CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA

FACULDADE DE TECNOLOGIA DE INDAIATUBA

DR. ARCHIMEDES LAMMOGLIA

JONAS MONTEIRO FERNANDES

Estudo sobre os métodos de autenticação do OSPF

Indaiatuba

Junho/2024

CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA

FACULDADE DE TECNOLOGIA DE INDAIATUBA

DR. ARCHIMEDES LAMMOGLIA

JONAS MONTEIRO FERNANDES

Estudo sobre os métodos de autenticação do OSPF

Trabalho de graduação apresentado por Jonas Monteiro Fernandes como pré-requisito para a conclusão do Curso Superior de Tecnologia em Redes de Computadores, da Faculdade de Tecnologia de Indaiatuba, elaborado sob a orientação do Prof. Mestre. Carlos Antonio Fragoso.

Indaiatuba

Junho/2024

Agradeço a Deus pela vida e pelo dom que me concedeu. Aos meus pais, meu mais profundo agradecimento pelo apoio incondicional ao longo deste trabalho. Ao meu irmão, João, gratidão pelas valiosas dicas e pelo apoio de sempre. À minha querida namorada Amanda, sou imensamente grato pelo carinho, por me fazer continuar, pelo apoio e paciência durante toda esta jornada. Não poderia deixar de expressar minha gratidão ao meu orientador, Prof. Ms. Carlos Antonio Fragoso, e aos professores, Prof. Ms. André Luiz Silva e Prof. Ms. Waldinelly, por compartilharem suas ideias, conhecimento teórico e por estarem sempre disponíveis para ajudar.

Obrigado a todos!

RESUMO

O Protocolo de Roteamento de Gateway Interno (*OSPF*) é amplamente reconhecido como um dos protocolos de roteamento interno mais utilizados em redes *IP*. Baseado em estado de enlace, o *OSPF* permite que os roteadores troquem informações detalhadas sobre suas conexões diretas. Essa abordagem traz vantagens como escalabilidade, rápida convergência e uma visão detalhada da topologia da rede. Ao segmentar a rede em áreas administrativas, o *OSPF* otimiza o tráfego e reduz a carga de processamento nos roteadores. Utilizando diversos tipos de *LSAs (Link-State Advertisements)* para trocar informações de roteamento, o *OSPF* estabelece adjacências entre roteadores em etapas, começando com a troca de pacotes *Hello*. Além disso, o *OSPF* oferece recursos avançados de filtragem e sumarização de rotas, permitindo um controle preciso sobre as rotas anunciadas e resumidas entre as áreas. Contudo, apesar de suas vantagens, a complexidade de configuração e o consumo de recursos computacionais são desafios a serem considerados. Para garantir a segurança das informações de roteamento, o *OSPF* oferece métodos de autenticação, como autenticação de área e autenticação de interface. A autenticação de área verifica os pacotes *OSPF* entre roteadores em uma área com uma senha compartilhada. A autenticação de interface opera em nível de interface, permitindo senhas diferentes para cada interface *OSPF* em um roteador. Esses métodos contribuem para a integridade e segurança das informações na rede *OSPF*. Essa abordagem modular e abrangente do *OSPF*, combinada com seus mecanismos de autenticação, torna-o uma escolha poderosa para redes *IP (Internet Protocol)* complexas, oferecendo escalabilidade, eficiência e segurança.

Palavras-chaves: *OSPF*. Roteamento. Estado de enlace. Escalabilidade. Convergência rápida. Topologia da rede. Segmentação de rede. *LSAs.* Adjacências. Filtragem de rotas. Autenticação e Segurança

ABSTRACT

The Internal Gateway Routing Protocol (OSPF) is widely recognized as one of the most widely used internal routing protocols in IP networks. Based on link state, OSPF allows routers to exchange detailed information about their direct connections. This approach brings advantages such as scalability, fast convergence and a detailed view of the network topology. By segmenting the network into administrative areas, OSPF optimizes traffic and reduces the processing load on routers. Using several types of LSAs (Link-State Advertisements) to exchange routing information, OSPF establishes adjacencies between routers in stages, starting with the exchange of Hello packets. Additionally, OSPF offers advanced route filtering and summarization capabilities, enabling precise control over advertised and summarized routes between areas. However, despite its advantages, configuration complexity and computational resource consumption are challenges to be considered. To ensure the security of routing information, OSPF provides authentication methods such as area authentication and interface authentication. Area authentication checks OSPF packets between routers in an area with a shared password. Interface authentication operates at the interface level, allowing different passwords for each OSPF interface on a router. Authentication type authentication makes it possible to configure different authentication methods on different interfaces of the router. These methods contribute to the integrity and security of information on the OSPF network. This modular, comprehensive approach to OSPF, combined with its authentication mechanisms, makes it a powerful choice for complex IP (Internet Protocol) networks, offering scalability, efficiency, and security.

Keywords: OSPF. Routing. Link state. Scalability. Fast convergence. Network topology. Network segmentation. LSAs. Adjacencies. Route filtering. Authentication and Security.

LISTA DE ILUSTRAÇÕES

Figura 1 - Cabeçalho de um pacote *OSPF*.....23
Figura 2 - Pacote *HELLO* 25
Figura 3 - Pacote de descrição da base de dados 26
Figura 4 - Pacote de requisição de estado de link 27
Figura 5 - Pacote de atualização de estado de link 28
Figura 6 - Pacote de *ACK* do estado de link 29
Figura 7 - Assinaturas digitais com o uso da criptografia de chave pública.....33

LISTA DE ABREVIAÇÕES E SIGLAS

APPC Advanced Program-to-Program Communication
ARPANET Advanced Research Projects Agency Network
AS Autonomous System
BDR Backup Designated Router
BGP Border Gateway Protocol
BSD Berkeley Software Distribution
CCNA Cisco Certified Network Associate
DBD Database Description
DES Data Encryption Standard
DR Designated Router
DSS Digital Signature Standard
DV Distance Vector
EGP Exterior Gateway Protocol
EIGRP Enhanced Interior Gateway Routing Protocol
HMAC Hash-based Message Authentication Code
HMAC-MD5 Hash-based Message Authentication Code using MD5
HMAC-SHA256 Hash-based Message Authentication Code using SHA-256
IBM International Business Machines Corporation
ID Identifier
IGP Interior Gateway Protocol
INTRA-AS Intra-Autonomous System
IP Internet Protocol
IPsec Internet Protocol Security
IS-IS Intermediate System to Intermediate System
ISO International Organization for Standardization
ISP Internet Service Provider
LSA Link State Advertisements
LSACK Link State Acknowledgment
LSDB Link State Database
LSR Link State Request
LSU Link State Update
MD5 Message Digest Algorithm 5
MOSPF Multicast Open Shortest Path First
NIST National Institute of Standards and Technology
OSI Open Systems Interconnection
OSPF Open Shortest Path First
RFC Request for Comments
RIP Routing Information Protocol
RSA Rivest-Shamir-Adleman
RTRPRI Router Priority
SHA-1 Secure Hash Algorithm 1

SHA256 Secure Hash Algorithm 256
SNA Systems Network Architecture
SPF Tree Shortest Path First tree
TCP/IP Transmission Control Protocol/Internet Protocol
UNIX Uniplexed Information and Computing System
XNS Xerox Network Systems

SUMÁRIO

INTRODUÇÃO……...10

CAPÍTULO I……12

1 Fundamentação Teórica……...12

1.1 Arquitetura de rede de computadores.……...……..……12

1.2 Modelo *OSI*.…….…….....13

1.3 Protocolos em redes de computadores…….…….....14

1.4 Roteamento *RIP*……...…….…….…...15

1.5 Sobre o *OSPF*……..……..17

1.6 Vantagens do *OSPF* sobre o *RIP*…….....20

1.7 Algoritmo de Dijkstra……..…...…21

1.8 O cabeçalho dos pacotes *OSPF*…….....…22

1.8.1 Sobre o Pacote *HELLO*…….....…23

1.8.2 Pacote de descrição de base de dados……..…25

1.8.3 Pacote de requisição de estado de link……..…..…26

1.8.4 Pacote de atualização de estado de link…….27

1.8.5 Pacote de *ACK* do estado de link……..…28

1.9 O protocolo de roteamento *OSPF*……29

1.10 Assinaturas Digitais……..……..……30

1.10.1 Assinaturas de chaves públicas……..……31

1.10.2 *MD5*…….....…33

1.11 Autenticação no *OSPF*…….…..…34

CAPÍTULO II……..36

2 Percurso Metodológico…….....36

2.1 Análise e discussão dos dados……37

Considerações Finais……41

Referências Bibliográficas……..43

INTRODUÇÃO

A segurança das redes de computadores é um aspecto crucial no mundo atual, onde a conectividade e a troca de informações são fundamentais para operações comerciais, governamentais e pessoais. Nesse contexto, o protocolo de roteamento *Open Shortest Path First (OSPF)* se destaca como uma ferramenta amplamente utilizada para determinar os melhores caminhos para a transmissão de dados, desempenhando um papel essencial na infraestrutura de rede. O *OSPF* é renomado por sua eficiência e adaptabilidade, incorporando vários métodos de autenticação para garantir que apenas roteadores autorizados participem do processo de roteamento. Essa precaução é vital para impedir a injeção de informações maliciosas ou incorretas que possam comprometer a integridade da rede. A escolha deste tema para meu trabalho de conclusão de curso se justifica pela crescente necessidade de segurança nas redes, especialmente em ambientes corporativos e entre grandes provedores de serviços de Internet. A autenticação no *OSPF* se faz necessária para manter a integridade e a confiabilidade das redes, prevenindo ataques que poderiam comprometer a transmissão de dados e a comunicação entre roteadores. Este estudo sobre os métodos de autenticação no *OSPF* tem como foco explorar suas características, vantagens e desafios, fornecendo uma base para melhorias contínuas na segurança de redes complexas. Minha pesquisa busca responder a questões fundamentais relacionadas à autenticação no *OSPF*: quais são os principais métodos de autenticação utilizados no *OSPF*? Quais são as vulnerabilidades associadas a cada método de autenticação? Como a autenticação no *OSPF* pode ser melhorada para enfrentar ameaças emergentes? E qual é o impacto da implementação de diferentes métodos de autenticação na eficiência e segurança da rede? Essas perguntas delineiam o problema central da pesquisa: compreender a eficácia e as limitações dos métodos de autenticação no *OSPF*, com o objetivo de fortalecer a segurança das redes que utilizam esse protocolo. Com base nessas questões, foram formuladas algumas hipóteses para guiar minha pesquisa: a autenticação *MD5* oferece uma segurança significativamente maior em comparação com a autenticação simples, devido ao uso de chaves secretas e hashes criptográficos; a implementação correta e consistente de métodos de autenticação robustos pode mitigar a maioria dos ataques

direcionados ao *OSPF*; e melhorias nos métodos de autenticação, incluindo o uso de algoritmos criptográficos mais avançados, podem aumentar a resiliência do *OSPF* contra novas ameaças. Os objetivos deste estudo são: identificar e descrever os métodos de autenticação atualmente utilizados no *OSPF*; descrever os métodos em termos de segurança e desempenho; analisar possíveis vulnerabilidades e desafios associados a cada método de autenticação; propor melhorias ou alternativas que possam fortalecer a autenticação no protocolo *OSPF*; e contribuir para o desenvolvimento de práticas mais seguras e eficientes na administração de redes de computadores. Além disso, este estudo busca fazer uma comparação entre os protocolos, destacando as diferenças e semelhanças nas abordagens de autenticação, suas implicações na segurança e desempenho das redes, e como cada protocolo pode ser otimizado para enfrentar ameaças emergentes. Ao atingir esses objetivos, espera-se fornecer uma contribuição significativa para a área de segurança de redes, garantindo uma comunicação mais segura e confiável entre os roteadores.

