UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

CAMILA RODRIGUES

TÉCNICA DE TRANSIÇÃO: IPV4 PARA IPV6

MONOGRAFIA

CURITIBA
2015

CAMILA RODRIGUES

TÉCNICA DE TRANSIÇÃO: IPV4 PARA IPV6

Monografia apresentada como requisito parcial à obtenção do título de Especialista no Curso de Pós Graduação em Configuração e Gerenciamento de Servidores e Equipamentos em Redes, do Departamento de Eletrônica, da Universidade Tecnológica Federal do Paraná.
Orientador: Prof. MsC. Juliano de Mello Pedroso

CURITIBA
2015

AGRADECIMENTOS

Agradeço a oportunidade de ter adquirido tanto conhecimento através da Universidade Tecnologia do Paraná, assim como os professores e colegas de classe, que estiveram presentes ensinando e apoiando.

Aos meus professores Juliano de Mello Pedroso e Augusto Foronda pela orientação e dedicação oferecida.

Ao Alex Sander Faria pelo incentivo e compreensão.

Aos meus familiares que possibilitaram a concretização deste sonho.

Aos meus amigos Daniel Kaiss e Danilo Renato de Assis pelo apoio e ajuda.

E a todos os nãos citados que intencionalmente ou não contribuíram nesta fase tão importante na minha carreira profissional e pessoal.

RESUMO

RODRIGUES, Camila. **Técnicas de Transição IPv4 e IPv4 com implementação IPSec.** 2015. 54 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

A presente monografia aborda o estudo para a implantação de técnicas de transição sobre IPv6, demonstrando diferenciais e características dentre algumas existentes, mostrar as vantagens de ativar IPSec em redes IPv6. O projeto inicializa-se utilizando método bibliográfico, seguido de estudo de caso, criação de um túnel em uma rede com funcionamento inicial em IPv4 que realize a troca de pacotes com hosts IPv6. O resultado será a pratica e a eficácia das técnicas de tunelamento

Palavras-chave: Redes. IPv6. IPv4. Túnel. Técnica de Transição. IPSec.

ABSTRACT

RODRIGUES, Camila. **Technical IPv4 and IPv4 transition with IPSec implementation**. 2015 54 f. Monograph (Specialization in Server Configuration and Management and Network Equipment). Federal Technological University of Paraná. Curitiba, 2015.

This monograph deals with the study for the implementation of IPv6 transition techniques, demonstrating differences and characteristics among some existing, show the advantages of enabling IPSec for IPv6 networks. The project starts up using literature method, followed by case study, creating a tunnel in a network with an initial operation in IPv4 conducting the exchange packets with IPv6 hosts. The result will be the practice and effectiveness of the techniques of tunneling.

Keywords: Networks. IPv6. IPv4. Tunnel. Technical Transition. IPSec.

LISTA DE SIGLAS

ARPANET - *Advanced Research Projects Agency Network*

ACL - *ACL - Access Control List*

AH – *Authentication Header*

DNS - *Domain Name System*

3-DES - *Triple Digital Encryption Standard*

DHCP - *Dynamic Host Configuration Protocol*

ESP – *Encapsulating Security Payload*

FTP – *File Transfer Protocol*

GRE - *Generic Routing Encapsulation*

ICMP - *Internet Control Message Protocol*

IANA - *Internet Assigned Numbers Authority*

IP – *Internet Protocol*

IPSec- *Internet Protocol Security*

IPv4- *Internet Protocol Version 4*

IPv6- *Internet Protocol Version 6*

ISATAP - *Intra-Site Automatic Tunnel Addressing Protocol*

LAN – *Local Area Network*

NAT - *Network Address Translation*

MD5 - *Message Digest 5*

OSI - *Open Systems Interconnection*

RFC - *Request for Comments*

RSVP - *Resource Reservation Protocol*

RIP – *Routing Information Protocol Next Generation*

RIPng - *Routing Information Protocol*

SLA - *Service Level Agreement*

TCP - *Transmission Control Protocol*

TCP/IP - *Transmission Control Protocol over Internet Protocol*

UDP - *User Datagram Protocol*

SHA - *secure hash algorithm*

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

1.1 TEMA

Com o aumento da internet e o número de equipamentos utilizando endereços ips, temos hoje o esgotamento do protocolo ipv4, o qual trouxe a necessidade de adaptar as tecnologias para a usabilidade do protocolo ipv6.

A Internet tem uma rica variedade de protocolos relacionados à camada de rede. Entre eles, encontram-se o protocolo de transporte de dados, o IP, os protocolos de controle ICMP, ARP e RARP, e os protocolos de roteamento OSPF e BGP. A Internet está esgotando rapidamente os endereços IP, e foi desenvolvida uma nova versão do IP, o IPv6, para resolver esse problema. (TANENBAUM, 2003, p. 364).

Como nem todos os equipamentos e tecnologias estão preparados e moldados para funcionarem no ipv6, será necessária a utilização de técnicas que farão o transporte das informações independente do protocolo que estiver previamente configurado.

Será detalhada cada técnica de transição dos protocolos e dentre as existentes escolhida duas para implementação em uma rede de computadores. O caso de uso trará detalhamento da configuração utilizada para criar um túnel onde os dados trafegaram de forma segura usando ambos os protocolos.

1.2 OBJETIVOS

1.2.1 Objetivos Gerais

Realizar uma comparação entre as técnicas de tunelamento existentes e determinar uma implementação pratica utilizando o software *Cisco Packet Tracer*, simulador de rede que possibilita aos usuários praticarem as mais diversas soluções para redes com equipamentos Cisco.

Será criada uma topologia de rede, a qual os protocolos ipv4 e ipv6 estarão funcionando de forma simultânea.

1.2.2 Objetivos Específicos

Para detalhar os objetivos gerais descritos acima, tornando assim, mais compreensivo o entendimento para leitor, observe os itens que também devem ser estudados:

- Especificar o funcionamento do protocolo ipv4: Cabeçalho, endereçamento, rede, etc.
- Estudo do protocolo ipv6.
- Informações sobre os mecanismos de transição. Comparação entre as mesmas.
- Caracterizar os motivos que levaram a necessidade de utilizar a técnica de tunelamento.
- Importância da camada de rede.
- Importância e implementação IPSec no túnel.

1.3 JUSTIFICATIVA

É tão relevante que a transição dos protocolos funcione de forma correta e simultânea, logicamente para isto é necessária uma adaptação de outros recursos e tecnologias.

Para solucionar problemas como à não adaptação de equipamentos que suportem o protocolo ipv6, temos a necessidade de que haja uma comunicação concreta e segura entre os protocolos ipv4 e ipv6. Independente da infraestrutura, tipo de software ou hardware usado.

A técnica de transição, conhecida assim, por tunelamento, se faz, de extrema importância e auxilio para esse procedimento, ela é a responsável pela migração entre os protocolos. E esta, vem a ser a principal justificativa para elaboração e aplicação em redes, para que as mesmas funcionem com endereçamento ipv4 ou ipv6 simultaneamente. Sem necessidade de alterações dos endereços inseridos nas configurações inicias.

Como ainda existe pouco material prático que demonstre passo – a –passo de uma técnica de transição o trabalho em si, tem por demonstrar com um breve tutorial que permitirá os dados trafegarem usando protocolos ipv4 e ipv6 na rede.

Solucionando assim, os problemas atuais, possibilitando uma evolução e ampliação ainda maior da nossa rede.

1.4 METODOLOGIA

A metodologia a ser utilizada será através da coleta de informações, usando pesquisas bibliográficas, tais como, livros, revistas cientificas, as quais irão fundamentar e tornar mais objetivos os dados acolhidos.

A busca em websites direcionados aos assuntos abordados, também ajudarão no incremento de novos conhecimentos.

A leitura de artigos científicos, publicados, vão permitir uma abordagem mais concreta e coerente, da mesma forma que mostrarão novos itens para estudos.

Na pesquisa descritiva será realizado um estudo de caso, que demonstrará de forma pratica o sistema de tunelamento entre protocolos de diferentes tipos.

1.5 PROCEDIMENTOS METODOLÓGICOS

Para que o projeto traga um bom embasamento teórico, a divisão será feita da seguinte forma:

- Definição sobre Redes
- Breve explicação do Modelo TCP/IP
- Função da Camada Rede
- Endereçamento IPV4
- Descrição do protocolo IPV6
- Técnicas de tunelamento

2 REFENCIAIS TEORICOS

2.1 REDES DE COMPUTADORES

Para que fique claro o funcionamento das técnicas de transição é preciso conhecer alguns conceitos, os quais iniciamos nossas definições falando sobre o que é uma rede de computadores.

Hoje com toda a evolução tecnológica, tanto referente a dispositivos e aparelhos, quanto aos sistemas que realização seu funcionamento e comunicação. Faz muitas vezes pensar em como isso ocorre.

As redes conectam pessoas e promovem uma comunicação não controlada. Todos podem se conectar, compartilhar e fazer a diferença (CISCO, 2015).

Uma rede de computadores é formada por dois ou mais dispositivos que interligados, juntamente com uma implementação logica, são sistemas e protocolos, realizam o compartilhamento de informações, dados e funcionalidades. Por exemplo, permitir que uma impressora atenda a várias maquinas ou um software seja instalado em um local físico e disponibilizado para outros equipamentos.

Podemos classificar as redes pelo seu tamanho, pela quantidade de equipamentos, topologia aplicada e a distância a qual serão transmitidos os dados e como ocorrerá esse processo. Por exemplo, uma Lan (*Local Area Network*), conhecida como rede local, formada por algumas maquinas conectadas através de um hub, switch ou roteador. Por outro lado, temos, a internet, uma rede muito mais complexa e de longa distância, aliás podemos dizer que ocupa o mundo todo. Por isso onde estivermos podemos acessar qualquer tipo de dado armazenado na nuvem.

Para que seja bem sucedia a realização deste compartilhamento de recursos é preciso seguir um padrão, desde cabeamento de cabos, ao roteamento das maquinas, etc. Segundo Tanembaum, Existem muitos fabricantes e fornecedores de redes, cada qual com sua própria concepção de como tudo deve ser feito. Sem coordenação, haveria um caos completo, e os usuários nada conseguiriam. A única alternativa de que a indústria dispõe é a criação de alguns padrões de rede. (Tanembaum, 2003). Para que haja uma padronização da estrutura foram criados alguns protocolos, entre os mais utilizados encontramos TCP/IP e OSI.

2.1.1 Modelo TCP/IP

O Modelo de referência TCP/IP foi desenvolvido em meados da década de 70, seu nome vem de dois protocolos, TCP e (*Transmission Control Protocol* - Protocolo de Controle de Transmissão) e IP (*Internet Protocol* - Protocolo de Internet), é um conjunto de protocolos de comunicação de arquitetura aberta, que realizam a transmissão dos dados entre equipamentos na rede, quando é usado um modelo, os computadores por exemplo, conseguem enviar e receber os pacotes usando uma mesma regra, padronizando assim a forma na qual cada máquina da rede entenda o que foi enviado ou recebido. E é formado por quatro protocolos: aplicação, transporte, internet e acesso à rede (Figura 1). Pode ser aplicado em estruturas de rede como Token-Ring, Ethernet, Frame-Relay, FDDI, PPP, ATM, X.25 e várias outras que façam uso do protocolo TCP/IP.

