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

DANIEL KAISS

ANÁLISE DA PERFORMANCE NAS REDES IPV6

MONOGRAFIA

CURITIBA
2015

DANIEL KAISS

ANÁLISE DA PERFORMANCE NAS REDES IPV6

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de servidores e equipamentos de rede, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTFPR
Orientador: Prof. Lincoln Herbert Teixeira.

CURITIBA
2015

RESUMO

KAISS, Daniel. **Análise da performance nas redes IPv6.** 2015. 32 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

Esta monografia foi feita através de uma pesquisa bibliográfica em artigos, livros e monografias já publicadas e aborda o estudo do IPv6 com ênfase no protocolo de segurança IPSec. Possui um referencial teórico sobre internet, redes, tipos de conexão, topologias, modelo OSI e TCP, protocolos IPV4 e IPv6, IPSec, RFC, *criptografia*, assinatura digital, certificado digital. Como prática, foi criada uma rede IPv4 com a implantação do protocolo de segurança IPSec, mostrando o passo a passo da configuração. Também foi criado uma rede simples usando o IPv6, tudo no programa Packet Tracer da Cisco.

Palavras-chave: Redes. IPv4. IPv6. IPSec. Protocolos.

ABSTRACT

Kaiss, Daniel. **Analysis of performance in IPv6 networks**. 2015 32 f. Monograph (Specialization in Server Configuration and Management and Network Equipment). Federal Technological University of Paraná. Curitiba, 2015.

This monograph was Made through Bibliographical Research Articles A ON, Books and Monographs already published and ABORDA IPv6 study with emphasis on the IPSec security protocol. HAVE A theoretical framework over Internet , networks , connection types, topologies , OSI and TCP protocols IPv4 and IPv6 , IPsec , RFC , encryption , digital signature digital certificate . As practice, it was Built An IPv4 network with IPSec security protocol Deployment, showing the Walkthrough the configuration . It was also CREATED A simple network using IPv6, not all Cisco Packet Tracer program.

Keywords: Networks. IPv4. IPv6. IPSec. Protocols.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Com o esgotamento dos endereços IPV4, veio a necessidade de criar o IPv6. Embora este tenha uma quantidade quase ilimitada de endereços IPs que devem durar várias gerações, vem a pergunta, teria este uma boa performance, ou a performance deste é superior ao IPv4.

Este trabalho visa apresentar a diferença entre os dois protocolos dando ênfase na segurança usando o protocolo IPSec.

Segundo vídeo no site http://ipv6.br acessado em agosto de 2015, o IPv6 reduz o processamento dos roteadores, pois possui um cabeçalho simplificado e isto aumenta a performance em relação ao protocolo anterior.

Com o aprimoramento do suporte a conexões móveis, onde a fragmentação de dados é realizada apenas na origem, o usuário pode se deslocar de uma rede a outra sem a necessidade de alterar o endereço. Isto aumentou a performance pois reduziu o overhead do cálculo dos cabeçalhos.

A representação dos prefixos de rede permite o agrupamento dos endereços de forma hierárquica, identificando a topologia de rede através de parâmetros como posição geográfica, provedor de acesso, identificação da rede, divisão da subrede. Com isso é possível reduzir o tamanho da tabela de roteamento e agilizar o encaminhamento dos pacotes.

1.1 OBJETIVOS

Buscar referencial teórico para comparar a performance do protocolo IPv6 com o seu antecessor. Estes serão localizados em sites, artigos, livros e monografias já publicadas.

Será mostrado algumas vantagens do protocolo IPv6 sobre o IPv4, porém na maior parte do trabalho será dado mais ênfase no protocolo de segurança IPSec, falando sobre as RFCs, *criptografia*, autenticação e outros.

1.2 JUSTIFICATIVA

Este trabalho se justifica pelo fato de o IPv6 ser um assunto relativamente novo, comparado com o IPv4 e também vai esclarecer algumas dúvidas em relação ao protocolo de segurança nativo no IPv6.

A cada dia que passa a Internet está sendo usada cada vez mais para uso corporativo, vendas online. Porém sabemos que também está menos segura.

Quando a Internet foi criada, ninguém imaginou que atingiria esta proporção.

Desde o seu surgimento foram criados inúmeros tipos de ataques com objetivos diversos, como roubo de senhas, dados bancários, segredos industriais e outros.

Vejo segurança como um dos pontos principais da Internet. Não foi dado muita ênfase no início, porém agora temos um protocolo com segurança nativa. E é por este motivo que será dado muita ênfase ao IPSec neste trabalho.

Este trabalho visa responder estas perguntas e mostrar estes resultados e outros que testam a performance da rede IPv6 com o objetivo principal de deixar claro quais são os pontos forte e fracos deste novo protocolo.

1.3 METODOLOGIA

Este trabalho de monografia seguirá em sua maior parte os procedimentos técnicos de pesquisa bibliográfica. Então será desenvolvida com base em material existente nos meios de pesquisa, formado por livros, artigos científicos, sites especializados, monografias, TCC, vídeos.

A opção pela pesquisa bibliográfica à pesquisa de campo justifica-se devido as intensas atividades laborais do autor firmadas em contrato trabalhista.

Como prática será realizado um tutorial mostrando como configurar uma rede IPv6 e também será aplicado o protocolo de segurança IPSec em uma rede IPv4.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Internet

A *Internet* surgiu em 1969 e desde então revolucionou nossa maneira de comunicar. A princípio a mesma foi criada para que os pesquisadores pudessem compartilhar suas descobertas, reduzindo custos e eliminando a duplicação de trabalhos. Tudo começou com quatro nós entre quatro universidades.

Os conceitos conhecidos como encapsulamento, *datagrama*, *gatway* só apareceram em 1973 em um ártico sobre TCP criado por Vint Cerf e Bob Kahn.

Atualmente a *internet* é composta por várias redes locais e remotas. A *Internet* está em constante mutação, todos os dias novas redes são acrescentadas ou eliminadas.

2.2 Comunicação de dados

A comunicação de dados é a troca de dados entre dois dispositivos por intermédio de algum tipo de transmissão, como um cabo condutor formado por fios, ondas de rádio, ondas de luz.

Atualmente as tomadas de decisão no mundo de negócios devem ser de forma rápida, precisa e segura. Isto é feito pela comunicação de dados. Esta comunicação é feita pelo compartilhamento de informações entre indivíduos.

2.3 Redes

Uma rede é um grupo de dispositivos (computador, impressora) conectados por *links* de comunicação. *Links* são caminhos de comunicação que transferem dados de um dispositivo para outro.

Uma rede de qualidade deve possuir segurança, desempenho e confiabilidade.

2.3.1 Segurança

Implementação de políticas e criação de procedimentos para a recuperação de perda de dados. Proteção do acesso não autorizado e proteção de dados contra danos.

2.3.2 Desempenho

O desempenho pode ser medido pela quantidade de tempo que uma informação leva para chegar de um dispositivo a outro. O desempenho depende dos tipos de meios de transmissão, *hardware*, *software* e do número de usuários.

O desempenho geralmente é avaliado pelo *throughput*, que é a capacidade de vazão e pelo *delay*.

“Se tentarmos enviar mais dados para a rede, podemos aumentar o *throughput*, mas aumentamos o *delay* em razão do congestionamento de tráfego na rede. ” (BEHROUZ, 2008, p.8)

2.3.3 Confiabilidade

Uma rede é confiável quando continua funcionando mesmo após falhas. Uma rede confiável tem precisão na entrega.

2.4 Tipos de Conexão

- Ponto a Ponto: aqui temos um *link* dedicado entre dois dispositivos onde toda a capacidade do *link* é reservada para este fim.
- Multiponto: aqui temos mais de um dispositivo compartilhando um único link.

2.4.1 Topologias

A topologia pode ser organizada fisicamente e logicamente. Quanto a física temos basicamente a anel, barramento, malha e estrela. Na topologia física temos o *layout* físico e o meio de conexão dos dispositivos de redes.

Na lógica que é a maneira como os sinais agem sobre os meios de rede. Não existe uma ligação entre a topologia física e lógica; podemos ter um *token* físico e uma estrela lógico.

2.4.2 Topologia anel

Aqui temos uma conexão ponto a ponto e o sinal percorre o anel em um sentido, passando de dispositivo para dispositivo até atingir seu destino.

2.4.3 Topologia barramento

No barramento temos uma conexão multiponto. Temos um grande cabo que interliga todos os dispositivos da rede.

2.4.4 Topologia malha

Aqui cada dispositivo possuem um *link* ponto a ponto dedicado com os outros dispositivos, isto é, o tráfego ocorre apenas entre os dois dispositivos conectados.

2.4.5 Topologia estrela

Nesta topologia que é a mais usada atualmente, cada dispositivo tem um *link* ponto a ponto dedicado que se liga com um controlador central. Então aqui os dispositivos não são conectados entre si, o que não permite tráfego direto entre os mesmos.

2.5 Modelos de rede

Várias empresas criam equipamentos de redes hoje em dia. Porém não existiria comunicação se estas redes não falassem a mesma língua.

Então para que exista uma comunicação entre as redes é necessário que todas falem a mesma língua. OS dois padrões mais conhecidos são o modelo OSI e o modelo TCP/IP.

2.5.1 Modelo OSI

OSI significa *Open Systems Interconnection*, Interconexão de Sistemas Abertos. Este modelo é um sistema aberto e segue o padrão da organização ISO (Organização internacional de padronização) que cuida dos padrões internacionais. Por ser um sistema aberto permite que sistemas diferentes se comuniquem.

Este modelo é um modelo de referência e serve para que possamos compreender e projetar a rede ideal, que é capaz de se comunicar com outros sistemas, adaptável e robusta.

Este projeto de redes é formado por sete camadas e é uma estrutura que autoriza a comunicação entre todos os tipos de sistemas.

Dentro destas camadas ocorrem a operação de protocolos interagindo com as camadas que estão embaixo ou em cima.

2.5.2 Modelo TCP/IP

Também conhecido como modelo DoD (Departamento de Defesa Americano), este é um modelo de protocolo e mostra toda a funcionalidade necessária para ligar a rede de dados a rede humana.

Aqui o modelo não foi planejado como no modelo OSI e a coleção de protocolos TCP/IP foi criada antes do modelo ser concebido.

