

**UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS
DEPARTAMENTO DE INFORMÁTICA**

**ESTUDO DE ROTEAMENTO DINÂMICO UNICAST COM O
PROTOCOLO OSPF UTILIZANDO A FERRAMENTA DE SIMULAÇÃO
GNS3 PARA A REDE DE COMPUTADORES DA UNIVERSIDADE
FEDERAL DO MARANHÃO**

JOSÉ RIBAMAR SANTANA NETTO

São Luís – MA

2014

JOSÉ RIBAMAR SANTANA NETTO

ESTUDO DE ROTEAMENTO DINÂMICO UNICAST COM O PROTOCOLO OSPF
UTILIZANDO A FERRAMENTA DE SIMULAÇÃO GNS3 PARA A REDE DE
COMPUTADORES DA UNIVERSIDADE FEDERAL DO MARANHÃO

Monografia apresentada
junto ao Curso de Ciência da
Computação da Universidade
Federal do Maranhão (UFMA),
como parte dos requisitos
necessários para obtenção do
grau de Bacharel em Ciência
da Computação.

Orientador: Prof. Dr. Geraldo Braz Júnior

São Luís – MA

2014

Santana Netto, José Ribamar

Estudo de roteamento dinâmico UNICAST com o protocolo OSPF utilizando a ferramenta de simulação GNS3 para a rede de computadores da Universidade Federal do Maranhão / José Ribamar Santana Netto. — São Luis, 2014.

68 f.

Impresso por computador (Fotocópia).

Orientador: Geraldo Braz Junior.

Monografia (Graduação) – Universidade Federal do Maranhão, Curso de Ciência da Computação, 2014.

1. Rede de computadores – UFMA. 2. Roteamento dinâmico UNICAST. 3. Protocolo OSPF. 4. Simulação GNS3. I. Título.

CDU 004.738:378(812.1)

UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS
DEPARTAMENTO DE INFORMÁTICA

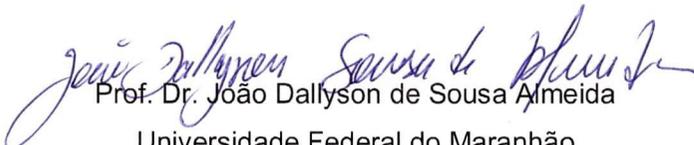
ESTUDO DE ROTEAMENTO DINÂMICO UNICAST COM O PROTOCOLO OSPF
UTILIZANDO A FERRAMENTA DE SIMULAÇÃO GNS3 PARA A REDE DE
COMPUTADORES DA UNIVERSIDADE FEDERAL DO MARANHÃO

JOSÉ RIBAMAR SANTANA NETTO

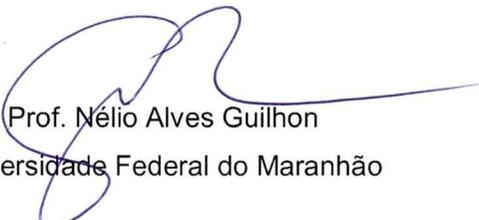
BANCA EXAMINADORA


Prof. Dr. Geraldo Braz Júnior

Universidade Federal do Maranhão
Orientador


Prof. Dr. João Dallyson de Sousa Almeida

Universidade Federal do Maranhão


Prof. Nélio Alves Guilhon

Universidade Federal do Maranhão

Aprovada em: 25 de novembro de 2014

UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS
DEPARTAMENTO DE INFORMÁTICA

ESTUDO DE ROTEAMENTO DINÂMICO UNICAST COM O PROTOCOLO OSPF
UTILIZANDO A FERRAMENTA DE SIMULAÇÃO GNS3 PARA A REDE DE
COMPUTADORES DA UNIVERSIDADE FEDERAL DO MARANHÃO

JOSÉ RIBAMAR SANTANA NETTO

BANCA EXAMINADORA

Prof. Dr. Geraldo Braz Júnior
Universidade Federal do Maranhão
Orientador

Prof. Dr. João Dallyson de Sousa Almeida
Universidade Federal do Maranhão

Prof. Nélio Alves Guilhon
Universidade Federal do Maranhão

Aprovada em: de novembro de 2014

Agradecimentos

Agradeço ao meu orientador, Prof. Geraldo Braz, por aceitar me acompanhar neste trabalho. Ao professor Nélio Guilhon pelo incentivo e amizade. E ao Departamento de Informática (DEINF/UFMA) por seu trabalho de formar grandes profissionais no estado do Maranhão.

Dedicatória

Ao meu Deus que é soberano e maior que tudo e todos! Que me sustenta e guarda todos os dias da minha vida.

Aos meus pais, Feitosa e Deuzimar, vocês são meu farol de caráter, amor e dedicação.

Ao meu irmão, Franklin, por ser amigo, companheiro e presente.

A minha esposa linda e preciosa! Obrigado pelo apoio, amor e sinceridade.

Aos meus lindos filhos, João Pedro e Melissa. Vocês são minha inspiração e que me proporcionam meu maior desafio, ser Pai. Amo vocês!

"Há muitos planos no coração do homem, mas é a vontade de Deus que se realiza".
(Provérbios 19:21)

Resumo

Existem muitos algoritmos de roteamento utilizados em redes de computadores com ideias e objetivos distintos, os quais visam solucionar vários problemas no roteamento de pacotes. Este trabalho visa apresentar uma visão sobre princípios de roteamento em rede IP (Internet Protocol), onde o algoritmo muito utilizado em redes de computadores, o protocolo de roteamento dinâmico OSPF (Open Shortest Path First), será apresentado e simulado em operação.

As simulações são realizadas através da conceituada ferramenta de simulação, o GNS3 (Graphical Network Simulator). O propósito é verificar as ações do protocolo OSPF numa simulação da estrutura da rede de computadores da UFMA e apresentar as particularidades da execução do protocolo e suas reações.

Palavras-chave: Redes, Roteamento, Protocolo, OSPF, GNS3.

Abstract

There are many routing algorithms used in computer networks with different ideas and objectives, which aim to solve various problems in the packet routing. This paper presents an overview of routing principles in IP (Internet Protocol), where the algorithm widely used in computer networks, the dynamic routing protocol OSPF (Open Shortest Path First), will be presented and simulated in operation.

Simulations are made by reputable simulation tool, the GNS3 (Graphical Network Simulator). The purpose is to check the actions of the OSPF protocol in a simulation of the UFMA computer network structure and present protocol implementation of the particularities and their reactions.

Keywords: Networking, Routing Protocol, OSPF, GNS3.

LISTA DE ILUSTRAÇÕES

Figura 2.1: Modelo do pacote de estado de enlace.....	18
Figura 2.2: Dinâmica do roteamento hierárquico.....	20
Figura 2.3: Tipos de rede compatíveis com o OSPF.....	24
Figura 2.4: Grafo da topologia de redes suportadas pelo OSPF.....	25
Figura 2.5: Possíveis adjacências em uma rede com capacidade Multiaccess.....	26
Figura 2.6: Adjacências estabelecidas com o roteador “A”.....	27
Figura 2.7: Áreas e roteadores no OSPF.....	29
Figura 2.8: Cabeçalho padrão dos subprotocolos OSPF.....	29
Figura 2.9: Tipos de pacotes originados no protocolo OSPF.....	30
Figura 2.10: Tipos de LSA no protocolo OSPF.....	34
Figura 2.11: Comportamentos dos tipos de LSA.....	35
Figura 3.1: A Rede UFMA.....	37
Figura 3.2: Topologia física de estrela estendida.....	38
Figura 3.3: Camadas da topologia hierárquica.....	38
Figura 3.4: Exemplo real de topologia hierárquica.....	39
Figura 3.5: Camadas da topologia hierárquica na Rede UFMA.....	39
Figura 3.6: Nova topologia física para a Rede UFMA.....	43
Figura 4.1: Interface gráfica do GNS3.....	45
Figura 4.2: Roteadores envolvidos na simulação.....	47
Figura 4.3: Parâmetros do protocolo OSPF dos roteadores envolvidos na simulação.....	47
Figura 4.4: Topologia lógica da simulação.....	49
Figura 4.5: Topologia no simulador GNS3.....	49
Figura 4.6: Topologia do cenário 1.....	50
Figura 4.7: Cenário 1 – Traceroute do primeiro teste.....	51
Figura 4.8: Cenário 1 – Traceroute do segundo teste.....	52
Figura 4.9: Cenário 1 – Traceroute do terceiro teste.....	52
Figura 4.10: Cenário 1 – Traceroute do quarto teste.....	53
Figura 4.11: Topologia do cenário 2.....	54
Figura 4.12: Cenário 2 – Traceroute do primeiro teste.....	55
Figura 4.13: Cenário 2 – Traceroute do segundo teste.....	55

LISTA DE ABREVIATURAS E SIGLAS

OSI	Open Systems Interconnection
IP	Internet Protocol
RIP	Routing Information Protocol
OSPF	Open Shortest Path First
IS-IS	Intermediate System-Intermediate System
IGP	Interior Gateway Protocol
EGP	Exterior Gateway Protocol
BGP	Border Gateway Protocol
SPF	Shortest Path First
DR	Designated Router
BDR	Backup Designated Router
LSA	Link State Advertisement
IPv6	Internet Protocol versão 6
IPv4	Internet Protocol versão 4
TCP	Transmission Control Protocol
VoIP	Voice over Internet Protocol
EAD	Ensino à Distância
GNS	Graphical Network Simulator

SUMÁRIO

1. INTRODUÇÃO	11
2. REFERENCIAL TEÓRICO	14
2.1 ALGORITMOS DE ROTEAMENTO	14
2.1.1 <i>Propriedades dos algoritmos de roteamento</i>	14
2.1.2 <i>Classificação dos algoritmos de roteamento</i>	15
2.1.3 <i>Principais algoritmos de roteamento</i>	16
2.2 PROTOCOLO OSPF	22
2.2.1 <i>Vantagens do OSPF</i>	23
2.2.2 <i>Funcionamento geral</i>	24
2.2.3 <i>Protocolos internos do OSPF</i>	30
3. A REDE DE COMPUTADORES DA UFMA	37
3.1 A REDE UFMA	37
3.2 EQUIPAMENTOS DE CONEXÃO	41
3.3 SERVIÇOS OFERECIDOS	41
3.4 UMA SOLUÇÃO DE REDUNDÂNCIA PARA REDE UFMA	43
4. SIMULAÇÃO DA NOVA REDE UFMA	46
4.1 SIMULADOR DE REDES, GNS3	46
4.2 DETALHES DE SIMULAÇÃO	47
4.3 TESTES REALIZADOS	51
5. CONCLUSÃO	57
REFERÊNCIAS	58
APÊNDICE A – PRINCÍPIOS DE ROTEAMENTO EM REDES IP (INTERNET PROTOCOL)	59

1. INTRODUÇÃO

Há anos o crescimento de redes de computadores tem tido uma atenção especial, pois cada vez mais pessoas usam computadores com acesso à Internet. As empresas cada vez mais são dependentes de computadores para a execução de suas atividades e comunicação com seus clientes e parceiros. Com isso as redes de computadores vêm crescendo de forma muito rápida ao ponto de ser necessário ter um melhor controle sobre seus recursos.

Diante desta necessidade, as falhas ou interrupções de acesso à rede ocasionam grandes perdas para toda uma cadeia produtiva da sociedade atual. Prejuízos estes que normalmente afetam também questões econômicas da sociedade. Hoje tudo está conectado e facilmente disponível para uso, o que tem gerado uma forte dependência da tecnologia da informação e comunicação (TIC) nas nossas tarefas diárias.

No cenário acadêmico isto não é diferente, os acadêmicos da nossa sociedade estão cada vez mais conectados e utilizando a TIC para criar, publicar, consumir e difundir suas produções acadêmicas. Agora com uma comunidade acadêmica internacional conectada ficou mais fácil a disseminação de conhecimento e troca de informações visando o avanço em várias áreas. O professor, aluno ou pesquisador pode agregar valor tanto aos seus conhecimentos, como dos outros em qualquer parte do planeta. A Internet tornou-se uma grande ferramenta de inovação que impulsionou a sociedade moderna.

Desta forma, a possibilidade de utilização de serviços avançados como: videoconferência, webconferência, voz sobre IP (VoIP), ferramentas colaboração, ensino a distância (EAD), redes sociais etc; em prol da ciência, acaba diminuindo a tolerância da comunidade acadêmica a indisponibilidade das redes. As universidades passarão a ir além dos seus muros e a chegar até as casas dos alunos, professores e pesquisadores, ou seja, a produção acadêmica pode ser gerada agora em qualquer lugar.

Então, pensar em uma comunidade conectada passa pela garantia de uma infraestrutura de conectividade que seja robusta, performática, confiável e disponível. Entregar todos estes serviços a uma comunidade que cresce diariamente com demanda de acesso requer uma preocupação constante com estes requisitos, de modo que a TIC seja uma grande apoiadora no processo de criação e desenvolvimento do conhecimento.

A Universidade Federal do Maranhão (UFMA), acompanhando e compreendendo as transformações da sociedade e da comunidade acadêmica brasileira, buscou investir fortemente na reestruturação da sua TIC e para tal, buscou investir nas diversas áreas da TIC como: LAN, WAN, Segurança da Informação, Data Center etc; porém visando sempre a performance e disponibilidade de seus serviços e infraestrutura local.

Para isto, o Núcleo de Tecnologia da Informação (NTI) desenvolveu diversos projetos de melhoria da comunicação institucional. Entre eles, a de modernização da rede de computadores da UFMA (Rede UFMA), através de uma nova estrutura dorsal (backbone) com o objetivo principal de garantir os requisitos listados acima. Como o foco principal é o desempenho e disponibilidade, os equipamentos a serem utilizados deverão acompanhar estas premissas de modo a garantir o funcionamento dos principais serviços mesmo em caso de falhas graves.

Porém com uma estrutura como esta, fica clara a necessidade de realizar um estudo que possa respaldar esta nova estrutura física redundante. Isto deve ser feito através de um novo projeto lógico para a Rede UFMA que apresente e teste todos os recursos possíveis desta nova rede física. Através do protocolo de roteamento dinâmico OSPF (Open Shortest Path First) será feita a organização e otimização das rotas de acesso da estrutura de rede de forma a torná-la auto configurável em caso de problemas ou falhas. Os testes são realizados usando o simulador GNS3 numa estrutura física e lógica similar ao que será proposto para a Rede UFMA. Este estudo tem o objetivo demonstrar os benefícios do protocolo de roteamento dinâmico OSPF na nova estrutura de modo que a Rede UFMA redundante e que os serviços ofertados sintam os efeitos benéficos desta estrutura redundante tanto fisicamente quanto logicamente.

Diante disto, este estudo busca demonstrar esta nova estrutura física da Rede UFMA e seu novo projeto lógico redundante. Para tal, encontra-se organizado da seguinte forma: no Capítulo 2 será observada uma referência teórica sobre a camada de rede, roteamento e seus protocolos de roteamento, como das áreas envolvidas, de forma que seja alicerce para a prática deste conhecimento no estudo de caso envolvido.

O Capítulo 3 apresenta informações sobre a Rede UFMA, de modo a ter uma visão clara da sua estrutura física, composição lógica e serviços oferecidos para a comunidade UFMA.

Já o Capítulo 4 mostra o estudo de caso das principais características do protocolo OSPF através da simulação da nova Rede UFMA utilizando o simulador GNS3. Como esta nova configuração da rede vai ajudar na busca por garantir a UFMA a uma estrutura de TIC disponível para sua comunidade.

Por fim, o capítulo 5, apresenta as principais conclusões do estudo e a perspectiva de trabalhos futuros com objetivo de expandir e melhorar a estrutura da Rede UFMA.

2. REFERENCIAL TEÓRICO

O assunto de rede de computadores é cercado de muitos tipos diferentes de redes. Contudo, tem objetivos, escalas e tecnologias que as diferem; e tornam o assunto interessante e técnico. Essas diversas tecnologias de rede foram ao longo do tempo desenvolvidas e evoluídas.

Entretanto, a forma como a informação trafega nesta rede tem diversas técnicas que serão apresentadas para uma compreensão da inteligência desta estrutura que requer desempenho e rapidez.

2.1 Algoritmos de Roteamento

Antes de continuar é necessário conceituar e classificar o coração de qualquer protocolo de roteamento, o algoritmo de roteamento (Kurose e Ross, 2003, pág. 219). Isto vai ajudar a compreender o assunto de forma mais clara.

Tanembaum (2003, pag. 372), afirma que algoritmo de roteamento “é a parte do software da camada de rede responsável pela decisão de sobre a linha de saída a ser usada na transmissão do pacote de entrada”.

Então, simplificando, a finalidade de um algoritmo de roteamento é que dada uma série de roteadores conectados por enlaces, este algoritmo descobre um bom caminho entre a fonte e o destino. Entretanto, o bom caminho é sempre aquele que tem o menor custo (Kurose e Ross, 2003, pág. 219).

2.1.1 Propriedades dos algoritmos de roteamento

Porém, segundo Tanembaum (2003, pag. 373), algumas propriedades são desejáveis para os algoritmos de roteamento. Essas propriedades desejáveis são “correção, simplicidade, robustez, estabilidade, equidade e otimização”.

Onde correção para o algoritmo é a capacidade corrigir após identificação qualquer falha e simplicidade é capacidade de ser simples na busca pelo objetivo. Para a robustez entende-se que o algoritmo de roteamento deve ser capaz de aceitar alterações na topologia e no tráfego sem interromper os equipamentos de conexão e a rede sempre que um roteador falhar.

Já a estabilidade é um objetivo importante do algoritmo de roteamento porque é necessário para que os algoritmos possam convergir para o equilíbrio e permanecer neste estado.

A equidade para o algoritmo de roteamento visa garantir para os fluxos volume de largura de banda iguais e a otimização visa a melhor rota possível para os fluxos de dados.

2.1.2 Classificação dos algoritmos de roteamento

Os algoritmos de roteamento possuem diversas formas de classificação. Cada tipo de classificação reflete as características e funcionamento que são peculiares aos algoritmos. Isso ajuda na análise dos algoritmos, pois eles podem ser analisados de acordo com essas peculiaridades nos diversos ambientes que existem nas redes de computadores (Kurose e Ross, 2003).

Portanto, os principais algoritmos de roteamento podem ser classificados como segue:

- Estático ou Dinâmico

Estes algoritmos são classificados com base na forma de aquisição das rotas. Algoritmos de roteamento estático são resultado de alguma intervenção humana e calculam as rotas entre os nós uma vez em sua primeira execução e não são mais executados. Devido ao fato de ser resultado de intervenção humana, modificam muito lentamente as rotas na rede (Kurose e Ross, 2003, pag. 220).

Já os algoritmos de roteamento dinâmico, os caminhos de roteamento mudam a medida que alterações na rede, como tráfego ou carga e à topologia da rede, acontecem. Executam periodicamente ou reagem (sensíveis), modificando as rotas à medida que a rede é alterada (Kurose e Ross, 2003, pag. 220).

Tanembaum (2003, pag. 374) também chama os algoritmos de roteamento estático de não-adaptativos devido ao fato de que as decisões de roteamento não se baseiam em medidas ou estimativas do tráfego e da topologia da rede. E de adaptativos os algoritmos de roteamento dinâmicos porque mudam suas decisões de roteamento conforme mudanças na topologia e também no tráfego.