CAPÍTULO I

Fundamentação Teórica

1.1 Arquitetura de redes de computadores

De acordo com Soares (1995), a arquitetura de rede é feita pelas camadas, interfaces e pelos protocolos. Cada camada fornece um aglomerado de serviços à camada superior, mas não estabelece a maneira que as operações são feitas. De acordo com essa estrutura, as camadas podem ser chamadas de níveis. O número, nome, conjunto de funções, serviços e protocolos de cada camada, variam de arquitetura para arquitetura. As máquinas se comunicam entre si pelos níveis de rede iguais. A comunicação é feita pelos programas que implementam protocolos, tais quais definem as regras de como os serviços irão funcionar. Os dados da máquina de origem percorrem verticalmente do nível i até o nível físico, onde então a comunicação ocorre horizontalmente com o nível 1 da máquina de destino, e depois sobem verticalmente até o nível 1 desta última. A fronteira entre níveis adjacentes é chamada de interface, que especifica como os processos acima dela podem acessá-la. Inicialmente, cada fabricante desenvolveu sua própria arquitetura, conhecidas como proprietárias. Com a necessidade de comunicação entre computadores de diferentes fabricantes, tornou-se essencial definir uma arquitetura comum. Para este propósito, a *International Organization for Standardization (ISO)* definiu o modelo de referência chamado *Open Systems Interconnection (OSI)*. Segundo Soares (1995), a arquitetura *ISO/OSI* foi originalmente projetada para redes de longa distância, embora também possa ser utilizada em redes locais. Para interconectar redes heterogêneas (locais, metropolitanas e de longa distância), foi desenvolvida a arquitetura Internet *TCP/IP (Transmission Control Protocol/Internet Protocol),* frequentemente referida apenas como Internet. Esta se tornou o padrão mundial para a interconexão de sistemas abertos. Os acrônimos *TCP* (*Transmission Control Protocol*) e *IP* (*Internet Protocol*) representam os dois principais protocolos dessa arquitetura.

1.2 O Modelo *OSI*

O Modelo *OSI* se baseia em uma proposta desenvolvida pela *ISO* como um primeiro passo em direção à padronização internacional dos protocolos empregados nas diversas camadas. Ele foi revisto em 1995 (DAY, 1995). O modelo é chamado Modelo de Referência *ISO/OSI*, pois ele trata da interconexão de sistemas abertos — ou seja, sistemas que estão abertos à comunicação com outros sistemas. A primeira camada, denominada Camada Física, é responsável pela transmissão física dos dados através de um meio de comunicação. Ela define as especificações elétricas, mecânicas e procedurais para estabelecer, manter e desativar conexões físicas. A Camada de Enlace de Dados, a segunda camada, gerencia o acesso ao meio físico e fornece entrega de dados confiável entre dispositivos diretamente conectados. Ela divide os dados em quadros e adiciona cabeçalhos e trailers para controle de erros. A Camada de Rede, terceira camada do modelo, lida com o roteamento e a comutação dos dados. Ela determina o melhor caminho para encaminhar pacotes de dados da origem para o destino através da rede, usando endereços lógicos *(IP).* A Camada de Transporte, quarta camada, garante a comunicação ponto a ponto entre dispositivos. Ela se encarrega de que os dados sejam entregues de maneira confiável, ordenada e sem duplicatas, controlando também o fluxo de dados. A quinta camada, Camada de Sessão, estabelece, gerencia e encerra sessões entre aplicações em diferentes dispositivos. Ela sincroniza a comunicação e gerencia o controle de diálogo. A Camada de Apresentação, sexta camada, garante que as informações sejam apresentadas corretamente para as aplicações. Ela lida com a sintaxe e a semântica da informação transmitida, realizando também compressão, criptografia e conversão de dados. Por fim, a Camada de Aplicação, sétima e última camada, fornece serviços de rede diretamente aos aplicativos do usuário. Ela permite o acesso a serviços como correio eletrônico, transferência de arquivos e navegação na web, atuando como interface entre o software de aplicação e o ambiente de rede.

1.3 Protocolos em redes de computadores

De acordo com (ROSS, 2008), um pacote é uma estrutura de dados utilizada para que dois computadores possam enviar e receber informações em uma rede. No modelo *OSI*, cada camada se relaciona com a camada superior e inferior, adicionando informações de controle aos pacotes. Cada camada do modelo *OSI* se comunica com a camada adjacente, ou seja, as camadas de um computador se comunicam com as mesmas camadas em outro computador. Para que dois computadores possam enviar e receber pacotes e para que as camadas possam se comunicar de forma adjacente (no mesmo nível), é necessário um software chamado protocolo. Quando uma camada *OSI* em um computador quer enviar dados para outra camada adjacente, é necessário que os dados sejam preparados e enviados segundo regras compreensíveis para ambos os computadores. Portanto, a condição básica para que dois computadores se comuniquem na rede é que utilizem o mesmo protocolo, ou seja, o mesmo conjunto de regras e padrões para a preparação e entrega dos pacotes. Os protocolos podem ser classificados como proprietários ou abertos. Protocolos proprietários são limitados a aplicações específicas ou empresas particulares, como o protocolo *APPC* (*Advanced Program-to-Program Communication*), que pertence à *IBM (International Business Machines Corporation)* e é utilizado na arquitetura de rede *SNA*. Por outro lado, os protocolos abertos são amplamente adotados por diversas empresas, divulgados e padronizados por organismos e associações internacionais, além de serem aceitos pela indústria de informática. Um exemplo de protocolo aberto amplamente utilizado é o *TCP/IP,* essencial para a comunicação entre computadores na Internet. Além de permitir a comunicação entre computadores, os protocolos têm a capacidade de fornecer diversas informações sobre a rede, como desempenho, erros, endereçamento, entre outros. A análise desses protocolos pode ser realizada através de ferramentas de software, que possibilitam a obtenção de informações críticas para o monitoramento eficiente da rede. Essas ferramentas permitem verificar o destino de um pacote, o tempo de chegada, o percurso realizado através de um roteador e se uma rota única ou alternativa foi utilizada. Kurose (2013) comparou um protocolo de rede a um protocolo humano, destacando que as entidades que trocam mensagens e executam ações são componentes de hardware ou software, presentes em dispositivos como computadores, smartphones, tablets, roteadores, entre outros

equipamentos de rede. Todas as atividades na Internet que envolvem a comunicação entre duas ou mais entidades remotas são regidas por protocolos. Por exemplo, protocolos executados no hardware de dois computadores conectados fisicamente controlam o fluxo de bits no cabo entre as placas de interface de rede; protocolos de controle de congestionamento nos sistemas finais regulam a taxa de transmissão de pacotes entre a origem e o destino; e protocolos em roteadores determinam o caminho que um pacote seguirá do ponto de origem ao destino. Assim como na comunicação entre pessoas, tanto no exemplo humano quanto no exemplo de rede, as trocas de mensagens e as ações realizadas ao enviar e receber essas mensagens são elementos fundamentais na definição de um protocolo. Um protocolo define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicativas, bem como as ações realizadas na transmissão e/ou recepção de uma mensagem ou outro evento. Portanto, a Internet e as redes de computadores em geral dependem fortemente de protocolos. Diversos tipos de protocolos são utilizados para realizar diferentes tarefas de comunicação. Durante o estudo desses protocolos, percebe-se que alguns são simples e diretos, enquanto outros são complexos e exigem maior profundidade intelectual. A compreensão dos protocolos de rede é crucial para dominar o campo das redes de computadores, pois permite entender o que são, por que existem e como funcionam os protocolos de rede.

1.4 Roteamento *RIP*

De acordo com Kurose (2013) Protocolos de roteamento *intra-AS* são usados para determinar como o roteamento ocorre dentro de um sistema autônomo *(SA)*. Esses protocolos, também conhecidos como protocolos de roteamento internos *(IGP - Interior Gateway Protocols*), desempenham um papel crucial na Internet, e historicamente, dois deles têm sido amplamente utilizados: o Protocolo de Informações de Roteamento (*RIP - Routing Information Protocol*) e o *OSPF*. Um protocolo intimamente relacionado ao *OSPF* é o *IS-IS* (*Intermediate System-to-Intermediate System*). O *RIP* foi um dos primeiros protocolos de roteamento *intra-AS* da Internet e ainda é amplamente utilizado. Originário da arquitetura *XNS* (*Xerox Network Systems*), o RIP foi incluído na versão do *UNIX (Uniplexed Information and Computing System)* do *Berkeley Software Distribution*

(BSD) de 1982, que suportava *TCP/IP*. A versão 1 do *RIP* está definida no *RFC* 1058 *(Request for Comments)*, e a versão 2, compatível com a versão 1, no *RFC* 2453. Na versão especificada no *RFC* 1058, utiliza contagem de saltos como métrica de custo, onde cada enlace tem um custo de 1. Os custos são definidos desde um roteador de origem até uma sub-rede de destino. O *RIP* utiliza o termo "salto" (hop), que é o número de sub-redes percorridas no caminho mais curto entre o roteador de origem e a sub-rede de destino, inclusive. O custo máximo de um caminho é limitado a 15, o que restringe seu uso a sistemas autônomos com menos de 15 saltos de diâmetro. Em protocolos *DV (Distance Vector)*, roteadores vizinhos trocam vetores de distância entre si. O vetor de distâncias para qualquer roteador é uma estimativa atual das distâncias dos caminhos de menor custo entre aquele roteador e as sub-redes no *AS*. No *RIP*, atualizações de roteamento são trocadas entre vizinhos a cada 30 segundos, aproximadamente, usando uma mensagem de resposta *RIP*, também conhecida como anúncios *RIP*. O *RIP* permite a agregação de registros de sub-redes usando técnicas de agregação de rotas. John Moy, em "Anatomy of an Internet Routing Protocol", destaca que o *OSPF* oferece uma visão detalhada da topologia da rede, trocando informações sobre os estados dos enlaces de comunicação entre os roteadores. Essa troca de informações permite que os roteadores tenham uma compreensão abrangente da rede, incluindo todos os caminhos disponíveis e os estados de conectividade de cada enlace. Essa visão detalhada da topologia da rede é fundamental para a segmentação da rede em áreas administrativas, permitindo aos administradores dividir a rede em áreas lógicas menores para facilitar o controle de tráfego e reduzir a carga de processamento nos roteadores. Cada área administrativa pode ter suas próprias políticas de roteamento e configurações específicas, possibilitando uma gestão mais eficiente e granular da rede. O *OSPF* utiliza algoritmos sofisticados para calcular os caminhos mais curtos entre os roteadores, garantindo uma otimização eficaz do tráfego e rápida convergência da rede em caso de alterações na topologia. Esses aspectos contribuem significativamente para um desempenho robusto e confiável da rede, conforme detalhado por (Moy, 1995) em seu livro.