A maior diferença entre os 2 modelos é que no TCP/IP houve uma união das 3 camadas superiores e as 2 inferiores. O modelo OSI tem 7 camadas e o TCP/IP tem 4.

Segue abaixo a Tabela 1 demonstrando as camadas. Foi usado como referência o próprio site do curso preparatório para o CCNA da cisco (2015), porém existem autores que sugerem que o modelo TCP/IP tem 5 camadas.

Modelo OSI	Modelo TCP/IP	Protocolos TCP/IP
Aplicação	Aplicação	HTTP, DNS, DHCP, FTP
Apresentação		
Sessão		
Transporte	Transporte	TCP, UDP
Rede	Internet	IPv4, IPv6, ICMPv4, ICMPv6
Enlace de Dados	Acesso a Rede	PPP, *Frame Relay*, *Ethernet*
Físico		

Tabela 1 - Modelos e suas camadas. Fonte: Autoria Própria

2.6 Arquitetura de rede

Arquitetura de rede é um conjunto de camadas e protocolos. Esta arquitetura de deve conter informação que permitam escrever um programa ou construir um *hardware* para cada camada. Este programa deve seguir as regras do protocolo.

A arquitetura mais usada atualmente é o TCP/IP, provavelmente por ser a mais usada obrigou os fabricantes a segui-la.

2.7 Protocolos

Protocolos são um conjunto de regras que controlam como os dados são transmitidos. Por exemplo, um brasileiro que só fala português não conseguiria falar com um americano que só se comunica em inglês.

Os protocolos são importantes para gerenciar os recursos de uma rede e com isso controlar seu comportamento.

Existem vários protocolos e os mesmo foram separados em camadas diferentes.

As redes são organizadas como uma séria de camada para reduzir sua complexidade de *design*. O objetivo de cada camada é oferecer certos serviços para as camadas mais altas.

2.8 Protocolo IP

Localizado da camada de rede no modelo OSI e na camada de *Internet* no modelo TCP/IP, esta camada que faz a comunicação lógica entre computadores.

Todos os dispositivos de rede precisam de um endereço IP, que é seu identificador lógico. Através dele, sabemos para onde um pacote de dados deve ir ou de onde ele veio.

Atualmente a versão mais usada do protocolo é a versão 4 que possui 32 bits no campo de endereço. A nova versão possui 128 bits e é a versão 6.

2.9 Protocolo IPv4

Este protocolo foi criado para se comunicar independente do meio físico utilizado e é o método de entrega usado pelo TCP/IP.

Em uma rede IPv4 cada pacote possui um endereço de destino e de origem de 32 bits. Este tamanho possibilita um máximo de 4.294.967.296 de IPs ou 2 elevado a 32, como 192.168.65.10.

O IPv4 é dividido em 4 grupos, cada um com 8 bits, separados por um ponto. Estes grupos são chamados de *octetos* e os números vão de 0 a 255.

No IPv4 temos 3 classes principais que são classe A, B e C. Temos também as classes D e E que são reservadas para teste ou uso futuro. Na classe A temos uma faixa de IP que vai de 1.0.0.0 até 127.0.0.0. Na classe B temos uma faixa de IP que vai de 128.0.0.0 até 191.255.0.0. Na classe C temos uma faixa de IP que vai de 192.0.0.0 até 223.255.255.0.

Estas classes estão divididas pelo número de *bytes* que representam na rede. Em um endereço de classe A o primeiro *byte* identifica a rede e os 3 *bytes* a direita representam os *hosts* que são os computadores das redes. Em um endereço de classe B os 2 primeiros *bytes* identificam a rede e os 2 *bytes* a direita representam os *hosts*. Em um endereço de classe C os 3 primeiros *bytes* identificam a rede e o último *byte* a direita representam os *hosts*.

Também existem classes D e E, porém, essas são reservadas para *multicast* e para uso de teste do IETF. Vale lembrar que em todas as classes há endereços reservados para fins específicos.

Os 3 tipos principais de endereço IPv4 são *multicast*, *unicast* e *broadcast*. O *multicast* transmite seus pacotes para grupos específicos. O *unicast* transmite seus pacotes para um único destino e o *broadcast* transmite seus pacotes para toda a rede dentro de uma determinada faixa de IPs.

A Tabela 2 mostra o cabeçalho IPv4.

<table>
<tr><td>Versão</td><td>Tamanho do Cabeçalho</td><td>Tipo de Serviço</td><td colspan="2">Tamanho Total</td></tr>
<tr><td colspan="3">Identificação</td><td>Flags</td><td>Deslocamento do Fragmento</td></tr>
<tr><td colspan="2">Tempo de Vida</td><td>Protocolo</td><td colspan="2">Soma de verificação do cabeçalho</td></tr>
<tr><td colspan="5">Endereço de Origem</td></tr>
<tr><td colspan="5">Endereço de Destino</td></tr>
<tr><td colspan="5">Opções + Complemento</td></tr>
</table>

Tabela 2 - Cabeçalho IPv4. Fonte: Autoria Própria

2.10 Deficiências do protocolo IPv4

Com a *internet* crescendo cada vez mais, algumas deficiências tornam ela inadequada. Para suprir a deficiência de falta de IP foram criadas soluções como o NAT e divisão de sub-redes. Porém o esgotamento de IPs é inevitável, e recursos como o NAT acabam com modelo de funcionamento fim-a-fim. Isto

causa deficiência como impedir o funcionamento de aplicações de voz sobre o IP baseadas em SIP, não funciona com o IPSec para segurança.

2.11 Protocolo IPv6

Esta versão do IP mantém a compatibilidade com a antiga versão (IPv4), uma vez que a transição está sendo feita gradativamente (BASSO, 2011).

Para superar as deficiências do protocolo IPv4 foi criado o protocolo IPv6 que significa *Internetworking Protocol*, versão 6. Este protocolo também é conhecido como IPng que significa *Internetworking Protocol*, próxima geração.

Provavelmente este protocolo vai acomodar o crescimento da *internet* por vários anos pois suporta números de 128 bits, o que dá um total de 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços.

Este novo protocolo vai atender essa nova requisição de uso da *Internet* e a necessidade de se manter conectado através de uma conexão fim-a-fim surge o IPv6 que possui mais segurança que o IPv4.

Tanto o formato, quanto o comprimento do endereço IP foram modificados juntamente com o formato dos pacotes (*datagramas*). Outros protocolos da camada de rede, como ARP, RARP E IGMP, foram excluídos ou incluídos no protocolo ICMPv6. Os protocolos de roteamento dinâmico foram modificados, dentre outras melhorias (FOROUZAN, 2010).

Entre as vantagens do IPv6 em relação a versão anterior temos além de um maior espaço de endereços, ele possui um formato mais adequado do cabeçalho onde as opões são separadas do cabeçalho base e são inseridas somente quando necessário. Este processo descomplica e agiliza o processo de roteamento.

O Ipv6 foi desenvolvido para permitir a extensão do protocolo e também para suportar a alocação de recursos, o que permite suportar tráfego de áudio e vídeo em tempo real.

Quanto à segurança, já vem nativo no IPv6 o IPSec que possui opções de *criptografia* e autenticação.

A Tabela 3 mostra o cabeçalho simplificado do IPv6.

Versão	Classe de Tráfego	Identificador de Fluxo	
Tamanho dos dados		Próximo cabeçalho	Limite de Encaminhamento
Endereço de Origem			
Endereço de Destino			

Tabela 3- Cabeçalho IPv6. Fonte: Autoria Própria

2.12 IPv4 contra IPv6

O protocolo IPv4 tem muitas limitações. Várias coisas atrapalham a implantação do protocolo IPv6, como o NAT, o DHCP e o CIDR. Porém o IPv6 está sendo adotado aos poucos e é inevitável.

Hoje em dia a *Internet* caminha para ter qualquer sistema eletrônico conectado nela, como computadores, relógios, eletrodomésticos e outros. A *Internet* das coisas está só começando.

Mas o protocolo IPv4 tem um grande problema que é a limitação de IPs. Com ele podemos conectar 4 bilhões de dispositivos a internet. Já com o protocolo IPv6 podemos conectar até 45 octilhões de endereços por habitante na Terra, pois possui 128 bits de endereçamento.

Outra vantagem é que temos uma distribuição de endereços hierárquica no IPv6. Isto faz com que a tabela de roteamento dos roteadores seja bem menor. Este detalhe melhora o seu desempenho.

No IPv4 usamos mais o protocolo RIP, já no IPv6 usamos os protocolos de roteamento dinâmicos, como o BGP e o OSPF.

Quanto aos cabeçalhos, o IPv6 possui 8 campos com tamanho fixo de 40 *bytes*. O IPv4 possui 12 campos com um tamanho variando entre 20 e 60 *bytes*.

O protocolo IPv4 possui cabeçalhos com 12 campos, com tamanhos que variam de 20 a 60 *Bytes*. Já o IPv6, contém cabeçalhos de apenas 8 campos com tamanho fixo de 40 *Bytes*.

Quanto aos cabeçalhos o IPv6 pode ter cabeçalhos de extensão com funções especificas que só serão lidos pelos roteadores caso seja necessário. Os outros só serão lidos pelo host de destino.

O fato de o IPv6 ter um tamanho quatro vezes maior do que o seu antecessor e ter o cabeçalho duas vezes maior faz com que o desempenho seja melhorado, pois os roteadores conseguem analisar melhor o tráfego.

No novo protocolo podemos usar o IPSec que pode ser feito diretamente no IPv6, sem precisar de programas adicionais. O IPSec é usado geralmente em VPNs e é obrigatório no IPv6, diferente do IPv4 que é opcional.

Quanto aos protocolos RARP e ARP que são usados para cuidar da resolução dos endereços físicos no IPv4, foram substituídos pelo protocolo ICMP no IPv6. Isto tornou impossível bloquear totalmente o tráfego ICMP, como fazíamos no IPv4. Se você precisa bloquear uma função como o *ping*, por exemplo, você não deve bloquear o protocolo todo e sim apenas a função específica do ICMP. Em uma rede, IPv6 é recomendado permitir o tráfego ICMP.