- Global ou Descentralizado

Os algoritmos de roteamento nesta classificação tem como referência o custo do menor caminho. Assim, algoritmos de roteamento globais precisam ter conhecimento global e completo de todos os nós da rede para calcular o menor custo. O cálculo das rotas é feito em cada nó, os quais procuram, através de mensagens, conhecer quais os nós fazem parte da rede (Kurose e Ross, 2003, pag. 220).

Os algoritmos de roteamento descentralizados, por sua vez, o cálculo de menor custo é realizado de modo interativo e distribuído. Não é necessário ter conhecimento global da rede. Cada nó procura obter o caminho de menor custo trocando informações de custos com os nós vizinhos. À medida que os dados de roteamento se modificam, o nó envia essa informação para os nós vizinhos, os quais modificam seus dados e os passam para os outros nós (Kurose e Ross, 2003, pag. 220).

- Planos ou hierárquicos

São classificados também através da forma como são agrupados. No plano, os nós são considerados como pares uns dos outros, não existindo subdivisões entre ele. Já nos hierárquicos, os roteadores são divididos em regiões, chamadas de sistemas autônomos (Kurose e Ross, 2003, pag. 233).

Uma região é independente da outra na execução dos seus algoritmos de roteamento. Porém, quando um pacote tem que ser enviado para fora da região, utiliza-se um roteador na borda da região, o qual envia o pacote para a região apropriada (Tanenbaum, 2003, pag. 389 a 391).

2.1.3 Principais algoritmos de roteamento

Como descrito por Tanenbaum (2003, págs. 379 e 380), as redes modernas utilizam algoritmos de roteamento dinâmicos ao invés de estático, pelo fato dele não levar em conta a carga da rede. Por isso dois algoritmos de roteamento dinâmico destacam-se, o roteamento por vetor de distância e o estado de enlace, e são mais conhecidos nas redes. Para tal, os algoritmos serão apresentados com ênfase em suas características principais.

- Algoritmo de vetor de distância

O algoritmo de vetor de distância mantém uma tabela de roteamento (vetor) com informações dos outros nós da rede, como custos e por qual nó ele pode ser alcançado. Esta tabela é atualizada através da troca de informações com vizinhos (TANEMBAUM, 2003; KUROSE e ROSS, 2003).

Esse algoritmo também é conhecido na literatura como algoritmo de roteamento distribuído de Bellman-Ford e também pode ser encontrado como algoritmo de Ford-Fulkerson. Os nomes referenciados – Bellman, Ford e Fulkerson - são dos pesquisadores que desenvolveram este algoritmo (TANEMBAUM, 2003, pág. 380).

Conforme Kurose e Ross (2003, pag. 223), o algoritmo de vetor de distância é distribuído, iterativo e assíncrono. Dito distribuído, pois o cálculo das rotas é feito localmente em cada roteador. Um roteador recebe informações da mudança de custos dos seus vizinhos e atualiza a sua tabela de acordo com as informações recebidas. Ao modificar sua tabela, o roteador envia essa informação para os seus vizinhos.

É iterativo, porque este processo de troca de informações acontece até que nenhuma informação seja mais trocada entre os vizinhos, não existe nenhum sinal para que o cálculo pare, ele apenas para. É assíncrono porque não existe a necessidade que todos os nós operem em cadência ou sequência.

Nisso, todos os roteadores convergem para o cálculo das rotas de menor custo entre os pares de nós (TANEMBAUM, 2003). Esse algoritmo também é dinâmico, pois à medida que há modificações na topologia, ele modifica os valores de custo na tabela do roteador (KUROSE e ROSS, 2003).

Kurose e Ross (2003) apresentam este algoritmo com uma estrutura de dados chamada de tabela de distâncias. Ela é mantida em cada nó e contém uma linha para cada destino da rede e uma coluna para cada um de seus vizinhos diretamente ligados. O custo nesta tabela é definido por Tanenbaum (2003, pag. 380) como uma unidade métrica que pode ser o número de saltos, o tempo de retardo, o número de pacotes enfileirados ou algo semelhante.

A partir desta estrutura Kurose e Ross (2003) define que se um nó X quer rotear para o destino Y por meio de um vizinho Z diretamente ligado, então, o registro na tabela de distâncias do nó X, é a soma do custo do enlace direto de um salto entre X e Z, mais o caminho de custo mínimo correntemente conhecido do vizinho Z até Y. Isto é traduzido pela equação de Bellman-Ford:

$$D_x(Y,Z) = c(X,Z) + \min\{D_z(Z,W)\}.$$

Onde,

$D_x(Y,Z)$ é a distância de menor custo de X até Y;

$c(X,Z)$ é o custo do enlace diretamente ligado a X;

$\min\{D_z(Z,W)\}$ é o custo mínimo de Z até o destino. A função min é calculada para todos os vizinhos de Z.

Entretanto, este algoritmo apresenta uma característica durante a mudança no custo do enlace ou falha no enlace que é um inconveniente na prática. Este algoritmo, em particular, reage com rapidez a “boas notícias” e devagar a “más notícias”. As “boas notícias”, são a troca de vetores para um custo melhor, que é processada em todos os nós com muita rapidez. No entanto, as “más notícias” são quando existe um aumento no custo do enlace e nenhum dos nós ficam com um custo melhor, o que gera um loop de roteamento até que depois de várias interações do algoritmo ele consegue convergir. Esta problemática é conhecida como contagem até o infinito, como relatado por Tanenbaum (2003).

Para tratar esta problemática, houve algumas tentativas de resolver, como a inversão envenenada (poisoned reverse) descrita na RFC 1058¹. Essa técnica, porém não resolve o problema geral da contagem até o infinito (KUROSE e ROSS, 2003).

Por fim, vale citar de acordo com Kurose e Ross (2003), que o algoritmo de vetor de distância é utilizado em muitos protocolos usuais de roteamento, como: RIP (Routing Information Protocol), Internet BGP (Border Gateway Protocol) e foi utilizado como algoritmo original da ARPANET.

- Algoritmo de estado de enlace

Diante dos problemas apresentados pelo algoritmo de vetor de distância, em 1979, a ARPANET deixou de lado este algoritmo para utilizar um algoritmo completamente novo, o algoritmo de estado de enlace (TANEMBAUM, 2003).

¹ Disponível em (<https://tools.ietf.org/html/rfc1058>).

Então, neste algoritmo de estado de enlace existe a necessidade de que a topologia da rede e todos os custos de enlace estejam disponíveis como dados para o algoritmo executar. Isto é possível fazendo com que cada nó transmita as identidades e os custos dos enlaces anexados a ele a todos os outros roteadores da rede, atividade que é executada através de uma transmissão broadcast do estado de enlace (KUROSE e ROSS, 2003).

O resultado desta transmissão broadcast é que todos os nós tem uma visão idêntica e completa da rede. Assim cada nó pode executar o algoritmo e calcular o mesmo conjunto de caminhos de menor custo para todos os outros nós.

A ideia desse algoritmo, segundo Tanenbaum (2003, pág. 383), pode ser estabelecida em cinco partes:

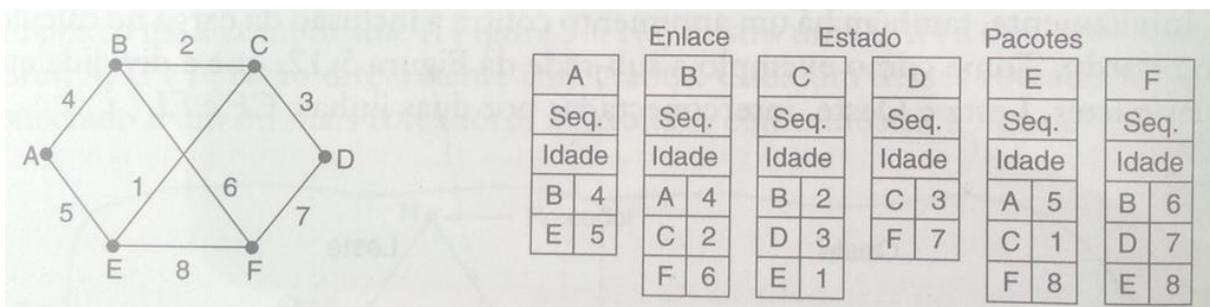
1. Descobrir seus vizinhos e aprender seus endereços de rede.
2. Medir o retardo ou o custo até cada um de seus vizinhos.
3. Criar um pacote que informe tudo o que ele acabou de aprender.
4. Enviar esse pacote a todos os outros roteadores.
5. Calcular o caminho mais curto até cada um dos outros roteadores.

A etapa 1 acima resume-se em aprender seus vizinhos, que é alcançado através de pacotes de HELLO especial em cada linha ponto a ponto, buscando os nomes globalmente exclusivos.

A etapa 2 resume-se a definir os custos de cada um dos vizinhos que pode ser utilizado o retardo, a carga ou a largura de banda do enlace.

Na etapa 3 com as informações necessárias de posse, o roteador cria um pacote com todos os dados. Este pacote deverá ter no mínimo: a identidade do transmissor, um número de sequência, a idade e uma lista de vizinhos com seus respectivos custos, conforme demonstrado na figura 2.1. Após isto, é só determinar quando cria-los, periodicamente ou na ocorrência de algum evento a algum vizinho.

Figura 2.1: Modelo do pacote de estado de enlace.



Fonte: TANEMBAUM, 2003, p. 386.

A etapa 4 trata da distribuição dos pacotes de estado de enlace, parte considerada complicada neste algoritmo. A ideia fundamental é usar um algoritmo de inundação para distribuir estes pacotes. Para controlar esta distribuição são utilizados os dados número de sequência e idade do pacote de estado de enlace. Eles são comparados em cada nó para evitar duplicidade ou utilização de informações antigas, o que pode gerar problemas de inconsistências e loops de roteamento.

Já a quinta parte trata do cálculo das novas rotas que agora com os dados de todos os nós, poderá criar um grafo da rede completo, pois todo enlace estará representado. Então, o algoritmo de estado de enlace utiliza o algoritmo de Dijkstra para criar o caminho mais curto até todos os destinos possíveis. O resultado da execução desse algoritmo pode ser instalado na tabela de roteamento e a operação normal ser continuada (TANEMBAUM, 2003).

O algoritmo de estado de enlace devido ao uso do algoritmo de Dijkstra tende a tornar-se complexo, diante das interações possíveis. Para uma grande rede com N roteadores, cada qual com K vizinhos serão necessários armazenar dados proporcionais a KN. Sendo que a ordem de complexidade da implementação será de N^2 , segundo Kurose e Ross (2003).

Portanto, o algoritmo de estado de enlace como mostra Tanenbaum (2003), é também muito utilizado por protocolos na Internet. Entre os protocolos que usam o algoritmo de estado de enlace, cabe citar o OSPF (Open Shortest Path First) e o IS-IS (Intermediate System- Intermediate System). O IS-IS é mais antigo que OSPF, portanto, herdou muitas características dele.

- Roteamento hierárquico

O estudo até aqui é simplista ao achar que todos os roteadores são idênticos e todas as redes executam o mesmo algoritmo de roteamento. Como as redes tendem a crescer, dois problemas ficam evidentes, a escala e a autonomia administrativa destas redes.

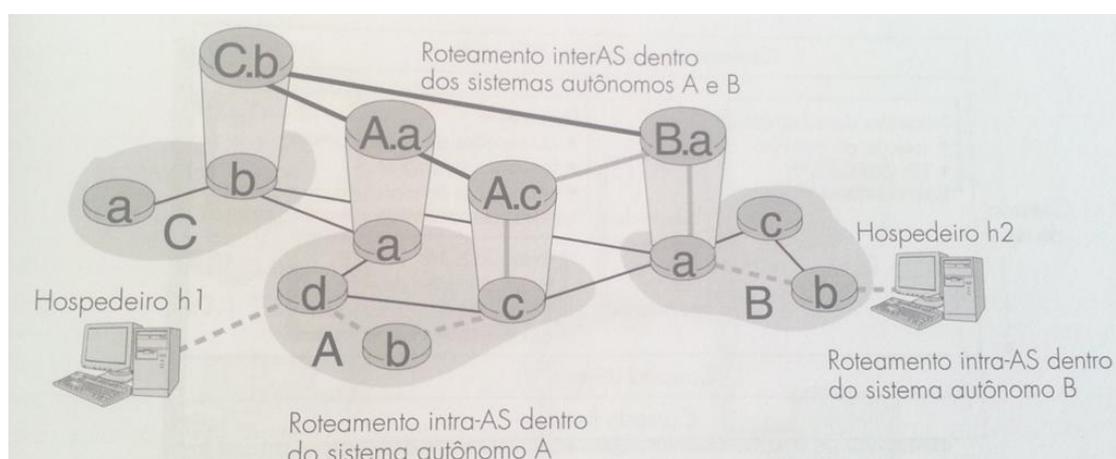
A problemática da escala é que com o aumento de roteadores em uma rede o aumento da sobrecarga de cálculo, armazenamento e comunicação de informações para tabela de roteamento tende a se tornar proibitiva, com milhões de rotas.

Já a autonomia administrativa, leva em conta a questão de a organização poder administrar sua rede de forma autônoma, executando e definindo seus parâmetros e políticas.

Então para resolver estes problemas foi criado o conceito de sistemas autônomos - autonomous systems (AS), que é um agrupamento de roteadores por regiões.

Dentro de um AS, todos os roteadores rodam o mesmo protocolo de roteamento e são chamados de protocolo de roteamento intra-AS ou IGP (Interior Gateway Protocol). Entretanto, um roteador chamado de roteador de borda que executam o protocolo de roteamento inter-AS ou EGP (Exterior Gateway Protocol), que determina os caminhos entre os AS. Isto garante que os AS possam conversar de forma hierárquica assim como na rede telefônica. A figura 2.2 mostra a dinâmica do roteamento hierárquico através dos AS. Onde cada tipo de protocolo de roteamento tem sua ação, como o protocolo EGP nos roteadores A.a, B.a e C.b.

Figura 2.2: Dinâmica do roteamento hierárquico.



Fonte: KUROSE E ROSS, 2003, p. 235.

Um exemplo de protocolo de roteamento inter-AS é o BGP, especificado na RFC 1771², 1772³ e 1773⁴. Hoje não sua versão 4 é o protocolo utilizado como inter-AS na Internet.

² Disponível em (<https://tools.ietf.org/html/rfc1771>).

³ Disponível em (<https://tools.ietf.org/html/rfc1772>).

⁴ Disponível em (<https://tools.ietf.org/html/rfc1773>).

Já o protocolo de roteamento intra-AS, tem três protocolos utilizados extensivamente dentro de AS na Internet. São eles, o RIP, OSPF, EIGRP (Enhanced Interior Gateway Routing Protocol) de propriedade da empresa Cisco.

Portanto, vale ressaltar, que o objetivo aqui não é detalhar os conceitos dos protocolos de roteamento da Internet na sua totalidade. O foco será dado a seguir no protocolo de roteamento OSPF visto ser o objeto de estudo para a Rede UFMA.

2.2 Protocolo OSPF

O OSPF (Open Short Path First) é um protocolo de roteamento utilizado no interior de sistemas autônomos, IGP, para troca de informações de rotas dos pacotes IP. Ele surgiu em substituição ao protocolo RIP devido suas limitações e em 1990 tornou-se um padrão da Internet Engineering Task Force (TANEMBAUM, 2003).

O uso “open” em sua nomenclatura é devido suas especificações estarem disponíveis ao público, através da RFC 2328⁵, que é a versão 2 do OSPF. Já existe a versão 3, RFC 5340⁶, que atende aos requisitos de IPv6. Também uma extensão para roteamento multicast, o MOSPF (Multicast OSPF), RFC 1584⁷.

Ele é um protocolo de estado de enlace, isto é, os roteadores rodando este protocolo trocam, entre si, informações sobre os estados dos enlaces de comunicação ligados às suas portas. Utiliza a inundação para troca de informações sobre o estado dos enlaces e o algoritmo de caminho de menor custo é o Shortest Path First (SPF) ou Dijkstra. Onde um roteador envia a todos os roteadores do AS informações de roteamento e não somente a seus vizinhos. (KUROSE e ROSS, 2003).

A seguir, de acordo com Thomas (2003), serão apresentadas vantagens e funcionalidades do protocolo. Por fim, a descrição dos subprotocolos que fazem parte do OSPF.

Cabe ressaltar que este trabalho apresenta apenas a versão 2 do protocolo OSPF e não trata da sua versão 3 e do MOSPF.

⁵ Disponível em (<https://tools.ietf.org/html/rfc2328>).

⁶ Disponível em (<https://tools.ietf.org/html/rfc5340>).

⁷ Disponível em (<https://tools.ietf.org/html/rfc1584>).

2.2.1 Vantagens do OSPF

A seguir serão apresentadas as principais vantagens do protocolo OSPF e que fazem com que ele seja tão utilizado como IGP na Internet.

- Fazer a convergência de maneira rápida e sem loops.

Ou seja, após a falha de um enlace, os melhores caminhos para determinados destinos mudam. Leva algum tempo para qualquer protocolo de roteamento encontrar os novos melhores caminhos. Enquanto isso acontece, os caminhos utilizados, às vezes são de qualidade inferior ou estão inutilizáveis. Este processo de encontrar o novo caminho é chamado de convergência.

- Utilizar métricas como caminho de maior vazão ou caminho com maior confiabilidade no cálculo do caminho mínimo.

Para o OSPF calcular o caminho mínimo ele precisa conhecer a topologia da rede, sendo assim, é possível utilizar diversas métricas no cálculo do caminho mínimo.

- O diâmetro da rede não é limitado a contagem de saltos por roteadores.

O protocolo RIP usa a contagem de saltos como métrica de roteamento, e o custo de um caminho pode variar entre 1 e 15. Isto limita o diâmetro da rede, porém o OSPF pode ser utilizado em grandes redes.

- Oferece a possibilidade de ter caminhos múltiplos de igual custo.

Uma maneira de aumentar a eficiência do protocolo OSPF é dividir o tráfego entre os diversos caminhos de mesmo custo. Assim não é preciso escolher um único caminho.

- Balanceamento de carga.

Do desdobramento de usar múltiplos caminhos surge outra vantagem, balanceamento de carga. Caso um único caminho utilizado se tornar indisponível, o tráfego será redirecionado através do outro caminho alternativo. Apenas uma parte do tráfego terá de ser redirecionada após a falha de um enlace. Para conexões TCP, os pacotes relacionados a uma determinada conexão sempre serão enviados por um único caminho.

- Tratamento de rotas internas e externas de forma mais precisa.

O protocolo OSPF consegue calcular caminhos para roteadores externos de maneira mais simples e utilizando métricas mais precisas. No OSPF as informações

de roteamento externo são rotuladas e são substituídas por informação de roteamento interno. Então, quando há apenas um roteador de saída para o mundo externo, os protocolos vetor distância e estado de enlace, se comportam de maneira semelhante, basta anunciar um caminho padrão para esse roteador. Porém quando é preciso escolher entre vários roteadores ou entre vários prestadores de serviços, a solução de anunciar uma rota padrão não é muito eficiente.

- Uso de hierarquia dentro de um AS.

Com o uso do conceito de áreas, ele pode estruturar hierarquicamente um domínio de roteamento, dividindo agrupamentos de roteadores. O benefício da hierarquia traz muitas vantagens como foi visto no assunto algoritmo de roteamento hierárquico da seção “Principais algoritmos de roteamento”.

- Diminuir a largura de banda utilizada pelas mensagens de controle do protocolo.

Com o advento das áreas, o OSPF consegue diminuir a troca de mensagens entre os roteadores visando uma otimização da banda consumida para controle do protocolo.