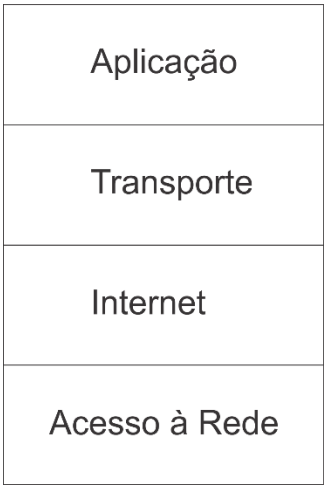

Figura 1 Modelo TCP/IP.
Fonte: própria

1. A camada de aplicação formada por vários protocolos e tem o papel de realizar a comunicação entre os aplicativos e a próxima camada, a de transporte. Os protocolos desta camada tem papeis importante para funcionamento de alguns serviços, por exemplo, enviar e receber e-mails, precisamos do SMTP, o conversor de nome: DNS, entre outros TELNET, FTP, DNS, TCP, UDP E IP.
2. A camada de Transporte é responsável por gerenciar o envio e recebimento os dados transmitidos pelos hosts e controla a o nível da conexão dessa

transmissão, verifica e separa pacote por pacote. Resumindo é quem realiza a conversação entre os pontos da rede. Os protocolos responsáveis por esse procedimento são o TCP e UDP

3. A camada de Internet utiliza o protocolo, o IP, responsável pelo endereçamento da rede, assim como o roteamento dos pacotes. Ele se preocupa apenas em definir a rota a qual os pacotes devem seguir. O IP é responsável por retirar os segmentos formatados do TCP, encapsulá-los em pacotes, atribuir a eles endereços apropriados, além de entregá-los pelo melhor caminho ao host destino (CISCO, 2015).
4. A camada de Acesso à rede é a principal responsável por fazer os mais diversos equipamentos de hardware se comunicarem, ele adapta um dos protocolos e cria uma comunicação do host com a rede e vice-versa. Conhecida também como camada de host/rede.

Uma rede que utiliza o padrão TCP/IP precisa que seus equipamentos tenham sido devidamente configurados, o número IP, Default Gateway e Máscara de sub-rede.

2.1.2 Camada De Rede

A camada de rede ou conhecida também por Camada 3, realiza o processo desde a saída até a entrega dos pacotes da rede. Ela realiza o endereçamento, encapsulamento, roteamento e por fim desencapsulamento.

A camada de rede deve escolher os caminhos mais apropriados atrás da rede. (TANENBAUM, 1997).

Inicialmente, todo e qualquer dispositivo precisa ter um endereço na rede, da mesma forma que você é reconhecido por seu carteiro pelo endereço da sua casa, os equipamentos da rede precisam de uma identificação, o IP. O protocolo ip é o principal responsável pela comunicação entre a rede e o host, ele quem identifica a mensagem enviada da origem até o destino correto, porém nesse trajeto podem ocorrer algumas dificuldades as quais faz o pacote chegar fora de ordem, ser duplicado ou até mesmo perdido.

O Ip é composto de um cabeçalho, o qual compõem do ip de origem, destino e conteúdo (dados a serem enviados). Veja os campos que compõem o endereço IP na Figura 2. Desde a implantação do protocolo usa-se a versão 4. Porém nos dias atuais enfrentamos alguns problemas, entre eles, o endereçamento ip esgotou-se,

devido ao aumento das redes, assim como a tabela de roteamento, e algumas dificuldades em priorizar pacotes e assegurar o conteúdo enviado.

A camada de rede também inclui o ICMP, *Internet Control Message Protocol*, que funciona juntamente com o protocolo ip, responsável por enviar mensagens entre roteadores, exemplo, caso um precise de algum tipo de orientação, ou caso aconteça erros ao enviar o datagrama. O ICMP retorna informando os motivos e o tipo de problema ocorrido.

O ICMP permite aos gateways enviar mensagens de erros ou de controle a outros gateways ou hosts. ICMP provê comunicação entre os softwares de IP numa máquina e o software de IP numa outra máquina. (ARTOLA, 2015)

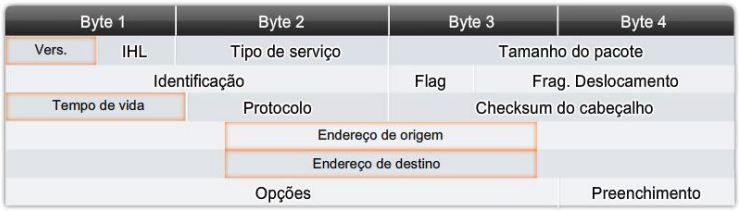

Figura 2 Campos do IP.

Fonte: CISCO Exploration, 2014

2.1.3 Endereçamento IPv4

O IPv4 é utilizado desde 1983 quando foi implantado na *Advanced Research Projects Agency Network* (ARPANET), que foi a precursora da Internet. A Internet é baseada principalmente em IPv4, que ainda é o protocolo de camada de rede mais amplamente usado. (CISCO Exploration, 2014).

O ipv4 é a versão 4 do protocolo IP, que tem por objetivo trafegar informações entre hosts e redes, graças a ele podemos ter acesso a internet e realizar usufruir dos inúmeros recursos que nos oferece. Após o seu aumento ao longo dos anos, considerado de fácil configuração e mesmo após seu termino, ainda enfrenta resistência a mudanças, por isso o uso do ipv6 vem sendo adiado ou usado através de tuneis, que permitem a comunicação entre ambas as versões de ip.

É composto de 8 bytes ou 32 bits para endereçamento, o qual suporta cerca de 4 bilhões de endereços, os quais foram divididos em rede e host e classificados em classes observe a Tabela 1 que apresenta os principais detalhes.

Tabela 1 Principais Classes IPv4.

Classe	Nº de Endereços	Endereçamento	Formato
Classe A	Pouco mais de 16 milhões	0.0.0.0 à 127.255.255.255	Rede|HOST|HOST|HOST
Classe B	Pouco mais de 65.000 mil	128.0.0.0 à 191.255.255.255	Rede|Rede|HOST|HOST
Classe C	256	192.0.0.255 à 223.255.255.255	Rede|Rede|Rede|HOST

Fonte: própria

O IPv4 tem um grande problema relacionado a segurança, inicialmente quando foi desenvolvido o proposito não exigia níveis proteção dos pacotes, tanto que se precisamos autenticar os dados necessitamos de protocolos auxiliares, a maioria dos ataques que ocorrem nas redes é devido a esse déficit do IPv4.

Quando os dados são transportados de um host para outro, o cabeçalho do ip é responsável por como e de que forma, serão transmitidos. Veja a Figura 3 que contém a representação do cabeçalho ipv4, onde é composto no total por 12 campos.

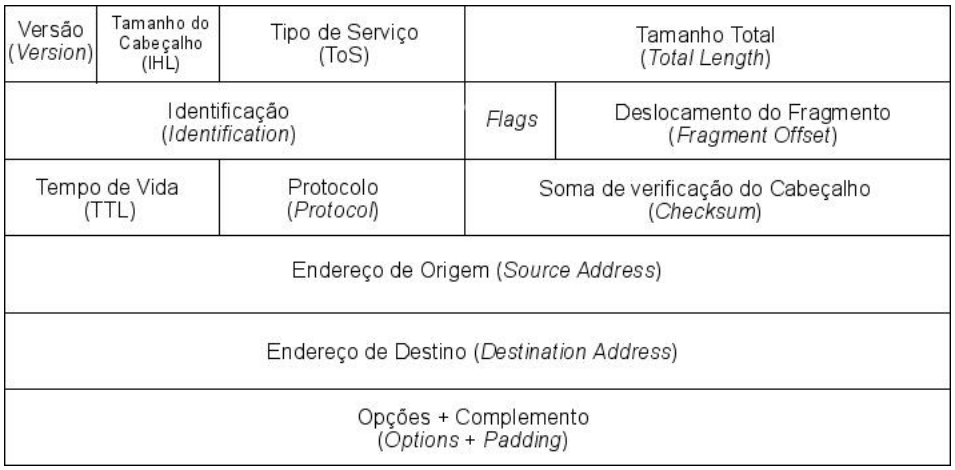

Figura 3 Cabeçalho IPv4.

Fonte: Nic.Br

2.1.4 Protocolo IPv6

O protocolo IPV6 foi criado por vários motivos, logicamente que o principal entre eles era pelo esgotamento dos endereços da versão ipv4, onde seria implementado gradativamente nas redes. Porém, os endereços na versão ipv4 terminaram antes do ipv6 ser totalmente adaptado.

De acordo com a CISCO, o IPv6 fornece algumas melhorias: espaço de endereço aumentado, melhor tratamento de pacotes, elimina a necessidade do NAT e segurança integrada.

No protocolo ipv6 podemos encontrar vários novos recursos, tais como, o roteamento entre os dispositivos é mais eficaz, o IPSec já vem com sua implementação ativa.

Era possível ter aproximadamente 4 bilhões de endereços na versão ipv4, já na versão 6 do ip temos mais de 340 undecilhões de endereços, quantidade a qual muitos estudiosos da área acreditam ser suficiente para atender os equipamentos de cada indivíduo do mundo. Algumas tecnologias poderão ser empregadas, não só em ou dentro das redes de computadores, mas em aparelhos eletrônicos, por exemplo, SmartGrid, que como principal objetivo facilitar a vida dos seus consumidores, ele oferece a facilidade de controlar e gerenciar os eletrônicos da rede, porem para que tal tecnologia seja implementada, será necessário um endereço ip para cada equipamento, com o uso do protocolo ipv6 podemos utilizar um endereço para cada item, possibilitando leitura remota dos medidores, tarifação diferenciada, interoperabilidade, escalabilidade, correção de falhas com maior rapidez. Facilitando assim, a vida do usuário, na economia financeira e no tempo gasto ao solucionar problemas, resumindo o ipv6 tem muitas vantagens a serem exploradas, o que causa certo desconforto é o seu formato de endereçamento.

O ipv6 tem a forma de endereçamento um pouco diferente da versão 4, são divididos em 8 conjuntos de 16 bits cada, por isso o total passou de 32 para 128 bits e de decimais para hexadecimal. A separação entre os conjuntos é feita por: (dois pontos). Veja o endereço abaixo tanto configurados na versão ipv4 quanto ipv6:

- Endereço IPV4 10.1.7.211
- Endereço IPV6 fe80:0:0:0:0:0:a01:7d3

Outra vantagem é a implementação do ipv6 em hosts que estejam previamente configurados com endereços ipv4, como ainda temos equipamentos os quais suas tecnologias só funcionam na versão ipv4, ter um host que comunique –se em ambos os protocolos permite uma compatibilidade maior entre os hardwares.

O cabeçalho do ipv6 tornou-se mais simples e eficaz, temos tamanho fixo, 40 bytes, 8 campos, tempo minimizado das execuções de tarefas (overhead). Veja a Figura 4 que mostra os campos que fazem parte do datagrama do protocolo ipv6.