O NAT é uma tecnologia que foi criada para permitir com que os equipamentos dentro de uma rede local acessassem a *Internet* usando um IP público do gateway. Usamos muito isso no IPv4, porem isto atrasou muito a adoção do IPv6.

O NAT quebra o modelo fim-a-fim da Internet, que foi o modelo proposto na sua criação. Podemos ter problemas com VPNs e P2P com o uso do NAT.

Mas com o IPv6 este problema é eliminado, pois não existe mais a necessidade de usar o NAT. Cada cliente pode usar um IP público devido a fartura de IPs.

Quanto ao roaming, que é a mudança de IPs quando saímos da rede 3G, depois entramos na rede wireless de casa. Sabemos que esta mudança de IPs nos dispositivos móveis pode derrubar as conexões. Já com o protocolo IPv6, podemos mudar de uma rede para outra e ao mesmo tempo preservar o endereço IPv6, desta forma, podemos ficar conectados o tempo todo, pois as conexões não serão perdidas.

Quanto a fragmentação dos pacotes, no IPv6 é feita somente na origem, pois a mecanismos que sabem qual é o menor tamanho máximo permitido em todo o trajeto, isto faz com que os roteadores não fragmentem os dados, melhorando assim o desempenho. Lembrando que na rede IPv4 os dados

passam por vários tipos de rede e cada uma delas permite um tamanho máximo dos pacotes de dados. Quando os dados são enviados pela rede, este pacote é dividido em pedaços menores, que podem ainda ser dividido em novos fragmentos, causando lentidão nos roteadores.

No IPv6, a fragmentação é feita somente na origem. Há mecanismos que permitem saber qual o menor tamanho máximo permitido em todo o trajeto. Os roteadores não fragmentam os dados. Isso melhora o desempenho.

Quanto a qualidade de serviço, o QOS, ele está implementado no protocolo IPv6 e não existe a necessidade de usar programas especiais. Isto faz com que programa de VoIP, por exemplo, tenha banda garantida.

O tamanho do frame no protocolo IPv6 é de 4 Gb, contra 1,5Kb do IPv4, porém ainda não existem aplicações que usem tudo isso.

No IPv6 não existe o broadcast e sim o *anycast*. Um pacote *anycast* é recebido somente pelo host mais próximo. O IPv6 sabe qual é o host mais próximo que responde a uma certa condição e que possui o mesmo prefixo IPv6. Em outras palavras, em uma mesma rede, pode haver hosts com prefixos diferentes. Um *anycast* só afetará as máquinas do mesmo prefixo, ao contrário do que ocorre num broadcast IPv4.

Lembrando que a rede no IPv4 geralmente fica mais lenta porque ela usa o broadcast que é recebido por todos os hosts.

Quanto aos endereços de rede e broadcast que são reservados o primeiro e o último no IPv4 em uma VLAN, por exemplo, os mesmos podem ser usados no IPv6.

O IPv6 é fundamental, então, para a expansão da Internet, possibilitando a continuidade da adição de novos usuários e o desenvolvimento da Internet das Coisas, interligando os mais diversos tipos de objetos inteligentes (Equipe IPv6.br, 2015).

2.13 Segurança na *internet* – IPSec no IPv4

O protocolo IPv4 ainda é usado hoje em dia e não possui nenhum tipo de segurança nativo. Quando a internet surgiu, a privacidade não era importante e

necessária quanto é hoje. Então, em resposta a falta de segurança no protocolo IPv4 foi criado o IPSec.

2.14 Segurança na *internet* – IPSec

IPSec significa *IPSecuriry* e foi desenvolvido pelo *Internet Engineering Task Force* (IETD). O IETD desenvolveu este conjunto de protocolos para atuar no nível da rede (IP) que ajuda a criar *datagramas* (pacotes) autenticados e confidenciais para esta camada. A Tabela 4 mostra o modelo TCP/IP.

Modelo TCP/IP
Aplicação
Transporte
IP
Acesso a Rede

Tabela 4- Modelo TCP/IP. Fonte: Autoria Própria

Em um túnel pode-se conectar vários aplicativos, serviços, usuários ou redes pelo canal existente de modo independente sem a necessidade de passar novo cabeamento (Santos, 2008).

Segundo a equipe IPV6.br a sua arquitetura foi primeiramente especificada na RFC 2401 (Kent e Atkinson, 1998) e na sequencia foi atualizada pela RFC 4301 (Kent e Seo, 2005).

Entre as RFCs temos a:

RFC 4301 (*The IP Security Architecture*), que define a arquitetura e os elementos originais IPsec comum a ambos AH e ESP.

RFC 4302 que define cabeçalhos de autenticação (AH).

- RFC 4303 – define o encapsulamento seguro de dados (ESP).

- RFC 2408 – ISAKMP.
- RFC 5996 – IKE v2 (setembro de 2010).
- RFC 4835 – Implementação do algoritmo criptográfico para ESP e AH.

Ele trabalha no modo túnel ou no modo transporte. No modo transporte é protegido aquilo que é estregue da camada transporte para a de rede. Este modo protege apenas o *payload* da camada IP. *Paylod* é parte dos dados transmitidos. O modo transporte protege apenas os pacotes da camada de transporte, não protege o cabeçalho IP. Aqui a *criptografia* e autenticação são realizadas apenas na parte de dados. A Figura 1 mostra o modo transporte.

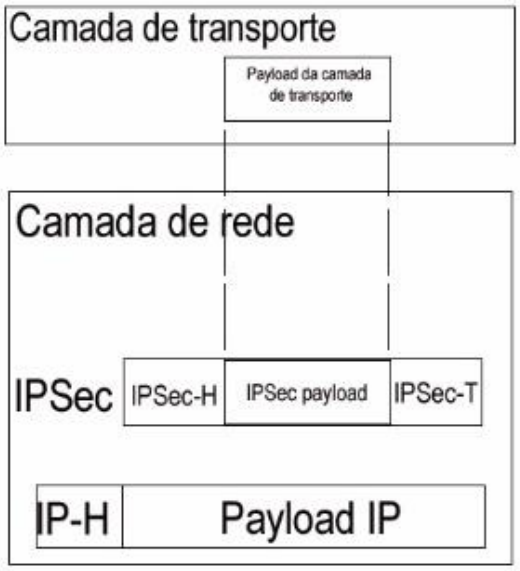

Figura 1- Modo Transporte. Fonte: Autoria Própria

Este modo de transporte geralmente é utilizado para proteger *host* a *host*, isto é, protege os dados fim a fim. Neste modo é necessário que os dois hosts que estão se comunicando usem e tenham suporte ao IPSec.

Já no modo túnel, o pacote IP é protegido por inteiro. Este modo é caracterizado pela comunicação entre dois roteadores de borda, porém ambos os roteadores necessitam de suporte ao IPSec.

No modo túnel, o roteador cria um outro pacote IP para encapsular o pacote original. Desta forma não precisamos configurar o IPSec nos hosts.

Aqui o gateway encapsula o pacote IP incluindo seu cabeçalho IP original com a *criptografia* do IPSec. Na sequência é adicionado um novo cabeçalho IP no pacote de dados que é enviado pela rede pública para outro *gateway*. Esta informação é decifrada e enviada ao endereço de destino em sua forma original.

No IPSec foram definidos dois protocolos de segurança, o protocolo AH (*Authentication Header*) e o protocolo ESP (*Encapsulating Security Payload*).

Estes pacotes foram criados para oferecer autenticação e *criptografia* aos pacotes IP.

O protocolo de cabeçalho de autenticação ou protocolo AH foi criado com o objetivo de autenticar o host de origem e também para garantir a integridade dos dados transportados no pacote IP.

O protocolo AH oferece apenas integridade de dados e autenticação da fonte, porém, não oferece privacidade.

O IP sozinho, não provê qualquer confidencialidade. Para isso o protocolo AH é utilizado para garantir a autenticidade e a integridade de pacotes IP.

No AH, um cabeçalho é acrescentado ao pacote IP. Neste cabeçalho é que estarão todos os dados de autenticação que serão analisados pelo receptor desta mensagem. A função usada para verificar os dados é a de *hash* como MD5, este é um algoritmo de 128 bits unidirecional desenvolvido pela RSA *Data Security*, muito usado em programas P2P e o SHA-1, este produz um valor de dispersão de 160 bits e foi criado pela agencia de segurança nacional dos Estados Unidos.

A função *hash* nada mais é do que um algoritmo para mapear dados de comprimento variável para dados de comprimento fixo.

Quando enviamos uma mensagem, é calculado uma sequência de bits de acordo com uma chave secreta e o conteúdo do pacote. O algoritmo usado neste processo é de *hash*. Na recepção desta mensagem, este *hash* é recalculado e comparado com o existente no cabeçalho AH.

É possível verificar se o pacote foi alterado pois apenas quem está se comunicando conhece a chave utilizada.

O texto original não poderá ser recuperado com uma função de *Hash*, pois esta não é uma técnica de *criptografia* e sim um resumo unilateral.

Existem vários algoritmos de funções *Hash*. Entre eles temos o MD2, MD4, MD5 e SHA-1.

O MD que significa *Message Digest*, produz um *Hash* de 128 bits. Entre as versões do MD, temos o MD2 e MD4 que são seguros, porém apresentam problemas de desempenho. Já o MD5 foi melhorado, porém não é aconselhado utilizá-lo por um longo período, pois é lento e também não é tão seguro comparado a outros algoritmos.

O algoritmo de *Hash* SHA-1 que significa *Secure Hash Algorithm*, é seguro e foi projetado pela NSA (*National Security Agency*). Ele produz 160 bits a partir de um tamanho arbitrário de mensagem.

As funções de *Hash* são muito importantes para a assinatura digital. Essas funções são utilizadas em documentos eletrônicos e verificam se uma mensagem foi alterada. A Tabela 5 mostra o protocolo AH.

Cabeçalho IP	Cabeçalho AH	Cabeçalho TCP/UDP	Dados

Tabela 5- Protocolo AH. Fonte: Autoria Própria

Já o protocolo ESP ou *payload* de segurança de encapsulamento foi criado para oferecer os recursos de autenticação de privacidade, fonte e integridade. Este protocolo adiciona um *trailer* e um cabeçalho. Todos os dados de autenticação são adicionados ao final do pacote. A Tabela 6Tabela 5 mostra o protocolo ESP.