- Suporte integrado para roteamento unicast e multicast.

Através de uma simples extensão ao OSPF foi possível tratar o roteamento multicast.

- Requisitos de segurança.

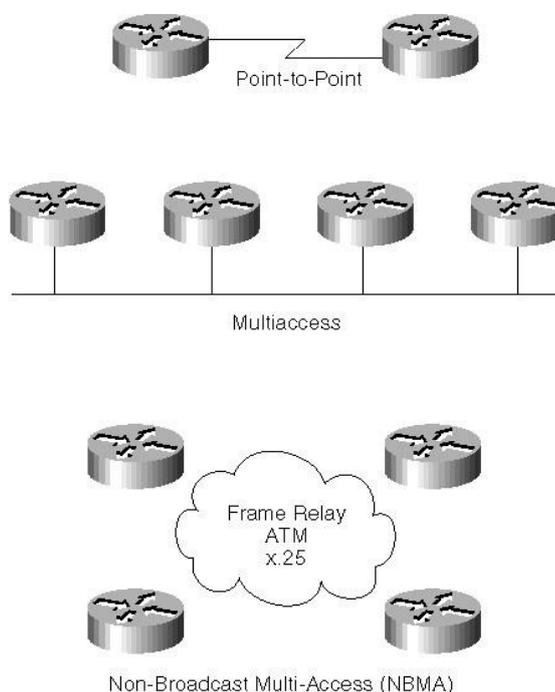
Todas as trocas de informações entre roteadores de um domínio são certificadas. Isto evita que intrusos mal-intencionados injetem informações incorretas na tabela de roteamento.

2.2.2 Funcionamento geral

O protocolo OSPF foi desenvolvido para diferenciar hosts e roteadores, redes com capacidade de multiacesso, redes sem capacidade de multiacesso e dividir redes muito grandes em áreas. Assim o OSPF é compatível com 3 tipos de conexões e redes, conforme demonstrado na figura 2.3:

1. Linhas ponto a ponto ou Point-to-Point entre dois roteadores;
2. Redes de multiacesso com difusão (broadcast) ou Multiaccess, por exemplo uma rede Ethernet;
3. Redes de multiacesso sem difusão (broadcast) ou Nonbroadcast Multiaccess (NBMA), por exemplo redes Frame Relay e X.25.

Figura 2.3: Tipos de rede compatíveis com o OSPF.



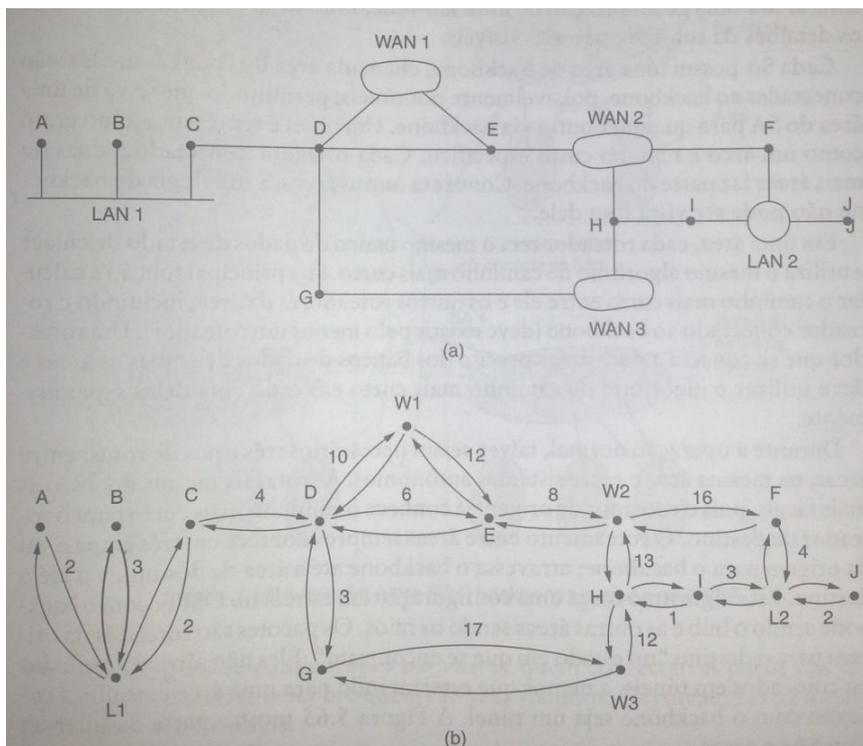
Fonte: THOMAS, 2003, p. 150.

Os hosts ou computadores em geral estão conectados à Internet através de um roteador. Se aplicado o modelo do estado de enlace, as relações entre cada host e o roteador devem ser inseridas na representação local da topologia, descrita em um grafo conforme mostra a figura 2.4, onde temos a representação dos tipos de rede que o OSPF suporta.

O protocolo OSPF permite uma simplificação, pois todos os hosts da rede Ethernet pertencem a uma única subrede. Sendo assim, é suficiente anunciar um enlace entre o roteador e a rede, neste caso chamada de subrede, onde na figura 2.4(b) a LAN 1 e LAN 2 são representados no grafo por L1 e L2.

O enlace para um roteador vizinho é identificado pelo endereço IP do vizinho. De maneira semelhante, o enlace para uma subrede é identificado pelo endereço da rede ou subrede.

Figura 2.4: Grafo da topologia de redes suportadas pelo OSPF.



Fonte: TANEMBAUM, 2003, p. 485.

Para que estes roteadores dentro do domínio OSPF possam existir é necessário que eles possuam uma identificação única na rede, o Router Identification (Router ID). O Router ID é um número de 32 bits único que identifica cada roteador dentro de um AS. Assim, através do Router ID, cada roteador poderá estabelecer vizinhança com os outros roteadores do AS, conhecer quem são os roteadores daquele domínio OSPF.

Então, após o OSPF descobrir seus vizinhos ele passa a formar adjacências. Adjacências são formadas para garantir a troca de informações de roteamento, porém nem todos os vizinhos formarão adjacência. Para isto acontecer será necessário ocorrer alguma destas condições: a rede ser ponto a ponto, o roteador ser um DR, o vizinho ser um roteador DR, o roteador ser um BDR e o vizinho ser um roteador BDR.

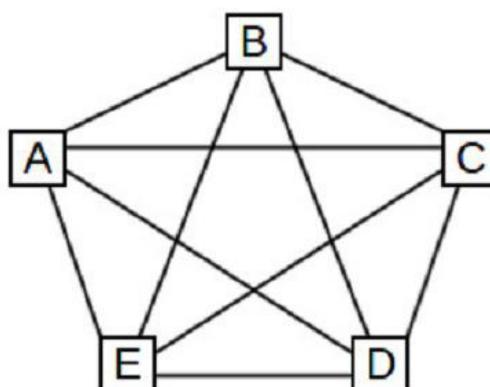
Diante disto, as redes com capacidade de Multiaccess apresentam duas características peculiares que precisam ser estudadas:

1. A primeira é que qualquer roteador pode enviar um pacote para qualquer outro roteador.

2. A segunda é que o pacote é recebido por todos os roteadores dentro da rede.

Desta forma, estas características causam um problema. Dados N roteadores na rede local, existe um total de $N(N - 1)/2$ enlaces entre estes roteadores. Então, cada roteador pode anunciar $N - 1$ enlaces para os outros roteadores, mais um enlace para os hosts da rede. Levando em conta todos os roteadores o total é da ordem de $O(N^2)$ adjacências. Um aumento considerável de adjacências que pode gerar uma grande quantidade de troca de informações. A Figura 2.5 mostra uma rede multiaccess com cinco roteadores na qual cada roteador estabelece adjacência com todos os roteadores, contudo, imaginar esta rede maior pode tornar a situação da rede insustentável.

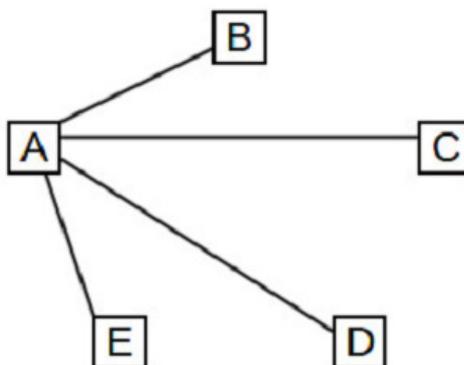
Figura 2.5: Possíveis adjacências em uma rede com capacidade Multiaccess.



Entretanto, o protocolo OSPF reduz este número para a ordem de somente $O(N)$ adjacências ao eleger um dos roteadores como roteador designado ou Designated Router (DR). Os demais roteadores estabelecem adjacências somente com o DR.

A Figura 2.6 mostra como se apresenta a mesma rede da figura 2.5 na qual o roteador "A" é eleito como DR e deve manter adjacência com os outros roteadores. Além disso, buscando uma garantia de redundância destas adjacências, um roteador reserva é eleito também juntamente com o DR e é chamado de roteador designado de reserva ou Backup Designated Router (BDR). O BDR é mantido atualizado para caso o DR falhe, ele será utilizado para substituí-lo de imediato.

Figura 2.6: Adjacências estabelecidas com o roteador “A”.



Logo os roteadores também devem estabelecer adjacência com o BDR. Neste caso cada roteador estabelece adjacências, com o DR e com o BDR. Com exceção dos roteadores DR e BDR que devem estabelecer adjacências com todos os roteadores da rede.

Este procedimento de utilizar um DR reduz a quantidade de tráfego utilizado pelas mensagens de controle do protocolo. Além disso, diminui o tamanho da representação da topologia que guarda os estados dos enlaces da rede. O protocolo OSPF aplica este mesmo gerenciamento para redes Multiaccess e redes NBMA.

Então as informações de roteamento são trocadas apenas com estes dois roteadores, DR e BDR. Assim, caminhos virtuais podem ser estabelecidos entre qualquer par de roteadores e os pacotes são transmitidos diretamente sobre estes caminhos virtuais, entretanto, estes caminhos são estabelecidos apenas sob demanda. Os únicos caminhos que serão usados permanentemente pelas atualizações de roteamento são os que ligam os roteadores com o DR e o BDR.

Outra característica interessante, é que o protocolo OSPF permite que diversas redes adjacentes sejam agrupadas. Cada grupo de redes adjacentes, em conjunto com os enlaces entre os roteadores pertencentes ao grupo, é chamado de área. Estas áreas no OSPF são numeradas de modo a individualizá-las.

Cada área executa uma cópia separada do protocolo de roteamento OSPF. Isto significa que cada área tem sua própria representação local da topologia, descrita por um grafo. A topologia de uma área é invisível para as demais áreas. Este isolamento permite reduzir o tráfego das mensagens do protocolo de roteamento.

Com a introdução de áreas, as representações da topologia nos roteadores deixam de ser idênticas. Cada roteador tem um grafo separado para cada área em que está conectado. Dois roteadores pertencentes a mesma área têm as representações da topologia desta área idênticas.

Assim cada AS possui uma área chamada backbone, que possui a numeração de área 0. Todas as demais áreas estão conectadas ao backbone, fazendo com que uma determinada área vá até outra dentro do AS via backbone como se ela fosse um hub. A topologia da área 0, assim como as demais não são vista fora dela. A principal função desta área é rotear o tráfego entre as áreas do AS.

O roteamento em um AS ocorre em dois níveis, dependendo da origem e o destino de um pacote, pertencem a diferentes áreas ou a mesma área. No roteamento dentro de uma área, o pacote é encaminhado utilizando apenas informações obtidas na área. Isso impede que os roteadores de uma determinada área influenciem de maneira nociva o roteamento das demais áreas.

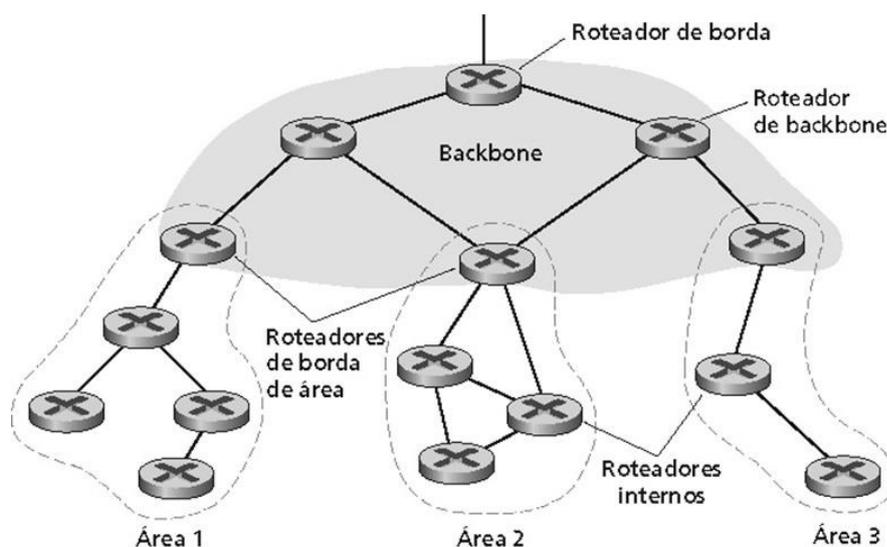
Sendo assim, numa operação normal, podem existir três tipos de rotas. Na mesma área, onde os roteadores já conhecem o caminho mais curto. Entre áreas, onde vão da origem para o backbone, do backbone ao destino e enfim ao destino. Entre AS, onde a origem deseja sair do AS de origem indo até um outro AS.

Devido esta dinâmica das rotas o posicionamento do roteador no OSPF para uma AS é distinguido em quatro classes:

1. Roteadores Internos ou Internal Routers (IR), que ficam inteiramente em uma área.
2. Roteadores de borda de área ou Area Border Routers (ABR), que conectam duas ou mais áreas.
3. Roteadores de backbone ou Backbone Routers (BR), ficam na área backbone.
4. Roteadores de fronteira de AS ou Autonomous System Border Routers (ASBR), interagem com roteadores de outro AS.

Essas classes podem se sobrepor. Por exemplo, um roteador de backbone que faz parte apenas da área 0, é considerado também um roteador interno. Isto é observado na figura 2.7 que mostra os conceitos de áreas, suas conexões e o posicionamento dos roteadores em um domínio OSPF.

Figura 2.7: Áreas e roteadores no OSPF.



Fonte: KUROSE E ROSS, 2003, p. 256.

2.2.3 Protocolos internos do OSPF

O protocolo OSPF tem suas atividades exercidas no protocolo IP e é composto de três subprotocolos: Hello, Exchange e Flooding, que serão descritos a seguir, baseado em Thomas (2003). Todos os subprotocolos possuem o cabeçalho padronizado de 24 bytes, conforme figura 2.8. O cabeçalho não será detalhado por ser composto por campos com conceitos já discutidos.

Por conta da sua estrutura e dos seus subprotocolos existem cinco tipos de pacotes OSPF, conforme figura 2.9, que detalha os tipos e as suas funções de forma resumida. Entretanto, cabe ressaltar que todos eles têm o cabeçalho padrão mostrado na figura 2.8.

Figura 2.8: Cabeçalho padrão dos subprotocolos OSPF.

Version #	Type	Packet length
Router ID		
Area ID		
Checksum	AuType	
Authentication		
Authentication		

Fonte: THOMAS, 2003, p. 156.

Figura 2.9: Tipos de pacotes originados no protocolo OSPF.

Tipo	Nome do pacote	Descrição
1	Hello	Descobre os vizinhos e cria adjacências entre eles
2	Descrição de banco de dados (DBD)	Verificações para a sincronização de banco de dados entre os roteadores
3	Solicitação de estado de link (LSR)	Registros específicos de estado de link de roteador para roteador
4	Atualização de estado do link (LSU)	Envia registro de estado de link especificamente solicitados
5	Reconhecimento de estado de link (LSAck)	Reconhece os outros tipos de pacotes

Fonte: THOMAS, 2003, p. 155.

- O Protocolo Hello

O protocolo Hello é utilizado para dois propósitos. Verificar o estado dos enlaces e eleger um DR e um BDR. Para isso, pacotes denominados hello são enviados pelos roteadores a cada hello-interval segundos. Os pacotes incluem o endereço do DR, ou 0 se ainda não houver DR, e o endereço do BDR ou 0. Além disso, também incluem uma lista de todos os vizinhos dos quais um pacote hello foi recebido nos últimos dead-interval segundos. Ambos os intervalos hello-interval e dead-interval são parâmetros dos enlaces que são configurados pelo administrador da rede.

A ligação entre dois roteadores é dita operacional se os pacotes podem fluir em ambas as direções. A conectividade bidirecional é identificada pela lista de roteadores conhecidos por um roteador vizinho. Se o identificador do roteador local não estiver listado nos pacotes hello enviados pelos roteadores vizinhos, isso significa que eles ainda não receberam os pacotes hello enviados pelo roteador local. O enlace é então declarado de sentido único e não pode ser usado para o roteamento. Se o roteador local está listado nos pacotes hello dos roteadores vizinhos, então o enlace é bidirecional.

Depois de estabelecer uma conexão bidirecional, os roteadores começam a determinar suas adjacências e para tal, é preciso selecionar o DR e BDR. O processo de eleição usa o campo de prioridade presente nos pacotes hello. Cada roteador é configurado com uma prioridade, que varia entre 0 e 255. Como resultado

da eleição é selecionado o roteador com a maior prioridade. Se o roteador de maior prioridade ficar inativo, outro será selecionado; esta seleção permanecerá mesmo depois do roteador de maior prioridade se tornar ativo novamente. Roteadores com prioridade zero, nunca serão selecionados como DR.

Imediatamente após os enlaces se tornarem ativos, o roteador permanece em um estado de espera durante um intervalo igual ao dead-interval. Durante este intervalo, o roteador irá transmitir pacotes de hello, mas não vai se candidatar a DR ou BDR.

Ele irá receber pacotes hello e inicializar os identificadores dos DR e BDR da seguinte forma. Para cada vizinho, o roteador guarda a prioridade do vizinho e o estado do enlace. Além disso, ele guarda se o vizinho se candidata como DR ou BDR. Se um ou vários vizinhos se candidatam como BDR, aquele com maior prioridade é selecionado; e em caso de empate, o roteador com o maior identificador é selecionado. Se nenhum vizinho se candidata a BDR, o vizinho com a maior prioridade é selecionado ou, em caso de empate, aquele com o maior identificador.

Se um ou vários vizinhos se candidatam a DR, aquele com a maior prioridade é selecionado como DR. Em caso de empate, o roteador com o maior identificador é selecionado. Se nenhum vizinho se candidata a DR, o BDR é promovido. Um roteador não pode se candidatar a ambos DR e BDR. Assim, se for preciso promover o BDR para DR, também será necessário eleger um novo roteador reserva.

Assim, pode-se concluir que a operação básica do protocolo Hello é:

1. Um roteador OSPF envia pacotes hello via broadcast;
2. O pacote hello é recebido pelo novo roteador OSPF;
3. Este novo roteador OSPF responde com seu próprio pacote hello.

- O Protocolo Exchange

Quando dois roteadores estabelecem conectividade bidirecional, eles devem sincronizar sua representação local da topologia da rede. Em redes multiaccess, isso ocorre entre os roteadores e o DR ou o BDR. A sincronização inicial é realizada através do protocolo Exchange. O protocolo Flooding, em seguida, é responsável por manter as representações da topologia da rede sincronizadas.