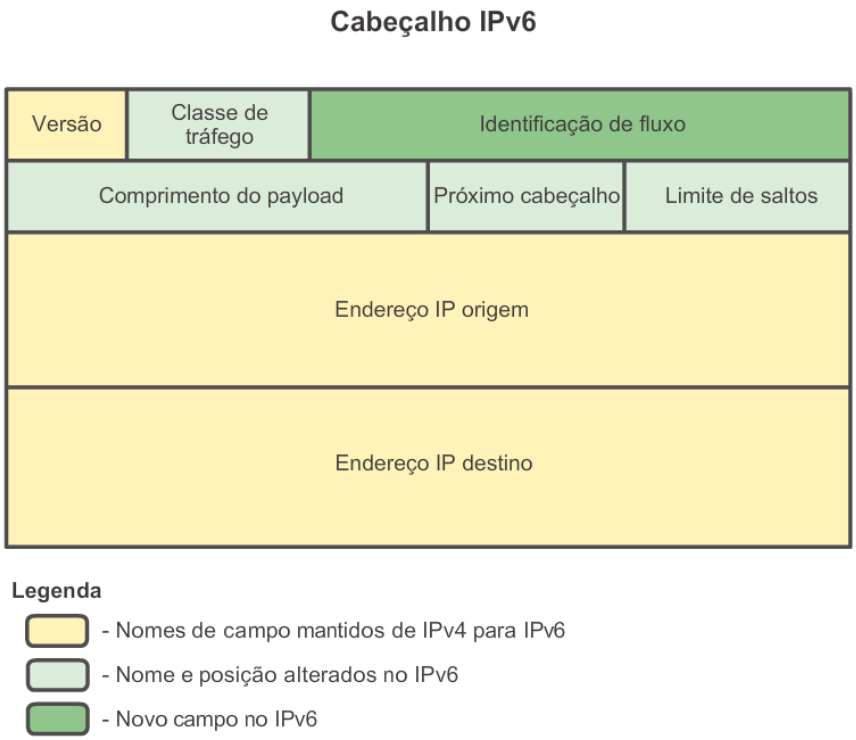

Figura 4 Cabeçalho IPv6.
Fonte: CISCO, 2015

Note alguns campos desapareçam em relação ao cabeçalho do ipv4, o Tamanho do Cabeçalho da internet, Identificação, Flag, Deslocamento de Fragmento, Checksum do Cabeçalho. Tais campos foram removidos por serem desnecessários, pois não precisamos mais mostrar o tamanho, já que o valor agora é fixo,

Podemos dizer que o protocolo na versão ipv6 foi desenvolvido para preservar a qualidade nos serviços, desde o processo da saída até a entrega do pacote. O cabeçalho do ipv6 é mais simplificado permitindo o roteamento entre

pacotes seja mais rápida, a conexão é fim-a-fim, pois não usa o NAT e endereços passaram de 32 bits para 128 bits. Campos do Datagrama cabeçalho ipv6:

- ✓ Campo classe de trafico (*Traffic Class*) - responsável pelos serviços da rede, quer dizer que o roteador vai priorizar o pacote, verificando o que e qual requisito o pacote forneceu.
- ✓ Campo versão - este campo é responsável por identificar a versão do pacote IP.
- ✓ Campo identificar de fluxo (*Flow Label*) - o campo terá por objetivo verificar quais pacotes precisem ser priorizados, por exemplo os pacotes gerados por multimídias, o roteador lê a qual fluxo pertence e determina qual tipo de tratamento.
- ✓ Comprimento do campo do Payload (*Payload Length*) – Traz a informação do tamanho total de bytes dos dados no pacote
- ✓ Prox. cabeçalho (*Next header*). Esse campo informa quais dos seis cabeçalhos de extensão (atuais) seguem esse cabeçalho, se houver algum. Se esse cabeçalho for o último cabeçalho do IP, o campo Next header revelará para qual tratador de protocolo de transporte (por exemplo, TCP, UDP) o pacote deverá ser enviado. (Tanenbaum, 2003)
- ✓ Limite de encaminhamento/saltos (*Hop Limit*) determina o número máximo de saltos que o pacote pode dar até ser descartado pelo roteador, impedindo assim que os saltos sejam eternos;
- ✓ Endereço de origem - É o endereço de origem do pacote
- ✓ Endereço de destino - É o endereço de destino do pacote.

2.1.4.1 Formato do Endereço IPv6

O formato do endereço IPv6 é composto por 8 grupos hexadecimais de 16bits, exemplo:

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

Para facilitar a demonstração do endereço são usadas algumas regras:

- ✓ Zeros a esquerda em cada duocteto podem ser omitidos, assim, 2001:CAAA:00CA:0000:000A:0000:0000:0001 pode ser representado por: 2001:CAAA:CA:0:A:0:0:1
- ✓ Quando ocorrer de ter grupos contínuos de zeros, podemos substituir por :: (quatro pontos) no endereço.

Exemplo:

O endereço 2001:CAAA:00CA:0000:000A:0000:0000:0001
Pode ser representado desta forma: 2001:CAAA:CA:0:A::1.

2.1.4.2 Tipos de Endereços

São divididos basicamente em três tipos:

- ✓ Unicast: utilizado principalmente em redes ponto-a-ponto, o pacote é entregue apenas a uma única interface IPv6. Segundo BIERINGER, por causa da definição original de endereços de site local não serem únicos, pode haver algum problema se duas redes já configuradas forem se conectar em um futuro próximo (overlap de subredes). Este e outros problemas foram os motivos para um novo tipo de endereço definido na RFC 4193 / Unique Local IPv6 *Unicast Addresses*.
- ✓ Multicast: Tipo de comunicação um-para-muitos significa que o endereço IPv6 identifica e envia várias interfaces para envio do pacote.
  O multicast é crucial para o funcionamento do IPv6, fazendo parte da essência da sua operacionalização por meio da criação/associação de vários grupos padronizados em que as interfaces passam a integrar no momento em que são ativadas (BRITO, 2013).
- ✓ Anycast: É enviado a várias interfaces simultaneamente, ele escolhe a interface mais próxima para entrega, definidos pela tabela de roteamento.
  Identifica um conjunto de interfaces, entretanto, um pacote enviado a um endereço multicast é entregue a todas as interfaces associadas a esse endereço. Um endereço multicast é utilizado em comunicações de um-para-muitos (Nic.br,2015).

Ao contrário do IPv4, o IPv6 não possui um endereço de broadcast. No entanto, há apenas um endereço multicast de todos os nós IPv6 que fornece essencialmente o mesmo resultado (CISCO,2015).

O IPv6 Unicast tem alguns tipos de endereços, *Unicast Global*, *Link local*, *Unique local*. Observe a Tabela 2, traz as características sobre os endereços.

Tabela 2 Endereços Unicast.

Global Unicast	**Link Local**	***Unique Local Address* (ULA)**
-Equivalente aos endereços públicos IPv4; -Globalmente roteável e acessível na Internet IPv6; -Ele é constituído por três partes: o prefixo de roteamento global, a identificação da sub-rede e a identificação da interface; -Exceto casos específicos, todas as sub-redes em IPv6 tem o mesmo tamanho de prefixo, 64 bits (/64), representação: 2000::/3.	-Pode ser usado apenas no enlace específico onde a interface está conectada; -Endereço link local é atribuído automaticamente utilizando o prefixo FE80::/64.	-Pode ser globalmente único; As são comunicações locais. Não deve ser roteável na Internet global; - Um endereço ULA é composto pelas seguintes partes: -**Prefixo:** FC00::/7. -**Flag Local (L):** se o valor for 1 (FD) o prefixo é atribuído localmente. Se o valor for 0 (FC), o prefixo deve ser atribuído por uma organização central. -**Identificador global:** identificador de 40 bits usado para criar um prefixo globalmente único. **Identificador da Interface:** identificador da interface de 64 bits.

Fonte: Adaptado de IPv6.br.br, 2015

No IPv6 *Unicast* temos os endereços especiais: *Loopback*; Endereço não especificado e IPv4 incorporado (Tabela 3);

Tabela 3 Endereços Especiais Unicast.

Não-Especificado (*Unspecified*)	Endereço Loopback	Endereços IPv4-mapeado
-Representado pelo endereço **0:0:0:0:0:0:0:0** ou **::0;** - Nunca deve ser atribuído a nenhum nó.	- Representado pelo endereço unicast: **0:0:0:0:0:0:0:1** ou **::1** **(**loopback **127.0.0.1)** -Utilizado para referenciar a própria máquina.	- Representado por **0:0:0:0:0:FFFF:wxyz** ou **::FFFF:wxyz;** Algumas faixas de endereços também são reservadas para uso específicos: -**2002::/16:** prefixo utilizado no mecanismo de transição 6to4; -**2001:0000::/32:** prefixo utilizado no mecanismo de transição TEREDO; **2001:db8::/32:** prefixo utilizado para representar endereços IPv6 em textos e documentações.

Fonte: Adaptado de Nic.br, 2015

Já o IPv6 Multcast tem apenas dois tipos:

- Multicast atribuído;
- Multicast do nó solicitado.

2.1.5 IPSec

IPSec (*IP Security*) é um recurso que permite que os hosts de uma rede envie e receba pacotes de forma segura independente do meio, definido pela RFC 4301.

Aumenta o nível de segurança dos dados criptografados compartilhados pelo host da rede IP. As informações, por exemplo, só irão se comunicar entre os equipamentos que estiverem devidamente configurados com IPSec, isso permite que os hosts se autentiquem mutuamente elevando a segurança na qual os dados são transmitidos (Figura 5). Ele fornece os seguintes serviços à rede.

Integridade dos dados (pacotes) verifica se não contém erros, se não foram alterados enquanto trafegam na rede ou estão corrompidos;

- ✓ Autenticação do host origem;

- ✓ Autenticação dos dados de origem;
- ✓ Privacidade nos dados (pacotes);
- ✓ Privacidade no fluxo dos dados (pacotes);
- ✓ Reenvio de pacotes;
- ✓ Confidencialidade de dados (criptografia chave simétrica), só abre o pacote ao destino que possui os dados de autenticação;
- ✓ Impede ataques de repetição/reprodução.

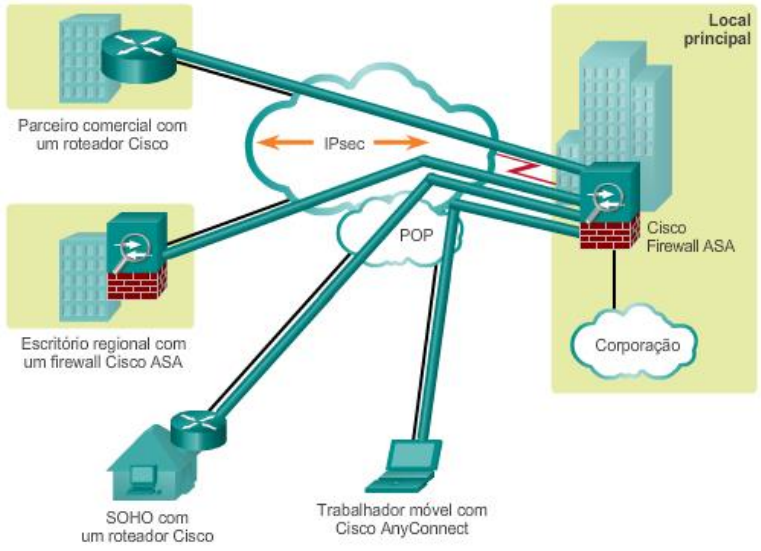

Figura 5 Funcionamento do IPSec.
Fonte CISCO, 2015

Podemos utilizar o IPSec nos modos de transporte e túnel.

É composto por diversas tecnologias, sendo que possui dois subprotocolos (Figura 6) principais que oferecem maior flexibilidade: AH e ESP. (BRITO 2013).

- AH: conhecido por IP *Autentication Header*, resumidamente oferece os recursos de autenticação e integridade dos dados, porém não ocorre criptografia e sim inclusão de assinatura digital.
- ESP: conhecido por IP *Encapsulating Security Payload*, que preza a confidencialidade, autenticação e integridade. Além da criptografia ocorre também a inclusão de assinatura digital.