Novo Cabeçalho IP	Cabeçalho ESP	Cabeçalho IP Original	Cabeçalho TCP/UDP	Dados	Trailer ESP	Autenticação ESP

Tabela 6- Protocolo ESP. Fonte: Autoria Própria

No IPSec temos suporte tanto ao IPv4, quanto ao IPv6. Porém apenas no IPv6 é que o ESP e o AH fazem parte do cabeçalho de extensão.

O protocolo AH é inferior ao ESP porque o ESP faz tudo o que ele faz, porém tem outra funcionalidade como a privacidade por exemplo. O AH está em uso em vários produtos comerciais e não vai sair do mercado antes que estes produtos saiam de linha.

Entre os serviços oferecidos pelos dois protocolos temos controle de acesso, autenticação de mensagens, autenticação de fontes de dados e proteção de ataques de reprodução.

Apenas na *criptografia* de mensagens usando o ESP é que temos confidencialidade, ela não existe no AH.

O IPsec usa o compartilhamento das chaves que são utilizadas para autenticação e *criptografia*. Para isto é utilizado o protocolo IKE ou *Internet Key Exchange*, este que garante segurança para a troca de chaves entre os dispositivos que utilizam IPsec. Esta troca de chaves pode ocorrer através do uso de certificados X.509 ou da utilização de chaves pré-compartilhadas. Então este protocolo é responsável pela gerência automática das chaves.

A chance de sofrermos um ataque é reduzida quando os dados são criptografados e autenticados.

A troca de chaves permite uma forma para os usuários estabelecerem uma chave secreta compartilhada, que só eles sabem, embora esteja sendo enviada através de um canal inseguro (WOJCIK, 2014).

Com o objetivo de criar um meio seguro para a troca de informações o IPSec fará a negociação de *algoritmos*, dos protocolos e chaves. Ele vai fazer o *refresh* (atualização) na conexão e também a troca de chaves. O gerenciamento das chaves pode ser feito em modo manual ou em modo automático.

Um dos pontos principais no funcionamento do IPsec é o compartilhamento das chaves utilizadas para a *criptografia* e a autenticação. Para garantir um meio seguro para a troca das chaves entre os dispositivos que utilizam IPsec usamos do protocolo IKE ou *Internet Key Exchange* e essa troca pode ocorrer mediante a utilização de certificados X.509 e também o uso de chaves pré-compartilhadas.

O protocolo IKE implementa automaticamente as chaves, pois é protocolo híbrido constituído pelo ISAKMP e pelo OAKLEY.

Este protocolo trabalha em duas etapas:

- A primeira é por meio de uma série de mensagens trocadas, a autenticidade dos dispositivos é verificada e uma chave ISAKMP SA que significa *Internet Security Association Key Management Security Association* é gerada.

- Na segunda etapa as chaves para o AH e ESP para esta comunicação são geradas a partir da chave ISAKMP SA e assim o começa a utilização do IPsec.

A responsabilidade pela negociação, pelo estabelecimento, pela exclusão e pela modificação das SA fica por conta do ISAKMP. Este explica os procedimentos e o formato dos pacotes. Para sua implementação utiliza-se a porta 500 do UDP.

Quem fornece o mecanismo de troca de chaves utilizado pelo ISAKMP é o OAKLEY. Este é uma modificação mais segura do algoritmo Diffie-Hellman.

Quanto aos parâmetros de segurança, o IPSec usa um mecanismo denominado associação de segurança ou SA (*Security Association*). Conforme Silva (2004) uma SA define os tipos medidas de segurança que devem ser aplicadas aos pacotes baseados em quem está enviando os pacotes, para onde eles estão indo e que tipo de dados eles estão conduzindo.

Entre os parâmetros, temos a chave de *criptografia* e de autenticação, o algoritmo de *criptografia* e de autenticação. Todas as informações são comuns ao emissor e ao receptor.

São 3 os parâmetros que identificam uma SA: o *Security Parameters Index*, o endereço IP de destino e o identificador de protocolo de segurança, que relaciona a SA ao ESP ou ao AH.

2.15 Arquitetura IPSec

O órgão responsável pelo desenvolvimento do IPSec é o IETF. Existem 18 RFC's: RFC2411 – IP *Security Document Roadmap*, RFC2401 – *Security Architecture for the Internet Protocol*, RFC2402 – IP *Authentication Header* (AH), RFC2406 – IP *Encapsulating security Payload* (ESP), RFC2409 – *The Internet*

Key Exchange (IKE), RFC2408 – *Internet Security Association and Key Management Protocol* (ISAKMP), RFC2407 – *The Internet IP Security Domain of Interpretation for* ISAKMP, RFC2412 – *The* OAKLEY *Key Determination Protocol*, RFC1828 – IP *Authentication using Keyed* MD5, RFC2104 – HMAC: *Keyed-Hashing for Message Authentication*, RFC2085 – HMAC-MD5 IP *Authentication with Replay Prevention*, RFC1829 – The ESP DES-CBC *Transform*, RFC2451 – *The* ESP CBC-*Mode Cipher Algorithms*, RFC2405 – The ESP DES-CBC *Cipher Algorithm With Explicit* IV, RFC2403 – *The Use of* HMAC-MD5-96 *within* ESP *and* AH, RFC2404 – *The Use of* HMAC-SHA-1-96 *within* ESP *and* AH, RFC2857 – *The Use of* HMAC-RIPEMD-160-96 *within* ESP *and* AH, RFC2410 – *The NULL Encryption Algorithm and Its Use With* IPSec, RFC2451 – *The* ESP CBC - *Mode Cipher Algorithms*, RFC2405 – *The* ESP DES-CBC *Cipher Algorithm With Explicit* IV, RFC2403 – *The Use of* HMAC-MD5-96 *within* ESP *and* AH, RFC2404 – *The Use of* HMAC-SHA-1-96 *within* ESP *and* AH, RFC2857 – *The Use of* HMAC-RIPEMD-160-96 *within* ESP *and* AH, RFC2410 – *The* NULL *Encryption Algorithm and Its Use With* IPSec.

As RFCs são a documentação mais completa sobre IPSec.

Existe uma divisão das RFC's em grupo. A Figura 2 mostra a arquitetura IPSec.

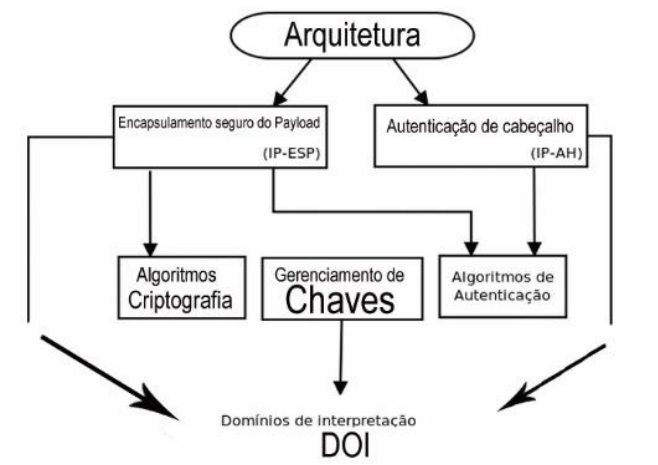

Figura 2- Arquitetura IPSec. Fonte: Autoria Própria

A arquitetura fala sobre mecanismos, requisitos, conceitos e definições do IPSec. O encapsulamento seguro de *Payload* é quem controla a formatação dos

pacotes IP, em relação à *criptografia*. A autenticação de cabeçalho é quem controla a formatação dos pacotes IP em relação à autenticação. Os *algoritmos* de *criptografia* definem quem são os *algoritmos* de *criptografia*. A gerência de chaves faz o controle dos mecanismos de gerência de chaves. O domínio de interpretação determina quais os objetivos de determinada *criptografia* ou autenticação.

2.16 Autenticação

Para realizar um negócio a longa distância, é necessário saber quem está na outra extremidade para o caminho ser considerado seguro. O IPsec oferece suporte para realizar esta autenticação. Entre os métodos de autenticação também temos o PSK onde temos uma chave secreta que é compartilhada entre as duas partes por meio de um canal seguro antes de ser usada. Estas chaves usam algoritmos com *criptografia* de chave simétrica. Cada PSK é usada para autenticar cada item de mesmo nível e é inserida manualmente nas duas extremidades. Para formar a chave de autenticação ela é agrupada as outras informações.

Nas assinaturas de RSA temos os certificados digitais que são trocados para autenticar os itens de mesmo nível. A assinatura será verdadeira somente se o *hash descriptografado* com chave pública corresponder ao *hash* recalculado. O *hash* original usa *criptografia* com chave privada e este é anexado à mensagem e encaminhado à extremidade remota.

O RSA é um sistema de *criptografia* com chave pública usado para autenticação no contexto do IKE e é usado pelo IPSec. A segurança de uma RSA é superior a uma PSK.

Segundo o material do curso CCNA da cisco 2015, em uma RSA um usuário que inicia e responde a uma sessão de IKE com assinaturas de RSA envia seu próprio valor de ID, seu certificado digital de identidade e um valor de assinatura de RSA que consiste em vários valores de IKE, todos criptografados pelo método de *criptografia* IKE negociado.

2.17 *Frameworks* de Segurança do IPSEC (AH e ESP)

Estes *Frameworks* usam recursos independentes para realizar suas finalidades. O IPSec possui *algoritmos* que podem ser alterados com o tempo, de acordo com a sua maturidade ou necessidade.

Entre os *algoritmos* pré-definidos suportados pelo IPSec temos para *criptografia* o DES (*Data Encryption Standard*) que usa chave de 64 bits mínima, da qual 56 bits estão disponíveis para definir a chave propriamente dita, e 8 bits são usados para fornecer detecção de erro na chave. Ele criptografa informações em código binário. Temos também o 3-DES que foi desenvolvido pela IBM e é baseado o DES. Este *algoritmo* usa 3 chaves de 64 bits. Aqui temos os dados *encriptados* com a primeira chave, e depois são *decriptados* com a segunda chave e ao final são *encriptados* novamente com a terceira chave. Este processo torna o 3-DES um pouco mais lento que o DES, porém oferece uma segurança melhor. Em *criptografia* temos também o AES que usa chave de 128 bits.