É importante notar que o protocolo Exchange é assimétrico. A primeira etapa do protocolo tem a função de selecionar um mestre e um escravo. Depois de

concordar sobre esses papéis, os dois roteadores trocam a descrição de seus grafos ou banco de dados de estado de enlaces, que representam a topologia da rede. Cada um irá listar os enlaces que serão requisitados em seguida. Estas informações serão trocadas através do pacote do protocolo Exchange.

No pacote utilizado pelo protocolo Exchange existem três bits utilizados para controle: I (Inicializa), M (Mais) e MS (Mestre-Escravo). O roteador que pretende iniciar o procedimento de sincronização envia um pacote vazio, com os bits I, M e MS definidos como 1 e o contador definido para um valor arbitrário, não visto anteriormente pelo outro roteador.

O outro roteador concorda em fazer a função de escravo durante a sincronização enviando um pacote igual ao que foi recebido, porém com o bit MS definido como 0. Uma vez que os papéis foram distribuídos, o mestre irá enviar a descrição dos enlaces presentes na representação local da topologia em uma sequência de pacotes, nos quais o bit I será definido como 0, o bit MS definido como 1 e o bit M definido como 1, exceto para o último pacote.

Os pacotes têm sequência numerada e devem ser enviados um de cada vez. Depois de cada pacote ser enviado, o escravo irá enviar uma confirmação de que recebeu o pacote. Os pacotes de confirmação contêm a descrição dos enlaces presentes na representação local da topologia do roteador escravo. Se a confirmação não for recebida dentro do intervalo de retransmissão, o mestre retransmite o seu pacote. Quando o escravo recebe um pacote com o valor do contador igual ao valor do pacote anterior, deve retransmitir o último pacote de confirmação. Quando o mestre transmite sua última descrição dos enlaces, ele vai definir o bit M como 0. Se o escravo ainda tem descrições de enlaces para transmitir, ele irá enviar uma confirmação com o bit M definido como 1. O mestre continuará enviando pacotes de descrição vazios com o bit M definido como 0. Como consequência, continuará aceitando confirmações, até que eventualmente receba uma confirmação com o bit M definido como 0. Nesse ponto a primeira etapa da sincronização está completa.

Durante a sincronização, o mestre e o escravo processam as descrições dos estados de enlace que se encontram nos pacotes e nas confirmações. Primeiro verificam se não há um enlace com a mesma descrição na representação local da topologia. Além disso, verificam, através do valor de um contador, se esse enlace não está desatualizado. Se alguma das condições for falsa, os roteadores devem

colocar a descrição do enlace em uma lista de enlaces pendentes. Na segunda etapa da sincronização, os roteadores irão solicitar informações dos enlaces pendentes. Após receber uma solicitação, cada roteador deve enviar um ou mais pacotes contendo um conjunto de atualizações de estado de enlace.

A transmissão destes pacotes utiliza exatamente os mesmos procedimentos do protocolo Flooding descrito a seguir.

- O Protocolo Flooding

Quando um enlace muda de estado (uma interface do roteador fica inativa), o roteador responsável por esse enlace vai transmitir uma nova versão do estado do enlace. Para cada enlace, o contador é comparado com o valor na representação local da topologia. Se o valor do contador indicar que o enlace presente na mensagem recebida é novo, então a mensagem recebida deve ser retransmitida em todas as interfaces. Em qualquer caso, o roteador que enviou a mensagem deve aguardar uma confirmação de recebimento.

Para tornar o protocolo Flooding confiável, o roteador deve retransmitir suas atualizações em intervalos regulares até que receba a confirmação. Cada pacote de confirmação pode ser responsável por informar o recebimento de uma ou mais mensagens, com informações de estado de enlace. Portanto é normal atrasar a sua transmissão, a fim de agrupar a confirmação de recebimento do estado de vários enlaces, em um único pacote. Este atraso deve ser curto, a fim de evitar retransmissões desnecessárias.

Por conta deste comportamento do protocolo Flooding, nascem os anúncios de estado de enlace ou Link-State Advertisement (LSA). Os LSA são pacotes que o OSPF utiliza para anunciar sempre que houver uma mudança de estado de enlace para outro roteador.

Então o pacote OSPF do tipo 4, chamado de LSU é o responsável pela atualização do banco de dados do estado de enlace ou Link-State Database (LSDB) de um outro roteador e que ajuda a manter a tabela de roteamento do roteador atualizada. Um pacote LSU é composto de um ou mais LSA. A figura 2.10 mostra os tipos LSA que o protocolo OSPF possui.

Figura 2.10: Tipos de LSA no protocolo OSPF.

Tipo de LSA	Descrição
1	LSAs do roteador
2	LSAs de rede
3 ou 4	LSAs de resumo
5	Sistema autônomo de LSAs externos

Fonte: THOMAS, 2003, p. 157.

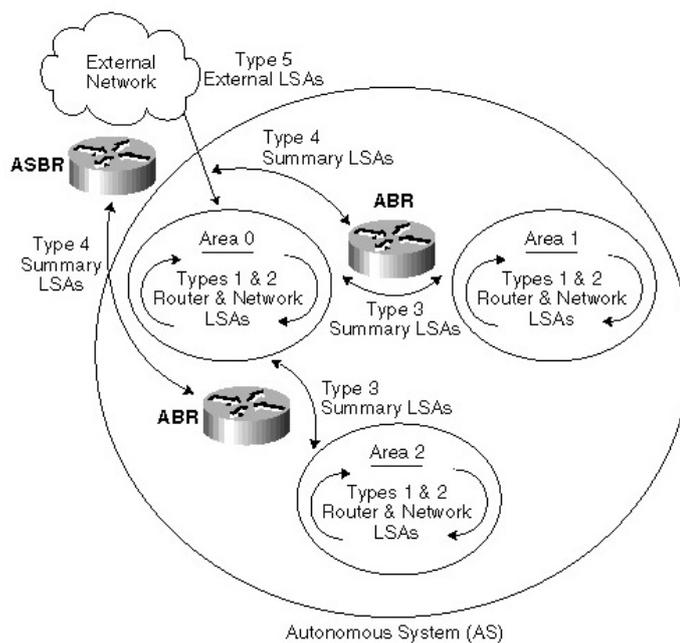
O LSA do tipo 1 são gerados por cada roteador para cada área a que pertencem e inclui a lista de links conectados diretamente. Ficam apenas dentro da área que pertencem. Já os LSA do tipo 2, são gerados pelo DR e descrevem um conjunto de roteadores ligados a uma rede em particular. Ficam apenas dentro da área que pertencem.

O LSA do tipo 3, são gerados pelo ABR e descrevem as rotas inter-áreas existentes. Chegam até outras áreas para divulgar as rotas. Já os LSA do tipo 4, são gerados pelo ABR e descrevem enlaces para ASBR existentes. Chegam até outras áreas para divulgar as rotas.

O LSA do tipo 5, são gerados pelo ASBR e descrevem as rotas para destinos externos ao AS.

A figura 2.11 demonstra a dinâmica dos tipos de LSA através das áreas e AS de modo que as rotas são mantidas atualizadas nas tabelas de roteamento.

Figura 2.11: Comportamentos dos tipos de LSA.



Fonte: THOMAS, 2003, p. 158.

3. A REDE DE COMPUTADORES DA UFMA

Neste capítulo será apresentada a Rede UFMA, como é chamada dentro universidade pela unidade gestora da rede, o NTI. Todas as informações presente aqui foram apresentadas pelo próprio NTI.

3.1 A Rede UFMA

A Rede UFMA foi criada em meados de 1993 por conta da reunião da SBPC que foi realizada na UFMA no ano seguinte. Ela foi implantada e é administrada pelo Núcleo de Tecnologia da Informação (NTI). Durante os anos que sucederam sua implantação ela passou por diversas atualizações tecnológicas e ampliações estruturais que a tornaram uma grande rede de computadores.

Sua estrutura é composta pelo campus do Bacanga (São Luís) e sua capilaridade se estende para o interior do Estado do Maranhão para atender os campi de Imperatriz, Chapadinha, Pinheiro, Codó, Bacabal, Grajáú, São Bernardo e Balsas. Ainda dentro da cidade de São Luís, possui 11 unidades de ensino, o que a torna de dimensões metropolitanas e estaduais.

Estas condições de espalhamento geográfico fizeram com que a rede UFMA, na cidade de São Luís, fosse transformada em uma Metropolitan Area Network (MAN⁸), no momento que interconecta a LAN das unidades dentro da cidade de São Luís até o campus Bacanga através de uma estrutura de fibras ópticas. Esta MAN garante que os serviços sejam disponibilizados também para estes locais em alta velocidade.

Outro fator que se desenrola deste espalhamento é a conexão dos campi do interior do Estado a rede UFMA. Isto traz uma realidade de rede Wide Area Network (WAN⁹) que aumenta a complexidade da rede ao utilizar outras tecnologia de conexão de longa distância através de operadoras de serviços de conectividade.

A rede, com exceção das conectividades do interior que utilizam tecnologias próprias das operadoras, utiliza a tecnologia de LAN chamada Ethernet. Esta tecnologia permite que a LAN tenha grande velocidade de acesso.

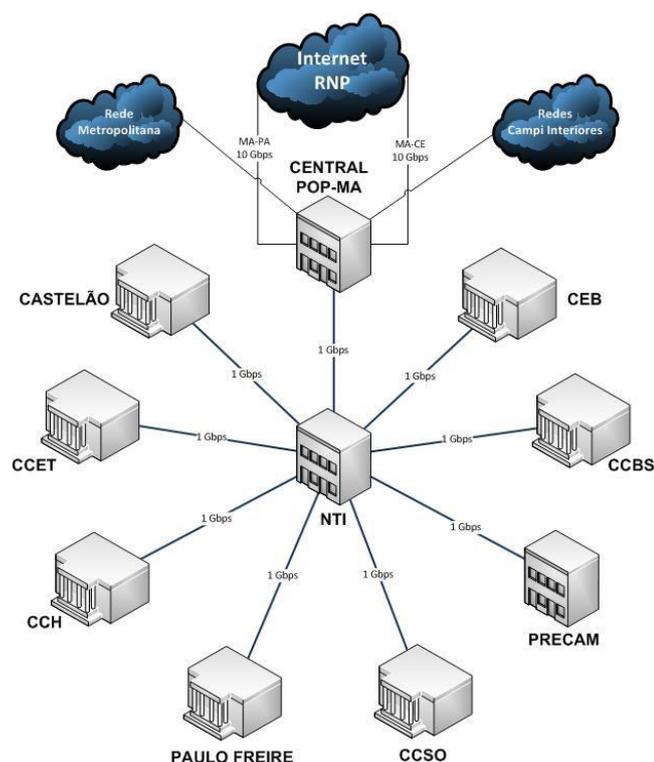
⁸ Um MAN é uma rede que cobre toda ou parte de um cidade, interligando LANs em alta velocidade (COELHO, 2003).

⁹ Uma WAN é uma rede de longa distância que interligam redes em municípios, estados e países. Normalmente, utilizam vários tipos de tecnologias de rede como LAN e MAN (COELHO, 2003).

Atualmente a Rede UFMA encontra-se como retratada na figura 3.1. Como mostrado, os principais prédios administrativos e acadêmicos da universidade estão ligados ao NTI através de conexões de 1 Gbps através de fibras ópticas. Dentro dos prédios as localidades e setores são ligadas a um equipamento de concentração também a 1 Gbps através de fibras ópticas ou cabo metálico. Então, cada principal prédio é responsável pela distribuição interna das conectividades e da ligação com o NTI.

O NTI, então, é responsável pelo provimento dos principais serviços de rede, sistemas de gestão da universidade e pela manutenção das conectividades da rede. Diante destas responsabilidades o NTI é o local chamado de centro de dados ou Data Center da UFMA.

Figura 3.1: A Rede UFMA.



As conexões dos usuários a Rede UFMA são feitas a velocidade de 100Mbps em algumas localidades e em outras a 1 Gbps. Entretanto, a capilaridade destas conexões é bem vasta dentro da universidade.

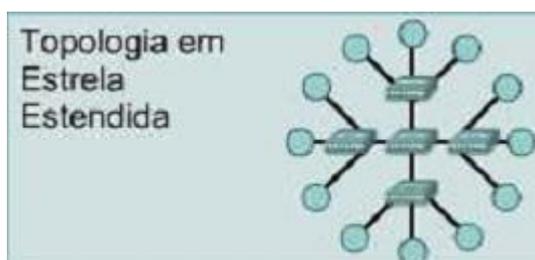
Outro local importante na rede a ser observado é o prédio da Central Telefônica, onde as conexões da Rede Metropolitana, dos campi dos interiores e a saída para Internet estão chegando. A conexão com a Internet é provida pela Rede

Nacional de Ensino e Pesquisa (RNP), que é responsável pelo backbone nacional acadêmico que interliga todos os centros de pesquisas e instituições de ensino superior do Brasil.

Como mostrado na figura 3.1, esta conexão a Internet é redundante pelo Pará e Ceará com 10 Gbps. Isto garante uma maior disponibilidade para uso da Internet pela UFMA.

A Rede UFMA está projetada por uma topologia física baseada em estrela estendida, onde os equipamentos de conexão se interligam formando várias estrelas interligadas, conforme figura 3.2. Uma vantagem desta topologia é a possibilidade da formação de hierarquia de acesso.

Figura 3.2: Topologia física de estrela estendida.



Esta estruturação em topologia hierárquica garante um projeto em três camadas: núcleo, distribuição e acesso. Cada camada exerce funções bem definidas de modo que a rede torne-se segmentada, facilmente expansível e de melhor administração. A figura 3.3 demonstra as camadas nesta topologia e a figura 3.4 demonstra um exemplo real desta topologia.

Figura 3.3: Camadas da topologia hierárquica.

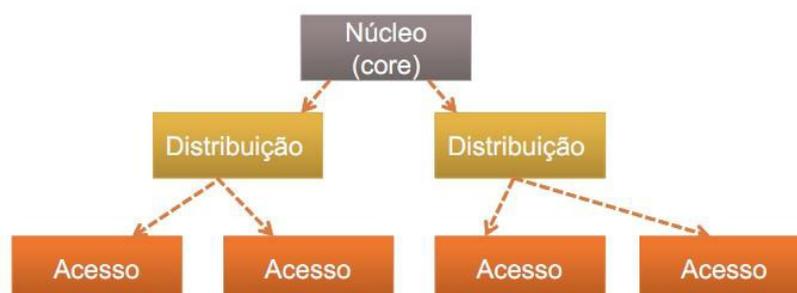
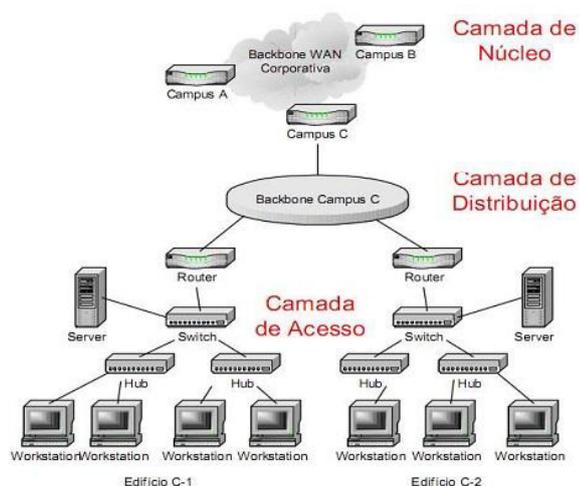
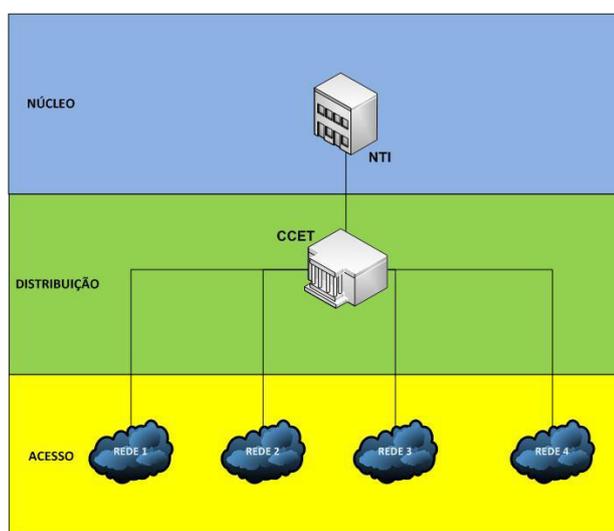


Figura 3.4: Exemplo real de topologia hierárquica.



A Rede UFMA dentro da proposta de hierarquia pode ser vista como demonstra a figura 3.5. As redes de acesso onde os usuários tem conectividade a rede, ficam ligadas ao equipamento de concentração do prédio CCET e consequentemente ligados ao NTI.

Figura 3.5: Camadas da topologia hierárquica na Rede UFMA.



Com relação a topologia lógica, a Rede UFMA utiliza o protocolo de roteamento OSPF para garantir o encaminhamento dos pacotes dentro da rede.

Com esta topologia hierárquica atual trabalhar os conceitos do protocolo é simples. Assim, cada prédio da distribuição representa uma área, com suas redes e

conexões. A área backbone é composta pelo NTI e pela Central Telefônica que garantem a comunicação entre as áreas e a Internet.

3.2 Equipamentos de conexão

Os equipamentos utilizados na Rede UFMA são equipamentos com capacidade de encaminhamento de pacotes. Normalmente os equipamentos utilizados para esta finalidade são chamados de roteadores, como é mostrado no Apêndice A.

No entanto, o mercado criou equipamentos de encaminhamento de quadros que trabalham na camada 2 do modelo OSI, chamados de switches, com capacidades de camada 3 e 4 do modelo OSI. Estes equipamentos são chamados de switches de camada 3, pois trabalham não somente na camada 2, mas fazem também o trabalho de roteamento de pacotes.

O porte destes equipamentos varia de acordo com a posição na topologia hierárquica. Para cada camada da topologia tem-se uma demanda de processamento, memória e capacidade de encaminhamento de quadros e pacotes.

Na Rede UFMA estes critérios são cumpridos visando garantir a estabilidade da performance da rede. Os equipamentos são escolhidos com dimensionamento suficiente para garantir a melhor capacidade.

Diante disto, busca-se sempre as linhas de equipamentos dos fornecedores onde a performance e desempenho sejam as compatíveis com as demanda da comunidade acadêmica da UFMA, que está cada vez mais conectada e requerendo a uma rede de computadores disponível e confiável.

3.3 Serviços oferecidos

Devido a rede UFMA ter crescido e desenvolvido sua tecnologia, serviços avançados de rede puderam ser disponibilizados para comunidade acadêmica, exemplos:

- Hospedagem de websites;
- Virtualização de servidores;

- Rede sem fio;
- Videoconferência;
- Vigilância eletrônica IP;
- Novos sistemas de gestão;
- Webconferência;
- Ensino a distância.

Grandes investimentos por parte da administração da UFMA estão sendo realizados de modo que os serviços possam melhorar e se estender para a maior quantidade de usuários destes serviços.

Como exemplo, a criação do centro de dados de reserva no prédio da Central Telefônica. A sua função é substituir, no caso de falha ou manutenção, o centro de dados do prédio do NTI. Este centro de dados reserva é uma versão menor visando apenas a contingência.

Logo, estes serviços estão cada vez mais sendo utilizados pela comunidade UFMA. Então, passam a ser requeridos com a maior disponibilidade possível. Devido a percepção atual do usuário de estar sempre conectado, a exigência aumenta proporcionalmente, tornando-os essenciais para a execução das suas atividades tanto administrativas quanto acadêmicas.

