados que estão operando com o protocolo EIGRP e monitorar o seu estado. Assim, como atualizações são realizadas somente quando ocorrem alterações nas informações de roteamento e existe o monitoramento dos vizinhos, enquanto a relação de vizinhança estiver normal, as últimas informações de roteamento podem ser consideradas válidas. Embora isso ocorra, as atualizações de roteamento do EIGRP ainda são de *distance-vector*, anunciando rotas e métricas aos vizinhos diretamente conectados.

O DUAL mantém uma tabela de topologia que inclui todos os caminhos aprendidos por meio de seus vizinhos. Esta tabela inclui os melhores caminhos livres de *loop* de roteamento, os caminhos *backup*, que o DUAL considera como uma rota alternativa sem *loop* que pode ser usada para um destino para o qual já existe um melhor caminho definido e outros caminhos, que o DUAL não pode garantir que sejam livres de *loop*.

Quando ocorre uma mudança na topologia de rede que provoca a remoção de uma rota da tabela de roteamento, o algoritmo DUAL busca em sua tabela de topologia por uma rota *backup*, caso esta rota exista, ela é inserida na tabela de roteamento, convergindo rapidamente à rede novamente. Caso não exista uma rota *backup*, o DUAL inicia o processo para eleger uma nova rota sem loop de roteamento.

A definição de uma rota *backup* evita que cálculos desnecessários do algoritmo DUAL sejam realizados e atrasem a convergência da rede. O algoritmo DUAL pode ser representado pela máquina de estados da Figura (4):

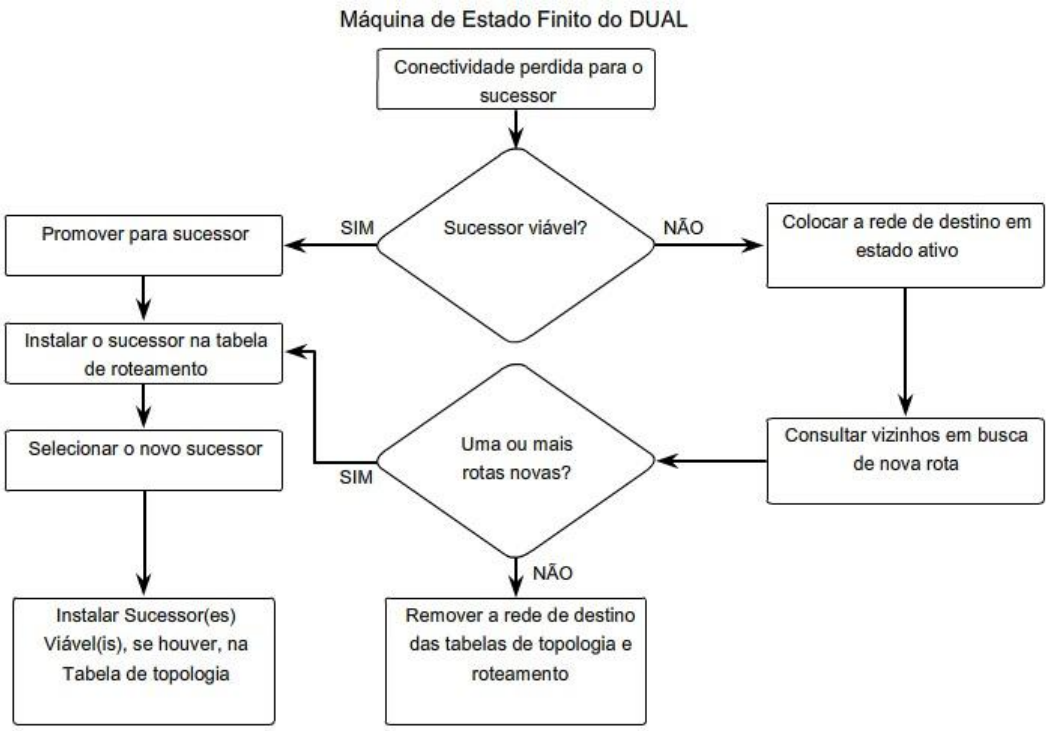


Figura 4 – Máquina de Estado DUAL (CISCO, 2009).

A métrica utilizada pelo algoritmo DUAL utiliza informações referentes à distância: largura de banda, atraso, confiabilidade e carga do link. Por padrão, apenas a largura de banda e atraso são utilizados. O processo de propagação de informações de topologia utilizando pacotes *Update* é feito da seguinte forma (CISCO, 2009):

1. Quando a informação é originada pelo roteador, ele adiciona ao pacote as seguintes informações da rota: endereço/prefixo da rede, atraso, largura de banda, MTU (*Maximum Transmission Unit*), carga e confiabilidade do link e *Hop* igual a zero.
2. Quando um roteador recebe por um *link* o pacote *Update* com informações de uma rota, ele trata as informações da seguinte maneira: soma o atraso do link ao contido no pacote, compara as larguras de banda do link e do pacote, utilizando a mais baixa, compara os MTUs, utilizando o mais baixo, compara a carga, utilizando a mais alta, compara a confiabilidade, utilizando a mais baixa e por fim soma um, ao valor de *hop* do pacote.

Após a coleta de todas as informações de rotas, a tabela de topologia é definida e as métricas são analisadas (com a menor métrica sendo a melhor) para determinar as melhores rotas e rotas de *backup*. Os roteadores que serão utilizados como próximo salto para os melhores caminhos são designados como *Successor Router*, os roteadores que serão utilizados como próximo salto para os caminhos de *backup* são designados como *Feasible Sucessor*. Estes são os roteadores que possuem uma rota alternativa para o melhor caminho e que atenderam a condição chamada de *Feasilbe Condition*. A condição determina que apenas roteadores que possuem uma rota com uma métrica menor que a atual métrica da rota utilizada para alcançar determinado caminho, podem ser considerados *Feasible Sucessor* para aquela rota.

2.5 PROTOCOLO OSPF

O protocolo aberto *Open Shortest Path First* (OSPF) é um protocolo de roteamento dinâmico baseado em *link-state* e projetado especificamente para redes de comunicação que utilizam a arquitetura TCP/IP. Foi desenvolvido para operar internamente ao *Autonomous System* (AS), sendo classificado como um protocolo *Internal Gateway Protocol* (IGP), o que significa que a distribuição de informações de roteamento é realizada somente entre os roteadores do mesmo AS. É inerentemente *classless*, suportando *Classless Inter-Domain Routing* (CIDR), e realiza a marcação de rotas derivadas de fontes externas de informações. A sua primeira versão, conhecida como OSPFv1, foi especificada e publicada em outubro de 1989 por meio da RFC 1131, foi basicamente experimental e ficou obsoleta com a publicação em julho de 1991 da RFC 1247 que especificou a segunda versão do protocolo, OSPFv2, atualizada pela RFC 2328 em abril de 1998. Por volta de um ano depois foi especificada a versão do protocolo para IPv6, OSPFVv3, na RFC 2740.

Baseado no algoritmo *Shortest Path First* (SPF), também conhecido como tecnologia *link-state* e algoritimo de Dijkstra, foi um marco em relação aos tradicionais protocolos de roteamento dinâmico baseados em *distance-vector*, que utilizam o algoritmo de *Bellman-Ford*. Em um cenário de protocolo de roteamento *link-state*, os roteadores passam a anunciar os estados de seus links, por meio de *Link-State Advertisements* (LSA) que contem informações como o estado de suas interfaces e das relações de vizinhança mantidas nestas interfaces, e não mais rotas como nos protocolos *distance-vector*. Cada roteador mantém uma base de dados chamada de *Link State Database* (LSDB) que contem informações do estado do link de cada roteador descrevendo a topologia de rede do AS. A partir destas informações, cada roteador executando o algoritmo paralelamente e de forma independente, utilizando a sua LSDB para construção da árvore *Shortest Path*, que reflete a sua perspectiva da rede, colocando-se como raiz desta árvore. Esta possui rotas para cada destino dentro do AS, com as rotas externas, destinos para fora do AS, aparecendo como folhas da árvore. A partir desta árvore, o roteador pode basear a construção da sua tabela de roteamento.

A métrica OSPF para determinar a melhor rota é chamada de custo. Um custo está associado com o lado de saída de cada interface do roteador. Este custo é configurável pelo administrador do sistema. Quanto menor o custo, mais provável será o uso da interface para encaminhar o tráfego de dados. Se múltiplos caminhos possuírem o menor custo igual para determinado destino, todos os caminhos serão utilizados para encaminhamento do tráfego, causando um balanceamento de carga sobre os caminhos (RFC 2328).

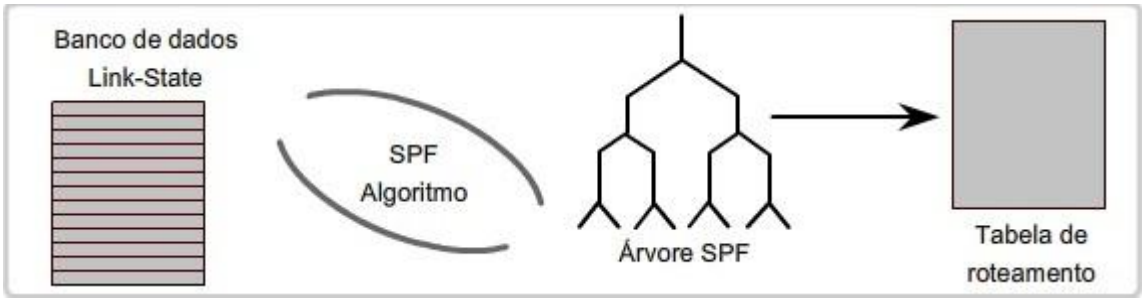


Figura 5 – Construção da Árvore SPF e da Tabela de Roteamento (Modificado CISCO, 2009).

A troca de informações entre vizinhos são realizadas quando uma adjacência completa é formada entre eles, vizinhança não é sinônimo de adjacência, ou seja, roteadores vizinhos não necessariamente vão trocar informações de roteamento. Os dados da mensagem OSPF são encapsulados em um pacote IP com o campo *type* do cabeçalho com o valor 89, indicando que o pacote IP trata-se de uma mensagem OSPF. Neste pacote, após o cabeçalho IP, vem o cabeçalho OSPF, sempre presente em todos os cinco tipos de pacotes utilizados pelo OSPF e por fim vem o campo de dados OSPF, específico para cada tipo de pacote. As mensagens são transmitidas por *multicast* (endereço IP 224.0.0.5 destinado a todos os roteadores OSPF e endereço IP 224.0.0.6 destinado a roteadores OSPF *Designated Router*). Os cinco pacotes OSPF são listados na Tabela (2):

Tabela 2 – Pacotes OSPF

Tipo	Nome	Função
Type 1	*Hello*	Utilizado para detectar e manter relações de vizinhança. Anuncio de parâmetros para formação de vizinhança e eleição de *Designated Router* (DR) e *Backup Designated* Router (BDR).
Type 2	*Database Description*	Utilizado para processos de sincronização do LSDB.
Type 3	*Link State Request*	Utilizado para solicitar registro de rotas completas para um *link-state*.
Type 4	*Link-State Update*	Utilizado para atualização e envio de *link-state* solicitados. Contem informações completas de LSA.
Type 5	*Link-Sate Acknowledgment*	Utilizado para confirmar o recebimento do *Link State Update*(LSU)

Todas as mensagens OSPF são autenticadas, ou seja, somente roteadores legitimados do AS podem trocar informações de roteamento. Três tipos de autenticação são determinados (RFC 2328):

- *Null Authentication* (*Type* 0): este tipo e autenticação significa que a troca de informações de roteamento não são autenticadas. O campo *Authentication* do cabeçalho OSPF é ignorado.
- *Simple Password* (*Type* 1): este tipo de autenticação determina que o campo *Authentication* será configurado com uma senha em clara de 64-bits por rede. Cada roteador precisa ser configurado com a senha antes de participar do processo de roteamento. Este tipo de autenticação basicamente evita que roteadores inadvertidamente entrem no domínio de roteamento, uma vez que a senha é visto em clara na troca de mensagens e vulnerável a ataques passivos.
- *Cryptographic Authentication* (*Type* 2): este tipo de autenticação utiliza uma chave secreta compartilhada trocada utilizando o algoritmo *Message Digest 5* (MD5) entre roteadores conectados a mesma rede. Adiciona proteção contra ataques passivos.

O encapsulamento dos pacotes OSPF dentro do pacote IP, assim como o conteúdo do cabeçalho OSPF, estão representados na Figura (6).

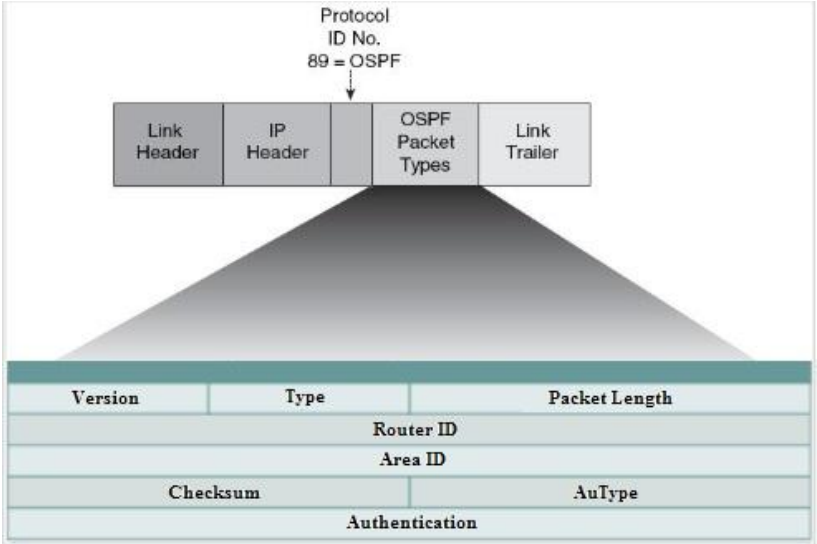


Figura 6 – Cabeçalho OSPF encapsulado no pacote IP (Adaptado de CISCO, 2009).

O OSPF possibilita a implementação de uma hierarquia baseada em áreas. A área principal chamada de área *backbone*, também conhecida como área 0, deve estar interligada a todas as outras áreas. Todo o tráfego entre áreas não *backbone* deve passar pela área 0. Cada roteador tem informações completas de topologia da área a qual pertence e informações parciais das outras áreas. A execução do algoritmo SPF é restrita a cada área, ou seja, um roteador executa o algoritmo apenas se houver uma mudança na topologia da área ao qual ele pertence, uma vez que ele deve ter informações completas sobre a sua área. Essa divisão em áreas proporciona escalabilidade e reduz o consumo de banda e processamento. As tabelas de topologia e de roteamento dos roteadores são reduzidas, poupando recursos do roteador para processamento das rotas. Com base nesta divisão de áreas, classificamos os roteadores como: *Backbone Router* (BR), todas as interfaces pertencem a área 0; *Internal Router* (IR), todas as interfaces pertencem a uma única área que não seja a backbone; *Area Border Router* (ABR), possui interfaces em áreas diferentes com pelo menos uma pertencente a área 0; *Autonomous System Border Router* (ASBR).

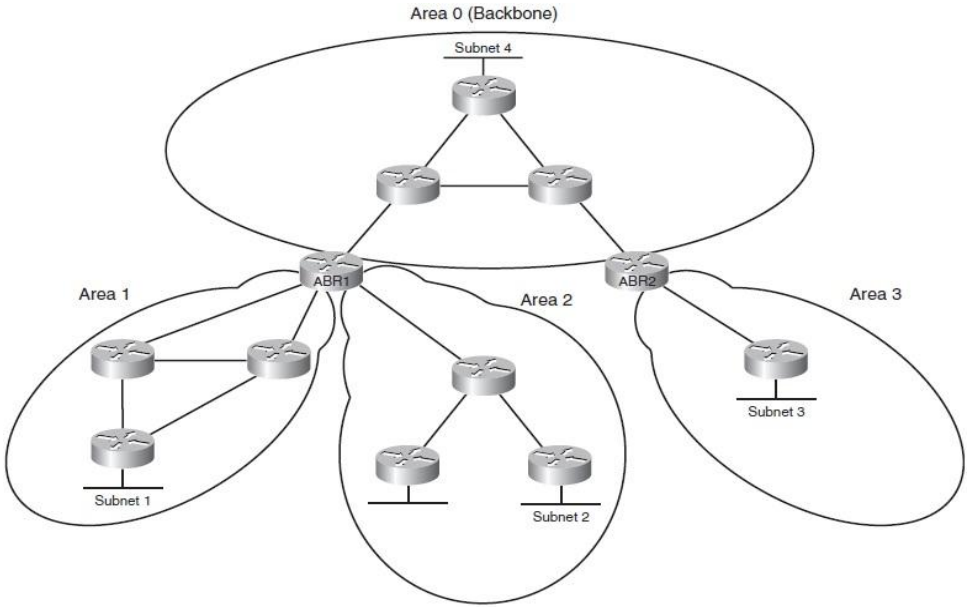


Figura 7 – Hierarquia OSPF Tradicional (CISCO, 2010).

Tabela 3 – OSPF *Link-State Advertisements*

Tipo	**Nome**	**Roteador Gerador**	**Função**
Type 1	*Router Link*	Todos	Representar o roteador na sua área. Contem informações do RID (*router-id*), IP e custo/estado das interfaces e RID dos vizinhos. O LSDB de cada área possui um *Router Link* para cada roteador pertencente à área.
Type 2	*Network Link*	DR	Representa as *subnets* e as interfaces dos roteadores conectados a *subnet*.
Type 3	*Net Summary Link*	ABR	Representa as *subnets* listadas em uma área pelo *type* 1 e 2 quando anunciadas em outra área. Possui informações de custo, mas não da topologia.

Type 4	*ASBR Summary Link*	ABR	Contem o custo do ABR para alcançar o ASBR quando aquele retransmite em uma área o LSA *type* 5 do ASBR.
Type 5	*AS External Link*	ASBR	Injetar rotas externas dentro do domínio OSPF.

A partir da hierarquia de áreas e da classificação de cada roteador, são gerados tipos de LSA, os mais importantes são listados na Tabela (3):

2.6 TECNOLOGIAS DE ACESSO

2.6.1 Frame Relay

É um protocolo WAN que utiliza comutação por pacotes para transmissão de dados, compartilhando dinamicamente e flexivelmente tanto a largura de banda como os meios de transmissão.

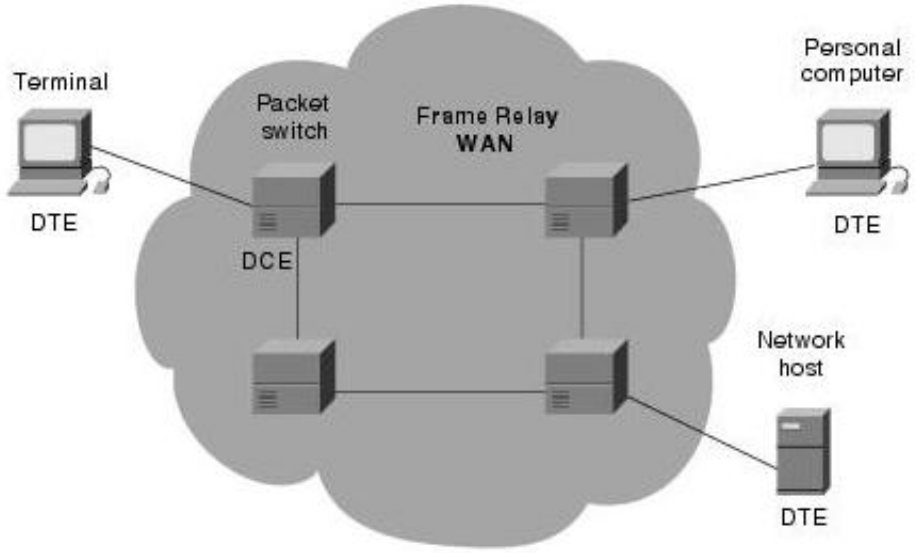


Figura 8 – Exemplo de uma rede com transmissão em Frame Relay (CISCO, 2009).

O Frame Relay utiliza a tecnologia de circuitos virtuais, o que cria para a transmissão um tipo de conexão dedicada, que podem ser *Switched Virtual Circuit* (SVC), para conexões temporárias feitas à medida que são necessárias, ou *Permanent Virtual Circuit* (PVC), feita de maneira permanente em que caso haja falhas pode se alterar toda a rede, mas não os componentes das extremidades.