1.5 Sobre o *OSPF*

O *OSPF*, assim como o *RIP*, é amplamente utilizado para o roteamento *intra-AS* na Internet. Tanto o *OSPF* quanto seu similar, o *IS-IS*, são geralmente implementados em *ISPs* de alto nível, enquanto o *RIP* é mais comum em *ISPs* de nível inferior e em redes corporativas. O termo "*open*" no *OSPF* indica que as especificações do protocolo de roteamento são de domínio público, ao contrário de protocolos proprietários como o *EIGRP* (*Enhanced Interior Gateway Routing Protocol*) da Cisco (KUROSE, 2013). A versão mais recente do *OSPF*, a versão 2, está detalhada no *RFC 2328*, um documento de acesso público. Desenvolvido como sucessor do *RIP*, o *OSPF* apresenta diversas características avançadas. Fundamentalmente, é um protocolo de estado de enlace que utiliza a inundação de informações de estado de enlace e o algoritmo de caminho de menor custo de Dijkstra. Com o *OSPF*, um roteador constroi um mapa topológico completo do sistema autônomo e executa localmente o algoritmo de Dijkstra para determinar uma árvore de caminho mais curto para todas as sub-redes, sendo ele próprio o nó raiz. Os custos dos enlaces individuais são configurados pelo administrador da rede, que pode definir todos os custos de enlace como 1, alcançando assim o roteamento com o mínimo de saltos, ou atribuir pesos inversamente proporcionais à capacidade do enlace para desencorajar o tráfego em enlaces de baixa largura de banda. O *OSPF* não impõe uma política específica sobre como os pesos dos enlaces devem ser determinados; em vez disso, oferece os mecanismos necessários para calcular o caminho de roteamento de menor custo para um dado conjunto de pesos de enlaces. No *OSPF*, um roteador transmite informações de roteamento por difusão a todos os outros roteadores no sistema autônomo, não apenas a seus vizinhos imediatos. As informações de estado de enlace são difundidas sempre que ocorre uma mudança no estado de um enlace, como uma alteração de custo ou uma mudança de estado (ativado/desativado). Além disso, o estado de um enlace é transmitido periodicamente, pelo menos a cada 30 minutos, mesmo que não haja mudanças. Essa atualização periódica de anúncios de enlace adiciona robustez ao algoritmo de estado de enlace, conforme destacado no *RFC* 2328. Os anúncios *OSPF* são contidos em mensagens *OSPF* transmitidas diretamente pelo *IP*, utilizando um código de protocolo de camada superior 89. Dessa forma, o próprio protocolo *OSPF* deve realizar funcionalidades como transferência confiável de

mensagens e transmissão de estado de enlace por difusão. O *OSPF* também verifica se os enlaces estão operacionais através de mensagens *Hello* enviadas aos vizinhos conectados ao enlace e permite que um roteador obtenha o banco de dados de estado de enlace de um roteador vizinho. O *OSPF* incorpora várias melhorias significativas, destacando-se em termos de segurança, utilização de caminhos múltiplos de igual custo e suporte para roteamento unicast e multicast. No aspecto de segurança, as trocas entre roteadores *OSPF*, como atualizações de estado de enlace, podem ser autenticadas para garantir que apenas roteadores confiáveis participem do protocolo dentro de um sistema autônomo, evitando que intrusos injetem informações incorretas nas tabelas de roteamento. Existem dois tipos de autenticação que podem ser configurados: simples e *MD5*. Na autenticação simples, a mesma senha é configurada em cada roteador e incluída em texto claro nos pacotes *OSPF*. Em contraste, a autenticação *MD5* utiliza chaves secretas compartilhadas, onde cada pacote *OSPF* enviado tem seu conteúdo combinado com a chave secreta para calcular um *hash MD5*. O roteador receptor verifica a autenticidade do pacote calculando seu próprio hash *MD5* e comparando-o com o valor recebido. Além disso, números de sequência são utilizados para proteger contra ataques de reenvio. Em relação aos caminhos múltiplos de igual custo, o *OSPF* permite o uso de vários caminhos até o destino quando estes possuem o mesmo custo, proporcionando maior flexibilidade e eficiência no roteamento. No que tange ao suporte para roteamento unicast e multicast, o *OSPF* integra essas capacidades, oferecendo suporte tanto para roteamento individual quanto para roteamento em grupo. O *multicast OSPF (MOSPF),* descrito no *RFC 1584*, fornece extensões ao *OSPF* para suportar roteamento em grupo, utilizando o banco de dados de enlaces existente no *OSPF* e acrescentando um novo tipo de anúncio de estado de enlace. Essas características avançadas fazem do *OSPF* uma escolha robusta e eficiente para o roteamento *intra-AS*, garantindo uma gestão otimizada e segura do tráfego de rede. O protocolo original de gateway interior da Internet, conhecido como *RIP*, utilizava o algoritmo de vetor de distância de Bellman-Ford, originado da *ARPANET*. Esse protocolo era eficaz em sistemas menores; contudo, à medida que os Sistemas Autônomos (SAs) expandiam, surgiam diversos problemas. O *RIP* enfrentava desafios como o problema da contagem ao infinito e, geralmente, apresentava uma convergência lenta. Assim, em maio de 1979, ele foi substituído por um protocolo de estado de enlace (TANENBAUM, 1988). Em 1988, a *Internet*

Engineering Task Force iniciou o desenvolvimento de um sucessor, chamado *OSPF*, que se tornou um padrão em 1990. Vários fornecedores de roteadores adotaram o *OSPF*, tornando-o o principal protocolo de gateway interior. O grupo que projetou o *OSPF* tinha uma lista extensa de requisitos, baseados em experiências com outros protocolos de roteamento. Primeiro, o algoritmo precisava ser amplamente conhecido na literatura técnica, justificando o "O" (de *Open*, ou aberto) na sigla *OSPF*. Soluções proprietárias de uma única empresa não seriam apropriadas. Em segundo lugar, o novo protocolo deveria suportar diversas unidades de medida de distância, incluindo distância física e latência. Terceiro, era necessário que o algoritmo fosse dinâmico, adaptando-se rapidamente às mudanças na topologia da rede. Uma inovação importante do *OSPF* era a capacidade de suportar roteamento baseado no tipo de serviço. O protocolo deveria ser capaz de rotear tráfego em tempo real de uma forma específica e outros tipos de tráfego de maneira diferente. Embora o protocolo *IP* incluísse um campo "*Type of Service*", nenhum protocolo de roteamento existente o utilizava. O *OSPF* incorporou esse campo, que foi posteriormente removido devido à falta de uso. Outro requisito crucial era a capacidade de balancear a carga, distribuindo-a por múltiplas rotas. A maioria dos protocolos anteriores enviava todos os pacotes pela melhor rota disponível, ignorando a segunda melhor rota. Dividir a carga por várias rotas pode melhorar significativamente o desempenho da rede. Além disso, o *OSPF* precisava suportar sistemas hierárquicos. Em 1988, a Internet havia crescido tanto que nenhum roteador conseguia conhecer toda a topologia da rede. Portanto, o protocolo foi projetado para que nenhum roteador precisasse ter uma visão completa da topologia. A segurança também era uma preocupação importante. Era essencial evitar que usuários mal-intencionados enganassem os roteadores, enviando informações de roteamento falsas. Por fim, era necessário que o *OSPF* lidasse com roteadores conectados à Internet por meio de túneis, uma área na qual os protocolos anteriores tinham dificuldades. Estas considerações detalhadas asseguraram que o *OSPF* se tornasse um protocolo robusto e amplamente adotado para o roteamento *intra-AS* na Internet.

1.6 Vantagens do *OSPF* sobre o *RIP*

De acordo com Neves (2017) O *OSPF* e o *RIP* são dois protocolos de roteamento amplamente utilizados em redes de computadores. No entanto, *OSPF* oferece várias vantagens significativas sobre o *RIP*, tornando-o uma escolha preferida para muitas implementações de rede, especialmente em ambientes corporativos e de grande escala. Uma das principais vantagens do *OSPF* sobre o *RIP* é a sua eficiência em termos de convergência. *OSPF* utiliza o algoritmo de Dijkstra para calcular o caminho mais curto para cada destino na rede, o que permite uma convergência rápida e precisa. Por outro lado, o *RIP*, que baseia suas decisões de roteamento na contagem de saltos, pode demorar mais para convergir, especialmente em redes maiores, devido à sua natureza baseada em tabelas de roteamento que são atualizadas periodicamente. Além disso, o *OSPF* é um protocolo de roteamento de estado de enlace, enquanto o *RIP* é um protocolo de vetor de distância. Isso significa que o *OSPF* tem uma visão mais detalhada e global da topologia da rede, permitindo-lhe tomar decisões de roteamento mais informadas e precisas. Cada roteador no *OSPF* mantém uma cópia idêntica do banco de dados de estado de enlace, que é atualizado sempre que há uma mudança na topologia, garantindo que todos os roteadores tenham informações consistentes. De outro ponto de vista, o *RIP* só conhece a rota mais curta em termos de número de saltos, sem considerar outros fatores que podem influenciar o desempenho da rede. A escalabilidade é outra área onde o *OSPF* se sobressai. *OSPF* suporta hierarquias de áreas, que permite a divisão de grandes redes em áreas menores e mais manejáveis. Isso reduz o tráfego de atualização de roteamento e a carga sobre os roteadores, melhorando a eficiência e o desempenho geral da rede. Em comparação, o *RIP* não suporta essa hierarquização e pode sofrer com problemas de escalabilidade em redes extensas, onde o número de saltos e o tráfego de atualização podem se tornar impraticáveis. A flexibilidade do *OSPF* também se destaca em relação ao *RIP*. *OSPF* permite a atribuição de diferentes custos a diferentes tipos de links, permitindo uma otimização mais sofisticada do roteamento com base na largura de banda, latência e outros critérios. *RIP*, com sua métrica simples de contagem de saltos, não oferece esse nível de granularidade, resultando em roteamento menos eficiente. A segurança é outro aspecto importante em que o *OSPF* tem uma vantagem. *OSPF* suporta a autenticação dos pacotes de

roteamento, incluindo opções para autenticação simples e *MD5*, o que ajuda a proteger a integridade das informações de roteamento. O *RIP*, especialmente nas suas versões mais antigas, tem capacidades de autenticação muito limitadas, tornando-se mais vulnerável a ataques como a injeção de rotas falsas. Finalmente, a capacidade do *OSPF* de suportar redes maiores e mais complexas faz dele uma escolha superior para muitos administradores de rede. A robustez, flexibilidade e eficiência do *OSPF* o tornam mais adequado para ambientes corporativos e de *ISP*, onde a performance e a confiabilidade são críticas. Em resumo, as vantagens do *OSPF* sobre o *RIP* incluem uma convergência mais rápida e eficiente, uma visão detalhada da topologia da rede, melhor escalabilidade, maior flexibilidade na atribuição de custos de rotas e melhores capacidades de segurança.