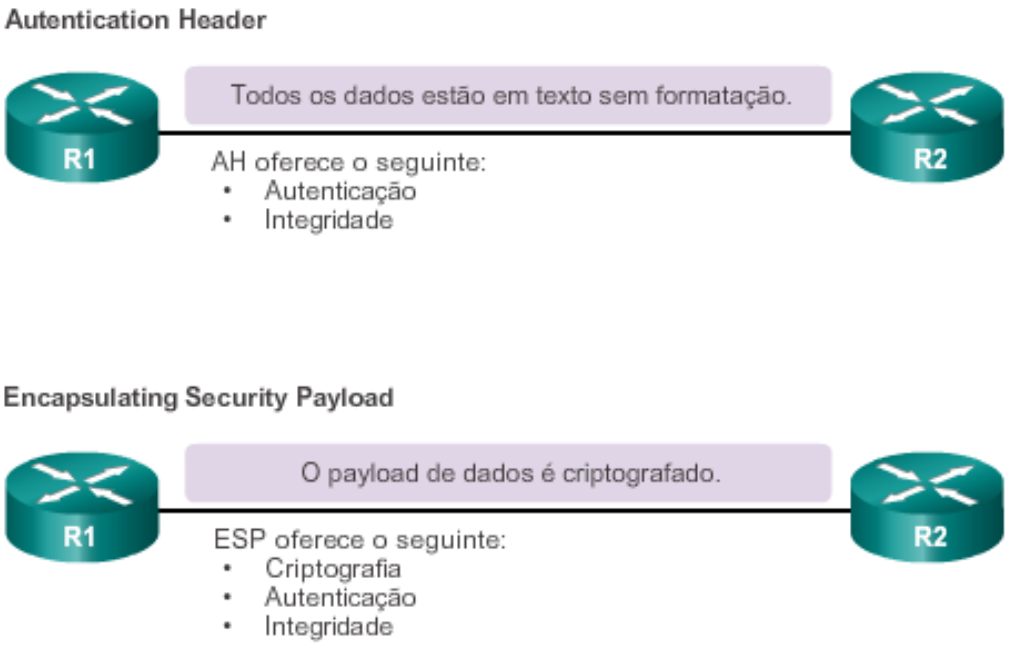

Figura 6 Estrutura de Protocolos IPSec.

Fonte: CISCO, Net. Academy.

Possui dois modos de operação conhecidos por transporte e túnel. Onde:

- Modo transporte: o cabeçalho não sofre alteração, somente os dados, os quais são criptografados.

Quando o modo de transporte é usado, o IPSec criptografa somente a carga de pagamento IP. O modo de transporte fornece a proteção de uma carga IP por meio de um cabeçalho AH ou ESP. As cargas IP típicas são segmentos TCP (contendo um cabeçalho TCP e dados de segmento TCP), uma mensagem UDP (contendo um cabeçalho UDP e dados de mensagem UDP) e uma mensagem ICMP (contendo um cabeçalho ICMP e dados de mensagem ICMP). (MICROSOFT, 2003).

- Modo Túnel: neste modo todo o pacote é criptografado ou autenticado, direcionado principalmente na comunicação *site-to-site*, ilhas na internet.

Segundo BRITO, é necessário que o pacote seja reencapsulado e receba um novo cabeçalho (túnel) ou, caso contrário, seria possível rodeá-lo pela internet.

2.1.5.1 Criptografia

Quando transportamos os pacotes pela rede utilizando criptografia matemos a privacidade entre eles, os dados só poderão ser lidos pelo receptor autorizado. O qual precisa saber as regras para descodificar a mensagem original enviada.

O grau de segurança depende do comprimento da chave do algoritmo de criptografia. À medida que o comprimento da chave aumenta, fica mais difícil decodificar a criptografia. No entanto, uma chave mais longa requer mais recursos do processador durante a criptografia e descriptografia de dados. (CISCO, 2015).

Temos dois tipos de criptografia:

- Criptografia simétrica: utilizam uma mesma chave, o qual é utilizado para criptografar e descriptografar os dados, conhecida também por criptografia de chave secreta (Figura 7).

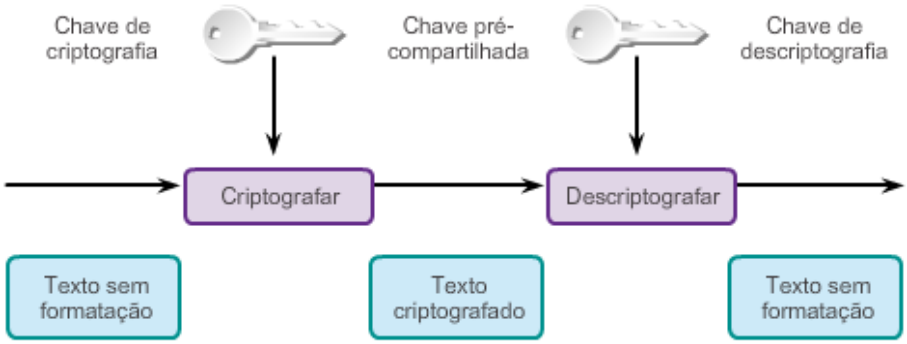

Figura 7 Criptografia simétrica.
Fonte: CISCO, Net. Academy.

- Criptografia assimétrica: faz uso de chaves diferentes tanto para criptografar os dados, quanto para descriptografar (Figura 8).

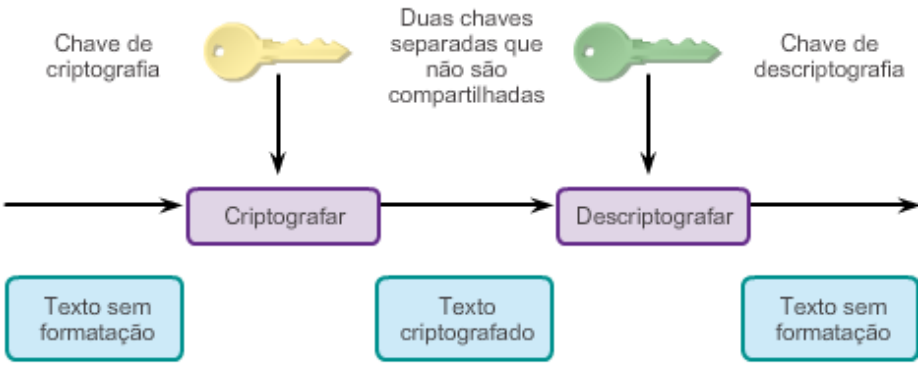

Figura 8 Criptografia assimétrica.

Fonte: CISCO, Net. Academy.

2.1.5.2 Autenticação

Ao implementar um túnel podemos aplicar autenticação nos dispositivos, desta forma tornamos o caminho seguro para transmitir os dados. São utilizadas duas maneiras de autenticar as extremidades da rede: PSK, chave secreta utilizada pelos dispositivos, a qual é formada pela combinação de informações. E assinaturas de RSA, utilizado pelo IPSec, ocorre a troca de certificados digitais únicos, para que ocorra a autenticação.

3 TECNICAS DE TRANSIÇÃO

As técnicas de tunelamento foram criadas pelo fato de que cada dia cresce o número de pessoas que fazem uso e criam equipamentos tecnológicos, isso fez com que a IANA (*Internet Assigned Numbers Authority*) anunciasse o fim dos endereços ips na versão 4, porém, mesmo com a criação do protocolo ipv6, sua implementação ainda pode demorar a ser totalmente aderida, muitos fatores influenciam, desde o software compatível encontrado em placas de rede ou sites já hospedados em servidores com suporte apenas a ipv4, por exemplo são alguns empecilhos encontrados. No geral o grande detalhe está na estrutura da rede e nos softwares (aplicações de rede), nem todo equipamento consegue entender ou funcionar no ipv6, a interoperabilidade entre os protocolos IPv4 e IPv6, tem sido grande causador do adiamento da implantação total do *Internet protocol* versão 6.

Pensando em soluções que fizessem os ips de versões diferentes trabalharem juntos, foram desenvolvidas e estudadas soluções temporários, neste caso temos as técnicas de tunelamento, que não são visíveis aos usuários finais, mais que fazem o ipv4 e ipv6 comunicarem e realizarem tarefas simultaneamente, de forma transparente. Desta forma, até que o ipv6 seja totalmente integrado nas redes, as técnicas de transição vão auxiliando para que as infraestruturas de rede consigam utilizar meios alternativos para a escassez de ips, entre outros problemas.

Dependendo de qual ação quer que ocorre entre os protocolos, podemos aplicar uma das técnicas, atualmente são destacados três tipos: Pilha dupla (Dual Stack), Tradução (Teredo), Tunelamento (Túneis). Cada uma age de forma diferenciada, a implementação vai de acordo com o objetivo do usuário. Acompanhe detalhes que explicam como essas técnicas funcionam, ao fim vou realizar a implementação de uma delas em uma topologia de rede configurada em IPv4, desta forma ficará mais fácil demonstrar sua real funcionalidade.

3.1 PILHA DUPLA

Técnica conhecida também por *Dual Stack* permite os equipamentos da estrutura física tenham datagramas para ambos os protocolos, desta forma eles tem a capacidade trabalhar com os dois pacotes, tanto o IPv4 quanto IPv6 para envio ou recebimento, a pilha armazena IPv4 e IPv6 e ao se comunicar com algum nó da

rede que seja IPv6 por exemplo o cabeçalho assume o IPv6, no caso do IPv4 o funcionamento é idêntico.

Caso não seja mais necessária a utilização de um dos protocolos, pode-se simplesmente desativar a pilha do protocolo em cada nó da rede. É preciso cuidar com a alguns detalhes da rede, verificar as configurações de roteamento e regras, serviços como DNS, DHCP e firewall para cada protocolo.

Resumindo nessa técnica o objetivo é fazer o equipamento de a rede comunicar-se em ambos os protocolos, para que aconteça esse processo os cabeçalhos Ips de cada pacote são traduzidos na versão solicitada, neste caso acabam ocorrendo problemas de complexidade da rede, a infraestrutura terá que rodar sempre com ambos os protocolos, observe a Figura 9.

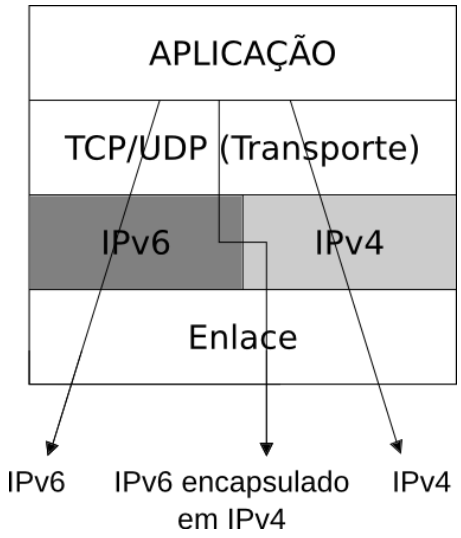

Figura 9 Funcionamento da pilha dupla.

Fonte: Nic.br

Segundo BRITO, sempre que possível deve-se optar pela adoção da pilha dupla nos dispositivos, porque essa é uma estratégia evolucionaria que traz consigo a adoção nativa do IPv6 na infraestrutura e maquinas da rede.

3.2 TRADUÇÃO

Técnica que realiza a tradução dos cabeçalhos do IPv4 e IPv6, significa que independente de qual datagrama a aplicação da rede esteja usando é realizando a troca dos cabeçalhos, convertendo os endereços, as APIs, trocando o trafego TCP

(*Transmission Control Protocol*) ou UDP (*User Datagram Protocol*). Se o nó reconhece apenas IPv4 ou só IPv6 a comunicação ocorre da mesma forma, lembrando que o roteamento ocorre de forma transparente. Recebem apenas endereços ipv6 do provedor, porém leem endereços ipv4.

Network Address Translation 64 (NAT64) permite que dispositivos com IPv6 ativo se comuniquem com dispositivos com IPv4 ativo usando uma técnica de conversão semelhante à NAT para IPv4. Um pacote IPv6 é traduzido em um pacote IPv4, e vice-versa, observe a Figura 10. (CISCO, 2015)

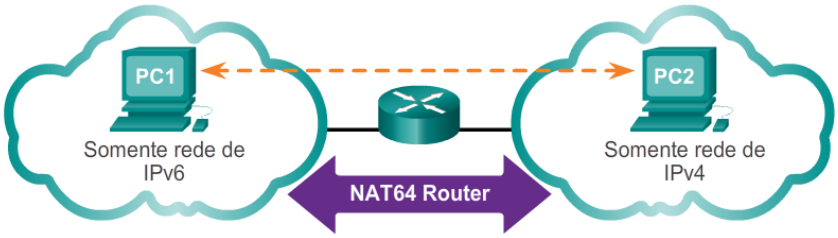

Figura 10 Funcionamento técnica de tradução.
Fonte: CISCO, 2015.