2.6.2 MPLS

O *Multiprotocol Label Switching* (MPLS) é um mecanismo de transporte de dados padronizado pelo *Internet Enginering Task Force* (IETF) através da RFC 3031. O MPLS tem como objetivo solucionar problemas diversos na rede de computadores como velocidade, criação de *Virtual Private Networks* (VPN), qualidade de serviço (QoS) e engenharia de tráfego.

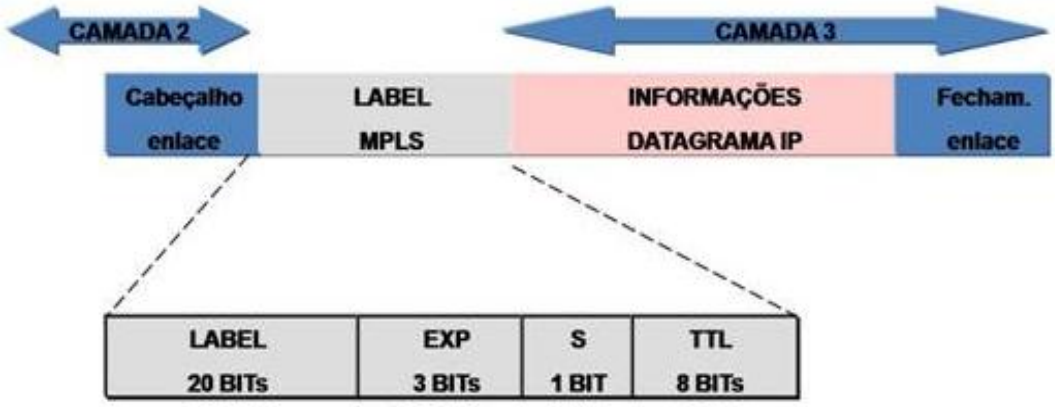


Figura 9 – Descrição do rótulo adicionado pelo protocolo MPLS (Afonso, 2011).

Basicamente, MPLS é uma tecnologia que consiste em adicionar informação ao pacote através de um rótulo, assim todo o transporte desse pacote através do *backbone* passa a ser feito baseado nas informações contidas nesse rótulo.

2.6.3 *Metro Ethernet*

O *Metro Ethernet* é o conceito de utilizar redes *Ethernet* em áreas Metropolitanas e geograficamente distribuídas, é regulado pela organização sem fins lucrativos *Metro Ethernet Forum*. A *Ethernet* se solidificou no mercado por ser simples e flexível, tornando-se uma rede confiável tanto para implantar quanto para sua manutenção. Esses serviços são fornecidos por uma interface padrão altamente conhecida ajudando tanto o usuário da rede quanto gerentes e gestores. A produção de equipamentos em massa e incentivos operacionais diminuem cada vez mais os custos da implantação do serviço *Ethernet*.

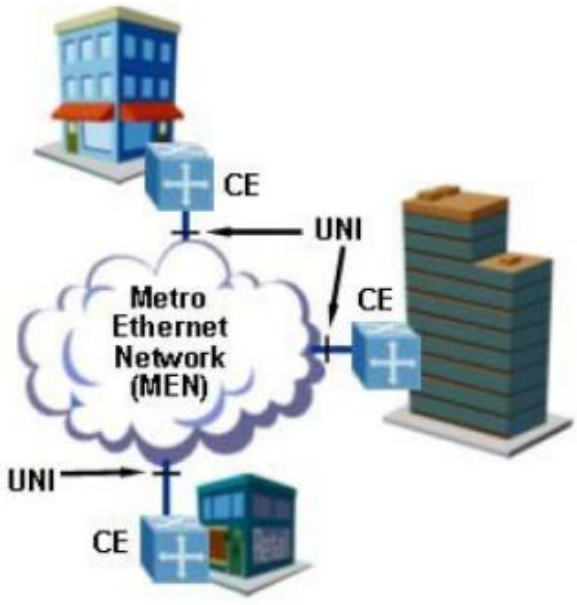


Figura 10 – Arquitetura básica *Metro Ethernet* (FRAULOB E PIACENTINI, 2006).

No *Metro Ethernet* o Cliente ou *Costumer Equipment* (CE) é conectado à *Metro Ethernet Network* (MEN) por meio de uma Interface de Rede do Usuário, *User-Network Interface* (UNI). Ocorrendo por uma interface *Ethernet* comum.

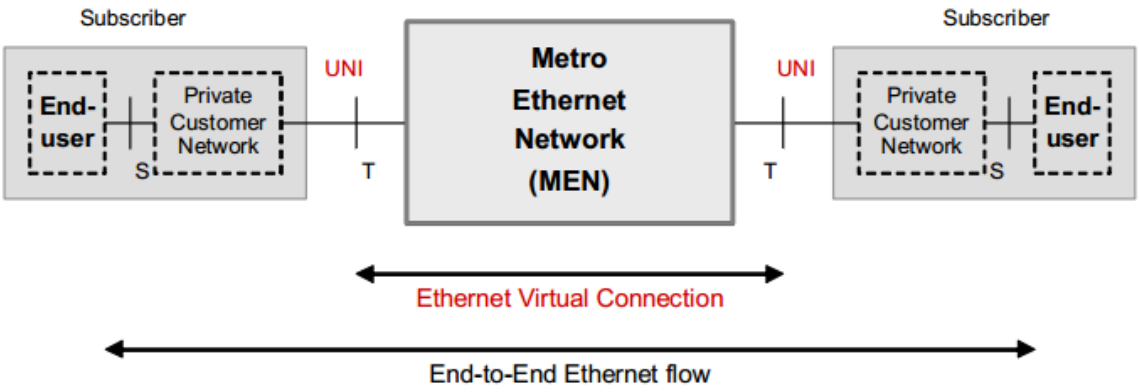


Figura 11 – Modelo de Referência da Arquitetura *Metro Ethernet* (FRAULOB E PIACENTINI, 2006).

O *Metro Ethernet Forum* apresenta um modelo básico para descrever os componentes internos e externos de uma rede *Metro Ethernet*, como podemos ver na Figura (11). Descrevendo suas interações através da interface e pontos de referência.

3 SEGURANÇA DA INFORMAÇÃO E REDISTRIBUIÇÃO DE ROTAS

Este capítulo aborda os principais problemas encontrados em conexões entre protocolos diferentes de uma maneira isolada, levantando suas principais características e causas.

3.1 ASPECTOS GERAIS

A evolução tecnológica aumentou a abrangência das redes de comunicações de dados elevando seu desempenho e as taxas de transmissão. Algumas das vantagens proporcionadas por estas tecnologias presentes nas redes de comunicações, assim como o seu crescimento, são garantidas em parte, pelos processos de troca de informações de roteamento realizados pelos protocolos de roteamento, ou seja, pela troca de informações que permitem os nós das redes, os roteadores, alcancem de maneira rápida e dinâmica os destinos necessários para permitir que a comunicação entre redes diferentes possam ocorrer.

Os protocolos de roteamento devem possuir rápida velocidade de convergência, tempo necessário para que, após uma mudança topológica, todos os roteadores da rede reorganizem as suas tabelas de roteamento com todos os destinos possíveis para nova convergência da rede e mecanismos para torna-los escaláveis, para que o crescimento da rede não prejudique efetivamente a velocidade de convergência ou sobrecarregue de maneira gerencial e técnica a rede com controles excessivos.

Alguns dos pontos críticos em relação à segurança e ao desempenho de uma rede de comunicação estão relacionadas ao controle e estabilidade das informações de roteamento. Por exemplo, uma rede que possui servidores com dados restritos, deve garantir que rotas de comunicação estejam sempre ativas e estáveis entre os servidores e as áreas que possuem autorização de acesso, já as áreas que não possuem autorização, não devem ter o conhecimento de tais rotas de comunicação para os servidores. Planejar os aspectos envolvidos no processo e entender como estas informações de roteamento devem ser originadas, propagadas e atualizadas na rede, assim como determinar como e para quem elas devem ser transmitidas, agregam segurança, desempenho e estabilidade a comunicação.

Projetos de redes de comunicações, principalmente projetos que envolvam alterações, fusões ou operações no mesmo ambiente de protocolos de roteamento heterogêneos, devem prezar pela segurança e estabilidade das rotas de rede, que dependendo do protocolo ou dos protocolos de roteamento utilizados em conjuntos, podem apresentar comportamentos diferentes do esperado pela simples mudança de arquitetura ou de tecnologia de acesso utilizada pela rede, provocando falhas e instabilidades que comprometem a comunicação.

3.2 RELAÇÃO DE ADJACÊNCIA

A troca de informações sobre como alcançar determinada rede de comunicação, é fundamental para que um roteador possua informações suficientes para transmitir um pacote de dados destinados a redes as quais ele não possui uma conexão ou uma ação explicita para o pacote. Isto evita que o pacote seja descartado pelo roteador, impossibilitando a comunicação entre usuários localizados em redes distintas.

Para realizar esta troca de informações, protocolos de roteamento sofisticados do tipo *link-state* e *distance-vector*, utilizam um mecanismo de estados de vizinhança, onde o estado mais elevado é designado como relação de adjacência. Ao qual, a relação é estabelecida com a análise de vários parâmetros que garantem que a troca de informações de roteamento possa, e principalmente, deva ser estabelecida entre dois roteadores conectados a mesma rede.

Esta troca de informações de roteamento é realizada pela troca de informações de rotas de rede, entre roteadores que executam o protocolo de roteamento EIGRP e pela troca de informações de topologias de rede, entre roteadores que executam o protocolo OSPF. O processo tem inicio com a validação de parâmetros necessários para estabelecer os estados de vizinhança entre os roteadores conectados a mesma rede. E se for necessário e possível, formar a relação de adjacência, que é o estado onde ocorre a troca efetiva de informações sobre a rede. O resultado final da troca de informações de roteamento é a construção da tabela de roteamento com as melhores rotas para cada rede.

3.2.1 Adjacência EIGRP

Por padrão o EIGRP envia pacotes *Hello* para o endereço reservado de *multicast* 224.0.0.10 para estabelecer o estado de vizinhança entre os roteadores diretamente conectados. Este pacote contém alguns parâmetros que são verificados e necessitam estar devidamente configurados em ambos os roteadores para que o estado de vizinhança possa ser estabelecido. Uma vez formado o estado de vizinhança entre roteadores EIGRP, eles estabelecem a relação de adjacência e trocam informações de rotas. No EIGRP, a formação do estado de vizinhança sempre resultará no estabelecimento da relação de adjacência. Assim, roteadores vizinhos sempre trocam informações de rotas.

Tabela 4 – Parâmetros EIGRP para vizinhança.

PARÂMETROS EIGRP	**ANALISADOS**
Conexão Ativa: receber e enviar pacotes	✓
Endereço primário na mesma sub-rede	✓
Interface não passiva	✓
Processo ASN (*Autonomous System Number*)	✓
Timers *Hello*/*Holdtime*	-
MTU	-
Métrica (*k-values*)	✓
RID único	-

Alguns parâmetros devem coincidir em ambos os roteadores EIGRP para que haja a formação do estado de vizinhança. Para estabelecer e monitorar esta relação, o EIGRP utiliza o pacote *Hello*, que contém parâmetros utilizados neste processo. Na Tabela (4), são identificados os parâmetros do pacote *Hello* que são analisados em cada roteador para formação do estado de vizinhança.

3.2.2 Adjacência OSPF

Assim como o protocolo EIGRP, o OSPF utiliza pacotes *Hello* para monitorar e estabelecer relações de vizinhança. Os pacotes *Hello* são enviados para o endereço reservado de *multicast* 224.0.0.5 e se todos os parâmetros necessários para a relação de vizinhança em ambos os roteadores OSPF forem aceitos, um estado de vizinhança pode ser formada.

A principal diferença em relação ao EIGRP é que no OSPF a formação de um estado de vizinhança entre roteadores não necessariamente culminará em uma relação de adjacência. O OSPF possui oito estados de vizinhança, onde a cada estado alcançado, ambos os roteadores verificam se devem

prosseguir para o próximo estado e assim por final estabelecer uma relação de adjacência, onde há a troca efetiva de informações da topologia entre os roteadores. Os estados são identificados na Figura (12), e as ações tomadas em cada estado são descritas em seguida (CISCO, 2010).

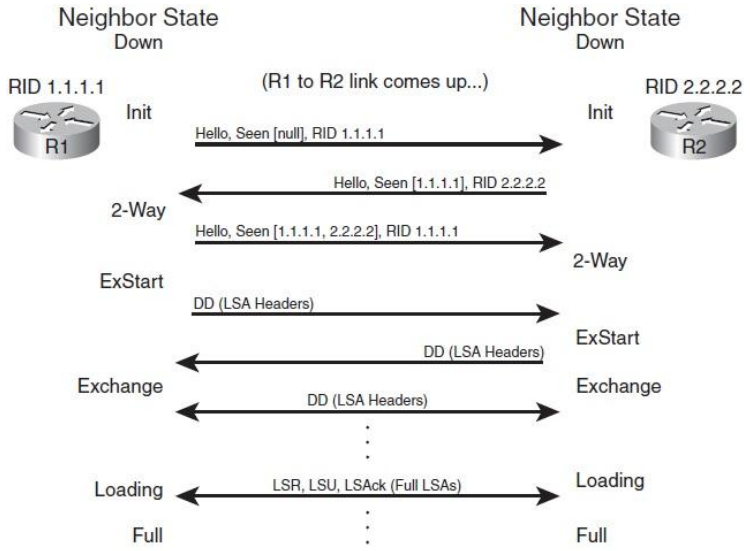


Figura 12 – Estados de Vizinhança OSPF (CISCO, 2010).

- *Down* – estado inicial para formação de vizinhança. Indica que não foram recebidas informações recentes de um vizinho.
- *Attempt* – estado válido somente para vizinhos conectados por meio de redes NBMA(*Non-Broadcast Multiple Access*). Indica que não foram recebidas informações recentes de um vizinho, mas um esforço mais concentrado deve ser realizado para contato com o vizinho. Ao invés de enviar pacotes *Hello* para endereço *multicast*, eles devem ser enviados para o endereço *unicast* do vizinho.
- *Init* – neste estado um pacote *Hello* foi recebido de um vizinho, mas a comunicação bidirecional ainda não foi estabelecida. Os parâmetros do pacote *Hello* são analisados para a formação da comunicação bidirecional.
- *2WAY* – estado de comunicação bidirecional entre os vizinhos. Alcançado quando um roteador recebe um pacote *Hello* listando seu próprio RID no campo *seen*. É o estado mais avançado antes de iniciar a relação de adjacência e estável, quando a relação de adjacência não deve ser estabelecida.
- *ExStart* – primeiro estado para a formação da relação de adjacência entre os vizinhos. São negociados os parâmetros de *DataBase Description* (DD), como o número sequencial inicial para troca de DD e qual dos roteadores terá a função de *Master*.
- *Exchange* – com a relação *Master/Slave* decidida, neste estado os roteadores descrevem toda a sua LSDB com a troca de pacotes DD para identificarem diferenças nas bases de dados.
- *Loading* – neste estado acontece a troca efetiva de informações da topologia com o envio de pacotes LSR, LSU, LSAck com informações completas dos LSA mais recentes que foram descobertos no estado anterior.
- *Full* – Neste estado, os roteadores estabeleceram uma relação completa de adjacência. A topologia OSPF foi totalmente trocada e ambos os roteadores possuem as mesmas informações na LSDB.

Tabela 5 – Parâmetros OSPF para vizinhança.

PARÂMETROS OSPF	ANALISADOS
Conexão Ativa: receber e enviar pacotes	✓
Endereço primário na mesma sub-rede	✓
Interface não passiva	✓
Processo OSPF	-
Timers Hello/Dead	✓
MTU	✓
Área OSPF	✓
RID único	✓

Os parâmetros analisados para iniciar a formação dos estados de vizinhanças são descritos na Tabela (5).

3.3 REDISTRIBUIÇÃO DE ROTAS

Grande parte das corporações utilizam em suas redes de comunicação um único protocolo de roteamento IGP para garantir maior controle e estabilidade da rede. No entanto, em alguns casos, como em fusões de grandes corporações e de empresas ISPs, quando estas utilizam protocolos IGPs diferentes, é necessário que as informações originadas em dado protocolo de roteamento sejam transferidas para outros protocolos de roteamento.

Isto é realizado para minimizar os riscos de uma migração completa de um IGP para outro, economizando tempo, o qual seria necessário para configurar múltiplos nós da rede, evitando falhas de operações, que poderiam deixar pontos da rede sem comunicação efetiva, isolando-os e permitindo continuidade da entrega de serviços e da comunicação.

A redistribuição de rotas permite que roteadores sejam conectados a domínios de roteamento diferentes e realizem a troca de rotas entre estes domínios. A redistribuição não provoca perturbação nos domínios existentes, permite que todos os destinos da nova rede sejam alcançados e que mudanças de topologia sejam reconhecidas automaticamente com uma rápida convergência da rede. A necessidade de utilizar redistribuição de rotas pode variar de acordo com a necessidade do negócio, além dos cenários já citados, estão incluídos casos de (CISCO, 2010):

- Fusão de redes quando diferentes IGP são utilizados;
- Fusão de redes quando o mesmo IGP é utilizado;
- Momentaneamente a corporação precisa utilizar múltiplos protocolos de roteamento;
- Divisão da corporação em diferentes setores por motivos de controle de segurança ou políticas;
- Conexão temporária ou permanente entre parceiros de negócios ou pesquisas;
- Interoperabilidade entre múltiplos fabricantes de equipamentos;
- Entre IGPs e BGP(*Border Gateway Protocol*) quando o BGP é utilizado entre corporações multinacionais;
- Redes WAN (MPLS).

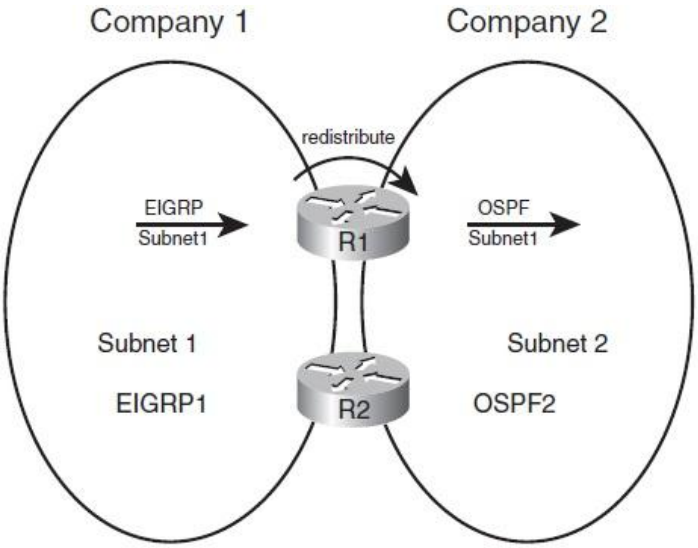


Figura 13 – Cenário de Redistribuição com Corporações Diferentes (CISCO, 2010).

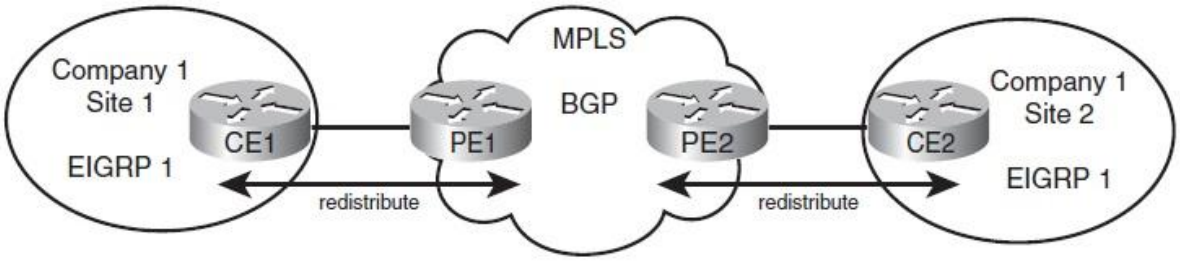


Figura 14 – Cenário de Redistribuição com mesma Corporação (CISCO, 2010).

Basicamente existem três requisitos necessários para realizar a redistribuição de rotas. O roteador precisa ter pelo menos um link ativo em cada domínio de roteamento, operar em cada um dos protocolos de roteamento utilizado em cada domínio e realizar uma espécie de tradução entre as informações que serão coletadas em um domínio de roteamento e injetadas em outro domínio. Esta espécie de tradução das informações entre os domínios de roteamento se faz necessária pela razão de diferentes protocolos de roteamento possuírem diferentes detalhes em relação á métricas, escolhas e propagação de rotas.