1.7 Algoritmo de Dijkstra

Como cita Cormen (2009), no contexto do protocolo de roteamento *OSPF*, o algoritmo de Dijkstra desempenha um papel importante na determinação das rotas mais eficientes através da rede. *OSPF* é um protocolo de roteamento dinâmico de estado de enlace que utiliza o algoritmo de Dijkstra para calcular o caminho mais curto de um roteador para todos os outros roteadores dentro da mesma área de roteamento. O algoritmo de Dijkstra, desenvolvido por Edsger Dijkstra em 1956, é um método para encontrar os caminhos mais curtos em um grafo, que neste caso representa a topologia da rede *OSPF*. Cada roteador no *OSPF* possui uma visão completa da topologia da rede, conhecida como a base de dados de estado de enlace (*LSDB*), que é construída e mantida através do *flooding* de *LSAs (Link-State Advertisements)*. Com base nesta base de dados, cada roteador executa o algoritmo de Dijkstra para calcular a tabela de roteamento. O processo de cálculo das rotas pelo algoritmo de Dijkstra em *OSPF* funciona da seguinte forma: inicialmente, o roteador define o custo para si mesmo como zero e para todos os outros roteadores na rede como infinito. Esses custos são armazenados em uma tabela de distâncias. O roteador mantém um conjunto de nós (roteadores) cujas rotas mais curtas já foram determinadas. Inicialmente, este conjunto contém apenas o nó inicial (o próprio roteador). O algoritmo seleciona, entre os nós não visitados, aquele com o menor custo cumulativo a partir do nó inicial. Este nó é então adicionado ao conjunto de nós visitados. Para cada nó adjacente ao nó recém-adicionado, o algoritmo calcula o

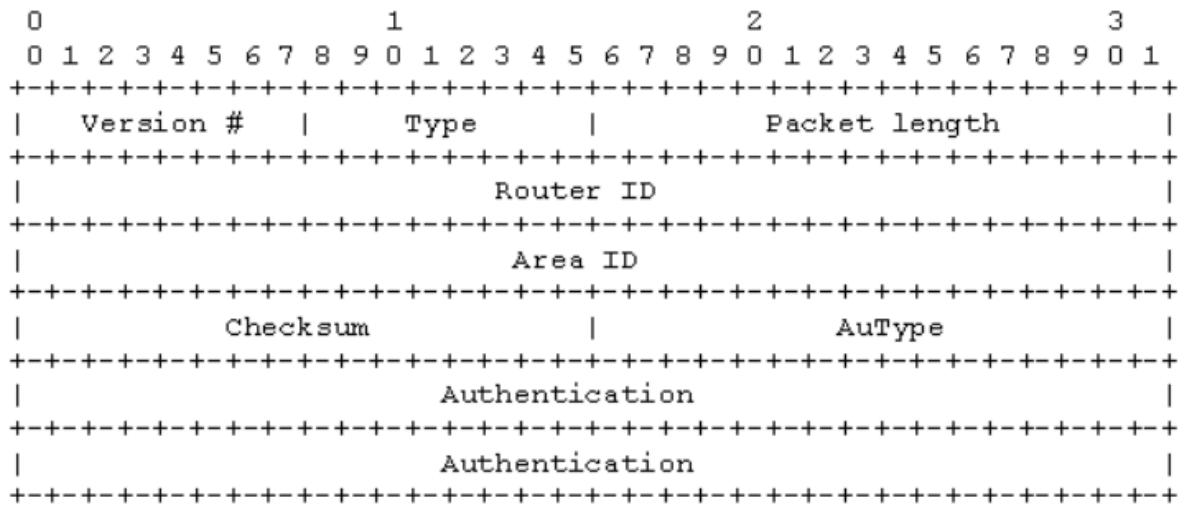
custo total do caminho até esse nó passando pelo nó recém-adicionado. Se esse custo for menor que o custo registrado anteriormente, o valor na tabela de distâncias é atualizado. O processo de seleção do próximo nó e atualização dos custos é repetido até que todos os nós tenham sido visitados e as rotas mais curtas para todos os nós tenham sido determinadas. Após a execução do algoritmo de Dijkstra, o roteador possui uma árvore de caminhos mais curtos, conhecida como a árvore de roteamento de caminho mais curto (*SPF tree*). A partir desta árvore, o roteador pode construir sua tabela de roteamento, que especifica a melhor rota para alcançar cada rede de destino. A eficiência do algoritmo de Dijkstra permite que o *OSPF* responda rapidamente a mudanças na topologia da rede. Sempre que ocorre uma alteração, como a falha de um enlace ou a adição de um novo roteador, as *LSAs* são atualizadas e disseminadas através do mecanismo de *flooding*. Cada roteador, ao receber as novas *LSAs*, atualiza sua *LSDB* e executa o algoritmo de Dijkstra para recalcular as rotas, garantindo que a rede converge rapidamente para uma nova configuração estável. Em resumo, o algoritmo de Dijkstra é fundamental para o funcionamento do *OSPF*, permitindo que cada roteador calcule as rotas mais eficientes com base em uma visão global da topologia da rede. Este método garante uma convergência rápida e uma operação eficiente, tornando o *OSPF* um protocolo robusto e confiável para grandes redes *IP*.

1.8 O cabeçalho dos pacotes *OSPF*

O pacote *OSPF* é essencial para o funcionamento do protocolo de roteamento *OSPF*, pois contém informações cruciais para a troca de informações de roteamento entre os roteadores que participam do protocolo. O cabeçalho do pacote *OSPF* possui uma estrutura bem definida e composta por vários campos: O campo Versão identifica a versão do protocolo *OSPF* sendo utilizada, ocupando 8 bits. O Tipo de Pacote indica o propósito do pacote, como pacotes *Hello, DBD* (*Database Description*), *LSR (Link State Request), LSU (Link State Update) e LSACK (Link State Acknowledgment*, também com 8 bits. O campo Tamanho do Pacote especifica o tamanho do pacote OSPF em bytes, incluindo o cabeçalho, e é representado por 16 bits. O *ID* de Roteador é um identificador único de 32 bits que indica o roteador que originou o pacote *OSPF*. O *ID* da Área identifica a área *OSPF* à qual o roteador pertence, também utilizando 32 bits. O *Checksum* é um campo de 16 bits que

garante a integridade do pacote durante a transmissão, usando um algoritmo de verificação de redundância cíclica (*CRC*). O *ID* do Autenticador é um campo opcional que pode ser utilizado para autenticar o pacote *OSPF*, enquanto o Tipo de Autenticação especifica o método de autenticação utilizado, como autenticação de texto claro, autenticação *MD5* ou *IPsec*. O Área Externa é utilizado apenas em pacotes *LSA* de Tipo-5 e anuncia redes externas na *OSPF*. O campo *OPC* (*Options*) contém flags que controlam o comportamento do protocolo *OSPF*, indicando suporte para áreas virtuais, múltiplas instâncias *OSPF*, entre outros. Por fim, a Lista de *LSAs* contém os *LSAs* incluídos no pacote *OSPF*, que fornecem informações detalhadas sobre a topologia da rede.

Figura 1 - Cabeçalho de um pacote *OSPF*



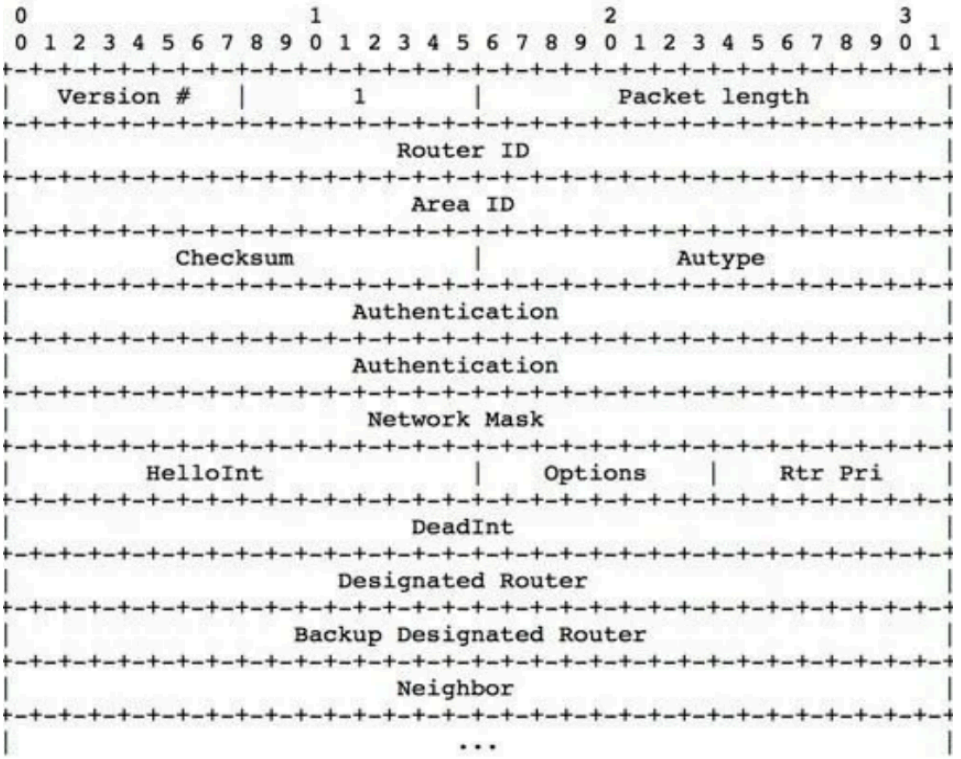
Fonte:
https://kambasdoip.wordpress.com/2015/05/27/ccnax-exame-200-120-ospf-custo-padrao-2/

1.8.1 Sobre o Pacote *HELLO*

Esse pacote é considerado do tipo 1. O pacote Hello é usado para descobrir vizinhos *OSPF* na mesma rede broadcast ou ponto a ponto. Ele é enviado periodicamente por cada roteador *OSPF* em intervalos configuráveis, geralmente a cada 10 segundos para redes broadcast e a cada 30 segundos para redes ponto a ponto. O *Network Mask* (Máscara de Rede) é um campo fundamental nos pacotes

OSPF que especifica a porção da rede de IP usada para identificar a sub-rede. Esta informação é essencial para o roteamento *IP*, permitindo aos roteadores *OSPF* determinar as redes vizinhas e calcular rotas. O *Hello Interval* (Intervalo Hello) é o período entre os pacotes *Hello* enviados por um roteador *OSPF* para descobrir e manter vizinhos *OSPF*. Este intervalo é utilizado para verificar se os vizinhos ainda estão ativos e disponíveis. Caso um roteador não receba um pacote *Hello* de um vizinho dentro do intervalo configurado, pode considerar o vizinho como inativo. *RtrPri (Router Priority - Prioridade do Roteador)* é um valor de 8 bits (de 0 a 255) usado para determinar a elegibilidade de um roteador *OSPF* para se tornar o *Designated Router (DR)* ou *Backup Designated Router (BDR - Roteador Designado de Backup)* em redes *broadcast*. Roteadores com uma prioridade maior têm uma chance maior de se tornarem *DR ou BDR*. *Router Dead Interval* (Intervalo de Inatividade do Roteador) é o tempo que um roteador *OSPF* espera antes de considerar um vizinho como inativo, caso não receba um pacote *Hello* do vizinho. Geralmente, esse intervalo é quatro vezes o intervalo Hello configurado. O *Designated Router* (*DR*) é um roteador *OSPF* eleito para representar uma rede broadcast, como *Ethernet*. Ele é responsável por originar as atualizações de *LSAs* para a rede e distribuí-las para os outros roteadores *OSPF* na mesma rede. O *DR* é eleito com base na prioridade do roteador (*RtrPri*), sendo o roteador com a maior prioridade o candidato mais provável a se tornar o *DR*. O *Backup Designated Router* é um roteador *OSPF* que assume a função de *DR* se o *DR* falhar ou se tornar inativo. Ele está preparado para assumir as funções do *DR* em caso de falha deste. A eleição do *BDR* segue os mesmos critérios de prioridade do roteador que a eleição do *DR*. *Neighbor* (Vizinho) refere-se a um roteador *OSPF* que estabeleceu uma adjacência com outro roteador *OSPF*. Os roteadores vizinhos trocam pacotes Hello e atualizações de estado de link (*LSAs*) para manter uma visão consistente da topologia da rede. A troca de informações entre vizinhos *OSPF* é essencial para a construção e manutenção das tabelas de roteamento *OSPF*.