Para autenticação temos o algoritmo HMAC que utiliza funções de *criptografia hash*. Este algoritmo pode ser usado com qualquer função *hash* como o MD5 por exemplo. Quanto ao algoritmo MD5, o mesmo produz um código de autenticação de 16 bytes a partir dos dados de qualquer tamanho com ou sem uma chave de qualquer tamanho. Temos também o SHA1, 2 e 3, que gera um valor *hash* de 160 bits, a partir de um tamanho arbitrário de mensagem.

2.18 Criptografia

Na *criptografia* estudamos algumas técnicas matemáticas aplicadas à segurança da informação tem o objetivo de esconder as palavras, tornando as mensagens secretas, com autenticação, confiabilidade, integridade dos dados.

A *criptografia* utiliza a própria mensagem e uma chave para produzir a mensagem codificada. Quando a mensagem cifrada é transmitida, o receptor utiliza a chave para reverter o processo e a própria mensagem para obter a mensagem original. Quando a chave para cifrar e a chave para reverter o

processo são iguais, significa que a *criptografia* é simétrica, caso contrário a *criptografia* é assimétrica.

Existe um método de *criptografia* de chaves assimétricas que utiliza números primos para a geração de chaves e seu nome é RSA.

Também usamos *criptografia* com o IPSec para criar conexões seguras e proteger a integridade das mensagens.

2.19 RFC - *Request for Comments*

As RFCs são documentos técnicos criados e sustentado pelo grupo *Internet Enginnering Task Force* ou IETF.

A IETF é a instituição que determina as normas que serão realizadas em toda a internet.

A RFC 2409 (protocolo IKE), por exemplo, tem o objetivo é negociar, e fornecer material de entrada autenticado para associações de segurança de uma forma protegida.

Quando um padrão se torna obsoleto, é gerado um outro arquivo chamado *Request for Change*, onde as pessoas que possuem a instrução necessária sobre a questão criam respostas para a dificuldade proposta. Estas respostas aos problemas são analisadas por um comitê e caso sejam aprovadas, tornam-se uma nova RFC sempre com um número diferente da RFC original. Esta não será excluída pois existem pessoas que podem querer aprender mais sobre o conteúdo.

2.20 Assinatura Digital

A assinatura digital ou eletrônica é como uma assinatura de punho reconhecida em cartório. Implementar sistemas de *criptografia* com a assinatura digital preserva o conteúdo das mensagens dos documentos assinados. Para cifrar e decifrar a mensagem, tanto a chave pública quanto a privada podem ser utilizadas segundo o RSA.

Para gerar uma assinatura digital usamos a função *Hash*. Aqui não é cifrado todo o conteúdo da mensagem na assinatura digital, apenas a saída da função *Hash* é aplicada sobre a mensagem original.

Entre as vantagens de usar a função *Hash* em assinaturas digitais temos um aumento significativo da velocidade de verificação e geração de assinaturas pois as saídas das funções *Hash* são menores que as mensagens completas. Outra vantagem é que a assinatura digital pode ser anexada a mensagem no instante que precisar, pois ela pode ser gerada em separado da mensagem propriamente dita.

Uma assinatura digital gera autenticidade e integridade ao documento, tirando a necessidade de imprimir e assinar manualmente o documento, isto é, ela dá legalidade a documentos eletrônicos.

2.21 Certificado Digital

O Certificado Digital é utilizado para comprovar a sua identidade em uma rede de computadores e é a versão eletrônica do RG de uma pessoa.

Estes Certificados Digitais são necessários para realizar transações eletrônicas de forma segura via Internet. A garantia da veracidade da identidade é feita através da apresentação dos seus respectivos Certificados.

O Certificado Digital vincula o valor de uma chave pública à identidade da pessoa, dispositivo ou serviço que contém a chave privada correspondente. É uma forma de assinar de forma digital os documentos. Todo certificado precisa ser emitido por uma Autoridade Certificadora (CA).

Uma CA deve garantir que os dados de identificação do certificado são verdadeiros e é a instituição responsável em certificar digitalmente uma empresa. Uma CA é dita por todos como confiável, pois faz o papel de um cartório eletrônico.

Quase todos os certificados são baseados no padrão X.509. Estes possuem informações da identificação do usuário, a chave pública do usuário, informações sobre a identificação do emissor do certificado, período de validade

e a assinatura digital da certificadora. A certificação digital garante a integridade, autenticidade e privacidade.

2.22 Mecanismos de defesa usados no IPSec

O IPSec precisa garantir confiabilidade, integridade e autenticidade na conexão. Confiabilidade é limita o acesso a informação somente às entidades autorizadas pelo proprietário da informação. Quando usamos os meios públicos de comunicação, interceptar os dados é simples. Então é importante que os dados sejam privados para que não possam ser entendidos caso sejam capturados.

A integridade da a garantia que toda a informação conserve todos os atributos originais determinados pelo proprietário da informação. Caso os dados sejam capturados, eles não podem ser adulterados e muito menos reencaminhados.

A autenticidade garante que a informação é original e que não foi modificada no processo.

Tanto a *criptografia* quanto a autenticação de pacotes no IPSec são feitas na camada de rede. Desta formo ele fornece uma solução de segurança fim-a-fim, garantindo a confidencialidade, a integridade e a autenticidade dos dados.

Quanto aos mecanismos de defesa, são cinco.

Na primeira chamada defesa *packet sniffing*, o IPSec não permite que o *software sniffer* faça a captura dos dados trafegados por este túnel, pois provê confidencialidade do fluxo de pacotes através do tunelamento dos gateways.

O segundo mecanismo de defesa é captura de usuário e senha nas seções FTP e *telnet*. Para evitar que o *hacker* identifique as sessões FTP e *Telnet* e tentem fazer uma autenticação para se passar por usuários, é feita uma autenticação de dados que identifica a fonte original do trafego de dados. Com isso o *hacker* não terá acesso às informações, a não ser que o mesmo quebre a senha. Caso isto aconteça, o *hacker* não conseguirá identificar o conteúdo da informação original, pois a mesma foi cifrada pelo túnel IPSec.

O terceiro é a defesa contra o ataque TCP SYN *flood* que pode tirar vantagem do 3 *WAY HANDSHAKE* efetuado pelo protocolo TCP durante a conexão. Neste ataque é feito um pedido de conexão para o servidor da vítima com alguns pacotes que carregam endereços falsos do IP de origem. Isto faz com que o servidor perca tempo e recursos da máquina. Neste caso o IPSec verifica a integridade de qualquer pacote IP individual sem precisar relacionar outro pacote. Isto significa que cada pacote pode ser validado sobre si próprio ou permanecer sozinho. Então para invadir pelo 3 *WAY HANDSHAKE* o atacante precisaria que os muitos pedidos de conexão fossem aceitos ao mesmo tempo. Caso isto ocorra, o IPsec tem uma forma de defesa contra este ataque com pacotes repetidos com um contador de pacotes.

A quarta defesa é contra o TCP *Session Hijacking*, também conhecido como ataque *man in the middle*, onde é um hacker toma controle de uma sessão TCP entre duas maquinas. Geralmente a autenticação ocorre no início de uma sessão TCP. Podemos evitar ataques desse tipo se usarmos um mecanismo de controle de acesso e autenticação. Lembrando que mesmo que o hacker tenha sucesso, as informações serão cifradas e por isto ele não terá acesso aos dados originais.

A quinta defesa é contra o IP *Spoofing*. Neste ataque é criado um pacote IP que utiliza o endereço IP da outra origem. O IPSec possui um mecanismo de controle e autenticação de acesso para prevenir este tipo de ataque. E mais uma vez, caso ocorram, existe o processo de ciframento da informação pelo túnel do IPSec.

Então pode-se ver que o IPSec é necessário para garantir o sigilo da informação e para proteger contra os ataques ao TCP/IP.

Basicamente o IPSec através do protocolo AH preveni 3 tipos de ataques: *Replay, Spoofing* e roubo de conexões. Para se proteger do ataque *Replay*, onde ocorre a interceptação de pacotes válidos, é utilizado o campo *Sequence Number*, para numerar os pacotes que trafegam dentro de uma AS. A autenticação resolve o problema do *Spoofing* e de roubo de conexões. Através do ESP previne ataques do tipo *Replay*, Particionamento de pacotes cifrados e *Sniffer*.

2.23 Vantagens e desvantagens do IPSec

O IPSec foi criado para trazer segurança e não deve ser usado em sistemas já comprometidos para não a segurança dos dados. A implementação do IPSec é complexa e pode sobrecarregar os hosts já que os algoritmos de *criptografia* podem deixar a rede mais lenta.

Mesmo assim o IPSec é arma contra vários tipos de ataques e invasões quando é utilizado de forma correta combinando os protocolos AH e o ESP. A configuração correta vai dificultar uma invasão.

3 PRÁTICA - IPSEC NO PACKET TRACER

Segue abaixo um tutorial explicando como aplicar o protocolo IPSec em uma rede IPv4 usando o programa Packet Tracer da Cisco.

Abaixo segue Figura 3 com o modelo da rede que será criada.