A tabela de topologia possui informações específicas de cada protocolo de roteamento, que são utilizadas para construção da tabela de roteamento. As informações contidas na tabela de topologia de dado protocolo de roteamento, podem não ser utilizadas e compreendidas pelos outros protocolos de roteamento. Por este motivo, o processo de redistribuição de rotas não interfere diretamente nas informações contidas na tabela de topologia entre os protocolos de roteamento. Ele utiliza uma fonte de informação que pode ser compreendida por ambos os protocolos, a tabela de roteamento.

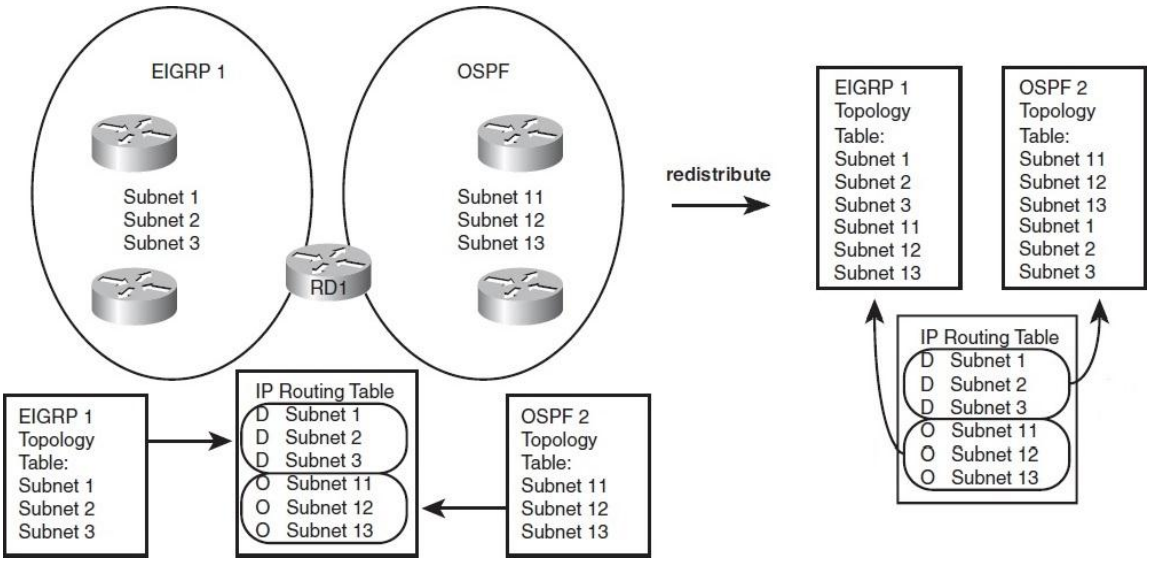


Figura 15 – Processo de Redistribuição (Modificado CISCO, 2010).

A tabela de roteamento é utilizada como fonte de informação para realizar a redistribuição de rotas, na qual, durante o processo de redistribuição, é analisada em busca das rotas inseridas por determinado protocolo de roteamento que devem ser redistribuídas em outro protocolo de roteamento. Na redistribuição, as rotas encontradas na tabela de roteamento que devem ser redistribuídas, são inseridas na tabela de topologia do protocolo de roteamento que irá realizar a redistribuição, a partir de então, as rotas são anunciadas no novo domínio. Alguns parâmetros devem ser ajustados de acordo com o protocolo que irá realizar a redistribuição para que a rota possa ser inserida corretamente na tabela de topologia e propagada no domínio de roteamento. (CISCO, 2010)

3.4 SEGURANÇA DA INFORMAÇÃO EM REDES

Uma rede é composta pelos mais diversos tipos de equipamentos de telecomunicações que se interconectam formando uma cadeia de dispositivos onde podem se comunicar entre si. O conceito de segurança da informação em redes se refere à proteção existente sobre a rede de uma determinada empresa ou pessoa. Ou seja, refere-se à proteção da rede pessoal ou coorporativa contra roubo ou uso inapropriado de informações confidenciais, contra ataques mal intencionados de vírus e *worms*, entre outros tipos de ataques. Para que a segurança de uma rede seja eficaz é necessário não só o uso de um método, mas sim o uso de um conjunto de medidas. Para que caso uma solução não cumpra o objetivo ainda possa esperar um resultado satisfatório das outras medidas implantadas, mantendo a rede protegida das mais variadas ameaças. A segurança da rede além de proteger contra ameaças internas e externas garante também a privacidade de toda a comunicação dessa rede. As ameaças a uma rede são as mais diversas, é necessário que a rede seja gerenciada e guiada para que possa manter protegidas as aplicações que a utilizam e dados que por ela trafeguem.

Para um levantamento e possível implantação de uma politica de gerencia de segurança em uma rede é necessária uma análise de todo tipo de exposição que a rede possa estar sofrendo para possíveis ameaças, levando em consideração da infraestrutura física até interfaces de comunicação, analisando todos os tipos de possíveis rotas que a informação possa vir a passar, e possíveis interfaces que possam ter acesso a essas informações, sejam elas passivas ou ativas.

Os tipos de ataques que visão ter acesso a informações em uma rede são os mais diversos, são ameaças que exploram vulnerabilidades na rede, a maioria dessas ameaças podem ser evitadas com politicas de segurança e de uso de serviços de rede, em que se é atribuído uma divisão de responsabilidades e deveres para os diversos usuários da rede. Para se obter uma política de segurança eficiente é necessário todo um levantamento das características da rede e seus diversos tipos de usuários e principalmente as características do tipo de informação que irá trafegar nessa rede.

3.5 INDENTIFICAÇÃO DE RISCOS EM FUSÃO DE REDES HETEROGENEAS

3.5.1 Captura de Informações Indevidas

A *Ethernet* foi projetada para o compartilhamento do meio de transmissão e assim os dispositivos presentes na mesma rede podem ler os pacotes que trafegam ali, mas acabam descartando esses pacotes quando não são os dispositivos de destino desses. Os *Sniffers* são programas ou dispositivos com o objetivo de interceptar pacotes na rede e analisar seu tráfego para análises e diagnósticos de desempenho de dispositivos de rede, atualmente usado de maneira maliciosa, para captura ilícita de pacotes destinados a outros dispositivos, onde muitas vezes podem conter informações sigilosas, como relatórios ou senhas. Os *Sniffers* são passivos, apenas capturando os pacotes que passam pelo dispositivo, o que torna muito trabalhoso sua descoberta.

Cada componente em uma rede *Ethernet* possui um endereço físico MAC (*Media Acess Control*), armazenado na placa de rede do próprio dispositivo, esse endereço será usado pelo protocolo *Ethernet* para envios de pacotes para esse dispositivo, que nesse caso normalmente só receberia pacotes destinados a seu endereço MAC, pacotes que não tenham o MAC correspondente do dispositivo são descartados. Com o meio físico baseado em compartilhamento e com um *sniffer* há a possibilidade de configurar a interface para o não descarte desses pacotes. Dessa maneira monitorando e obtendo o tráfego dessa rede.

A utilização de *hubs* e *switch* nas redes facilita o uso de *sniffers* para captura de pacotes de maneira maliciosa. Os *hubs* transmitem para todos os dispositivos que estão conectados a ele, cabendo ao próprio dispositivo o descarte dos pacotes não endereçados a ele. Já o *switch* a segurança é maior, já que o mesmo faz um controle de tráfego analisando os endereços MACs de cada dispositivo ligado a uma de suas portas para melhor uso da banda disponível, para uma captura de pacotes maliciosos é necessário explorar falhas no switch, os dois métodos mais conhecidos são ARP *Spoofing* e MAC *Flooding*.

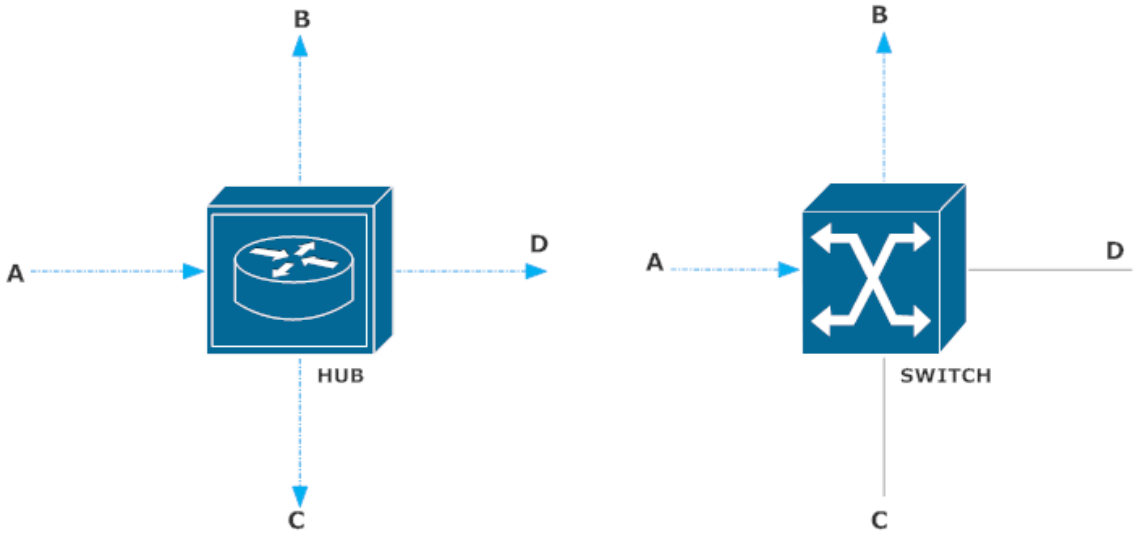


Figura 16 – Modelo comparativo de mensagens enviadas por Hub e Switch.

No ARP *Spoofing*, o nó malicioso irá gerar endereços MAC e IP falsos para se passar pela máquina alvo do ataque, esses endereços serão colocados em uma espécie de tabela de endereços do dispositivo que está enviando a mensagem, *cache* ARP (*Address Resolution Protocol*), onde os endereços IP serão convertido em endereços MAC. O protocolo ARP é *stateless*, isto é, pode receber respostas de endereço sem ter exigido de algum dispositivo, ARP *request* e *reply*, essa falha gera uma grande brecha para ataques já que o nó malicioso pode enviar uma mensagem ARP *reply* falsa para um dispositivo, redirecionando o fluxo de informação tendo acesso a todos os pacotes com destino a outro endereço MAC. Para não ser percebido o nó malicioso direciona os pacotes para o real destino.

Já no MAC *Flooding* o ataque é diretamente no *switch*, onde o nó malicioso investe no *switch*. O *switch* possui uma memória limitada onde o mesmo mantem os endereços MAC dos dispositivos conectados a ele para estabelecer circuitos virtuais. O ataque consiste em entulhar de endereços MACs falsos à memória do switch até alcançar o estado *fail open*, onde o mesmo trabalha como um *hub*, enviando os pacotes para todos os dispositivos conectados a ele, sem fazer controle através de endereços na memória.

3.5.2 Formação de Adjacências Indevidas

O processo de formação de adjacência é necessário para que roteadores que executam os protocolos de roteamento OSPF e EIGRP possam realizar a troca de informações referentes à topologia e as rotas da rede. Por padrão, este processo é realizado com o envio de pacotes *Hello* sem autenticação por comunicação *multicast* pelas interfaces referentes às redes anunciadas.

Este comportamento padrão possui algumas vulnerabilidades. A falta de autenticação permite que qualquer agente possa participar do processo e estabelecer uma relação de adjacência com roteadores legítimos da rede. E o envio de pacotes *Hello* por comunicação *multicast* pelas interfaces referentes às redes anunciadas, facilita a análise dos dados contidos nos pacotes *Hello* e a obtenção das informações sobre quais parâmetros estão sendo utilizados no processo de formação de adjacência.

Estas vulnerabilidades podem ser exploradas tendo como propósito o estabelecimento de uma relação de adjacência entre roteadores legítimos da rede e agentes não legítimos. Por meio desta relação de adjacência indevida, as informações de rotas e de topologia da rede podem ser coletadas pelo agente não legitimo, permitindo-o ter o conhecimento de parte ou de toda a arquitetura da rede. Além de permitir, por meio das informações coletadas da rede, que outras vulnerabilidades possam ser exploradas.

3.5.3 Inconsistência de Relação de Adjacências

As relações de adjacências entre os roteadores são fundamentais para que a rede possa manter um estado de convergência que permita a comunicação entre todos os pontos da rede. Em cenários de fusão de redes, quando há adição ou mudanças no enlace de comunicação, tecnologias utilizadas ou protocolos, o estado de convergência pode ser prejudicado devido ao não alinhamento dos parâmetros utilizados no processo de formação de adjacência. Alguns destes parâmetros são (Odom, 2010):

- Processo ASN EIGRP

  Quando roteadores possuem o número de processo ASN divergentes não é estabelecida a relação de adjacência.

- Métricas *k-values* EIGRP

  Quando roteadores utilizam diferentes pesos para as métricas utilizadas na composição do cálculo de melhor rota, ocorrem problemas quanto à escolha da melhor rota, assim não é estabelecida a relação de adjacência.

- Temporizadores *Hello* e *Dead* OSPF

  Quando roteadores utilizam diferentes valores para os temporizadores *Hello* e *Dead*, ocorrem problemas com o sincronismo do estado de operação do vizinho, assim não é estabelecida a relação de adjacência.

- Área OSPF

  Quando roteadores são conectados por interfaces pertencentes a áreas OSPF diferentes, a continuidade e hierarquia de áreas são desrespeitadas, assim não é estabelecida a relação de adjacência.

- *Router-ID* OSPF

  Quando roteadores vizinhos possuem o mesmo *Router-ID*, ocorrem problemas quanto a estabilidade na distribuição de informações de topologia, assim não é estabelecida a relação de adjacência.

- MTU

  Quando roteadores são configurados com MTU diferentes ou existe entre eles um salto de camada de enlace com MTU diferente, ocorrem problemas quanto à fragmentação e comunicação efetiva devido ao descarte de pacotes, assim a relação de adjacência é dita não efetiva ou a relação de adjacência torna-se instável, com o estabelecimento e queda da relação indefinidamente.

- Autenticação

  Quando roteadores vizinhos utilizam autenticação diferente não é estabelecida a relação de adjacência.

3.5.4 Injeção de Rotas e Desvio de Tráfego

A injeção de rotas em uma rede de comunicação é um tipo de ataque que se aproveita de vulnerabilidades na configuração de protocolos dinâmicos como o RIP e o OSPF. Esses protocolos tem entre suas funções a definição das tabelas de rotas da rede, endereços de destino e de origem das informações que ali trafegarem como também informar aos componentes da rede as melhores rotas para tráfego de informações. Nesse contexto o nó atacante tem como objetivo injetar rotas nas tabelas de roteamento dos integrantes da rede que está sendo instanciada por esses protocolos, abrindo portas para diversos tipos de ataques mais sérios. A Figura (17) demonstra um exemplo de quando um roteador C desvia o tráfego entre os roteadores A e B para interceptar informações trocadas entre esses componentes.

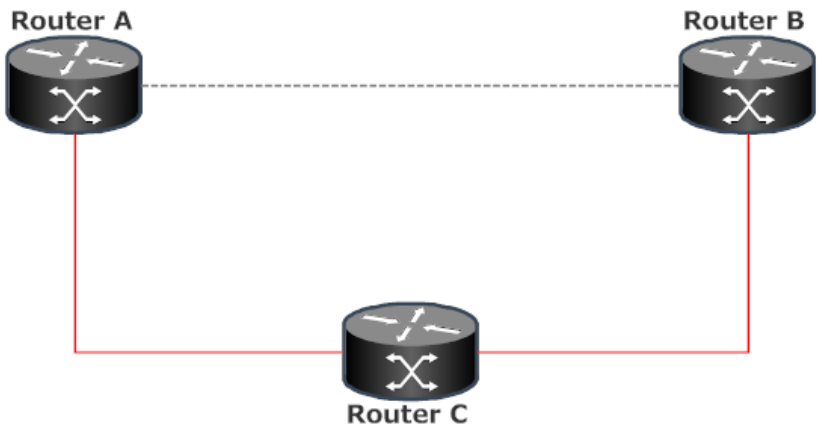


Figura 17 – Modelo de rede com rotas injetadas.

Com essas rotas injetadas nas tabelas de roteamento o nó atacante pode monitorar a rede desviando informações, atuando como um novo roteador nessa rede obtendo todo tipo de informação que passa nessa rede, de maneira que qualquer informação passará por esse agente antes de passar para o destino final.

O nó atacante pode também fazer com que a rede não forneça mais serviços algum, já que está repleta de rotas erradas ou inexistentes, prejudicando todos os componentes da rede em questão.

3.5.6 Áreas Descontínuas

Como foi visto anteriormente, o protocolo OSPF implementa uma hierarquia baseada em áreas. Sempre com uma área principal, *backbone* ou Área 0, onde todas as outras áreas devem estar ligadas e toda comunicação entre áreas passar por ela. Há casos onde isso não é possível sendo necessário o uso de um *Virtual Link* (VL) para ligar áreas ao *backbone* através de outra área *não-backbone*. O *virtual link* pode também ser usado para ligar partes de um *backbone* descontínuo, usando áreas *não-backbone* da mesma maneira. É necessário para a criação de um *virtual link* que a área *não-backbone*

usada, chamada também de área de trânsito, tenha toda a informação referente ao roteamento da rede, representado na Figura (18).

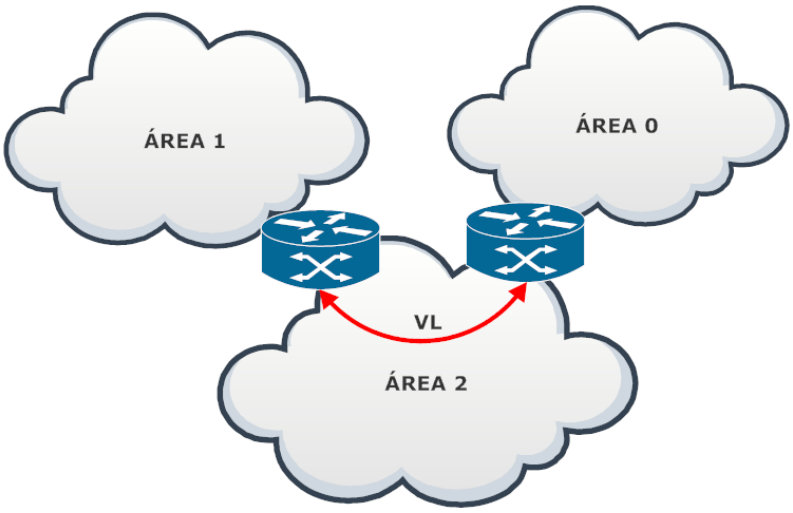


Figura 18 – Modelo de rede baseada em OSPF com Área descontinua.

Inicialmente o roteador da área desconexa com o *backbone* não tem conhecimento de como chegar à outra extremidade do *virtual link*. Na área de trânsito é necessário um envio em massa dos LSAs (*link-state advertisements*) desse *virtual link* para todos os componentes, *flooding*, para que todos os roteadores por onde passará esse *virtual link* possam calcular o SPF (*shortest path first*) e assim saber como transmitir a informação entre o *backbone* e a área descontinua.

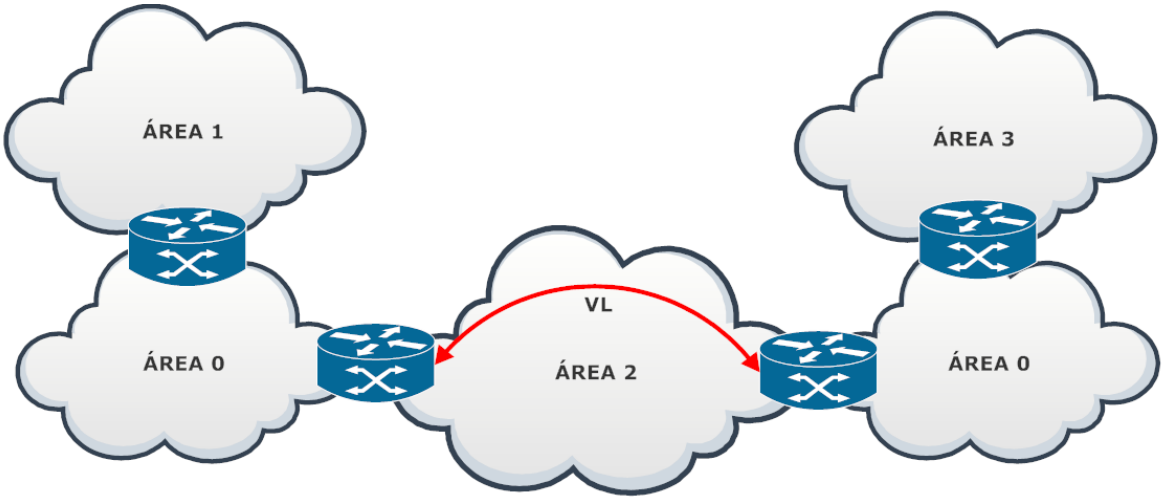


Figura 19 – Modelo de rede baseada em OSPF com um Backbone descontinuo.