3.3 TUNELAMENTO

Tuneis são usamos em redes que funcionam em IPv4, e aplicamos a equipamentos com o conteúdo do datagrama IPv6 onde são encapsulados em pacotes IPv4, Figura 11.

Encapsulamento é um método de transportar um pacote de IPv6 em uma rede IPv4. O pacote IPv6 é encapsulado dentro de um pacote IPv4 semelhante a outros tipos de dados (CISCO, Netacad 2015).

Desta forma, se uma infraestrutura de rede esteja configurada e em funcionamento com o protocolo IPv4 podemos configurar os nós no IPv6 sem menor problema na comunicação dos pacotes. Resumindo é basicamente a maneira de encapsular um pacote dentro de outro.

Quando optamos em utilizar o tunelamento em nossa rede, devemos estudar e determinar quais das técnicas de tunelamento será a que melhor se enquadra a nossa estrutura de rede, independentes se são manuais ou automáticos.

Nos túneis manuais a configuração é feita nas interfaces de destino e origem dos routers, a conexão é sempre permanente. São utilizados em conexões de

router-to-router e *host-to-router*. Podemos dizer que são robustos e sensíveis a falhas, devido ao fato de serem configurados manualmente, esse tende de ser um dos seus problemas. Imagine que ocorre uma falha em um dos pontos da rede, ela deverá ser refeita por inteiro. É necessário que o endereçamento ipv4 seja configurado manualmente e também tenham suporte para pilha dupla.

Nos túneis automáticos os endereços são configurados seguindo a base do endereçamento ipv4, só funcionam em unicast (não suporta multcast). O túnel automático ocorre no momento que um nó da rede se conecta com outro nó que dispõem do endereçamento ipv4.

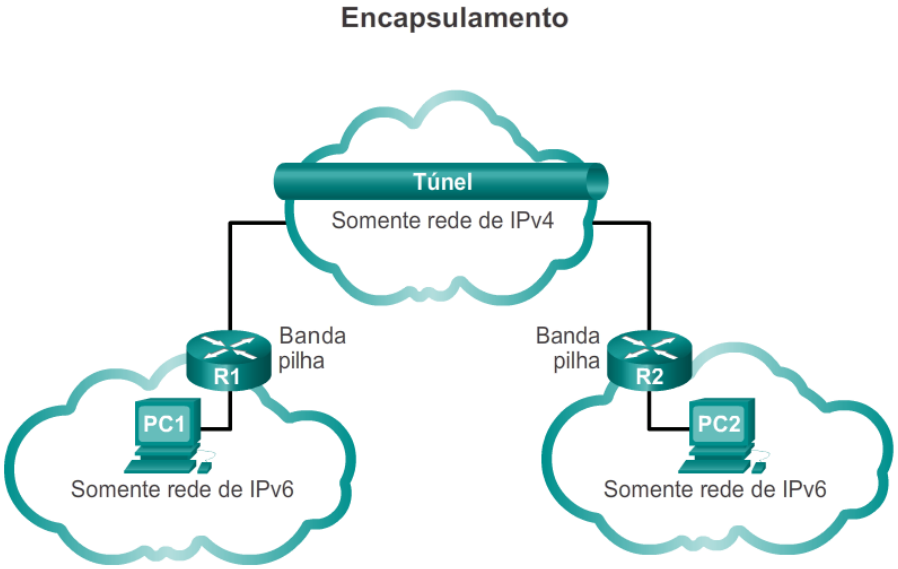

Figura 11 Funcionamento Túnel.
Fonte: CISCO, 2015.

Existem diversas técnicas de tunelamento, dentre elas destacam-se algumas:

- Túnel 6to4
- Túnel Broker
- Túnel ISATAP
- Túnel Teredo
- Túnel GRE

3.3.1 Túnel 6TO4

Definido pela RFC 3056, realiza a comunicação entre várias ilhas ipv6 sobre redes ipv4 o tunelamento acontece de forma automática, ele insere os pacotes IPv6 dentro de pacotes IPv4, neste tipo de túnel os hosts enxergam os hosts da outra ponta (Figura 12). Esse tipo de túnel tem muitas falhas de segurança, devido diversas versões de sistemas operacionais ativarem automaticamente o túnel, muitas vezes sem o usuário saber, isso fez com que redes, principalmente corporativas desativem o recurso.

A conexão é ponto-a-ponto entre redes ipv6 sobre uma rede ipv4 da internet. Não funcionam com NAT, devido ao fato do NAT- traduzir TCP e UDP.

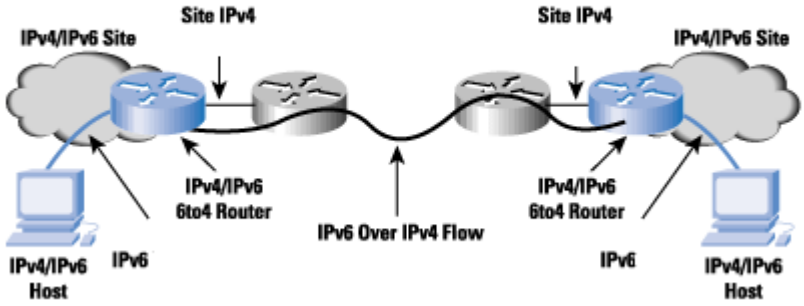

Figura 12 Túnel 6to4.
Fonte: Cisco,2015.

De acordo com a Cisco, O mecanismo de "6to4" transição "Conexão de Domínios IPv6 via Nuvens IPv4", fornece uma solução para o problema da complexidade do uso de túneis configurados manualmente, especificando um prefixo de roteamento única para cada site para usuário final que carrega um IPv4 no túnel.

Esse tipo de túnel foi muito tradicional e ainda é utilizado na internet, no entanto, traz consigo alguns problemas que tem resultado no seu desuso. O maior desses problemas diz respeito à segurança, afinal, os relays são bem conhecidos e, portanto, qualquer atacante pode praticar um ataque de negação de serviço nesses roteadores públicos na internet. (BRITO, 2013).

3.3.2 Túnel Broker

Definida pela RFC 3053, esse tipo de túnel permite que usuários de redes ipv4 consigam realizar a conectividade e acessem redes ipv6, por exemplo, acessando servidores ipv6; esse tipo de técnica usa a Pilha-Dupla (*dual-stack*). Ele vai realizar a identificação e autenticação dos pacotes vindos pelo túnel, assim como a troca dos pacotes IPv6 e IPv4, observe a Figura 13.

Para facilitar o processo de estabelecimento do túnel no lado do usuário que possui endereços dinâmicos, normalmente é disponibilizado um software cliente que faz a conexão e configuração automática sempre que o usuário quiser se conectar. (BRITO, 2013).

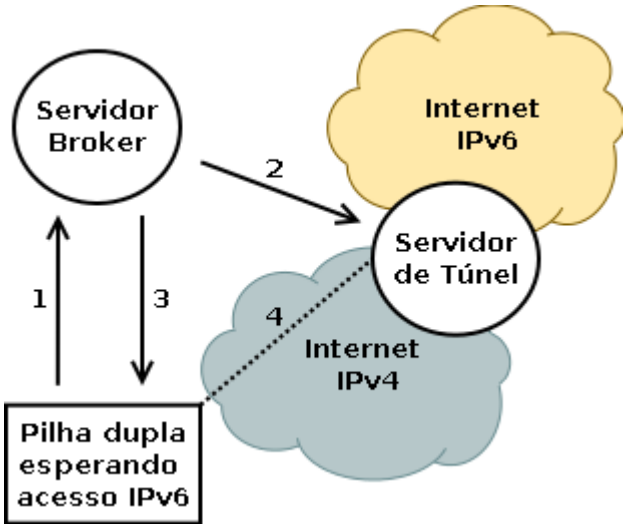

Figura 13 Topologia lógica do Tunnel Broker.
Fonte: NIC.br

Para facilitar o processo de estabelecimento do túnel no lado do usuário que possui endereços dinâmicos, normalmente é disponibilizado um software cliente que faz a conexão e configuração automática sempre que o usuário quiser se conectar. Para empresas ou usuários que tenham um endereço IPv4 fixo, pode-se optar por fazer a configuração manualmente sem utilizar o software cliente, no entanto, o serviço pode exigir que o túnel seja mantido ativo por tempo continuo em contrapartida a conectividade. (BRITO, 2013).

3.3.3 Túnel ISATAP

Intra-Site Automatic Tunnel Addressing Protocol (Protocolo de endereçamento automático de túnel *intra-site*), definida pela RFC 5214, permite que seja realizado o tunelamento automático, desde que exista Pilha dupla dos dois protocolos.

ISATAP é projetado para transportar pacotes IPv6 dentro de um local onde uma infraestrutura IPv6 nativa ainda não está disponíve (CISCO, 2015).

O sistema operacional do host precisa ter configurado as duas pilhas, este mecanismo de tunelamento verifica se já existe um endereçamento ipv4 por exemplo, e cria uma interface com o ipv6. Desta forma o tunelamento acontece automaticamente

É possível realizar 3 configurações:

- Criar túnel ISATAP na mesma sub-rede;
- Criar túnel ISATAP em sub-redes diferentes;
- Cliente ISAPAT conectando puramente com um ipv6.

O túnel ISATAP é muito similar a outros mecanismo de tunelamento utilizando encapsulamento, por exemplo túnel automático e 6to4, porém nessa tecnica os pacotes IPv6 são transportados dentro de um site, não entre sites, como acontece em outras.

3.3.4 Túnel Teredo

Técnica definida pela RFC 4380 e criada pela Microsoft realiza a conexão (unicast) ipv6 em maquinas que usam NAT para ligar os hosts a internet (backbone). Os pacotes ipv6 são encapsulados em UDP ipv4, onde servidor realiza a conexão tanto do host de origem e destino, esse tipo de túnel tem muitos problemas com configurações e overhead.

Teredo é uma tecnologia NAT para o tráfego IPv6 (Figura 14). O tráfego IPv6 encapsulado usando Teredo pode cruzar um ou vários NATs e permitir que um cliente Teredo para acessar os hosts na Internet IPv6 e outros clientes Teredo na Internet IPv4. A capacidade de se conectar a outros clientes Teredo que estão conectados à Internet IPv4 permite a comunicação entre as aplicações que de outra forma teriam problemas de comunicação ao longo de um NAT. Com Teredo, aplicações IPv6-habilitado pode se comunicar com sucesso com mais frequência através da Internet IPv4 (MICROSOFT, 2015).

O túnel Teredo é basicamente composto pelas seguintes partes:

- Clientes;
- Servidores;
- Relays.

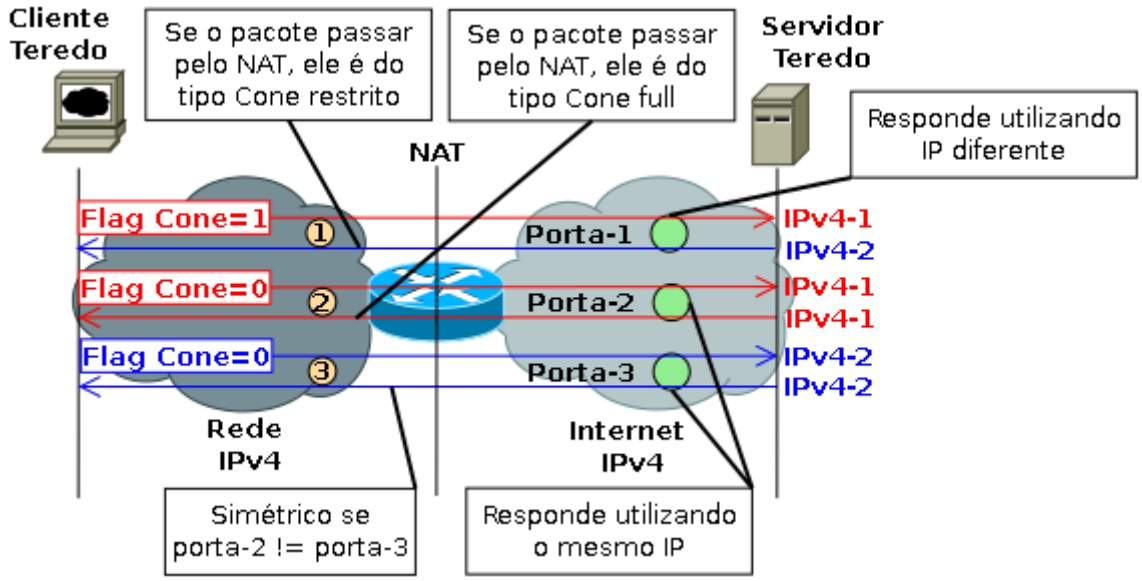

Figura 14 Túnel Teredo.