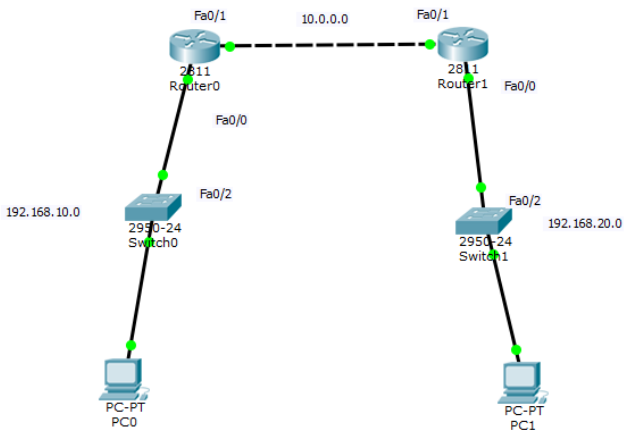

Figura 3- Rede com IPSec. Fonte: Autoria Própria

- Inserir 2 Roteadores 2811
- Inserir 2 *Switches* 2950 de 24 portas
- Inserir 2 computadores *Desktop*
- Use o sistema automático para fazer o cabeamento

- Será feita uma VPN entre o roteador 0 e roteador 1
- Configure o primeiro computador (PC0) como a Figura 4 abaixo:

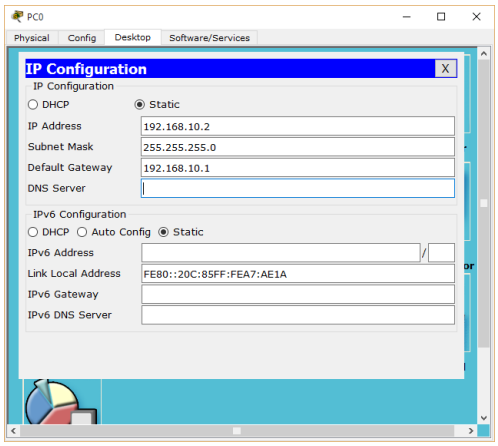

Figura 4- Configuração PC0. Fonte: Autoria Própria

- Configure o segundo computador (PC1) como a Figura 5.

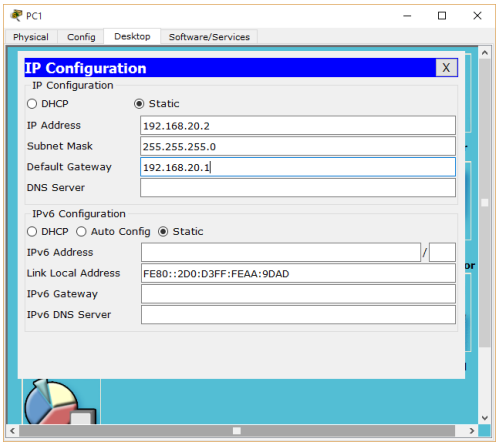

Figura 5- Configuração PC1. Fonte: Autoria Própria

- Agora faça a configuração do Roteador 0
- Primeiro configure a *FastEthernet* 0/0 com na Figura 6.

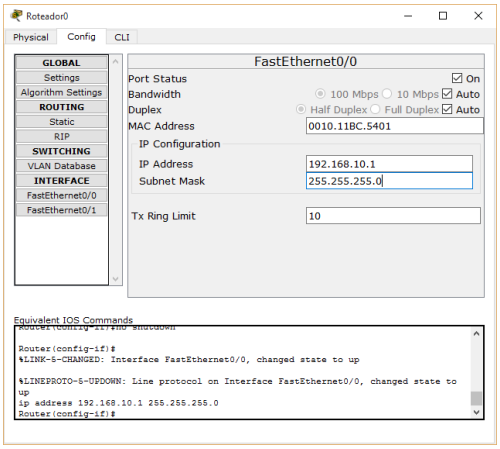

Figura 6- Configuração FastEthernet 0/0. Fonte: Autoria Própria

- Depois configure a *FastEthernet* 0/1 como na Figura 7.

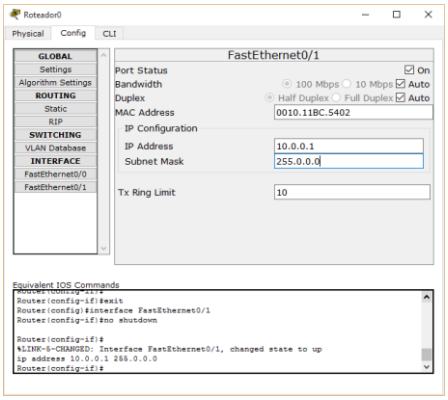

Figura 7- Configuração FastEthernet 0/1. Fonte: Autoria Própria

- Cria as rotas 192.168.10.0 e 10.0.0.0 como na Figura 8, Figura 9 e Figura 10.

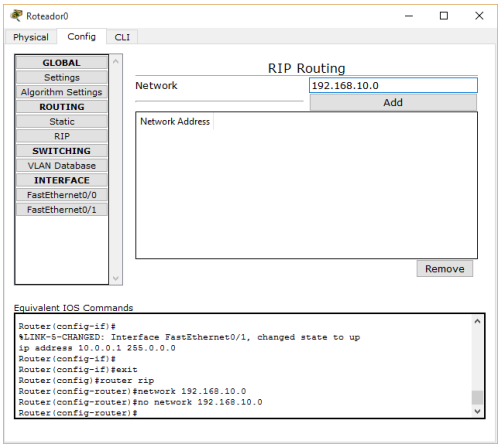

Figura 8- Rota 192.168.10.0. Fonte: Autoria Própria

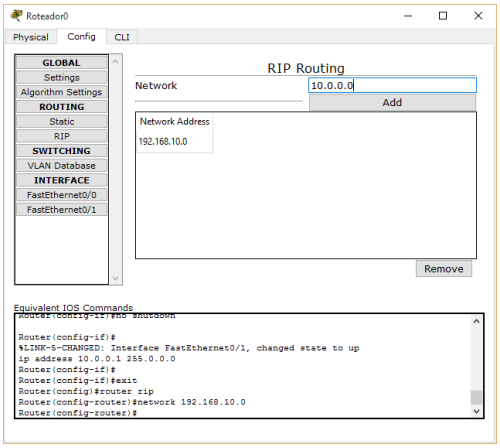

Figura 9- Rota 10.0.0.0. Fonte: Autoria Própria

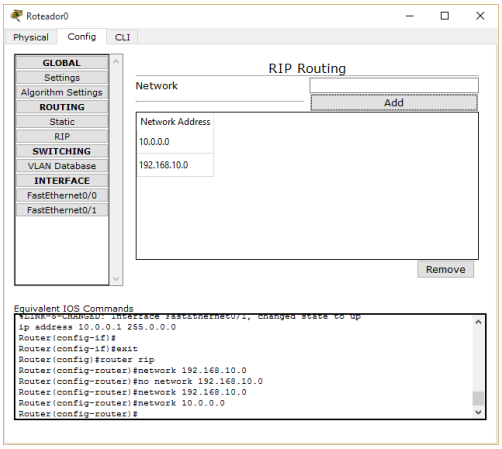

Figura 10- As duas rotas. Fonte: Autoria Própria

- Agora faça a configuração do Roteador 1
- Primeiro configure a *FastEthernet* 0/0 como na Figura 11.

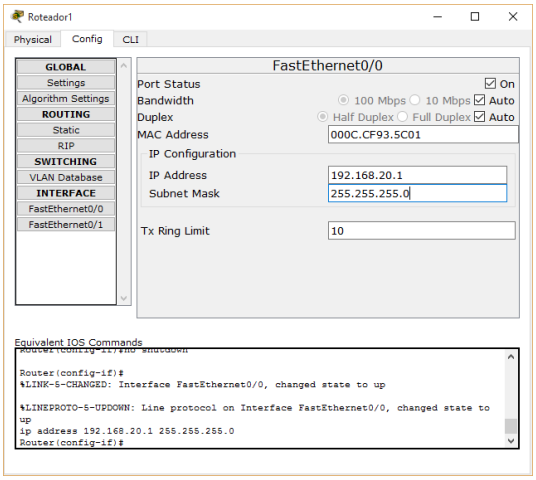

Figura 11- Configuração FastEthernet 0/0 do Roteador1. Fonte: Autoria Própria

- Configure a *FastEthernet* 0/1 como na Figura 12.

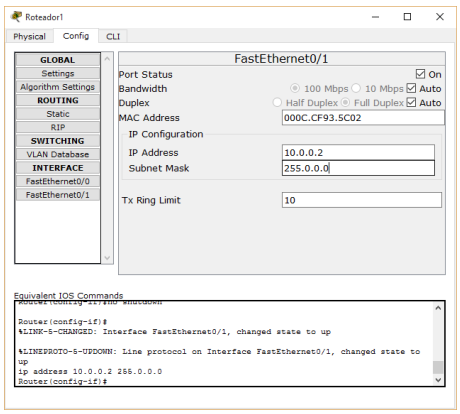

Figura 12- Configuração FastEthernet 0/1 do Roteador 1. Fonte: Autoria Própria

- Configure as Rotas 192.168.20.0 e 10.0.0.0 como na Figura 13, Figura 14 e Figura 15.

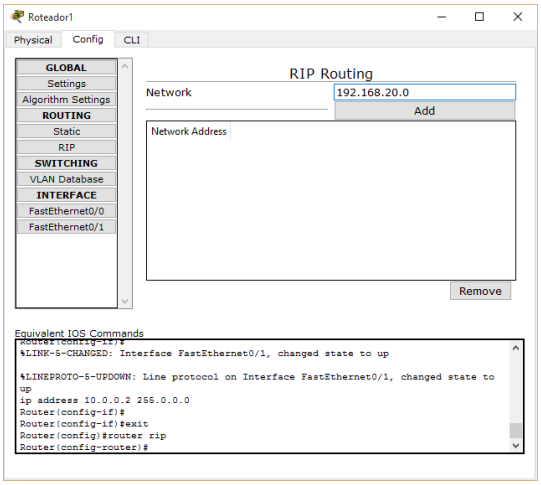

Figura 13- Rota 192.168.20.0. Fonte: Autoria Própria

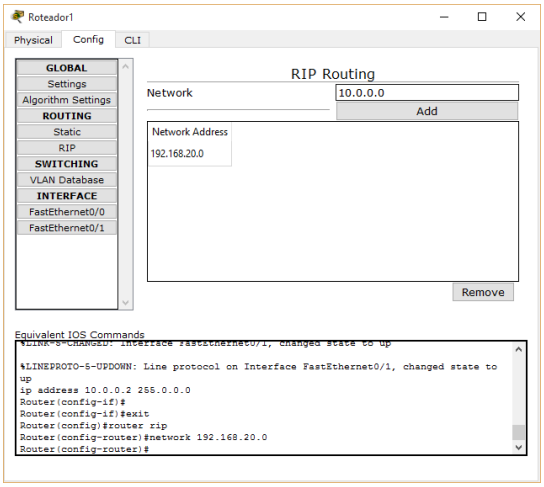

Figura 14- Rota 10.0.0.0. Fonte: Autoria Própria

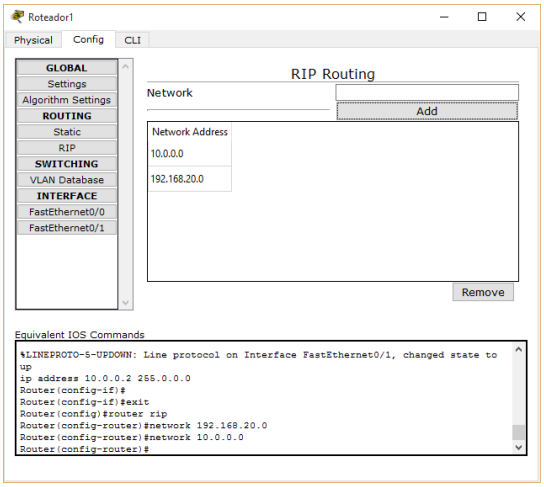

Figura 15- As duas Rotas. Fonte: Autoria Própria

- Pronto, já foram configurados todos os dispositivos na rede.
- Agora vamos configurar a VPN do Roteador 0
- Primeiramente configuraremos os parâmetros ISAKMP
- O número 10 é apenas o identificador da política (podemos ter mais que uma)