A partir de agora, através do *virtual link* haverá a tentativa de criação da adjacência entre os roteadores das extremidades. Obtido a adjacência no v*irtual link*, o roteador da área desconexa é agora considerado um ABR (*Area Border Router*) por estar ligado através do *virtual link* ao *backbone* e com isso é criado um *summary* LSA nas demais áreas. Caso ocorra um erro no momento de programação do *virtual link* não serão criados os *summary* LSAs, já que o ABR não seria criado na área descontínua, representado na Figura (19).

4 ESTUDO DE CASO

Este capítulo apresenta um estudo de caso adaptado constituído por duas redes de comunicação de duas corporações distintas e da união entre estas, que será analisado com o intuito de evidenciar vulnerabilidades que possam comprometer o desempenho, estabilidade e segurança da rede de comunicação.

4.1 CONTEXTUALIZAÇÃO DO CENÁRIO DO ESTUDO DE CASO

A complexidade do domínio de roteamento tende a crescer de acordo com o aumento do número de ativos, tecnologias e serviços utilizados na rede de comunicação. Este crescimento pode ser considerado como um fator de risco para a rede de comunicação pela tendência de provocar o aumento de vulnerabilidades existentes ou do surgimento destas.

Com o objetivo de analisar as vulnerabilidades presentes nos diferentes domínios de roteamento e na operação conjunta destes domínios, o ambiente em questão é um estudo de caso adaptado de um cenário real envolvendo duas redes de comunicação de duas corporações, que chamaremos de corporação A e de corporação B. Inicialmente, a rede de cada corporação é analisada separadamente e posteriormente a analise é realizada para o cenário de fusão entre elas.

4.1.1 Arquitetura de Rede da Corporação A

A Figura (20) ilustra os principais pontos de parte da topologia de rede da corporação A analisada:

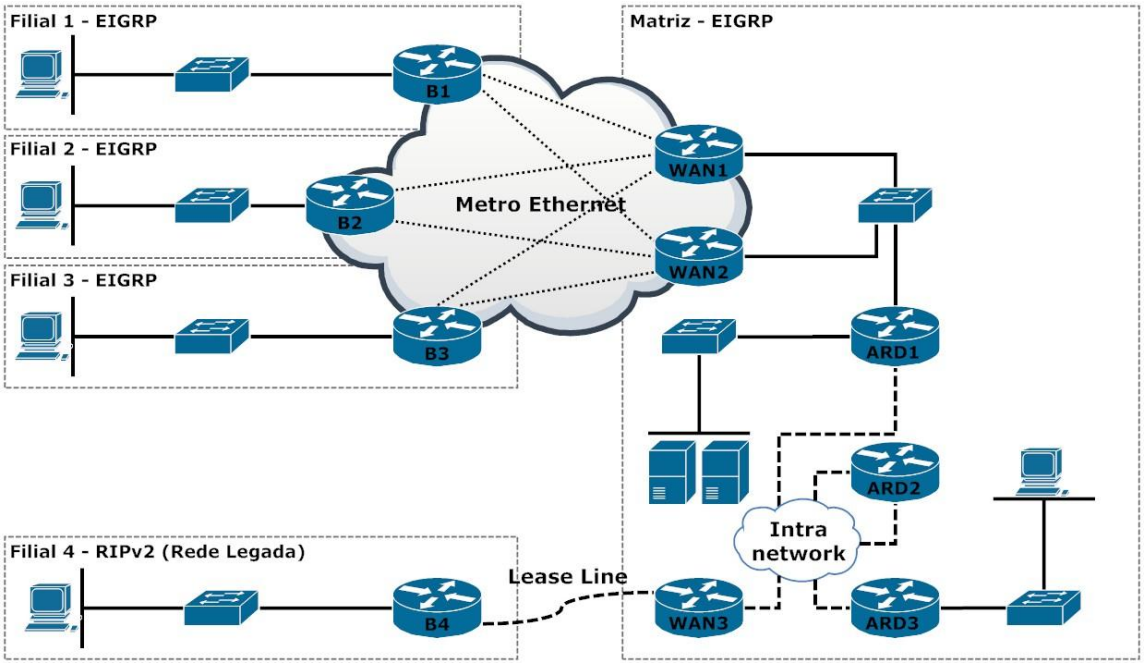


Figura 20 – Topologia de Rede Corporação A.

Esta topologia apresentada os seguintes elementos principais:

- Cisco *Router* 7200 *Series*;
- Cisco *Catalyst* 3750-X;

- Roteador legado RIP (B4);
- Servidor de Arquivos – Windows Server 2008 R2.
- Servidor Web – Linux Apache
- Estações de Trabalho.

A conexão WAN *Metro Ethernet* apresentada na topologia é utilizada para realizar a comunicação entre a matriz da corporação e três filiais, denominadas filial 1, 2 e 3. Esta conexão é realizada por meio de uma *User-Network Interface* (UNI) do provedor de serviço *Metro Ethernet* e estabelecida por um *Ethernet Virtual Connection* (EVC), podendo ser basicamente do tipo *point-to-point* ou *multipoint-to-multipoint*.

A UNI é uma interface do padrão *Ethernet*, que pode ser do padrão 10 Mbps, 100 Mbps, 1 Gbps ou 10 Gbps, a qual o roteador da corporação se conecta ao serviço WAN *Metro Ethernet* do provedor de serviço. A conexão entre o roteador da corporação e a UNI do provedor de serviço permite que da perspectiva do roteador da corporação, este considere que a conexão é realizada a uma rede *Ethernet* normal. Isso permite que as tecnologias de transporte utilizadas dentro da rede *Metro Ethernet* do provedor de serviço sejam totalmente transparentes para a corporação.

A comunicação entre duas ou mais UNIs, ou seja, entre dois ou mais roteadores da corporação é realizada por meio de um EVC. O EVC estabelece uma associação de duas ou mais UNIs possibilitando a transferência de dados entre elas e impedindo a transferência de dados entre UNIs que não são associadas ao mesmo EVC, o que adiciona privacidade e segurança ao serviço. Mas isso não impede que uma única UNI possa estar associada a mais de um EVC simultaneamente.

A conexão realizada por um EVC pode ser do tipo *point-to-point* ou *multipoint-to-multipoint*. Na conexão *point-to-point* existem apenas duas UNIs associadas ao EVC, ou seja, realiza a comunicação somente entre dois pontos. Na conexão *multipoint-to-multipoint* existem duas ou mais UNIs associadas ao EVC, a comunicação ocorre entre todas as UNIs associadas ao mesmo EVC.

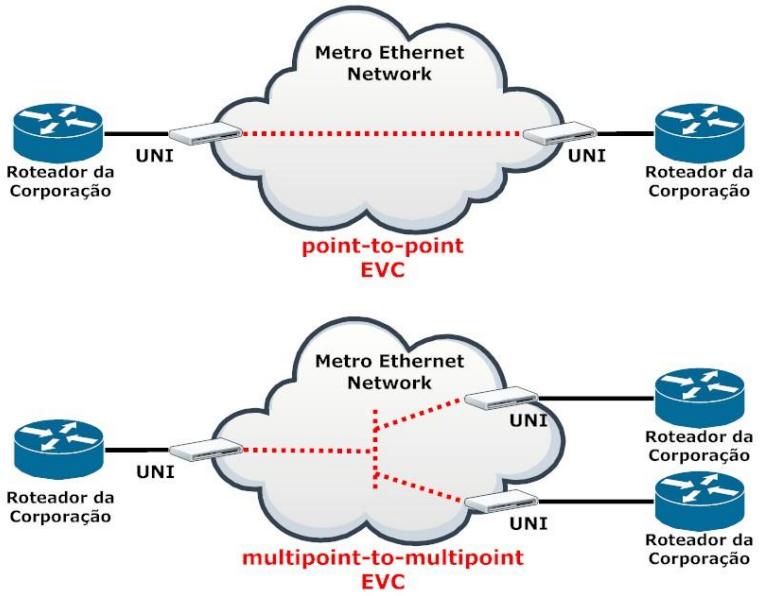


Figura 21 – *Ethernet Virtual Chanel point-to-point* e *multipoint-to-multipoint*.

O *Metro Ethernet Forum* define dois tipos de serviços *Metro Ethernet*: o *Ethernet Line* (E-Line) e o *Ethernet Lan* (E-Lan). O serviço E-Line estabelece uma conexão *point-to-point* EVC entre duas UNIs provendo comunicação ponto a ponto. Da perspectiva do roteador da corporação este serviço funciona como um circuito virtual, semelhante ao *permanent virtual circuits* (PVC) do *Frame Relay* e a *Lease lines*. O serviço E-LAN estabelece uma conexão *multipoint-to-multipoint* EVC entre duas ou mais UNIs provendo comunicação multiponto. Da perspectiva do roteador da corporação este serviço funciona como uma LAN. O tipo de tráfego que pode ser transmitido pela conexão WAN *Metro*

Ethernet vária de acordo com o provedor de serviço, determinando quais *frames* do usuário podem ser transmitidos pela rede *Metro Ethernet* (Santitoro, 2006).

Na topologia da corporação A apresentada, os roteadores que participam da conexão WAN *Metro Ethernet* utilizam o serviço E-Line estabelecendo uma conexão *point-to-point* EVC onde é permitida a transmissão de todos os tipos de *frames* de controle e tráfego *unicast*, *multicast* e *broadcast*. Os roteadores da matriz denominados WAN1 e WAN2 possuem uma conexão para cada um dos roteadores localizados nas filiais 1, 2 e 3, sendo eles denominados respectivamente por B1, B2 e B3. Todos os roteadores envolvidos na conexão executam o protocolo de roteamento EIGRP.

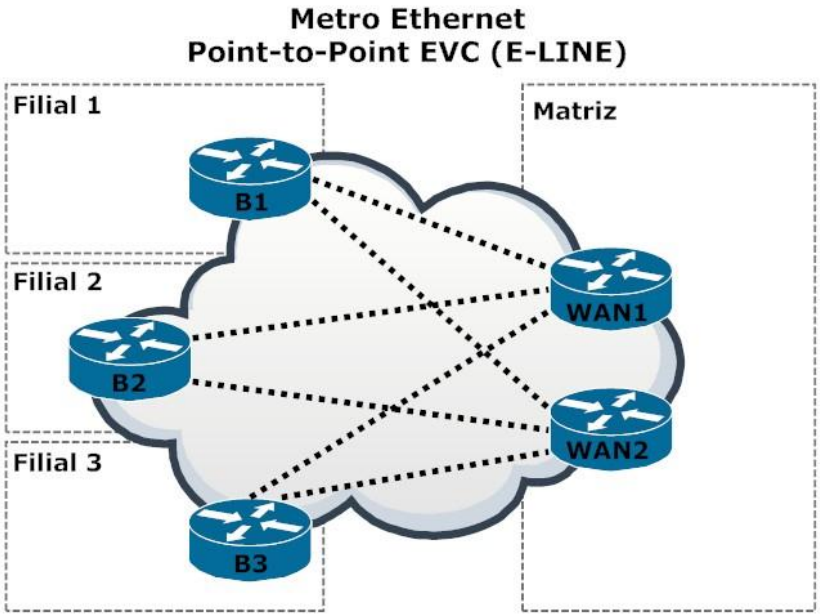


Figura 22 – Conexão WAN Metro *Ethernet* E-LINE.

A filial 4 é uma parte peculiar da corporação A, pois apresenta uma infraestrutura de sistemas legados que precisa estar operante devido a funcionalidades específicas que estes sistemas desempenham. A existência e manutenção de tal cenário ocorrem em parte pelo fato do custo/benefício de uma migração destes sistemas para tecnologias atuais não ser economicamente atraente para corporação.

A comunicação entre a matriz e esta filial é realizada através de uma conexão serial por meio de uma *lease line* que conecta o roteador da filial denominado B4, ao roteador da matriz denominado WAN3. Como a filial utiliza o protocolo de roteamento RIP versão 2 (RIPv2) e a matriz utiliza o protocolo de roteamento EIGRP, o roteador WAN3 utiliza em sua conexão com o roteador B4 o protocolo RIPv2, sendo responsável por redistribuir as rotas anunciadas pelo roteador B4 dentro do domínio EIGRP da matriz. Isso permite que qualquer *host* da corporação consiga se comunicar com os *hosts* da filial 4.

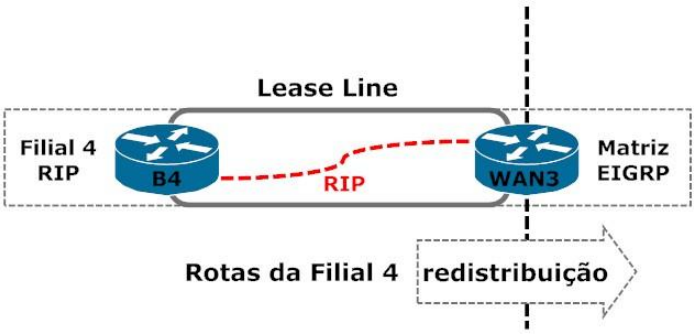


Figura 23 – Conexão WAN Matriz e Filial 4.

A matriz e as filiais 1, 2 e 3 utilizam em toda a sua extensão o protocolo de roteamento EIGRP, exceto o roteador da matriz WAN3, que como visto anteriormente, executa também o protocolo de roteamento RIPv2 em sua interface de conexão com a filial 4.

Na matriz, os roteadores WAN são responsáveis por realizarem a comunicação com as filias e os roteadores denominados ARD1, ARD2 e ARD3 são responsáveis pela comunicação interna envolvendo uma *intra network*. Conectado ao roteador ARD1 existe uma rede de servidores, onde um servidor de arquivos e um servidor *web* estão evidenciados na topologia. Conectado ao roteador ARD3 existe uma rede de desenvolvimento que se comunica com a rede de servidores. O roteador ARD2 realiza a intermediação de tráfego entre o roteador ARD1 e ARD3, agregando todo o fluxo de dados da comunicação entre a rede de desenvolvimento e a rede de servidor. A *intra network* presente entre o roteador ARD1, ARD2 e ARD3, representa a existência de uma topologia de rede interna.

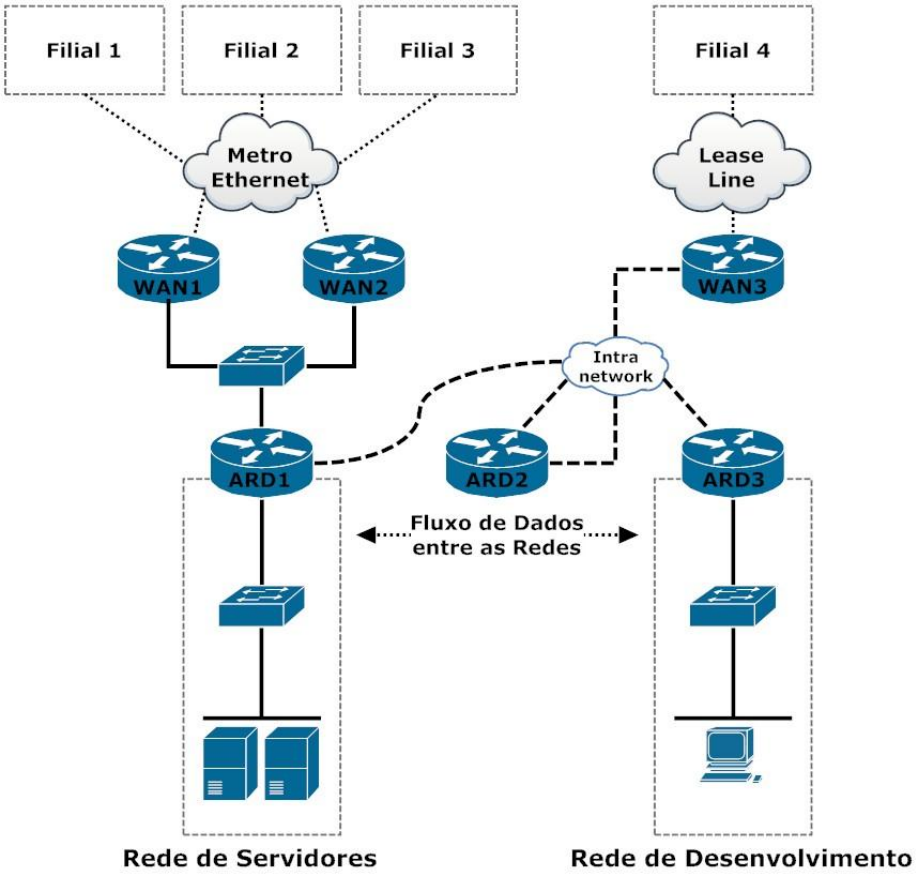


Figura 24 – Topologia de Rede da Matriz da Corporação A.

4.1.2 Arquitetura de Rede da Corporação B

A Figura (25) ilustra os principais pontos de parte da topologia de rede da corporação B analisada:

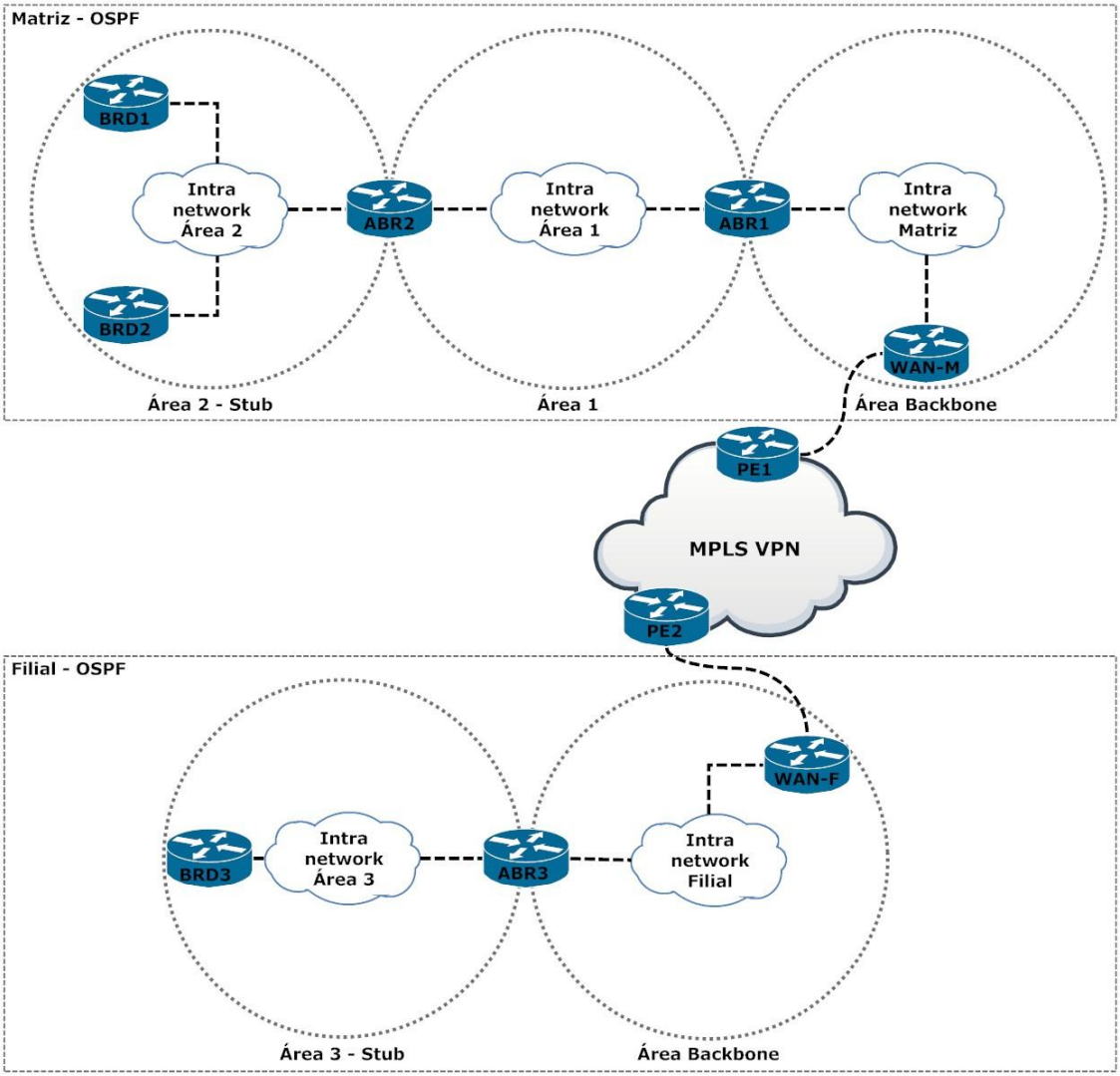


Figura 25 – Topologia de Rede Corporação B.