A Rede UFMA, neste caso, torna-se uma infraestrutura de grande importância para que os serviços não sofram descontinuidade na oferta aos usuários. Ela deve suportar não somente a demanda de acesso, mas também o desempenho visto que todas as tecnologias estão convergindo para as redes IP.

Então diante desta realidade, surge uma problemática para a Rede UFMA da forma que está projetada e funcional. Verificando o modelo adotado de conexão da rede, observa-se que não existem conexões redundantes entre o NTI e os prédios que concentram a distribuição.

Este fato que precisa ser solucionado para que o objetivo dos serviços serem disponíveis seja alcançado e a percepção da comunidade UFMA seja mantida em alto nível.

3.4 Uma solução de redundância para Rede UFMA

Diante do cenário mostrado no item anterior é necessário fazer uma avaliação da estrutura adotada atualmente na Rede UFMA.

Como o NTI é o centro de dados da universidade, estar conectado a ele é essencial para as distribuições que residem nos prédios principais. Na atual topologia as distribuições têm a responsabilidade de interligar os acessos ao NTI.

Da forma como está hoje, cada distribuição só tem uma maneira de chegar até o NTI e posteriormente ao a Central Telefônica. Assim, os serviços e a saída para Internet ficam dependentes destes dois prédios. A manutenção ou falha de qualquer de qualquer destes importantes prédios pode ocasionar um problema de disponibilidade.

Problemas de energia ou mesmo queima de uma interface de rede em uma distribuição afetam todos os usuários daquela localidade.

Avaliando este ponto, uma solução para tornar a Rede UFMA com disponibilidade para os serviços que a compõem é elevar o modelo de topologia física.

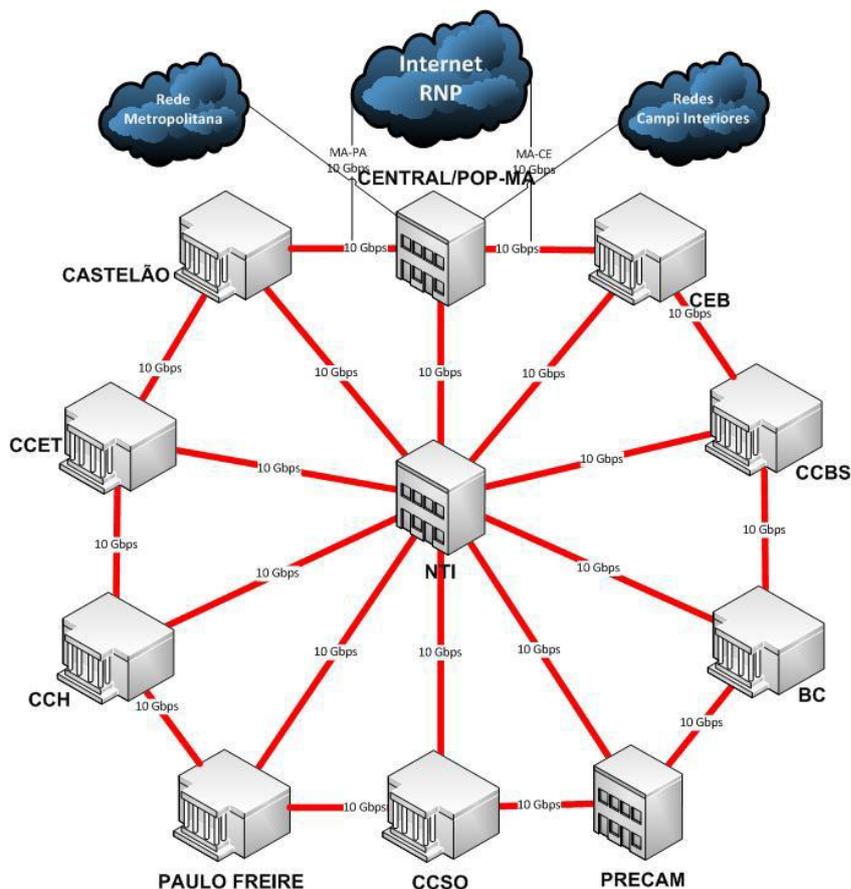
Neste aspecto será necessário não somente manter a topologia em estrela que existe hoje entre a camada de núcleo e distribuição da rede. Será preciso criar uma topologia em anel que interliguem os prédios da distribuição da rede. A ideia básica é cada prédio da distribuição seja conectado, via fibras ópticas, ao próximo prédio geograficamente imediato. Isto formará um anel óptico dentro da Rede UFMA.

Então, com esta proposição, a nova topologia resultante será a mescla da topologia em estrela com um novo anel. Esta estrutura pode garantir um novo patamar de disponibilidade para os serviços oferecidos pela Rede UFMA.

Na figura 3.6 é apresentada a nova topologia física para a Rede UFMA. Onde cada prédio que tem uma distribuição passa a contar com no mínimo três conexões para fluir o tráfego para o NTI com para outros prédios dentro da rede.

Outro fato importante a ser tratado, é evoluir a velocidade do backbone para 10 Gbps, devido a crescente demanda por banda por parte dos usuários e dos serviços avançados de rede. Assim garantir o desempenho da rede sem gerar gargalos.

Figura 3.6: Nova topologia física para a Rede UFMA.



Entretanto, apenas criar uma nova topologia física com características redundantes não é suficiente. É necessário validar esta nova realidade na topologia lógica, onde as questões relacionadas a camada 3 são determinadas.

Com esta nova topologia física, criam-se novas rotas para todos os prédios da universidade. O nível de complexidade da rede aumenta e torna-se necessário um protocolo de roteamento que seja capaz de lidar com esta nova realidade.

O protocolo de roteamento OSPF, que foi estudado aqui no capítulo 2, é o protocolo IGP mais utilizado na Internet. Como visto, adaptável, com suporte a rede multiaccess e a topologia hierárquica.

Como o OSPF já é utilizado atualmente na Rede UFMA como protocolo de roteamento, e é bem sucedido, é necessária uma ampliação da atuação dele para este novo cenário.

Este estudo objetiva verificar como o protocolo OSPF tratará as rotas e garantirá que os acessos dos usuários da Rede UFMA, mesmo em caso de falha de

componentes da rede ou manutenções, aconteçam de forma satisfatória e sem interrupções aos serviços oferecidos.

Por fim, a proposta é uma validação da atuação do protocolo OSPF no quesito de disponibilidade lógica que a nova rede impõe. Assim, simular esta nova rede é uma forma de testar a operação do protocolo OSPF e validar as ações de melhoria da Rede UFMA.

4. SIMULAÇÃO DA NOVA REDE UFMA

Este capítulo está destinado à simulação do protocolo OSPF na nova Rede UFMA através da ferramenta de simulação GNS3, conforme Fuzsner (2008).

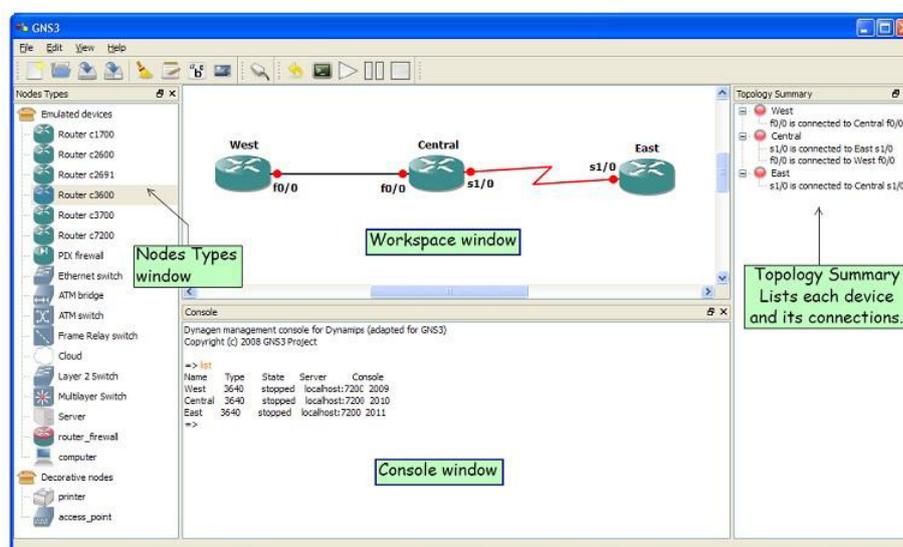
4.1 Simulador de redes, GNS3

O GNS3 é um simulador gráfico de redes, que permite a emulação de redes variadas e complexas. Assim como é possível fazer um ambiente virtual com softwares de computadores em outros programas de emulação. O GNS3 emula um ambiente que possibilita executar sistemas operacionais de diversos fornecedores, como Cisco, Juniper, Mikrotik, Extreme Networks etc. Este programa cria um ambiente virtual no computador, que gera a possibilidade da utilização destes sistemas operacionais e assim testar situações reais em laboratório (FUZSNER, 2008).

Dentro do GNS3 é possível usar máquinas virtuais das plataformas Windows ou Linux, por meio do hypervisor VirtualBox, o que permite a simulação de uma rede simples ou complexa. Isto dependendo da capacidade do hardware hospedeiro onde será feita a configuração da rede.

A figura 4.1 mostra a interface gráfica da ferramenta e suas áreas de trabalho. Ela tem uma aparência simples visando um rápido desenho de uma rede que se queira simular.

Figura 4.1: Interface gráfica do GNS3.



Fonte: FUZSNER, 2008, p. 20.

Para esta simulação da tecnologia, será usado o GNS3 com o sistema operacional da empresa Extreme Networks, o ExOS (Extreme Operating System).

Outra característica interessante é a possibilidade de captura das informações durante a execução da simulação. Onde pode-se fazer análises e correções durante todo a simulação. Diante disto, o GNS3 é usado não só para simular o estudo de uma tecnologia de rede, mas também para projetar redes.

Como não é objetivo detalhar a ferramenta e suas configurações, nos próximos itens será demonstrado a simulação da Rede UFMA e seus resultados.

4.2 Detalhes de simulação

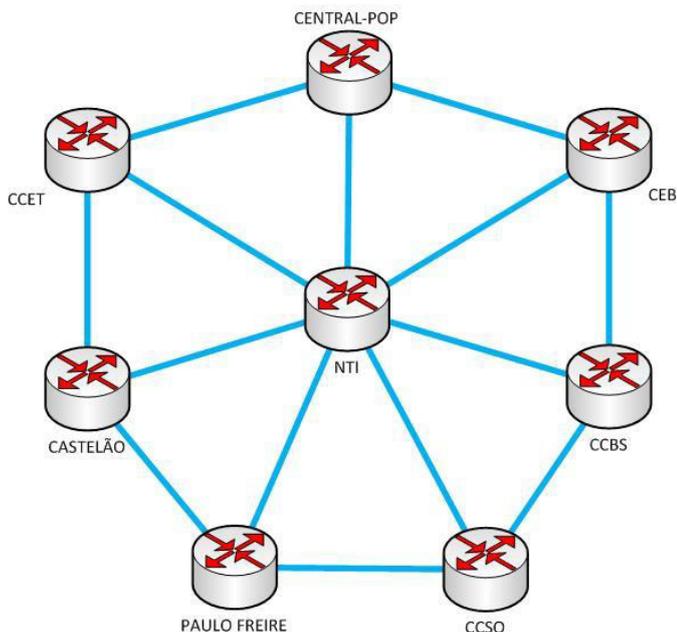
Para entender esta simulação será detalhado os principais aspectos e parâmetros na implementação do protocolo OSPF. Não serão abordados os detalhes de configuração dos equipamentos, o foco será no funcionamento lógico do OSPF como solução ao problema e não o funcionamento do protocolo em si.

De acordo com a topologia física proposta na figura 3.6, existem dez prédios que terão roteadores com função de distribuição e o NTI que é o núcleo da rede. Porém, devido a limitação da máquina virtual do sistema operacional ExOS, os equipamentos só poderão ter no máximo oito interfaces.

Diante desta limitação, o NTI que é ligado a todos os outros prédios, somente poderá interligar oito prédios da simulação. Por isto, foram eliminados três equipamentos de distribuição de modo a evitar esta limitação.

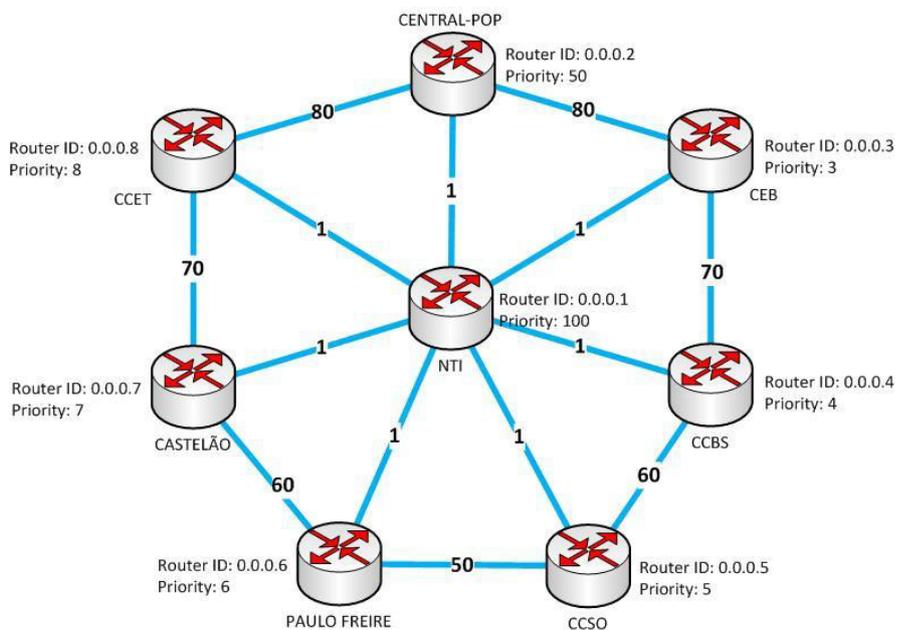
A retirada destes roteadores destas localidades não altera o propósito deste trabalho que é validar a disponibilidade da rede referente ao roteamento dos pacotes. Então, para esta simulação será usado a topologia física apresentada na figura 4.2. Ela apresenta os roteadores que estarão envolvidos na simulação e a forma como estão interconectados.

Figura 4.2: Roteadores envolvidos na simulação.



O OSPF será configurado nos equipamentos com os parâmetros de identificador de roteador (Router ID), prioridade (Priority) e os custos de cada enlace entre os roteadores (Cost), de acordo com a figura 4.3.

Figura 4.3: Parâmetros do protocolo OSPF dos roteadores envolvidos na simulação.



Estes parâmetros mostrados na figura 4.3 são essenciais para o correto funcionamento do OSPF. Pois influenciaram a forma como as tabelas de roteamento serão formadas e quais os equipamentos serão utilizados como DR e BDR.

Para esta simulação os equipamentos que serão inicialmente o DR e BDR, são respectivamente, os roteadores do NTI e POP. Motivo pelo qual, suas prioridades são 100 e 50, respectivamente.

Já os custos apresentados foram adotados levando em consideração os critérios a seguir, entretanto outros custos foram testados de modo a garanti-los:

- 1) A rota preferencial ser o roteador do NTI, motivo pelo qual o custo de seus enlaces serem 1.
- 2) Os custos dos enlaces do anel foram sugeridos de forma a dar preferência ao sentido do roteador a direita, por uma questão de desempate na escolha do caminho preferencial no caso em que os enlaces radiais apresentassem falha.

Os identificadores de roteadores foram determinados primeiramente por uma questão de melhor prática, pois a não escolha afeta o desempenho do OSPF. E segundo por uma questão de padronização a identificação dos roteadores no domínio OSPF.

Finalmente, para a realização da simulação adotou-se a topologia lógica de acordo com a figura 4.4. Nela, ilustra-se os blocos de IP envolvidos, assim como, os IPs dos roteadores nos segmentos do anel e das radiais. As áreas que foram utilizadas, incluindo a área 0, conhecida como backbone.

Na figura 4.5, a topologia da figura 4.4 é apresentada no simulador GNS3 para execução da simulação.

Figura 4.4: Topologia lógica da simulação.

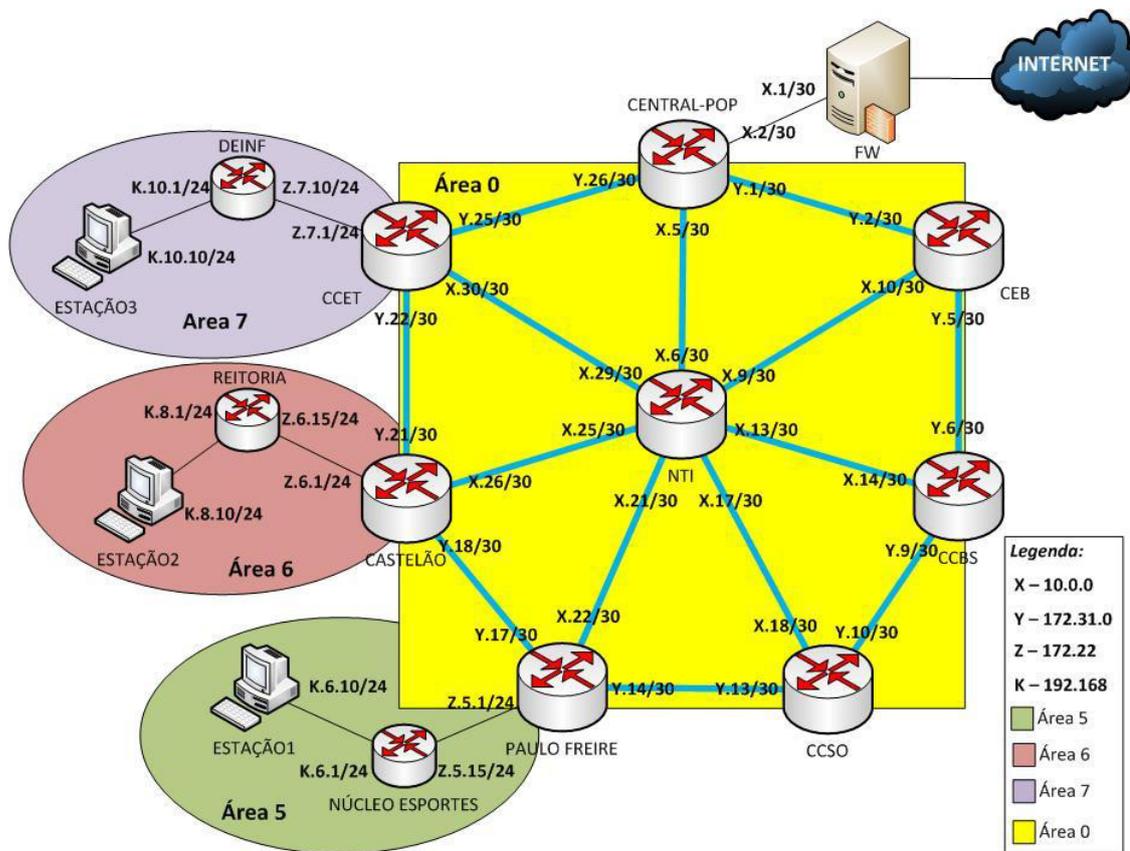
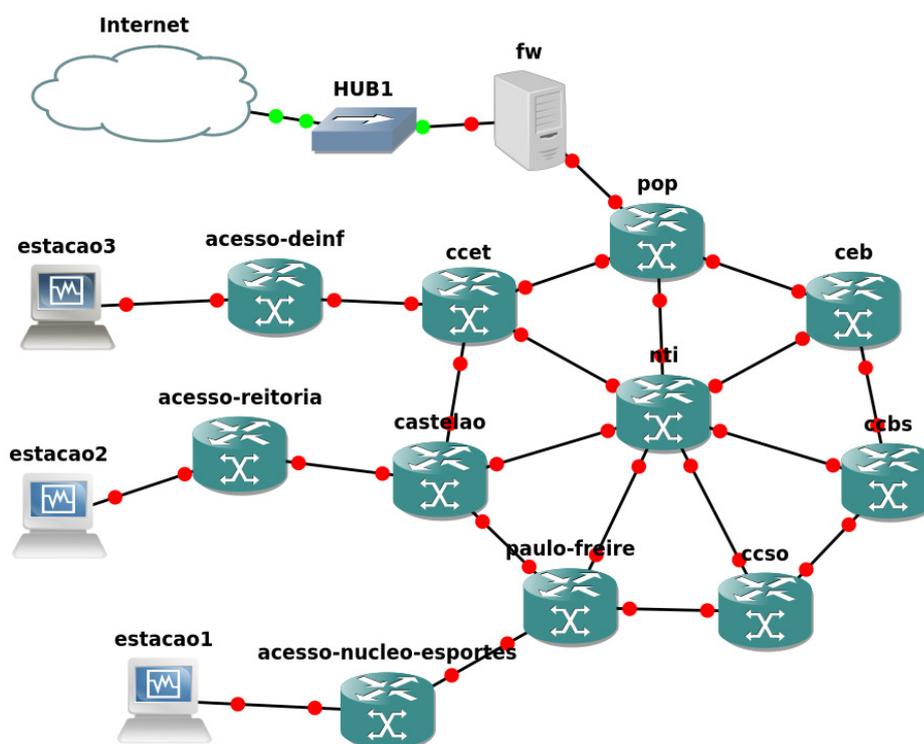


Figura 4.5: Topologia no simulador GNS3.