Entre no CLI e siga os seguintes passos:

- Passo 1

- Router(config)#crypto isakmp policy 10

- Passo 2 - Como método de autenticação use:

- Router(config-isakmp)#authentication pre-share

- Passo 3 - Use o algoritmo de *hash* SHA:

- Router(config-isakmp)#hash sha

- Passo 4 - Como *algoritmo* de *criptografia* use o AES-256:

- Router(config-isakmp)#encryption aes 256

- Passo 5 - Comando para a troca de chaves Diffie-Hellman:

- Router(config-isakmp)#group 2

- Passo 6 - Use o tempo de vida em segundos do *Security Association*:

- Router(config-isakmp)#lifetime 86400
- Router(config-isakmp)#exit

- Passo 7 - Use uma chave compartilhada para comunicação com o outro *peer*:

- Router(config)#crypto isakmp key toor address 10.0.0.2

- Passo 8 - Segue a definição da fase 2 dos parâmetros IKE. Aqui vamos criar o *transform-set* para definir os parâmetros que serão usados pelo túnel IPSec. Use o ESP-SHA-HMAC para *hash* (Obs: TSET é o nome do *transform-set*) e o ESP-AES para *criptografia*:

- Router(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac

- Passo 9 - Defina qual será o tráfego protegido pelo túnel IPSec com uma ACL:

- Router(config)#access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255

- Passo 10 - Faça o agrupamento das regras para construção do túnel criando o *Crypto Map* (CMAP é o nome do *crypto map* e 10 é o identificador):

- Router(config)#crypto map CMAP 10 ipsec-isakmp

- Passo 11 - Faça o apontamento do *peer* remoto dentro dele:

- Router(config-crypto-map)#set peer 10.0.0.2

- Passo 12 - Agora aplique a ACL:

- Router(config-crypto-map)#match address 101

- Passo 13 - Use o *Transform Set*:

- Router(config-crypto-map)#set transform-set TSET
- Router(config-crypto-map)#exit

- Passo 14 - Aplique na interface WAN do Router0:

- Router(config)#interface fastEthernet 0/1
- Router(config-if)#crypto map CMAP
- Router(config-if)#do wr

- Passo 15 - Agora faça a mesma configuração no Router1:

Router>enable
Router#configure terminal
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#hash sha
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#exit
Router(config)#crypto isakmp key toor address 10.0.0.1
Router(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac
Router(config)#access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config)#crypto map CMAP 10 ipsec-isakmp
Router(config-crypto-map)#set peer 10.0.0.1
Router(config-crypto-map)#match address 101

Router(config-crypto-map)#set transform-set TSET
Router(config-crypto-map)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#crypto map CMAP
Router(config-if)#do wr

- Passo 16 - Use o comando abaixo para confirmar a criptografia:

Router#show crypto isakmp sa
Router#show crypto ipsec sa

4 PRÁTICA – CRIANDO REDE IPv6 NO PACKET TRACER

Nesta prática será criada uma rede IPv6 ligando os dois ambientes da Figura 16 abaixo.

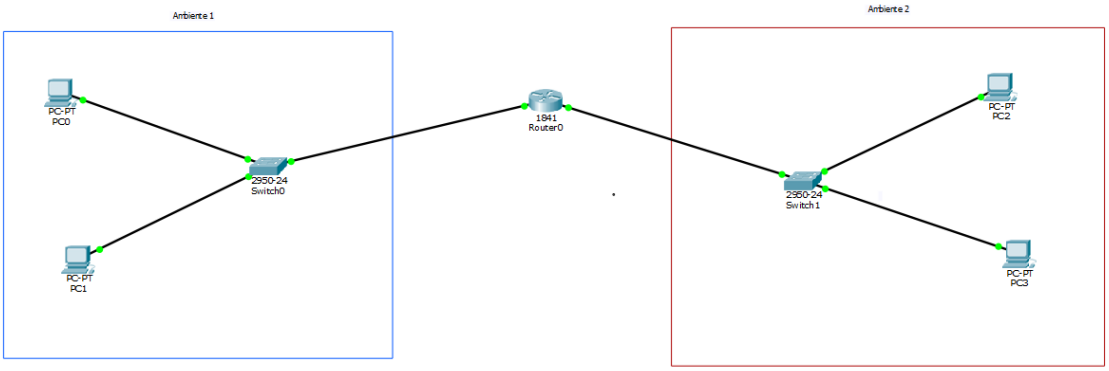

Figura 16- Rede IPv6. Fonte: Autoria Própria

O objetivo é criar 2 ambientes com 2 computadores, 1 switch cada um e um roteador ligando os 2 ambientes. Fazer a ligação de cabos e fazer a configuração dos IPs nas máquinas, todas em IPv6.

Configure o ambiente 1 da seguinte forma:

- Adicionar o IPv6 *Gateway* 2001:ABDA:ABDA::1 ao PC0 como na Figura 17.

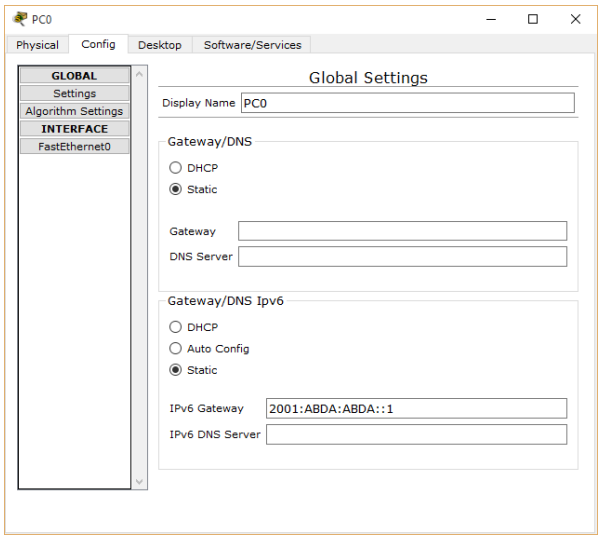

Figura 17- Gateway do PC0. Fonte: Autoria Própria

- Adicionar IP estático 2001:ABDA:ABDA::10 / 64 como na Figura 18.

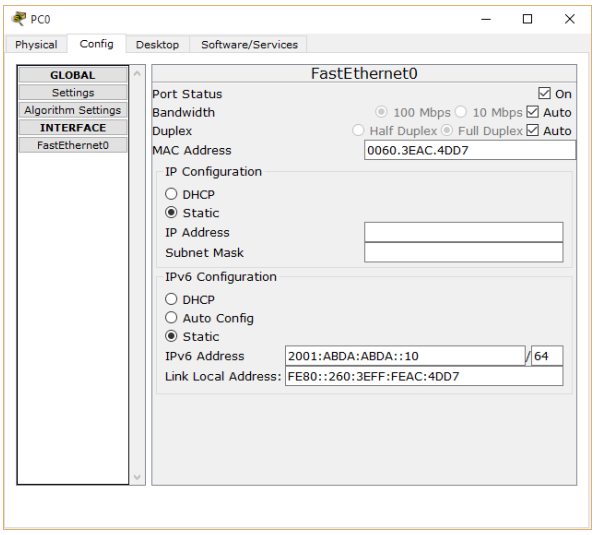

Figura 18- IP Estático PC0. Fonte: Autoria Própria

- Fazer o mesmo no PC1
- *Gateway*: 2001:ABDA:ABDA::1
- IP estático: 2001:ABDA:ABDA::11 / 64 como na Figura 19 e Figura 20.

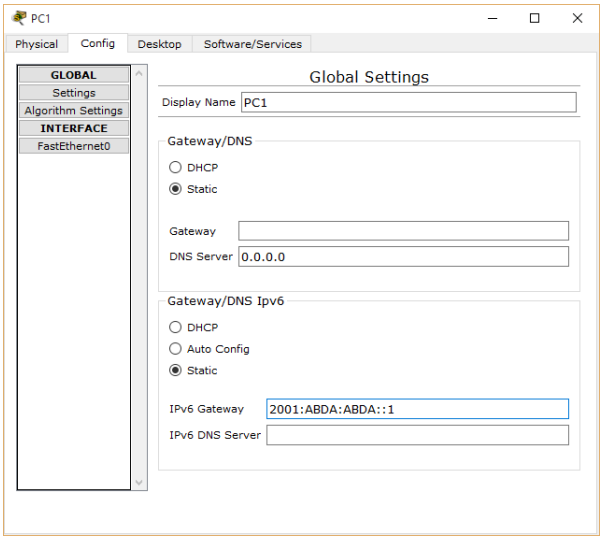

Figura 19- Gateway PC1. Fonte: Autoria Própria

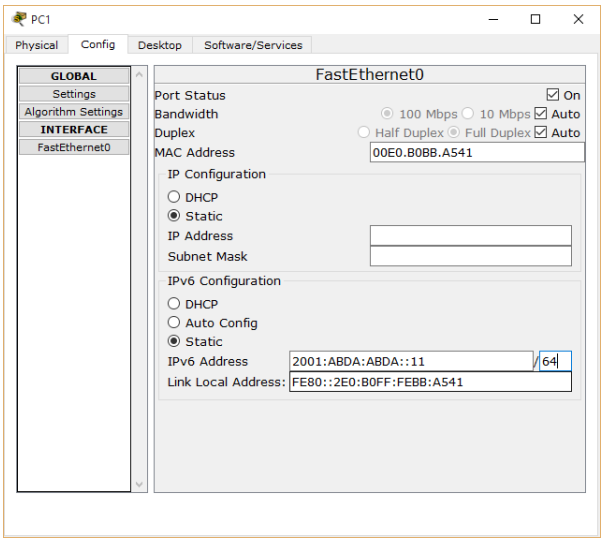

Figura 20- IP estático PC1. Fonte: Autoria Própria

- Configurar ambiente 2 da seguinte forma:
- No PC2
- *Gateway*: 2001:ABCD:ABCD::1
- IP estático: 2001:ABCD:ABCD::10/ 64 como na Figura 21 e Figura 22.