Esta topologia apresentada os seguintes elementos principais:

- Cisco *Router* 7200 *Series*;
- Áreas OSPF Matriz;
- Áreas OSPF Filial;
- *Intra Network* das Áreas OSPF Matriz;
- *Intra Network* das Áreas OSPF Filial;
- Conexão WAN MPLS VPN.

A conexão WAN MPLS VPN apresentada na topologia é utilizada para realizar a comunicação entre a matriz da corporação e sua filial. Esta conexão é realizada em dois pontos da topologia, o primeiro ponto está localizado entre o roteador da matriz denominado WAN-M e o roteador do provedor de serviço denominado PE1, o segundo ponto esta localizado entre o roteador da filial denominado WAN-F e o roteador do provedor de serviço denominado PE2.

Algumas peculiaridades em relação a estrutura do protocolo OSPF podem ocorrer quando uma conexão WAN MPLS VPN é utilizada para realizar a comunicação entre dois pontos remotos que devem pertencer ao mesmo domínio de roteamento OSPF. O funcionamento conjunto do OSPF e do MPLS VPN resulta em algumas alterações de designe para a rede OSPF, principalmente quanto a hierarquia de áreas OSPF e a troca de informações de topologia pelos diversos tipos de LSA.

A primeira mudança de designe está relacionada à formação de adjacência OSPF entre os roteadores da corporação que participam desta conexão WAN. Normalmente, quando são utilizadas tecnologias WAN como *Frame Relay, Metro Ethernet* ou *Lease Lines*, os roteadores da corporação que participam da conexão WAN estabelecem relações de adjacência entre si, não alterando a hierarquia de áreas OSPF ou a propagação das informações de LSA que alimentam a LSDB. Isso significa que nestas tecnologias, a partir de uma arquitetura WAN projetada adequadamente para realizar as conexões entre os roteadores da corporação, nenhuma consideração adicional precisa ser realizada para que o protocolo OSPF opere de acordo com o esperado, com os roteadores WAN da corporação estabelecendo relação de adjacência entre si e trocando informações de LSAs normalmente.

Quando a tecnologia utilizada para a conexão WAN é a MPLS VPN, este cenário envolvendo a formação de relações de adjacência e da troca de informações de LSAs sofrem algumas modificações. Isso ocorre principalmente pelo fato desta tecnologia oferecer, na prática, um serviço de camada de rede. Nesta camada da pilha de protocolos do modelo TCP/IP, o roteador do provedor de serviço, da perspectiva da rede da corporação, torna-se um salto de rede. O roteador do provedor de serviço não pode ser mais considerado transparente a rede da corporação, sendo considerado um nó da rede com papel ativo. Diferenciando, por exemplo, da tecnologia *Frame Relay* que oferece, na prática, um serviço de camada de enlace, onde o roteador do provedor de serviço pode ser considerado transparente a rede da corporação, não sendo considerado como um nó da rede, não interferindo assim no designe e funcionamento dos protocolos de camadas superiores. No MPLS VPN a relação de adjacência é estabelecida entre os roteadores da corporação e os roteadores do provedor de serviço, a troca de LSAs não é mais realizada diretamente entre os roteadores WAN da corporação.

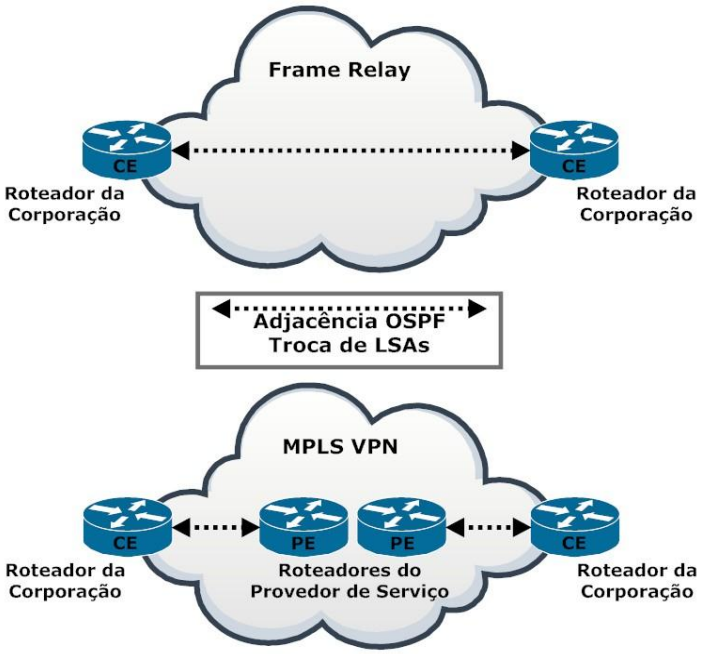


Figura 26 – Relação de Adjacência OSPF em conexões WAN.

Estabelecer a relação de adjacência entre o roteador da corporação e o roteador do provedor de serviço requer uma mudança em relação à definição e hierarquia de áreas OSPF, assim como a troca de informações de topologia entre os roteadores da corporação por LSAs.

Na arquitetura tradicional OSPF dois roteadores pertencentes à mesma área OSPF devem trocar informações de LSAs do tipo 1 ou 2. Como a relação de adjacência é estabelecida com o roteador do provedor de serviço, para que as informações de roteamento da corporação possam ser trocadas entre os seus roteadores WAN, é necessário que elas sejam propagadas dentro da nuvem MPLS VPN do provedor de serviço até alcançar o roteador do provedor que mantém uma relação de adjacência com o roteador da corporação e assim repassar as informações a este. Esta nuvem MPLS VPN utiliza um protocolo de roteamento diferente do utilizado pela corporação, normalmente são utilizados protocolos

de roteamento EGP, o que torna necessário a redistribuição de rotas entre o protocolo utilizado pela corporação e o protocolo utilizado pela nuvem MPLS VPN. Como consequência, o MPLS VPN não permite que os roteadores da corporação que realizam a conexão WAN sejam considerados como pertencentes à mesma área OSFP, pois neste cenário não ocorre a troca de informações de LSA do tipo 1 ou 2 entre eles.

No caso do EGP utilizado pela nuvem MPLS VPN ser o protocolo BGP, a redistribuição das informações de roteamento entre o protocolo OSPF e o BGP afeta a arquitetura tradicional OSPF. Dois pontos da corporação pertencentes ao mesmo domínio OSPF recebem as informações um do outro como informações externas, ou seja, esta redistribuição não preserva o tipo de LSA anunciado. Quando um roteador WAN da corporação anuncia um LSA do tipo 1 ou 2 para o roteador do provedor de serviço, este realiza a redistribuição da informação do LSA dentro da nuvem MPLS VPN, que ao alcançar o roteador do provedor de serviço que possui relação de adjacência com o outro roteador WAN da corporação, injeta estas informações como um LSA tipo 5 em áreas *backbone* e como um LSA tipo 7 em áreas NSSA(*Not-So-Stubby-Area*). Os roteadores da corporação em cada ponto da conexão WAN se enxergam em domínios de roteamento OSPF diferentes com a propagação das informações entre eles como rotas externas, o que provoca algumas ressalvas (CISCO, 2004):

- Rotas externas não podem ser sumarizadas;
- Rotas externas são propagadas por todas as áreas do domínio OSPF;
- Rotas externas podem usar diferentes tipos de métrica;
- Rotas internas são sempre preferidas sobre as rotas externas, independentemente de seus custos.

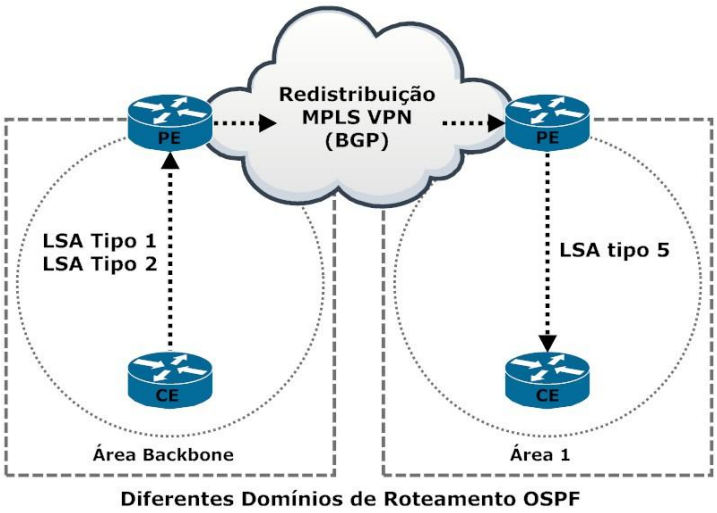


Figura 27 – Propagação de LSA com MPLS VPN utilizando BGP.

Na topologia da corporação B apresentada, o roteador da matriz denominado WAN-M e o roteador da filial denominado WAN-F participam da conexão WAN MPLS VPN. O roteador WAN-M estabelece uma conexão com o roteador do provedor de serviço denominado PE1 e o roteador WAN-F estabelece uma conexão com o roteador do provedor de serviço denominado PE2.

Os roteadores do provedor de serviço, PE1 e PE2, utilizam para sua comunicação interna o protocolo de roteamento MP-BGP para implementação de uma nova área chamada de *superbackbone*, que resolve em parte as alterações de designe de rede OSPF sofridas quando a nuvem MPLS VPN usa o protocolo BGP tradicional. Esta nova área é constituída pelos roteadores do provedor de serviço envolvidos, ou seja, pela nuvem MPLS VPN.

O MP-BGP utilizado entre os roteadores do provedor de serviço permite que os atributos presentes nos LSAs anunciados pelos roteadores WAN da corporação, para os roteadores do provedor de serviço, sejam mantidos quando forem redistribuídos dentro da nuvem MPLS VPN. Isso permite que a nova

área hierárquica, a *superbackbone*, que possui o maior nível hierárquico do ponto de vista do provedor de serviço, localizada no topo do designe de áreas, possa ser implementada de maneira transparente a corporação.

Esta área *superbackbone* permite que a corporação possa implementar diferentes designes de áreas OSPF. Permite implementar um designe de áreas *backbone* descontinuas. Onde cada área *backbone* descontinua da corporação, através da conexão com o roteador do provedor de serviço, é conecta a área *superbackbone* que realiza a comunicação entre estas áreas *backbone* descontinuas. E permite o oposto, que nenhuma área *backbone* precise ser implementada no designe de áreas OSPF pela corporação. Onde a área *superbackbone* atua como se fosse uma única área *backbone*, com todas as áreas não *backbone* da corporação conectas através dos roteadores do provedor de serviço a área *superbackbone*.

A implementação da área *superbackbone* tem como um dos pontos principais a nova interpretação que os roteadores WAN da corporação fazem dos roteadores do provedor de serviço ao qual estão conectados. Os roteadores WAN da corporação interpretam que estes roteadores do provedor de serviço são roteadores ABR, influenciando como os LSA são propagados entre os pontos da corporação pela conexão WAN.

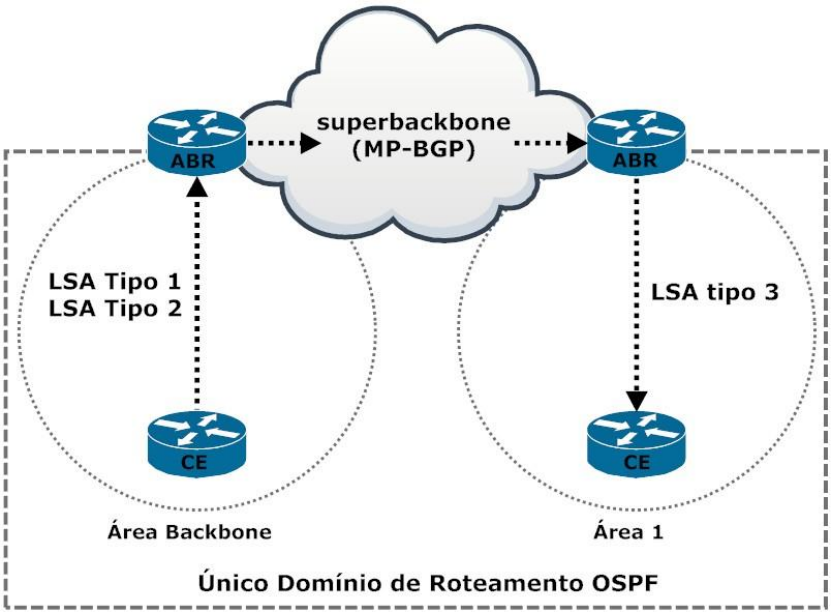


Figura 28 – Propagação de LSA com *Superbackbone* (MPLS VPN com MP-BGP).

Quando a conexão é realizada entre um roteador WAN da corporação que pertence a uma área *backbone*, ele considera que o roteador do provedor de serviço é um ABR que está conectado a uma área normal, não *backbone*. Se a conexão é realizada entre um roteador WAN da corporação que pertence a uma área não *backbone*, ele considera que o roteador do provedor de serviço é um ABR que está conectado a área *backbone*. O roteador WAN da corporação não tem conhecimento real do que está além do roteador do provedor de serviço. As informações propagadas na área *superbackbone* são injetadas pelos roteadores do provedor de serviço dentro das áreas em que os roteadores WAN da corporação realizam conexão com aqueles, como LSAs tipo 3.

A área *superbackbone* permite que localidades diferentes da corporação possam se comunicar pelo serviço WAN MPLS VPN mantendo um único domínio de roteamento OSPF. Evitando as instabilidades que podem ocorrer quando as localidades da corporação são consideradas como domínios de roteamento OSPF diferentes. Mas não muda o fato da relação de adjacência ser estabelecida entre os roteadores WAN da corporação e os roteadores PE do provedor de serviço WAN MPLS VPN.

Assim, a rede de comunicação da corporação B apresenta um único domínio de roteamento OSPF que abrange a matriz e sua filial. A matriz é constituída por três áreas OSPF: a área *backbone*; a área 1 e a

área 2. A Filial é constituída por duas áreas OSPF: a área *backbone* e a área 3. Cada área apresenta sua própria rede *intra network*, que representa a existência de uma topologia de rede interna da área.

As áreas 2 e 3, devido ao design de áreas OSPF implementado na corporação, são definidas como áreas *stub*. Onde os roteadores ABR2 e ABR3, são os responsáveis por suprir as rotas externas LSA tipo 5 que são propagadas por todo o domínio OSPF, dentro das áreas 2 e 3, respectivamente. Sendo também responsáveis em anunciar uma rota *default*, LSA tipo 3, dentro da área *stub* a qual cada um pertence. Como as áreas 2 e 3 possuem somente um caminho para alcançar as redes que são externas a sua área, ao defini-las como áreas *stub*, reduzimos o consumo de processamento e de memória com a redução de informações propagadas dentro da área.

Uma observação adicional referente à área 2, é a de que ela não está diretamente conectada a área *backbone* da matriz. O que implica o uso de um *virtual link* realizado entre o roteador ABR2 e o roteador ABR1 para suprir com os requisitos de designe de hierarquia de áreas OSPF, onde é determinado que todas as áreas devem ser conectadas a área *backbone*.

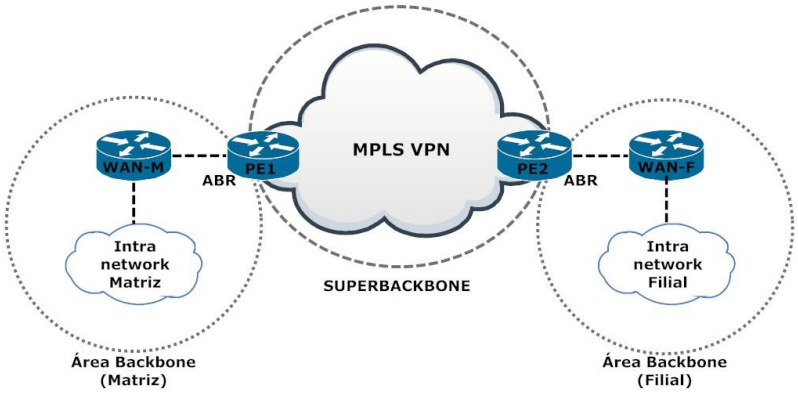


Figura 29 – *Superbackbone* Corporação B.

As áreas *backbones*, da matriz e da filial, são conectadas por meio do serviço WAN MPLS VPN. Que é realizado pela conexão do roteador da matriz denominado WAN-M com o roteador do provedor de serviço PE1 e pela conexão do roteador da filial denominado WAN-F com o roteador do provedor de serviço PE2, onde em cada conexão respectivamente é estabelecido uma relação de adjacência entre os roteadores WAN da corporação e os roteadores PE do provedor de serviço.

4.1.3 Arquitetura de Rede da Fusão da Corporação A e Corporação B

A Figura (30) ilustra os principais pontos relacionados à fusão entre as redes de comunicação da corporação A e da corporação B analisadas:

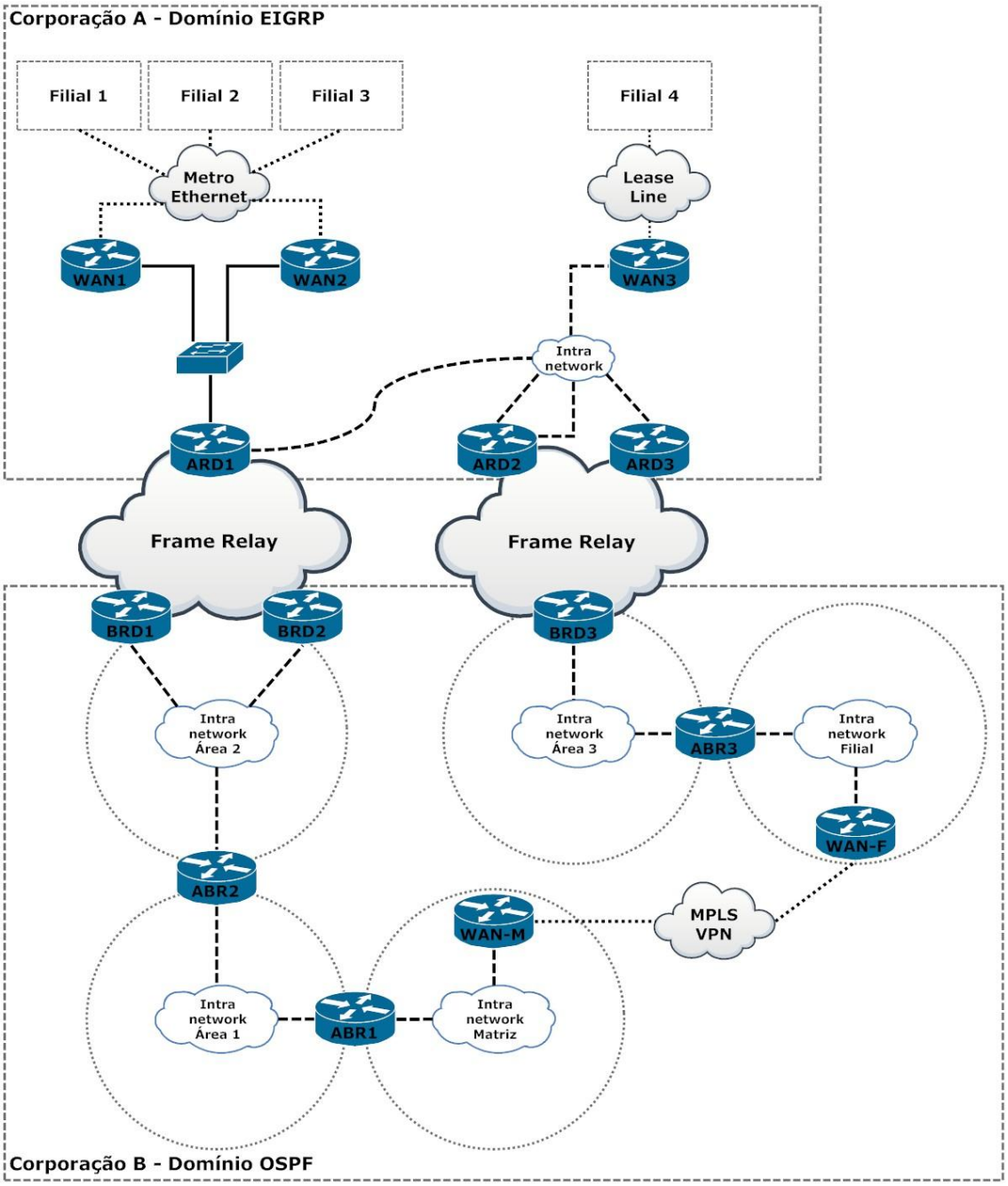


Figura 30 – Topologia de Rede da Fusão da Corporação A e Corporação B.