Figura 2 - Pacote *HELLO*



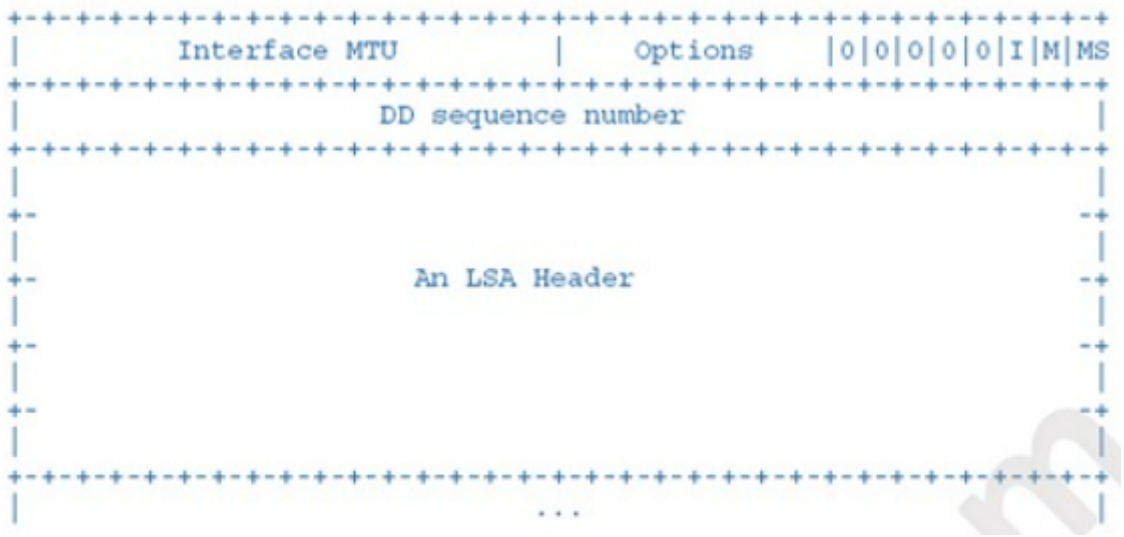
Fonte:
https://www.techrepublic.com/article/how-to-integrate-a-synolgy-nas-in-your-vmware-lab/

1.8.2 Pacote de descrição de base de dados

Os pacotes de descrição de base de dados (*DBD*) no protocolo *OSPF* são mensagens do tipo "tipo 2". Esses pacotes são trocados quando uma adjacência começa a se formar entre roteadores *OSPF* vizinhos e descrevem o conteúdo da topologia de rede. Durante a troca de *DBD*, múltiplos pacotes podem ser utilizados para descrever a base de dados, sendo um dos roteadores designado como mestre e o outro como escravo. O roteador mestre envia mensagens de descrição de base de dados (coleta), que são reconhecidas pelas mensagens de descrição enviadas pelo roteador escravo (respostas). O formato do pacote de descrição de base de dados é muito semelhante aos pacotes de requisição de estado de link (*LSR*) e *ACK* de requisição de estado de link (*LSACK*), sendo a parte principal deste pacote composta pelas informações de uma parte da base de dados da topologia de rede. A seguir, falarei sobre os campos desta mensagem, que incluem o cabeçalho. O

primeiro campo, "0", é reservado e possui um valor fixo de zero. Em seguida, o campo "*Options*" indica as capacidades opcionais suportadas pelo roteador, referentes ao Tipo de Serviço. O "*I-bit*" (*Bit Init*) é um bit que, quando setado para 1, indica que o pacote *DBD* é o primeiro da sequência. Já o "*M-bit*" (Bit Mais), quando setado para 1, indica que mais pacotes na sequência estão por vir. O "MS-bit" é um bit que indica se o roteador é mestre (1) ou escravo (0) durante o processo de troca de mensagens de *DBD*. Por fim, o campo "*DD sequence number*" (Número de Sequência do *DBD*) é um número de sequência das mensagens enviadas, que é incrementado até que toda a descrição da base de dados tenha sido enviada. Esses campos são fundamentais para garantir que os roteadores *OSPF* vizinhos mantenham uma visão consistente e atualizada da topologia da rede, promovendo a eficiência e a estabilidade das operações do protocolo *OSPF*. Estes campos permitem que os roteadores *OSPF* vizinhos sincronizem suas bases de dados de estado de link de forma eficiente e precisa.

Figura 3 - Pacote de descrição da base de dados



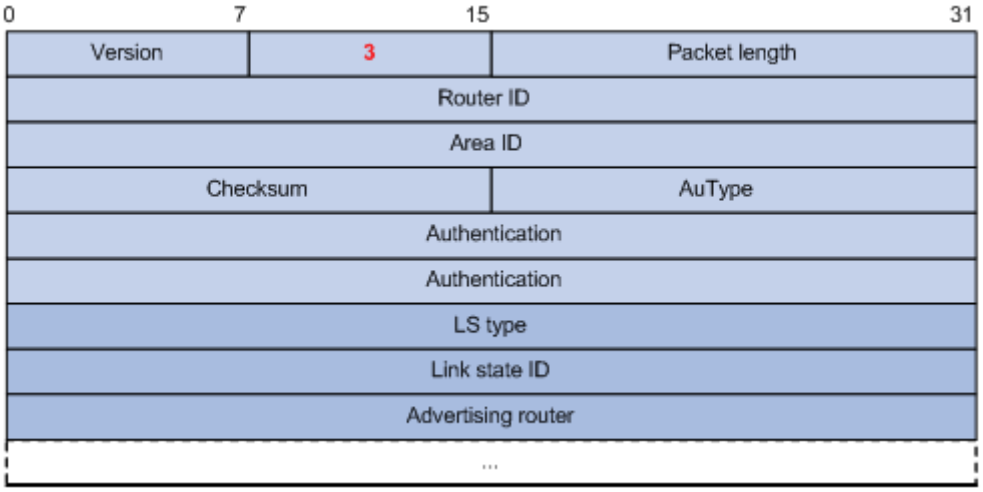
Fonte: https://ipwithease.com/ospf-dbd-database-descriptor-packets/

1.8.3 Pacote de requisição de estado de link

Os pacotes de requisição de estado de link (*LSR*) são identificados como tipo 3 no protocolo *OSPF*. Após a troca de pacotes de descrição de base de dados (*DBD*) com os roteadores adjacentes, um roteador *OSPF* pode identificar partes da

topologia que estejam desatualizadas. Os pacotes *LSR* são utilizados para solicitar informações de base de dados aos roteadores vizinhos, permitindo a atualização da própria base de dados de estado de link, caso necessário. Esse processo é essencial para garantir que todos os roteadores *OSPF* possuam uma visão consistente e precisa da topologia de rede. O envio dos pacotes *LSR* marca o último passo para estabelecer as adjacências *OSPF*. Quando um roteador *OSPF* envia um pacote *LSR*, ele especifica as partes específicas da base de dados de estado de link que necessita. Estas partes são definidas pelos campos de número de sequência de *LS, checksum* de *LS* e idade de *LS*, embora esses detalhes não sejam especificados diretamente no pacote *LSR*. Ao receber um pacote *LSR*, um roteador *OSPF* pode enviar versões atualizadas das informações solicitadas em resposta à requisição. Isso permite que os roteadores mantenham suas bases de dados de estado de link atualizadas e consistentes, o que é fundamental para o funcionamento adequado do *OSPF* na rede.

Figura 4 - Pacote de requisição de estado de link



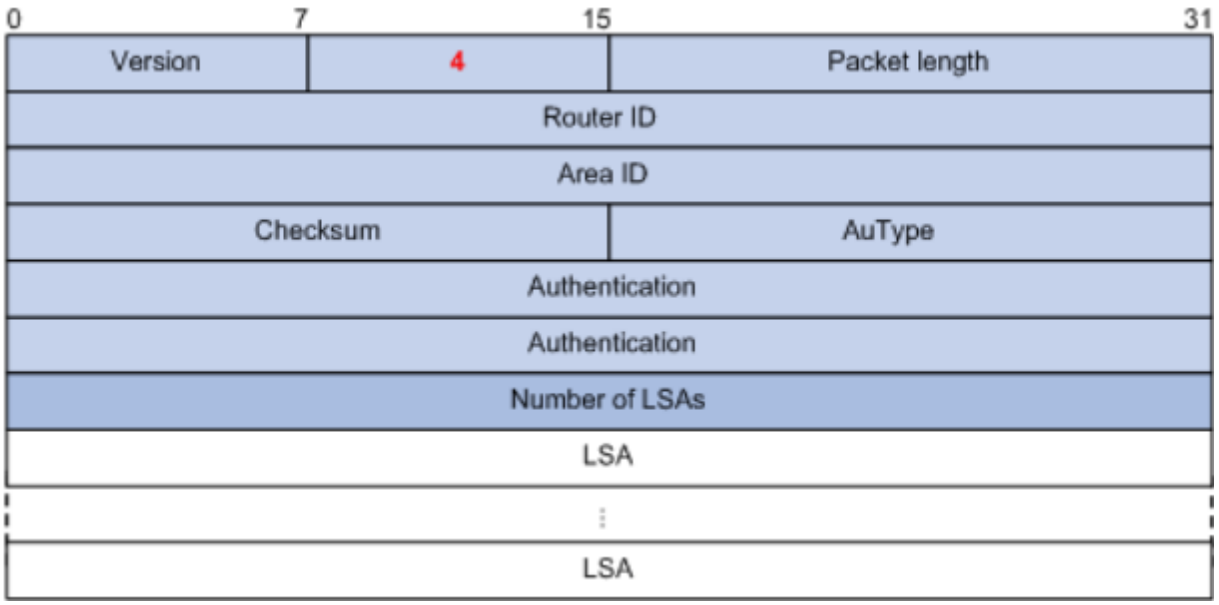
Fonte:
https://techhub.hpe.com/eginfolib/networking/docs/switches/3600v2/5998-7619r_l3-ip-rtng_cg/content/442284154.htm, Figure 28.

1.8.4 Pacote de atualização de estado de link

Os pacotes de atualização de estado de link (*LSU*) são responsáveis por distribuir informações de estado de link através da rede *OSPF*. Cada pacote *LSU*

contém uma coleção de informações de estado de link de um roteador além de sua origem. Isso significa que múltiplas atualizações de estado de link podem ser incluídas em um único pacote, otimizando a eficiência da transmissão. Os pacotes *LSU* são multicast em seus domínios físicos que suportam multicast/broadcast. Isso garante que todos os roteadores *OSPF* dentro do domínio recebam as atualizações de estado de link necessárias. Para assegurar que a transmissão desses pacotes de atualização seja confiável, eles são confirmados utilizando pacotes de confirmação correspondentes. Esse processo de "inundação" dos pacotes *LSU* é essencial para manter a sincronização das bases de dados de estado de link entre todos os roteadores *OSPF* dentro do mesmo domínio.