4.3 Testes realizados

Nestes testes para esta simulação foi avaliado o comportamento dos pacotes na topologia proposta na ocorrência de casos específicos de falhas de enlaces na rede. Como ferramenta de prova de conceito são visualizados os caminhos dos pacotes até o seu destino, através do comando “traceroute” em uma estação Linux.

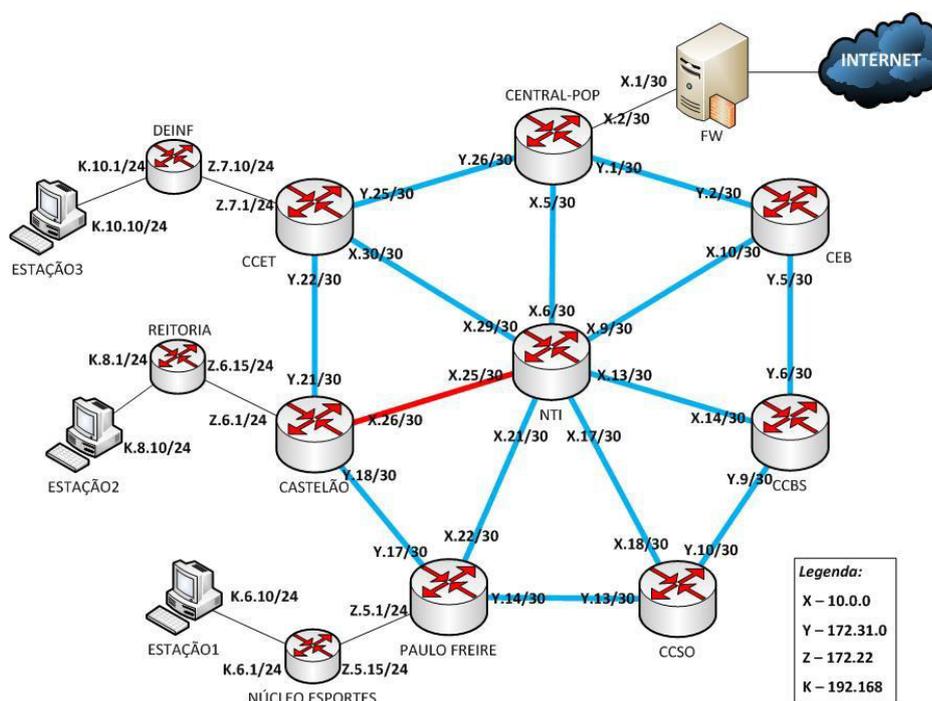
Os cenários propostos para estes testes, são observados em relação a comunicação com Internet e entre hosts da rede, nas seguintes circunstâncias:

- 1) Rompimento de um enlace radial;
- 2) Rompimento de dois enlaces radiais e um enlace no anel entre dois vizinhos.

- Cenário 1:

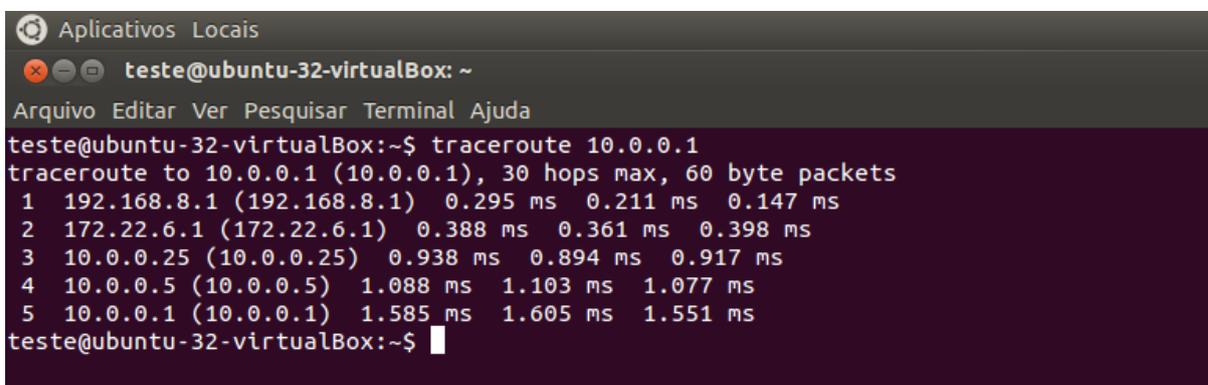
Neste teste é utilizada a distribuição localizada no prédio do Castelão, onde o enlace no sentido para o NTI ocorre uma falha, conforme figura 4.6 onde a linha em vermelho indica o segmento em falha. Neste prédio existe um host chamado de “estação2” de onde é observado o comportamento dos pacotes provenientes dele que são encaminhados para o host chamado de “estação1” localizado no roteador do prédio Paulo Freire e o caminho dos pacotes até o firewall no prédio localizado no PoP, simulando a comunicação com a Internet.

Figura 4.6: Topologia do cenário 1.



Neste primeiro teste ao utilizar o traceroute antes da queda do enlace, observa-se que a saída de menor custo para a Internet passa pelo roteador do NTI. Isto se dá pelo fato do custo do enlace ser menor do que para seus vizinhos que estão no anel. Desta forma a saída para a Internet é realizada pelo roteador de acesso (salto 1), passando pelo roteador do Castelão (salto 2), pelo roteador do NTI (salto 3), logo em seguida para o roteador do POP (salto 4) e chegando ao destino que é o firewall (salto 5), que pode ser verificado na figura 4.7.

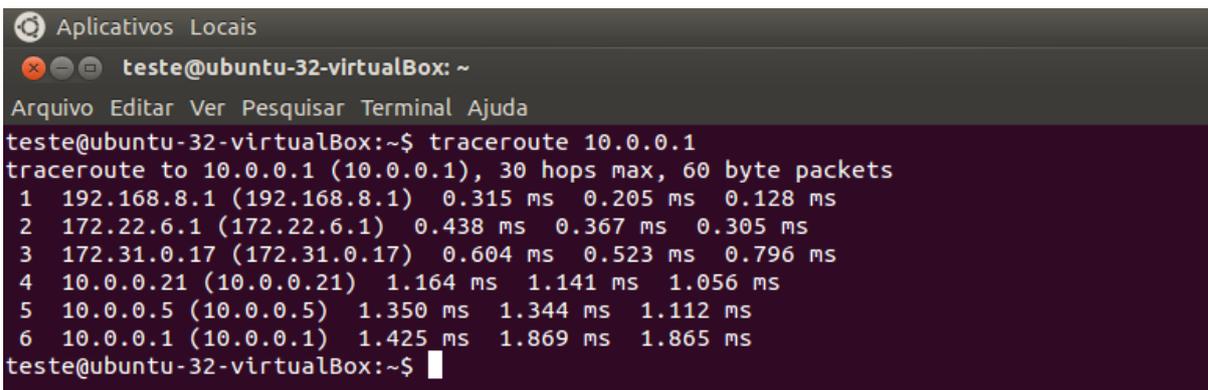
Figura 4.7: Cenário 1 – Traceroute do primeiro teste.



```
Aplicativos Locais
teste@ubuntu-32-virtualBox: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
teste@ubuntu-32-virtualBox:~$ traceroute 10.0.0.1
traceroute to 10.0.0.1 (10.0.0.1), 30 hops max, 60 byte packets
 1 192.168.8.1 (192.168.8.1)  0.295 ms  0.211 ms  0.147 ms
 2 172.22.6.1 (172.22.6.1)  0.388 ms  0.361 ms  0.398 ms
 3 10.0.0.25 (10.0.0.25)  0.938 ms  0.894 ms  0.917 ms
 4 10.0.0.5 (10.0.0.5)  1.088 ms  1.103 ms  1.077 ms
 5 10.0.0.1 (10.0.0.1)  1.585 ms  1.605 ms  1.551 ms
teste@ubuntu-32-virtualBox:~$
```

No segundo teste, agora com o enlace em queda, conforme figura 4.6, o caminho que o fluxo de pacotes toma é diferente. Pode ser observado, ao utilizar o traceroute, que o tráfego de pacotes para a Internet que passava originalmente pelo roteador do NTI agora passa pelo roteador do Paulo Freire (salto 3). Isto se dá pelo fato do custo do enlace do roteador do Paulo Freire ser menor do que do roteador do CCET, sendo estes os vizinhos do roteador do Castelão no anel. Após isto, o fluxo continua pelo roteador do NTI (salto 4), logo em seguida para o roteador do PoP (salto 5) e chegando ao destino que é o firewall (salto 6), que pode ser verificado na figura 4.8.

Figura 4.8: Cenário 1 – Traceroute do segundo teste.



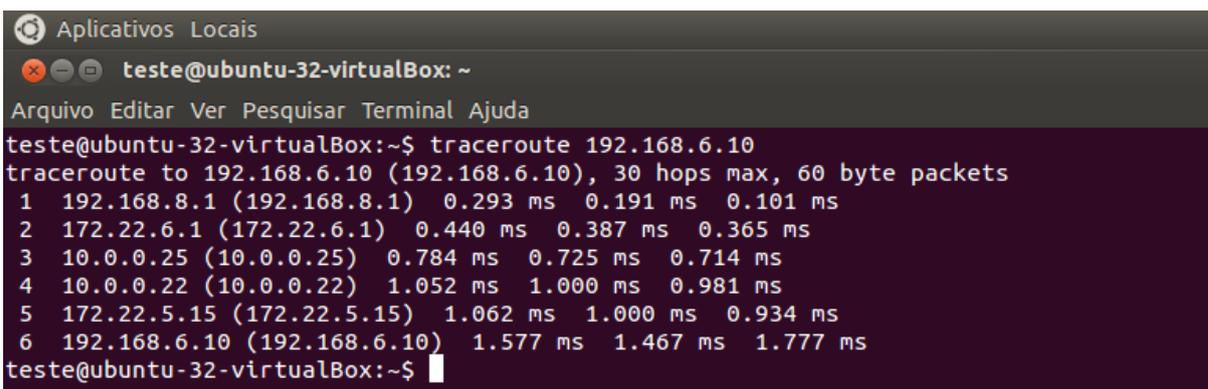
```

Aplicativos Locais
teste@ubuntu-32-virtualBox: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
teste@ubuntu-32-virtualBox:~$ traceroute 10.0.0.1
traceroute to 10.0.0.1 (10.0.0.1), 30 hops max, 60 byte packets
 1 192.168.8.1 (192.168.8.1) 0.315 ms 0.205 ms 0.128 ms
 2 172.22.6.1 (172.22.6.1) 0.438 ms 0.367 ms 0.305 ms
 3 172.31.0.17 (172.31.0.17) 0.604 ms 0.523 ms 0.796 ms
 4 10.0.0.21 (10.0.0.21) 1.164 ms 1.141 ms 1.056 ms
 5 10.0.0.5 (10.0.0.5) 1.350 ms 1.344 ms 1.112 ms
 6 10.0.0.1 (10.0.0.1) 1.425 ms 1.869 ms 1.865 ms
teste@ubuntu-32-virtualBox:~$

```

No terceiro teste, também utilizamos traceroute antes da queda do enlace, observa-se que a saída de menor custo para a comunicação com a “estação1” passa originalmente pelo roteador do NTI. Isto se dá pelo fato do custo do enlace dele ser menor do que o dos vizinhos que estão no anel. Desta forma, o caminho para a “estação1” passa pelo roteador de acesso (salto 1), continua pelo roteador do Castelão (salto 2), pelo roteador do NTI (salto 3), logo em seguida pelo roteador do Paulo Freire (salto 4), pelo roteador de acesso da “estação1” (salto 5) e chegando ao destino que é a “estação1” (salto 6), que pode ser verificado na figura 4.9.

Figura 4.9: Cenário 1 – Traceroute do terceiro teste.



```

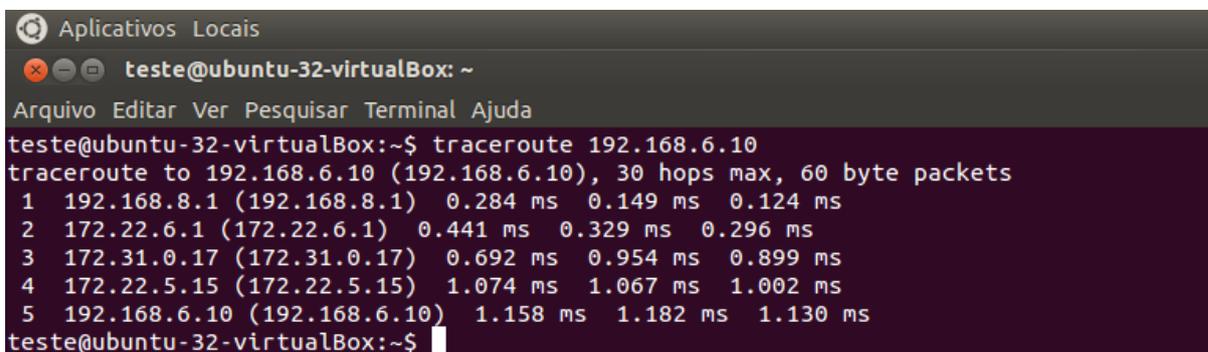
Aplicativos Locais
teste@ubuntu-32-virtualBox: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
teste@ubuntu-32-virtualBox:~$ traceroute 192.168.6.10
traceroute to 192.168.6.10 (192.168.6.10), 30 hops max, 60 byte packets
 1 192.168.8.1 (192.168.8.1) 0.293 ms 0.191 ms 0.101 ms
 2 172.22.6.1 (172.22.6.1) 0.440 ms 0.387 ms 0.365 ms
 3 10.0.0.25 (10.0.0.25) 0.784 ms 0.725 ms 0.714 ms
 4 10.0.0.22 (10.0.0.22) 1.052 ms 1.000 ms 0.981 ms
 5 172.22.5.15 (172.22.5.15) 1.062 ms 1.000 ms 0.934 ms
 6 192.168.6.10 (192.168.6.10) 1.577 ms 1.467 ms 1.777 ms
teste@ubuntu-32-virtualBox:~$

```

No quarto teste, ao utilizar o traceroute com a queda do enlace, observa-se que a saída de menor custo para a comunicação com a “estação1” que passava pelo roteador do NTI agora passa pelo roteador do Paulo Freire (salto 3). Isto se dá pelo fato do custo do enlace ser menor do que seu vizinho o roteador do CCET que está

no anel. Após isto, pelo roteador de acesso da “estação1” (salto 4) e chegando ao destino que é a “estação1” (salto 5), que pode ser verificado na figura 4.10.

Figura 4.10: Cenário 1 – Traceroute do quarto teste.



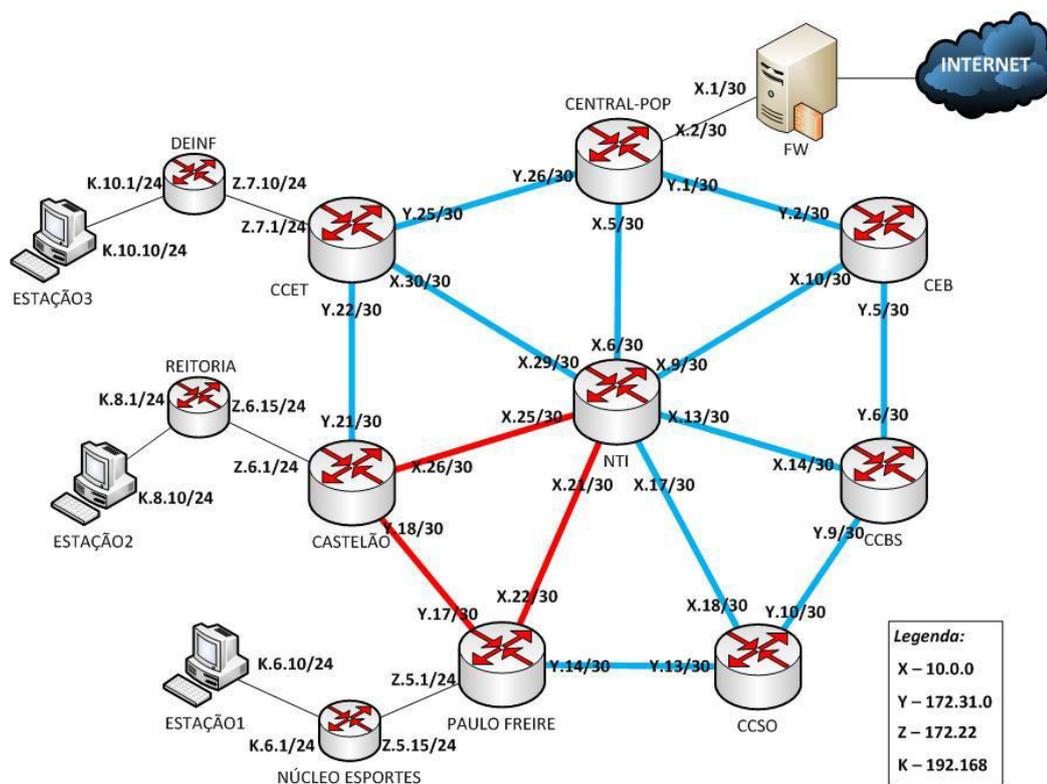
```
Aplicativos Locais
teste@ubuntu-32-virtualBox: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
teste@ubuntu-32-virtualBox:~$ traceroute 192.168.6.10
traceroute to 192.168.6.10 (192.168.6.10), 30 hops max, 60 byte packets
 1 192.168.8.1 (192.168.8.1)  0.284 ms  0.149 ms  0.124 ms
 2 172.22.6.1 (172.22.6.1)  0.441 ms  0.329 ms  0.296 ms
 3 172.31.0.17 (172.31.0.17)  0.692 ms  0.954 ms  0.899 ms
 4 172.22.5.15 (172.22.5.15)  1.074 ms  1.067 ms  1.002 ms
 5 192.168.6.10 (192.168.6.10)  1.158 ms  1.182 ms  1.130 ms
teste@ubuntu-32-virtualBox:~$
```

- Cenário 2:

No segundo cenário, novamente é utilizado o roteador localizado no prédio do Castelão, só que agora o enlace com o roteador do NTI ocorre falha, assim como, no enlace com o roteador do prédio do Paulo Freire e no enlace do roteador do Paulo Freire com o roteador do NTI, conforme figura 4.11 onde a linha em vermelho indica os segmentos em falha.