Esta topologia apresenta os seguintes elementos principais:

- Cisco *Router* 7200 *Series*;
- Conexão WAN *Frame Relay* para interligação da matriz da corporação A com a filial da corporação B;
- Conexão WAN *Frame Relay* para interligação da matriz da corporação A com a matriz da corporação B;

A fusão das redes de comunicação das corporações é realizada em dois pontos distintos para aumentar a disponibilidade da comunicação em caso de falha de algum dos pontos. Estes pontos utilizam para a comunicação entre as corporações o serviço WAN *Frame Relay*.

A conexão WAN *Frame Relay* apresentada na topologia pode ser do tipo *point-to-point* ou *poit-to-multipoint* e ser implementada em uma arquitetura *full mesh* ou *partial mesh* utilizando *permanent virtual circuits* (PVC) ou *switched virtual circuits* (SVC).

O PVC é um circuito virtual permanente entre dois nós em que o canal para esta comunicação está sempre formado. Quando se deseja transmitir um tráfego WAN ele é simplesmente enviado pelo canal. Embora as rotas entre os dois nós ligados por um PVC possam mudar, o canal utilizado pelos nós para a comunicação está sempre ativo e preparado para encaminhar o tráfego WAN, mesmo quando não existe tráfego de dados entre os nós. O SVC é um circuito virtual comutado entre dois nós em que o canal para a comunicação é formado sob demanda. Quando se deseja transmitir um tráfego WAN, é necessário antes do envio dos dados um processo de formação do canal, para então iniciar a comunicação.

Os tipos de conexões *poin-to-point* e *point-to-multipoint* podem utilizar tanto interfaces físicas do roteador como sub-interfaces, sendo utilizados para realizar a comunicação entre dois ou mais nós. A conexão *point-to-point* usa uma interface do roteador para estabelecer uma comunicação apenas entre dois nós, onde uma sub-rede é utilizada para o endereçamento dos nós. Isso significa que para cada conexão *point-to-point* é necessário utilizar uma interface do roteador e o endereçamento de uma sub-rede diferente para possibilitar a comunicação entre os nós. Este tipo de conexão trabalha semelhante a conexões realizadas por *lease lines*.

A conexão *poin-to-multipoint* usa uma interface do roteador para estabelecer uma comunicação entre mais de dois nós, onde apenas uma sub-rede é utilizada para o endereçamento dos nós. Esta conexão permite que apenas uma interface do roteador e uma sub-rede sejam necessárias para que mais de dois nós possam se comunicar.

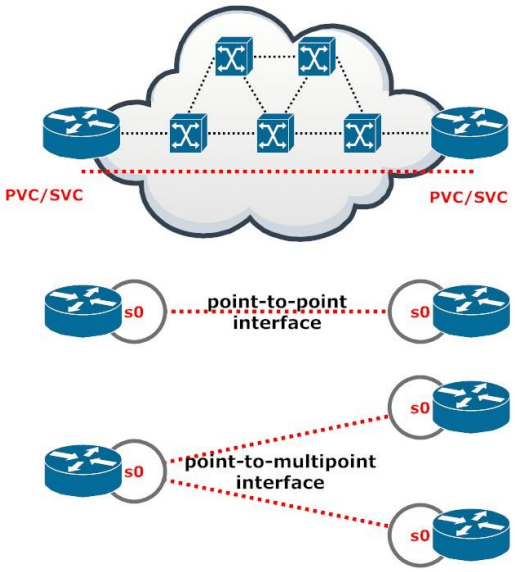


Figura 31 – Conexão Frame Relay.

A arquitetura *full mesh* consiste na existência de um canal entre cada nó participante da conexão WAN *Frame Relay*, já a arquitetura *partial mesh* não possui um canal entre cada nó participante.

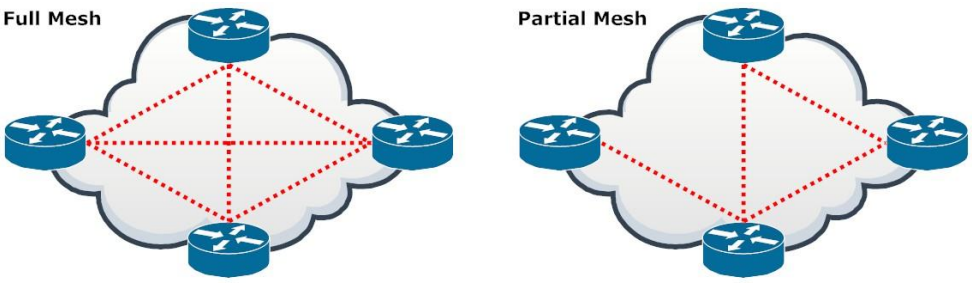


Figura 32 – Arquitetura *Full Mesh* e *Partial Mesh*.

Na topologia de fusão apresentada, os roteadores que participam das conexões WAN *Frame Relay* possuem conexão *point-to-multipoint* utilizando canais PVC em uma arquitetura *partial mesh*.

O primeiro ponto de fusão realiza a comunicação entre a matriz da corporação A, utilizando o roteador ARD1 e a matriz da corporação B, utilizando os roteadores BRD1 e BRD2, com o roteador ARD1 possuindo uma conexão, um PVC, para cada um dos roteadores BRD1 e BRD2. Estes roteadores utilizam o protocolo EIGRP na conexão WAN para se comunicarem tornando os roteadores BRD1 e BRD2 membros do domínio EIGRP da corporação A, com estes realizando a redistribuição bidirecional de rotas entre os domínios de roteamento.

O segundo ponto de fusão realiza a comunicação entre a matriz da corporação A, utilizando os roteadores ARD2 e ARD3 e a filial da corporação B, utilizando o roteador BRD3, com o roteador BRD3 possuindo uma conexão, um PVC, para cada um dos roteadores ARD2 e ARD3. Estes roteadores utilizam o protocolo OSPF na conexão WAN para se comunicarem, tornando os roteadores ARD2 e ARD3 membros do domínio OSPF da corporação B, com estes realizando a redistribuição bidirecional de rotas entre os domínios de roteamento.

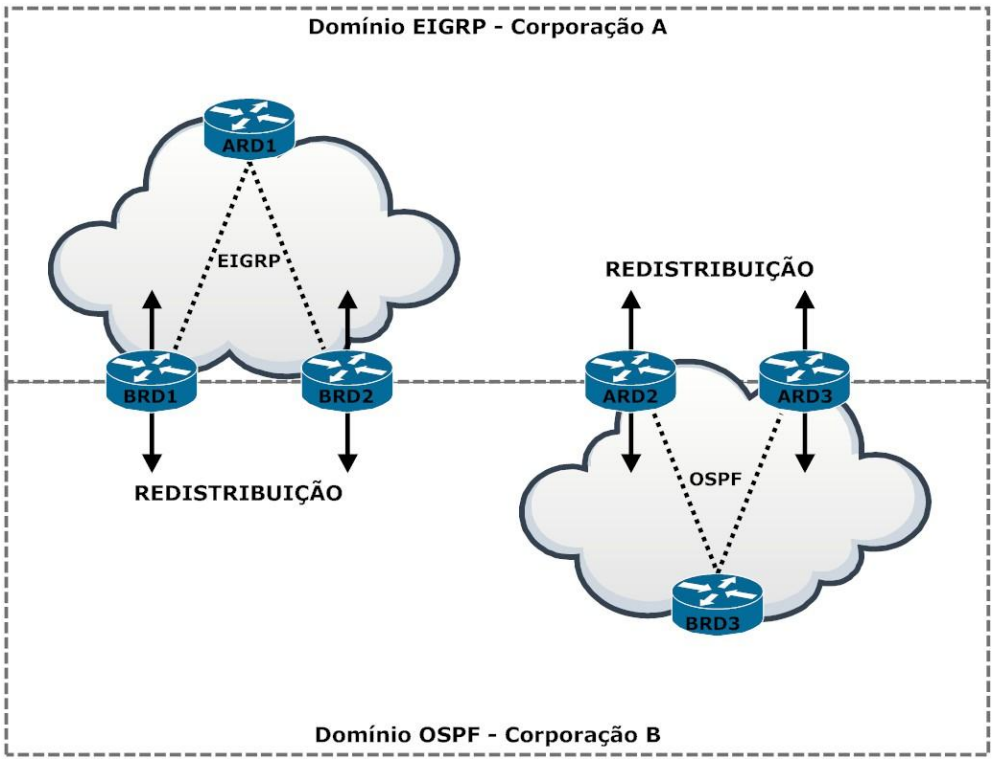


Figura 33 – Conexão WAN *Frame Relay Point-to-Multipoint* e Redistribuição de Rotas.

4.2 PONTOS DE VULNERABILIDADE ENCONTRADOS

As arquiteturas de redes de comunicação apresentadas da corporação A, da corporação B e da fusão entre elas, possuem alguns pontos importantes do ponto de vista de segurança e de estabilidade do domínio de roteamento. Alguns desses pontos principais são evidenciados nas Figuras (34), (35) e (36):

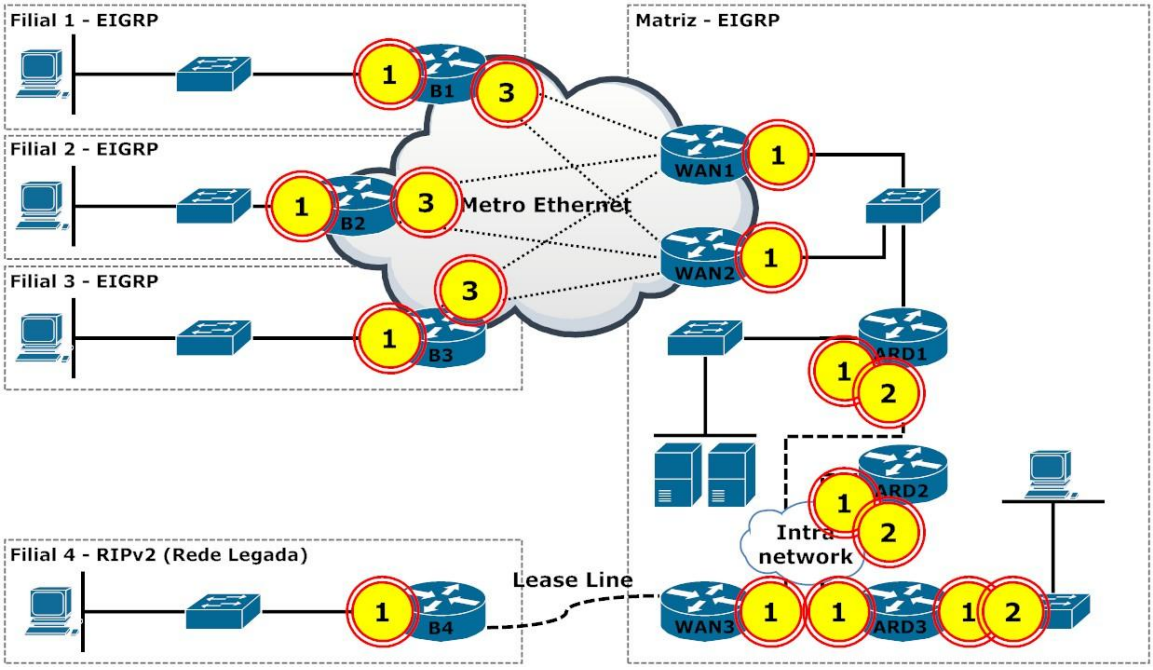


Figura 34 – Pontos de Vulnerabilidade da Topologia da Corporação A.

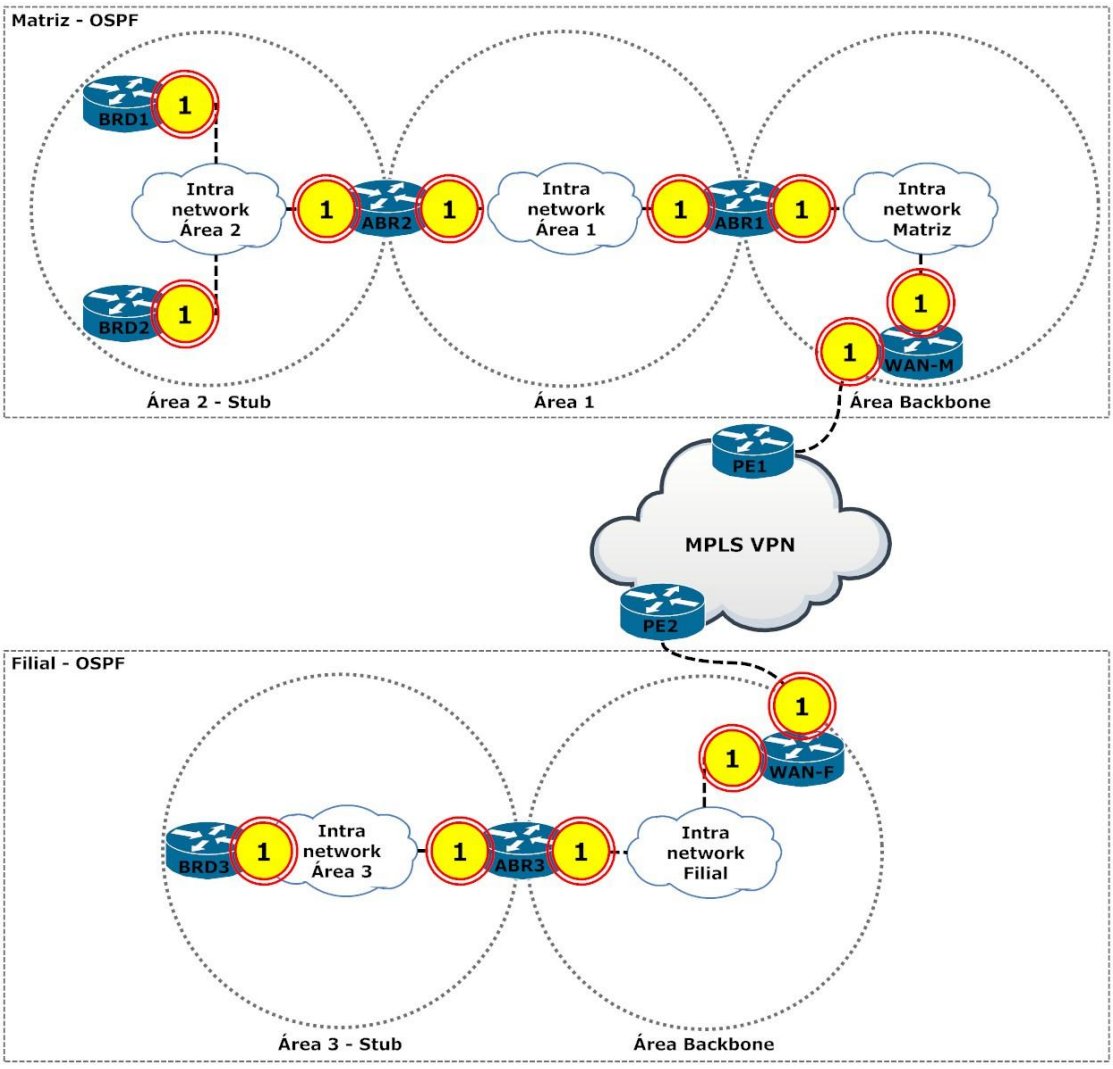


Figura 35 – Pontos de Risco da Topologia da Corporação B.

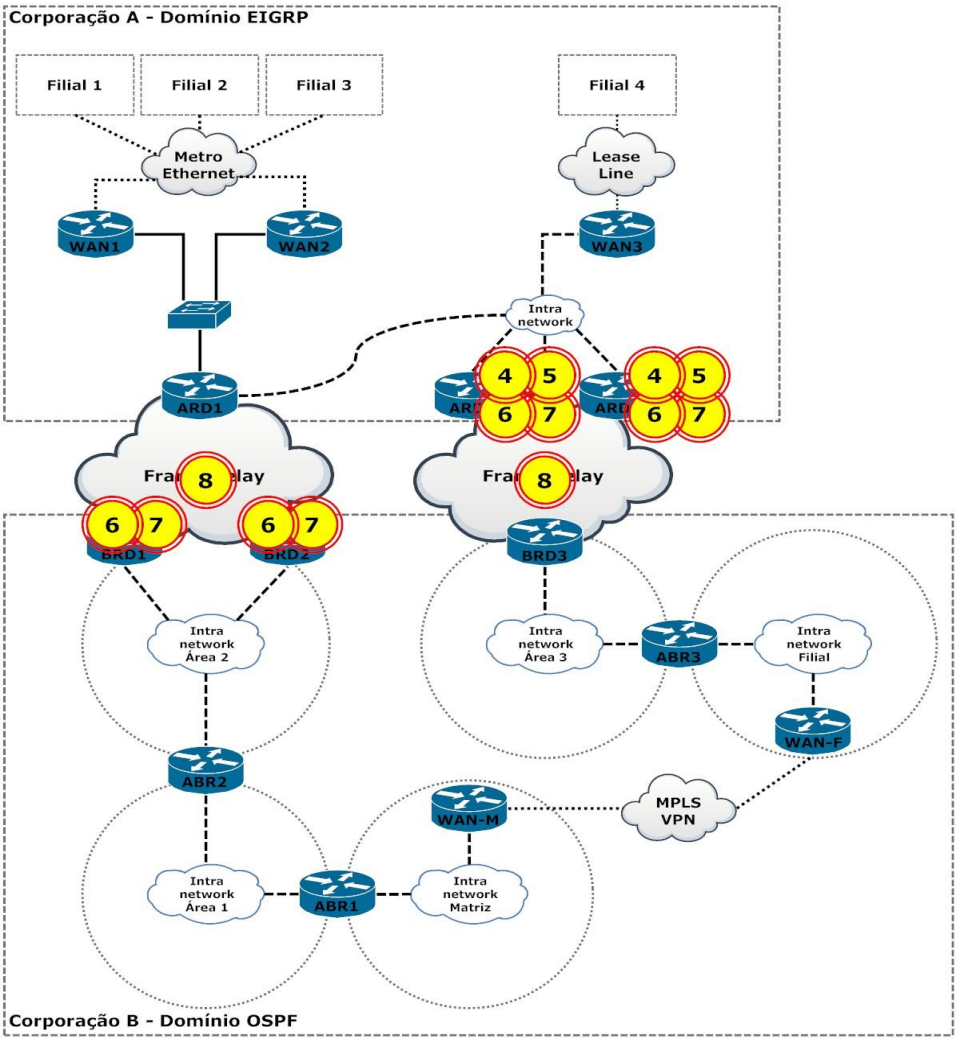


Figura 36 – Pontos de Risco da Fusão: Corporação A e Corporação B.

Os pontos destacados nas Figuras (34), (35) e (36), numerados de 1 a 8, representam pontos que apresentam algum tipo de vulnerabilidade para a rede de comunicação, seja por possuírem alguma característica que pode ser usada para realizar e/ou potencializar algum tipo de ataque ou por poderem provocar instabilidade de operação do domínio de roteamento, ambos prejudicando a comunicação na rede. Estes pontos destacados estão relacionados aos seguintes fatores:

1. Formação de Adjacência Indevida;
2. Desvio do Tráfego de Dados;
3. Saturação de Link;
4. Falha de Convergência de Rede;
5. Falha de Redistribuição de Rotas;
6. Loop na Redistribuição de Rotas;
7. Escolha não ótima de Melhor Rota na Redistribuição de Rotas;
8. Falha na Troca de Informações e Convergência de Rede por conexão WAN.

Embora na Figura (36), fusão das corporações, não esteja marcado os pontos 1 e 2, presentes nas Figuras (34) e (35), rede individual de cada corporação, como a fusão é o resultado da união das redes individuais, as vulnerabilidades são conservadas, ou seja, todos os pontos destacados nas Figuras (34) e (35), estão presentes também na topologia de fusão das corporações. A omissão destes pontos na Figura (36) foi realizada para destacar as vulnerabilidades pré-existentes de cada rede individualmente, das vulnerabilidades presentes apenas na fusão.