Fonte: IPv6.br

3.3.5 Túnel GRE

Generic Routing Encapsulation, definido pela RFC 2784, desenvolvido pela Cisco em 1994, e aderido em 2000. Realiza ligações ponto-a-ponto, ligados em dois pontos, isso significa que são configurados em routers entrada e saída.

O GRE é usado para criar um túnel VPN entre dois sites, observe a Figura 15 (CISCO, 2015).

Os pacotes devem estar encapsulados com algum protocolo para então serem encapsulados também com um protocolo chamado GRE, é usado como protocolo de transporte, é o único que realiza esse procedimento entre os túneis existentes.

Figura 15 Túnel GRE.
Fonte: CISCO, 2015.

Nessa técnica basicamente é configurado as extremidades do túnel, muito similar ao que acontece em túneis manuais, configurado no roteador de entrada e no roteador de saída e além do encapsulamento do cabeçalho é inserido um novo cabeçalho GRE (Figura 16) que contém informações do endereço e informações do destino final, quando este pacote chega ao destino o cabeçalho GRE é descartado para que então seja entregue o pacote devidamente ao destino.

GRE é feito apenas o encapsulamento, de forma que não há nenhuma proteção aos dados trafegados. Para isso seria necessário a utilização do IPSEC, ou qualquer outro protocolo para criptografar as informações. (BRAINWORK, 2009).

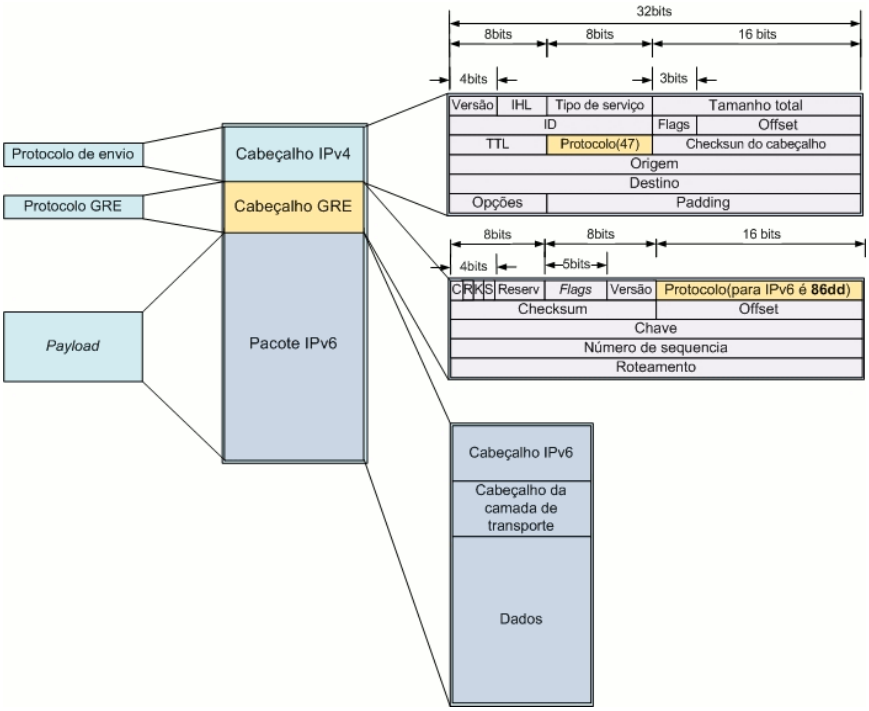

Figura 16 Pacote com cabeçalho GRE.
Fonte : NIC.br

Os principais problemas enfrentados pelo tunelamento GRE são os cabeçalhos administrativos, o escalonamento de grande número de túneis, desempenho e a qualidade do serviço. Como os túneis GRE têm de ser configurados manualmente, há uma grande quantidade de cabeçalhos administrativos fundamentais para a manutenção dos mesmos, além disso, cada mudança do destino final do túnel, nova configuração deve ser realizada. Apesar de parecer pequeno o processo de encapsulamento GRE, há uma relação direta entre o número de túneis e o tempo de processamento de encapsulamento, o que pode tornar o processo lento. (Duarte, 2015).

4 MÉTODO

4.1 SIMULAÇÃO PRÁTICA

O objetivo desta simulação é possibilitar um melhor entendimento do leitor em relação às técnicas de transição. Para a criação da desta prática será utilizado o software educacional Cisco *Packet Tracer*, programa que simula a criação e configuração de redes de computadores, com equipamentos similares aos reais.

Será criada uma rede (Figura 17) com duas simulações, as quais terão a aplicação das técnicas de transição estudas. Nos exemplos abaixo, foi optado pela configuração do Túnel Manual e do Tunelamento GRE com IPSec.

Apenas lembrando que para ambos as redes não foram implementadas e/ou criadas senhas de aceso aos roteadores, recomendação apropriada em ambientes reais.

4.1.1 Topologia

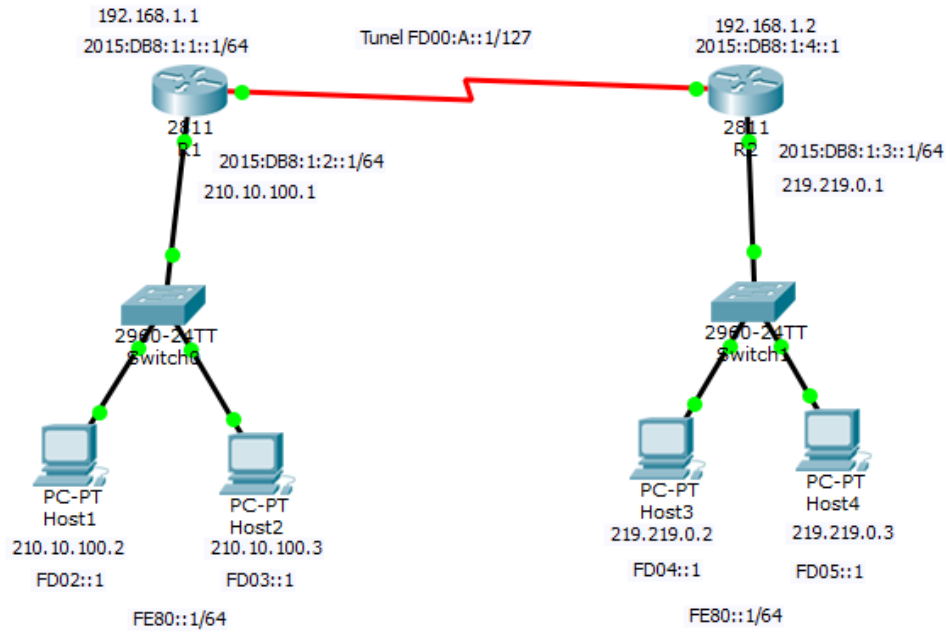

Figura 17 Topologia de Rede

Fonte própria.

4.1.2 Tabela de Endereçamento

Tabela 4 Tabela de Endereçamento

Dispositivo	Interface	Endereço IP	Máscara	Gateway
R1	Fa0/0	210.10.100.1	255.255.255.0	-
	Fa0/0	2015:BF8:1:1::1	64	-
	S0/1/0 DCE	192.168.1.1	255.255.255.0	-
	S0/1/0	2015:BF8:1:2::1	64	-
	Túnel0	192.168.1.2	-	-
R2	Fa0/0	219.219.0.1	255.255.255.0	-
	Fa0/0	2015:BF8:1:3::1	64	-
	S0/1/0	192.168.1.2	255.255.255.0	-
	S0/1/0	2015:BF8:1:4::1	64	-
	Túnel0	192.168.1.1	-	-
Host1	-	210.10.100.2	255.255.255.0	210.10.100.1
	-	FD01::2	64	FE80::1
Host2	-	210.10.100.3	255.255.255.0	210.10.100.1
	-	FD01::3	64	FE80::1
Host3	-	219.219.0.2	255.255.255.0	219.219.0.1
	-	FD01::4	64	FE80::1
Host4	-	219.219.0.3	255.255.255.0	219.219.0.1
	-	FD01::5	64	FE80::1

Fonte própria

4.1.3 RECURSOS NECESSÁRIOS

- 2 roteadores 2811;
- 2 switches 2960;
- 04 PCS (genérico);
- Cabo serial DCE;
- Cabo direto (*copper straight through*).

4.2 CONFIGURAÇÃO TÚNEL MANUAL

Objetivos:

- Definição das configurações básicas dos dispositivos de acordo com a Tabela 4;
- Configuração do túnel manual;
- Ativar o roteamento no túnel.

Recrie a topologia, conecte corretamente os roteadores, switches e pc, com os cabos adequados. Para acrescentar os ips indicados na Tabela 4 nos hosts da rede, clique duas vezes sobre o equipamento, em seguida clique sobre Desktop > IP Configuration.

1. Configuração do roteador R1

Configuração do endereço de rede para as interfaces do roteador na versão IPv4 e juntamente com suas respectivas rotas (Quadro 1).

Roteador R1
Router>enable **Router #configure terminal** **Router(config)#hostname R1** **R1(config)#interface FastEthernet0/0** **R1(config-if)#ip address 210.10.100.1 255.255.0.0** **R1(config-if)#no shutdown** **R1(config-if)#exit** **R1(config)#router rip** **R1(config-router)#version 2** **R1(config-router)#network 210.10.100.0** **R1(config-router)#network 192.168.1.0** **R1(config-router)#network 219.219.0.0** **R1(config-router)#exit** **R1(config)#interface Serial 0/1/0** **R1(config-if)#ip address 192.168.1.1 255.255.255.0** **R1(config-if)#clock rate 2000000** **R1(config-if)#no shutdown** **R1(config-if)#exit** **R1(config)#router rip** **R1(config-router)#version 2** **R1(config-router)#network 210.10.100.0** **R1(config-router)#network 192.168.1.0** **R1(config-router)#network 219.219.0.0** **R1(config-if)#no shutdown** **R1(config-if)#exit**

Quadro 1 Configuração IPv4 - R1

Fonte própria.

Configuração do endereço de rede para as interfaces do roteador na versão IPv6 e juntamente com suas respectivas rotas (Quadro 2).

Roteador R1
R1>enable **R1#configure terminal** **R1(config)#ipv6 unicast-routing** **R1(config)#interface Serial 0/1/0** **R1(config-if)#ipv6 enable** **R1(config-if)#ipv6 address 2015:db8:1:2::1/64** **R2(config-if)#ipv6 address FE80::1 link-local** **R1(config-if)#no shutdown** **R1(config-if)#exit** **R1(config)#interface FastEthernet0/0** **R1(config-if)#ipv6 address 2015:db8:1:1::1/64** **R2(config-if)#ipv6 address FE80::1 link-local** **R1(config-if)#no shutdown** **R1(config-if)#exit** **R1(config)#ipv6 router rip CISCO** **R1(config-rtr)#exit** **R1(config)#interface fastEthernet 0/0** **R1(config-if)#ipv6 rip CISCO enable** **R1(config-if)#exit** **R1(config)#interface Serial 0/1/0** **R1(config-if)#ipv6 rip CISCO enable** **R1(config-if)#exit**

Quadro 2 Configuração IPv6 - R1

Fonte própria.