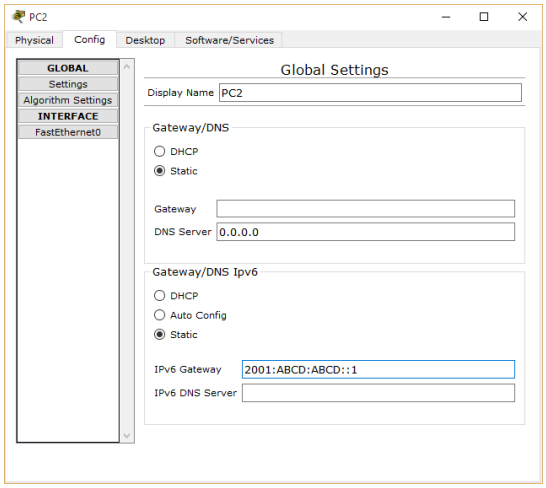

Figura 21- Gateway PC2. Fonte: Autoria Própria

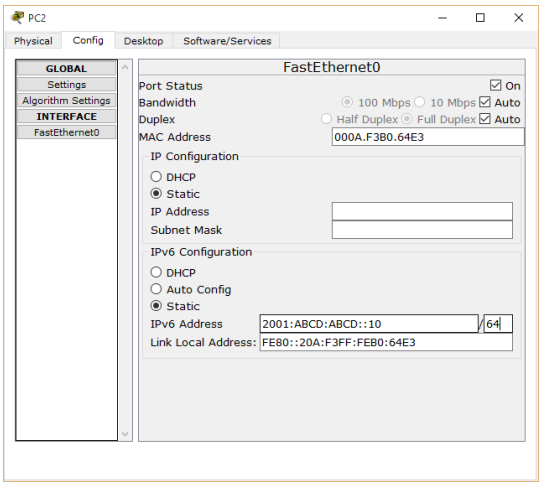

Figura 22- IP estático PC2. Fonte: Autoria Própria

- No PC3
- *Gateway*: 2001:ABCD:ABCD::1
- IP estático: 2001:ABCD:ABCD::11/ 64 como na Figura 23 e Figura 24.

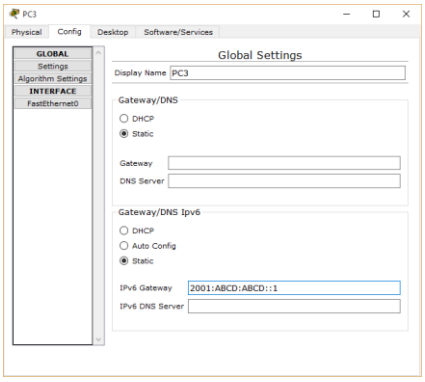

Figura 23- Gateway PC3. Fonte: Autoria Própria

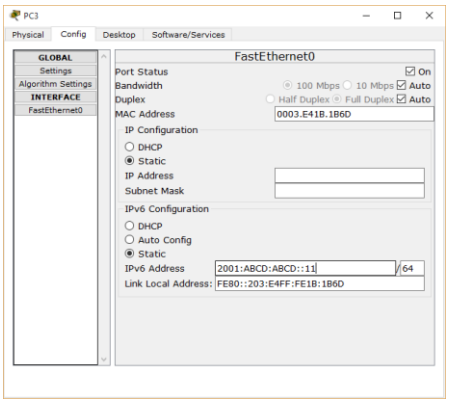

Figura 24- IP estático PC3. Fonte: Autoria Própria

- No *Router* deverá ligar as portas *FastEthernet* do roteador. Ligar a 0/0 e a 0/1.
- Configurar as portas *FastEthernet* clicando em CLI como na Figura 25.

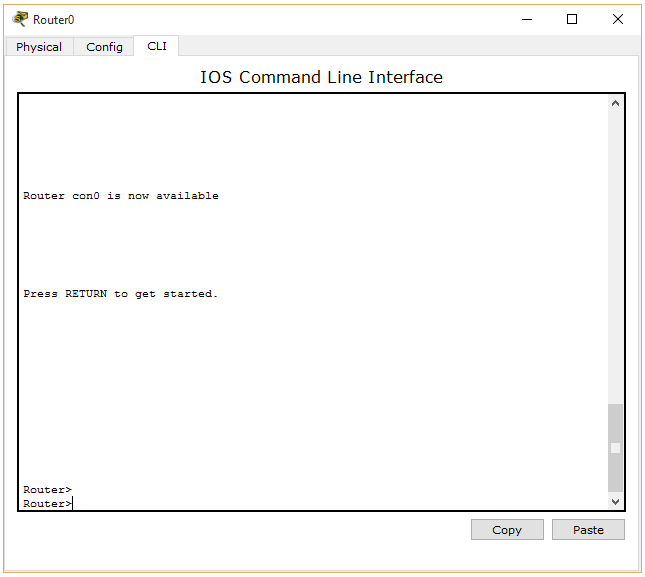

Figura 25- CLI do Router0. Fonte: Autoria Própria

- Comandos que serão usados seguem abaixo:

  Router>

  Router>enable

  Router#configure terminal

  Router(config)#ipv6 unicast-routing

  Router(config)#interface fastEthernet 0/0

  Router(config-if)#ipv6 enable

Router(config-if)#ipv6 address 2001:abda:abda::1/64
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit

- Agora começa novamente para configurar a próxima porta
  Router>enable
  Router#configure terminal
  Router(config)#ipv6 unicast-routing
  Router(config)#interface fastEthernet 0/1
  Router(config-if)#ipv6 enable
  Router(config-if)#ipv6 address 2001:abcd:abcd::1/64
  Router(config-if)#no shutdown
  Router(config-if)#exit
  Router(config)#exit

  Saia do *Router*

5 CONCLUSÃO

Este trabalho de referencial teórico confirma a superioridade da performance do protocolo IPv6 sobre o protocolo IPv4. Tanto os problemas de segurança como problemas de lentidão foram melhorados.

Os benefícios do novo protocolo são muitos. Ele resolveu a questão do espaço de endereçamento, qualidade dos serviços, segurança e melhorou o suporte a gerenciamento de endereços.

Quantos aos problemas de segurança nas empresas onde a comunicação com troca de dados, o IPSec mostrou-se bem eficiente em ataques com *software sniffer, man in the middle* e outros. Isso acontece porque o IPSec tem um sistema poderoso de verificação de integridade, confidencialidade e a autenticidade dos pacotes de dados.

6 REFERÊNCIAS BIBLIOGRÁFICAS

BEHROUZ, Rafael Francisco. **Análise de desempenho de tráfego de rede IPv4/IPv6 em uma Intranet Fast Ethernet/Gigabit Ethernet**. Minas Gerais (Lavras), 2005. Disponível em: <http://www.ginux.ufla.br/files/mono-RafaelThibes.pdf>. Acesso em: 11 de junho de 2015.

CURSO DE INTRODUÇÃO AO IPV6. Oferecido pelo CGI.br e NIC.br, 2015. Disponível no site: <http://ipv6.br/curso>. Acesso em: 27 de maio de 2015.

Forouzan, Behrouz A. **Comunicação de dados e redes de computadores**. São Paulo: McGraw-Hill, 2008.

SILVA, Lino Sarlo da**. Public Key Infrastructure – PKI: Conheça a Infra-estrutura de Chaves Públicas e a Certificação Digital.** São Paulo: Novatec, 2004.

Laboratório de IPv6 [livro eletrônico]: **Aprenda na prática usando um emulador de redes / Equipe IPV6.br**. – São Paulo: Novatec Editora, 2015.

KENT, S; SEO, K. **Security Architecture for the Internet Protocol**. RFC 4301, IETF. 2005. Disponível em: <http://www.ietf.org/rfc/rfc4301.txt> Acesso em: setembro de 2015.

BASSO, CRISTINA. **IMPLEMENTAÇÃO DE IPSEC INTEGRADO COM O IPv6.** Disponível em: < ieeexplore.ieee.org > Acesso em: agosto de 2015.

WOJCIK, EDUARDO. **ANÁLISE E SIMULAÇÃO DE VPN COM IPSEC EM ROTEADORES CISCO.** Disponível em: < ieeexplore.ieee.org > Acesso em: agosto de 2015.

CISCO, Networking Academy. **CCNA EXPLORATION – FUNDAMENTOS DE REDE**. Cisco Systems, Inc., 2015.

ALMEIDA, ERICSON NOGUEIRA. INES, OLGA ABREU DE SANTA**. INTRODUÇÃO AO PROTOCOLO IPV6 E ANÁLISE DE DESEMPENHO DO IPSEC SOBRE OS PROTOCOLOS IPV4 E IPV6.** Disponível em: < ieeexplore.ieee.org > Acesso em: agosto de 2015.

Santos, Marcos Victor Boni de Vasconcelos. **Análise de Desempenho do Tráfego da informação de uma Simulação VPN Com o Conjunto de Protocolos IPSec.** Disponível em: < ieeexplore.ieee.org > Acesso em: agosto de 2015.

WOJCIK, EDUARDO. **ANÁLISE E SIMULAÇÃO DE VPN COM IPSEC EM ROTEADORES CISCO.** Disponível em: < ieeexplore.ieee.org > Acesso em: agosto de 2015.