5 ANÁLISE DAS VULNERABILIDADES E RESULTADOS

Este capítulo apresenta a análise das vulnerabilidades levantadas nas arquiteturas de rede utilizadas no estudo de caso modificado e um conjunto de recomendações a fim de minimizar ou eliminar os riscos advindos destas vulnerabilidades.

5.1 ANÁLISE DAS VULNERABILIDADES ENCONTRADAS

A partir da identificação dos pontos de vulnerabilidades encontrados no capítulo anterior, podemos analisa-los de uma maneira mais aprofundada, no intuito de entender os riscos envolvidos nestes pontos e buscar ações ou práticas que possam minimizar ou eliminar estas ameaças.

5.1.1 Formação de Adjacência Indevida

Por padrão, a comunicação entre os roteadores que executam os protocolos de roteamento OSPF, EIGRP e RIP são realizadas sem autenticação com o envio de pacotes *Hello* em *multicast* pelas interfaces pertencentes às redes anunciadas no domínio de roteamento. Nas arquiteturas de rede apresentadas, o ponto identificado como 1, apresentam este comportamento padrão, representando uma vulnerabilidade para a rede de comunicação.

Nestes pontos não é possível garantir que haja uma formação de adjacência somente entre roteadores legítimos da rede. Um agente malicioso localizado em uma das redes em que o roteador está enviando pacotes *Hello* em comunicação *multicast*, pode coletar as informações contidas nestes pacotes *Hello* e obter os parâmetros necessários para estabelecer uma relação de adjacência com este roteador. A partir da formação desta relação, de acordo com a topologia das redes apresentadas, destacamos dois tipos de ameaças possíveis:

Captura de Informações Indevidas

> O agente malicioso pode capturar informações de rotas e de topologia das redes obtendo informação parcial ou total da arquitetura de rede e se utilizar destas informações para potencializar ou possibilitar outros tipos de ameaças.

Negação de Comunicação

> O agente malicioso pode passar ao roteador legitimo informações falsas sobre determinadas rotas. Estas informações ao serem propagadas dentro do domínio de roteamento, podem causar uma nova convergência de rede interrompendo a comunicação entre alguns pontos da rede e as redes referenciadas nas informações falsas propagadas. A informação falsa pode ser, por exemplo, uma rota para determinado destino com a melhor métrica dentro do domínio de roteamento, mas que não possui um caminho real para alcançar o destino.

5.1.2 Desvio do Tráfego de Dados

A vulnerabilidade explicada no item anteriormente pode possibilitar o surgimento de outra ameaça, o desvio de tráfego de dados. Esta ameaça esta relacionada à injeção de rotas maliciosas para alterar o caminho normal do tráfego de dados entre redes. Observamos que essa ameaça está presente na topologia de rede da corporação A. Um agente malicioso pode realizar o desvio de tráfego de dados entre a rede de servidores e a rede de desenvolvimento ao explora a vulnerabilidade do ponto 1 e injetar rotas maliciosas para modificar as rotas dos roteadores envolvidos na comunicação.

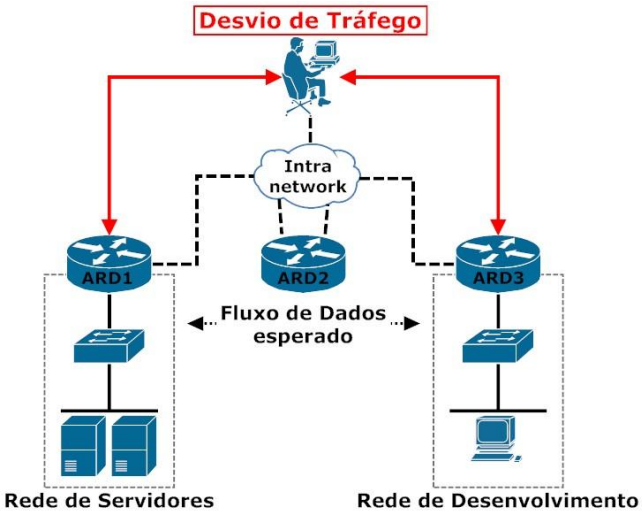


Figura 37 – Desvio de tráfego de dados entre a Rede de Servidores e a Rede de Desenvolvimento.

5.1.3 Saturação de Link

Os roteadores das filiais 1, 2 e 3 da corporação A, denominados B1, B2 e B3, estão conectados pela conexão WAN *Metro Ethernet* E-LINE aos roteadores WAN1 e WAN2 da matriz da corporação A. Ao analisarmos a topologia desta comunicação WAN, percebemos que existe um caminho possível para que estes roteadores WAN alcancem a matriz sem utilizar as suas próprias conexões diretas ao *switch* da matriz. Este caminho passa pela conexão de um dos roteadores WAN com um dos roteadores da Filial e depois segue deste para o outro roteador WAN. Esse caminho possível em determinadas situações de falha, pode acarretar na saturação do link de uma das filiais, impossibilitando a comunicação com a matriz. (Odom, 2010)

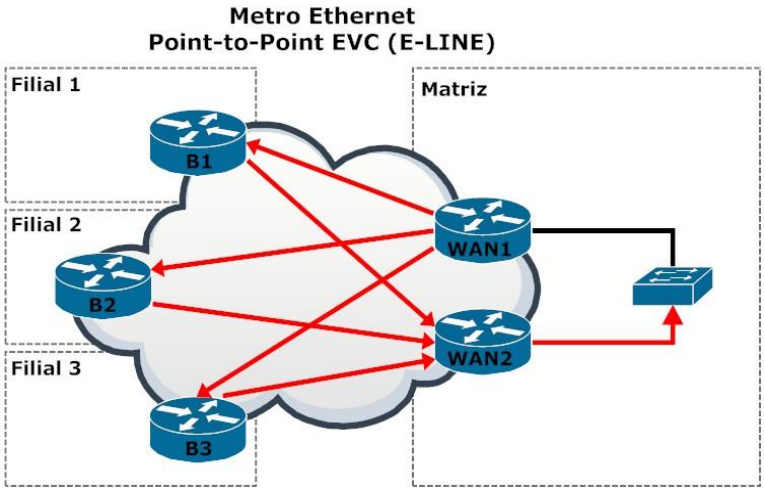


Figura 38 – Saturação de Link.

5.1.4 Falha de Convergência de Rede

Um domínio de roteamento OSPF requer que todos os roteadores participantes deste domínio tenham uma identificação única, o RID. Em casos de duplicação do RID, seja dentro da mesma área ou em áreas diferentes, o processo de convergência da rede pode apresentar um mau funcionamento. Como um LSA é identificado pelos campos *Type*, *Link State* ID e *Advertising Router*, este representado pelo RID do roteador, RIDs duplicados podem causar a flutuação de rotas na tabela de roteamento e de LSAs no banco de dados LSDB, além de impedirem que roteadores que possuam o mesmo RID troquem informações de topologia, resultando na falha de convergência de rede.

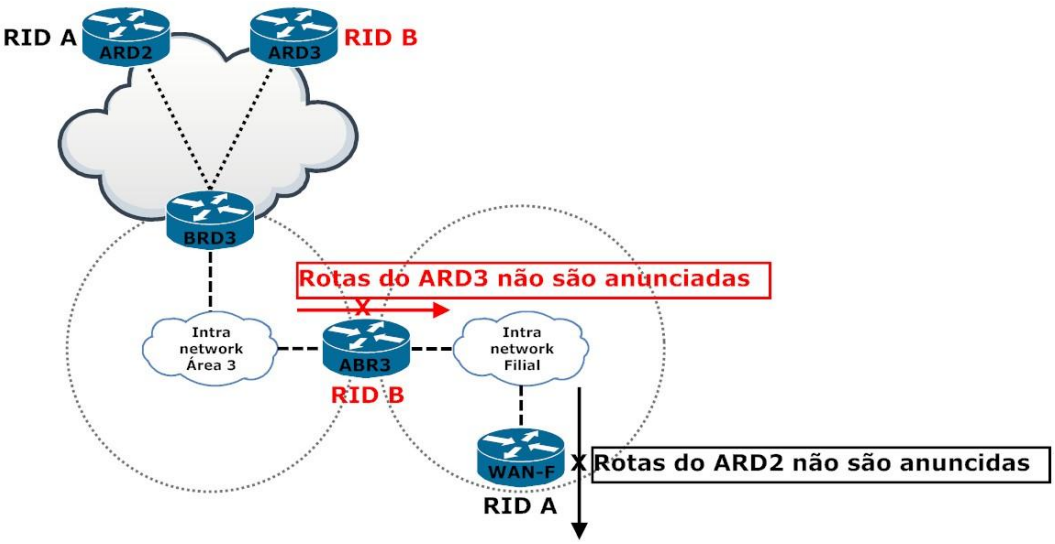


Figura 39 – Falha de Convergência por RIDs duplicados

A fusão entre a matriz da corporação A e a filial da corporação B, como observado na Figura (36), adiciona os dois roteadores ARD2 e ARD3 ao domínio OSPF, surgindo à possibilidade destes roteadores utilizarem um RID já existente no domínio, visto que anteriormente as corporações possuíam redes de comunicação independentes, prejudicando a convergência de rede.

5.1.5 Falha de Redistribuição de Rotas

A hierarquia de áreas OSPF determina o papel de cada área e algumas funções que devem ser desempenhadas ou não de acordo com o tipo de roteador OSPF pertencente às áreas. Por exemplo, a área *backbone* deve agregar todas as informações de topologia originadas pelas demais áreas, sendo responsável por encaminha-las para todas as áreas do domínio. A área *Stub* pode ser considerada como uma área que envia todo ou a maior parte do seu tráfego não destinado às redes da área, por um único caminho de saída. Ela não precisa ter o conhecimento de rotas externas e nem deve divulgar tais rotas, visto que possui apenas um único caminho para o tráfego externo a sua área. Assim, rotas externas não são propagadas e não podem ser originadas dentro de uma área *Stub*.

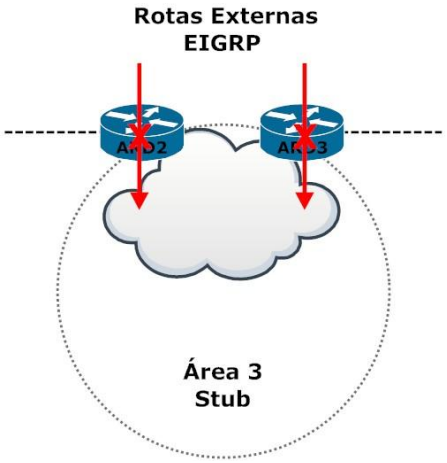


Figura 40 – Não Redistribuição de Rotas em Áreas *Stub*.

A fusão entre a matriz da corporação A e a filial da corporação B pela conexão WAN *Frame Relay*, que conecta os roteadores ADR2 e ADR3 ao roteador BRD3, é realiza dentro de uma área OSPF *Stub*.

Como está área não pode originar e propagar rotas externas, a fusão não funcionará corretamente neste ponto, visto que as informações de rotas da corporação A não irão ser redistribuídas para dentro do domínio OSPF. Os roteadores ADR2 e ADR3 são impedidos de atuarem como roteadores ASBR e redistribuírem rotas dentro desta área.

5.1.6 Loop na Redistribuição de Rotas

Quando a redistribuição de rotas é realizada em mais de um ponto de ligação entre os domínios de roteamento e de forma bidirecional, com os roteadores redistribuindo informações de e para ambos os domínios, uma rota pode sofrer uma espécie de *loop* de redistribuição. Uma rota que originalmente estava sendo propagada em um dos domínios, ao ser redistribuída para o outro domínio, pode ser injetada novamente por este domínio, de volta ao primeiro domínio.

As rotas que foram redistribuídas pelo roteador WAN3 para dentro do domínio EIGRP, ao alcançarem os roteadores ARD2 e ARD3, na fusão da matriz da corporação A com a filial da corporação B e os roteadores BRD1 e BRD2, na fusão da matriz da corporação A com a matriz da corporação B, irão ser redistribuídas agora para dentro do domínio OSPF e poderão voltar a serem redistribuídas por estes roteadores novamente no domínio EIGRP. Os roteadores ARD2, ARD3, BRD1 e BRD2, por meio da rede *intra-network* da matriz da corporação A, recebem as rotas redistribuídas pelo roteador WAN3, rotas externas EIGRP, com uma distância administrativa padrão de 170. Quando aqueles roteadores realizam a redistribuição destas rotas dentro do domínio OSPF, elas recebem uma distância administrativa padrão OSPF de 110. Que ao serem propagadas dentro do domínio OSPF, pode ocorrer de um dos roteadores ARD2 ou ARD3 e BRD1 ou BRD2, receberem essas rotas por meio do domínio OSPF com distância administrativa 110, menor do que as recebidas por meio do domínio EIGRP com distância administrativa 170. Como a menor distância administrativa é escolhida como sendo a rota mais confiável, a rota escolhida para constar na tabela de roteamento será a rota pelo domínio OSPF e como estes roteadores estão realizando a redistribuição bidirecional, esta rota será novamente redistribuída dentro do domínio EIGRP por um destes roteadores (ODOM, 2010).

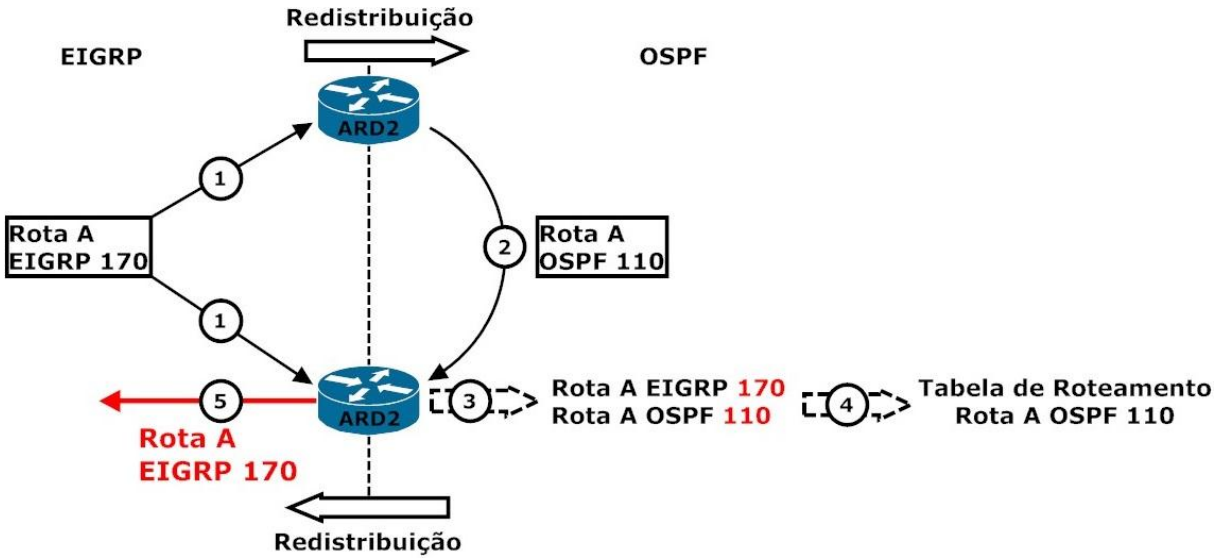


Figura 41 – Loop de Redistribuição de Rota.

5.1.7 Escolha Não Ótima de Melhor Rota na Redistribuição de Rotas

Como uma das consequências do loop na redistribuição de rotas envolvendo os roteadores ARD2 e ARD3, pode ocorrer de um roteador interno a *intra-network* da matriz da corporação A, optar pela rota de loop para alcançar determinada rede da filial 4 da corporação A ao invés de escolher o caminho direto pelo roteador WAN3.

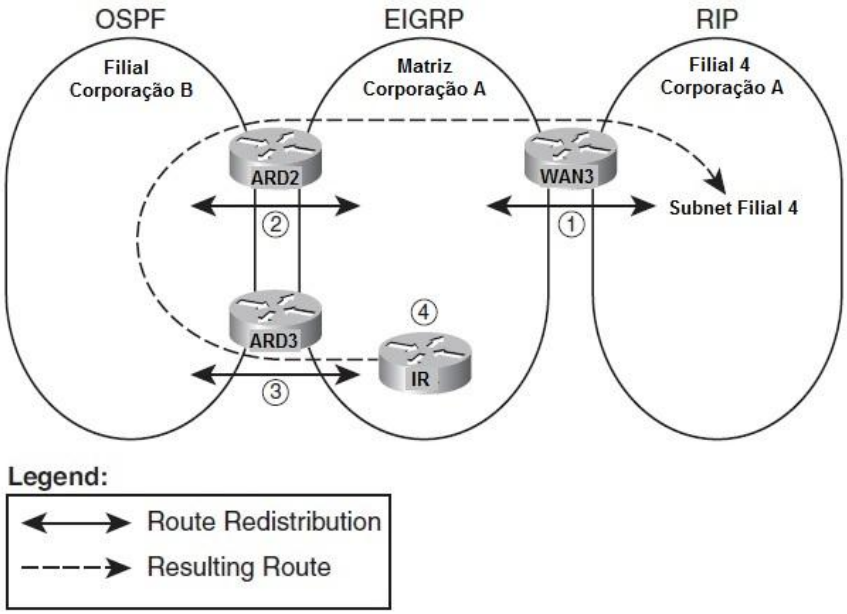


Figura 42 – Escolha não ótima: Rota de Loop (Modificado de Odom, 2010).

Outra escolha não ótima de melhor rota está relacionada à redistribuição realizada pelos roteadores BRD1 e BRD2 que por padrão, realizam a redistribuição de rotas para dentro do domínio OSPF como rotas externas do tipo 2, este tipo de rotas externas não sofrem alteração de métrica durante a propagação dentro do domínio OSPF. Não são levadas em consideração as métricas internas dos roteadores no caminho para alcançar os roteadores que estão propagando as rotas externas tipo 2, apenas a própria métrica estipulada por estes roteadores é levada em conta. O que pode fazer com que os roteadores do domínio OSPF optem por uma pior rota interna para alcançar as rotas externas.

5.1.8 Falha na Troca de Informações e de Convergência de Rede por Conexão WAN

Os pontos de fusão entre as corporações são realizados por meio de conexões WAN *Frame Relay* do tipo *point-to-multipoint* utilizando canais PVC em uma arquitetura *partial mesh*. No ponto de fusão entre as matrizes, o roteador ARD1 desempenha um papel de *hub*, possuindo uma conexão para cada um dos roteadores BRD1 e BRD2, considerados *spoke* e no caso da fusão entre a matriz da corporação A e a filial da corporação B, o roteador BRD3 desempenha o papel de *hub*, possuindo uma conexão para cada um dos roteadores ARD2 e ARD3, considerados *spoke*.

Este tipo de arquitetura pode apresentar algumas inconsistências quanto à troca de informações de roteamento quando são utilizados protocolos de roteamento tanto do tipo *distance-vector*, quanto do tipo *link-state*.

A comunicação entre os roteadores ARD1, BRD1 e BRD2, é realizada pelo protocolo EIGRP, que apesar de possuir diferenças significativas com os protocolos tradicionais *distance-vector*, continua a ser um protocolo deste tipo. Tornando necessário que algumas características deste tipo de protocolo sejam analisadas devido à arquitetura utilizada para a fusão entre as matrizes das corporações.

O EIGRP, assim como os protocolos de *distance-vector*, utilizam alguns métodos para evitar *loops* de roteamento, um deles é chamado *split-horizon*. Este método determina que uma rota aprendida por uma interface, não deve ser anunciada por esta interface.

O *split-horizon* utilizado pelo EIGRP pode provocar inconsistências na troca de informações na arquitetura de fusão utilizada, visto que as rotas aprendidas pelo roteador ARD1 por meio dos roteadores BRD1 e BRD2, não serão anunciadas para estes. As rotas anunciadas pelo roteador BRD1 para o roteador ARD1, não serão repassadas para o roteador BRD2, assim como as rotas anunciadas pelo roteador BRD2 para o roteador ARD1, não serão repassadas para o roteador BRD1. Em certas situações este comportamento pode causar problemas para convergência e escalabilidade de rede,

principalmente com o crescimento e adição de novos roteadores de outras localidades a esta arquitetura, podendo levar a falha de comunicação entre pontos remotos das corporações.