Figura 5 - Pacote de atualização de estado de link



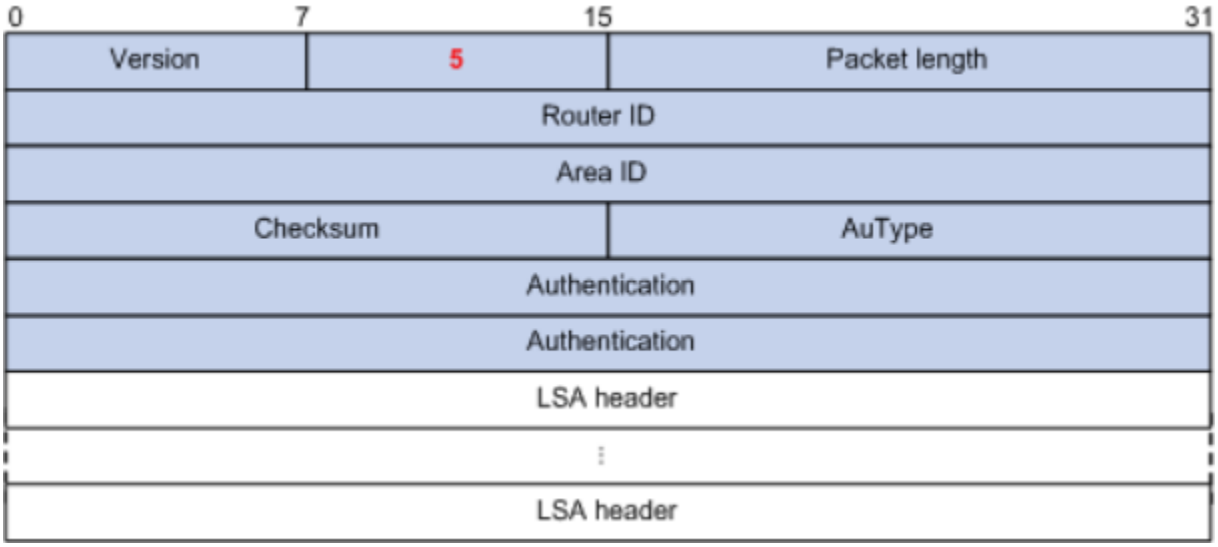
Fonte:
https://techhub.hpe.com/eginfolib/networking/docs/switches/3600v2/5998-7619r_l3-ip-rtng_cg/content/442284154.htm, Figure 29.

1.8.5 Pacote de *ACK* do estado de link

Para garantir a confiabilidade da transmissão dos pacotes de estado de link, eles são explicitamente confirmados. Essas confirmações são realizadas através da troca de pacotes de confirmação, mesmo que uma única confirmação possa ser usada para vários links contidos em um mesmo pacote. Dependendo do estado da

interface que envia e da fonte das informações sendo confirmadas, os pacotes são enviados tanto para o endereço *multicast AllSPFRouters e AllDRouters*, quanto como uma mensagem *unicast*. Esse procedimento assegura que todos os roteadores *OSPF* dentro do domínio recebam e confirmem as atualizações de estado de link de forma confiável.

Figura 6 - Pacote de ACK do estado de link



Fonte:
https://techhub.hpe.com/eginfolib/networking/docs/switches/3600v2/5998-7619r_l3-ip-rtng_cg/content/442284154.htm, Figure 30.

1.9 O protocolo de roteamento *OSPF*

Protocolos são conjuntos de diretrizes que governam a comunicação entre entidades, permitindo a troca de informações e mensagens. Nos ambientes de rede, os protocolos de roteamento desempenham um papel crucial ao facilitar a comunicação entre roteadores, essencial para a atualização dinâmica de suas tabelas de rotas através de algoritmos específicos de roteamento. Estes protocolos permitem que os roteadores selecionem o melhor caminho para o destino dos dados, preenchendo suas tabelas de roteamento e descrevendo o estado da rede. Na Internet, destacam-se dois tipos principais de protocolos de roteamento: os internos e os externos. Os protocolos externos são utilizados entre sistemas autônomos da Internet para facilitar a interconexão entre redes. Por exemplo, o *BGP*

(Border Gateway Protocol) utiliza o algoritmo de vetor de distância, enquanto o *EGP (Exterior Gateway Protocol)* é mais simples e é destinado a anunciar endereços *IP* internos para roteadores externos. Dentre os protocolos internos, o *RIP* utiliza o algoritmo de vetor de distância para construir tabelas de rotas dentro de um Sistema Autônomo (*AS*). Por outro lado, o *OSPF* é um protocolo de roteamento usado em sistemas autônomos para trocar informações de roteamento. Ao contrário do *RIP*, o *OSPF* pode obedecer a uma hierarquia e é baseado em estado de enlace, com roteadores trocando informações sobre os estados dos enlaces de comunicação ligados às suas portas (MOY, 1998). De acordo com John Moy em *"Anatomy of an Internet Routing Protocol"*, o *OSPF* oferece uma visão detalhada da topologia da rede por meio da troca de informações sobre os estados dos enlaces de comunicação entre os roteadores. Essa troca de informações permite que os roteadores tenham uma compreensão abrangente da rede, incluindo todos os caminhos disponíveis e os estados de conectividade de cada enlace. Essa visão detalhada da topologia da rede é fundamental para a segmentação da rede em áreas administrativas, permitindo que os administradores de rede dividam a rede em áreas lógicas menores para facilitar o controle de tráfego e reduzir a carga de processamento nos roteadores. Cada área administrativa pode ter suas próprias políticas de roteamento e configurações específicas, o que permite uma gestão mais eficiente e granular da rede. Além disso, o *OSPF* utiliza algoritmos sofisticados para calcular os caminhos mais curtos entre os roteadores, garantindo uma otimização eficaz do tráfego e uma rápida convergência da rede em caso de alterações na topologia. Esses aspectos contribuem significativamente para um desempenho robusto e confiável da rede, conforme detalhado por (Moy, 1995) em seu livro.

1.10 Assinaturas Digitais

A verificação de autenticidade de documentos legais, financeiros e de outros tipos é tradicionalmente realizada por meio de assinaturas autorizadas. Contudo, este método não é aplicável a fotocópias. Para que os sistemas de mensagens digitais possam substituir o transporte físico de documentos em papel, é imprescindível desenvolver um método de assinatura digital que seja infalsificável. A criação de um substituto para as assinaturas manuscritas é um desafio complexo. É necessário um sistema pelo qual uma parte possa enviar uma mensagem "assinada"

para outra parte, garantindo que o receptor possa verificar a identidade do remetente, que o remetente não possa repudiar o conteúdo da mensagem posteriormente, e que o receptor não possa forjar a mensagem. Por exemplo, o primeiro requisito é fundamental em sistemas financeiros. Quando o computador de um cliente solicita ao computador de um banco a compra de uma tonelada de ouro, o banco deve assegurar que o pedido realmente se origina da empresa titular da conta a ser debitada. O segundo requisito protege o banco contra fraudes. Imagine que o banco compre a tonelada de ouro e, em seguida, o preço do ouro caia drasticamente. Um cliente desonesto poderia processar o banco, alegando que nunca fez tal pedido de compra. Mesmo se o banco apresentasse a mensagem no tribunal, o cliente poderia negar seu envio. Esta característica, onde nenhuma das partes de um contrato pode negar tê-lo assinado posteriormente, é conhecida como não repúdio. Os esquemas de assinatura digital ajudam a assegurar o não repúdio. O terceiro requisito protege o cliente no caso de o preço do ouro subir drasticamente, evitando que o banco falsifique uma mensagem assinada na qual o cliente supostamente solicitava apenas uma barra de ouro em vez de uma tonelada. Neste cenário fraudulento, o banco ficaria com o restante do ouro para si. Estes requisitos evidenciam a importância de um sistema de assinaturas digitais robusto e confiável, que assegure a integridade e autenticidade das comunicações digitais, substituindo de forma segura as assinaturas manuscritas em documentos físicos.

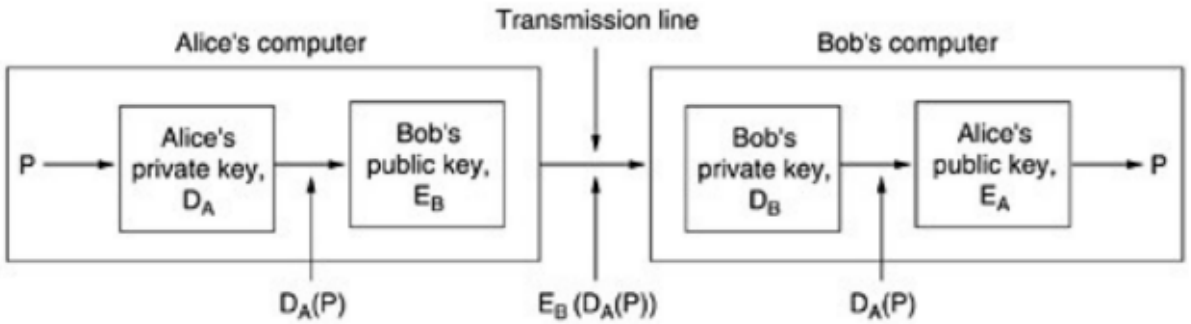
1.10.1 Assinaturas de chaves públicas

Um problema fundamental com a utilização da criptografia de chave simétrica para assinaturas digitais é a necessidade de confiar em uma autoridade central, frequentemente referida como Big Brother. Além disso, essa autoridade precisa ter acesso a todas as mensagens assinadas. Os candidatos mais óbvios para operar o servidor central incluem o governo, bancos, contadores e advogados. Contudo, nenhuma dessas entidades inspira confiança absoluta em todos os cidadãos. Portanto, seria ideal se a assinatura de documentos não requeresse a intervenção de uma autoridade confiável. Felizmente, a criptografia de chave pública oferece uma solução promissora para este dilema. Vamos supor que os algoritmos de criptografia e descriptografia de chave pública possuam a propriedade de que $E(D(P)) = P$, além da propriedade habitual de que $D(E(P)) = P$. O algoritmo RSA

(Rivest-Shamir-Adleman) possui essa característica, portanto, essa suposição é razoável. Considerando esse cenário, Alice pode enviar uma mensagem de texto simples assinada, P, para Bob, transmitindo EB(DA(P)). Alice conhece sua própria chave de descriptografia (privada), DA, assim como a chave pública de Bob, EB; portanto, a criação dessa mensagem é algo que Alice pode realizar. Para entender como a assinatura digital funciona, suponha que posteriormente Alice negue ter enviado a mensagem P para Bob. Se a disputa chegar aos tribunais, Bob poderá apresentar tanto P quanto DA(P). O juiz poderá facilmente verificar que Bob possui uma mensagem válida criptografada por DA aplicando EA à mensagem. Como Bob não conhece a chave privada de Alice, a única forma de ele ter obtido uma mensagem criptografada por essa chave seria se Alice realmente a tivesse enviado. Enquanto enfrenta acusações de perjúrio e fraude, Alice terá bastante tempo para refletir sobre novos algoritmos de chave pública. Apesar da elegância do uso da criptografia de chave pública para assinaturas digitais, existem desafios relacionados ao ambiente operacional e não ao algoritmo em si. Por exemplo, Bob só poderá provar que uma mensagem foi enviada por Alice enquanto DA permanecer secreta. Se Alice divulgar sua chave secreta, qualquer um, inclusive Bob, poderia ter enviado a mensagem. Suponha que Bob seja o corretor de ações de Alice. Alice solicita a Bob que compre ações ou títulos de uma determinada empresa. Logo após a compra, o preço das ações despenca. Para negar a autoria da mensagem enviada a Bob, Alice pode alegar à polícia que sua casa foi roubada e seu computador, contendo a chave privada, foi levado. Dependendo da legislação local, Alice pode ou não ser processada, especialmente se alegar que só descobriu o roubo várias horas depois. Outro problema surge se Alice decidir alterar sua chave. Embora isso seja legal e, provavelmente, uma boa prática de segurança, pode complicar questões jurídicas futuras. Se um caso semelhante ao descrito anteriormente surgir, o juiz aplicará a chave pública atual EA a DA(P) e descobrirá que não produz P, complicando a situação de Bob. Em teoria, qualquer algoritmo de chave pública pode ser usado para assinaturas digitais. O padrão de facto da indústria é o algoritmo *RSA*, amplamente utilizado em produtos de segurança. No entanto, em 1991, o *NIST (National Institute of Standards and Technology)* propôs uma variante do algoritmo de chave pública de El Gamal como parte do novo padrão *DSS* (*Digital Signature Standard*). A segurança do El Gamal é baseada na dificuldade de calcular

logaritmos discretos, ao contrário da dificuldade de fatorar números grandes, como no caso do *RSA*.