De forma semelhante ao primeiro cenário, é observado a comunicação entre o host “estação2” e o host “estação1” localizado na distribuição do prédio Paulo Freire e o caminho dos pacotes até o firewall no prédio localizado no PoP, simulando a comunicação com a Internet.

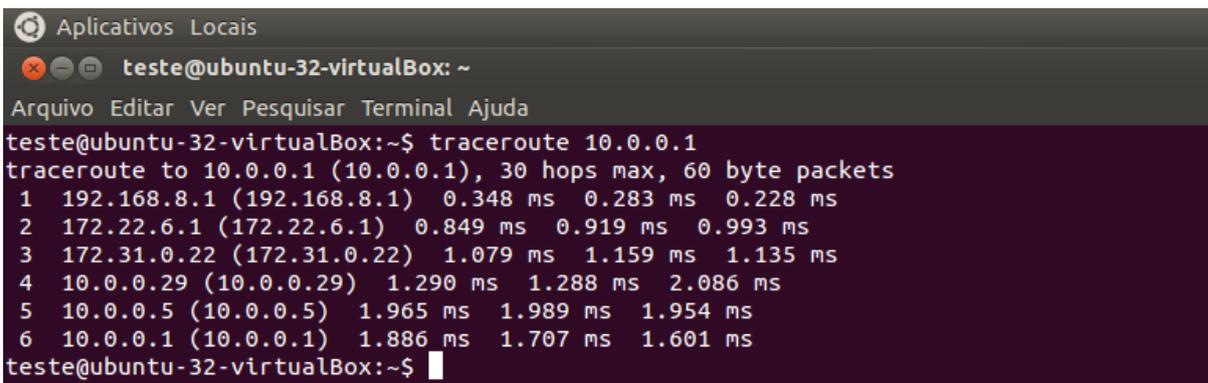
Figura 4.11: Topologia do cenário 2.



Neste primeiro teste do cenário 2, ao utilizar o traceroute após a queda dos enlaces conforme figura 4.11, observa-se que a saída de menor custo para a Internet que passava originalmente pelo roteador do NTI, conforme o primeiro teste do cenário 1, agora se dá através do roteador do CCET (salto 3) pelo fato que agora é o único caminho disponível. Já que tanto as radiais do roteador do Castelão e do roteador do Paulo Freire estão com problema, além do enlace do roteador do Castelão com o Paulo Freire no anel também estar com problema.

Sendo assim, a saída para a Internet é realizada pelo roteador de acesso (salto 1), passando pelo roteador do Castelão (salto 2), pelo roteador do CCET (salto 3), logo em seguida para o roteador do NTI (salto 4), pelo roteador do PoP (salto 5) e chegando ao destino que é o firewall (salto 6), que pode ser verificado na figura 4.12.

Figura 4.12: Cenário 2 – Traceroute do primeiro teste.



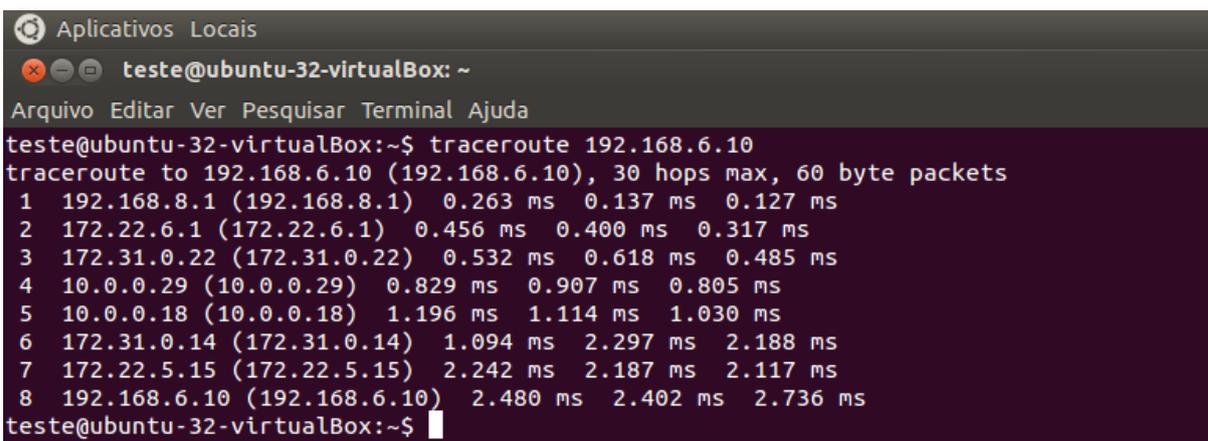
```

Aplicativos Locais
teste@ubuntu-32-virtualBox: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
teste@ubuntu-32-virtualBox:~$ traceroute 10.0.0.1
traceroute to 10.0.0.1 (10.0.0.1), 30 hops max, 60 byte packets
 1  192.168.8.1 (192.168.8.1)  0.348 ms  0.283 ms  0.228 ms
 2  172.22.6.1 (172.22.6.1)  0.849 ms  0.919 ms  0.993 ms
 3  172.31.0.22 (172.31.0.22)  1.079 ms  1.159 ms  1.135 ms
 4  10.0.0.29 (10.0.0.29)  1.290 ms  1.288 ms  2.086 ms
 5  10.0.0.5 (10.0.0.5)  1.965 ms  1.989 ms  1.954 ms
 6  10.0.0.1 (10.0.0.1)  1.886 ms  1.707 ms  1.601 ms
teste@ubuntu-32-virtualBox:~$

```

No segundo teste deste cenário, ao utilizar o traceroute com as quedas dos enlaces conforme figura 4.11, observa-se que a saída de menor custo para a comunicação com a “estação1” que passava pelo roteador do NTI (salto 3) e pelo roteador do Paulo Freire (salto 4), conforme terceiro teste do cenário 1, agora passa pelo roteador do CCET (salto 3). Devido ao fato do roteador do CCET ser seu vizinho no anel mais próximo. Logo em seguida pelo roteador do NTI (salto 4), depois disso pelo roteador do CCSO (salto 5). Após isto, pelo roteador do Paulo Freire (salto 6), logo após, o roteador de acesso da “estação1” (salto 7) e finalmente chegando ao destino que é a “estação1” (salto 8), que pode ser verificado na figura 4.13.

Figura 4.13: Cenário 2 – Traceroute do segundo teste.



```

Aplicativos Locais
teste@ubuntu-32-virtualBox: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
teste@ubuntu-32-virtualBox:~$ traceroute 192.168.6.10
traceroute to 192.168.6.10 (192.168.6.10), 30 hops max, 60 byte packets
 1  192.168.8.1 (192.168.8.1)  0.263 ms  0.137 ms  0.127 ms
 2  172.22.6.1 (172.22.6.1)  0.456 ms  0.400 ms  0.317 ms
 3  172.31.0.22 (172.31.0.22)  0.532 ms  0.618 ms  0.485 ms
 4  10.0.0.29 (10.0.0.29)  0.829 ms  0.907 ms  0.805 ms
 5  10.0.0.18 (10.0.0.18)  1.196 ms  1.114 ms  1.030 ms
 6  172.31.0.14 (172.31.0.14)  1.094 ms  2.297 ms  2.188 ms
 7  172.22.5.15 (172.22.5.15)  2.242 ms  2.187 ms  2.117 ms
 8  192.168.6.10 (192.168.6.10)  2.480 ms  2.402 ms  2.736 ms
teste@ubuntu-32-virtualBox:~$

```

5. CONCLUSÃO

Ao finalizar esse trabalho, pode-se concluir que foram atingidos os objetivos traçados desde o início do trabalho. De fato, foi apresentado um texto explicativo sobre os tópicos como algoritmos de roteamento dinâmico e o protocolo OSPF (capítulo 2).

Em seguida, foi apresentada a Rede UFMA (capítulo 3) e seus desafios quanto a disponibilidade dos serviços avançados que estão sendo oferecidos para a comunidade da UFMA. Tendo em vista, este desafio, o NTI concebeu um projeto visando melhorar a disponibilidade desta rede através de uma solução que consiste de uma nova topologia física e lógica.

No capítulo 4, simula-se a solução proposta através da ferramenta GNS3 com o intuito de verificar o comportamento da mesma visando avaliar se a disponibilidade da rede pode ser melhorada através dela. Para isto foram testados (no tópico “Testes realizados”) diversos cenários onde se pode observar se a solução proposta atende os objetivos de disponibilidade dos serviços do NTI.

Através dos resultados apresentados no ambiente de testes, pode-se concluir que a proposta de topologia física e lógica em conjunto com o protocolo OSPF podem garantir a disponibilidade tanto do acesso a Internet quanto aos serviços avançados ofertados pelo NTI a comunidade acadêmica da UFMA.

Isto porque mesmo que ocorra uma falha geral tanto no prédio do NTI como em qualquer um dos prédios de distribuição, a rede tem acesso ao centro de dados reserva e a conexão à Internet devido suas múltiplas conexões.

Ficam as seguintes sugestões para trabalhos futuros:

1. Desenvolver um trabalho comparativo com o outro protocolo de estado de enlace, IS-IS, com o protocolo OSPF;
2. Planejamento de migração para rede IPv6 utilizando o OSPFv3.

REFERÊNCIAS

KUROSE, James F.; ROSS, Keith W. Redes de computadores e a internet: uma abordagem top-down. 3. ed. São Paulo, SP: Pearson Addison-Wesley, 2003.

TANEMBAUM, A. S. Redes de Computadores. 4. ed. Rio de Janeiro, RJ: Campus, 2003.

THOMAS, Thomas M. OSPF Network Design Solutions: A practical handbook for OSPF network design and deployment. Indianapolis, IN: Cisco Press, 1998.

FUSZNER, Mike. GNS3 – Graphical Network Simulator. Disponível em: < <http://iweb.dl.sourceforge.net/project/gns-3/GNS3/0.5/GNS3-0.5-tutorial.pdf> > Acesso em 20 nov. 2014.

APÊNDICE A – PRINCÍPIOS DE ROTEAMENTO EM REDES IP (INTERNET PROTOCOL)

Como exemplo, as usuais redes locais ou Local Area Network (LAN¹⁰), que segundo Tanenbaum (2003), foram idealizadas para interconectar computadores em áreas com poucos quilômetros de extensão e com tamanho restrito. Estas LANs tinham como objetivo principal o compartilhamento de recursos e troca informações da empresa. Atualmente, o mais popular padrão para LAN utilizado é o Ethernet¹¹, que continua em pleno desenvolvimento e expansão.

Outro exemplo são as redes Asynchronous Transfer Mode (ATM¹²), que foram criadas com a finalidade de utilização em redes geograficamente distribuídas. Elas despertaram um grande interesse das empresas de telefonia por propor unir voz, dados, televisão e outros meios de comunicação em um único sistema integrado que fazia tudo por todos (TANENBAUM, 2003). Porém ficou apenas na estrutura da telefonia como principal transporte interno sem ser percebido pelos usuários.

Contudo, o que fez com que usuários de diferentes tipos de redes pudessem compartilhar recursos e informações em toda a parte, foi a adoção do TCP/IP como protocolo oficial em 1º de janeiro de 1983. Com a explosão de redes na década de 1980 logo as redes de computadores antes isoladas geográfica e tecnologicamente, podem ser interligadas visando à troca de informações (TANENBAUM, 2003).

Daí o fato de Tanenbaum (2003) declarar:

“Os elementos que formam a base da Internet são o modelo de referência TCP/IP e a pilha de protocolos TCP/IP. O TCP/IP possibilita a criação de um serviço universal e pode ser comparado ao sistema telefônico e a adoção da bitola padrão pelas ferrovias no século XIX ou com a adoção de protocolos comuns de sinalização por todas as companhias telefônicas”.

Depois desta revolução que o TCP/IP gerou, as redes passaram a formar redes regionais, nacionais e por fim continentais. Esta expansão foi denominada de inter-redes, o que depois se tornou a conhecida e importante rede mundial, Internet.

Por isso, as redes IP fazem parte da rotina de todos que utilizam Tecnologia da Informação e Comunicação (TIC) nas suas tarefas diárias. Sejam através do

¹⁰ “São redes privadas contidas em um único edifício ou campus universitário com até alguns quilômetros de extensão” (TANENBAUM, 2003).

¹¹ É um padrão de rede que para transmitir dados, todo nó disputa o meio de comunicação e a transmissão se dá por broadcast, onde todos os outros nós da rede escutam essa transmissão (COELHO, 2003).

¹² É uma tecnologia de comunicação orientada a conexão e utiliza célula de tamanho fixo onde não há compartilhamento de canal (COELHO, 2003).

computador, smartphone, tablet etc; todas estas tecnologias utilizam as redes IP com engrenagem para facilitar e viabilizar sua comunicação.

Entretanto, a forma como a informação trafega nesta rede tem diversas técnicas que serão apresentadas para uma compreensão da inteligência desta estrutura que requer desempenho e rapidez.

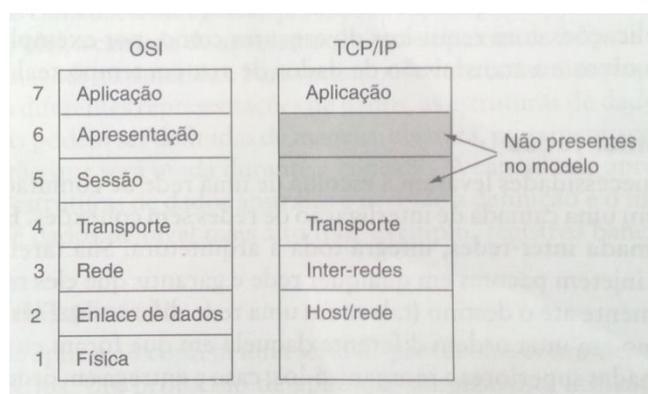
1. Camada de Rede

Quando se menciona a camada de rede, seja no modelo de referência OSI ou TCP/IP, é importante entender a função principal e as secundárias que esta camada desempenha.

Kurose e Ross (2003, p. 39) simplificam dizendo que a camada de rede é responsável pelo roteamento dos datagramas de uma máquina para outra e Tanenbaum (2003, pag. 45) diz que “é determinar a maneira como os pacotes são roteados da origem até o destino”.

Assim concordar com Tanenbaum (2003, pag. 45) que a função da camada inter-redes do modelo de referência TCP/IP é muito parecida com a camada de rede do modelo de referência OSI é simples, pelo fato desta camada providenciar os caminhos ou rotas a serem seguidos até seu destino, conforme demonstrado na figura 1.

Figura 1: Comparação da função da camada de rede nos modelos OSI e TCP/IP.

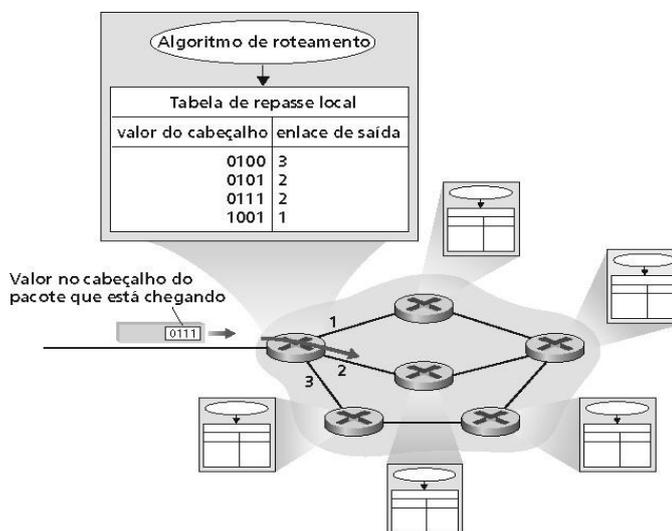


Fonte: TANENBAUM, 2003, p. 46.

Outra função é de comutação que é a capacidade de conduzir um pacote que chega na entrada de um roteador até o enlace de saída correto (Kurose e Ross,

2003, pag. 213). Como mostra a figura 2, a interação entre a função de roteamento e comutação da camada de rede faz com que os pacotes possam ser movimentados.

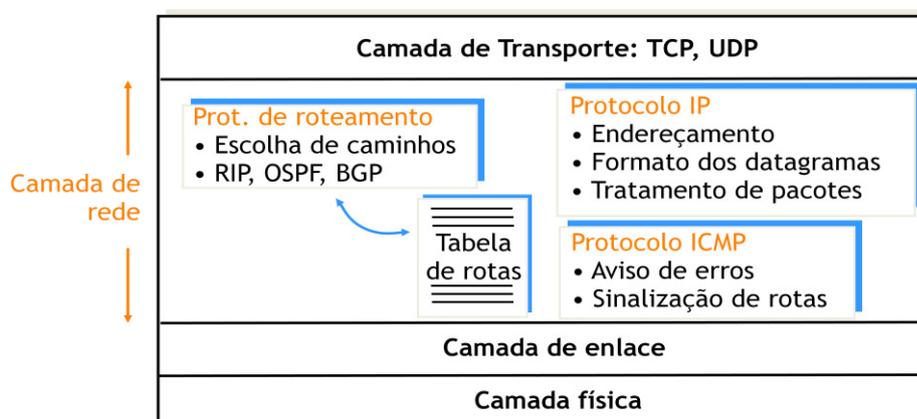
Figura 2: Interação do algoritmo de roteamento e comutação da camada de rede.



Fonte: KUROSE E ROSS, 2003, p. 216.

Porém como evidenciado por Kurose e Ross (2003, pag. 39) esta camada no modelo de referência TCP/IP, também conhecida como camada de rede da Internet, possui dois principais componentes: o protocolo IP e os protocolos de roteamento. A figura 3 demonstra estes componentes e suas relações.

Figura 3: Relações entre o protocolo IP e os protocolos de roteamento.



O protocolo IP é responsável por determinar os campos no datagrama bem como os roteadores e sistemas finais agem nestes campos. É através deste protocolo que a Internet mantém sua integridade e todos os componentes da

Internet que têm a camada de rede precisam executar este protocolo, daí o fato de chamar a camada de rede de camada IP.

Então, com o protocolo IP na camada de rede, foi definido o formato de pacote oficial. Por isso esta camada controla a operação da sub-rede e possibilita a função de que redes de diferentes tipos possam conversar livremente. Como mostra Tanenbaum (2003, pag. 43) na sua explicação:

“Quando um pacote tem de viajar de uma rede para outra até chegar a seu destino, podem surgir muitos problemas. O endereçamento utilizado pela segunda rede pode ser diferente do que é empregado pela primeira rede. Talvez a segunda rede não aceite o pacote devido a seu tamanho excessivo. Os protocolos podem ser diferentes e assim por diante. Cabe à camada de rede superar todos esses problemas, a fim de permitir que redes heterogêneas sejam interconectadas”.