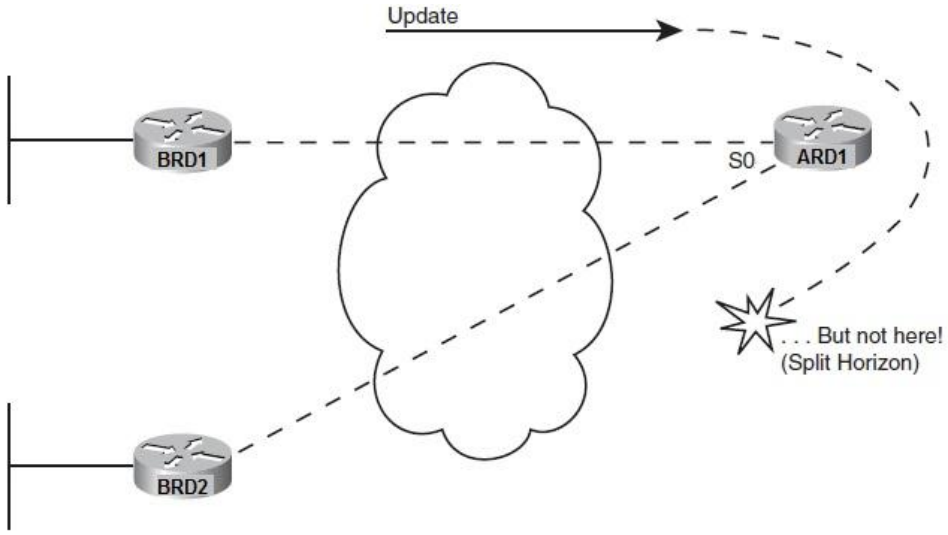


Figura 43 – *Frame Relay* e *Split Horizon* na Fusão das Matrizes (Modificado de ODOM, 2010).

A comunicação entre os roteadores ARD2, ARD3 e BRD3, é realizada pelo protocolo OSPF, um protocolo do tipo *link-state*. Sendo necessário também, que algumas características deste tipo de protocolo sejam analisadas devido ao tipo de arquitetura utilizada na fusão entre a matriz da corporação A e a filial da corporação B.

O OSPF a partir da definição do tipo de *interface* sobre a qual está operando, determina alguns comportamentos que serão desempenhados em relação ao protocolo *Hello*, que é utilizado no processo de descoberta de vizinhos e em relação à eleição de roteadores *designated router* (DR) e *backup designated router* (BDR). Por exemplo, em uma interface conectada a uma rede *broadcast*, o OSPF determina que o processo de descoberta de vizinhos pelo protocolo *Hello* seja realizado dinamicamente por comunicação *multicast* e que a eleição DR/BDR ocorra.

A conexão WAN *Frame Relay* é considerada como uma rede *non-broadcast multiple access* (NBMA), nela podem existir múltiplos *hosts* conectados ao mesmo segmento e uma limitação quanto ao tráfego de tipo *broadcast*. Assim, o protocolo OSPF implementado pelos roteadores ARD2, ARD3 e BRD3 consideram que a interface que participa da conexão WAN *Frame Relay* está conectada a uma rede NBMA, determinando que a eleição DR/BDR ocorra e que o processo de descoberta de vizinhos pelo protocolo *Hello* seja realizado estaticamente por comunicação *unicast*.

Este comportamento apresenta problemas com a arquitetura WAN *Frame Relay* utilizada, pois é necessário que os roteadores eleitos como DR e BDR possuam uma comunicação direta com todos os demais roteadores presentes nos segmento. Em certas situações podendo causar problemas para convergência e escalabilidade de rede, principalmente com o crescimento e adição de novos roteadores de outras localidades a esta arquitetura, podendo levar a falha de comunicação entre pontos remotos das corporações.

Outro problema vinculado ao uso do protocolo OSPF com a arquitetura WAN *Frame Relay* utilizada, esta relacionado ao processo de troca de informações de topologia e com a escolha de melhor rota. Todos os roteadores pertencentes à mesma área do domino OSPF, vão possuir as mesmas informações em suas LSDBs, ou seja, os mesmos LSAs. Então, mesmo que não exista uma comunicação direta, um PVC, entre os roteadores da conexão WAN *Frame Relay*, por possuírem as mesmas informações na LSDB, pode ocorrer que um dos roteadores escolha uma rota para determinado destino, em que o *next-hop* desta rota seja um roteador ao qual ele não possui um PVC, impossibilitando a comunicação com o destino.

5.2 PROPOSTA DE RECOMENDAÇÕES PARA INTEGRAÇÃO DE PROTOCOLOS HETEROGÊNEOS

A revisão literária e os estudos realizados até então neste trabalho, somados as análises realizadas na seção anterior, permite a elaboração de uma proposta de recomendações com o intuito de minimizar ou eliminar as vulnerabilidades e riscos levantados para o estudo de caso durante este trabalho. É importante ressaltar que esta proposta esta restrita aos cenários anteriormente apresentados.

5.2.1 Adotar o Uso de Interfaces Passivas, Comunicação *Unicast* e Autenticação

Os protocolos de roteamento RIPv2, OSPF e EIGRP, por padrão se comunicam pelo envio de pacotes *Hello* em *multicast* sem autenticação por todas as interfaces que possuam um endereço de rede pertencente as redes que estão sendo propagadas no domínio de roteamento, conforme vimos nos capítulos anteriores.

Esse comportamento pode ser considerado uma vulnerabilidade por permitir ameaças como captura de informação indevida, negação de comunicação e injeção de rotas maliciosas para desvio de tráfego, como visto anteriormente.

Uma boa prática para evitar estes tipos de ameaças é alterar o comportamento padrão dos protocolos de roteamento realizando as seguintes ações:

- Utilizar Interfaces Passivas

  Os pacotes *Hello* devem ser enviados somente pelas interfaces onde é esperada uma relação de vizinhança com algum roteador legítimo da rede. Assim, as interfaces onde esta relação não é esperada, devem ser definidas como interfaces passivas. Estas interfaces não enviam pacotes *Hello*, mas as redes as quais elas pertencem continuam sendo propagadas no domínio de roteamento.

- Utilizar Comunicação *Unicast*

  Envio de pacotes *Hello* devem ser feitos por comunicação *unicast*. Com o endereço de destino do pacote *Hello* igual ao endereço IP do roteador legítimo da rede ao qual se deve estabelecer uma relação de vizinhança. Reduzindo a possibilidade dos pacotes *Hello* serem capturados ou recebidos por outros agentes maliciosos no segmento.

- Utilizar Autenticação *Message-Digest algorithm 5* (MD5)

  Os pacotes *Hello* devem ser autenticados usando o algoritmo de *hash* MD5. A fim de se garantir a integridade e autenticidade dos pacotes, reduzindo a possibilidade de agentes maliciosos estabelecerem relação de vizinhança com os roteadores legítimos da rede.

Estas recomendações quando adotadas em conjunto, reduzem drasticamente a probabilidade de ocorrência dos riscos acima citados.

5.2.2 Delimitar Áreas *Stub* e Realizar a Definição de RID

O RID e as áreas OSPF são fundamentais para o bom funcionamento do protocolo OSPF, o mau planejamento ou a má execução de algum destes aspectos pode acarretar em problemas de convergência de rede e de falha de redistribuição como vistos anteriormente.

O RID dos roteadores utilizados no estudo de caso, quando não definidos diretamente são determinados na seguinte ordem: como o IP mais alto configurado nas interfaces *loopback* ativas, caso não exista, como o IP mais alto configurado nas interfaces ativas. As áreas OSPF determinam algumas funções que devem ser desempenhadas ou não de acordo com o tipo de roteadores OSPF pertencentes às áreas, como redistribuição, por exemplo.

A realização das seguintes ações podem minimizar os problemas de operação do OSPF relacionados a falha de convergência e redistribuição de rotas:

- Controlar e definir explicitamente o RID

Determinar diretamente o RID de cada roteador por configuração explicita e manter um controle sobre estes identificadores. Reduz a possibilidade que novos roteadores utilizem um RID já existente no domínio de roteamento, evitando flutuação de rotas na tabela de roteamento e falhas na convergência de rede.

- Não realizar a fusão sobre áreas *Stubs*

  Áreas *Stubs* não devem ser consideradas no planejamento e nem utilizadas como ponto de fusão entre domínios de roteamento. Estas áreas não podem intermediar a comunicação entre outros dois pontos. Caso não seja possível utilizar outra área para realizar a fusão, converter a área *Stub* em área *not-so-stubby* (NSSA).

Em algumas arquiteturas EIGRP de conexão entre filiais e matriz, as filiais não devem ser responsáveis por encaminhar qualquer outro tipo de tráfego para matriz que não seja originado por elas mesmo. Tal encaminhamento pode saturar o link com a matriz e interromper a comunicação, para que isso não ocorra, a seguinte ação pode ser realizada:

- Definir Filiais em pontos remotos como uma área *Stub* EIGRP

  Áreas *Stub* EIGRP, por padrão, anunciam somente redes diretamente conectadas e rotas sumarizadas automaticamente ou manualmente, não anunciam as rotas aprendidas por seus vizinhos, além de não serem consultadas em um processo de busca por rotas. (CISCO PRESS, CCNP ROUTE 642-902).

5.2.3 Realizar a Filtragem de Rotas, Ajustar Métricas e Distância Administrativa

Problemas de *loop* na redistribuição de rotas, além de aumentar a quantidade de informação redundante nos domínios de roteamento podem acabar causando problemas de escolha não ótima de melhor rota, como visto na secção anterior.

As seguintes ações podem ser realizadas para evitar estes tipos de problemas (ODOM, 2010):

- Filtrar rotas em uma das direções de redistribuição

  Uma rota recebida por um domínio de roteamento não deve ser redistribuída novamente para este domínio, devendo ser filtrada dos pacotes de informação de rotas enviados para o domínio ao qual aquela rota foi recebida em todos os roteadores que executam a redistribuição. Isso evita que uma rota que já esta sendo propagada dentro de um domínio de roteamento seja novamente redistribuída neste domínio.

- Ajustar a Métrica das rotas redistribuídas

  As rotas redistribuídas em um domínio devem ter suas métricas ajustadas para valores que sejam maiores que a pior métrica encontrada neste domínio. Isso evita que, caso já exista uma rota no domínio de roteamento para determinado destino, que essa mesma rota seja escolhida por redistribuição ou que uma rota redistribuída seja escolhida ao invés de uma rota interna.

- Ajustar a Distância Administrativa nos roteadores que realizam a redistribuição

  Alterar a distancia administrativa localmente para determinadas rotas anunciadas por outros roteadores que estão realizando redistribuição no mesmo domínio, influenciando se estas rotas devem ou não serem escolhidas para tabela de roteamento e consequentemente devem ou não serem redistribuídas.

5.2.4 Desabilitar *Split-Horizon*, Alterar Tipo de Interfaces OSPF e Realizar o *Frame Relay Map*

Quando arquiteturas *partial-mesh*, no caso particular de *hub-and-spoke*, e *point-to-multipoint* são utilizadas para conexão WAN *Frame Relay*, observamos alguns problemas relacionados à troca de rotas pelos protocolos de roteamento do tipo *distance-vector*, no caso o protocolo EIGRP, causado pelo método *Split-Horizon*. Neste tipo de arquitetura, uma ação simples pode solucionar a inconsistência de rotas:

- Desabilitar o *Split-Horizon*

  Desabilitar o *Split-Horizon* possibilita que em uma arquitetura *hub-and-spoke* com o uso de interfaces *point-to-multipoint*, os *spokes* da arquitetura possam receber as informações de rotas originadas pelos demais *spokes* buscando uma convergência de rede consistente.

Quando esta arquitetura é utilizada com protocolos de roteamento OSPF, dois problemas podem estar presentes, um está relacionado à eleição dos roteadores DR/BDR, que devem possuir comunicação direta com todos os demais roteadores participantes do segmento e o outro esta relacionado à possibilidade de uma rota escolhida para constar na tabela de roteamento não possuir um caminho na camada de enlace para alcançar o destino. As seguintes ações podem ajudar a eliminar estes problemas:

- Alterar o tipo de interface OSPF para *Point-to-Multipoint*

  Este tipo de interface OSPF não elege roteadores DR/BDR, não sendo mais um problema o fato de não existir comunicação direta entre os roteadores da conexão WAN.

- Realizar mapeamento *Frame-Relay* indireto

  Utilizar PVCs intermediários para alcançar o *next-hop* da rota. Isso evita que mesmo contendo na tabela de roteamento a rota e o *next-hop*, quando for para a camada de enlace, o pacote seja descartado por falta de um LDCI especifico para alcançar aquele IP de *next-hop*. Assim o pacote será encaminhado para um roteador intermediário que possui um PVC para o *next-hop*. (Odom, 2010)

6 CONCLUSÃO

Este capítulo apresenta uma conclusão de todas as observações e análises realizadas durante este trabalho de conclusão de curso que teve como foco a operação individual e conjunta de domínios de roteamento sobre diversas perspectivas de arquiteturas presentes no estudo de caso apresentado.

Foram apresentados os principais aspectos de segurança e roteamento envolvidos em um cenário real modificado de uma rede coorporativa com protocolos heterogêneos. Nesse modelo vimos os principais problemas de maneira generalizada e possíveis formas de controlar e até mesmo evitar essas ameaças.

No primeiro capítulo enumeramos os objetivos específicos do trabalho, elucidando toda a metodologia utilizada como também explicamos toda a justificativa e motivação da escolha do tema. Em seguida, no segundo capítulo, foram ilustrados os principais protocolos e tecnologias de acesso e suas principais características.

No terceiro capítulo foi visto de forma isolada diversas ameaças e vulnerabilidade no contexto de redes de comunicação, onde notamos que até os mais simples problemas na implantação da rede podem gerar grandes riscos no projeto como um todo. Levantamos as principais características de cada ameaça de maneira que pudéssemos usar todo conhecimento adquirido para um estudo mais eficiente do cenário coorporativo com protocolos heterogêneos.

Logo após, no quarto capítulo, foram apresentadas as redes coorporativas com protocolos diferentes, mostrando suas características singulares, seus aspectos gerais e principais desafios. Apresentamos também o cenário da fusão coorporativa dessas redes e seus principais desafios de implantação. Por fim, nesse capítulo, levantamos os principais pontos de vulnerabilidade dessa rede de maneira isolada e quando ocorre a fusão coorporativa.

Por fim, no quinto capitulo, foi feita a análise das vulnerabilidades levantadas no cenário coorporativo mostrado anteriormente propondo uma série de mudanças para reduzi-las ou até mesmo evita-las.

Logo essas recomendações foram estabelecidas com o estudo aprofundado do cenário proposto, podendo ser adotadas para integrar e consolidar a gestão de uma rede semelhante ou com características próximas à proposta. Apoia também o planejamento de fusão e crescimento de redes que venham a usar protocolos heterogêneos, garantindo assim um melhor monitoramento, segurança e gestão dessas redes coorporativas.

Com as análises e modelagens propostas nesse documento pode se concluir que cada vez mais as redes estão complexas e dinâmicas, motivos os quais levam a mercados cada vez mais distribuídos e possivelmente vulneráveis. É fato que para cada caso de redistribuição o gestor da rede deve propor comportamentos e respostas diferentes à medida que for levantado todo as possíveis fragilidades. Assim esperamos poder ter contribuído para a consolidação de um conhecimento fragmentado em diversas literaturas em um único trabalho.

REFERÊNCIAS BIBLIOGRÁFICAS

AFONSO, Eduardo. PROTOCOLO M.P.L.S.. Disponível em <http://www.tiespecialistas.com.br/2011/04/protocolo-m-p-l-s/#.UeYO6Y2-2uJ> acessado em 05 de julho de 2013.

ALENCAR, M. Engenharia de Redes de Computadores. ed. Érica, 2012.

ASSIS, Alexandre Urtado de; FERRAZ, Tatiana Lopes; ALBUQUERQUE, Marcelo Portes; ALBUQUERQUE, Márcio Portes; ALVES, Nilton Junior. Nota Técnica 007/02 - Centro Brasileiro de Pesquisas Físicas (CBPF), 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO 27001 - Tecnologia da Informação - Técnicas de Segurança - Gestão de Riscos de Segurança da Informação - Requisitos. Rio de Janeiro: ABNT, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO 27002 - Tecnologia da Informação - Técnicas de Segurança - Código de Práticas para a Gestão de Segurança da Informação. Rio de Janeiro: ABNT, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO 27005 - Tecnologia da Informação - Técnicas de Segurança - Gestão de Riscos de Segurança da Informação. Rio de Janeiro: ABNT, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO 31000 - Gestão de Riscos - Princípios e Diretrizes. Rio de Janeiro: ABNT, 2009.

BRITTO, Fernando de; CÂNDIDO, Silvio Mário. Análise dos Aspectos de Segurança da Informação em um Ambiente de Comunicações Unificadas. Trabalho de Graduação (Graduação em Engenharia de Redes de Comunicação), Universidade de Brasília. Brasília. 2013.

BRITO, S. Laboratório de Tecnologias Cisco em Infraestrutura de Redes. ed. Novatec, 2012.

CASAGRANDE, Rogério Antônio. Técnicas de Detecção de Sniffers. Dissertação de Mestrado em Ciência da Computação. Universidade Federal do Rio Grande do Sul. 2003.

CISCO SYSTEMS INC., OSPF Virtual Link, Janeiro, 2007 disponível em <http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a00801ec9ee.shtml?referring_site=smartnavRD>, acessado em 23/06/2013.

CISCO SYSTEMS INC., Using OSPF in an MPLS VPN Environment. 2002. Disponível em < https://www.racf.bnl.gov/Facility/TechnologyMeeting/Archive/06-30-04-CISCO/Using-OSPF-in-MPLS-VPN-Environment.pdf>, acessado em 10 de julho de 2013

COMER, D.; STEVENS, D. Interligação em Rede com TCP/IP: Princípios Protocolos e Arquitetura. 2. ed. Rio de Janeiro: Campus, v. 1, 1998.

DHAR, Sumit. Sniffers – Básico e Detecção. Linux Security Magazine. Ano 1 Edição nº 2, 2000

FERREIRA, M. O que vem a ser Segurança da Informação, 2005. disponível em: <http://www.apinfo.com/artigo81.htm>. Acesso em: 21 Janeiro 2013.

FRAULOB, Davi M.; PIACENTINI, Edgar J.. Metro Ethernet – Mestrado em Informática Aplicada - Pontifícia Universidade Católica do Paraná (PUC-PR), 2006

HALABI, Sam, OSPF Design Guide. CISCO SYSTEMS INC., Abril, 1996.

INTERNET ENGINEERING TASK FORCE - IETF. RFC 1247 - OSPF: version 2, Junho 1991.

INTERNET ENGINEERING TASK FORCE - IETF. RFC 2328 - OSPF: Standards Track, Abril 1998.

KUROSE, J.; ROSS, K. Redes de computadores e a internet: uma abordagem top-down. 5. ed. São Paulo: Pearson Addison Wesley, 2009.

LAGES, Walter Fetter. Pilha TCP/IP. Programa de Pós-Graduação em Engenharia Elétrica. Universidade Federal do Rio Grande do Sul.

LAKATO, Eva Maria; MARCONI, Marina de Andrade. Fundamentos de Metodologia Científica. 5a Edição. São Paulo: Editora ATLAS, 2003.

MARQUES, Manoel Carvalho; BEZERRA, Romildo Martins da Silva, Protocolos de Roteamento RIP e OSPF - Monografia no Mestrado de Redes de Computadores da UNIFACS, 2002.

MATTHEWS, Jeanna. Computer Networking: Internet Protocols in Action, Janeiro de 2005.

METRO ETHERNET FORUM, Metro Ethernet Services – A Technical Overview, 2003, Rolf Sanitoro, disponível em <http://www.metroethernetforum.org/>, maio, 2013.

MORAES, A. Cisco Firewalls - Concepts, Design and Deployment for Cisco Stateful Firewall Solutions. 1. Ed. Indianapolis: CISCO SYSTEMS INC., Abril, 1996, 2011.

NIC BR SECURITY OFFICE - Práticas de Segurança para Administradores de Redes Internet. Versão 1.2. Maio, 2003

ODOM, Wendell. Guia de Certificação Oficial para o Exame CCENT/CCNA ICND1. Ed Alta Book, Rio de Janeiro 2008

ODOM, Wendell. Guia de Certificação Oficial para o Exame CCENT/CCNA ICND2. Ed Alta Book, Rio de Janeiro 2008

ODOM, Wendell. CCNP ROUTE 642-902 Official Certification Guide. CISCO PRESS. Fev,2010

ROSEN, E., WISWANATHAN, A., CALLON, R., "RFC 3031 Multiprotocol Label Switching Architecture", Janeiro de 2010

SANTITORO, RALPH. Metro Ethernet Services - A Technical Overview. MEF-2006

TORRES, G. Redes de Computadores. Ed. Revisada e Atualizada, ed.Nova Terra, 2009.