Figura 7 - Assinaturas digitais com o uso da criptografia de chave pública



Fonte: Tanenbaum (1988, p. 569)

1.10.2 MD5

Diversas funções de resumo de mensagens foram propostas ao longo do tempo, com destaque para o *MD5 (Rivest, 1992)* e o *SHA-1 (NIST, 1993)*. O *MD5* é a quinta função de uma série desenvolvida por Ronald Rivest. Esta função atua embaralhando os bits de forma complexa, de modo que todos os bits de saída são influenciados por todos os bits de entrada. Inicialmente, o *MD5* expande o tamanho da mensagem até atingir 448 bits (módulo 512). Em seguida, o tamanho original é anexado como um inteiro de 64 bits, resultando em uma entrada cujo tamanho é múltiplo de 512 bits. Antes de iniciar os cálculos, um buffer de 128 bits é inicializado com um valor fixo. Os cálculos começam com a extração de um bloco de 512 bits de entrada, que é então inserido no buffer de 128 bits. Para aumentar a precisão dos cálculos, é utilizada uma tabela derivada da função seno. A escolha de uma função conhecida como o seno visa evitar suspeitas de que o projetista tenha introduzido uma vulnerabilidade intencional, e não porque a função seja mais aleatória do que um gerador de números aleatórios. A decisão da *IBM* de não divulgar os princípios de projeto das caixas S do *DES* gerou muita especulação sobre possíveis armadilhas secretas. Cada bloco de entrada passa por quatro rodadas de processamento. Esse processo continua até que todos os blocos de entrada sejam processados. O conteúdo final do buffer de 128 bits constitui o resumo da mensagem. O *MD5* está em uso há mais de uma década e tem sido alvo de muitos

ataques. Algumas vulnerabilidades foram identificadas, mas certas etapas internas do algoritmo dificultam a sua quebra total. No entanto, se as defesas internas restantes do *MD5* forem comprometidas, ele poderá eventualmente falhar. Apesar disso, até o momento, o *MD5* continua a ser resistente e amplamente utilizado.

1.11 Autenticação no *OSPF*

O *OSPF* é um protocolo de roteamento aberto amplamente utilizado, especialmente na certificação Cisco *CCNA (Cisco Certified Network Associate)*. Por padrão, o *OSPF* não utiliza autenticação em suas trocas de mensagens, mas oferece dois métodos opcionais para aumentar a segurança da comunicação entre os roteadores. Um dos métodos de autenticação é a autenticação de pacotes, que permite que os roteadores *OSPF* participem de domínios de roteamento com base em senhas pré-configuradas pelo administrador. Isso ajuda a garantir que apenas roteadores autorizados possam trocar informações de roteamento. Outra opção é a autenticação de pacotes com criptografia, que adiciona uma camada adicional de segurança ao criptografar as informações de roteamento trocadas entre os roteadores *OSPF*. Isso torna mais difícil para invasores interceptar e interpretar as mensagens de roteamento, aumentando a segurança da rede. Essas medidas de autenticação ajudam a proteger a integridade e a confiabilidade das informações de roteamento no *OSPF*, contribuindo para uma comunicação mais segura entre os roteadores. A autenticação *OSPF* criptografa os pacotes *OSPF* ao incluir um campo de autenticação dos mesmos, garantindo a segurança da rede. Um dispositivo local verifica o campo de autenticação nos pacotes *OSPF* recebidos de um dispositivo remoto e descarta os pacotes se não contiverem a mesma senha de autenticação configurada localmente, proporcionando autodefesa. Em termos de tipo de pacote, a autenticação *OSPF* é categorizada da seguinte maneira: Autenticação de Área: configurada na visualização da área *OSPF* e se aplica aos pacotes recebidos por todas as interfaces na área *OSPF*. Autenticação de Interface: configurada na visualização da interface e se aplica a todos os pacotes recebidos pela interface. Em relação ao tipo de autenticação de pacote, a autenticação *OSPF* é classificada da seguinte forma: Sem autenticação: A autenticação não é realizada. Autenticação simples: Uma senha configurada é adicionada diretamente aos pacotes para autenticação. Esse método de autenticação é inseguro. Autenticação com algoritmo

de resumo de mensagem 5 (*MD5*): Uma senha configurada é hashada usando um algoritmo como *MD5*, e a senha criptografada é adicionada aos pacotes para autenticação. Esse método de autenticação melhora a segurança da senha. Atualmente, MD5 e código de autenticação de mensagem baseado em hash para *HMAC-MD5 (Hash-based Message Authentication Code using SHA-256)* são os algoritmos suportados. Devido à insegurança dos métodos simples, *MD5* ou *HMAC-MD5*, é recomendável usar um método de autenticação mais seguro. Autenticação de corrente de chave: Uma corrente de chave consiste em várias chaves de autenticação, cada uma contendo um *ID* e uma senha. Cada chave tem um ciclo de vida, e as chaves são selecionadas dinamicamente em uma corrente de chave com base no ciclo de vida de cada uma. Uma corrente de chave também pode selecionar dinamicamente uma chave de autenticação para reforçar a defesa contra ataques. A autenticação *HMAC-SHA256*: Uma senha configurada é hashada usando o algoritmo *HMAC (Hash-based Message Authentication Code)* para o algoritmo de hash seguro 256 *(HMAC-SHA256)*, e a senha criptografada é adicionada aos pacotes para autenticação. Esse método de autenticação melhora a segurança da senha.

CAPÍTULO II

Procedimento Metodológico

Bastos e Keller (1995, p. 53) afirmam que a pesquisa científica é uma exploração metódica sobre um tema específico, visando esclarecer os aspectos em análise. Conforme Gil (2002, p. 17), a pesquisa torna-se necessária quando não há informações suficientes para resolver o problema ou quando os dados disponíveis estão tão desorganizados que não podem ser devidamente correlacionados com o problema. A pesquisa científica possui diversas modalidades, incluindo a pesquisa bibliográfica, que será discutida nesta monografia, detalhando todas as etapas necessárias para sua execução. Este tipo de pesquisa é descrito por vários autores, entre eles Marconi e Lakatos (2003) e Gil (2002). O presente trabalho foi realizado através de uma pesquisa bibliográfica, que consiste na revisão da literatura relacionada à temática abordada. Para tanto, foram utilizados livros, periódicos, artigos, sites da Internet entre outras fontes. De acordo com Boccato (2006), a pesquisa bibliográfica busca a resolução de um problema (hipótese) por meio de referenciais teóricos publicados, analisando e discutindo as várias contribuições científicas. Esse tipo de pesquisa trará subsídios para o conhecimento sobre o que foi pesquisado, como e sob que enfoque e/ou perspectivas foi tratado o assunto apresentado na literatura científica. A pesquisa proposta tem como objetivo identificar os desafios e problemas relacionados à autenticação no protocolo *OSPF*, incluindo possíveis vulnerabilidades, limitações na implementação e manutenção, e as dificuldades enfrentadas pelos administradores de redes. Compreender essas questões é essencial para garantir a integridade e a segurança das redes que utilizam o *OSPF*. Além disso, o estudo busca descrever os principais métodos de autenticação utilizados no *OSPF*, analisando suas características, vantagens, desvantagens e impactos na segurança e eficiência da rede. Ao explorar as vulnerabilidades associadas a cada método de autenticação, a pesquisa pretende propor melhorias ou alternativas para mitigar essas vulnerabilidades, contribuindo assim para a segurança e robustez do protocolo *OSPF*. É fundamental identificar quais aspectos específicos de cada método podem ser aprimorados para fortalecer a defesa contra ataques e garantir que a comunicação entre os roteadores permaneça

segura e confiável. A investigação também se dedica a examinar como as práticas atuais de autenticação no *OSPF* podem ser aprimoradas para enfrentar ameaças emergentes. Com o avanço constante das tecnologias e a evolução das ameaças cibernéticas, é importante que as soluções de autenticação sejam dinâmicas e adaptáveis. Por fim, este estudo visa fornecer uma visão abrangente sobre a autenticação no protocolo *OSPF*, destacando os desafios e propondo soluções práticas para melhorar a segurança e a eficiência das redes de computadores. Ao abordar essas questões, a pesquisa espera contribuir para o desenvolvimento de redes mais seguras e robustas, capazes de resistir às crescentes ameaças no cenário digital atual.

2.1 Análise e discussão dos dados

Em termos de eficiência de convergência, o *OSPF* se destaca significativamente. Segundo Kurose (2013), o *OSPF* utiliza o algoritmo de Dijkstra para calcular os caminhos mais curtos, o que resulta em uma convergência rápida e precisa. Moy (1998) complementa ao destacar que o *OSPF* oferece uma visão detalhada da topologia da rede, permitindo rápida adaptação a mudanças. Em contraste, o *RIP* apresenta uma eficiência de convergência inferior. Kurose (2013) observa que o *RIP*, ao utilizar uma simples contagem de saltos, pode demorar mais para convergir, especialmente em redes maiores. Neves (2017) reforça essa visão ao apontar que o *RIP*, sendo baseado em tabelas de roteamento atualizadas periodicamente, apresenta uma convergência mais lenta comparada ao *OSPF*. No quesito segurança, o *OSPF* também leva vantagem. Kurose (2013) e Neves (2017) mencionam que o *OSPF* suporta autenticação simples e MD5, fornecendo uma camada adicional de segurança. A *RFC* 1321 (Rivest, 1992) detalha o funcionamento do *MD5*, que é usado no *OSPF* para autenticação segura, prevenindo que informações incorretas sejam injetadas nas tabelas de roteamento. Moy (1998) destaca que essa camada de segurança é crucial para evitar que intrusos comprometam a rede. Em contrapartida, o *RIP* possui capacidades limitadas de autenticação, conforme observado por Neves (2017), tornando-o mais vulnerável a ataques. Quando é feita a análise da escalabilidade, o *OSPF* novamente demonstra superioridade. Kurose (2013) destaca que o *OSPF* suporta hierarquias de áreas, permitindo a divisão de grandes redes em segmentos menores e mais