2. Configuração do roteador R2

Configuração do endereço de rede para as interfaces do roteador na versão IPv4 e juntamente com suas respectivas rotas (Quadro 3).

Roteador R2
Router >enable **Router #configure terminal** **Router(config)#hostname R1** **R2(config)#interface FastEthernet0/0** **R2(config-if)#ip address 219.219.0.1 255.255.0.0** **R2(config-if)#no shutdown** **R2(config-if)#exit** **R2(config)#router rip** **R2(config-router)#version 2** **R2(config-router)#network 210.10.100.0** **R2(config-router)#network 192.168.1.0** **R2(config-router)#network 219.219.0.0** **R2(config-router)#exit** **R2(config)#interface Serial 0/1/0** **R2(config-if)#ip address 192.168.1.2 255.255.255.0** **R2(config-if)#exit**

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 210.10.100.0
R2(config-router)#network 192.168.1.0
R2(config-router)#network 219.219.0.0
R2(config-if)#no shutdown
R2(config-if)#exit
```

Quadro 3 Configuração IPv4 - R2

Fonte própria.

Configuração do endereço de rede para as interfaces do roteador na versão IPv6 e juntamente com suas respectivas rotas (Quadro 4).

Roteador R2
R2>enable **R2#configure terminal** **R1(config)#ipv6 unicast-routing** **R2(config)#interface Serial 0/1/0** **R2(config-if)#ipv6 address 2015:db8:1:4::1/64** **R2(config-if)#ipv6 address FE80::1 link-local** **R2(config-if)#no shutdown** **R2(config-if)#exit** **R2(config)#interface FastEthernet0/0** **R2(config-if)#ipv6 address 2015:db8:1:3::1/64** **R2(config-if)#no shutdown** **R2(config-if)#exit** **R2(config)#ipv6 unicast-routing** **R2(config)#ipv6 router rip CISCO** **R2(config-rtr)#exit** **R2(config)#interface fastEthernet 0/0** **R2(config-if)#ipv6 rip CISCO enable** **R2(config-if)#exit** **R2(config)#interface Serial0/1/0** **R2(config-if)#ipv6 rip CISCO enable** **R2(config-if)#exit**

Quadro 4 Configuração IPv6 – R2

Fonte própria.

Foi utilizado na configuração do roteamento o protocolo RIPng (*Routing Information Protocol - next generation*), protocolo baseado no RIPv2 onde possível algumas características em comum.

Observe a descrição (Tabela 5) sobre os comandos usados nos roteadores da rede.

Tabela 5 Comandos do roteador

Comando	Objetivo
enable	Entra no modo privilegiado EXEC
configure terminal	Entra no modo de configuração global.
hostname	Configura o nome do roteador
interface fastEthernet 0/0	Entra na interface fastEthernet 0/0
interface serial 0/1/0	Entra na interface serial 0/1/0
ip address (ip) (mascara)	Configura o ip e máscara (IPv4)
router rip	Configuração da rota usando *rip2*
version 2	
network (endereço da rede)	
clock rate (valor em bps)	Configura o clock, lembrando que deve apenas ser configurado na interface DCE
ipv6 unicast-routing	Habilita o IPv6
ipv6 address (ip) (mascara)	Configura o ip e máscara (IPv6)
ipv6 router rip (nome)	Configura o roteamento do rip no IPv6
ipv6 router rip (nome) enable	Habilita o roteamento rip na versão IPv6

Fonte própria

3. Configuração do túnel

Configuração para funcionamento do túnel manual nos roteadores R1(Quadro 5) e R2 (Quadro 6).

Roteador R1
R1>enable **R1#configure terminal** **R1(config)#interface Serial0/1/0** **R1(config-if)#int tunnel 0** **R1(config-if)#ipv6 address fd00:a::0/127** **R1(config-if)#tunnel source serial 0/1/0** **R1(config-if)#tunnel destination 192.168.1.2** **R1(config-if)#tunnel mode ipv6ip** **R1(config-if)#exit** **R1(config)#ipv6 unicast-routing** **R1(config)#ipv6 route fd01::/64 fe08::1** **R1(config)#exit**

Quadro 5 Túnel manual - R1

Fonte própria.

Roteador R2
R2>enable **R2#configure terminal** **R2(config)#interface Serial0/1/0** **R2(config-if)# interface tunnel 0** **R2(config-if)#ipv6 address fd00:a::1/127** **R2(config-if)#tunnel source serial 0/1/0** **R2(config-if)#tunnel destination 192.168.1.1** **R2(config-if)#tunnel mode ipv6ip** **R2(config-if)#exit** **R2(config)#ipv6 unicast-routing** **R2(config)#ipv6 route fd01::/64 fe08::1** **R2(config)#exit**

Quadro 6 Túnel manual – R2

Fonte própria.

Acompanhe na Tabela 5, a descrição dos comandos utilizados nos roteadores para elaboração e configuração do *tunnel* (Tabela 6).

Tabela 6 Comandos - configuração Túnel manual

Comando	Objetivo
interface tunnel (número)	Criação da interface do túnel
ipv6 address (ip)	Atribuição do endereço ip para o túnel
tunnel source serial 0/1/0	Definição do endereço de origem do túnel
tunnel destination 192.168.1.1	Definição do endereço de destino do túnel
tunnel mode ipv6ip	Define o encapsulamento e transporte do túnel IPv6 *over* IPv4.
ipv6 route (endereço ip)	Configuração rota estática.

Fonte própria

Lista de comandos úteis

- show ip route
- show run
- show ipv6 interface tunnel 0
- show ip interface brief

Teste os comandos e verifique se o túnel está ativado em ambos os roteadores. Veja os exemplos nas Figura 18 e Figura 19, a utilização do comando *show interface tunnel 0.*

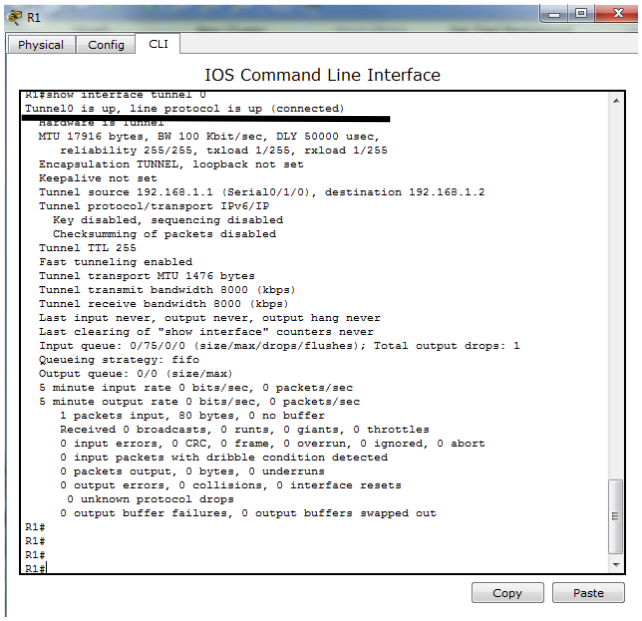

Figura 18 Tela Packer Trace- Roteador R1

Fonte própria

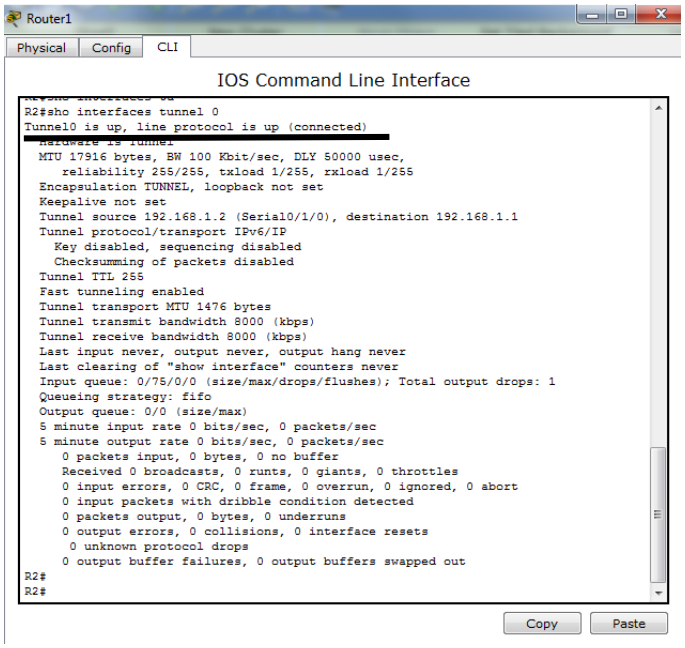

Figura 19 Tela Packer Trace- Roteador R2

Fonte própria

4.2 CONFIGURAÇÃO GRE COM IPSEC

Objetivos:

- Ativação do túnel GRE;
- Ativação do IPSec.

Lembrado que a topologia será a mesma da Figura 17 Topologia de Rede, juntamente com as configurações realizadas.

1. Configuração do túnel GRE com IPSec

Configuração para funcionamento do túnel protegido nos roteadores R1(Quadro 7) e R2(Quadro 8).

Roteador R1
R1>enable **R1#configure terminal** **R1(config)#ipv6 unicast-routing** **R1(config)#interface tunnel 1** **R1(config-if)#ipv6 address fd00::1/64** **R1(config-if)#tunnel mode gre ip** **R1(config-if)#tunnel source serial 0/1/0** **R1(config-if)#tunnel destination 192.168.1.2** **R1(config-if)#exit** **R1(config)crypto isakmp policy 10** **R1(config-isakmp-policy)#authentication pre-share** **R1(config-isakmp-policy)#hash md5** **R1(config-isakmp-policy)#group 2** **R1(config-isakmp-policy)#encryption 3 des** **R1(config-isakmp-policy)#exit** **R1(config)# crypto isakmp key cisco10 address 192.168.1.2** **R1(config)# crypto ipsec transform-set myset esp-des esp-md5-hmac** **R1(config)# access-list 100 permit ip 210.10.100.0 0.0.0.255 219.219.0.0 0.0.0.255** **R1(config)#crypto map mymap 10 ipsec-isakmp** **R1(config-crypto-map)# set peer 192.168.1.1** **R1(config-crypto-map)#set transform-set myset** **R1(config-crypto-map)#match address 100** **R1(config-crypto-map)#exit** **R1(config)#interface fastEthernet 0/0** **R1(config-if)#crypto map mymap** **R1(config-if)#exit** **R1(config)#interface serial 0/1/0** **R1(config-if)#crypto map mymap** **R1(config-if)#exit**

Quadro 7 túnel GRE com IPSec- R1

Fonte própria.

Roteador R2
R1>enable **R1#configure terminal** **R1(config)#ipv6 unicast-routing** **R1(config)#interface tunnel 1** **R1(config-if)#ipv6 address fd00::1/64** **R1(config-if)#tunnel mode gre ip** **R1(config-if)#tunnel source serial 0/1/0** **R1(config-if)#tunnel destination 192.168.1.1** **R1(config-if)#exit** **R1(config)crypto isakmp policy 10** **R1(config-isakmp-policy)#authentication pre-share** **R1(config-isakmp-policy)#hash md5** **R1(config-isakmp-policy)#group 2** **R1(config-isakmp-policy)#encryption 3 des** **R1(config-isakmp-policy)#exit** **R1(config)# crypto isakmp key cisco10 address 192.168.1.2** **R1(config)# crypto ipsec transform-set myset esp-des esp-md5-hmac** **R1(config)# access-list 100 permit ip 219.219.0.0 0.0.0.255 210.10.100.0 0.0.0.255** **R1(config)#crypto map mymap 10 ipsec-isakmp** **R1(config-crypto-map)# set peer 192.168.1.2** **R1(config-crypto-map)#set transform-set myset** **R1(config-crypto-map)#match address 100** **R1(config-crypto-map)#exit** **R1(config)#interface fastEthernet 0/0** **R1(config-if)#crypto map mymap** **R1(config-if)#exit** **R1(config)#interface serial 0/1/0** **R1(config-if)#crypto map mymap** **R1(config-if)#exit**