Porém como ressalta Coelho (2003, pag. 379), além do protocolo IP, existem ainda os protocolos IPX e Appletalk, que fazem parte desta importante camada de interconexão. Vale ressaltar que não é objetivo aqui detalhar o protocolo IP que possuem as versões 4 (IPv4) e 6 (IPv6).

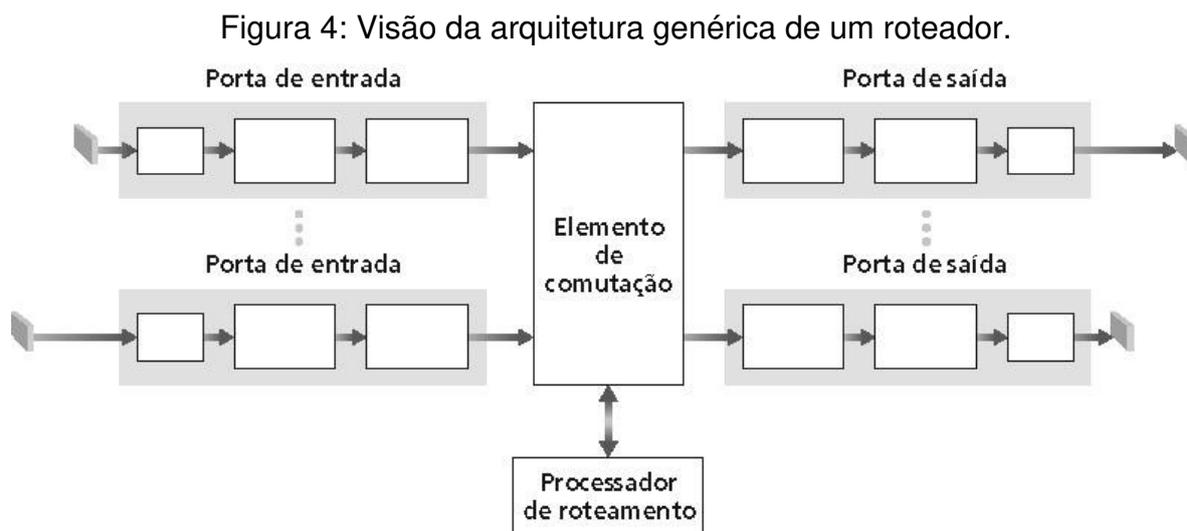
Já os protocolos de roteamento, que são variados devido ao fato de que dentro de uma rede o administrador poder executar o protocolo de roteamento desejado, possui a função de determinar as rotas que os datagramas devem seguir das origens até os seus destinos, e que é o foco deste trabalho (Kurose e Ross, 2003, pag. 39).

Por fim, outra função que deve ser apontada é o controle de congestionamento que ocorre quando muitos pacotes dividem um mesmo caminho e provocam gargalos. Num sentido geral, trata-se diretamente do fornecimento de qualidade do serviço, como: retardo, tempo de trânsito, etc (Tanenbaum, 2003, pag. 43).

2. ROTEADOR

Depois de analisar a camada de rede, suas funções e seus componentes, é necessário observar ainda a função de comutação desta camada. Trabalho este realizado pelo equipamento denominado roteador, que segundo Coelho (2003, pág. 379) é um equipamento que “... trabalha na camada 3 do modelo OSI, ou seja, ele trabalha com endereço lógico ou endereço que depende das características do protocolo”.

Como o trabalho real da camada de rede é repassar datagramas, um componente chave neste processo, é a transferência de datagramas de um enlace de entrada de um roteador para um enlace de saída. E diante da importância deste equipamento será apresentada uma visão de alto nível da arquitetura genérica de um roteador de acordo com a figura 4 (Kurose e Ross, 2003, pág. 260).



Fonte: KUROSE E ROSS, 2003, p. 260.

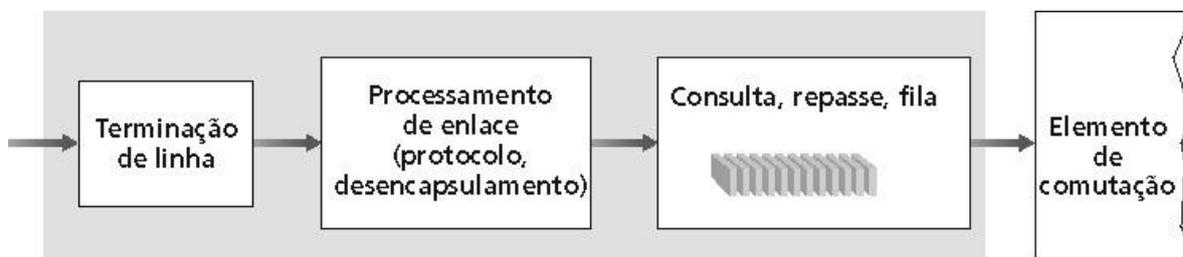
O roteador possui quatro componentes com funções bem definidas, conforme detalhado por Kurose e Ross (2003, págs. 259 e 260) e demonstrado no quadro 1.

Quadro 1: Definições das funções dos componentes de roteador.

COMPONENTE	FUNÇÕES
Portas de entrada	<ul style="list-style-type: none"> • Realiza a função da camada física, ou seja, terminação física de um enlace; • Realiza a função da camada de enlace; • Realiza a função de exame e de repasse ao elemento de comutação (ver figura 5).
Elemento de comutação	<ul style="list-style-type: none"> • Conecta as portas de entrada com as portas de saída; • Cria uma rede dentro do roteador entre as portas (ver figura 6).
Portas de saída	<ul style="list-style-type: none"> • Realiza a função inversa da porta de entrada, com relação a camada de enlace e a camada física, respectivamente (ver figura 7).
Processador de roteamento	<ul style="list-style-type: none"> • Executa os protocolos de

	roteamento; <ul style="list-style-type: none"> • Mantém as tabelas de roteamento; • Realiza as funções de gerenciamento da rede dentro do roteador.
--	---

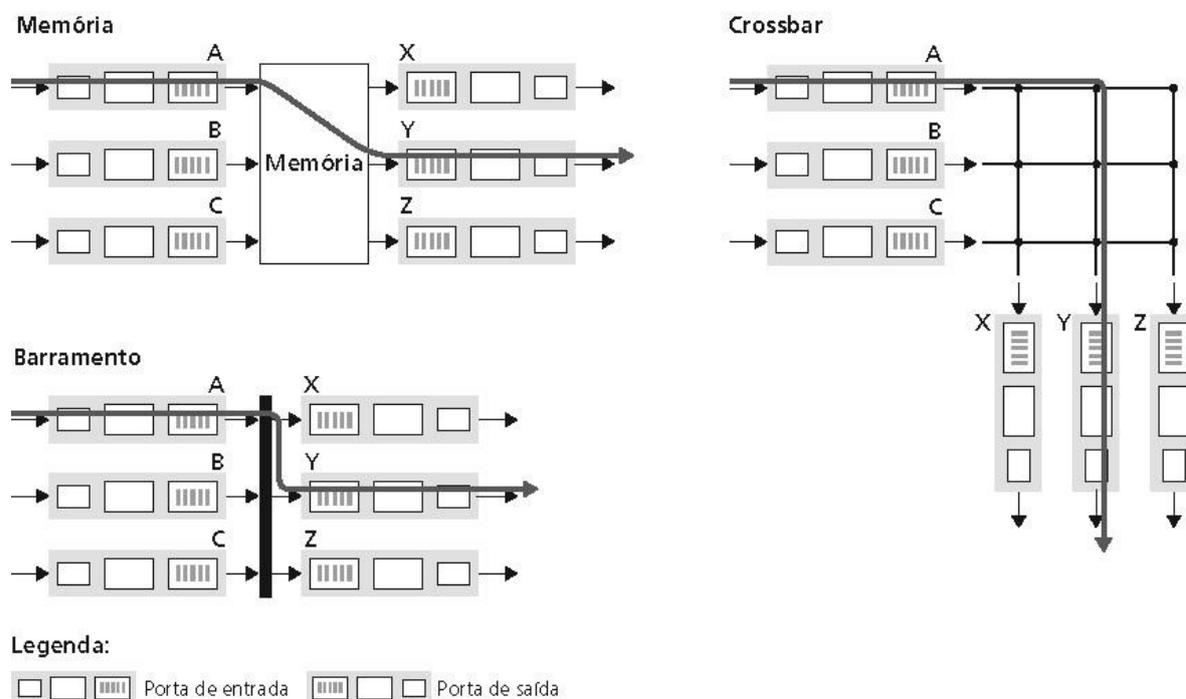
Figura 5: Processamento na porta de entrada de um roteador.



Fonte: KUROSE E ROSS, 2003, p. 261.

Este equipamento é fabricado por diversos fabricantes e pode ser dividido em roteadores de pequeno, médio e grande porte. Isto vai influenciar diretamente no mercado que vai atuar e nas suas características (FILIPPETTI, 2009).

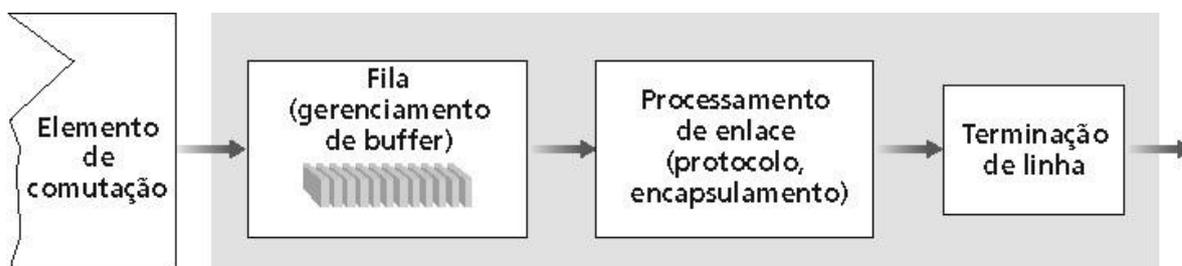
Figura 6: Técnicas de comutação.



Fonte: KUROSE E ROSS, 2003, p. 263.

Como exemplo de fabricantes de roteadores atuantes no mercado pode-se citar a Cisco e Juniper, que possuem um grande portfólio de equipamentos, conforme a divisão definida acima.

Figura 7: Processamento na porta de saída de um roteador.



Fonte: KUROSE E ROSS, 2003, p. 265.

3. TABELA DE ROTEAMENTO

Como resultado direto das funções da camada de rede nasce o conceito da tabela de roteamento, que Coelho (2003, pág. 381) dá a seguinte definição:

“Cada roteador (ou computador¹³) individualmente em uma rede precisa dispor de informações sobre a(s) rede(s) a(s) qual(is) está conectado. Tais informações permitem ao roteador (ou computador) fazer a entrega dos dados. Este conjunto de informações armazenadas é chamado de Tabela de Roteamento”.

Logo a tabela de roteamento guarda informações de quais conexões estão disponíveis, de desempenho, de custo do uso de uma conexão etc. Então, antes de enviar qualquer datagrama, um roteador ou computador deve consultar sua tabela de roteamento para decidir o melhor caminho e fazer a entrega do datagrama de forma direta (a rede de destino está diretamente conectada) ou indireta através de um roteador (a rede de destino não está diretamente conectada) (Coelho, 2003). A figura 8 mostra uma tabela de roteamento de computador com um sistema operacional Windows 7, como exemplo.

¹³ “Até mesmo um computador com uma única placa de rede deve tomar decisões sobre como encaminhar seus pacotes e, portanto, também possui tabela de roteamento” (Coelho, 2003, pág. 381).

Figura 8: Tabela de roteamento de computador.

```

C:\Windows\system32\cmd.exe
C:\Users\Santana Netto>route print -4
=====
Lista de interfaces
14...00 27 10 85 ac 55 .....Microsoft Virtual WiFi Miniport Adapter
13...1c 65 9d 01 b6 75 .....Dispositivo Bluetooth (Rede Pessoal)
11...00 27 10 85 ac 54 .....Intel(R) Centrino(R) Advanced-N 6200 AGN
10...5c 26 0a 25 fa 37 .....Intel(R) 82577LM Gigabit Network Connection
18...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
19...00 50 56 c0 00 00 .....VMware Virtual Ethernet Adapter for VMnet8
1.....
22...00 00 00 00 00 00 e0 .....Software Loopback Interface 1
23...00 00 00 00 00 00 e0 .....Adaptador do Microsoft ISATAP
24...00 00 00 00 00 00 e0 .....Adaptador do Microsoft ISATAP #2
17...00 00 00 00 00 00 e0 .....Teredo Tunneling Pseudo-Interface
24...00 00 00 00 00 00 e0 .....Adaptador do Microsoft ISATAP #3
25...00 00 00 00 00 00 e0 .....Adaptador do Microsoft ISATAP #4
26...00 00 00 00 00 00 e0 .....Adaptador do Microsoft ISATAP #5
21...00 00 00 00 00 00 e0 .....Adaptador do Microsoft ISATAP #6
=====

Tabela de rotas IPv4
=====
Rotas ativas:
Endereço de rede      Máscara      Ender. gateway      Interface      Custo
0.0.0.0                0.0.0.0        192.168.0.1         192.168.0.100  20
127.0.0.0              255.0.0.0        No vínculo         127.0.0.1      306
127.0.0.1              255.255.255.255 No vínculo         127.0.0.1      306
127.255.255.255       255.255.255.255 No vínculo         127.0.0.1      306
192.168.0.0            255.255.255.0   No vínculo         192.168.0.1    276
192.168.0.0            255.255.255.0   No vínculo         192.168.0.100  276
192.168.0.1            255.255.255.255 No vínculo         192.168.0.1    276
192.168.0.100         255.255.255.255 No vínculo         192.168.0.100  276
192.168.0.255         255.255.255.255 No vínculo         192.168.0.1    276
192.168.0.255         255.255.255.255 No vínculo         192.168.0.100  276
192.168.237.0         255.255.255.0   No vínculo         192.168.237.1  276
192.168.237.1         255.255.255.255 No vínculo         192.168.237.1  276
192.168.237.255       255.255.255.255 No vínculo         192.168.237.1  276
224.0.0.0              240.0.0.0        No vínculo         127.0.0.1      306
224.0.0.0              240.0.0.0        No vínculo         192.168.0.1    276
224.0.0.0              240.0.0.0        No vínculo         192.168.237.1  276
224.0.0.0              240.0.0.0        No vínculo         192.168.0.100  276
255.255.255.255       255.255.255.255 No vínculo         127.0.0.1      306
255.255.255.255       255.255.255.255 No vínculo         192.168.0.1    276
255.255.255.255       255.255.255.255 No vínculo         192.168.237.1  276
255.255.255.255       255.255.255.255 No vínculo         192.168.0.100  276
=====
Rotas persistentes:
Nenhuma
C:\Users\Santana Netto>

```

Por fim, é útil fazer a distinção entre o processo de roteamento e o processo de encaminhamento dentro de um roteador, pelo fato, de estarem diretamente ligados a tabela de roteamento. Onde o processo de encaminhamento vai tratar de cada pacote que chega procurando uma linha de saída na tabela de roteamento. Já o processo de roteamento, vai preencher e atualizar a tabela de roteamento, onde entra em cena o algoritmo de roteamento que será explicado adiante (Tanenbaum, 2003, pag. 373).

4. ABSTRAÇÃO DA REDE

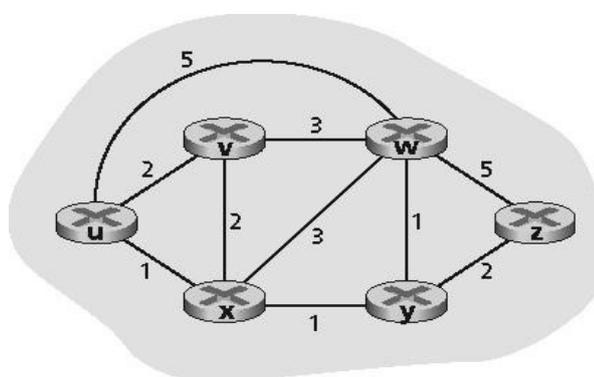
Para representação gráfica de redes e implementação dos algoritmos de roteamento é necessária uma estrutura de dados chamada grafo. Os algoritmos usados nas redes de computadores foram desenvolvidos sobre essa estrutura de modo a facilitar a visualização da topologia da rede (KUROSE e ROSS, 2003).

O conjunto de roteadores e enlaces é representado através de um grafo, $G=(N, A)$, onde N é o conjunto de nós do grafo não vazio, e A representa o conjunto de

arestas desse grafo, sendo que, cada aresta, é um par de nós conectados pertencentes ao conjunto N . Os nós correspondem aos roteadores da rede e as arestas, aos enlaces que conectam os roteadores (KUROSE e ROSS, 2003).

Na figura 9 encontra-se um exemplo de abstração de rede com roteadores e enlaces que os conectam. Nesse exemplo, os roteadores são os nós u , v , w , x , y e z ; e cada enlace que conectam os roteadores corresponde a uma aresta do grafo. Diversas definições da teoria dos grafos são bastante úteis no contexto de roteamento em redes de computadores (KUROSE e ROSS, 2003).

Figura 9: Modelo abstrato de uma rede.



Fonte: KUROSE E ROSS, 2003, p. 219.

Então, sob a perspectiva da topologia de rede, ela é representada por um grafo, onde cada aresta representa um enlace na rede. Cada aresta é inserida por um roteador que é responsável pelo enlace respectivo. Os enlaces contêm um identificador de interface, o identificador do enlace e informações que descrevem seu estado. Cada roteador pode calcular o caminho mais curto de si mesmo para todos os outros roteadores. Como todos os roteadores têm a mesma representação local da topologia e executam o mesmo algoritmo, as rotas são coerentes e ciclos não podem ocorrer. Quando um roteador detecta a mudança no estado de um enlace, ele deve atualizar a aresta respectiva em seu grafo da topologia da rede.

Além disso, ele deve transmitir esta informação para os demais roteadores. É necessário tomar precauções para que mensagens antigas, que ainda estão circulando na rede, não alterem o grafo com informações incorretas. Portanto, cada mensagem contém um contador. Deste modo, é possível ignorar mensagens antigas. Quando um roteador recebe uma nova mensagem, ele procura pelas arestas, contidas na mensagem, em seu grafo. Se alguma das arestas ainda não

está presente, então adiciona a aresta no grafo e retransmite a mensagem para os demais roteadores. Se o contador na aresta do grafo for menor do que o contador da mensagem, então atualiza grafo com o valor da aresta da mensagem e retransmite a mensagem para os demais roteadores. Se o contador na aresta do grafo for maior, então transmite o valor desta aresta em uma nova mensagem.

De conhecimento destes conceitos, entende-se que um algoritmo de roteamento utiliza uma ou mais métricas para seleção do caminho entre dois nós. Essas métricas também podem ser denominadas de funções de custo de uma aresta (KUROSE e ROSS, 2003), as quais podem ser: o tamanho físico do enlace, a velocidade de transmissão, o valor monetário associado ao enlace, o número de saltos (quantidade de arestas percorridas), a confiabilidade, a largura de banda disponível, a carga aplicada ao caminho, a espera que o caminho vai impor sobre o pacote etc (KUROSE e ROSS, 2003).

Os algoritmos estudados neste trabalho usam apenas uma métrica para calcular o caminho entre dois nós. Essa única métrica pode ser apenas uma das mencionadas anteriormente ou uma combinação delas (TANEMBAUM, 2003).