manejáveis, o que melhora a eficiência e desempenho. Neves (2017) afirma que essa capacidade de hierarquização permite uma melhor escalabilidade em grandes redes. Por outro lado, o *RIP* é limitado pelo custo máximo de 15 saltos, como mencionado por Kurose (2013), o que restringe seu uso a sistemas autônomos menores. Neves (2017) reforça que o *RIP* pode enfrentar problemas de escalabilidade em redes extensas devido à sua simples métrica de contagem de saltos. A flexibilidade na atribuição de custos é outro ponto onde o *OSPF* se destaca. Kurose (2013) indica que o *OSPF* permite a atribuição de diferentes custos a diferentes tipos de links, possibilitando uma otimização mais sofisticada. Neves (2017) aponta que essa flexibilidade resulta em um roteamento mais eficiente baseado em múltiplos critérios como largura de banda e latência. Em contraste, o *RIP* utiliza uma métrica simples de contagem de saltos, conforme mencionado por Kurose (2013), sem considerar outros fatores que influenciam o desempenho da rede. No suporte a redes complexas, o *OSPF* é claramente preferido. Kurose (2013) e Moy (1998) destacam que o *OSPF* é adequado para redes de grande escala e complexas, oferecendo suporte para segmentação em áreas administrativas e roteamento eficiente. Neves (2017) também observa que o *OSPF* é amplamente adotado em ambientes corporativos e de *ISPs* devido à sua robustez e flexibilidade. Em contrapartida, Neves (2017) indica que o RIP é mais adequado para redes menores e menos complexas, como *ISPs* de nível inferior e redes corporativas simples. Dados complementares e comparativos reforçam essas análises. Em redes que utilizam *OSPF*, a convergência é mais rápida e eficiente, o que é crítico para manter a rede operacional durante falhas ou mudanças. Estudos comparativos mostram que *OSPF* pode se adaptar a alterações na topologia em segundos, enquanto o RIP pode levar minutos. Redes *OSPF*, com suas capacidades de autenticação avançadas, são menos suscetíveis a ataques como injeção de rotas falsas. Comparativamente, redes usando *RIP* são mais vulneráveis devido à falta de autenticação robusta. *OSPF* é projetado para escalar eficientemente em grandes redes através da segmentação em áreas, enquanto RIP enfrenta limitações em redes com mais de 15 saltos. *OSPF* permite uma gestão granular dos custos de enlace, facilitando o roteamento otimizado, enquanto a abordagem simples de contagem de saltos do *RIP* não oferece a mesma flexibilidade. Finalmente, *OSPF* é preferido em ambientes corporativos e *ISPs* devido ao seu suporte para redes

hierárquicas e complexas, enquanto o *RIP* é mais limitado a redes menores e menos dinâmicas.

No *OSPF*, dois principais métodos de autenticação são utilizados: autenticação simples e autenticação *MD5*. A autenticação simples utiliza uma senha de texto simples que é incluída nos pacotes *OSPF*. Porém, a principal vulnerabilidade deste método é que a senha é transmitida sem criptografia, o que significa que pode ser facilmente interceptada por hackers que possuem acesso à rede. Isso torna o método inadequado para ambientes que necessitam de alta segurança. Por outro lado, a autenticação *MD5* utiliza o algoritmo de *hash MD5* (Message Digest 5) para criar uma assinatura criptográfica dos pacotes *OSPF*. A senha é combinada com os dados do pacote para gerar um hash, que é incluído no pacote enviado. Mesmo que o *MD5* seja mais seguro que a autenticação simples, ele não é completamente invulnerável. A técnica de colisão, onde dois diferentes conjuntos de dados produzem o mesmo hash *MD5*, é uma das vulnerabilidades conhecidas. Além disso, o *MD5* não oferece proteção contra ataques de repetição. Para enfrentar ameaças emergentes, a autenticação no *OSPF* pode ser melhorada adotando métodos de autenticação mais robustos e modernos. A utilização de algoritmos de hash mais avançados, como *SHA-256* ou *SHA-3*, pode substituir o *MD5*, oferecendo maior resistência a ataques de colisão e força bruta. A implementação de *SHA-256* ou *SHA-3* no *OSPF* tornaria a autenticação mais segura contra vulnerabilidades conhecidas do *MD5*. Outra opção seria o uso de *HMAC (Hash-based Message Authentication Code)* com *SHA-256*, que oferece uma forma de autenticação menos suscetível a ataques de repetição e colisão. *HMAC* inclui uma chave secreta adicional no processo de hash, proporcionando uma camada extra de segurança, assegurando tanto a integridade dos dados quanto a autenticidade das mensagens *OSPF*. Além disso, protocolos de segurança de rede adicionais como *IPsec (Internet Protocol Security)* podem ser implementados para proteger os pacotes OSPF. IPsec oferece autenticação, integridade e criptografia, tornando a interceptação e modificação de pacotes muito mais difícil, e pode ser configurado para fornecer uma camada robusta de segurança para todos os pacotes de roteamento, incluindo *OSPF*. A implementação de diferentes métodos de autenticação tem impactos variados na eficiência e segurança da rede. A autenticação simples é muito eficiente em termos de processamento, pois não requer cálculos complexos, mas a segurança é muito baixa, tornando-o inadequado

para ambientes que exigem proteção contra interceptação e ataques de injeção de pacotes. A autenticação *MD5* é relativamente eficiente, com overhead moderado de processamento, já que a maioria dos roteadores modernos pode calcular *hashes MD5* rapidamente. Em termos de segurança, oferece uma melhora em relação à autenticação simples, mas ainda é vulnerável a ataques de colisão e repetição. A segurança é considerada aceitável para muitas aplicações, mas não para ambientes altamente seguros. Métodos como *SHA-256* ou *HMAC* introduzem um maior overhead de processamento em comparação com *MD5*, o que pode afetar a eficiência da rede, especialmente em roteadores com menos capacidade de processamento. No entanto, são significativamente mais seguros que *MD5*, fornecendo resistência contra uma ampla gama de ataques, incluindo colisões e repetição, sendo ideais para ambientes que exigem alta segurança. Por fim, o uso de *IPsec* pode introduzir um overhead substancial devido à necessidade de criptografia e decriptografia de pacotes, impactando o desempenho em redes de alta velocidade ou em dispositivos com limitações de processamento. Apesar disso, oferece o mais alto nível de segurança, garantindo a integridade, autenticidade e confidencialidade dos pacotes *OSPF*, sendo ideal para ambientes onde a segurança é crítica. Em resumo, a autenticação no *OSPF* pode ser melhorada através dos métodos de hash mais fortes como *SHA-256* ou *HMAC* e pela implementação de IPsec para uma segurança completa dos pacotes de roteamento. Embora métodos avançados de autenticação possam introduzir algum overhead de processamento, o aumento da segurança justifica este custo em ambientes críticos. Portanto, a escolha do método de autenticação deve equilibrar as necessidades de segurança e a capacidade de processamento dos dispositivos de rede.

Considerações finais

As considerações finais deste estudo sobre os métodos de autenticação no protocolo *OSPF* visam responder às questões problemáticas apresentadas na introdução, revisitar as hipóteses formuladas e verificar se os objetivos foram alcançados. Ao longo deste trabalho, foi identificado e analisado os desafios e problemas relacionados à autenticação no *OSPF*, incluindo possíveis vulnerabilidades, limitações na implementação e manutenção, bem como as dificuldades enfrentadas pelos administradores de redes. Observa-se que os principais métodos de autenticação utilizados no *OSPF*, como a autenticação simples, *MD5* e *HMAC*, apresentam características distintas, com vantagens e desvantagens que impactam a segurança e eficiência da rede. Confirma-se a hipótese de que a autenticação *MD5* proporciona maior segurança em comparação com a autenticação simples, devido ao uso de chaves secretas e hashes criptográficos. No entanto, reconhece-se que, apesar de sua robustez, o *MD5* não está isento de vulnerabilidades, o que justifica a necessidade de melhorias contínuas. A hipótese de que a implementação correta e consistente de métodos de autenticação robustos pode mitigar a maioria dos ataques ao *OSPF* também foi validada, enfatizando a importância de práticas adequadas de gerenciamento de segurança. Nossa análise das vulnerabilidades associadas a cada método de autenticação e a proposta de melhorias ou alternativas contribuíram para o entendimento das formas de fortalecer a segurança e a melhora do protocolo *OSPF*. Além disso, exploramos como as práticas atuais de autenticação podem ser aprimoradas para enfrentar ameaças emergentes, garantindo uma comunicação segura e confiável entre roteadores em ambientes de rede complexos. Em relação à metodologia utilizada, constatou-se que a pesquisa bibliográfica profunda em livros especializados e artigos acadêmicos foi suficiente para realizar os procedimentos necessários e obter uma compreensão abrangente sobre os métodos de autenticação no *OSPF*. No entanto, reconhece-se algumas limitações, como a ausência de experimentos práticos ou estudos de caso que poderiam enriquecer ainda mais a análise. Este estudo ampliou significativamente a compreensão sobre o tema, revelando não apenas os desafios atuais, mas também apontando direções para futuros estudos. Descobriu-se que, além das vulnerabilidades conhecidas, há a

necessidade de explorar novas ameaças e desenvolver métodos de autenticação ainda mais avançados e seguros. Como recomendações para futuros estudos, sugere-se a realização de experimentos práticos para testar a eficácia das melhorias propostas e a investigação de novas técnicas criptográficas que possam ser aplicadas ao *OSPF*. Ademais, estudos focados na integração de soluções de autenticação com outras camadas de segurança da rede podem oferecer uma visão mais holística e reforçada da proteção contra ataques. Conclui-se que os objetivos deste trabalho foram alcançados, proporcionando uma contribuição relevante para a área de segurança de redes no contexto do protocolo *OSPF*.

Referências Bibliográficas

Bastos, L. C., & Keller, B. A. (1995). Fundamentos da Pesquisa Científica. São Paulo: Editora Acadêmica.

Boccato, V. R. da S. (2006). Metodologia da pesquisa bibliográfica na área odontológica*. São Paulo: Artes Médicas.

Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). Introduction to Algorithms. MIT Press.

Day, J. D. (1995). The OSI reference model. In Networks and telecommunications, 21-26.

Gil, A. C. (2002). Como Elaborar Projetos de Pesquisa (4. ed.). São Paulo: Atlas.

Kurose, J. F., & Ross, K. W. (2013). Redes de Computadores e a Internet: Uma Abordagem Top-Down. Pearson.

Marconi, M. A., & Lakatos, E. M. (2003). Fundamentos de Metodologia Científica (5. ed.). São Paulo: Atlas.

Moy, J. (1998). OSPF: Anatomy of an Internet Routing Protocol. Addison-Wesley.

Neves, Jailton Santos das Neves. O Protocolo OSPF. Academia.edu. 2017. Disponível em: https://www.academia.edu/download/30249810/ospf.pdf. Acesso em: 20 maio 2024.

Ross, J. (2008). Redes de Computadores. Editora Julio Ross.

Rivest, R. (1992). The MD5 Message-Digest Algorithm. RFC 1321. Disponível em: https://tools.ietf.org/html/rfc1321. Acesso em: 20 maio 2024.

Soares, L. F. G., Lemos, G., & Colcher, S. (1995). Redes de Computadores: das LANs, MANs e WANs às Redes ATM. Rio de Janeiro: Campus.

TANENBAUM, Andrew S. Computer Networks. 2nd ed. Englewood Cliffs: Prentice Hall, 1988.