Quadro 8 túnel GRE com IPSec- R2

Fonte própria.

Acompanhe nas Tabela 7,

Tabela 8 e Tabela 9 o detalhamento dos comandos utilizados para configuração do túnel GRE com IPSec.

1.1 Configuração das políticas ISAKMP

Tabela 7 Configuração das políticas ISAKMP

Comando	Objetivo
interface tunnel (número)	Criação da interface do túnel
ipv6 unicast-routing	Habilita o IPv6
ipv6 address (ip)	Atribuição do endereço ip para o túnel
tunnel mode gre ip	Atribui o modo do túnel sendo GRE sobre ip

tunnel source (interface)	Especifica o endereço de origem para o túnel.
tunnel destination (ip)	Especifica o endereço de destino do túnel.
crypto isakmp policy (numero)	Entra em modo de configuração ISAKMP
authentication pre-share	Alteração do método de chaves pré-partilhadas para o processo de autenticação
hash tipo (md5)	Definição do algoritmo de hash a ser usado
encryption tipo (3 des)	Definição do algoritmo usado para encriptação, o 3des (Triple Data Encrytpion Standard) usa 3 chaves.
group tipo (2)	Definição do grupo para as chaves *Diffie-Hellman* que realizaram a troca das chaves entre os pares
crypto isakmp key (password) address (ip)	Criação da chave que será utilizada entre os roteadores

Fonte própria

1.2 Configuração do IPSec e Access-list

Tabela 8 Configuração do IPSec e Access-list

Comando	**Objetivo**
crypto ipsec transform-set myset esp-des esp-md5-hmac	Definição do algoritmo de encriptação (esp-des) e o algoritmo *hash*(esp-md5-hmac).
access-list 100	Criação da lista de acesso, que será protegida pelo túnel IPSec

Fonte própria

1.3 Configuração do crypto map

Tabela 9 Configuração do crypto map

Comando	**Objetivo**
crypto map (nome) (número de sequências) ipsec-isakmp	Definição do nome para o crypto map e o número de sequências.

set peer (ip)	Definição da VPN.
set transform-set myset	Definir o nome do transform-set que vai ficar agregado na VPN no crypto-map
match address (acl)	Definição a access-list que define o tráfego da VPN
crypto map mymap	Relacionar o crypto map definido anteriormente com a interface.

Fonte própria

Lista de comandos úteis

- show ip route;
- show run;
- show ipv6 interface tunnel 1;
- show ip interface brief;
- debug crypto ipsec;
- debug crypto isakmp.

Teste os comandos e verifique se o túnel está ativado juntamente com as proteções configurações em ambos os roteadores. Veja o exemplos na Figura 20 comando *show interfaces tunnel 1*, além da verificação citada é possível verificar se o túnel configurado é o GRE.

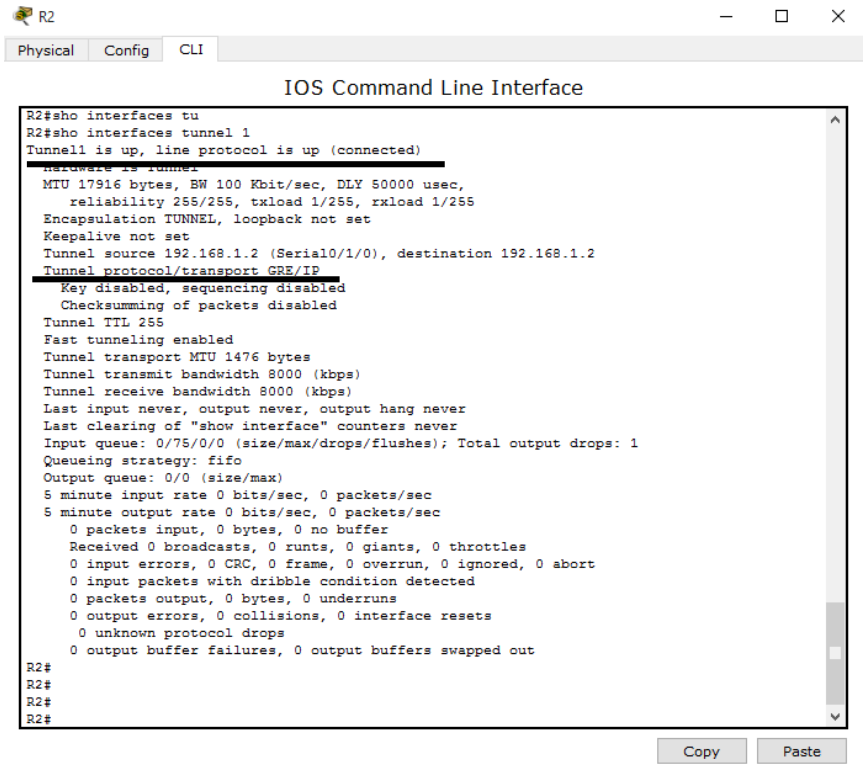

Figura 20 Tela Packer Trace- Comando show interfaces tunnel1

Fonte própria

5 CONCLUSÃO

Com a realização desta pesquisa foi possível confirmar que através do protocolo IPv6 a internet e as redes de computadores poderão se expandir de forma imaginável, facilitando a criação e o desenvolvimento de novas tecnologias.

A utilização das técnicas de transição possibilitam que possamos adaptar as redes já existentes que utilizam o protocolo IPv4 ou até mesmo conectar novas redes IPv6, permitindo a troca de pacotes entre redes distintas.

Para testar o desempenho desse recurso realizei a configuração de duas técnicas de tunelamento, túnel manual e túnel GRE com IPSec, o qual demonstraram sucesso na conexão entre as redes IPv4 e IPV6, agindo de forma totalmente transparente, sem que seja necessária quaisquer configuração extras. Exceto as necessárias para realização do procedimento.

A configuração dos túneis não exigem tanta dedicação dos administradores de rede, sendo assim, é possível adaptar ou criar redes sem muitos problemas.

Em uma das simulações foi realizada além da configuração e ativação do túnel, também do IPSec, que garante mais segurança, autenticidade e confidencialidade das informações trafegadas pela rede.

Sendo assim, túneis configurados com o IPSec além de realizarem a comunicação entre equipamentos que usam protocolos diferentes protegem os dados transmitidos.

6 REFERÊNCIAS BIBLIOGRÁFICAS

IPv6.br. **Transição**. Disponível em: < http://ipv6.br/entenda/transicao/> Acesso 25 de Maio de 2015.

TANENBAUM, Andrew. S. **Redes de Computadores**. 4. ed. Rio de Janeiro: Campus, 2003.

BRITO, Samuel H. B. **IPv6 O Novo Protocolo Da Internet.** 1. ed. São Paulo: Novatec, 2013

TELECO INTELIGÊNCIA EM TELECOMUNICAÇÕES. **Internet Protocol version 6 (IPv6)**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialipv6/Default.asp>. Acesso em: 29 de Maio de 2015.

LABCISCO. **Túnel Manual 6in4 (IPv6 em IPv4)**. Disponível em:<http://labcisco.blogspot.com.br/>. Acesso em 03 de Junho de 2015.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Tutorial sobre IPv6**. Disponível em: < http://gtrh.tche.br/ovni/ipv6/>. Acesso em: 03 de Junho de 2015.

MOREIRAS, Antonio. M. **O esgotamento do ipv4**. Disponível em:<http://www.hardware.com.br/artigos/esgotamento-ipv4/>. Acesso em: 06 de Junho de 2015.

MOREIRAS, Antonio. M. **IPv4**. Disponível em:<http://www.hardware.com.br/termos/ipv4./>. Acesso em: 10 de Julho de 2015.

IPv6. **Introdução ao IPv6**. Disponível em:< http://ipv6.br/entenda/introducao/>. Acesso em: 10 de Julho de 2015.

MORIMOTO, Carlos E. **Redes, guia prático**. 2ª. ed., 2011

STOROZ, S.; JAMHOUR, E. **Mecanismos de transição para implementar a comunicação ipv4/ipv6 em redes móveis**. Rio de Janeiro, 2003. Disponível

em:<http://www.ppgia.pucpr.br/jamhour/Download/pub/Artigos/MobileNetworks/tip6.pf. Acesso em: 12 Julho 2015.

FOROUZAN, A. Behrouz (2006) “Comunicação de Dados e Redes de Computadores. Porto Alegre, 4ª edição.

CISCO. **Tradução IPv6 para IPv4**. Disponível em:< http://ciscoredes.com.br/2011/08/10/traducao-ipv6-para-ipv4/> Acesso 14 de Julho de 2015.

CISCO. **Tecnologias**. Disponível em:< http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html/> Acesso 14 de Julho de 2015.

CISCO. **Voz por Ip**. Disponível em:< http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/10_0_1/ccmfeat/CUCM_BK_F3AC1C0F_00_cucm-features-services-guide-100/CUCM_BK_F3AC1C0F_00_cucm-features-services-guide-100_chapter_0100100.pdf. Acesso 14 de Julho de 2015.

NETWORK. **Protocolo IPv6**. Disponível em:< http://www.networksorcery.com/enp/protocol/ipv6.htm/> Acesso em 29 de julho de 2015.

LACNIC. **Portal do IP**. Disponível em:< http://portalipv6.lacnic.net/pt-br/mecanismos-de-transicao//> Acesso em 03 de agosto de 2015

BRAINWORK. **Túnel GRE**. Disponível em http://brainwork.com.br/2009/02/09/tnel-gre/> Acesso em 04 de agosto de 2015

MIRRORS. **IPv6**. Disponível em:<http://mirrors.deepspace6.net/Linux+IPv6-HOWTO-pt_BR/> Acesso 10 de Agosto de 2015.

LACNIC. **Mecanismos de Transição**. Disponível em:<http://portalipv6.lacnic.net/pt-br/mecanismos-de-transicao/> Acesso 20 de Agosto de 2015.

Duarte, Otto C. M. B. **VNP (Virtual Private Network)**. Disponível em: <http://www.gta.ufrj.br/grad/08_1/vpn/tiposrede.html/> Acesso 21 de Agosto de 2015.

CCNA 5.0. **Introdução a Redes**. Disponível em:<http://www.ct.utfpr.edu.br/deptos/cisco/material/CCNA5.0/1%20-%20Introdu%C3%A7%C3%A3o%20a%20Redes/course/module2/index.html#2.3.2/> Acesso 21 de Agosto de 2015.

CISCO. **Artigo IPv6**. Disponível em:<http://www.ciscopress.com/articles/article.asp?p=2104948/> Acesso 22 de Agosto de 2015.

CISCO. **Manual de Configuração de Túnel**. Disponível em:<http://docwiki.cisco.com/wiki/Ipv6_manual_tunnel_Configuration_Example/> Acesso 22 de Agosto de 2015.

MICROSOFT. **Túnel Teredo**. Disponível em:< https://technet.microsoft.com/en-us/library/bb457011.aspx/> Acesso 24 de Agosto de 2015.

MICROSOFT. **Túnel Teredo**. Disponível em:< http://www.brandontek.com/microsoft/ipv6-tunneling-with-teredo/> Acesso 25 de Agosto de 2015.

MICROSOFT. **IPSec Modo de Transporte**. Disponível em:<https://technet.microsoft.com/pt-br/library/cc739674(v=ws.10).aspx /> Acesso 10 de Outubro de 2015.